

BỘ CÔNG AN

NHÀ XUẤT BẢN
CHÍNH TRỊ QUỐC GIA SỰ THẬT

BẢO ĐẢM CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG



TẬP 1

KỸ YẾU HỘI THẢO KHOA HỌC CẤP QUỐC GIA



NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT

Chịu trách nhiệm xuất bản
GIÁM ĐỐC - TỔNG BIÊN TẬP
PGS.TS. PHẠM MINH TUẤN

Chịu trách nhiệm nội dung
PHÓ GIÁM ĐỐC - PHÓ TỔNG BIÊN TẬP
ThS. NGUYỄN HOÀI ANH

| | |
|--------------------|--|
| Biên tập nội dung: | TS. HOÀNG MẠNH THẮNG ThS. PHẠM THỊ NGỌC BÍCH TS. VŨ THỊ HƯƠNG ThS. VŨ QUANG HUY |
| Trình bày bìa: | ĐƯỜNG HỒNG MAI |
| Chế bản vi tính: | NGUYỄN THỊ HẰNG |
| Sửa bản in: | TẠ THU THỦY |
| Đọc sách mẫu: | VŨ QUANG HUY |

ăng ký m "j q ej "xuất bản số: 6292-2021/CXBIPH/3/72/CTQG.
Quyết định xuất bản số: : 2-QĐ/NXBCTQG, ngày 24/3/2021.
Mã số ISBN: 978-604-57-9498/: 0
In xong và nộp lưu chiểu tháng 14 năm 2021.

BẢO ĐẢM
CHỦ QUYỀN QUỐC GIA
TRÊN KHÔNG GIAN MẠNG

TẬP 1

KỶ YẾU HỘI THẢO KHOA HỌC CẤP QUỐC GIA

BỘ CÔNG AN

**NHÀ XUẤT BẢN
CHÍNH TRỊ QUỐC GIA SỰ THẬT**



BẢO ĐẢM CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG

TẬP 1

KỶ YẾU HỘI THẢO KHOA HỌC CẤP QUỐC GIA

**NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT
Hà Nội - 2021**

BAN CHỈ ĐẠO HỘI THẢO

| | |
|-------------------------------|---|
| Đại tướng, GS.TS. TÔ LÂM | Ủy viên Bộ Chính trị, Bí thư Đảng ủy Công an Trung ương, Bộ trưởng Bộ Công an |
| Đồng chí NGUYỄN TRỌNG NGHĨA | Bí thư Trung ương Đảng, Trưởng Ban Tuyên giáo Trung ương |
| Thiếu tướng, TS. LÊ QUỐC HÙNG | Ủy viên Trung ương Đảng, Thứ trưởng Bộ Công an |
| PGS.TS. PHẠM MINH TUẤN | Giám đốc - Tổng Biên tập Nhà xuất bản Chính trị quốc gia Sự thật |

BAN TỔ CHỨC HỘI THẢO

Thiếu tướng, TS. LÊ QUỐC HÙNG

| | |
|------------------------------|-----------------------------|
| Trung tướng, TS. ĐỖ LÊ CHI | Đồng chí PHẠM THỊ THINH |
| Thượng tá NGUYỄN QUANG THẮNG | Đồng chí NGUYỄN HOÀI ANH |
| Thiếu tướng VŨ HỮU TÀI | Đồng chí HOÀNG MẠNH THẮNG |
| Đại tá NGUYỄN NGỌC CƯỜNG | Đồng chí PHẠM THỊ NGỌC BÍCH |
| Đại tá, TS. BÙI ANH TUẤN | Đồng chí NGUYỄN HỮU VIỆT |
| Thượng tá PHẠM VĂN DINH | Đồng chí DƯƠNG NHẬT HUY |
| Trung tá NGUYỄN VIỆT HÙNG | Đồng chí TRẦN QUỐC THẮNG |

LỜI NHÀ XUẤT BẢN

Thế giới hiện nay đang chứng kiến sự phát triển mạnh mẽ của Cách mạng công nghiệp lần thứ tư, đặc biệt là công nghệ thông tin, internet đã tạo ra một không gian chiến lược mới - “không gian mạng”. Với những đặc tính như tốc độ truyền tải, tìm kiếm thông tin nhanh, lưu trữ thông tin khổng lồ; tính liên kết cộng đồng, không biên giới, tính đa phương tiện, tương tác rất cao, không gian mạng đã trở thành là một bộ phận cấu thành của xã hội, bao trùm mọi mặt đời sống xã hội, mang lại những thời cơ, vận hội mới để các quốc gia, dân tộc hợp tác và phát triển. Tuy nhiên, không gian mạng cũng ẩn chứa rất nhiều khó khăn, thách thức, trong đó có thách thức về bảo đảm an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng.

Trước tình hình đó, Đảng và Nhà nước đã ban hành nhiều chủ trương, chính sách và biện pháp nhằm bảo đảm an toàn, an ninh thông tin mạng, góp phần quan trọng bảo đảm chủ quyền quốc gia trên không gian mạng. Đảng ta khẳng định: Chủ quyền trên không gian mạng là bộ phận quan trọng của chủ quyền quốc gia, bảo đảm chủ quyền quốc gia trên không gian mạng là nhiệm vụ cấp bách, lâu dài của cả hệ thống chính trị, đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý của Nhà nước; là yếu tố then chốt hình thành không gian mạng quốc gia an toàn và ổn định, tạo bước đột phá trong xây dựng, bảo vệ Tổ quốc Việt Nam xã hội

chủ nghĩa. Bảo đảm chủ quyền quốc gia trên không gian mạng là 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; bảo đảm 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. Chủ động phòng vệ, sẵn sàng đáp trả hợp pháp các mối đe dọa, bảo vệ vững chắc chủ quyền, an ninh quốc gia trên không gian mạng và xây dựng lực lượng bảo vệ chủ quyền quốc gia trên không gian mạng chính quy, tinh nhuệ và hiện đại. Ứng dụng công nghệ thông tin trong tất cả các lĩnh vực phải gắn với bảo đảm an toàn, an ninh thông tin, bảo vệ chủ quyền quốc gia trên không gian mạng. Huy động sức mạnh mọi nguồn lực của hệ thống chính trị và toàn xã hội, tạo thế trận quốc phòng toàn dân gắn với thế trận an ninh nhân dân để bảo vệ chủ quyền quốc gia trên không gian mạng. Trong đó, chú trọng nâng cao nhận thức toàn diện về chủ quyền quốc gia và bảo vệ chủ quyền quốc gia trên không gian mạng trong tình hình mới là vấn đề hết sức quan trọng nhằm khơi dậy tinh thần yêu nước, ý thức tự tôn, lòng tự hào dân tộc, đấu tranh bảo vệ vững chắc chủ quyền quốc gia không gian mạng trong kỷ nguyên thông tin và Cách mạng công nghiệp lần thứ tư.

Để quán triệt sự lãnh đạo, chỉ đạo của Đảng, đặc biệt là những yêu cầu mới đặt ra đối với công tác bảo đảm an ninh quốc gia được nhấn mạnh trong các văn kiện Đại hội đại biểu toàn quốc lần thứ XIII của Đảng; làm rõ hơn những vấn đề chung về không gian mạng và bảo đảm chủ quyền quốc gia

trên không gian mạng; đánh giá thực trạng của hoạt động sử dụng không gian mạng trong bảo vệ an ninh quốc gia hiện nay; rút ra bài học kinh nghiệm, phương hướng, giải pháp và khuyến nghị nhằm phát huy vai trò của nhân dân, của các lực lượng nòng cốt trong bảo đảm chủ quyền quốc gia trên không gian mạng, từ đó góp phần nâng cao hiệu quả xây dựng thể trận an ninh nhân dân trên không gian mạng, Nhà xuất bản Chính trị quốc gia Sự thật xuất bản cuốn sách ***Bảo đảm chủ quyền quốc gia trên không gian mạng (Kỷ yếu Hội thảo khoa học cấp quốc gia)***.

Nội dung cuốn sách tập hợp các bài tham luận tại Hội thảo khoa học cấp quốc gia *Bảo đảm chủ quyền quốc gia trên không gian mạng* do Nhà xuất bản Chính trị quốc gia Sự thật và Bộ Công an phối hợp tổ chức.

Xin giới thiệu cuốn sách với bạn đọc.

Tháng 11 năm 2021

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT

QUAN ĐIỂM CỦA ĐẢNG VÀ NHÀ NƯỚC VỀ BẢO VỆ CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG VÀ BẢO ĐẢM AN NINH MẠNG

Đồng chí NGUYỄN TRỌNG NGHĨA*

Sự phát triển mạnh mẽ của internet, mạng xã hội là xu thế khách quan, tất yếu, đã và đang đóng góp quan trọng đối với sự phát triển của các lĩnh vực kinh tế, văn hóa, xã hội, quốc phòng, an ninh, đối ngoại của từng quốc gia, dân tộc trên thế giới. Nhận thức và nắm bắt đúng đắn, kịp thời xu thế của thời đại, nhất là những lợi ích của internet, mạng xã hội mang lại, ngay từ sớm (năm 1997), Đảng và Nhà nước ta đã có chủ trương phát triển internet ở Việt Nam, đồng thời ban hành nhiều chủ trương, chính sách lãnh đạo, chỉ đạo, quản lý, nhờ đó internet và mạng xã hội đã phát triển nhanh chóng, ngày càng thâm nhập sâu rộng vào mọi mặt đời sống xã hội, đóng góp quan trọng vào thành tựu của 35 năm thực hiện công cuộc đổi mới.

Mặt khác, internet, mạng xã hội cũng tồn tại những mối đe dọa về an ninh mà rất nhiều nước trên thế giới, kể cả những nước phát triển luôn đặc biệt quan tâm. Đứng trước

* Bí thư Trung ương Đảng, Trưởng Ban Tuyên giáo Trung ương.

thách thức này, các nước đã áp dụng chiến lược an ninh mạng và những giải pháp, biện pháp phù hợp để bảo vệ sự an toàn trước nguy cơ mất an ninh trên không gian mạng. Ở Việt Nam, trong thời gian gần đây, nhiều cuộc tấn công mạng và những hành vi phá hoại an ninh chính trị, an ninh kinh tế, an ninh văn hóa, trật tự, an toàn xã hội, vi phạm pháp luật trên không gian mạng ngày càng gia tăng về số vụ, thủ đoạn tinh vi và tính chất phức tạp, mức độ nguy hiểm, gây thiệt hại nghiêm trọng tới các lĩnh vực của đời sống kinh tế - xã hội. Thời gian qua, tại Việt Nam đã phát hiện trên 3.000 trang web, blog, tài khoản mạng xã hội và gần 100 hội, nhóm trên mạng xã hội facebook, thường xuyên đăng tải thông tin chống Đảng, Nhà nước, kích động gây rối an ninh, trật tự. Những hội, nhóm và tài khoản mạng xã hội của các thế lực thù địch, phản động, cơ hội chính trị, tội phạm mạng đang triệt để lợi dụng không gian mạng để tiến hành các hoạt động xâm phạm an ninh quốc gia, tuyên truyền chống phá Đảng, Nhà nước, kích động biểu tình, bạo loạn, thực hiện “cách mạng màu”, “cách mạng đường phố”, xâm phạm chủ quyền quốc gia trên không gian mạng.

Nhằm kịp thời kiểm soát các hoạt động lợi dụng không gian mạng để tuyên truyền, phát tán các quan điểm thù địch, sai trái chống phá Đảng, Nhà nước, kích động tập trung đông người bất hợp pháp, gây rối an ninh, trật tự, trước, trong và sau Đại hội lần thứ XIII của Đảng, các lực lượng chuyên trách đã gỡ bỏ hàng trăm trang web, hàng nghìn hội, nhóm, tài khoản mạng xã hội phát tán thông tin xuyên tạc, bôi nhọ lãnh đạo Đảng, Nhà nước; xuyên tạc, bịa đặt về công tác nhân sự của Đảng; gỡ bỏ bài viết và xử phạt hành chính các

đối tượng lợi dụng mối quan tâm của cộng đồng về công tác phòng, chống đại dịch Covid-19 nhằm xuyên tạc những nỗ lực của Đảng, Chính phủ và toàn hệ thống chính trị trong công tác phòng, chống dịch bệnh và đánh cắp thông tin, dữ liệu cá nhân của người dùng. Trong thời gian đại dịch Covid-19 đang bùng phát hiện nay, không gian mạng tiếp tục là môi trường chủ yếu để các thế lực thù địch, đối tượng phản động, chống đối tán phát thông tin bịa đặt về tình hình dịch bệnh, xuyên tạc, đả kích sự chỉ đạo, điều hành trong phòng, chống dịch bệnh của Chính phủ và chính quyền các cấp. Những hoạt động đó đã tác động tiêu cực tới tư tưởng, nhận thức của một bộ phận cán bộ, đảng viên và nhân dân; gây tâm lý hoang mang, hoài nghi, làm suy giảm lòng tin vào chế độ xã hội chủ nghĩa và vai trò lãnh đạo của Đảng, sự quản lý của Nhà nước.

Để bảo đảm an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng, Đảng và Nhà nước ta đã ban hành nhiều chủ trương, chính sách, pháp luật¹, trong đó Nghị quyết

1. Nghị quyết số 13-NQ/TW, ngày 16/01/2012 tại Hội nghị Trung ương 4 khóa XI *Về xây dựng hệ thống kết cấu hạ tầng đồng bộ nhằm đưa nước ta cơ bản trở thành nước công nghiệp theo hướng hiện đại vào năm 2020*; Nghị quyết số 28-NQ/TW, ngày 25/10/2013 tại Hội nghị Trung ương 8 khóa XI *Về chiến lược bảo vệ Tổ quốc trong tình hình mới*; Chỉ thị số 46-CT/TW, ngày 22/6/2015 của Bộ Chính trị khóa XI *Về tăng cường sự lãnh đạo của Đảng đối với công tác bảo đảm an ninh, trật tự trong tình hình mới*; Chỉ thị số 28-CT/TW, ngày 16/9/2013 của Ban Bí thư khóa XI *Về tăng cường công tác bảo đảm an toàn thông tin mạng trong tình hình mới*; Chỉ thị số 15/CT-TTg, ngày 17/6/2014 của Thủ tướng Chính phủ *Về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới*; Chỉ thị số 30-CT/TW, ngày 25/12/2013 của Bộ Chính trị

của Bộ Chính trị về Chiến lược an ninh mạng quốc gia; Chiến lược bảo vệ Tổ quốc trên không gian mạng; một số chủ trương, chính sách chủ động tham gia Cách mạng công nghiệp lần thứ tư; Luật an ninh mạng; Luật an toàn thông tin mạng, mang tính chỉ đạo chiến lược cho công cuộc bảo đảm an ninh mạng, bảo vệ chủ quyền quốc gia trên không gian mạng, “bước đầu hình thành hệ thống pháp luật và cơ sở vật chất cho việc bảo đảm an ninh mạng, an toàn thông tin quốc gia, không gian mạng quốc gia”¹.

Quan điểm của Đảng, Nhà nước về an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng thể hiện sự nhất quán về nguyên tắc Đảng lãnh đạo tuyệt đối, trực tiếp về mọi mặt đối với sự nghiệp bảo vệ Tổ quốc, đồng thời thể hiện bước phát triển về tư duy, sự đổi mới về nhận thức của Đảng đối với công cuộc bảo vệ đất nước trong tình hình

khóa XI Về phát triển và tăng cường quản lý báo chí điện tử, mạng xã hội và các loại hình truyền thông khác trên internet; Nghị định số 101/2016/NĐ-CP, ngày 01/7/2016 của Chính phủ Quy định chi tiết trách nhiệm thực hiện và các biện pháp ngăn chặn hoạt động sử dụng không gian mạng để khủng bố; Nghị định số 66/2017/NĐ-CP, ngày 19/5/2017 của Chính phủ Quy định điều kiện kinh doanh thiết bị, phần mềm nguy trang dùng để ghi âm, ghi hình, định vị; Luật an ninh mạng năm 2018; Nghị quyết số 29-NQ/TW, ngày 25/7/2018 của Bộ Chính trị khóa XII 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 35- NQ/TW, ngày 22/10/2018 của Bộ Chính trị khóa XII Về tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới...

1. Đảng Cộng sản Việt Nam: Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.I, tr.68.

không gian mạng phát triển đa chiều và xuyên quốc gia. Quan điểm chỉ đạo của Đảng, Nhà nước về vấn đề này được thể hiện rõ trong nhiều văn bản, nhất là trong các nghị quyết của Bộ Chính trị như: Nghị quyết số 29-NQ/TW về *Chiến lược bảo vệ Tổ quốc trên không gian mạng*, Nghị quyết số 30-NQ/TW về *Chiến lược an ninh mạng quốc gia*, Nghị quyết số 35-NQ/TW *Về tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới*,... như sau:

Một là, an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng là nhiệm vụ trọng tâm, chiến lược của toàn Đảng, toàn dân, toàn quân và cả hệ thống chính trị, dưới sự lãnh đạo của Đảng, sự quản lý của Nhà nước.

Không gian mạng là vùng lãnh thổ đặc biệt của quốc gia, được xác định bằng phạm vi không gian do Nhà nước quản lý, kiểm soát bằng chính sách, pháp luật và năng lực công nghệ có vai trò quan trọng như những vùng lãnh thổ khác (đất liền, hải đảo, vùng biển, vùng trời). Với những đặc tính vượt trội như tốc độ truyền tải, tìm kiếm thông tin nhanh, khả năng lưu trữ thông tin lớn, liên kết cộng đồng không giới hạn về không gian, thời gian, không gian mạng đang là môi trường “lý tưởng” cho các hoạt động xâm phạm an ninh quốc gia, phát tán tin giả, thông tin sai sự thật, kích động biểu tình, gây rối trật tự, an toàn xã hội hòng thực hiện hoạt động “diễn biến hòa bình”, “tự diễn biến”, “tự chuyển hóa”, “phi chính trị hóa” lực lượng vũ trang nhân dân. Hoạt động tội phạm và những hành vi vi phạm pháp luật trên không gian mạng ngày càng gia tăng về số vụ, thủ đoạn và tính chất, mức độ nguy hiểm, gây thiệt hại nghiêm trọng

trên các lĩnh vực của đời sống xã hội. Việt Nam thường xuyên nằm trong top 3 quốc gia bị tấn công mạng nhiều nhất trong những năm 2018, 2019, 2020 (theo số liệu thống kê của Kaspersky security network)¹ và là quốc gia có tỷ lệ gặp phải mã độc tống tiền cao nhất châu Á - Thái Bình Dương năm 2019 (theo báo cáo ngày 24/6/2020 của Microsoft, về các mối đe dọa bảo mật)².

Chính vì vậy, bảo đảm an ninh mạng, bảo vệ chủ quyền quốc gia trên không gian mạng là nhiệm vụ trọng yếu, cấp bách cần phải triển khai đồng bộ, quyết liệt, thường xuyên, liên tục, bền bỉ trong mọi tình huống, mọi hoàn cảnh. Toàn Đảng, toàn dân, toàn quân và cả hệ thống chính trị đồng sức, đồng lòng quyết tâm giữ vững an ninh quốc gia trên không gian mạng, bảo đảm trật tự, an toàn xã hội, phòng ngừa, phát hiện, ngăn chặn, xử lý hiệu quả các hành vi xâm phạm an ninh mạng quốc gia; xác lập, quản lý và bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng, góp phần bảo vệ độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc và lợi ích quốc gia - dân tộc, giữ vững môi trường hòa bình, ổn định để xây dựng và phát triển đất nước nhanh, bền vững. Luôn nêu cao cảnh giác, làm thất bại mọi âm mưu, hoạt động chống phá, xâm phạm chủ quyền, lợi ích quốc gia - dân tộc trên không gian mạng; không để bị động, bất ngờ trong mọi tình huống.

1. Xem <https://thanhnien.vn/cong-nghe/viet-nam-nam-trong-top-3-quoc-gia-bi-tan-cong-mang-nhieu-nhat-1058542.html>.

2. Xem <https://news.microsoft.com/vi-vn/2020/06/24/bao-cao-cua-microsoft-viet-nam-la-quoc-gia-co-ty-le-nhiem-ma-doc-tong-tien-caonhat-chau-a-thai-binh-duong-nam-2019>.

Hai là, kết hợp có hiệu quả thực hiện nhiệm vụ quốc phòng, an ninh với nhiệm vụ phát triển kinh tế, văn hóa, xã hội trong từng chiến lược, quy hoạch, kế hoạch phát triển kinh tế - xã hội; giữa triển khai thực hiện các chiến lược quốc phòng, an ninh.

Cần nhận thức sâu sắc mối quan hệ biện chứng giữa đổi mới, ổn định và phát triển. Để kinh tế, văn hóa, xã hội của đất nước phát triển cần có môi trường chính trị, xã hội ổn định, an ninh trật tự được bảo đảm và ngược lại, những thành tựu của sự phát triển kinh tế - xã hội mang lại điều kiện để bảo đảm cho sự ổn định chính trị, xã hội. Vì vậy, trong thực hiện nhiệm vụ phát triển kinh tế, văn hóa, xã hội phải bảo đảm yêu cầu về giữ vững quốc phòng, an ninh, trong đó có an ninh mạng. Trong triển khai thực hiện Chiến lược bảo vệ Tổ quốc, Chiến lược quốc phòng, Chiến lược quân sự, Chiến lược bảo vệ an ninh quốc gia, Chiến lược bảo vệ biên giới quốc gia và Chiến lược bảo vệ Tổ quốc trên không gian mạng cần có sự lãnh đạo, chỉ đạo thống nhất, đồng bộ, hiệu quả.

Ba là, nhiệm vụ bảo đảm an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng là bảo vệ Đảng, Cương lĩnh chính trị, đường lối của Đảng; bảo vệ nhân dân¹; Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam; bảo vệ công cuộc đổi mới, công nghiệp hóa, hiện đại hóa đất nước và hội nhập quốc tế; bảo vệ lợi ích quốc gia - dân tộc; giữ gìn môi trường hòa bình, ổn định để phát triển đất nước.

1. Bảo vệ các quyền con người, quyền công dân về chính trị, dân sự, kinh tế, văn hóa, xã hội theo Hiến pháp năm 2013. Chú trọng an ninh, an toàn là một trong những yếu tố hàng đầu trong cuộc sống của người dân.

Bốn là, phát huy mạnh mẽ “thế trận lòng dân” góp phần xây dựng và củng cố vững chắc thế trận quốc phòng toàn dân và thế trận an ninh nhân dân trên không gian mạng.

“Nhân dân là trung tâm, là chủ thể của công cuộc đổi mới, xây dựng và bảo vệ Tổ quốc”¹ nên việc xây dựng “thế trận lòng dân” vững chắc từ cơ sở là yêu cầu cấp thiết trong công cuộc bảo vệ Tổ quốc trên bất kỳ vùng lãnh thổ nào. Kế thừa và phát huy truyền thống dân tộc trong quá trình lãnh đạo cách mạng Việt Nam, Đảng ta luôn coi trọng, vun đắp cho sự đoàn kết, thống nhất trong Đảng và khối đại đoàn kết toàn dân tộc, củng cố sự đồng thuận và lòng tin của nhân dân đối với Đảng, Nhà nước trong mọi lĩnh vực và trên mọi mặt trận. Công cuộc bảo đảm an ninh mạng, bảo vệ chủ quyền quốc gia trên không gian mạng cũng không nằm ngoài quỹ đạo đó. Để củng cố và phát huy sức mạnh của “thế trận lòng dân” trên không gian mạng cần quy tụ và phát huy sức mạnh nội sinh của mỗi con người, mỗi tập thể và của cả dân tộc; tuyên truyền, giáo dục, định hướng cho mỗi cá nhân hiểu được lợi ích cũng như tác hại tiềm ẩn trên không gian mạng, nâng cao tinh thần cảnh giác, chủ động phòng tránh, nâng cao sức đề kháng và khả năng tự xử lý tình huống khi bị tấn công trên không gian mạng. Mỗi tài khoản trên không gian mạng là một chiến sĩ và mỗi bài viết tuyên truyền, đấu tranh phản bác là những vũ khí sắc bén tấn công trực diện vào thế lực thù địch, phản động, cơ hội chính trị.

1. Đảng Cộng sản Việt Nam: Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII, Sdd, t.I, tr.27-28.

“Thế trận lòng dân” là nền tảng gốc rễ để xây dựng thế trận quốc phòng toàn dân và thế trận an ninh nhân dân vững chắc. Thực hiện lời dạy của Chủ tịch Hồ Chí Minh tại Lễ thành lập Công an nhân dân vũ trang (nay là Bộ đội Biên phòng) vào tháng 3/1959: “Công an và Quân đội là hai cánh tay của nhân dân, của Đảng, của Chính phủ, của vô sản chuyên chính. Vì vậy, càng phải đoàn kết chặt chẽ với nhau, giúp đỡ lẫn nhau, ra sức phát triển ưu điểm, khắc phục những tư tưởng không đúng”¹. Trên thực tế, lực lượng Quân đội nhân dân và Công an nhân dân đã phối hợp chặt chẽ với nhau xây dựng, bố trí lực lượng, tiềm lực trên không gian mạng, vì vậy đã nâng cao hiệu quả công tác bảo đảm chủ quyền quốc gia trên không gian mạng và bảo đảm an ninh mạng.

Năm là, xây dựng lực lượng chuyên trách bảo vệ an ninh mạng, bảo vệ chủ quyền quốc gia trên không gian mạng chính quy, tinh nhuệ, hiện đại.

Đại hội lần thứ XIII của Đảng đã chỉ rõ: “Tiếp tục xây dựng Quân đội nhân dân, Công an nhân dân cách mạng, chính quy, tinh nhuệ, từng bước hiện đại, ưu tiên hiện đại hóa một số quân chủng, binh chủng, lực lượng: hải quân, phòng không - không quân, tác chiến điện tử, trinh sát kỹ thuật,... an ninh mạng và đấu tranh phòng, chống tội phạm công nghệ cao”². Lực lượng chuyên trách bảo vệ an ninh

1. Hồ Chí Minh: *Toàn tập*, Nxb. Chính trị quốc gia, Hà Nội, 2011, t.12, tr.153.

2. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội Đại biểu toàn quốc lần thứ XIII, Sdd*, t.I, tr.276-277.

mạng, bảo vệ chủ quyền quốc gia trên không gian mạng được bố trí tại Bộ Quốc phòng, Bộ Công an, các bộ, ngành, Ủy ban nhân dân cấp tỉnh, các cơ quan, tổ chức quản lý hệ thống thông tin về an ninh, chủ quyền quốc gia. Đây là một trong số những lực lượng đang được Đảng, Nhà nước quan tâm, ưu tiên nguồn lực để xây dựng và đào tạo tiến nhanh lên “hiện đại”, làm chủ khoa học công nghệ, thích ứng kịp thời, nhạy bén với những tình huống bất ngờ, thủ đoạn tinh vi, chủ động đấu tranh có hiệu quả.

Để công tác bảo vệ chủ quyền quốc gia trên không gian mạng đạt hiệu quả, lực lượng chuyên trách tại các đơn vị phải chủ động liên kết, phối hợp chặt chẽ với nhau trong hành động, tác chiến, thực hiện nhiệm vụ theo sự phân công, phân nhiệm rõ ràng đến từng cấp, từng lực lượng. Theo đó, bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội theo chức năng, nhiệm vụ của Bộ Công an; nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng theo chức năng, nhiệm vụ của Bộ Quốc phòng; bảo đảm an toàn thông tin mạng theo chức năng, nhiệm vụ của Bộ Thông tin và Truyền thông và hệ thống Tuyên giáo các cấp là nòng cốt trong bảo vệ nền tảng tư tưởng của Đảng, đấu tranh, phản bác các quan điểm sai trái, thù địch.

Sáu là, đẩy mạnh công tác đối ngoại trong bảo đảm an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng.

An ninh mạng là vấn đề toàn cầu, tác động trực tiếp đến hòa bình, ổn định và phát triển của mỗi quốc gia. Vì vậy, việc tăng cường mở rộng hợp tác quốc tế trên không gian mạng là hết sức cần thiết, tạo vành đai an ninh bảo vệ

Tổ quốc từ sớm, từ xa. Việt Nam ủng hộ và sẵn sàng hợp tác với các đối tác nhằm xây dựng một môi trường không gian mạng hòa bình, ổn định, an toàn, vì người dân và phát triển bền vững¹. Bên cạnh đó, chú trọng vận dụng linh hoạt, đúng đắn quan điểm của Đảng, Nhà nước về “đối tác, đối tượng” trên không gian mạng, tranh thủ “đối tác” để thiết lập quan hệ quốc tế rộng rãi, đề cao tinh thần chủ động phòng ngừa, phát hiện sớm và xử lý kịp thời các hoạt động chống phá của “đối tượng”.

Bây là, kết hợp chặt chẽ giữa nhiệm vụ chuyển đổi số quốc gia với nhiệm vụ bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội, bảo vệ chủ quyền quốc gia trên không gian mạng.

Phát triển kinh tế số là một trong những xu thế lớn trên thế giới được nhiều quốc gia nghiên cứu, ứng dụng. Tại Việt Nam, xu hướng số hóa được triển khai mạnh mẽ trong mọi lĩnh vực hướng tới mục tiêu chuyển đổi số quốc gia, phát triển kinh tế số, xã hội số. Bước đầu xây dựng và phát triển hạ tầng thông tin viễn thông, đẩy mạnh nghiên cứu, chuyển đổi, ứng dụng tiến bộ khoa học công nghệ, đặc biệt là những thành tựu của Cách mạng công nghiệp lần thứ tư tạo nền tảng thúc đẩy nhanh quá trình chuyển đổi số. Đầu tư, nghiên cứu, ứng dụng công nghệ thông tin trong các lĩnh vực gắn liền với đầu tư cho công tác an ninh mạng, bảo vệ Tổ quốc trên không gian mạng. Phát huy ý chí tự lực, tự cường, phát huy mạnh mẽ nhân tố

1. Xem <https://dangcongsan.vn/doi-ngoai/viet-nam-chu-dong-tich-cuc-tham-gia-cac-co-che-an-ninh-mang-584263.html>.

con người, lấy con người là trung tâm, là chủ thể, là nguồn lực chính để xây dựng và sớm hình thành ngành công nghệ mạng Việt Nam. Các doanh nghiệp Việt Nam từng bước làm chủ về công nghệ, thiết kế, chế tạo các sản phẩm công nghệ mang thương hiệu “Việt Nam”, hạn chế tối đa sự phụ thuộc vào các sản phẩm công nghệ nước ngoài.

Kinh tế số, xã hội số phát triển mạnh mẽ đặt ra hai vấn đề: Kinh tế phát triển đồng nghĩa với việc sẽ có sự đổi mới, cải tiến về kỹ thuật, công nghệ là tiền đề quan trọng để đổi mới công nghệ an ninh mạng, góp phần nâng cao năng lực xử lý tình huống, phát hiện đấu tranh với các thế lực thù địch trên không gian mạng. Song song với những lợi ích trên, sự phát triển nhanh chóng của kinh tế số, xã hội số làm gia tăng nguy cơ xâm phạm hệ thống an ninh mạng, xâm phạm chủ quyền quốc gia trên không gian mạng. Vì vậy, chuyển đổi số quốc gia, phát triển kinh tế số, xã hội số phải luôn đi liền với bảo đảm an ninh mạng, bảo vệ chủ quyền quốc gia trên không gian mạng. Mọi hoạt động kinh tế trong thời đại Cách mạng công nghiệp lần thứ tư phải tuyệt đối tuân thủ luật pháp quốc tế, luật pháp Việt Nam hướng tới mục tiêu phát triển đất nước nhanh, bền vững.

Trong những năm qua, dưới sự lãnh đạo, chỉ đạo của Đảng, sự quản lý thống nhất của Nhà nước, sự vào cuộc quyết liệt của các ban, bộ, ngành, địa phương và đặc biệt là sự tích cực, chủ động trong vai trò nòng cốt của lực lượng chuyên trách, công tác bảo đảm an toàn, an ninh mạng được giữ vững góp phần quan trọng bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng. Kết cấu hạ tầng viễn thông,

internet được xây dựng đồng bộ, công nghệ thông tin được ứng dụng rộng rãi từ Trung ương đến địa phương; kinh tế số được hình thành và phát triển nhanh dần trở thành bộ phận quan trọng của nền kinh tế.

Tuy nhiên, tình hình mất an toàn thông tin mạng tại một số nơi còn diễn ra phức tạp; công tác bảo đảm an ninh mạng, bảo vệ chủ quyền quốc gia trên không gian mạng còn nhiều vấn đề đặt ra: Đấu tranh bảo vệ chủ quyền quốc gia, toàn vẹn lãnh thổ còn nhiều thách thức¹; công tác nắm tình hình, dự báo chiến lược về quốc phòng, an ninh có lúc chưa thật chủ động; công tác quản lý, bảo đảm an toàn thông tin, an ninh mạng còn hạn chế². Bên cạnh đó, việc chủ động, tích cực tham gia Cách mạng công nghiệp lần thứ tư là yêu cầu tất yếu khách quan nhằm mang lại cơ hội cho phát triển kinh tế - xã hội, đồng thời cũng đặt ra những thách thức với công tác bảo đảm an toàn, an ninh mạng. Với xu hướng tự động hóa, internet kết nối vạn vật, hoạt động tấn công mạng của các thế lực thù địch, tội phạm mạng sẽ ngày càng gia tăng, không chỉ dừng lại ở mục đích thu thập thông tin bí mật, mà còn phá hoại cơ sở dữ liệu, hạ tầng công nghệ thông tin, thậm chí trở thành những loại vũ khí nguy hiểm, có sức tàn phá nặng nề, xâm phạm đến chủ quyền, lợi ích quốc gia - dân tộc trên không gian mạng.

Trong thời gian tới, để tiếp tục thực hiện có hiệu quả quan điểm của Đảng, Nhà nước về bảo đảm an ninh mạng,

1, 2. Xem Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Sdd, t.I, tr.32, 87-88.

bảo vệ chủ quyền quốc gia trên không gian mạng, cần triển khai một số nhiệm vụ cấp bách sau:

Thứ nhất, tăng cường sự lãnh đạo của Đảng, nâng cao hiệu lực quản lý của Nhà nước đối với nhiệm vụ bảo đảm an ninh mạng và bảo vệ Tổ quốc trên không gian mạng. Quy định rõ trách nhiệm của cấp ủy và người đứng đầu cơ quan, tổ chức, chính quyền các cấp trong tổ chức triển khai và thực hiện nhiệm vụ bảo đảm an toàn, an ninh mạng, bảo vệ Tổ quốc trên không gian mạng.

Thứ hai, tiếp tục hoàn thiện chính sách, pháp luật và nâng cao hiệu lực, hiệu quả quản lý nhà nước về công nghệ thông tin, truyền thông và an ninh mạng; quản lý chặt chẽ các hoạt động cung cấp, sử dụng dịch vụ viễn thông, internet tại Việt Nam; nâng cao hiệu quả phối hợp giữa các ngành chức năng trong quản lý nhà nước về an ninh mạng. Xây dựng Bộ quy tắc ứng xử trên không gian mạng phù hợp với từng cơ quan, tổ chức, từng lĩnh vực; cơ chế trao đổi, chia sẻ thông tin giữa các cơ quan, đơn vị chủ quản hệ thống thông tin với các ban, ngành chức năng.

Thứ ba, kết hợp chặt chẽ, có hiệu quả công tác bảo đảm an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng với việc thực hiện các nhiệm vụ phát triển kinh tế, văn hóa, xã hội, quốc phòng, an ninh, đối ngoại và nhiệm vụ xây dựng, chỉnh đốn Đảng. Công tác bảo đảm an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng phải trực tiếp phục vụ việc triển khai thực hiện có hiệu quả các mục tiêu, chỉ tiêu, nhiệm vụ, giải pháp của Đại hội lần thứ XIII đề ra.

Thứ tư, tăng cường quản lý hoạt động báo chí, xuất bản, phát thanh, truyền hình, nhất là trang thông tin điện tử, báo điện tử theo quy định của pháp luật; kịp thời định hướng để báo chí tuyên truyền có hiệu quả, cung cấp thông tin chính thống đến cán bộ, đảng viên và nhân dân về các sự kiện phức tạp, nhạy cảm, nhất là các sự kiện được dư luận quan tâm. Xây dựng quy chuẩn văn hóa của những người đưa thông tin lên mạng, như không đưa tin thất thiệt, không rõ nguồn lên mạng, đồng thời, phải có chế tài đối với những người vi phạm, đưa tin thất thiệt, gây ảnh hưởng xấu đến cộng đồng, xã hội. Công tác thông tin, tuyên truyền phải “làm chủ” không gian mạng. Lực lượng tuyên giáo, các cơ quan truyền thông cần tăng cường truyền thông nâng cao nhận thức về an ninh mạng cho nhân dân; tăng cường thông tin chính thống, cổ vũ cái tốt, nhân rộng các điển hình theo phương châm “lấy cái đẹp dẹp cái xấu”; chủ động trong bảo vệ nền tảng tư tưởng của Đảng, kiên quyết đấu tranh phản bác thông tin xấu, độc, các quan điểm sai trái, thù địch trên không gian mạng.

Thứ năm, kiện toàn tổ chức, xây dựng và phát triển lực lượng chuyên trách an ninh mạng, bảo vệ chủ quyền quốc gia trên không gian mạng ngày càng tinh nhuệ, hiện đại, làm chủ thời cuộc, làm chủ công nghệ, chủ động ngăn ngừa các nguy cơ chiến tranh, xung đột từ sớm, từ xa; sẵn sàng đấu tranh bảo vệ chủ quyền quốc gia trên vùng lãnh thổ mới. Xây dựng cơ chế, chính sách thu hút, trọng dụng, đãi ngộ, phát triển đội ngũ chuyên gia giỏi, có phẩm chất đạo đức tốt làm việc trong các cơ quan, tổ chức bảo đảm an toàn, an ninh mạng.

Thứ sáu, tăng cường hợp tác quốc tế trên các lĩnh vực an toàn, an ninh mạng, tác chiến không gian mạng, tác chiến điện tử, công nghệ thông tin; tích cực tham gia các hoạt động duy trì hòa bình, ổn định và phát triển an ninh mạng của các tổ chức quốc tế, hướng tới xây dựng giải pháp toàn cầu đối với lĩnh vực an ninh mạng và chủ quyền quốc gia trên không gian mạng.

MỘT SỐ KINH NGHIỆM CỦA QUÂN ĐỘI VỀ CHỈ ĐẠO, TỔ CHỨC ĐẤU TRANH PHẢN BÁC CÁC QUAN ĐIỂM SAI TRÁI, THÙ ĐỊCH TRÊN KHÔNG GIAN MẠNG

Trung tướng TRỊNH VĂN QUYẾT*

Hiện nay, các thế lực thù địch, cơ hội chính trị và phản động đang triệt để lợi dụng không gian mạng để phát tán tài liệu, thông tin xấu, độc, các quan điểm sai trái, thù địch nhằm chống phá Đảng, Nhà nước và chế độ ta. Việc bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trên không gian mạng là nhiệm vụ rất quan trọng, cấp bách của toàn Đảng, toàn dân, toàn quân và của cả hệ thống chính trị, trong đó Quân đội nhân dân Việt Nam là một trong những lực lượng giữ vai trò quan trọng, nòng cốt.

Thực hiện âm mưu, hoạt động “diễn biến hòa bình”, thúc đẩy “tự diễn biến”, “tự chuyển hóa” trong nội bộ, “phi chính trị hóa” lực lượng vũ trang, các thế lực thù địch đang ráo riết thực hiện các chiêu trò chống phá Đảng, Nhà nước,

* Ủy viên Trung ương Đảng, Phó Chủ nhiệm Tổng cục Chính trị Quân đội nhân dân Việt Nam.

Quân đội và Công an. Chúng liên tục gia tăng tần suất phát tán tin, bài, video clip có nội dung xuyên tạc, phủ nhận chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước; chống phá đại hội đảng các cấp và Đại hội lần thứ XIII của Đảng, bầu cử đại biểu Quốc hội khóa XV và bầu cử đại biểu Hội đồng nhân dân các cấp nhiệm kỳ 2021 - 2026; bịa đặt, tung tin sai trái nhằm hạ thấp uy tín, danh dự của các đồng chí lãnh đạo Đảng, Nhà nước, Quân đội và Công an,...

Cùng với đó, chúng còn lợi dụng các vấn đề “dân chủ”, “nhân quyền”, “dân tộc”, “tôn giáo” để kích động tư tưởng hẹp hòi, tâm lý kỳ thị dân tộc, hướng đồng bào các dân tộc thiểu số thành lập “Vương quốc Mông tự trị” ở Tây Bắc, “Nhà nước Đêga Môngtanha” ở Tây Nguyên, “Vương quốc Khơme Crôm” ở Tây Nam Bộ; xúi giục đồng bào di cư tự do, vượt biên trái phép; thổi phồng những mâu thuẫn, thiếu sót trong tổ chức quản lý kinh tế, những vấn đề “nóng” của đời sống xã hội như công tác phòng, chống tham nhũng, tiêu cực, xét xử một số vụ án phức tạp, kéo dài, tranh chấp đất đai, khiếu kiện đông người, cứu hộ, cứu nạn, những khó khăn trong phòng, chống đại dịch Covid-19,... để xuyên tạc, kích động, gây mất lòng tin của nhân dân đối với Đảng, Nhà nước và chế độ.

Trước tình hình đó, Quân ủy Trung ương, Bộ Quốc phòng, Tổng cục Chính trị đã quán triệt sâu sắc và thực hiện nghiêm đường lối, chủ trương của Đảng, chính sách, pháp luật của Nhà nước, tập trung xây dựng, ban hành đồng bộ hệ thống văn bản lãnh đạo, chỉ đạo, hướng dẫn; tạo

cơ sở pháp lý để cấp ủy, tổ chức đảng, đội ngũ chính ủy, chính trị viên, chỉ huy các cấp triển khai thực hiện nhiệm vụ đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch một cách đồng bộ, thống nhất, hiệu quả. Toàn quân đã tiến hành thành lập, kiện toàn và phát huy hiệu quả hoạt động của các Ban chỉ đạo 35, cơ quan tham mưu, giúp việc và phân công cán bộ chuyên trách, kiêm nhiệm ở các cấp từ Quân ủy Trung ương đến sư đoàn và tương đương, bảo đảm phù hợp với quy mô tổ chức chỉ huy trong quân đội, thuận lợi cho hoạt động phối hợp, hiệp đồng, tổ chức đấu tranh. Nhờ đó, đã nâng cao chất lượng, hiệu quả các chuyên trang, chuyên mục về phòng, chống “diễn biến hòa bình”, “tự diễn biến”, “tự chuyển hóa”; “nhận diện sự thật”; chuyên mục quân sự, quốc phòng địa phương trên các phương tiện thông tin; các bài viết chuyên sâu của chuyên gia, các nhà khoa học, nhà báo, lực lượng cộng tác viên ở các cơ quan, đơn vị. Phối hợp chặt chẽ với các cơ quan, đơn vị trong và ngoài quân đội để đẩy nhanh ứng dụng thành tựu công nghệ thông tin và các phương tiện chuyên dùng vào phục vụ công tác tuyên truyền, đấu tranh phản bác các quan điểm sai trái, thù địch; gỡ bỏ các bài viết xuyên tạc sự thật, bôi đen, nói xấu Đảng, Nhà nước và chế độ ta.

Bằng những hoạt động thiết thực, hiệu quả, các lực lượng đấu tranh của quân đội đã chủ động, tích cực nghiên cứu, biên soạn tài liệu, viết tin, bài, comment (bình luận) chia sẻ thông tin tích cực, định hướng chính trị, dư luận xã hội, qua đó thể hiện rõ thái độ kiên quyết, kiên trì đấu

tranh, phản bác các quan điểm sai trái, thông tin xấu, độc của các thế lực thù địch, cơ hội chính trị và phản động. Các cơ quan, đơn vị đều có cách làm hay, biện pháp mới, sáng tạo nên phát huy tốt vai trò, hiệu quả đấu tranh trên các trang blog, “nhóm kín”, fanpage,... thu hút đông đảo bạn đọc truy cập, chia sẻ thông tin trên mạng xã hội. Các đơn vị kỹ thuật thường xuyên phối hợp chặt chẽ với các lực lượng nghiệp vụ giám sát hàng nghìn kênh báo điện tử trong và ngoài nước, các trang truyền thông điện tử, các tài khoản và nhóm phản động; vô hiệu hóa hàng nghìn webside, tài khoản Facebook, kênh YouTube có nội dung xấu, độc; chặn, lọc hàng vạn bài viết có nội dung xuyên tạc, kích động, chống phá Đảng, Nhà nước và chế độ ta. Đồng thời, làm tốt công tác biên tập, phát hành tin, bài, không để xảy ra tình trạng lộ, lọt tin mật, các tin, bài, hình ảnh chất lượng thấp đăng tải trên các báo in, báo điện tử.

Từ thực tiễn đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch, có thể khái quát một số kinh nghiệm của quân đội về chỉ đạo, tổ chức đấu tranh phản bác các quan điểm sai trái, thù địch trên không gian mạng như sau:

Một là, phát huy vai trò của cấp ủy, tổ chức đảng, Ban chỉ đạo 35 các cấp, tổ chức chỉ huy các cơ quan, đơn vị trong lãnh đạo, chỉ đạo và tổ chức đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch.

Hoạt động đấu tranh, phản bác những luận điệu, quan điểm sai trái, thù địch, cơ hội chính trị trên không gian mạng phải đặt dưới sự lãnh đạo, chỉ đạo của cấp ủy, tổ chức

đảng, Ban chỉ đạo 35 các cấp, sự quản lý, điều hành của người chỉ huy, chính ủy, chính trị viên và cơ quan chính trị. Để phát huy vai trò của các tổ chức, lực lượng này, Thường vụ Quân ủy Trung ương, Bộ Quốc phòng, Tổng cục Chính trị đã ban hành các nghị quyết, chỉ thị, đề án, kế hoạch lãnh đạo, chỉ đạo và hướng dẫn các cơ quan, đơn vị triển khai thực hiện đồng bộ, thống nhất các chủ trương, biện pháp phù hợp với tình hình thực tiễn. Trong quá trình thực hiện nhiệm vụ, cấp ủy, tổ chức đảng các cơ quan, đơn vị đã quán triệt sâu sắc và thực hiện nghiêm túc: Chiến lược quân sự, Chiến lược quốc phòng, Chiến lược bảo vệ Tổ quốc trên không gian mạng, Chiến lược bảo vệ biên giới quốc gia,... gắn với thực hiện Nghị quyết Trung ương 4 khóa XII¹; Chỉ thị số 05-CT/TW của Bộ Chính trị khóa XII²; Chỉ thị số 855-CT/QUTW của Thường vụ Quân ủy Trung ương³..., trong thực hiện Nghị quyết số 35-NQ/TW của Bộ Chính trị⁴; chú

1. Nghị quyết số 04-NQ/TW, ngày 30/10/2016 của Ban Chấp hành Trung ương Đảng khóa XII *Về tăng cường xây dựng, chỉnh đốn Đảng; ngăn chặn, đẩy lùi sự suy thoái về tư tưởng chính trị, đạo đức, lối sống, những biểu hiện “tự diễn biến”, “tự chuyển hóa” trong nội bộ.*

2. Chỉ thị số 05-CT/TW, ngày 15/5/2016 của Bộ Chính trị khóa XII *Về đẩy mạnh học tập và làm theo tư tưởng, đạo đức, phong cách Hồ Chí Minh.*

3. Chỉ thị số 855-CT/QUTW, ngày 12/8/2019 của Thường vụ Quân ủy Trung ương *Về đẩy mạnh thực hiện Cuộc vận động Phát huy truyền thống, cống hiến tài năng, xứng danh “Bộ đội Cụ Hồ” thời kỳ mới.*

4. Nghị quyết số 35-NQ/TW, ngày 22/10/2018 của Bộ Chính trị khóa XII *Về tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới.*

trọng giáo dục, tuyên truyền, nâng cao nhận thức cho cán bộ, đảng viên, chiến sĩ về chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước, nhiệm vụ xây dựng quân đội, củng cố quốc phòng, bảo vệ Tổ quốc; coi công tác đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch là nhiệm vụ chính trị trọng tâm, là trách nhiệm của cấp ủy, tổ chức đảng, của cán bộ, đảng viên, chiến sĩ.

Hàng năm, Ban chỉ đạo 35 các cấp và các lực lượng tham gia đấu tranh trong toàn quân xây dựng kế hoạch và chương trình hành động, xác định rõ nội dung, yêu cầu, thời gian thực hiện, trách nhiệm của cơ quan, đơn vị trong phối hợp đấu tranh, bảo đảm các hoạt động lãnh đạo, chỉ đạo, tổ chức triển khai thực hiện thống nhất, đồng bộ các chủ trương, biện pháp đấu tranh. Đội ngũ cán bộ, cơ quan tham mưu, giúp việc chủ động thực hiện tốt việc phân cấp, phân quyền, hoàn thành chức trách, nhiệm vụ được giao trong tổ chức thực hiện nhiệm vụ xây dựng lực lượng đấu tranh (*một người có thể tham gia nhiều việc nhưng một việc chỉ có một người chịu trách nhiệm*), khắc phục tình trạng chung chung, chồng chéo nhiệm vụ, thời gian thực hiện.

Hai là, quán triệt và thực hiện tốt phương châm: “Dự báo sớm, nhận diện đúng, phản ứng nhanh, đấu tranh kịp thời, hiệu quả”; kết hợp chặt chẽ các biện pháp, lấy “xây” để “chống”, lấy thông tin tích cực đẩy lùi thông tin tiêu cực.

Không gian mạng là môi trường kết nối, chia sẻ và tiếp nhận thông tin ngày càng trở nên phổ biến và mở rộng.

Những tác động của nó tới đời sống con người ngày càng rõ rệt, thể hiện trên cả hai phương diện tích cực và tiêu cực. Vì vậy, Ban chỉ đạo 35 các cấp luôn chủ động chỉ đạo, hướng dẫn công tác thông tin, định hướng tuyên truyền, nhất là trước các sự kiện được dư luận xã hội quan tâm; qua đó, bảo đảm thông tin nhanh, kịp thời, chính xác, không để các thế lực thù địch lợi dụng “khoảng trống” thông tin để chống phá Đảng, Nhà nước và chế độ. Đồng thời, các cơ quan, đơn vị trong quân đội giám sát chặt chẽ các báo điện tử, tài khoản facebook, nhóm phản động chống phá Đảng, Nhà nước, lực lượng vũ trang; website, blog, tài khoản đưa tin, hình ảnh giả mạo cán bộ quân đội, công an với dụng ý xấu, bài viết có nội dung xuyên tạc, kích động nhân dân, chia rẽ quân đội, công an với Đảng, Nhà nước,... Đồng thời, luôn bám sát sự chỉ đạo, định hướng của các ban, bộ, ngành Trung ương và nguồn thông tin chính thống trên báo chí để tuyên truyền, giáo dục, định hướng chính trị, nâng cao nhận thức cho cán bộ, chiến sĩ quân đội và dư luận xã hội, giúp họ nhận thức đúng chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước, nhiệm vụ quân sự quốc phòng, an ninh, bảo vệ Tổ quốc.

Sử dụng và phát huy hiệu quả các nguồn thông tin chính thống trên báo chí, tài liệu được cấp phát, toàn quân chú trọng đổi mới nội dung, hình thức, biện pháp đấu tranh theo hướng coi trọng sử dụng thông tin tích cực, đẩy mạnh tuyên truyền chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước; bản chất, truyền thống, chức năng, nhiệm vụ của quân đội. Nâng cao chất lượng

hoạt động của các cơ quan báo chí quân đội, nhất là Báo Quân đội nhân dân, Truyền hình Quốc phòng Việt Nam,... trong định hướng tư tưởng và dư luận xã hội. Với phương châm kết hợp chặt chẽ giữa “xây” và “chống” để khẳng định tính đúng đắn trong lãnh đạo, chỉ đạo của Đảng, những thành tựu nổi bật về chính trị, kinh tế, xã hội, văn hóa, quốc phòng, an ninh, đối ngoại của đất nước với nhận diện sự thật, kiên quyết vạch trần bản chất, âm mưu, thủ đoạn “diễn biến hòa bình” và tích cực đấu tranh, phản bác các luận điệu sai trái, thù địch chống phá Đảng, Nhà nước và chế độ ta. Đồng thời, chỉ đạo sát sao công tác quản lý báo chí, tờ tin thuộc quân khu, quân chủng, Bộ đội Biên phòng, Bộ Tư lệnh Thủ đô Hà Nội, Bộ Tư lệnh Thành phố Hồ Chí Minh, Cảnh sát biển, các học viện, nhà trường, cơ quan, đơn vị tiếp tục duy trì chuyên trang, chuyên mục phòng, chống “diễn biến hòa bình”, “tự diễn biến”, “tự chuyển hóa” và các nội dung phản ánh hoạt động quân sự, quốc phòng, kết quả thực hiện các chức năng, nhiệm vụ của Quân đội nhân dân Việt Nam trong từng giai đoạn.

Ba là, coi trọng công tác tổ chức, xây dựng lực lượng nòng cốt, chuyên sâu trong đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch.

Đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch thực chất là cuộc đấu tranh giai cấp trên lĩnh vực ý thức hệ; là cuộc chiến đấu trong thời bình, rất gay go, quyết liệt và phức tạp, với thời gian, không gian ngày càng mở rộng, cường độ cao, nhịp độ nhanh nhưng phải bảo đảm chính xác, hiệu quả, thiết thực.

Trong cuộc đấu tranh này, các thế lực thù địch, cơ hội chính trị, phản động đã và đang triệt để sử dụng các lực lượng bất mãn tham gia, được trang bị một số công cụ, phương tiện hiện đại. Để đấu tranh, làm thất bại mọi âm mưu, thủ đoạn, hoạt động chống phá của chúng, Quân ủy Trung ương, Bộ Quốc phòng đã tập trung xây dựng, bồi dưỡng, phát triển lực lượng nòng cốt đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch. Xây dựng đội ngũ cán bộ, đảng viên, chiến sĩ có bản lĩnh chính trị vững vàng, có trình độ lý luận và khả năng luận chiến cao, sức thuyết phục lớn, có nhiệt huyết, dũng khí đấu tranh bảo vệ Đảng, Nhà nước và chế độ xã hội chủ nghĩa. Trong đó, chú trọng nâng cao trình độ lý luận, nhận thức, kinh nghiệm và khả năng tổ chức thực hiện đấu tranh, phát huy vai trò quản trị viên, trưởng nhóm, chủ tài khoản các trang blog, “nhóm kín”, trang fanpage trong tham gia đấu tranh, tiếp cận thông tin, chia sẻ, bình luận lan tỏa thông tin tích cực trong cộng đồng mạng và trong xã hội; qua đó, định hướng thông tin tích cực, tạo dòng chủ lưu chính trên không gian mạng; truyền cảm hứng, lan tỏa lập trường, quan điểm, thái độ đấu tranh phản bác các quan điểm sai trái, thông tin xấu, độc của các thế lực thù địch đến mọi người, góp phần xây dựng môi trường chính trị và dư luận tích cực cho cán bộ, chiến sĩ và nhân dân.

Tích cực tham gia diễn tập đấu tranh trên không gian mạng thông qua tập huấn, bồi dưỡng phương pháp, kỹ năng đấu tranh, tạo lập trang, nhóm, cách thức sử dụng

các trang bị, phương tiện đấu tranh trên không gian mạng, nhất là máy tính ảo, phần mềm máy tính ảo trên máy tính xách tay, trên các thiết bị cầm tay (máy tính bảng, ipad, điện thoại thông minh), hướng dẫn phương pháp thẩm định, khai thác nguồn thông tin để chia sẻ, lan truyền thông tin; từng bước tiếp cận và sử dụng hiệu quả phần mềm ứng dụng Mocha 35..., góp phần nâng cao chất lượng, hiệu quả đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch trên không gian mạng.

Bốn là, chủ động, tích cực làm tốt công tác kiểm tra, giám sát, đánh giá hiệu quả đấu tranh; kịp thời biểu dương, khen thưởng, nhân rộng điển hình tiên tiến, cách làm hay, mô hình mới, sáng tạo.

Góp phần nâng cao chất lượng, hiệu quả công tác chỉ đạo, tổ chức đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch trên không gian mạng, Quân ủy Trung ương, Bộ Quốc phòng, Cơ quan Thường trực Ban Chỉ đạo 35 Quân ủy Trung ương thường xuyên kiểm tra, giám sát cấp ủy, chỉ huy các cơ quan, đơn vị trong lãnh đạo, chỉ đạo, cụ thể hóa quan điểm, nhiệm vụ, giải pháp đấu tranh mà Nghị quyết số 35-NQ/TW, ngày 22/10/2018 *Về tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới* của Bộ Chính trị đã xác định. Nhờ đó, hệ thống văn bản, sổ sách, quy chế hoạt động, chương trình hành động, kế hoạch công tác, chỉ thị, hướng dẫn của các cơ quan, đơn vị được tổ chức thực hiện nghiêm túc, hiệu quả.

Toàn quân đã phát huy tốt vai trò, chức năng, nhiệm vụ của cơ quan tham mưu và lực lượng chuyên trách trong giúp việc cấp ủy, người chỉ huy xác định chủ trương, biện pháp lãnh đạo, chỉ đạo và tổ chức đấu tranh trực diện trên không gian mạng; kết hợp chặt chẽ thông tin, thông báo, kịp thời định hướng chủ trương, biện pháp ngăn chặn tác động, ảnh hưởng xấu từ hoạt động chống phá của các thế lực thù địch cho cán bộ, chiến sĩ và nhân dân.

Các cơ quan, đơn vị đã làm tốt công tác phát hiện, bồi dưỡng, nhân rộng điển hình tiên tiến, mô hình tiêu biểu, cách làm hay, sáng tạo, hiệu quả đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch. Trong lãnh đạo, chỉ đạo, hướng dẫn đấu tranh đã tập trung đổi mới đồng bộ, toàn diện các bước, các khâu: phát hiện, bồi dưỡng, sơ kết, tổng kết và nhân rộng điển hình tiên tiến,... Việc xây dựng và nhân rộng điển hình tiên tiến, cách làm hay, gương người tốt, việc tốt trong phong trào thi đua quyết thắng có ý nghĩa động viên tinh thần, cổ vũ cán bộ, chiến sĩ; qua đó, tạo sức lan tỏa làm cho phong trào thi đua quyết thắng đi vào cuộc sống, đạt được hiệu quả thiết thực.

Năm là, phối hợp chặt chẽ các cơ quan, đơn vị, lực lượng trong và ngoài quân đội; đẩy mạnh ứng dụng công nghệ thông tin phục vụ công tác quản lý và tổ chức đấu tranh.

Đấu tranh phòng, chống “diễn biến hòa bình” và các quan điểm sai trái, thù địch trên không gian mạng là nội dung quan trọng của cuộc chiến đấu trong thời bình, tuy không có khói súng nhưng vô cùng gay go, quyết liệt và

phức tạp. Đây là nhiệm vụ quan trọng của toàn Đảng, toàn dân và toàn quân, trực tiếp là các tổ chức, các lực lượng chuyên trách, trước hết là Ban chỉ đạo 35 các cấp. Vì vậy, Quân ủy Trung ương, Bộ Quốc phòng luôn coi trọng công tác xây dựng và thực hiện nghiêm túc cơ chế, quy chế phối hợp giữa quân đội với các ban, bộ, ngành của Trung ương, cấp ủy, chính quyền, đoàn thể địa phương để kịp thời phát hiện âm mưu, thủ đoạn, hoạt động chống phá của các thế lực thù địch. Toàn quân thường xuyên duy trì, thực hiện nghiêm chế độ giao ban định kỳ để phản ánh đúng tình hình, trao đổi thông tin, thống nhất biện pháp phối hợp đấu tranh, kịp thời ngăn chặn âm mưu, hoạt động móc nối, tập hợp lực lượng chống phá; quản lý chặt chẽ và đấu tranh hiệu quả với các phần tử cơ hội, bất mãn, nhất là việc kích động, chia rẽ nội bộ Đảng, Nhà nước và khối đại đoàn kết toàn dân tộc. Sự phối hợp đấu tranh được thực hiện chặt chẽ, đúng quy chế, quy định trên cơ sở phù hợp với nhiệm vụ chính trị, khả năng và thế mạnh của mỗi cơ quan, đơn vị; sự chỉ đạo, quản lý, định hướng của Cơ quan Thường trực Ban Chỉ đạo 35 Quân ủy Trung ương, cơ quan chức năng cấp trên về nội dung, hình thức và biện pháp đấu tranh, với phương châm “chặt chẽ, khoa học, an toàn”. Đối với các lực lượng ngoài quân đội, sự phối hợp đấu tranh được thực hiện thông qua quy chế, quy định và chương trình ký kết, trên cơ sở thống nhất các biện pháp tổ chức đấu tranh, ngăn chặn, phòng ngừa, hạn chế sự tác động, ảnh hưởng tiêu cực đến tình hình, nhiệm vụ của Đảng, Nhà nước, Quân đội, Công an và địa phương;

xác định rõ vai trò, trách nhiệm của cơ quan chủ trì, cơ quan phối hợp; nội dung, hình thức, cơ chế phối hợp cụ thể, thiết thực, phù hợp với yêu cầu, nhiệm vụ, khả năng và thể mạnh của mỗi cơ quan, đơn vị, trên tinh thần đoàn kết, hợp tác, đồng thuận và giúp đỡ nhân dân cùng hoàn thành nhiệm vụ của các cơ quan, đơn vị.

Trước yêu cầu, nhiệm vụ mới, các cơ quan, đơn vị toàn quân theo chức năng, nhiệm vụ luôn đẩy mạnh nghiên cứu, ứng dụng công nghệ thông tin, trí tuệ nhân tạo trong đấu tranh phòng, chống “diễn biến hòa bình”, các quan điểm sai trái, thù địch trên không gian mạng. Tiếp tục bổ sung, hoàn thiện, đưa vào khai thác, sử dụng các phần mềm quản lý kết quả đấu tranh và hỗ trợ các hoạt động đấu tranh trên không gian mạng; chủ động, tích cực thực hiện các chiến dịch truyền thông. Đồng thời, đẩy mạnh công tác nghiên cứu, thử nghiệm và đề xuất các phương án sử dụng phần mềm Mocha Viettel, sản xuất điện thoại di động nội bộ, đáp ứng nhu cầu thông tin, giải trí lành mạnh, bảo đảm an toàn, góp phần quản lý tình hình tư tưởng, dư luận xã hội và hoạt động đấu tranh của cán bộ, chiến sĩ quân đội trên không gian mạng.

Đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, phản động của các thế lực thù địch trên không gian mạng là nhiệm vụ chiến đấu lâu dài, khó khăn, phức tạp nhưng rất vẻ vang. Với vai trò là lực lượng nòng cốt, xung kích đi đầu, các cơ quan, đơn vị toàn quân tiếp tục vận dụng sáng tạo những kinh nghiệm hay, cách làm tốt, hiệu quả trong chỉ đạo, tổ chức đấu tranh để

không ngừng nâng cao chất lượng, hiệu lực, hiệu quả đấu tranh, làm thất bại âm mưu, thủ đoạn, hoạt động “diễn biến hòa bình” của các thế lực thù địch, bảo vệ Đảng, Nhà nước, nhân dân và chế độ xã hội chủ nghĩa trong tình hình mới.

BÀN VỀ CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG - NHỮNG YÊU CẦU BẢO ĐẢM CÁC CHỈ SỐ AN NINH, AN TOÀN TRONG BỐI CẢNH HIỆN NAY

Thượng tướng, PGS.TS. NGUYỄN VĂN THÀNH*

1. Tư duy mới về bảo vệ an ninh quốc gia

Theo quan niệm truyền thống, an ninh quốc gia mang nội hàm đồng nghĩa với sử dụng sức mạnh để chống xâm lược, bảo vệ sự thống nhất và toàn vẹn lãnh thổ của một quốc gia. Ngày nay, trong bối cảnh toàn cầu hóa và hội nhập quốc tế, khái niệm “an ninh quốc gia” cần được hiểu một cách toàn diện hơn, không chỉ có các vấn đề an ninh chính trị, quân sự truyền thống, mà còn bao quát cả những vấn đề an ninh phi truyền thống như an ninh kinh tế, an ninh thông tin, an ninh tài chính - tiền tệ, an ninh năng lượng, an ninh lương thực, an ninh dân số, an ninh môi trường... Đó là những vấn đề an ninh nổi lên bắt nguồn từ những nguy cơ mới, tác động đa chiều của quá trình phát triển; bổ sung cho các vấn đề an ninh chính trị, quân sự vốn là những vấn đề trung tâm của

* Phó Chủ tịch Hội đồng Lý luận Trung ương.

thời kỳ Chiến tranh lạnh và nay đang có xu hướng giảm đi trong tiến trình toàn cầu hóa và hội nhập quốc tế.

Theo đó, an ninh quốc gia bao gồm: an ninh chính trị, an ninh kinh tế, an ninh quân sự, an ninh đối ngoại, an ninh tư tưởng - văn hóa, an ninh xã hội, an ninh thông tin, an ninh tài chính - tiền tệ, an ninh năng lượng, an ninh lương thực, an ninh dân số, an ninh môi trường... Trong đó, an ninh kinh tế là nền tảng (trung tâm), an ninh chính trị là cốt lõi, xuyên suốt và cùng với an ninh tư tưởng - văn hóa, an ninh quân sự trở thành bốn trụ cột của Chiến lược an ninh quốc gia trong thế kỷ XXI.

Trong bối cảnh toàn cầu hóa và hội nhập quốc tế, sự phát triển của Cách mạng công nghiệp lần thứ tư (4.0) đã tác động sâu sắc đến tư duy về sức mạnh, nguồn lực bảo đảm an ninh quốc gia, nhất là sức mạnh tổng hợp quốc gia gồm 9 yếu tố cấu thành: vị trí địa lý, nguồn tài nguyên thiên nhiên, khả năng sản xuất công nghiệp, dân số, lực lượng vũ trang, chí khí dân tộc, khả năng ngoại giao, năng lực và hiệu quả quản lý, điều hành của chính phủ. Vì thế, chiến lược bảo vệ an ninh quốc gia phải được xem như một bộ phận quan trọng của chiến lược phát triển quốc gia. Và vì vậy, tư duy về bảo vệ an ninh quốc gia không chỉ giới hạn trong phạm vi biên giới hành chính quốc gia, mà cần được mở rộng nhằm bảo vệ lợi ích của Việt Nam ở nước ngoài và sự phát triển của đất nước trong tương lai. Phải chuyển từ tư duy thụ động, bó hẹp, khép kín, biệt lập sang tư duy chủ động, hợp tác và phát triển.

Bảo vệ an ninh quốc gia là tổng thể các hoạt động đối nội, đối ngoại của hệ thống chính trị và của cả dân tộc để tạo nên

sức mạnh tổng hợp nhằm ngăn chặn, loại trừ các nguy cơ đe dọa đến an ninh quốc gia. Nói cách khác, bảo vệ an ninh quốc gia chính là việc sử dụng mọi lực lượng, bằng mọi hình thức, mọi biện pháp để xây dựng, củng cố tiềm lực an ninh quốc gia và thường xuyên phát hiện, hạn chế, loại bỏ những nhân tố đe dọa nhằm giữ vững an ninh quốc gia. Từ khái niệm trên, rút ra 6 đặc điểm nổi bật của công tác bảo vệ an ninh quốc gia là:

(1) Bảo vệ an ninh quốc gia là bảo vệ những lợi ích cực kỳ quan trọng của quốc gia, của dân tộc; những lợi ích này quan hệ trực tiếp đến vận mệnh của đất nước, đến bản chất và sự tồn tại của chế độ chính trị; là điều kiện trước hết và có ý nghĩa quyết định để xây dựng và phát triển đất nước về mọi mặt; vì vậy, bảo vệ an ninh quốc gia mang “*tính phòng ngừa*” rất cao.

(2) Quá trình ngăn chặn, loại trừ các nguy cơ đe dọa để bảo vệ an ninh quốc gia, thể hiện tập trung tính chất gay go, quyết liệt, phức tạp và lâu dài của đấu tranh giai cấp, đấu tranh vì lợi ích dân tộc. Bảo vệ an ninh quốc gia thể hiện “*tính chiến đấu*” thường xuyên, liên tục trong mọi hoàn cảnh (thời chiến và thời bình) nhằm chống lại những âm mưu, hoạt động phá hoại của các thế lực thù địch đối với sự nghiệp cách mạng của Đảng, của dân tộc ta.

(3) Các hoạt động của quá trình bảo vệ an ninh quốc gia thường không có giới hạn “phạm vi không gian” cố định, mà nó diễn ra trên các lĩnh vực của đời sống xã hội (chính trị, kinh tế, văn hóa, xã hội, quốc phòng, đối ngoại...), diễn ra trong từng tổ chức, từng địa phương, trong cả nước và có khi ở cả phạm vi quốc tế.

(4) Bảo vệ an ninh quốc gia thực chất là cuộc đấu tranh cùng lúc với nhiều kẻ thù, nhiều loại đối tượng khác nhau ở cả trong nước và ngoài nước; các loại kẻ thù này hoạt động vừa bí mật, vừa công khai trắng trợn, bằng nhiều thủ đoạn thâm độc, xảo quyệt để thực hiện ý đồ phá hoại và che đậy bản chất. Vì vậy, để vạch trần bản chất và chiến thắng chúng phải bằng nhiều hình thức, những biện pháp cần thiết và sức mạnh to lớn.

(5) Bảo vệ an ninh quốc gia chịu sự tác động, chi phối trực tiếp của diễn biến tình hình quốc tế, tác động của nhiều yếu tố về kinh tế - xã hội, trong đó có nhiều diễn biến khó lường; vì vậy, phải luôn chủ động nắm chắc tình hình, dự báo những tình huống phức tạp nhất có thể xảy ra để chủ động đối phó.

(6) Trong thế giới toàn cầu hóa, bảo vệ an ninh quốc gia đã và đang có xu hướng mở rộng cả trong không gian thuộc quyền quản lý của quốc gia, không gian mạng. Bảo vệ an ninh quốc gia không chỉ giới hạn trong phạm vi biên giới hành chính quốc gia mà còn được mở rộng trong không gian chiến lược nhằm bảo vệ lợi ích của đất nước.

2. Chủ quyền quốc gia trên không gian mạng hiện nay

Trên thế giới, các quốc gia sử dụng một số thuật ngữ khác nhau như “cyber security”, “network security” để chỉ an ninh, an toàn mạng; “information security” (hay “security of information”) để chỉ an ninh, an toàn thông tin. Mỹ giải thích khái niệm “information security” (an ninh, an toàn thông tin) tại Luật “Federal Information Security Management Act of 2002” (H.R. 2458 - 48) và Luật “Federal Information Security Modernization Act of 2014” (Public Law 113-283, 113th

Congress) như sau: Thuật ngữ “an ninh, an toàn thông tin” có nghĩa là bảo vệ thông tin và hệ thống thông tin không bị truy cập trái phép, sử dụng, tiết lộ, gián đoạn, thay đổi hoặc phá hoại nhằm bảo đảm: *tính nguyên vẹn* (nghĩa là bảo vệ chống lại việc sửa đổi hoặc phá hoại thông tin trái phép, bao gồm việc bảo đảm thông tin xác thực và không bị gián đoạn); *tính bảo mật* (nghĩa là hạn chế quyền tiếp cận và tiết lộ thông tin, bao gồm cả việc bảo vệ thông tin cá nhân và thông tin riêng); *tính khả dụng* (nghĩa là bảo đảm cho việc có thể truy cập được và sử dụng được thông tin một cách kịp thời và tin cậy).

Trung Quốc giải thích khái niệm “an ninh, an toàn mạng” tại dự thảo Luật an ninh, an toàn mạng như sau: “An ninh, an toàn mạng” là áp dụng các biện pháp cần thiết để ngăn chặn tấn công, xâm nhập, can nhiễu, phá hoại hoặc sử dụng phi pháp mạng cũng như những sự cố ngoài ý muốn giữ cho mạng ở trạng thái vận hành ổn định và tin cậy cũng như bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin được lưu trữ, truyền tải và xử lý trên mạng.

Ở Việt Nam, Quốc hội đã thông qua Luật an toàn thông tin mạng năm 2015, trong đó có giải thích thuật ngữ “an toàn thông tin mạng”. Theo đó, “an toàn thông tin mạng được hiểu là sự bảo vệ hệ thống thông tin và thông tin truyền đưa trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin”.

Không gian mạng là mạng lưới kết nối toàn cầu của các kết cấu hạ tầng công nghệ thông tin, bao gồm internet, các mạng viễn thông, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, là môi trường đặc biệt mà con người thực

hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian. Qua nghiên cứu khái niệm “không gian mạng” của các quốc gia trên thế giới, nhất là các quốc gia có trình độ công nghệ thông tin, an ninh mạng phát triển và căn cứ vào tình hình thực tế của Việt Nam cho thấy, không gian mạng có bản chất vật lý và tính chất xã hội.

Về bản chất vật lý, không gian mạng có cấu trúc ba lớp: (1) Hạ tầng truyền dẫn vật lý bao gồm các thiết bị phần cứng công nghệ thông tin kết nối một cách hợp lý với nhau, tạo ra các loại mạng. (2) Hạ tầng dịch vụ lõi và các dịch vụ tạo ra các giao thức để lưu trữ, xử lý, trao đổi thông tin, chủ yếu bao gồm các quy định chuẩn, hệ điều hành, các công nghệ nền tảng như công nghệ phần mềm, công nghệ mạng, giao diện, phương thức giao tiếp, giao thức, truyền dẫn xử lý thông tin, điều khiển... phần mềm ứng dụng với việc tạo các thư viện và dịch vụ dùng chung. (3) Hệ thống ứng dụng công nghệ thông tin và cơ sở dữ liệu, các phần mềm ứng dụng để thông tin dưới dạng số được tạo ra, lưu trữ, xử lý trao đổi nhằm phục vụ nhu cầu cuộc sống và tác động đến nhận thức của con người.

Về tính chất xã hội, không gian mạng là môi trường xã hội đặc biệt của con người hội tụ đủ 6 thành tố: (1) chính sách, pháp luật; (2) năng lực công nghệ; (3) nội dung thông tin; (4) nguồn nhân lực; (5) cơ cấu tổ chức bộ máy; (6) ý thức của con người trên không gian mạng, tạo ra môi trường xã hội đặc biệt của con người. Trong đó *chính sách, pháp luật* là những quy định, quy tắc ứng xử điều chỉnh hành vi và các mối quan hệ giữa cá nhân, tổ chức, cơ quan quản lý nhà nước, các quốc gia, các tổ chức quốc tế khi tham gia vào

không gian mạng. Nó tạo hành lang pháp lý bảo đảm cho sự hoạt động an toàn và hiệu quả của không gian mạng, mở đường cho công nghệ phát triển. *Năng lực công nghệ* là công nghệ đã được ứng dụng và khả năng nghiên cứu, phát triển công nghệ mới cho hạ tầng công nghệ thông tin, phần mềm, dịch vụ,... cấu thành nên không gian mạng, bao gồm các loại công nghệ nền tảng như công nghệ mạng, công nghệ điện tử, bán dẫn, vi xử lý, công nghệ phần mềm... Bên cạnh đó, còn có các quy định chuẩn công nghệ, các quy trình phương thức giao tiếp, giao diện giữa các tầng kiến trúc của một công nghệ nào đó... *Nội dung thông tin* là những nội dung được lưu trữ, xử lý và trao đổi trên không gian mạng. *Nguồn nhân lực* là con người tham gia vào hoạt động quản lý, điều hành, sử dụng hệ thống mạng. *Tổ chức bộ máy* là bộ máy quản lý nhà nước quản lý các bộ phận cấu thành nên không gian mạng, từ hạ tầng kỹ thuật đến dịch vụ ứng dụng, bảo vệ và điều tiết chính sách, pháp luật trên không gian mạng. *Ý thức của con người trên không gian mạng* là việc con người chấp hành chính sách, pháp luật, chuẩn công nghệ, quy tắc nghiệp vụ, đạo đức, chuẩn mực văn hóa khi tham gia vào không gian mạng.

“Chủ quyền quốc gia trên không gian mạng” là quyền tối cao, tuyệt đối, đầy đủ và riêng biệt của quốc gia đối với các vùng thông tin do Nhà nước quản lý, kiểm soát trực tiếp hoặc gián tiếp bằng chính sách, pháp luật và năng lực công nghệ phù hợp với luật pháp quốc tế.

Cũng giống như chủ quyền lãnh thổ, các quốc gia có quyền tối cao, tuyệt đối, hoàn toàn và riêng biệt đối với phạm vi không gian mạng thuộc quyền kiểm soát của mình,

tức là có chủ quyền quốc gia trên không gian mạng. Việc xác định chủ quyền quốc gia trên không gian mạng cần căn cứ vào phạm vi không gian mạng mà một quốc gia được quyền kiểm soát, chi phối trên cơ sở chủ quyền, lợi ích quốc gia và luật pháp quốc tế. Thực chất việc quốc gia xác lập chủ quyền không gian mạng là xác lập quyền quản lý, kiểm soát đối với kết cấu hạ tầng không gian mạng và thông tin được tạo ra, lưu trữ, xử lý và truyền đưa trên đó, được thực hiện thông qua xác lập chủ quyền, quyền tài phán theo luật pháp quốc tế đối với kết cấu hạ tầng mạng thuộc sở hữu cả ở trong và ngoài lãnh thổ quốc gia; đồng thời mã hóa thông tin số truyền đưa trên không gian mạng toàn cầu.

Kết cấu hạ tầng không gian mạng được cấu thành từ: hạ tầng truyền dẫn vật lý; hạ tầng các dịch vụ lõi; các dịch vụ, hệ thống ứng dụng công nghệ thông tin và cơ sở dữ liệu. Các thành phần này là các thiết bị vật lý, tương đối ổn định và hữu hình. Mọi quốc gia có quyền kiểm soát kết cấu hạ tầng không gian mạng và các hoạt động trên toàn bộ vùng lãnh thổ có chủ quyền của mình. Kết cấu hạ tầng không gian mạng có thể nằm trong lãnh thổ đất liền, nội thủy, lãnh hải (bao gồm cả thềm lục địa và đáy biển), các quần đảo và không phận quốc gia đều thuộc chủ quyền của quốc gia có chủ quyền với vùng lãnh thổ đó.

3. Thực trạng an ninh, an toàn trên không gian mạng của các quốc gia trên thế giới hiện nay: Cơ hội và thách thức

Theo nghiên cứu của Hãng bảo mật Kaspersky Lab đưa ra dự đoán xu hướng an ninh mạng nổi bật trong những năm

gần đây gồm: các cuộc tấn công với mục tiêu xác định và gián điệp mạng nhằm vào các doanh nghiệp, các kết cấu hạ tầng xung yếu và cơ quan chính phủ; các cuộc tấn công của tin tặc mang động cơ chính trị (hacktivism); xu hướng hợp pháp hóa việc sử dụng công cụ giám sát của các chính phủ; nguy cơ an ninh từ điện toán đám mây; quyền riêng tư của người dân ngày càng bị đe dọa; sử dụng chứng chỉ số giả mạo cho trang web độc hại; các phần mềm tống tiền trực tuyến; mã độc trên hệ điều hành MacOS tăng nhanh; bùng nổ mã độc di động; tăng cường khai thác lỗ hổng trong các ứng dụng nhằm cài đặt mã độc lên máy tính nạn nhân. Theo đó, hiện có 8 xu hướng mới, có thể làm thay đổi phương thức bảo đảm an ninh mạng thông tin, gồm:

(1) *Các mạng di động, mạng riêng ảo và người dùng chuyển vùng.* Trong những năm gần đây, giải pháp an ninh mạng thông tin sử dụng tường lửa đang ngày càng trở nên yếu thế, dễ dàng bị vượt qua do khả năng truy cập mọi nơi từ các thiết bị như iPad, điện thoại Android, máy tính bảng và máy tính cá nhân. Bên cạnh đó, việc mở rộng mạng kết nối đến các chi nhánh nhỏ hoặc văn phòng tại nhà cũng là một trọng tâm phát triển của nhiều cơ quan, doanh nghiệp. Theo đó, chiến lược mạng của cơ quan, doanh nghiệp sẽ cần phải xem xét đến khả năng bảo đảm truy cập vào hệ thống trên một mạng lưới rộng, không ranh giới trên phạm vi toàn cầu.

(2) *Các cuộc tấn công nhắm đến các mục tiêu chủ định, các mối đe dọa liên tục được nâng cao cả về kỹ thuật và chiến thuật.* Ngày nay, APTs (hay các mối đe dọa liên tục nâng cao) đại diện cho thế hệ tiếp theo của phần mềm tội phạm trên mạng internet. Trong nhiều năm qua, khả năng bảo mật

mạng như lọc web hoặc IPS đóng một vai trò quan trọng trong việc xác định các cuộc tấn công như vậy. Với việc những kẻ tấn công phát triển mạnh bạo hơn và sử dụng kỹ thuật tiên tiến hơn, việc bảo đảm an ninh mạng thông tin ngày nay phải được kết hợp với các dịch vụ bảo mật khác để có thể phát hiện các cuộc tấn công.

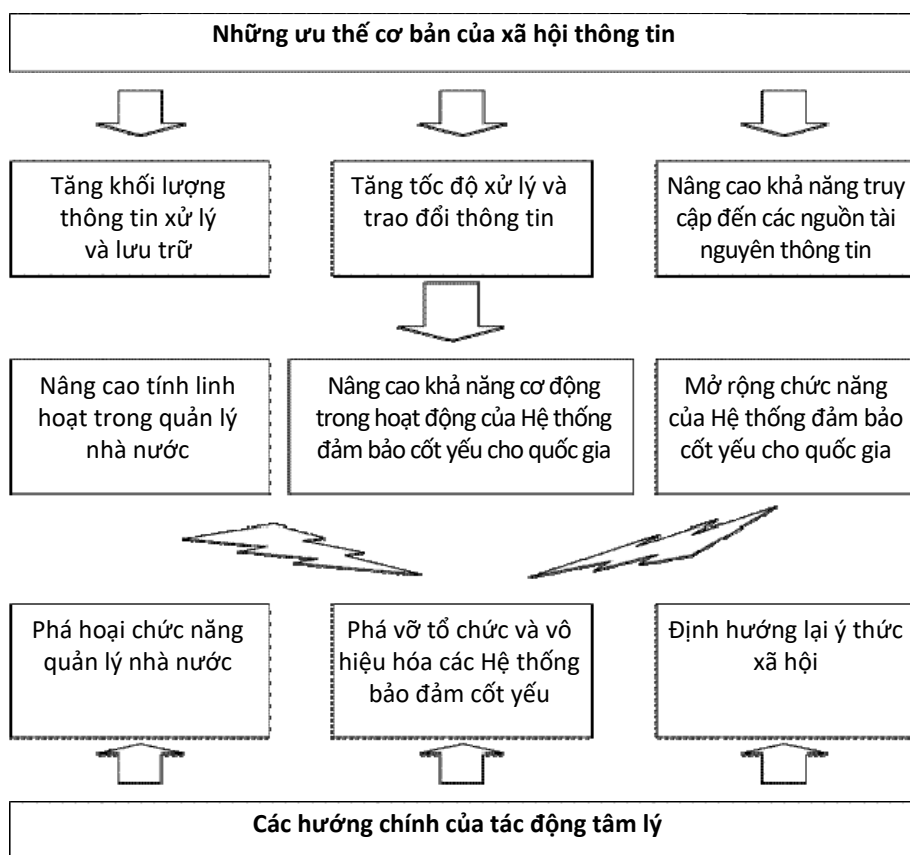
(3) *Thói quen sử dụng và làm việc trên thiết bị cá nhân “BYOD”*. Gần đây, thói quen mang theo và làm việc trên thiết bị của cá nhân như iPad, iPhone và các điện thoại Android đang ngày càng gia tăng nhanh chóng. Để đối phó với phương thức làm việc mới kèm theo nhiều nguy cơ mất an ninh mạng này, chiến lược an ninh mạng thông tin cần tập trung vào bảo đảm an ninh mạng thông tin cho các thiết bị không được thiết lập để hoạt động ở chế độ ổn định.

(4) *Ứng dụng web và bảo vệ máy chủ web*. Các mối đe dọa từ các cuộc tấn công vào ứng dụng web để trích xuất dữ liệu hoặc phát tán mã độc hại vẫn tồn tại. Tội phạm mạng phát tán mã độc của chúng thông qua các máy chủ web hợp pháp khi các máy chủ này bị xâm nhập. Tuy nhiên, các cuộc tấn công đánh cắp dữ liệu, phần nhiều trong số đó có được sự chú ý của phương tiện truyền thông, cũng là một mối đe dọa lớn. Trước đây, nhiều cơ quan, doanh nghiệp đã tập trung đầu tư giải pháp bảo mật trên máy tính và trang bị khả năng ngăn chặn phần mềm độc hại lây lan thông thường sang và vào mạng của mình, tuy nhiên, đến nay cần phải chú trọng nhiều hơn vào việc bảo vệ các máy chủ web và các ứng dụng web. Ngoài ra, những thách thức tương tự đối với an ninh mạng còn ở phía trước khi sử dụng công nghệ mới như HTML5.

(5) *IPv6*. IPv6 là giao thức internet mới thay thế IPv4. Trong khi IPv6 là một thay thế hiệu quả trong việc đưa ra các địa chỉ IP có sẵn, có một số thay đổi cơ bản cần phải được xem xét thận trọng trong chính sách bảo mật. Cho dù cơ quan, doanh nghiệp chưa có kế hoạch để chuyển đổi sang IPv6 trong thời gian ngắn, cần bảo đảm chắc chắn rằng IPv6 luôn nằm trong chương trình phát triển an ninh mạng.

(6) *Đối phó với các dịch vụ điện toán đám mây*. Ngày nay, hầu hết các doanh nghiệp nhỏ, vừa và lớn đều đang bắt đầu triển khai dịch vụ điện toán đám mây và SaaS với tốc độ lớn hơn. Xu hướng này là một thách thức lớn đối với an ninh mạng. Ngoài ra, khi số lượng các ứng dụng sẵn có trong các đám mây phát triển, việc kiểm soát chính sách cho các ứng dụng web và dịch vụ điện toán đám mây cũng cần phải phát triển theo.

(7) *Bảo mật dữ liệu*. Mã hóa dữ liệu ở mọi cấp độ sẽ bảo vệ sự riêng tư và tính toàn vẹn của dữ liệu. Có thể thấy rằng, việc triển khai mã hóa ở tất cả các lớp đang ngày càng được quan tâm. Tuy nhiên, sử dụng nhiều mã hóa sẽ mang lại nhiều thách thức cho các thiết bị an ninh mạng. Ví dụ, làm thế nào để tiện ích phòng, chống mất mát dữ liệu mạng sẽ theo dõi được lưu lượng mã hóa từ đầu đến cuối như khi truy cập một dịch vụ đám mây nào đó. Sự hợp tác giữa các mạng và thiết bị đầu cuối để cung cấp khả năng bảo mật toàn diện trong các tình huống xảy ra sẽ rất quan trọng. Các cơ quan, doanh nghiệp cần phải có một chiến lược tích hợp an ninh mạng với các lớp khác về an ninh như thiết bị đầu cuối, bảo vệ web và thiết bị di động.



(8) *Không gian mạng có tính đàn hồi.* Phạm vi không gian mạng đang ngày càng được mở rộng một cách đàn hồi bao gồm 4G tốc độ cao và mạng LTE, điểm truy cập không dây, văn phòng chi nhánh, văn phòng tại nhà, người sử dụng chuyển vùng, dịch vụ đám mây, và các bên thứ ba truy cập vào các ứng dụng và dữ liệu của cơ quan, doanh nghiệp để thực hiện các tác vụ khác nhau. Những thay đổi về kích thước, phạm vi của không gian mạng có thể dẫn đến lỗi cấu hình hoặc thay đổi lỗi kiểm soát, từ đó có thể dẫn đến vi phạm an ninh mạng. Các cơ quan, doanh nghiệp sẽ cần các giải pháp bảo mật luôn có thể triển khai tại mỗi thiết bị hoặc

điểm của kết cấu hạ tầng và cần được quản lý tập trung để bảo đảm sự linh hoạt của kết cấu hạ tầng đàn hồi.

Chiến tranh mạng, là hoạt động tấn công quy mô lớn trên không gian mạng của một quốc gia hay vùng lãnh thổ để phá hoại, làm tê liệt hệ thống, nguồn tài nguyên thông tin cũng như các kết cấu hạ tầng thông tin quan trọng, xâm phạm chủ quyền quốc gia trên không gian mạng của Việt Nam nhằm có được lợi thế về quân sự, chính trị, kinh tế, đe dọa nghiêm trọng độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ của nước ta.

Nhiều quốc gia đã coi không gian mạng là miền chiến trường thứ năm và chiến tranh mạng đã trở thành một hình thái chiến tranh mới. Nghị quyết số 28-NQ/TW, ngày 25/10/2013 của Ban Chấp hành Trung ương Đảng khóa XII về *Chiến lược bảo vệ Tổ quốc trong tình hình mới* đã xác định: “Cộng đồng quốc tế phải đối phó ngày càng quyết liệt hơn với các thách thức an ninh truyền thống, phi truyền thống, đặc biệt là an ninh mạng và hình thái chiến tranh mới”; “nguy cơ xảy ra khủng bố, chiến tranh mạng, mất an ninh thông tin ngày càng tăng”.

Theo cách hiểu phổ biến hiện nay, “chiến tranh mạng” được mô tả theo cả nghĩa rộng và nghĩa hẹp. Theo nghĩa hẹp, “chiến tranh mạng” không chỉ bao gồm sự đối kháng giữa các hệ thống thông tin quân sự. Theo nghĩa rộng, “chiến tranh mạng” là việc sử dụng thông tin trên mạng để đạt được mục đích của quốc gia. Nó chỉ mọi hoạt động chiến tranh và phi chiến tranh sử dụng công nghệ thông tin, diễn ra không chỉ trên lĩnh vực quân sự mà còn cả trên lĩnh vực chính trị, kinh tế, văn hóa, xã hội, ngoại giao... “Chiến tranh mạng”

không bị hạn chế ở những cuộc đối đầu trong lĩnh vực quân sự mà còn thâm nhập vào mọi khía cạnh của đời sống xã hội, sử dụng các phương tiện điện tử, mạng máy tính và cả tác động tâm lý... để tấn công vào toàn bộ hệ thống thông tin, vũ khí thông tin hóa (bao gồm cả con người), phá hoại luồng thông tin chiến trường nhằm mục đích làm ảnh hưởng, suy giảm và phá hủy khả năng chỉ huy, kiểm soát của đối phương, đồng thời bảo vệ khả năng chỉ huy, kiểm soát của mình khỏi những ảnh hưởng bởi hoạt động tương tự của đối phương.

“Chiến tranh mạng” là một hình thái chiến tranh mới, vượt khỏi khuôn khổ khái niệm về chiến tranh quân sự truyền thống. Lực lượng tiến hành không cần hùng hậu, mà chỉ cần một nhóm người, thậm chí là một cá nhân tiến hành, chỉ một lực lượng nhỏ cũng có thể gây thiệt hại rất lớn cho đối phương. “Chiến tranh mạng” bất đối xứng, quốc gia nào phát triển hơn, ứng dụng công nghệ thông tin sâu rộng hơn thì càng dễ bị tấn công và bị thiệt hại nặng nề. Trong chiến tranh mạng, các bên tham chiến không sử dụng khí tài quân sự truyền thống mà sử dụng lực lượng tinh nhuệ để lập trình, chế tạo, sản xuất và nhân bản hàng loạt vũ khí mạng đặc thù như mã độc, hệ thống công cụ tấn công mạng, tình báo mạng, gián điệp mạng... “Chiến tranh mạng” có tính nặc danh, diễn ra với tốc độ cực nhanh bởi không gian mạng mang tính toàn cầu và đối tượng phát động chiến tranh hoàn toàn có thể giả mạo hoặc lợi dụng hệ thống mạng của quốc gia trung gian để tấn công quốc gia khác. Dù được tiến hành trên không gian mạng nhưng hậu quả của chiến tranh mạng vượt ra ngoài không gian ảo và

có sức tàn phá, hủy diệt không kém, thậm chí vượt xa chiến tranh quân sự truyền thống.

Tác chiến không gian mạng và đối tượng tác chiến trên không gian mạng: “Tác chiến không gian mạng” là hoạt động đánh địch có tổ chức của lực lượng tác chiến không gian mạng trên không gian mạng nằm trong thế trận chiến tranh nhân dân nhằm bảo vệ chủ quyền quốc gia trên không gian mạng, bảo vệ hệ thống thông tin quan trọng quốc gia và bảo vệ độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

“Đối tượng tác chiến không gian mạng” là tổ chức, cá nhân có các hoạt động chuẩn bị tiến công hoặc tiến công xâm phạm chủ quyền quốc gia, trong đó có chủ quyền quốc gia trên không gian mạng, gây chiến tranh xâm lược hoặc phương hại đến độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: lực lượng quân sự nước ngoài có hoạt động xâm phạm chủ quyền quốc gia, chuẩn bị tiến công hoặc tiến công xâm lược nước ta; tổ chức, cá nhân tiến công vào các kết cấu hạ tầng quân sự, quốc phòng; tổ chức, cá nhân tiến công vào các kết cấu hạ tầng quan trọng của quốc gia trong phạm vi quản lý, phối hợp bảo vệ.

4. Tình hình an ninh mạng, tội phạm công nghệ cao trên thế giới và ở Việt Nam

Thứ nhất, hệ thống mạng thông tin Việt Nam phát triển nhanh, nhưng kết cấu hạ tầng chưa đáp ứng đầy đủ yêu cầu phòng, chống tội phạm mạng và bảo đảm an ninh, an toàn không gian mạng quốc gia. Việc áp dụng các biện pháp bảo

đảm an toàn, an ninh mạng và thông tin mạng quốc gia chưa được các cơ quan, tổ chức, doanh nghiệp chú trọng; chưa có quy trình, thao tác xử lý khi xảy ra sự cố, thậm chí còn buông lỏng, không áp dụng biện pháp bảo đảm an ninh thông tin, an ninh không gian mạng. Mức độ nhận biết các loại hình tấn công mạng, áp dụng các giải pháp bảo đảm an ninh thông tin, ban hành các quy trình thao tác phản ứng xử lý sự cố thông tin chưa cao.

Thứ hai, hoạt động tấn công mạng nhằm vào hệ thống thông tin Việt Nam diễn ra nghiêm trọng, đòi hỏi phải có hệ thống giải pháp tổng thể, toàn diện như sử dụng không gian mạng để tấn công nhằm phá hoại, gây đình trệ hệ thống hạ tầng công nghệ thông tin, hoạt động của cơ quan, tổ chức và cá nhân. Mục tiêu tấn công là các hệ thống thông tin quan trọng như: hệ thống điều khiển giao thông đường bộ, đường hàng không, cung cấp điện, nước, điều khiển nông nghiệp công nghệ cao; các sân bay, nhà ga, bến cảng, kho bạc, ngân hàng...

Tấn công vào cơ sở dữ liệu của các cơ quan, tổ chức, tập đoàn kinh tế lớn nhằm thu thập, đánh cắp thông tin, dữ liệu. Tháng 7/2016, trang web của Vietnam Airlines bị hacker tấn công và hậu quả là trên 400.000 tài khoản của khách hàng thuộc chương trình Bông sen vàng đã bị lộ; trong các ngày 08, 09, 10/3/2017, tin tặc đã tấn công, thay đổi giao diện website Cảng hàng không quốc tế Tân Sơn Nhất, Đà Nẵng, Phú Quốc, Rạch Giá...

Thứ ba, tội phạm sử dụng mạng máy tính gia tăng với mức độ ngày càng nghiêm trọng, nổi lên là lừa đảo chiếm đoạt tài sản thông qua hoạt động kinh doanh đa cấp, thương

mại điện tử; gian lận, trộm cắp trong hoạt động thanh toán thẻ và thanh toán điện tử; trộm cắp, mua bán thông tin thẻ tín dụng nhằm chiếm đoạt tài sản; đánh bạc và tổ chức đánh bạc thông qua mạng internet; trộm cắp tài khoản người dùng mạng xã hội để lừa đảo chiếm đoạt tài sản; truyền bá, phát tán ấn phẩm đồi trụy, tổ chức môi giới mại dâm, phát tán thông tin xuyên tạc, hình ảnh riêng tư để xúc phạm, làm nhục người khác (Năm 2019, các đơn vị chức năng Bộ Công an đã khởi tố đối với hơn 1.000 bị can; bắt và bàn giao Cảnh sát các nước trên 500 đối tượng hoạt động sử dụng không gian mạng thực hiện hành vi phạm tội).

Nhiều vụ chiếm quyền điều khiển máy tính, thiết bị số, truy cập bất hợp pháp vào hệ thống công nghệ thông tin của các cơ quan, tổ chức, doanh nghiệp, chiếm quyền điều khiển từ xa, thay đổi giao diện website hoặc cơ sở dữ liệu... nhằm mục đích tống tiền hoặc hạ uy tín của các đơn vị này (Trong vụ tấn công bằng mã độc WannaCry năm 2017, Việt Nam có trên 1.900 máy tính bị lây nhiễm mã độc này, trong đó có khoảng 1.600 máy tính của gần 250 cơ quan, tổ chức, doanh nghiệp).

Thứ tư, hoạt động sử dụng không gian mạng để xâm phạm an ninh quốc gia của các thế lực thù địch, phản động ngày càng phức tạp và nguy hiểm, tuyên truyền phá hoại tư tưởng, phá hoại nội bộ, kích động biểu tình, bạo loạn, lật đổ chính quyền, thông qua các trang mạng xã hội để liên minh, liên kết, móc nối trong ngoài, tập hợp lực lượng nhằm lật đổ chính quyền đương nhiệm không thân Mỹ tại một số quốc gia, điển hình là phong trào “Cách mạng hoa nhài” hay “Mùa xuân Ả rập” thời gian qua.

Triệt để sử dụng mạng xã hội thực hiện âm mưu “diễn biến hòa bình”, đẩy mạnh khoét sâu các mâu thuẫn tồn tại trong xã hội để hô hào, kích động người dân xuống đường biểu tình, kêu gọi các quốc gia khác can thiệp và tập hợp lực lượng nhằm lật đổ chính quyền; tuyên truyền gây mất đoàn kết và phá hoại nội bộ lãnh đạo, gây suy giảm lòng tin của quần chúng nhân dân với Đảng, Nhà nước.

Thứ năm, công tác quản lý nhà nước về an toàn, an ninh mạng và thông tin mạng quốc gia chưa đáp ứng yêu cầu trong tình hình mới. Trong những năm qua, Việt Nam đã chứng kiến những bước phát triển kinh tế ngoạn mục, nhờ những quyết sách, định hướng đúng đắn của Đảng, Nhà nước về phát triển, ứng dụng công nghệ thông tin, với những bước đi, lộ trình phù hợp, coi khoa học - công nghệ là một ngành kinh tế mũi nhọn để thúc đẩy kinh tế tri thức, tạo sự chuyển biến trong các chuỗi giá trị từ trong nước để hội nhập với toàn cầu; đồng thời, biết nắm bắt thời cơ, vận hội mới, tranh thủ các thành tựu khoa học - công nghệ tiên tiến để đẩy nhanh hơn tiến trình công nghiệp hóa, hiện đại hóa đất nước, ngày càng hội nhập sâu rộng, hiệu quả hơn vào nền kinh tế thế giới, không ngừng nâng cao tiềm lực về quốc phòng, an ninh (Theo số liệu thống kê tính đến tháng 01/2020, Việt Nam có 68,17 triệu người sử dụng internet, chiếm gần 70% dân số, nằm trong top 20 quốc gia có tỷ lệ người dùng internet cao nhất thế giới).

Tuy nhiên, sự phát triển của các thiết bị di động thông minh có kết nối mạng đang đặt ra nhiều thách thức đối với công tác quản lý.

5. Một số kiến nghị, đề xuất về chủ trương, giải pháp bảo đảm chủ quyền quốc gia trên không gian mạng hiện nay

(1) Mục tiêu cụ thể: Nâng cao hiệu lực quản lý nhà nước về an toàn, an ninh mạng và thông tin mạng quốc gia.

- Cơ bản hoàn thiện hệ thống văn bản quy phạm pháp luật về an ninh thông tin, an ninh mạng, bảo đảm đồng bộ, thống nhất và có sự phân công, phân cấp rõ ràng trong quản lý nhà nước.

- Tiếp tục kiện toàn bộ máy tổ chức của cơ quan quản lý nhà nước về an toàn, an ninh mạng và thông tin mạng quốc gia.

- Thực hiện nghiêm công tác hướng dẫn, thanh tra, kiểm tra, xử lý, giám sát việc thực hiện các quy định của pháp luật về an toàn, an ninh mạng và thông tin mạng quốc gia. Hoàn thành các tiêu chuẩn, quy chuẩn về an toàn, an ninh mạng và thông tin mạng quốc gia phù hợp với xu thế phát triển, đáp ứng được yêu cầu quản lý trong thời kỳ mới.

(2) Những giải pháp chủ yếu:

Thứ nhất, hoàn thiện, nâng cao năng lực bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia cho các cơ quan, ban, ngành, địa phương; các công trình hạ tầng trọng yếu có kết nối mạng, các tập đoàn kinh tế quan trọng.

(i) Kiện toàn bộ máy, tổ chức, nhân sự có kiến thức, đủ năng lực về an toàn, an ninh mạng và thông tin mạng quốc gia tại các cơ quan trung ương và địa phương.

(ii) Hình thành nguồn nhân lực chất lượng cao về an toàn, an ninh thông tin, an ninh mạng, đáp ứng nhu cầu về

cán bộ an toàn, an ninh mạng và thông tin mạng quốc gia cho các cơ quan nhà nước.

(iii) Đội ngũ nhân lực về an toàn, an ninh mạng và thông tin mạng quốc gia có khả năng làm chủ công nghệ, hạn chế và tiến tới không phụ thuộc vào công nghệ và thiết bị của nước ngoài.

(iv) Hoàn thiện hệ thống hạ tầng thông tin, thiết bị công nghệ thông tin bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia cho các cơ quan trung ương và địa phương; các công trình hạ tầng trọng yếu, các tập đoàn kinh tế quan trọng có kết nối mạng.

(v) Các hệ thống thông tin quan trọng quốc gia được xác định, áp dụng các biện pháp bảo vệ tương xứng, liên tục từ giai đoạn thiết kế, xây dựng, phát triển, vận hành và sử dụng.

(vi) Tập trung được nguồn lực toàn xã hội trong bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia.

(vii) Nhà nước bảo đảm kinh phí cho công tác an toàn, an ninh mạng và thông tin mạng quốc gia.

Thứ hai, xây dựng môi trường không gian mạng lành mạnh.

(i) Nhận thức, năng lực bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia của toàn xã hội được nâng cao. Người sử dụng có kiến thức cơ bản về bảo mật trong môi trường mạng; thường xuyên được cập nhật về tình hình, mức độ rủi ro mất an toàn thông tin để có thể tự phòng ngừa hiệu quả. Hệ thống mạng thông tin bảo đảm các tiêu chuẩn về bảo mật.

(ii) Các doanh nghiệp công nghệ thông tin trong nước lớn mạnh, làm chủ thị trường, không bị lệ thuộc vào sản phẩm của nước ngoài.

(iii) Các loại hình báo chí chính thống giữ vai trò chủ đạo, định hướng dư luận để đủ sức đề kháng đối với các thông tin xấu, độc trên không gian mạng.

(iv) Huy động sức mạnh của cả hệ thống chính trị và toàn dân trong đấu tranh phản bác, vô hiệu hóa các thông tin xấu, luận điệu phản tuyên truyền trên không gian mạng.

Thứ ba, xây dựng lực lượng chuyên trách đủ năng lực, chủ động đối phó với mọi nguy cơ xảy ra trên không gian mạng.

(i) Lực lượng chuyên trách bảo đảm an ninh thông tin, an ninh không gian mạng quốc gia trực thuộc Bộ Công an; lực lượng thực hiện nhiệm vụ quốc phòng trên không gian mạng trực thuộc Bộ Quốc phòng; lực lượng bảo đảm an toàn thông tin trực thuộc Bộ Thông tin và Truyền thông đủ năng lực, sẵn sàng, chủ động đối phó với mọi nguy cơ xảy ra trên không gian mạng.

(ii) Đội ngũ chuyên gia an ninh mạng có năng lực xử lý các sự cố, tình hình an ninh thông tin, an ninh mạng.

(iii) Hình thành các chuyên ngành đào tạo về an ninh thông tin, an ninh mạng.

(iv) Hoàn thiện cơ chế, chính sách thu hút các học sinh, sinh viên khá, giỏi theo học chuyên ngành an ninh thông tin, an ninh mạng; thu hút, trọng dụng, đãi ngộ các chuyên gia giỏi làm việc cho các cơ quan nhà nước.

(v) Nâng cao chất lượng đào tạo tại các trường trọng điểm về an toàn thông tin nhằm đáp ứng yêu cầu của tình hình mới.

Thứ tư, quan hệ hợp tác quốc tế trên lĩnh vực bảo đảm an toàn, an ninh thông tin, an ninh mạng được mở rộng và tăng cường.

(i) Mở rộng quan hệ hợp tác quốc tế với các nước trên thế giới về bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia, tranh thủ sự ủng hộ của cộng đồng quốc tế đấu tranh phản bác luận điệu sai trái của các thế lực thù địch chống Việt Nam.

(ii) Tham gia các công ước, thỏa thuận quốc tế về bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia, phòng, chống tội phạm mạng phù hợp với chủ trương, đường lối, chính sách, pháp luật của Đảng, Nhà nước.

(iii) Triển khai có hiệu quả, thiết thực các nghị định thư, thỏa thuận hợp tác về phòng, chống tội phạm mạng đã ký kết với các nước.

Tăng cường hợp tác với các nước có trình độ phát triển cao về công nghệ thông tin để đào tạo nguồn nhân lực, tiếp thu khoa học, công nghệ mới, học hỏi kinh nghiệm bảo đảm an toàn, an ninh mạng và thông tin mạng quốc gia.

*

* *

Chủ quyền quốc gia trên không gian mạng là quyền tối cao, tuyệt đối, đầy đủ và riêng biệt của quốc gia đối với các vùng thông tin do nhà nước quản lý, kiểm soát trực tiếp hoặc gián tiếp bằng chính sách, pháp luật và năng lực công nghệ phù hợp với luật pháp quốc tế và quy định của luật pháp quốc tế.

Các quốc gia có quyền tối cao, tuyệt đối, hoàn toàn và riêng biệt đối với phạm vi không gian mạng thuộc quyền kiểm soát của mình, tức là có chủ quyền quốc gia trên không gian mạng; việc xác định chủ quyền quốc gia trên không gian mạng là quyền kiểm soát, chi phối trên cơ sở chủ quyền,

lợi ích quốc gia và luật pháp quốc tế. Thực chất việc quốc gia xác lập chủ quyền không gian mạng là xác lập quyền quản lý, kiểm soát đối với kết cấu hạ tầng không gian mạng và thông tin được tạo ra, lưu trữ, xử lý và truyền đưa trên đó, được thực hiện thông qua xác lập chủ quyền, quyền tài phán theo luật pháp quốc tế đối với kết cấu hạ tầng mạng thuộc sở hữu cả ở trong và ngoài lãnh thổ quốc gia; đồng thời mã hóa thông tin số truyền đưa trên không gian mạng toàn cầu.

XUẤT BẢN SÁCH LÝ LUẬN, CHÍNH TRỊ PHỤC VỤ SỰ NGHIỆP BẢO VỆ CHỦ QUYỀN QUỐC GIA TRONG TÌNH HÌNH MỚI

PGS.TS. PHẠM MINH TUẤN*

Trong quá trình xây dựng, trưởng thành và đảm nhận sứ mệnh lãnh đạo cách mạng Việt Nam, Đảng ta luôn xác định: Công tác tư tưởng, lý luận là một bộ phận cấu thành đặc biệt quan trọng trong toàn bộ hoạt động của Đảng; là lĩnh vực trọng yếu để xây dựng, bồi đắp nền tảng chính trị của chế độ, tuyên truyền, giáo dục, động viên và tổ chức nhân dân thực hiện các nhiệm vụ cách mạng, khẳng định và nâng cao vai trò tiên phong của Đảng về chính trị, lý luận, trí tuệ, văn hóa và đạo đức; thể hiện vai trò đi trước, mở đường trong sự nghiệp xây dựng và bảo vệ Tổ quốc¹. Là một bộ phận quan trọng trong công tác tư tưởng, lý luận của Đảng, sách lý luận, chính trị là một vũ khí sắc bén, công cụ đắc lực của Đảng trên mặt trận tư tưởng - văn hóa. Đặc biệt, trong bối cảnh toàn cầu hóa và Cách mạng công nghiệp lần thứ tư đang phát triển như vũ bão hiện nay, sách lý luận, chính trị càng phải phát huy hơn nữa vai trò tiên phong trong bảo vệ

* Giám đốc - Tổng Biên tập Nhà xuất bản Chính trị quốc gia Sự thật.

1. Xem Đảng Cộng sản Việt Nam: *Văn kiện Đảng toàn tập*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2017, t.66, tr.418.

nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch; góp phần xây dựng và bảo vệ Tổ quốc; bảo vệ chủ quyền quốc gia.

1. Vấn đề bảo vệ chủ quyền quốc gia trong tình hình mới

Chủ quyền quốc gia là quyền thiêng liêng, tối cao, bất khả xâm phạm của một quốc gia độc lập, được thể hiện trên mọi phương diện chính trị, an ninh, quốc phòng, ngoại giao, kinh tế, văn hóa, xã hội và được bảo đảm toàn vẹn, đầy đủ mọi mặt cả về lập pháp, hành pháp lẫn tư pháp của quốc gia trong phạm vi lãnh thổ của quốc gia mình. Nguyên tắc này được ghi nhận trong Hiến chương Liên hợp quốc, trong điều lệ của các tổ chức thuộc hệ thống Liên hợp quốc, của đại đa số các tổ chức quốc tế và khu vực, trong nhiều điều ước quốc tế đa phương, song phương và nhiều văn bản quốc tế quan trọng khác. Theo đó, tất cả các quốc gia, không phân biệt quy mô lãnh thổ, dân số, chế độ chính trị - xã hội, đều có chủ quyền quốc gia.

Đảng và Nhà nước ta luôn khẳng định chủ quyền quốc gia là thiêng liêng, bất khả xâm phạm và phải kiên quyết bảo vệ bằng mọi giá. Bảo vệ chủ quyền quốc gia không chỉ là giữ gìn độc lập, an ninh, thống nhất, toàn vẹn lãnh thổ, mà còn là bảo vệ chủ quyền chính trị, chủ quyền kinh tế, bảo tồn và phát huy bản sắc văn hóa, giá trị dân tộc, quyền độc lập trong quan hệ đối ngoại và nâng cao vị thế quốc tế của Việt Nam trên trường quốc tế.

Ngày nay, toàn cầu hóa là một xu thế phát triển khách quan của nhân loại. Các quốc gia không còn là những cá thể

riêng biệt mà được gắn bó chặt chẽ thông qua các mối liên kết từ chính trị, kinh tế, văn hóa đến an ninh, quốc phòng. Quá trình này mang đến những cơ hội, nhưng cũng đặt ra thách thức không nhỏ về bảo vệ chủ quyền quốc gia trên tất cả các lĩnh vực.

Đối với Việt Nam, vấn đề bảo vệ chủ quyền quốc gia đứng trước những thách thức như: âm mưu “diễn biến hòa bình”, can thiệp nội bộ, chi phối các vấn đề nội bộ quốc gia, tranh chấp chủ quyền lãnh thổ quốc gia, chủ quyền biển, đảo... Trước vấn đề này, Đảng ta khẳng định: “Bảo vệ độc lập, thống nhất, toàn vẹn lãnh thổ... là yêu cầu cấp thiết”¹, và “Bảo đảm cao nhất lợi ích quốc gia - dân tộc trên cơ sở các nguyên tắc cơ bản của Hiến chương Liên hợp quốc và luật pháp quốc tế, bình đẳng, hợp tác, cùng có lợi”².

Bên cạnh đó, *Cách mạng công nghiệp lần thứ tư, nhất là sự phát triển mạnh mẽ của công nghệ số, đã tạo đột phá trên nhiều lĩnh vực của đời sống xã hội, đặc biệt đã tạo một bước ngoặt vĩ đại trong lịch sử truyền thông nhân loại, xóa bỏ mọi ranh giới về không gian và thời gian. Với những phương tiện và phương thức truyền thông trên nền tảng kỹ thuật số, con người có thể tiếp cận, khai thác và sở hữu thông tin một cách nhanh chóng, chính xác và thuận tiện. Trong đó, sự ra đời của sách điện tử, sách nói cùng với các thiết bị đọc và phần mềm hỗ trợ đọc có thể sử dụng tiện ích trên máy tính, các thiết bị di động..., giúp người đọc có thể*

1, 2. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.I. tr.108, 161-162.

tiếp cận thông tin một cách nhanh nhất, tạo ra bước đột phá trong lĩnh vực xuất bản và phát triển văn hóa đọc.

Song, cùng với mặt tích cực, Cách mạng công nghiệp lần thứ tư cũng tạo ra những mặt trái, hệ lụy phức tạp mà các thế lực thù địch, phản động lợi dụng để chống phá Đảng, Nhà nước và xâm phạm chủ quyền quốc gia. Thực tiễn hiện nay cho thấy, vấn đề bảo vệ chủ quyền quốc gia không chỉ cấp thiết đối với không gian địa lý: đất liền, hải đảo, vùng biển và vùng trời, mà còn hết sức cần thiết trên không gian mạng (không gian ảo). Trên lĩnh vực không gian mạng, không phải một quốc gia, một chính phủ nào, mà bất kỳ một cá nhân, tổ chức, thậm chí cả những kẻ khủng bố... đều có thể gây ảnh hưởng trực tiếp đến quyền lực chính trị, nền chính trị. Các thế lực thù địch, phản động, cơ hội chính trị đã lợi dụng không gian mạng để chống phá Đảng, Nhà nước ta, xâm phạm an ninh thông tin. Chúng lợi dụng một số xuất bản điện tử, xuất bản phẩm không được cấp phép để lan truyền các thông tin xấu, độc, xuyên tạc với tốc độ cực nhanh, tiếp cận với số lượng người cực lớn nhằm chống phá, bôi nhọ, đánh lừa dư luận. Trong khi phản ứng của chúng ta, trong nhiều trường hợp, lại chưa kịp thời và tương xứng.

Như vậy, xu thế phát triển và tình hình trên đã mang lại nhiều thời cơ nhưng cũng đặt ra không ít thách thức đối với mỗi quốc gia, trong đó có Việt Nam. Việc bảo vệ chủ quyền quốc gia phụ thuộc rất nhiều vào yếu tố khách quan và chủ quan, chịu sự tác động của các nhân tố kinh tế, chính trị, quân sự..., trong đó, cần sự đi đầu của công tác tư tưởng chính trị, tạo sự đồng thuận về nhận thức và sự đoàn kết trong toàn Đảng, toàn quân, toàn dân.

2. Xuất bản sách lý luận, chính trị phục vụ sự nghiệp bảo vệ chủ quyền quốc gia trong tình hình mới

Là một vũ khí sắc bén trên mặt trận tư tưởng - văn hóa của Đảng, kết tinh từ kết quả nghiên cứu lý luận và tổng kết thực tiễn của cách mạng Việt Nam, sách lý luận, chính trị có vai trò, nhiệm vụ quan trọng, truyền tải những thông điệp, chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước đến với nhân dân, phục vụ nhu cầu thông tin, tri thức về lý luận, chính trị của các tầng lớp nhân dân, đáp ứng nhiệm vụ chính trị của đất nước. Hiện nay, cả nước có 59 nhà xuất bản và gần 300 đơn vị tham gia hoạt động liên kết xuất bản, trong đó mảng sách lý luận, chính trị chủ yếu tập trung ở các nhà xuất bản như: Nhà xuất bản Chính trị quốc gia Sự thật, Nhà xuất bản Công an nhân dân, Nhà xuất bản Quân đội nhân dân, Nhà xuất bản Lý luận chính trị, Nhà xuất bản Thông tin và Truyền thông... Trong bối cảnh Cách mạng công nghiệp lần thứ tư, các nhà xuất bản đã không ngừng nâng cao chất lượng, số lượng các đầu sách thực hiện nhiệm vụ chính trị, trong đó có nhiệm vụ bảo vệ chủ quyền quốc gia nói chung và bảo vệ chủ quyền quốc gia trên không gian mạng nói riêng, thể hiện ở những thành tựu cơ bản như:

Thứ nhất, sách lý luận, chính trị đã tuyên truyền, phổ biến chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước về bảo vệ chủ quyền quốc gia; phương châm, nguyên tắc giải quyết các vấn đề liên quan đến xâm phạm chủ quyền quốc gia.

Sách lý luận, chính trị đã khẳng định, phân tích, làm rõ chủ trương, đường lối của Đảng, chính sách, pháp luật của

Nhà nước, tư tưởng Hồ Chí Minh về vấn đề chủ quyền quốc gia, trong đó khẳng định: Chủ quyền quốc gia là điều tất yếu, là tuyệt đối, có ý nghĩa chiến lược, xuyên suốt quá trình cách mạng, chi phối các hoạt động lập pháp, hành pháp và tư pháp, đến mọi lĩnh vực hoạt động từ kinh tế, xã hội đến chính trị, từ văn hóa đến khoa học, từ ngoại giao đến quốc phòng, an ninh... của quốc gia, dân tộc. Những bộ sách lớn do Nhà xuất bản Chính trị quốc gia Sự thật xuất bản như: *Văn kiện Đảng toàn tập, Hồ Chí Minh toàn tập, Văn kiện Quốc hội toàn tập...* đều chứa đựng nội dung khẳng định: Việc thực hiện chủ quyền quốc gia cũng chính là việc thực hiện độc lập dân tộc, là tư tưởng chủ đạo, chi phối toàn bộ sự nghiệp cách mạng của Đảng ta.

Trong việc bảo vệ chủ quyền quốc gia, bảo vệ toàn vẹn lãnh thổ quốc gia, chủ quyền biển, đảo cũng là nhiệm vụ tối quan trọng. Đối với vấn đề này, các sách lý luận, chính trị đã cung cấp thông tin về các cứ liệu lịch sử, căn cứ pháp lý, luật pháp quốc tế để chứng minh về chủ quyền của Việt Nam đến với công chúng, một số cuốn sách là luận cứ trong các hồ sơ đệ trình tại các phiên tòa quốc tế. Có thể kể đến một số đầu sách tiêu biểu cung cấp bằng chứng lịch sử và cơ sở pháp lý khẳng định chủ quyền biển, đảo của Tổ quốc như: *Chủ quyền của Việt Nam đối với hai quần đảo Hoàng Sa và Trường Sa*, bộ sách *Văn hóa biển đảo Việt Nam* (9 tập), *Chủ quyền quốc gia Việt Nam trên Biển Đông, Tài nguyên, môi trường và chủ quyền biển, đảo Việt Nam...* (Nxb. Chính trị quốc gia Sự thật); *Những bằng chứng về chủ quyền của Việt Nam đối với hai quần đảo Hoàng Sa, Trường Sa, Đội Hoàng Sa, từ cội nguồn đến lễ tri ân* (Nxb. Giáo dục); *Bằng chứng lịch sử và*

cơ sở pháp lý Hoàng Sa, Trường Sa là của Việt Nam (Nxb. Trẻ); *Chủ quyền của Việt Nam ở Hoàng Sa, Trường Sa - Tư liệu và sự thật lịch sử* (Nxb. Đại học Quốc gia Hà Nội),... Đây là những tài liệu quan trọng để khẳng định và bảo vệ chủ quyền biển, đảo thiêng liêng của Tổ quốc.

Bên cạnh đó, nhiều sách lý luận, chính trị đã nghiên cứu, phân tích làm rõ về chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước về xây dựng một nền kinh tế độc lập, tự chủ; một nền chính trị ổn định; một nền văn hóa, tiên tiến, đậm đà bản sắc dân tộc; một nền ngoại giao toàn diện, hiện đại; một nền quốc phòng, an ninh vững mạnh... Đây cũng chính là những nội dung quan trọng cốt yếu để bảo vệ chủ quyền quốc gia trên các lĩnh vực kinh tế, văn hóa, ngoại giao, quốc phòng, an ninh..., được các nhà xuất bản chú trọng với nhiều ấn phẩm có chất lượng, trong đó có thể kể đến một số cuốn sách được xuất bản gần đây như: *Kinh tế Việt Nam - Thăng trầm và đột phá*, *Các thành phần kinh tế Việt Nam: Vấn đề và định hướng chính sách*, *Vấn đề an ninh phi truyền thống trong quan hệ quốc tế hiện nay*, *Đối ngoại quốc phòng*, *Phòng ngừa các tội phạm an ninh quốc gia ở Việt Nam hiện nay*, *Ngoại giao Việt Nam* (Sách xanh ngoại giao, xuất bản hằng năm)... (Nxb. Chính trị quốc gia Sự thật)... Nội dung của những cuốn sách này đã chuyển tải một khối lượng thông tin phong phú, bảo đảm tính khoa học, thực tiễn, là những cứ liệu toàn diện về vấn đề thực hiện chủ quyền và quyền chủ quyền quốc gia trên tất cả các lĩnh vực của đời sống xã hội. Việc xuất bản và tuyên truyền rộng rãi các cuốn sách này đã góp phần củng cố nền tảng tư tưởng của Đảng đối với việc thực hiện công

cuộc đổi mới, phát triển toàn diện đất nước và hội nhập quốc tế sâu rộng trên tất cả các lĩnh vực.

Thứ hai, sách lý luận, chính trị cung cấp thông tin, làm rõ âm mưu, thủ đoạn xâm phạm chủ quyền quốc gia và lật đổ chế độ xã hội chủ nghĩa ở Việt Nam của các thế lực thù địch.

Thông qua lăng kính đa chiều và nhìn nhận một cách khách quan, nội dung các sách lý luận, chính trị đã nhận diện rõ các quan điểm sai trái của các thế lực thù địch như: phủ nhận, hạ thấp vai trò của chủ nghĩa Mác - Lênin; xuyên tạc tư tưởng Hồ Chí Minh; phủ nhận vai trò lãnh đạo của Đảng Cộng sản Việt Nam; xuyên tạc, phủ định các quan điểm, chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước, phủ nhận mục tiêu và con đường đi lên chủ nghĩa xã hội của Việt Nam; vu cáo Việt Nam vi phạm dân chủ, nhân quyền, cố tình đổi trắng thay đen, dựng chuyện Việt Nam đàn áp tôn giáo, kỳ thị, phân biệt đối xử với các dân tộc thiểu số... Để cung cấp các luận cứ đấu tranh với các âm mưu, thủ đoạn xâm phạm chủ quyền quốc gia, lật đổ chế độ xã hội chủ nghĩa của các thế lực thù địch, các sách lý luận, chính trị được xuất bản ở nước ta như: *Đấu tranh phòng, chống “diễn biến hòa bình” ở nước ta hiện nay*, Phòng, chống “diễn biến hòa bình” ở Việt Nam - Mệnh lệnh cuộc sống (Nxb. Chính trị quốc gia Sự thật); *Phòng, chống “diễn biến hòa bình” trên lĩnh vực quốc phòng*, Phòng, chống “diễn biến hòa bình” trên lĩnh vực văn hóa, Phòng, chống “diễn biến hòa bình” trên lĩnh vực kinh tế, Phòng, chống “diễn biến hòa bình” trên lĩnh vực chính trị, tư tưởng, Phòng, chống “diễn biến hòa bình” ở Việt Nam trong tình hình mới, Chiến lược

“diễn biến hòa bình” - Nhận diện và đấu tranh (9 tập)...
(Nxb. Quân đội nhân dân)...

Đặc biệt, ngày 22/10/2018, Bộ Chính trị đã ban hành Nghị quyết số 35-NQ/TW về *Tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới*. Thực hiện Nghị quyết này, trong một thời gian ngắn đã có nhiều công trình được nghiên cứu và xuất bản.

Là cơ quan xuất bản, phát hành sách lý luận, chính trị nòng cốt của Đảng và Nhà nước, thời gian qua, Nhà xuất bản Chính trị quốc gia Sự thật luôn xác định việc xuất bản sách bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch là một nhiệm vụ chính trị trọng tâm; cung cấp thông tin chính thống, bảo đảm sự chính xác về nội dung chính trị, khoa học của xuất bản phẩm, từ đó góp phần quan trọng giữ vững và mở rộng trận địa tư tưởng của Đảng. Nhiều cuốn sách chất lượng đã được xuất bản như: *Luận cứ phê phán các quan điểm sai trái, thù địch; Phê phán các quan điểm sai trái, bảo vệ nền tảng tư tưởng, cương lĩnh, đường lối của Đảng Cộng sản Việt Nam; Phê phán các quan điểm sai trái, xuyên tạc cuộc đấu tranh chống suy thoái về tư tưởng chính trị, những biểu hiện “tự diễn biến”, “tự chuyển hóa” về chính trị trong Đảng...* Đặc biệt, tháng 9/2021, Nhà xuất bản Chính trị quốc gia Sự thật đã ra mắt *Tủ sách Bảo vệ nền tảng tư tưởng của Đảng*, bao gồm các ấn phẩm tiêu biểu về chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, văn kiện Đảng; sách khẳng định vai trò lãnh đạo, cầm quyền của Đảng Cộng sản Việt Nam; sách học tập tư tưởng, đạo đức, phong cách Hồ Chí Minh; sách bảo vệ

chủ quyền, an ninh quốc gia; sách đấu tranh phòng, chống biểu hiện “tự diễn biến”, “tự chuyển hóa” trong nội bộ; sách nhận diện các âm mưu, thủ đoạn chống phá sự nghiệp xây dựng và bảo vệ Tổ quốc của các thế lực thù địch;... Bên cạnh đó, Nhà xuất bản Chính trị quốc gia Sự thật đã phối hợp với Bộ Công an tổ chức biên soạn, xuất bản các ấn phẩm sách lý luận, chính trị và tổ chức các hội thảo khoa học, như: *Trách nhiệm nêu gương của cán bộ, đảng viên Công an nhân dân trong tình hình mới; 50 năm Công an nhân dân thực hiện Di chúc của Chủ tịch Hồ Chí Minh; Tư tưởng Hồ Chí Minh về Công an nhân dân - Giá trị lý luận và thực tiễn; Tư tưởng Hồ Chí Minh về vai trò của nhân dân trong sự nghiệp giữ gìn trật tự, an ninh...*; lịch sử truyền thống ngành; giới thiệu và phân tích những điểm mới, nội dung cốt lõi về an ninh quốc gia trong Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII của Đảng... Các hoạt động có ý nghĩa này đã góp phần quan trọng củng cố niềm tin, sự trung thành tuyệt đối của cán bộ, chiến sĩ lực lượng Công an nhân dân vào sự lãnh đạo của Đảng; xây dựng lực lượng Công an nhân dân cách mạng, chính quy, tinh nhuệ, từng bước hiện đại.

Thứ ba, với sự phát triển các nền tảng số trong cuộc Cách mạng công nghiệp lần thứ tư, sách lý luận, chính trị đã bước đầu được đổi mới với các dạng thức mới như: sách điện tử, sách nói..., để đáp ứng yêu cầu bảo vệ chủ quyền quốc gia trong tình hình mới.

Thích ứng với xu thế phát triển của thời đại Cách mạng công nghiệp lần thứ tư, đối với nhiệm vụ bảo vệ chủ quyền quốc gia, bên cạnh xuất bản sách giấy, sách lý luận, chính trị đang được đẩy mạnh phát triển sách điện tử e-book. Sách

điện tử có thể là “phiên bản điện tử của một cuốn sách in”, nhưng cũng có một số sách điện tử tồn tại mà không có một bản in tương đương...; được đọc trên nhiều thiết bị kỹ thuật số khác nhau như: máy vi tính, máy tính bảng, điện thoại thông minh, hay chuyên nghiệp hơn là máy đọc sách điện tử - eReader (như: Kindle của Amazon; Rakuten Kobo; Barnes & Noble’s Nook...).

Xuất bản phẩm điện tử của Việt Nam hiện chủ yếu là các hình thức sách được số hóa từ sách đã được xuất bản lần đầu dưới dạng sách in và phát hành trên internet, hoặc thông qua các ứng dụng cài đặt vào các thiết bị cá nhân như máy tính, smartphome, tablet... Hiện nay, Việt Nam đã có 15 đơn vị (gồm 11 nhà xuất bản, 4 đơn vị) được cấp phép xuất bản và phát hành xuất bản phẩm điện tử; đây vẫn là con số nhỏ bé so với 59 nhà xuất bản cùng gần 300 đơn vị tham gia vào hoạt động liên kết xuất bản trên cả nước.

Hiện nay, sách điện tử lý luận, chính trị chủ yếu được xuất bản tại Nhà xuất bản Chính trị quốc gia Sự thật, Nhà xuất bản Công an nhân dân, Nhà xuất bản Quân đội nhân dân... *Sự tương tác trên các nền tảng số giúp cho các đơn vị xuất bản sách lý luận, chính trị thuận lợi và dễ dàng hơn trong việc đưa các loại sách này đến với đông đảo cán bộ, đảng viên và nhân dân bằng nhiều hình thức khác nhau; từ đó thực hiện tuyên truyền, phổ biến, bảo vệ và phát triển chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước, bảo vệ chủ quyền quốc gia trên tất cả các lĩnh vực kinh tế, chính trị, văn hóa, xã hội, quốc phòng, an ninh, đối ngoại...* Bên cạnh đó, với dữ liệu được lưu trữ trên không gian mạng,

các nhà lãnh đạo, quản lý, nhà khoa học có thể đối chiếu, so sánh các nội dung nhanh và theo nhiều tiêu chí, từ đó nhanh chóng, có cơ sở vững chắc, tăng tính thuyết phục cho các lập luận, phản bác các quan điểm sai trái, thù địch.

Nhà xuất bản Công an nhân dân là một trong những nhà xuất bản có uy tín trong cả nước, có nhiều ấn phẩm chất lượng cung cấp cho lực lượng Công an và xã hội khối lượng lớn thông tin, kiến thức trên nhiều lĩnh vực chính trị, đặc biệt là vấn đề an ninh quốc gia. Năm 2016, Nhà xuất bản Công an nhân dân đã ra mắt *Hệ thống phát hành sách điện tử*, cung cấp những ấn phẩm về lĩnh vực an ninh, trật tự, xây dựng lực lượng Công an nhân dân... Nhà xuất bản Quân đội nhân dân cũng không ngừng đẩy mạnh và phát triển hệ thống xuất bản điện tử trên *EbookQĐND* với các loại hình như sách điện tử, sách nói, sách video, giúp người đọc có cơ hội cập nhật tri thức, thông tin chính thống một cách nhanh nhất, góp phần tuyên truyền, bảo vệ chủ quyền quốc gia trên không gian mạng.

Đặc biệt, Nhà xuất bản Chính trị quốc gia Sự thật - nhà xuất bản của Đảng và Nhà nước, là đơn vị xuất bản hàng đầu về sách lý luận, chính trị cũng có nhiều nỗ lực trong xuất bản sách điện tử. Trong đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch trên không gian mạng, Nhà xuất bản đã ra mắt *Tủ sách điện tử Bảo vệ nền tảng tư tưởng của Đảng* trên *Stbook.vn* với khoảng 50 đầu sách điện tử. Toàn thể cán bộ, đảng viên và nhân dân khi đăng ký tài khoản trên hệ thống *Stbook.vn* sẽ được đọc miễn phí. Trong thời gian tới, Nhà xuất bản tiếp tục xây dựng *Tủ sách chi bộ*, *Tủ sách Nhà nước và pháp luật*, *Tủ sách thông tin đối ngoại*, *Tủ sách giáo dục lý luận chính trị*...

và bổ sung nhiều ấn phẩm điện tử trên hệ thống xuất bản điện tử: *Stbook.vn* và *thuvienoso.vn* để phục vụ cán bộ, đảng viên và nhân dân đọc, tra cứu miễn phí các ấn phẩm có giá trị này. Các sách giấy đều có mã QR-Code chỉ dẫn đến bản sách điện tử.

Bên cạnh kết quả đạt được, việc xuất bản sách lý luận, chính trị với nhiệm vụ bảo vệ chủ quyền quốc gia nói chung, chủ quyền quốc gia trên không gian mạng nói riêng còn những hạn chế nhất định: Dù có nhiều đầu sách lý luận, chính trị về chủ đề này, nhưng số sách hay, có giá trị cao chưa nhiều, các sách còn khá đơn điệu, khô khan, nhất là những sách chuyên sâu về bảo vệ nền tảng tư tưởng của Đảng, đấu tranh, phản bác các quan điểm sai trái, thù địch; vẫn còn tình trạng sai sót về nội dung, quan điểm, dẫn đến một số hệ lụy, ảnh hưởng đến lợi ích quốc gia, dân tộc. Đặc biệt, việc thực hiện việc ứng dụng công nghệ thông tin và chuyển đổi số trong xuất bản sách lý luận, chính trị còn hạn chế, các hình thức của sách điện tử chưa được phổ biến..., trong khi đó, sách, báo của các thế lực thù địch lại tận dụng triệt để nền tảng số để lan truyền những quan điểm sai trái, xuyên tạc một cách nhanh chóng, điều này đặt ra vấn đề cần phải đổi mới, nâng cao hơn nữa công tác xuất bản điện tử, đáp ứng ngày càng tốt hơn nhiệm vụ bảo vệ chủ quyền quốc gia, đặc biệt là chủ quyền quốc gia trên không gian mạng.

3. Những vấn đề đặt ra và giải pháp xuất bản sách lý luận, chính trị đối với việc bảo vệ chủ quyền quốc gia trong tình hình mới

Từ vai trò và thực tiễn công tác xuất bản sách lý luận, chính trị, với tư cách là vũ khí sắc bén trên mặt trận tư tưởng -

văn hóa, việc xuất bản sách lý luận, chính trị đối với sự nghiệp bảo vệ chủ quyền quốc gia trong tình hình mới đặt ra những vấn đề sau:

Một là, xu thế toàn cầu hóa ngày càng phát triển, quá trình hội nhập quốc tế của nước ta ngày càng sâu rộng, do đó cuộc đấu tranh chống các quan điểm sai trái, thù địch về vấn đề chủ quyền quốc gia đặt ra nhiều vấn đề lý luận cần được làm sáng tỏ. Điều đó đòi hỏi phải tăng cường tổng kết thực tiễn, nghiên cứu lý luận để tiếp tục hoàn thiện hệ thống lý luận về đường lối đổi mới, về chủ nghĩa xã hội và con đường đi lên chủ nghĩa xã hội ở nước ta làm căn cứ tổ chức biên soạn các cuốn sách phục vụ trực tiếp cuộc đấu tranh bảo vệ chủ quyền quốc gia.

Hai là, hiện nay với sự phát triển mạnh mẽ của Cách mạng công nghiệp lần thứ tư đã tạo nên một “thế giới phẳng”, đặt ra những thách thức an ninh phi truyền thống, trong đó có an ninh mạng. Vì vậy, việc nghiên cứu lý luận và thực tiễn vấn đề này cũng được đặt ra cấp bách, trong đó sách lý luận, chính trị cần chuyển tải thông tin một cách chính xác, hệ thống, khoa học và kịp thời, đáp ứng nhiệm vụ chính trị đặt ra.

Ba là, trong thời đại Cách mạng công nghiệp lần thứ tư đang phát triển mạnh mẽ, với sự bùng nổ của công nghệ thông tin, các xuất bản phẩm được truyền tải với nhiều phương thức phong phú và hệ thống ngôn ngữ đa phương tiện như: văn bản, âm thanh, hình ảnh, video, tương tác,... Điều này đòi hỏi công tác xuất bản sách lý luận, chính trị phải đổi mới mạnh mẽ về nội dung, hình thức, phương thức

phát hành, ứng dụng công nghệ, các nền tảng số, đáp ứng yêu cầu nhiệm vụ trong tình hình mới.

Để giải quyết các vấn đề đặt ra, nhằm tiếp tục phát huy vai trò của sách lý luận, chính trị trong cuộc đấu tranh bảo vệ nền tảng tư tưởng của Đảng, cần tập trung làm tốt các giải pháp sau:

Thứ nhất, lấy “xây” để “chống”, lấy thông tin chính thống đẩy lùi thông tin xấu, độc; phát hiện, cổ vũ cái tốt, nhân rộng các điển hình, mô hình vì nước, vì dân, vì cộng đồng, đề cao lợi ích chung, nghĩa đồng bào, tinh thần tương thân tương ái... Đồng thời, đấu tranh mạnh mẽ, lên án, loại bỏ cái xấu, điều lệch lạc. Để thực hiện giải pháp này, cần nâng cao hiệu quả công tác lãnh đạo của Đảng, quản lý của Nhà nước và chú trọng công tác nghiên cứu, biên soạn, xuất bản sách lý luận, chính trị về bảo vệ chủ quyền quốc gia tạo nguồn bản thảo chất lượng, có giá trị khoa học và thực tiễn cao.

Thứ hai, định hướng, quản lý và phát triển các cơ quan báo chí, xuất bản, truyền thông; phát huy và nâng cao hơn nữa vai trò của các kênh thông tin truyền thông chính thống; tăng cường giáo dục nâng cao nhận thức và bản lĩnh chính trị, đạo đức nghề nghiệp trong đội ngũ người làm công tác xuất bản, báo chí, truyền thông... Tăng cường đầu tư để phát triển ngành xuất bản nói chung, xuất bản sách lý luận, chính trị nói riêng theo hướng hiện đại, phù hợp với xu thế phát triển của Cách mạng công nghiệp lần thứ tư, trong đó cần đầu tư về ứng dụng, phát triển công nghệ thông tin, xây dựng dữ liệu quốc gia về sách lý luận, chính trị. Các ấn phẩm được xuất bản với nhiều hình thức (sách giấy, sách điện tử...) để tạo sự lan tỏa “không giới hạn” và sự đồng

thuận về nhận thức trong mọi tầng lớp nhân dân về vấn đề chủ quyền quốc gia.

Thứ ba, cần xây dựng hệ thống quy định về rào cản kỹ thuật và rào cản pháp lý tạo cơ sở cho việc phát hiện, đấu tranh, xử lý... và để cho nguồn sách chính thống, tin cậy chiếm lĩnh hoàn toàn không gian mạng. Những cuốn sách có nhiều giá trị về tri thức, có tính thuyết phục, tính khoa học, tính thực tiễn cao phải được tuyên truyền, phổ biến rộng rãi trên không gian mạng.

Thứ tư, cần có sự vào cuộc quyết liệt hơn của các đơn vị chức năng thuộc Bộ Công an trong bảo vệ an ninh chính trị nội bộ ngành báo chí - xuất bản, kịp thời xử lý các hành vi can thiệp, sửa chữa nội dung sách và đăng tải nội dung sách sai lệch, phản động... trên không gian mạng.

Tóm lại, với thế và lực mới của đất nước, cơ hội đi liền với khó khăn và thử thách, sách lý luận, chính trị cần tiếp tục phát huy mạnh mẽ hơn nữa vai trò của mình trong việc tuyên truyền chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước; bảo vệ nền tảng tư tưởng của Đảng, đấu tranh chống các quan điểm sai trái của các thế lực thù địch; nâng cao nhận thức, niềm tin của cán bộ, đảng viên và nhân dân vào sự lãnh đạo của Đảng, quản lý của Nhà nước đối với bảo vệ chủ quyền thiêng liêng của quốc gia, dân tộc.

NGUY CƠ, THÁCH THỨC ĐẶT RA ĐỐI VỚI NHIỆM VỤ BẢO VỆ CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG TRONG TÌNH HÌNH MỚI

Thiếu tướng, TS. PHẠM VIỆT TRUNG*

1. Nội hàm của khái niệm “chủ quyền quốc gia trên không gian mạng”

“Chủ quyền quốc gia” là thuật ngữ dùng để chỉ quyền thiêng liêng, bất khả xâm phạm của một quốc gia độc lập được thể hiện trên mọi phương diện chính trị, an ninh, quốc phòng, ngoại giao, kinh tế, văn hóa, xã hội và được bảo đảm toàn vẹn, đầy đủ mọi mặt cả lập pháp, hành pháp lẫn tư pháp của quốc gia trong phạm vi lãnh thổ của quốc gia mình. Có thể nhận thấy chủ quyền quốc gia là thuộc tính chính trị - pháp lý không thể tách rời của quốc gia, bao gồm hai nội dung, đó là: Quyền tối cao của quốc gia trong phạm vi lãnh thổ của mình và quyền độc lập của quốc gia trong quan hệ quốc tế.

Từ định nghĩa trên, chúng ta có thể thấy việc đặt ra nguyên tắc và hành lang pháp lý nhằm ghi nhận và bảo vệ

* Phó Tư lệnh - Tham mưu trưởng, Bộ Tư lệnh tác chiến không gian mạng, Bộ Quốc phòng.

chủ quyền quốc gia là rất quan trọng, tuy nhiên vấn đề cốt lõi là làm thế nào các quốc gia có thể bảo vệ chủ quyền của mình trong bối cảnh tình hình mới. Những năm gần đây, thế giới chứng kiến việc công dân của quốc gia này hoàn toàn có thể thực hiện các hoạt động dân sự hay chính trị trên lãnh thổ của quốc gia khác mà không cần có sự hiện diện về mặt thể nhân. Ví dụ, chúng ta ở Việt Nam nhưng vẫn có thể tham gia hoạt động mua sắm hay làm việc cho các công ty ở Mỹ. Các tập đoàn, công ty công nghệ mặc dù không có trụ sở, tài sản ở một quốc gia nhất định nhưng họ vẫn thực hiện các hoạt động kinh doanh, buôn bán, cung cấp dịch vụ cho người dân của các quốc gia này. Các cá nhân, tổ chức có thể sử dụng công nghệ cao, đặc biệt là mạng internet để can thiệp vào các hoạt động chính trị tại các quốc gia có chủ quyền. Năm 2020, Nga bị cáo buộc đã sử dụng các tài khoản Facebook, Twitter giả để can thiệp vào cuộc bầu cử Tổng thống Mỹ bằng việc định hướng tâm lý cử tri theo hướng có lợi cho cựu tổng thống Donald Trump, ứng cử viên của Đảng Cộng hòa và tung thông tin sai lệch về ông Jode Biden, ứng cử viên của Đảng Dân chủ. Như vậy là các chủ thể ở bất cứ một quốc gia nào cũng có thể thực hiện các hoạt động trên không gian mạng với mục tiêu gây thiệt hại về kinh tế, chính trị cho cá nhân và tổ chức ở các quốc gia mà họ không cần hiện diện thể nhân.

Công nghệ ngày càng phát triển khiến cho việc thực hiện các chức năng vốn có của chính phủ như: Tiến hành bầu cử, thu thuế, quản lý và kiểm soát các hoạt động của các chủ thể trên phạm vi lãnh thổ quốc gia mình ngày càng trở nên ít rõ ràng hơn. Các chính phủ đang phải hoạt động trong những

khuôn khổ cực kỳ hạn chế mà Moises Naim, cố vấn cao cấp của Ngân hàng Thế giới gọi là “sự suy tàn của quyền lực”. Internet đã làm biến đổi xã hội, chính trị và cả quyền lực¹, nó cũng làm thay đổi các vấn đề liên quan đến việc thực thi chủ quyền quốc gia. Nếu như trước đây các quốc gia đã từng đổ máu để giữ vững chủ quyền của mình thông qua việc bảo vệ các đường biên giới thì giờ đây các đường biên giới gần như đã bị dịch chuyển. Vấn đề diện tích, quy mô của vùng lãnh thổ nằm dưới quyền cai trị của một quốc gia sẽ không còn có ý nghĩa tuyệt đối đối với cuộc sống của từng cá nhân. Vì vậy, việc bảo vệ chủ quyền quốc gia không chỉ là việc bảo vệ các đường biên giới mà được mở rộng hơn rất nhiều. Những cuộc tranh luận sôi nổi trên các diễn đàn quốc tế hiện nay phần lớn liên quan đến các quy tắc của không gian mạng và những thách thức mang tính hệ thống đối với việc quản trị toàn cầu trong không gian mạng. Các chính phủ đã nỗ lực không ngừng trong việc bảo vệ quyền vốn có của mình, theo đó khái niệm chủ quyền quốc gia trên không gian mạng ra đời.

Mặc dù đã có nhiều nỗ lực cho việc thống nhất các quan điểm thì cho đến nay, chủ quyền quốc gia trên không gian mạng vẫn còn là chủ đề gây nhiều tranh cãi. Nhiều quốc gia cho rằng nguyên tắc chủ quyền quốc gia dựa trên lãnh thổ là cơ sở pháp lý hiệu quả để xây dựng các quy phạm về an ninh mạng nhằm bảo vệ chủ quyền quốc gia trên không gian mạng. Theo đó, các quốc gia có quyền quản lý và áp dụng luật pháp quốc gia về không gian mạng trong phạm vi lãnh

1. Xem Moises Naim: *Sự suy tàn của quyền lực*, Nxb. Hồng Đức, Hà Nội, 2017.

thổ của mình theo quan điểm của luật pháp quốc tế. Do đó các công ty, tập đoàn cung cấp dịch vụ trên không gian mạng cần đặt hệ thống cơ sở hạ tầng trong phạm vi lãnh thổ của quốc gia để chính phủ của quốc gia đó có thể thực thi quyền quản lý. Tuy nhiên, điều này hoàn toàn bất khả thi về mặt thực tế, và câu hỏi đặt ra là vậy thì các quốc gia có quyền quản lý với các hoạt động của các chủ thể nếu họ không đặt hệ thống cơ sở hạ tầng tại quốc gia đó.

Để đạt được mục đích cuối cùng là các cá nhân và tổ chức có quyền truy cập sử dụng mạng cho mục đích cá nhân của mình nhưng không làm tổn hại đến lợi ích của các chủ thể khác cũng như không vi phạm quốc phòng, an ninh của các quốc gia có chủ quyền, nguyên tắc về chủ quyền quốc gia trên không gian mạng đã được hình thành. Trên phương diện hợp tác đa phương, các quốc gia đã thỏa thuận nhằm đưa ra nguyên tắc trong việc công nhận chủ quyền quốc gia trên không gian mạng. Theo nguyên tắc này, các quốc gia sẽ hợp tác để hỗ trợ lẫn nhau trong việc truy tìm nguồn gốc ban đầu của các cuộc tấn công mạng nhằm xác định các tác nhân cụ thể phải chịu trách nhiệm, đồng thời truy tố hoặc dẫn độ những cá nhân đó. Từ năm 2013 đến năm 2017, các chuyên gia trên lĩnh vực an ninh mạng đã xây dựng quy tắc hướng dẫn sử dụng mạng. Theo quy tắc này, các chủ thể không được tiến hành các hoạt động trên không gian mạng vi phạm chủ quyền của một quốc gia khác. Đồng thời, các quốc gia có quyền kiểm soát đối với việc truy cập và sử dụng không gian mạng để thực hiện các hoạt động trên phạm vi lãnh thổ của họ. Các quốc gia được yêu cầu phải tuân thủ và công nhận chủ quyền quốc gia của các quốc gia khác trên

không gian mạng, đồng thời có thể thực hiện một số biện pháp kiểm soát đối với không gian mạng của mình. Như vậy, cũng giống như khái niệm chủ quyền quốc gia trên bộ, trên biển, trên không và trong không gian vũ trụ, khái niệm chủ quyền quốc gia trên không gian mạng vẫn có cơ sở từ khái niệm chủ quyền quốc gia theo nghĩa truyền thống.

2. Nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng

Từ ý nghĩa nội hàm của khái niệm chủ quyền quốc gia trên không gian mạng, trong các văn bản quy phạm pháp luật của nước ta đã đưa ra định nghĩa về khái niệm này, làm cơ sở để thực hiện nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng, cụ thể: Theo Nghị định số 142/2016/NĐ-CP, ngày 14/10/2016 của Chính phủ, chủ quyền quốc gia trên không gian mạng là tất cả quyền của nhà nước đối với không gian mạng, phù hợp với quy định của luật pháp quốc tế. Luật an ninh mạng năm 2018 đã định nghĩa không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không giới hạn bởi không gian và thời gian.

Căn cứ vào những khái niệm trên, chúng ta có thể hiểu nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng là những chính sách, biện pháp của một quốc gia nhằm bảo vệ mạng lưới kết nối cơ sở hạ tầng công nghệ thông tin trong phạm vi quản lý. Nói như vậy không có nghĩa là nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng chỉ đơn

thuần là bảo vệ một không gian liên lạc với những trang thiết bị vật lý; bởi vì, như chúng ta đã biết, nhân loại đang bước vào Cách mạng công nghiệp lần thứ tư, với các đặc trưng: Kỹ thuật số, internet vạn vật (IoT), trí tuệ nhân tạo..., thì vai trò của không gian mạng càng trở nên đặc biệt quan trọng, đã trở thành một vùng lãnh thổ mới gắn chặt với chủ quyền, lợi ích, quốc phòng và an ninh quốc gia. Trong lĩnh vực quân sự - quốc phòng, không gian mạng đã trở thành môi trường tác chiến thứ 5 (trên bộ, trên biển, trên không, vũ trụ và không gian mạng), nơi tiến hành tác chiến mạng và tác chiến thông tin khi xảy ra chiến tranh cục bộ, xung đột vũ trang, tranh chấp tài nguyên, chủ quyền lãnh thổ, biển, đảo, cũng như xung đột sắc tộc, tôn giáo, hoạt động can thiệp, lật đổ, ly khai, khủng bố,...

Như vậy, có thể nói bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng là góp phần quan trọng bảo vệ độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc và lợi ích quốc gia - dân tộc; giữ vững môi trường hòa bình, ổn định để xây dựng và phát triển đất nước.

3. Nguy cơ, thách thức đặt ra đối với nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng trong tình hình mới

Nhìn lại tiến trình phát triển nhận thức cũng như hoạt động mà các quốc gia đã triển khai nhằm bảo vệ chủ quyền của mình trên không gian mạng, có thể thấy một số thách thức chung đối với thế giới cũng như tại Việt Nam như sau:

Thứ nhất, những thách thức do thiếu cơ sở pháp lý cũng như các cơ chế hợp tác quốc tế để bảo vệ chủ quyền quốc gia

trên không gian mạng. Thế giới đã đi đến nhiều đồng thuận trong việc cần phải bảo vệ chủ quyền quốc gia trên không gian mạng nhưng vẫn chưa đi đến thống nhất để có thể xây dựng, thiết lập các nguyên tắc pháp lý mang tính quốc tế đối với các hoạt động này. Năm 2011, Nga đưa ra sáng kiến về việc Liên hợp quốc nên xây dựng công ước về bảo đảm an ninh thông tin quốc tế trong đó đề cập các tiêu chuẩn điều phối hoạt động trên internet, các hoạt động liên quan đến chủ nghĩa khủng bố, hình sự, chính trị và quân sự. Tuy nhiên, sáng kiến này của Nga không được các quốc gia chấp thuận. Đến năm 2015, một nỗ lực để đạt được các thỏa thuận quốc tế nhằm xây dựng bộ quy tắc ứng xử trên không gian mạng tiếp tục được đưa ra. Các chuyên gia của Liên hợp quốc đã đi đến một thỏa thuận với bốn nguyên tắc nhằm bảo đảm hòa bình trong không gian mạng. Tuy nhiên, các quốc gia như Nga và Trung Quốc lại có những cách tiếp cận khác nhau đối với việc xây dựng các quy chuẩn chung này. Cho đến nay, thế giới mới chỉ có các thỏa thuận riêng lẻ giữa các quốc gia trong từng khu vực liên quan đến bảo đảm an ninh mạng mà chưa có các quy chuẩn pháp lý mang tính quốc tế để điều chỉnh các hoạt động trên lĩnh vực này. Liên minh châu Âu có Công ước Budapest năm 2001 nhằm thiết lập khuôn khổ pháp lý chung cho các quốc gia châu Âu trong công tác phòng, chống tội phạm mạng. Đến nay Công ước đã được đàm phán và mở rộng cho các quốc gia thành viên ở châu Á như: Nhật Bản, Philíppin. Tuy nhiên, Nga, Trung Quốc và Braxin lại cho rằng để công ước này trở thành công ước chung cho toàn thế giới cần phải đàm phán để xây dựng lại Công ước này bởi bản thân công ước được xây dựng dựa

trên những đặc thù của khu vực nên không phản ánh hết các điều kiện và nhu cầu của tất cả các quốc gia trên thế giới. Việc thiếu cơ sở pháp lý mang tính quốc tế khiến cho việc thực hiện các hoạt động bảo vệ chủ quyền trên không gian mạng của quốc gia gặp nhiều khó khăn, cũng như các hoạt động hợp tác, phối hợp trong bảo vệ chủ quyền của các quốc gia sẽ không được thúc đẩy trên thực tế.

Đối với khu vực ASEAN, trong những năm qua, các nước trong khu vực đã có mối quan hệ chặt chẽ, thường xuyên tổ chức nhiều cuộc hội thảo, họp bàn các cấp về chiến lược, định hướng, hoạt động hợp tác cụ thể về an toàn, an ninh mạng; ASEAN đã thống nhất xây dựng bộ tài liệu Cơ chế phối hợp an toàn mạng ASEAN và thành lập Ủy ban điều phối liên ngành ASEAN, đồng thời tiếp tục xây dựng bộ quy tắc trên không gian mạng của ASEAN nhằm hướng tới một không gian mạng tự cường trong khối ASEAN; trên tinh thần đó, Đại hội đồng Liên nghị viện Hiệp hội các nước Đông Nam Á lần thứ 42 (AIPA-42) đã thông qua Nghị quyết tăng cường an ninh mạng và bảo vệ dữ liệu hướng tới một không gian mạng tự cường trong ASEAN. Tại Việt Nam, trên cơ sở nhận thức, đánh giá đúng, đầy đủ, sâu sắc về những nguy cơ, thách thức đối với đất nước trên không gian mạng; Việt Nam đã xây dựng một hành lang pháp lý cơ bản đầy đủ về bảo vệ chủ quyền quốc gia trên không gian mạng cũng như bảo đảm an toàn, an ninh mạng, nổi bật là các nghị quyết của Bộ Chính trị: Nghị quyết số 29-NQ/TW, ngày 25/7/2018 về *Chiến lược bảo vệ Tổ quốc trên không gian mạng*; Nghị quyết số 30-NQ/TW, ngày 25/7/2018 về *Chiến lược an ninh*

mạng quốc gia và Luật an toàn thông tin mạng năm 2015, Luật an ninh mạng năm 2018,...

Thứ hai, liên quan đến năng lực thực thi của các quốc gia. Việc triển khai các hoạt động phòng, chống các cuộc tấn công trên không gian mạng, ngăn chặn tin tặc hay tội phạm công nghệ cao luôn gặp phải những giới hạn liên quan đến nguồn lực như năng lực thực thi của các cơ quan công quyền, hạn chế trong hệ thống hạ tầng công nghệ. Pháp luật của các quốc gia đôi khi lạc hậu hơn so với sự phát triển và thay đổi nhanh chóng của các hoạt động tội phạm dựa trên công nghệ số. Chính vì thế mà nhiều quốc gia đã và đang thiết lập không gian mạng riêng đáp ứng nhu cầu sử dụng mạng an toàn của người dân, trong đó có thể kể đến mạng internet riêng của Nga (Runet), hệ thống Đại Tường lửa của Trung Quốc (Great Firewall). Tại nước ta, nhiều người cũng đặt ra câu hỏi là: Liệu Việt Nam có nên thiết lập một hệ thống mạng riêng cho người Việt giống như những gì mà Trung Quốc đang thực hiện? Tuy nhiên cần phải thấy rằng, việc làm này đi ngược lại với tinh thần và nền tảng của cuộc cách mạng công nghệ số là kết nối vạn vật, không giới hạn không gian và thời gian. Điều đó chỉ chứng tỏ sự hạn chế hay sự bất lực của nhà nước trong việc kiểm soát các hoạt động trên không gian mạng. Phương án này cũng được cho là bất khả thi với các quốc gia có dân số không quá lớn. Do đó, các quốc gia trên thế giới nói chung và Việt Nam nói riêng cần phải tìm ra các phương thức toàn diện, phù hợp hơn trong việc quản lý và kiểm soát các hoạt động trên không gian mạng nhằm bảo vệ hòa bình, ổn định, bảo đảm các quyền cơ bản của con người mà không làm mất đi đặc tính ưu việt của công nghệ.

Thứ ba, thách thức trong việc xác định ranh giới giữa hoạt động bảo vệ chủ quyền quốc gia trên không gian mạng với các hoạt động được coi là vi phạm quyền tự do cơ bản của con người. Rõ ràng, để bảo vệ an ninh mạng, bảo vệ chủ quyền quốc gia thì các loại hoạt động tội phạm mạng, gián điệp mạng, khủng bố mạng... là các hoạt động bị cấm. Tuy nhiên, một thách thức đặt ra cho các cơ quan chức năng là làm thế nào để xác định được các hoạt động mạng gây thiệt hại cho an ninh quốc gia, trật tự công cộng, an toàn tài sản và tính mạng của người dân. Vẫn có những hoạt động đứng giữa lần ranh của hai thái cực và những xung đột giữa việc bảo vệ quyền kiểm soát của chính phủ với việc bảo vệ các quyền tự do cơ bản của người dân. Chính phủ Pháp đã từng có nhiều nỗ lực nhằm ngăn chặn các cá nhân tìm cách tải các phim hay nhạc bất hợp pháp trên internet nhưng lại gặp phải sự phản đối của người dân và điều này chỉ được thông qua gần đây sau những sự phản đối của các ca sĩ. Hay việc Liên minh châu Âu “yêu cầu tất cả các nhà cung cấp dịch vụ internet lưu giữ thông tin về lưu lượng email, truy cập vào các trang web và các cuộc gọi điện thoại qua internet trong 12 tháng”, yêu cầu này đã dẫn đến những phản ứng của một số nhóm. Điều này phần nào đó cũng giống như việc các thế lực phản động, cơ hội chính trị, một số tổ chức nhân quyền và một bộ phận người dân bày tỏ thái độ bất bình, lo ngại khi Quốc hội xây dựng, ban hành Luật an ninh mạng. Do vậy, việc các quốc gia áp đặt chủ quyền trên không gian mạng thông qua việc yêu cầu xác định rõ hơn các tác nhân không gian mạng không phải lúc nào cũng đạt được sự đồng

thuận hay ủng hộ từ phía người dân, bởi rất khó để xác định ranh giới của các hoạt động bảo vệ an ninh mạng với các hoạt động vi phạm quyền tự do cơ bản của con người.

4. Một số giải pháp nhằm bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng

Từ những thách thức đối với bảo vệ chủ quyền quốc gia trên không gian mạng trong thời gian qua, để bảo đảm công cuộc xây dựng và bảo vệ Tổ quốc trong thời kỳ mới, cần tập trung thực hiện các nội dung và giải pháp sau:

Một là, xác lập và thực thi đầy đủ chủ quyền, lợi ích, an ninh quốc gia của Việt Nam trên không gian mạng, trên cơ sở luật pháp quốc gia và pháp luật quốc tế.

Hai là, hoàn thiện cơ chế, chính sách, pháp luật về quản lý không gian mạng quốc gia phù hợp với xu thế phát triển, tạo môi trường không gian mạng lành mạnh; trước mắt cần tập trung xác định rõ trách nhiệm của cá nhân, tổ chức, doanh nghiệp trong nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng nhằm hạn chế tối đa những bất cập, chồng chéo về chức năng, nhiệm vụ của các ban, bộ, ngành trong quá trình thực hiện nhiệm vụ.

Ba là, chú trọng đầu tư, phát triển lực lượng tác chiến mạng của Bộ Quốc phòng, lực lượng an ninh mạng của Bộ Công an, các lực lượng bảo đảm an ninh, an toàn thông tin và lực lượng chuyên ngành công nghệ thông tin của các cấp, các ngành. Phòng vệ chủ động, sẵn sàng đáp trả kịp thời các mối đe dọa, bảo vệ vững chắc chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng. Xây dựng lực lượng an ninh mạng quốc gia chính quy, tinh nhuệ, hiện đại.

Bốn là, xây dựng thế trận quốc phòng toàn dân, thế trận an ninh nhân dân bảo vệ không gian mạng quốc gia với nòng cốt là lực lượng vũ trang. Coi trọng công tác tuyên truyền, giáo dục, vận động người sử dụng internet tuân thủ pháp luật, chuẩn mực đạo đức xã hội, văn hóa, đủ năng lực nhận biết, phân biệt đúng sai, thật giả, tích cực đấu tranh, phê phán các thông tin sai trái, bịa đặt, vu cáo, độc hại trên không gian mạng. Sớm hoàn thiện quy chuẩn văn hóa của những người đưa thông tin lên mạng, kịp thời chấn chỉnh trật tự, kỷ cương, chủ động đấu tranh phản bác các luận điệu sai trái tuyên truyền, phá hoại tư tưởng.

Năm là, xác định rõ vai trò, tầm quan trọng đặc biệt của phòng, chống chiến tranh thông tin, chiến tranh không gian mạng trong thực hiện nhiệm vụ bảo vệ không gian mạng quốc gia góp phần quan trọng vào sự nghiệp xây dựng và bảo vệ vững chắc Tổ quốc trong tình hình mới. Đây là nhiệm vụ vừa cấp bách, vừa lâu dài của cả hệ thống chính trị và toàn dân, nòng cốt là lực lượng vũ trang, đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý của Nhà nước và sự tham gia tích cực của toàn dân. Khuyến nghị các cơ quan, tổ chức cần chú trọng đầu tư cơ sở hạ tầng kỹ thuật; tăng cường nghiên cứu, tìm kiếm, triển khai các giải pháp phòng thủ, giám sát, bảo đảm cho các hệ thống thông tin, trọng tâm là hệ thống thông tin quân sự, quốc phòng và quan trọng quốc gia.

Sáu là, tăng cường công tác phối hợp giữa các ban, bộ, ngành, doanh nghiệp sở hữu và vận hành hạ tầng công nghệ thông tin, nhà cung cấp dịch vụ công, cung cấp nội dung trên

internet, nhà nghiên cứu và sản xuất các giải pháp bảo mật,... để phát huy sức mạnh tổng hợp, huy động tiềm lực đủ mạnh, thế mạnh của các lực lượng chuyên trách, từ đó nâng cao hiệu quả nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng.

Bảy là, đẩy mạnh, nâng cao hiệu quả đầu tư, nghiên cứu trong lĩnh vực an toàn thông tin, an ninh mạng; cần chú trọng đầu tư cơ sở hạ tầng kỹ thuật và tăng cường nghiên cứu, tìm kiếm, triển khai các giải pháp phòng thủ, giám sát, bảo đảm an toàn thông tin cho các hệ thống thông tin, ưu tiên hệ thống thông tin quân sự, quốc phòng và quan trọng quốc gia. Huy động mọi nguồn lực của hệ thống chính trị, toàn xã hội và tranh thủ nguồn lực quốc tế cho nhiệm vụ bảo vệ toàn vẹn vùng “lãnh thổ đặc biệt” của quốc gia.

Tám là, quản lý chặt chẽ các dịch vụ trên không gian mạng quốc gia cung cấp xuyên biên giới vào Việt Nam. Các tổ chức, doanh nghiệp, cá nhân nước ngoài cung cấp dịch vụ viễn thông, internet trên lãnh thổ Việt Nam phải tôn trọng chủ quyền và tuân thủ pháp luật Việt Nam; đặt cơ quan đại diện và máy chủ dữ liệu người dùng hoạt động trên lãnh thổ Việt Nam, theo yêu cầu của nhà nước Việt Nam.

*

* *

Không gian mạng mang lại lợi ích to lớn cho sự phát triển của các quốc gia trên thế giới. Nó trở thành một bộ phận không thể thiếu trong đời sống hiện nay, ảnh hưởng trực tiếp đến kinh tế, chính trị, xã hội và chủ quyền của mỗi quốc gia. Tuy nhiên, nó cũng đem lại những nguy cơ, thách thức lớn

cho mỗi quốc gia, đặc biệt là Việt Nam. Vì thế, xác định rõ những nguy cơ, thách thức từ không gian mạng, để bảo vệ chủ quyền của Việt Nam trên không gian mạng là nhiệm vụ trọng yếu, thường xuyên của toàn Đảng, toàn dân, toàn quân và cả hệ thống chính trị.

NÂNG CAO Ý THỨC LÀM CHỦ VÀ BẢO VỆ KHÔNG GIAN MẠNG CỦA CÁN BỘ, ĐẢNG VIÊN HIỆN NAY

PGS.TS. LÊ VĂN LỢI*

Với sự phát triển như vũ bão của khoa học - công nghệ, nhất là công nghệ thông tin, không gian mạng đã mang lại những lợi ích vô cùng to lớn cho xã hội, đồng thời cũng chứa đựng những nguy cơ gây ảnh hưởng đến an ninh chính trị, trật tự, an toàn xã hội, lợi ích quốc gia - dân tộc, quyền và lợi ích hợp pháp của tổ chức, công dân. Bảo vệ không gian mạng lành mạnh, an toàn được xác định là nhiệm vụ trọng tâm, chiến lược của các quốc gia nói chung, Việt Nam nói riêng. Để thực hiện thắng lợi nhiệm vụ trên, cần phát huy sức mạnh tổng hợp của các lực lượng, của cả hệ thống chính trị, huy động được sự tham gia đông đảo của cán bộ, đảng viên và nhân dân. Trong đó, vấn đề quan trọng, mang tính bản lề là phải nâng cao nhận thức, ý thức làm chủ và bảo vệ không gian mạng của cán bộ, đảng viên để thực sự trở thành “cư dân mạng” có trách nhiệm và tiếp tục hướng dẫn, giáo dục quần chúng nhân dân thực hiện tốt quyền,

* Phó Giám đốc Học viện Chính trị quốc gia Hồ Chí Minh.

nghĩa vụ, trách nhiệm theo các quy định của pháp luật về an ninh mạng.

1. Không gian mạng được hiểu là “mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian”¹.

Với sự phát triển nhanh chóng của khoa học - công nghệ và tốc độ bao phủ của internet ở Việt Nam hiện nay, không gian mạng đã trở thành không gian xã hội mới đáp ứng gần như mọi nhu cầu xã hội của cá nhân mà không bị giới hạn bởi không gian và thời gian, với độ mở và sự linh hoạt thậm chí còn lớn hơn đời sống xã hội trên thực tế. Đồng thời, không gian mạng cung cấp những tài nguyên, cơ sở dữ liệu thiết yếu bảo đảm hoạt động của các cơ quan, tổ chức, doanh nghiệp, nhất là những bộ phận hạ tầng quan trọng của quốc gia như tài chính, giao thông, năng lượng...; là môi trường tương tác hiệu quả giữa các cơ quan, tổ chức với người dân. Ở phạm vi rộng hơn, không gian mạng với nguồn tài nguyên số vô tận đã tác động tới tất cả các lĩnh vực kinh tế, chính trị, xã hội, trở thành không gian kiến tạo và gia tăng sức mạnh của quốc gia. Với ý nghĩa đó, không gian mạng được xem là phần “lãnh thổ đặc biệt”, “lãnh thổ mở rộng” của quốc gia, chứa đựng các lợi ích quốc gia - dân tộc, nơi các quốc gia xác định “biên giới mạng” và thực thi chủ quyền quốc gia trên không gian mạng. Bảo vệ an ninh, an toàn không gian mạng quốc gia là yêu cầu hết sức cần thiết, góp

1. Điều 2, Luật an ninh mạng năm 2018.

phần bảo vệ vững chắc an ninh quốc gia, là nhiệm vụ của cả hệ thống chính trị dưới sự lãnh đạo của Đảng, là trách nhiệm của mỗi cán bộ, đảng viên.

Bên cạnh những lợi ích to lớn, không gian mạng đồng thời cũng chứa đựng những nguy cơ, thách thức lớn với an ninh quốc gia. Đó là những thách thức về bảo đảm an ninh, an toàn bí mật nhà nước, hệ thống thông tin quan trọng về an ninh quốc gia trước các hoạt động gián điệp mạng, tấn công mạng, khủng bố mạng và trước nguy cơ hệ thống thông tin quan trọng về an ninh quốc gia bị kiểm soát bởi các quốc gia, tổ chức nước ngoài; xử lý “khoảng trống thông tin”, không để tin giả, thông tin xấu, độc dẫn dắt dư luận. Một số chuyên gia còn cảnh báo nguy cơ đang hiện hữu về một cuộc chiến tranh mạng trong tương lai. Các thế lực thù địch, phản động triệt để lợi dụng không gian mạng để tuyên truyền phá hoại tư tưởng, phát tán các thông tin tấn công vào nền tảng tư tưởng, cương lĩnh, đường lối, chủ trương của Đảng, chính sách, pháp luật của Nhà nước, xuyên tạc tình hình đất nước, kích động gây mâu thuẫn nội bộ, chia rẽ Đảng, Nhà nước với nhân dân; tiến hành lôi kéo, tập hợp lực lượng và tổ chức đào tạo, huấn luyện, chỉ đạo các hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội. Trong một số vụ việc, đã có dấu hiệu các đối tượng lợi dụng không gian mạng để kích động, lôi kéo một bộ phận quần chúng nhân dân, thậm chí có cả cán bộ, đảng viên vào các hoạt động biểu tình gây ảnh hưởng đến an ninh chính trị, trật tự, an toàn xã hội. Những thông tin trên đang hàng ngày, hàng giờ tác động tới cán bộ, đảng viên, nhân dân; nếu không có bản lĩnh chính trị vững vàng và “bộ lọc”, kỹ năng cần thiết sẽ rất dễ bị tác động, lôi

kéo hoặc vô tình có các hoạt động gây phương hại đến lợi ích, an ninh quốc gia.

Nghị quyết số 29-NQ/TW, ngày 25/7/2018 của Bộ Chính trị khóa XII về *Chiến lược bảo vệ Tổ quốc trên không gian mạng* và Nghị quyết số 30-NQ/TW, ngày 25/7/2018 của Bộ Chính trị khóa XII về *Chiến lược an ninh mạng quốc gia* xác định bảo vệ Tổ quốc trên không gian mạng là nhiệm vụ thường xuyên của cả hệ thống chính trị dưới sự lãnh đạo của Đảng, với biện pháp chủ yếu là tuyên truyền, giáo dục, vận động, đi đôi với nâng cao năng lực và phát huy vai trò của các lực lượng chuyên trách để thực hiện nhiệm vụ bảo vệ Tổ quốc trên không gian mạng. Chính vì vậy, nâng cao nhận thức, ý thức làm chủ và bảo vệ không gian mạng của cán bộ, đảng viên là yêu cầu rất cần thiết, góp phần phát huy sức mạnh tổng hợp của các lực lượng để góp phần bảo vệ lợi ích quốc gia - dân tộc, xây dựng không gian mạng lành mạnh, an toàn.

2. Thời gian qua, ý thức làm chủ, bảo vệ không gian mạng của cán bộ, đảng viên có sự chuyển biến rất quan trọng theo hướng tích cực; tình trạng nhiễu loạn thông tin trên không gian mạng từng bước được chấn chỉnh, góp phần xây dựng không gian mạng ngày càng lành mạnh¹. Bên cạnh việc cán bộ, đảng viên chủ động nâng cao nhận thức về vấn đề này, kết quả trên là do công tác tuyên truyền, giáo dục về bảo vệ không gian mạng nói chung, bảo vệ an ninh, an toàn thông tin nói riêng cho cán bộ, đảng viên đã được quan tâm thực hiện. Thủ tướng Chính phủ đã ban hành

1. Xem Bộ Thông tin và Truyền thông: *An toàn thông tin khi sử dụng mạng xã hội*, Nxb. Thông tin và Truyền thông, Hà Nội, 2020, tr.62.

Quyết định số 1907/QĐ-TTg, ngày 23/11/2020 phê duyệt Đề án tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021 - 2025, xác định rõ mục tiêu, quan điểm chỉ đạo, giải pháp thực hiện. Cấp ủy, thủ trưởng các cơ quan, đơn vị, địa phương và lực lượng chuyên trách đã tổ chức các hoạt động tuyên truyền về bảo đảm an ninh mạng cho cán bộ, đảng viên với hình thức ngày càng đa dạng, phong phú, kết hợp giữa trực tiếp và trực tuyến, giữa các hoạt động cụ thể với tuyên truyền, vận động thông qua các ứng dụng công nghệ.

Các quy định của pháp luật về bảo vệ an ninh, an toàn không gian mạng ngày càng hoàn thiện và được tuyên truyền, phổ biến rộng rãi nhằm nâng cao nhận thức và ý thức chấp hành pháp luật cho cán bộ, đảng viên, nhân dân, điển hình là Luật an toàn thông tin mạng; Luật an ninh mạng; Luật bảo vệ bí mật nhà nước; 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; Nghị định số 15/2020/NĐ-CP, ngày 03/02/2020 của Chính phủ quy định về xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử. Gần đây nhất, Bộ quy tắc ứng xử trên mạng xã hội được Bộ Thông tin và Truyền thông ban hành kèm theo Quyết định số 874/QĐ-BTTTT, ngày 17/6/2021 hướng tới xây dựng chuẩn mực ứng xử chung trên không gian mạng để mọi “cư dân mạng” có ý thức điều chỉnh hành vi, đạo đức phù hợp với lợi ích chung của cộng đồng trên tinh thần tôn trọng pháp

luật, góp phần xây dựng, phát triển không gian mạng lành mạnh, bảo đảm quyền con người, quyền công dân và phù hợp với chuẩn mực, thông lệ quốc tế.

Tuy nhiên, nhận thức, ý thức làm chủ và bảo vệ không gian mạng của một bộ phận cán bộ, đảng viên còn chủ quan, đơn giản. Đáng chú ý là thói quen quan tâm tìm hiểu, thích (like) và chia sẻ (share) một cách cố ý hoặc vô ý mà không tính đến hậu quả với những thông tin giật gân, tiêu cực, phản ánh “mặt trái” của xã hội hơn là thông tin tích cực. Nhận thức “mạng xã hội là ảo nên không phải chịu trách nhiệm về việc phát ngôn, hành xử của mình” của một bộ phận cán bộ, đảng viên chưa được loại trừ¹. Một bộ phận cán bộ thờ ơ, vô cảm, không bày tỏ thái độ trước các thông tin tấn công vào Đảng, Nhà nước và chế độ; thậm chí có trường hợp lợi dụng internet, mạng xã hội để phát tán thông tin gây rối nội bộ, xuyên tạc chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước, phản biện vô nguyên tắc, trái tính đảng, vi phạm những điều đảng viên không được làm. Từ sự lệch lạc trong nhận thức về các vấn đề chính trị, văn hóa, xã hội dẫn đến sai lầm trong hành vi, gây ảnh hưởng đến an ninh chính trị, trật tự, an toàn xã hội, xâm phạm lợi ích quốc gia - dân tộc².

3. Thời gian tới, sự phát triển nhanh chóng về khoa học - công nghệ trong Cách mạng công nghiệp lần thứ tư tiếp tục

1. Xem Bộ Thông tin và Truyền thông: *An toàn thông tin khi sử dụng mạng xã hội*, *Sdd*, tr.57.

2. Xem Trúc Giang: “Sử dụng mạng internet và mạng xã hội có trách nhiệm”, <https://hcmcpv.org.vn>, truy cập ngày 02/3/2021.

làm thay đổi mạnh mẽ phương thức hoạt động kinh tế, chính trị, xã hội, văn hóa trên phạm vi quốc gia và quốc tế. Công nghiệp công nghệ thông tin sẽ trở thành ngành kinh tế chủ đạo, quyết định sự phát triển nhanh, bền vững của quốc gia. Năng lực làm chủ không gian mạng sẽ là ưu tiên hàng đầu để bảo vệ an ninh quốc gia và là lợi thế so sánh về sức mạnh quốc gia so với các nước khác. Trong bối cảnh đó, Đảng, Nhà nước đã có nhiều chủ trương, chính sách nhằm chủ động khai thác triệt để các cơ hội mà Cách mạng công nghiệp lần thứ tư mang lại. Bộ Chính trị khóa XII đã ban hành Nghị quyết số 52-NQ/TW, ngày 27/9/2019 về *Một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư*. Chính phủ đã ban hành chiến lược chuyển đổi số quốc gia với ba trụ cột là Chính phủ số, Kinh tế số và Xã hội số. Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII của Đảng xác định yêu cầu thúc đẩy chuyển đổi số quốc gia, phát triển kinh tế số, xã hội số một cách mạnh mẽ để tạo sự bứt phá về năng suất, chất lượng, hiệu quả, sức cạnh tranh của nền kinh tế.

Tuy nhiên, nhiệm vụ bảo vệ an ninh quốc gia, bảo vệ chủ quyền quốc gia trên không gian mạng đang gặp phải một số thách thức cơ bản. Đó là sự thiếu hụt những nguyên tắc pháp lý mang tính quy chuẩn chung cho các quốc gia và cơ chế hợp tác quốc tế về vấn đề này, nguyên nhân chủ yếu là do sự khác biệt về quan điểm chính trị, pháp luật, bảo đảm an ninh và lợi ích của các quốc gia. Đó là khả năng kiểm soát các hoạt động trên không gian mạng của các quốc gia bằng các biện pháp hành chính và kỹ thuật do những hạn chế về hạ tầng công nghệ, hệ thống pháp luật và năng lực của các cơ quan bảo đảm an ninh mạng. Đó là sự hài hòa

giữa yêu cầu bảo vệ chủ quyền quốc gia với bảo đảm các quyền cơ bản của con người trên không gian mạng, nhất là quyền tự do thông tin¹.

Thấm nhuần quan điểm “dân là gốc” trong Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII của Đảng, cần tiếp tục xác định nhiệm vụ bảo vệ Tổ quốc trên không gian mạng về bản chất chính là xây dựng nền quốc phòng toàn dân và thế trận quốc phòng toàn dân gắn với thế trận an ninh nhân dân và nền an ninh nhân dân trên không gian mạng². Trong đó, cán bộ, đảng viên là chủ thể bảo vệ không gian mạng và cũng chính là “đối tượng bảo vệ” quan trọng. Vì vậy, nhiệm vụ đầu tiên và hết sức quan trọng là phải tiếp tục nâng cao ý thức làm chủ và bảo vệ không gian mạng của cán bộ, đảng viên để nhận thức đầy đủ vai trò, trách nhiệm của mình, những gì được làm, không được làm, quyền và nghĩa vụ, “kỹ năng” ứng xử trên không gian mạng nhằm góp phần xây dựng không gian mạng lành mạnh, an toàn. Để thực hiện tốt nhiệm vụ trên, cần tập trung triển khai các giải pháp trọng tâm sau đây:

Thứ nhất, cần xác định rõ vai trò, trách nhiệm của cả hệ thống chính trị, trước hết là vai trò chủ đạo, trách nhiệm chính của cấp ủy, thủ trưởng các cơ quan, đơn vị, địa phương và lực lượng chuyên trách bảo vệ an ninh mạng trong việc

1. Xem Hoàng Thị Quyên: “Bảo vệ chủ quyền quốc gia trên không gian mạng trong thời đại công nghệ số”, <http://lyluanchinhtri.vn>, truy cập ngày 18/01/2021.

2. Xem Đại tướng Tô Lâm: “Những nhận thức mới, tư duy mới về bảo vệ an ninh quốc gia”, Báo điện tử Đảng Cộng sản Việt Nam, <https://dangcongsan.vn>, truy cập ngày 28/3/2021.

nâng cao nhận thức, ý thức làm chủ và bảo vệ không gian mạng của cán bộ, đảng viên. Vai trò, trách nhiệm đó thể hiện trên ba khía cạnh cơ bản: (1) Tổ chức tuyên truyền, giáo dục các quy định của pháp luật về an ninh mạng, an toàn thông tin, những kiến thức, kỹ năng cơ bản để tương tác trên không gian mạng; (2) Cung cấp thông tin chính thống; (3) Xây dựng, hoàn thiện quy chế, quy định về bảo vệ không gian mạng và tăng cường kiểm tra, giám sát việc thực hiện, xử lý nghiêm các hành vi vi phạm.

Ban Tuyên giáo Trung ương sớm hoàn thiện quy định về trách nhiệm của cán bộ, đảng viên trong việc lập, sử dụng mạng xã hội, trong đó đề cao “tính chính danh” và trách nhiệm khi đăng tải, chia sẻ thông tin cũng như việc tương tác khi tiếp nhận thông tin của cán bộ, đảng viên; bảo đảm quản lý được hoạt động của cán bộ, đảng viên trên không gian mạng. Các cơ quan chức năng sớm hoàn thiện các quy định của pháp luật về bảo vệ an ninh, an toàn không gian mạng quốc gia, như: Nghị định thi hành một số điều của Luật an ninh mạng; Nghị định về việc xử phạt vi phạm hành chính về an ninh mạng; Nghị định về bảo vệ dữ liệu cá nhân. Từng cơ quan, đơn vị, địa phương sớm hoàn thiện quy chế, quy định về bảo vệ bí mật nhà nước (trong đó có bảo vệ bí mật nhà nước trên không gian mạng); bổ sung quy định về văn hóa ứng xử của công chức, viên chức, người lao động, trong đó cụ thể hóa các nội dung về ứng xử trên không gian mạng; xây dựng chương trình, kế hoạch tuyên truyền, giáo dục nhằm tạo chuyển biến mạnh mẽ trong nhận thức, ý thức chấp hành pháp luật về bảo vệ không gian mạng của cán bộ, đảng viên; tổ chức các biện pháp bảo vệ chính trị nội bộ trên không gian mạng.

Thứ hai, đổi mới nội dung tuyên truyền, giáo dục cho cán bộ, đảng viên về an toàn, an ninh thông tin trên không gian mạng cho phù hợp với từng diện đối tượng. Cần tuyên truyền để cán bộ, đảng viên nhận thức rõ các nguy cơ đến từ không gian mạng không chỉ là nguy cơ “ảo” mà hiện hữu trên thực tế và là một trong những vấn đề nguy hiểm nhất đối với an ninh quốc gia, chủ quyền quốc gia hiện nay. Nâng cao ý thức chính trị, trách nhiệm, nghĩa vụ của cán bộ, đảng viên xây dựng ý thức tôn trọng và bảo vệ quyền và lợi ích của tổ chức, cá nhân, lợi ích của quốc gia - dân tộc trong quá trình tương tác trên không gian mạng, mà vấn đề cốt yếu là tuân thủ, thực hiện nghiêm các quy định của pháp luật về an ninh mạng.

Cấp ủy, thủ trưởng các cơ quan, đơn vị, địa phương thường xuyên phối hợp với lực lượng chuyên trách về an ninh mạng phổ biến, quán triệt các quy định của Đảng, pháp luật của Nhà nước về quản lý, bảo vệ không gian mạng, như: Quy định số 47-QĐ/TW, ngày 01/11/2011 của Bộ Chính trị khóa XI *Về những điều đảng viên không được làm*; Quy định số 102-QĐ/TW, ngày 15/11/2017 của Bộ Chính trị khóa XII *Về xử lý kỷ luật đảng viên vi phạm*; Nghị quyết số 04-NQ/TW, ngày 30/10/2016 của Ban Chấp hành Trung ương Đảng khóa XII *Về tăng cường xây dựng, chỉnh đốn Đảng, ngăn chặn, đẩy lùi sự suy thoái về tư tưởng chính trị, đạo đức, lối sống, những biểu hiện “tự diễn biến”, “tự chuyển hóa” trong nội bộ*; Bộ luật hình sự; Luật an toàn thông tin mạng; Luật an ninh mạng; Luật bảo vệ bí mật nhà nước; 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; Nghị định số 15/2020/NĐ-CP, ngày 03/02/2020 của Chính phủ quy định về xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử; Quyết định số 874/QĐ-BTTTT, ngày 17/6/2021 của Bộ Thông tin và Truyền thông ban hành Bộ quy tắc ứng xử trên mạng xã hội. Tập trung tuyên truyền, giáo dục, nâng cao nhận thức cho cán bộ, đảng viên về những hành vi bị cấm trên không gian mạng, nhất là việc “lợi dụng các phương tiện thông tin đại chúng, internet, mạng xã hội... để xuyên tạc, kích động, gây mất đoàn kết nội bộ”¹, phá hoại thuần phong mỹ tục; cố ý làm lộ bí mật nhà nước, bí mật công tác, bí mật cá nhân, bí mật gia đình gây ảnh hưởng đến quyền và lợi ích hợp pháp của tổ chức, cá nhân; kích động, xúi giục, lôi kéo người khác phạm tội; thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng...

Bên cạnh đó, cần chú trọng trang bị cho cán bộ, đảng viên về phương thức, thủ đoạn mới của các thế lực thù địch, đối tượng phản động, chống đối, cơ hội chính trị lợi dụng không gian mạng để phát tán thông tin sai trái, thù địch; nâng cao ý thức bảo vệ bí mật nhà nước trên không gian mạng, kỹ năng nhận diện, “ứng xử” với thông tin xấu, độc, quan điểm sai trái, thù địch; kỹ năng phòng tránh, tự vệ khi bị tấn công mạng. Trên cơ sở đó, huy động cán bộ, đảng viên tham gia bảo vệ nền tảng tư tưởng của Đảng trên không

1. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.II, tr.244-245.

gian mạng với hình thức phù hợp, có tổ chức, không thực hiện một cách tự phát, dễ bị các đối tượng tấn công lại.

Thứ ba, đa dạng hóa hình thức tuyên truyền, giáo dục kiến thức, kỹ năng bảo vệ, làm chủ không gian mạng cho cán bộ, đảng viên, tận dụng lợi thế của khoa học - công nghệ để phản ánh nội dung một cách chủ động, linh hoạt, thông minh và rộng khắp, “lấy cái đẹp dẹp cái xấu”. Nâng cao hiệu quả công tác bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trên không gian mạng, coi đây là kênh thông tin hiệu quả để tuyên truyền, giáo dục cán bộ, đảng viên nhận thức rõ “cái đúng”, “cái tốt”, phê phán các biểu hiện lệch lạc, lợi dụng quyền tự do, dân chủ, tự do ngôn luận để phát tán các luận điệu chống Đảng, Nhà nước, lợi ích quốc gia - dân tộc.

Tăng cường cung cấp thông tin chính thống về các vấn đề cán bộ, đảng viên quan tâm, tiến tới làm chủ mặt trận thông tin trên không gian mạng, không tạo “khoảng trống thông tin” để các thế lực thù địch, đối tượng chống đối lợi dụng phát tán thông tin để hướng lái dư luận trước khi cơ quan chức năng công bố thông tin. Xây dựng, nâng cao chất lượng các kênh thông tin chính thống trên mạng xã hội của các cơ quan, tổ chức (như facebook “Thông tin Chính phủ”) để thu hút đông đảo cán bộ, đảng viên theo dõi, truy cập, sớm công bố các thông tin sai sự thật, tin giả để cán bộ, đảng viên, nhân dân sớm nắm bắt (gần đây cơ quan chức năng đã xây dựng website “tingia.gov.vn” nhưng cần thường xuyên cập nhật hơn). Nâng cao chất lượng, hiệu quả, sức hấp dẫn, độ lan tỏa và tính định hướng của các cơ quan báo chí chính thống, phát triển báo chí theo hướng đa phương

tiện để đáp ứng yêu cầu của độc giả, gắn với nâng cao chất lượng và tính kịp thời của các tuyến bài về những vấn đề “nóng”, “nổi” mà cán bộ, đảng viên và dư luận quan tâm trong từng thời điểm.

Thứ tư, phát huy vai trò của các học viện, nhà trường trong bồi dưỡng, giáo dục, nâng cao ý thức làm chủ và bảo vệ không gian mạng cho cán bộ, đảng viên. Tích hợp nội dung bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trên không gian mạng vào tất cả các hệ lớp, các chương trình đào tạo, bồi dưỡng cán bộ lãnh đạo, quản lý trung, cao cấp của cả hệ thống chính trị để thông qua đội ngũ cán bộ này tiếp tục lan tỏa ý thức làm chủ, bảo vệ không gian mạng đến cán bộ, đảng viên các cơ quan, đơn vị, địa phương. Bổ sung các quan điểm chỉ đạo của Đảng về bảo vệ không gian mạng quốc gia vào chương trình đào tạo, bồi dưỡng cho phù hợp với các ngành học, cấp học, nhất là quan điểm gắn kết chặt chẽ giữa “xây” và “chống”, vấn đề phát huy sức mạnh tổng hợp của các lực lượng, của hệ thống chính trị và toàn dân trong bảo đảm an toàn, an ninh mạng. Tiếp tục nghiên cứu làm rõ các vấn đề về bảo vệ quyền con người trên không gian mạng trong mối quan hệ với bảo vệ không gian mạng để có sự điều chỉnh phù hợp về cơ chế, chính sách, pháp luật, vừa phù hợp với thông lệ quốc tế, vừa bảo đảm yêu cầu giữ vững chủ quyền quốc gia trên không gian mạng.

Thứ năm, lực lượng chuyên trách cần tăng cường sử dụng các biện pháp kỹ thuật để đánh giá dòng thông tin chủ lưu trên không gian mạng trong từng thời điểm (nhất là thông tin liên quan đến những sự kiện nhạy cảm, được cộng đồng mạng quan tâm), dự đoán mức độ lan tỏa của thông tin, trên cơ sở đó

đẩy mạnh lan tỏa dòng thông tin tích cực đi đôi với rà quét, lọc bỏ thông tin xấu, độc.

Phát hiện, xử lý nghiêm các trường hợp lợi dụng không gian mạng để phát tán tin giả, thông tin xấu, độc, sai trái, phản động và công khai trên các phương tiện truyền thông đại chúng, mạng xã hội, coi đây là biện pháp quan trọng để răn đe những trường hợp khác. Vừa qua, chúng ta đã làm tốt công tác tuyên truyền, lan tỏa thông tin tích cực, xử lý nghiêm một số trường hợp đăng tải thông tin sai sự thật liên quan đến đại dịch Covid-19, khởi tố một số đối tượng có hành vi lợi dụng không gian mạng để chống Nhà nước (về tội “Tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam”; “Làm, tàng trữ, phát tán hoặc tuyên truyền thông tin, tài liệu, vật phẩm nhằm chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam”). Tuy nhiên, một số cá nhân đăng tải thông tin chống Đảng, Nhà nước, tấn công vào đội ngũ cán bộ, đảng viên vẫn chưa được xử lý nghiêm bằng các biện pháp pháp luật, đây là vấn đề cần khắc phục thời gian tới.

Tóm lại, với sự phát triển mạnh mẽ của khoa học - công nghệ, không gian mạng đã trở thành “lãnh thổ đặc biệt” của quốc gia, bao trùm hầu như toàn bộ đời sống chính trị, kinh tế, văn hóa, xã hội, mang lại những cơ hội, điều kiện mới để quốc gia phát triển và hội nhập. Tuy nhiên, không gian mạng cũng chứa đựng nhiều yếu tố tác động tiêu cực đến sự ổn định và phát triển của quốc gia, của đời sống xã hội và của mỗi “cư dân mạng”. Vì vậy, nâng cao nhận thức, ý thức làm chủ và bảo vệ không gian mạng của cán bộ, đảng viên và nhân dân là hết sức cần thiết. Đây là trách nhiệm trước hết

của cấp ủy, thủ trưởng các cơ quan, đơn vị, địa phương, của các lực lượng chuyên trách và của chính bản thân mỗi cán bộ, đảng viên để thật sự trở thành “cư dân mạng thông thái” với những kiến thức, kỹ năng cần thiết. Và trước hết, cán bộ, đảng viên phải có bản lĩnh chính trị thật sự vững vàng để không bị tác động và từng bước phản bác lại các thông tin xấu, độc trên không gian mạng hiện nay.

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG TRUYỀN THÔNG XÃ HỘI Ở VIỆT NAM HIỆN NAY

PGS.TS. VŨ TRỌNG LÂM*

TS. VŨ THỊ HƯƠNG**

Thế giới đang đứng trước tác động của Cách mạng công nghiệp lần thứ tư với nền tảng là công nghệ thông tin đang chuyển hóa một phần thế giới thực thành thế giới số và cùng song song tồn tại. Sự phát triển vượt bậc của công nghệ số đã và đang là nền tảng cho sự phát triển các lĩnh vực kinh tế, văn hóa, xã hội nhằm phục vụ và nâng cao chất lượng cuộc sống của con người, trong đó tác động mạnh mẽ trước hết là truyền thông xã hội.

Với khả năng tương tác, kết nối cao so với các loại hình truyền thông truyền thống, truyền thông xã hội đang đáp ứng yêu cầu ngày càng cao của xã hội. Với truyền thông xã hội, thông tin được truyền tải trên môi trường internet, người đọc có thể phản hồi, chia sẻ thông tin với nhau, qua đó tạo môi trường đa chiều trong tiếp cận, chia sẻ thông tin. Sự thay đổi trong cách truyền tải thông tin, tiếp cận thông tin,

* Phó Tổng Biên tập Tạp chí Cộng sản.

** Nhà xuất bản Chính trị quốc gia Sự thật.

chia sẻ thông tin của truyền thông xã hội đã có những đóng góp tích cực vào sự phát triển xã hội. Tuy nhiên, bên cạnh những lợi ích không thể phủ nhận, truyền thông xã hội cũng đang tiềm ẩn nhiều nguy cơ, thách thức liên quan đến an ninh thông tin. Đây là vấn đề cần được quan tâm nghiên cứu nhằm cung cấp cơ sở lý luận và thực tiễn phục vụ công tác xây dựng chính sách, pháp luật của Nhà nước; tăng cường hiệu lực, hiệu quả quản lý nhà nước về an ninh thông tin trên các phương tiện truyền thông xã hội; định hướng cho người dân trong việc tiếp cận, chia sẻ thông tin trên môi trường số.

1. Khái quát về truyền thông xã hội

Truyền thông xã hội là một loại hình truyền thông đại chúng được thực hiện dựa trên nền tảng công nghệ thông tin, điện tử, các tiện ích internet; đó là quá trình đưa và nhận thông tin với sự tham gia của đông đảo các thành viên trong xã hội. Trong lịch sử đã xuất hiện nhiều loại hình truyền thông, nhưng chỉ đến khi sự phát triển của công nghệ cho phép con người ở mọi nơi có thể trao đổi với nhau một cách nhanh chóng và thuận tiện thì mới có truyền thông xã hội¹. Cần lưu ý sự khác biệt giữa *truyền thông xã hội* (social media) và *mạng xã hội* (social network). Theo khoản 22, Điều 3 Nghị định số 72/2013/NĐ-CP, ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên

1. Xem Lê Hải: *Phương tiện truyền thông xã hội với giới trẻ Việt Nam*, Nxb. Chính trị quốc gia, Hà Nội, 2017.

mạng: “Mạng xã hội (social network) là hệ thống thông tin cung cấp cho cộng đồng người sử dụng mạng các dịch vụ lưu trữ, cung cấp, sử dụng, tìm kiếm, chia sẻ và trao đổi thông tin với nhau, bao gồm dịch vụ tạo trang thông tin điện tử cá nhân, diễn đàn (forum), trò chuyện (chat) trực tuyến, chia sẻ âm thanh, hình ảnh và các hình thức dịch vụ tương tự khác”. Truyền thông xã hội là công cụ truyền thông mà công chúng có thể tạo ra và trao đổi thông tin trên mạng internet. Về mặt bản chất công nghệ, truyền thông xã hội và mạng xã hội đều cùng chỉ một bản thể: đó là những website dựa trên nền tảng web 2.0 để giúp người sử dụng có thể tạo lập và truyền tải thông tin. Tuy vậy, thuật ngữ truyền thông xã hội mang nghĩa rộng hơn, bao hàm cả phương tiện lẫn nội dung truyền thông, trong khi mạng xã hội nhấn mạnh nhiều hơn đến nền tảng công nghệ tạo ra nó¹.

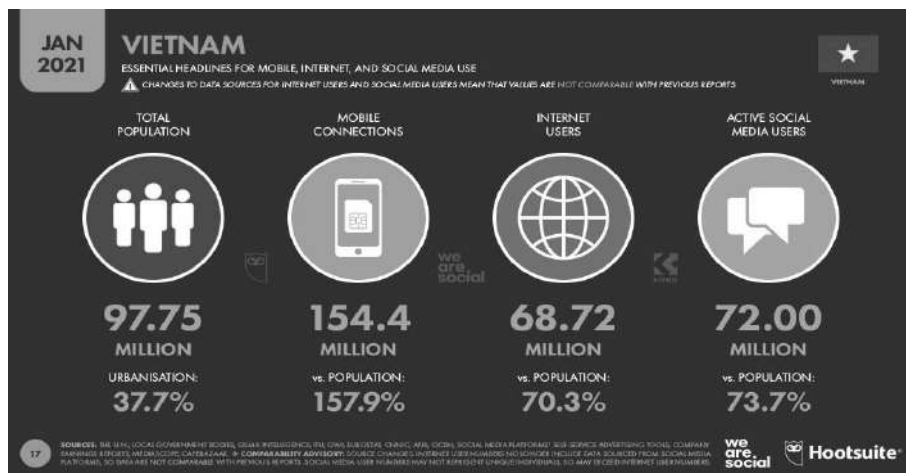
Theo số liệu thống kê của tổ chức Internet World Stats, tính đến ngày 31/5/2020, Việt Nam là quốc gia có lượng người sử dụng internet cao thứ 14 trên thế giới và đứng thứ 8 trong tổng số 35 quốc gia, vùng lãnh thổ khu vực châu Á². Tính đến tháng 01/2021, ở Việt Nam có 68,72 triệu người dùng internet, tương ứng với 70,3% dân số cả nước; 72 triệu người sử dụng các phương tiện truyền thông xã hội, với tỷ lệ 73,7%

1. Xem Nguyễn Khắc Giang: “Ảnh hưởng của truyền thông xã hội đến môi trường báo chí Việt Nam, tạp chí *Khoa học: Khoa học xã hội và nhân văn*, Đại học Quốc gia Hà Nội, 2015, số 1, tập 31.

2. Xem *Digital 2021: Vietnam*, <http://datareportal.com/reports/digital-2021-vietnam>.

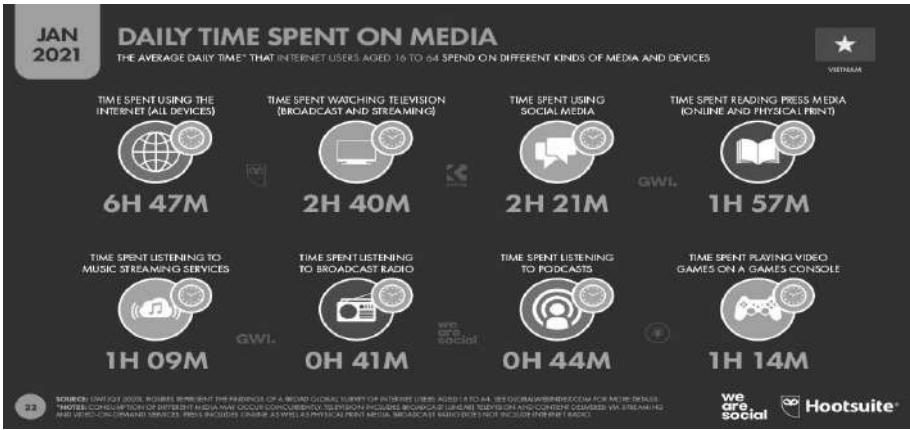
dân số; có tới hơn 154,4 triệu thiết bị kết nối mạng dữ liệu di động tại Việt Nam, chiếm 157,9% dân số, điều đó có nghĩa là mỗi người có thể sử dụng nhiều thiết bị kết nối mạng dữ liệu di động để luân phiên thực hiện công việc, giải trí,... (xem Hình 1). Hằng ngày, mỗi người Việt Nam dành 6 giờ 47 phút để truy cập internet (xem Hình 2) (gần tương đương với mức bình quân của thế giới là 6 giờ 54 phút), trong đó, khoảng 2 giờ 21 phút sử dụng các phương tiện truyền thông xã hội, gần tương đương với mức trung bình của thế giới (2 giờ 25 phút) (xem Hình 3).

Hình 1: Số lượng người sử dụng thiết bị kết nối mạng dữ liệu di động, internet và truyền thông xã hội ở Việt Nam



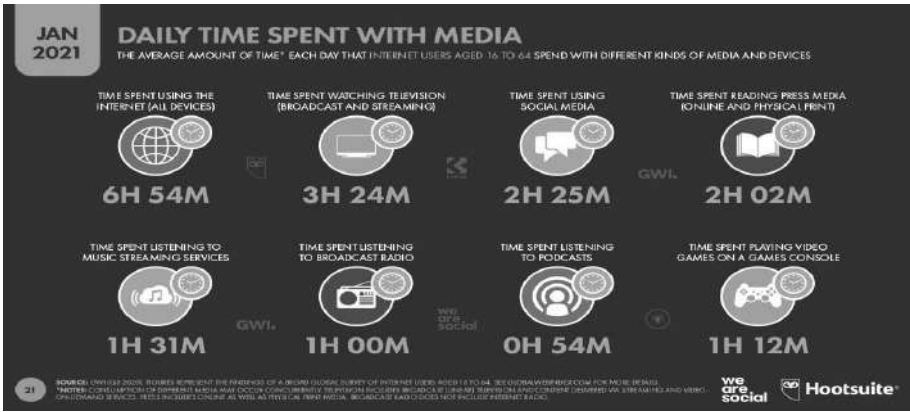
Nguồn: Digital 2021: Vietnam, <https://datareportal.com/reports/digital-2021-vietnam>.

Hình 2: Số lượng người sử dụng internet ở Việt Nam



Nguồn: Digital 2021: Vietnam, <https://datareportal.com/reports/digital-2021-vietnam>.

Hình 3: Thời gian bình quân hằng ngày sử dụng internet và truyền thông xã hội trên thế giới

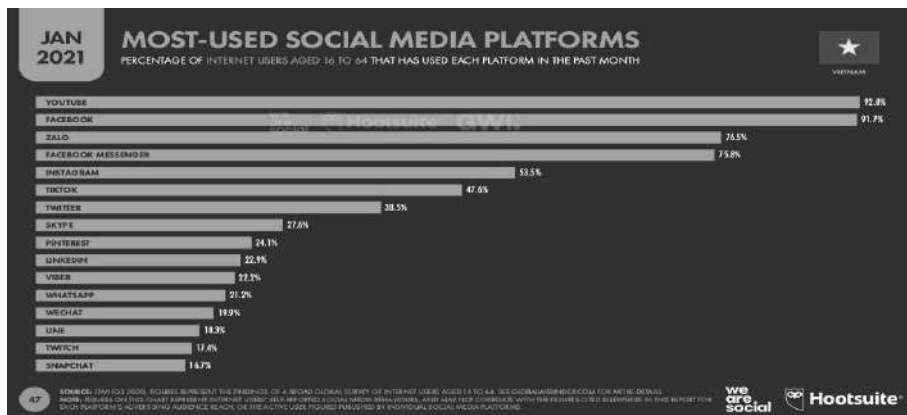


Nguồn: Digital 2021: Global Overview Report, <https://datareportal.com/reports/digital-2021-global-overview-report>.

Tại Việt Nam, các phương tiện truyền thông xã hội có số lượng người sử dụng lần lượt từ cao đến thấp là: YouTube - Facebook - Zalo - FB Messenger - Instagram - Tiktok -

Twitter - Skype - Printest - Linkedin - Viber - Whatsapp - Wechat - Line - Twitch - Snapchat (xem Hình 4).

Hình 4: Các phương tiện truyền thông xã hội được sử dụng phổ biến ở Việt Nam



Nguồn: Digital 2021: Vietnam, <https://datareportal.com/reports/digital-2021-vietnam>.

Sự ra đời của truyền thông xã hội đã làm thay đổi cách thức và chủ thể truyền thông. Với các phương tiện truyền thông truyền thống như báo in, đài phát thanh, truyền hình, chủ yếu truyền thông một chiều, một nguồn phát tin - nhiều nguồn tiếp nhận, người nhận tin không hoặc có rất ít cơ hội để truyền tin trở lại, thì truyền thông xã hội có sự tham gia của đông đảo thành viên trong xã hội với cả hai tư cách vừa là người nhận tin, vừa là chủ thể truyền tin. Khác với các loại hình truyền thông truyền thống, truyền thông xã hội có sự tương tác rõ rệt giữa chủ thể truyền tin và chủ thể nhận tin; người nhận tin có thể trở thành chủ thể truyền tin và ngược lại. Mặt khác, với truyền thông xã hội, các cá nhân, tổ chức trong xã hội đều có thể trở thành

chủ thể truyền thông thông qua các mạng xã hội, các dịch vụ trực tuyến, các công cụ comment phản hồi báo chí, trang tin điện tử...

2. Tác động của truyền thông xã hội đối với các lĩnh vực của xã hội

Dựa trên nền tảng công nghệ thông tin, điện tử, các tiện ích trên mạng internet, các thiết bị, phương tiện nhận và truyền thông tin cố định, di động, viễn thông, truyền thông xã hội giúp có thể đưa và nhận thông tin ở bất kỳ nơi nào trên thế giới. Các phương tiện kết nối có khả năng tích hợp các chức năng, dịch vụ để thực hiện tất cả các loại hình truyền thông cá nhân, liên cá nhân, nhóm hay cả xã hội một cách thuận lợi với chi phí ngày càng thấp. Cùng với đó, trên truyền thông xã hội được tích hợp các ứng dụng thông minh, tiện ích phục vụ nhu cầu xã hội của con người như: mua bán, giao dịch, đầu tư, tìm địa chỉ, học tập...

Truyền thông xã hội có đầy đủ các chức năng thông tin - liên kết xã hội; giáo dục, tư tưởng, đạo đức; giải trí; giám sát - phản biện xã hội... Sự ra đời của truyền thông xã hội đã có tác động tới các lĩnh vực của đời sống xã hội, đến các đối tượng, thành phần của xã hội, đặc biệt là giới trẻ - một trong những đối tượng bị tác động mạnh mẽ nhất của truyền thông xã hội. Đa số người dùng ở Việt Nam hiện nay có thái độ, ứng xử tích cực trên môi trường truyền thông xã hội, sử dụng các tiện ích của nó để cập nhật thông tin, quảng bá hình ảnh, liên lạc, làm quen, kết bạn, chia sẻ kinh nghiệm, giải tỏa tâm lý. Truyền thông xã hội giúp thúc đẩy quá trình tự giáo dục đạo đức của giới trẻ, góp phần bồi đắp giá trị, hình thành nhân cách tích cực.

Với kho tài nguyên tri thức khổng lồ, truyền thông xã hội góp phần tác động tích cực trong việc trang bị tri thức cho người dùng.

Truyền thông xã hội trở thành một kênh truyền thông quan trọng để vận động, huy động và tập hợp sức mạnh to lớn của quần chúng. Các ý kiến góp ý, phản biện về những vấn đề kinh tế - xã hội, về các chủ trương, chính sách của Đảng và Nhà nước có ý nghĩa quan trọng góp phần nâng cao hiệu lực quản lý nhà nước, hoàn thiện các chủ trương, chính sách, phù hợp với thực tiễn. Cùng với đó, các doanh nghiệp cũng tận dụng khả năng tương tác, kết nối vượt trội của truyền thông xã hội trong quảng bá thương hiệu, sản phẩm, xúc tiến thương mại và đầu tư, thông qua ý kiến phản hồi của người tiêu dùng để hoàn thiện, nâng cao chất lượng sản phẩm, đáp ứng nhu cầu khách hàng. Nhiều thanh niên biết tận dụng truyền thông xã hội như một công cụ để lập thân, lập nghiệp, phát triển, khẳng định mình.

Với tính năng kết nối gần như không giới hạn và số lượng người sử dụng đông đảo, truyền thông xã hội đã trở thành công cụ rất hữu hiệu mà các cơ quan nhà nước sử dụng nhằm tiếp cận người dân. Đến nay, đã có nhiều cơ quan nhà nước từ trung ương đến địa phương sử dụng các phương tiện truyền thông xã hội để tăng cường kết nối với người dân, doanh nghiệp, thêm kênh truyền tải các chủ trương, chính sách của Đảng, Nhà nước, phục vụ công tác chỉ đạo, điều hành của Chính phủ, Thủ tướng Chính phủ, các bộ, ngành và địa phương, đáp ứng nhu cầu thông tin của nhân dân mọi lúc, mọi nơi. Không chỉ để tiếp nhận phản hồi, góp ý của người dân và doanh nghiệp, nhiều cơ quan nhà nước đã sử

dụng truyền thông xã hội như là một công cụ để cung cấp dịch vụ công. Từ tháng 10/2015, Chính phủ đã lập hai tài khoản Facebook là “Thông tin Chính phủ” và “Diễn đàn Cạnh tranh quốc gia”; ngoài ra, Cổng thông tin điện tử chính phủ cũng có kênh giao tiếp trên Zalo,...

Tuy nhiên, bên cạnh những mặt tích cực, truyền thông xã hội đã có những tác động và tiềm ẩn nhiều nguy cơ về an ninh, trật tự. Truyền thông xã hội sử dụng môi trường mạng, nên nó mang tính “ảo”, nặc danh, khó xác định, khả năng bảo mật thông tin có giới hạn. Những người tham gia truyền thông xã hội thường ẩn danh dưới các nick, tài khoản ảo, những mối quan hệ phát sinh trong truyền thông xã hội ẩn chứa nhiều rủi ro. Đồng thời, tính bảo mật thông tin của những người tham gia quá trình truyền thông xã hội phụ thuộc vào chất lượng bảo mật của ứng dụng - phần mềm; nhận thức của người dùng... Do đó, những thông tin của người dùng có thể bị các đối tượng xấu khai thác, chiếm đoạt, phục vụ ý đồ xấu. Với sự tham gia của số đông trong xã hội, truyền thông xã hội là công cụ hữu hiệu để tạo ra dư luận xã hội theo các chiều hướng khác nhau. Những vấn đề nhạy cảm lan truyền trên truyền thông xã hội có thể dễ dàng tác động đến tư tưởng, tình cảm của xã hội, hướng lái dư luận. Nếu không kiểm soát được những thông tin độc hại, truyền thông xã hội có thể tạo ra các hành động tiêu cực của một nhóm, thậm chí cả xã hội. Trên thực tế, do kinh nghiệm và nhận thức xã hội còn hạn chế, lại bị tác động từ lượng lớn, đa chiều các thông tin xấu, độc hại, đã khiến một bộ phận người tham gia truyền thông xã hội, nhất là giới trẻ bị ảnh hưởng tiêu cực về tư tưởng, lối sống, có những hành vi lệch lạc, nhiều trường hợp vi phạm pháp luật.

Thời gian qua, lợi dụng tâm lý đám đông, tính tò mò của một bộ phận công chúng, một số đối tượng xấu đã sử dụng thủ đoạn thâm độc, vu khống, bịa đặt thông tin, cắt - ghép video làm hình ảnh minh họa để phao tin đồn thất thiệt, gây dư luận xã hội tiêu cực. Việc người dùng mạng xã hội có thể dễ dàng và nhanh chóng đưa ra những phát ngôn bôi nhọ, nói xấu bằng những ngôn từ thiếu kiểm soát, sẽ có thể mang lại những hậu quả khôn lường. Tác động xấu từ truyền thông xã hội có thể dẫn đến những hậu quả trực tiếp, tức thì, nhưng cũng có những hậu quả len lỏi, lâu dài tích tụ vào ứng xử, lối sống, dần dần phá vỡ những hệ giá trị văn hóa và đạo đức tốt đẹp. Những đổ vỡ về giá trị, những tổn thương về tâm lý ảnh hưởng đến đời sống mỗi cá nhân, từ đó, tác động đến ổn định chính trị, xã hội của quốc gia¹. Một vấn đề đáng quan tâm, đó là nhiều người dùng mạng xã hội hiện nay đang nhầm lẫn ranh giới giữa phản biện cá nhân, nói ra chính kiến, quan điểm, sự góp ý mang tính phản biện với việc đưa ra những bình luận, phát ngôn bôi nhọ, nói xấu, tạo nên sự thù nghịch. Ngoài ra, không ít người còn lầm tưởng rằng, mạng xã hội nước ngoài như Facebook, YouTube,... không chịu sự điều chỉnh của pháp luật Việt Nam nên họ không bị cấm hay hạn chế, không chịu trách nhiệm trong việc “tự do” đưa ra các phát ngôn, bình luận thiếu suy nghĩ².

1. Xem Võ Văn Thường: “Sử dụng mạng xã hội có trách nhiệm”, <http://tuoitre.vn/su-dung-mang-xa-hoi-co-trach-nhiem-20190616170545024.htm>.

2. Xem Bộ Thông tin và Truyền thông: *Báo cáo tổng kết năm 2018 và phương hướng, nhiệm vụ, giải pháp năm 2019*.

3. Phương hướng bảo đảm an toàn thông tin trong truyền thông xã hội ở Việt Nam hiện nay

Nền tảng pháp lý được coi là một trong những chìa khóa của sự phát triển kinh tế số, trong đó có truyền thông xã hội. Trước sự tác động hai chiều của truyền thông xã hội, nhiều nước trên thế giới đã chủ động có những biện pháp nhằm phát huy những mặt tích cực, hạn chế những tác động tiêu cực từ truyền thông xã hội, xây dựng các quy định cụ thể để tăng cường quản lý, đồng thời xử lý nghiêm các hành vi vi phạm trong lợi dụng loại hình truyền thông mới này.

Việt Nam đã ban hành nhiều chủ trương, chính sách quy định trách nhiệm của các cá nhân, tổ chức trong bảo đảm an toàn thông tin trên internet nói chung, đối với truyền thông xã hội nói riêng. Đây là cơ sở pháp lý quan trọng để các cơ quan quản lý nhà nước tổ chức các hoạt động quản lý nhằm ngăn chặn mọi hành vi lợi dụng internet nói chung, truyền thông xã hội nói riêng vi phạm pháp luật.

Trên cơ sở đó, các cơ quan chức năng đã tăng cường các biện pháp bảo đảm an ninh mạng, xử lý các hành vi vi phạm trên không gian mạng, trong đó có truyền thông xã hội; chủ động ngăn chặn, vô hiệu hóa việc lợi dụng truyền thông xã hội gây nguy hại đến an ninh, trật tự. Trong năm 2019, thực hiện yêu cầu của các cơ quan quản lý nhà nước Việt Nam, Facebook đã gỡ bỏ 207 tài khoản (trong đó có 46 tài khoản giả danh lãnh đạo Đảng, Nhà nước, còn lại là các tài khoản tuyên truyền thông tin giả mạo, nói xấu, kích động chống phá Nhà nước Việt Nam; gỡ bỏ 2.444 link rao bán sản phẩm bất hợp pháp; 271 link phát ngôn gây thù hận, bôi nhọ lãnh

đạo Đảng, Nhà nước, các thương hiệu, cá nhân và tổ chức; gỡ bỏ 330 fanpages quảng cáo game cờ bạc, đổi thưởng. YouTube đã gỡ bỏ 9.501 video vi phạm, ngăn chặn truy cập từ Việt Nam vào 19/62 kênh YouTube phản động thường xuyên đăng tải nội dung chống phá Nhà nước Việt Nam, chứa khoảng 5.000 video clip; tiếp tục xem xét, ngăn chặn các kênh còn lại. Trên Google Play, Google đã gỡ 108/111 game, trong đó có 104 game bài và một game có tên “Lấy lại quê hương” có nội dung phản động, chống phá Nhà nước Việt Nam và các game không phép¹...

Tuy nhiên, công tác quản lý nhà nước và việc giám sát, ngăn chặn, vô hiệu hóa các thông tin độc hại trên truyền thông xã hội còn gặp nhiều khó khăn, bất cập:

Một là, trong bối cảnh khoa học và công nghệ phát triển mạnh mẽ, tội phạm mạng sử dụng nhiều thủ đoạn tinh vi, ứng dụng các thành tựu khoa học hiện đại để tiến hành các chiến dịch tấn công mạng, dẫn dắt dư luận trên truyền thông xã hội khiến công tác phòng ngừa, ngăn chặn của cơ quan chức năng gặp nhiều khó khăn.

Hai là, hệ thống văn bản quy phạm pháp luật liên quan công tác bảo đảm an ninh mạng đã được xây dựng nhưng chưa hoàn thiện; vai trò và hiệu lực quản lý nhà nước trên lĩnh vực an ninh mạng nói chung, truyền thông xã hội nói riêng còn nhiều bất cập.

1. Xem Thủy Diệu: “Sẽ có biện pháp cứng rắn hơn để Facebook tuân thủ pháp luật Việt Nam”, <http://vneconomy.vn/se-co-bien-phap-cung-ran-hon-de-facebook-tuan-thu-phap-luat-viet-nam-20191218134833497.htm>.

Ba là, ý thức của một số cơ quan, đơn vị và người dùng về công tác bảo vệ bí mật nhà nước, bảo vệ bí mật riêng tư trên môi trường internet chưa cao, chưa nhận thức đầy đủ vị trí, tầm quan trọng của công tác bảo đảm an toàn, an ninh mạng; kiến thức, kỹ năng bảo đảm an ninh mạng còn hạn chế. Không ít các cơ quan, tổ chức, doanh nghiệp chưa chú trọng áp dụng các biện pháp bảo đảm an toàn, an ninh thông tin.

Bốn là, các hệ thống mạng thông tin ở nước ta chưa theo một tiêu chuẩn thống nhất, nhiều nơi chưa có thẩm định về an ninh mạng; nhiều cơ quan, bộ, ngành sử dụng các thiết bị mạng lõi của một số tập đoàn công nghệ vẫn tồn tại lỗ hổng bảo mật, có nguy cơ bị theo dõi, giám sát, thu thập thông tin từ xa; hầu hết linh kiện điện tử giá rẻ tại Việt Nam đều có nguồn gốc từ nước ngoài, chứa nhiều lỗ hổng bảo mật hoặc bị cài sẵn các tài khoản truy cập “cửa hậu” (backdoor), khiến Việt Nam luôn nằm trong danh sách các quốc gia bị ảnh hưởng bởi các “mạng máy tính ma” lớn nhất thế giới¹.

Năm là, công tác bảo vệ an ninh thông tin, an ninh mạng chưa được đầu tư tương xứng và thỏa đáng. Sự phát triển như vũ bão về khoa học - công nghệ đã khiến cho vòng đời của sản phẩm an ninh mạng ngắn lại; yêu cầu đầu tư để theo kịp sự phát triển, không bị lạc hậu trong điều kiện kinh tế đất nước còn nhiều khó khăn là một trong những thách thức đang đặt ra. Nghiên cứu, ứng dụng và phát triển khoa học - công nghệ vào bảo đảm an ninh mạng ở nước ta chưa

1. Xem Bộ Thông tin và Truyền thông: *Sách trắng về công nghệ thông tin và truyền thông 2012, 2013, 2014, 2015, 2018*.

theo kịp tốc độ phát triển khoa học - công nghệ của thế giới; chưa tự chủ, sản xuất được các thiết bị công nghệ thông tin, dẫn đến lệ thuộc nhiều vào các sản phẩm nước ngoài.

Sáu là, công tác đào tạo nguồn nhân lực, chuyên gia an ninh mạng chưa theo kịp yêu cầu về số lượng và chất lượng, thiếu lực lượng chuyên gia chuyên trách bảo vệ an ninh mạng; chính sách đãi ngộ còn nhiều bất cập nên chưa phát huy hết năng lực chuyên môn của đội ngũ này.

Thời gian tới, sự phát triển của những công nghệ mới mang tính đột phá về truyền dẫn internet sẽ có những tác động trực tiếp tới sự phát triển của truyền thông xã hội. Điều đó dẫn đến khả năng kiểm soát, xử lý những tiêu cực từ truyền thông xã hội sẽ gặp nhiều khó khăn. Do đó, công tác quản lý nhà nước về truyền thông xã hội cần hết sức được coi trọng, trong đó tập trung vào một số nội dung sau:

Thứ nhất, cần xây dựng và hoàn thiện các văn bản pháp luật, tạo cơ sở pháp lý hoàn chỉnh cho quản lý nhà nước đối với các phương tiện truyền thông xã hội. Các quy phạm pháp luật cần cụ thể hóa và có cách tiếp cận đúng đắn, đầy đủ về thuật ngữ “truyền thông xã hội”, vì hiện nay các quy định pháp luật mới tập trung điều chỉnh đối với các hành vi liên quan mạng xã hội, internet, trong khi đó mạng xã hội chỉ là một loại hình phương tiện truyền thông xã hội.

Thứ hai, xây dựng chế tài phù hợp với thông lệ quốc tế trong quản lý nhà nước đối với các phương tiện truyền thông xã hội nước ngoài cung cấp dịch vụ cho người dùng tại Việt Nam. Tăng cường quản lý thị trường cung cấp dịch vụ và ứng dụng trên các phương tiện truyền thông xã hội; kiên quyết thực hiện nguyên tắc các nhà mạng, cung cấp, khai

thác dịch vụ mạng, nhất là các doanh nghiệp nước ngoài phải có trách nhiệm tuân thủ pháp luật Việt Nam, tôn trọng chủ quyền, lợi ích, an ninh quốc gia Việt Nam. Coi trọng các biện pháp kinh tế, yêu cầu trách nhiệm của các doanh nghiệp phải tương xứng với lợi ích mà họ được hưởng. Có chính sách đầu tư, hỗ trợ các phương tiện truyền thông xã hội có nền tảng công nghệ trong nước phát triển; khuyến khích các cơ quan, tổ chức trong nước xây dựng mạng xã hội nội bộ.

Thứ ba, trước lượng thông tin khổng lồ trên truyền thông xã hội, cần tăng cường ứng dụng công nghệ hiện đại để phòng ngừa, phát hiện, xử lý kịp thời các thông tin sai sự thật, xấu, độc có ảnh hưởng đến ổn định chính trị, xã hội; chú trọng sử dụng công nghệ, trí tuệ nhân tạo để xử lý, phân loại thông tin. Nâng cao năng lực phân tích, điều tra, nghiên cứu công chúng, đo lường thái độ của người sử dụng internet, tham gia truyền thông xã hội đối với những vấn đề được dư luận quan tâm.

Tăng cường các biện pháp tuyên truyền nâng cao hiểu biết pháp luật, ý thức, trách nhiệm khi tham gia các nền tảng truyền thông xã hội của mọi công dân. Giáo dục định hướng giá trị để giới trẻ biết và tránh các biểu hiện lệch lạc về nhận thức và hành vi; trang bị cho học sinh, sinh viên kỹ năng tự bảo vệ thông tin cá nhân, cách thức chất lọc, tiếp nhận thông tin. Phát huy vai trò của các tổ chức và cá nhân, nhất là những người điều hành website, blog, fanpage, KOLs, influencers, giới trẻ trong xây dựng môi trường internet, mạng xã hội lành mạnh¹.

1. Xem Võ Văn Thương: “Sử dụng mạng xã hội có trách nhiệm”, *Tlđđ*.

Thứ tư, phát huy vai trò của các phương tiện truyền thông chính thống trong định hướng, dẫn dắt truyền thông xã hội đi đúng hướng. Phải tạo dựng được một thế trận truyền thông mạnh đủ sức lấn át các dòng thông tin độc hại trên truyền thông xã hội.

Cần nâng cao vai trò của truyền thông chính thống trong đấu tranh, phản bác các quan điểm thù địch, sai trái và đưa tin định hướng dư luận trước những sự kiện thu hút được sự quan tâm của dư luận; ngăn chặn hiệu quả tâm lý đám đông, dư luận bị dẫn dắt bởi truyền thông xã hội dẫn tới những hiệu ứng tiêu cực; bảo đảm dòng thông tin từ truyền thông chính thống là thông điệp chủ đạo, chất lượng, chính xác, kịp thời, là bộ lọc đáng tin cậy về các vấn đề dư luận quan tâm.

TĂNG CƯỜNG ĐẤU TRANH TRÊN KHÔNG GIAN MẠNG BẢO VỆ VỮNG CHẮC NỀN TẢNG TƯ TƯỞNG CỦA ĐẢNG

ThS. PHẠM THỊ THINH*

Luật an ninh mạng năm 2018 nêu rõ: “Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian”. Với sự phát triển nhanh và đa dạng của mạng viễn thông, internet, không gian mạng từ một không gian ảo đã dần trở thành “không gian thực” trong đời sống xã hội, có tác dụng tích cực trong việc thúc đẩy sự phát triển của xã hội. Tuy nhiên, đây cũng là công cụ hữu ích mà các thế lực thù địch tận dụng để tiến hành các hoạt động tuyên truyền tấn công vào nền tảng tư tưởng của Đảng Cộng sản Việt Nam, làm ảnh hưởng đến uy tín và vai trò lãnh đạo của Đảng đối với đất nước, đe dọa an ninh chính trị của quốc gia. Vì thế, tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trên

* Phó Giám đốc - Phó Tổng Biên tập Nhà xuất bản Chính trị quốc gia Sự thật.

không gian mạng là một yêu cầu cấp thiết nhằm bảo đảm sự lãnh đạo của Đảng đối với Nhà nước và xã hội, nhất là trong bối cảnh Cách mạng công nghiệp lần thứ tư đang phát triển mạnh mẽ trên toàn cầu, tình hình thế giới, khu vực có nhiều biến động như hiện nay.

1. Đặt vấn đề

Sinh thời Chủ tịch Hồ Chí Minh từng nói: “Đảng có vững cách mệnh mới thành công, cũng như người cầm lái có vững thuyền mới chạy. Đảng muốn vững thì phải có chủ nghĩa làm cốt, trong đảng ai cũng phải hiểu, ai cũng phải theo chủ nghĩa ấy. Đảng mà không có chủ nghĩa cũng như người không có trí khôn, tàu không có bàn chỉ nam”¹. Đồng thời, Người cũng nêu rõ rằng: “Bây giờ học thuyết nhiều, chủ nghĩa nhiều, nhưng chủ nghĩa chân chính nhất, chắc chắn nhất, cách mệnh nhất là chủ nghĩa Lênin”². Quán triệt quan điểm này của Người, trong quá trình tiến hành công cuộc đổi mới đất nước, Đảng ta luôn khẳng định: “Đảng lấy chủ nghĩa Mác - Lênin và tư tưởng Hồ Chí Minh làm nền tảng tư tưởng, kim chỉ nam cho hành động”³. Do đó, việc bảo vệ nền tảng tư tưởng của Đảng là bảo vệ sự đúng đắn, trong sáng của chủ nghĩa Mác - Lênin và tư tưởng Hồ Chí Minh, bảo vệ Đảng, bảo vệ Cương lĩnh chính trị, đường lối của Đảng; bảo vệ đội ngũ cán bộ, đảng viên và nhân dân; bảo vệ

1, 2. Hồ Chí Minh: *Toàn tập*, Nxb. Chính trị quốc gia, Hà Nội, 2011, t.2, tr.289.

3. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XI*, Nxb. Chính trị quốc gia, Hà Nội, 2011, tr.88.

Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam và công cuộc đổi mới đất nước trong điều kiện hội nhập quốc tế; bảo vệ lợi ích quốc gia - dân tộc, giữ gìn môi trường hòa bình, ổn định và phát triển.

Trong Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII (2021), Đảng ta tiếp tục nhấn mạnh: “Công tác tư tưởng phải kết hợp giữa “xây” và “chống”, lấy “xây” là nhiệm vụ cơ bản, chiến lược, lâu dài, làm cho tư tưởng tiến bộ, tích cực thấm sâu vào toàn bộ đời sống xã hội, có tác dụng uốn nắn những biểu hiện lệch lạc, cải tạo những tư tưởng lạc hậu, đẩy lùi những sai trái”¹. Và để bảo vệ nền tảng tư tưởng của Đảng, cần phải: “Tiếp tục đổi mới mạnh mẽ nội dung, phương thức công tác tư tưởng, bảo đảm tính đảng, tính khoa học, tính chiến đấu, tính thực tiễn, kịp thời và hiệu quả; nâng cao chất lượng tuyên truyền, giáo dục, học tập chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh”².

Trong những năm qua, công tác bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch đã đạt được nhiều kết quả quan trọng, góp phần giữ vững, bổ sung và phát triển nền tảng tư tưởng của Đảng, ngăn chặn, đẩy lùi các âm mưu, thủ đoạn chống phá của các thế lực thù địch, phản động, an ninh chính trị, trật tự, an toàn xã hội được giữ vững. Niềm tin của nhân dân đối với Đảng, Nhà nước và chế độ xã hội chủ nghĩa do đó cũng được củng cố và nâng cao. Đặc biệt, sau khi có Nghị quyết số 35-NQ/TW, ngày 22/10/2018 của

1, 2. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.II, tr.232-233, 233.

Bộ Chính trị về *Tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới*, công tác đấu tranh, bảo vệ nền tảng tư tưởng của Đảng đã được triển khai ngày càng bài bản, thống nhất, đồng bộ, toàn diện, quyết liệt, đi vào chiều sâu.

Tuy nhiên, thực tiễn đã cho thấy, việc bảo vệ nền tảng tư tưởng của Đảng trong bối cảnh hiện nay là vô cùng phức tạp và khó khăn bởi “sự chống phá của các thế lực thù địch, tổ chức phản động ngày càng tinh vi hơn”¹. “Các thế lực thù địch, phản động chưa bao giờ từ bỏ ý đồ chống phá nền tảng tư tưởng của Đảng ta, luôn toan tính tạo ra “khoảng trống” về tư tưởng, lý luận trong đời sống chính trị - xã hội của nước ta với âm mưu cơ bản, lâu dài và rất thâm độc, đó là xoay chuyển quỹ đạo phát triển của đất nước ta đi chệch hướng xã hội chủ nghĩa”². Trong khi đó, “Công tác tư tưởng còn có mặt hạn chế, thiếu kịp thời, tính thuyết phục chưa cao. Đấu tranh bảo vệ nền tảng tư tưởng của Đảng, phản bác các quan điểm sai trái, thù địch, có lúc, có nơi còn bị động, thiếu sắc bén, tính chiến đấu chưa cao”³. Thực tiễn này đặt ra trong bối cảnh phát triển ngày càng mạnh mẽ của Cách mạng công nghiệp lần thứ tư sẽ càng phức tạp và khó khăn hơn nữa. Sự phát triển mạnh mẽ của công nghệ thông tin và mạng internet đã và đang làm cho không gian mạng, mạng xã hội trở thành nhu cầu tất yếu của cuộc sống, biến đời sống ảo

1, 3. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Sđd, t.II, tr.164, 222.

2. GS.TS. Nguyễn Xuân Thắng: *Tư tưởng, lý luận với đổi mới và phát triển đất nước*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, tr.467.

thành đời sống thực. Đấu tranh bảo vệ nền tảng tư tưởng của Đảng trong không gian thực đã khó khăn, phức tạp, song đấu tranh bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng lại càng khó khăn hơn gấp bội phần, bởi sự lan tỏa thông tin trên không gian mạng diễn ra nhanh chóng, khó sàng lọc, phán đoán và ngăn chặn. Thống kê cho thấy, Việt Nam là quốc gia có tốc độ tăng trưởng internet, mạng xã hội nhanh nhất thế giới. Theo số liệu thống kê đến tháng 01/2020, trong số 96,9 triệu dân cả nước có 68,17 triệu người (chiếm 70% dân số) dùng internet, cao thứ 12 trên thế giới và thứ 6 châu Á; 65 triệu người (chiếm 67% dân số) dùng mạng xã hội, chủ yếu là Facebook (đứng thứ 7 trong số 10 quốc gia sử dụng Facebook nhiều nhất) và là một trong 10 nước có số người dùng YouTube cao nhất thế giới. Trong đó, 94% người dùng internet hằng ngày là sinh viên, trí thức trẻ, thanh niên¹. Do đó, cần phải có sự nhận diện, đánh giá đúng đắn sự tấn công, chống phá của các thế lực thù địch, phản động vào nền tảng tư tưởng của Đảng trên không gian mạng, trên cơ sở đó đưa ra các giải pháp để ngăn chặn, đấu tranh, phản bác lại.

2. Nhận diện sự tấn công, chống phá của các thế lực thù địch, phản động trên không gian mạng

Ngày nay, đất nước đã được thống nhất, nhân dân được sống trong hòa bình, tự do và ổn định. Đời sống của nhân dân ở cả trong nước và nước ngoài đều đã được nâng cao một

1. Nhóm phóng viên thời sự: “Đập tan những âm mưu chống phá Đại hội XIII của Đảng”, Bài 1: “Nhận diện những thủ đoạn chống phá trước thềm Đại hội”, *Báo điện tử Đảng Cộng sản Việt Nam*, ngày 20/01/2021.

cách rõ rệt. Quan hệ đối ngoại của Việt Nam với các nước, các khu vực và các vùng lãnh thổ đã được cải thiện, nâng cao và ngày càng mở rộng, đa dạng, thân thiện, có sự gắn kết và hợp tác bền chặt. Vai trò và uy tín của Việt Nam trên trường quốc tế đã được nâng cao. Đó là thành tựu nổi bật của quá trình đổi mới đất nước 35 năm qua dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, điều đó chứng minh nền tảng tư tưởng và đường lối cách mạng của Đảng là đúng đắn, phù hợp với xu thế phát triển của thời đại và dân tộc. Tuy nhiên, các thế lực thù địch, phản động ở cả trong và ngoài nước vẫn không thừa nhận sự phát triển của đất nước, không thừa nhận vai trò lãnh đạo của Đảng, mà luôn tìm đủ mọi cách để chống phá, nhất là trên lĩnh vực tư tưởng. Sự tấn công, chống phá của các thế lực thù địch, phản động vào nền tảng tư tưởng của Đảng chưa bao giờ dừng lại, mà diễn ra liên tục với những hình thức ngày càng tinh vi, hiện đại. Và sự phát triển của công nghệ thông tin, của mạng xã hội đã trở thành công cụ hữu ích cho các thế lực thù địch, phản động tấn công vào nền tảng tư tưởng của Đảng. Trong khi đó, “việc dự báo, nắm bắt tình hình tư tưởng của cán bộ, đảng viên, tâm tư, nguyện vọng của nhân dân và định hướng dư luận xã hội có lúc chưa kịp thời. Kết quả thực hiện một số chủ trương của Đảng về quản lý báo chí, truyền thông, xuất bản, internet, mạng xã hội chưa đáp ứng yêu cầu”¹. Chính vì thế, không gian mạng là địa bàn mới, đặc thù mà các thế lực thù địch, phản động đang tích cực hoạt động tấn công

1. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Sdd, t.II, tr.172.

vào nền tảng tư tưởng của Đảng. Theo dõi sự chống phá của các thế lực thù địch, phản động có thể thấy, “chúng triệt để lợi dụng không gian mạng để tung các thông tin xấu độc, quan điểm sai trái, thù địch. Đây được coi là vùng “lãnh thổ đặc biệt” đang bị các thế lực thù địch lợi dụng triệt để nhằm chống phá Đảng và Nhà nước ta”¹.

Những luận điệu mà các thế lực thù địch, phản động dùng để tấn công vào nền tảng tư tưởng của Đảng được tập trung vào một số vấn đề sau:

Một là, tấn công trực tiếp vào nền tảng lý luận của chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh nhằm phủ nhận tính khoa học, đúng đắn của chủ nghĩa Mác - Lênin và tư tưởng Hồ Chí Minh.

Hai là, phủ nhận, hạ thấp vai trò lãnh đạo của Đảng và thể chế chính trị xã hội chủ nghĩa bằng các luận điệu xuyên tạc các sự kiện lịch sử, chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước.

Ba là, xuyên tạc tình hình đất nước, khoét sâu vào những hạn chế, yếu kém trong thực thi công vụ của một số cơ quan nhà nước, một số cán bộ lãnh đạo, quản lý để chia rẽ Đảng, Nhà nước với nhân dân; rêu rao cái gọi là “khủng hoảng toàn diện”, dùng con bài nhân quyền, dân chủ, tự do và bình đẳng tôn giáo, dân tộc,... để tấn công vào nền tảng tư tưởng của Đảng, hòng gây ra sự nhiễu loạn về an ninh chính trị, trật tự, an toàn xã hội, thậm chí là lật đổ Chính phủ.

1. Nhóm phóng viên thời sự: “Đập tan những âm mưu chống phá Đại hội XIII của Đảng”, Bài 1: “Nhận diện những thủ đoạn chống phá trước thềm Đại hội”, *Tlđđ*.

Bốn là, xâm nhập vào nội bộ ta, tìm cách phân hóa tổ chức, vận động những phần tử thoái hóa, biến chất trong hàng ngũ cán bộ, đảng viên để phát tán những tư tưởng phản động chống phá Đảng, Nhà nước.

Năm là, phá hoại đường lối đối ngoại độc lập, tự chủ, đa dạng hóa, đa phương hóa trong hội nhập quốc tế của Đảng ta; lôi kéo đồng bào ta ở nước ngoài, kêu gọi chính phủ các nước, các tổ chức quốc tế can thiệp vào công việc nội bộ của Việt Nam, gây sức ép đối với Việt Nam về các vấn đề dân chủ, nhân quyền...

Thủ đoạn mới của các thế lực phản động là chuyển từ bôi nhọ, phủ nhận chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh bằng luận điệu “du nhập ngoại lai”, “nhập khẩu lý luận” sang “đánh tráo, thay thế các khái niệm, thổi phồng cái gọi là “chủ thuyết phát triển mới”, đối lập C. Mác với V.I. Lênin, kêu gọi dùng “chủ nghĩa Hồ Chí Minh” để thay thế chủ nghĩa Mác - Lênin, trong khi chúng lờ đi một sự thật hiển nhiên, rõ ràng là tư tưởng Hồ Chí Minh là sự vận dụng và phát triển sáng tạo chủ nghĩa Mác - Lênin vào thực tiễn cụ thể của Việt Nam”¹. Sự tinh vi của các thế lực thù địch, phản động được thể hiện ở chỗ, chúng trích dẫn cắt xén, nửa vời những quan điểm của chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, đan cài bằng những quan điểm giả danh mácxít, làm cho người đọc mất phương hướng, lẫn lộn, không phân biệt được đúng - sai. Trên các trang mạng, các thế lực chống phá thường rêu rao rằng: “Đảng và Nhà nước Việt Nam, các nhà khoa học,

1. GS.TS. Nguyễn Xuân Thắng: *Tư tưởng, lý luận với đổi mới và phát triển đất nước*, Sđd, tr.471.

chính giới lý luận của ta đã dịch sai, hiểu sai quan điểm của C. Mác, Ph. Ăngghen, đồng thời chúng diễn giải lại theo cách hiểu xuyên tạc, méo mó hòng làm cho cán bộ, đảng viên và nhân dân hoang mang, dao động, suy giảm niềm tin vào sự lãnh đạo của Đảng, vào chủ nghĩa xã hội và con đường đi lên chủ nghĩa xã hội ở nước ta”¹. Bên cạnh đó, chúng còn đẩy mạnh tuyên truyền, cổ xúy du nhập các trào lưu tư tưởng cực đoan, chủ nghĩa dân túy, chủ nghĩa thực dụng, chủ nghĩa dân tộc cực đoan từ bên ngoài, kết hợp với kích động chủ nghĩa cá nhân, chủ nghĩa cơ hội, chủ nghĩa bè phái, chủ nghĩa hưởng lạc từ bên trong, nhằm thúc đẩy “tự diễn biến”, “tự chuyển hóa” trong nội bộ. Đặc biệt trong thời gian qua, chúng kích động, “hà hơi tiếp sức” cho những kẻ nhân danh “lòng yêu nước” để biểu tình gây rối trật tự, trị an; “triệt để lợi dụng các vụ án phức tạp, nhạy cảm để kích động, xuyên tạc, quy kết, vu cáo Đảng, Nhà nước yếu kém, đả kích các cơ quan tư pháp, kích động “bất tuân dân sự” trong xã hội”².

Như vậy có thể thấy, sự tấn công của các thế lực thù địch, phản động vào nền tảng tư tưởng của Đảng là toàn diện, có tổ chức và mục đích rõ ràng. Hàng loạt các tài khoản (nick name) cá nhân, các nhóm hội được lập ra trên nền tảng của các trang mạng xã hội như: Yahoo, Google, Facebook, YouTube, Zalo, Twitter, BBC, RFA, RFI, VOA,... để viết và đăng bài, chia sẻ các thông tin chống phá nền tảng tư tưởng, chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước. Chúng lúc ngấm ngầm, lúc công khai ra mặt tấn

1, 2. GS.TS. Nguyễn Xuân Thắng: *Tư tưởng, lý luận với đổi mới và phát triển đất nước*, Sđd, tr.471-472, 473.

công vào nền tảng tư tưởng của Đảng. Với chiêu bài trao đổi học thuật để “bảo vệ Đảng”, “chống lật sủ”, “chống chủ nghĩa xét lại lịch sử”..., nhiều nhóm hội đã công khai tấn công vào nền tảng tư tưởng của Đảng mà nếu người dùng mạng xã hội không có tư tưởng chính trị vững vàng sẽ khó có thể sàng lọc thông tin để nhận biết đúng - sai ra sao. Trong số những kẻ tấn công vào nền tảng tư tưởng của Đảng, cũng không thiếu những cán bộ vốn đã ở trong hàng ngũ của Đảng, song do bất mãn mà dung túng cho các hoạt động chống phá của các thế lực thù địch.

Bên cạnh đó, chúng còn lợi dụng chiêu bài bảo vệ Đảng để chống phá Đảng, nói xấu, hạ thấp và phủ nhận vai trò, đóng góp của Chủ tịch Hồ Chí Minh và các lãnh tụ cách mạng tiền bối của Đảng và Nhà nước, những người có công lao lớn đối với Đảng và quốc gia - dân tộc như Tổng Bí thư Lê Duẩn, Thủ tướng Chính phủ Võ Văn Kiệt, Đại tướng Võ Nguyên Giáp,... và cả những cán bộ cấp cao của Đảng hiện nay. Chiêu bài của chúng là tung ra một bài viết có nội dung bảo vệ Đảng hay một lãnh tụ nào đó, rồi để mặc nhiên cho các phần tử phản động, thù địch vào comment và chia sẻ những thông tin trái chiều không đúng sự thật. Điều này cho thấy, việc đấu tranh bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng đã trở thành nhiệm vụ cấp bách, thường xuyên của cả hệ thống chính trị. Văn kiện Đại hội XIII của Đảng nêu rõ: “Tăng cường bảo vệ nền tảng tư tưởng của Đảng, kiên quyết và thường xuyên đấu tranh phản bác các quan điểm sai trái, thù địch, cơ hội chính trị; đấu tranh, ngăn chặn, đẩy lùi sự suy thoái về tư tưởng chính trị, đạo đức, lối sống, những biểu hiện “tự diễn biến”,

“tự chuyển hóa” trong nội bộ”¹. Đồng thời, phải “thiết lập thể trận an ninh liên hoàn bên trong với bên ngoài biên giới quốc gia và trên không gian mạng; đặc biệt coi trọng an ninh mạng”².

3. Quan điểm của Đại hội XIII về đấu tranh bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng và định hướng, giải pháp cơ bản

Đại hội XIII của Đảng khẳng định, cần tiếp tục “kiên định và không ngừng vận dụng, phát triển sáng tạo chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh phù hợp với thực tiễn Việt Nam trong từng giai đoạn. Kiên định mục tiêu độc lập dân tộc gắn liền với chủ nghĩa xã hội. Kiên định đường lối đổi mới vì mục tiêu dân giàu, nước mạnh, dân chủ, công bằng, văn minh”³. Do đó, phải “coi trọng xây dựng Đảng về tư tưởng”⁴, coi đây là nhiệm vụ cơ bản, chiến lược lâu dài, làm cho tư tưởng tiến bộ, tích cực thấm sâu vào toàn bộ đời sống xã hội, có tác dụng uốn nắn những biểu hiện lệch lạc, cải tạo những tư tưởng lạc hậu, đẩy lùi những sai trái. Đồng thời, phải “tăng cường bảo vệ nền tảng tư tưởng của Đảng, kiên quyết và thường xuyên đấu tranh phản bác các quan điểm sai trái, thù địch, cơ hội chính trị”⁵; chủ động cung cấp thông tin kịp thời, chính xác, khách quan, đúng định hướng để phòng, chống “diễn biến hòa bình”, thông tin xấu, độc trên

1, 2, 3, 5. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.I, tr.183, 280, 181, 183.

4. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Sđd, t.II, tr.232.

internet, mạng xã hội. Đại hội cũng nêu rõ, để bảo vệ nền tảng tư tưởng của Đảng, trước hết cần phải “tiếp tục đổi mới mạnh mẽ nội dung, phương thức công tác tư tưởng, bảo đảm tính đảng, tính khoa học, tính chiến đấu, tính thực tiễn, kịp thời và hiệu quả; nâng cao chất lượng tuyên truyền, giáo dục, học tập chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh”¹. Đây là những định hướng đúng đắn của Đại hội XIII về công tác đấu tranh bảo vệ nền tảng tư tưởng của Đảng. Các quan điểm này đã nêu rõ vấn đề bảo vệ nền tảng tư tưởng của Đảng chính là bảo đảm tính đảng, tính khoa học, tính chiến đấu và tính thực tiễn của chủ nghĩa Mác - Lênin và tư tưởng Hồ Chí Minh; bảo vệ định hướng xã hội chủ nghĩa, bảo vệ quan điểm độc lập dân tộc gắn liền với chủ nghĩa xã hội của Đảng. Việc đấu tranh bảo vệ nền tảng tư tưởng của Đảng là một trong những nhiệm vụ quan trọng hàng đầu nhằm củng cố, tăng cường quốc phòng, bảo đảm an ninh quốc gia, trật tự, an toàn xã hội. Do đó, phải “tích cực, chủ động xây dựng kế hoạch, phương án tác chiến, nâng cao trình độ, khả năng sẵn sàng chiến đấu bảo vệ vững chắc độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ và giữ vững ổn định chính trị, an ninh quốc gia, trật tự, an toàn xã hội, giữ vững chủ quyền số quốc gia trên không gian mạng trong mọi tình huống”².

Về giải pháp tăng cường đấu tranh bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng, Đại hội XIII của Đảng nêu rõ: “Tăng cường quản lý và định hướng hoạt động của các cơ quan báo chí; tập trung đào tạo, xây dựng đội ngũ

1, 2. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Sdd, t.I, tr.183, 277.

cán bộ quản lý báo chí, phóng viên, biên tập viên có bản lĩnh chính trị, phẩm chất đạo đức trong sáng và tinh thông nghiệp vụ để nâng cao hiệu quả công tác tuyên truyền”¹. Quan điểm này cho thấy Đảng đã nhìn nhận trúng và đánh giá cao vai trò của các cơ quan báo chí, truyền thông trong công tác đấu tranh bảo vệ nền tảng tư tưởng của Đảng. Do đó, việc tập trung đào tạo đội ngũ cán bộ quản lý báo chí, phóng viên, biên tập viên có bản lĩnh chính trị vững vàng là điều cần thiết, vì đây chính là đội ngũ “đứng mũi chịu sào” trong việc thu thập, xử lý thông tin và truyền bá thông tin. Mà nếu họ không có bản lĩnh chính trị vững vàng, không có đủ nhận thức lý luận sẽ rất dễ trở thành công cụ tuyên truyền cho các thế lực thù địch, phản động. Việc một số kênh truyền hình, báo, đài gần đây thường xuyên phải đăng tin sửa sai đã cho thấy công tác quản lý báo chí, truyền thông và chất lượng đội ngũ phóng viên, biên tập viên chưa thực sự tốt, cần tăng cường hơn nữa.

Đại hội XIII cũng chỉ rõ, phải “xử lý nghiêm theo quy định của Đảng và pháp luật của Nhà nước đối với các cơ quan báo chí, phóng viên đăng tải thông tin chưa được xác minh, kiểm chứng, không có cơ sở, căn cứ, gây ảnh hưởng không tốt đến dư luận xã hội; phát huy hơn nữa vai trò của văn học, nghệ thuật trên mặt trận tư tưởng; đẩy mạnh ứng dụng thành tựu khoa học - công nghệ phục vụ công tác tuyên truyền, bảo đảm an ninh tư tưởng trên môi trường không gian mạng”².

1, 2. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Sdd, t.II, tr.234.

Để đấu tranh bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng có hiệu quả, cần thực hiện tốt các giải pháp sau:

Một là, quán triệt sâu sắc tầm quan trọng của công tác bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trên không gian mạng trong cán bộ, đảng viên và nhân dân, đặc biệt là đối với lực lượng Công an nhân dân và cán bộ bảo vệ nội bộ. Xác định đây là nhiệm vụ vừa cấp bách, vừa lâu dài, là nhiệm vụ có ý nghĩa sống còn của cả hệ thống chính trị.

Hai là, đa dạng hóa nội dung, phương thức, hình thức bảo vệ nền tảng tư tưởng của Đảng với nhiều cấp độ, phù hợp với từng đối tượng. Nhận diện rõ các thông tin xấu, độc, xuyên tạc trên không gian mạng để xác định biện pháp đấu tranh trực diện hay gián tiếp theo kịch bản chặt chẽ, thống nhất, đa dạng, rộng rãi, có sự phối hợp của nhiều lực lượng để tăng tính hiệu quả và độ lan tỏa. Đẩy mạnh công tác quản lý nhà nước về truyền thông trên không gian mạng; hoàn thiện các quy định pháp lý về quản lý hoạt động trên không gian mạng, tạo căn cứ để cảnh báo, răn đe và xử lý các trường hợp vi phạm, lợi dụng những “điểm nóng”, vụ việc phức tạp, nhạy cảm để phát ngôn, gây sự chú ý của dư luận xã hội. Song song với đó, phải tập trung phòng, chống từ nội bộ, ngăn ngừa sự suy thoái về tư tưởng chính trị, đạo đức, lối sống, “tự diễn biến”, “tự chuyển hóa” trong mỗi cán bộ, đảng viên.

Ba là, tăng cường các giải pháp về công nghệ, kỹ thuật để sớm phát hiện, ngăn chặn nguồn tuyên truyền, phát tán những tư tưởng, quan điểm sai trái, thù địch trên không gian mạng, ngăn chặn các trang mạng độc hại. Xây dựng các

trang mạng của ta để đưa thông tin chính thức, sâu rộng, lập luận sắc bén, thuyết phục về những thành tựu phát triển đất nước, xây dựng và bảo vệ Tổ quốc, các định hướng nhiệm vụ chính trị, kinh tế - xã hội của đất nước, của địa phương để phản bác, vạch trần âm mưu, thủ đoạn xuyên tạc của các thế lực thù địch bằng những thông tin tích cực, những bằng chứng sát thực, từng bước giành thế chủ động về thông tin trên không gian mạng.

Bốn là, nhận diện rõ những vấn đề mà các thế lực thù địch tập trung chống phá để xây dựng luận cứ khoa học thuyết phục nhằm trực tiếp đấu tranh phản bác. Nâng cao hơn nữa chất lượng nghiên cứu tổng kết lý luận, lấy đó làm tiền đề, luận cứ để hoạch định đường lối, chủ trương của Đảng, đồng thời phản biện lại các quan điểm sai trái, thù địch. “Tiếp tục bổ sung, phát triển hệ thống các quan điểm về chủ nghĩa xã hội và con đường đi lên chủ nghĩa xã hội ở Việt Nam. củng cố các cơ quan nghiên cứu lý luận chính trị của Đảng và Nhà nước. Tập trung lãnh đạo, chỉ đạo nghiên cứu các vấn đề lý luận khó, phức tạp phát sinh từ thực tiễn hoặc tồn tại trong thời gian dài; những vấn đề chưa rõ về cơ sở lý luận, còn có nhiều ý kiến khác nhau, mạnh dạn cho thí điểm, tổng kết kịp thời để có kết luận nhằm thống nhất về mặt nhận thức”¹. Trong luận giải những quan điểm của chủ nghĩa Mác - Lênin, cần chú ý một số nội dung mà các thế lực thù địch luôn chống phá kịch liệt, như các vấn đề đấu tranh giai cấp, vấn đề tiếp thu, vận dụng chủ nghĩa Mác - Lênin ở nước

1. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Sđd, t.II, tr.235.

ta, những giá trị bền vững của chủ nghĩa Mác - Lênin trong thời đại ngày nay. Tiếp tục nghiên cứu trên quan điểm khách quan, khoa học những tư tưởng, học thuyết, lý thuyết mới, tiến bộ để chất lọc, tiếp thu những giá trị tinh hoa văn hóa của nhân loại.

Năm là, nâng cao chất lượng đào tạo và bồi dưỡng đội ngũ cán bộ, đảng viên để qua đó nâng cao tính chiến đấu và hiệu quả trong việc đấu tranh với các thế lực thù địch, phản động trên không gian mạng. Đặc biệt đẩy mạnh việc tuyên truyền rộng rãi trên không gian mạng về lịch sử dân tộc, lịch sử cách mạng và lịch sử Đảng để cán bộ, đảng viên và nhân dân phân biệt rõ đúng - sai, miễn nhiễm với thông tin xấu, độc. Tiếp tục phát triển đội ngũ chuyên gia đầu ngành và tầm cao về lý luận, đội ngũ cán bộ chuyên trách làm công tác tư tưởng lý luận, lực lượng Công an nhân dân bảo đảm an ninh trên không gian mạng có bản lĩnh, trí tuệ, năng lực, phương pháp và kỹ năng đấu tranh trên không gian mạng đáp ứng yêu cầu nhiệm vụ trong tình hình mới. Đối với lực lượng chuyên trách bảo vệ an ninh mạng, cần tăng cường tiềm lực, nhất là trình độ khoa học công nghệ, kỹ thuật nghiệp vụ để lực lượng này chủ động, kịp thời phòng ngừa, ngăn chặn, vô hiệu hóa từ xa các hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia. Xây dựng cơ chế bảo vệ những người tham gia đấu tranh chống các quan điểm sai trái, thù địch để tránh việc họ bị các thế lực thù địch tấn công trở lại. Chủ động trấn áp, xử lý tội phạm, những phần tử phản động, thù địch vi phạm pháp luật của Nhà nước ta.

MẠNG XÃ HỘI: LỢI ÍCH VÀ CÁC MỐI ĐE DỌA AN NINH

ThS. NGUYỄN HOÀI ANH*

Thế giới đang chứng kiến hàng loạt những đột phá về khoa học và công nghệ, đã được coi là những xu hướng và động lực dẫn dắt của Cách mạng công nghiệp lần thứ tư. Bản chất của Cách mạng công nghiệp lần thứ tư là dựa trên nền tảng công nghệ số và tích hợp tất cả các công nghệ thông minh để tối ưu hóa quy trình, phương thức sản xuất; trong đó những công nghệ đang và sẽ có tác động lớn nhất là công nghệ in 3D, công nghệ sinh học, công nghệ vật liệu mới, công nghệ tự động hóa, người máy,... Những thành tựu của cuộc cách mạng này là cơ hội thuận lợi để các quốc gia trên thế giới, trong đó có các nước đang phát triển như Việt Nam có thể thực hiện “đi tắt”, “đón đầu”, tiến thẳng vào lĩnh vực công nghệ mới, tranh thủ thành tựu khoa học và công nghệ, đẩy nhanh tiến trình công nghiệp hóa, hiện đại hóa đất nước, hội nhập quốc tế và thu hẹp khoảng cách phát triển so với các nước phát triển hàng đầu thế giới. Tuy nhiên,

* Phó Giám đốc - Phó Tổng Biên tập Nhà xuất bản Chính trị quốc gia Sự thật.

cuộc cách mạng này cũng đặt ra nhiều thách thức, trong đó đặc biệt nghiêm trọng là những thách thức an ninh trên mạng xã hội.

1. Theo Nghị định số 72/2013/NĐ-CP, ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng: “mạng xã hội là hệ thống thông tin cung cấp cho cộng đồng người sử dụng mạng các dịch vụ lưu trữ, cung cấp, sử dụng, tìm kiếm, chia sẻ và trao đổi thông tin với nhau, bao gồm dịch vụ tạo trang thông tin điện tử cá nhân, diễn đàn (forum), trò chuyện (chat) trực tuyến, chia sẻ âm thanh, hình ảnh và các hình thức dịch vụ tương tự khác”. Theo đó, mạng xã hội có những đặc trưng sau: (1) là một ứng dụng/dịch vụ được cung cấp trực tuyến trên mạng internet; (2) cho phép người dùng thiết lập hồ sơ cá nhân, tạo lập và chia sẻ thông tin, tương tác, kết nối và thiết lập các cộng đồng với số lượng không giới hạn; (3) không bị giới hạn kết nối cả về không gian, thời gian.

Những lợi ích to lớn mà mạng xã hội mang lại cho con người là không thể phủ nhận. Thông tin trên mạng xã hội có tốc độ lan truyền nhanh, tiếp cận đến từng cá nhân người dùng, nên có thể sử dụng mạng xã hội làm công cụ tuyên truyền, phổ biến chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước; tuyên truyền, nâng cao nhận thức cho nhân dân trước hoạt động phá hoại về tư tưởng chính trị, đạo đức, lối sống; tán phát thông tin xấu, độc của các thế lực thù địch, phản động.

Mạng xã hội cũng là kênh cung cấp thông tin quan trọng và kịp thời cho nhân dân khi xảy ra các vụ việc phức tạp, dư luận quan tâm nếu được tổ chức có hiệu quả, tránh tạo ra

nhiều luồng thông tin trái chiều làm nhiễu loạn xã hội. Bên cạnh đó, mạng xã hội nếu được khai thác triệt để sẽ trở thành phương tiện hữu hiệu góp phần xây dựng và hoàn thiện mối quan hệ giữa nhà nước và công dân. Sự tương tác giữa nhà nước và công dân thông qua mạng xã hội thể hiện qua việc cơ quan nhà nước tiếp nhận và giải quyết những bức xúc, khó khăn, vướng mắc của người dân trong thực hiện các thủ tục hành chính nhằm bảo đảm quyền và lợi ích hợp pháp của người dân; lấy ý kiến phản hồi của người dân trong quá trình quản lý, điều hành phát triển kinh tế - xã hội một cách nhanh chóng để có sự điều chỉnh, đáp ứng kịp thời. Trong kỷ nguyên số, thông tin, dữ liệu của cá nhân, cơ quan, tổ chức trên cộng đồng mạng trở thành nguồn tài nguyên rất quan trọng cần được quản lý, bảo vệ và khai thác phục vụ phát triển kinh tế - xã hội.

Ngoài ra, sự phát triển của công nghệ thông tin, truyền thông và mạng xã hội cũng trở thành cơ hội để thúc đẩy phát triển mô hình “kinh tế chia sẻ”, “kinh tế mạng lưới” và các phong trào khởi nghiệp sáng tạo, qua đó giúp tận dụng, tối ưu hóa các nguồn lực, tài nguyên còn dư thừa trong thời kỳ Cách mạng công nghiệp lần thứ tư. Mạng xã hội cũng là “cánh tay nối dài” của báo chí truyền thống, góp phần thúc đẩy thông tin, truyền thông xã hội phát triển, đáp ứng nhu cầu thông tin ngày càng lớn của người dân. Nhiều cơ quan báo chí đã thiết lập trang mạng xã hội, có hoạt động liên kết với các mạng xã hội lớn, có nhiều người sử dụng để mở rộng thông tin và tăng khả năng tiếp cận tới người dân.

Trên thế giới, nhiều chính khách đã sử dụng mạng xã hội như một kênh hữu hiệu để chia sẻ thông tin về hoạt động của

chính phủ, truyền thông điệp của chính phủ tới người dân trong nước và thế giới. Ở Việt Nam, hồi đầu tháng 9/2021, Chủ tịch Ủy ban nhân dân Thành phố Hồ Chí Minh là chính khách đầu tiên sử dụng mạng xã hội làm phương tiện để chính quyền thông tin, giao lưu trực tuyến với người dân thành phố về những định hướng lớn của Thành phố Hồ Chí Minh sau giãn cách xã hội do đại dịch Covid-19.

2. Tuy nhiên, sự phát triển nhanh chóng của công nghệ thông tin và các dịch vụ mạng đặt ra vấn đề về an ninh mạng cho các chính phủ. An ninh mạng được hiểu là “sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân”¹. Các mối đe dọa an ninh từ mạng xã hội xuất phát từ nguyên nhân là nội dung thông tin trên mạng xã hội do người dùng tự sáng tạo ra. Với khả năng cập nhật nhanh chóng, ít bị kiểm duyệt, cộng với cơ chế tiếp cận theo hành vi, thói quen của người dùng được hỗ trợ bởi nền tảng công nghệ hiện đại đã khiến thông tin trên mạng xã hội có tốc độ lan tỏa nhanh, dễ tạo hiệu ứng hoặc các xu hướng (trend) trên mạng xã hội. Chính bởi vậy, sự phát triển của mạng xã hội cũng sớm bộc lộ những nguy cơ tác động tiêu cực tới sự ổn định chính trị - xã hội, an ninh quốc gia và an ninh, an toàn thông tin của các tổ chức, cá nhân.

Tính đến đầu năm 2021, tỷ lệ người dùng internet tại Việt Nam chiếm tới 70,3% dân số, trong tổng số dân là 97,75 triệu người thì có đến 154,4 triệu thuê bao di động được đăng ký,

1. Theo *Luật an ninh mạng*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2018, Điều 2.

có 72 triệu người dùng mạng xã hội, tỷ lệ tài khoản mạng xã hội/tổng dân số là 73,7%, thiết bị có kết nối mạng viễn thông phổ biến được ưa chuộng là điện thoại thông minh, tỷ lệ thuê bao di động sử dụng điện thoại thông minh chiếm 96,9%, cao hơn mức trung bình chung của thế giới, thời gian sử dụng internet trung bình hàng ngày (trong độ tuổi 16 - 64) là 6 giờ 47 phút, trong đó 2 giờ 21 phút là thời gian cho mạng xã hội. Các mạng xã hội được sử dụng nhiều nhất tại Việt Nam là: YouTube, Facebook, Zalo, Instagram, Tiktok, Twitter...¹, các dịch vụ mạng xã hội Việt Nam ra đời sau, nhắm tới đối tượng người dùng trong nước là chủ yếu, đang trong quá trình trưởng thành, nâng cao sức cạnh tranh với mạng xã hội của nước ngoài.

Chính bởi vậy, mạng xã hội cũng là “môi trường và không gian lý tưởng” để các thế lực thù địch và đối tượng xấu lợi dụng thực hiện các hành vi vi phạm pháp luật, đe dọa an ninh quốc gia, như: tuyên truyền, truyền bá những thông tin gây hiệu ứng đám đông, phục vụ các mục đích về kinh tế, chính trị, quân sự, ngoại giao; truyền bá ý thức hệ đối lập, tôn giáo cực đoan, kích động, gây mất ổn định chính trị; thực hiện chiến lược “diễn biến hòa bình”, thông qua việc tài trợ, hậu thuẫn cho các tổ chức, phần tử chống đối sử dụng mạng xã hội để xuyên tạc, tuyên truyền chống phá chế độ, đòi tự do, dân chủ, nhân quyền; dùng điệp báo tấn công mạng nhằm lấy cắp thông tin nhạy cảm, bí mật quốc gia... Do đó, nguy cơ mất tài nguyên thông tin và mất kiểm soát

1. Xem “Chuyển đổi số tại Việt Nam và những thống kê ấn tượng đầu năm 2021”, <https://specials.laodong.vn>.

an ninh, an toàn thông tin trên mạng xã hội sẽ dẫn tới nguy cơ trở thành “thuộc địa số”, lệ thuộc vào công nghệ nước ngoài khiến chủ quyền, lợi ích quốc gia không được bảo đảm phát triển bền vững¹. Bên cạnh đó, tội phạm trên mạng xã hội cũng đang tạo ra thách thức ngày càng trực tiếp đối với an ninh của các quốc gia. Trên không gian mạng hiện có bốn mối đe dọa đến an ninh quốc gia là: chiến tranh không gian mạng; gián điệp kinh tế; tội phạm mạng và khủng bố trên không gian mạng².

Đối với Việt Nam, các thế lực thù địch tăng cường lợi dụng internet và mạng xã hội để thực hiện các hoạt động chống phá Đảng, Nhà nước ta và sự nghiệp cách mạng của nhân dân ta. Các trang mạng xã hội nước ngoài như Facebook, YouTube... liên tục cập nhật, bổ sung các tính năng mới, trong đó đáng chú ý nhất là các tính năng: livestream (truyền hình trực tiếp); messenger (tích hợp đầy đủ các tính năng quay phim, chụp ảnh, gọi thoại, gọi video, nhắn tin bằng chữ hoặc âm thanh, gửi tài liệu, hình ảnh...); tạo nhóm kín để trao đổi; gợi ý nội dung tương tự nội dung người dùng quan tâm hoặc thích xem; hiển thị nội dung theo mối quan tâm của từng nhóm đối tượng cụ thể... Đây là những tính năng giúp cho việc kết nối, trao đổi, chia sẻ thông tin giữa người dùng mạng xã hội trở nên rất tiện lợi và bí

1. Theo Bộ Công an, Học viện An ninh nhân dân: *Đảm bảo an ninh thông tin trong kỷ nguyên 4.0*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2019, tr.336-337.

2. Theo TS. Nguyễn Việt Lâm (Chủ biên): *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, 2019, tr.9-10.

mật, đồng thời giúp cho các thông điệp mà người dùng mạng xã hội muốn chuyển tải đến những người khác trở nên vô cùng dễ dàng và có độ chính xác rất cao theo từng nhóm đối tượng về độ tuổi, giới tính, quan điểm chính trị, tôn giáo, sở thích, mối quan tâm chung, công việc, khu vực, địa điểm... Các thế lực thù địch đã tăng cường sử dụng những tính năng này của mạng xã hội để không chỉ tung tin giả, tuyên truyền xuyên tạc, nói xấu Đảng, Nhà nước, chế độ ta, mà còn tiến hành các hoạt động lôi kéo, tập hợp lực lượng, kích động, dẫn dắt, điều hành các hoạt động biểu tình, bạo loạn, lật đổ, thực hiện âm mưu “diễn biến hòa bình”, “cách mạng màu” tại Việt Nam. Thống kê của các cơ quan chức năng thuộc Bộ Công an cho thấy, từ năm 2010 đến tháng 12/2018, các thế lực thù địch, phần tử xấu đã, đang sử dụng 8.784 web, blog có tên miền nước ngoài; 381 web, blog có tên miền trong nước thường xuyên đăng tải thông tin xấu, độc. Cơ quan Công an các cấp đã phát hiện 279 vụ sử dụng internet xâm phạm an ninh quốc gia, đấu tranh với hơn 200 đối tượng, bắt, xử lý 140 đối tượng. Đáng chú ý, trong đó có 219 vụ kích động biểu tình trên không gian mạng; 138 hội, nhóm trá hình hoạt động trên không gian mạng; 45.498 lượt cổng thông tin, trang tin điện tử có tên miền .vn bị tấn công, trong đó có 2.113 lượt tấn công các cổng thông tin, trang tin điện tử của cơ quan Đảng, Nhà nước, gây ra những hậu quả nghiêm trọng¹. Theo số liệu thống kê của Cục An toàn thông tin, Bộ Thông tin và Truyền thông, trong 6 tháng đầu năm 2019, Việt Nam đã xảy ra 3.159 vụ

1. Theo Cục An ninh mạng: *Báo cáo tổng kết của Cục An ninh mạng từ năm 2010 đến năm 2018*.

tấn công mạng vào các hệ thống thông tin, trong đó có tới 968 cuộc tấn công thay đổi giao diện (Deface), 635 cuộc tấn công cài cắm mã độc (Malware), 1.556 cuộc tấn công lừa đảo (Phishing)... Hệ thống giám sát của Bộ Thông tin và Truyền thông cũng đã ghi nhận được 203 triệu sự kiện an toàn mạng trong 6 tháng đầu năm 2019, tăng 9% so với cùng kỳ năm 2018. Trong đó, các cuộc tấn công nguy hiểm liên quan đến mã độc trong hệ thống phục vụ chính phủ điện tử được phát hiện tăng gấp 2 lần¹.

3. Có thể nói, ứng dụng công nghệ thông tin và các dịch vụ trên không gian mạng đã trở thành động lực quan trọng để phát triển kinh tế - xã hội, tạo thời cơ mới cho Việt Nam sử dụng thành tựu khoa học - công nghệ tiên tiến nhằm đẩy mạnh hơn tiến trình công nghiệp hóa, hiện đại hóa đất nước và thu hẹp khoảng cách phát triển, hội nhập sâu rộng hơn, hiệu quả hơn vào nền kinh tế thế giới, phát triển văn hóa - xã hội, củng cố quốc phòng, an ninh. Tuy nhiên, những lỗ hổng an ninh cũng đặt ra nhiệm vụ cấp bách trong bảo đảm an ninh thông tin trên mạng xã hội ở Việt Nam. Đảng và Nhà nước ta nhất quán khẳng định: An ninh mạng là một bộ phận không thể tách rời của an ninh quốc gia, bao gồm sự bất khả xâm phạm về chủ quyền quốc gia trên không gian mạng, bảo đảm mọi thông tin và hoạt động trên không gian mạng không gây phương hại đến sự ổn định, phát triển bền vững của chế độ xã hội chủ nghĩa và Nhà nước Việt Nam, đến độc lập,

1. Theo Cục An toàn thông tin - Bộ Thông tin và Truyền thông: *Báo cáo tổng kết tình hình, kết quả tấn công hệ thống thông tin 6 tháng đầu năm 2019*.

chủ quyền, thống nhất và toàn vẹn lãnh thổ, trật tự, an toàn xã hội. Đại hội đại biểu toàn quốc lần thứ XIII của Đảng (tháng 01/2021) tiếp tục khẳng định: “Tích cực, chủ động xây dựng kế hoạch, phương án tác chiến, nâng cao trình độ, khả năng sẵn sàng chiến đấu bảo vệ vững chắc độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ và giữ vững ổn định chính trị, an ninh quốc gia, trật tự, an toàn xã hội, giữ vững chủ quyền số quốc gia trên không gian mạng trong mọi tình huống”¹.

Thời gian qua, Đảng và Nhà nước đã ban hành nhiều nghị quyết, chỉ thị nhằm tăng cường năng lực quản trị an ninh mạng, như: Chỉ thị số 58-CT/TW, ngày 17/10/2000 của Bộ Chính trị khóa VIII *Về đẩy mạnh ứng dụng và phát triển công nghệ thông tin phục vụ sự nghiệp công nghiệp hóa, hiện đại hóa*; Chỉ thị số 28-CT/TW, ngày 16/9/2013 của Ban Bí thư khóa XI *Về tăng cường công tác bảo đảm an toàn thông tin mạng*; Chỉ thị số 15/CT-TTg, ngày 17/6/2014 của Thủ tướng Chính phủ *Về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới*. Đặc biệt là Nghị quyết số 28-NQ/TW, ngày 25/10/2013 của Ban Chấp hành Trung ương Đảng khóa XI về *Chiến lược bảo vệ Tổ quốc trong tình hình mới*; Nghị quyết số 29-NQ/TW, ngày 25/7/2018 của Bộ Chính trị khóa XII 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 khóa XII về *Chiến lược an ninh mạng quốc gia*; Nghị quyết số 33-NQ/TW, ngày 28/9/2018 của Bộ Chính trị khóa XII về *Chiến lược bảo vệ biên giới*

1. Đảng Cộng sản Việt Nam: Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.I, tr.277.

quốc gia; Luật an ninh mạng năm 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 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;... Trên cơ sở nhận định nguy cơ xảy ra chiến tranh mạng, mất an ninh thông tin ngày càng tăng, các văn bản đều thống nhất khẳng định: Chủ quyền trên không gian mạng là bộ phận quan trọng của chủ quyền quốc gia; bảo vệ chủ quyền quốc gia trên không gian mạng là nhiệm vụ cấp bách, lâu dài của cả hệ thống chính trị, đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý của Nhà nước và đặt ra mục tiêu phải chủ động phòng ngừa, ngăn chặn có hiệu quả chiến tranh mạng; chuẩn bị nguồn lực sẵn sàng để thực hiện tác chiến trên không gian mạng, góp phần bảo vệ Tổ quốc từ sớm, từ xa.

Với thế mạnh vốn có của mạng xã hội về sự đa dạng và lan truyền nhanh của thông tin, mức tương tác và liên kết xã hội cũng như sự độc quyền trong quản lý, sử dụng thông tin, người sử dụng cũng đã và sẽ tiếp tục dẫn tới những phức tạp, hệ lụy khó lường. Tuy nhiên, không thể hạn chế, ngăn cấm sự phát triển của mạng xã hội bằng các biện pháp hành chính, mà cần áp dụng tổng thể các giải pháp để quản lý, định hướng sự phát triển của mạng xã hội theo hướng phát huy tối đa mặt tích cực nhằm bảo vệ, lan tỏa những giá trị tốt đẹp được xã hội thừa nhận, hạn chế tác động, ảnh hưởng của mặt tiêu cực tới an ninh, trật tự của đất nước.

Một là, cần nhận thức rõ tính hai mặt của mạng xã hội, nhất là mặt tiêu cực để đưa ra giải pháp đẩy mạnh và đổi mới công tác thông tin, góp phần tuyên truyền, nâng cao

nhận thức, trách nhiệm và ý thức cho người sử dụng. Tuyên truyền, giáo dục để người dân khi sử dụng mạng xã hội có ý thức cảnh giác, chủ động kiểm chứng thông tin, hạn chế tình trạng vô tình tiếp tay cho việc lan truyền các thông tin xấu, độc hoặc thông tin không chính xác, dung tục, phản cảm, thông tin có ý đồ xấu... Nâng cao tinh thần cảnh giác, ý thức bảo vệ thông tin cá nhân, thông tin thuộc bí mật nội bộ của các cơ quan, tổ chức và thông tin bí mật quốc gia khi cung cấp, trao đổi, chia sẻ trên mạng xã hội.

Hai là, sử dụng mạng xã hội trở thành công cụ truyền thông hữu hiệu, cùng với truyền thông truyền thống tạo ra môi trường thông tin lành mạnh, tin cậy, phục vụ phát triển kinh tế - xã hội và bảo đảm an ninh thông tin. Tăng cường tính liên kết chặt chẽ, thường xuyên giữa mạng xã hội với báo điện tử, trang thông tin điện tử tổng hợp của các cơ quan, tổ chức, nhất là cơ quan nhà nước để chủ động tiếp cận, chuyển tải thông tin nhanh chóng, chính xác, kịp thời tới người dân.

Ba là, tiếp tục rà soát, bổ sung, hoàn thiện các quy định pháp luật về quản lý, sử dụng mạng internet, mạng xã hội tại Việt Nam, làm cơ sở pháp lý cho bảo đảm an ninh thông tin. Tạo hành lang pháp lý cho phép các cơ quan chức năng công khai chặn lọc, kiểm soát thông tin trên mạng xã hội và quản lý công khai đối với các tài khoản mạng xã hội có lượng người theo dõi, tương tác lớn; đồng thời phát triển các công cụ, phần mềm tự động lọc và phân tích thông tin của Việt Nam để chủ động theo dõi, giám sát thông tin trên mạng xã hội, kịp thời phòng ngừa, cảnh báo và ngăn chặn ngay từ đầu đối với những dòng thông tin xấu, độc, sai sự thật.

Bốn là, khuyến khích phát triển hạ tầng công nghệ thông tin, công nghệ số, tạo điều kiện phát triển mạng xã hội có nền tảng công nghệ trong nước, đặc biệt xây dựng mạng xã hội nội bộ ở những cơ quan, tổ chức trọng yếu. Đẩy mạnh quan hệ quốc tế với chính phủ nước ngoài, các tổ chức, các nhà cung cấp dịch vụ mạng xã hội lớn trên thế giới để có sự phối hợp thường xuyên, liên tục trong quản lý, chọn lọc thông tin.

Năm là, phát huy vai trò và trách nhiệm của các cơ quan, tổ chức, người dân khi tham gia mạng xã hội. Đẩy mạnh công tác quản lý, định hướng, giáo dục văn hóa sử dụng mạng xã hội của các thành viên trong cơ quan, tổ chức, hiệp hội. Phát huy vai trò tiên phong, gương mẫu của cán bộ, đảng viên, công chức, viên chức trong việc xây dựng bộ quy tắc ứng xử chung, thực hiện văn hóa tham gia, sử dụng mạng xã hội; nâng cao trách nhiệm bảo vệ và lan tỏa những giá trị cốt lõi, nền tảng, nhân văn, đồng thời không chia sẻ, tiếp tay và kịp thời phản bác các thông tin xấu, độc, những quan điểm sai trái, thù địch.

TĂNG CƯỜNG HỢP TÁC QUỐC TẾ BẢO VỆ CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG

Thiếu tướng, PGS.TS. VŨ CƯỜNG QUYẾT*

Chủ quyền quốc gia trên không gian mạng là các quyền quản lý, kiểm soát đối với kết cấu hạ tầng không gian mạng và thông tin được tạo ra, lưu trữ, xử lý, trao đổi trên đó; được thực hiện thông qua quyền tài phán theo luật pháp quốc tế đối với kết cấu hạ tầng thuộc sở hữu ở trong và ngoài lãnh thổ quốc gia bằng các mật mã bảo vệ thông tin số truyền dẫn trên không gian mạng toàn cầu. Chủ quyền không gian mạng của quốc gia bao hàm bốn yếu tố cơ bản: các hệ thống thông tin (lãnh thổ); chủ thể các hoạt động trên mạng quốc gia (dân số); số liệu - đối tượng thao tác trên mạng, biểu đạt trạng thái tín hiệu mà con người có thể lý giải được (tài nguyên); quy tắc xử lý và truyền dữ liệu (chính phủ). Tôn trọng chủ quyền quốc gia là một nguyên tắc cơ bản được ghi nhận trong hệ thống luật pháp quốc tế. Theo đó, tất cả các quốc gia không tính đến quy mô lãnh thổ, dân số, chế độ chính trị - xã hội, đều có chủ quyền.

* Viện trưởng Viện Chiến lược quốc phòng, Bộ Quốc phòng.

Đối với nước ta, Đảng và Nhà nước Việt Nam đã có nhiều văn bản đề cập vấn đề bảo đảm chủ quyền, an ninh quốc gia trên cơ sở nội dung về các nguy cơ, biện pháp bảo đảm an toàn, an ninh, bảo vệ bí mật quốc gia trong không gian mạng như: Nghị quyết số 29-NQ/TW, ngày 25/7/2018 của Bộ Chính trị khóa XII 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 khóa XII về *Chiến lược an ninh mạng quốc gia*; Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII của Đảng; Luật an toàn thông tin mạng năm 2015; Luật an ninh mạng năm 2018 và Luật quốc phòng năm 2018 đã từng bước thể chế hóa các chủ trương, đường lối, chính sách của Đảng và Nhà nước về an toàn thông tin, đáp ứng yêu cầu phát triển bền vững kinh tế - xã hội, bảo vệ thông tin và hệ thống thông tin, góp phần bảo đảm quốc phòng, an ninh, chủ quyền và lợi ích quốc gia - dân tộc trên không gian mạng. Các nghị quyết, chỉ thị của Đảng và các văn bản quy phạm pháp luật của Nhà nước đều thống nhất quan điểm chỉ đạo về bảo đảm an toàn, an ninh thông tin và bảo vệ chủ quyền quốc gia trên không gian mạng. Khẳng định chủ quyền quốc gia trên không gian mạng là tất cả các quyền của Nhà nước đối với không gian mạng theo quy định của pháp luật Việt Nam, phù hợp với quy định của luật pháp quốc tế. Chủ quyền trên không gian mạng là bộ phận quan trọng của chủ quyền quốc gia; việc bảo vệ chủ quyền quốc gia trên không gian mạng là nhiệm vụ cấp bách, lâu dài của cả hệ thống chính trị, đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý thống nhất của Nhà nước.

Những năm qua, ở cấp độ toàn cầu, nước ta đã chủ động tham gia vào các quá trình thảo luận về vấn đề không gian

mạng và an ninh mạng, trong đó có nội dung chủ quyền không gian mạng, tại các diễn đàn đa phương quốc tế, nhất là tại Liên hợp quốc. Chủ động tham gia trao đổi, thảo luận tại các diễn đàn ở kênh học giả quốc tế về vấn đề này, tranh thủ chia sẻ quan điểm của Việt Nam về bảo vệ chủ quyền, lợi ích quốc gia - dân tộc trên không gian mạng. Ở cấp độ khu vực, nước ta đã từng bước lồng ghép ở mức độ phù hợp về vấn đề chủ quyền không gian mạng vào vấn đề an ninh mạng, không gian mạng của các cơ chế hợp tác khu vực, nhất là ASEAN, thông qua các hoạt động thực tế, như tăng cường hợp tác, diễn tập quốc tế về phòng, chống tấn công mạng, cũng như điều tra, truy tìm nguồn gốc tấn công mạng. Tranh thủ nguồn lực từ các cơ chế hợp tác khu vực mà Việt Nam tham gia để thúc đẩy việc đào tạo, nâng cao trình độ đối với nguồn nhân lực liên quan đến hoạt động ngoại giao, đối ngoại quốc phòng về không gian mạng, an ninh mạng và kinh nghiệm bảo vệ chủ quyền, an ninh quốc gia trên không gian mạng. Chủ động tham gia thúc đẩy nội dung chủ quyền không gian mạng trong các mạng lưới nghiên cứu có uy tín của ASEAN...

Mặc dù đã tích cực, chủ động triển khai hợp tác quốc tế bảo vệ chủ quyền quốc gia trên không gian mạng, nhưng thực trạng an toàn thông tin, an ninh mạng ở nước ta vẫn đang diễn biến khá phức tạp và nguy hiểm. Vì vậy, trong thời gian tới, tăng cường hợp tác quốc tế bảo vệ chủ quyền quốc gia trên không gian mạng cần tập trung vào những vấn đề chủ yếu sau:

Một là, nâng cao nhận thức, năng lực, bổ sung, hoàn thiện hệ thống pháp luật, cơ chế, chính sách về hợp tác quốc tế trong bảo vệ chủ quyền quốc gia trên không gian mạng.

Đây là giải pháp quan trọng hàng đầu, bởi vì, không gian mạng, bảo vệ chủ quyền quốc gia trên không gian mạng là lĩnh vực mới, phức tạp, nhạy cảm cần phải nhận thức thống nhất, có cơ chế, chính sách đầy đủ để triển khai thực hiện. Các vấn đề: công nghệ thông tin, an ninh mạng và phòng, chống chiến tranh không gian mạng là những vấn đề cốt yếu, trong đó an ninh mạng mang tính toàn cầu, tác động sâu sắc tới tình hình an ninh, hòa bình của thế giới và khu vực, đe dọa đến chủ quyền không gian mạng; trong khi hiện nay các nước có xu hướng quan tâm hợp tác, tăng cường đoàn kết để ngăn ngừa, phòng, chống các mối nguy hại từ an ninh mạng, cùng nhau duy trì hòa bình, ổn định, bảo đảm chủ quyền, lợi ích quốc gia - dân tộc của mỗi nước trên không gian mạng. Do đó, nâng cao nhận thức và năng lực hợp tác quốc tế về an ninh mạng sẽ huy động được các nguồn lực từ bên ngoài, tranh thủ sự giúp đỡ về khoa học công nghệ, nguồn lực của các đối tác cho xây dựng không gian mạng quốc gia an toàn, lành mạnh, rộng khắp để bảo vệ Tổ quốc trên không gian mạng.

Xuất phát từ nhận thức an ninh mạng là bộ phận cấu thành của an ninh quốc gia, là nội dung chủ yếu để bảo vệ chủ quyền quốc gia trên không gian mạng; bảo đảm an toàn, an ninh mạng là một trong những động lực quan trọng phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh, nâng cao vị thế đất nước trong quá trình hội nhập, do đó, cần chú trọng hợp tác quốc tế, phát triển khoa học công nghệ, năng lực kỹ thuật, biện pháp bảo vệ tương xứng để hướng đến làm chủ các phần cứng, phần mềm ứng dụng; từng bước hình thành không gian mạng sạch, tạo điều kiện an toàn cho việc lưu trữ cơ sở dữ liệu;

hợp tác trong đầu tư nghiên cứu, ứng dụng công nghệ, mã hóa thông tin đối với hệ thống thông tin quan trọng về an ninh quốc gia bảo đảm an ninh mạng, phòng, chống các vi phạm và tội phạm mạng. Với đặc tính không biên giới, không gian mạng có phạm vi toàn cầu và ảnh hưởng đến toàn thế giới, vì vậy hợp tác bảo đảm an ninh mạng phải tiến hành chặt chẽ giữa các nước, trực tiếp là lực lượng chuyên trách bảo vệ an ninh mạng. Chủ động mở rộng quan hệ và tăng cường hợp tác quốc tế về phòng, chống tội phạm, nhất là đối với các nước có trình độ cao và phát triển ứng dụng công nghệ thông tin trong phòng, chống tội phạm mạng, nâng cao năng lực thu thập, khai thác, trao đổi, xử lý thông tin về phòng ngừa, đấu tranh với các loại tội phạm mạng, xây dựng không gian mạng an toàn tiến đến thúc đẩy các dịch vụ trực tuyến chính phủ điện tử, chính phủ thông minh, thương mại điện tử.

Nâng cao nhận thức và năng lực hợp tác quốc tế trong lĩnh vực công nghệ thông tin, an ninh mạng và phòng, chống chiến tranh không gian mạng cần quán triệt, nắm vững các quan điểm chỉ đạo của Đảng, Nhà nước 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, chính sách đối ngoại của Việt Nam trên không gian mạng. Đẩy mạnh hoạt động tuyên truyền, giáo dục pháp luật Việt Nam và luật pháp quốc tế về phát triển công nghệ thông tin và an toàn, an ninh thông tin; nâng cao nhận thức đối với hệ thống chính trị và toàn thể nhân dân, đặc biệt là các lực lượng làm công tác đối ngoại, lực lượng nòng cốt bảo vệ chủ quyền quốc gia trên không gian mạng.

Hệ thống pháp luật, cơ chế, chính sách về hợp tác quốc tế trong bảo đảm an toàn, an ninh mạng và phòng, chống chiến tranh thông tin, không gian mạng là hành lang pháp lý để triển khai hợp tác quốc tế bảo vệ chủ quyền quốc gia trên không gian mạng hiệu quả. Hiện nay, tuy đã được thể hiện khá đầy đủ để các ban, bộ, ngành, địa phương triển khai các hoạt động hợp tác, song an ninh mạng liên quan đến nhiều quốc gia, vì vậy cần phải tiếp tục bổ sung hoàn thiện hệ thống pháp luật, cơ chế, chính sách dựa trên luật pháp, thông lệ quốc tế, phù hợp với điều kiện đặc thù của Việt Nam, bảo đảm hoạt động hợp tác quốc tế hiệu quả. Theo đó, cần tiếp tục xây dựng hoàn thiện các văn bản quản lý chặt chẽ các mạng internet, viễn thông, truyền hình và các dịch vụ, thông tin điện tử, mạng xã hội trên internet phù hợp với điều kiện thực tế Việt Nam và xu thế quốc tế. Quản lý các doanh nghiệp nước ngoài khi cung cấp dịch vụ, nội dung thông tin trên không gian mạng phải tuân thủ pháp luật, lợi ích, chủ quyền quốc gia của Việt Nam, quyền lợi hợp pháp của tổ chức, cá nhân đang hoạt động trên lãnh thổ Việt Nam và phù hợp với thông lệ quốc tế, cam kết quốc tế và chiều hướng hội nhập của nước ta. Hoàn thiện luật pháp, chính sách về đầu tư trực tiếp nước ngoài theo hướng nâng cao tiêu chuẩn công nghệ, khuyến khích hình thức liên doanh và tăng cường liên kết, chuyển giao công nghệ giữa doanh nghiệp trong nước với các doanh nghiệp đầu tư trực tiếp nước ngoài; quản lý chặt chẽ hoạt động của các doanh nghiệp dựa trên nền tảng cung cấp dịch vụ xuyên quốc gia để bảo đảm môi trường kinh doanh bình đẳng.

Hai là, đẩy mạnh các hoạt động hợp tác, chia sẻ kinh nghiệm với chính phủ các nước và các tổ chức quốc tế.

Tăng cường hợp tác, chia sẻ kinh nghiệm trong xây dựng chính sách, thể chế quản lý và thúc đẩy ứng dụng, phát triển công nghệ thông tin và an toàn, an ninh thông tin, phòng, chống chiến tranh thông tin và không gian mạng là nội dung quan trọng để tăng cường hợp tác quốc tế bảo vệ chủ quyền quốc gia trên không gian mạng. Trong đó, cần chủ động tham gia các công ước, thỏa thuận quốc tế về bảo vệ không gian mạng, phòng, chống tội phạm mạng, phòng, chống chiến tranh không gian mạng phù hợp với chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước và triển khai có hiệu quả, thiết thực các nghị định thư, thỏa thuận hợp tác về phòng, chống tội phạm mạng đã ký kết với các nước.

Tiếp tục phối hợp với Cơ quan phòng, chống ma túy và tội phạm của Liên hợp quốc (UNODC) để thúc đẩy xây dựng một công ước trong khuôn khổ Liên hợp quốc về tội phạm mạng phù hợp với điều kiện, khả năng và bảo đảm chủ quyền, lợi ích quốc gia của Việt Nam trên không gian mạng. Chủ động hợp tác, xây dựng Bộ quy tắc ứng xử trên không gian mạng song phương và đa phương nhằm xây dựng một không gian mạng an toàn, lành mạnh trên phạm vi toàn cầu, tiến tới xây dựng luật quốc tế về không gian mạng. Trong khu vực ASEAN, chúng ta cần tham gia xây dựng một bộ quy tắc chung, chủ động và mở về hành vi quốc gia trên không gian mạng để thúc đẩy sự tin cậy và lòng tin về việc sử dụng không gian mạng cho lợi ích toàn diện là sự thịnh vượng và hội nhập kinh tế trong khu vực; tiến tới xây dựng một không gian mạng hòa bình, an toàn

và tự cường đáp ứng sự phát triển kinh tế, tăng cường kết nối khu vực và cải thiện các điều kiện sống tốt hơn cho tất cả các nước thành viên; tiếp tục tham gia thảo luận và xây dựng chính sách an ninh mạng, ngoại giao, hợp tác tại các diễn đàn của khu vực như Hội nghị thượng đỉnh ASEAN; Hội nghị Bộ trưởng Ngoại giao ASEAN; Hội nghị Bộ trưởng Quốc phòng ASEAN; Hội nghị Bộ trưởng về an ninh mạng.

Tăng cường công tác đối ngoại, tranh thủ sự ủng hộ của các nước, các tổ chức, tập đoàn công nghệ thông tin quốc tế nhằm tạo các điều kiện có lợi cho Việt Nam tham gia vào các hiệp ước thương mại quốc tế. Nâng cao hiệu quả đối ngoại quốc phòng và hợp tác quốc tế về công nghệ thông tin và an ninh mạng, phòng, chống chiến tranh, bảo vệ chủ quyền quốc gia trên không gian mạng nhằm tạo môi trường hòa bình trong giải quyết các vấn đề về an ninh mạng, chiến tranh không gian mạng. Tiếp cận các công nghệ, kỹ thuật mới trên không gian mạng, chủ động, tích cực tham gia nghiên cứu, xây dựng các công ước, thỏa thuận quốc tế về không gian mạng và bảo vệ chủ quyền, lợi ích quốc gia trên không gian mạng phù hợp với đường lối, chủ trương, chính sách của Đảng, Nhà nước. Thúc đẩy nghiên cứu, đàm phán gia nhập các điều ước quốc tế, thỏa thuận quốc tế; tích cực tham gia các cuộc diễn tập quốc tế về bảo đảm an toàn thông tin, an ninh mạng, phòng, chống chiến tranh không gian mạng và bảo vệ chủ quyền quốc gia trên không gian mạng. Tranh thủ sự giúp đỡ của các nước và tập đoàn công nghệ lớn trên thế giới; thu hút đầu tư, tài trợ quốc tế trong việc xây dựng không gian mạng an toàn, lành mạnh, rộng khắp và bảo vệ chủ quyền, lợi ích quốc gia trên không gian mạng.

Ba là, đẩy mạnh hợp tác quốc tế trong giáo dục và đào tạo, nghiên cứu và phát triển về công nghệ thông tin; an ninh, an toàn mạng.

Đẩy mạnh hợp tác quốc tế trong giáo dục, đào tạo và phát triển nguồn lực vừa là nội dung, vừa là giải pháp để tăng cường hợp tác quốc tế bảo vệ chủ quyền quốc gia trên không gian mạng. Tích cực hợp tác quốc tế về giáo dục, đào tạo để tranh thủ sự giúp đỡ của các nước trong việc xây dựng, phát triển nguồn nhân lực chất lượng cao, hình thành đội ngũ chuyên gia đầu ngành, chuyên môn sâu, ngang tầm với các nước trong khu vực và trên thế giới về công nghệ thông tin, an toàn, an ninh mạng và tác chiến không gian mạng. Đẩy mạnh thu hút và sử dụng hiệu quả các nguồn lực từ nước ngoài và các đối tác quốc tế cho hoạt động nghiên cứu, ứng dụng, đổi mới sáng tạo, khởi nghiệp sáng tạo, chuyển giao công nghệ về không gian mạng.

Coi trọng công tác hợp tác quốc tế về đào tạo, bồi dưỡng nguồn nhân lực chất lượng cao trong lĩnh vực công nghệ thông tin, hợp tác chặt chẽ với các nước và tổ chức cảnh sát quốc tế để tạo nguồn nhân lực phòng, chống kịp thời, hiệu quả tội phạm mạng, đội ngũ chuyên gia về công nghệ thông tin, nhất là chuyên gia phần mềm, quản trị mạng cao cấp; kết hợp giữa đào tạo trong nước và quốc tế bằng cả nguồn ngân sách nhà nước, tập thể, cá nhân và các chương trình tài trợ của nước ngoài, gắn đào tạo với sử dụng tạo ra môi trường hấp dẫn thu hút tài năng công nghệ thông tin phục vụ đất nước.

Mở rộng và làm sâu sắc hơn hợp tác về khoa học công nghệ với các đối tác, đặc biệt là đối tác chiến lược có trình độ khoa học công nghệ tiên tiến, đi đầu trong Cách mạng công

nghiệp lần thứ tư. Đẩy mạnh hợp tác, học tập kinh nghiệm quốc tế và tranh thủ sự giúp đỡ của các nước, các tổ chức quốc tế và các tập đoàn công nghệ lớn trên thế giới để xây dựng không gian mạng an toàn, lành mạnh, rộng khắp và xây dựng tiềm lực bảo vệ Tổ quốc trong tình hình mới. Tăng cường hợp tác, chia sẻ thông tin, xây dựng chính sách và tổ chức đào tạo, huấn luyện nguồn nhân lực; nghiên cứu phát triển và chuyển giao khoa học công nghệ về tác chiến không gian mạng và công nghệ thông tin, an ninh mạng.

Bốn là, tăng cường hợp tác quốc tế phối hợp xử lý an ninh mạng, tội phạm mạng, phòng, chống chiến tranh không gian mạng, nhất là xử lý hoạt động tiến công mạng.

Đây là giải pháp không thể thiếu trong hợp tác quốc tế, phù hợp với đặc thù hợp tác về an ninh mạng, phòng, chống tội phạm mạng và chiến tranh mạng. Sự phát triển mạnh mẽ của công nghệ thông tin, điện tử, viễn thông trong môi trường không gian mạng đã xuất hiện nhiều vấn đề phức tạp trong bảo vệ chủ quyền quốc gia trên không gian mạng. Đặc biệt, đối với lĩnh vực quốc phòng, an ninh sẽ phải đối phó với các mức độ nguy hiểm như: các tổ chức, cá nhân sử dụng không gian mạng tiến hành các hoạt động tiến công mạng, gián điệp mạng, khủng bố mạng và tội phạm phá hoại về kinh tế, chính trị, văn hóa, xã hội, quốc phòng, an ninh, đối ngoại gây mất an ninh quốc gia; các thế lực thù địch, tổ chức phản động lợi dụng không gian mạng để đánh cắp thông tin, bí mật nhà nước, bí mật quân sự, gây sự cố làm gián đoạn hệ thống thông tin, đe dọa an ninh, đe dọa chủ quyền quốc gia trên không gian mạng; lợi dụng không gian mạng để tiến hành các hoạt động “diễn biến hòa bình”,

kích động gây rối an ninh, chính trị, trật tự, an toàn xã hội nhằm xóa bỏ vai trò lãnh đạo của Đảng Cộng sản, chế độ xã hội chủ nghĩa ở nước ta; tiến hành chiến tranh không gian mạng, sử dụng các thủ đoạn để phá vỡ các hạ tầng quốc gia, gây rối loạn, làm tê liệt hệ thống lãnh đạo của Đảng, quản lý, điều hành của Nhà nước về lĩnh vực quốc phòng, quân sự, tiến công phá hủy tiềm lực quốc phòng gây hoang mang tinh thần của lực lượng vũ trang và nhân dân, làm mất khả năng kiểm soát không gian mạng, làm suy yếu khả năng của ta để tạo điều kiện tiến công xâm lược. Mức độ nguy hiểm cao nhất xảy ra khi các thế lực thù địch tiến hành chiến tranh không gian mạng kết hợp với các hình thái chiến tranh khác.

Đẩy mạnh hợp tác, chia sẻ nhận thức, kinh nghiệm giữa các quốc gia nhằm đạt được sự đồng thuận trong nhận thức, thống nhất trong xử lý các vấn đề trên không gian mạng. Các nước cần cử cơ quan đầu mối để thiết lập kênh liên lạc trao đổi thông tin bảo đảm kịp thời, phối hợp xử lý các vấn đề trên không gian mạng. Tăng cường phối hợp với các quốc gia, tổ chức quốc tế thông qua các công ty cung cấp dịch vụ trên internet xuyên biên giới để phối hợp xử lý, ngăn chặn các hoạt động sử dụng không gian mạng vi phạm pháp luật Việt Nam, đặc biệt là các hoạt động cung cấp thông tin giả mạo, sai sự thật để chống phá Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, biểu tình, phá rối an ninh, gây rối trật tự công cộng; xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân của Việt Nam. Thường xuyên phối hợp tiến hành các cuộc diễn tập song phương và đa phương về an ninh

mạng nhằm tăng cường hiểu biết lẫn nhau giữa các quốc gia trong bảo vệ an ninh mạng. Chủ động mở rộng quan hệ hợp tác sâu rộng với lực lượng tác chiến không gian mạng của quân đội các nước có quan hệ tốt đẹp với Việt Nam, đặc biệt là các quốc gia có quan hệ đối tác chiến lược toàn diện nhằm trao đổi thông tin, nghiên cứu khoa học, đào tạo nguồn nhân lực và mua sắm vũ khí. Quan hệ hợp tác quốc tế theo đúng đường lối, quan điểm của Đảng, sự chỉ đạo của Bộ Quốc phòng và các bộ liên quan.

Chủ quyền trên không gian mạng - bộ phận quan trọng của chủ quyền quốc gia, bảo vệ chủ quyền quốc gia trên không gian mạng là một tất yếu khách quan. Trong bối cảnh hội nhập quốc tế ngày càng sâu rộng và toàn diện, để bảo vệ chủ quyền quốc gia trên không gian mạng cần phải giải quyết nhiều vấn đề, trong đó hợp tác quốc tế là vấn đề quan trọng, có tính cấp thiết. Hợp tác quốc tế bảo vệ chủ quyền quốc gia trên không gian mạng đặt dưới sự lãnh đạo của Đảng, quản lý của Nhà nước; lực lượng Quân đội nhân dân, Công an nhân dân, lực lượng Cơ yếu, Thông tin và Truyền thông, Đối ngoại làm nòng cốt nhằm thực hiện có hiệu quả chủ trương, đường lối, chính sách của Đảng và Nhà nước về an toàn thông tin, đáp ứng yêu cầu phát triển bền vững kinh tế - xã hội, bảo vệ thông tin và hệ thống thông tin, góp phần bảo đảm quốc phòng, an ninh, chủ quyền và lợi ích quốc gia - dân tộc trên không gian mạng; bảo vệ chủ quyền thiêng liêng của Tổ quốc, bao gồm chủ quyền không gian mạng, an ninh của quốc gia trong tình hình mới. Tuy nhiên, những vấn đề nêu trên cần được tiếp tục cập nhật, bổ sung phù hợp với sự phát triển mới của tình hình.

TÍNH NHÂN BẢN TỰ NHIÊN - PHƯƠNG PHÁP TIẾP CẬN GIÁ TRỊ CHUNG CỦA QUYỀN CON NGƯỜI VÀ CHỦ QUYỀN QUỐC GIA TRONG TƯ TƯỞNG HỒ CHÍ MINH

TS. VÕ VĂN BÉ*

ThS. PHAN DUY ANH**

Nhân quyền và chủ quyền quốc gia luôn là vấn đề quan trọng của các quốc gia trên thế giới trong lịch sử cận, hiện đại và Việt Nam cũng không ngoại lệ. Quan niệm về quyền con người, giải quyết các vấn đề nhân quyền nói chung, mối quan hệ giữa quyền con người và chủ quyền quốc gia nói riêng ở Việt Nam được soi sáng bởi các nguyên lý cơ bản của chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh. Từ truyền thống dân tộc, đặc điểm thời đại, con người hiện thực, Hồ Chí Minh là một trong những người Việt Nam đầu tiên đề cập khái niệm “nhân quyền” và dùng quan niệm nhân quyền trong các lập luận đấu tranh chống chủ nghĩa thực dân, giành lại chủ quyền cho quốc gia - dân tộc. Đặc biệt, với Hồ Chí Minh, phương pháp tiếp cận quyền con người và

* Nhà xuất bản Chính trị quốc gia Sự thật.

** Trường Đại học Bách khoa, Đại học Quốc gia Thành phố Hồ Chí Minh.

chủ quyền quốc gia là từ giá trị nhân bản tự nhiên: dù là nhân quyền hay chủ quyền quốc gia thì đều xoay quanh vấn đề con người, và không có con người chung chung, trừu tượng mà chỉ có những con người hiện thực; dù bảo đảm và thực thi quyền con người hay chủ quyền quốc gia thì cũng luôn hướng đến giải phóng con người, nâng con người thành CON NGƯỜI với những giá trị nhân bản đúng nghĩa.

1. Độc lập và tự do - giá trị khẳng định quyền tự nhiên của con người và quyền tự quyết của các quốc gia - dân tộc

Độc lập, tự do là quyền cơ bản nhất của mọi quốc gia - dân tộc. Mọi người sinh ra đều có quyền tự do và các dân tộc phải được bình đẳng. Mất độc lập, tự do là điều không thể chấp nhận được đối với mọi dân tộc. Mất tự do, con người sẽ trở thành nô lệ, thành “động vật biết nói”, tự do là giá trị nhân bản của con người. Song, với “quyền của kẻ mạnh”, thực dân Pháp đã tước đi độc lập, tự do của dân tộc Việt Nam. Dưới chế độ thực dân, “đối với người An Nam, ca tụng tự do là một tội nặng”¹. Điều đó hoàn toàn trái ngược với *Tuyên ngôn nhân quyền và dân quyền* của cuộc đại cách mạng tư sản Pháp mà nước Pháp luôn ca ngợi và truyền bá. Khẳng định tự do là quyền tự nhiên của con người, nhưng ở Đông Dương, chính thực dân Pháp lại tước đi bản chất tự nhiên đó của người dân thuộc địa. Chính sách của thực dân Pháp đối với nhân dân Việt Nam thực sự là sự áp bức về mặt

1. Hồ Chí Minh: *Toàn tập*, Nxb. Chính trị quốc gia, Hà Nội, 2011, t.2, tr.101.

con người. Dưới ngòi bút của Nguyễn Ái Quốc - Hồ Chí Minh, qua *Bản án chế độ thực dân Pháp* và nhiều tác phẩm khác, đã hiện lên bức tranh tương phản giữa một bên là quyền con người và những giá trị mang bản chất người của người dân bản xứ - “những giá trị có ý nghĩa nâng xã hội của họ lên trình độ xã hội loài người, làm cho sự tồn tại của họ là tồn tại người”¹ với một bên là hiện thực do chế độ thực dân tạo ra - một hiện thực kéo con người về với xã hội loài vật, với tồn tại vật. Đó là bức tranh tương phản giữa “nhân tính” và “thú tính”.

Nhưng con người là gì? Theo Hồ Chí Minh: “Chữ người, nghĩa hẹp là gia đình, anh em, họ hàng, bầu bạn. Nghĩa rộng là đồng bào cả nước. Rộng nữa là cả loài người”². Theo cách hiểu này, con người có tính xã hội, là con người xã hội, là thành viên của một cộng đồng xã hội nhất định. Hồ Chí Minh xác định cụ thể, cộng đồng đó là gia đình, họ tộc, làng xóm, dân tộc, đất nước cho đến cả nhân loại. Với Hồ Chí Minh, con người không phải là những cá thể biệt lập. Chỉ có trong quan hệ xã hội, trong hoạt động thực tiễn xã hội, con người mới có lao động, ngôn ngữ, tư duy,... mới thực sự trở thành con người để phân biệt với mọi loài động vật khác. Những quan hệ xã hội mà Hồ Chí Minh quan tâm trước hết là những quan hệ gắn bó con người với cộng đồng, tạo thành các cộng đồng từ nhỏ đến lớn, từ hẹp đến rộng. Chính từ cách định nghĩa con người này, Hồ Chí Minh đã đi từ cách tiếp cận

1. Lại Quốc Khánh: *Biện chứng của tư tưởng Hồ Chí Minh về chủ nghĩa xã hội ở Việt Nam*, Nxb. Chính trị quốc gia, Hà Nội, 2009, tr.150.

2. Hồ Chí Minh: *Toàn tập, Sdd*, t.6, tr.130.

quyền tự nhiên của con người đến quyền tự quyết của các dân tộc. Trong *Tuyên ngôn độc lập*, sau khi khẳng định những quyền tự nhiên của con người đã được nêu rõ trong *Tuyên ngôn độc lập* của Mỹ và *Tuyên ngôn nhân quyền và dân quyền* của Pháp, Người đã nêu bật chân lý: “Tất cả các dân tộc trên thế giới đều sinh ra bình đẳng, dân tộc nào cũng có quyền sống, quyền sung sướng và quyền tự do”¹. Từ quyền tự nhiên của con người phát triển lên thành quyền đấu tranh chống áp bức của các dân tộc thuộc địa, quyền làm người và quyền tự quyết của các dân tộc nô lệ, bị áp bức, Người đã khẳng định một triết lý chính trị sâu sắc: “Tự do độc lập là quyền trời cho của mỗi dân tộc”² và “*Không có gì quý hơn độc lập, tự do*”³. Với Hồ Chí Minh, đấu tranh cho độc lập và tự do là “lý tưởng cao quý nhất của loài người”⁴. Ngay sau khi đất nước giành được độc lập, thay mặt Chính phủ và nhân dân Việt Nam, Người đã gửi đến toàn thế giới một thông điệp: “Chúng tôi muốn gửi thế giới lời này: là ước mong tất cả các người dân chủ trên thế giới đoàn kết với nhau để bảo vệ cho nền dân chủ trong các nước nhỏ cũng như trong các nước lớn. Mong các người làm cho quyền tự quyết của các dân tộc là quyền do các Hiến chương Đại Tây Dương và Cựu Kim Sơn bảo đảm, được tôn trọng”⁵. Đó là một thông điệp thể hiện sâu sắc chân lý của thời đại và nguyện vọng của các quốc gia - dân tộc bị áp bức, các lực lượng tiến bộ trên thế giới.

1, 4. Hồ Chí Minh: *Toàn tập, Sđd*, t.4, tr.1, 75.

2, 5. Hồ Chí Minh: *Toàn tập, Sđd*, t.5, tr.9, 164.

3. Hồ Chí Minh: *Toàn tập, Sđd*, t.15, tr.131.

Có thể thấy, từ quyền tự nhiên của con người, Hồ Chí Minh đã chuyển thành quyền làm người của các dân tộc nô lệ, bị áp bức, đó là quyền được sống trong độc lập, tự do. Độc lập, tự do là những giá trị, là quyền được hưởng của con người, đồng thời cũng là quyền của các quốc gia - dân tộc.

2. Công lý và hòa bình - giá trị bảo đảm môi trường tồn tại của con người và chủ quyền quốc gia - dân tộc

Từ thuở bình minh của văn minh nhân loại, công lý đã xuất hiện như một khát vọng cháy bỏng về tự do, công bằng, chính nghĩa, lẽ phải, lòng nhân ái và những phẩm hạnh cao quý trong mỗi con người, mỗi xã hội. Bộ luật Hammurabi, bộ luật thành văn cổ xưa nhất của loài người (ra đời khoảng từ năm 1792 - 1750 Tr.CN) đã coi công lý và chính nghĩa là cơ sở của nền cai trị nhân từ, công bằng nhằm đem lại sự thái bình và hạnh phúc chân chính cho người dân. Thần thoại Hy Lạp (ra đời khoảng từ năm 2000 - 1100 Tr.CN) đã khắc họa hình ảnh nữ thần công lý Thémis một tay cầm cân, một tay cầm thanh kiếm, mắt bịt một băng vải để chứng tỏ sự vô tư, không thiên vị, đem lại sự ổn định và phát triển hài hòa của thế gian. Trong Sáng thế ký của Kinh Thánh (khoảng từ năm 1400-400 Tr.CN), câu chuyện Vườn địa đàng không chỉ thuần túy là câu chuyện tôn giáo, mà còn là sự khởi đầu cho một tư duy pháp lý mang tính chất tiên nghiệm có ý nghĩa khoa học và nhân văn sâu sắc. Đó chính là nguyên tắc, là nghĩa vụ phải hành động một cách công bằng, công chính, dù người đó là ai, từ Thiên chúa hay là mỗi con người bình thường trong xã hội. Có thể thấy, xuyên suốt trong tư duy nhân loại, công lý là yếu tố định

hình môi trường cho con người và quốc gia - dân tộc tồn tại và phát triển.

Trong mọi thời đại, bất kỳ ở đâu, con người đều đấu tranh cho một môi trường công lý và hòa bình thực sự. Nhưng vào những năm cuối thế kỷ XIX, đầu thế kỷ XX, thực dân Pháp với cái gọi là “khai hóa văn minh” đã thiết lập nên ở Việt Nam một nền công lý: “người Âu nào đã giết chết, tàn sát hoặc cưỡng dâm người bản xứ, thì trong trường hợp vụ án không thể im hoàn toàn, anh ta chắc chắn rằng mình được toà án tha bổng, mình ra tòa chẳng qua là chuyện hình thức. Đó là việc áp dụng nguyên tắc nhằm bảo tồn bằng mọi cách uy tín của người da trắng trước bọn da vàng”¹. Được “hưởng thụ” nền “công lý” đó, Nguyễn Ái Quốc đã nhận định rằng: “Ấy là công lý bị bán đứt cho kẻ nào mua đắt nhất, trả giá hời nhất”². Hồ Chí Minh mỉa mai nền công lý thuộc địa qua hình ảnh của nữ thần công lý Thesmis: “Công lý được tượng trưng qua hình ảnh một nữ thần tay cầm cân và tay cầm kiếm. Nhưng Đông Dương lại ở quá xa nước Pháp, muôn trùng cách trở nên khi nữ thần tới xứ này thì cán cân đã mất thăng bằng, đĩa cân đã chảy lỏng và biến thành những tẩu thuốc phiện và những chai rượu ty. Trên tay nữ thần ấy chỉ còn độc một cái kiếm để chém giết. Bà đã chém những người vô tội và cũng chỉ chém có họ mà thôi”³.

Tình yêu và khát vọng về một nền công lý chân chính xuất hiện ở Hồ Chí Minh từ rất sớm. Khi khảo cứu hệ thống các tác phẩm của Hồ Chí Minh có thể thấy khái niệm “công lý” xuất hiện ngay từ bài chính luận đầu tiên -

1, 2, 3. Hồ Chí Minh: *Toàn tập, Sđd*, t.1, tr.11-12, 12, 51, XXIII.

Tâm địa thực dân và còn xuất hiện trước cả khái niệm “độc lập”. Nhưng ở Hồ Chí Minh, công lý là một giá trị tự nhiên định hình môi trường sống của con người. Nếu không có công lý thì con người cũng không thể có một môi trường cân bằng để tồn tại.

Hồ Chí Minh cho rằng, công lý là mẫu mực của cuộc sống, là mục đích của cuộc sống, là tiên thiên của pháp luật, nó giúp cho pháp luật giữ gìn sự thanh bình của cuộc sống, nó bảo đảm sự ổn định và phát triển của xã hội. Công lý như là cái thế thăng bằng, nếu thái quá nó sẽ là bất công, thiếu sót nó sẽ làm tổn hại xã hội, công lý là sự bình đẳng, nó có khoảng cách như nhau giữa lợi ích và sự mất mát, thua thiệt trong quan hệ xã hội. Cho nên công lý “làm thần” đứng “ở giữa” là vì vậy. Điều này cũng khẳng định, với Hồ Chí Minh, một nền chính trị đích thực thì trước hết phải có “công lý đứng làm thần”.

Hồ Chí Minh gắn liền công lý với hòa bình. Người luôn thể hiện rõ quan điểm “công bình và lý tưởng dân chủ phải thay cho chiến tranh”¹. Trong tuyên bố với phóng viên báo Paris - Saigon, Hồ Chí Minh đã khẳng định: “Đồng bào tôi và tôi thực sự muốn hòa bình. Tôi biết nhân dân Pháp không muốn chiến tranh. Cuộc chiến tranh này chúng tôi muốn tránh bằng đủ mọi cách... Việt Nam không muốn là nơi chôn vùi hàng bao nhiêu sinh mạng... Cả nước Pháp lẫn nước Việt Nam đều không thể phí sức gây một cuộc chiến tranh khốc hại...”². Trong *Thư gửi đồng bào Việt Nam, nhân dân Pháp*

1. Hồ Chí Minh: *Toàn tập, Sđd*, t.1, tr.XXIII.

2. Hồ Chí Minh: *Toàn tập, Sđd*, t.4, tr.526.

và *thế giới* nhằm kêu gọi hòa bình, Hồ Chí Minh viết: “Than ôi, trước lòng bác ái, thì máu Pháp hay máu Việt cũng đều là máu, người Pháp hay người Việt cũng đều là người”¹. Trong cuộc kháng chiến chống Mỹ, cứu nước, Người chia sẻ nỗi đau của các gia đình Mỹ có người thân mất ở Việt Nam: “Chính phủ Mỹ đã buộc hàng chục vạn thanh niên Mỹ phải chết và bị thương vô ích trên chiến trường Việt Nam... chúng tôi muốn sống hòa bình hữu nghị với tất cả các dân tộc trên thế giới, cả với nhân dân Mỹ”². Trong chính sách đối ngoại của nước Việt Nam mới, Hồ Chí Minh luôn nêu rõ: “Đối với các nước trên thế giới, nước Việt Nam Dân chủ Cộng hòa thiết tha mong muốn duy trì tình hữu nghị và thành thật hợp tác trên cơ sở bình đẳng và tương trợ để xây dựng hòa bình thế giới lâu dài”³.

Trong suốt quá trình đấu tranh cách mạng, Hồ Chí Minh luôn gửi thông điệp hòa bình đến toàn thế giới qua con đường thuyết phục và thương lượng. “Đó là một thông điệp về sự hy vọng và quyết tâm cho nhân dân Việt Nam hướng tới ngày thống nhất và độc lập hoàn toàn. Đồng thời, đó cũng là thông điệp về công lý và nhân văn cho các dân tộc yêu chuộng hòa bình trên khắp thế giới để ủng hộ những người kém may mắn hơn. Và đó cũng là một thông điệp cho các thế lực có âm mưu cần suy nghĩ lại về các hậu quả lâu dài từ hành động của mình”⁴. Thông điệp hòa bình của Hồ Chí Minh được xây

1. Hồ Chí Minh: *Toàn tập, Sđd*, t.4, tr.510.

2. Hồ Chí Minh: *Toàn tập, Sđd*, t.15, tr.414-415.

3. Hồ Chí Minh: *Toàn tập, Sđd*, t.11, tr.269.

4. Nguyễn Đài Trang: *Hồ Chí Minh - Nhân văn và phát triển*, Nxb. Chính trị quốc gia, Hà Nội, 2013, tr.142.

dựng trên một triết lý sâu sắc: “Bảo vệ hòa bình tức là chống chiến tranh”¹. Đặc biệt với Người, “hòa bình thật sự không thể tách khỏi độc lập thật sự”².

3. Dân chủ và hạnh phúc - giá trị bảo đảm cho con người và quốc gia - dân tộc phát triển

Năm 1911, khi Việt Nam đã hoàn toàn trở thành thuộc địa của thực dân Pháp, Nguyễn Ái Quốc không hoàn toàn tán thành con đường cứu nước của các bậc tiền bối, quyết tâm đi sang phương Tây tìm con đường cứu nước mới. Suy nghĩ và mong muốn lớn nhất của Người lúc đó là giải phóng đồng bào, tức là lật đổ, xóa bỏ ách áp bức, bóc lột của thực dân, phong kiến, giành độc lập dân tộc. Nhưng Hồ Chí Minh không bao giờ chấp nhận độc lập dân tộc dưới chế độ quân chủ chuyên chế, càng không chấp nhận chế độ thực dân không kém phần chuyên chế. Bởi vì, đó là chế độ mà người dân bị đầu độc về tinh thần lẫn thể xác, bị bịt mồm và bị giam hãm. Với Hồ Chí Minh, chỉ có xây dựng một xã hội mà ở đó giá trị dân chủ và hạnh phúc thực sự mới nâng con người phát triển lên thành CON NGƯỜI đúng nghĩa.

Hồ Chí Minh khẳng định: “Dân chủ là thế nào? Là dân làm chủ”³. Rõ ràng, theo Hồ Chí Minh thì dân chủ là dân làm chủ khi nhân dân Việt Nam đã làm chủ đất nước mình, nghĩa là dân là chủ và dân làm chủ. Chỉ khi vị trí là chủ của dân được xác định, thì vai trò làm chủ của dân mới được xác

1. Hồ Chí Minh: *Toàn tập, Sđd*, t.11, tr.517.

2. Hồ Chí Minh: *Toàn tập, Sđd*, t.15, tr.3.

3. Hồ Chí Minh: *Toàn tập, Sđd*, t.10, tr.572.

lập, tức là dân chủ phải thể hiện bằng hoạt động thực tiễn. Hồ Chí Minh khẳng định dứt khoát dân là chủ, dân làm chủ. Chính định nghĩa này mà dân chủ là của dân, nó ở trong ý thức nhân dân, trong hành vi và hoạt động của dân, dân chủ là quyền lực của dân, thuộc về dân.

Dân là chủ đã khẳng định rõ địa vị người chủ trong chế độ chính trị, trong xã hội và nhà nước thuộc về người dân. Dân là chủ đối lập với nô lệ, thần dân hay thảo dân trong chế độ phong kiến cũng như thân phận nô lệ dưới chế độ thực dân. Dưới xã hội phong kiến, vua là chủ thể của quyền lực, được xem là thiên tử, là chủ của dân. Trong chế độ chính trị mới mà Hồ Chí Minh đấu tranh xây dựng, nhìn trong hệ quy chiếu quyền lực thì dân là chủ thể quyền lực, là chủ của xã hội. Dân làm chủ phản ánh năng lực thực thi dân chủ của người dân. Năng lực đó được biểu hiện ở trình độ văn hóa, bản lĩnh, ý thức, trách nhiệm..., đó là nội hàm của năng lực dân chủ, thể hiện hành vi làm chủ. Chính địa vị người chủ và năng lực làm chủ đã khái quát đầy đủ nhất trong nhận thức về dân chủ của Hồ Chí Minh. Làm chủ là hành động của người dân, biểu hiện năng lực thực hành dân chủ, thước đo về trình độ phát triển ý thức dân chủ của dân với tư cách là chủ thể quyền lực, thực hiện sự ủy quyền chân chính của mình vào thể chế chính trị. Địa vị và năng lực đó biểu hiện ra trong sự vận động của chính trị, đó là “bao nhiêu quyền hạn đều của dân”, “mọi quyền hành và lực lượng đều ở nơi dân”¹. Nhân dân là chủ thể gốc của quyền lực và Nhà nước là chủ thể đại diện cho nhân dân. Nhà nước là một thực thể mà

1. Hồ Chí Minh: *Toàn tập, Sdd*, t.6, tr.232.

nhân dân là chủ sở hữu, là chủ thể ủy quyền, Nhà nước thực hiện sự ủy quyền của nhân dân.

Trong quan niệm của Hồ Chí Minh, dân chủ còn chính là khát vọng vươn lên để xây dựng một cuộc sống ấm no, hạnh phúc cho mỗi con người. Theo Hồ Chí Minh, nước độc lập, tự do là do nhân dân giành lại thì không có lý do gì mà nhân dân không được làm chủ. Làm chủ trong quan hệ dân - nước, trong quan hệ sở hữu. Không có một nước dân chủ nào khi dân đã là chủ mà lại không có quy định quyền làm chủ bản thân, làm chủ cuộc sống của người dân. Với các nước thuộc địa, quá trình đi đến dân chủ là quá trình xác lập địa vị làm chủ đất nước của dân, để dân làm chủ thực sự, làm chủ mọi mặt đời sống xã hội trong sự thống nhất giữa làm chủ của cộng đồng với làm chủ của cá nhân. Có như vậy nhân dân mới có cuộc sống hạnh phúc thực sự. Hồ Chí Minh đã từng khẳng định: “Chúng ta tranh được tự do, độc lập rồi mà dân cứ chết đói, chết rét, thì tự do, độc lập cũng không làm gì. Dân chỉ biết rõ giá trị của tự do, của độc lập khi mà dân được ăn no, mặc đủ”¹. Như vậy, khái niệm hạnh phúc theo quan điểm của Hồ Chí Minh là người dân có được cơm no, áo ấm, không bị chết đói, chết rét; được là công dân của một nước độc lập, không còn mang nỗi nhục nô lệ; được học hành để nâng cao kiến thức và có khả năng chọn lựa, quyết định tương lai của mình. Với Hồ Chí Minh, hạnh phúc thực sự của con người là mục tiêu cuối cùng của chính trị, của phát triển xã hội. Quan điểm của Hồ Chí Minh cũng giống như điều mà Tổng thống Mỹ Thomas Jefferson từng khẳng định: “Chăm lo

1. Hồ Chí Minh: *Toàn tập, Sdd*, t.5, tr.9.

cuộc sống và hạnh phúc con người... là mục tiêu chính đáng duy nhất của một chính phủ tốt”¹. Điều này cũng được Amartya Sen - người đoạt giải Nobel kinh tế năm 1998, nêu rõ: “Mục tiêu sau cùng của phát triển là đem lại cho con người khả năng làm công việc mang đến lợi ích và hạnh phúc cho bản thân, gia đình và xã hội. Một cách ngắn gọn, hạnh phúc con người không chỉ ở vật chất, mà chính là khả năng người ấy có thể sử dụng vật chất mình có, sự tự do mình có, để đem lại hạnh phúc cho bản thân và xã hội”².

Hồ Chí Minh quan niệm, ấm no, hạnh phúc chính là chủ nghĩa xã hội. Người khẳng định: “Chủ nghĩa xã hội là gì? Là mọi người được ăn no mặc ấm, sung sướng, tự do”³, “là làm cho mọi người dân được ấm no, hạnh phúc và học hành tiến bộ”⁴, “Chủ nghĩa xã hội là tất cả mọi người các dân tộc cùng ấm no, con cháu chúng ta ngày càng sung sướng”⁵, “Chủ nghĩa xã hội là làm cho dân giàu nước mạnh”⁶. Những mục tiêu cụ thể này một lần nữa được Hồ Chí Minh khái quát súc tích và nhất quán, khi Người khẳng định: “xã hội chủ nghĩa không có bóc lột và áp bức dân tộc”⁷, là “một xã hội bảo đảm cho đất nước phát triển rực rỡ một cách nhanh chóng chưa từng thấy, đưa quần chúng lao động đến một

1. Nguyễn Đài Trang: *Hồ Chí Minh - Nhân văn và phát triển*, *Sđd*, tr.336-337.

2. Michael P. Todaro & Stephen C. Smith: *Economic Development*, Don Mills, ON: Pearson Addison-Wesley, 2012, p.16.

3, 6. Hồ Chí Minh: *Toàn tập*, *Sđd*, t.10, tr.593, 390.

4. Hồ Chí Minh: *Toàn tập*, *Sđd*, t.12, tr.521.

5. Hồ Chí Minh: *Toàn tập*, *Sđd*, t.13, tr.78.

7. Hồ Chí Minh: *Toàn tập*, *Sđd*, t.11, tr.160.

cuộc sống xứng đáng, vẻ vang và ngày càng phồn vinh, làm cho người lao động có một Tổ quốc tự do, hạnh phúc và hùng cường, hướng tới những chân trời tươi sáng mà trước kia không thể nghĩ tới”¹. Có thể thấy, theo Hồ Chí Minh, chủ nghĩa xã hội chính là mục tiêu nâng cao vị thế tồn tại của con người.

Độc lập, tự do, công lý, hòa bình, dân chủ, hạnh phúc chính là những giá trị nhân bản, những yếu tố quy định là con người và cũng chính là những giá trị mà một quốc gia phải có. Ở Hồ Chí Minh, các giá trị đó là tự nhiên vốn có của con người, nghĩa là đã là con người thì đều có hòa bình, độc lập, tự do, dân chủ, hạnh phúc và các yếu tố này gắn chặt với nhau, hòa quyện vào nhau. Đồng thời các giá trị này cũng phải là những giá trị thể hiện chủ quyền của một quốc gia - dân tộc. Hồ Chí Minh khẳng định: “Muốn thống nhất phải có hòa bình. Muốn độc lập thì phải thống nhất. Muốn độc lập thật sự thì phải có dân chủ. Bốn điểm đó như bầu trời có bốn phương: Đông, Tây, Nam, Bắc; như một năm có bốn mùa: Xuân, Hạ, Thu, Đông; không thể tách rời nhau, không thể thiếu một điểm nào”². Cách mạng Tháng Tám - một cuộc cách mạng xã hội cũng đấu tranh vì các mục tiêu đó: “Mục đích của Cách mạng Tháng Tám là gì? Là giành lại hòa bình, thống nhất, độc lập và dân chủ cho Tổ quốc ta, cho nhân dân ta”³. Cuộc kháng chiến chống Pháp và chống Mỹ cũng vì mục tiêu đó: “Nhân dân Việt Nam anh dũng chiến đấu mục đích

1. Hồ Chí Minh: *Toàn tập*, *Sđd*, t.11, tr.161.

2. Hồ Chí Minh: *Toàn tập*, *Sđd*, t.9, tr.244-245.

3. Hồ Chí Minh: *Toàn tập*, *Sđd*, t.5, tr.9.

là thực hiện một nước hòa bình, độc lập, thống nhất, dân chủ, tự do”¹. Chủ nghĩa xã hội - xây dựng một xã hội lý tưởng cũng vì mục tiêu đó: “Mục đích của chủ nghĩa xã hội là gì? Nói một cách đơn giản và dễ hiểu là: không ngừng nâng cao đời sống vật chất và tinh thần cho nhân dân”².

Tựu trung, Hồ Chí Minh đã thể hiện một phương pháp tiếp cận quyền con người và chủ quyền quốc gia từ góc độ tính nhân bản tự nhiên: giá trị đích thực của quyền con người và chủ quyền quốc gia là những giá trị nhân bản tự nhiên và việc đấu tranh bảo vệ và thực thi quyền con người, chủ quyền quốc gia là đấu tranh giải phóng và phát triển những giá trị mang bản chất người đó.

Trong bối cảnh một số nước phương Tây đưa ra cái gọi là “nhân quyền cao hơn chủ quyền”, “nhân quyền không biên giới” nhằm can thiệp vào công việc nội bộ của các quốc gia - dân tộc, việc nắm vững những quan điểm của Hồ Chí Minh về nhân quyền và chủ quyền quốc gia - dân tộc càng có ý nghĩa sâu sắc. Quyền con người phải gắn liền với quyền dân tộc. Nhân quyền không thể tách rời chủ quyền quốc gia - dân tộc. Nhân quyền trước hết phải là quyền độc lập dân tộc. Đất nước mất độc lập thì nhân dân không thể có tự do, các quyền con người không được tôn trọng và bảo vệ. Trong xu thế toàn cầu hóa và hội nhập quốc tế ngày càng sâu rộng, nhiều vấn đề phức tạp nảy sinh mà không một quốc gia nào có thể tự giải quyết mà cần phải có sự hợp tác quốc tế. Song, sự hợp tác quốc tế phải dựa trên cơ sở bình đẳng, tôn trọng độc lập,

1. Hồ Chí Minh: *Toàn tập, Sđd*, t.8, tr.474.

2. Hồ Chí Minh: *Toàn tập, Sđd*, t.13, tr.30.

chủ quyền và toàn vẹn lãnh thổ của nhau và trên cơ sở luật pháp quốc tế. Không một quốc gia nào, dù lớn mạnh và phát triển đến đâu, có quyền đơn phương dùng vũ lực áp đặt ý muốn của mình đối với các quốc gia - dân tộc khác, lôi kéo các tổ chức quốc tế thực hiện các mưu đồ chính trị khi xử lý các vấn đề nhân quyền.

NHỮNG THÁCH THỨC ĐỐI VỚI VIỆC BẢO VỆ CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG

Đại tá, TS. NGUYỄN CÔNG XUÂN*

Không gian mạng ra đời đã tạo ra nhiều cơ hội thuận lợi trong sự nghiệp bảo vệ Tổ quốc, nhưng từ không gian mạng cũng xuất hiện nhiều khó khăn, thách thức mới đe dọa trực tiếp đến chủ quyền đất nước. Chiến lược phát triển kinh tế - xã hội 10 năm 2021 - 2030 trong Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII của Đảng khẳng định: “Tích cực, chủ động xây dựng kế hoạch, phương án tác chiến, nâng cao trình độ, khả năng sẵn sàng chiến đấu bảo vệ vững chắc độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ và giữ vững ổn định chính trị, an ninh quốc gia, trật tự, an toàn xã hội, giữ chủ quyền số quốc gia trên không gian mạng trong mọi tình huống”¹. Đây là quan điểm mới về bảo vệ chủ quyền quốc gia phù hợp với xu thế chung của khu vực, thế giới, thực trạng phát triển không gian mạng Việt Nam và sự tác động của Cách mạng công nghiệp lần thứ tư.

* Viện Chiến lược Quốc phòng, Bộ Quốc phòng.

1. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.I, tr.277.

Nghị định số 101/2016/NĐ-CP, ngày 01/7/2016 của Chính phủ quy định chi tiết trách nhiệm thực hiện và các biện pháp ngăn chặn hoạt động sử dụng không gian mạng để khủng bố nêu rõ: không gian mạng là mạng lưới kết nối toàn cầu của kết cấu hạ tầng công nghệ thông tin bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin; là môi trường đặc biệt mà con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian. Không gian mạng là môi trường thông tin hoạt động trên phổ điện từ trường; được tạo nên bởi các kết cấu hạ tầng thông tin và hoạt động của các thành phần xã hội trên kết cấu hạ tầng thông tin đó nhằm cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin. Nội hàm chung của không gian mạng mang bản chất vật lý và bản chất xã hội. Mạng lưới kết nối không gian mạng bao gồm nhiều thành phần không giới hạn bởi không gian, thời gian, đan xen nhiều tầng hệ thống như: hệ thống mạng internet, hệ thống thông tin, cơ sở dữ liệu, mạng xã hội... Mọi hoạt động của xã hội đều diễn ra trên không gian mạng đã tạo ra nhiều thách thức đa dạng, phức tạp, khó lường hơn nhiều so với các môi trường khác. Không gian mạng nước ta, mặc dù có tốc độ phát triển nhanh với diện rộng, nhưng ý thức sử dụng của đa số người dân còn thấp, hệ thống luật pháp, chính sách chưa thật đồng bộ, quản lý còn bất cập, trình độ công nghệ chưa phát triển, còn phụ thuộc nước ngoài. Vì vậy, trên môi trường không gian mạng nảy sinh nhiều thách thức hơn so với các môi trường khác trong bảo vệ chủ quyền quốc gia.

Bảo vệ chủ quyền quốc gia trên không gian mạng là bảo vệ tất cả các quyền của Nhà nước đối với không gian mạng, phù

hợp với quy định của luật pháp quốc tế. Đảng, Nhà nước ta sớm nhận thức vấn đề này và ra nhiều chủ trương, biện pháp định hướng cho các cấp triển khai thực hiện. Vấn đề bảo vệ chủ quyền quốc gia trên không gian mạng rất mới, phức tạp, khó khăn. Đối tượng của bảo vệ chủ quyền quốc gia trên không gian mạng đa dạng, khó xác định, có trình độ công nghệ cao, trong khi lực lượng nòng cốt bảo vệ chủ quyền quốc gia trên không gian mạng của ta mới thành lập, trình độ và phương tiện chưa phát triển, sự phối hợp chưa đồng bộ giữa các ban, bộ, ngành, địa phương. Không gian mạng có đặc tính toàn cầu không biên giới, vừa mang tính hữu hình, vừa vô hình; vừa thực, vừa ảo, gồm cấu trúc vật lý và cấu trúc xã hội. Vì vậy, bảo vệ chủ quyền quốc gia trên không gian mạng Việt Nam càng thách thức, phức tạp, khó khăn hơn nhiều so với các lĩnh vực truyền thống, gồm nhiều nội dung, ngày càng nảy sinh, xuất hiện những thách thức mới từ phía đối tượng chống phá, trình độ phát triển khoa học công nghệ liên quan đến mọi ngành trong xã hội và lực lượng bảo vệ chủ quyền quốc gia trên không gian mạng.

Một là, thách thức đối với các hoạt động “diễn biến hòa bình” của các thế lực thù địch, phản động nhằm xóa bỏ vai trò lãnh đạo của Đảng Cộng sản Việt Nam, chế độ xã hội chủ nghĩa ở nước ta.

“Diễn biến hòa bình” của các thế lực thù địch đối với nước ta là một trong bốn nguy cơ được Đảng chỉ ra tại Hội nghị giữa nhiệm kỳ Đại hội lần thứ VII (tháng 01/1994) ngày càng hiện hữu, ảnh hưởng nguy hại đến bảo vệ chủ quyền quốc gia. Các thế lực thù địch, phản động thực hiện chiến lược “diễn biến hòa bình” trên không gian mạng với phạm vi rộng,

mức độ tinh vi, dữ dội, thâm độc, nham hiểm hơn đã tạo ra thách thức lớn đối với bảo vệ chủ quyền quốc gia. Mục tiêu cao nhất của chúng là xóa bỏ sự lãnh đạo của Đảng, Nhà nước xã hội chủ nghĩa, nhân tố quyết định để giữ vững, bảo vệ chủ quyền quốc gia. Lợi dụng tính đặc thù của không gian mạng, các thế lực thù địch, phản động thực hiện “diễn biến hòa bình”, thúc đẩy “tự diễn biến”, “tự chuyển hóa” với cường độ ngày càng quyết liệt, kích động bạo loạn, “cách mạng màu”, “cách mạng đường phố”, kết hợp với can thiệp quân sự lật đổ chế độ xã hội chủ nghĩa ở Việt Nam, câu kết với các tổ chức phản động, lực lượng cơ hội, suy thoái chính trị, đạo đức, lối sống sử dụng không gian mạng để thực hiện các hoạt động tuyên truyền, chống phá nền tảng tư tưởng, lý luận của Đảng, phủ nhận vai trò lãnh đạo của Đảng, sự quản lý của Nhà nước và con đường đi lên chủ nghĩa xã hội; thúc đẩy “tự diễn biến”, “tự chuyển hóa” để chia rẽ, lôi kéo, thay đổi bản chất cộng sản của Đảng, chuyển hướng Việt Nam đi theo con đường “xã hội dân chủ” của phương Tây; tuyên truyền, kích động, lôi kéo quần chúng nhân dân tham gia biểu tình, bạo loạn chính trị, thực hiện “cách mạng màu”, “cách mạng đường phố”, kích động bạo loạn, ly khai ở các trung tâm chính trị, kinh tế, văn hóa - xã hội hoặc ở một số vùng chiến lược hoặc cả nước, lật đổ, thành lập chính quyền ly khai, kêu gọi thế giới can thiệp.

Công kích nền tảng tư tưởng của Đảng là chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh nhằm xóa bỏ vai trò lãnh đạo của Đảng, xóa bỏ chế độ xã hội chủ nghĩa. Chống phá sự lãnh đạo của Đảng bằng cách xuyên tạc mục tiêu, lý tưởng của Đảng, con đường đi lên chủ nghĩa xã hội, xuyên tạc

cương lĩnh, đường lối, chủ trương của Đảng; chính sách, pháp luật của Nhà nước, xuyên tạc các nguyên lý xây dựng Đảng, đòi xóa bỏ Điều 4 trong Hiến pháp, đòi Đảng từ bỏ nguyên tắc tập trung dân chủ để hướng theo tư tưởng đa nguyên chính trị, đa đảng đối lập. Lợi dụng internet và các mạng xã hội triệt để tăng cường các hoạt động chống phá Đảng, Nhà nước ngày càng công khai, trực diện. Sử dụng sức mạnh của internet để truyền bá quan điểm, tư tưởng, giá trị phương Tây, lối sống tự do, thúc đẩy “tự diễn biến”, “tự chuyển hóa”. Chúng tập trung xuyên tạc, phản bác chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước, thực trạng kinh tế - xã hội, tình hình an ninh chính trị, trật tự, an toàn xã hội, bôi nhọ uy tín cá nhân... Tận dụng các hãng thông tấn nước ngoài để tuyên truyền, quảng bá, kích động hoạt động chống phá, chỉ trích Việt Nam vi phạm dân chủ, nhân quyền. Thông qua internet, mạng xã hội, chúng đẩy mạnh tấn công tư tưởng cán bộ, đảng viên và nhân dân, từ đó kích động, lôi kéo nhân dân tham gia biểu tình, gây mất an ninh chính trị, trật tự, an toàn xã hội, hạ thấp uy tín Việt Nam trên trường quốc tế.

Tuyên truyền, phá hoại tư tưởng, chia rẽ lực lượng vũ trang, đòi “phi chính trị hóa” quân đội và công an, công kích nền tảng tư tưởng của Đảng. Lợi dụng sự sụp đổ của chế độ xã hội chủ nghĩa ở Liên Xô và Đông Âu, các thế lực thù địch đã tấn công quyết liệt vào nền tảng tư tưởng của Đảng, Nhà nước ta là chủ nghĩa Mác - Lênin và tư tưởng Hồ Chí Minh; thường xuyên đăng tải các bài viết, lợi dụng những thiếu sót trong lãnh đạo, quản lý để xuyên tạc vai trò lãnh đạo, xuyên tạc bản chất của Đảng, đồng nhất Đảng Cộng sản với một số

ít cán bộ, đảng viên thoái hóa, biến chất, khuếch đại hạn chế, yếu kém, khuyết điểm của Đảng, Nhà nước, yếu kém trong phát triển kinh tế. Các thế lực thù địch, phản động tăng cường hoạt động trên không gian mạng để chống phá về chính trị, kinh tế, tư tưởng, văn hóa, dân chủ, nhân quyền, dân tộc, tôn giáo; xâm phạm chủ quyền, lợi ích quốc gia - dân tộc; thực hiện “diễn biến hòa bình”, thúc đẩy “tự diễn biến”, “tự chuyển hóa” nhằm thay đổi chế độ chính trị ở nước ta. Tình hình mất an toàn, an ninh thông tin mạng sẽ tiếp tục diễn biến phức tạp, đe dọa đến sự phát triển kinh tế, xã hội, quốc phòng, an ninh... Các thế lực thù địch sẵn sàng chuyển từ phá hoại sang can thiệp vũ trang, tiến hành chiến tranh mạng và các hình thái chiến tranh khác khi có thời cơ.

Hai là, thách thức gây mất an ninh quốc gia thông qua các hoạt động tiến công mạng, gián điệp mạng, khủng bố mạng và tội phạm phá hoại về kinh tế, chính trị, văn hóa, xã hội, quốc phòng, an ninh, đối ngoại.

An ninh mạng là một bộ phận của an ninh quốc gia. Mất an ninh mạng sẽ dẫn đến mất an ninh quốc gia và đe dọa nghiêm trọng đến chủ quyền đất nước. Trên không gian mạng ngày nay xuất hiện nhiều nhân tố bất ổn, phức tạp như các hoạt động tấn công mạng, gián điệp mạng, khủng bố mạng, tội phạm mạng... với tính chất rất nghiêm trọng. Không gian mạng là một mặt trận tiến hành các cuộc chiến tranh thông tin, chiến tranh không gian mạng và các phương thức tác chiến mạng độc lập hoặc kết hợp với các phương thức tác chiến trên môi trường tự nhiên trong chiến tranh cục bộ, xung đột dân tộc, sắc tộc, vũ trang, tranh chấp tài

nguyên, chủ quyền lãnh thổ, biển đảo, xung đột dân tộc, sắc tộc, tôn giáo, hoạt động can thiệp lật đổ, ly khai và khủng bố. An ninh mạng hiện có bốn mối đe dọa chủ yếu là: tấn công mạng, gián điệp mạng, khủng bố mạng và tội phạm mạng. Hoạt động gián điệp mạng và tội phạm mạng gây ra nhiều thiệt hại lớn về kinh tế, nhưng khủng bố mạng và tấn công mạng có thể trở thành mối đe dọa lớn hơn trong thập niên tới.

Thông tin kích động trên không gian mạng có nguy cơ xảy ra bạo loạn, phá rối an ninh, khủng bố; tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia; tấn công nhiều hệ thống thông tin trên quy mô lớn, cường độ cao; tấn công mạng nhằm phá hủy công trình quan trọng về an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia; tấn công mạng xâm phạm nghiêm trọng chủ quyền, lợi ích, an ninh quốc gia; gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Thực tế, nguy cơ mất an ninh, an toàn mạng máy tính còn có thể phát sinh ngay từ bên trong, do người sử dụng có quyền truy cập hệ thống nắm được điểm yếu của hệ thống hay vô tình tạo cơ hội cho những đối tượng khác xâm nhập hệ thống.

Tấn công mạng ngày càng trở nên thách thức thực sự đe dọa đến an ninh mạng tại nước ta. Các hành vi tấn công mạng, liên quan đến tấn công mạng tạo thách thức đối với bảo vệ chủ quyền an ninh quốc gia gồm: phát tán chương trình tin học gây hại cho mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử; gây cản

trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu; xâm nhập, làm tổn hại, chiếm đoạt dữ liệu được lưu trữ, truyền đưa qua mạng, hệ thống, cơ sở dữ liệu, phương tiện điện tử; xâm nhập, tạo ra hoặc khai thác điểm yếu, lỗ hổng bảo mật và dịch vụ hệ thống để chiếm đoạt thông tin. Tấn công mạng có thể thông qua các phương thức lỗ hổng bảo mật, tấn công chèn mã lệnh, tấn công qua thiết bị phần cứng, tấn công hệ thống thông tin, hạ tầng trọng yếu quốc gia.

Khủng bố mạng thực sự là mối đe dọa lớn đối với an ninh của bất kỳ quốc gia nào, trong đó nước ta không nằm ngoài thách thức đó. Mối đe dọa thậm chí còn lớn hơn vì Việt Nam còn nhiều lỗ hổng an ninh mạng. Việc xác định khủng bố mạng chủ yếu dựa vào việc theo dõi hoạt động của các đối tượng trên mạng internet. Tuy nhiên, có những thách thức về mặt pháp lý và kỹ thuật cản trở việc theo dõi này. Các quyền cơ bản, dân chủ và quy tắc pháp luật cần được bảo vệ và duy trì trong không gian mạng ngày càng mở rộng bởi tốc độ phát triển nhanh chóng của internet dưới tác động của Cách mạng công nghiệp lần thứ tư.

Tội phạm mạng ngày càng gia tăng, phức tạp, tinh vi, đe dọa trực tiếp đến an ninh mạng. Chúng có thể hoạt động phát tán chương trình tin học gây hại cho mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử; gây cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu của các mạng, hệ thống thông tin, xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập, làm tổn hại, chiếm đoạt dữ

liệu được lưu trữ, truyền đưa qua mạng, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử; xâm nhập, tạo ra hoặc khai thác điểm yếu, lỗ hổng bảo mật và dịch vụ hệ thống để chiếm đoạt thông tin, thu lợi bất chính; sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng tấn công mạng, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử để sử dụng vào mục đích trái pháp luật.

Thách thức gián điệp mạng ngày càng phát triển trở thành mối đe dọa đối với an ninh mạng. Hoạt động tình báo giữa các quốc gia không phải là một hiện tượng mới mẻ, nhưng vài thập niên gần đây thế giới đã chuyển sang một lĩnh vực gián điệp hoàn toàn mới. Đối với nước ta, hoạt động tình báo mạng của đối phương sẽ ảnh hưởng đến các mối quan hệ kinh tế và chính trị trong đối ngoại, làm thay đổi dạng thức chiến tranh hiện đại. Vì vậy, hàng loạt vấn đề mới đã nổi lên. Gián điệp có thể là người nước ngoài hoặc người trong nước hoạt động bằng nhiều thủ đoạn che giấu, tinh vi. Trong số các quốc gia trên thế giới đang tiến hành hoạt động này, Mỹ, Nga và Trung Quốc được xem là những nước có năng lực hoạt động gián điệp mạng nổi trội nhất với công nghệ hiện đại nhất. Thách thức của gián điệp mạng đối với nước ta là: xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng; chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức,

cá nhân; cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng; cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật; cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại.

Ba là, thách thức xảy ra chiến tranh không gian mạng, chiến tranh không gian mạng kết hợp với các hình thái chiến tranh khác đe dọa nghiêm trọng đến độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ.

Nếu xảy ra chiến tranh mạng, chiến tranh mạng kết hợp với các hình thái chiến tranh khác sẽ đe dọa trực tiếp đến chủ quyền quốc gia, chủ quyền quốc gia trên không gian mạng. Chiến tranh mạng khác nhiều so với chiến tranh truyền thống, có thể xảy ra độc lập hoặc kết hợp với các hình thái chiến tranh khác. Đây là hình thái chiến tranh khác với các hình thái chiến tranh truyền thống. Đối tượng tác chiến rất đa dạng, có trình độ công nghệ cao, khó phát hiện đối tượng, thời gian.

Hoạt động cảnh báo, phát hiện sớm dấu hiệu chiến tranh rất khó khăn, dễ nhầm lẫn với tiến công mạng đơn thuần. Đối phương tiến hành chiến tranh không gian mạng bằng cách sử dụng các thủ đoạn để phá vỡ hạ tầng hệ thống

mạng quốc gia, gây rối loạn làm tê liệt hệ thống lãnh đạo của Đảng, quản lý, điều hành của Nhà nước về lĩnh vực quân sự, quốc phòng; tiến công phá hủy tiềm lực quốc phòng gây hoang mang tinh thần của lực lượng vũ trang và nhân dân, làm mất khả năng kiểm soát không gian mạng, làm suy yếu khả năng của ta để tạo điều kiện tấn công xâm lược.

Chiến tranh không gian mạng kết hợp với các hình thái chiến tranh khác đe dọa nghiêm trọng đến chủ quyền quốc gia với mức độ rất nguy hiểm. Trên chiến trường không gian mạng, đối phương sẽ phá hoại làm ngưng trệ hoặc tê liệt hệ thống lãnh đạo, chỉ huy điều hành tác chiến, hệ thống tự động hóa chỉ huy, hệ thống điều khiển vũ khí công nghệ cao. Chiếm quyền điều khiển hệ thống thông tin kết hợp với các hoạt động trên các chiến trường để thực hiện mục đích chiến tranh xâm lược. Tiến hành chiến tranh mạng phục vụ cho chiến tranh xâm lược là hoạt động tấn công quy mô lớn trên không gian mạng quốc gia để phá hoại, làm tê liệt hệ thống, nguồn tài nguyên thông tin cũng như các kết cấu hạ tầng thông tin quan trọng, xâm phạm chủ quyền quốc gia về quân sự, chính trị, kinh tế, đe dọa nghiêm trọng độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ Tổ quốc.

Địch có thể tấn công mạng cường độ cao, gây tê liệt, ngưng trệ, phá hủy hệ thống thông tin quan trọng quốc gia, đặc biệt là hệ thống điều hành chỉ huy, hệ thống vũ khí công nghệ cao, hạ tầng quân sự, công nghiệp quan trọng, hệ thống điều khiển tự động, các hệ thống điều khiển quan trọng quốc gia như năng lượng, giao thông... Tiến hành chiến tranh thông tin, chiến tranh không gian mạng, các đối tượng trong và ngoài nước tiến hành xâm

nhập vào không gian mạng để kiểm soát, điều khiển, chế áp thông tin của Việt Nam, tiến hành các chiến dịch truyền thông nhằm can thiệp các công việc nội bộ của Việt Nam; gây bất lợi, thậm chí cô lập Việt Nam trên trường quốc tế; tạo có phát động chiến tranh xâm lấn, xâm lược. Tiến hành các hoạt động làm gián đoạn hoặc phá hủy các hệ thống thông tin phục vụ lãnh đạo, chỉ đạo, điều hành của Đảng, Nhà nước, quân đội và các hệ thống điều khiển vũ khí bằng phương tiện điện tử. Tiến hành xâm nhập, cài đặt vũ khí mạng tạo thế trận trên không gian mạng để thực hiện các hoạt động trinh sát, thu thập thông tin tình báo; sẵn sàng tấn công, chiếm quyền điều khiển các hệ thống thông tin quan trọng quốc gia nhằm phá hủy hoặc làm bàn đạp tấn công, phá hủy các kết cấu hạ tầng kinh tế - xã hội, quốc phòng - an ninh.

Bốn là, thách thức lệ thuộc vào công nghệ, kỹ thuật, không kiểm soát được các tiêu chuẩn về an toàn thông tin và phải đối diện với các hoạt động tác chiến không gian mạng trên nhiều lĩnh vực.

Đây là thách thức ảnh hưởng gián tiếp nhưng rất lâu dài, toàn diện đến bảo vệ chủ quyền quốc gia trên không gian mạng. Đối phương triệt để sử dụng ưu thế về phát triển công nghệ, kỹ thuật để gây ảnh hưởng khiến ta phụ thuộc trong kiểm soát an ninh, an toàn thông tin trên không gian mạng. Các sản phẩm an toàn thông tin của ta chủ yếu xuất xứ từ nước ngoài có thể dẫn đến sự lệ thuộc vào công nghệ, kỹ thuật, không kiểm soát được các tiêu chuẩn về an toàn thông tin và an ninh thông tin, bị cài sẵn kênh ngầm, “cửa hậu”, phát tán mã độc thông qua hình thức phát tán mã độc, kẻ

tấn công thường lây nhiễm mã độc vào hệ thống thông tin quan trọng quốc gia nhằm đánh cắp, thu thập những dữ liệu nhạy cảm, đe dọa đến tính bí mật, tính xác thực và tính sẵn sàng của thông tin và hệ thống thông tin.

Mã độc có thể được phát tán qua mạng xã hội, lây nhiễm vào máy tính khi người dùng truy cập internet, các phần mềm hoặc ứng dụng của bên thứ ba. Mã độc lây lan thông qua phần mềm có nguồn gốc không rõ ràng, sử dụng các phần mềm lậu hoặc các phần mềm bị nhiễm mã độc. Qua thư điện tử, mã độc được lây lan qua các tệp tin đính kèm trong email, khi người dùng trong hệ thống gửi email cho nhau. Qua các thiết bị di động như USB, ổ cứng di động có chứa mã độc cũng rất dễ được chuyển tới các máy tính khác trong hệ thống. Rất nhiều trang web hiện nay trên internet bị nhiễm các phần mềm có chứa mã độc, hay các đoạn mã được chèn thêm vào chính website. Khi người dùng truy cập vào thì máy tính bị nhiễm mã độc. Hiện nay, một số phần mềm độc hại có thể lợi dụng lỗ hổng phần mềm tự phát tán và nhân bản tới các máy khác. Thu chặn, thu trộm thông tin bằng kỹ thuật công nghệ cao, thông tin có thể bị chặn bắt, nghe lén khi đang truyền tải bởi tin tặc dùng các công cụ thu thập gói tin trên luồng dữ liệu mạng, sau đó phân tích gói tin nhằm thu thập thông tin nhạy cảm.

Một số thông tin của người dùng được phần mềm lưu trên bộ nhớ RAM, tin tặc cũng có thể chiếm được bằng cách dò tìm (dump) bộ nhớ của máy tính. Tấn công xen giữa là một hình thức phổ biến để nghe lén thông tin giữa hai điểm trên một hệ thống mạng, hoặc tin nhắn, cuộc gọi, hình ảnh có thể bị ghi lại và được bí mật chuyển về máy chủ ở nước

ngoài bởi các phần mềm mã độc. Cài cắm “cửa hậu”, “kênh ngầm” vào các thiết bị công nghệ thông tin. Hiện nay, phần lớn các sản phẩm công nghệ thông tin và viễn thông, đặc biệt là các thiết bị an toàn thông tin và các máy chủ có xuất xứ từ nước ngoài, dẫn đến sự lệ thuộc về công nghệ, kỹ thuật, không kiểm soát được các tiêu chuẩn về an toàn thông tin và an ninh thông tin. Các thiết bị này có thể bị cài sẵn kênh ngầm, “cửa hậu” nhưng vẫn được sử dụng trong các hệ thống thông tin quan trọng quốc gia.

Quan điểm bảo vệ chủ quyền quốc gia trên không gian mạng nước ta là chủ trương đúng đắn của Đảng nhằm bảo vệ vững chắc độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ Tổ quốc trong tình hình mới. Bảo vệ chủ quyền quốc gia trên không gian mạng Việt Nam là vấn đề mới, đối tượng hoạt động trên không gian mạng phức tạp gắn với phương tiện và trình độ công nghệ cao, lực lượng nòng cốt bảo vệ chủ quyền trên không gian mạng của ta mới thành lập, trình độ và phương tiện chưa phát triển đã nảy sinh nhiều thách thức về bảo vệ chủ quyền quốc gia trên không gian mạng. Nhận thức đầy đủ các thách thức để có giải pháp đối phó phù hợp, hiệu quả là vấn đề quan trọng, cần thiết góp phần bảo vệ chủ quyền quốc gia trên không gian mạng, bảo vệ vững chắc chủ quyền quốc gia trong tình hình mới.

ỨNG XỬ CỦA CÁC QUỐC GIA TRÊN KHÔNG GIAN MẠNG: TĂNG CƯỜNG HỢP TÁC VÀ ĐẤU TRANH TRÊN MẶT TRẬN NGOẠI GIAO

TS. CHU MINH THẢO*

Cùng với sự phát triển vũ bão của khoa học công nghệ, nhất là công nghệ thông tin, thế giới đang đứng trước những cơ hội cũng như khó khăn, thách thức chưa từng có trong thế kỷ XXI, đó là an ninh thông tin, tội phạm trên không gian mạng. Trong một thế giới kết nối một mạng lưới phức tạp ở cấp độ toàn cầu, các mối đe dọa, xung đột an ninh mạng có thể tác động đến hòa bình và an ninh toàn cầu. Liên hợp quốc đã xây dựng và thông qua Nghị quyết về 11 chuẩn mực về ứng xử có trách nhiệm của các nhà nước trên không gian mạng. Cùng với đó, ASEAN cũng đang thảo luận xây dựng khuôn khổ để thực hiện các chuẩn mực này. Song hành với nỗ lực của các tổ chức quốc tế và khu vực trong việc xây dựng các chuẩn mực quốc tế và khu vực, thì quá trình triển khai các chuẩn mực này còn gặp nhiều khó khăn, do khoa học - công nghệ liên tục phát triển trong khi các bên liên quan còn thiếu nhận thức, năng lực thực thi các

* Viện Nghiên cứu chiến lược ngoại giao, Bộ Ngoại giao.

chuẩn mực. Bên cạnh đó là quá trình “quân sự hóa”, “chính trị hóa” an ninh mạng và cạnh tranh nước lớn trong quá trình xây dựng và triển khai các chuẩn mực quốc tế, hiện đang gây ra những tác động lớn đối với việc định hình trật tự thế giới.

Bối cảnh này đặt ra cả cơ hội và thách thức cho các nước đang phát triển như Việt Nam trong nỗ lực bảo vệ an ninh quốc gia, bảo đảm chủ quyền trên không gian mạng, đòi hỏi sự quan tâm của các cấp lãnh đạo, cũng như tăng cường nhận thức và năng lực thực thi các chuẩn mực về ứng xử có trách nhiệm trong không gian mạng hơn nữa. Việt Nam cũng đã tham gia các chuẩn mực này của Liên hợp quốc với nhận thức về tầm quan trọng của các chuẩn mực này trong việc điều chỉnh hành vi, tránh xung đột tiềm tàng, tăng tính minh bạch và dự đoán, góp phần bảo vệ chủ quyền quốc gia, nhất là không gian mạng. Bài toán đặt ra cho Việt Nam hiện nay là cần phải tiếp tục định hướng tăng cường hợp tác xây dựng trên lĩnh vực về ứng xử không gian mạng như thế nào cả ở cấp song phương, khu vực và quốc tế. Việt Nam cần tiếp tục chủ động, tích cực tham gia vào quá trình định hình các thiết chế, định chế, quản trị, luật lệ đa phương về không gian mạng, một lĩnh vực luôn phát triển và biến đổi, đồng thời thúc đẩy các hợp tác song phương để thực hiện hiệu quả các chuẩn mực đã ký kết cũng như xây dựng, phát triển các chuẩn mực mới liên quan đến an ninh mạng.

1. Khái niệm

Không gian mạng và các khái niệm liên quan được hiểu theo nhiều cách khác nhau. Tuy nhiên, một số khái niệm cơ

bản có thể được hiểu thống nhất như sau: An ninh mạng bao gồm tất cả các yếu tố cần thiết liên quan đến phòng vệ và ứng phó với các mối đe dọa từ không gian mạng (ví dụ, công nghệ, thiết bị, chính sách, các khái niệm an ninh, phòng vệ an ninh, hướng dẫn, các cách tiếp cận quản lý rủi ro, hành động, đào tạo, thông lệ tốt nhất...). Các rủi ro không gian mạng bao gồm khả năng một sự kiện xảy ra liên quan đến hệ thống thông tin kết nối, gây ảnh hưởng đến tài sản và danh tiếng. Các mối đe dọa không gian mạng có thể gây các hậu quả không mong muốn, gây hại đến hệ thống hay tổ chức, có thể bắt nguồn từ bên trong hay tác động từ bên ngoài, do các cá nhân hay tổ chức gây ra. Các cuộc tấn công không gian mạng sử dụng các mã độc hại ảnh hưởng đến vi tính và mạng lưới, dẫn đến tội phạm không gian mạng, như trộm danh tính hay thông tin. Khả năng chống chịu trong không gian là khả năng hệ thống và tổ chức chống chịu các sự kiện không gian mạng, bao gồm cả thời gian bị đổ vỡ và phục hồi. Tội phạm không gian mạng bao gồm các hình thức tội phạm khác nhau liên quan đến vi tính hay mạng lưới thông tin truyền thông số, được dùng để tấn công hay bị tấn công.

2. Hiện trạng về các thỏa thuận về ứng xử của các quốc gia trên không gian mạng

Hiện nay, một trong những xu hướng chính trong không gian mạng là xu hướng “quân sự hóa”, “tội phạm hóa” không gian mạng, khiến không gian mạng trở thành một lĩnh vực tiềm ẩn nguy cơ rủi ro chiến tranh mới, cần phát triển cả năng lực phòng thủ và tấn công. Những nước đứng hàng đầu về năng lực không gian mạng năm 2020 phải kể đến như Mỹ,

Trung Quốc, Anh, Nga,... hay những nước dù là cường quốc về công nghệ thông tin như Ấn Độ nhưng không nằm trong danh sách các quốc gia hàng đầu về không gian mạng, trước những nguy cơ hiện hữu, đều phải hợp tác với nhau để đưa ra các chuẩn mực về ứng xử có trách nhiệm cho các nhà nước trên không gian mạng.

Các thỏa thuận quốc tế và khu vực:

Bên cạnh việc tập trung vào các biện pháp kỹ thuật và công nghệ để khắc phục bất cập trong an ninh mạng, Liên hợp quốc đã chú trọng đến các yếu tố con người trong việc bảo đảm an ninh mạng, nhất là vai trò của các nhà nước và hợp tác quốc tế giữa các nước. Tại cấp toàn cầu, tháng 12/2018, Đại hội đồng Liên hợp quốc đã thông qua Nghị quyết về Thúc đẩy ứng xử có trách nhiệm của các quốc gia trên không gian mạng trong bối cảnh an ninh quốc tế, nhằm nỗ lực tăng cường an ninh thông tin và hợp tác quốc tế. Quá trình xây dựng Nghị quyết dựa trên cơ sở các nước thảo luận và thống nhất về các chuẩn mực, nguyên tắc, luật lệ, các thông lệ và kinh nghiệm tốt nhất, cùng nhau đưa ra các biện pháp phù hợp để giải quyết các mối đe dọa và thách thức liên quan đến an ninh mạng.

Liên hợp quốc đã đưa ra 11 chuẩn mực về hành vi có trách nhiệm của nhà nước trên không gian mạng như sau:

- Hợp tác an ninh giữa các nước.
- Xem xét tất cả các thông tin liên quan.
- Ngăn chặn việc lạm dụng công nghệ thông tin - truyền thông trong phạm vi lãnh thổ quốc gia.
- Hợp tác chống tội phạm và khủng bố.

- Tôn trọng nhân quyền và quyền riêng tư.
- Không gây thiệt hại cho kết cấu hạ tầng quan trọng.
- Bảo vệ kết cấu hạ tầng quan trọng.
- Phản hồi yêu cầu hỗ trợ.
- Bảo đảm an ninh chuỗi cung ứng.
- Báo cáo lỗ hổng công nghệ thông tin - truyền thông.
- Không gây thiệt hại cho đội ứng cứu khẩn cấp.

Có thể thấy các chuẩn mực này chủ yếu xoay quanh một số vấn đề trọng tâm: (i) Tăng cường hợp tác an ninh, chú trọng tăng cường tính minh bạch; (ii) Ngăn chặn việc lạm dụng công nghệ thông tin - truyền thông; (iii) Bảo vệ các kết cấu hạ tầng, tôn trọng các quyền con người, nhất là quyền riêng tư, chuỗi cung ứng. Đặc điểm của các chuẩn mực trên không gian mạng là có tính chất “luật mềm”, không ràng buộc, không áp đặt đối với các nước, mà trên cơ sở tự nguyện, do đây là các thỏa thuận có tính chất chính trị nhiều hơn là hiệp ước có tính luật pháp quốc tế. Mục tiêu của các chuẩn mực này là nhằm định hướng hành vi, tạo tính dễ định đoán trong hành vi và xây dựng lòng tin giữa các quốc gia liên quan đến việc thực thi luật pháp quốc tế. Bên cạnh đó, các chuẩn mực này còn nhằm cung cấp những hướng dẫn tích cực, mang tính khích lệ các hành xử có trách nhiệm cho các quốc gia, và để các quốc gia chuẩn bị những năng lực cần thiết, và đồng thời tăng cường hợp tác liên quốc gia ở các cấp hành động, chiến thuật và chiến lược.

Tại cấp khu vực, từ năm 2018, các nước ASEAN đã thảo luận các sáng kiến, cơ chế phối hợp trong xây dựng chính sách, hướng đến các bộ quy tắc, tiêu chuẩn chung về an

ninh mạng trong khu vực dựa trên các nguyên tắc và 11 chuẩn mực của Liên hợp quốc. Năm 2019, Hội nghị Bộ trưởng ASEAN về an ninh mạng đã nhất trí thiết lập một ủy ban công tác quan chức cấp cao tập trung vào xây dựng khuôn khổ hành động thực thi. Năm 2021, Đại hội đồng Liên nghị viện Hiệp hội các quốc gia Đông Nam Á lần thứ 42 (AIPA 42) tập trung vào tăng cường an ninh mạng, hướng tới không gian mạng tự cường trong ASEAN, thúc đẩy an ninh con người trong lĩnh vực kỹ thuật số bao trùm cho ASEAN, và tăng cường ngoại giao nghị viện hướng tới Cộng đồng ASEAN.

Thỏa thuận liên quốc gia:

Tại cấp tiểu đa phương, năm 2019, Mỹ đã đưa ra thông cáo chung thúc đẩy ứng xử có trách nhiệm của các quốc gia trên không gian mạng, gồm có 27 nước (5 đối tác Five Eyes, 18 trong số 28 nước thành viên EU, gồm cả Đức và Pháp), Nhật Bản, Hàn Quốc, Colômbia và Na Uy. Mục tiêu của Mỹ là nhằm củng cố, ủng hộ trật tự dựa trên luật lệ, khẳng định giá trị của luật pháp quốc tế trong việc điều chỉnh hành vi ứng xử giữa các nước. Các thỏa thuận đó có thể giúp các nước tự nguyện đưa ra và tuân thủ các chuẩn mực về hành vi ứng xử phù hợp của các quốc gia trong thời bình, giúp xây dựng lòng tin, giảm thiểu rủi ro xung đột, đồng thời giúp tăng cường năng lực hỗ trợ cho các nước tham gia thực thi khuôn khổ chung và bảo vệ mạng lưới của mình. Các nước tham gia khi thấy cần thiết có thể cùng nhau, trên tinh thần tự nguyện, yêu cầu các nước có hành động trái với khuôn khổ đã thỏa thuận phải có trách nhiệm giải trình về những ứng xử của mình, để từ đó các nước hướng tới thực hiện các biện

pháp bảo đảm tính minh bạch và tuân thủ luật pháp quốc tế, tránh các hành vi không lành mạnh¹.

Nhiều nước đã sớm nhận diện các thách thức về tội phạm mạng nên đã sớm thúc đẩy và giới thiệu các chuẩn mực bảo đảm an ninh mạng trong khuôn khổ chiến lược quốc gia, luật pháp và chính sách của nước mình. Các chiến lược này có một số đặc điểm chung: (i) Hòa hòa với các thỏa thuận quốc tế; (ii) Nhấn mạnh vai trò của chủ thể nhà nước trong việc triển khai, thực hiện các biện pháp nhằm bảo đảm an ninh mạng; (iii) Tập trung vào các biện pháp, công cụ chính trị, ngoại giao, hòa bình nhằm xây dựng niềm tin và giảm thiểu rủi ro. Tại cấp quốc gia, các chuẩn mực này được hướng tới lồng ghép trong các luật, chiến lược, chính sách của các nước. Chiến lược không gian mạng phải chi phối một chu trình khép kín không gian mạng bao gồm: (i) Giai đoạn chuẩn bị và ngăn ngừa (chuẩn bị về nhân sự, máy móc thiết bị để bảo vệ chống lại các nguy cơ mạng, thúc đẩy an ninh và tránh các công nghệ dễ tổn thương); (ii) Xác định nguy cơ nhanh nhất có thể; (iii) Phản ứng: Nhận diện và sửa chữa các nguyên nhân gây đứt gãy².

Vấn đề thiết lập các chuẩn mực về ứng xử của các quốc gia trên không gian mạng không đơn thuần là vấn đề kỹ thuật, là một lĩnh vực mới, là nơi diễn ra cạnh tranh gay gắt giữa các quốc gia. Việc thiết lập các ứng xử có trách nhiệm

1. Xem Dig.watch: “USA and 26 countries issue joint statêmnt on responsbile behaviour in cyberspace”, 2021, <https://dig.watch/updates/usa-and-26-countries-issue-joint-statement-responsible-behaviour-cyberspace>.

2. Xem Antonio Garcia Zaballo, Felix Gonzalez Herranz: “From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation”, Technical Note No. IDB-TN-588, 2013.

giữa các nhà nước là một phần trong nỗ lực thiết lập, định hình trật tự thế giới trong bối cảnh khoa học công nghệ có những bước tiến vượt bậc, làm nảy sinh nhiều vấn đề, rủi ro và chưa được quy định đầy đủ trong các thỏa thuận, chuẩn mực và luật lệ quốc tế. Mỹ sớm nhận định các rủi ro tiêu cực tiềm tàng có thể có trên không gian mạng, trong đó nghiêm trọng nhất là việc các hình thức xung đột truyền thống có xu hướng mở rộng phát triển trên không gian mạng. Vì vậy, từ năm 2011, Mỹ đã đưa ra Chiến lược quốc tế về không gian mạng nhằm phát triển quyền lực trên không gian mạng.

Tuy nhiên, trong khi hầu hết các nước đang tiếp tục tuân thủ luật pháp quốc tế hiện tại, như Hiến chương Liên hợp quốc, hay các công ước của Liên hợp quốc như Tuyên ngôn phổ quát về quyền con người, quyền dân sự và chính trị, Công ước Geneva về Bảo vệ nạn nhân chiến tranh, thì một số nước có phản ứng trái chiều với các thỏa thuận như vậy. Ví dụ, Trung Quốc đánh giá rằng những thỏa thuận đó phân chia không gian mạng thành hai thời điểm, đó là thời điểm hòa bình và thời điểm không hòa bình. Bên cạnh đó, với mong muốn trở thành cường quốc trên không gian mạng, tự do và độc lập với công nghệ nước ngoài, và viết lại quy tắc quản trị không gian mạng toàn cầu¹, Trung Quốc và Nga hợp tác chặt

1. Xem Sam Sacks: "Beijing Wants to Rewrite the Rules of the Internet", *The Atlantic*, June 18, 2018, <https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/>; (translation) "Xi Jinping: Accelerating the Independent Innovation of Network Information Technology and Making Unremitting efforts towards the goal of building a network power", *Xinhua*, October 9, 2016, http://www.xinhuanet.com/politics/2016-10/09/c_1119682204.htm.

chẽ với nhau ứng phó với các vấn đề về an ninh mạng, và cùng với một số nước đang bàn thảo để đưa ra các luật và chuẩn mực mới. Ví dụ, Tổ chức Hợp tác Thượng Hải (SCO) năm 2015 đề xuất Quy tắc hành xử quốc tế về an ninh thông tin; Trung Quốc đề xuất sáng kiến an ninh dữ liệu toàn cầu (2020), hay Nga đề xuất tại Đại hội đồng Liên hợp quốc (UNGA) dự thảo Công ước Liên hợp quốc về hợp tác phòng, chống tội phạm thông tin.

Sự tham gia của Việt Nam:

- Chính sách về an ninh mạng của Việt Nam:

Vấn đề an ninh mạng ngày càng trở thành vấn đề nhức nhối, cấp bách, ảnh hưởng không chỉ đến Chính phủ mà còn đến doanh nghiệp và người dân. Cùng với việc khoa học công nghệ, nhất là kỹ thuật số đóng vai trò quan trọng trong phát triển thì Việt Nam vẫn gặp nhiều thách thức lớn, nhất là khi Việt Nam là quốc gia có tỷ lệ nhiễm mã độc tống tiền cao nhất trong khu vực châu Á - Thái Bình Dương¹.

Nhận thức về sự cần thiết và quan trọng của việc xây dựng các quy tắc ứng xử có trách nhiệm trên không gian mạng nhằm góp phần duy trì một không gian mạng lành mạnh, an toàn và giúp cho việc bảo đảm an ninh, an toàn thông tin hiệu quả hơn², quan điểm của Việt Nam là ủng hộ

1. Xem News.microsoft.com: “Báo cáo của Microsoft: Việt Nam là quốc gia có tỷ lệ nhiễm mã độc tống tiền cao nhất châu Á - Thái Bình Dương năm 2019”, 2020, <https://news.microsoft.com/vi-vn/2020/06/24/bao-cau-cua-microsoft-viet-nam-la-quoc-gia-co-ty-le-nhiem-ma-doc-tong-tien-cau-nhat-chau-a-thai-binh-duong-nam-2019/>.

2. Xem “Hội nghị Bộ trưởng ASEAN về an ninh mạng lần thứ 5 (AMCC-5)”, <http://bocongan.gov.vn/tintuc/Pages/lists.aspx?Cat=20&ItemID=28915>.

khuôn khổ quốc tế, đưa ra các luật lệ và chuẩn mực về ứng xử có trách nhiệm của các nhà nước, nhằm bảo đảm hoạt động trên không gian mạng tuân thủ Hiến chương của Liên hợp quốc và luật pháp quốc tế. Quan điểm về các chuẩn mực ứng xử này là một phần trong chính sách đối ngoại của Việt Nam, và vì vậy góp phần bảo đảm các mục tiêu an ninh, phát triển đất nước và nâng cao vị thế của Việt Nam. Cụ thể:

Thứ nhất, Việt Nam hướng tới mục tiêu duy trì hòa bình, ổn định, bảo đảm an ninh thông qua tăng cường đối thoại, hợp tác quốc tế, tạo sự ổn định, giảm rủi ro xung đột với quan điểm nhìn nhận rằng an ninh mạng là một vấn đề toàn cầu. Với sự phát triển của Cách mạng công nghiệp lần thứ tư, đi kèm với các lợi ích về phát triển là sự lo ngại về vấn đề an ninh quốc tế, vấn đề an ninh mạng trở thành lĩnh vực an ninh quan trọng mà Việt Nam cần phải bảo vệ chủ quyền quốc gia, đoàn kết đất nước, chống lại các tội phạm xuyên quốc gia trên không gian mạng, các thông tin sai lệch. Nội dung các chuẩn mực của Liên hợp quốc cơ bản đều tương đồng với các nhu cầu thiết yếu của Việt Nam liên quan đến bảo đảm an ninh mạng, giúp tạo ra không gian mạng toàn cầu an toàn, hòa bình và phát triển cho mỗi nước¹, như bảo vệ kết cấu hạ tầng công nghệ thông tin - truyền thông, tăng cường hợp tác quốc tế, xây dựng niềm tin và trách nhiệm giải trình. Lãnh đạo đất nước sớm nhận thức an ninh mạng đe

1. Xem United Nations: “Explosive growth of digital technologies creating new potential for conflict, disarmament chief tells Security Council in first-ever debate on Cyberthreats”, 2021, <https://www.un.org/press/en/2021/sc14563.doc.htm>.

dọa đến hòa bình, an ninh, phát triển và thịnh vượng ở cấp quốc gia và toàn cầu, đòi hỏi phải có giải pháp toàn cầu và liên quốc gia đối phó với các cuộc tấn công mạng.

Thứ hai, các chuẩn mực ứng xử còn góp phần vào phục vụ sự phát triển của Việt Nam. Khoa học - công nghệ, trong đó kỹ thuật số, phát triển không gian mạng là một nhân tố thúc đẩy phát triển, tạo cơ hội cho những nước đi sau như Việt Nam bứt phá. Phải bảo vệ được kết cấu hạ tầng mạng thì mới có nền tảng và cơ sở để kết nối thông suốt, giảm khoảng cách số¹. Cùng với các chuẩn mực này, ở trong nước, Việt Nam đã đưa ra một trong những trọng tâm phát triển của Việt Nam là phát triển kinh tế số, hướng tới mục tiêu đạt 30% GDP đến năm 2030. Việt Nam cũng đạt năng lực cao về công nghệ thông tin, nhất là 5G, giúp cho việc tự chủ về công nghệ thông tin và vì vậy bảo vệ chủ quyền quốc gia trên không gian mạng.

Thứ ba, sự tham gia trong các chuẩn mực về ứng xử trên không gian mạng giúp Việt Nam tham gia có hiệu quả và trách nhiệm vào quá trình định hình, xây dựng các chuẩn mực và luật lệ quốc tế, phù hợp với những định hướng của Đại hội lần thứ XIII đề ra là tham gia vào quá trình định hình trật tự kinh tế - chính trị khu vực và quốc tế, giúp nâng cao vị thế, vai trò có trách nhiệm của Việt Nam đối với hòa bình, an ninh của khu vực và thế giới.

- Quá trình triển khai các chuẩn mực ứng xử của các quốc gia trên không gian mạng:

1. Xem European Council on Foreign Relations: “Europe’s digital sovereignty: From rulemaker to superpower in the age of US-China rivalry”, 2020, https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/.

Việt Nam đã thực hiện các chuẩn mực về ứng xử của các nhà nước trên không gian mạng thông qua việc:

+ Tham gia các thỏa thuận, chuẩn mực quốc tế, khu vực và song phương.

Ở cấp toàn cầu, Việt Nam đã thông qua Nghị quyết UNGA 70/237 của Liên hợp quốc về các chuẩn mực ứng xử có trách nhiệm của các nhà nước trên không gian mạng. Ở cấp khu vực, Việt Nam đã thông qua thông cáo của Hội nghị Bộ trưởng ASEAN về không gian mạng. Tại Hội nghị Bộ trưởng ASEAN về an ninh mạng lần thứ 5 (tháng 10/2020), Việt Nam cùng với các đối tác như Trung Quốc, Nga đồng tổ chức một phiên trong Diễn đàn An ninh ASEAN (ARF) tháng 4/2021, với chủ đề “*Chống tội phạm sử dụng công nghệ thông tin truyền thông*”. Bên cạnh đó, Việt Nam cũng đang tích cực tham gia xây dựng một khuôn khổ về chuẩn mực ứng xử của các nhà nước trong không gian mạng tương tự của Liên hợp quốc ở cấp ASEAN trong khuôn khổ Hội nghị Bộ trưởng ASEAN về an ninh mạng. Ở cấp song phương, Việt Nam đã tham gia đối thoại với các nước như Nhật Bản, Ấn Độ, Hàn Quốc, Xingapo về chủ đề chống tội phạm an ninh mạng. Ngoài ra, Chính phủ Việt Nam cũng đã rất cởi mở, khi một loạt bộ, ngành đã ký Biên bản ghi nhớ với Tập đoàn Microsoft về thúc đẩy sự phát triển của công nghệ thông tin tại Việt Nam trong những lĩnh vực như thúc đẩy an toàn mạng, nâng cao công tác bảo mật trong bối cảnh hiểm họa mất an toàn thông tin ngày càng tăng tại Việt Nam.

+ Nội luật hóa, xây dựng các chương trình, chính sách.

Việt Nam đã ban hành Luật an ninh mạng, thực hiện các biện pháp về an ninh mạng, tăng cường hợp tác với các nước,

bảo vệ các kết cấu hạ tầng quan trọng. Đồng thời, Việt Nam cũng đã lồng ghép các nội dung chính của các chuẩn mực về ứng xử trên không gian mạng vào các chiến lược, chương trình, kế hoạch ngành để thực hiện đồng bộ, có hệ thống. Đặc biệt, Việt Nam đã phê duyệt Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030, phát triển chính phủ điện tử, kết nối và chia sẻ dữ liệu, và chú trọng phòng, chống tội phạm mạng.

+ Thiết lập thể chế, tổ chức thực hiện.

Việt Nam đã sớm thiết lập cơ chế phối hợp liên ngành gồm nhiều bộ, ngành khác nhau trong quá trình tham gia và thực hiện các thỏa thuận khu vực và quốc tế. Chủ thể chính thực hiện các cam kết của Việt Nam liên quan đến chuẩn mực ứng xử của các nhà nước trong không gian mạng là Chính phủ. Các bên liên quan chính là Bộ Ngoại giao, Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Tư pháp, Bộ Khoa học và Công nghệ, Bộ Quốc phòng.

+ Tuyên truyền, nâng cao nhận thức, trình độ, năng lực.

Các bộ, ngành, nhất là Bộ Công an đã chú trọng đào tạo, nâng cao trình độ, năng lực cho lực lượng chuyên trách bảo vệ an ninh mạng và tăng cường tiềm lực an ninh mạng để bảo vệ các kết cấu hạ tầng thông tin trọng yếu.

Quá trình tham gia và thực hiện các chuẩn mực về ứng xử trong lĩnh vực an ninh mạng đem lại cả cơ hội và thách thức cho Việt Nam. Một mặt, việc tham gia đàm phán, xây dựng các chuẩn mực về an ninh mạng ở cấp khu vực và quốc tế giúp Việt Nam xây dựng hình ảnh một thành viên có trách nhiệm và chủ động, tích cực trong cộng đồng quốc tế. Đồng thời, việc triển khai các chuẩn mực về an ninh

mạng ở cấp quốc gia cũng giúp nâng cao nhận thức của người dân, chuẩn hóa các hành vi ứng xử, và giúp môi trường an ninh mạng an toàn hơn. Mặt khác, Việt Nam cũng đứng trước nhiều thách thức, nhất là trong bối cảnh có nhiều sáng kiến nổi lên liên quan đến an ninh công nghệ thông tin và không gian mạng ở các cấp khác nhau, từ các quốc gia có quan điểm xung đột nhau. Trước tình trạng “phân tách” về công nghệ thông tin và an ninh mạng, các quyết sách của Việt Nam trong lĩnh vực công nghệ, an ninh mạng cần được xây dựng hiệu quả, phù hợp với lợi ích quốc gia, tránh dấy lên những nghi ngại rằng Việt Nam đang nghiêng về một bên, nhất là trong lĩnh vực công nghệ. Bài toán đặt ra cho Việt Nam là phải cân bằng trong quan hệ giữa các nước, minh bạch thông tin và bảo đảm bảo vệ lợi ích quốc gia.

3. Khuyến nghị cho Việt Nam

Đại hội đại biểu toàn quốc lần thứ XIII của Đảng đã đưa ra những định hướng lớn về vấn đề an ninh, quốc phòng cũng như hợp tác về chính trị trong lĩnh vực an ninh, trong đó có an ninh mạng. Nhận định các vấn đề như an ninh mạng “ngày càng tác động mạnh, nhiều mặt, đe dọa nghiêm trọng đến sự phát triển ổn định, bền vững của thế giới, khu vực và đất nước ta”¹, Nghị quyết Đại hội lần thứ XIII của Đảng đã đưa ra định hướng phát triển đất nước giai đoạn 2021 - 2030: “Giữ vững an ninh chính trị, bảo đảm trật tự, an toàn xã hội,

1. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.I, tr.31.

an ninh con người, an ninh kinh tế, an ninh mạng, xây dựng xã hội trật tự, kỷ cương”¹.

Trên cơ sở đó, một số khuyến nghị được đưa ra để thúc đẩy việc thực hiện các chuẩn mực ứng xử của các nhà nước trên không gian mạng, góp phần thúc đẩy tăng cường hợp tác về an ninh mạng nói riêng và hội nhập quốc tế về quốc phòng, an ninh, chính trị nói chung như sau:

- Tiếp tục thúc đẩy việc xây dựng, định hình một thỏa thuận ở cấp khu vực - ASEAN về không gian mạng trên cơ sở tham gia có hiệu quả ở cấp toàn cầu về vấn đề an ninh mạng, và trên cơ sở thực hiện tốt các chuẩn mực của Liên hợp quốc.

- Tiếp tục triển khai thực hiện các chuẩn mực ứng xử này thông qua việc xây dựng, thiết lập các luật lệ, quy định, thể chế hóa, nội luật hóa.

- Tiếp tục xây dựng các đề án, chương trình, kế hoạch thực hiện các chuẩn mực, để lồng ghép các chuẩn mực này vào các chương trình ngành, phát triển kinh tế - xã hội, phù hợp với định hướng Đại hội XIII.

- Tiếp tục tham gia vào quá trình định hình các thể chế, định chế, quản trị, luật lệ khu vực và quốc tế liên quan đến ứng xử của các nhà nước trên không gian mạng; đẩy mạnh việc ký kết các thỏa thuận, khung hợp tác song phương với các đối tác quan trọng chiến lược, nhất là những nước đi đầu trong việc thiết lập các luật lệ, nhằm bảo đảm lợi ích quốc gia, góp phần giữ vững hòa bình, an ninh khu vực và quốc tế.

1. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.II, tr.331.

- Tăng cường nâng cao năng lực, tuyên truyền nâng cao nhận thức về tầm quan trọng của các chuẩn mực về ứng xử trên không gian mạng.

*

* *

Vấn đề ứng xử có trách nhiệm trên không gian mạng của các nhà nước là một trong những vấn đề cơ bản nhằm bảo đảm an toàn, an ninh, chủ quyền lãnh thổ trên không gian mạng. Việt Nam đã và đang tiếp tục khẳng định cam kết hướng tới xây dựng không gian mạng mở, hòa bình và an toàn thông qua việc tham gia vào các chuẩn mực về ứng xử mà Liên hợp quốc đã đưa ra. Vấn đề đặt ra là triển khai hiệu quả các chuẩn mực này trong thời gian tới. Để thực hiện được điều này, Việt Nam sẽ cần tích cực xây dựng niềm tin, tăng cường hợp tác quốc tế để chia sẻ và học hỏi các kinh nghiệm trên thế giới, nhất là trong bối cảnh dịch chuyển địa - chính trị, đa dạng về lợi ích chính trị và quan điểm của các nước. Ngoài ra, Việt Nam cũng cần lồng ghép, xây dựng các chuẩn mực này trong các văn bản pháp luật, chiến lược, chính sách nhằm bảo đảm sự thống nhất trong nhận thức và hành động giữa các cấp chính quyền và địa phương. Bên cạnh đó, cần phải tiếp tục huy động sự tham gia tích cực của khu vực tư nhân, các học giả cũng như các chuyên gia, nhất là khi các chuẩn mực này ảnh hưởng và liên quan rất rộng đến nhiều đối tượng và lĩnh vực.

VỀ CHỦ QUYỀN KHÔNG GIAN MẠNG TRONG QUAN HỆ QUỐC TẾ CỦA TRUNG QUỐC VÀ KINH NGHIỆM THAM KHẢO CHO VIỆT NAM

TS. NGUYỄN VIỆT LÂM*

Trong những năm qua, bên cạnh vấn đề an ninh mạng trong quan hệ quốc tế thì vấn đề chủ quyền không gian mạng là một trong những nội dung ưu tiên trong chiến lược, chính sách quan trọng, trong đó bao gồm việc xây dựng Trung Quốc trở thành cường quốc trong không gian mạng. Đây là vấn đề mới, thu hút sự quan tâm của cộng đồng quốc tế, đặc biệt trong bối cảnh Trung Quốc và Mỹ gia tăng cạnh tranh toàn diện về nhiều mặt, đặc biệt là cạnh tranh công nghệ. Do vậy, việc tìm hiểu, làm rõ quan điểm và triển khai trong thực tiễn của Trung Quốc về chủ quyền không gian mạng sẽ là những kinh nghiệm tham khảo hữu ích cho Việt Nam, phục vụ công tác bảo vệ chủ quyền và các lợi ích quốc gia - dân tộc của Việt Nam trên không gian mạng và bảo vệ Tổ quốc Việt Nam xã hội chủ nghĩa trong thời đại mới.

* Phái đoàn đại diện thường trực Việt Nam tại Liên hợp quốc, New York, Hoa Kỳ.

Trong quan hệ quốc tế đương đại, chủ quyền quốc gia bao gồm một số nội dung chính, như: mọi nhà nước đều bình đẳng về mặt pháp luật; mỗi nhà nước đều phải tôn trọng thực tế thực thể pháp lý của các nhà nước khác; tính toàn vẹn lãnh thổ và độc lập chính trị của mỗi nhà nước là bất khả xâm phạm; mỗi nhà nước phải thực hiện các nghĩa vụ pháp lý quốc tế của mình và chung sống hòa bình với các nhà nước khác; mỗi nhà nước có quyền lựa chọn và phát triển các hệ thống chính trị, kinh tế, văn hóa, xã hội của riêng mình¹.

1. Về chủ quyền không gian mạng ở Trung Quốc

Khái niệm “không gian mạng” (Cyberspace) có thể được coi là sự kết hợp của mạng (Cyber) và không gian (Space). Trong số đó, “Cyber - mạng” liên quan đến các thuộc tính kỹ thuật và tập trung vào các hình thức khác nhau trong trình độ công nghệ thông tin. “Space - không gian” liên quan đến các thuộc tính xã hội và tập trung vào những người sử dụng mạng và cách mà họ sử dụng không gian mạng. Do đó, không gian mạng không chỉ tham gia vào thế giới số vì sự lưu thông của thông tin, mà còn trong thế giới thực vì có

1. Một điểm đáng lưu ý ở đây là chủ quyền quốc gia không đồng nghĩa với quyền lực vô hạn và vô điều kiện của quốc gia. Các quốc gia có thể có các nghĩa vụ quốc tế, nhất là khi tham gia vào các điều ước quốc tế. Mặc dù các quốc gia có quyền lựa chọn có tham gia vào các điều ước này, hay không, nhưng một khi đã tham gia vào các điều ước, họ buộc phải tuân thủ các nghĩa vụ và trao lại một phần chủ quyền của mình cho cộng đồng quốc tế. Xem Đào Minh Hồng - Lê Hồng Hiệp: *Thuật ngữ quan hệ quốc tế*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2018, tr.121.

liên quan đến người sử dụng và cách hành xử của họ trong không gian mạng¹.

Từ góc độ lý thuyết, giới nghiên cứu của Trung Quốc trong những năm qua cho rằng chủ quyền quốc gia là một khái niệm đang phát triển. Sự phát triển của công nghệ hàng hải trong thế kỷ XVII đã biến lãnh hải trở thành một bộ phận thuộc chủ quyền quốc gia; sự tiến bộ của công nghệ hàng không vào đầu thế kỷ XX đã biến quyền vùng trời trở thành một bộ phận của chủ quyền quốc gia; sự phát triển nhanh chóng của công nghệ internet khiến chủ quyền quốc gia đương nhiên mở rộng ra không gian mạng. Dịch vụ thông tin có thể vượt qua biên giới quốc gia, nhưng không gian mạng không thể không có chủ quyền². Bên cạnh đó, các học giả Trung Quốc cũng coi những quốc gia có chủ quyền là những chủ thể chính trong việc thực hiện các hoạt động và duy trì trật tự trong không gian mạng. Nguyên tắc bình đẳng chủ quyền được ghi trong Hiến chương Liên hợp quốc là một quy phạm cơ bản điều chỉnh các mối quan hệ quốc tế đương đại, gồm tất cả các khía cạnh của mối quan hệ giữa các nhà nước, luật lệ, cũng được áp dụng cho không gian mạng. Tuy nhiên, vẫn còn các cách hiểu khác nhau và thực tiễn

1. Xem Fang BinXing: Cybersapce Sovereignty, Reflections on Building a Community of Common Future in Cyberspace, Sience Press Beijing and Springer Nature Singapore Pte Ltd, 2018, tr.1.

2. Phát biểu của Lu Wei, Giám đốc Văn phòng thông tin internet quốc gia Trung Quốc tại Hội nghị bàn tròn giữa Trung Quốc và Hàn Quốc năm 2013, xem thêm 安全决定成败 发展引领未来 (An toàn quyết định sự thành công hay thất bại, sự phát triển dẫn dắt tương lai) http://www.xinhuanet.com//world/2013-12/10/c_125838121.htm.

triển khai xung quanh vấn đề này. Các học giả Trung Quốc cho rằng, để tạo điều kiện thuận lợi cho quản trị internet toàn cầu công bằng và bình đẳng hơn cũng như xây dựng một cộng đồng chung trong không gian mạng vì lợi ích chung của nhân loại, cộng đồng quốc tế cần tuân thủ và thực hành khái niệm chủ quyền trong không gian mạng trên cơ sở phù hợp với các nguyên tắc tham vấn bình đẳng, gạt bỏ khác biệt và tìm kiếm điểm chung tối đa¹.

Từ góc độ thực tiễn, giới nghiên cứu và các cơ quan của Trung Quốc thời gian qua tích cực đưa ra những lập luận cơ sở thực tiễn trên thế giới thông qua các tuyên bố, văn kiện các hội nghị quốc tế trong những năm qua có nội dung liên quan đến không gian mạng, an ninh mạng, trong đó có chủ quyền không gian mạng. Ví dụ như Tuyên bố về các nguyên tắc của Hội nghị thượng đỉnh thế giới về xã hội thông tin (WSIS) diễn ra vào năm 2003, tại Geneva (Thụy Sĩ); Báo cáo năm 2015 và năm 2021 của Nhóm các chuyên gia chính phủ của Liên hợp quốc (UN GGE); Hội nghị thượng đỉnh Nhóm các nền kinh tế phát triển và mới nổi hàng đầu thế giới (G-20) năm 2015; Tuyên bố Goa của Hội nghị thượng đỉnh Nhóm các nền kinh tế mới nổi (BRICS) năm 2016...

Trên cơ sở đó, Trung Quốc cho rằng chủ quyền không gian mạng đề cập các quyền tài phán quốc gia đối với kết cấu hạ tầng công nghệ thông tin và truyền thông đến mọi hoạt

1. Xem Sovereignty in Cyberspace Theory and Practice (Version 2.0), truy cập ngày 25/11/2020, https://www.wicwuzhen.cn/web20/information/release/202011/t20201125_21724588.shtml.

động mà con người tiến hành trên kết cấu hạ tầng đó. Chủ quyền không gian mạng bao gồm các hình thức chủ quyền như chủ quyền dữ liệu, chủ quyền thông tin, chủ quyền không gian điện tử và chủ quyền kỹ thuật¹. Chủ quyền không gian mạng gồm bốn yếu tố, bốn quyền cơ bản và bốn nguyên tắc cơ bản. *Bốn yếu tố* là: (i) công nghệ thông tin truyền thông hỗ trợ sự tồn tại của không gian mạng; (ii) dữ liệu được tạo ra, lưu trữ, xử lý, truyền và trình chiếu trong hệ thống công nghệ thông tin truyền thông; (iii) các vai trò của mạng truyền và xử lý dữ liệu; và (iv) kiểm soát các nguyên tắc xử lý và truyền dữ liệu. *Các quyền cơ bản* gồm: (i) quyền độc lập về không gian mạng, tức là kết cấu hạ tầng không gian mạng được đặt trên lãnh thổ Trung Quốc hoạt động một cách tự chủ và không thể bị can thiệp bởi các quốc gia; (ii) bình đẳng trên không gian mạng, tức là mọi quốc gia đều có địa vị quản trị bình đẳng trong kết nối mạng quốc tế và nhà nước có quyền tự vệ trên không gian mạng để bảo vệ không gian mạng của họ không bị xâm phạm; (iii) quyền tài phán trên không gian mạng, tức là các cơ sở cấu thành không gian mạng và dữ liệu của chúng được bảo vệ bởi quyền tài phán quốc gia. *Bốn nguyên tắc cơ bản* gồm: (i) tôn trọng chủ quyền không gian mạng của tất cả mọi người ở các quốc gia; (ii) mọi quốc gia không vi phạm không

1. Chủ quyền dữ liệu đề cập quyền sở hữu và định đoạt dữ liệu; chủ quyền thông tin đề cập quyền công bố thông tin; chủ quyền không gian điện tử đề cập để kiểm soát không gian điện tử của nhà nước; chủ quyền kỹ thuật đề cập sự tự chủ, tự định hướng và phát triển độc lập của công nghệ. Xem Fang BinXing, *Tlđđ*, tr.357.

gian mạng của các quốc gia khác; (iii) mọi quốc gia không can thiệp vào hoạt động quản lý không gian mạng của các quốc gia khác; (iv) chủ quyền không gian mạng của tất cả các quốc gia có vị thế bình đẳng trong quản trị không gian mạng quốc tế các hoạt động¹.

2. Tại sao Trung Quốc thúc đẩy chủ quyền không gian mạng?

Bên cạnh các nguyên nhân lý giải cho việc Trung Quốc thúc đẩy nội dung chủ quyền không gian mạng, xin nêu ba nguyên nhân chính liên quan đến chính trị, đối ngoại như sau:

Thứ nhất, chủ quyền không gian mạng gắn liền với an ninh quốc gia của Trung Quốc. Chủ tịch nước Trung Quốc Tập Cận Bình đã khẳng định: “Không thể có an ninh quốc gia nếu không có an ninh mạng, internet và an ninh thông tin đã trở thành thách thức mới đối với Trung Quốc vì cả hai đều gắn liền với an ninh quốc gia và ổn định xã hội”². Bộ Quốc phòng Trung Quốc cũng xác định: “không gian mạng đã trở thành một trụ cột mới cho phát triển kinh tế - xã hội”³. Do đó, những năm gần đây, Trung Quốc chủ động tham gia

1. Xem Fang BinXing, *Tlđđ*, tr.321.

2. Phát biểu của Chủ tịch nước Trung Quốc Tập Cận Bình tại Hội nghị thành lập Tiểu tổ chỉ đạo giám sát an ninh internet và phát triển công nghệ thông tin Trung ương Trung Quốc, <https://baotintuc.vn/the-gioi/ong-tap-can-binh-lam-to-truong-giam-sat-an-ninh-mang-20140228172333746.htm>.

3. Xem Hoàng Duy Long: “Tác chiến mạng: “Lực lượng hỗ trợ chiến lược” của Trung Quốc”, <https://tuoitre.vn/tac-chien-mang-luc-luong-ho-tro-chien-luoc-cua-trung-quoc-20180321114242903.htm>.

và thúc đẩy vai trò lớn hơn trong quản trị internet toàn cầu, kêu gọi các quốc gia tôn trọng “chủ quyền không gian mạng” của Trung Quốc với ý tưởng các quốc gia nên tự do kiểm soát và kiểm duyệt kết cấu hạ tầng internet của mình nếu thấy phù hợp¹.

Thứ hai, giới nghiên cứu Trung Quốc cho rằng, một trong những quan ngại chính của các nước đang phát triển là các quốc gia mạnh về internet có khả năng trở thành độc quyền về mức giá đối với các quốc gia yếu về không gian mạng thông qua việc thiết lập bá quyền cũng như độc quyền trong không gian mạng về tài nguyên và công nghệ cốt lõi, do đó các nước này sẽ cướp bóc và khai thác nền kinh tế của quốc gia yếu về không gian mạng; bằng cách phủ nhận chủ quyền không gian mạng và chống lại các quy định nội dung thông tin².

Thứ ba, chủ quyền không gian mạng là cách giúp các nước đang phát triển chống lại sự bá quyền, độc quyền trong không gian mạng. Giới nghiên cứu Trung Quốc lập luận rằng các nước đang phát triển³ mong muốn có một trật tự không gian mạng mới khi ngày càng lo ngại việc các nước lớn bá chủ toàn cầu trong môi trường internet sẽ dễ dẫn đến các nguy cơ vi phạm các quyền văn hóa và lợi ích của các quốc gia khác, thực hiện xâm nhập hệ tư tưởng, can thiệp vào các vấn đề đối nội của quốc gia hoặc thậm chí để thực hiện chủ nghĩa thực

1. Phát biểu của Chủ tịch nước Trung Quốc Tập Cận Bình tại Hội nghị thế giới về internet năm 2015, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml.

2. Xem Fang BinXing, *Tlđđ*, tr.124-125.

3. Trung Quốc lâu nay vẫn khẳng định là một quốc gia đang phát triển.

dân mạng, là nguyên nhân khiến các quốc gia đang phát triển phụ thuộc vào các quốc gia có internet mạnh mẽ về chính trị và nền kinh tế, và làm tổn hại đến quyền và lợi ích lâu dài của họ¹. Tuy nhiên, cũng có ý kiến của học giả phương Tây cho rằng Trung Quốc thúc đẩy chủ quyền không gian mạng là muốn thực hiện Chiến lược trở thành cường quốc trong không gian mạng được thể hiện qua cụm từ 络强国² (cường quốc mạng) trong các phát biểu ở trong nước của lãnh đạo Trung Quốc về Chiến lược công nghệ thông tin truyền thông của nước này từ năm 2014³.

Thực tiễn triển khai, thúc đẩy chủ quyền không gian mạng của Trung Quốc thời gian qua:

Chủ tịch Trung Quốc Tập Cận Bình là lãnh đạo đầu tiên trên thế giới đưa ra khái niệm về chủ quyền không gian mạng trên thế giới⁴. Từ năm 2014 đến nay, Trung Quốc cũng đề cập rất nhiều lần về nội dung này trong các bài phát biểu

1. Xem Fang BinXing, *Tlđđ*, tr. 124-125.

2. Năm 2014, thuật ngữ “cường quốc mạng” lần đầu tiên trở nên nổi bật trong thời gian diễn ra cuộc họp đầu tiên của nhóm Tiểu tổ chỉ đạo giám sát an ninh internet và phát triển công nghệ thông tin Trung ương Trung Quốc do Chủ tịch Tập Cận Bình đứng đầu (xem Lexicon: 络强国, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/> và “Ông Tập Cận Bình làm tổ trưởng giám sát an ninh mạng”, <https://baotintuc.vn/the-gioi/ong-tap-can-binh-lam-to-truong-giam-sat-an-ninh-mang-20140228172333746.htm>).

3. Xem China as a “cyber great power”: Beijing’s two voices in telecommunications, xem <https://www.brookings.edu/research/china-as-a-cyber-great-power-beijings-two-voices-in-telecommunications/>, truy cập ngày 18/8/2021.

4. Xem Fang BinXing, *Tlđđ*, tr.171.

của lãnh đạo và các cơ quan chính phủ ở các cấp, trong các văn bản pháp quy, văn bản luật, các quy định trong nước cũng như tài liệu quốc tế và các hiệp định song phương..., trong đó thể hiện rất rõ nội hàm về chủ quyền không gian mạng. Cụ thể như sau:

Ở cấp độ toàn cầu: Những năm qua, Trung Quốc tập trung thúc đẩy nội dung chủ quyền không gian mạng là một nguyên tắc quản trị internet tại các diễn đàn Liên hợp quốc¹ và các diễn đàn đa phương khác. Trung Quốc mong muốn biến Liên hợp quốc thành cơ quan chính trong điều chỉnh các vấn đề không gian mạng và giảm bớt vai trò của Tổ chức quản lý Tên và địa chỉ mạng quốc tế (ICANN). Ví dụ, tháng 8/2017, các nhà ngoại giao Trung Quốc tại Liên hợp quốc đã thể hiện quan điểm của Trung Quốc về vai trò của Liên hợp quốc trong quản trị internet qua một tài liệu. Tài liệu nêu rõ: “Trung Quốc sẽ tiếp tục ủng hộ Liên hợp quốc với tư cách là kênh chính trong việc bảo vệ an ninh mạng quốc tế, thiết lập trật tự và phát triển các quy tắc quốc tế về không gian mạng”². Bên cạnh đó, Trung Quốc cũng tập trung xây dựng

1. Cách tiếp cận đa phương ở Liên hợp quốc của Trung Quốc về thúc đẩy nội dung chủ quyền không gian mạng có hai lợi ích cho Bắc Kinh: Thứ nhất, cách này ưu tiên lợi ích của các chính phủ hơn lợi ích của các công ty công nghệ và các nhóm xã hội dân sự. Thứ hai, Trung Quốc có nhiều cơ hội trong vận động phiếu bầu của các nước đang phát triển, trong đó nhiều nước cũng muốn kiểm soát internet và luồng thông tin tự do.

2. Colum Lynch and Elias Groll: “As U.S. Retreats from World Organizations, China Steps In to Fill the Void”, *Foreign Policy*, October 6, 2017, <https://foreignpolicy.com/2017/10/06/as-u-s-retreats-from-world-organizations-china-steps-in-the-fill-the-void>.

đồng minh và các đối tác có cùng quan điểm để đối phó với sự thống trị của Mỹ và phương Tây trên không gian mạng¹.

Trước đó, Báo cáo năm 2015 và năm 2021 (có sự đồng thuận của Trung Quốc) của Nhóm các chuyên gia chính phủ của Liên hợp quốc (UN GGE) cho rằng chủ quyền quốc gia và các chuẩn mực, nguyên tắc quốc tế xuất phát từ chủ quyền áp dụng cho hành vi của các quốc gia có hoạt động liên quan đến công nghệ thông tin - truyền thông và quyền tài phán của họ đối với kết cấu hạ tầng công nghệ thông tin - truyền thông trong lãnh thổ của họ, đồng thời khẳng định hiện có các quy định của luật pháp quốc tế được áp dụng cho những hoạt động liên quan đến lĩnh vực công nghệ thông tin - truyền thông của các quốc gia².

Trong thương thảo Báo cáo của Nhóm công tác mở về an ninh mạng (OEWG) của Liên hợp quốc từ năm 2020 đến tháng 5/2021, Trung Quốc luôn thúc đẩy các nội dung liên quan đến chủ quyền không gian mạng qua các phát biểu, đóng góp của mình, tập trung vào bốn điểm gồm: (i) các quốc

1. Fang Binxing được coi là cha đẻ của Bức tường lửa của Trung Quốc, trong bài phát biểu năm 2016 tại Diễn đàn Trung - Nga về chủ quyền internet, cho rằng hầu hết cơ sở hạ tầng internet được đặt tại Mỹ, điều đó có nghĩa là quản trị internet ngày nay được đặt dưới sự kiểm soát của Mỹ. The Chinese Cyber Sovereignty Concept (Part 2), <https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-2/>, truy cập ngày 08/8/2021.

2. Xem Michael Schmitt: "The Sixth United Nations GGE and International Law in Cyberspace", truy cập ngày 10/6/2021, <https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/>.

gia nên thực hiện quyền tài phán đối với kết cấu hạ tầng công nghệ thông tin - truyền thông, các nguồn lực cũng như các hoạt động liên quan đến công nghệ thông tin - truyền thông trong lãnh thổ của mình; (ii) các quốc gia có quyền đưa ra các chính sách công liên quan đến công nghệ thông tin - truyền thông phù hợp với hoàn cảnh quốc gia để quản lý các vấn đề công nghệ thông tin - truyền thông của riêng mình và bảo vệ lợi ích hợp pháp của công dân trong không gian mạng; (iii) các quốc gia nên hạn chế sử dụng công nghệ thông tin - truyền thông để can thiệp vào công việc nội bộ của các quốc gia khác và phá hoại sự ổn định chính trị, kinh tế và xã hội của quốc gia đó; (iv) các quốc gia nên tham gia vào việc quản lý và phân phối các tài nguyên internet quốc tế trên nguyên tắc bình đẳng. Báo cáo sau đó được thông qua vào tháng 5/2021, tuy không đề cập nội dung chủ quyền không gian mạng, nhưng Bản tóm tắt của Chủ tịch Nhóm (kèm theo Báo cáo) có nêu quan điểm trên của Trung Quốc và một số nước khác đối với việc áp dụng một số nguyên tắc cụ thể của luật quốc tế trong đó có “chủ quyền quốc gia, bình đẳng chủ quyền đối với việc duy trì hòa bình, ổn định và thúc đẩy môi trường công nghệ thông tin - truyền thông hòa bình, dễ tiếp cận, an toàn, ổn định và mở rộng...”¹.

Ngoài ra, lãnh đạo Trung Quốc sử dụng các hội nghị quốc tế về internet, công nghệ là nơi để thúc đẩy nội dung về chủ

1. Ghi chú của Chủ tịch OEWG, ban hành kèm theo Báo cáo của OEWG về ICT <https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf>.

quyền không gian mạng¹. Tháng 12/2015, trong bài phát biểu khai mạc Hội nghị Internet thế giới ở Wuzhen, Chủ tịch Tập Cận Bình đã đưa ra bốn nguyên tắc và năm kiến nghị, trong đó nguyên tắc đầu tiên là “tôn trọng chủ quyền không gian mạng”; cho rằng nguyên tắc chủ quyền được quy định trong Hiến chương Liên hợp quốc bao gồm tất cả các lĩnh vực trong mối quan hệ giữa các quốc gia với nhau, trong đó có không gian mạng; nhấn mạnh không có quốc gia nào được theo đuổi cường quyền mạng, can thiệp vào công việc nội bộ của các nước khác hay can thiệp, ủng hộ các hoạt động mạng mà phá hoại an ninh quốc gia của các quốc gia khác². Năm 2017, Hội nghị này thu hút sự tham dự và phát biểu của Giám đốc điều hành các tập đoàn công nghệ lớn trên thế giới như Tim Cook của Apple, Chuck Robbins của Cisco và Sundar Pichai của Google. Tại các hội nghị gần đây, Trung Quốc thúc đẩy khái niệm mà Chủ tịch Tập Cận Bình đưa ra năm 2015, đó là về xây dựng một cộng đồng có chung vận mệnh trong không gian mạng. Khái niệm tổng thể này gắn với chủ quyền, nhấn mạnh sự bình đẳng của tất cả các chủ thể nhà nước, và bao gồm các vấn đề như: bắc cầu phân chia kỹ thuật số, thúc đẩy thương mại điện tử và tạo điều kiện thuận lợi cho luồng dữ liệu xuyên biên giới.

1. Chủ tịch Tập Cận Bình phát biểu tại WIC năm 2015, năm 2016, tại Hội nghị chuyên đề về an ninh mạng và ứng dụng thông tin (2016), tại Quốc hội Braxin (2014).

2. Xem Xi Jinping's speech at the opening ceremony of the second World Internet Conference (full text), https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml, truy cập ngày 21/8/2021.

Các văn kiện như Tuyên bố của các cuộc họp của Nhóm các nền kinh tế mới nổi BRICS (gồm Braxin, Nga, Ấn Độ, Trung Quốc và Nam Phi) cũng nhấn mạnh chủ quyền như một nguyên tắc chính của luật pháp quốc tế và sự ủng hộ của nhóm đối với một tiến trình đa phương mở bao gồm tất cả các quốc gia và công nhận tất cả các nhu cầu và lợi ích của các quốc gia. Ví dụ: Tuyên bố Hạ Môn năm 2017 nhấn mạnh tầm quan trọng hàng đầu của các nguyên tắc luật pháp quốc tế được ghi trong Hiến chương Liên hợp quốc, đặc biệt là chủ quyền quốc gia, độc lập chính trị, toàn vẹn lãnh thổ và bình đẳng chủ quyền của các quốc gia, không can thiệp vào nội bộ. Năm 2018, BRICS cũng tuyên bố sẽ hoạt động để thúc đẩy một mạng internet toàn cầu mở, an toàn, không phân mảnh.

Ở cấp độ khu vực: Trung Quốc thúc đẩy nội dung chủ quyền không gian mạng để củng cố vị thế trong khu vực và củng cố vai trò lãnh đạo của mình trong các nhóm quốc gia đang phát triển. Năm 2009, các thành viên Tổ chức Hợp tác Thượng Hải (SCO) ký một thỏa thuận xác định các lĩnh vực hợp tác trong lĩnh vực an ninh thông tin, bao gồm việc tạo ra một hệ thống giám sát chung các mối đe dọa mạng, xây dựng các quy định trong luật pháp quốc tế để hạn chế “việc phát tán và sử dụng vũ khí thông tin đe dọa năng lực quốc phòng, an ninh quốc gia và an toàn công cộng”, chống tội phạm mạng và sử dụng công nghệ thông tin - truyền thông để chống khủng bố, đào tạo và tập trận chung. Năm 2011 và năm 2015, Đại hội đồng Liên hợp quốc thông qua Bộ quy tắc ứng xử quốc tế về an ninh thông tin do Trung Quốc, Nga và các thành viên SCO đề xuất, trong đó đều nhấn mạnh quyền chủ quyền của các quốc gia và xác định chủ quyền là nguyên

tắc xác định của luật pháp quốc tế và tái khẳng định thẩm quyền chính sách đối với các vấn đề chính sách công liên quan đến internet là quyền chủ quyền của các quốc gia.

Ở cấp độ quốc gia: Về xây dựng thể chế và triển khai chính sách, Trung Quốc tập trung xây dựng và hoàn thiện nhiều văn bản, chính sách về không gian mạng, an ninh mạng, trong đó có nội dung chủ quyền không gian mạng¹. Đáng chú ý là Luật an ninh mạng năm 2016 của Trung Quốc bao gồm 79 điều và 7 chương, tập trung vào các nội dung quan trọng, như bảo vệ chủ quyền không gian mạng quốc gia, bảo vệ kết cấu hạ tầng thiết yếu, dữ liệu và bảo vệ thông tin cá nhân. Việc địa phương hóa dữ liệu được coi là thành tố quan trọng góp phần bảo vệ và gìn giữ chủ quyền không gian mạng của Trung Quốc. Năm 2017, Trung Quốc ban hành Chiến lược an ninh không gian mạng quốc gia đã xác định 9 nhiệm vụ cụ thể, trong đó có nội dung bảo vệ chủ quyền không gian mạng². Bên cạnh đó, việc ban hành Luật bảo vệ thông tin cá nhân (tháng 8/2021), cùng với Luật an ninh mạng (2016) và Luật an toàn dữ liệu (tháng 8/2021) đã hoàn thành bộ ba cơ chế quản lý dữ liệu nền tảng của Trung Quốc và sẽ mở ra một kỷ nguyên mới về tuân thủ dữ liệu cho các

1. Sách trắng về internet của Trung Quốc (2010), Chiến lược không gian mạng quốc gia (tháng 12/2016), Chiến lược hợp tác quốc tế về không gian mạng (tháng 3/2017), Dự thảo Chiến lược thông tin hóa quốc gia.

2. (1) bảo vệ chủ quyền không gian mạng; (2) bảo vệ an ninh quốc gia; (3) bảo vệ hạ tầng thông tin then chốt; (4) tăng cường xây dựng văn hóa mạng; (5) tấn công tội phạm mạng và phần tử khủng bố mạng; (6) hoàn thiện hệ thống quản lý mạng; (7) xây dựng nền tảng an ninh mạng vững chắc; (8) nâng cao khả năng bảo vệ không gian mạng; và (9) tăng cường hợp tác quốc tế trong lĩnh vực không gian mạng.

công ty công nghệ, đồng thời nhằm tạo ra cơ chế quản lý internet của Trung Quốc trong tương lai. Sự phát triển của các thể chế, luật và hướng dẫn mới về an ninh mạng và khả năng cạnh tranh công nghệ ngày càng tăng của các công ty công nghệ Trung Quốc đã giúp làm tăng khả năng chủ quyền trên không gian mạng. Các công ty Trung Quốc hiện đang là đối tác công nghệ quan trọng dọc theo các tuyến đường BRI và ở Đông Âu, và họ có vai trò lớn hơn trong các tổ chức tiêu chuẩn quốc tế. Về các nội dung liên quan đến tiêu chuẩn, kỹ thuật công nghệ, Trung Quốc tập trung xây dựng tên miền tiếng Trung riêng, và tên miền .cn để giảm sự phụ thuộc vào Tổ chức quản lý Tên và địa chỉ mạng quốc tế (ICANN) đặt trụ sở tại Mỹ; đưa ra các quy định về quản lý tên miền thuộc quyền tài phán của Trung Quốc và đặt máy chủ gốc bên trong lãnh thổ Trung Quốc¹. Bên cạnh đó, Trung Quốc đặt ra các

1. Có thể coi Hệ thống phân giải tên miền (DNS) như sổ địa chỉ của internet, trong đó mỗi địa chỉ số IP được gán với một địa chỉ bằng chữ cho dễ nhớ. Ví dụ: Google có địa chỉ IP 216.239.37.99 tương ứng với địa chỉ DNS www.google.com. Năm 2017, Trung Quốc ban hành các quy định về DNS, theo đó yêu cầu các thực thể chạy máy chủ gốc DNS đã đăng ký tại Trung Quốc phải đặt máy chủ của họ bên trong lãnh thổ Trung Quốc. Các cơ quan đăng ký tên miền (Domain Registries) phải có trụ sở trong nước và các tên miền cấp cao nhất mà các cơ quan đăng ký này quản lý do đó rõ ràng thuộc quyền tài phán của Trung Quốc. Các nhà đăng ký tên miền (Domain Registrars) đều phải là các thực thể Trung Quốc điều hành hệ thống của họ trong lãnh thổ Trung Quốc. Cả tổ chức đăng ký tên miền và nhà đăng ký tên miền phải thiết lập hệ thống ứng phó khẩn cấp trong nước và tạo bản sao lưu cơ sở dữ liệu của họ đã được bản địa hóa. Xem MIIT. 2017. “Hulianwang yuming guanli banfa (Internet Domain Name Management Regulations)”, 16 August 2017, Accessed 29 November 2019, <https://baike.baidu.com/item/互联网域名管理办法/23443734?fromtitle=中国互联网络域名管理办法&fromid=1778530>, truy cập ngày 05/8/2021.

tiêu chuẩn về an ninh mạng để thúc đẩy việc yêu cầu bắt buộc sử dụng các công nghệ nội địa nhằm hạn chế sử dụng các công nghệ của nước ngoài - một hình thức được cho là dần xác lập về lãnh thổ riêng của Trung Quốc về mạng¹.

Ngoài ra, trong quan hệ song phương với các nước, Trung Quốc thúc đẩy ký các thỏa thuận hợp tác về không gian mạng, an ninh mạng với các quốc gia như Mỹ, Nga, Braxin².

3. Những vấn đề đặt ra đối với Trung Quốc

Một là, mặc dù Trung Quốc đã đạt được tiến triển vững chắc trong việc hoàn thành các mục tiêu trên không gian mạng, tuy nhiên, cạnh tranh chiến lược toàn diện giữa Mỹ và Trung Quốc, trong đó có cạnh tranh về công nghệ hiện nay đang đặt ra nguy cơ về phân tách công nghệ trên thế giới nói chung và những thách thức đối với Trung Quốc nói riêng trong thúc đẩy nội dung quản trị toàn cầu về internet, bao gồm chủ quyền không gian mạng. Việc Mỹ và các đồng minh phương Tây từ năm 2020 đưa ra các biện pháp trừng phạt, tẩy chay các công ty công nghệ của Trung Quốc như Huawei (công nghệ 5G), phần mềm Wechat... đã gây khó khăn cho việc triển khai sáng kiến, nội dung nhằm thúc đẩy chủ quyền không gian mạng.

1. Ủy ban Kỹ thuật 260 phụ trách phát triển các tiêu chuẩn an ninh mạng, đã ban hành 300 dự thảo về các tiêu chuẩn riêng biệt, nhiều tiêu chuẩn trong số đó hiện đã có hiệu lực thi hành.

2. Tuyên bố chung giữa Chủ tịch Tập Cận Bình và Tổng thống Putin về hợp tác phát triển không gian thông tin tháng 6/2016; Hiệp định hợp tác Trung Quốc và Nga về bảo đảm an ninh thông tin quốc tế năm 2015; Tuyên bố chung giữa Trung Quốc và Braxin về làm sâu sắc hơn nữa quan hệ Đối tác chiến lược toàn diện tháng 7/2014.

Hai là, thách thức trong đối phó, làm việc với Mỹ và đồng minh phương Tây để đạt được sự thỏa hiệp đối với sự tồn tại của chủ quyền quốc gia trong không gian mạng. Có những ý kiến từ Mỹ và phương Tây cho rằng các nỗ lực chủ quyền trên không gian mạng của Trung Quốc bao gồm cả trong nước và quốc tế, sẽ dẫn đến kết quả là một mạng internet sẽ ít cởi mở và miễn phí hơn; việc xây dựng mạng internet riêng, biệt lập để bảo vệ chủ quyền trên không gian mạng mà Trung Quốc thúc đẩy, cổ xúy có thể tạo ra sự thiếu công bằng với các doanh nghiệp nước ngoài, cũng như hạn chế tự do trong không gian mạng. Cũng có ý kiến cho rằng vấn đề chủ quyền không gian mạng nổi lên là do sự phổ biến của thông tin sai lệch, các mối đe dọa đối với quyền riêng tư và sự tập trung quyền lực kinh tế và chính trị của các công ty công nghệ lớn - các vấn đề xuất hiện từ một tổ chức không được kiểm soát hoặc không được kiểm soát internet¹.

Ba là, sự khác biệt về thể chế chính trị, đa dạng về văn hóa, bản sắc dân tộc giữa các quốc gia cũng là một khó khăn đối với Trung Quốc trong việc thúc đẩy, đạt nhận thức chung quốc tế, đặc biệt là tại Liên hợp quốc về các nội dung liên quan đến chủ quyền không gian mạng như quản trị toàn cầu trong không gian mạng/internet, áp dụng các nguyên tắc, nội hàm của chủ quyền quốc gia được quy định trong Hiến chương Liên hợp quốc và các văn bản quốc tế trong không gian mạng.

1. Xem Nadege Rolland: An Emergin China's centric-order: China's vision for the new world order in practice. Adam Segal, China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace, 2020, p.86.

Bốn là, thách thức thúc đẩy chủ quyền quốc gia trong bối cảnh các tập đoàn công nghệ lớn ngày càng có vai trò trong việc định hình, kiểm soát thông tin, thậm chí là các hoạt động chính trị thông qua các nền tảng công nghệ của mình. Ví dụ như từ tháng 01/2021 đến nay, cựu Tổng thống Mỹ Donald Trump bị khóa tài khoản Twitter, Facebook, YouTube..., do vậy, ông Trump bị hạn chế trong việc thực hiện các hoạt động chính trị của mình. Thực tế, những năm qua, Trung Quốc và các quốc gia trên thế giới tìm kiếm các công cụ mới trong việc kiểm soát dòng chảy thông tin cũng như kiểm tra quyền lực của các tập đoàn công nghệ lớn, đã ban hành các biện pháp để kiểm soát dòng chảy thông tin và kiểm tra quyền lực của các tập đoàn công nghệ lớn thông qua việc ban hành các luật, văn bản pháp lý về an ninh mạng, dữ liệu mạng¹. Tuy nhiên, đây vẫn là những thách thức mà Trung Quốc và các quốc gia đang phải đối mặt.

4. Kinh nghiệm tham khảo cho Việt Nam

Có thể thấy quan điểm, cách tiếp cận và triển khai thúc đẩy nội dung chủ quyền không gian mạng của Trung Quốc

1. Luật về triển khai mạng của Đức quy định các công ty truyền thông xã hội có thể đối mặt với mức phạt 50 triệu euro nếu các công ty này không dỡ bỏ các phát ngôn tiêu cực bất hợp pháp và các bài viết/dăng tải khác trong vòng 24 giờ kể từ khi nhận được thông báo của nhà chức trách. Xingapo yêu cầu các nền tảng mạng xã hội thực hiện các cảnh báo đối với những bài viết/dăng tải bị Chính phủ cho là sai và dỡ bỏ các bình luận không phù hợp với “lợi ích công cộng”. Tại Mỹ, các nhà lập pháp của Đảng Dân Chủ và Đảng Cộng hòa đang nghiên cứu việc sửa đổi hoặc thu hồi Mục 230 của Đạo luật về khuôn phép trong thông tin năm 1996. Nhờ vào Mục 230 này phần lớn đã giải phóng một số công ty internet khỏi trách nhiệm pháp lý đối với nội dung của bên thứ ba.

được thực hiện rất bài bản, ở tất cả cấp độ (toàn cầu, khu vực và quốc gia) và ở tất cả các khía cạnh liên quan đến công nghệ, kỹ thuật. Nó cho thấy đây được coi là ưu tiên rất quan trọng của Trung Quốc trong tiến trình Trung Quốc đang vươn lên trở thành cường quốc toàn cầu với mong muốn xây dựng một trật tự thế giới mới trong tầm nhìn về “cộng đồng chung vận mệnh”. Đối với Việt Nam, các nghị quyết, chỉ thị của Đảng cũng như các văn bản quy phạm pháp luật của Nhà nước đều thống nhất quan điểm chỉ đạo về bảo đảm an toàn, an ninh thông tin và bảo vệ chủ quyền quốc gia trên không gian mạng¹. Tuy nhiên, trên thực tế, Việt Nam vẫn chưa có quan điểm chính toàn diện về nội dung, nội hàm của chủ quyền không gian mạng ở cấp độ chính sách và triển khai ở khía cạnh kỹ thuật.

Trên cơ sở những phân tích nêu trên về quá trình xây dựng, triển khai và thúc đẩy chủ quyền không gian mạng của Trung Quốc, Việt Nam có thể tham khảo một số kinh nghiệm ở ba cấp độ (toàn cầu, khu vực và quốc gia) từ Trung Quốc về vấn đề này, cụ thể như sau:

Ở cấp độ toàn cầu, cần nhắc chủ động tham gia vào các quá trình thảo luận về vấn đề không gian mạng và an ninh mạng, trong đó có nội dung chủ quyền không gian mạng

1. Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII của Đảng; Nghị quyết số 29-NQ/TW, ngày 25/7/2018 của Bộ Chính trị khóa XII 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 khóa XII về *Chiến lược an ninh mạng quốc gia...*, xem Nguyễn Việt Lâm: “Chủ quyền không gian mạng: Lý thuyết, thực tiễn trong quan hệ quốc tế và những vấn đề đặt ra hiện nay”, Tạp chí *Cộng sản*, số 971 (8/2021), tr.110-111.

phù hợp với lợi ích quốc gia - dân tộc và phù hợp với khả năng của Việt Nam tại các diễn đàn đa phương quốc tế, nhất là tại Liên hợp quốc. Ví dụ: tham gia vào tiến trình thảo luận của OWEG, nội dung về công nghệ thông tin truyền thông (Ủy ban 4 - Liên hợp quốc), thương lượng các văn bản, điều ước quốc tế về chống các hoạt động tội phạm mạng đe dọa đến an ninh, chủ quyền quốc gia; cân nhắc có hình thức thể hiện các quan điểm về nội dung chủ quyền không gian mạng của Việt Nam là mang tính xây dựng, vì cái chung và độc lập trên cơ sở đường lối đối ngoại độc lập, tự chủ, hòa bình hữu nghị, hợp tác và phát triển, đa phương hóa, đa dạng hóa quan hệ đối ngoại, đồng thời bảo vệ cao nhất các lợi ích quốc gia - dân tộc trên cơ sở các nguyên tắc cơ bản của Hiến chương Liên hợp quốc và luật pháp quốc tế, bình đẳng, hợp tác cùng có lợi.

Ở cấp độ khu vực, tham khảo các nội dung cách tiếp cận về chủ quyền không gian mạng gồm các nội dung về quản trị toàn cầu, bảo vệ dữ liệu... trong các văn bản, tuyên bố ở các khu vực mà Trung Quốc tham gia, thúc đẩy, qua đó xây dựng, đưa ra cách tiếp cận của Việt Nam ở cấp độ khu vực về vấn đề này. Trước mắt, nếu thấy phù hợp và đủ khả năng với Việt Nam thì cân nhắc đề xuất, thậm chí là dẫn dắt về xây dựng văn bản/khung của ASEAN trong bảo vệ dữ liệu xuyên quốc gia trong ASEAN và hợp tác của ASEAN với các đối tác lớn như Trung Quốc. Tranh thủ nguồn lực từ các cơ chế hợp tác khu vực mà Việt Nam tham gia để thúc đẩy việc đào tạo, nâng cao trình độ đối với nguồn nhân lực liên quan đến hoạt động ngoại giao, đối ngoại quốc phòng về không gian mạng, an ninh mạng và kinh nghiệm bảo vệ chủ quyền,

an ninh quốc gia trên không gian mạng. Chủ động tham gia thúc đẩy nội dung chủ quyền không gian mạng trong các mạng lưới nghiên cứu có uy tín của ASEAN.

Ở cấp độ quốc gia, cần nhắc việc đưa nội dung chủ quyền quốc gia không gian mạng trong các chiến lược phát triển của đất nước; tiến hành trao đổi hợp tác với các đối tác chiến lược toàn diện/đối tác chiến lược/đối tác toàn diện về an ninh mạng, an toàn, an ninh thông tin. Đối với Trung Quốc, trên cơ sở tình hữu nghị truyền thống, quan hệ đối tác hợp tác chiến lược toàn diện giữa hai nước, tham khảo kinh nghiệm, tiếp thu có chọn lọc và tranh thủ thúc đẩy hợp tác ở các kênh đảng, chính phủ, quốc hội, học giả giữa hai nước về xây dựng thể chế, nguồn lực, phát triển công nghệ, xây dựng các tiêu chuẩn kỹ thuật an ninh mạng, tăng cường năng lực về an ninh mạng và nội dung, nội hàm về chủ quyền không gian mạng.

Bên cạnh đó, cần nhắc sớm ban hành văn bản của Nhà nước về quy định quản lý dữ liệu trên cơ sở tham khảo kinh nghiệm và hệ thống quy định của quốc tế và các nước, trong đó có nội dung về chủ quyền dữ liệu phù hợp với luật pháp quốc tế, Hiến chương Liên hợp quốc và các thỏa thuận, hiệp định thương mại thế hệ mới, quy định của WTO, các nghĩa vụ quốc tế mà Việt Nam tham gia ký kết, làm cơ sở cho việc phát triển, mở rộng nội hàm về chủ quyền không gian mạng; thúc đẩy nghiên cứu tác động của việc thực hiện chủ quyền số trong không gian mạng đối với an ninh, phát triển và vị thế của Việt Nam, trong bối cảnh hội nhập quốc tế ngày càng sâu rộng và toàn diện, cũng như đề xuất các hướng giải quyết; nghiên cứu, xây dựng nội hàm về chủ quyền không

gian mạng của Việt Nam¹, từ đó có những điều chỉnh, bổ sung kịp thời trong xây dựng và triển khai chính sách đối ngoại của Việt Nam.

1. Nội hàm về chủ quyền không gian mạng có thể bao gồm các nội dung chính, như: phạm vi mở rộng chủ quyền quốc gia trong không gian mạng, quyền độc lập trong việc lựa chọn con đường phát triển trong không gian mạng, phòng thủ không gian mạng và quyền bình đẳng trong tham gia quản trị toàn cầu không gian mạng, các nguyên tắc liên quan trong Hiến chương Liên hợp quốc áp dụng trong không gian mạng...

NÂNG CAO “SỨC ĐỀ KHÁNG” VỚI CÁC LUẬN ĐIỀU CỦA CÁC THỂ LỰC THÙ ĐỊCH

PGS.TS. NGUYỄN MINH TUẤN*

Cho dù lịch sử cách mạng Việt Nam 91 năm qua dưới sự lãnh đạo của Đảng đã giành được những thắng lợi vĩ đại trong công cuộc giải phóng dân tộc, bảo vệ đất nước và xây dựng chủ nghĩa xã hội, để *“đất nước ta chưa bao giờ có được cơ đồ, tiềm lực, vị thế và uy tín quốc tế như ngày nay”*¹, nhưng các thể lực thù địch vẫn luôn tìm mọi cách hạ thấp vai trò lãnh đạo của Đảng, phủ nhận những thành quả cách mạng mà Đảng và nhân dân ta đã giành được.

Vì sao vậy?

Kể từ năm 1847 - Đảng Cộng sản đầu tiên trên thế giới do C. Mác và Ph. Ăngghen sáng lập ra đời đến nay, các thể lực thù địch luôn tìm mọi cách phủ nhận, thậm chí tiêu diệt Đảng Cộng sản và những người theo chủ nghĩa Mác. Đảng Cộng sản Việt Nam cũng không phải là ngoại lệ.

Đồng thời, đối với nước ta, sau mấy chục năm dưới ách thống trị của chủ nghĩa thực dân, phong kiến, các lực lượng

* Học viện Chính trị quốc gia Hồ Chí Minh.

1. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.I, tr.25.

phục vụ cho chế độ cũ thua trận, trốn ra nước ngoài theo địch với số lượng rất lớn - hàng triệu người nên nhiều người trong số đó và thậm chí thế hệ con cháu của họ luôn mang trong mình lòng hận thù dân tộc, luôn tìm mọi cách chống đối thể chế chính trị hiện nay và chưa bao giờ từ bỏ âm mưu lật đổ chế độ chính trị mà Đảng và nhân dân ta đã chọn.

Hơn nữa, trong quá trình lãnh đạo Nhà nước và xã hội, Đảng ta “có lúc cũng phạm sai lầm, khuyết điểm”¹, thậm chí sai lầm trong chủ trương phát triển kinh tế - xã hội. Đặc biệt, một bộ phận cán bộ, đảng viên của Đảng suy thoái về tư tưởng chính trị, đạo đức, lối sống, “tự diễn biến”, “tự chuyển hóa” hiện nay cùng với nhiều người với nhiều lý do khác nhau, thiếu niềm tin, thậm chí bất mãn với chế độ, cố xúi cho những tư tưởng sai trái, thù địch và rất dễ chuyển sang chống đối chế độ.

Ngoài những lý do trên, những “lỗ hổng” trong lý luận chính trị, nhiều vấn đề nảy sinh nhưng việc lý giải chưa đủ sức thuyết phục, chậm được giải quyết, những yếu kém trong nhận thức lý luận của đội ngũ đảng viên; công tác tư tưởng chưa thực sự sắc bén, kịp thời; tình trạng tham nhũng, lãng phí, tiêu cực chậm được ngăn chặn, đẩy lùi; một bộ phận cán bộ, đảng viên thiếu gương mẫu, giàu nhanh, thậm chí quan liêu, xa dân, vi phạm quyền làm chủ của nhân dân... cũng đã làm cho một bộ phận đảng viên thiếu niềm tin, thậm chí hoang mang, dao động, nghi ngờ một phần hoặc toàn bộ lý luận đổi mới của Đảng, từng bước xa rời chủ nghĩa Mác -

1. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XI*, Nxb. Chính trị quốc gia, Hà Nội, 2011, tr.64.

Lênin, tư tưởng Hồ Chí Minh, thiếu tin tưởng vào vai trò lãnh đạo của Đảng.

Để khắc phục có hiệu quả tình trạng đó, Đảng ta đã đề ra nhiều chủ trương, giải pháp nhằm tăng cường xây dựng Đảng về chính trị: “Kiên định chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, không ngừng vận dụng và phát triển sáng tạo phù hợp với thực tiễn Việt Nam”¹. Đồng thời, “*tích cực đấu tranh, phản bác có hiệu quả quan điểm sai trái của các thế lực thù địch*”²...

Tuy nhiên, có một giải pháp căn cốt nhất, cơ bản nhất, bền vững nhất và cũng là khó khăn nhất đó là nâng cao “sức đề kháng”, vô hiệu hóa, “miễn dịch” với luận điệu của các thế lực thù địch.

“*Sức đề kháng*” - một thuật ngữ thường được dùng trong ngành y tế, là khả năng phòng vệ và chống lại các tác nhân xâm nhập vào cơ thể con người. Nếu sức đề kháng tốt thì cho dù các tác nhân đó có thể rất nguy hại như các vi sinh vật siêu vi khuẩn ký sinh trùng cũng không gây bệnh được cho con người và không thể dẫn đến cái chết của con người. Nếu sức đề kháng yếu sẽ là điều kiện thuận lợi cho nhiều loại vi rút gây bệnh phát triển và khi đó con người sẽ ốm yếu dần, khó chữa khỏi và có thể dẫn đến cái chết.

“*Sức đề kháng của Đảng*” có thể hiểu là khả năng “miễn dịch”, khả năng “phòng vệ” của các tổ chức đảng, đảng viên và nhân dân trước sự tấn công trên lĩnh vực tư tưởng của các thế lực thù địch, luôn kiên định con đường mà Đảng, Bác Hồ và

1, 2. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.II, tr.231.

nhân dân ta đã chọn, kiên định chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, kiên định đường lối đổi mới của Đảng và kiên định các nguyên tắc xây dựng Đảng cùng phấn đấu thực hiện mục tiêu “dân giàu, nước mạnh, dân chủ, công bằng, văn minh”.

Để có “sức đề kháng” tốt, Đảng phải thường xuyên chăm lo công tác xây dựng, chỉnh đốn Đảng để Đảng luôn trong sạch, vững mạnh toàn diện về chính trị, tư tưởng, đạo đức, tổ chức và cán bộ. Đảng phải mạnh dạn thẳng thắn chỉ rõ khuyết điểm, dám thừa nhận khuyết điểm và kiên quyết sửa chữa khuyết điểm, để không còn điểm yếu - chỗ cho “virus” có thể dễ dàng xâm nhập vào “cơ thể” Đảng và hủy hoại từng bộ phận “cơ thể” tiến tới hủy hoại toàn “cơ thể” Đảng.

Hơn nữa, Đảng ta đã xác định nguyên tắc trong xây dựng, chỉnh đốn Đảng là phải kết hợp tốt giữa “xây” và “chống”, trong đó “xây” là nhiệm vụ cơ bản, chiến lược, toàn diện, lâu dài và có ý nghĩa quyết định; “chống” là nhiệm vụ quan trọng, cấp bách, thường xuyên. Theo đó, để có “sức đề kháng” tốt thì Đảng phải tích cực, thường xuyên chăm lo công tác xây dựng Đảng và “xây dựng Đảng” thực sự trở thành nhiệm vụ cơ bản, chiến lược, toàn diện, lâu dài và có ý nghĩa quyết định đối với sự phát triển của Đảng.

Những giải pháp về xây dựng, chỉnh đốn Đảng được xác định trong Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII của Đảng đã đề cập đầy đủ, tổng thể, đồng bộ và bao trùm mọi lĩnh vực của công tác xây dựng Đảng. Nói cách khác, “sức đề kháng của Đảng” tốt hay không phụ thuộc vào việc tổ chức thực hiện những nhiệm vụ, giải pháp: (1) Tăng cường xây dựng Đảng về chính trị; (2) Coi trọng xây dựng Đảng về

tư tưởng; (3) Tập trung xây dựng Đảng về đạo đức; (4) Đẩy mạnh xây dựng Đảng về tổ chức; tiếp tục đổi mới, hoàn thiện tổ chức bộ máy và nâng cao hiệu quả hoạt động của hệ thống chính trị; (5) củng cố, nâng cao chất lượng tổ chức cơ sở đảng và đội ngũ đảng viên; (6) Tăng cường xây dựng Đảng về cán bộ ở tất cả các cấp, nhất là cấp chiến lược và người đứng đầu; (7) Nâng cao hiệu lực, hiệu quả công tác kiểm tra, giám sát, kỷ luật đảng; (8) Thắt chặt hơn nữa mối quan hệ mật thiết với nhân dân, dựa vào nhân dân để xây dựng Đảng; (9) Kiên quyết, kiên trì đấu tranh phòng, chống tham nhũng, lãng phí, tiêu cực; (10) Tiếp tục đổi mới mạnh mẽ phương thức lãnh đạo của Đảng trong điều kiện mới.

Tuy nhiên, xét theo những khía cạnh, những mặt của công tác xây dựng Đảng đang là những điểm yếu mà các thế lực thù địch rất dễ “khoét sâu” để tấn công - “virus” dễ “xâm nhập” vào “cơ thể” Đảng, cần chú trọng thực hiện những giải pháp cơ bản sau đây:

Thứ nhất, nâng tầm lý luận của toàn Đảng, của mỗi cán bộ, đảng viên và nhân dân về chủ nghĩa xã hội và con đường đi lên chủ nghĩa xã hội ở Việt Nam.

Đây là nhiệm vụ quan trọng, lâu dài, cần phải được chú trọng thực hiện thường xuyên, kiên trì mà hiệu quả bền vững trước hết phụ thuộc vào sức thuyết phục của tri thức khoa học về nền tảng tư tưởng, về vai trò, chức năng, nhiệm vụ của Đảng duy nhất cầm quyền. Lịch sử xây dựng chủ nghĩa xã hội cho thấy: những sai lầm kéo dài về duy trì cơ chế quản lý kinh tế - xã hội tập trung quan liêu, bao cấp, hệ thống xã hội chủ nghĩa lâm vào tình trạng thoái trào, nhiều đảng cộng sản cầm quyền đã mất vai trò lãnh đạo xã hội và bị phân hóa

thành nhiều khuynh hướng chính trị khác nhau. Điều đó càng làm cho các thế lực thù địch hí hửng tấn công, khoét sâu vào những khuyết điểm đó mà lập luận, minh chứng, dự báo cho sự sụp đổ tất yếu của chủ nghĩa xã hội. Trong quá trình đổi mới, Đảng ta đã từng bước làm sáng tỏ lý luận về con đường đi lên chủ nghĩa xã hội, khẳng định sự trưởng thành của Đảng trên lĩnh vực hệ trọng này trong thế giới đầy biến động nhưng vẫn còn nhiều vấn đề cần tiếp tục làm rõ hơn, có sức thuyết phục cao hơn như: (1) đổi mới mô hình, thể chế thực hiện dân chủ ở nước ta, làm rõ mô hình thực hiện dân chủ, cơ chế Đảng lãnh đạo, Nhà nước quản lý, nhân dân làm chủ; (2) giải quyết mối quan hệ giữa thực hiện dân chủ với chế độ một đảng cầm quyền duy nhất với nền chính trị nhất nguyên, làm rõ vai trò, phương thức lãnh đạo, cầm quyền của Đảng trong mối quan hệ với xây dựng Nhà nước pháp quyền xã hội chủ nghĩa; (3) giải quyết mối quan hệ giữa dân chủ và nhân quyền, làm rõ nội dung phát huy dân chủ xã hội chủ nghĩa với bảo đảm quyền con người - hai giá trị chung của nhân loại trong chế độ xã hội chủ nghĩa ở nước ta; (4) xây dựng và hoàn thiện các cơ chế, chế định thực hiện dân chủ (trực tiếp, đại diện), phát huy quyền làm chủ của nhân dân, xác định rõ cơ chế để nhân dân kiểm soát quyền lực nhà nước một cách hiệu quả nhất; (5) làm rõ và quán triệt những nguyên tắc thực hiện dân chủ ở nước ta, làm rõ mối quan hệ giữa quyền và nghĩa vụ công dân; (6) nhận thức đầy đủ những thuận lợi, khó khăn, thách thức của quá trình thực hiện dân chủ xã hội chủ nghĩa ở nước ta hiện nay... Đây là nhiệm vụ quan trọng của đảng cầm quyền, cũng là trách nhiệm chính trị, là lực lượng duy nhất

lãnh đạo Nhà nước và xã hội, “chỉ lối soi đường” cho toàn dân tộc nên rất cần tầm nhìn chiến lược và sự trưởng thành trên lĩnh vực lý luận của Đảng. Đây cũng là biện pháp căn bản, lâu dài và rất cần thiết để lý luận chủ nghĩa xã hội đủ sức thuyết phục trong toàn Đảng và mọi tầng lớp nhân dân bằng căn cứ khoa học.

Thứ hai, đẩy mạnh việc hoàn thiện thể chế kiểm soát quyền lực, phòng, chống có hiệu quả đối với tệ tham nhũng, lãng phí, tiêu cực.

Đây là yếu tố quan trọng nhất để “miễn dịch” với sự công kích của các thế lực thù địch về vai trò lãnh đạo duy nhất của Đảng Cộng sản. Trong điều kiện đảng cầm quyền, nền dân chủ thể hiện thông qua đường lối của Đảng và phụ thuộc vào sự trong sạch, vững mạnh của bộ máy chính quyền các cấp.

Chúng ta thừa nhận, dân chủ trong điều kiện Đảng Cộng sản Việt Nam duy nhất cầm quyền rất dễ nảy sinh những tiêu cực khi đảng viên của Đảng nắm giữ những vị trí then chốt trong chính quyền. Điều này cũng được lãnh tụ V.I. Lênin và Chủ tịch Hồ Chí Minh cảnh báo từ rất sớm. Vì trong điều kiện Đảng Cộng sản duy nhất cầm quyền, vai trò, uy tín của Đảng chủ yếu thông qua sự trong sạch, vững mạnh, tận tụy phục vụ nhân dân của bộ máy và cán bộ, công chức chính quyền nhà nước. Vì thế, những khuyết điểm của Đảng, sự yếu kém trong quản lý nhà nước trong một thời điểm nào đó và ở một số nơi nào đó chính là những vết thương mà các thế lực thù địch thường khoét sâu nhất để tuyên truyền, kích động trên lĩnh vực tư tưởng. Hàng vạn việc tốt thì họ không nhắc tới nhưng chỉ vài việc chưa tốt thì họ tìm mọi cách khai thác, tuyên truyền kích động,

thậm chí thổi phồng, thêu dệt và gán cho nó không thiếu nguyên nhân nhằm công kích sự lãnh đạo của Đảng.

Nhiều nhiệm kỳ đại hội, nhất là nhiệm kỳ Đại hội lần thứ XII, Đảng ta quyết liệt thực hiện nhiệm vụ “then chốt” xây dựng Đảng, xây dựng hệ thống chính trị trong sạch, vững mạnh, thực hiện có hiệu quả công tác phòng, chống tệ quan liêu, tham nhũng, lãng phí, tiêu cực, không có vùng cấm, không có ngoại lệ để làm trong sạch Đảng, đem lại niềm tin trong nhân dân. Đây là điểm sáng nhất để “miễn dịch” với sự công kích của các thế lực thù địch về vai trò lãnh đạo duy nhất của Đảng Cộng sản. Tuy nhiên, đó mới chỉ là kết quả bước đầu. Vẫn còn đó nguy cơ không thể xem thường về tình trạng suy thoái, tham nhũng trong bộ máy nhà nước gây nhức nhối trong xã hội. Vai trò kiểm tra, giám sát, kiểm soát quyền lực của đảng cầm quyền trong cơ quan Quốc hội và hội đồng nhân dân các cấp còn mờ nhạt, thiếu tính khả thi và hiệu quả thấp. Đây cũng là điểm yếu dễ bị kẻ thù công kích, gây hoang mang, dao động, thiếu niềm tin vào khả năng kiểm soát của Đảng và nhân dân đối với chính quyền.

Thứ ba, tiếp tục đổi mới mạnh mẽ và nâng cao chất lượng, hiệu quả công tác cán bộ.

Vấn đề sống còn của công tác xây dựng, chỉnh đốn Đảng vẫn là công tác cán bộ. Ở đâu cán bộ tốt, nhất là người đứng đầu có đạo đức trong sáng, năng lực chuyên môn tốt, sống và làm việc chí công vô tư, thì ở đó tổ chức đảng vững mạnh, nhiệm vụ công tác hoàn thành, nội bộ đoàn kết, quần chúng tin tưởng. Xác định được điều đó, Đảng đã chỉ đạo tập trung xây dựng đội ngũ cán bộ các cấp, nhất là cấp chiến lược,

người đứng đầu đủ phẩm chất, năng lực, uy tín, ngang tầm nhiệm vụ. Kết quả chống tham nhũng trong công tác cán bộ đã và đang được coi trọng nhưng vẫn còn nhiều khâu thực hiện chưa tốt, thậm chí làm đúng quy trình nhưng vẫn không tìm kiếm được người tài đức nổi trội, gây bất bình trong dư luận và ngay trong nội bộ Đảng. Vì thế, cần lựa chọn một số khâu để giải quyết nhằm tạo bước đột phá trong công tác quan trọng nhưng hết sức nhạy cảm này. Trong các nội dung về công tác cán bộ hiện nay, cần đặc biệt chú trọng đổi mới, hoàn thiện, quản lý chặt chẽ *khâu đánh giá cán bộ*. Cần tập trung đổi mới, nâng cao chất lượng đánh giá cán bộ theo hướng: Xác định rõ thẩm quyền, trách nhiệm cụ thể của cán bộ; mở rộng diện tham gia đánh giá, các kênh đánh giá cán bộ, phát huy vai trò của Mặt trận Tổ quốc, các tổ chức chính trị - xã hội và vai trò của nhân dân, báo chí; bảo đảm dân chủ, công khai, minh bạch, sâu sát, chính xác trong quá trình đánh giá cán bộ. Xây dựng quy định đánh giá cán bộ theo hướng xuyên suốt, tích cực, đa chiều theo tiêu chí cụ thể bằng sản phẩm, hiệu quả công việc; công khai kết quả và so sánh với các chức danh tương đương, gắn đánh giá cá nhân với tập thể, kết quả thực hiện nhiệm vụ của cơ quan, đơn vị.

Thứ tư, tăng cường thực hiện nêu gương của cán bộ, đảng viên, nhất là cán bộ lãnh đạo các cấp.

Để tạo chuyển biến căn bản trong phòng, chống suy thoái về tư tưởng chính trị, đạo đức, lối sống, “tự diễn biến”, “tự chuyển hóa” trong nội bộ, phải phát huy hơn nữa trách nhiệm nêu gương của cán bộ, đảng viên, nhất là cán bộ chủ chốt các cấp, người đứng đầu, cán bộ giữ chức vụ

càng cao càng phải gương mẫu, đúng với tư tưởng của Chủ tịch Hồ Chí Minh: “Một tấm gương sống còn có giá trị hơn một trăm bài diễn văn tuyên truyền”¹. Các quy định về chế độ nêu gương, về trách nhiệm công tác, đổi mới sáng tạo, đạo đức, tác phong, thực hành dân chủ, gắn bó với nhân dân của từng tổ chức đảng... đã khá đầy đủ nhưng vấn đề còn thiếu và yếu là sự cam kết chính trị của người đứng đầu còn ít và còn chung chung, khó kiểm tra, giám sát. Vì vậy, cần phải gắn việc giáo dục tuyên truyền tấm gương đảng viên tích cực với tập trung kiểm tra, giám sát tổ chức đảng, người đứng đầu, cán bộ chủ chốt ở những lĩnh vực, địa bàn, vị trí công tác dễ xảy ra tiêu cực, nơi người dân có nhiều bức xúc, dư luận xã hội quan tâm. Đồng thời xử lý kịp thời, kiên quyết, nghiêm minh các tổ chức đảng, đảng viên vi phạm. Kết hợp giữa nêu gương với kiểm tra, giám sát để đánh giá, sử dụng, bảo vệ hoặc kỷ luật đối với cán bộ.

Khi đảng duy nhất cầm quyền, lãnh đạo Nhà nước và xã hội thực sự là vì nhân dân; khi Đảng thực sự trong sạch, vững mạnh và khi nhân dân gửi trọn niềm tin vào Đảng thì không một thế lực thù địch nào có thể chia rẽ được.

Đúng như V.I. Lênin đã cảnh báo những sai lầm về chính trị mà những người cộng sản có thể mắc phải. Đảng lãnh đạo, cầm quyền bằng cương lĩnh, đường lối chính trị, nhưng đường lối do đảng đề ra có thể sai lầm. Sai lầm trong đường lối chính trị là điều nguy hại lớn nhất: “Không ai có thể tiêu

1. Hồ Chí Minh: *Toàn tập*, Nxb. Chính trị quốc gia, Hà Nội, 2012, t.1, tr.284.

diệt được chúng ta, ngoài những sai lầm của bản thân chúng ta. Toàn bộ vấn đề là ở chữ “nếu” này. Nếu chúng ta do sai lầm mà gây ra sự chia rẽ thì tất cả sẽ sụp đổ”¹. Chủ tịch Hồ Chí Minh cũng đã nói: “Đảng ta là đạo đức, là văn minh”. Muốn xứng đáng với danh hiệu cao quý đó, Đảng phải không ngừng được xây dựng, chỉnh đốn để thực sự là người lãnh đạo cách mạng, là “hiện thân của trí tuệ, danh dự và lương tâm của dân tộc”².

1. V.I. Lênin: *Toàn tập*, Nxb. Chính trị quốc gia, Hà Nội, 2005, t.42, tr.311.

2. Hồ Chí Minh: *Toàn tập*, *Sđd*, t.9, tr.412.

ĐỊNH HƯỚNG, GIẢI PHÁP BẢO VỆ NỀN TẢNG TƯ TƯỞNG CỦA ĐẢNG TRÊN MÔI TRƯỜNG MẠNG XÃ HỘI Ở VIỆT NAM HIỆN NAY

PGS.TS. MAI ĐỨC NGỌC*

Việt Nam là quốc gia đang trong quá trình hình thành và phát triển xã hội thông tin. Mạng xã hội là những nền tảng truyền thông trực tuyến đa dạng, không bị yếu tố địa lý cản trở và cung cấp rất nhiều tiện ích cho người tham gia và sử dụng nó. Trong kỷ nguyên số và thời kỳ hội nhập, sẽ là sai lầm lớn nếu chúng ta coi nhẹ tầm quan trọng của mạng xã hội và tác động của nó đối với người dân, với các cơ quan, tổ chức, địa phương và quốc gia. Mạng xã hội là công cụ tạo vốn xã hội cho các cá nhân, các nhóm xã hội khi họ trực tiếp tham gia chia sẻ, tương tác trên mạng xã hội và tạo vốn xã hội cho chính các cơ quan, tổ chức có trách nhiệm quản lý báo chí truyền thông. Mạng xã hội đồng thời là một công cụ truyền thông có khả năng mạnh mẽ trong việc tổ chức các hoạt động thông tin - giao tiếp xã hội, tạo liên kết xã hội, thậm chí có ảnh hưởng không nhỏ tới các mối quan hệ xã hội.

Tuy nhiên, thực tế đã chứng minh sự tác động có tính hai mặt của mạng xã hội đến đời sống của con người. Bên cạnh

* Học viện Chính trị quốc gia Hồ Chí Minh.

những tác động tích cực, mạng xã hội cũng gây ra không ít những tác động tiêu cực, nhất là trên lĩnh vực tư tưởng - văn hóa, đặc biệt trong bối cảnh các thế lực thù địch, phản động đang lợi dụng sự phát triển của mạng xã hội để tiến hành chống phá cách mạng Việt Nam.

Thực tế cho thấy, do sự lan tỏa nhanh chóng của thông tin trên mạng xã hội trong khi khả năng kiểm chứng và kiểm soát còn hạn chế, rất nhiều thông tin xấu, độc, thông tin giả đã tác động tiêu cực đến tư tưởng, tình cảm, tâm lý của quần chúng nhân dân, gây trở ngại cho việc thực hiện chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước, gây bất ổn chính trị - xã hội. Thậm chí các thế lực thù địch, phản động còn lợi dụng mạng xã hội để lôi kéo, kích động người dân tiến hành các hoạt động nhằm làm suy yếu, tiến tới lật đổ chế độ xã hội chủ nghĩa ở nước ta. Đây chính là một nguy cơ không thể xem nhẹ trong bối cảnh hiện nay. Do đó, bảo vệ nền tảng quan điểm của Đảng, đấu tranh ngăn chặn những quan điểm sai trái, thù địch trên mạng xã hội là một nhiệm vụ cấp bách để phát huy tác động tích cực, hạn chế tác động tiêu cực của mạng xã hội đến đời sống tinh thần của nhân dân ta trong giai đoạn hiện nay. Bài viết đề xuất một số định hướng, giải pháp nhằm góp phần thực hiện nhiệm vụ quan trọng nêu trên.

1. Các định hướng tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội ở Việt Nam trong thời gian tới

Một là, đối với chủ thể bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Để bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội ở nước ta hiện nay cần *phát huy mạnh mẽ vai trò của chủ thể, chủ động, tích cực tự đề kháng, tự miễn dịch* đối với toàn Đảng, toàn quân và toàn dân ta. Trong đó, Đảng là chủ thể lãnh đạo, Nhà nước là chủ thể quản lý, toàn quân, toàn dân là chủ thể tham gia đấu tranh. Thực tế cho thấy, Đảng và Nhà nước ta *luôn chủ động* phát huy tốt vai trò chủ thể lãnh đạo, quản lý trong quá trình định hướng công tác bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mọi mặt trận, trong đó có mạng xã hội. Trước sự tấn công của các thế lực thù địch, phản động nhằm chống phá nền tảng tư tưởng của Đảng, chống phá Nhà nước, chống phá chế độ..., Đảng và Nhà nước ta đã không ngừng nâng cao hiệu quả trong công tác lãnh đạo, quản lý của các cấp ủy đảng, chính quyền từ Trung ương đến địa phương và các tầng lớp nhân dân tích cực tham gia cuộc đấu tranh bảo vệ nền tảng tư tưởng của Đảng, ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội. Thời gian qua, Đảng và Nhà nước đã *chủ động* ban hành nhiều chỉ thị, nghị quyết, các bộ luật nhằm khẳng định rõ vai trò của mình trong việc lãnh đạo, chỉ đạo, định hướng đối với công tác bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mọi mặt trận trong đó có mạng xã hội.

Có thể thấy, bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội thực chất là cuộc đấu tranh tư tưởng, lại diễn ra trên một mặt trận hoàn toàn mới - mạng xã hội, vì vậy vai trò

lãnh đạo của Đảng, vai trò quản lý của Nhà nước là những nhân tố quyết định sự thắng lợi của cuộc đấu tranh này cũng như quyết định việc phát huy được vai trò tích cực của các chủ thể trong đấu tranh bảo vệ nền tảng tư tưởng của Đảng, chống các quan điểm sai trái, thù địch trên mạng xã hội.

Bên cạnh Đảng và Nhà nước, trách nhiệm bảo vệ nền tảng tư tưởng của Đảng còn thuộc về nhân dân và các lực lượng xã hội. Đây là những lực lượng xung kích, trực tiếp tham gia đấu tranh bảo vệ nền tảng tư tưởng của Đảng, chống các quan điểm sai trái, thù địch trên mạng xã hội. Trong các lực lượng xung kích thì những người làm công tác giáo dục, đào tạo, nghiên cứu lý luận chính trị; đội ngũ những người làm công tác tư tưởng, tuyên giáo,... là lực lượng trực tiếp, thường xuyên và có vai trò quan trọng nhất.

Như vậy, có thể thấy, chủ thể bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội là toàn Đảng, toàn dân và toàn quân ta, là toàn bộ hệ thống chính trị. *Mỗi chủ thể cần chủ động “tự đề kháng”, “tự miễn dịch” cho mình là con đường tốt nhất để các thông tin xấu, độc hại không thể phát huy tác dụng.*

Hai là, đối với đối tượng bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Căn cứ quan trọng để xác định quan điểm định hướng đối với đối tượng bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội xuất phát từ chính việc xác định những nhóm đối tượng đang tuyên truyền các quan điểm sai trái, thù địch trên mạng xã hội ở nước ta hiện nay và mục đích của chúng.

Đối tượng đang chống phá nền tảng tư tưởng của Đảng trên mọi mặt trận, trong đó có mạng xã hội ở nước ta, có thể chia làm ba nhóm chính: 1) Nhóm đối tượng đối lập về mặt hệ tư tưởng. Hệ tư tưởng của Đảng ta là hệ tư tưởng vô sản, thì những người theo hệ tư tưởng tư sản và các hệ tư tưởng tàn dư khác cũng chống đối chúng ta một cách quyết liệt; 2) Các thế lực thù địch về chính trị, chống lại chế độ xã hội chủ nghĩa (những đối tượng phản động, cơ hội chính trị); 3) Là những người vốn là đảng viên cộng sản nhưng suy thoái về tư tưởng chính trị, đạo đức, lối sống, "tự diễn biến", "tự chuyển hóa". Đây chính là các đối tượng trong bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Xuất phát từ việc xác định rõ các nhóm đối tượng này và mục tiêu của chúng, thì quan điểm, định hướng đối với đối tượng bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội chính là: Bảo vệ Đảng, Nhà nước, nhân dân; bảo vệ chế độ xã hội chủ nghĩa, bảo vệ con đường đi lên chủ nghĩa xã hội; bảo vệ lợi ích quốc gia - dân tộc Việt Nam.

Ba là, đối với nội dung bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Nội dung bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội rất phong phú, đa dạng, bao quát nhiều vấn đề, bao gồm các nội dung chủ yếu sau: *Trước hết*, bảo vệ chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh - nền tảng tư tưởng của Đảng; *thứ hai*, bảo vệ Cương lĩnh, chủ trương, đường lối của Đảng,

chính sách, pháp luật của Nhà nước, bảo vệ lịch sử dân tộc, lịch sử Đảng, lịch sử cách mạng, bảo vệ uy tín, danh dự của các đồng chí lãnh đạo, lãnh tụ của Đảng và Nhà nước...; *thứ ba*, bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội phải gắn liền với cuộc đấu tranh chống suy thoái về tư tưởng chính trị, đạo đức, lối sống, “tự diễn biến”, “tự chuyển hóa” trong một bộ phận không nhỏ cán bộ, đảng viên ở nước ta hiện nay.

Như vậy, có thể thấy nội dung bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội cần phải được đổi mới theo hướng đa dạng hóa, bao quát, toàn diện hơn để phù hợp với cuộc đấu tranh trong tình hình mới, nhất là đấu tranh trên mạng xã hội - một mặt trận hoàn toàn mới đối với cuộc đấu tranh tư tưởng ở nước ta hiện nay.

Bốn là, đổi mới phương thức bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Định hướng phương thức (phương pháp và cách thức) bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội cần phải căn cứ vào hai điểm: *thứ nhất*, cần phân biệt rõ hai quan điểm: sai trái và thù địch; *thứ hai*, cần xác định rõ các phương thức tấn công vào nền tảng tư tưởng của Đảng của các thế lực thù địch trên mạng xã hội.

Trên mặt trận mới - mạng xã hội, phương thức bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch cần được đổi mới theo những cách thức, phương pháp đấu tranh mới, đa dạng, thể hiện rõ tính

chủ động, kịp thời và kiên quyết trong đấu tranh. Cụ thể như: 1) Trực tiếp xây dựng các tài khoản chính thống trên mạng xã hội để tuyên truyền chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước; 2) Xây dựng một môi trường thông tin trong sạch trên mạng xã hội thông qua việc loại bỏ những quan điểm xuyên tạc, sai trái của các thế lực thù địch; 3) Chủ động nắm bắt tình hình để sớm phát hiện các hoạt động chống phá có tổ chức của các thế lực thù địch trên mạng xã hội; 4) Cần phải thực hiện tốt công tác điều tra, xử lý những đối tượng tung tin sai trái, bịa đặt và cả những đối tượng tiếp tay lan truyền những thông tin đó trên mạng xã hội.

Năm là, đối với các điều kiện bảo đảm cho việc bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Để tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội cần bảo đảm những điều kiện cơ bản sau: *Một là*, trong bất kỳ hoàn cảnh nào cũng phải kiên định chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh - nền tảng tư tưởng quyết định bản chất khoa học, cách mạng của Đảng; *hai là*, giữ vững vai trò lãnh đạo của Đảng, nâng cao vai trò quản lý của Nhà nước là điều kiện cơ bản nhất để bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội; *ba là*, phát huy tính chủ động, tích cực của mọi tầng lớp nhân dân trong sự nghiệp bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội; *bốn là*, tăng cường

cơ sở vật chất - kỹ thuật cho công tác bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội; *năm là*, hợp tác quốc tế trong việc bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

2. Một số giải pháp nhằm tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội ở Việt Nam trong thời gian tới

Để thực hiện các định hướng nêu trên, góp phần bảo vệ vững chắc nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn có hiệu quả các quan điểm sai trái, thù địch trên mạng xã hội, chúng tôi đề xuất một số giải pháp sau đây:

Thứ nhất, xây dựng và hoàn thiện thể chế, chính sách đối với chủ thể lãnh đạo, quản lý và người sử dụng mạng xã hội.

Trong thời gian tới, để bảo vệ vững chắc nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn có hiệu quả các quan điểm sai trái, thù địch trên mạng xã hội, Đảng và Nhà nước cần tiếp tục bổ sung hoàn thiện các quy định của Đảng, pháp luật của Nhà nước theo các hướng sau: *Một là*, cần tập trung xây dựng, hoàn thiện các quy định của Đảng để nâng cao trách nhiệm của cán bộ, đảng viên đấu tranh với những âm mưu, thủ đoạn, phương thức chống phá của các thế lực thù địch; *hai là*, xây dựng cơ chế bảo vệ người tham gia đấu tranh. Trên thực tế có những trường hợp tham gia đấu tranh chống quan điểm sai trái, thù địch, chống sự suy thoái trong cán bộ, đảng viên nhưng khi bị các thế lực thù địch tấn công trở lại thì ta lại không có cơ chế bảo vệ, thậm chí

cũng không có tiếng nói để bảo vệ những nhân tố tích cực này, từ đó không khuyến khích được những người tham gia đấu tranh; *ba là*, cần có quy định để phân biệt giữa những người tích cực tham gia đóng góp ý kiến mang tính xây dựng với những quan điểm sai trái của các thế lực thù địch. Đây là vấn đề rất quan trọng để phát huy dân chủ, tăng cường trao đổi, đối thoại, phản biện để xây dựng và hoàn thiện đường lối, chủ trương, chính sách phát triển đất nước; *bốn là*, tiếp tục hoàn thiện các quy định về nêu gương trong cán bộ, đảng viên, nhất là cán bộ, đảng viên cấp cao tham gia đấu tranh, phản bác các quan điểm sai trái, thù địch, coi đây là một nội dung quan trọng trong đánh giá hoàn thành nhiệm vụ. Đối với những trường hợp đảng viên (kể cả cán bộ cấp cao, nguyên lãnh đạo cấp cao) nếu vi phạm về công tác này, thể hiện những quan điểm sai trái mà qua tuyên truyền, vận động không chuyển biến, không nhận ra sai lầm, khuyết điểm thì cần kiên quyết thi hành kỷ luật đảng từ cảnh cáo tới cách chức, khai trừ, thậm chí xử lý hình sự theo quy định của pháp luật nếu vi phạm nghiêm trọng.

Thứ hai, xây dựng, đổi mới nội dung, phương thức bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Nội dung bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch phải bảo đảm kết hợp giữa “xây” và “chống”. “Xây” là cơ bản, lâu dài, “chống” phải quyết liệt, hiệu quả. Việc đổi mới nội dung bảo vệ nền tảng tư tưởng của Đảng cần bám sát các quan điểm, luận điệu sai trái của các thế lực thù địch để đưa ra những luận cứ bác bỏ chúng.

Trong thời gian tới, cần tăng cường xây dựng, mở rộng về nội dung, đa dạng về hình thức các trang thông tin của các cơ quan đảng, nhà nước, các tổ chức chính trị - xã hội trên mạng nhằm chiếm lĩnh trận địa không gian mạng. Chủ động đưa thông tin tích cực lên mạng xã hội, gồm những nội dung cơ bản của chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh; giá trị, truyền thống tốt đẹp của dân tộc; những thành công của các cuộc kháng chiến vĩ đại của dân tộc; những thành tựu to lớn của công cuộc đổi mới đất nước; việc vận dụng sáng tạo chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh vào thực tiễn cách mạng Việt Nam; nền văn hiến, lịch sử vẻ vang của dân tộc Việt Nam, hình ảnh quê hương, đất nước, con người Việt Nam,...

Chú trọng những luận cứ lý luận và thực tiễn để làm cơ sở cho việc đấu tranh, phản bác. Tăng cường đối thoại, thuyết phục; phát huy dân chủ trong nghiên cứu lý luận; tranh thủ ý kiến của những người có uy tín trong xã hội, trí thức khoa học công nghệ, văn nghệ sĩ, già làng, trưởng bản, chức sắc tôn giáo...

Chú trọng tuyên truyền, lan tỏa các thông tin bảo vệ nền tảng tư tưởng của Đảng qua mạng xã hội thông qua giới trẻ, đặc biệt là đội ngũ học sinh, sinh viên, nguồn nhân lực chất lượng cao của đất nước, để từ đó lan tỏa ra toàn xã hội. Ở các trường đào tạo lý luận chính trị, các trường Đảng có thể tổ chức các đội, nhóm sinh viên, học viên nòng cốt tham gia tuyên truyền bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội. Có thể thông qua chi bộ hoặc tổ chức Đoàn Thanh niên để giao nhiệm vụ phù hợp, như “like”, “chia sẻ”, viết bài tuyên

truyền,... những thông tin tích cực bảo vệ nền tảng tư tưởng của Đảng trên mạng xã hội.

Tăng cường hiệu quả công tác giáo dục lý luận chính trị qua các kênh truyền thông mới và trong hệ thống giáo dục quốc dân. Ứng dụng công nghệ thông tin trong đào tạo, bồi dưỡng lý luận chính trị. Tăng cường các hình thức tuyên truyền, giáo dục qua mạng xã hội, các hình thức học tập lý luận chính trị trực tuyến,...

Phát huy vai trò tiên phong của đội ngũ giảng viên, chuyên gia và học viên của hệ thống trường Đảng trong việc bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội. Tăng cường trách nhiệm của các cán bộ, giảng viên, học viên của các trường Đảng, giảng viên lý luận chính trị của các cơ sở đào tạo khi tham gia mạng xã hội. Xác định rõ trách nhiệm mỗi cán bộ, giảng viên, học viên của hệ thống trường Đảng, giảng viên lý luận chính trị của các cơ sở đào tạo là một chiến sĩ tiên phong trong sự nghiệp cách mạng của Đảng, chủ động, tự giác bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn có hiệu quả các quan điểm sai trái, thù địch trên mạng xã hội. Chia sẻ, lan tỏa rộng rãi những kết quả nghiên cứu về lý luận chính trị, nội dung, phương thức mới bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Phát huy hơn nữa vai trò của các cơ quan báo chí, truyền thông trong việc tham gia các diễn đàn trên mạng xã hội, tham gia trực tiếp vào cuộc đấu tranh bảo vệ nền tảng tư tưởng của Đảng, ngăn chặn các quan điểm sai trái, thù địch. Các cơ quan báo chí, truyền thông cần chủ động,

tích cực lan tỏa các thông tin chính thống, đúng đắn về các sự kiện, về đường lối, chính sách của Đảng và Nhà nước nhằm định hướng dư luận xã hội, góp phần đẩy lùi ảnh hưởng các thông tin xấu, độc trên mạng xã hội. Tăng cường ý thức, trách nhiệm của đội ngũ nhà báo, phóng viên, biên tập viên trên mạng xã hội.

Thứ ba, đẩy mạnh đào tạo, bồi dưỡng đội ngũ cán bộ nòng cốt bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Để phát huy vai trò của các chủ thể trong việc bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội, cần coi trọng công tác đào tạo, bồi dưỡng đội ngũ cán bộ nòng cốt của hoạt động này:

Một là, nghiên cứu nhu cầu và xây dựng chiến lược đào tạo, bồi dưỡng đội ngũ cán bộ nòng cốt nhằm tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội, nhất là đối với đội ngũ cán bộ làm công tác tư tưởng, lý luận về chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, cần nâng cao chất lượng và số lượng của đội ngũ cán bộ này. Để làm được điều này, chúng ta cần có chiến lược đào tạo đội ngũ cán bộ lý luận chính trị dài hạn, bài bản, ở trình độ đại học, thạc sĩ, tiến sĩ, có trình độ ngoại ngữ và công nghệ thông tin tốt, có tiềm năng trở thành những chuyên gia lý luận giỏi trong lĩnh vực này. Bên cạnh đó, cần có các chính sách tuyển sinh theo hướng tạo điều kiện để thu hút đầu vào và nâng cao chất lượng đào tạo các ngành lý luận chính trị. Cụ thể như: có chính sách miễn học phí hoặc cấp học bổng theo số lượng chỉ tiêu nhất định và bố trí việc làm sau đào tạo như học viên các

trường đào tạo sĩ quan công an, quân đội đối với các ngành đào tạo giảng viên lý luận chính trị nhằm khắc phục khó khăn trong thu hút đầu vào của các ngành này. Mặt khác, cần nâng cao hơn nữa chất lượng đào tạo các ngành lý luận chính trị thông qua việc chuẩn hóa chương trình, tăng cường nghiên cứu khoa học và yêu cầu về chuyên môn của giảng viên các ngành này. *Hai là*, xác định rõ mục tiêu, chương trình, nội dung đào tạo, bồi dưỡng đội ngũ cán bộ nòng cốt. *Ba là*, phân khúc rõ đối tượng đào tạo, bồi dưỡng bảo đảm tính hệ thống, phù hợp với mục tiêu đào tạo và đầu vào của quá trình đào tạo, bồi dưỡng. *Bốn là*, đổi mới mạnh mẽ phương pháp và hình thức đào tạo, bồi dưỡng đội ngũ cán bộ nòng cốt. *Năm là*, tiếp tục xây dựng và hoàn thiện cơ sở vật chất - kỹ thuật cho hoạt động đào tạo, bồi dưỡng đội ngũ cán bộ nòng cốt.

Để các giải pháp trên được thực thi hiệu quả, cần tạo cơ chế thuận lợi để tổ chức các khóa đào tạo văn bằng hai các ngành đào tạo: giảng viên lý luận chính trị, báo chí - truyền thông, công tác tư tưởng - văn hóa nhằm bổ sung lực lượng nòng cốt bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch ở các bộ, ngành, đoàn thể và địa phương. Thực tế quá trình lịch sử cách mạng Việt Nam cho thấy, ở những thời kỳ khó khăn cần huy động tối đa sức người, sức của phục vụ tiền tuyến, Đảng ta rất coi trọng đào tạo đội ngũ cán bộ làm công tác tư tưởng, báo chí - truyền thông. Có những thời điểm có tới hơn một chục trường Tuyên huấn Trung ương chuyên đào tạo đội ngũ cán bộ tư tưởng của Đảng ở khắp các vùng, miền của Tổ quốc. Tuy nhiên, ở các giai đoạn sau này, việc đào tạo

đội ngũ cán bộ chuyên trách làm công tác tư tưởng, lý luận, báo chí - truyền thông chưa được coi trọng đúng mức. Do vậy, trong cuộc đấu tranh cam go, quyết liệt, phức tạp này chúng ta cần quan tâm hơn nữa đến công tác đào tạo, bồi dưỡng đội ngũ cán bộ làm công tác tư tưởng, lý luận. Cần tập trung bồi dưỡng chuyên sâu cho đội ngũ cán bộ nòng cốt, đặc biệt là đội ngũ cán bộ ở các cơ quan báo chí - truyền thông nhằm nâng cao vị trí, vai trò của báo chí - truyền thông trong đấu tranh ngăn chặn các quan điểm sai trái, thù địch; góp phần xử lý thông tin sai lệch, xuyên tạc trên lĩnh vực tư tưởng, lý luận và văn học, nghệ thuật. Bên cạnh đó, cần tìm kiếm các giải pháp tăng cường hợp tác quốc tế trong đào tạo, bồi dưỡng cho giảng viên, chuyên gia và các cơ sở đào tạo chuyên sâu về lĩnh vực này.

Thứ tư, tăng cường đầu tư các nguồn lực, xây dựng các mô hình bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Để tăng cường các nguồn lực, thiết kế, phát triển các mô hình bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội, chúng ta cần thực hiện các yêu cầu sau: *Một là*, đầu tư nguồn lực con người, đặc biệt về bản lĩnh chính trị, trình độ lý luận chính trị, phương pháp, kỹ năng; *hai là*, tăng cường đầu tư cơ sở vật chất - kỹ thuật và các điều kiện bảo đảm theo hướng hiện đại; *ba là*, xây dựng mô hình lực lượng chuyên trách, nòng cốt; *bốn là*, xây dựng mô hình phối, kết hợp giữa các lực lượng nhằm phát huy vai trò, sức mạnh tổng hợp và ưu thế của tất cả các lực lượng, từ Trung ương đến cơ sở, trên tất cả các lĩnh vực trong bảo vệ nền

tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Thứ năm, sử dụng sức mạnh tổng hợp của cả hệ thống chính trị, các tổ chức xã hội trong bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Để phát huy sức mạnh tổng hợp của cả hệ thống chính trị và các tổ chức xã hội trong bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội, chúng ta cần thực hiện các yêu cầu sau: *Một là*, các cơ quan trong hệ thống chính trị phải thường xuyên bám sát các chỉ đạo, định hướng, hướng dẫn của Ban Chấp hành Trung ương, Bộ Chính trị, Ban Bí thư về đấu tranh phản bác các quan điểm sai trái, thù địch, bảo vệ nền tảng tư tưởng của Đảng; *hai là*, các cơ quan trong hệ thống chính trị tùy theo chức năng, nhiệm vụ của mình, hằng năm cần xây dựng kế hoạch, chương trình, giải pháp cụ thể để thực hiện nội dung đấu tranh phản bác các quan điểm sai trái, thù địch, bảo vệ nền tảng tư tưởng của Đảng; *ba là*, tăng cường công tác lãnh đạo, chỉ đạo, rà soát để chủ động nắm tình hình, phát hiện sớm hoạt động của các đối tượng chống phá, xuyên tạc. Rà soát thường xuyên, nắm tình hình, phát hiện các trang blog, trang facebook, trang website, các diễn đàn thường đăng tải các thông tin không đúng sự thật, xuyên tạc, chống phá nền tảng tư tưởng của Đảng; *bốn là*, phát huy vai trò của cấp ủy, tổ chức đảng, người đứng đầu, ban tuyên giáo các cấp, Ban Chỉ đạo 35, cơ quan chức năng các cấp, nhất là vai trò, trách nhiệm nêu gương của cán bộ, đảng viên; *năm là*, cấp ủy, chính quyền các cấp cần tích cực thông tin và tăng

cường đối thoại với nhân dân; chủ động, linh hoạt tham gia các vấn đề cụ thể của xã hội. Thường xuyên duy trì, thực hiện có hiệu quả việc phối hợp với các cơ quan chức năng. Phát huy vai trò của các cơ quan báo chí, tạo thế trận rộng khắp, chặt chẽ trong đấu tranh phản bác các quan điểm sai trái, thù địch, bảo vệ nền tảng tư tưởng của Đảng; *sáu là*, lồng ghép hoạt động bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội trong các sinh hoạt của đảng bộ, chi bộ, tăng cường tổ chức sinh hoạt chuyên đề tại các chi bộ; *bảy là*, tăng cường hoạt động quản lý, kiểm soát đối với các trang mạng xã hội và chủ động sử dụng các biện pháp kỹ thuật, ngăn chặn việc truy cập vào các trang mạng “độc hại” một cách có hiệu quả. Nâng cao nhận thức và đề cao cảnh giác với các biểu hiện của bệnh giáo điều, cơ hội, thực dụng và xét lại trên mạng xã hội ngay trong đội ngũ cán bộ, đảng viên của hệ thống chính trị và các tổ chức xã hội. Xây dựng thế trận lòng dân, xây dựng lực lượng có tính toàn dân, rộng rãi để đấu tranh bảo vệ nền tảng tư tưởng của Đảng, ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Thứ sáu, tăng cường ứng dụng khoa học - kỹ thuật và công nghệ trong bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội.

Để bảo vệ nền tảng tư tưởng của Đảng và đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội có hiệu quả, cần hết sức coi trọng ứng dụng khoa học - kỹ thuật và công nghệ trong hoạt động này, cụ thể: *một là*, đẩy mạnh ứng dụng công nghệ thông tin, trí tuệ nhân tạo,

quan tâm đầu tư cơ sở vật chất, trang thiết bị điện tử phục vụ nhiệm vụ đấu tranh phản bác quan điểm sai trái, thù địch trên internet, mạng xã hội; *hai là*, hoàn thiện hệ thống pháp luật về sử dụng internet và mạng xã hội, bảo đảm môi trường pháp lý bình đẳng và minh bạch, tạo ra khung pháp lý nhằm răn đe, xử lý cá nhân, tổ chức đưa thông tin giả mạo trên internet và mạng xã hội; *ba là*, kiên quyết đấu tranh chống các quan điểm sai trái, thù địch, những đối tượng cơ hội chính trị trên không gian mạng nói chung, mạng xã hội facebook nói riêng; *bốn là*, tăng cường đầu tư tiềm lực cho lực lượng chuyên trách bảo vệ an ninh mạng, nhất là trình độ khoa học công nghệ, kỹ thuật, nghiệp vụ nhằm chủ động, kịp thời phòng ngừa, ngăn chặn, vô hiệu hóa từ xa các hoạt động không gian mạng xâm phạm an ninh quốc gia; *năm là*, tăng cường mở rộng hợp tác quốc tế trên lĩnh vực bảo vệ an ninh mạng.

Tóm lại, trong bối cảnh Cách mạng công nghiệp lần thứ tư đang diễn ra mạnh mẽ, một thế giới số đầy tiềm năng nhưng cũng đầy thách thức mở ra đối với mỗi cá nhân và dân tộc Việt Nam, chúng ta cần tận dụng tốt những cơ hội và khắc phục, ngăn ngừa những nguy cơ, thách thức đối với sự nghiệp xây dựng chủ nghĩa xã hội. Nghiên cứu về định hướng, giải pháp bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên mạng xã hội chính là nhằm góp phần thực hiện mục đích ấy. Hy vọng với việc thực hiện đồng bộ các giải pháp trên sẽ góp phần quan trọng vào sự nghiệp bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn có hiệu quả các quan điểm sai trái, thù địch trên môi trường mạng xã hội, góp phần xây dựng thành công chủ nghĩa xã hội ở nước ta.

Ý NGHĨA CỦA VIỆC SỬ DỤNG INTERNET VÀ MẠNG XÃ HỘI CÓ TRÁCH NHIỆM

PGS.TS. NGUYỄN XUÂN TOÀN*

Sau hơn 20 năm xuất hiện tại Việt Nam, internet mang lại nhiều giá trị tích cực, góp phần nâng cao đời sống vật chất và tinh thần của người dân và phát triển đất nước về mọi mặt. Tuy nhiên, internet và mạng xã hội cũng gây ra nhiều hệ lụy. Lợi dụng internet và mạng xã hội, các thế lực thù địch, phản động, các loại tội phạm gia tăng hoạt động, gây hậu quả ngày càng nghiêm trọng. Môi trường mạng đang bị vẩn đục bởi các hành vi giao tiếp, ứng xử thiếu văn hóa, lợi dụng các diễn đàn công khai để đả kích, nói xấu, bôi nhọ lẫn nhau, đặc biệt là đưa thông tin sai sự thật, gây hoang mang dư luận. Xây dựng môi trường văn hóa mạng thực sự an toàn, lành mạnh là nhu cầu cấp thiết, trong đó, việc sử dụng internet và mạng xã hội có trách nhiệm của các chủ thể có vai trò, ý nghĩa quan trọng hàng đầu.

1. Đặt vấn đề

Internet chính thức có mặt tại Việt Nam từ năm 1997; mạng xã hội được du nhập vào nước ta từ những năm 2000

* Đại học Quốc gia Hà Nội.

dưới hình thức các trang nhật ký điện tử (blog). Từ đó đến nay, internet, mạng xã hội đã phát triển nhanh chóng, ngày càng thâm nhập vào mọi mặt đời sống xã hội. Sử dụng thiết bị di động thông minh, internet, mạng xã hội dần trở thành nhu cầu của đa số người dân thuộc các tầng lớp khác nhau, từ cán bộ, công chức, viên chức, người lao động đến học sinh, sinh viên, người về hưu, người nội trợ... Hiện nay, Việt Nam là nước có số lượng người dùng internet và mạng xã hội thuộc tốp đầu trên thế giới. Theo thống kê của các cơ quan chức năng và cơ quan truyền thông, năm 2020, ở nước ta đã có hơn 68 triệu người dùng internet (chiếm khoảng 70% dân số) với hơn 145 triệu thiết bị di động được kết nối với internet; tính đến tháng 6/2021, tổng số người dùng mạng xã hội ở nước ta đã lên tới hơn 80 triệu người, có 829 mạng xã hội đã được cấp phép, trong đó, một số mạng có số lượng người dùng lớn (hàng chục triệu người) như Facebook, YouTube, Zalo...

Sự phát triển không ngừng của các dịch vụ internet, nhất là sự xuất hiện và phát triển nhanh chóng của các kết nối không dây, các thiết bị di động thông minh, dịch vụ điện toán đám mây và mạng xã hội đã tạo thuận lợi cho mọi người kết nối, tương tác đa chiều, phản ánh sinh động, nhanh chóng muôn mặt đời sống xã hội. Internet và mạng xã hội đã trở thành không gian xã hội mới của con người (được gọi là “không gian mạng”). Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi

không gian và thời gian¹. Ngày nay, không gian mạng đã trở thành “*không gian chiến lược mới*”, “*vùng lãnh thổ đặc biệt*” gắn chặt với chủ quyền về đất liền, biển, đảo, trên không và vũ trụ; là ưu tiên hàng đầu của quốc gia trên tất cả các cấp độ: chính phủ, doanh nghiệp, người dân để xây dựng không gian mạng an toàn, lành mạnh, trở thành nguồn lực quan trọng cho phát triển kinh tế - xã hội.

Trong những năm qua, Việt Nam đã đẩy mạnh phát triển và ứng dụng công nghệ thông tin, sử dụng hiệu quả internet, mạng xã hội trong phát triển các lĩnh vực của đời sống xã hội, chủ động tham gia vào Cách mạng công nghiệp lần thứ tư và đạt được nhiều thành tựu quan trọng. Kết cấu hạ tầng viễn thông được xây dựng khá đồng bộ. Kinh tế số được hình thành, phát triển nhanh, ngày càng trở thành bộ phận quan trọng của nền kinh tế; công nghệ số được áp dụng trong các ngành công nghiệp, nông nghiệp và dịch vụ; xuất hiện ngày càng nhiều hình thức kinh doanh, dịch vụ mới, xuyên quốc gia, dựa trên nền tảng công nghệ số và internet đang tạo nhiều cơ hội việc làm, thu nhập, tiện ích, nâng cao chất lượng cuộc sống của người dân. Việc xây dựng chính phủ điện tử, tiến tới chính phủ số được triển khai quyết liệt, bước đầu đạt được nhiều kết quả tích cực². Công nghiệp công nghệ thông tin - truyền thông, từ chỗ là một ngành công nghiệp nhỏ bé, sau 20 năm, đã trở thành ngành kinh tế (cấp II) lớn nhất,

1. Xem *Luật an ninh mạng* năm 2018.

2. Xem 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*.

có mức tăng trưởng cao nhất, có năng suất lao động cao nhất và giá trị xuất khẩu lớn nhất. Lao động của ngành công nghệ thông tin - truyền thông chỉ hơn 1 triệu người, thấp hơn một số ngành khác, nhưng đóng góp vào GDP của Việt Nam lớn nhất (14,3%)¹. Phát triển, ứng dụng công nghệ thông tin, sử dụng internet, mạng xã hội đã góp phần quan trọng củng cố, nâng cao chất lượng, hiệu quả hoạt động bảo đảm quốc phòng, an ninh và đối ngoại của đất nước. Đối với các tầng lớp nhân dân, internet và mạng xã hội mang lại nhiều lợi ích, giá trị tích cực: cho phép người dùng tìm kiếm, chia sẻ thông tin trên tất cả các lĩnh vực; thể hiện bản thân, giao lưu, gắn kết cộng đồng, chia sẻ tình cảm; giải trí và trải nghiệm cuộc sống; là môi trường học tập, làm việc, kinh doanh hiệu quả; thúc đẩy các lĩnh vực khác của đời sống xã hội. Internet và mạng xã hội đã trở thành “người bạn đồng hành” của giới trẻ và các tầng lớp khác nhau trong xã hội.

Tuy nhiên, internet và mạng xã hội cũng có thể gây ra nhiều hệ lụy. Những năm gần đây, mạng xã hội đã trở thành môi trường để một số người truyền bá luận điệu sai trái, phát tán thông tin xấu, độc, gây hại, công bố phát ngôn gây thù hận. Các thế lực thù địch, phản động lợi dụng mạng xã hội để hô hào tụ tập đông người phản đối chủ trương, chính sách của Đảng và Nhà nước, kích động dư luận, biến bức xúc thành bạo động, khiến sinh hoạt xã hội trở nên phức tạp.

1. Xem GS. Nguyễn Thiện Nhân: “Sự phát triển vượt bậc của công nghiệp công nghệ thông tin và triển vọng đột phá tăng năng suất lao động, đổi mới mô hình tăng trưởng của Việt Nam”, báo *Nhân Dân điện tử*, ngày 26/12/2020.

Họ triệt để lợi dụng mạng xã hội để hình thành cái gọi là “truyền thông độc lập”, tách khỏi sự quản lý của Nhà nước; thực hiện các thủ đoạn tuyên truyền phá hoại tư tưởng, kích động tâm lý hoài nghi với chính quyền, thổi bùng bức xúc trong nhân dân để tạo điều kiện, môi trường thực hiện “cách mạng màu”; cổ xúy cho các luận điệu dân chủ, nhân quyền, đòi tự do biểu tình, tự do ngôn luận, tự do lập hội, tự do báo chí, tự do tôn giáo theo quan điểm phương Tây, thúc đẩy “tự diễn biến”, “tự chuyển hóa” trong nội bộ, tiến hành “diễn biến hòa bình” để âm mưu chuyển hóa chính trị tại Việt Nam. Tội phạm mạng, tội phạm sử dụng công nghệ cao gia tăng, diễn biến ngày càng phức tạp, gây hậu quả ngày càng nghiêm trọng, nhất là các hành vi xâm phạm an ninh quốc gia, lừa đảo, chiếm đoạt tài sản, đánh bạc, tổ chức đánh bạc, cho vay lãi nặng, tán phát, tuyên truyền văn hóa phẩm đồi trụy...

Đáng chú ý là nạn tin giả, đưa thông tin sai sự thật, gây hoang mang dư luận ngày càng gia tăng trên môi trường mạng. Trong một số trường hợp, mạng xã hội làm cho thông tin chính thống bị nhiễu loạn, ảnh hưởng xấu đến an ninh, trật tự, an toàn xã hội. Có thể nói, mạng xã hội đang giống như “mê hồn trận”, làm cho người tiếp cận khó phân biệt đâu là tin thật, đâu là tin giả. Thời gian qua, lợi dụng diễn biến phức tạp của đại dịch Covid-19, các thế lực thù địch, phản động trong và ngoài nước đã lợi dụng phát tán trên mạng nhiều thông tin sai sự thật, xuyên tạc tình hình dịch bệnh và công tác chỉ đạo, điều hành của Chính phủ và các bộ, ngành, địa phương trong nỗ lực phòng, chống dịch Covid-19 tại Việt Nam. Nhiều cá nhân đã đăng tải những thông tin sai sự thật, làm nhiễu loạn, tạo tâm lý hoang mang, gây khó khăn

cho công tác phòng, chống dịch của Nhà nước, các cấp, các ngành, các địa phương¹.

Thật đáng buồn là môi trường mạng đang bị vẩn đục bởi các hành vi giao tiếp, ứng xử thiếu văn hóa. Một số người lợi dụng các diễn đàn công khai để thể hiện hành vi phản văn hóa, vi phạm thuần phong mỹ tục, sử dụng ngôn từ tục tĩu để thóa mạ, chửi bới người không có cùng quan điểm, đả kích, nói xấu, bôi nhọ lẫn nhau. Không thiếu những lời nói tục, chửi thề, những phát ngôn gây sốc, những hành động trả thù bằng video clip, những lời bình luận miệt thị hay “ném đá” tập thể. Các biểu hiện lệch lạc về tư tưởng, đạo đức, văn hóa truyền thống trên mạng đã đến mức đáng báo động. Nếu không sớm có biện pháp giáo dục, chấn chỉnh kịp thời, các thiết chế, chế tài ngăn chặn thì rất có thể những hiện tượng đó sẽ tiếp tục lan rộng và phát triển thành những hành vi nguy hiểm cho xã hội, làm mất đi hình ảnh đẹp về đất nước, con người, văn hóa Việt Nam trên trường quốc tế.

An ninh mạng là lĩnh vực thuộc an ninh phi truyền thống, bảo đảm an ninh mạng ngày càng trở nên cấp thiết hơn đối với nước ta, nhất là trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư và xây dựng chính phủ số, nền kinh tế số, xã hội số đang được đẩy mạnh hiện nay. Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII của Đảng xác định

1. Xem “Không gian mạng gắn chặt với chủ quyền quốc gia”, mic.gov.vn, truy cập ngày 10/11/2020; Cao Xuân - Hồng Mai: “Không để tin giả phá hoại nỗ lực phòng, chống dịch bệnh”, *Công an nhân dân online*, truy cập ngày 08/8/2021.

phải bảo vệ chủ quyền quốc gia trên không gian mạng¹. Nhà nước ta đã ban hành Luật an ninh mạng, Luật an toàn thông tin mạng, các luật chuyên ngành liên quan, nhiều văn bản hướng dẫn, quy định chi tiết các luật đó. Bộ quy tắc ứng xử trên mạng xã hội cũng vừa được Bộ Thông tin và Truyền thông ban hành². Xây dựng môi trường văn hóa mạng thực sự an toàn, lành mạnh là nhu cầu cấp thiết, trong đó, việc sử dụng mạng internet và mạng xã hội có trách nhiệm của các chủ thể có vai trò, ý nghĩa quan trọng hàng đầu.

2. Ý nghĩa của việc sử dụng internet và mạng xã hội có trách nhiệm

Internet và mạng xã hội có an toàn, lành mạnh hay không liên quan đến trách nhiệm của các chủ thể (người dùng mạng, người cung cấp dịch vụ mạng). Trách nhiệm ở đây được hiểu là trách nhiệm của chủ thể đối với Nhà nước, xã hội (cộng đồng) và bản thân, xét trên các phương diện pháp luật, đạo đức và văn hóa khi sử dụng mạng, cung cấp dịch vụ mạng.

Về phương diện pháp luật:

Pháp luật là hệ thống các quy tắc xử sự chung do nhà nước ban hành hoặc là thừa nhận, mang tính bắt buộc phải thực hiện và được bảo đảm thực hiện bằng các biện pháp giáo

1. Xem Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.I, tr.280.

2. Quyết định số 874/QĐ-BTTTT, ngày 17/6/2021 của Bộ Thông tin và Truyền thông ban hành Bộ quy tắc ứng xử trên mạng xã hội.

dục, cưỡng chế nhằm điều chỉnh các quan hệ xã hội. Bất cứ nhà nước nào cũng xây dựng, hoàn thiện hệ thống pháp luật của mình để điều chỉnh các quan hệ xã hội trên tất cả các lĩnh vực của đời sống xã hội. Việt Nam không phải ngoại lệ. Các tổ chức, cá nhân phải nghiêm chỉnh thực hiện pháp luật (có bốn hình thức: tuân thủ, thi hành, sử dụng, áp dụng pháp luật). Theo đó, cơ quan, tổ chức Việt Nam hoạt động trên cơ sở Hiến pháp và pháp luật; công dân Việt Nam sống, làm việc theo Hiến pháp và pháp luật; tổ chức, cá nhân nước ngoài sinh sống, làm việc tại Việt Nam phải tuân thủ pháp luật Việt Nam.

Trong nhà nước pháp quyền, quyền của mỗi chủ thể luôn đi liền với nghĩa vụ. Sử dụng internet, mạng xã hội là quyền tự do của mỗi chủ thể nhưng việc sử dụng internet, mạng xã hội có trách nhiệm phải được hiểu là nghĩa vụ của các chủ thể đó. Nghĩa vụ ở đây chính là nghĩa vụ tôn trọng, nghiêm chỉnh thực hiện pháp luật Việt Nam, áp dụng đối với mọi chủ thể. Xã hội văn minh là xã hội ở đó mọi công dân đều có tinh thần và ý thức thượng tôn pháp luật. Muốn đất nước ổn định và phát triển, cùng với nỗ lực của chính quyền, của mọi công dân, cộng đồng, thì ý thức tôn trọng, tuân thủ pháp luật là một trong các yếu tố giữ vai trò chi phối, bảo đảm các nguyên tắc cơ bản quyết định sự phát triển an toàn, lành mạnh của xã hội. Nếu cố tình đi ngược lại hoặc phá hoại các nguyên tắc đó là vô trách nhiệm đối với xã hội và con người.

Vì vậy, khi sử dụng internet, mạng xã hội, các chủ thể có trách nhiệm ứng xử phù hợp (tôn trọng, thực hiện nghiêm chỉnh) các chuẩn mực pháp lý của Việt Nam nói chung, quy định của pháp luật trong lĩnh vực an toàn, an ninh thông tin,

an ninh mạng, về sử dụng internet, mạng xã hội nói riêng; tôn trọng quyền và lợi ích hợp pháp của tổ chức, cá nhân và phải chịu trách nhiệm về các hành vi, ứng xử của mình trên mạng. Với các hành vi, ứng xử ngược lại, chủ thể sẽ bị đánh giá là vi phạm tiêu chuẩn cộng đồng, vi phạm pháp luật, thậm chí là tội phạm và sẽ bị xử lý tùy theo mức độ vi phạm. Chủ thể vi phạm có trách nhiệm phối hợp với các cơ quan chức năng để xử lý hành vi, nội dung thông tin vi phạm pháp luật.

Về phương diện đạo đức:

Đạo đức là hệ thống các quy tắc, chuẩn mực xã hội mà nhờ đó con người tự giác điều chỉnh hành vi của mình cho phù hợp với lợi ích của cộng đồng, của xã hội. Những quy tắc và chuẩn mực đạo đức phổ biến gồm: độ lượng, khoan dung, chính trực, khiêm tốn, dũng cảm, trung thực, tín, thiện; nó đối lập với tàn bạo, tham lam, kiêu ngạo, hèn nhát, phản bội, bất tín... Đạo đức của người cán bộ, đảng viên là đạo đức cách mạng, thể hiện ở phẩm chất chính trị, tư tưởng, đạo đức, lối sống, là lòng trung thành vô hạn đối với Đảng, với Tổ quốc, với nhân dân, với chế độ xã hội chủ nghĩa; là trình độ giác ngộ mục tiêu, lý tưởng xã hội chủ nghĩa, sẵn sàng chiến đấu, hy sinh vì mục tiêu, lý tưởng cao đẹp đó. Đạo đức được thể hiện ở sự trong sáng, thành thật, trung thực, không cơ hội, thật sự cần, kiệm, liêm, chính, chí công vô tư, biết hy sinh lợi ích cá nhân để phục tùng lợi ích tập thể, lợi ích của Tổ quốc, của nhân dân. Có lối sống trong sạch, lành mạnh, gần gũi với quần chúng, gương mẫu gắn bó với nhân dân, khiêm tốn học hỏi, thực sự cầu thị. Có tinh thần đoàn kết, thương yêu, tương thân,

tương ái lẫn nhau. Bác Hồ coi đạo đức cách mạng là “nền tảng”, là “cái gốc” của người cán bộ.

Internet, mạng xã hội đã trở thành không gian xã hội mới, nơi con người có thể thực hiện các hành vi mang bản chất xã hội của mình, không bị giới hạn bởi không gian và thời gian. Các hành vi của con người trên không gian mạng như giao tiếp, sáng tạo, lao động, sản xuất, tiêu dùng, học tập và vui chơi giải trí thể hiện đạo đức của chủ thể như các hành vi trong đời thực: yêu/ghét, trung thực/lừa dối, khiêm nhường/kiêu ngạo, trung thành/phản bội... Các hành vi đó cũng có thể mang lại kết quả hoặc hậu quả trong đời thực. Rõ ràng, mạng tuy được coi là “không gian ảo” nhưng đạo đức, hành vi của con người thể hiện trên đó là thật, những tác động (nhất là hậu quả) của nó thì lại rất thật và có thể liên quan đến nhiều chủ thể, trong một thời gian dài.

Vì vậy, khi sử dụng internet, mạng xã hội, các chủ thể có trách nhiệm ứng xử phù hợp với các giá trị đạo đức truyền thống tốt đẹp của dân tộc Việt Nam và rộng ra là phù hợp với giá trị đạo đức tốt đẹp của toàn nhân loại. Với các hành vi, ứng xử ngược lại, chủ thể sẽ bị đánh giá là ứng xử thiếu chuẩn mực đạo đức, thậm chí vô đạo đức và sẽ bị cộng đồng phản bác, lên án, tẩy chay; trường hợp vi phạm nghiêm trọng sẽ bị xử lý.

Về phương diện văn hóa:

Văn hóa ứng xử là hệ thống giá trị chi phối nhận thức, thái độ và hành vi ứng xử của cá nhân và cộng đồng người trong các mối quan hệ giữa con người với môi trường tự nhiên, môi trường xã hội và với chính bản thân mình, dựa trên các chuẩn mực xã hội. Đó là sức mạnh mềm làm nên nét

đẹp và là chìa khóa thành công của mỗi người, mỗi dân tộc. Dân tộc nào cũng có văn hóa ứng xử riêng, đồng thời thể hiện đặc trưng văn hóa ứng xử chung của toàn nhân loại.

Thực tiễn sử dụng internet, mạng xã hội của các chủ thể đã hình thành nên văn hóa ứng xử trên mạng. Trong mối quan hệ với chính bản thân chủ thể, văn hóa ứng xử trên internet, mạng xã hội được thể hiện với các giá trị như: sự khiêm tốn, thật thà, dũng cảm, có chính kiến, lập trường, quan điểm rõ ràng; tinh thần cầu thị, học hỏi, không tự kiêu, tự đại hoặc tâm lý tự ti, thiếu tin tưởng vào bản thân... Do đặc điểm các mối quan hệ trên mạng có phạm vi rất rộng, đa dạng và khó kiểm soát hơn mối quan hệ trong đời thực nên văn hóa ứng xử trên internet, mạng xã hội được thể hiện với các giá trị như: cẩn trọng, trung thực, tôn trọng người khác, biết quan tâm, lắng nghe, chia sẻ, thông cảm, kiềm chế cảm xúc và hành vi thái quá, có ý thức giữ gìn bản sắc văn hóa của dân tộc, giữ gìn sự trong sáng của tiếng Việt...

Vì vậy, khi sử dụng internet, mạng xã hội, các chủ thể có trách nhiệm ứng xử phù hợp với các giá trị văn hóa truyền thống tốt đẹp của dân tộc Việt Nam và cũng là đặc trưng giá trị văn hóa chung của toàn nhân loại. Với các hành vi, ứng xử ngược lại, chủ thể sẽ bị đánh giá là ứng xử thiếu chuẩn mực văn hóa, thậm chí vô văn hóa và sẽ bị cộng đồng phản bác, lên án, tẩy chay; trường hợp vi phạm nghiêm trọng sẽ bị xử lý.

Ý nghĩa của việc sử dụng internet, mạng xã hội có trách nhiệm được hiểu là giá trị, tác dụng mang lại từ việc sử dụng mạng một cách an toàn, lành mạnh đối với các chủ thể. Việc sử dụng internet và mạng xã hội có trách nhiệm

mang lại ý nghĩa thiết thực cho nhiều chủ thể, thể hiện ở nhiều khía cạnh khác nhau, trên các phương diện pháp luật, đạo đức và văn hóa. Theo cách tiếp cận đó, xin nêu tóm tắt ý nghĩa của việc sử dụng internet và mạng xã hội có trách nhiệm đối với một số chủ thể.

Đối với công dân, ý nghĩa của việc sử dụng internet và mạng xã hội có trách nhiệm thể hiện trên các khía cạnh sau đây:

- Thể hiện ý thức công dân, sự nghiêm chỉnh thực hiện Hiến pháp và pháp luật của Nhà nước.

- Thể hiện phẩm chất đạo đức: sự tôn trọng người khác, tôn trọng cộng đồng, tính khách quan, sự trung thực, lòng tự trọng, sự ôn hòa, tính nhân văn...

- Thể hiện yếu tố văn hóa, văn minh: phát ngôn, hành vi ứng xử chuẩn mực trên môi trường mạng như ứng xử trong môi trường sống thật, phù hợp các chuẩn mực văn hóa, truyền thống tốt đẹp của dân tộc.

- Thể hiện lòng yêu nước, bản lĩnh cá nhân: sự dũng cảm thể hiện quan điểm, chính kiến trước hiện tượng tiêu cực, tệ nạn, phản văn hóa, phản khoa học, vi phạm pháp luật và tội phạm; tinh táo, vững vàng trước các cám dỗ...

- Thể hiện trình độ hiểu biết về các lĩnh vực: pháp luật, công nghệ thông tin, văn hóa - xã hội và các lĩnh vực khác.

- Thể hiện tính mục đích, sự quyết đoán: sử dụng mạng để kinh doanh, học tập, làm việc; nắm bắt cơ hội do mạng mang lại, rèn kỹ năng nghề nghiệp, làm việc, kinh doanh, học tập hiệu quả...

- Thể hiện là người sản xuất, người tiêu dùng thông minh: người dân tham gia mạng vừa là người sản xuất, vừa

là người tiêu dùng (thông tin, sản phẩm), họ biết sử dụng mạng có trách nhiệm vào những việc có ích, có lợi cho mình, cho cộng đồng và góp phần làm cho môi trường mạng an toàn, lành mạnh; tránh hệ lụy tiêu cực do mạng mang lại.

Đối với cán bộ, đảng viên (bao gồm: đảng viên, cán bộ, công chức, viên chức, đoàn thể, lực lượng vũ trang), ý nghĩa của việc sử dụng internet và mạng xã hội có trách nhiệm thể hiện trên các khía cạnh sau đây:

- Trước hết, với vai trò là công dân, việc sử dụng mạng có trách nhiệm thể hiện mình là công dân tốt, có tinh thần thượng tôn pháp luật, thực hiện nghiêm chỉnh pháp luật.

- Là cách để thể hiện yếu tố đạo đức, văn hóa, văn minh của một cá nhân khi tham gia các hoạt động trên không gian mạng.

- Thể hiện sự gương mẫu, nêu gương của cán bộ, đảng viên; là một tiêu chí để khẳng định cán bộ, đảng viên đã thực hiện tốt việc tu dưỡng, rèn luyện bản thân phù hợp với các tiêu chí và quy định của tổ chức mà mình là thành viên (Đảng, Nhà nước, Mặt trận Tổ quốc, đoàn thể, đơn vị vũ trang, đơn vị sự nghiệp công lập).

- Sử dụng không gian mạng có trách nhiệm là góp phần bảo vệ Đảng, Nhà nước và chế độ, thể hiện trong việc tích cực tham gia viết bài, nêu ý kiến phản bác, vạch trần các luận điệu sai trái, thù địch, các thủ đoạn phá hoại tư tưởng; phòng, chống tội phạm, vi phạm pháp luật, tham nhũng, tiêu cực, lãng phí; chống các biểu hiện “tự diễn biến”, “tự chuyển hóa” trong nội bộ; bảo vệ Tổ quốc, nhân dân, bảo vệ Đảng, Nhà nước, chế độ.

- Sử dụng mạng có trách nhiệm còn là cơ sở để các cơ quan có thẩm quyền giám sát, đánh giá về đạo đức, văn hóa ứng xử, sinh hoạt, nhận thức, lối sống của cán bộ, đảng viên thể hiện khi tham gia mạng xã hội. Trên cơ sở đó, các cơ quan, đơn vị, tổ chức đảng có thể thực hiện việc giám sát, đánh giá công tác thi đua, khen thưởng, kỷ luật chính xác hơn; phân tích chất lượng đảng viên và thực hiện công tác cán bộ phù hợp hơn.

Đối với cơ quan, tổ chức, ý nghĩa của việc sử dụng internet và mạng xã hội có trách nhiệm thể hiện trên các khía cạnh sau đây:

- Cơ quan, tổ chức được thành lập, hoạt động trên cơ sở pháp luật; sử dụng internet, mạng xã hội là một phương thức hoạt động mới, có hiệu quả cao. Việc sử dụng internet và mạng xã hội có trách nhiệm thể hiện cơ quan, tổ chức tôn trọng, tuân thủ pháp luật, thích ứng với phương thức làm việc mới, nâng cao hiệu quả hoạt động thực hiện chức năng, nhiệm vụ, quyền hạn của mình.

- Là một chủ thể người dùng internet, mạng xã hội, cơ quan nhà nước vừa phải có trách nhiệm trong sử dụng mạng an toàn, lành mạnh, phục vụ chính các hoạt động của mình, đồng thời, với vai trò chủ thể quản lý, cơ quan nhà nước còn phải tạo ra, cung cấp các bảo đảm (pháp lý, quy tắc, hạ tầng kỹ thuật, quản lý...) tạo điều kiện cho các chủ thể khác có thể thực hiện được trách nhiệm của mình trong quá trình sử dụng internet, mạng xã hội một cách an toàn, lành mạnh.

- Sử dụng mạng có trách nhiệm, bảo đảm mạng được phát triển, sử dụng an toàn, lành mạnh, qua đó, Nhà nước thực hiện được trách nhiệm của mình là bảo vệ chủ quyền quốc gia, bảo vệ quyền con người trên không gian mạng.

- Nhà nước là chủ thể quản lý mọi lĩnh vực của đời sống xã hội, trong đó có lĩnh vực an toàn, an ninh thông tin, an ninh mạng. Nhà nước cùng các chủ thể sử dụng mạng có trách nhiệm góp phần bảo đảm mạng được phát triển, sử dụng an toàn, lành mạnh, đây là điều kiện, môi trường thuận lợi để nâng cao hiệu lực, hiệu quả quản lý nhà nước trên các lĩnh vực của đời sống xã hội, nhất là trong bối cảnh Cách mạng công nghiệp lần thứ tư, xây dựng chính phủ số, nền kinh tế số, xã hội số hiện nay.

Đối với gia đình, nhà trường, xã hội (cộng đồng), ý nghĩa của việc sử dụng internet và mạng xã hội có trách nhiệm thể hiện trên các khía cạnh sau đây:

- Thể hiện ý thức tôn trọng, tuân thủ pháp luật của các chủ thể trong gia đình, nhà trường và xã hội (cộng đồng).

- Thể hiện vai trò, trách nhiệm của gia đình đối với việc bảo đảm điều kiện thuận lợi để sinh viên, học sinh học tập, vui chơi, giải trí; phát huy những lợi thế và hạn chế những mặt trái, hệ lụy của internet, mạng xã hội, chủ động bảo vệ trẻ em khi cho tham gia, sử dụng máy tính, thiết bị thông minh truy cập vào mạng.

- Thể hiện sự chủ động nắm bắt cơ hội trong triển khai phương thức dạy - học mới, nâng cao chất lượng, hiệu quả dạy - học, nghiên cứu khoa học và công tác quản lý của nhà trường; tạo môi trường an toàn, lành mạnh để sinh viên, học sinh học tập, rèn luyện, phát triển lành mạnh, đạt các mục tiêu giáo dục, đào tạo và phát triển nhân cách.

- An ninh, an toàn thông tin, an ninh mạng được bảo đảm, không gian mạng an toàn, lành mạnh là điều kiện, môi trường để phát triển đất nước về mọi mặt, gia tăng các giá trị

của cuộc sống, nâng cao đời sống vật chất và tinh thần của nhân dân. Nếu xã hội có nhiều người sử dụng không gian mạng có trách nhiệm thì xã hội ít xảy ra các vi phạm pháp luật, tội phạm, vi phạm thuần phong mỹ tục, tập quán, truyền thống của địa phương, quốc gia - dân tộc, góp phần tạo nên môi trường mạng lành mạnh, an toàn, văn minh, tiến bộ.

Đối với tổ chức, cá nhân nước ngoài tại Việt Nam, ý nghĩa của việc sử dụng internet và mạng xã hội có trách nhiệm thể hiện trên các khía cạnh sau đây:

- Thể hiện tổ chức, cá nhân nước ngoài ở Việt Nam được bảo đảm quyền tự do ngôn luận, tự do trong tiếp cận, sử dụng internet, mạng xã hội tại Việt Nam, không bị cản trở, ngăn cấm.

- Biểu hiện về việc thực hiện nghĩa vụ tôn trọng, tuân thủ pháp luật Việt Nam và luật pháp quốc tế, tôn trọng chủ quyền của Việt Nam trên không gian mạng; là cơ sở để hoàn thành chức trách, vị trí công việc của họ tại Việt Nam.

- Thể hiện đạo đức và văn hóa giao tiếp, ứng xử của chủ thể; thể hiện sự hiểu biết về phong tục, tập quán, truyền thống văn hóa của nước sở tại.

Đối với doanh nghiệp cung cấp dịch vụ mạng, ý nghĩa của việc sử dụng internet và mạng xã hội có trách nhiệm thể hiện trên các khía cạnh sau đây:

- Thể hiện doanh nghiệp làm tròn nghĩa vụ tôn trọng, tuân thủ pháp luật Việt Nam; tôn trọng quyền của người sử dụng mạng (là khách hàng của mình).

- Là bảo đảm cho sự phát triển bền vững của doanh nghiệp, góp phần xây dựng môi trường văn hóa trong doanh

nghiệp và xây dựng đội ngũ doanh nhân, người lao động có đạo đức, có văn hóa.

3. Giải pháp để các chủ thể có thể sử dụng internet và mạng xã hội một cách có trách nhiệm

Để sử dụng internet và mạng xã hội một cách có trách nhiệm, làm cho môi trường mạng an toàn, lành mạnh, phục vụ hữu ích cho sự phát triển đất nước và đời sống người dân, cần có sự vào cuộc của cả hệ thống chính trị, gia đình, nhà trường, cộng đồng, người dân và doanh nghiệp. Với vị trí, vai trò, trách nhiệm của mình, các chủ thể thực hiện đồng bộ nhiều giải pháp cụ thể để xây dựng văn hóa mạng (trước hết là văn hóa ứng xử trên mạng xã hội) thực sự lành mạnh. Xin nêu một số định hướng giải pháp chung như sau:

- Tiếp tục hoàn thiện chính sách, pháp luật về lĩnh vực này, trước hết là hoàn thiện các văn bản hướng dẫn, quy định chi tiết Luật an ninh mạng. Tích cực tuyên truyền sâu rộng hơn nữa Luật an ninh mạng, Luật an toàn thông tin mạng, Luật bảo vệ bí mật nhà nước, các luật, pháp lệnh có liên quan và văn bản hướng dẫn giúp mỗi người hiểu rõ ý nghĩa, giá trị, nội dung, quyền, nghĩa vụ, trách nhiệm và những hành vi bị cấm liên quan đến sử dụng mạng, văn hóa ứng xử khi tham gia mạng xã hội. Triển khai thực hiện các văn bản pháp luật và Bộ quy tắc ứng xử trên mạng xã hội.

- Văn hóa mạng là một bộ phận cấu thành của văn hóa Việt Nam, cần phải được quan tâm xây dựng, phát triển. Huy động nguồn lực và tăng cường phối hợp các lực lượng, cơ quan có trách nhiệm (tuyên giáo, văn hóa, chuyên trách an ninh mạng, thông tin và truyền thông, nhà trường, các đoàn

thể xã hội, cộng đồng và gia đình) trong giáo dục đạo đức, lối sống, xây dựng môi trường văn hóa mạng thực sự lành mạnh. Phối hợp chặt chẽ giữa tổ chức, cơ quan, nhà trường và gia đình trong xây dựng văn hóa mạng; thực hiện Đề án “Xây dựng văn hóa ứng xử trong trường học giai đoạn 2018 - 2025”; Đề án “Tăng cường quản lý, giáo dục chính trị, tư tưởng đối với học sinh, sinh viên trên môi trường mạng đến năm 2025”; Đề án “Bảo vệ và hỗ trợ trẻ em tương tác lành mạnh, sáng tạo trên môi trường mạng”. Cán bộ, đảng viên, thầy, cô giáo, các bậc phụ huynh phát huy vai trò nêu gương, phải mẫu mực về văn hóa, có biện pháp quản lý chặt chẽ khi con em tham gia mạng xã hội; có những lời khuyên hữu ích và có những tác động điều chỉnh khi cần thiết.

- Chú trọng tăng cường các biện pháp tuyên truyền nâng cao hiểu biết pháp luật, ý thức, trách nhiệm khi tham gia các nền tảng truyền thông xã hội của mọi công dân. Giáo dục định hướng giá trị để người trẻ biết tránh khỏi các biểu hiện lệch lạc về nhận thức và hành vi. Tăng cường đăng tải bài viết phân tích lợi ích, tác hại của mạng, hướng dẫn cách sử dụng tốt mạng xã hội. Sử dụng các giải pháp về công nghệ hỗ trợ cho xây dựng văn hóa ứng xử trên mạng xã hội; trang bị cho học sinh, sinh viên kỹ năng tự bảo vệ thông tin cá nhân, cách thức chất lọc, tiếp nhận thông tin.

- Tích cực “dọn rác trên mạng” để những giá trị đặc trưng văn hóa Việt Nam luôn được lưu giữ, bảo tồn và phát triển, thực sự trở thành nền tảng tinh thần của xã hội; là mục tiêu, động lực, đột phá phát triển kinh tế - xã hội, hội nhập quốc tế trong bối cảnh hiện nay. Xử lý nghiêm các tổ chức, cá nhân

(trong nước và nước ngoài) vi phạm pháp luật Việt Nam, bảo đảm vừa có tính răn đe nhưng vẫn nhân văn, công bằng, khi đó, cơ quan, tổ chức, người dân sẽ tuân thủ và có trách nhiệm hơn trong sử dụng mạng xã hội. Cần phải có các quy định cụ thể để các doanh nghiệp, mạng xã hội lớn cung cấp nền tảng xuyên biên giới có trách nhiệm liên đới, phải gỡ bỏ các thông tin vi phạm pháp luật Việt Nam khi được yêu cầu.

- Khi tham gia vào không gian mạng, mỗi chủ thể đồng thời là người sản xuất thông tin, người tiêu thụ thông tin và người phát tán thông tin. Suy đến cùng, không gian mạng có lành mạnh hay không, những vi phạm có thể bị ngăn chặn, đẩy lùi hay không phụ thuộc rất lớn vào nhận thức, ý thức trách nhiệm và hành vi của các chủ thể. Do đó, với tư cách chủ thể tham gia mạng, mỗi người cần nâng cao ý thức, trình độ, kỹ năng tham gia mạng xã hội đúng cách, tỉnh táo, hiệu quả, tuân thủ pháp luật, có văn hóa, có trách nhiệm, tôn trọng người khác, biết quan tâm, lắng nghe, chia sẻ, cảm thông... Cán bộ, đảng viên phải tu dưỡng, rèn luyện tư tưởng, đạo đức, tác phong, nâng cao nhận thức về mọi mặt, nêu cao tính tiên phong, gương mẫu. Mỗi cán bộ, đảng viên, đoàn viên, hội viên tham gia mạng xã hội phải giữ vai trò là lực lượng nòng cốt đăng tải, chia sẻ, lan tỏa thông tin tích cực và xem đây là giải pháp thường xuyên, lâu dài.

HOẠT ĐỘNG XUẤT BẢN GÓP PHẦN TUYÊN TRUYỀN, GIÁO DỤC NÂNG CAO NHẬN THỨC VỀ BẢO VỆ CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG

ThS. PHẠM THỊ NGỌC BÍCH*

ThS. NGUYỄN THỊ THÚY**

Sự bùng nổ của công nghệ thông tin, đã góp phần to lớn đẩy nhanh quá trình công nghiệp hóa, hiện đại hóa đất nước, thúc đẩy phát triển mọi mặt kinh tế, văn hóa, xã hội, y tế, giáo dục, phát huy sức sáng tạo và quyền làm chủ của nhân dân, giữ vững an ninh, quốc phòng. Sự phát triển vượt bậc của công nghệ thông tin và mạng internet cũng đưa lại nhiều cơ hội, thách thức đan xen. Hiện nay, internet và mạng xã hội đã trở thành công cụ phổ biến mà các thế lực thù địch, phản động sử dụng để chống phá, xuyên tạc các quan điểm, đường lối, chủ trương, chính sách của Đảng và Nhà nước ta, trong đó có vấn đề chủ quyền quốc gia. Điều này đòi hỏi cần phải tăng cường hơn nữa công tác thông tin, tuyên truyền, giáo dục về việc bảo đảm an ninh mạng, bảo vệ chủ quyền quốc gia trên không gian mạng, trong đó hoạt động xuất bản đóng góp một vai trò quan trọng.

*, ** Nhà xuất bản Chính trị quốc gia Sự thật.

Thông qua những ấn phẩm được xuất bản, không chỉ cung cấp những thông tin chính thống, khách quan, khoa học về vấn đề bảo vệ chủ quyền quốc gia, dân tộc, mà còn nhận diện, chỉ ra những âm mưu, thủ đoạn, hành vi của các thế lực thù địch đang sử dụng nhằm mục đích xâm phạm chủ quyền quốc gia, trong đó có những hành vi xâm phạm chủ quyền quốc gia trên không gian mạng, đồng thời lên tiếng nói góp phần đấu tranh chống lại các quan điểm, âm mưu chống phá của các thế lực thù địch, nâng cao nhận thức của các tầng lớp nhân dân về bảo vệ chủ quyền quốc gia.

1. Cung cấp thông tin, tri thức về chủ quyền quốc gia trên không gian mạng

Không gian mạng ngày nay trở thành một không gian xã hội mới, nơi con người có thể thực hiện các hành vi giao tiếp, sáng tạo, lao động, sản xuất, tiêu dùng, học tập và vui chơi giải trí mà không bị giới hạn bởi không gian và thời gian. Sự tiện ích cộng với những trải nghiệm thú vị mà internet và mạng xã hội mang lại đã thu hút một lượng lớn người dùng cùng tham gia vào không gian chung này. Tuy nhiên, bên cạnh những lợi ích to lớn mà không gian mạng mang lại, thì nó cũng đang tạo ra các nguy cơ và thách thức đối với an ninh quốc gia, an ninh con người và trật tự, an toàn xã hội. Các thế lực thù địch lợi dụng internet và mạng xã hội để xuyên tạc cương lĩnh, đường lối, quan điểm, nền tảng tư tưởng của Đảng; lôi kéo, kích động các phần tử bất mãn, tập hợp lực lượng, thành lập các tổ chức chống đối; phát tán tài liệu, kêu gọi biểu tình, bạo loạn, gây mất ổn định an ninh chính trị, trật tự, an toàn xã hội.

Nghiêm trọng hơn, các thế lực thù địch đã và đang lợi dụng không gian mạng để thực hiện các hành vi vi phạm chủ quyền quốc gia, gây ảnh hưởng trực tiếp đến an ninh và lợi ích quốc gia. Vì chủ quyền quốc gia là thiêng liêng và bất khả xâm phạm, do đó, việc định hướng tuyên truyền, cung cấp thông tin về vấn đề chủ quyền quốc gia nói chung, chủ quyền quốc gia trên không gian mạng nói riêng giữ vai trò cực kỳ quan trọng.

Trong những năm qua, hoạt động xuất bản đã làm tốt nhiệm vụ thông tin, tuyên truyền đường lối, chủ trương, chính sách, pháp luật của Đảng và Nhà nước Việt Nam về vấn đề bảo vệ chủ quyền quốc gia đến với các tầng lớp nhân dân thông qua nhiều ấn phẩm có giá trị. Đặc biệt, khi vấn đề chủ quyền biển, đảo trở thành chủ đề “nóng” trên các diễn đàn, các nhà xuất bản đã tích cực đẩy mạnh việc tổ chức, khai thác những bản thảo hay, có giá trị nhằm cung cấp cơ sở pháp lý và bằng chứng lịch sử khẳng định chủ quyền của Việt Nam đối với quần đảo Hoàng Sa và Trường Sa, phù hợp với luật pháp quốc tế, cũng như khẳng định quyền chủ quyền, quyền tài phán quốc gia đối với các vùng biển được xác lập phù hợp với công ước của Liên hợp quốc về Luật biển năm 1982 (UNCLOS), như các ấn phẩm: *Chủ quyền quốc gia Việt Nam tại hai quần đảo Hoàng Sa và Trường Sa qua tư liệu Việt Nam và nước ngoài* (Nxb. Thông tin và Truyền thông); *Chủ quyền Việt Nam trên Biển Đông* (Nxb. Chính trị quốc gia Sự thật); *Bằng chứng lịch sử và cơ sở pháp lý: Hoàng Sa, Trường Sa là của Việt Nam* (Nxb. Trẻ); *Hoàng Sa, Trường Sa là máu thịt Việt Nam* (Nxb. Thông tin và Truyền thông); *Về vấn đề Biển Đông*

(Nxb. Chính trị quốc gia Sự thật); *Những bằng chứng về chủ quyền của Việt Nam đối với hai quần đảo Hoàng Sa, Trường Sa* (Nxb. Giáo dục); *Chủ quyền của Việt Nam ở Hoàng Sa, Trường Sa - Tư liệu và sự thật lịch sử* (Nxb. Đại học Quốc gia Hà Nội);...

Trước sự phát triển mạnh mẽ của internet và mạng xã hội, vấn đề an ninh mạng đang nổi lên như một thách thức toàn cầu và chủ quyền quốc gia trên không gian mạng trở thành vấn đề cần được quan tâm chú trọng. Hoạt động xuất bản với chức năng thông tin, tuyên truyền, giáo dục của mình, đã có những ấn phẩm cung cấp cho người đọc thông tin, tri thức cần thiết về các vấn đề liên quan như: không gian mạng, an ninh mạng, chủ quyền quốc gia trên không gian mạng, với một số đầu sách như: *Luật an ninh mạng* (Nxb. Chính trị quốc gia Sự thật); *Một số vấn đề cơ bản của Luật an ninh mạng* (Nxb. Công an nhân dân); *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); *An toàn thông tin mạng* (Nxb. Thông tin và Truyền thông); *Gián điệp mạng - Từ góc nhìn mối đe dọa an ninh toàn cầu* (Nxb. Công an nhân dân)... Từ đó, các cuốn sách đã góp phần định hướng người đọc trong quá trình nhận thức, đánh giá các vấn đề liên quan đến việc bảo vệ chủ quyền quốc gia trên không gian mạng một cách khách quan, đúng đắn.

Không chỉ đẩy mạnh việc xuất bản các ấn phẩm in trên giấy, các nhà xuất bản đã tích cực ứng dụng công nghệ thông tin, mạng internet để cung cấp các loại sách điện tử nhằm đáp ứng nhu cầu bạn đọc thông qua thiết bị điện tử, phần

mềm hỗ trợ đọc như máy đọc sách, máy tính, điện thoại... Sự tiện ích, yếu tố đa phương tiện (sử dụng âm thanh, hình ảnh minh họa) của sách điện tử giúp cho loại sách này trở thành một “công cụ” hữu hiệu trong quá trình truyền tải thông tin đến bạn đọc. Đặc biệt, trong việc tuyên truyền, phổ biến các thông tin, tri thức liên quan đến chủ quyền quốc gia, sách điện tử không chỉ cung cấp những tư liệu phong phú về căn cứ lịch sử, pháp lý thông qua các văn bản, bản đồ (bản đồ 3D,...) mà còn có thể kết hợp với phim tài liệu, tư liệu, phóng sự truyền hình để làm rõ hơn những nội dung, thông điệp cần truyền tải đến bạn đọc một cách sống động, hấp dẫn, ấn tượng, dễ hiểu, dễ nhớ. Nhờ đó, bạn đọc có thể dễ dàng tìm hiểu, nắm bắt được các thông tin liên quan đến chủ quyền quốc gia nói chung và chủ quyền quốc gia trên không gian mạng nói riêng.

Để làm tốt nhiệm vụ cung cấp thông tin, tri thức về vấn đề chủ quyền quốc gia trên không gian mạng trong bối cảnh hiện nay, hoạt động xuất bản, thông qua các ấn phẩm, cần giúp người đọc hiểu được chính xác nội hàm của khái niệm “chủ quyền quốc gia trên không gian mạng”, từ đó định hướng người đọc về vấn đề bảo vệ chủ quyền quốc gia trên không gian mạng, đồng thời nhận diện và đấu tranh với những hành vi vi phạm chủ quyền quốc gia trên không gian mạng.

Trong hai cuốn sách *Sự suy tàn của quyền lực* (Nxb. Hồng Đức) và *Chủ nghĩa tự do truyền thống* (Nxb. Tri thức), các tác giả đã cung cấp cho bạn đọc một số thông tin, nhận định để góp phần xác định khái niệm “chủ quyền quốc gia trên không gian mạng”, đó là: (1) Internet đã làm biến đổi

xã hội, chính trị và cả quyền lực, nó cũng làm thay đổi các vấn đề liên quan đến việc thực thi chủ quyền quốc gia. Nếu như trước đây các quốc gia đã từng đổ máu để giữ vững quyền thống trị của mình thông qua việc bảo vệ các đường biên giới quốc gia thì giờ đây các đường biên giới gần như đã bị dịch chuyển. (2) Vấn đề diện tích, quy mô của vùng lãnh thổ nằm dưới quyền cai trị của một quốc gia sẽ không còn có ý nghĩa tuyệt đối đối với cuộc sống của từng cá nhân¹. Từ những nhận định này có thể thấy, việc bảo vệ chủ quyền quốc gia không chỉ là việc bảo vệ các đường biên giới quốc gia mà đã được mở rộng hơn rất nhiều, trong đó bao gồm việc bảo vệ chủ quyền quốc gia trên không gian mạng. Vậy, khái niệm “chủ quyền quốc gia trên không gian mạng” cần được hiểu như thế nào?

Như chúng ta đã biết, chủ quyền quốc gia là quyền làm chủ một cách độc lập, toàn vẹn và đầy đủ về các mặt lập pháp, hành pháp và tư pháp của một quốc gia trong phạm vi lãnh thổ của quốc gia đó. Quốc gia thể hiện chủ quyền của mình trên mọi phương diện kinh tế, chính trị, văn hóa, quân sự, ngoại giao. Chủ quyền quốc gia là đặc trưng chính trị và pháp lý thiết yếu của một quốc gia độc lập, được thể hiện trong hoạt động của các cơ quan nhà nước và trong hệ thống pháp luật quốc gia. Tôn trọng chủ quyền quốc gia là một nguyên tắc cơ bản của luật pháp quốc tế. Hiến chương Liên hợp quốc khẳng định nguyên tắc bình đẳng về chủ quyền

1. Dẫn theo ThS. Hoàng Thị Quyên: “Bảo vệ chủ quyền quốc gia trên không gian mạng trong thời đại công nghệ số”, nguồn: <https://hcma.vn/vanban/Pages/van-ban-quan-ly.aspx?ItemId=30799&CateID=0>.

giữa các quốc gia; không một quốc gia nào được can thiệp hoặc khống chế, xâm phạm chủ quyền của quốc gia khác. “Không gian mạng” là mạng lưới kết nối của kết cấu hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian. Do đó, chủ quyền trên không gian mạng là bộ phận quan trọng của chủ quyền quốc gia; bảo vệ chủ quyền quốc gia trên không gian mạng là nhiệm vụ cấp bách, lâu dài của cả hệ thống chính trị, đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý của Nhà nước; là yếu tố then chốt hình thành không gian mạng quốc gia an toàn và ổn định, tạo bước đột phá trong xây dựng, bảo vệ Tổ quốc Việt Nam xã hội chủ nghĩa.

Tại khoản 5, Điều 8 Luật an ninh mạng năm 2018 đã quy định, một trong những hành vi bị nghiêm cấm về an ninh mạng liên quan đến bảo vệ chủ quyền quốc gia, đó là: 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. Nhiệm vụ của hoạt động xuất bản chính là cung cấp cho người đọc những thông tin, tri thức thiết thực liên quan đến việc bảo vệ chủ quyền quốc gia trên không gian mạng, từ đó góp phần chủ động phòng vệ, sẵn sàng “đáp trả hợp pháp” các thông tin sai lệch, xuyên tạc, hành vi vi phạm chủ quyền quốc gia Việt Nam trên không gian mạng. Làm rõ nội dung của bảo vệ chủ quyền quốc gia trên không gian mạng 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, dữ liệu; bảo đảm quyền bình đẳng trong tham gia quản lý mạng internet quốc tế; độc lập trong vận hành kết cấu hạ tầng 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, dữ liệu của quốc gia.

Việc tuyên truyền, giáo dục cho người dân, đặc biệt là thế hệ trẻ (đối tượng sử dụng công nghệ thông tin, internet và mạng xã hội nhiều nhất nên cũng dễ bị tác động nhất) thông qua các ấn phẩm có giá trị nhằm góp phần nâng cao nhận thức toàn diện về chủ quyền quốc gia và bảo vệ chủ quyền quốc gia trên không gian mạng trong tình hình mới là vấn đề hết sức quan trọng nhằm khơi dậy tinh thần yêu nước, ý thức tự tôn, lòng tự hào dân tộc, đấu tranh bảo vệ vững chắc chủ quyền quốc gia không gian mạng trong kỷ nguyên thông tin và Cách mạng công nghiệp lần thứ tư.

2. Nhận diện và đấu tranh với quan điểm sai trái, thù địch góp phần tuyên truyền, giáo dục, nâng cao nhận thức về bảo vệ chủ quyền quốc gia trên không gian mạng

Hiện nay, cùng với các vấn đề liên quan đến dân chủ, nhân quyền, tôn giáo, dân tộc, các thế lực thù địch và phản động thường xuyên lợi dụng internet và mạng xã hội để xuyên tạc quan điểm của Việt Nam về vấn đề chủ quyền biển, đảo. Chúng sử dụng các website của các báo, đài phản động ở nước ngoài như BBC, Đài châu Á tự do (RFA)..., các trang mạng

xã hội như Facebook, YouTube, Twitter,... để phát tán tài liệu, hình ảnh, video xuyên tạc tình hình, diễn biến phức tạp trên Biển Đông, xuyên tạc quan điểm, chủ trương, chính sách của Đảng và Nhà nước trong cuộc đấu tranh bảo vệ chủ quyền biển, đảo trên không gian mạng. Mục đích của các thế lực thù địch, tổ chức, cá nhân phản động, chống đối là nhằm lợi dụng lòng yêu nước, tự hào dân tộc và những bức xúc của người dân trước những diễn biến phức tạp trên Biển Đông để kích động nhân dân chống lại Đảng, Nhà nước, chia rẽ mối quan hệ giữa Đảng với nhân dân. Đồng thời, chúng lợi dụng những bất đồng quan điểm về vấn đề Biển Đông để hòng làm chia rẽ mối quan hệ đối ngoại của Việt Nam với các nước có liên quan, kích động tư tưởng bài xích một số nước trong một bộ phận người dân. Mặt khác, chúng xuyên tạc quan điểm, chủ trương, chính sách của Đảng và Nhà nước ta để lôi kéo, kích động nhân dân, tạo nên lực lượng đối lập ở trong nước dưới danh nghĩa “đấu tranh” bảo vệ chủ quyền biển, đảo hòng gây mất an ninh chính trị, trật tự, an toàn xã hội, hạ thấp uy tín Việt Nam trên trường quốc tế...

Xuất bản là một hoạt động thuộc lĩnh vực công tác tư tưởng, văn hóa, có vai trò quan trọng trong việc định hướng dư luận xã hội. Đặc biệt, hoạt động xuất bản cần phải phát huy tốt vai trò cung cấp thông tin, tri thức về vấn đề bảo vệ chủ quyền quốc gia nói chung, chủ quyền quốc gia trên không gian mạng nói riêng, đồng thời trở thành công cụ đấu tranh, phê phán lên án những hành vi lợi dụng không gian mạng để vi phạm chủ quyền quốc gia, dân tộc.

Trong công tác đấu tranh làm thất bại âm mưu, hoạt động chống phá của các thế lực thù địch để nâng cao hiệu

qua giáo dục ý thức bảo vệ chủ quyền quốc gia trên không gian mạng, hoạt động xuất bản cần đặc biệt chú ý việc tuyên truyền, giáo dục để bạn đọc nhận diện đầy đủ, sâu sắc và tích cực, chủ động đấu tranh phê phán, bác bỏ các quan điểm sai trái, hành vi vi phạm chủ quyền quốc gia của các thế lực thù địch, phản động. Để làm được điều đó, các ấn phẩm cần tập trung phân tích, làm rõ âm mưu, thủ đoạn của các thế lực thù địch, phần tử cơ hội lợi dụng internet và mạng xã hội để đưa các thông tin tuyên truyền sai sự thật, xuyên tạc về tình hình đất nước, thực hiện “diễn biến hòa bình” nhằm phủ nhận vai trò lãnh đạo của Đảng, gây chia rẽ giữa Đảng, Nhà nước và nhân dân trong vấn đề bảo vệ chủ quyền quốc gia Việt Nam trên không gian mạng, chia rẽ quan hệ đối ngoại giữa Việt Nam với các nước có liên quan, làm cho Việt Nam rơi vào tình trạng đối đầu, bị cô lập. Bên cạnh đó, công tác đấu tranh cần làm rõ những hành vi của các thế lực thù địch lợi dụng diễn biến phức tạp trên Biển Đông sử dụng mạng xã hội để kích động một bộ phận nhân dân tham gia biểu tình, tuần hành gây mất ổn định an ninh chính trị, trật tự, an toàn xã hội, từ đó tác động tiêu cực tới nhận thức, tư tưởng, gây tâm lý hoang mang, hoài nghi, làm suy giảm lòng tin của nhân dân đối với sự lãnh đạo của Đảng. Đó là những âm mưu thâm độc, thủ đoạn tinh vi mà các thế lực thù địch đã lợi dụng không gian mạng để chống phá, thực hiện những hành vi vi phạm chủ quyền quốc gia mà mỗi người dân cần phải nhận diện một cách chính xác để từ đó có những cách thức đấu tranh, phản bác hiệu quả.

Để đấu tranh, phản bác có hiệu quả đối với những luận điệu sai trái, xuyên tạc của các thế lực thù địch, phản động

về chủ quyền quốc gia trên không gian mạng, hoạt động xuất bản cần làm tốt một số nội dung sau:

Thứ nhất, tăng cường xuất bản các ấn phẩm có nội dung tuyên truyền, giáo dục cho cán bộ, đảng viên và nhân dân (đặc biệt là thế hệ trẻ - đối tượng sử dụng internet và mạng xã hội nhiều nhất) về chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước trong việc bảo vệ chủ quyền quốc gia nói chung, bảo vệ chủ quyền quốc gia trên không gian mạng nói riêng. Đa dạng hóa các loại hình xuất bản phẩm như sách ảnh, bản đồ, sách in, sách nói, sách điện tử,... có nội dung liên quan đến chủ quyền quốc gia, an ninh mạng, nhằm tăng tính hấp dẫn, kích thích sự quan tâm, chú ý của bạn đọc. Đặc biệt, hoạt động xuất bản cần phải tập trung phát triển hơn nữa các loại hình ấn phẩm được phát hành trên internet và mạng xã hội để nhân dân, đặc biệt là thế hệ trẻ dễ dàng tiếp cận, tìm hiểu những thông tin chính thống của Đảng và Nhà nước về vấn đề chủ quyền quốc gia, chủ quyền quốc gia trên không gian mạng, từ đó tích lũy, cập nhật kiến thức, có khả năng nhận biết các vấn đề một cách khách quan, đúng đắn. Mục đích chính của các ấn phẩm là làm cho nhân dân Việt Nam hiểu rõ lập trường, quan điểm của Đảng và Nhà nước ta về vấn đề chủ quyền, toàn vẹn lãnh thổ quốc gia, an ninh quốc gia là nhất quán và vì lợi ích quốc gia - dân tộc, đồng thời củng cố niềm tin của nhân dân vào sự lãnh đạo của Đảng trong cuộc đấu tranh bảo vệ chủ quyền quốc gia trên không gian mạng; góp phần làm cho cộng đồng quốc tế hiểu rõ và đồng tình, ủng hộ cuộc đấu tranh bảo vệ chủ quyền quốc gia - dân tộc chính đáng, hợp pháp của Việt Nam.

Thứ hai, tăng cường xuất bản các ấn phẩm phân tích, vạch rõ âm mưu, thủ đoạn của các thế lực thù địch, phản động lợi dụng không gian mạng để thông tin sai trái, xuyên tạc về vấn đề chủ quyền quốc gia, làm ảnh hưởng đến quốc phòng, an ninh quốc gia, uy tín lãnh đạo của Đảng và Nhà nước; từ đó kịp thời phát hiện, đấu tranh lên án những hành động sai trái vi phạm chủ quyền quốc gia cũng như những hành vi lợi dụng diễn biến phức tạp ở Biển Đông để thực hiện mưu đồ chống phá Đảng, Nhà nước và công cuộc bảo vệ chủ quyền quốc gia của Việt Nam. Trong cuộc đấu tranh bảo vệ chủ quyền quốc gia trên không gian mạng hiện nay, ngành xuất bản cùng với báo chí cần phát huy vai trò định hướng xã hội trong việc đưa thông tin, sự kiện một cách kịp thời, phát đi thông điệp chính thức của Việt Nam và truyền tải tinh thần yêu nước của nhân dân Việt Nam để tranh thủ sự đồng tình, ủng hộ của bạn bè và cộng đồng quốc tế đối với công cuộc bảo vệ chủ quyền quốc gia đối với vùng biển, vùng trời, đất liền và cả trên không gian mạng của Việt Nam.

Thứ ba, hoạt động xuất bản cần tập trung đầu tư tăng cường cơ sở vật chất, kết cấu hạ tầng và ứng dụng công nghệ thông tin, công nghệ AI (Artificial Intelligence - trí tuệ nhân tạo) vào các khâu của hoạt động xuất bản; mở rộng giao lưu hợp tác, trao đổi xuất bản phẩm, phối hợp xuất bản với các nhà xuất bản nước ngoài để bạn bè quốc tế hiểu biết thêm về đất nước, con người Việt Nam, lập trường, quan điểm của Việt Nam đối với vấn đề chủ quyền quốc gia, bảo vệ chủ quyền quốc gia, an ninh quốc gia cũng như các vấn đề quốc tế đang diễn ra. Tuy nhiên, cần có sự kiểm soát nghiêm ngặt đối với các ấn phẩm nhập khẩu để kịp thời

phát hiện và xử lý những ấn phẩm có nội dung thông tin sai lệch, xuyên tạc, vi phạm trên lĩnh vực chủ quyền quốc gia, dân tộc của Việt Nam.

Như vậy, có thể khẳng định rằng, bảo vệ chủ quyền quốc gia, trong đó có chủ quyền quốc gia trên không gian mạng là nhiệm vụ trọng yếu, thường xuyên trong quá trình xây dựng và phát triển đất nước. “Nước Cộng hòa xã hội chủ nghĩa Việt Nam là một nước độc lập, có chủ quyền, thống nhất và toàn vẹn lãnh thổ, bao gồm đất liền, hải đảo, vùng biển và vùng trời”¹. “Mọi hành vi chống lại độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ, chống lại sự nghiệp xây dựng và bảo vệ Tổ quốc đều bị nghiêm trị”². Hoạt động xuất bản, với nhiệm vụ thông tin, tuyên truyền, giáo dục nâng cao nhận thức của các tầng lớp nhân dân về đường lối, chủ trương, chính sách, pháp luật của Đảng và Nhà nước Việt Nam trong vấn đề bảo vệ chủ quyền quốc gia, đã và đang ngày càng khẳng định được vai trò quan trọng của mình trong sự nghiệp xây dựng và bảo vệ Tổ quốc nói chung và bảo vệ chủ quyền quốc gia nói riêng, trong đó có việc bảo vệ chủ quyền quốc gia trên không gian mạng trong giai đoạn hiện nay.

1, 2. *Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam*, Nxb. Chính trị quốc gia, Hà Nội, 2013, tr.8-9, 14-15.

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUÁ TRÌNH CHUYỂN ĐỔI SỐ CỦA DOANH NGHIỆP

TẬP ĐOÀN CÔNG NGHIỆP -
VIỄN THÔNG QUÂN ĐỘI (VIETTEL)

1. Vấn đề chung

Trước hết, nói về mặt định nghĩa, Chuyển đổi số (Digital transformation) là việc tích hợp công nghệ và kỹ thuật số vào quá trình hoạt động kinh doanh của tổ chức, với mục tiêu chính là gia tăng hiệu quả vận hành, nâng cao trải nghiệm và làm hài lòng khách hàng và hơn nữa là tạo được lợi thế cạnh tranh trên thị trường.

Chuyển đổi số đòi hỏi tổ chức phải có một quyết tâm thay đổi từ “gốc rễ”, liên tục thách thức những thói quen, không ngừng thử nghiệm cái mới và học làm quen với thất bại. Chính vì thế, nhiều tổ chức rất chật vật trong quá trình chuyển đổi số vì không thể nào bỏ được những giá trị cốt lõi.

Những giá trị lớn mà chuyển đổi số mang lại cho doanh nghiệp là:

- Giảm thiểu chi phí;
- Cải thiện chiến lược khách hàng;
- Cải thiện hệ thống vận hành;
- Phân tích và bảo mật dữ liệu tốt hơn;

- Tập trung hơn vào khách hàng tiềm năng;
- Sản phẩm/dịch vụ mới;
- Phân khúc thị trường chính xác;
- Trải nghiệm khách hàng với thị trường rộng hơn;
- Tăng sự đổi mới cho nhân sự;
- Liên kết các phòng, ban trong nội bộ tổ chức;
- Tăng tỷ lệ tiếp xúc khách hàng mọi lúc, mọi nơi.

Quá trình chuyển đổi đi kèm với nhiều lợi ích - trên thực tế, trong một số trường hợp, nó có thể cho thấy sự khác biệt lớn giữa thành công và thất bại của doanh nghiệp đó.

Một ví dụ điển hình là Blockbuster - từng là công ty thống trị thị trường cho thuê video, Blockbuster đã có cơ hội đầu tư vào dịch vụ phát trực tuyến theo phong cách Netflix, vào thời điểm mà nó sẽ có sức mạnh thương hiệu và lòng trung thành của khách hàng để thành công. Nhưng công ty tin rằng việc chuyển đổi kỹ thuật số này sẽ quá tốn kém và rủi ro. Công ty đã thất bại không lâu sau sự gia tăng của các dịch vụ phát trực tuyến, do mức tiêu thụ phim và thói quen của khách hàng thay đổi.

Không phải tất cả các ví dụ đều nghiêm trọng như vậy - nhưng khi các doanh nghiệp không bắt đầu hành trình chuyển đổi kỹ thuật số, họ có nguy cơ mất doanh thu, khách hàng và nhân viên có hiệu suất cao.

2. Phân tích các xu thế công nghệ trong chuyển đổi số

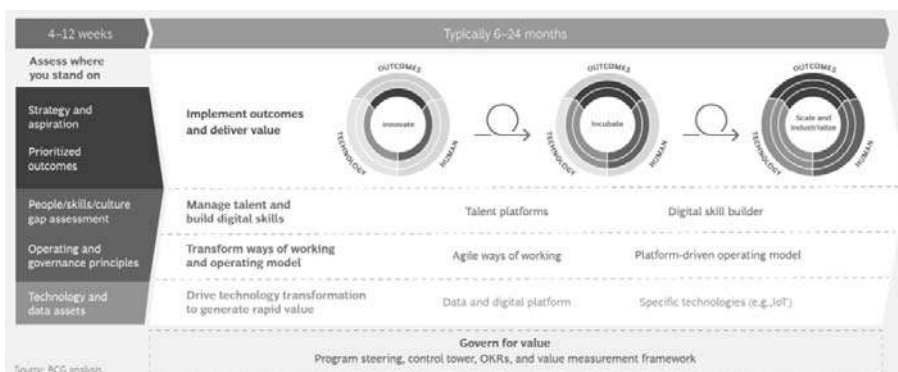
Chuyển đổi số là xu hướng tất yếu của các doanh nghiệp trên toàn cầu, tuy nhiên tình hình đại dịch Covid-19 đã đẩy mạnh xu hướng này, với các doanh nghiệp đang mong muốn đẩy nhanh tốc độ, agile và đưa ra các quyết định dựa trên số liệu (data-driven).

Khảo sát của BCG năm 2020 với hơn 5.000 cấp quản lý và nhân viên đã đưa ra các kết quả nổi bật như: 83% các công ty đã tiến hành đẩy nhanh chuyển đổi số, 80% cho rằng giải pháp số sẽ giúp doanh nghiệp vượt qua tình hình kinh tế ảm đạm sau đại dịch Covid-19, 65% đã tăng đầu tư vào chuyển đổi số.

Tuy nhiên, chỉ có 30% doanh nghiệp tiến hành chiến lược chuyển đổi số thành công. BCG đã đề ra 6 nhân tố chính bảo đảm tỷ lệ thành công lên đến trên 80% của chiến lược chuyển đổi số là:

- Kết hợp chiến lược với mục tiêu chuyển đổi rõ ràng;
- Cam kết của cấp lãnh đạo từ CEO tới quản lý bậc cao, trung;
- Yếu tố phát triển con người;
- Tư duy quản trị agile;
- Quản lý hiệu quả dựa trên hiệu quả đầu ra (outcomes);
- Platform công nghệ và dữ liệu định hướng kinh doanh.

Dựa trên báo cáo quý IV năm 2020 của Forrester Research Wave về chuyển đổi số, BCG đã đề ra mô hình tiếp cận chuyển đổi số dựa trên các hiệu quả đầu ra (outcomes) có thể đo lường được:



Mô hình chuyển đổi số gồm 5 thành phần chính:

- Thực hiện dựa trên hiệu quả đầu ra (outcomes);
- Quản lý con người và xây dựng kỹ năng số;
- Chuyển đổi vận hành và làm việc mô hình số và agile;
- Chuyển dịch công nghệ số theo các xu hướng nổi bật;
- Tăng trưởng dựa trên giá trị (Value measurement).

Trong đó, việc chuyển dịch và ứng dụng công nghệ số theo các xu hướng toàn cầu là điều quan trọng và cần thiết, để bảo đảm kết quả mang đến là toàn diện, đồng bộ với công cuộc xây dựng và kiến tạo xã hội số của Chính phủ, tránh việc xây dựng và áp dụng rời rạc, khó khăn trong việc chuẩn hóa, đồng bộ dữ liệu, ảnh hưởng đến bản thân doanh nghiệp và đến cuộc sống số của người dùng cuối.

Các công nghệ xu thế cho chuyển đổi số có thể tổng hợp về 5 nhóm chính sau, bao gồm:

- Data Analytics & Platform: Để bắt kịp với kỳ vọng ngày càng tăng của khách hàng, các tổ chức đang tìm kiếm những cách nhanh hơn để hiểu sâu về dữ liệu và thu thập thông tin chi tiết. Năm 2021 sẽ là năm dữ liệu giúp các đơn vị vượt qua đối thủ cạnh tranh. Khả năng mở khóa, phân tích và hành động trên dữ liệu sẽ trở thành nền tảng để phát triển. Bên cạnh đó, các tổ chức đang đầu tư vào phân tích dữ liệu để chuyển đổi trải nghiệm của khách hàng. Giá trị của phân tích dữ liệu sẽ phụ thuộc vào dữ liệu mà chúng được cung cấp từ đâu, như thế nào.

- Connected Cloud (Public, Private, Hybrid): Các tổ chức hiện nay nhận ra rằng chỉ sử dụng một trong các loại hình cloud như public cloud hay private cloud hoặc chỉ các trung tâm dữ liệu không phải là lựa chọn tốt nhất. Nhu cầu của họ

khác nhau và một lựa chọn duy nhất ngày càng trở nên hạn chế theo thời gian. Do đó, các mô hình cloud được kết nối, tích hợp và tương tác với nhau, nhằm đáp ứng nhu cầu ngày càng phát triển của các công ty, cho dù họ cần lưu trữ, mạng hay bảo mật đều xuất phát từ cloud computing.

Machine Learning & AI: Học máy và trí tuệ nhân tạo (AI) là một phần của xu hướng chuyển đổi kỹ thuật số toàn cầu trong năm 2021, mở đường cho các tổ chức đưa AI trở thành một thành phần không thể thiếu trong chiến lược chuyển đổi số của họ. Từ đó, tất cả các hệ thống cốt lõi, quy trình và chiến lược kinh doanh sẽ được thiết kế lại xung quanh AI với mục tiêu cuối cùng của việc xây dựng một tổ chức nơi con người và máy móc sẽ hợp tác để khai thác thông tin chi tiết theo hướng dữ liệu.

Theo nghiên cứu của Net Solutions, 57,7% các nhà lãnh đạo doanh nghiệp từ ngành chăm sóc sức khỏe đang có kế hoạch đầu tư vào AI để thúc đẩy chuyển đổi kỹ thuật số.

- Internet of Thing (IoT): IoT là một trong những xu thế công nghệ mới có mức độ ảnh hưởng tăng lên khi xảy ra cuộc khủng hoảng bởi đại dịch Covid-19. Các tổ chức của tất cả các ngành đang có kế hoạch đón nhận IoT như một trong những công nghệ số hàng đầu; tuy nhiên, các nhà lãnh đạo ngành sản xuất và chăm sóc sức khỏe đã thể hiện sự quan tâm đến IoT nhiều hơn các ngành khác.

Một số nhóm ngành hàng đầu thuộc nhóm IoT hiện nay phải kể đến là:

- + Smart City/Smart Home: đô thị và nhà thông minh;
- + Smart Industry: công nghiệp thông minh (sản xuất, năng lượng,...);

+ Digital Healthcare: Y tế số (khám bệnh từ xa, chăm sóc sức khỏe trực tuyến,...);

+ Digital Payment: Thanh toán số (không tiền mặt, trực tuyến,...);

+ Khác: Nông nghiệp, Giáo dục, Vận tải,...

- Cyber Security: 37,3% tổ chức tin rằng bảo đảm an toàn thông tin số là thách thức lớn nhất mà họ phải đối mặt trên con đường chuyển đổi số. Một số tổ chức đã nhận ra rằng nâng cao an toàn an ninh mạng là một thách thức lớn và đã bắt đầu đưa văn hóa, thực tiễn và công cụ bảo mật vào từng giai đoạn của chiến lược DevOps của họ. Cách tiếp cận mới này hiện là một phần của xu hướng chuyển đổi số trong khoảng 2 năm trở lại đây, được đặt tên là DevSecOps, bên cạnh các xu thế bảo đảm an toàn thông tin tất yếu song hành, ứng dụng cùng các xu thế công nghệ chung của chuyển đổi số.

3. Định hướng bảo đảm an toàn thông tin trong xu thế chuyển đổi số

An ninh mạng là vấn đề ưu tiên hàng đầu đối với mọi tổ chức. Đối với các nhóm công nghệ thông tin, danh sách các mối quan tâm đã được tăng lên bởi lực lượng lao động phân tán hơn và nhu cầu đánh giá các rủi ro liên quan đến sự gia tăng của các thiết bị được kết nối và bối cảnh mối đe dọa luôn thay đổi. Việc tăng cường áp dụng điện toán đám mây cũng đặt ra những thách thức cố hữu. Tất cả những biến số này buộc các tổ chức cần phải chuyển đổi phương thức tiếp cận và triển khai các biện pháp bảo mật của họ để bảo vệ khỏi các nguy cơ có thể xảy ra và thay đổi liên tục.

Bên cạnh đó, sự phức tạp ngày càng tăng của kiến trúc ứng dụng phân tán do chuyển đổi số mang lại thêm các thách thức ngay cả khi các hoạt động bảo mật được triển khai đầy đủ ở mức độ ưu tiên cao nhất. Do kết quả của quá trình chuyển đổi số nhanh chóng, các phương thức bảo đảm an toàn an ninh mạng cần được cập nhật và điều chỉnh để hỗ trợ sự phức tạp ngày càng tăng này.

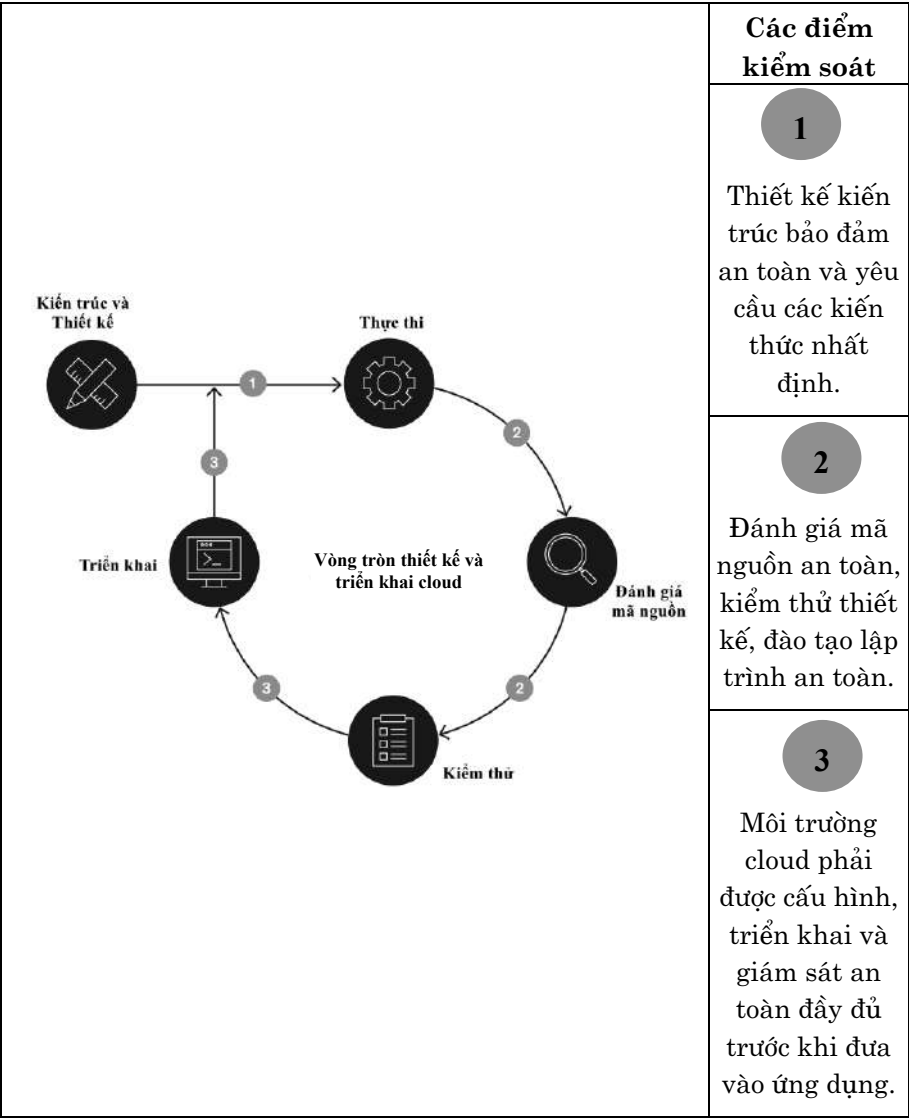
Để thích ứng với quá trình số hóa mạnh mẽ, một số chức năng của các giải pháp bảo đảm an toàn thông tin trên thế giới đang bắt đầu chuyển đổi khả năng của chúng dọc theo ba chiều: sử dụng phân tích rủi ro định lượng để ra quyết định, xây dựng chiến lược an ninh mạng gắn với giá trị chuỗi kinh doanh của doanh nghiệp và đưa vào hoạt động các nền tảng kết hợp nhiều công nghệ đổi mới, bao gồm các phương pháp tiếp cận theo agile, tự động hóa, điện toán đám mây và DevOps (sự kết hợp của phần mềm phát triển và các hoạt động công nghệ thông tin để rút ngắn thời gian phát triển và cung cấp các tính năng mới, các bản sửa lỗi, và cập nhật phù hợp với doanh nghiệp).

Xu hướng 1: Xu hướng chuyển dịch tích hợp cloud

Theo báo cáo của Flexera về xu hướng sử dụng điện toán đám mây cho biết chi phí đầu tư trong năm 2021 sẽ tăng 47% và triển khai ở tất cả lĩnh vực. Các doanh nghiệp lớn tại Việt Nam đã và đang bắt đầu chuyển dịch lên hạ tầng cloud, tiềm ẩn các nguy cơ tấn công an ninh mạng và lộ, lọt thông tin. Cloud-based security tiếp tục là mối quan tâm của các doanh nghiệp để bảo đảm bảo mật an toàn thông tin trên cloud.

Mô hình vận hành an toàn thông tin hiện nay chưa thích ứng với tốc độ cloud hóa. Đa số vẫn đi theo phương

thức phát triển rồi mới chuyển dịch sang mô hình mới và gắn với các giải pháp bảo đảm an toàn thông tin. Như vậy, khi có vấn đề sẽ tốn nhiều thời gian và nguồn lực xử lý. Mô hình mới vận hành theo hướng tích hợp các bước song song, vừa phát triển và chuyển dịch, đồng thời đánh giá rủi ro ở các bước để tối ưu hoá giá trị mang lại.



| Các hoạt động chính | | | | |
|--|---|---|--|---|
| Kiến trúc và thiết kế: phân tích nguồn lực, phân tích các khả năng đáp ứng. Phát triển giải pháp thiết kế và thiết kế sơ bộ. | Thực thi: khởi tạo việc phát triển và kiểm thử môi trường. Bắt đầu các giải pháp thực hiện. | Đánh giá mã nguồn: bảo đảm an toàn, thực hiện dò quét mã nguồn tự động, đưa mã nguồn vào cơ sở mã. | Kiểm thử: phát triển các kịch bản, liên tục kiểm tra đánh giá, khắc phục lỗi. Thực hiện kiểm tra hồi quy. | Triển khai: chuẩn bị hạ tầng, thực thi các dịch vụ cloud, cài đặt ứng dụng lên môi trường cloud. Thực hiện kiểm thử chung cuộc trước khi đưa vào ứng dụng. |

Xu hướng 2: Xu hướng Internet of Thing - IoT

Sự bùng nổ của Cách mạng công nghiệp lần thứ tư cùng với những lợi ích vô cùng lớn về kinh tế, xã hội của các nhóm chuyển đổi số mạnh mẽ như: đô thị thông minh, y tế số, tài chính số,... dẫn tới xu hướng Internet of Things (IoT) được dự đoán sẽ có tác động mạnh mẽ tới an toàn thông tin. Dự đoán tới năm 2025, sẽ có khoảng 30 tỷ kết nối IoT. Xu hướng IoT có ảnh hưởng rất lớn đến an toàn thông tin trên toàn cầu và Việt Nam, tuy nhiên kéo theo đó là các rủi ro rất lớn từ vấn đề mất an toàn thông tin có thể gây ảnh hưởng trực tiếp tới an sinh xã hội. Điều này đã xảy ra trong thực tế như: bệnh viện ở khắp nước Anh bị tê liệt do bị tin tặc tấn công (2017) hay hơn 150.000 camera an ninh của hãng Verkada bị xâm nhập,...

Xu hướng bảo đảm an toàn thông tin cho IoT thường theo 3 giai đoạn chính:

- Kiểm tra đánh giá an toàn thông tin cho các dòng thiết bị IoT trước khi đưa vào sử dụng (IoT Security Assessment/ Audit).
- Triển khai các giải pháp bảo vệ các thiết bị IoT tùy vào mô hình và đặc thù từng nhóm ngành. Ví dụ: Cloud WAAP

hay còn gọi là WAF-on-Cloud cho hệ thống camera giao thông để chống tấn công từ chối dịch vụ và khai thác lỗ hổng hệ thống tập trung; giải pháp giám sát mạng cho hệ thống điều khiển công nghiệp ICS/SCADA;...

- Triển khai giám sát và xử lý sự cố an toàn thông tin 24/7 cho các hệ thống quan trọng, các hệ thống lớn như Smart City, năng lượng trọng yếu,...

Xu hướng 3: Xu hướng làm việc từ xa (Work on the go)

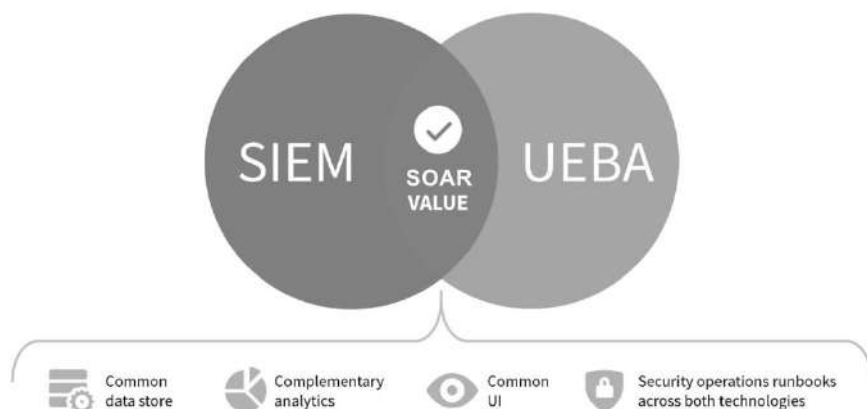
Nhu cầu làm việc từ xa tăng cao trong thời điểm dịch bệnh Covid-19 kéo theo rất nhiều rủi ro về an ninh mạng. Các xu hướng mới như Zero Trust thay cho các giải pháp VPN truyền thống đang được các công ty, doanh nghiệp quan tâm. Zero Trust được giới thiệu lần đầu tiên vào năm 2010 bởi John Kinderrvag, Forrester Research analyst với nguyên lý cơ bản “Never trust, always verify”. Đại dịch Covid-19 năm 2020 - 2021 đã đẩy nhanh quá trình ứng dụng Zero Trust trong bảo mật an toàn thông tin. Các giải pháp Zero Trust Network Acces (ZTNA) hay Secure Access Service Edge (SASE) đang thu hút sự quan tâm trên toàn cầu.



Xu hướng 4: Ứng dụng công nghệ AI và Machine Learning

Theo báo cáo “Do AI and Machine Learning make a difference in cybersecurity” của Webroot năm 2020, 96% người tham gia hiện đang sử dụng các sản phẩm cybersecurity với AI/ML.

Việc ứng dụng AI & Machine Learning theo xu thế chung, bên cạnh giúp phát hiện các hành vi bất thường, phát hiện sớm các cuộc tấn công còn tăng cường tính tự động hóa trong hoạt động quản trị vận hành đang được các công ty an ninh mạng áp dụng để nâng cao trong các giải pháp an toàn thông tin như SOAR, UEBA, SIEM. Từ đó giúp các tổ chức doanh nghiệp tối ưu hóa nguồn lực, giảm tải chi phí vận hành trong bối cảnh thiếu hụt nhân sự an toàn thông tin hiện nay.

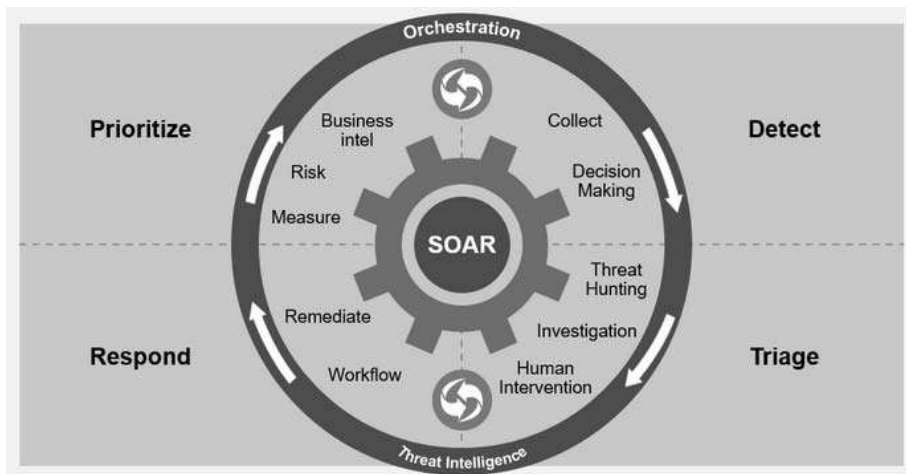


Xu hướng 5: Xu hướng tích hợp (platform)

Năm 2020 theo khảo sát CISO Effectiveness của Gartner, 78% CISOs có từ 16 công cụ an ninh mạng trở lên. Việc sử dụng nhiều hãng an toàn thông tin dẫn đến vận hành phức tạp và gia tăng nhu cầu nhân lực. Xu hướng hợp nhất và tích

hợp các sản phẩm an toàn thông tin được các hãng lớn quan tâm. Điều này xuất phát từ nhu cầu giảm chi phí, giảm thiểu rủi ro khi vận hành.

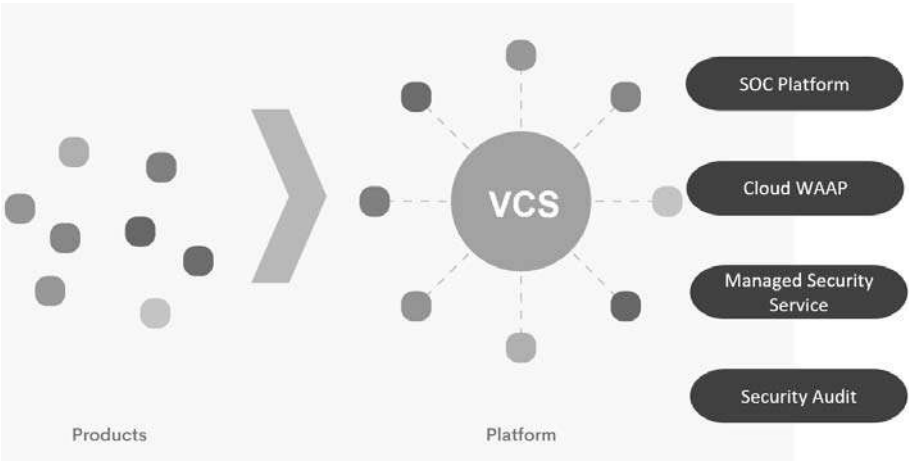
Đây cũng là xu thế chung trong việc chuyển đổi số, khi mà mỗi ứng dụng, mỗi hệ thống được phát triển từ các đơn vị khác nhau, nhưng kết quả thu được là sự hợp nhất trên một nền tảng để điều phối, xử lý và ứng phó các vấn đề có thể xảy ra trong hệ thống thông tin.





4. Phương pháp tiếp cận của Viettel




Từ năm 2016, khi bắt đầu xây dựng và triển khai các giải pháp bảo đảm an toàn thông tin cho Tập đoàn Công nghiệp - Viễn thông Quân đội Viettel cũng như cung cấp dịch vụ và giải pháp an toàn thông tin cho khách hàng bên ngoài, Trung tâm An ninh mạng Viettel và sau này là Công ty An ninh mạng Viettel đã định hướng xây dựng và phát triển theo hướng platform hệ sinh thái chứ không phát triển nhỏ lẻ nhằm đưa đến cho khách hàng giải pháp tổng thể, toàn diện,

không phân mảnh trên cả 4 bước chính theo kiến trúc an toàn thông tin của Gartner bao gồm: Predict (cảnh báo sớm), Bảo vệ (Protection), Phát hiện (Detection) và Xử lý (Remediation)

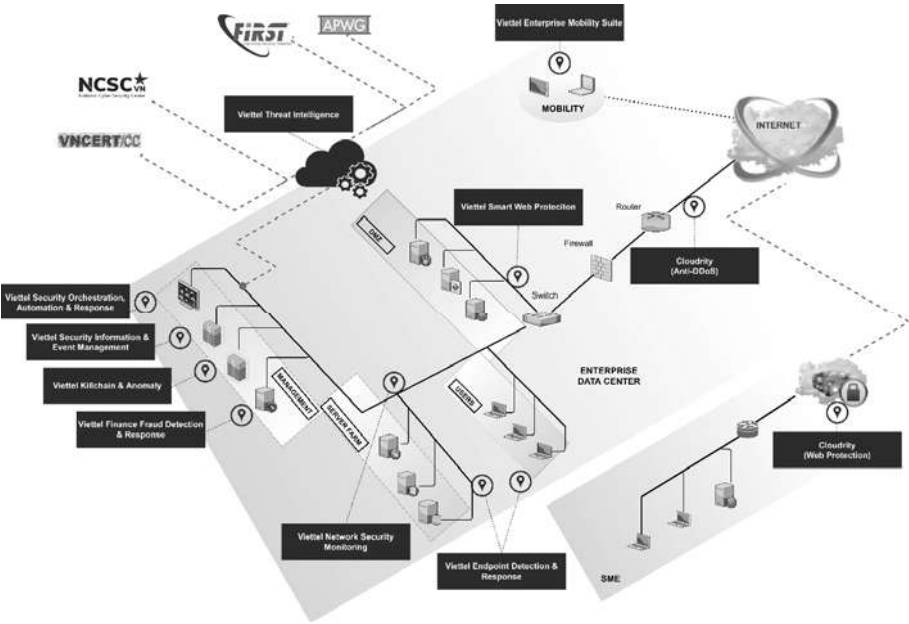


Hệ sinh thái sản phẩm dịch vụ trải rộng, tận dụng được lợi thế Big Data từ nhà mạng số 1 Việt Nam và Đông Nam Á trong việc bổ sung tri thức và dữ liệu phục vụ cho việc phát hiện bất thường và cảnh báo sớm các mối nguy:

| Xu thế an toàn thông tin trong chuyển đổi số | | Sản phẩm VCS |
|---|-------------------------------------|---|
|  | Xu hướng chuyển dịch tích hợp cloud | Cloudrity SOC-on-Cloud |
|  | Xu hướng Internet of Thing - IoT | IoT Security Audit Threat Intelligence Cloudrity |

| Xu thế an toàn thông tin trong chuyển đổi số | | Sản phẩm VCS |
|---|---------------------------------|---|
|  | Xu hướng làm việc từ xa | VCS M-Suite |
|  | Ứng dụng AI và Machine Learning | VCS-KIAN VCS-F2DR VCS-CyM VCS-CyCir Threat Intelligence |
|  | Xu hướng tích hợp platform | VCS-CyCir Threat Intelligence SOC platform |

Bản đồ sản phẩm trong hệ sinh thái An toàn thông tin của Viettel:



MỐI QUAN HỆ GIỮA AN TOÀN THÔNG TIN VÀ QUÁ TRÌNH CHUYỂN ĐỔI SỐ QUỐC GIA

ThS. ĐINH VĂN KẾT*

Trước tác động của đại dịch Covid-19 và Cách mạng công nghiệp lần thứ tư, các cơ quan, tổ chức, doanh nghiệp đã đẩy mạnh chuyển đổi nhiều hoạt động lên không gian mạng và tăng cường áp dụng công nghệ số. Trong bối cảnh đó, bảo đảm an toàn thông tin trên không gian mạng được coi là yếu tố then chốt để chuyển đổi số thành công và bền vững, đồng thời là phần xuyên suốt, không thể tách rời của chuyển đổi số. Việc nắm bắt được mối quan hệ giữa an toàn thông tin và quá trình chuyển đổi số quốc gia sẽ giúp các doanh nghiệp, tổ chức, cơ quan nhà nước và người dân có giải pháp bảo đảm an toàn thông tin phù hợp. Chủ động hạn chế các nguy cơ, rủi ro mất an toàn thông tin, ngăn chặn kịp thời các cuộc tấn công mạng và giảm thiểu thiệt hại khi xảy ra sự cố.

1. Chuyển đổi số

a) Chuyển đổi số là gì?

Có thể hiểu một cách đơn giản về chuyển đổi số như sau:

* Cục An toàn thông tin, Bộ Thông tin và Truyền thông.

“Chuyển đổi số là quá trình thay đổi tổng thể và toàn diện của các cá nhân và tổ chức về cách sống, cách làm việc và phương thức sản xuất trên *môi trường số* với các *công nghệ số*”. Theo Bộ trưởng Bộ Thông tin và Truyền thông Nguyễn Mạnh Hùng: “Chuyển đổi số đơn giản là chuyển đổi hoạt động của chính quyền, của nền kinh tế và của xã hội lên môi trường số”.

Có thể thấy, trong định nghĩa trên có ba ý cơ bản của chuyển đổi số như sau:

Một là, chuyển đổi số là một quá trình thay đổi tổng thể và toàn diện.

Hai là, chuyển đổi số là quá trình thay đổi về cách sống (thường về cá nhân con người), cách làm việc và phương thức sản xuất (thường về các tổ chức và doanh nghiệp) để thích ứng với môi trường số.

Ba là, sự thay đổi trong chuyển đổi số dựa vào các công nghệ số.

Khi thực hiện được chuyển đổi số, chính quyền sẽ nâng cao được hiệu quả, hiệu lực; nền kinh tế sẽ nâng cao được năng lực cạnh tranh; xã hội sẽ thu hẹp được khoảng cách số, nhân văn và tốt đẹp hơn.

Chuyển đổi số bắt nguồn từ sự giao thoa giữa điện toán đám mây (Cloud Computing), dữ liệu lớn (Big Data), Internet vạn vật (IoT) và trí tuệ nhân tạo (AI). Ngày nay, chuyển đổi số đóng vai trò sống còn trong tất cả các ngành công nghiệp. Một số quan điểm cho rằng, nó là sức mạnh của công nghệ số áp dụng vào mọi khía cạnh của tổ chức. Một số khác thì nhắc đến nó như là việc áp dụng công nghệ số và sử dụng các phân tích nâng cao nhằm tạo ra giá trị kinh tế, sự linh hoạt và tốc độ.

Nếu đạt kết quả, hoạt động này sẽ biến đổi một cách toàn diện cách thức hoạt động, tăng hiệu quả hợp tác, tối ưu hóa hiệu suất làm việc và mang lại nhiều giá trị từ quy mô một tổ chức, doanh nghiệp cho đến quy mô quốc gia.

Trước hết cần phải hiểu rõ rằng, chuyển đổi số không đơn thuần là sự nâng cấp liên tục các thế hệ công nghệ thông tin hay chỉ đơn giản là số hóa quy trình, dữ liệu và thông tin. Hay có thể hiểu “đầu tư vào công nghệ không đồng nghĩa với chuyển đổi số”.

Để hiểu chuyển đổi số, trước hết cần nắm được hai khái niệm “Số hóa dữ liệu” và “Số hóa quy trình”. Về bản chất, số hóa quy trình là cấp phát triển cao hơn, đã có yếu tố “số” bao hàm để làm thay đổi cách làm hiện tại, mang lại hiệu quả hơn.

Số hóa dữ liệu (Digitization):

Quá trình chuyển đổi thông tin từ dạng analog ở thế giới thực sang định dạng kỹ thuật số. Đây có thể coi là bước tin học hóa, là thành phần tiên quyết của quá trình chuyển đổi số.

Số hóa có tầm quan trọng rất lớn đối với xử lý, lưu trữ và truyền dữ liệu, bởi vì nó cho phép thông tin của tất cả các loại ở mọi định dạng được thực hiện với cùng hiệu quả và cũng được xen kẽ. Mặc dù thông tin được lưu trữ ở dạng analog thường ổn định hơn, nhưng dữ liệu số có thể dễ dàng được chia sẻ và truy cập hơn, có thể được truyền đi vô thời hạn mà không bị mất mát qua thời gian và qua các lần sao chép, miễn là nó được chuyển sang các định dạng mới, ổn định.

Số hóa quy trình (Digitalization):

Quá trình ứng dụng kỹ thuật số sử dụng các dữ liệu số để

đơn giản hóa và tự động hóa quy trình. Đây là việc sử dụng thông tin đã được số hóa để làm cho cách thức hoạt động trở nên đơn giản và hiệu quả hơn. Digitalization về bản chất không phải là thay đổi mô hình mà là việc tiếp tục, nhưng nhanh và tốt hơn.

Khi công nghệ kỹ thuật số phát triển, ý tưởng về sử dụng công nghệ để tạo ra những cách làm mới. Đây là khi ý tưởng về chuyển đổi số bắt đầu hình thành, với các công nghệ mới, những điều mới và cách thức mới, không chỉ để giải quyết những bài toán cũ nhanh hơn.

Vậy, chuyển đổi số là sự thay đổi toàn diện của mô hình và tổ chức kinh doanh bằng các thông tin kỹ thuật số.

Đó là khi chúng ta đã có trong tay dữ liệu số, thì tổ chức/doanh nghiệp, quốc gia phải ứng dụng những công nghệ như điện toán đám mây, Big Data, AI, IoT để phân tích xử lý dữ liệu, biến đổi nó và tạo ra một giá trị khác.

b) Vì sao phải chuyển đổi số?

Mục tiêu tổng thể của chuyển đổi số là tối ưu năng suất và khả năng sáng tạo (ra quyết định, tính kết nối, sự đổi mới và cải tiến) đối với từng cá nhân và tổ chức. Tại đây, các công nghệ - chẳng hạn như thiết bị thông minh, điện toán đám mây, Big Data, phân tích, mạng kết nối, IoT, điện toán nhận thức và AI - cung cấp năng lực tiếp cận chưa từng có tới các nguồn tri thức và tài nguyên, làm cơ sở cho sự đổi mới và kết quả tốt hơn nhiều lần.

Bên cạnh việc mở rộng phạm vi tiếp cận của các tổ chức một cách triệt để, chuyển đổi số còn tìm cách tận dụng các khả năng và cơ hội mà công nghệ mới mang lại theo cách nhanh hơn, tốt hơn và sáng tạo hơn. Về cơ bản, chuyển đổi số

sẽ đặt các tổ chức trở thành những mô hình hoạt động nhanh nhạy và tối ưu, thiết lập chúng để phát hiện, phản hồi và thích ứng một cách nhanh chóng với những thay đổi trong nhu cầu và kỳ vọng của xã hội, cũng như bối cảnh hội nhập ngày một sâu rộng hơn.

Đối với doanh nghiệp, chuyển đổi số chính là câu trả lời mang tính khác biệt và những doanh nghiệp này sẽ thể hiện sự vượt trội trên thị trường so với các đối thủ truyền thống. Chuyển đổi số sẽ là xu thế không thể đảo ngược, trong đó dữ liệu sẽ trở thành tài sản lớn nhất của doanh nghiệp bởi dữ liệu có ích cho doanh nghiệp ngày càng đa dạng và chi phí để thu nhập dữ liệu có ích cho doanh nghiệp giảm nhanh. Theo số liệu nghiên cứu của McKensey chỉ ra rằng, vào năm 2025, mức độ tác động của chuyển đổi số tới GDP của nước Mỹ là khoảng 25%, Braxin là 35%, các nước châu Âu là khoảng 36%. Từ đây, có thể thấy khả năng tác động của chuyển đổi số đối với tăng trưởng GDP là rất lớn.

Đối với một quốc gia, việc tạo ra lộ trình số hóa, chuyển đổi số, tiến hành xây dựng mô hình chính phủ điện tử, chính phủ số, các mô hình này tạo ra sự thay đổi trong hệ thống điều hành, quản lý, hướng đến mối liên kết chặt chẽ giữa Nhà nước với nhân dân, Chính phủ với doanh nghiệp, tạo ra sự đồng bộ, nhất quán giữa các cơ quan bộ, ban, ngành, đoàn thể, góp phần đổi mới kinh tế, cải cách hành chính... Với tài nguyên đặc biệt là dữ liệu thông tin, các mô hình như chính phủ số, chính phủ điện tử chắc chắn sẽ giúp cải cách, rút gọn nhiều thủ tục hành chính phức tạp, tăng năng suất lao động, bảo đảm đầy đủ quyền và nghĩa vụ của mọi công dân trong xã hội.

c) Khó khăn trong tiến trình chuyển đổi số

Khó khăn lớn nhất của chuyển đổi số chính là thay đổi thói quen và thách thức lớn nhất của chuyển đổi số là có nhận thức đúng. Xã hội con người đã quá quen với môi trường thực trong nhiều thế kỷ, do đó việc chuyển lên môi trường số chính là thay đổi thói quen. Thay đổi thói quen là việc khó và mang tính lâu dài. Thay đổi thói quen ở một tổ chức phụ thuộc chủ yếu vào quyết tâm của người đứng đầu.

Chuyển đổi số là chuyện chưa có tiền lệ, vì vậy, để thay đổi và nhận thức đúng là việc khó. Nhận thức đúng về chuyển đổi số còn phải đặt trong bối cảnh cụ thể của một tổ chức. Chuyển đổi số là vấn đề nhận thức chứ không phải là vấn đề công nghệ, là chuyện dám làm hay không dám làm của người lãnh đạo.

Chuyển đổi số cũng giống như mọi thứ khác trên đời, luôn luôn có hai mặt, bởi vì công nghệ số là cội nguồn của những điều tốt đẹp lớn lao và cũng là nguồn gốc của những tác hại khủng khiếp tiềm tàng. Chúng ta có thể chưa hình dung hết được tất cả về những điều tốt đẹp và điều khủng khiếp đó ở thời điểm hiện nay.

Những hệ lụy đến từ môi trường số có thể kể ra như những chiêu trò lừa đảo, những chiến dịch bắt nạt trên mạng, những trang của các nhóm hận thù và những trang của các nhóm khủng bố.

2. Vai trò của an toàn thông tin trong chuyển đổi số quốc gia

Ngoài vấn đề lớn trong tiến trình chuyển đổi số là việc thay đổi thói quen và nhận thức, thì bên cạnh đó vấn đề

an toàn thông tin chính là rào cản lớn nhất, mang yếu tố then chốt và quyết định thành bại trong chuyển đổi số quốc gia.

Hiện nay, trên không gian mạng trung bình có khoảng 1.000 cuộc tấn công mạng được ghi nhận trong mỗi giây¹ và hơn 300 mã độc mới được tạo ra trong vòng một phút². Tội phạm mạng được coi là mối đe dọa lớn nhất đối với mọi tổ chức trên thế giới và là một trong những thách thức lớn nhất với nhân loại trong 2 thập kỷ tới³.

Tại các quốc gia châu Âu, khoảng 32% doanh nghiệp có chính sách bảo mật công nghệ thông tin. Tuy nhiên, tỷ lệ này rất khác nhau giữa các quốc gia và theo quy mô doanh nghiệp. Trong khi 27% doanh nghiệp nhỏ ở châu Âu có chính sách bảo mật công nghệ thông tin chính thức, tỷ lệ này ở Mỹ thấp hơn ở mức 23%. Theo Báo cáo khảo sát về an ninh mạng và tội phạm mạng của Canada năm 2017 cho thấy, chỉ có 13% doanh nghiệp Canada có chính sách bằng văn bản để quản lý hoặc báo cáo sự cố an ninh kỹ thuật số.

Số liệu trên thể hiện, các doanh nghiệp chưa có sự quan tâm, đầu tư thích đáng vào việc bảo đảm an toàn thông tin trên môi trường kỹ thuật số. Theo Báo cáo của OECD, trung bình 23% người dùng internet trong khu vực OECD đã báo cáo gặp sự cố bảo mật kỹ thuật số vào năm 2015. Ở Hungary và Mêxicô, tỷ lệ này là gần 40%. Báo cáo của Ponemon năm 2018 đã chỉ rằng ít nhất 70% các doanh nghiệp SMBs đã

1. <http://www.horangi.com/blog/the-cost-of-cyber-attacks-to-businesses>.

2. <http://www.av-test.org/en/statistics/malware>.

3. <http://www.herjavecgroup.com/wp-content/upload/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>.

từng trải một cuộc tấn công mạng¹, ước tính thiệt hại trung bình cho mỗi cuộc tấn công vào khoảng 3,62 triệu đôla². Các con số này tăng dần theo thời gian, Forrester ước tính năm 2020 có đến 91% các doanh nghiệp đã ảnh hưởng bởi các cuộc tấn công mạng ít nhất một lần³, tổng mức thiệt hại ước tính là 130 tỷ đôla trên toàn cầu.

Chiến lược bảo đảm an toàn thông tin là việc mô tả cách các quốc gia chuẩn bị và ứng phó với các cuộc tấn công vào các mạng kỹ thuật số. Chúng có thể được coi là một khía cạnh quan trọng của sự sẵn sàng quốc gia về mặt quản lý rủi ro an ninh kỹ thuật số trong quá trình chuyển đổi số. Xét trên bình diện tất cả các quốc gia trên thế giới, chỉ có 38% quốc gia công bố chiến lược bảo mật kỹ thuật số, 11% có chiến lược bảo mật kỹ thuật số chuyên dụng, 12% đang phát triển chiến lược an ninh mạng. Mặc dù có đến hơn một nửa số quốc gia không có chiến lược bảo mật kỹ thuật số, nhưng 61% trong tổng số quốc gia trên thế giới đều có lực lượng, cơ quan chuyên trách về bảo đảm an toàn thông tin (ví dụ: CIRT, CSRIT hoặc CERT). Tuy nhiên, chỉ có 21% trong số này thực hiện công bố số liệu về các sự cố an ninh mạng.

Số hóa thông tin và kết nối mạng đang tạo ra những thách thức mới để bảo vệ dữ liệu nhạy cảm của người dân và

1. <http://prnewswire.com/news-releases/nearly-70-percent-of-smbs-experience-cyber-attacks-half-do-not-know-how-to-protect-their-companies-300749965.html>.

2. <http://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked>.

3. <http://www.dailysabah.com/opinion/columns/cybersecurity-is-serious-business-170-billion-serious>.

doanh nghiệp, ảnh hưởng đến niềm tin của các doanh nghiệp và cá nhân trong các hoạt động trực tuyến. Để hoàn toàn nắm bắt và khai thác hiệu quả chuyển đổi số, người dân, doanh nghiệp và Chính phủ cần phải có niềm tin khi tham gia vào môi trường kỹ thuật số để tiến hành các hoạt động kinh tế và xã hội.

Chúng ta cần xác định bảo đảm an toàn thông tin là yếu tố then chốt để chuyển đổi số thành công và bền vững, đồng thời là phần xuyên suốt, không thể tách rời của chuyển đổi số.

Cách mạng là một công cuộc chuyển mình, từ bỏ cái cũ để hướng đến cái mới, một niềm tin về ánh bình minh tỏa sáng rực rỡ. Niềm tin chính là công cụ quan trọng nhất để mỗi cuộc cách mạng thành công. Cách mạng “chuyển đổi số” cũng vậy. Bởi vậy, tại buổi lễ khai mạc Đại hội đồng liên Nghị viện Hiệp hội các quốc gia Đông Nam Á (Đại hội đồng AIPA) lần thứ 42 vừa qua, Chủ tịch Quốc hội Vương Đình Huệ đã nêu rõ quan điểm: “Tăng cường các chính sách và khung pháp lý, ủng hộ các sáng kiến trong khuôn khổ các kênh hợp tác của ASEAN cũng như với các đối tác về bảo đảm an ninh mạng, an toàn thông tin, dữ liệu, tạo lập niềm tin trong không gian số. Hạ tầng số hiện đại cùng với niềm tin số sẽ tạo ra một không gian mới mở rộng cho sự phát triển nhanh và bền vững của các nước ASEAN”.

Xu hướng thế giới cho thấy, bảo đảm an toàn thông tin, tạo lập niềm tin là điều kiện cần thiết để chuyển đổi số nhanh, bền vững. Số hóa thông tin và kết nối mạng đang tạo ra những thách thức mới để bảo vệ dữ liệu nhạy cảm của người dân và doanh nghiệp, ảnh hưởng đến niềm tin của các doanh nghiệp và cá nhân trong các hoạt động trực tuyến.

Một trong những thách thức lớn nhất trong tiến trình chuyển đổi số chính là công tác bảo đảm an toàn thông tin. Chuyển đổi số sẽ được thực hiện ở nhiều khía cạnh khác nhau: số hóa dữ liệu, thông tin; số hóa tổ chức; chuyển đổi toàn diện tổ chức từ tư duy, mô hình, lãnh đạo, văn hóa và hoạt động của doanh nghiệp. Trong quá trình chuyển đổi số này, các tổ chức sẽ phải đối mặt với thách thức về bảo vệ hệ thống thông tin, dữ liệu các nguy cơ về an toàn thông tin.

Hoạt động quản lý, điều hành truyền thống chỉ coi công nghệ thông tin, công nghệ số là công cụ cho các hoạt động vận hành của tổ chức. Tất cả thông tin, dữ liệu của tổ chức đều có sao lưu, dự phòng bằng các tài liệu “giấy” truyền thống, thông tin cá nhân của người dùng cũng được lưu trữ cá nhân hóa riêng biệt. Tuy nhiên, khi chuyển đổi số, mọi thông tin, dữ liệu của tổ chức, doanh nghiệp, cá nhân đều sẽ được số hóa và lưu trữ trên các hạ tầng công nghệ chia sẻ. Mọi hoạt động của tổ chức, doanh nghiệp sẽ phụ thuộc hoàn toàn vào các công nghệ số này, từ hạ tầng mạng internet, các phần mềm, ứng dụng dịch vụ... Mọi vấn đề phát sinh, sự cố lớn nhỏ đều sẽ ảnh hưởng đến hoạt động bình thường của tổ chức. Chính vì vậy, việc các tổ chức, doanh nghiệp không có chiến lược, phương án bảo vệ dữ liệu, hệ thống thông tin các nguy cơ về an toàn thông tin sẽ khiến các đơn vị này sẽ phải trả giá bằng chính dữ liệu và tiền bạc của chính mình.

Do đó, các tổ chức, người dùng cần nhận thức đầy đủ hơn, chuẩn bị các nguồn lực về kỹ thuật, con người để bảo vệ thông tin và dữ liệu; đồng thời sẵn sàng ứng phó với các sự cố an toàn thông tin. Trên cơ sở đó, tổ chức và người dân sẽ có

niềm tin khi tham gia vào môi trường kỹ thuật số để thực hiện các hoạt động phát triển kinh tế và xã hội.

3. Bảo đảm an toàn thông tin trong chuyển đổi số quốc gia

Những lợi ích mà chuyển đổi số mang lại cho doanh nghiệp và xã hội rõ ràng sẽ vô cùng lớn - đó là những lợi ích tạo ra ở cấp độ của một cuộc cách mạng công nghiệp. Những công nghệ mới này sẽ thúc đẩy tăng trưởng kinh tế, thúc đẩy sự toàn diện, cải thiện môi trường và kéo dài thời gian và chất lượng cuộc sống con người. Chuyển đổi số sẽ có tác động sâu rộng đến các ngành công nghiệp, không chỉ đơn thuần ảnh hưởng đến tăng trưởng kinh tế và việc làm, mà còn tạo ra lợi ích về môi trường.

Song hành với đó, việc thiết lập môi trường an toàn thông tin được đánh giá là yêu cầu cần thiết để thực hiện thành công chuyển đổi số quốc gia. Với vai trò quan trọng đó cùng những nền tảng hiện có, ngành công nghiệp an toàn an ninh mạng đứng trước cơ hội lớn để phát triển, nhất là khi Bộ Thông tin và Truyền thông đang hoàn thiện cơ chế, chính sách thúc đẩy trở thành một ngành công nghiệp mới.

Chúng ta cần xác định bảo đảm an toàn, an ninh mạng là then chốt để chuyển đổi số thành công và bền vững, đồng thời là phần xuyên suốt, không thể tách rời của chuyển đổi số. Qua đó, quan tâm thực hiện đồng bộ các giải pháp bảo đảm an toàn, an ninh mạng sau:

Thứ nhất, bảo đảm an toàn, an ninh mạng từ thiết kế, xây dựng kế hoạch. Trong kế hoạch chuyển đổi số phải có hạng mục an toàn, an ninh mạng được thiết kế ngay từ ban đầu;

đồng thời dành tối thiểu 10% ngân sách đầu tư công nghệ thông tin hằng năm cho hạng mục này theo chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 14/CT-TTg, ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.

Thứ hai, nâng cao nhận thức về an toàn, an ninh mạng. Cần nhận thức rõ, an toàn, an ninh mạng gắn liền với sự an toàn, phát triển ổn định, lợi ích quốc gia trên không gian số. Người dùng cuối luôn là điểm yếu nhất của mọi hệ thống. Chỉ cần mỗi tổ chức, cá nhân có ý thức phòng ngừa, có thói quen, văn hóa, kỹ năng bảo đảm an toàn, an ninh mạng cơ bản là đã có thể phòng ngừa đến hơn 80% nguy cơ, rủi ro mất an toàn, an ninh mạng. Ngoài ra, cần tham khảo kinh nghiệm quốc tế trong việc xây dựng các bộ quy tắc ứng xử, tạo lập niềm tin trong môi trường số, hình thành văn hóa số gắn liền với bảo vệ các giá trị đạo đức căn bản của nhân loại và văn hóa truyền thống của Việt Nam.

Thứ ba, bảo đảm an toàn, an ninh mạng theo mô hình 4 lớp thống nhất từ Trung ương đến địa phương. Mô hình bảo đảm an toàn thông tin chuyên nghiệp 4 lớp bao gồm: lực lượng tại chỗ; tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp; tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ; kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia. Mô hình 4 lớp sẽ bảo đảm các hệ thống thông tin được bảo vệ, giám sát và kiểm tra, đánh giá định kỳ với các tổ chức, doanh nghiệp chuyên nghiệp và độc lập. Từ đó sẽ thúc đẩy sự tham gia, phát triển các doanh nghiệp tại thị trường an toàn, an ninh mạng của Việt Nam.

Thứ tư, phát triển hệ sinh thái sản phẩm, dịch vụ an toàn, an ninh mạng “Make in Vietnam”. Làm chủ công nghệ

mới bảo đảm an toàn, an ninh mạng, chúng ta không thể an toàn nếu chỉ sử dụng sản phẩm, công nghệ của nước ngoài. Vì vậy, hệ sinh thái sản phẩm an toàn, an ninh mạng cho Việt Nam phải là “Make in Vietnam”. Phát triển hệ sinh thái sản phẩm an toàn, an ninh mạng sẽ phục vụ Chính phủ điện tử, đô thị thông minh, hệ thống thông tin quan trọng quốc gia và tiến trình chuyển đổi số quốc gia. Muốn làm được điều này, ngoài sự tham gia, vào cuộc của các doanh nghiệp, các dự án đầu tư về công nghệ thông tin, công nghệ kỹ thuật số phải có yêu cầu về hạng mục an toàn, an ninh mạng. Mỗi cơ quan phải có ít nhất một tổ chức hoặc một doanh nghiệp bảo đảm an toàn, an ninh mạng.

Thứ năm, xây dựng lực lượng chuyên gia an toàn thông tin. Tương tự như bảo vệ chủ quyền quốc gia cần quân đội mạnh, bảo vệ không gian mạng quốc gia cần lực lượng an toàn thông tin giỏi, chuyên sâu. Đây là vấn đề có tầm quan trọng đặc biệt. Trên không gian mạng, một chuyên gia giỏi về an toàn thông tin có thể “một người địch vạn người”. Ngoài lực lượng an toàn thông tin chính quy tại Bộ Thông tin và Truyền thông, Bộ Quốc phòng, Bộ Công an thì đội ngũ chuyên gia giỏi hiện nằm số đông ở khu vực dân sự. Nhiều trong số đó là những người Việt ở nước ngoài. Với quyết tâm nhằm hiện thực hóa tầm nhìn đưa Việt Nam trở thành cường quốc về an toàn thông tin, Bộ Thông tin và Truyền thông đã xây dựng và trình Thủ tướng Chính phủ ban hành Quyết định số 21/QĐ-TTg, ngày 06/01/2021 phê duyệt “Đề án đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021 - 2025”. Đây sẽ là lực lượng quan trọng để đáp ứng yêu cầu của thị trường

nhằm phát triển hạ tầng số, nền tảng số và bảo vệ các hệ thống thông tin của đất nước.

Không gian mạng là tương lai của thế giới. Cường quốc an ninh mạng cũng giống như cường quốc quân sự trong thế giới thực. Việt Nam đang bước vào tiến trình chuyển đổi số, phát triển Chính phủ số, kinh tế số, xã hội số. Vì vậy, an toàn, an ninh mạng là điều kiện cơ bản, yếu tố sống còn, không thể tách rời, đóng vai trò quan trọng trong việc ứng dụng công nghệ số để phát triển kinh tế.

NÂNG CAO NHẬN THỨC CỦA SINH VIÊN ĐỐI VỚI LUẬT AN NINH MẠNG NĂM 2018

LÊ MỘNG THO*

1. Sự cần thiết của việc giáo dục nâng cao ý thức của sinh viên đối với Luật an ninh mạng

Việc phát triển mạnh mẽ không gian mạng những năm gần đây ở Việt Nam đã trở thành một bộ phận đóng vai trò rất quan trọng trong việc xây dựng xã hội thông tin, kinh tế tri thức, cũng như góp phần to lớn đẩy nhanh quá trình công nghiệp hóa, hiện đại hóa đất nước. Tuy nhiên, bên cạnh những mặt đạt được thì sự phát triển này còn mang lại nhiều vấn đề tiêu cực, kẻ xấu và các thế lực thù địch dễ dàng sử dụng mạng viễn thông, internet để tuyên truyền, gây rối, bạo loạn nhằm lật đổ chính quyền, thay đổi chế độ chính trị ở nước ta. Hàng nghìn trang thông tin điện tử, blog, trang mạng xã hội như Zalo, Viber, Twitter..., đặc biệt là Facebook, có nội dung xấu, đăng tải ấn phẩm đồi trụy, bạo lực trái với thuần phong mỹ tục của dân tộc hay đưa ra những thông tin sai sự thật gây hoang mang dư luận. Trước những diễn biến phức tạp, khó lường, ngày càng xuất hiện

* Trường Đại học Bách khoa, Đại học Quốc gia Thành phố Hồ Chí Minh.

nhiều cuộc tấn công mạng với quy mô lớn, gia tăng về tính chất lẫn mức độ nguy hiểm gây ảnh hưởng không chỉ đến sự phát triển của đất nước mà còn về vấn đề an ninh quốc gia và trật tự, an toàn xã hội.

Đối với sinh viên - thế hệ trẻ, tương lai của đất nước thì đây là lứa tuổi tiếp cận nhanh với công nghệ thông tin, với không gian mạng. Đặc biệt trong giai đoạn hiện nay, việc học tập online đã trở nên ngày càng phổ biến, trong khi phần lớn chưa có kỹ năng kiểm chứng thông tin và kinh nghiệm ứng xử với các tin tức xấu, độc. Từ đó, có thể bị tác động xấu, ảnh hưởng đến việc hình thành nhân cách và lối sống của giới trẻ, thậm chí trong nhiều trường hợp, chính các em lại vô tình tiếp tay cho tin giả lan truyền rộng. Vấn đề an ninh trên mạng cũng giống như an ninh ngoài đời sống, theo đó mọi công dân, nhất là sinh viên đều phải có những nhận thức nhất định về vấn đề an ninh mạng. Chính vì vậy, việc giáo dục cho sinh viên - thế hệ trẻ nâng cao nhận thức về bảo đảm an toàn, an ninh trên không gian mạng, các vấn đề về chủ quyền quốc gia và bảo vệ chủ quyền quốc gia trên không gian mạng trong tình hình mới là vấn đề hết sức quan trọng nhằm khơi dậy tinh thần yêu nước, ý thức tự tôn, lòng tự hào dân tộc, đấu tranh bảo vệ vững chắc chủ quyền quốc gia không gian mạng trong kỷ nguyên thông tin và Cách mạng công nghiệp lần thứ tư. Theo đó, cần tập trung giáo dục nâng cao nhận thức của sinh viên đối với Luật an ninh mạng năm 2018 nhằm trang bị cho sinh viên những kiến thức cơ bản về an ninh mạng, về việc đấu tranh ngăn chặn các hành vi vi phạm pháp luật trên không gian mạng.

2. Những nội dung trong Luật an ninh mạng cần tập trung giáo dục nâng cao ý thức của sinh viên

Tại kỳ họp thứ năm, Quốc hội khóa XIV, sau nhiều phiên thảo luận, ngày 12/6/2018, Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam đã chính thức thông qua Luật an ninh mạng với tỷ lệ cao (86,86% đại biểu Quốc hội tán thành). Luật an ninh mạng năm 2018 ra đời tạo cơ sở pháp lý vững chắc cũng như chế tài nghiêm minh đối với việc sử dụng internet, mạng xã hội... không chỉ bảo vệ, bảo đảm tốt hơn độc lập dân tộc, chủ quyền quốc gia trên không gian mạng mà còn tạo điều kiện bảo đảm tốt hơn lợi ích quốc gia, dân tộc. Đây là điều quan trọng nhất trong điều kiện internet, mạng xã hội đang phát triển như vũ bão ở nước ta. Chính vì vậy, việc giáo dục nâng cao ý thức của sinh viên về bảo đảm an toàn, an ninh trên không gian mạng trong tình hình mới - cụ thể Luật an ninh mạng năm 2018 cần tập trung vào một số nội dung chủ yếu như sau:

Thứ nhất, hướng dẫn sinh viên nhận thức về một số khái niệm trong Luật an ninh mạng năm 2018.

Luật an ninh mạng năm 2018 quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. Hiện nay, ở nước ta, hoạt động trên không gian mạng ngày càng phát triển. Theo đó, tại khoản 3, Điều 2 Luật an ninh mạng năm 2018 quy định: “Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở

dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian”. Từ những quy định của Luật an ninh mạng năm 2018 cần hướng dẫn sinh viên có nhận thức rõ ràng hơn khái niệm về không gian mạng ở nước ta được hiểu theo nghĩa rộng hơn internet.

Thuật ngữ “An ninh mạng” được hiểu như thế nào? Theo quy định tại khoản 1, 2, Điều 2 Luật an ninh mạng thì “An ninh mạng” là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Việc phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng được hiểu là bảo vệ an ninh mạng.

Thông qua việc hướng dẫn một số khái niệm trong Luật an ninh mạng năm 2018, sinh viên sẽ có nhận thức khái quát hơn về vấn đề an ninh mạng, phòng, chống vi phạm pháp luật trên không gian mạng.

Thứ hai, nâng cao nhận thức của sinh viên về một số nội dung cơ bản của Luật an ninh mạng năm 2018.

Nâng cao nhận thức của sinh viên về nội dung các quy định của Luật an ninh mạng năm 2018 hoàn toàn phù hợp với luật pháp quốc tế như Hiến chương Liên hợp quốc, Tuyên ngôn về quyền con người của Đại hội đồng Liên hợp quốc (1948), Công ước quốc tế về các quyền dân sự và chính trị (1966). Xét về góc độ quyền con người, Luật an ninh mạng năm 2018 chỉ cho phép các cơ quan chức năng điều tra, làm rõ chủ thể của những nguồn thông tin độc hại khi cần thiết và việc áp dụng chế tài chỉ được áp dụng đối với những hành vi vi phạm. Đối với những kẻ đã và đang có những âm mưu, kế hoạch lợi dụng không gian mạng để chống lại Nhà nước

Việt Nam hoặc làm tổn thương đến công dân Việt Nam, thì Luật an ninh mạng sẽ có những chế tài nghiêm khắc. Như vậy, Luật an ninh mạng năm 2018 không hạn chế về quyền và lợi ích của con người, không xâm phạm “quyền riêng tư”, “quyền tự do ngôn luận” hay “cướp đi quyền sử dụng internet của công dân” như nhiều nguồn thông tin phản ánh sai lệch. Cần hướng dẫn sinh viên nâng cao nhận thức về Luật an ninh mạng trực tiếp bảo vệ các quyền của con người thông qua việc phân tích các quy định cụ thể như sau:

Luật an ninh mạng năm 2018 nghiêm cấm những hành vi đưa thông tin sai sự thật gây hoang mang trên không gian mạng và các hành vi 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. Các hành vi bị nghiêm cấm được liệt kê cụ thể tại Điều 8, bao gồm những hành vi như sau: *Một là*, sử dụng không gian mạng để thực hiện hành vi: tổ chức, hoạt động, cấu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; 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 gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng; xúi giục, lôi kéo, kích động người khác phạm tội.

Hai là, 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. *Ba là*, 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. Như vậy, những hành vi nào bị nghiêm cấm và xâm phạm đến các quyền con người như: quyền sống, quyền tự do ngôn luận, xâm hại bí mật đời tư; xâm hại danh dự hay uy tín cá nhân; xâm hại đến quyền tự do tư tưởng, tín ngưỡng và tôn giáo của công dân... thì sẽ phải chịu những chế tài do Luật an ninh mạng quy định.

Hơn nữa, để bảo vệ tối đa quyền và lợi ích hợp pháp của tổ chức, cá nhân, Luật an ninh mạng năm 2018 đã dành Chương III (từ Điều 16 đến Điều 22) quy định đầy đủ các biện pháp phòng ngừa, đấu tranh, xử lý nhằm loại bỏ các nguy cơ đe dọa, phát hiện và xử lý hành vi vi phạm pháp luật, bao gồm: phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống;

xâm phạm trật tự quản lý kinh tế; phòng, chống gián điệp mạng, bảo vệ thông tin bí mật nhà nước, bí mật công tác, thông tin cá nhân trên không gian mạng; phòng ngừa, xử lý hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh, trật tự; phòng, chống tấn công mạng; phòng, chống khủng bố mạng; phòng, chống chiến tranh mạng; phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng; đấu tranh bảo vệ an ninh mạng. Đây là hành lang pháp lý vững chắc để người dân có thể yên tâm buôn bán, kinh doanh hay hoạt động trên không gian mạng.

Luật an ninh mạng năm 2018 quy định doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ. Riêng doanh nghiệp nước ngoài phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam, tức doanh nghiệp nước ngoài phải lưu trữ dữ liệu người dùng tại Việt Nam. Ngoài yêu cầu phải lưu trữ dữ liệu người dùng tại Việt Nam thì các doanh nghiệp trong và ngoài nước không được cung cấp hoặc phải ngừng cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng cho tổ chức, cá nhân đăng tải trên mạng thông tin bị nghiêm cấm theo quy định tại Điều 8, khi có yêu cầu của lực lượng bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông. Theo đó, việc các doanh nghiệp này ngừng cung cấp dịch vụ mạng chỉ xảy ra khi có yêu cầu

của cơ quan chức năng có thẩm quyền. Đồng thời, các doanh nghiệp phải có trách nhiệm cung cấp thông tin người dùng để phục vụ điều tra cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng.

Từ sự phân tích các quy định trên nhằm nâng cao nhận thức của sinh viên về nội dung của Luật an ninh mạng năm 2018 được xây dựng và ban hành trên cơ sở bảo đảm các quyền con người. Theo đó, Luật An ninh mạng năm 2018 hoàn toàn không có những quy định mang tính cấm đoán các doanh nghiệp nước ngoài như: Facebook, Google... cung cấp dịch vụ ở Việt Nam hay cấm công dân truy cập, sử dụng thông tin cũng như tham gia các hoạt động trên không gian mạng... Tuy nhiên, chỉ trong trường hợp các cá nhân, tổ chức sử dụng không gian mạng để thực hiện các hành vi vi phạm pháp luật, hành vi pháp luật cấm như tại Điều 8 thì mới bị xử lý. Do đó, quyền con người trong Luật an ninh mạng không bị bất cứ hạn chế hay vi phạm nào, ngược lại Luật an ninh mạng là công cụ pháp lý hữu hiệu nhằm bảo vệ các quyền, lợi ích hợp pháp của mọi người, đặc biệt là trẻ em - thế hệ trẻ trên không gian mạng, nhằm thoát khỏi vấn đề “ô nhiễm” thông tin trên không gian ảo này. Bởi lẽ, Luật an ninh mạng năm 2018 có một quy định rất nhân văn về bảo vệ trẻ em trên không gian mạng tại Điều 29, theo đó: Các doanh nghiệp phải bảo đảm kiểm soát nội dung để không gây nguy hại cho trẻ em; đồng thời, xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em.

Thứ ba, những hậu quả pháp lý đối với hành vi vi phạm Luật an ninh mạng năm 2018.

Nếu trong trường hợp tổ chức, cá nhân bày tỏ các quan điểm xâm phạm các vấn đề về an ninh mạng như trên thì hậu quả pháp lý đối với họ ra sao? Cá nhân, tổ chức phải chịu trách nhiệm về các hành vi, ứng xử trên mạng xã hội; phối hợp với các cơ quan chức năng để xử lý hành vi, nội dung thông tin vi phạm pháp luật. Cụ thể, Luật an ninh mạng năm 2018 quy định việc xử lý vi phạm pháp luật về an ninh mạng được thực hiện dựa trên quy định tại Điều 9. Bên cạnh đó, Điều 16 Luật an ninh mạng năm 2018 quy định khi tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng có nội dung vi phạm thì phải gỡ bỏ thông tin khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và chịu trách nhiệm theo quy định của pháp luật. Theo đó, tùy theo tính chất, mức độ vi phạm mà người vi phạm có thể bị xử phạt vi phạm hành chính theo Nghị định số 15/2020/NĐ-CP, ngày 03/02/2020 của Chính phủ quy định về xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử. Ngoài ra, người thực hiện hành vi nếu có đủ các yếu tố cấu thành tội phạm quy định tại Bộ luật hình sự thì còn có thể bị truy cứu trách nhiệm hình sự như tội làm nhục người khác quy định tại Điều 155 Bộ luật hình sự hoặc tội vu khống quy định tại Điều 156 Bộ luật hình sự.

Thông qua việc hướng dẫn sinh viên nhận thức đúng và đầy đủ đối với Luật an ninh mạng năm 2018 về một số nội dung cơ bản trên sẽ góp phần nêu cao ý thức chính trị, trách nhiệm, nghĩa vụ công dân đối với nhiệm vụ bảo vệ không

gian mạng quốc gia. Từ đó, sinh viên sẽ có ý thức tuân thủ quy định của pháp luật; kịp thời cung cấp thông tin liên quan đến cơ quan quản lý nhà nước có thẩm quyền về bảo đảm an ninh mạng. Tuy nhiên, nhằm bảo đảm hiệu quả cho công tác nâng cao nhận thức của sinh viên đối với vấn đề an ninh mạng thì các hình thức giáo dục cần được tiến hành thường xuyên, thay đổi liên tục. Bên cạnh việc phối hợp giữa các cơ quan chức năng với các cơ quan, địa phương, đơn vị, doanh nghiệp, nói chuyện chuyên đề, phổ biến và tuyên truyền Luật an ninh mạng thì các cuộc thi tìm hiểu về an toàn thông tin; về Luật an ninh mạng cần được triển khai rộng rãi trong công tác đoàn, hội, đến mọi sinh viên. Hơn hết, việc hướng dẫn các kỹ năng để sinh viên nghiên cứu và sử dụng tốt các biện pháp kỹ thuật bảo đảm an toàn thông tin mạng như bảo vệ tài khoản cá nhân như thế nào, cách nhận diện những trang web lạ hoặc trang “web đen”, những email chưa rõ danh tính ra sao... hay giáo dục kỹ năng phát hiện bị tấn công trên không gian mạng cũng rất quan trọng, cần được chú trọng bên cạnh việc nâng cao nhận thức đối với Luật an ninh mạng năm 2018.

NHỮNG VẤN ĐỀ ĐẶT RA VỀ BẢO ĐẢM AN NINH KINH TẾ SỐ CỦA VIỆT NAM

Thượng tá, TS. HOÀNG MINH HUỆ*

1. Kinh tế số là gì?

Hiện nay, khoa học, công nghệ phát triển nhanh, Cách mạng công nghiệp lần thứ tư và kinh tế số trở thành một trong những xu hướng phát triển chủ yếu của thời đại. Đảng ta xác định trong Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII là thúc đẩy phát triển kinh tế số, xã hội số và đặt ra mục tiêu đến năm 2025, kinh tế số đạt khoảng 20% GDP; đến năm 2030, kinh tế số đạt khoảng 30% GDP.

Có nhiều định nghĩa về kinh tế số. Trong thực tế, kinh tế số đôi khi cũng được gọi là kinh tế internet (Internet Economy), kinh tế mới (New Economy), hay kinh tế kỹ thuật số hoặc kinh tế mạng (Web Economy). Ngày nay, với sự lan tỏa của “số hóa” vào nền kinh tế thực thì việc phân định rạch ròi kinh tế số với kinh tế truyền thống không đơn giản.

Theo định nghĩa từ Nhóm cộng tác kinh tế số của Oxford thì kinh tế số là “*một nền kinh tế vận hành chủ yếu dựa trên*

* Cục Khoa học, Chiến lược và Lịch sử Công an, Bộ Công an.

công nghệ số, đặc biệt là các giao dịch điện tử tiến hành thông qua internet”.

Với định nghĩa này, kinh tế số bao gồm tất cả các lĩnh vực và nền kinh tế (công nghiệp, nông nghiệp, dịch vụ; sản xuất, phân phối, lưu thông hàng hóa, giao thông vận tải, logistics, tài chính, ngân hàng,...) mà công nghệ số được áp dụng.

Theo nghĩa hẹp, kinh tế số chỉ liên quan đến lĩnh vực viễn thông và công nghệ thông tin (ICT). Theo nghĩa rộng thì là những lĩnh vực gắn gũi với công nghệ số, ví dụ như các nền tảng số. Theo nghĩa rộng nhất thì là tất cả các lĩnh vực mà có sử dụng công nghệ số.

Kinh tế số là các hoạt động kinh tế có sử dụng thông tin số, tri thức số như là yếu tố sản xuất chính; sử dụng mạng internet, mạng thông tin làm không gian hoạt động; và sử dụng ICT, tức là viễn thông và công nghệ thông tin, để tăng năng suất lao động và để tối ưu nền kinh tế. Nếu nói đơn giản thì là nền kinh tế liên quan đến công nghệ số.

Kinh tế số sử dụng mạng internet, mạng thông tin làm không gian hoạt động; sử dụng viễn thông và công nghệ thông tin để tăng năng suất lao động.

Ở Việt Nam, tại Diễn đàn Kinh tế tư nhân Việt Nam năm 2019, kinh tế số được hiểu là toàn bộ hoạt động kinh tế dựa trên nền tảng số, và phát triển kinh tế số là sử dụng công nghệ số và dữ liệu để tạo ra những mô hình kinh doanh mới. Trong nền kinh tế số, các doanh nghiệp sẽ đổi mới quy trình sản xuất, kinh doanh truyền thống sang mô hình theo hệ sinh thái, liên kết từ khâu sản xuất, thương mại đến sử dụng và điều này sẽ làm tăng năng suất cũng như hiệu quả lao động.

Như vậy, có rất nhiều khái niệm khác nhau và chưa có khái niệm nào được chấp nhận chính thức về kinh tế số, nhưng theo cách hiểu phổ biến nhất mà phần lớn các quốc gia và tổ chức quốc tế thống nhất thì *kinh tế số là nền kinh tế dựa trên công nghệ số và nền tảng số, với các hoạt động kinh tế bằng công nghệ số và nền tảng số, đặc biệt là các giao dịch điện tử tiến hành trên internet*. Đây cũng là khái niệm được bài viết này lựa chọn để trình bày các nội dung tiếp theo.

Từ đó có thể thấy, kinh tế số bao gồm các hiện tượng mới nổi như công nghệ blockchain, nền tảng số, phương tiện truyền thông xã hội, doanh nghiệp điện tử (ví dụ như thương mại điện tử, các ngành truyền thống như sản xuất hoặc nông nghiệp có sử dụng công nghệ số hỗ trợ); các doanh nghiệp liên quan đến phát triển phần mềm, ứng dụng, phát triển nội dung số và truyền thông, các dịch vụ và đào tạo liên quan, cùng với các doanh nghiệp tham gia vào sản xuất và phát triển thiết bị công nghệ thông tin và truyền thông.

Về bản chất, đây là các mô hình tổ chức và phương thức hoạt động của nền kinh tế dựa trên ứng dụng công nghệ số. Ta có thể dễ dàng bắt gặp hàng ngày những biểu hiện của công nghệ số xuất hiện ở bất cứ đâu trong đời sống như các trang thương mại điện tử, quảng cáo trực tuyến hay các ứng dụng về ăn uống, vận chuyển, giao nhận,... cũng tích hợp công nghệ số để đáp ứng nhu cầu thuận tiện cho khách hàng. Xét ở tầm vĩ mô, kinh tế số cũng có những đóng góp không nhỏ trong sự hội nhập của các doanh nghiệp Việt Nam vào chuỗi công nghệ toàn cầu.

Kinh tế số không chỉ tạo ra quy mô và tốc độ tăng trưởng cho các nền kinh tế, mà còn làm các nền kinh tế thay đổi trên hai bình diện, đó là (i) phương thức sản xuất (nguồn lực, hạ tầng, cách thức vận hành sản xuất, kinh doanh); (ii) cấu trúc kinh tế, và thậm chí là phá hủy số¹. Trong đó, đáng chú ý là bên cạnh các nguồn lực truyền thống thì đã xuất hiện nguồn lực phát triển mới là tài nguyên số, của cải số. Quyền lực tài chính đang dần chuyển sang quyền lực thông tin. Sức mạnh của một quốc gia được đo bằng sự phát triển của công nghệ cao², thông tin và trí tuệ con người.

Bên cạnh đó, kinh tế số cũng giúp tăng trưởng bền vững hơn, bởi công nghệ sẽ cho chúng ta những giải pháp tốt, hiệu quả hơn đối với việc sử dụng tài nguyên, xử lý các vấn đề ô nhiễm môi trường,... Đồng thời, với chi phí tham gia thấp và dễ tiếp cận, kinh tế số cũng tạo ra nhiều cơ hội hơn cho người lao động, mọi thành phần, khu vực, qua đó góp phần làm giảm khoảng cách giàu nghèo, giải quyết nhiều vấn đề xã hội thông qua đo lường tâm trạng xã hội, sự tham gia của người dân vào hoạch định chính sách,...

2. Thế giới làm gì với kinh tế số

Mỹ, nơi khởi nguồn cho sự bùng nổ của công nghệ thông tin với nhiều công ty nổi tiếng, như Google, Amazon,

1. Đơn cử như sự thay thế các sản phẩm hoặc dịch vụ trong nền kinh tế: một số sản phẩm gần như mất đi khi kinh tế số xuất hiện, như bản đồ truyền thống bị thay thế bằng bản đồ số định vị tiện dụng và thông minh GPS.

2. Một số công nghệ lõi của nền kinh tế số hiện nay là: điện toán đám mây, chuỗi khối (blockchain) hoặc internet.

Facebook, Apple,... tiếp tục nhận thức được tầm quan trọng của thúc đẩy kinh tế số. Châu Âu có kế hoạch “Single Digital Market” (tạm dịch là thị trường số thống nhất), Ôxtrâylia có “Digital Australia”,... Hàn Quốc, Trung Quốc nhờ biết thực hiện chiến lược “rút ngắn”, ưu tiên tập trung nguồn lực cho đổi mới sáng tạo đã có những bước tiến đáng kể trong phát triển kinh tế số. Hàn Quốc có chiến lược Sáng tạo công nghiệp chế tác 3.0 giúp doanh nghiệp nhỏ và vừa tạo dựng các quy trình sản xuất tối ưu, thông minh. Trung Quốc trong 10 lĩnh vực then chốt của sáng kiến “Made in China 2025” đã ưu tiên hai lĩnh vực chính là phát triển công nghệ thông tin, công cụ số và robotics.

Với ASEAN, nhiều nước đang rất quan tâm đến vấn đề này và đã có các giải pháp, cơ quan hỗ trợ cho kinh tế số phát triển. Đơn cử, Thái Lan đã thành lập Bộ Xã hội và Kinh tế kỹ thuật số để thay thế Bộ Công nghệ thông tin và Truyền thông, trong khi Malaixia đặt mục tiêu là giá trị của nền kinh tế số sẽ chiếm 17% tỷ trọng nền kinh tế của nước này, còn Xingapo có khẩu hiệu “Smart Nation” (quốc gia thông minh) lấy công nghệ làm cốt lõi,...

**Danh sách 10 công ty lớn nhất thế giới
năm 2008 và năm 2018**

| 2018 | | | | 2008 | | | |
|----------|---------|-----------|--------|----------|------------|-----------|--------|
| Xếp hạng | Công ty | Thành lập | Tỷ USD | Xếp hạng | Công ty | Thành lập | Tỷ USD |
| 1 | Apple | 1976 | 890 | 1 | PetroChina | 1999 | 728 |
| 2 | Google | 1998 | 768 | 2 | Exxon | 1870 | 492 |

| 2018 | | | | 2008 | | | |
|----------|-----------|-----------|--------|----------|--------------|-----------|--------|
| Xếp hạng | Công ty | Thành lập | Tỷ USD | Xếp hạng | Công ty | Thành lập | Tỷ USD |
| 3 | Microsoft | 1975 | 680 | 3 | General | 1892 | 358 |
| 4 | Amazon | 1994 | 592 | 4 | China Mobile | 1997 | 344 |
| 5 | Facebook | 2004 | 545 | 5 | ICBC (China) | 1984 | 336 |
| 6 | Tencent | 1998 | 526 | 6 | Gazprom | 1989 | 332 |
| 7 | Berkshire | 1955 | 496 | 7 | Microsoft | 1975 | 313 |
| 8 | Alibaba | 1999 | 488 | 8 | Royal Dutch | 1907 | 266 |
| 9 | J&J | 1886 | 380 | 9 | Sinopec | 2000 | 257 |
| 10 | JP Morgan | 1871 | 375 | 10 | AT&T | 1885 | 238 |

Nguồn: Thời báo Kinh tế Việt Nam, số 100+101, ngày 26/4/2019.

3. Kinh tế số ở Việt Nam

Ở Việt Nam, kinh tế số xuất hiện từ khi có máy tính, đặc biệt là khi có máy tính cá nhân, vào cuối những năm 1980; bắt đầu mạnh mẽ là khi có internet, vào cuối những năm 1990; phổ cập là khi mật độ điện thoại thông minh chiếm trên 50%, vào cuối những năm 2000; và được thúc đẩy mạnh mẽ là khi xuất hiện Cách mạng công nghiệp lần thứ tư, vào cuối những năm 2010.

Công nghệ di động đang thay đổi cách thức người dân sống và làm việc, cung cấp cho họ khả năng tiếp cận tốt hơn đến các thị trường và những cơ hội mới. Năm 2019, Việt Nam sở hữu 61 triệu người dùng internet, trung bình người Việt

dành hơn 3 giờ 12 phút sử dụng internet trên thiết bị di động như điện thoại thông minh (smartphone), theo tỷ lệ, nhóm các ứng dụng mạng xã hội và truyền thông liên lạc (52%), ứng dụng xem video (20%) và game (11%), cùng các ứng dụng cho công việc. Giá trị giao dịch thiết bị công nghệ thông tin, viễn thông tăng đều đặn hàng năm... đã tạo ra nền tảng lý tưởng để đẩy mạnh hơn nữa các nỗ lực phát triển kinh tế số.

Theo báo cáo của Google và Temasek, năm 2018, quy mô thị trường kinh tế số khu vực Đông Nam Á đạt giá trị 72 tỷ USD; Việt Nam xếp vị trí thứ 6 sau Ấn Độ, Malaixia, Philippin, Xingapo, Thái Lan và Việt Nam chỉ chiếm 1/8 tổng giá trị (tương ứng khoảng 11%). Dự báo đến năm 2025, quy mô thị trường kinh tế số khu vực Đông Nam Á sẽ tăng lên 240 tỷ USD và Việt Nam chiếm khoảng 18% giá trị thị trường kinh tế số Đông Nam Á.

Theo báo cáo *Nền kinh tế số Đông Nam Á 2019* (e-Conomy Southeast Asia 2019) do Google, Temasek và Bain công bố, nền kinh tế số Việt Nam năm 2019 trị giá 12 tỷ USD (đóng góp 5% GDP), cao gấp 4 lần so với giá trị của năm 2015 và dự đoán chạm mốc 43 tỷ USD vào năm 2025, với các lĩnh vực: thương mại điện tử, du lịch trực tuyến, truyền thông trực tuyến và gọi xe công nghệ.

Nền kinh tế số Việt Nam, cùng Ấn Độ, đang dẫn đầu về tốc độ tăng trưởng trong khu vực Đông Nam Á, với trung bình 38%/năm so với 33%/năm của cả khu vực tính từ năm 2015.

Tổng giá trị giao dịch (GMV) trên thị trường thương mại điện tử Việt Nam ước đạt 5 tỷ USD trong năm 2019, cao gấp 12,5 lần mức 0,4 tỷ USD của năm 2015 và sẽ tăng

tới 23 tỷ USD vào năm 2025, với tốc độ tăng trưởng xấp xỉ 49%. Bên cạnh đó, các ngành dịch vụ du lịch trực tuyến, truyền thông trực tuyến và gọi xe trực tuyến cũng có sự vươn lên mạnh mẽ, đóng góp vào sự phát triển của nền kinh tế số Việt Nam.

Việt Nam cũng được đánh giá là một trong những quốc gia có tốc độ phát triển kinh tế số ở mức khá trong khu vực ASEAN với hạ tầng viễn thông - công nghệ thông tin khá tốt, phủ sóng rộng, mật độ người dùng cao. Hiện có khoảng 72% dân số đang sử dụng điện thoại thông minh, 68% số người Việt Nam xem video và nghe nhạc mỗi ngày trên thiết bị di động, có 70% số thuê bao di động đang sử dụng 3G hoặc 4G,... Dựa trên số liệu của Tập đoàn Miniwatts Marketing, Việt Nam hiện xếp thứ 13 trong top 20 quốc gia có số dân sử dụng mạng internet đông nhất thế giới. Năm 2018, Việt Nam đạt 41/100 điểm, đứng thứ 14 trong bảng xếp hạng về độ phủ dịch vụ đám mây.

Xu hướng số hóa xuất hiện ở nhiều lĩnh vực, ngành kinh tế, từ thương mại, thanh toán đến giao thông, giáo dục, y tế... và đã có những đóng góp quan trọng cho nền kinh tế. Hiện có khoảng 30.000 doanh nghiệp phần cứng, phần mềm, nội dung số, các dịch vụ viễn thông và công nghệ thông tin (ICT) với tổng doanh thu năm 2017 đạt 91,6 tỷ USD, gấp 12 lần so với năm 2010 (7,6 tỷ USD). Công nghiệp phần mềm với khoảng 10.000 doanh nghiệp, có tốc độ tăng trưởng cao (15 - 20%/năm), doanh thu năm 2017 đạt 3,7 tỷ USD. Doanh thu thương mại điện tử năm 2017 đạt khoảng 8 tỷ USD (tăng trung bình 35%/năm), là lĩnh vực có tốc độ phát triển nhanh nhất. Việt Nam có 48 công ty

Fintech cung cấp dịch vụ thanh toán tiền gửi và tiền điện tử. Trong kinh doanh nội dung số, công nghiệp quảng cáo trực tuyến đạt doanh thu 390 triệu USD năm 2016, doanh thu trò chơi trực tuyến đạt khoảng 500 triệu USD. Hàng năm có hàng chục nghìn doanh nghiệp khởi nghiệp sáng tạo trong lĩnh vực số. Năm 2017, 21 doanh nghiệp khởi nghiệp trong lĩnh vực thương mại điện tử Việt Nam nhận đầu tư nước ngoài với tổng số vốn lên đến 83 triệu USD. Nhiều doanh nghiệp đã chứng tỏ được năng lực công nghệ số, thực hiện nhiều dự án công nghệ cao như: xe tự lái, robot, AI,...

Đảng và Nhà nước luôn quan tâm, sớm ban hành nhiều chủ trương, giải pháp cho quá trình chuyển đổi sang nền kinh tế số, có thể kể đến Nghị quyết số 36-NQ/TW, ngày 01/7/2014 của Bộ Chính trị khóa XI về đẩy mạnh phát triển công nghệ thông tin đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế. Thể chế hóa chủ trương của Đảng, Chính phủ đã ban hành nhiều nghị quyết về vấn đề này, như Nghị quyết số 41/NQ-CP, ngày 26/5/2016, của Chính phủ về chính sách ưu đãi thuế thúc đẩy việc phát triển và ứng dụng công nghệ thông tin tại Việt Nam và Chỉ thị số 16/CT-TTg, ngày 04/5/2017 của Thủ tướng Chính phủ về tăng cường năng lực tiếp cận Cách mạng công nghiệp 4.0. Tháng 8/2018, Ủy ban Quốc gia về chính phủ điện tử được thành lập do Thủ tướng trực tiếp làm Chủ tịch Ủy ban. Chiến lược về Cách mạng công nghiệp 4.0 cùng Chương trình hành động về chuyển đổi số đang được nghiên cứu, soạn thảo và sẽ được lồng ghép vào Chiến lược phát triển kinh tế - xã hội giai đoạn 2021 - 2030. Tháng 9/2019, Bộ Chính trị đã ban

hành Nghị quyết số 52-NQ/TW đặt mục tiêu đến năm 2025, nền kinh tế số Việt Nam sẽ đạt 20% GDP, phát triển được một cộng đồng doanh nghiệp công nghệ số Việt Nam lớn mạnh. Ngày 03/6/2020, Thủ tướng Chính phủ đã ký ban hành Quyết định số 749/QĐ-TTg phê duyệt Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030 với mục tiêu Việt Nam thuộc nhóm 50 nước dẫn đầu về chính phủ điện tử, liên quan đến phát triển kinh tế số, nâng cao năng lực cạnh tranh của nền kinh tế.

4. Bảo đảm an ninh kinh tế số

Theo báo cáo của Tổ chức Cảnh sát hình sự quốc tế, tội phạm sử dụng công nghệ cao đứng thứ hai trong các loại tội phạm nguy hiểm nhất, sau tội phạm khủng bố và 90% tội phạm truyền thống đã chuyển sang môi trường mạng hoặc có sử dụng các thiết bị công nghệ cao¹. Hoạt động tấn công mạng gây thiệt hại về kinh tế, làm mất uy tín, gián đoạn hoạt động của cơ quan, tổ chức, đe dọa trực tiếp đến an ninh quốc gia và trật tự, an toàn xã hội trên không gian mạng.

Hoạt động lợi dụng không gian mạng xâm phạm hoạt động kinh tế số ở Việt Nam diễn ra ngày càng gia tăng về số vụ, tính chất, mức độ nghiêm trọng, xảy ra trên tất cả các lĩnh vực của đời sống xã hội. Sự phát triển của không gian mạng cho phép ứng dụng phổ biến công nghệ kỹ thuật số với hệ thống dữ liệu kết nối ở hầu hết các giao dịch kinh tế,

1. Xem “*Tội phạm mạng sẽ ngày càng nguy hiểm*”, nguồn: <https://nhandan.com.vn/hangthang/toi-pham-mang-se-ngay-cang-nguy-hiem-281653/>, truy cập ngày 15/4/2021.

tài chính, thương mại nhưng lại chứa đựng các nguy cơ tiềm ẩn mất an toàn, an ninh; nguy cơ xảy ra các cuộc tấn công đánh cắp thông tin trong giao dịch kinh tế, thương mại và đầu tư thông qua hệ thống số; thanh toán thương mại điện tử, cho vay ngân hàng, huy động vốn bằng tiền ảo tiềm ẩn nguy cơ gây thất thoát tài chính quốc gia, đe dọa an ninh hệ thống tài chính, gây bất ổn xã hội; thị trường thanh toán điện tử tăng nhanh dẫn đến nguy cơ mất kiểm soát hệ thống; hoạt động cho vay ngân hàng trực tuyến trên nền tảng công nghệ tài chính chưa có cơ chế quản lý, bị lợi dụng để cho vay nặng lãi, biến tướng với hình thức huy động vốn bất hợp pháp, đe dọa an ninh tài chính, tiền tệ, tiềm ẩn nguy cơ phát sinh tội phạm¹. Tính riêng năm 2020, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an đã phát hiện khoảng 4.100 vụ việc liên quan đến tội phạm lừa đảo, chiếm đoạt tài sản qua không gian mạng, trong đó có 776 vụ việc lừa đảo qua mạng viễn thông bằng thủ đoạn giả danh cơ quan thực thi pháp luật, các doanh nghiệp cung cấp dịch vụ viễn thông, bưu điện... Các đối tượng ở trong và ngoài nước sử dụng không gian mạng để cá độ, đánh bạc và tổ chức đánh bạc, điển hình là qua website⁷⁸⁹, các đối tượng đã tổ chức đánh bạc và đánh bạc với số tiền lên tới 1.224 tỷ đồng. Ngoài ra, hoạt động kinh doanh trái phép trò chơi điện tử trực tuyến, làm giả thẻ tín dụng để chiếm đoạt tài sản, lợi dụng các dịch vụ thanh toán trực tuyến để chiếm đoạt tài sản, trộm cắp cước

1. Xem Cục An ninh kinh tế: *Báo cáo tổng kết tình hình, công tác bảo đảm an ninh kinh tế năm 2020*, Hà Nội, 2020.

viễn thông quốc tế... có xu hướng gia tăng, tác động xấu đến an ninh, trật tự. Thiệt hại do các đối tượng lợi dụng không gian mạng xâm phạm trật tự, an toàn xã hội là rất lớn về vật chất, ảnh hưởng đến uy tín, hình ảnh của Việt Nam.

Thời gian qua, cơ quan công an đã phát hiện các hoạt động tấn công mạng ở Việt Nam để phá hoại, trong đó có phá hoại các hoạt động kinh tế số. Từ năm 2013 đến nay, đã có trên 15.000 lượt website tên miền “.vn” bị tin tặc tấn công thay đổi giao diện trang chủ, chiếm quyền điều khiển, chỉnh sửa, chèn thêm nội dung, cài mã độc, đánh cắp thông số kỹ thuật, mật khẩu để thực hiện các cuộc tấn công mạng với quy mô lớn vào hệ thống thông tin trọng yếu của các cơ quan, doanh nghiệp. Điển hình như: ngày 29/7/2016, tin tặc đã tấn công vào hệ thống máy chủ của Việt Nam Airlines; tháng 3/2017, xảy ra 2 vụ tấn công các trang web của Cảng Hàng không quốc tế Tân Sơn Nhất, các sân bay Phú Quốc, Rạch Giá, Tuy Hòa, Thọ Xuân, Vinh, Liên Khương, Buôn Ma Thuột và Đà Nẵng; 6 tháng đầu năm 2019, trên 4.600 trang/cổng thông tin điện tử của nước ta bị tấn công.

Ta đã tích cực, chủ động đấu tranh có hiệu quả với hoạt động đưa tin giả gây phương hại đến các hoạt động phát triển kinh tế số: đã theo dõi, giám sát trên 3.000 trang mạng có nội dung xấu, độc; chủ động nắm tình hình, theo dõi, giám sát chặt chẽ tình hình trên không gian mạng, xác minh, truy tìm, đấu tranh với đối tượng tán phát tin giả, tin sai sự thật phá hoại kinh tế. Thực hiện các biện pháp nghiệp vụ và kỹ thuật chuyên biệt, tổ chức tấn công, vô hiệu hóa các trung tâm phát tán tin giả lớn, có mức độ bảo vệ an ninh mạng cao. Tăng cường công tác quản lý nhà nước về bảo đảm an ninh mạng,

phối hợp với các nhà cung cấp dịch vụ internet, viễn thông trong nước thực hiện ngăn chặn hàng nghìn trang mạng có nội dung xấu, độc, máy chủ đặt tại nước ngoài; yêu cầu Facebook, Google gỡ bỏ hơn 10.874 bài viết, video, đường dẫn có nội dung xấu, độc, vi phạm pháp luật Việt Nam, xâm hại an ninh kinh tế số. Triển khai các chuyên án, kế hoạch nghiệp vụ đấu tranh, qua đó, bắt khởi tố, xử lý hình sự nhiều đối tượng.

Bên cạnh những kết quả đạt được, công tác bảo đảm an ninh kinh tế số ở nước ta còn gặp những khó khăn, vướng mắc nhất định: Nhận thức về kinh tế số và bảo đảm an ninh kinh tế số là những vấn đề còn hết sức mới mẻ, do đó chưa có sự thống nhất nhận thức và hành động; hoạt động bảo đảm an ninh kinh tế nói chung đang chủ yếu là tiếp cận đối tượng bảo vệ là các hoạt động kinh tế truyền thống nên việc chuyển sang đối tượng bảo vệ mới là các hoạt động kinh tế số, chắc chắn còn cần thêm thời gian nhất định nữa mới thích ứng kịp; đội ngũ nhân lực bảo đảm an ninh kinh tế số, đa phần chưa có nhiều kinh nghiệm và kỹ năng về điều tra số và các tri thức về công nghệ số cũng như các hoạt động kinh tế số; hành lang pháp lý cũng như lý luận nghiệp vụ bảo đảm an ninh kinh tế số còn nhiều vấn đề cần được tiếp tục đầu tư hoàn thiện; cơ chế, chính sách và các điều kiện bảo đảm, nhất là về trang thiết bị, phương tiện kỹ thuật cho đấu tranh bảo đảm an ninh kinh tế số còn chưa ngang tầm nhiệm vụ; hoạt động phối hợp, hợp tác trong và ngoài nước cần được đẩy mạnh hơn nữa trong thời gian tới...

5. Những vấn đề đặt ra

Thời gian tới, những vấn đề đặt ra đối với bảo đảm an ninh kinh tế số là:

Một là, vấn đề dịch chuyển không gian an ninh kinh tế. Cùng với sự phát triển mạnh mẽ của khoa học và công nghệ, nhất là tác động của Cách mạng công nghiệp lần thứ tư, không gian an ninh kinh tế chắc chắn sẽ được mở rộng và tiếp nối từ không gian thực với các hoạt động kinh tế truyền thống vốn có sẽ dần dịch chuyển mạnh mẽ sang hoạt động kinh tế trên không gian số, không gian mạng, cùng với đó, các hoạt động xâm phạm kinh tế cũng sẽ dịch chuyển theo hướng chủ yếu phạm tội kinh tế số. Do đó, đòi hỏi chúng ta phải nhanh chóng thay đổi tư duy và hành động để theo kịp thực tiễn đó.

Hai là, vấn đề âm mưu, phương thức, thủ đoạn phạm tội đối với hoạt động kinh tế số hiện nay và trong thời gian tới cần được khẩn trương dự báo và nghiên cứu làm rõ, từ đó xây dựng và hoàn thiện các biện pháp bảo đảm an ninh kinh tế số, nhất là các biện pháp nghiệp vụ chuyên biệt đấu tranh với hoạt động xâm phạm an ninh kinh tế số trong tình hình mới.

Ba là, bảo đảm an ninh kinh tế số cần gắn với bảo đảm an ninh đối với các nguồn lực, hạ tầng, cách thức vận hành sản xuất, kinh doanh số; bảo đảm an ninh, an toàn các nền tảng số (Platform); bảo đảm an ninh giao dịch điện tử; thương mại điện tử; bảo đảm an ninh hoạt động thanh toán điện tử; hỗ trợ sự phát triển của thương mại điện tử, hợp đồng điện tử, chữ ký số; bảo đảm an ninh hạ tầng kỹ thuật số; bảo đảm an ninh cơ sở dữ liệu, dữ liệu điện tử, nhất là các trung tâm dữ liệu lớn của quốc gia; bảo đảm an ninh mạng xã hội; bảo đảm an ninh hệ sinh thái đổi mới sáng tạo trong nền kinh tế.

Bốn là, vấn đề bảo vệ bí mật nhà nước trên không gian mạng phải được tiếp tục tăng cường và coi trọng; nhất là bảo vệ bí mật kinh tế, kinh tế số; bảo đảm an ninh, an toàn không gian mạng; bảo vệ quyền sở hữu trí tuệ trong môi trường số, trong nền kinh tế số.

Năm là, vấn đề bảo đảm tính cạnh tranh, bình đẳng, an ninh, an toàn của các doanh nghiệp, nhất là doanh nghiệp khởi tạo, doanh nghiệp công nghệ phát triển lành mạnh, vì đây là một trong các chủ thể quan trọng của nền kinh tế số.

Sáu là, vấn đề bảo đảm an ninh đối với quyền riêng tư; đấu tranh với tin giả tràn lan trên mạng xã hội; đấu tranh với hoạt động phá hoại, tình báo, gián điệp kinh tế số; phòng, chống tội phạm lừa đảo và các hành vi phạm tội trên không gian số.

6. Khuyến nghị giải pháp

Một là, tăng cường tổng kết thực tiễn, nghiên cứu khoa học, xây dựng cơ sở lý luận bảo đảm an ninh kinh tế số của Việt Nam. Đề nghị Bộ Công an chủ trì, phối hợp với Bộ Khoa học và Công nghệ, Bộ Thông tin và Truyền thông sớm nghiên cứu và xây dựng chương trình khoa học và công nghệ trọng điểm về vấn đề này. Trên cơ sở đó, giao và đặt hàng công an các đơn vị, địa phương phối hợp với các đơn vị liên quan triển khai nghiên cứu theo hướng tập trung vào những vấn đề lớn, có trọng tâm, trọng điểm và dành đầu tư thỏa đáng về kinh phí, huy động các trung tâm nghiên cứu lớn của ngành công an chủ trì, phối hợp với các đơn vị thực tiễn trong và ngoài ngành cùng nghiên cứu nhằm từng bước làm rõ các vấn đề đang đặt ra về bảo đảm an ninh kinh tế số hiện nay.

Hai là, hoàn thiện hành lang pháp lý và cơ chế, chính sách bảo đảm an ninh kinh tế số mà trước hết là rà soát, đồng bộ, sửa đổi, bổ sung các vấn đề bảo đảm an ninh kinh tế số trong các văn bản pháp luật hiện hành có liên quan, như: Luật giao dịch điện tử (2005), Luật công nghệ thông tin (2006), Luật tần số vô tuyến điện (2009), Luật an ninh mạng (2018),... Bên cạnh đó, từng bước tích hợp chính sách bảo đảm an ninh kinh tế số trong các chính sách, chiến lược phát triển kinh tế - xã hội.

Ba là, quan tâm đầu tư kết cấu hạ tầng kỹ thuật phục vụ đấu tranh bảo đảm an ninh kinh tế số cho các lực lượng chức năng, mà trước hết là cơ sở vật chất - kỹ thuật, trang thiết bị kỹ thuật và tăng cường năng lực giám định dữ liệu điện tử; đầu tư các bộ công cụ kỹ thuật phục vụ điều tra số bảo đảm cho các lực lượng chức năng đủ năng lực khoa học, công nghệ hoàn thành tốt nhiệm vụ bảo đảm an ninh kinh tế số.

Bốn là, chủ động đào tạo đội ngũ nhân lực chủ công trên mặt trận bảo đảm an ninh kinh tế số, theo hướng kết hợp đào tạo, bồi dưỡng nghiệp vụ an ninh với kiến thức khoa học kỹ thuật và công nghệ, nhất là các công nghệ số, công nghệ mạng, cùng với kiến thức pháp luật kinh tế quốc tế và đẩy mạnh hợp tác quốc tế trong đào tạo và đấu tranh bảo đảm an ninh kinh tế số.

Năm là, kiến nghị Bộ Chính trị, Ban Bí thư ban hành nghị quyết, chỉ thị về bảo đảm an ninh kinh tế số trong tình hình mới, trong đó đề ra các chủ trương, quan điểm, nhiệm vụ và giải pháp lớn có tính toàn diện nhằm huy động sức

mạnh tổng hợp của cả hệ thống chính trị mà nòng cốt là lực lượng công an bảo đảm an ninh kinh tế số nước ta nhằm đạt mục tiêu đến năm 2030 chiếm khoảng 30% GDP; đề nghị Chính phủ nghiên cứu ban hành Chương trình quốc gia bảo đảm an ninh kinh tế số, hướng tới an ninh xã hội số vì một Việt Nam phồn vinh và hạnh phúc.

BẢO VỆ QUYỀN VỀ ĐỜI SỐNG RIÊNG TƯ TRÊN MÔI TRƯỜNG KHÔNG GIAN MẠNG THEO PHÁP LUẬT VIỆT NAM, KINH NGHIỆM QUỐC TẾ VÀ KIẾN NGHỊ HOÀN THIỆN PHÁP LUẬT

CAO HỒNG QUÂN*

LÊ NHẬT HỒNG**

Sự phát triển mạnh mẽ của thời đại công nghệ số đã mang lại những chuyển biến tích cực trong quá trình tăng trưởng, phát triển kinh tế ở Việt Nam, đặc biệt là lĩnh vực thương mại điện tử, dịch vụ điện tử,... song song đó, sự cải tiến của công nghệ số đã tạo ra một môi trường “tinh thần” cho đời sống con người được thỏa mãn phù hợp với nhu cầu xã hội. Mặc dù vậy, những vấn đề phát sinh trên không gian mạng vẫn luôn được đặt ra, nổi bật là câu chuyện về đời sống riêng tư - bí mật cá nhân khi tham gia vào không gian mạng đòi hỏi chủ thể phải đặt sự quan tâm về tính “an toàn”, “riêng tư”. Trong bài viết này, nhóm tác giả đánh giá thực trạng quy định pháp luật Việt Nam về vấn đề đời sống riêng tư, bí mật cá nhân, đồng thời nghiên cứu mô hình hệ thống

* Trường Đại học Bách khoa, Đại học Quốc gia Thành phố Hồ Chí Minh.

** Trường Đại học Luật Thành phố Hồ Chí Minh.

quản lý từ một số quốc gia châu Âu để đề xuất kiến nghị hoàn thiện quy định pháp luật trong tương lai.

1. Bảo vệ quyền về đời sống riêng tư theo pháp luật Việt Nam

a) Quy định của pháp luật quyền về đời sống riêng tư

Đời sống riêng tư là thuật ngữ khoa học pháp lý thường xuyên được sử dụng trong các văn bản quy phạm pháp luật, như: Điều 21 Hiến pháp năm 2013, Điều 38 Bộ luật dân sự năm 2015 và Điều 17 Luật an ninh mạng năm 2018. Nhìn chung, các quy định này vẫn chưa đưa ra định nghĩa về “đời sống riêng tư”. Để hiểu về đời sống riêng tư, trước hết chúng ta cần hiểu về thông tin riêng, thông tin cá nhân. Khái niệm về thông tin cá nhân trước đây được ghi nhận tại khoản 16, Điều 3, Nghị định số 72/2013/NĐ-CP, ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng như sau: “Thông tin cá nhân là thông tin gắn liền với việc xác định danh tính, nhân thân của cá nhân bao gồm tên, tuổi, địa chỉ, số chứng minh nhân dân, số điện thoại, địa chỉ thư điện tử và thông tin khác theo quy định của pháp luật”. Sau này, khoản 15, Điều 3 Luật an toàn thông tin mạng năm 2015 ghi nhận “thông tin cá nhân là thông tin gắn với việc xác định danh tính của một người cụ thể”. Theo chúng tôi, đời sống riêng tư của cá nhân được xây dựng dựa trên những thông tin cá nhân gắn liền với quyền riêng tư của họ. Suy rộng ra, đời sống riêng tư là thuật ngữ tổng hợp tất cả những yếu tố thông tin cá nhân gắn liền với cá nhân xác định, thông qua những yếu tố này có thể phân biệt được cá nhân này với cá nhân khác; và đời sống riêng tư

còn bao gồm tất cả những bí mật cá nhân chứa đựng quyền riêng tư thuộc nhân thân cá nhân, chỉ có cá nhân mới có quyền định đoạt chia sẻ những thông tin này hay không.

Xét về mặt quan hệ pháp lý, quyền về đời sống riêng tư của cá nhân là quyền do luật định. Việc thực hiện quyền này, phạm vi và mức độ thực hiện đến đâu là do chính cá nhân tự định đoạt bằng hành vi của mình, vì mục đích của mình, cho riêng mình và tự do hưởng dụng những lợi ích nào đó cho riêng mình, chỉ là của mình và không ai được xâm phạm¹.

Pháp luật Việt Nam đã quy định việc bảo vệ quyền về đời sống riêng tư trong nhiều văn bản luật có vị trí trung tâm. Trong Hiến pháp năm 2013, quyền về đời sống riêng tư được coi là quyền bất khả xâm phạm: “Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; có quyền bảo vệ danh dự, uy tín của mình. Thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo đảm an toàn”.

Bản thân Hiến pháp năm 2013 đã khẳng định tầm quan trọng của đời sống riêng tư, Hiến pháp ghi nhận đời sống riêng tư là một khoản không gian và thời gian của từng cá thể riêng biệt, ảnh hưởng trực tiếp đến đời sống của cá nhân. Chính vì vậy, quyền về đời sống riêng tư là nhu cầu, lợi ích chính đáng được có của mỗi con người, là quyền con người được pháp luật quy định và bảo vệ.

1. Xem Phùng Trung Tập: “Quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình”, *Kiểm sát online (kiemsat.vn)*, truy cập ngày 26/8/2021.

Cụ thể thì mỗi cá nhân đều có quyền bất khả xâm phạm đối với đời sống cá nhân và mọi thông tin liên quan đời sống cá nhân luôn được bảo đảm an toàn bởi hệ thống quy định của pháp luật. Tính bất khả xâm phạm thể hiện được sự tuyệt đối của quyền nhân thân này, trong mọi hoàn cảnh phải được sự tôn trọng.

Trong bối cảnh đời sống xã hội thì đời sống riêng tư là cách hành xử độc lập không phiền đến ai và cũng không ai được tiếp cận đời sống riêng tư của chủ thể khác. Do đó, quyền về đời sống riêng tư được pháp luật xem là quyền nhân thân không thể thiếu của mỗi người, đây cũng chính là nội dung của Điều 38 Bộ luật dân sự năm 2015: “Đời sống riêng tư, bí mật cá nhân, bí mật gia đình là bất khả xâm phạm và được pháp luật bảo vệ”. Tương tự Hiến pháp năm 2013, phía Bộ luật dân sự cũng đưa ra cơ chế quyền về đời sống riêng tư là quyền được pháp luật bảo vệ một cách tuyệt đối và toàn diện, không một tổ chức hay cá nhân nào có thể xâm phạm quyền này khi chưa được sự chấp nhận của chủ thể có quyền. Mọi cá nhân, bất kỳ chủ thể nào đều có quyền về đời sống riêng tư và được pháp luật bảo vệ.

Vấn đề xâm phạm đời sống riêng tư hiện nay diễn ra vô cùng phức tạp, nhất là việc xâm phạm đời sống riêng tư trên không gian mạng.

Nếu Hiến pháp năm 2013 và Bộ luật dân sự năm 2015 chỉ quy định một cách khái quát về bảo vệ quyền về đời sống riêng tư thì đến Luật an ninh mạng năm 2018 đã cụ thể hóa hơn các hành vi được cho là hành vi xâm phạm đến đời sống riêng tư trên không gian mạng tại khoản 1, Điều 17, như: Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin đời sống

riêng tư của cơ quan, tổ chức, cá nhân; cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng; đưa lên không gian mạng những thông tin đời sống riêng tư trái quy định của pháp luật...

Luật an ninh mạng nghiêm cấm những hành vi trên không gian mạng tại khoản 1, Điều 17. Theo đó, khoản 1, Điều 17 Luật an ninh mạng năm 2018 khẳng định bất cứ hành vi chiếm đoạt, thu giữ, mua bán, tiếp cận, tiết lộ, chiếm đoạt, làm thay đổi,... hay bất kỳ tác động nào đối với thông tin liên quan đến đời sống riêng tư dù dưới hình thức nào khi không được sự cho phép của chủ thể có quyền trên không gian mạng đều được xem là hành vi xâm phạm đến đời sống riêng tư của người khác.

b) Các biện pháp bảo vệ quyền về đời sống riêng tư trên môi trường không gian mạng

Khi đời sống riêng tư của một cá nhân bị xâm phạm sẽ ảnh hưởng trực tiếp hoặc gián tiếp đến danh dự, uy tín, nhân phẩm của cá nhân đó. Vì vậy, việc đề ra các biện pháp nhằm giúp các quy định bảo vệ quyền về đời sống riêng tư được thực hiện một cách nghiêm chỉnh trong bối cảnh xã hội ngày càng phát triển là điều hết sức cần thiết.

Nếu quyền đời sống riêng tư bị xâm phạm, cá nhân có thể yêu cầu bồi thường thiệt hại theo Bộ luật dân sự năm 2015. Cơ chế được áp dụng ở đây là bồi thường thiệt hại khi xâm phạm đời sống riêng tư dẫn đến thiệt hại về danh dự, nhân phẩm, uy tín của chủ thể khác. Người bị xâm phạm các thông tin liên quan đời sống riêng tư sẽ được bồi thường nếu chứng minh có hành vi trái pháp luật xâm phạm đời

sống riêng tư; có thiệt hại xảy ra, nhất là thiệt hại tổn thất về tinh thần, tài sản; có mối quan hệ nhân quả giữa hành vi xâm phạm và thiệt hại cho người bị xâm phạm. Khi thỏa mãn các điều kiện trên, chủ thể sẽ được bồi thường về chi phí hạn chế, khắc phục thiệt hại, thu nhập bị mất do hành vi xâm phạm gây ra, các thiệt hại khác, kể cả là thiệt hại về tổn thất tinh thần. Mức bồi thường do các bên thỏa thuận và trong giới hạn mà pháp luật quy định đối với thiệt hại về tổn thất tinh thần (xem Điều 584, 585, 592 Bộ luật dân sự năm 2015).

Hành vi xâm phạm đời sống riêng tư, đối với trách nhiệm hành chính, bị xử phạt theo điểm g, khoản 3, Điều 66 Nghị định số 174/2013/NĐ-CP¹. Đối với hành vi xâm phạm đời sống riêng tư gây ra hậu quả nghiêm trọng, người xâm phạm còn có thể bị truy cứu trách nhiệm hình sự theo Điều 159 Bộ luật hình sự về 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; điểm b, khoản 1, Điều 288; và khoản 1, Điều 155 nếu sử dụng đời sống riêng tư người khác nhằm mục đích làm nhục.

Internet hay thế giới mạng ngày càng phát triển nên việc chia sẻ các thông tin diễn ra nhanh chóng, tiện lợi hơn rất nhiều. Tuy nhiên cũng dẫn đến hệ lụy đó là việc xâm phạm đời sống riêng tư diễn ra ngày một nhiều hơn do tính năng

1. Mức phạt lên đến 20.000.000 đồng, theo điểm g, khoản 3, Điều 66 Nghị định số 174/2013/NĐ-CP, ngày 13/11/2013 của Chính phủ về quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện.

hiện đại của công nghệ nên việc xâm phạm các thông tin của cá nhân dễ dàng thực hiện hơn.

Vì vậy, Luật an ninh mạng đã xây dựng hệ thống các biện pháp chung trong hoạt động bảo vệ an ninh mạng tại Điều 5 của luật này, bao gồm các biện pháp: thẩm định an ninh mạng; kiểm tra an ninh mạng; giám sát an ninh mạng; yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật; khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật tố tụng hình sự... Có thể thấy, các biện pháp này là tập hợp của một quy trình xử lý các hành vi xâm phạm đến an ninh không gian mạng nói chung hay xâm phạm đời sống riêng tư nói riêng. Các biện pháp nói trên vừa mang tính chất phòng bị, ngăn chặn hành vi vi phạm pháp luật có thể xảy ra, vừa có thể xử lý những trường hợp vi phạm.

2. Thực trạng việc bảo vệ quyền về đời sống riêng tư trên môi trường không gian mạng hiện nay ở Việt Nam, kinh nghiệm quốc tế và kiến nghị giải pháp pháp lý cho Việt Nam

a) Thực trạng việc bảo vệ quyền về đời sống riêng tư trên môi trường không gian mạng hiện nay ở Việt Nam

Công nghệ đã thay đổi cách xã hội vận hành. Những tiến bộ vượt bậc của công nghệ trong những thập niên gần đây đã dẫn đến sự thay đổi sâu rộng đối với hoạt động của hầu hết mọi hình thức trao đổi giữa con người với nhau trên toàn thế giới. Mặc dù Luật an ninh mạng năm 2018 ra đời điều chỉnh các vấn đề về hành vi bị nghiêm cấm và chế tài pháp lý đối với việc xâm phạm đến đời sống cá nhân của người khác dưới

bất kỳ hình thức nào, tuy nhiên, trên thực tế, tình trạng đánh cắp thông tin cá nhân, chia sẻ công khai các vấn đề về đời sống của người khác một cách tràn lan trên mạng xã hội vẫn tồn tại và ngày càng ở mức độ tinh vi hơn, thể hiện đa phần ở hai khía cạnh: (1) chia sẻ thông tin, (2) tấn công mạng.

Không khó để bắt gặp các trường hợp trên mạng xã hội Facebook, Instagram hay Zalo, người dùng tự ý chia sẻ các thông tin về đời sống cá nhân của mình, của người khác bao gồm: hình ảnh, sở thích, đời sống, tình trạng hôn nhân,..., thậm chí vấn đề chia sẻ còn lan rộng sang các trang hội nhóm với số lượng tiếp cận và tốc độ lan truyền cao hơn. Đặc biệt đối với những người nổi tiếng, dường như cuộc sống riêng tư, bí mật của các ca sĩ, diễn viên, người của công chúng thu hút sự tò mò, yêu thích và quan tâm rất nhiều của cộng đồng mạng xã hội. Mạng xã hội là môi trường ảo, tuy nhiên, sức mạnh của nó trong xã hội với sự phát triển mạnh mẽ của big data, khoa học, công nghệ thì không thể phủ nhận. Chính môi trường này cũng sản sinh ra rất nhiều các hành vi vi phạm pháp luật, trong đó, điển hình là việc xâm phạm quyền về đời sống riêng tư của người khác. Việc chia sẻ tràn lan các thông tin cá nhân của người khác, về đời sống riêng tư của người khác mà chưa có sự đồng ý của họ chính là sự xâm phạm nghiêm trọng đối với quyền mà pháp luật tôn trọng và bảo vệ.

Bên cạnh đó, biểu hiện của hành vi xâm phạm này còn thể hiện một cách tinh vi hơn và có mục đích rõ ràng hơn đó là sự tấn công mạng vào chính các tài khoản cá nhân của người dùng để khai thác thông tin. Trên thế giới, số liệu khảo sát cho thấy, trong năm 2020, “các cuộc tấn công

chiếm đoạt đã tăng từ 34% số vụ gian lận năm 2019 lên 54% vào cuối tháng 12/2020, kẻ xấu có thể đánh cắp thông tin đăng nhập và chiếm quyền kiểm soát tài khoản trực tuyến bất cứ lúc nào. Các phương pháp gian lận phổ biến tiếp theo là rửa tiền với 16%, gian lận tài khoản mới chiếm 14% và chỉ 12% trường hợp sử dụng các công cụ truy cập từ xa để tấn công¹. Đây chính là các hành vi xâm phạm an ninh mạng nghiêm trọng. Đương nhiên, như đã trình bày, Luật an ninh mạng và các văn bản pháp luật khác đã đưa chúng vào các hành vi bị nghiêm cấm, tuy nhiên, điều này cho thấy, rõ ràng môi trường không gian mạng chưa đủ an toàn; liệu chế tài có đủ để xử lý hết các hành vi vi phạm và liệu rằng để cho hậu quả xảy ra ta mới bắt đầu giải quyết thì có còn hợp lý hay không?

Các mạng máy tính, truyền thông, vận tải và mạng kinh tế đều phụ thuộc vào mức độ bảo mật cho hoạt động của chúng. Hầu hết tất cả các mạng đều được bảo vệ bằng các khoản đầu tư bảo mật. Ví dụ: các máy tính cá nhân sử dụng tính năng quét virus và không truy cập các trang web có vẻ đáng ngờ. Miền sử dụng tường lửa và các thiết bị bảo mật khác để ngăn chặn việc tiếp xúc với virus và phần mềm độc hại là một trong những yêu cầu mà pháp luật đặt ra đối với các trang mạng xã hội².

1. “Các cuộc tấn công chiếm đoạt tài khoản tăng đột biến trong năm 2020”, <https://nhandan.vn>, truy cập ngày 27/8/2021.

2. Xem Daron Acemoglu, Azarakhsh Malekian, Asu Ozdaglar: “Daron Acemoglu, Azarakhsh Malekian, Asu Ozdaglar”, *Journal of Economic Theory*, 2016, p.1.

b) Chính sách bảo vệ quyền riêng tư và không gian mạng ở một số quốc gia

Ở Nhật Bản, việc bảo vệ quyền riêng tư nói chung được ghi nhận bởi Đạo luật về quyền riêng tư đầu tiên của Nhật Bản (APPI - Đạo luật về bảo vệ thông tin cá nhân), là một trong những “luật bảo vệ dữ liệu lâu đời nhất của châu Á”¹. Đến nay, Luật quyền riêng tư hiện tại đã được hoàn thiện vào năm 2017. Theo đó, các định nghĩa về thông tin cá nhân đã được đưa ra tại Điều 2-1 như sau: thông tin cá nhân là thông tin có thể nhận dạng cá nhân bằng tên, ngày sinh và các mô tả khác bao gồm tài liệu, bản vẽ, hồ sơ điện tử hoặc giọng nói, chuyển động và các phương tiện khác. Thay vào đó, số nhận dạng cá nhân được mô tả trong Điều 2-2; chúng là các chữ cái, số, dấu và các mã khác thuộc (1) các đặc điểm của bộ phận cơ thể cho mục đích sử dụng máy điện tử, có thể nhận dạng được cho cá nhân hoặc, (2) người dùng hoặc người mua được chỉ định, được viết hoặc ghi lại trong việc sử dụng dịch vụ hoặc bán hàng.

Ở châu Âu, Quy định chung về bảo vệ dữ liệu cá nhân (GDPR - General Data Protection Regulation) đưa ra các cơ sở tương tự cho hợp tác quốc tế trong lĩnh vực truyền dữ liệu cá nhân với các nước thứ ba. Trên thực tế, Điều 45 nêu rõ rằng một cơ chế truyền dữ liệu mà không cần sự cho phép

1. Pearson, Harriet, Brill, Julie, Parsons, Mark and Imai, Hiroto: “Changes in Japan Privacy Law to Take Effect in Mid-2017; Key Regulator Provides Compliance Insights” Hogan Lovells, Retrieved June 2, 2021 from: <https://www.lexology.com/library/detail.aspx?g=efa0a2b0-b73e-456c-b4fa-26a268e9e751>.

trước hoặc các biện pháp bảo vệ cụ thể của bộ điều khiển được áp dụng với những quốc gia bảo đảm mức độ bảo vệ dữ liệu thích hợp. Một “quyết định thỏa đáng” như vậy là kết quả của một quá trình đánh giá tương đối dài (trước khi đàm phán) do Ủy ban châu Âu thực hiện, trong đó các tiêu chí sau đây đóng vai trò là thước đo đánh giá: sự tuân thủ chung (và cụ thể) đối với các quy định của pháp luật và dân sự liên quan đến quyền riêng tư, các cơ quan quản lý phù hợp chịu trách nhiệm giám sát, thực thi và giám sát và cam kết quốc tế mà quốc gia đã thực hiện bằng các cách thức của bất kỳ công cụ luật công quốc tế nào¹. Các thông tin cá nhân nhạy cảm hay thông tin nói chung như khái niệm, định nghĩa sẽ được pháp luật bảo vệ, đặc biệt trên môi trường không gian mạng, việc sao chép, chia sẻ, tiết lộ, sử dụng thông tin không được cho phép đều được xem là xâm phạm quyền riêng tư của người khác và phải chịu trách nhiệm pháp lý. Với định nghĩa này, có thể nhận thấy, dễ dàng bóc tách và xác định được hành vi xâm phạm quyền riêng tư. Các doanh nghiệp vi phạm quy định về bảo vệ dữ liệu, thông tin cá nhân có thể bị xử phạt với mức khá cao. GDPR nâng mức vi phạm tiềm ẩn đối với các điều khoản của nó lên đến 20 triệu Euro hoặc 4% doanh thu hàng năm của một doanh nghiệp trên toàn cầu. Tuy nhiên, không phát sinh trách nhiệm hình sự theo quy định. Ngược lại, Đạo luật của Nhật Bản có giới hạn trừng phạt vi phạm thấp hơn (ví dụ, đối với hành vi ăn cắp cơ sở

1. Xem Fioretti, J: EU sees data transfer deal with Japan early next year, Reuters, Retrieved August 27, 2021, <http://news.trust.org/item/20171215124551-cd0x4>.

dữ liệu, mức phạt lên tới 500.000 Yên, tương đương 4.200 Euro), trong khi rõ ràng là có thể bị phạt tù một năm.

Để bảo vệ môi trường mạng tránh các hành vi xâm phạm quyền riêng tư, Nhật Bản cũng như châu Âu đã xây dựng hệ thống mô hình quản lý chặt chẽ, tạo nên một môi trường an toàn cho người dùng mạng xã hội. Theo đó, vào tháng 02/2000, Văn phòng An ninh công nghệ thông tin trong Ban Thư ký Nội các được thành lập; sau đó vào năm 2005, Trung tâm An toàn thông tin quốc gia và Hội đồng Chính sách an toàn thông tin được thành lập¹. Đạo luật cơ bản có một số nguyên tắc và khái niệm, trong đó nó cung cấp định nghĩa về “an ninh mạng” trong thuật ngữ pháp lý, đó là “việc xem xét, duy trì và quản lý các biện pháp cần thiết để ngăn chặn sự rò rỉ, phá hủy hoặc làm hỏng thông tin được báo cáo hoặc truyền hoặc nhận bằng cách điện tử, cách từ tính hoặc các cách khác mà con người không thể nhận ra, hoặc để quản lý việc kiểm soát an toàn thông tin đó, hoặc để bảo đảm an toàn và độ tin cậy của hệ thống thông tin hoặc mạng thông tin và truyền thông”², các nguyên tắc cơ bản của chính sách an ninh mạng, trách nhiệm của các bên liên quan, cấu trúc và chức năng của chiến lược và thành phần trụ sở chính về an ninh mạng. Do đó, tất cả các lĩnh vực chủ đề như vậy đã được củng cố trong

1. Xem Yamauchi, T: Cybersecurity strategy in Japan, Retrieved August 27, 2021, https://project.inria.fr/FranceJapanICST/files/2017/05/TYamauchi_presentation_2017.pdf.

2. Basic Act on Cybersecurity, Act No.104 of November 12, 2014 (amended 2016).

hệ thống pháp luật Nhật Bản bằng cách được xây dựng trong một văn bản pháp luật có hệ thống và duy nhất¹.

Ở châu Âu, việc bảo vệ an ninh mạng thực hiện bởi ENISA - Cơ quan An ninh mạng của EU - được Đạo luật An ninh mạng trao nhiệm vụ vĩnh viễn cung cấp cho cơ quan này nhiều nguồn lực hơn cũng như các nhiệm vụ mới. ENISA sẽ có vai trò chính trong việc thiết lập và duy trì khung chứng nhận an ninh mạng của châu Âu bằng cách chuẩn bị cơ sở kỹ thuật cho các chương trình chứng nhận cụ thể. Cơ quan này sẽ chịu trách nhiệm thông báo cho công chúng về các chương trình chứng nhận và các chứng chỉ đã được cấp thông qua một trang web chuyên dụng. Đạo luật An ninh mạng của Liên minh châu Âu giới thiệu một khuôn khổ chứng nhận an ninh mạng trên toàn Liên minh châu Âu cho các sản phẩm, dịch vụ và quy trình công nghệ thông tin - truyền thông. Các công ty kinh doanh ở EU sẽ được hưởng lợi từ việc chỉ phải chứng nhận các sản phẩm, quy trình và dịch vụ ICT của họ một lần và chứng nhận của họ được công nhận trên toàn Liên minh châu Âu².

Ở Hoa Kỳ, việc bảo vệ an ninh mạng được thực hiện bởi Hệ thống Bảo vệ an ninh mạng quốc gia (NCPS). Đây là một hệ thống tích hợp cung cấp một loạt các khả năng, chẳng hạn như phát hiện xâm nhập, phân tích, chia sẻ thông tin và ngăn chặn xâm nhập. Những khả năng này cung cấp nền

1. Xem Kim, K., Park, S.Lim, J: Changes of cybersecurity legal system in East Asia: Focusing on comparison between Korea and Japan, *Computer Science*, vol.9503, 2015, p.2016.

2. Xem Retrieved August 27, 2021 from: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>.

tảng công nghệ cho phép Cơ quan An ninh mạng và kết cấu hạ tầng (CISA) bảo mật và bảo vệ kết cấu hạ tầng công nghệ thông tin của Cơ quan Điều hành dân sự Liên bang (FCEB) trước các mối đe dọa mạng tiên tiến. NCPS bao gồm phần cứng, phần mềm, quy trình hỗ trợ, đào tạo và dịch vụ mà chương trình có được. Một trong những công nghệ quan trọng của CISA trong NCPS là EINSTEIN, một trong nhiều công cụ và khả năng hỗ trợ phòng thủ mạng liên bang. Mục tiêu của bộ khả năng NCPS EINSTEIN là cung cấp cho Chính phủ Liên bang một hệ thống cảnh báo sớm, cải thiện nhận thức tình huống về các mối đe dọa xâm nhập đối với mạng FCEB, xác định gần thời gian thực hoạt động mạng độc hại và ngăn chặn hoạt động mạng độc hại đó¹.

Nhìn chung, các quốc gia có hệ thống an ninh mạng tiên tiến xây dựng cho mình một cơ quan riêng biệt đảm nhiệm chức năng chính yếu để thực hiện các giải pháp chuyên môn và chính sách liên quan đến việc bảo vệ an ninh mạng quốc gia nói chung và trên các mạng xã hội nói riêng. Bất kỳ một hành vi chia sẻ thông tin đe dọa đến việc làm lan truyền hay ảnh hưởng đến quyền lợi hợp pháp của cá nhân, an toàn trên mạng xã hội đều sẽ bị theo dõi, phát hiện và xử lý kịp thời.

c) Kiến nghị thực thi có hiệu quả các biện pháp bảo vệ quyền về đời sống riêng tư trên môi trường không gian mạng ở Việt Nam

Khi nói về an ninh mạng, cũng cần phải nói rõ rằng rất khó để xóa dữ liệu được thu thập và lưu trữ trong thế giới ảo

1. Xem Retrieved August 27, 2021 from: <https://www.cisa.gov/national-cybersecurity-protection-system-ncps>.

của internet. Mọi thứ được thực hiện bởi mọi người trong thế giới ảo sẽ được lưu trữ dưới một hình thức nào đó. Thông qua internet, con người đã và sẽ tiếp tục đạt được những khả năng mới và giao tiếp toàn cầu trở nên dễ dàng hơn rất nhiều, nhưng con người kỹ thuật số hoàn toàn minh bạch và phải nhận thức được việc mất tự do và quyền riêng tư của mình¹.

Nhận thấy, việc bảo vệ môi trường không gian mạng là một lĩnh vực không đơn giản bởi tính đa dạng và tinh vi của các hành vi trên một không gian vô hình, khó kiểm soát. Vấn đề này không chỉ là thách thức đối với Việt Nam, mà còn là vấn đề rất được quan tâm trong việc thiết lập các chính sách an ninh ở các quốc gia. Xuất phát từ tính cấp thiết đó, nhận thấy các quy định pháp luật cũng như cách thức tiến hành các giải pháp bảo vệ an ninh mạng ở Việt Nam hiện nay vẫn chưa thực sự hoàn chỉnh, mang tính manh mún, sơ khai. Do đó, xét đến bối cảnh ở nước ta và kinh nghiệm trong việc lập chính sách, mô hình quản trị mạng xã hội và mối liên hệ với việc bảo vệ quyền về đời sống cá nhân, tác giả đề xuất một số nội dung như sau:

Thứ nhất, cần có sự định nghĩa giới hạn về quyền về đời sống riêng tư một cách chính xác, theo đó, bao hàm nội dung về thông tin cá nhân, hình ảnh, dữ liệu về thông tin được thể hiện dưới bất kỳ hình thức nào. Đây sẽ là căn cứ pháp lý

1. Xem Elias G. Carayannis, David F.J. Campbell, Marios Panagiotis Efthymiopoulos: *Cyber-Development, Cyber-Democracy and Cyber-Defense - Challenges, Opportunities and Implications for Theory, Policy and Practice*, Springer, 2014, p.15-16.

quan trọng để xác định rõ về các hành vi vi phạm, tạo sự hiểu biết cho người dùng mạng xã hội để họ có các ứng xử phù hợp với quy định của pháp luật.

Thứ hai, ban hành quy chế cho các doanh nghiệp cung cấp dịch vụ mạng xã hội. Theo đó, ràng buộc trách nhiệm của họ đối với Nhà nước trong việc kiểm soát, quản lý các hành vi xâm phạm đời sống riêng tư của người khác nói riêng hay đến an ninh quốc gia, an toàn thông tin nói chung. Các doanh nghiệp này phải tự kiểm soát, cung cấp thông tin cho Nhà nước về hành vi vi phạm, kịp thời ngăn chặn bằng công cụ kỹ thuật. Đây là giải pháp quan trọng nhằm tăng cường sự phối hợp giữa Nhà nước và tổ chức tư nhân trong việc chung tay xây dựng môi trường mạng sạch, an toàn.

Thứ ba, trang bị mô hình kiểm soát, quản lý mạng xã hội của cơ quan chịu trách nhiệm về an ninh mạng là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05). Đây là vấn đề thuộc về mặt kỹ thuật và đầu tư cho hệ thống quản lý của cơ quan nhà nước. Bên cạnh đó, quy định chi tiết thêm trách nhiệm trong việc phát hiện xâm nhập, phân tích, chia sẻ thông tin và ngăn chặn xâm nhập của nhóm cơ quan này, đồng thời ghi nhận quyền và nghĩa vụ xây dựng bộ quy tắc ứng xử chung và quản lý việc thực thi có hiệu quả chúng để góp phần tạo môi trường mạng xã hội an toàn, trong sạch.

Như vậy, giải pháp hiệu quả chính là sự tổng hòa các phương pháp trên, việc kết hợp chúng là nhu cầu cơ bản để góp phần tạo nên hiệu quả trong việc bảo vệ môi trường không gian mạng xã hội ở Việt Nam được an toàn hơn và bảo đảm được các giá trị mà chúng mang lại, tránh việc trở thành

công cụ để thực hiện các hành vi xâm phạm quyền về đời sống riêng tư của người khác.

*

* *

Các nền kinh tế phát triển và đang phát triển đều phải đối mặt với sự khan hiếm tài nguyên ngày càng tăng và sự cạnh tranh gay gắt. Khoa học và công nghệ ngày càng xuất hiện như một nguồn lợi thế cạnh tranh có tính bền vững của các quốc gia và khu vực. Tuy nhiên, chính nó lại trở thành tác nhân mới tạo nên môi trường cho các hành vi xâm phạm các quyền cá nhân của con người, trong đó có quyền về đời sống riêng tư. Do đó, để bảo đảm môi trường mạng xã hội thực sự trở thành công cụ hỗ trợ con người một cách an toàn, cần phải thiết lập hệ thống các giải pháp phòng ngừa, kiểm soát và xử lý một cách hiệu quả.

THỰC TRẠNG PHÁP LUẬT VIỆT NAM VỀ QUYỀN BẢO VỆ THÔNG TIN CÁ NHÂN TRÊN KHÔNG GIAN MẠNG

HỒ BẢO*

Sự kiện tháng 3/2018, mạng xã hội Facebook sa vào bê bối Cambridge Analytica gây hậu quả khoảng 50 triệu tài khoản người dùng bị lộ, lọt thông tin cá nhân¹ đã làm dấy lên mối lo ngại về vấn đề bảo mật thông tin cá nhân của người dùng mạng xã hội này. Trong bê bối này, Facebook ước tính có 427.446 tài khoản người dùng Việt Nam (đứng thứ 9 trên thế giới) bị lộ thông tin cá nhân, mức độ nghiêm trọng khiến Nhà nước Việt Nam hết sức quan tâm. Sự việc trên càng đáng lo ngại khi tại Việt Nam, tính đến tháng 7/2021, có hơn 77 triệu người dùng mạng xã hội Facebook, chiếm 77,4% dân số cả nước².

* Trường Đại học Luật Thành phố Hồ Chí Minh.

1. Xem Cadwalladr, C. & Graham - Harrison, E. (2018, 3 17): *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. Retrieved 8 6, 2021, from The Guardian: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

2. Xem *Facebook users in Vietnam*. (2021, 7). Retrieved 8 6, 2021, from NapoléonCat: <https://napoleoncat.com/stats/facebook-users-in-vietnam/2021/07>.

Tháng 5/2021, thông tin của hơn 10.000 giấy chứng minh nhân dân, thẻ căn cước công dân của người Việt Nam bị rao bán làm xôn xao dư luận, vụ việc đang được Bộ Công an xem xét và yêu cầu các đơn vị chức năng vào cuộc xác minh, điều tra làm rõ. Các số liệu đi kèm nhiều sự kiện vừa nêu chứng minh thực tiễn quyền bảo vệ thông tin cá nhân trên không gian mạng hiện nay đang diễn biến hết sức phức tạp, đòi hỏi cần sự vào cuộc, đóng góp của nhiều ngành, nhiều lĩnh vực mà trong đó, lĩnh vực pháp luật giữ vị trí rất quan trọng trong việc củng cố, tạo khung thể chế, pháp lý cho hoạt động bảo vệ thông tin cá nhân.

Với vai trò là một trong các thành tố xác lập nên không gian mạng¹, các chính sách, pháp luật chịu trách nhiệm quy định quy tắc ứng xử cho tổ chức, cá nhân khi tham gia không gian mạng, quy định trách nhiệm, quyền hạn của quản lý nhà nước đối với tổ chức, cá nhân; tạo hành lang pháp lý bảo đảm hoạt động an toàn và hiệu quả của không gian mạng, bảo vệ thông tin cá nhân đi liền với quyền và lợi ích hợp pháp của các bên tham gia không gian mạng².

Do đó, việc nghiên cứu hoàn thiện chính sách, pháp luật về quyền bảo vệ thông tin cá nhân trên không gian mạng là

1. “Không gian mạng” được cấu thành bởi 6 thành tố: (1) Chính sách, pháp luật; (2) Năng lực công nghệ; (3) Nội dung thông tin; (4) Nguồn nhân lực; (5) Tổ chức bộ máy; (6) Ý thức của con người.

2. Người viết cho rằng, thành tố pháp luật trong khái niệm “Không gian mạng” đang phát triển, hoàn thiện thành một ngành luật độc lập bên cạnh các ngành luật đã tồn tại, với những thể chế riêng biệt và giữ một vị trí quan trọng trong hệ thống pháp luật các quốc gia hiện đại, nó có thể được gọi là “luật mạng” (cyberlaw).

một trong những việc mấu chốt để xây dựng môi trường tương tác lành mạnh, hợp pháp và tiến bộ giữa cơ quan, tổ chức, cá nhân với nhau trên không gian mạng.

1. Thực trạng pháp luật Việt Nam về quyền bảo vệ thông tin cá nhân trên không gian mạng

a) Về khái niệm quyền

- Khái niệm thông tin cá nhân trên không gian mạng.

Về khái niệm thông tin cá nhân:

Luật an toàn thông tin mạng năm 2015 đã đưa ra định nghĩa “thông tin cá nhân” là *những thông tin gắn với việc xác định danh tính của một người cụ thể*, tức là những thông tin xoay quanh đời sống dân sự của một cá nhân có lai lịch cụ thể, đồng thời còn là căn cứ giúp người khác xác định hoặc nhận dạng cá nhân được nhắc đến bởi (những) thông tin đó.

Đây không phải là lần đầu tiên “thông tin cá nhân” được định nghĩa trong một văn bản quy phạm pháp luật, trước đó tại khoản 5, Điều 3 Nghị định số 64/2007/NĐ-CP, ngày 10/4/2007 của Chính phủ quy định về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước đã bước đầu đưa ra định nghĩa “Thông tin cá nhân: là thông tin đủ để xác định chính xác danh tính một cá nhân, bao gồm ít nhất nội dung trong những thông tin sau đây: họ tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ liên hệ, địa chỉ thư điện tử, số điện thoại, số chứng minh nhân dân, số hộ chiếu. Những thông tin thuộc bí mật cá nhân gồm có hồ sơ y tế, hồ sơ nộp thuế, số thẻ bảo hiểm xã hội, số thẻ tín dụng và những bí mật cá nhân khác”. Căn cứ Nghị định số 64/2007/NĐ-CP,

khoản 3, Điều 3 Thông tư số 25/2010/TT-BTTTT, ngày 15/11/2010 của Bộ Thông tin và Truyền thông quy định việc thu thập, sử dụng, chia sẻ, bảo đảm an toàn và bảo vệ thông tin cá nhân trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước cũng giải thích tương tự. Có thể thấy, trước khi được luật hóa, định nghĩa về “thông tin cá nhân” trong các văn bản dưới luật về cơ bản không khác nhau khi phân chia thông tin cá nhân thành hai loại gồm thông tin cá nhân thông thường (họ tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ liên hệ, địa chỉ thư điện tử, số điện thoại, số chứng minh nhân dân, số hộ chiếu) và bí mật cá nhân (hồ sơ y tế, hồ sơ nộp thuế, số thẻ bảo hiểm xã hội, số thẻ tín dụng và những bí mật cá nhân khác).

Đến Luật an toàn thông tin mạng năm 2015 đã không liệt kê các dạng thông tin theo từng loại thông tin cụ thể như Nghị định số 64/2007/NĐ-CP và Thông tư số 25/2010/TT-BTTTT mà chỉ nêu nội hàm để mô tả “thông tin cá nhân”. Theo đó, bất kỳ thông tin nào có thể dùng để xác định danh tính của một người cụ thể thì được xem là thông tin cá nhân mà không cần xét tới đó là thuộc loại thông tin nào. Xét trong bối cảnh công nghệ thông tin và đời sống dân sự phát triển ngày càng phong phú, mạnh mẽ, đa dạng và tinh vi hơn, cách quy định này của Luật an toàn thông tin mạng góp phần bảo vệ, bảo đảm tốt hơn quyền được bảo vệ thông tin cá nhân, kể cả trên không gian mạng.

Về khái niệm không gian mạng:

Đối với khái niệm “không gian mạng”, theo khoản 3, Điều 2, Luật an ninh mạng năm 2018, “không gian mạng” được hiểu là “mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin,

bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian”. Theo cách định nghĩa này, không gian mạng bao gồm hai bản chất là bản chất vật lý và bản chất xã hội.

Xét theo bản chất vật lý, không gian mạng là mạng lưới kết nối trên phạm vi toàn cầu của các kết cấu hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu. Định nghĩa của Luật an ninh mạng năm 2018 đã phân chia cấu trúc của không gian mạng, gồm 3 lớp: (1) Hạ tầng truyền dẫn vật lý bao gồm các thiết bị, phần cứng (hardware) công nghệ kết nối với nhau tạo ra các loại mạng như *mạng viễn thông, mạng internet, mạng máy tính*; (2) Hạ tầng dịch vụ lõi và các dịch vụ tạo ra các giao thức (protocol) *xử lý và điều khiển thông tin*; (3) Hệ thống ứng dụng công nghệ thông tin và *cơ sở dữ liệu* (database). Ngoài ra, cấu trúc không gian mạng còn có những cách phân chia khác, Gálik, S., và Tolnaiová, S.G. cho rằng, cấu trúc không gian mạng bao gồm kỹ thuật và ngữ nghĩa (vật lý, logic, thông tin và con người)¹.

Xét theo bản chất xã hội, không gian mạng là nơi mà con người thực hiện các hành vi theo bản chất xã hội của mình bằng mọi cách thức mà không hạn chế về không gian

1. Xem Gálik, S. & Tolnaiová, S.G. (2019, 7 25): Cyberspace as a New Existential Dimension of Man. Retrieved 8 2021, 7, from IntechOpen: <https://www.intechopen.com/chapters/68281>.

và thời gian. Trong không gian mạng, người ta có thể lao động, học tập, vui chơi, giải trí, sáng tạo,... trong bối cảnh mọi thứ được vận hành nhanh chóng và tiện nghi; phản ánh một “xã hội mạng” thông qua tính đa chiều và khả năng tương tác vô hạn. Các tác giả Gálik, S., và Tolnaiová, S.G. chỉ ra không gian mạng đại diện cho một loại thế giới hoặc chiều không gian được xây dựng mang tính xã hội, một Agora điện tử - một không gian công cộng trung tâm¹.

Bản chất xã hội của không gian mạng cũng là nguồn gốc của mối liên hệ biện chứng giữa thông tin cá nhân trên không gian mạng và không gian mạng. Nó biểu hiện ở chỗ, trong quá trình tương tác, thực hiện hành vi xã hội của mình trên không gian mạng, con người phải cần chia sẻ các thông tin cá nhân để thực hiện các hành vi đó; mặt khác, không gian mạng là nơi chứa đựng, xử lý, lưu trữ, truyền đưa,... thông tin cá nhân của một người cụ thể, khi họ thực hiện các hành vi xã hội của mình.

Từ các phân tích trên, người viết đưa ra định nghĩa *“thông tin cá nhân trên không gian mạng là những thông tin tồn tại trong mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin gắn với việc xác định danh tính của một người cụ thể nhằm thực hiện các hành vi xã hội của mình”*.

- *Khái niệm quyền bảo vệ thông tin trên không gian mạng:*

Như đã phân tích trên, cá nhân khi thực hiện các hành vi xã hội của mình trên không gian mạng đều ít nhiều phải

1. Xem Gálik, S. & Tolnaiová, S. G. (2020, 3 28): Cyberspace as a New Living World and Its Axiological Contexts. Retrieved 8 2021, 7, from IntechOpen: <https://www.intechopen.com/chapters/71568>.

chia sẻ thông tin cá nhân của mình cho các chủ thể khác cùng tham gia theo cách thức chủ động hoặc bị động. Từ đó phát sinh nhu cầu được bảo vệ các thông tin cá nhân đó khỏi những mục đích, hành vi xấu gây thiệt hại về nhân thân và tài sản đối với chủ thể thông tin cá nhân, hay nói cách khác, mỗi cá nhân khi tham gia không gian mạng đều có quyền bảo vệ thông tin cá nhân của mình trên không gian mạng.

Khi nói đến quyền bảo vệ thông tin cá nhân, dù là trên không gian mạng hay bất cứ nơi nào khác, cũng cần xuất phát từ góc nhìn dân sự. Bởi lẽ, quyền bảo vệ thông tin cá nhân của một người mang đầy đủ các đặc điểm của một quyền nhân thân của người đó; là quyền dân sự gắn liền với mỗi cá nhân, không thể chuyển giao cho người khác, trừ trường hợp luật có quy định khác. Hơn nữa, hầu hết các quyền nhân thân được liệt kê trong Mục 2, Chương 3 Bộ luật dân sự năm 2015 đều là các quyền đối với thông tin xác định cá nhân, như họ tên, dân tộc, quốc tịch, hình ảnh, giới tính, đời sống riêng tư, bí mật cá nhân, bí mật gia đình. Điều đó cho thấy, quyền được bảo vệ thông tin cá nhân là một quyền nhân thân trong các quyền dân sự được pháp luật dân sự bảo hộ với vai trò là nền tảng, bên cạnh sự bảo hộ của các lĩnh vực pháp luật khác.

Từ phân tích trên, người viết cho rằng, quyền bảo vệ thông tin cá nhân trên không gian mạng là *quyền nhân thân nhằm bảo vệ những thông tin tồn tại trong mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin gắn với việc xác định danh tính của một người cụ thể nhằm thực hiện các hành vi xã hội của mình*.

b) Về các nguyên tắc thực hiện quyền bảo vệ thông tin cá nhân trên không gian mạng

Nguyên tắc thứ nhất: Nguyên tắc tự bảo vệ.

Luật an toàn thông tin mạng năm 2015 quy định các nguyên tắc bảo vệ thông tin cá nhân trên mạng, trong đó nguyên tắc tiên quyết và chủ yếu được luật nhấn mạnh là nguyên tắc “Tự bảo vệ”. Cụ thể, khoản 1, Điều 16 luật này quy định cá nhân tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng. Bởi lẽ, không ai khác ngoài cá nhân, cũng chính là chủ thể thông tin cá nhân của bản thân, là người biết rõ và có đầy đủ các điều kiện để tìm hiểu về thông tin cá nhân của mình. Đồng thời, cá nhân chủ thể thông tin cá nhân có toàn quyền trong việc quyết định có cung cấp, chia sẻ thông tin cá nhân của mình cho người khác hay không, kể cả trên không gian mạng. Do đó, cá nhân phải có trách nhiệm đối với thông tin cá nhân của mình, phải có ý thức đề phòng, bảo mật thông tin cá nhân của mình, đặc biệt là đời sống riêng tư, bí mật cá nhân, bí mật gia đình trong lúc sử dụng các dịch vụ trên không gian mạng.

Nguyên tắc thứ hai: Nguyên tắc tôn trọng quyền bảo vệ thông tin cá nhân của chủ thể thông tin cá nhân.

Bên cạnh việc nhấn mạnh đến ý thức tự bảo vệ thông tin cá nhân trên không gian mạng, Điều 16, Luật an toàn thông tin mạng năm 2015 còn đưa ra các quy định nhằm buộc cơ quan, tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lý (khoản 2); đồng thời, buộc tổ chức, cá nhân xử lý thông tin cá nhân phải xây dựng và công bố công khai biện

pháp xử lý, bảo vệ thông tin cá nhân của tổ chức, cá nhân mình (khoản 3). Có thể thấy, các biện pháp mà Luật an toàn thông tin mạng năm 2015 đưa ra nhằm cụ thể hóa nguyên tắc hiến định bất khả xâm phạm về thông tin đời sống riêng tư, bí mật cá nhân, bí mật gia đình (Điều 21, Hiến pháp năm 2013). Đồng thời, đây cũng là sự phối hợp giữa các ngành luật công - tư khi Luật an toàn thông tin mạng năm 2015 có các quy định ràng buộc buộc cơ quan, tổ chức, cá nhân xử lý thông tin cá nhân để bảo đảm tốt hơn quyền dân sự được bảo vệ liên quan đến đời sống riêng tư, bí mật cá nhân và bí mật gia đình được quy định trong Bộ luật dân sự năm 2015.

Đây không phải lần đầu tiên thông tin cá nhân trên không gian mạng được một đạo luật đề ra các biện pháp yêu cầu các cơ quan, tổ chức, cá nhân khác phải có trách nhiệm bảo vệ. Trước đó, khoản 2, Điều 46 Luật giao dịch điện tử năm 2005 đã ràng buộc cơ quan, tổ chức, cá nhân không được sử dụng, cung cấp hoặc tiết lộ thông tin về bí mật đời tư hoặc thông tin của cơ quan, tổ chức, cá nhân khác mà mình tiếp cận hoặc kiểm soát được trong giao dịch điện tử nếu không được sự đồng ý của họ, trừ trường hợp pháp luật có quy định khác. Ngoài ra, còn nhiều đạo luật cũng quy định về quyền bảo vệ thông tin cá nhân trên không gian mạng tương ứng với mỗi lĩnh vực mà mình điều chỉnh.

c) Về nội dung quyền và giới hạn của quyền bảo vệ thông tin cá nhân trên không gian mạng

- Nội dung quyền:

Nhìn chung, quyền bảo vệ thông tin cá nhân trên không gian mạng được pháp luật Việt Nam tiếp cận dưới góc độ quyền dân sự chủ động. Theo đó, Luật an toàn thông tin

mạng năm 2015 quy định chủ thể thông tin cá nhân được thực thi quyền của mình theo hai cách thức:

Một là, cá nhân có quyền quyết định trong việc cung cấp, chia sẻ thông tin và yêu cầu cung cấp thông tin cá nhân của mình. Đối với việc cá nhân có quyền quyết định trong việc cung cấp, chia sẻ thông tin, khoản 1, Điều 17, Luật an toàn thông tin mạng năm 2015 quy định tổ chức, cá nhân xử lý thông tin cá nhân chỉ được tiến hành thu thập thông tin cá nhân sau khi có sự đồng ý của chủ thể thông tin cá nhân về phạm vi, mục đích của việc thu thập và sử dụng thông tin đó; đồng thời, các tổ chức, cá nhân này chỉ sử dụng thông tin cá nhân đã thu thập vào mục đích khác mục đích ban đầu sau khi có sự đồng ý của chủ thể thông tin cá nhân.

Điều đó có nghĩa là quyền quyết định cho phép tổ chức, cá nhân khác có quyền thu thập thông tin của mình thuộc về chủ thể thông tin cá nhân. Chủ thể thông tin cá nhân còn có quyền quyết định phạm vi, mục đích sử dụng thông tin cá nhân của mình đối với tổ chức, cá nhân xử lý thông tin cá nhân. Quy định này trong Luật an toàn thông tin mạng năm 2015 tương đồng với quy định tại khoản 2, Điều 38, Bộ luật dân sự năm 2015 quy định việc thu thập, lưu giữ, sử dụng, công khai thông tin liên quan đến đời sống riêng tư, bí mật cá nhân phải được người đó đồng ý, việc thu thập, lưu giữ, sử dụng, công khai thông tin liên quan đến bí mật gia đình phải được các thành viên gia đình đồng ý, trừ trường hợp luật có quy định khác.

Bên cạnh đó, khoản 3, Điều 17, Luật an toàn thông tin mạng năm 2015 còn cho phép chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân cung

cấp thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ.

Hai là, khoản 1, Điều 18 Luật an toàn thông tin mạng năm 2015 quy định chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân cập nhật, sửa đổi, hủy bỏ thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ hoặc ngừng cung cấp thông tin cá nhân của mình cho bên thứ ba. Theo đó, chủ thể thông tin cá nhân không những có quyền trước khi thông tin cá nhân được thu thập mà còn có quyền đối với thông tin cá nhân của mình sau khi được tổ chức, cá nhân thu thập, các quyền đó có thể là yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân thay đổi (cập nhật, sửa đổi) hoặc hủy bỏ thông tin cá nhân của mình trong hệ thống lưu trữ, xử lý của tổ chức, cá nhân đó.

Về phần mình, Luật an ninh mạng năm 2018 đã quy định cụ thể về bảo vệ thông tin thuộc bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng (Điều 17). Theo đó, luật này quy định các hành vi được xem là hành vi xâm phạm bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng bao gồm:

- Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

- Cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin thuộc bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng;

- Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật cá nhân, bí mật gia đình và đời sống riêng tư;

- Đưa lên không gian mạng những thông tin thuộc bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật;

- Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại;

- Hành vi khác cố ý xâm phạm bí mật cá nhân, bí mật gia đình và đời sống riêng tư.

Điểm a, khoản 2, Điều 26 Luật an ninh mạng cũng quy định các doanh nghiệp trong và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm bảo mật thông tin, tài khoản của người dùng. Quy định này nhằm hạn chế, ngăn chặn việc bán thông tin người dùng cho các doanh nghiệp cung cấp dịch vụ hoặc bên thứ ba mà chưa có sự đồng ý của người dùng.

- Giới hạn quyền:

Như bất kỳ quyền nào khác của con người, của công dân, quyền bảo vệ thông tin cá nhân trên không gian mạng cũng có giới hạn. Xuất phát từ nguyên tắc hiến định “Quyền con người, quyền công dân chỉ có thể bị hạn chế theo quy định của luật trong trường hợp cần thiết vì lý do quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, đạo đức xã hội, sức khỏe của cộng đồng” (khoản 2, Điều 14, Hiến pháp năm 2013), các đạo luật trong lĩnh vực an toàn thông tin đều ghi nhận giới hạn quyền đối với quyền bảo vệ thông tin cá nhân trên không gian mạng. Cụ thể:

Khoản 5, Điều 16, Luật an toàn thông tin mạng năm 2015 ghi nhận việc xử lý thông tin cá nhân phục vụ mục đích bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn

xã hội thì không thuộc phạm vi điều chỉnh của luật này mà được thực hiện theo quy định khác của pháp luật có liên quan. Như vậy, điểm giới hạn của quyền bảo vệ thông tin cá nhân trên không gian mạng được đặt ra đối với trường hợp nhằm bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, việc xử lý thông tin cá nhân không bị chi phối bởi các quyền của chủ thể thông tin cá nhân được quy định trong Luật an toàn thông tin mạng năm 2015.

Đồng thời, so với nguyên tắc hiến định “quyền con người, quyền công dân chỉ bị hạn chế theo quy định của luật”, Luật an toàn thông tin mạng năm 2015 đã giảm cấp độ hiệu lực văn bản điều chỉnh từ “theo quy định của luật” thành “theo pháp luật có liên quan”, cụm từ “pháp luật” ở đây chỉ các đạo luật và cả văn bản dưới luật.

Sang đến Luật an ninh mạng năm 2018, điểm a, khoản 2, Điều 26 luật này quy định doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng. Như vậy, khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng, các doanh nghiệp phải cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an.

Ngoài ra, giới hạn của quyền bảo vệ thông tin cá nhân trên không gian mạng còn được thể hiện ở Điều 223, Bộ luật tố tụng hình sự năm 2015 quy định một số biện pháp điều tra

tố tụng đặc biệt. Cụ thể, sau khi khởi tố vụ án, trong quá trình điều tra, người có thẩm quyền tiến hành tố tụng có thể áp dụng các biện pháp điều tra tố tụng đặc biệt như: ghi âm, ghi hình bí mật, nghe điện thoại bí mật và thu thập bí mật dữ liệu điện tử. Tuy nhiên, bộ luật này cũng quy định chỉ có thể áp dụng biện pháp điều tra tố tụng đặc biệt đối với các trường hợp là tội xâm phạm an ninh quốc gia, tội phạm về ma túy, tội phạm về tham nhũng, tội khủng bố, tội rửa tiền và tội phạm khác có tổ chức thuộc loại tội phạm đặc biệt nghiêm trọng. Đồng thời, thông tin, tài liệu thu thập được bằng biện pháp điều tra tố tụng đặc biệt chỉ được sử dụng vào việc khởi tố, điều tra, truy tố, xét xử vụ án hình sự; thông tin, tài liệu không liên quan đến vụ án phải tiêu hủy kịp thời. Nghiêm cấm sử dụng thông tin, tài liệu, chứng cứ thu thập được vào mục đích khác.

d) Một số bất cập về quyền bảo vệ thông tin cá nhân trên không gian mạng

Qua tìm hiểu, phân tích các quy định pháp luật về quyền bảo vệ thông tin cá nhân trên không gian mạng, người viết nhận thấy pháp luật Việt Nam có một số bất cập gây khó khăn, vướng mắc trong khi áp dụng pháp luật. Cụ thể là:

Thứ nhất, các quy định pháp luật về quyền bảo vệ thông tin cá nhân trên không gian mạng quy định một cách rời rạc, tản mạn trong nhiều văn bản pháp luật khác nhau gây khó khăn trong việc tìm hiểu, vận dụng và pháp điển hóa. Không những tồn tại trong các văn bản pháp luật lĩnh vực an ninh, an toàn thông tin, quy định pháp luật về quyền bảo vệ thông tin cá nhân trên không gian mạng tồn tại trong hàng loạt các văn bản pháp luật của nhiều lĩnh vực khác nhau như

Luật giao dịch điện tử, Luật công nghệ thông tin, Luật viễn thông, Luật khám bệnh, chữa bệnh, Luật quản lý thuế,... và nhiều văn bản dưới luật khác.

Thứ hai, các quy định định nghĩa “thông tin cá nhân” còn chưa thống nhất giữa các văn bản pháp luật cùng đang có hiệu lực như đã nêu, không những vậy, pháp luật Việt Nam còn sản sinh ra nhiều thuật ngữ luật định có liên quan, tương tự nhau, giao nhau về nội hàm như “đời sống riêng tư”, “bí mật cá nhân”, “bí mật đời tư”,... đều chưa được định nghĩa rõ ràng và khó phân biệt, gây vướng mắc trong việc nghiên cứu và áp dụng pháp luật nhằm bảo vệ thông tin cá nhân trên không gian mạng trong nhiều trường hợp.

Thứ ba, về vị trí trung tâm của các biện pháp bảo vệ, mặc dù tiếp cận quyền bảo vệ thông tin cá nhân trên không gian mạng dưới góc độ quyền chủ động nhưng các luật về an ninh, an toàn thông tin lại đưa ra quá ít biện pháp để một cá nhân có thể linh hoạt trong việc yêu cầu chủ thể khác bảo vệ thông tin cá nhân của mình trên không gian mạng mà chỉ tập trung vào việc đưa ra các biện pháp ràng buộc tổ chức, cá nhân xử lý thông tin cá nhân. Người viết đồng ý với quan điểm của tác giả Nguyễn Hương Ly khi cho rằng thay vì nên đặt chủ thể thông tin cá nhân ở vị trí của mọi biện pháp bảo vệ thì quy định của Luật an toàn thông tin mạng và các luật liên quan khác ở nước ta vẫn tập trung hơn vào quyền và trách nhiệm của các tổ chức, doanh nghiệp thu thập và xử lý dữ liệu¹.

1. Xem Nguyễn Hương Ly: *Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã*. Được truy lục từ Pháp luật hiện hành của Việt Nam về bảo vệ dữ liệu, thông tin cá nhân và quyền riêng tư: <https://nacis.gov.vn/nguyen-cuu-trao-doi/-/view-content/214123/phap-luat-hien-hanh-cua-viet-nam-ve-bao-ve-du-lieu-thong-tin-ca-nhan-va-quyen-rieng-tu>, ngày 25/12/2020.

2. Kiến nghị hoàn thiện pháp luật về quyền bảo vệ thông tin cá nhân trên không gian mạng

Từ những bất cập nói trên, người viết xin nêu một số kiến nghị nhằm giải quyết các bất cập, kiện toàn khung pháp lý, hoàn thiện pháp luật về quyền bảo vệ thông tin cá nhân trên không gian mạng như sau:

Thứ nhất, tập hợp hóa quy định pháp luật về quyền bảo vệ thông tin cá nhân trên không gian mạng. Trước mắt, trong bối cảnh, điều kiện chưa cho phép ban hành một văn bản riêng biệt chứa quy phạm pháp luật điều chỉnh hành vi, xử sự trên không gian mạng nói chung và bảo vệ thông tin cá nhân trên không gian mạng nói riêng, thì các cơ quan nhà nước có thẩm quyền cần tập hợp hóa pháp luật trong bộ pháp điển theo hướng sắp xếp các quy phạm đó theo một trật tự logic, hợp lý và dễ dàng tra cứu.

Thứ hai, đồng bộ hóa quy định pháp luật về các thuật ngữ có ngữ nghĩa tương đồng, chồng lấn nhau về nội hàm. Cần kiến nghị Ủy ban Thường vụ Quốc hội thực hiện trách nhiệm, quyền hạn giải thích luật đối với các từ ngữ “thông tin cá nhân”, “đời sống riêng tư”, “bí mật cá nhân”, “bí mật đời tư”... còn chưa thống nhất giữa các văn bản pháp luật cùng đang có hiệu lực như đã nêu.

Thứ ba, cần đặt chủ thể thông tin cá nhân ở vị trí trung tâm của mọi biện pháp bảo vệ; đổi mới tư duy trong mọi hoạt động lập pháp, lập quy về quyền bảo vệ thông tin cá nhân trên không gian mạng cần theo hướng bảo đảm “an ninh con người” trên không gian mạng. Chỉ có như vậy, pháp luật mới thực sự bảo vệ, bảo đảm quyền con người, quyền công dân,

lấy con người làm trung tâm thay vì ràng buộc trách nhiệm, nghĩa vụ cho các tổ chức, doanh nghiệp, cá nhân cung cấp dịch vụ mạng.

Tóm lại, xu hướng phát triển không gian mạng là quy luật tất yếu không thể đảo ngược trên phạm vi toàn cầu. Tuy mang tính phi truyền thống, song không gian mạng là một nơi không thể thiếu vắng các quy định pháp luật nhằm bảo vệ quyền con người, quyền công dân, một trong những ưu tiên hàng đầu là bảo vệ các quyền nhân thân liên quan đến thông tin cá nhân của mỗi người. Cần ghi nhận pháp luật Việt Nam đã nhanh chóng thích ứng với nhiều đòi hỏi chưa có tiền lệ của Cách mạng công nghiệp lần thứ tư (cách mạng số), kịp thời có khung pháp lý điều chỉnh quan hệ xã hội phát sinh trên không gian mạng. Tuy nhiên, một số bất cập đã phát sinh cần bổ khuyết, củng cố để hoàn thiện pháp luật nhằm đáp ứng tốt hơn diễn biến của nền kinh tế - xã hội trong công cuộc công nghiệp hóa, hiện đại hóa đất nước.

CHỦ THỂ DỮ LIỆU, CHỦ THỂ KIỂM SOÁT DỮ LIỆU VÀ CHỦ THỂ XỬ LÝ DỮ LIỆU TRONG PHÁP LUẬT VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN

ThS. NGUYỄN TẤN HOÀNG HẢI*

TRẦN VÕ KIỀU ANH**

HOÀNG THỊ KHÁNH HIỀN***

NGUYỄN PHẠM THANH HOA****

Dữ liệu cá nhân là những thông tin liên quan đến một cá nhân và có thể giúp xác định ra cá nhân đó. Trong pháp luật bảo vệ dữ liệu cá nhân, cá nhân đó được gọi là chủ thể dữ liệu. Chủ thể dữ liệu có những quyền nhất định đối với dữ liệu cá nhân của mình, chẳng hạn như quyền được thông báo khi dữ liệu cá nhân bị tác động bởi một bên, bất kể gián tiếp hay trực tiếp. Giữa chủ thể dữ liệu và chủ thể có hành vi tác động nói trên tồn tại một quan hệ pháp luật xung đột về quyền lợi. Qua đó, việc nhận diện các chủ thể liên quan đến dữ liệu cá nhân một cách rõ ràng, đầy đủ và toàn diện là cơ sở quan trọng để góp phần làm hài hòa mối xung đột và bảo vệ dữ liệu cá nhân.

*, **, ***, **** Trường Đại học Luật Thành phố Hồ Chí Minh.

1. Khái niệm về chủ thể dữ liệu

Mục đích chính của các quyền của chủ thể dữ liệu là để bảo vệ quyền riêng tư cho cá nhân, những người được gọi là chủ thể dữ liệu. Pháp luật bảo vệ dữ liệu cá nhân còn có các mục đích khác như góp phần phát triển nền kinh tế kỹ thuật số và chính phủ điện tử, nhưng lý do chính cho sự tồn tại của nó là để bảo vệ chủ thể dữ liệu và công nhận rằng họ cần sự bảo vệ pháp lý chuyên biệt trong thời đại kỹ thuật số¹.

Chủ thể dữ liệu được gọi tên theo nhiều cách khác nhau trong pháp luật bảo vệ dữ liệu ở châu Âu, Ôxtrâyliya, Xingapo và Nhật Bản. Tuy vậy, chủ thể dữ liệu vẫn có những đặc điểm tương đồng trong các văn bản pháp luật bảo vệ dữ liệu. Theo Quy định chung về bảo vệ dữ liệu cá nhân của Liên minh châu Âu (GDPR), chủ thể dữ liệu là một cá nhân được xác định hoặc có thể xác định được². Luật bảo vệ quyền riêng tư của Ôxtrâyliya (APP), Luật bảo vệ thông tin cá nhân của Xingapo (PDPA) và Luật bảo vệ thông tin cá nhân của Nhật Bản (APPI) đều dùng thuật ngữ “cá nhân” để chỉ chủ thể dữ liệu. Cá nhân đó đã xác định hoặc có thể được xác định³ và phải đang sống.

Khoản 16, Điều 3 Luật an toàn thông tin mạng năm 2015 của Việt Nam quy định chủ thể thông tin cá nhân là người được xác định từ thông tin cá nhân đó. Trong khi đó, dự thảo số 2 Nghị định về bảo vệ dữ liệu cá nhân năm 2021 (sau đây

1. Xem Peter Blume: “The Data Subject”, *European Data Protection Law Review*, 2015, p.258.

2. Khoản 1, Điều 4 GDPR.

3. Điều 6; khoản 4, Điều 4 PDPA.

gọi tắt là Dự thảo Nghị định) định nghĩa chủ thể dữ liệu là người mà dữ liệu cá nhân phản ánh (khoản 5, Điều 2).

Như vậy, để hình thành cơ sở phân biệt giữa chủ thể dữ liệu với một số chủ thể khác trong hoạt động xử lý dữ liệu cá nhân thì phải làm rõ ba yếu tố tạo nên khái niệm chủ thể dữ liệu.

Thứ nhất, chủ thể dữ liệu là cá nhân. Các thực thể khác như pháp nhân sẽ không được xem là chủ thể dữ liệu và không thuộc phạm vi điều chỉnh của pháp luật bảo vệ dữ liệu cá nhân, vì cá nhân và pháp nhân khác nhau về đặc điểm nhận dạng và địa vị pháp lý¹. Thay vào đó, pháp nhân sẽ được điều chỉnh bởi pháp luật khác².

Thứ hai, chủ thể dữ liệu là người đang sống. Nói cách khác, định nghĩa này không bao gồm người đã qua đời. Đối với GDPR, việc bảo vệ dữ liệu của những cá nhân đã qua đời sẽ do các quốc gia thành viên quyết định³. Đáng chú ý là, ở Xingapo, PDPA vẫn điều chỉnh dữ liệu của cá nhân đã chết từ mười năm trở xuống, nhưng lại không áp dụng đối với các dữ liệu cá nhân mà đã được lưu trữ 100 năm ngay cả khi đó là dữ liệu về một cá nhân vẫn đang sống⁴. Ở Việt Nam, tuy không được nói rõ trong Luật an toàn thông tin mạng và Dự thảo Nghị định nhưng chủ thể dữ liệu có thể ngầm hiểu là đang sống. Quy định về đặc điểm của chủ thể dữ liệu là một

1, 2. Xem Peter Blume: “The Data Subject”, *Tlidd*, p.258-264.

3. Xem One Trust Data Guidance, Mills Oakley: “Comparing privacy laws: GDPR v. Australian Privacy Act” 2020, tr.4, https://www.dataguidance.com/sites/default/files/gdpr_v_australia.pdf, truy cập ngày 15/5/2021.

4. Khoản 4, Điều 4 PDPA.

cá nhân đang còn sống hoàn toàn phù hợp. Vì thực tế, người chết không thể tham gia vào các quan hệ pháp luật liên quan đến dữ liệu cá nhân, nên việc pháp luật điều chỉnh đối tượng này hầu như không cần thiết, trừ việc nhận dạng trên giấy chứng tử. Tuy nhiên, trong một số trường hợp, từ dữ liệu cá nhân của người chết, có thể suy ra thông tin của những người thân quen đang sống; điều này cũng dấy lên mối lo ngại khi mà việc xử lý dữ liệu cá nhân của người chết không bị pháp luật điều chỉnh.

Thứ ba, cá nhân đó xác định hoặc có khả năng xác định qua dữ liệu cá nhân.

Một là, cá nhân xác định, cụ thể người này đã được xác định trước đó qua các thông tin liên quan. Tức là, cá nhân đã được xác định cụ thể và có thể được nhận dạng thông qua các dữ liệu cá nhân mà họ cung cấp như tên, địa chỉ, mã số nhận dạng, giấy phép lái xe,... hoặc một số thông tin liên quan trực tiếp đến cá nhân đó.

Hai là, cá nhân có khả năng xác định, cụ thể người này chưa được xác định trước đó nhưng có thể được xác định từ các dữ liệu cá nhân¹. Tức là, cá nhân chưa được xác định ngay lập tức và phải dựa vào những thông tin liên quan khác thì mới có thể xác định và nhận dạng được. Nhận dạng cá nhân trong trường hợp này được xem là mất thời gian hơn so với trường hợp cá nhân xác định vì cần nhiều thông tin khác.

1. Xem Nadezhda Purtova: “The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology”, <https://doi.org/10.1080/17579961.2018.1452176>, 2018, truy cập ngày 16/02/2021.

Cần hiểu “xác định” ở đây không chỉ là xác định về danh tính như tên, tuổi; vì trên thực tế, chủ thể dữ liệu có thể thu thập và xác định cá nhân thông qua việc xác định thói quen, sở thích, xu hướng mà không có nhu cầu biết tên, tuổi để thực hiện các chiến lược quảng cáo sản phẩm. Điển hình là hồ sơ bóng tối của mạng xã hội Facebook¹. Cụ thể, người dùng mạng xã hội Facebook dù không để lại tên, tuổi nhưng quan điểm sống, thói quen, tư tưởng của họ có thể được Facebook xác định dựa trên những hành động, dấu vết mà họ để lại thông qua các bình luận hoặc bằng các biểu tượng cảm xúc. Nguy hiểm hơn là, mặc dù cá nhân không sử dụng mạng xã hội Facebook nhưng thông qua những người dùng khác xung quanh họ, các thông tin của họ có thể bị thu thập mà họ không hề hay biết. Từ đó, việc xác định cá nhân không còn là điều khó khăn trong thời đại công nghệ hiện nay, song nó cũng được xem là mối nguy hiểm đối với người sử dụng mạng xã hội nói riêng và cá nhân có dữ liệu nói chung.

Muốn biết một cá nhân có khả năng xác định hay không thì cần xem xét mọi phương thức xác định hợp lý, dù là trực tiếp hoặc gián tiếp. Trong đó, tính hợp lý của các phương thức được đánh giá qua các nhân tố khách quan như chi phí và thời gian cần thiết, công nghệ tại thời điểm xử lý dữ liệu cá nhân². Chẳng hạn, tại thời điểm xử lý dữ liệu, thời gian xác định một cá nhân có thể khác nhau nếu phương thức

1. Xem Đỗ Quyên: “Facebook giữa tâm bão: Hồ sơ bóng tối”, <https://nld.com.vn>, truy cập ngày 30/4/2021.

2. Phụ lục giải thích số 26 của GDPR.

đánh giá khác nhau. Đối với dữ liệu cá nhân thu thập gián tiếp từ bên thứ ba, thời gian thực tế để xác định cá nhân đó có thể sẽ lâu hơn đối với dữ liệu cá nhân được thu thập trực tiếp từ cá nhân đó. Đối với trường hợp dữ liệu cá nhân được thu thập thông qua các phương tiện như điện thoại, thư điện tử, fax thì sẽ nhanh chóng và hiệu quả hơn so với việc thu thập dữ liệu cá nhân bằng các tài liệu giấy.

Quan điểm của các nhà lập pháp Việt Nam về chủ thể dữ liệu trong Dự thảo Nghị định khá tương đồng với các quốc gia trên thế giới: chủ thể dữ liệu là cá nhân xác định hoặc có khả năng xác định từ dữ liệu cá nhân.

2. Khái niệm về chủ thể kiểm soát và chủ thể xử lý dữ liệu

Để bảo đảm việc bảo vệ dữ liệu cá nhân, việc thực thi nghĩa vụ của các chủ thể có trách nhiệm đóng vai trò quan trọng. Chính vì sự quan trọng này mà pháp luật bảo vệ dữ liệu cá nhân luôn phải xác định rõ ràng những chủ thể cụ thể nào chịu trách nhiệm tuân thủ pháp luật cũng như quy định rõ nghĩa vụ và trách nhiệm của họ¹. Thông qua nghĩa vụ của những chủ thể đó, chủ thể dữ liệu sẽ gián tiếp được pháp luật bảo vệ những quyền về dữ liệu cá nhân².

Theo thời gian, các thuật ngữ dùng để chỉ những chủ thể chịu trách nhiệm cho việc xử lý dữ liệu cá nhân đã có sự phát

1. Xem Privacy International: “The Keys to Data Protection”, 2018, p.28, <https://www.internetlab.org.br/wp-content/uploads/2018/09/Data-Protection-COMLETE.pdf>, truy cập ngày 02/7/2021.

2. Xem Peter Blume: “The Data Subject”, *Tlđđ*, p.258.

triển đáng kể. Mặc dù các thuật ngữ này rất đa dạng ở những luật bảo vệ dữ liệu khác nhau, nhưng thông thường sẽ có hai chủ thể. Đó là chủ thể kiểm soát và chủ thể xử lý dữ liệu¹.

GDPR và PDPA phân biệt rõ chủ thể kiểm soát (*controller*) và chủ thể xử lý (*processor*). Đối với chủ thể kiểm soát, theo GDPR, đây là chủ thể có các nghĩa vụ được quy định, bất kể họ hoạt động có vì lợi nhuận hay không, ở quy mô nào và thuộc khu vực công hay tư, miễn là họ tự mình hoặc cùng với chủ thể khác quyết định mục đích và phương tiện của việc xử lý dữ liệu cá nhân², trừ khi việc xử lý dữ liệu hoàn toàn vì mục đích cá nhân hoặc hộ gia đình³. PDPA lại sử dụng thuật ngữ “tổ chức” (*organization*) với phạm vi về nghĩa vụ tương tự như chủ thể kiểm soát của GDPR. Chủ thể này bao gồm bất kỳ cá nhân, công ty, hiệp hội hoặc cơ quan nào của cá nhân, hợp nhất hoặc chưa hợp nhất... nhưng không bao gồm các cơ quan công quyền hoặc tổ chức nào thay mặt cho cơ quan công quyền như GDPR.

Ngoài chủ thể kiểm soát, GDPR và PDPA còn quy định nghĩa vụ cho chủ thể thực hiện việc xử lý dữ liệu cá nhân theo sự ủy quyền của chủ thể kiểm soát dữ liệu, thường được gọi là chủ thể xử lý. GDPR quy định chủ thể xử lý dữ liệu là cá nhân hoặc pháp nhân, cơ quan công quyền, cơ quan hoặc tổ chức khác xử lý dữ liệu cá nhân thay mặt cho chủ thể

1. Xem Privacy International: “The Keys to Data Protection”, 2018, p.28, <https://www.internetlab.org.br/wp-content/uploads/2018/09/Data-Protection-COMLETE.pdf>, truy cập ngày 02/7/2021.

2. Khoản 7, Điều 4 GDPR.

3. Điều 18, Phần giới thiệu của GDPR.

kiểm soát¹. Tương tự, PDPA sử dụng thuật ngữ “trung gian dữ liệu” (*data intermediary*) để chỉ chủ thể xử lý dữ liệu, tức tổ chức xử lý dữ liệu cá nhân thay mặt cho một tổ chức khác, nhưng không bao gồm nhân viên của tổ chức khác đó².

Trong khi đó, APP và APPI không phân biệt chủ thể kiểm soát dữ liệu và chủ thể xử lý dữ liệu. APP sử dụng một thuật ngữ chung, đó là “thực thể APP” (*APP entity*), bao gồm các cá nhân, hầu hết các tổ chức tư nhân và cả các cơ quan nhà nước³. Trong khi đó, APPI lại dùng thuật ngữ “chủ thể kiểm soát dữ liệu cá nhân”, tức chủ thể cung cấp cơ sở dữ liệu cá nhân, v.v. để sử dụng trong kinh doanh⁴. APPI còn quy định rằng một số cơ quan nhà nước và các tổ chức khác không nằm trong định nghĩa này.

Ở Luật an ninh thông tin mạng và Dự thảo Nghị định, chủ thể kiểm soát dữ liệu và chủ thể xử lý dữ liệu được gọi chung bằng một thuật ngữ là “bên xử lý dữ liệu cá nhân” nên khái niệm về “chủ thể kiểm soát dữ liệu” không tồn tại⁵. “Bên xử lý dữ liệu cá nhân” được định nghĩa là “cơ quan, tổ chức, cá nhân trong và ngoài nước thực hiện hoạt động xử lý dữ liệu cá nhân” (khoản 8, Điều 2, Dự thảo Nghị định). Theo tác giả,

1. Khoản 8, Điều 4 GDPR.

2. Khoản 1, Điều 2 PDPA.

3. Mục B.3, chương B Văn bản hướng dẫn Luật bảo vệ quyền riêng tư Ôxtrâyliá.

4. Khoản 5, Điều 2 APPI.

5. Xem Le Ton Viet, Russin & Vecchi: “Data Protection In Vietnam: Overview”, 2019, p.22, <https://www.amchamvietnam.com/wp-content/uploads/2019/05/Data-Protection-in-Vietnam-Overview-April-2019.pdf>, truy cập ngày 11/3/2021.

cần có sự phân biệt giữa chủ thể kiểm soát dữ liệu và chủ thể xử lý dữ liệu. Vì thực tế, hai chủ thể này sẽ tham gia vào quá trình xử lý dữ liệu với vai trò khác nhau, việc hiểu rõ bản chất của từng chủ thể là cơ sở để đặt ra các nghĩa vụ riêng và mức độ chịu trách nhiệm riêng đối với từng chủ thể. Có những trường hợp chủ thể kiểm soát sẽ quyết định mục đích xử lý dữ liệu nhưng không trực tiếp xử lý. Như vậy, với định nghĩa về “bên xử lý dữ liệu cá nhân” hiện nay của Dự thảo Nghị định, các cá nhân, cơ quan và tổ chức không tác động trực tiếp lên dữ liệu cá nhân nhưng tham gia quyết định việc xử lý dữ liệu sẽ nằm ngoài phạm vi điều chỉnh của pháp luật và không phải chịu trách nhiệm trong trường hợp có liên quan đến hành vi vi phạm.

Do vậy, việc đưa ra hai định nghĩa về chủ thể kiểm soát và chủ thể xử lý là cần thiết trong việc thực hiện các nghĩa vụ liên quan tới quá trình xử lý dữ liệu cá nhân. Cụ thể, với sự tham khảo từ GDPR và PDPA, chủ thể kiểm soát dữ liệu có thể được định nghĩa là một cá nhân hoặc pháp nhân, thuộc khu vực công hay tư, tự mình hoặc liên kết với chủ thể khác, quyết định mục đích và phương tiện của việc xử lý dữ liệu cá nhân¹. Đối với chủ thể xử lý, đặc điểm cơ bản của chủ thể này là xử lý dữ liệu theo sự ủy quyền của chủ thể kiểm soát, theo như GDPR và PDPA. Vậy nên, tác giả kiến nghị rằng, yếu tố trên nên được thêm vào định nghĩa “bên xử lý dữ liệu cá nhân” trong Dự thảo Nghị định. Dựa vào GDPR và PDPA, chủ thể xử lý dữ liệu có thể được hiểu là một cá nhân hoặc

1. Xem Privacy International: “The Keys to Data Protection”, *Tlđđ*, p.21.

pháp nhân, thuộc khu vực công hay tư, tự mình hoặc liên kết với những chủ thể khác, thực hiện việc xử lý dữ liệu cá nhân theo sự ủy quyền của chủ thể kiểm soát dữ liệu¹.

Một vấn đề quan trọng cần lưu ý khi bàn về chủ thể kiểm soát và chủ thể xử lý là phạm vi áp dụng của pháp luật bảo vệ dữ liệu đối với các chủ thể này theo không gian. Pháp luật bảo vệ dữ liệu hiện đại cần phải đặt chủ thể dữ liệu làm trung tâm của việc bảo vệ dữ liệu, nhằm bảo đảm rằng các quyền của họ luôn được bảo vệ, bất kể dữ liệu của họ được xử lý trong hay ngoài lãnh thổ nơi họ sinh sống².

Theo pháp luật các nước, hiệu lực trong lãnh thổ thường được quy định không rõ ràng, được hiểu rất hẹp và chỉ áp dụng cho các chủ thể có trụ sở tại một khu vực tài phán cụ thể. Cho nên, các công ty có xu hướng sử dụng lỗ hổng này để tránh đưa ra các biện pháp bảo vệ cho người dùng. GDPR áp dụng cho các tổ chức được thành lập ở EU, bất kể việc xử lý dữ liệu có diễn ra ở EU hay không³. Đối với APP, các thực thể APP sẽ chịu sự điều chỉnh của APP nếu chúng được thành lập ở Ôxtrâlia, như vậy yếu tố “thành lập” này khá giống với GDPR. PDPA cũng quy định tới yếu tố này vì nó áp dụng cho tất cả các tổ chức thực hiện các hoạt động liên quan đến việc thu thập, sử dụng và tiết lộ dữ liệu cá nhân ở Xingapo⁴. Tuy nhiên, APPI lại không đề cập yếu tố “thành lập” khi quy định về hiệu lực trong lãnh thổ.

1, 2. Xem Privacy International: “The Keys to Data Protection”, *Tlidd*, p.30, 34.

3. Điều 18, Phần giới thiệu của GDPR.

4. Khoản 1, Điều 2 PDPA.

Luật an toàn thông tin mạng quy định ở Điều 2 rằng “Luật này áp dụng đối với cơ quan, tổ chức, cá nhân Việt Nam, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động an toàn thông tin mạng tại Việt Nam”. Như vậy, luật này đã quy định về hiệu lực trong lãnh thổ đối với việc xử lý dữ liệu vì nó áp dụng đối với việc xử lý dữ liệu cá nhân do chủ thể xử lý đặt tại Việt Nam thực hiện. Đối với Dự thảo Nghị định, phạm vi lãnh thổ chưa được làm rõ. Vậy nên, hiệu lực theo không gian trong Dự thảo Nghị định cần được quy định theo hướng của Luật an toàn thông tin mạng nhằm bảo đảm quyền và lợi ích hợp pháp của chủ thể dữ liệu.

Với xu thế toàn cầu hóa hiện nay, việc bảo vệ dữ liệu bị giới hạn bởi ranh giới lãnh thổ quốc gia là không còn phù hợp. Các khuôn khổ bảo vệ dữ liệu đã bắt đầu đẩy mạnh theo hướng áp dụng ngoài lãnh thổ, để các cá nhân không bị tước các quyền lợi chính đáng của họ chỉ vì nơi đặt trụ sở của chủ thể kiểm soát hoặc chủ thể xử lý nằm ngoài lãnh thổ quốc gia¹. GDPR áp dụng cho các tổ chức bên ngoài EU (những tổ chức không có trụ sở ở EU) nếu họ cung cấp hàng hóa, dịch vụ hoặc giám sát hành vi của các chủ thể dữ liệu ở EU². Giống như GDPR, APP cũng có hiệu lực ngoài lãnh thổ vì nó áp dụng cho hoạt động xử lý được thực hiện trong hoặc ngoài nước Ôxtrâyliia (và các lãnh thổ bên ngoài của Ôxtrâyliia) bởi thực thể APP³. PDPA áp dụng cho các tổ chức thực hiện việc

1. Xem Privacy International: “The Keys to Data Protection”, *Tlđđ*, p.38.

2. Điều 23, Phần giới thiệu GDPR.

3. Điều 5B, Phần 1 APP.

thu thập, sử dụng và tiết lộ dữ liệu cá nhân ở Xingapo, bất kể có được hình thành hoặc công nhận theo luật của Xingapo, hoặc cư trú hoặc có văn phòng hoặc địa điểm kinh doanh tại Xingapo hay không¹. Đối với APPI, Điều 75 của luật này nêu rõ một số điều khoản có phạm vi ngoài lãnh thổ, trong đó bao gồm trường hợp xử lý ở nước ngoài đối với dữ liệu của cá nhân có quốc tịch Nhật Bản.

Như vậy, hiệu lực ngoài lãnh thổ có thể hiểu là chủ thể có hoạt động xử lý dữ liệu nằm ngoài lãnh thổ mà chủ thể dữ liệu sinh sống hoặc mang quốc tịch thì vẫn thuộc đối tượng điều chỉnh của pháp luật về bảo vệ dữ liệu cá nhân ở lãnh thổ đó. Tương tự, Luật an toàn thông tin mạng cũng áp dụng đối với chủ thể xử lý ở cả: trong và ngoài Việt Nam, nếu việc xử lý liên quan đến đối tượng dữ liệu: 1) đặt tại Việt Nam; hoặc 2) có quốc tịch Việt Nam². Tuy nhiên, trong Dự thảo Nghị định, phạm vi ngoài lãnh thổ vẫn chưa được làm rõ nên cần được bổ sung như Luật an toàn thông tin mạng quy định.

Tóm lại, Dự thảo Nghị định cần có sự phân biệt giữa chủ thể kiểm soát và chủ thể xử lý thay vì chỉ quy định chung trong một định nghĩa là “bên xử lý dữ liệu cá nhân” như hiện nay. Cụ thể, chủ thể kiểm soát có thể được định nghĩa như sau: cá nhân hoặc pháp nhân, thuộc khu vực công hay tư, tự mình hoặc liên kết với chủ thể khác, tham gia quyết định mục đích và phương tiện của việc xử lý dữ liệu cá nhân. Trong khi đó, chủ thể xử lý nên được hiểu là cá nhân hoặc

1. Khoản 1, Điều 2 PDPA.

2. Xem Le Ton Viet, Russin & Vecchi: “Data Protection In Vietnam: Overview”, *Tlđđ*.

pháp nhân, thuộc khu vực công hay tư, tự mình hoặc liên kết với những chủ thể khác, thực hiện việc xử lý dữ liệu cá nhân theo sự ủy quyền của chủ thể kiểm soát dữ liệu. Ngoài ra, phạm vi áp dụng của pháp luật bảo vệ dữ liệu đối với các chủ thể kiểm soát và chủ thể xử lý này theo không gian cần được quy định rõ trong Dự thảo Nghị định, bao gồm phạm vi trong và ngoài lãnh thổ.

*

* *

Trong thời đại kỹ thuật số, dữ liệu cá nhân của con người đối mặt với nguy cơ cao bị mất an toàn do các hành vi thu thập, xử lý hoặc sử dụng trái phép gây ra. Dữ liệu cá nhân đang bị giao dịch như một hàng hóa với giá trị lợi nhuận lớn¹. Vì thế, để bảo vệ dữ liệu cá nhân, không thể phủ nhận rằng pháp luật là công cụ hữu hiệu nhất. Dự thảo Nghị định của Việt Nam về bảo vệ dữ liệu cá nhân được kỳ vọng sẽ từng bước khắc phục tình thế mất an toàn của cơ sở dữ liệu cá nhân. Tuy nhiên, để hoàn thiện thêm, Việt Nam cần cân nhắc sửa đổi những bất cập trong dự thảo liên quan đến khái niệm chủ thể dữ liệu, chủ thể kiểm soát dữ liệu và chủ thể xử lý dữ liệu. Đặc biệt, cần có sự phân biệt rõ giữa khái niệm chủ thể kiểm soát và chủ thể xử lý dữ liệu, đồng thời quy định rõ về phạm vi áp dụng của pháp luật bảo vệ dữ liệu đối với hai chủ thể này.

1. Xem Anne de Hingh: “Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation”, *German Law Journal*, 2018, p.1271-1272.

QUY ĐỊNH CỦA PHÁP LUẬT VÀ VAI TRÒ CỦA NHÀ NƯỚC TRONG VIỆC BẢO ĐẢM THI HÀNH CÁC QUY ĐỊNH VỀ AN TOÀN, AN NINH THÔNG TIN

ThS. NGUYỄN THANH QUYÊN*

ThS. HUỖNH THỊ HỒNG NHIÊN**

Hiện nay, an ninh thông tin đã trở thành một bộ phận quan trọng của an ninh quốc gia. Tuy nhiên, do nhiều nguyên nhân chủ quan và khách quan khác nhau mà nguy cơ gây mất an ninh thông tin là mối đe dọa lớn và ngày càng gia tăng đối với an ninh quốc gia. Vì vậy, nghiên cứu về pháp luật an toàn và an ninh thông tin luôn là một yêu cầu cấp thiết hiện nay.

1. Khái quát chung về an toàn, an ninh thông tin và tình hình an ninh thông tin ở Việt Nam hiện nay

a) Khái quát về an toàn, an ninh thông tin và phân biệt với các thuật ngữ có liên quan

An ninh thông tin là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức,

*, ** Trường Đại học Luật Thành phố Hồ Chí Minh.

cá nhân¹. Như vậy, có thể phân biệt khái niệm về an ninh thông tin với các thuật ngữ có liên quan như:

- Hệ thống thông tin là tập hợp các thiết bị viễn thông, công nghệ thông tin bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

- Thông tin trên mạng là thông tin được lưu trữ, truyền đưa, thu thập và xử lý thông qua mạng.

- Thông tin tổng hợp là thông tin được tổng hợp từ nhiều nguồn thông tin, nhiều loại hình thông tin về một hoặc nhiều lĩnh vực quân sự, chính trị, kinh tế, văn hóa, xã hội.

- An toàn thông tin là sự bảo vệ thông tin và hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. An toàn thông tin bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

b) Tình hình an ninh thông tin ở Việt Nam hiện nay

Hiện nay, Nhà nước ta đã và đang chú trọng nghiên cứu, xây dựng, áp dụng đồng bộ các giải pháp để tăng cường

1. Xem khoản 13, Điều 3, Quy chế quản lý, cung cấp và sử dụng dịch vụ internet trong Quân đội nhân dân Việt Nam ban hành kèm theo Thông tư số 110/2014/TT-BQP, ngày 22/8/2014 của Bộ Quốc phòng ban hành Quy chế quản lý, cung cấp và sử dụng dịch vụ internet trong Quân đội nhân dân Việt Nam.

bảo đảm an ninh thông tin. Bên cạnh những kết quả đã đạt được, công tác bảo đảm an ninh thông tin ở Việt Nam hiện nay còn gặp nhiều khó khăn và hạn chế. Cụ thể là:

- Các thế lực phản động trong nước và nước ngoài liên tục thực hiện có tổ chức và quy mô lớn liên quan đến hoạt động tình báo, gián điệp, khủng bố, phá hoại hệ thống thông tin; tán phát thông tin xấu, độc hại nhằm tác động chính trị nội bộ, can thiệp, hướng lái chính sách, pháp luật của Việt Nam, đặc biệt là gia tăng hoạt động tấn công mạng nhằm vào hệ thống thông tin quan trọng về an ninh quốc gia.

- Tội phạm và vi phạm pháp luật trong lĩnh vực an ninh thông tin diễn biến phức tạp, gia tăng về số vụ, thủ đoạn tinh vi, gây thiệt hại nghiêm trọng về nhiều mặt với hành vi phá hoại kết cấu hạ tầng thông tin; gây mất an toàn, hoạt động bình thường, vững mạnh của mạng máy tính, mạng viễn thông, phương tiện điện tử của các cơ quan, tổ chức, cá nhân và hệ thống thông tin vô tuyến điện,...¹.

Như vậy, có thể thấy, hệ thống thông tin của Việt Nam tồn tại nhiều điểm yếu, lỗ hổng, nhiều nguy cơ đe dọa đến an ninh thông tin gây khó khăn cho công tác quản lý, kiểm soát của các cơ quan chức năng.

1. Theo kết quả đánh giá an ninh mạng do Tập đoàn công nghệ Bkav thực hiện, trong năm 2019, chỉ tính riêng thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên tới 20.892 tỷ đồng (tương đương 902 triệu USD), hơn 1,8 triệu máy tính bị mất dữ liệu do sự lan tràn của các loại mã độc mã hóa dữ liệu tống tiền (ransomware), trong đó có nhiều máy chủ chứa dữ liệu của các cơ quan, gây đình trệ hoạt động của nhiều cơ quan, doanh nghiệp. (Theo Tập đoàn Bkav: Báo cáo tổng kết công tác an ninh mạng năm 2019).

2. Quy định của pháp luật về an ninh thông tin

a) Quy định của một số quốc gia trên thế giới

Tại Hoa Kỳ:

Các đạo luật của Hoa Kỳ được ban hành nhằm quy định về vấn đề an toàn, an ninh thông tin theo hướng an toàn và chặt chẽ, cụ thể:

Luật bảo vệ quyền về sự riêng tư video: ngăn chặn việc tiết lộ sai thông tin của một cá nhân xuất phát từ việc cho thuê hoặc mua tài liệu nghe nhìn của họ¹.

Luật về sự riêng tư của người tiêu dùng của bang California (CCPA): thông qua vào tháng 6/2018 sau vụ bê bối Cambridge Analytica², dự kiến sẽ trở thành luật về quyền về sự riêng tư dữ liệu toàn diện nhất ở Hoa Kỳ.

Luật phổ biến dữ liệu Hoa Kỳ (S.142): áp đặt các yêu cầu về quyền về sự riêng tư đối với các nhà cung cấp dịch vụ internet tương tự như các yêu cầu áp đặt cho các cơ quan liên bang theo Luật về quyền về sự riêng tư năm 1974³.

Luật bảo vệ quyền về sự riêng tư và quyền lợi người tiêu dùng trên phương tiện truyền thông xã hội năm 2019 (S.189)⁴: yêu cầu các chủ thể cung cấp cho người dùng một bản sao miễn phí dưới dạng điện tử những dữ liệu cá nhân

1. Xem Global Internet Liberty Campaign: *"Privacy and human rights - An International Survey of Privacy Laws and Practice"*, 2004, <http://gilc.org/privacy/survey/intro.html>, truy cập ngày 15/8/2021.

2. Xem HG.org, *"Data Protection Law"*, <https://www.hg.org/data-protection.html>, truy cập ngày 15/8/2021.

3. Xem tại: <https://www.justice.gov/opcl/privacy-act-1974>.

4. Xem tại: <https://www.congress.gov/bill/116th-congress/senate-bill/189>.

mà nhà điều hành đã xử lý và thông báo cho người dùng trong vòng 72 giờ sau khi biết rằng dữ liệu của người dùng đã bị truyền đi mà vi phạm nền tảng bảo mật¹.

Luật đám mây của Hoa Kỳ (The Clarifying Lawful Overseas Use of Data Act - CLOUD Act) 2018²: các cơ quan tình báo Hoa Kỳ có quyền truy cập vào dữ liệu được lưu trữ bởi các công ty Hoa Kỳ trong một số trường hợp nhất định dù nơi đặt máy chủ chứa dữ liệu ở đâu. Quy định này đã dấy lên mối lo ngại của EU khi Hoa Kỳ ngày càng giành quyền kiểm soát tất cả các thiết bị trong thương mại điện tử³.

Luật tăng cường an ninh mạng và bảo vệ dữ liệu người tiêu dùng năm 2006 quy định: Cấm truy cập hoặc điều khiển từ xa một máy tính được bảo vệ mà không được phép lấy thông tin; mở rộng phạm vi “máy tính được bảo vệ”; mở rộng định nghĩa về “lừa đảo”, bao gồm lừa đảo trên môi trường máy tính; xác định tội tống tiền, đe dọa quyền truy cập mà không được phép (hoặc vượt quá quyền truy cập được phép) của dữ liệu lưu trữ; áp dụng hình phạt hình sự

1. Xem Hoàng Thị Ngọc Lan: “Những thành tựu cơ bản của các cuộc cách mạng công nghiệp trong lịch sử thế giới”, 2019, <http://vtec.edu.vn>, truy cập ngày 14/8/2021.

2. Xem H.R.4943 - CLOUD Act, 115th Congress (2017 - 2018), <https://www.congress.gov/bills/115/congressional-legislation/4943/text>, truy cập ngày 15/8/2021.

3. Xem tại: <https://bnews.vn/sieu-quyen-luc-ve-dien-toan-dam-may-cua-my-khien-eu-lo-lang/165378.html>. Lý giải cho sự việc trên là bởi: Các thể nhân lớn ở EU như Deutsche Bank, Lufthansa, Orange, Renault, Volkswagen hay cả Bộ Y tế Pháp đều sử dụng các nền tảng cung cấp điện toán đám mây đến từ Hoa Kỳ như Google Cloud, Amazon Web Services hay Microsoft.

đối với âm mưu lừa đảo trên môi trường máy tính; phạt tiền hoặc phạt tù nếu không thông báo cho cơ quan mật vụ Hoa Kỳ hoặc Cục Điều tra liên bang (FBI) về một vi phạm an ninh lớn trong hệ thống máy tính, với mục đích cản trở cuộc điều tra về vi phạm đó, nếu vi phạm đó gây ra nguy cơ đánh cắp thông tin đáng kể¹.

Luật bảo vệ quyền về sự riêng tư trực tuyến của trẻ em (COPPA)²: cung cấp cho phụ huynh quyền kiểm soát đối với những thông tin mà các trang web có thể thu thập từ con cái họ.

Luật về trách nhiệm giải trình và trách nhiệm bảo hiểm y tế (HIPPA)³: bảo đảm tính bảo mật của bệnh nhân đối với tất cả các dữ liệu liên quan đến chăm sóc sức khỏe.

Ngoài ra, còn có các văn bản pháp luật khác điều chỉnh từng lĩnh vực cụ thể liên quan đến an toàn, an ninh thông tin như: Luật quyền riêng tư và quyền giáo dục gia đình (The Family Education Rights and Privacy Act - FERPA); Luật Gramm-Leach Bliley (The Gramm Leach Bliley Act - GLBA); Luật trách nhiệm giải trình và cung cấp bảo hiểm y tế (The Health Insurance Portability and Accountability Act - HIPAA)⁴; Luật về quyền riêng tư của truyền thông điện tử

1. Xem tại: <https://www.congress.gov/bill/109th-congress/house-bill/5318/summary/00>, truy cập ngày 10/8/2021.

2. Xem tại: <https://www.ftc.gov/tips-advice>.

3. Xem tại: <https://www.cdc.gov/phlp/publications/topic/hipaa.html>.

4. HoganLovells: *Cloud Computing: A Primer on Legal Issues, Including Privacy and DataSecurity Concerns*, 2010, http://www.cisco.com/web/about/doing_business/legal/privacy_compliance/docs/CloudPrimer.pdf, truy cập ngày 15/8/2021.

(The Electronic Communications Privacy Act - ECPA)¹, Luật truyền thông được lưu trữ (The Stored Communications Act - SCA)², Luật yêu nước³, Nguyên tắc thực hành thông tin công bằng (Fair Information Practice Principles - FIPPs) của Ủy ban Thương mại liên bang Hoa Kỳ (Federal Trade Commission - FTC)⁴; Luật tự do thông tin (FOIA); Quy tắc thực hành thông tin công bằng của FTC⁵; Tiêu chuẩn bảo mật thẻ thanh toán (PCIDSS), Luật Sarbanes-Oxley; Quy định của NARA (Mục 36 của Bộ luật quy định liên bang) và Thực hành thông tin công bằng của FTC⁶...

Có thể nhận thấy rằng, Hoa Kỳ có những động thái tích cực, phong phú và hiệu quả về mặt lập pháp để bảo đảm an toàn, an ninh thông tin.

1. Đạo luật đưa ra các biện pháp bảo vệ người tiêu dùng chống lại quyền truy cập của chính phủ vào thư điện toán và các dữ liệu điện toán khác do các bên (chẳng hạn như nhà cung cấp dịch vụ internet) nắm giữ.

2. Đạo luật này đề cập việc tiết lộ thông tin tự nguyện và bắt buộc liên quan đến hồ sơ giao dịch và truyền thông điện tử được lưu trữ do các nhà cung cấp dịch vụ internet hoặc bên thứ ba nắm giữ.

3. Đạo luật ban hành vào năm 2001 và được sửa đổi vào năm 2005, bao gồm các điều khoản cho phép FBI truy cập vào hồ sơ kinh doanh bằng cách buộc các nhà cung cấp đám mây cung cấp hồ sơ.

4. Các nguyên tắc này đề cập việc thu thập, sử dụng thông tin cá nhân, chất lượng dữ liệu, bảo mật, tính minh bạch, làm cơ sở cho nhiều khuyến nghị về quyền riêng tư mà các cơ quan liên bang đưa ra.

5, 6. Xem Jansen W., Grance.T: *Guidelines on security and privacy in public cloud computing*, NIST Special Publication 800-144, December 2011, <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>, truy cập ngày 15/8/2021.

Tại Trung Quốc:

Ở quốc gia này, vấn đề an toàn, an ninh thông tin được ghi nhận ở các văn bản sau:

Luật thương mại điện tử năm 2019¹: cho phép Chính phủ yêu cầu các nhà khai thác thương mại điện tử cung cấp dữ liệu thương mại điện tử, bao gồm thông tin cá nhân, quyền riêng tư và bí mật kinh doanh và các nhà khai thác thương mại điện tử không thể từ chối yêu cầu cung cấp thông tin của Chính phủ². Trên thực tế, Chính phủ Trung Quốc vẫn là cơ quan kiểm soát tối cao vì họ kiểm soát các kết nối internet giữa lãnh thổ của mình và thế giới bên ngoài³, bằng việc sử dụng một phần mềm riêng WeChat⁴.

Luật an ninh mạng Trung Quốc năm 2017⁵ quy định: các nhà cung cấp sản phẩm và dịch vụ mạng thu thập thông tin người dùng có nghĩa vụ thông báo cho người dùng và phải nhận được sự đồng ý của họ. Theo quy định của luật, thông tin cá nhân và các dữ liệu quan trọng được các nhà khai thác thông tin thu thập phải được lưu trữ trong nước; nghĩa là,

1. Xem tại: <https://npcobserver.com/legislation/e-commerce-law/>.

2. Điều 25, Luật thương mại điện tử Trung Quốc năm 2019.

3. Xem Samuel Woodhams: “*The Rise of Internet Sovereignty and the End of the World Wide Web?*”, Globe Post (Apr. 23, 2019), <https://theglobepost.com/2019/04/23/internet-sovereignty/>, truy cập ngày 15/8/2021.

4. Xem WeChat Shares Consumer Data With Chinese Government, PYMNTS (September 25, 2017), <https://www.pymnts.com/safety-and-security/2017/wechat-hands-over-user-data-to-chinese-government-amid-privacy-concerns/>.

5. Xem tại: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>.

các công ty nước ngoài muốn khai thác thông tin phải lắp đặt máy chủ tại Trung Quốc. Tuy nhiên, luật cũng quy định một trường hợp ngoại lệ là thông tin có thể được cung cấp nếu sau khi xử lý không có cách nào để xác định danh tính một cá nhân cụ thể (nghĩa là không thể nhận được “sự đồng ý” từ phía người dùng)¹.

Luật bảo mật dữ liệu mới sẽ bắt đầu có hiệu lực từ ngày 01/9/2021. Khi đó, tất cả các quyết định liên quan đến bảo mật dữ liệu đều phải thông qua các cơ quan chính phủ. Những công ty vi phạm có thể bị phạt nặng, bị thu hồi giấy phép hoạt động hoặc thậm chí bị buộc phải ngừng kinh doanh vĩnh viễn². Theo đó, có bốn điểm cần lưu ý về Luật bảo mật dữ liệu mới của Trung Quốc là: (1) “*Dữ liệu quan trọng*” được chính quyền trung ương xác định; (2) Chính quyền trung ương và địa phương sẽ giám sát “*dữ liệu cốt lõi*”; (3) Có cơ chế cho luồng dữ liệu, nhưng vẫn chưa thực sự rõ ràng; (4) Đây là bước đầu tiên trong việc xác định dữ liệu “*nhạy cảm*” và “*không nhạy cảm*”³.

Một dự thảo luật mới liên quan đến bảo vệ thông tin cá nhân trên các nền tảng internet lớn, đang được đệ trình lên cơ quan lập pháp hàng đầu của Trung Quốc. Luật có thể sẽ có hiệu lực vào năm 2021, được áp dụng cho tất cả công ty và

1. Điều 42, Luật an ninh mạng Trung Quốc năm 2017.

2. Xem Nguyệt Thu: “Luật bảo mật dữ liệu mới của Trung Quốc áp chế quyền lực tuyệt đối của chính phủ đối với những tập đoàn công nghệ lớn”, <http://www.antoanthongtin.vn>, truy cập ngày 15/8/2021.

3. Xem Brady Ng: “4 things you should know about China’s new data security law”, <https://kr-asia.com/4-things-you-should-know-about-chinas-new-data-security-law>, truy cập ngày 15/8/2021.

tổ chức hoạt động tại Trung Quốc, cũng như bất kỳ doanh nghiệp nước ngoài nào xử lý dữ liệu của công dân Trung Quốc tại nước này¹.

Nhìn chung, Trung Quốc đã và đang hoàn thiện hệ thống pháp luật để bảo đảm an toàn, an ninh thông tin.

b) Quy định của pháp luật Việt Nam về an ninh thông tin

Hiện nay chưa có văn bản luật về quy định an toàn, an ninh thông tin nhưng có thể kể đến một vài văn bản dưới luật do các chủ thể có thẩm quyền ban hành quy định về vấn đề này như sau:

(1) Quyết định số 1671/QĐ-BTTTT, ngày 10/10/2019 của Bộ Thông tin và Truyền thông quy định về Thành lập và quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam trực thuộc Cục An toàn thông tin.

(2) Thông tư số 13/2018/TT-BTTTT, ngày 15/10/2018 của Bộ Thông tin và Truyền thông quy định về 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.

(3) Quyết định số 1616/QĐ-BTTTT, ngày 05/10/2018 của Bộ Thông tin và Truyền thông quy định về Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin.

1. Xem Karry Lai: “Primer: China’s draft Personal Information Protection Law”, <https://www.iflr.com/article/b1sx4yq13xr3g0/primer-chinas-draft-personal-information-protection-law>, truy cập ngày 15/8/2021.

(4) Quyết định số 469/QĐ-BTTTT, ngày 03/4/2018 của Bộ Thông tin và Truyền thông về Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Chi nhánh Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam tại thành phố Đà Nẵng.

(5) Quyết định số 468/QĐ-BTTTT, ngày 03/4/2018 của Bộ Thông tin và Truyền thông quy định về Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Chi nhánh Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam tại Thành phố Hồ Chí Minh.

(6) Thông tư số 20/2017/TT-BTTTT, ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

(7) Quyết định số 632/QĐ-TTg, ngày 10/5/2017 của Thủ tướng Chính phủ quy định về 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.

(8) Nghị định số 85/2016/NĐ-CP, ngày 01/7/2016 của Chính phủ quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ.

(9) Quyết định số 99/QĐ-TTg, ngày 14/01/2014 của Thủ tướng Chính phủ quy định về Phê duyệt Đề án “Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020”.

Đại dịch Covid-19 đã ảnh hưởng đến các quy định của pháp luật về bảo đảm an toàn, an ninh thông tin và vai trò của Nhà nước trong việc bảo đảm thi hành các quy định này.

Tình hình an toàn, an ninh thông tin ở Việt Nam đã và đang có những diễn biến phức tạp do ảnh hưởng bởi đại dịch

Covid-19. Các thế lực thù địch, phản động tăng cường hoạt động tình báo, gián điệp, khủng bố, phá hoại hệ thống thông tin; tán phát thông tin xấu, độc hại nhằm tác động chính trị nội bộ, can thiệp, hướng lái chính sách, pháp luật của Việt Nam. Hoạt động tấn công mạng gia tăng mạnh nhằm vào hệ thống thông tin quan trọng của quốc gia, hệ thống thông tin quan trọng về an ninh quốc gia. Theo thống kê, trung bình mỗi năm, qua kiểm tra, kiểm soát, các cơ quan chức năng đã phát hiện trên 850.000 tài liệu chiến tranh tâm lý, phản động, ân xá quốc tế, tài liệu tuyên truyền tà đạo trái phép; gần 750.000 tài liệu tuyên truyền chống Đảng, Nhà nước được tán phát vào Việt Nam qua đường bưu chính. Từ năm 2010 đến năm 2019 đã có 53.744 lượt cổng thông tin, trang tin điện tử có tên miền “.vn” bị tấn công, trong đó có 2.393 lượt cổng thông tin, trang tin điện tử của các cơ quan Đảng, Nhà nước có tên miền “.gov.vn”, xuất hiện nhiều cuộc tấn công mang màu sắc chính trị, gây ra những hậu quả nghiêm trọng¹.

Bên cạnh đó, trong bối cảnh đại dịch Covid-19, tội phạm và vi phạm pháp luật trong lĩnh vực thông tin diễn biến phức tạp, gia tăng về số vụ, thủ đoạn tinh vi, gây thiệt hại nghiêm trọng về nhiều mặt. Các hành vi phá hoại kết cấu hạ tầng thông tin; gây mất an toàn, hoạt động bình thường, vũing mạnh của mạng máy tính, mạng viễn thông, phương tiện điện tử của các cơ quan, tổ chức, cá nhân và hệ thống thông tin

1. Xem Lê Văn Thắng: *An ninh thông tin của Việt Nam trong điều kiện hiện nay: Thực trạng, vấn đề đặt ra và giải pháp*, Đề tài khoa học cấp Nhà nước, Hà Nội, 2019.

vô tuyến điện,... đã và đang gây ra những thiệt hại lớn về kinh tế, xâm hại trực tiếp đến quyền, lợi ích hợp pháp của các cơ quan, tổ chức và cá nhân. Năm 2020, thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã đạt kỷ lục mới, vượt mốc 1 tỷ USD (23,9 nghìn tỷ đồng). Đây là kết quả được đưa ra từ chương trình đánh giá an ninh mạng do Tập đoàn công nghệ Bkav thực hiện tháng 12/2020¹.

Hệ thống thông tin của Việt Nam tồn tại nhiều điểm yếu, lỗ hổng bảo mật dễ bị khai thác, tấn công, xâm nhập; tình trạng lộ, mất bí mật nhà nước qua hệ thống thông tin gia tăng đột biến; hiện tượng khai thác, sử dụng trái phép cơ sở dữ liệu, tài nguyên thông tin quốc gia, dữ liệu cá nhân người dùng diễn biến phức tạp; xuất hiện nhiều dịch vụ mới, hiện đại gây khó khăn cho công tác quản lý, kiểm soát của các cơ quan chức năng. Khi đại dịch Covid-19 bùng phát, hàng loạt doanh nghiệp, cơ quan, tổ chức chuyển sang làm việc từ xa. Các phần mềm làm việc trực tuyến được tìm kiếm và download rầm rộ. Nhiều đơn vị buộc phải mở hệ thống trên internet để nhân viên có thể truy cập và làm việc từ xa... Điều này tạo môi trường cho kẻ xấu khai thác lỗ hổng, tấn công, đánh cắp thông tin. Theo quan sát của Bkav, tại Việt Nam, nhiều trang thương mại điện tử lớn, một số nền tảng giao hàng trực tuyến có nhiều người sử dụng, đã bị xâm nhập và đánh cắp dữ liệu².

Các thế lực thù địch triệt để sử dụng hệ thống thông tin để tác động, can thiệp nội bộ, hướng lái chính sách, thao túng

1, 2. Xem Tập đoàn Bkav: *Báo cáo tổng kết công tác an ninh mạng năm 2020*.

dư luận; xâm phạm độc lập, chủ quyền quốc gia trên không gian mạng, tiến hành chiến tranh thông tin đối với Việt Nam. Các tổ chức phản động lưu vong, khủng bố tăng cường hoạt động tấn công, phá hoại hệ thống thông tin quan trọng về an ninh quốc gia; sử dụng không gian mạng để tán phát thông tin xấu, độc hại, kích động biểu tình, bạo loạn; hình thành các hội, nhóm, các tổ chức chính trị đối lập,... Các tổ chức tin tặc, tổ chức tội phạm thực hiện các cuộc tấn công mạng tự phát, đơn lẻ hoặc có chủ đích nhằm vào hệ thống thông tin trọng yếu quốc gia, làm tê liệt, gây gián đoạn hoạt động lãnh đạo, chỉ đạo, điều hành, quản lý kinh tế - xã hội của các cơ quan Đảng, Nhà nước¹.

Để bảo đảm thi hành các quy định của pháp luật về bảo đảm an toàn, an ninh thông tin, Nhà nước đóng vai trò rất quan trọng:

Một là, nâng cao nhận thức về an toàn, an ninh thông tin và bảo đảm an toàn, an ninh thông tin. Bảo đảm an toàn, an ninh thông tin là nhiệm vụ trọng yếu, thường xuyên của toàn Đảng, toàn dân, của cả hệ thống chính trị, trong đó lực lượng Công an nhân dân là nòng cốt. Để bảo đảm an toàn, an ninh thông tin cần coi trọng và sử dụng đồng bộ các biện pháp chính trị, pháp luật, khoa học kỹ thuật, tuyên truyền - giáo dục, tổ chức - hành chính, kinh tế, ngoại giao và nghiệp vụ chuyên môn. Chú trọng tuyên truyền, phổ biến cho mọi người dân về các nguy cơ, các yếu tố gây mất an ninh, đe dọa gây

1. Xem Tân Long: “Cảnh giác, phòng, chống âm mưu lợi dụng hợp tác quốc tế về xây dựng pháp luật để chống phá Việt Nam”, <http://tapchiquptd.vn>, truy cập ngày 13/8/2021.

mất an ninh thông tin. Nâng cao bản lĩnh chính trị, khả năng nhận biết, tiếp nhận thông tin, khả năng tự vệ, “miễn dịch” trước những thông tin giả, thông tin xấu, độc hại¹. Có kế hoạch đưa nội dung về nhận diện các nguy cơ, yếu tố gây mất an toàn, an ninh thông tin và trách nhiệm bảo đảm an toàn, an ninh thông tin vào hệ thống giáo dục quốc dân, qua đó giáo dục ý thức, trách nhiệm, nâng cao nhận thức cho toàn dân về vấn đề này.

Hai là, nghiên cứu xác lập, bảo đảm giữ vững độc lập, tự chủ, chủ quyền và lợi ích quốc gia trên không gian thông tin quốc tế; bảo vệ và khai thác có hiệu quả tài nguyên thông tin quốc gia. Tiếp thu có chọn lọc kinh nghiệm quốc tế, tập trung nghiên cứu, xác lập không gian mạng quốc gia: (1) Phát triển công nghệ phần cứng; (2) Phát triển công nghệ phần mềm; (3) Phát triển công nghệ bảo mật riêng và hệ thống kiểm tra, giám sát an toàn, an ninh thông tin; (4) Xây dựng hệ cơ sở dữ liệu quốc gia tích hợp, liên thông, an toàn; (5) Xây dựng hệ thống tuyên truyền, định hướng thông tin hiện đại, an toàn và có trách nhiệm; (6) Xây dựng, hoàn thiện thể chế, chính sách, pháp luật. Điều này một mặt vừa khẳng định vị thế quốc gia, bảo đảm độc lập, tự chủ, chủ quyền quốc gia trên không gian mạng, từng bước hạn chế sự lệ thuộc vào công nghệ của nước ngoài, nâng cao khả năng bảo mật và khả năng tự chủ trong bảo đảm

1. Xem Nguyễn Ngọc Thiện: “Tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021 - 2025 trên địa bàn tỉnh Thái Nguyên”, <http://thanhtra.thainguyen.gov.vn/tin-hoat-dong/>, truy cập ngày 13/8/2021.

an ninh thông tin, bảo đảm lợi ích kinh tế quốc gia, tạo thuận lợi cho việc bảo tồn, phát huy giá trị văn hóa dân tộc, chủ động trong việc tiếp nhận thông tin và tạo thuận lợi trong thông tin, tuyên truyền của Đảng, Nhà nước, ngăn chặn có hiệu quả các thông tin xấu, độc hại, gia tăng khả năng bảo đảm bí mật thông tin cá nhân người dùng. Đồng thời, cần có kế hoạch hợp lý khai thác và bảo vệ tài nguyên thông tin quốc gia phục vụ phát triển kinh tế - xã hội, bảo đảm quốc phòng - an ninh¹.

Ba là, tăng cường sự lãnh đạo, chỉ đạo của Đảng, nâng cao hiệu lực, hiệu quả quản lý nhà nước về an toàn, an ninh thông tin. Tập trung xây dựng, hoàn thiện chính sách, pháp luật về bảo đảm an toàn, an ninh thông tin, tạo môi trường pháp lý để bảo đảm sự an toàn, tin cậy cho nền kinh tế số, cho việc chia sẻ dữ liệu số, cho quản lý hoạt động của các doanh nghiệp cung cấp dịch vụ thông tin qua biên giới vào Việt Nam. Tiếp tục nghiên cứu xây dựng luật về chống thông tin giả, thông tin xấu, độc hại; luật bảo vệ thông tin cá nhân. Có cơ chế công khai giám sát, chặn lọc thông tin xuyên tạc, sai sự thật trên không gian mạng; quy định cụ thể và thực hiện nghiêm túc quy định bắt buộc sử dụng thông tin thật khi đăng ký tài khoản trên mạng². Xây dựng bộ quy tắc ứng xử trên không gian mạng; quy định về

1. Xem Đại tướng, GS.TS. Tô Lâm: “Bảo vệ an ninh quốc gia trong tình hình mới”, <https://nhandan.vn/>, truy cập ngày 14/8/2021.

2. Xem PGS.TS. Dương Trung Ý: “Đổi mới mạnh mẽ phương thức lãnh đạo của Đảng đối với Nhà nước trong điều kiện mới”, <https://www.tapchiconsan.org.vn>, truy cập ngày 15/8/2021.

bảo vệ, kiểm tra, sử dụng tài nguyên thông tin quốc gia, dữ liệu cá nhân người dùng.

Bốn là, nâng cao năng lực phòng thủ, phục hồi, đấu tranh có hiệu quả với các hoạt động xâm phạm an toàn, an ninh thông tin. Thường xuyên rà soát, phát hiện, khắc phục lỗ hổng bảo mật trên toàn hệ thống, bổ sung thiết bị, phần mềm chuyên dụng có khả năng kiểm tra, kiểm soát an ninh, an toàn thông tin trên môi trường mạng viễn thông, internet, tần số vô tuyến điện,... Xây dựng, triển khai thực hiện các giải pháp kỹ thuật chuyên biệt nhằm kiểm tra, phát hiện các nguy cơ gây mất an ninh thông tin. Tổ chức diễn tập hằng năm về phòng, chống tấn công mạng cấp quốc gia với sự tham gia của cơ quan chính phủ, các tập đoàn kinh tế trọng yếu, các doanh nghiệp cung cấp dịch vụ viễn thông, internet và các cơ quan, tổ chức có liên quan, bảo đảm xử lý kịp thời các nguy cơ gây mất an ninh, đe dọa gây mất an ninh thông tin ở Việt Nam. Chú trọng dự báo, triển khai các giải pháp đấu tranh vô hiệu hóa hoạt động xâm hại an toàn, an ninh thông tin của các đối tượng, nhất là hoạt động tấn công làm tê liệt hệ thống thông tin trọng yếu quốc gia¹.

Năm là, tập trung nguồn lực để phát triển nền công nghiệp công nghệ thông tin, đặc biệt là công nghiệp an toàn, an ninh thông tin. Nhà nước cần có cơ chế đặc biệt, triển khai ngay các giải pháp đi tắt, đón đầu để từng bước làm chủ và xuất khẩu công nghệ thông tin. Khuyến khích nghiên cứu,

1. Xem Thiếu tướng, PGS.TS. Lê Văn Thắng: “An ninh thông tin ở Việt Nam trong điều kiện hiện nay - Vấn đề đặt ra và giải pháp”, <https://tuyengiao.vn>, truy cập ngày 15/8/2021.

phát triển, sử dụng các phần mềm, dịch vụ thông tin riêng của Việt Nam, đáp ứng yêu cầu bảo mật thông tin, sự an toàn của bí mật nhà nước, giám sát an ninh mạng¹. Thành lập các quỹ đầu tư cho nghiên cứu, phát triển các giải pháp bảo đảm an toàn, an ninh thông tin. Thủ tướng Chính phủ đã phê duyệt Đề án “Tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021 - 2025”. Mục tiêu đến năm 2025 là 100% các bộ, ngành, địa phương xây dựng và triển khai kế hoạch tuyên truyền, phổ biến về thói quen, trách nhiệm và kỹ năng cơ bản bảo đảm an toàn thông tin khi ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, chính phủ điện tử, chính quyền điện tử, đô thị thông minh cho cán bộ, công chức, viên chức, người lao động².

Trong giai đoạn đại dịch Covid-19 diễn biến phức tạp và thời đại cách mạng công nghiệp phát triển nhanh chóng, vấn đề an toàn, an ninh thông tin ngày càng trở thành một nội dung quan trọng. Nghiên cứu về an toàn, an ninh thông tin và pháp luật về bảo đảm an toàn, an ninh thông tin luôn là một yêu cầu bức thiết hiện nay.

1. Xem PGS.TS. Vũ Văn Phúc: “Cách mạng khoa học - công nghệ hiện đại và nền kinh tế tri thức”, <https://www.tapchicongsan.org.vn>, truy cập ngày 15/8/2021.

2. Xem “Nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin”, <http://antoanthongtin.gov.vn>, truy cập ngày 15/8/2021.

QUY ĐỊNH CỦA PHÁP LUẬT VIỆT NAM VỀ AN NINH MẠNG - SO SÁNH VỚI PHÁP LUẬT CỦA MỘT SỐ QUỐC GIA TRÊN THẾ GIỚI

ThS. NGUYỄN TRUNG DƯƠNG*

Trong bối cảnh các cuộc tấn công qua môi trường mạng ngày càng trở nên phổ biến và có ảnh hưởng không nhỏ đến hoạt động của Nhà nước, của các tổ chức, cá nhân trong xã hội, ngày 12/6/2018, Luật an ninh mạng của Việt Nam đã được Quốc hội khóa XIV thông qua tại Kỳ họp thứ 5. Theo đó, luật này quy định những nội dung cơ bản về bảo vệ an ninh mạng đối với hệ thống thông tin an ninh quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; triển khai hoạt động bảo vệ an ninh mạng và quy định trách nhiệm của cơ quan, tổ chức, cá nhân. Luật an ninh mạng được ban hành đã bảo đảm tính thống nhất với hệ thống pháp luật Việt Nam, phù hợp với thông lệ quốc tế và góp phần tích cực nâng cao hiệu quả công tác bảo vệ an ninh mạng, góp phần tạo nên một không gian mạng có tính an toàn, lành mạnh hơn.

* Trường Đại học Luật Thành phố Hồ Chí Minh.

1. Thực trạng vấn đề an ninh mạng tại Việt Nam

Sự phát triển của không gian mạng cùng với Cách mạng công nghiệp lần thứ tư đã và đang mang lại những lợi ích vô cùng to lớn trong phát triển kinh tế - xã hội, cũng như làm thay đổi nhận thức, hành vi và lối sống của con người. Song, bên cạnh những lợi ích mang lại, không gian mạng cũng đặt ra nhiều nguy cơ, thách thức, tác động trực tiếp đến chủ quyền, an ninh quốc gia và trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của các tổ chức, cá nhân. Các cuộc tấn công mạng với động cơ chính trị vào hệ thống thông tin trọng yếu của các nước ngày càng gia tăng, gây thiệt hại nghiêm trọng về kinh tế, quốc phòng và an ninh. Tội phạm mạng ngày càng nguy hiểm với nhiều thủ đoạn tinh vi, kỹ thuật cao, sử dụng các loại mã độc ứng dụng trí tuệ nhân tạo để tấn công, xâm nhập. Không gian mạng đang trở thành môi trường thuận lợi để các cơ quan đặc biệt nước ngoài, cá nhân, tổ chức khủng bố liên lạc, tuyển mộ lực lượng, gây quỹ, truyền bá tư tưởng chống đối cực đoan, kích động sự hận thù và bạo lực.

Việt Nam nằm trong nhóm các quốc gia có tốc độ phát triển internet nhanh nhất thế giới, không gian mạng ở nước ta cũng xuất hiện nhiều nguy cơ, thách thức lớn tác động đến an ninh quốc gia và trật tự, an toàn xã hội, cụ thể là¹:

- Các thế lực thù địch, phản động tăng cường sử dụng không gian mạng để phá hoại tư tưởng, phá hoại nội bộ, thực hiện âm mưu “diễn biến hòa bình”, gây mâu thuẫn dân tộc,

1. Xem “Hoàn thiện pháp luật về an ninh mạng trong tình hình hiện nay”, <https://www.tapchicongsan.org.vn>, truy cập ngày 05/8/2021.

kích động biểu tình, bạo loạn nhằm chuyển hóa thể chế chính trị tại Việt Nam.

- Nạn tin giả, thông tin sai sự thật, tin xấu, độc, làm tổn hại đến quyền và lợi ích hợp pháp của các tổ chức, cá nhân đang diễn ra nghiêm trọng.

- Hệ thống mạng của nước ta nằm trong nhóm các quốc gia phải đối mặt với hoạt động tấn công mạng quy mô lớn, cường độ cao, tính chất nghiêm trọng và ngày càng nguy hiểm. Nước ta đứng thứ 20 trong số các nước trên thế giới có hệ thống mạng bị tấn công bởi phần mềm độc hại, đứng thứ 8 trong số 10 quốc gia hàng đầu thế giới về tình trạng lây nhiễm mã độc cục bộ. Từ cuối năm 2015 đến nay, đã có 12.360 trang tin, cổng thông tin điện tử tên miền quốc gia (.vn) của Việt Nam bị tin tặc tấn công, thay đổi giao diện, trong đó có trên 400 trang tin, cổng thông tin điện tử của cơ quan nhà nước; có 9.763 trang tin bị tấn công bởi tin tặc nước ngoài và 2.597 trang tin bị tấn công bởi các đối tượng, nhóm tin tặc trong nước (chiếm 21%).

- Tình hình chiếm đoạt thông tin, làm lộ bí mật nhà nước, lộ thông tin cá nhân của người dùng internet diễn ra một cách đáng lo ngại.

- Hoạt động tội phạm sử dụng công nghệ cao gia tăng về số vụ, thủ đoạn tinh vi, gây thiệt hại nghiêm trọng về nhiều mặt và hệ lụy lâu dài cho xã hội, trong đó có các hoạt động tội phạm, như lừa đảo, tổ chức đánh bạc trực tuyến.

- Công tác quản lý nhà nước về không gian mạng đối mặt với nhiều thách thức trước những dịch vụ mới trên mạng, như thanh toán trực tuyến, thương mại điện tử, trò chơi trực tuyến, kinh doanh tiền ảo, kinh doanh đa cấp. Đồng thời, đặt ra một số vấn đề về an ninh quốc gia, nguy cơ mất an ninh thanh toán,

an ninh thông tin mạng, như nguy cơ mất an ninh thông tin mạng tạo điều kiện cho các thế lực thù địch tiến hành thu thập tin tức tình báo; nguy cơ thất thu thuế, mất chủ quyền không gian thanh toán; tình trạng cạnh tranh không bình đẳng giữa các doanh nghiệp hoạt động trong lĩnh vực thanh toán, trung gian thanh toán trong và ngoài nước tạo môi trường lý tưởng cho tội phạm sử dụng công nghệ cao hoạt động phạm tội, xâm phạm trật tự quản lý kinh tế, trật tự xã hội.

- Công tác đào tạo chuyên gia an ninh mạng còn hạn chế, chưa đáp ứng yêu cầu thực tiễn đặt ra.

Thực tế cho thấy, các cuộc tấn công và các hoạt động phi pháp của giới tội phạm mạng trong thời gian qua ngày càng gia tăng và có chiều hướng tinh vi hơn. Do đó, việc chống lại các cuộc tấn công mạng thực sự là một cuộc chiến gay go, phức tạp và sẽ kéo dài. Theo báo cáo an ninh website trong 9 tháng đầu năm 2020 của CyStack¹, số cuộc tấn công vào các trang mạng tại Việt Nam là 3.041 vụ, xếp thứ 18 trong số các quốc gia được khảo sát². Trong số này có nhiều website là trang chủ, cổng thông tin điện tử của các cơ quan, tổ chức nhà nước. Có thể dẫn ra một số sự vụ đáng chú ý như: năm 2016, tin tặc tấn công Hãng hàng không quốc gia Vietnam Airlines; năm 2018 tấn công website của Ngân hàng Thương mại cổ phần Ngoại thương Việt Nam (Vietcombank)...

Gần đây, theo thông tin từ Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an), một

1. Công ty chuyên về lĩnh vực an ninh mạng. Tham khảo thêm tại địa chỉ <https://cystack.net/vi>, truy cập ngày 05/8/2021.

2. Cystack: *Báo cáo An ninh website 9 tháng đầu năm 2020*, <https://resources.cystack.net/report>, truy cập ngày 05/8/2021.

ngân hàng đã bị tin tặc tấn công gây tổn thất lên đến 44 tỷ đồng. Cũng theo thống kê trên trang zone-h.org¹, nhiều website tên miền của Việt Nam vẫn đang bị nhóm Cuộc cách mạng của người Maroc (Moroccan Revolution) chiếm quyền kiểm soát. Thông tin trên cũng được chính Trung tâm Giám sát an toàn không gian mạng quốc gia (Cục An toàn thông tin, Bộ Thông tin và Truyền thông) xác nhận khi đơn vị này cho biết: Từ đầu năm 2021 đã có 163 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam².

Do vậy, việc xây dựng, hoàn thiện hệ thống pháp luật về an ninh mạng là yêu cầu hết sức cấp thiết. Đây là cơ sở pháp lý quan trọng trong phòng ngừa, đấu tranh, xử lý các hoạt động vi phạm pháp luật trên không gian mạng, bảo vệ quyền và lợi ích hợp pháp của các tổ chức, cá nhân; tạo hành lang pháp lý để nâng cao năng lực bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia, góp phần bảo đảm chủ quyền, an ninh, trật tự và xây dựng môi trường an toàn, lành mạnh trên không gian mạng.

2. Nội dung quy định của pháp luật Việt Nam về an ninh mạng

a) An ninh mạng và một số khái niệm có liên quan

An ninh mạng:

Theo quy định của Luật an ninh mạng năm 2018 thì “an ninh mạng” được hiểu là sự bảo đảm hoạt động trên không

1. Trang web mà các tin tặc thường chia sẻ thông tin. Tham khảo thêm tại địa chỉ <https://zone-h.org>, truy cập ngày 05/8/2021.

2. Xem “Bảo đảm an toàn thông tin trước yêu cầu chuyển đổi số”, <https://nhandan.vn/>, truy cập ngày 05/8/2021.

gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân¹. Tương tự như vậy, định nghĩa này cũng được ghi nhận tại khoản 24, Điều 3, Nghị định số 72/2013/NĐ-CP, ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng. Với định nghĩa trên, chúng ta cần làm rõ một số nội dung như sau:

Một là, an ninh mạng trong trường hợp này không chỉ được đề cập trong các vấn đề có liên quan tới quốc gia, dân tộc hay trật tự, an toàn xã hội mà quyền và lợi ích hợp pháp khác của các tổ chức, cá nhân trong nền kinh tế cũng được pháp luật ghi nhận và bảo vệ. Điều này là hợp lý, bởi lẽ, bên cạnh các cuộc tấn công mạng nhằm vào mục đích chính trị thì tình trạng rò rỉ dữ liệu người dùng vẫn chưa được kiểm soát tại Việt Nam. Cho đến nay, nhiều trang mạng trong nước và quốc tế vẫn liên tục rao bán kho dữ liệu chứa thông tin quan trọng của hàng triệu người Việt Nam như: căn cước công dân, số điện thoại, thư điện tử. Được biết, thông tin cá nhân người dùng đã bị các tổ chức tin tặc đánh cắp từ các diễn đàn trực tuyến, trang thương mại điện tử, các trang web cung cấp dịch vụ chăm sóc khách hàng... Từ đó, tin tặc đã thực hiện các cuộc tấn công nhằm vào các chủ thể là cá nhân gây hậu quả nghiêm trọng.

Hai là, cần phân biệt khái niệm “an ninh mạng” theo Luật an ninh mạng năm 2018 với một số khái niệm khá tương đồng được quy định trong một số văn bản quy phạm pháp luật khác có liên quan nhằm tránh trường hợp nhầm lẫn

1. Khoản 1, Điều 2, Luật an ninh mạng năm 2018.

như khái niệm về “an toàn thông tin” được quy định tại Nghị định số 72/2013/NĐ-CP hay “an ninh thông tin” được quy định tại Thông tư số 110/2014/TT-BQP, ngày 22/8/2014 của Bộ Quốc phòng về quy chế quản lý, cung cấp và sử dụng dịch vụ internet trong Quân đội nhân dân Việt Nam. Theo đó:

An toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

An ninh thông tin là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Khi nghiên cứu pháp luật của Xingapo, tác giả nhận thấy rằng Luật an ninh mạng năm 2018 của nước này có định nghĩa về “an ninh mạng” tập trung vào yếu tố hoạt động bình thường của máy tính hoặc hệ thống máy tính, cụ thể:

An ninh mạng có nghĩa là trạng thái trong đó máy tính hoặc hệ thống máy tính được bảo vệ khỏi bị truy cập hoặc tấn công trái phép và do trạng thái đó:

(a) máy tính hoặc hệ thống máy tính tiếp tục khả dụng và hoạt động;

(b) tính toàn vẹn của máy tính hoặc hệ thống máy tính được duy trì;

(c) tính toàn vẹn và bí mật của thông tin được lưu trữ trong xử lý hoặc truyền qua máy tính hoặc hệ thống máy tính được duy trì¹;

1. Xem Mục 2, Phần 1, Luật an ninh mạng năm 2018 của Xingapo.

Một số khái niệm khác có liên quan:

Ngoài định nghĩa trung tâm cần làm rõ là “an ninh mạng”, Luật an ninh mạng năm 2018 của nước ta cũng quy định một số khái niệm khác có liên quan cần thiết phải phân biệt. Cụ thể là:

Thứ nhất, “bảo vệ an ninh mạng” là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng (khoản 2, Điều 2, Luật an ninh mạng năm 2018). Nội dung này cũng được ghi nhận tương tự trong pháp luật về an ninh mạng của Thái Lan¹ và Mỹ².

Thứ hai, “nguy cơ đe dọa an ninh mạng” là tình trạng không gian mạng xuất hiện dấu hiệu đe dọa xâm phạm an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân (khoản 12, Điều 2, Luật an ninh mạng năm 2018). Thuật ngữ “mối đe dọa an ninh mạng” cũng được sử dụng tương tự trong quy định của Xingapo³ và Mỹ⁴.

Thứ ba, “sự cố an ninh mạng” là sự việc bất ngờ xảy ra trên không gian mạng 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 (khoản 13, Điều 2, Luật an ninh mạng năm 2018) được sử dụng tương tự trong quy định của Xingapo⁵ và Thái Lan⁶.

1, 6. Điều 3, Luật an ninh mạng năm 2019 của Thái Lan.

2. Tiểu mục 4, Mục 102, Đạo luật chia sẻ thông tin an ninh mạng năm 2015 của Mỹ.

3, 5. Điều 2, Luật an ninh mạng năm 2018 của Xingapo.

4. Tiểu mục 5, Mục 102, Đạo luật chia sẻ thông tin an ninh mạng năm 2015 của Mỹ.

Thứ tư, “tình huống nguy hiểm về an ninh mạng” là sự việc xảy ra trên không gian mạng khi có hành vi xâm phạm nghiêm trọng an ninh quốc gia, gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân (khoản 14, Điều 2, Luật an ninh mạng năm 2018) được sử dụng tương tự trong quy định của Xingapo¹ và Thái Lan².

b) Các hành vi bị cấm trong lĩnh vực an ninh mạng

Các hành vi bị nghiêm cấm về an ninh mạng được quy định tại Điều 8, Luật an ninh mạng năm 2018 và được cụ thể hóa thành một số nhóm như sau:

- Nhóm các hành vi có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế (Điều 16, Luật an ninh mạng năm 2018).

- Nhóm các hành vi gián điệp mạng; xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng (Điều 17, Luật an ninh mạng năm 2018).

- Nhóm các hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội (Điều 18, Luật an ninh mạng năm 2018).

- Nhóm các hành vi tấn công mạng (xem Điều 19, Luật an ninh mạng năm 2018).

1. Điều 2, Luật an ninh mạng năm 2018 của Xingapo.

2. Điều 3, Luật an ninh mạng năm 2019 của Thái Lan.

- Nhóm các hành vi khủng bố mạng (xem Điều 20, Luật an ninh mạng năm 2018).

Khi nghiên cứu pháp luật của Xingapo và Thái Lan, tác giả nhận thấy rằng ở cả hai quốc gia này đều không chỉ ra một cách minh thị các nhóm hành vi xâm phạm an ninh mạng như pháp luật Việt Nam. Thay vào đó, Thái Lan và Xingapo lại có cách phân loại theo mức độ nghiêm trọng của các hành vi này.

Theo đó, pháp luật Thái Lan chia các hành vi đe dọa tới an ninh mạng thành 3 mức độ¹ (1) Mỗi đe dọa an ninh mạng ở mức độ không nghiêm trọng; (2) Mỗi đe dọa an ninh mạng ở mức độ nghiêm trọng; (3) Mỗi đe dọa an ninh mạng ở mức độ đặc biệt nghiêm trọng. Đồng thời, việc xác định chi tiết về đặc điểm của các mối đe dọa trên mạng, các biện pháp phòng ngừa, đối phó hay đánh giá, ngăn chặn và đình chỉ các mối đe dọa này ở mỗi cấp độ sẽ được trao cho Ủy ban An ninh mạng quốc gia² quyết định.

Tương tự như vậy, pháp luật Xingapo cũng đặt ra các điều kiện để xác định một mối đe dọa an ninh mạng đạt ngưỡng nghiêm trọng nếu³:

(a) nó tạo ra nguy cơ gây hại đáng kể đối với kết cấu hạ tầng thông tin quan trọng;

(b) nó tạo ra nguy cơ gián đoạn việc cung cấp một dịch vụ thiết yếu;

1. Điều 60, Luật an ninh mạng năm 2019 của Thái Lan

2. National Cyber Security Committee - NCSC - Ủy ban An ninh mạng quốc gia Thái Lan. Quy định cụ thể tại Điều 5, Luật an ninh mạng năm 2019 của Thái Lan.

3. Tiểu mục 3, Điều 20, Luật an ninh mạng năm 2018 của Xingapo.

(c) nó tạo ra mối đe dọa đối với an ninh quốc gia, quốc phòng, quan hệ đối ngoại, kinh tế, sức khỏe cộng đồng, an toàn công cộng hoặc trật tự công cộng của Xingapo;

(d) nó tạo ra mối đe dọa hoặc sự cố an ninh mạng có tính chất nghiêm trọng, xét về mức độ nghiêm trọng của tác hại có thể gây ra cho những người ở Xingapo hoặc số lượng máy tính hoặc giá trị của thông tin có nguy cơ bị đe dọa, cho dù máy tính hoặc hệ thống máy tính có nguy cơ chính là kết cấu hạ tầng thông tin quan trọng.

Như vậy, dường như pháp luật Việt Nam có quy định chi tiết hơn trong việc gọi tên các hành vi cụ thể có nguy cơ gây mất an ninh trên không gian mạng so với hai quốc gia được tác giả khảo sát là Xingapo và Thái Lan. Việc mô tả chi tiết các hành vi này là căn cứ quan trọng để nhận diện và xử lý các trường hợp vi phạm trên thực tế.

c) Các hình thức xử lý vi phạm trong lĩnh vực an ninh mạng

Luật an ninh mạng năm 2018 chỉ ghi nhận nguyên tắc chung trong xử lý vi phạm pháp luật về an ninh mạng. Theo đó, người nào có hành vi vi phạm quy định của luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật (Điều 9, Luật an ninh mạng năm 2018). Như vậy, luật này đã trao quyền quy định chi tiết các hình thức xử phạt cho các văn bản quy phạm pháp luật khác có liên quan.

Xử lý vi phạm hành chính:

Nếu các hành vi vi phạm quy định về an ninh mạng chưa tới mức phải truy cứu trách nhiệm hình sự thì có thể bị xử lý

vi phạm hành chính. Theo đó, các quy định hiện nay được ghi nhận rai rác trong rất nhiều văn bản. Cụ thể là:

Thứ nhất, Luật sửa đổi, bổ sung một số điều của Luật xử lý vi phạm hành chính¹ quy định mức phạt tiền tối đa là 100.000.000 đồng đối với cá nhân vi phạm trong lĩnh vực an ninh mạng (khoản 10, Điều 4); đối với tổ chức thì bằng 2 lần mức phạt tiền đối với cá nhân. Việc bổ sung quy định về mức phạt tiền tối đa trong lĩnh vực an ninh mạng bên cạnh lĩnh vực an toàn thông tin mạng theo đánh giá của tác giả là cần thiết và hợp lý, bởi lẽ, trong Luật xử lý vi phạm hành chính năm 2012 chưa có quy định này. Điều này nhằm tạo ra sự đồng bộ với Luật an ninh mạng năm 2018.

Thứ hai, Nghị định số 167/2013/NĐ-CP, ngày 12/11/2013 của Chính phủ 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 và chữa cháy; phòng, chống bạo lực gia đình quy định mức phạt tiền từ 2.000.000 đồng đến 3.000.000 đồng đối với hành vi viết, phát tán, lưu hành tài liệu có nội dung xuyên tạc bịa đặt, vu cáo làm ảnh hưởng đến uy tín của tổ chức, cá nhân.

Thứ ba, Nghị định số 15/2020/NĐ-CP, ngày 03/02/2020 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 quy định hành vi truy cập trái phép vào mạng để chiếm quyền điều khiển của người khác, làm cản trở hoạt động cung cấp dịch vụ, ngăn chặn

1. Luật sửa đổi, bổ sung một số điều của Luật xử lý vi phạm hành chính có hiệu lực thi hành từ ngày 01/01/2022.

việc truy cập đến thông tin của tổ chức, cá nhân trên môi trường mạng... thì bị phạt tiền từ 30.000.000 - 50.000.000 đồng. Hình thức xử phạt bổ sung là trục xuất khỏi lãnh thổ nước Việt Nam đối với người nước ngoài có hành vi vi phạm quy định tại các khoản 1 và 2 Điều 80 của Nghị định này.

Truy cứu trách nhiệm hình sự:

Chủ thể thực hiện hành vi lợi dụng không gian mạng nhằm cung cấp hoặc phát tán các nội dung thông tin sai lệch, thất thiệt thì tùy theo tính chất, mức độ vi phạm có thể bị xử lý về tội quy định tại: Điều 117¹; điểm e, khoản 2, Điều 155²; điểm e, khoản 2, Điều 156³; điểm g, khoản 2, Điều 326⁴ hoặc có thể bị truy cứu về “Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông”⁵, “Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử” của Bộ luật hình sự năm 2015 (sửa đổi, bổ sung năm 2017)⁶.

Như vậy, có thể dễ dàng nhận thấy rằng các quy định về xử phạt trong lĩnh vực an ninh mạng hiện nay tại Việt Nam được quy định trong khá nhiều các văn bản quy phạm pháp luật khác nhau. Điều này dẫn tới tình trạng khó khăn trong quá trình tìm hiểu, phổ biến pháp luật đến người dân cũng như quá trình xử phạt của các cơ quan nhà nước

1. Tội làm, tàng trữ, phát tán hoặc tuyên truyền thông tin, tài liệu, vật phẩm nhằm chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

2. Tội làm nhục người khác.

3. Tội vu khống.

4. Tội truyền bá văn hóa phẩm đồi trụy.

5. Điều 288, Bộ luật hình sự năm 2015 (sửa đổi, bổ sung năm 2017).

6. Điều 287, Bộ luật hình sự năm 2015 (sửa đổi, bổ sung năm 2017).

có thẩm quyền. Tham khảo quy định của Xingapo¹ và Thái Lan², tác giả nhận thấy rằng ở cả hai quốc gia này đều có các văn bản quy định khá tập trung về các hình thức xử phạt đối với hành vi vi phạm pháp luật về an ninh mạng. Đặc biệt là Thái Lan còn có riêng một đạo luật quy định về tội phạm mạng. Thiết nghĩ Việt Nam không nhất thiết phải quy định theo hướng tổng hợp tất cả các hình thức xử phạt tội phạm về an ninh mạng vào cùng một văn bản giống như vậy. Tuy nhiên, để thuận lợi hơn trong công tác phổ biến và áp dụng pháp luật thì các cơ quan nhà nước có thẩm quyền nên có sự dẫn chiếu cụ thể tại các văn bản hướng dẫn. Điều này sẽ hạn chế được tình trạng “hoang mang” cho các tổ chức, cá nhân khi tìm kiếm các quy định có liên quan về vấn đề này.

*

* *

An ninh thông tin không chỉ là vấn đề “nóng” đặt ra với Việt Nam mà còn là vấn đề mà hầu hết các quốc gia trên thế giới quan tâm, đặc biệt là trong bối cảnh bùng nổ của công nghệ thông tin và sự gia tăng đáng kể các cuộc tấn công của tin tặc. Do đó việc hoàn thiện các quy định của pháp luật về an ninh thông tin cũng như phổ biến những quy định này

1. <https://www.cybercrimelaw.net/Singapore.html>, truy cập ngày 07/8/2021.

2. <https://www.cybercrimelaw.net/Thailand.html>, truy cập ngày 07/8/2021.

tối đông đảo các chủ thể trong xã hội là rất cần thiết. Bên cạnh đó, việc tăng cường điều tra và xử lý nghiêm các hành vi xâm phạm an ninh mạng cũng sẽ góp phần giảm thiểu các mối nguy hại trên không gian số; bảo đảm tốt hơn quyền lợi của Nhà nước và các tổ chức, cá nhân trong xã hội.

PHÁP LUẬT VIỆT NAM VỀ GIỚI HẠN QUYỀN TỰ DO BIỂU ĐẠT TRÊN KHÔNG GIAN MẠNG

ThS. VŨ LÊ HẢI GIANG*

Quyền tự do biểu đạt là một trong những quyền cơ bản đã được quy định trong Tuyên ngôn quốc tế nhân quyền năm 1948 của Liên hợp quốc. Tuy nhiên, quyền tự do biểu đạt rất dễ bị lạm dụng gây ảnh hưởng đến trật tự công cộng, an ninh quốc gia, sức khỏe, đạo đức cộng đồng, các quyền và tự do của người khác, đặc biệt là trong thời đại thông tin bùng nổ và lan truyền dễ dàng trên internet hiện nay, do vậy mà quyền tự do biểu đạt cần được giới hạn.

1. Giới hạn quyền tự do biểu đạt trên không gian mạng theo pháp luật quốc tế

a) Định nghĩa quyền tự do biểu đạt

Quyền tự do biểu đạt đã được ghi nhận trong văn kiện quốc tế đầu tiên về quyền con người - Tuyên ngôn quốc tế nhân quyền năm 1948 của Liên hợp quốc (Universal Declaration of Human Rights - sau đây gọi là “UDHR”). Theo đó, Điều 19 UDHR tuyên bố: “Mọi người đều có quyền tự do quan điểm và biểu đạt ý kiến,

* Trường Đại học Luật Thành phố Hồ Chí Minh.

cũng như tự do bảo lưu quan điểm mà không bị can thiệp, và tự do tìm kiếm, tiếp nhận và truyền bá các ý tưởng và thông tin bằng bất kỳ phương tiện truyền thông nào và không có giới hạn về biên giới”. Quyền này được gọi chung là “quyền tự do quan điểm và biểu đạt”¹.

Quyền tự do quan điểm và biểu đạt được tiếp tục khẳng định trong Điều 19 Công ước về các quyền chính trị và dân sự năm 1966 (International Covenant on Civil and Political Rights - sau đây gọi là “ICCPR”). Điều 19 ICCPR đã cụ thể hóa thành *quyền bảo lưu quan điểm*: “Mọi người có quyền bảo lưu quan điểm của mình mà không bị can thiệp”; và *quyền tự do biểu đạt*: “Mọi người có quyền tự do biểu đạt. Quyền này bao gồm tự do tìm kiếm, tiếp nhận và truyền đạt mọi thông tin, ý tưởng, không giới hạn về biên giới, thể hiện dưới hình thức tuyên truyền bằng miệng, bằng bản viết, in, hoặc dưới hình thức nghệ thuật, thông qua bất kỳ phương tiện thông tin đại chúng nào tùy theo sự lựa chọn của họ”².

Sau này, quyền tự do biểu đạt cũng được ghi nhận tương tự tại Công ước nhân quyền của châu Âu (European Convention on Human Rights - sau đây gọi là “ECHR”): “Mọi người đều có quyền tự do biểu đạt. Quyền này bao gồm tự do bảo lưu quan điểm cũng như tiếp nhận và truyền đạt mọi thông tin và ý tưởng mà không bị can thiệp bởi chính quyền

1. Xem *Tuyên ngôn quốc tế nhân quyền năm 1948*, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>, truy cập ngày 10/8/2021.

2. Xem *Công ước về các quyền chính trị và dân sự năm 1966*, <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, truy cập ngày 12/8/2021.

và bị không giới hạn về biên giới”¹. Những nội dung tương tự cũng được ghi nhận tại Điều 13 Công ước nhân quyền của châu Mỹ và Điều 9 Công ước nhân quyền của châu Phi.

Hiện nay, trong hiến pháp của hầu hết quốc gia trên thế giới đều có ghi nhận về quyền tự do biểu đạt dưới các khía cạnh như quyền tự do ngôn luận, quyền tự do báo chí, quyền tự do thông tin, ví dụ như: Hiến pháp Mỹ quy định Hạ viện không được ban hành một đạo luật tước đi tự do ngôn luận hay tự do báo chí của công dân². Hiến pháp của Pháp không quy định về quyền con người và quyền công dân, nhưng Lời mở đầu của Hiến pháp đã dẫn chiếu đến Tuyên ngôn Nhân quyền và Dân quyền năm 1789, trong đó nhấn mạnh “quyền được trao đổi ý tưởng và quan điểm là một trong những quyền con người quý giá nhất: do đó mọi công dân có quyền tự do ngôn luận, viết, in ấn, trừ trường hợp lạm dụng quyền này trong các trường hợp cụ thể được quy định trong luật”³. Điều 29 Hiến pháp của Liên bang Nga quy định: “Mọi người được bảo đảm quyền tự do tư tưởng và ngôn luận [...] Mỗi người đều có quyền tự do tìm hiểu, tiếp nhận, phổ biến thông tin bằng bất kỳ hình thức hợp pháp nào”⁴.

1. Khoản 1, Điều 10 ECHR, https://www.echr.coe.int/documents/convention_eng.pdf, truy cập ngày 11/8/2021.

2. *Tu chính thứ nhất của Hiến pháp Mỹ*, xem thêm tại: <https://constitution.congress.gov/constitution/>, truy cập ngày 15/8/2021.

3. Điều XI, Tuyên ngôn Nhân quyền và Dân quyền của Pháp năm 1789, xem https://avalon.law.yale.edu/18th_century/rightsof.asp, truy cập ngày 16/8/2021.

4. Hiến pháp của Liên bang Nga, <http://www.constitution.ru/en/10003000-03.htm>, truy cập ngày 15/8/2021.

Tóm lại, có thể hiểu quyền tự do biểu đạt là quyền tự do tìm kiếm, tiếp nhận và truyền đạt mọi thông tin, ý tưởng không giới hạn về biên giới, hình thức và phương tiện biểu đạt. Việc biểu đạt một thông tin hay ý tưởng có thể được thực hiện bằng nhiều phương thức đa dạng như thông qua lời nói, sách, báo chí, phim ảnh, âm nhạc hay các bài đăng trên mạng xã hội. Vì vậy, quyền tự do biểu đạt cũng hàm chứa quyền tự do ngôn luận, quyền tự do báo chí, quyền tự do thông tin và các quyền liên quan.

Quyền bảo lưu quan điểm là quyền tuyệt đối, không thể bị hạn chế hay tước bỏ trong bất cứ hoàn cảnh nào¹. Còn quyền tự do biểu đạt quan điểm của một cá nhân chắc hẳn sẽ ảnh hưởng tới quan điểm của người khác, thậm chí có thể còn tiềm ẩn những mối đe dọa đối với quyền tự do và an ninh của các cá nhân cũng như trật tự xã hội, an ninh quốc gia. Trong thời đại bùng nổ thông tin và truyền thông qua không gian mạng, quyền tự do biểu đạt đặc biệt dễ bị lạm dụng nhằm kích động, xúi giục người khác vì mục đích không chính đáng, hoặc lan truyền thông tin sai sự thật gây hoang mang dư luận. Do vậy mà các công ước quốc tế về quyền con người, song song với việc ghi nhận, đã quy định những giới hạn chặt chẽ của quyền tự do biểu đạt.

b) Giới hạn quyền tự do biểu đạt

Theo cách hiểu phổ biến trên thế giới, sự hạn chế/giới hạn đối với một quyền con người nào đó được hiểu là việc

1. Xem *Bình luận chung số 34 (về tự do quan điểm và biểu đạt)* của Văn phòng Cao ủy nhân quyền của Liên hợp quốc (Office of the United Nations High Commissioner for Human Rights), được thông qua vào kỳ họp thứ 102 năm 2011, các đoạn 5 và đoạn 9.

Nhà nước không cho phép các chủ thể thụ hưởng quyền có thể thực hiện quyền đó ở mức độ tuyệt đối¹. Việc giới hạn các quyền là tất yếu và khách quan, bởi nếu như tất cả các quyền đều là tuyệt đối và không bị hạn chế thì không hình thành nên xã hội, không thể hình thành các cộng đồng người². Vì thế mà ngay từ khi quan điểm về quyền con người xuất hiện trong lịch sử loài người, song song với đó là nhận thức về giới hạn quyền³. Các quốc gia hiện đại đều giống nhau ở chỗ công nhận các quyền và tự do, nhưng khác nhau ở phạm vi giới hạn quyền và phương pháp đặt ra các giới hạn đó. Không có quyền con người trừu tượng được đặt cao hơn cộng đồng và chủ quyền quốc gia, quyền con người phải được ghi nhận cụ thể và thể chế phù hợp với trình độ phát triển những nét đặc thù về trình độ kinh tế, văn hóa, tín ngưỡng, truyền thống chính trị của mỗi quốc gia, dân tộc⁴. Nhìn chung, việc giới hạn quyền con người, quyền công dân chủ yếu nhằm các mục đích sau: bảo vệ trật tự công cộng, sức khỏe cộng đồng, đạo đức công cộng, an ninh quốc gia, an toàn công cộng, các quyền và tự do của người khác⁵.

1. Xem Aharon Barak: *Proportionality: Constitutional Rights and Their Limitations*, Cambridge University Press, 2012, p.102.

2, 4. Xem Viện Khoa học pháp lý - Bộ Tư pháp: “Chuyên đề: Nguyên tắc hạn chế quyền con người, quyền công dân theo Hiến pháp năm 2013”, tạp chí *Thông tin khoa học pháp lý*, số 03/2018, tr.10, 9.

3. Xem Nguyễn Minh Tuấn (Chủ biên): *Giới hạn chính đáng đối với các quyền con người, quyền công dân trong pháp luật quốc tế và pháp luật Việt Nam*, Nxb. Hồng Đức, Hà Nội, 2015, tr.15.

5. Những mục đích này được xem là chính đáng trong các Điều 12, 14, 19, 21 và 22 của ICCPR.

Điều 19 ICCPR quy định việc giới hạn quyền tự do biểu đạt phải cần thiết, chính đáng và phải được luật định. Các mục đích chính đáng bao gồm: (1) để bảo vệ quyền và danh dự của người khác; và (2) để bảo vệ an ninh quốc gia, trật tự công cộng, hoặc đạo đức hay sức khỏe cộng đồng¹. Đồng thời, Điều 20 ICCPR cũng nghiêm cấm việc lợi dụng quyền tự do biểu đạt để tuyên truyền kích động chiến tranh, hoặc chủ trương thù hận dân tộc, sắc tộc, tôn giáo hay kích động phân biệt chủng tộc, thù địch hay bạo lực. Một số nội dung của Điều 20 ICCPR đã được Văn phòng Cao ủy nhân quyền của Liên hợp quốc đã làm rõ trong Bình luận chung số 11 như sau²:

Thứ nhất, việc cấm các hoạt động tuyên truyền kích động chiến tranh, hoặc chủ trương thù hận dân tộc, sắc tộc, tôn giáo hay kích động phân biệt chủng tộc, thù địch hay bạo lực là cần thiết và phù hợp với Điều 19 ICCPR về quyền tự do biểu đạt.

Thứ hai, các quốc gia có quyền cấm tất cả những hình thức tuyên truyền đe dọa thực hiện hành động xâm lược hay phá hoại hòa bình trái với Hiến chương Liên hợp quốc. Đồng thời, những hành động chủ trương thù hận dân tộc, sắc tộc, tôn giáo hay kích động phân biệt chủng tộc, thù địch hay bạo lực cũng có thể bị cấm, bất kể diễn ra ở bên trong hay bên ngoài lãnh thổ của quốc gia đó.

1. Xem Khoản 3, Điều 19 ICCPR.

2. Xem *Bình luận chung số 11 (về Điều 20 ICCPR)* của Văn phòng Cao ủy Nhân quyền Liên hợp quốc (Office of the United Nations High Commissioner for Human Rights), được thông qua vào kỳ họp thứ 19 năm 1983, đoạn 2.

Cũng như ICCPR, ECHR tuyên bố việc thực hiện các tự do kể trên phải tuân theo những thủ tục, điều kiện, giới hạn, hình phạt cần thiết và đã được luật định. Các trường hợp “cần thiết” cũng được liệt kê cụ thể bao gồm: bảo vệ an ninh quốc gia, toàn vẹn lãnh thổ hay trật tự công cộng; ngăn ngừa tội phạm; bảo vệ đạo đức và sức khỏe cộng đồng; bảo vệ quyền và danh dự của người khác; ngăn chặn việc tiết lộ thông tin mật; hoặc nhằm duy trì thẩm quyền và tính độc lập của tư pháp¹.

Hiến pháp của các quốc gia trên thế giới cũng đều trực tiếp hay gián tiếp quy định về những giới hạn của quyền tự biểu đạt. Điều 29 Hiến pháp của Liên bang Nga cũng đặt ra giới hạn của quyền tự do biểu đạt đối với những thông tin gây thù hận hoặc phân biệt về mặt xã hội, chủng tộc, sắc tộc, tôn giáo. Tại Mỹ, mặc dù không được hiến định chính thức, song quyền tự do ngôn luận của công dân Mỹ cũng có những giới hạn được quy định trong các án lệ. Ví dụ như trong vụ *Chaplinsky v. New Hampshire* (1942), Tòa án Tối cao Liên bang tuyên bố không bảo vệ các diễn ngôn bạo lực nhằm kích động việc phá hoại hòa bình²; hay vụ *New York Times Co. v. Sullivan* (1964) xác lập quy định rằng những phỉ báng sai sự thật về các công chức có thể bị cấm³;... Hiến pháp của

1. Xem khoản 2, Điều 10 ECHR.

2. Xem J. Michael Bitzer: *Chaplinsky v. New Hampshire* (1942), The First Amendment Encyclopedia, Middle Tennessee State University, 2009, <https://www.mtsu.edu/first-amendment/article/293/chaplinsky-v-new-hampshire>.

3. Xem Stephen Wermiel: *New York Times Co. v. Sullivan* (1964), The First Amendment Encyclopedia, Middle Tennessee State University, 1964, <https://www.mtsu.edu/first-amendment/article/186/new-york-times-co-v-sullivan>, accessed in 10/8/2021.

Cộng hòa Liên bang Đức cũng quy định các quyền tự do biểu đạt, nghệ thuật và khoa học bị giới hạn bởi các luật chung, các quy định liên quan tới trẻ vị thành niên và quy định bảo vệ danh dự của người khác¹.

c) Giới hạn quyền tự do biểu đạt trên không gian mạng

Theo định nghĩa của Từ điển Cambridge, “không gian mạng” (cyberspace) được hiểu theo các nghĩa sau:

(1) Đồng nghĩa với khái niệm internet được hiểu như không gian ảo không có giới hạn mà người dùng có thể gặp nhau hoặc tìm kiếm thông tin về bất kỳ đối tượng nào;

(2) Một hệ thống điện tử cho phép người dùng máy tính trên khắp thế giới giao tiếp với nhau hoặc truy cập thông tin cho bất kỳ mục đích nào;

(3) Internet được coi là một không gian ảo tồn tại các email, trang web,... đặc biệt là khi thông tin được truyền giữa máy tính này và máy tính khác.

Như vậy có thể hiểu không gian mạng là một không gian ảo mà thông tin được lan truyền không biên giới và gần như tức thì bằng nhiều phương tiện như các email, trang web, mạng xã hội,...

Có thể nói sự xuất hiện và phổ biến của không gian mạng làm thay đổi căn bản mọi mặt trong đời sống xã hội ở mọi bình diện. Giao tiếp, truyền thông và tra cứu thông tin chưa bao giờ dễ dàng như hiện nay khi chỉ cần một cú click chuột, người dùng có thể truy cập vào hàng nghìn cơ sở dữ liệu đồ sộ cũng như các mạng xã hội sôi động. Tuy nhiên, chính sự tiện

1. Xem Điều 5 Hiến pháp Cộng hòa Liên bang Đức, https://www.gesetze-im-internet.de/englisch_gg/, accessed in 15/8/2021.

lợi ấy lại tiềm ẩn nguy cơ to lớn về tin giả, gây xâm hại đến quyền và lợi ích của cá nhân, tổ chức, xã hội, hay thậm chí là đe dọa đến trật tự công cộng và an ninh quốc gia, đặc biệt là trong những giai đoạn như thiên tai, dịch bệnh... Do đó mà Nghị quyết số A/HRC/RES/20/8 của Ủy ban Nhân quyền của Liên hợp quốc đã đề ra một nguyên tắc: các quyền được bảo vệ như thế nào trên thực tế thì được bảo vệ như thế ấy trên không gian mạng¹. Điều này cũng có nghĩa là các giới hạn của quyền tự do biểu đạt cũng được áp dụng đầy đủ trên không gian mạng. Tuy nhiên, vì những đặc thù của thông tin trên không gian mạng như tính không biên giới, tính tức thời, mà ngoài việc áp dụng những nguyên tắc cố hữu trong việc giới hạn quyền tự do biểu đạt, luật lệ và thực tiễn giới hạn quyền này tại các quốc gia cũng thay đổi tương ứng với sự phát triển của internet².

Hiện nay đã có 138 nước ban hành các đạo luật an ninh mạng, nhằm vừa bảo vệ quyền con người, quyền công dân, vừa bảo vệ an ninh thông tin quốc gia trước các vi phạm đi quá giới hạn³. Có thể nói, việc ban hành những giới hạn

1. Xem Human Rights Council: *Resolution A/HRC/RES/20/8 on the promotion, protection and enjoyment of human rights on the Internet*, Report of the Council on its twentieth session (A/HRC/20/2), 2012, chap. I., p.1.

2. Xem Wolfgang Benedek and Matthias C. Kettmann: *Freedom of expression and the Internet*, Council of Europe Publishing, 2013, p.54.

3. Xem Đặng Dũng Chí: “Cách nhìn của các quốc gia về quyền con người trên không gian mạng”, Tạp chí *Xây dựng Đảng*, http://www.xaydungdang.org.vn/home/nhan_quyen/2021/14702/cach-nhin-cua-cac-quoc-gia-ve-quyen-con-nguoi-tren-khong-gian-mang.aspx, truy cập ngày 15/8/2021.

riêng cho tự do biểu đạt trên không gian mạng là xu thế phổ biến và tất yếu trên thế giới hiện nay. Nghiên cứu của Hội đồng châu Âu cũng cho thấy Tòa án Nhân quyền châu Âu đã và đang đứng trước thách thức trong các vụ việc liên quan đến tự do biểu đạt trên internet: một mặt phải tuân thủ các nguyên tắc giới hạn quyền và mặt khác, phải áp dụng phù hợp với các đặc điểm của không gian mạng¹. Vì thế mà phán quyết của các tòa án tại châu Âu liên quan đến tự do biểu đạt trên internet thường phụ thuộc vào bối cảnh của từng vụ việc cụ thể². Điều này cũng có nghĩa là giới hạn của việc thực hiện quyền tự do biểu đạt trên internet sẽ được xác lập khác với việc thực hiện quyền này trên thực tế.

2. Giới hạn quyền tự do biểu đạt trên không gian mạng trong pháp luật Việt Nam

Hiến pháp đầu tiên của nước Việt Nam Dân chủ Cộng hòa ra đời năm 1946 đã tuyên bố công dân Việt Nam có các quyền tự do ngôn luận, tự do xuất bản (Điều 10, Hiến pháp năm 1946). Kế thừa quy định tiến bộ ấy, Điều 25, Hiến pháp hiện hành quy định: “Công dân có quyền tự do ngôn luận, tự do báo chí, tiếp cận thông tin, hội họp, lập hội, biểu tình. Việc thực hiện các quyền này do pháp luật quy định”. Bên cạnh đó, Hiến pháp hiện hành cũng quy định giới hạn nói chung của các quyền con người, quyền công dân như sau: (1) quyền con người, quyền công dân chỉ có thể bị hạn chế theo quy định của luật trong trường hợp cần thiết vì

1, 2. Xem Wolfgang Benedek and Matthias C. Kettmann: *Freedom of expression and the Internet*, Council of Europe Publishing, 2013, p.54, 50.

lý do quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, đạo đức xã hội, sức khỏe của cộng đồng (Điều 14, Hiến pháp năm 2013); và (2) việc thực hiện quyền con người, quyền công dân không được xâm phạm lợi ích quốc gia, dân tộc, quyền và lợi ích hợp pháp của người khác (Điều 15, Hiến pháp năm 2013). Đây là những giới hạn chung có giá trị như nguyên tắc giới hạn quyền con người, quyền công dân nói chung và quyền tự do biểu đạt nói riêng tại nước ta.

Trong phạm vi không gian mạng, những giới hạn này được quy định cụ thể chủ yếu trong Bộ luật hình sự và Luật an ninh mạng hiện hành. Theo đó, chủ thể lạm dụng tự do biểu đạt mà vượt quá các giới hạn này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật. Cụ thể như sau:

a) Giới hạn quyền tự do biểu đạt để bảo vệ quyền và danh dự của người khác trên không gian mạng

Nhằm bảo vệ quyền và danh dự của người khác trên không gian mạng, pháp luật nước ta không cho phép biểu đạt, lan truyền các thông tin có nội dung:

- Xúc phạm nghiêm trọng nhân phẩm, danh dự của người khác¹.
- Bịa đặt hoặc loan truyền những điều biết rõ là sai sự thật nhằm xúc phạm nghiêm trọng nhân phẩm, danh dự

1. Điều 155, Bộ luật hình sự năm 2015 (sửa đổi, bổ sung năm 2017) quy định về tội làm nhục người khác. Đây cũng là thông tin không được biểu đạt trên không gian mạng theo điểm a, khoản 3, Điều 16, Luật an ninh mạng năm 2018.

hoặc gây thiệt hại đến quyền, lợi ích hợp pháp của người khác; hoặc bịa đặt người khác phạm tội và tố cáo họ trước cơ quan có thẩm quyền¹.

- Cố ý công bố thông tin sai lệch hoặc che giấu thông tin trong hoạt động chào bán, niêm yết, giao dịch, hoạt động kinh doanh chứng khoán, tổ chức thị trường, đăng ký, lưu ký, bù trừ hoặc thanh toán chứng khoán².

- Đưa lên mạng máy tính, mạng viễn thông những thông tin trái với quy định của pháp luật, hoặc mua bán, trao đổi, tặng cho, sửa chữa, thay đổi hoặc công khai hóa thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân trên mạng máy tính, mạng viễn thông mà không được phép của chủ sở hữu thông tin đó hoặc các hành vi khác sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông³.

- Thông tin sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác (điểm d, khoản 1, Điều 8 và khoản 5, Điều 16, Luật an ninh mạng năm 2018).

1. Điều 156, Bộ luật hình sự năm 2015 (sửa đổi, bổ sung năm 2017) quy định về tội vu khống. Đây cũng là thông tin không được biểu đạt trên không gian mạng theo điểm b, khoản 3 Điều 16, Luật an ninh mạng năm 2018.

2. Điều 209, Bộ luật hình sự năm 2015 (sửa đổi, bổ sung năm 2017) quy định về tội cố ý công bố thông tin sai lệch hoặc che giấu thông tin trong hoạt động chứng khoán.

3. Điều 288, Bộ luật hình sự năm 2015 (sửa đổi, bổ sung năm 2017) quy định về tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông.

b) Giới hạn quyền tự do biểu đạt để bảo vệ an ninh quốc gia, trật tự công cộng, hoặc đạo đức hay sức khỏe cộng đồng trên không gian mạng

Nhằm bảo vệ an ninh quốc gia và trật tự công cộng, pháp luật Việt Nam không cho phép biểu đạt, lan truyền các thông tin có nội dung:

- Xuyên tạc, phỉ báng chính quyền nhân dân, hoặc có nội dung bịa đặt, gây hoang mang trong nhân dân, hoặc gây chiến tranh tâm lý¹.

- Kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước (khoản 1, Điều 16, Luật an ninh mạng năm 2018).

- Kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng, bao gồm kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự (khoản 2, Điều 16, Luật an ninh mạng năm 2018).

- Tổ chức, hoạt động, cấu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam (điểm b, khoản 1, Điều 8, Luật an ninh mạng năm 2018).

1. Điều 117, Bộ luật hình sự năm 2015 (sửa đổi, bổ sung năm 2017) quy định về tội làm, tàng trữ, phát tán hoặc tuyên truyền thông tin, tài liệu, vật phẩm nhằm chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

- Xúi giục, lôi kéo, kích động người khác phạm tội (điểm e, khoản 1, Điều 8, Luật an ninh mạng năm 2018) hoặc hướng dẫn người khác thực hiện hành vi vi phạm pháp luật (điểm đ, khoản 1, Điều 18, Luật an ninh mạng năm 2018).

- Biểu đạt thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế, bao gồm thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác hoặc thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán (khoản 4, Điều 16, Luật an ninh mạng năm 2018).

Bên cạnh đó, để bảo vệ đạo đức và sức khỏe cộng đồng, pháp luật Việt Nam không cho phép biểu đạt, lan truyền các thông tin có nội dung:

- Xúc phạm Quốc kỳ, Quốc huy, Quốc ca¹, xúc phạm vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc (điểm c, khoản 1, Điều 16, Luật an ninh mạng năm 2018).

- 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 (điểm c, khoản 1, Điều 8, Luật an ninh mạng năm 2018).

- Đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng (điểm đ, khoản 1, Điều 8, Luật an ninh mạng năm 2018).

1. Điều 351, Bộ luật hình sự năm 2015 (sửa đổi, bổ sung năm 2017) quy định về tội xúc phạm Quốc kỳ, Quốc huy, Quốc ca.

Từ những nội dung trên, có thể rút ra một số kết luận như sau:

Thứ nhất, quyền tự do biểu đạt đã được hiến định tại Điều 25, Hiến pháp hiện hành như một quyền cơ bản của công dân dưới các khía cạnh tự do ngôn luận và tự do báo chí, tiếp cận thông tin. Hiến pháp hiện hành cũng đã quy định nguyên tắc giới hạn và hạn chế quyền nói chung, còn các giới hạn cụ thể đối với quyền tự do biểu đạt thì được quy định trong luật. Cách quy định này có thể tìm thấy tương tự trong Hiến pháp của các nước tiến bộ như Mỹ, Đức, Nga... Bởi với tư cách là luật cơ bản của nước Cộng hòa xã hội chủ nghĩa Việt Nam, có hiệu lực pháp lý cao nhất, Hiến pháp chỉ quy định những vấn đề chung nhất, khái quát nhất, mang tính nền tảng, nguyên tắc.

Thứ hai, các giới hạn của tự do biểu đạt trên không gian mạng theo pháp luật Việt Nam không chỉ nhằm bảo vệ an ninh quốc gia, trật tự công cộng trong lĩnh vực thông tin, mà còn nhằm bảo vệ quyền con người, quyền công dân và danh dự của cá nhân cũng như bảo vệ đạo đức, sức khỏe cộng đồng. Những mục đích này là hoàn toàn chính đáng và cần thiết phù hợp với yêu cầu của Điều 19 và Điều 20 ICCPR.

Thứ ba, các giới hạn của tự do biểu đạt trên không gian mạng theo pháp luật Việt Nam đều đã được luật định. Điều này một mặt khẳng định sự tương thích của các quy định này trong pháp luật Việt Nam với pháp luật quốc tế¹, mặt khác,

1. Khoản 3, Điều 19 ICCPR quy định các giới hạn của quyền tự do biểu đạt phải được luật định.

bảo đảm các giới hạn này mang tính bền vững, dự đoán được và không bị áp dụng một cách tùy tiện.

Tóm lại, có thể khẳng định rằng pháp luật nước ta đã quy định về quyền tự do biểu đạt nói chung và giới hạn quyền này nói riêng, một mặt hoàn toàn phù hợp với pháp luật nhân quyền quốc tế về bảo đảm và hạn chế quyền, mặt khác phù hợp với tình hình phát triển và hội nhập của Việt Nam trong thời đại mới.

GIÁO DỤC, NÂNG CAO NHẬN THỨC CHO SINH VIÊN VỀ BẢO VỆ CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG

ThS. LÊ VŨ XUÂN UYÊN*

Đảng ta luôn đề cao vai trò, vị trí của thanh niên, sinh viên - xác định đây là lực lượng xung kích cách mạng, góp phần đấu tranh trên mặt trận chính trị, tư tưởng, phê phán các quan điểm sai trái, thù địch, bảo vệ nền tảng tư tưởng, cương lĩnh, đường lối của Đảng Cộng sản Việt Nam. Đặc biệt, với nhiệt huyết cách mạng, sự trẻ trung, nhạy bén, sáng tạo của tuổi trẻ, đấu tranh bảo vệ chủ quyền quốc gia trên không gian mạng của sinh viên Việt Nam đã và đang được xem là trọng trách lớn của thanh niên hiện nay. Tuy nhiên, với mức độ tinh vi, các thế lực thù địch luôn tìm cách tạo nhiều thông tin nhiễu loạn, gây hoang mang ý chí của lớp trẻ. Bài viết này đưa ra một số giải pháp nhằm giáo dục, nâng cao nhận thức cho sinh viên về bảo vệ chủ quyền quốc gia trên không gian mạng.

* Học viện Chính trị khu vực II, Học viện Chính trị quốc gia Hồ Chí Minh.

1. Quan điểm của Đảng về bảo vệ Tổ quốc trong tình hình mới

Quan điểm về quốc phòng, an ninh của Đảng được nêu trong Nghị quyết Đại hội đại biểu toàn quốc lần thứ XIII như sau: “Kiên quyết, kiên trì bảo vệ vững chắc độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc; bảo vệ Đảng, Nhà nước, nhân dân và chế độ xã hội chủ nghĩa. Giữ vững an ninh chính trị, bảo đảm trật tự, an toàn xã hội, an ninh con người, an ninh kinh tế, an ninh mạng, xây dựng xã hội trật tự, kỷ cương. Chủ động ngăn ngừa các nguy cơ chiến tranh, xung đột từ sớm, từ xa; phát hiện sớm và xử lý kịp thời những yếu tố bất lợi, nhất là những yếu tố nguy cơ gây đột biến; đẩy mạnh đấu tranh làm thất bại mọi âm mưu và hoạt động chống phá của các thế lực thù địch”¹.

Nâng cao nhận thức cho mọi người về tư duy mới bảo vệ Tổ quốc của Đảng ta là rất cần thiết. Trong đó, “kiên quyết, kiên trì đấu tranh bảo vệ vững chắc độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc” là quan điểm cơ bản, tư tưởng chỉ đạo xuyên suốt của Đảng ta. Bởi vì, bảo vệ Tổ quốc xã hội chủ nghĩa là một trong hai nhiệm vụ chiến lược, là sự nghiệp của toàn Đảng, toàn dân, toàn quân ta. Sự nghiệp cao cả ấy phải thường xuyên được coi trọng, không được lơ là, phải gắn chặt với nhiệm vụ xây dựng đất nước. Hiện nay tác động của tình hình quốc tế và trong nước, sự chống phá của các thế lực thù địch đối với nước ta;

1. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2021, t.II, tr.331.

bài học kinh nghiệm quý báu “dựng nước phải đi đôi với giữ nước” được đúc kết trong lịch sử và đã trở thành quy luật tồn tại, phát triển của dân tộc ta. Mặt khác, thực hiện quan điểm trên có quan hệ trực tiếp tới sự tồn vong của chế độ, đất nước, dân tộc ta. Vì thế, bất luận trong hoàn cảnh nào, kiên quyết, kiên trì bảo vệ vững chắc Tổ quốc là trách nhiệm chính trị, là nghĩa vụ thiêng liêng cao cả của các thế hệ người Việt Nam.

Lịch sử của dân tộc ta là những trang sử hào hùng trong dựng nước và giữ nước. Việt Nam là quốc gia có chủ quyền được quốc tế công nhận, đây là cơ sở pháp lý mà không một ai hay một thế lực nào dù mạnh đến đâu có thể phản bác, chối bỏ hoặc xâm phạm. Chủ quyền thiêng liêng của nước ta là kết quả quá trình đấu tranh cách mạng của nhân dân ta dưới sự lãnh đạo của Đảng và Chủ tịch Hồ Chí Minh. Trách nhiệm cao cả của mỗi người dân hôm nay và mai sau là phải giữ cho được chủ quyền quốc gia - dân tộc; đó là quyền chủ quyền, quyền được tôn trọng tại các tổ chức, diễn đàn, hội nghị quốc tế,... mà ta tham gia với tư cách là thành viên. Chủ quyền quốc gia cần được giữ vững và thể hiện một cách đầy đủ trên thực tế, trên tất cả các lĩnh vực, trong các vấn đề đối nội và đối ngoại.

Bảo vệ vững chắc toàn vẹn lãnh thổ của Tổ quốc là nghĩa vụ và trách nhiệm chính trị của toàn Đảng, toàn dân, toàn quân ta. Nhiệm vụ này càng trở nên quan trọng khi tình hình Biển Đông đang diễn biến phức tạp, tiềm ẩn những nguy cơ khó lường đe dọa đến chủ quyền, quyền chủ quyền, an ninh vùng biển nước ta. Những năm gần đây có nước đã bất chấp luật pháp, thông lệ quốc tế, nhất là Công ước của

Liên hợp quốc về Luật biển năm 1982, Quy định về cách ứng xử của các bên ở Biển Đông, ngang nhiên có những hành động xâm phạm vùng biển nước ta. Vì thế, hơn bao giờ hết, chúng ta phải thường xuyên nâng cao cảnh giác, chủ động, tích cực đấu tranh với mọi hành động xâm phạm chủ quyền, lãnh thổ của Tổ quốc. Chúng ta không cho phép bất cứ ai xâm phạm lãnh thổ Tổ quốc, đây là nguyên tắc, là quan điểm nhất quán của Đảng, Nhà nước và nhân dân ta.

Cùng với quá trình trên, cần “kiên quyết, kiên trì” đấu tranh bảo vệ vững chắc độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc. Trong đó, kiên quyết thể hiện quyết tâm dứt khoát, tạo sự đồng thuận cao hơn trong toàn Đảng, toàn dân, toàn quân ta về yêu cầu bảo vệ chủ quyền, lợi ích đất nước; kiên quyết giữ vững những vấn đề có tính nguyên tắc, bảo vệ đến cùng lợi ích quốc gia - dân tộc với quyết tâm cao nhất. Kiên trì thể hiện cuộc đấu tranh bảo vệ chủ quyền, lợi ích đất nước sẽ còn lâu dài, đòi hỏi toàn Đảng, toàn dân, toàn quân ta không lơ là, mất cảnh giác, không nản lòng mà nuôi dưỡng ý chí quyết tâm thật cao; kiên trì giải quyết những bất đồng, tranh chấp bằng biện pháp hòa bình, trên mọi lĩnh vực, mọi mặt như: đối thoại, pháp lý, quốc phòng, an ninh, văn hóa..., trên cơ sở bảo đảm lợi ích quốc gia - dân tộc.

Bên cạnh đó, cần kiên quyết, kiên trì đấu tranh với mọi âm mưu, thủ đoạn sai trái, thù địch, nhất là trên không gian mạng để bảo vệ Đảng, Nhà nước, nhân dân và chế độ xã hội chủ nghĩa. Tích cực nâng cao chất lượng tổng hợp và sức mạnh chiến đấu của Quân đội nhân dân, Công an nhân dân, tuyệt đối trung thành với Đảng, Nhà nước, nhân dân và chế độ

xã hội chủ nghĩa. Trong bất cứ điều kiện, hoàn cảnh nào, Quân đội nhân dân và Công an nhân dân đều tỏ rõ bản lĩnh chính trị, kiên định, vững vàng, luôn xứng đáng là lực lượng nòng cốt trong thực hiện nhiệm vụ quốc phòng, an ninh, bảo vệ Tổ quốc, chủ động tham gia cứu hộ, cứu nạn, khắc phục hậu quả thiên tai.

Nhận thức nhiệm vụ bảo vệ Tổ quốc từ sớm, từ xa là sự kế thừa và phát huy truyền thống chủ động giữ nước trong thời bình của cha ông. Đó là tổng thể các hoạt động của Đảng, Nhà nước, nhân dân, các lực lượng vũ trang diễn ra một cách chủ động, thường xuyên; sớm phát hiện, ngăn chặn, vô hiệu hóa mọi âm mưu, hoạt động chống phá chế độ chính trị, xâm phạm độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ, lợi ích quốc gia, giữ vững hòa bình, ổn định, không để bị động, bất ngờ, bảo vệ vững chắc Tổ quốc Việt Nam xã hội chủ nghĩa trong mọi tình huống.

2. Thực trạng nhận thức của sinh viên Việt Nam trong đấu tranh bảo vệ chủ quyền quốc gia trên không gian mạng

Sinh viên là nhóm người trong độ tuổi thanh niên - những người có tri thức về khoa học - kỹ thuật, có tinh thần và nhiệt huyết của tuổi trẻ, có sự sáng tạo trong học tập và lao động, nhạy cảm với cái mới trong đời sống xã hội. Trước sự tác động của nền kinh tế thị trường, của quá trình toàn cầu hóa và cuộc cách mạng khoa học công nghệ, bên cạnh đại bộ phận sinh viên có nhận thức chính trị tích cực, có lập trường và bản lĩnh chính trị vững vàng, có niềm tin vào sự lãnh đạo của Đảng, vào công cuộc đổi mới và con đường đi lên chủ nghĩa xã hội,

có ý thức tự cường dân tộc, có sức “đề kháng” trước các âm mưu, thủ đoạn của các thế lực thù địch, thì vẫn còn một số tỏ ra dao động, mất phương hướng phấn đấu, xa rời mục tiêu, lý tưởng của Đảng, ít quan tâm, thờ ơ với vấn đề chính trị - xã hội của đất nước, mơ hồ, lệch lạc trong tư tưởng chính trị, đạo đức và lối sống, vi phạm pháp luật.

Các thế lực thù địch luôn xác định thanh niên - sinh viên là đối tượng quan trọng để thực hiện âm mưu “diễn biến hòa bình”, thúc đẩy “tự diễn biến”, “tự chuyển hóa” trong nội bộ. Trong thời gian qua, các thế lực phản động trong và ngoài nước luôn tìm cách lợi dụng, lôi kéo, kích động giới trẻ. Chúng sử dụng nhiều thủ đoạn, chiêu bài như nhân danh tự do, nhân quyền, tôn giáo... với mục đích tạo ra một thế hệ trẻ sống ảo tưởng, cổ xúy cho chủ nghĩa thực dụng, thích ăn chơi, lười lao động, sống vụ lợi, vị kỷ, thậm chí là xét lại lịch sử, quá khứ... Với sự phát triển của công nghệ thông tin, chúng lợi dụng các trang mạng xã hội trên internet để phát tán những tài liệu có nội dung đi ngược lại với chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước, trái với thuần phong, mỹ tục, truyền thống văn hóa tốt đẹp của dân tộc ta để “chuyển hóa” dần dần lớp trẻ. Chúng bịa đặt ra những thông tin sai lệch, có tính chất giật gân và tạo ra các diễn đàn nóng nhân danh “tự do ngôn luận” để thu hút những người trẻ tuổi truy cập và đưa ra ý kiến bình luận, chia sẻ.

Internet, không gian mạng, chủ yếu là mạng xã hội là phương thức mà các thế lực thù địch, cơ hội, phản động sử dụng chủ yếu để chống phá cách mạng nước ta. Các thế lực thù địch sử dụng mạng xã hội nhằm tổ chức truyền tải thông tin

độc hại, bịa đặt, phát tán các quan điểm phản động, xuyên tạc, kích động thông qua việc thiết lập hàng nghìn trang website, blog, tài khoản Facebook, Zalo, trang fanpage, dịch vụ thư điện tử (email), các dịch vụ hội thoại (chat), điện thoại (VoIP), diễn đàn (forum), Twitter, MySpace,... với hầu hết máy chủ đặt ở nước ngoài, tổ chức hàng trăm chiến dịch tuyên truyền, phát tán với tần suất và số lượng lớn các tin, bài bình luận, video clip... có nội dung xấu, độc, thật - giả, trắng - đen lẫn lộn, tạo tâm lý tò mò và hiệu ứng đám đông, qua đó, khuyến khích mọi người, nhất là lớp trẻ trao đổi, thu nhận thông tin, bày tỏ quan điểm cực đoan, làm “nóng” các vấn đề xã hội, nhất là vấn đề có liên quan đến chủ quyền biên giới quốc gia trên đất liền và hải đảo.

Các thế lực thù địch không ngừng truyền bá luận điệu xuyên tạc về vấn đề quốc phòng, an ninh, đối ngoại. Họ cho rằng, quân đội và công an chỉ làm nhiệm vụ bảo vệ đất nước và an ninh, trật tự xã hội, không nên bị chi phối bởi chính trị. Nhiệm vụ cao nhất, duy nhất của quân đội và công an là bảo vệ Tổ quốc, bảo vệ nhân dân, không phải là bảo vệ Đảng, chế độ. Do vậy, cần “phi chính trị hóa” quân đội và công an. Họ còn xuyên tạc quan điểm đối tác, đối tượng; tìm cách chia rẽ mối quan hệ truyền thống giữa Việt Nam với các nước láng giềng, triệt để lợi dụng vấn đề biên giới, lãnh thổ để chống phá.

Trên kênh You Tube, các đối tượng dựng lên nhiều bộ phim, video với việc dùng kỹ thuật và công nghệ chỉnh sửa dữ liệu cũ, chỉnh sửa hình ảnh, cắt ghép, tạo bằng chứng và thông tin giả; tự bịa ra các bài phỏng vấn nhân vật, sự kiện, bịa đặt các trang hồ sơ liên quan đến các nhân vật nổi tiếng,

các nhà lãnh đạo, thân nhân của họ và kích thích trí tò mò của công chúng bằng những thứ gọi là “thông tin lẻ trái”, “thông tin bí mật”... để tuyên truyền các luận điệu xuyên tạc, bôi nhọ, nói xấu Đảng. Để thu hút người truy cập, trong giai đoạn đầu, những nhóm quản trị các trang web, các diễn đàn này đã cố gắng tổng hợp, đăng tải các tin tức từ nguồn báo chí chính thống và các nguồn tin từ nước ngoài theo kiểu “khách quan”. Khi đã thu hút được một số lượng công chúng truy cập thường xuyên, chúng trà trộn các thông tin xấu, độc theo tỷ lệ tăng dần cả về số lượng và mức độ bịa đặt, bóp méo sự thật, luận điệu phản động, sai trái cũng sẽ tăng dần. Chính vì thế, nhiều người truy cập mạng, đặc biệt là giới trẻ, chỉ đọc báo mạng thông qua đường dẫn (link) của bạn bè trên mạng xã hội, dễ dàng “mắc mưu” của các thế lực thù địch, dễ bị dẫn dắt và bị động trong việc tiếp nhận thông tin xấu, độc. Chịu sự tác động đó, trong thời gian gần đây đã xuất hiện một số trí thức, học sinh, sinh viên giảm sút lòng tin vào công cuộc đổi mới của đất nước do Đảng Cộng sản Việt Nam lãnh đạo.

Nhìn chung, lợi dụng ưu thế trên không gian mạng và sự thiếu hiểu biết của thế hệ trẻ về vấn đề dân tộc nói chung, vấn đề quốc phòng, an ninh, đối ngoại nói riêng, các nhóm đối tượng liên tục gieo rắc sự hoài nghi, khiến không ít sinh viên, lớp trẻ cảm thấy bi quan, chán nản, dẫn đến mất phương hướng chính trị, thậm chí phủ nhận đường lối, quan điểm của Đảng, làm giảm sút lòng tin vào Đảng, vào chế độ, tạo nguy cơ “tự diễn biến”, “tự chuyển hóa”. Với những thay đổi ngày càng tinh vi, phức tạp cả về thủ đoạn và sách lược để tác động và nắm được lực lượng thanh niên, và nhất là sinh viên - thế hệ

đang và sẽ là rường cột, là tương lai của đất nước, các thế lực chống phá cách mạng Việt Nam ở nước ngoài và lực lượng phản động trong nước đang từng bước thực hiện ý đồ “chiến thắng không cần chiến tranh”.

3. Một số biện pháp giáo dục, nâng cao nhận thức của sinh viên trong việc bảo vệ chủ quyền quốc gia trên không gian mạng hiện nay

Trước những diễn biến phức tạp của bối cảnh mới và cuộc đấu tranh trên lĩnh vực chính trị, tư tưởng, bảo vệ nền tảng tư tưởng, quan điểm của Đảng, cũng như vai trò và những tác động của không gian mạng đối với sinh viên... thì cách ứng xử của tuổi trẻ nói chung trên không gian mạng trước những luận điệu xuyên tạc của các thế lực thù địch là rất quan trọng, góp phần không nhỏ vào cuộc đấu tranh bảo vệ Tổ quốc, bảo vệ chủ quyền quốc gia, dân tộc. Để phát huy vai trò của sinh viên trên mặt trận này, cần lưu ý một số giải pháp sau:

Một là, giáo dục ý thức chính trị cho sinh viên.

Giáo dục ý thức chính trị cho sinh viên không chỉ dừng lại ở việc hình thành tư tưởng, kiến thức chính trị mà quan trọng hơn đó là hình thành niềm tin và phát huy hành động chính trị, tính tích cực chính trị trong đời sống chính trị - xã hội cho sinh viên. Đồng thời, thông qua đó hình thành thế giới quan khoa học, nhân sinh quan tích cực trong bản thân mỗi sinh viên. Giáo dục ý thức chính trị cho sinh viên là hoạt động tuyên truyền, giáo dục chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, chủ trương, đường lối, quan điểm của Đảng, chính sách, pháp luật của Nhà nước cùng với những

giá trị truyền thống của dân tộc, đạo đức, lối sống, thẩm mỹ cho sinh viên. Cần bồi dưỡng lý tưởng cách mạng, bản lĩnh chính trị vững vàng cho sinh viên, bảo đảm cho sinh viên đủ sức “miễn dịch” và có môi trường thuận lợi để đấu tranh phòng, chống quan điểm sai trái, xuyên tạc. Qua đó, hình thành thế giới quan khoa học, nhân sinh quan tích cực và phương pháp tư duy biện chứng, từng bước hoàn thiện tri thức, đạo đức, nhân cách, hành vi của mình; nâng cao nhận thức chính trị, củng cố niềm tin, bản lĩnh chính trị, định hướng các giá trị chính trị tích cực, phát huy tính tích cực chính trị của sinh viên trong hoạt động thực tiễn chính trị - xã hội.

Hai là, trang bị cho sinh viên các kỹ năng đấu tranh trên không gian mạng.

Cần đẩy mạnh công tác giáo dục, nâng cao nhận thức cho sinh viên về mạng xã hội, cách sử dụng mạng xã hội hợp lý. Động viên sinh viên tự học, tự trang bị các kiến thức, kinh nghiệm sống để nhận diện thông tin xấu, độc, hình thành khả năng phân tích trước các thông tin tràn lan trên mạng xã hội. Phát huy vai trò định hướng của cơ quan chính trị, tổ chức đoàn các cấp và tính tự giác của sinh viên khi tham gia mạng xã hội; đề ra cơ chế kiểm soát thông tin, loại bỏ các nội dung xuyên tạc, gây bất an trong dư luận trên mạng xã hội. Định kỳ tổ chức tập huấn, bồi dưỡng kỹ năng công tác đoàn và phong trào thanh niên để cán bộ đoàn, sinh viên tham gia đấu tranh chống “diễn biến hòa bình” trên lĩnh vực tư tưởng, văn hóa; đấu tranh trên không gian mạng,... Coi việc đấu tranh, phòng, chống hiệu quả âm mưu, thủ đoạn “diễn biến hòa bình”, chống lại các quan

điểm xuyên tạc chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, tạo ra hệ “miễn dịch” đối với mọi thông tin sai trái, xấu, độc của các thế lực thù địch là thước đo kết quả xây dựng bản lĩnh chính trị của đoàn viên, thanh niên.

Ba là, tuyên truyền, giáo dục sinh viên luôn đề cao cảnh giác cách mạng, tích cực phát hiện, đấu tranh ngăn chặn, đẩy lùi các tư tưởng phản động và hành động sai trái, xấu, độc trên không gian mạng liên quan đến vấn đề chủ quyền quốc gia - dân tộc.

Mục đích của biện pháp này nhằm hạn chế tối đa những tác hại của thông tin xuyên tạc ảnh hưởng đến nhận thức của sinh viên, đồng thời củng cố niềm tin, góp phần bảo vệ chủ quyền quốc gia, kiên định mục tiêu độc lập dân tộc và chủ nghĩa xã hội, tạo ra sức đề kháng trước những luận điệu tuyên truyền xuyên tạc, kích động của các thế lực thù địch trên internet, mạng xã hội. Cần chú trọng kết hợp hiệu quả vừa cung cấp thông tin có tính định hướng, tính chính thống, vừa cung cấp đậm nét các thông tin mang tính chiến đấu trực diện với các quan điểm sai trái. Bên cạnh đó, cần thường xuyên nắm chắc dư luận, kịp thời cung cấp thông tin, định hướng nội dung, hình thức, biện pháp đấu tranh...

Bốn là, chủ động tuyên truyền những thông tin chính thống về chủ quyền quốc gia trong phạm vi năng lực cho phép của sinh viên trên không gian mạng.

Việc tuyên truyền có thể sử dụng linh hoạt dưới nhiều hình thức khác nhau như: bài viết, bài phân tích, chia sẻ, lồng ghép trong các câu chuyện tuyên truyền, tuyên giáo trên internet và mạng xã hội (thông qua các tài khoản, fanpage,

group... trên Facebook, Zalo,...), hướng đến nhiều đối tượng với đặc thù về trình độ nhận thức khác nhau.

Năm là, coi trọng xây dựng lực lượng nòng cốt trong thanh niên, sinh viên để chủ động đấu tranh bảo vệ chủ quyền quốc gia trên không gian mạng.

Một số gợi ý cho đội ngũ này bao gồm: tập trung vào đội ngũ cán bộ trẻ trong những cơ quan nghiên cứu, giảng dạy lý luận chính trị, khoa học xã hội và nhân văn; sinh viên hoạt động trên các lĩnh vực báo chí, xuất bản, văn hóa, nghệ thuật... Theo đó, cần lựa chọn những sinh viên có bản lĩnh chính trị vững vàng, có trình độ lý luận chính trị và khả năng diễn đạt các vấn đề cần lên tiếng nói,... để động viên, khích lệ họ chủ động tham gia đấu tranh chống các quan điểm sai trái, bảo vệ chủ quyền quốc gia - dân tộc. Để phát huy vai trò của lực lượng này, phải có cơ chế cung cấp thông tin kịp thời, phương tiện tác nghiệp phù hợp và có những chính sách hợp lý.

*

* *

Xây dựng chủ nghĩa xã hội đi đôi với bảo vệ Tổ quốc Việt Nam xã hội chủ nghĩa là một quy luật của cách mạng Việt Nam, thể hiện một cách sinh động quy luật “dựng nước phải gắn liền với giữ nước” của dân tộc ta. Bảo vệ chủ quyền quốc gia là một tất yếu khách quan trong quá trình đấu tranh và phát triển đất nước. Đấu tranh, phản bác, phòng, chống các quan điểm sai trái, thù địch trong tình hình hiện nay là cuộc chiến hết sức khó khăn, phức tạp, là trách nhiệm của toàn

Đảng, toàn dân và toàn quân, trong đó, đoàn viên, thanh niên - sinh viên Việt Nam là một trong những lực lượng quan trọng. Các tổ chức Đoàn Thanh niên, Hội Sinh viên Việt Nam cần tích cực tuyên truyền, giáo dục, rèn luyện, nâng cao nhận thức, lập trường cách mạng, ý thức chính trị cho sinh viên. Đồng thời, bản thân mỗi sinh viên cần ra sức học tập, nghiên cứu lý luận chính trị để góp phần bảo vệ Đảng, Nhà nước, nhân dân, bảo vệ chế độ xã hội chủ nghĩa, bảo vệ chủ quyền và lợi ích của quốc gia - dân tộc.

CÔ ĐƠN TRÊN MẠNG VÀ NGUY CƠ BỊ TỘI PHẠM CÔNG NGHỆ CAO TẤN CÔNG TRONG GIỚI TRẺ Ở VIỆT NAM HIỆN NAY

ThS.NCS. PHAN DUY ANH*

Trong tiến trình phát triển của lịch sử nhân loại, có thể khẳng định rằng, khoa học, kỹ thuật, công nghệ đóng vai trò quan trọng và tạo nên những bước đột phá, tác động mạnh mẽ đến xã hội loài người. Những phát minh của con người từ viên đá lửa cho đến các công cụ bằng kim loại, động cơ hơi nước, năng lượng điện cho đến máy tính điện tử, mạng internet, trí tuệ nhân tạo... đều là nền móng, trụ cột cho sự phát triển của tất cả các ngành và lĩnh vực. Nhờ sự tiến bộ đó mà con người trở nên giàu có, khỏe mạnh và sống lâu hơn. Nhưng cũng chính sự phát triển của khoa học công nghệ đem đến cho con người những thách thức rất lớn cần phải vượt qua. Đặc biệt trước bối cảnh sự phát triển nhanh chóng của Cách mạng công nghiệp lần thứ tư hiện nay đang dần lộ diện những rủi ro và các nguy cơ tiềm ẩn, mà trong đó đáng báo động là sự gia tăng tội phạm sử dụng công nghệ cao tấn công vào giới trẻ.

* Trường Đại học Bách khoa, Đại học Quốc gia Thành phố Hồ Chí Minh.

Và một trong những nguyên nhân chính của nguy cơ này là sự cô đơn trên mạng xã hội của họ.

1. Cô đơn trên mạng - hiện trạng công nghệ cách ly xã hội và giới trẻ

Tiến bộ công nghệ là chuyện tất yếu, thường được ưa chuộng và mang lại lợi ích cho con người, nhưng nhất định nó đi kèm theo một cái giá nào đó; rõ ràng nhất là tác động của mạng xã hội - một sản phẩm từ sự đi lên của công nghệ. Thế kỷ XXI là thế kỷ của khoa học công nghệ nhưng cũng chính trong một thế giới mà công nghệ phát triển như vũ bão, con người - đặc biệt là những người trẻ - rất dễ mắc phải tình trạng cô đơn kéo dài. Đây không phải là một nhận định vô căn cứ. Đối với giới trẻ, một hiện tượng dễ thấy trong cuộc sống của họ hiện nay là tình trạng cả ngày gắn liền với điện thoại di động và máy tính. Công nghệ mới tác động giúp con người thực hiện mọi thứ đơn giản, nhanh chóng và hiệu quả hơn. Nhưng nó cũng làm thay đổi cách giao tiếp và mối liên kết giữa cá nhân với cá nhân. Do đặc tính đơn giản và tiện lợi, con người đang có xu hướng giao tiếp với nhau không qua tiếp xúc trực tiếp mà thông qua các phương tiện liên lạc trực tuyến. Cách giao tiếp truyền thống với những mối quan hệ thân quen, gần gũi chuyển sang dạng các liên kết xã hội lỏng lẻo hơn, con người gắn bó với các thiết bị di động mang theo hơn là với con người. Thêm vào đó, với ý thức về sự riêng tư trong giới trẻ rất cao dẫn tới sự biệt lập với xã hội, sống ảo gia tăng¹.

1. Xem Nguyễn Văn Bình (Chủ biên): *Chủ trương, chính sách của Việt Nam chủ động tham gia cuộc cách mạng công nghiệp lần thứ tư*, Nxb. Đại học Kinh tế quốc dân, Hà Nội, 2019, tr.60.

Việt Nam được đánh giá là một trong những quốc gia có số dân tham gia kết nối trực tuyến lớn nhất tại khu vực ASEAN. Đây là điều kiện lý tưởng để cho các mạng xã hội xuất hiện và nhanh chóng phổ biến. Tính đến năm 2020, trong hơn 30 triệu người sử dụng internet tại Việt Nam, có khoảng 87,5% đã và đang sử dụng các mạng xã hội, nằm trong độ tuổi 15 - 34 (khoảng 71%). Các trang mạng xã hội được giới trẻ Việt Nam sử dụng nhiều như Facebook, Instagram, YouTube..., trong đó, Facebook được sử dụng nhiều nhất. Chỉ tính riêng ở Thành phố Hồ Chí Minh, qua khảo sát 1.000 bạn trẻ (11 - 35 tuổi), có đến 89,3% dùng Facebook; sau Facebook là YouTube với tính năng xem và chia sẻ video với 56,3% người dùng; đứng thứ ba là Instagram (24,5%) chuyên xem và chia sẻ ảnh; Zingme (16,8%) hỗ trợ chơi game, nghe nhạc trực tuyến; các mạng Viber, Zalo chiếm tỷ lệ 10%. Phần lớn thanh, thiếu niên đã sử dụng mạng xã hội trên 4 năm (43,8%), chiếm tỷ lệ cao thứ hai là từ 2 - 4 năm (34,2%), từ 1 - 2 năm (17,5%) và dưới 1 năm chiếm tỷ lệ thấp nhất (4,5%)¹.

Hiện nay, giới trẻ đang dùng mạng xã hội thông qua các công cụ điện tử để giao tiếp ở bất kỳ đâu có thể kết nối mạng internet. Những cuộc giao tiếp điện tử này thực chất là quá trình truyền đạt thông tin với những người đang không ở cùng họ. Nhu cầu giao tiếp này ám ảnh giới trẻ đến nỗi “đường như họ coi trọng việc nói chuyện với người không

1. Xem Đỗ Thị Phương Anh: “Nâng cao tính tích cực của mạng xã hội cho giới trẻ”, <https://tapchicongthuong.vn>.

có mặt hơn là người thực sự có mặt xung quanh họ”¹. Có thể thấy phổ biến tình trạng này ở các quán cà phê, nơi mà những người bạn đang ngồi với nhau nhưng lại cầm trên tay những chiếc điện thoại để nói chuyện, giao tiếp với người khác không ở đó. Ai cũng biết sự kết nối bằng giọng nói, hình ảnh và cảm xúc không chỉ là những nhu cầu của người lớn tuổi mà còn tuyệt đối quan trọng giữa cha mẹ và con cái để hình thành sợi dây gia đình và kích thích sự phát triển tâm hồn cho giới trẻ. Nhưng những cuộc giao tiếp trên các thiết bị điện tử trong cuộc sống hiện đại không mang lại được những điều đó. Việc đắm mình trong những cuộc trò chuyện trên mạng xã hội khiến cho sự xa cách giữa cha mẹ và con trẻ ngày càng tăng. Phần ảo được tạo ra đi cùng với sự ra đời của công nghệ và mạng xã hội. Và phần ảo đang dần chiếm mất thời gian cho phần thực, tâm trí giới trẻ dường như nằm phần nhiều ở đó.

Sống trong thế giới ảo đó có tốt cho giới trẻ hay không? Ở trên không gian đó, người trẻ có thể kết nối rộng hơn, nhanh hơn nhưng cần phải thấy rằng “người trẻ tuổi mong manh hơn và ít trải đời hơn những người trưởng thành, bởi thế càng dễ bị rơi vào những sai lầm, lạc lối và chưa được chuẩn bị cho những tác động tiêu cực của thời đại giao tiếp bằng công nghệ điện tử”². Sự cô lập khỏi những mối dây liên lạc trực diện giữa người với người sẽ phá hủy khả năng giao tiếp xã hội lâu bền của tất cả mọi người liên quan, và nó đang là một cái bẫy phân cách ngày càng lớn với những người

1, 2. Peter Townsend: *Mặt trái của công nghệ (bản dịch)*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2018, tr.387, 390.

cảm thấy bất an, thương tổn, hoặc với những người xuất thân từ gia đình không có một định hướng nhất định về sử dụng mạng xã hội. Có thể nói, cảm giác ban đầu của giới trẻ khi hòa nhập vào thế giới ảo thường là sự hồ hởi, phấn khích và tự hào khi thấy mình giờ đây đã trở thành một cư dân mạng, là thành viên của một cộng đồng được hình thành dựa trên những thành quả trí tuệ đầy ấn tượng của con người đương đại. Nhưng càng “đắm mình” vào các góc ngách của nó thì lại càng thấm thía sự vô danh, sự cô đơn của một cá thể.

2. Thực trạng tội phạm công nghệ cao tấn công vào giới trẻ hiện nay

Tội phạm sử dụng công nghệ cao là một trong những loại tội phạm mới xuất hiện khoảng một thập niên gần đây, nhưng do sự phát triển vượt bậc của khoa học công nghệ, đặc biệt là mạng internet, đã làm nảy sinh, tồn tại và phát triển nhanh chóng loại tội phạm này tại Việt Nam. Đây là loại tội phạm có sử dụng những thành tựu mới của khoa học - kỹ thuật và công nghệ hiện đại làm công cụ, phương tiện để thực hiện hành vi phạm tội một cách cố ý hay vô ý, gây nguy hiểm cho xã hội.

Bốn yếu tố cấu thành loại tội phạm có sử dụng công nghệ cao có thể thấy: (1) Về chủ thể: ngoài yêu cầu chung của chủ thể do Bộ luật hình sự quy định, điều đặc trưng ở đây là chủ thể của loại tội phạm này luôn có trình độ nhất định về công nghệ cao và sử dụng nó như một điều kiện cần để thực hiện hành vi phạm tội; (2) Về khách thể: khách thể bị xâm hại là quyền và lợi ích hợp pháp của các cá nhân, tổ chức, sự ổn định của xã hội, được quy định trong

Bộ luật hình sự, làm ảnh hưởng đến an ninh quốc gia và trật tự, an toàn xã hội; (3) Về chủ quan: hành vi luôn được thực hiện dưới hình thức là lỗi cố ý trực tiếp. Động cơ phạm tội chủ yếu là vụ lợi (ngoại trừ một số hoạt động phạm tội xâm phạm an ninh quốc gia); (4) Về khách quan: cũng tồn tại những hành vi phạm tội truyền thống như lừa đảo, trộm cắp, đánh bạc, khủng bố, tống tiền, mại dâm... và nhóm hành vi được Bộ luật hình sự năm 1999 quy định về tội phạm máy tính (gồm 3 nhóm hành vi quy định tại Điều 224, 225, 226 và Điều 226a, 226b theo Bộ luật hình sự sửa đổi, bổ sung năm 2017). Ngoài ra còn phát sinh một loạt các hành vi mới cần bổ sung vào luật như sử dụng trái phép thông tin¹...

Một thực trạng báo động ở Việt Nam hiện nay, có đến 70% tội phạm sử dụng công nghệ cao là người trẻ, chủ yếu từ 18 - 30 tuổi². Do hiểu rõ tâm lý và thói quen sử dụng mạng xã hội của giới trẻ nên đối tượng mà tội phạm sử dụng công nghệ cao nhắm đến thường là các bạn trẻ vừa ra trường, đang manh nha khởi nghiệp, hoặc học sinh, sinh viên muốn có việc làm thêm để trang trải chi phí học tập, sinh hoạt và những bạn trẻ thích “có tiền từ trên trời rơi xuống”... Theo đó, phổ biến nhất hiện nay là các đối tượng lừa đảo thông qua những thông tin của nạn nhân chia sẻ trên mạng xã hội đã giả mạo thành nhân viên các nhà mạng

1. Xem Đào Văn Vạn: “Nhận diện tội phạm có sử dụng công nghệ cao”, Tạp chí *Khoa học Cảnh sát nhân dân*, số 11, 2015, tr.24.

2. Xem Chu Miên: “70% tội phạm công nghệ cao là người trẻ tuổi”, 2015, <https://vov.vn>.

VNPT, FPT... hoặc giả mạo cán bộ công an, viện kiểm sát... để gọi điện thoại, lừa nạn nhân chuyển tiền cho chúng. Không chỉ vậy, các đối tượng lừa đảo sau khi chiếm được tài khoản mạng xã hội của một người nào đó, sẽ dùng tài khoản này để nhắn tin đến bạn bè, người thân của người đó để nhờ mua card điện thoại. Nhiều người vì tin đó là bạn bè, người thân của mình thật nên đã mua card gửi cho các tài khoản này và đã bị mất rất nhiều tiền. Bên cạnh đó, tội phạm công nghệ cao còn sử dụng các ứng dụng “Ai hay theo dõi bạn? Ai là bạn thân nhất của bạn?” trên mạng xã hội để lừa đảo và đánh cắp các thông tin cá nhân của người dùng, bao gồm cả những thông tin nhạy cảm như: thẻ tín dụng, hình ảnh cá nhân... và có thể còn bị chiếm tài khoản mạng xã hội để thực hiện các hành vi lừa đảo khác. Đây là những biểu hiện của nhóm tội phạm truyền thống có sử dụng công nghệ cao; là các hành vi phạm tội đã được quy định trong Bộ luật hình sự nhưng đối tượng không theo các phương thức thủ đoạn đã được biết trước đây mà sử dụng công nghệ hiện đại như máy tính, mạng máy tính, mạng viễn thông, mạng internet để thực hiện hành vi phạm tội. Những tội này được áp dụng xử lý theo Điều 139 về tội lừa đảo chiếm đoạt tài sản và Điều 138 tội trộm cắp tài sản của Bộ luật hình sự.

Thêm một hình thức phạm tội sử dụng công nghệ cao nữa là các đối tượng gửi cho những người trẻ tuổi sử dụng mạng xã hội những đường link clip, hình ảnh nóng. Chúng thường xuất hiện dưới dạng các comment kèm theo link bên dưới các bài viết trong các group. Nạn nhân vì tò mò mà bấm vào, dẫn đến bị chiếm đoạt tài khoản Facebook và thông tin cá nhân. Chưa kể đường link đó còn kèm theo yêu cầu cài đặt phần mềm

như Flash Player mà nếu nạn nhân cài vào máy thì sẽ bị kiểm soát cả máy tính, mất các thông tin, tài liệu quan trọng lưu trữ trong máy tính. Đây là biểu hiện của nhóm tội phạm máy tính và mạng máy tính. Nhóm này được đặc trưng bởi mục tiêu tấn công là cơ sở dữ liệu của máy tính, hoặc mạng máy tính, trong đó những hành vi chủ yếu là: tạo ra và lan truyền, phát tán các chương trình virus tin học; đột nhập trái phép cơ sở dữ liệu của máy tính, trộm cắp dữ liệu, thông tin (đặc biệt là thông tin về quốc gia, an ninh, quốc phòng), tấn công từ chối dịch vụ (DDOS-botnet), sử dụng trái phép dữ liệu, đưa thông tin trái phép lên mạng, khai thác trái phép mạng máy tính... Xem xét trong Bộ luật hình sự sửa đổi, bổ sung năm 2017 có 4 tội danh thuộc nhóm này là: 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).

3. Một số giải pháp ngăn ngừa tội phạm sử dụng công nghệ cao tấn công giới trẻ trong thời đại Cách mạng công nghiệp lần thứ tư

Hiện nay, các hành vi phạm tội sử dụng công nghệ cao ngày càng tinh vi, đe dọa tới độ an toàn thông tin có thể đến từ nhiều nơi, theo nhiều cách của giới trẻ nói riêng và an ninh thông tin quốc gia nói chung. Dự báo diễn biến của

tình hình tội phạm do tội phạm công nghệ cao thực hiện tại Việt Nam sẽ ngày càng phức tạp cả về số vụ, số đối tượng phạm tội. Về cơ cấu tình hình tội phạm theo đơn vị hành chính, không chỉ xuất hiện, tập trung tại các thành phố lớn như Thành phố Hồ Chí Minh, Hà Nội mà sẽ còn rộng ra nhiều tỉnh, thành phố khác trên quy mô cả nước; cũng không chỉ tập trung ở các đô thị mà phát triển về các vùng thôn quê, huyện lỵ. Sự xuất hiện, gia tăng, phát triển của tội phạm có sử dụng công nghệ cao để phạm tội, theo quy luật: Ở đâu có hạ tầng công nghệ thông tin phát triển, sự gia tăng mật độ dân cư, có tốc độ tăng trưởng về kinh tế, có số lượng người sử dụng internet gia tăng, độ phân hóa giàu, nghèo cao... nơi ấy sẽ xuất hiện tội phạm công nghệ cao và sẽ có sự gia tăng nhanh đối với loại tội phạm này. Tuổi của người phạm tội có sử dụng công nghệ cao để phạm tội có xu hướng trẻ hóa nhanh, hiện tập trung ở lứa tuổi từ 18 đến 30 tuổi, sẽ chuyển dần sang từ 18 đến 25 tuổi. Người phạm tội có trình độ học vấn cao sẽ chiếm tỷ lệ cao, sinh viên các trường đại học, cao đẳng, một số đã tốt nghiệp nhưng chưa có việc làm, việc làm không ổn định sẽ là những đối tượng phạm tội tiềm năng. Đối tượng tấn công của tội phạm công nghệ cao vẫn sẽ là giới trẻ và mở rộng thêm nhiều đối tượng khác. Chính vì vậy, việc đưa ra các chính sách và phương pháp để phòng đối tượng này trong giới trẻ là điều cần thiết.

Trước hết, cần nâng cao chất lượng tuyên truyền, giáo dục nhận thức, trách nhiệm cho nhân dân, trước hết là sinh viên, học sinh khi sử dụng mạng xã hội. Để thực hiện tốt nội dung này, các cấp cần đổi mới nội dung, hình thức, phương pháp tuyên truyền, giáo dục cho phù hợp với từng đối tượng,

làm cho họ nhận thức và thực hiện tốt đường lối, chủ trương của Đảng, chính sách, pháp luật của Nhà nước về quyền tự do thông tin, tự do báo chí, công tác quản lý, sử dụng internet và mạng xã hội. Trọng tâm là: Chỉ thị số 46-CT/TW, ngày 27/7/2010 của Ban Bí thư (khóa X) về “Chống sự xâm nhập của các sản phẩm văn hóa độc hại gây hủy hoại đạo đức xã hội”; Nghị quyết số 33-NQ/TW, ngày 09/6/2014 của Hội nghị lần thứ 9 Ban Chấp hành Trung ương Đảng (khóa XI) “Về xây dựng và phát triển văn hóa, con người Việt Nam đáp ứng yêu cầu phát triển bền vững đất nước”, Luật báo chí năm 2016; Luật tiếp cận thông tin năm 2016; Luật an ninh mạng năm 2018 và các bộ luật, luật liên quan. Quá trình thực hiện, cần làm thường xuyên, liên tục, phối hợp, phát huy sức mạnh tổng hợp của các tổ chức trong hệ thống chính trị, hệ thống thông tin, truyền thông từ trung ương đến cơ sở; kết hợp giáo dục, tuyên truyền theo chuyên đề với chủ đề, giáo dục trong nhà trường và gia đình, các loại hình truyền thông, thông tin từ truyền thống đến hiện đại cho phù hợp với không gian, thời gian và đối tượng, v.v. Qua đó, góp phần nâng cao nhận thức, trách nhiệm tuân thủ pháp luật, quy tắc xã hội, xây dựng phong cách văn hóa cho các đối tượng khi tham gia mạng xã hội; đồng thời, ngăn chặn, vô hiệu hóa những thông tin xấu, độc, hành vi phản cảm, thiếu văn hóa.

Thứ hai, để bảo vệ chính mình và người thân trước tội phạm công nghệ cao, giới trẻ phải biết bảo vệ thông tin cá nhân trên không gian mạng. Không chia sẻ các thông tin cá nhân như: họ và tên, địa chỉ, số điện thoại, địa chỉ email, số tài khoản ngân hàng, mã OTP..., vì đây chính là những kẻ hở ban đầu để các đối tượng xây dựng “kịch bản” đưa người trẻ

vào bẫy của chúng. Đối với người dùng mạng xã hội, không nên kết giao với người lạ, nhất là đối tượng là người nước ngoài khi chưa có mối quen biết. Đặc biệt, không cung cấp bất kỳ thông tin nào cho những số điện thoại lạ gọi đến. Không trao đổi và thực hiện theo các yêu cầu từ những số điện thoại không quen biết hay giới thiệu là nhân viên giao hàng, nhân viên bưu điện...

Thứ ba, cần tiếp tục kiện toàn tổ chức, lực lượng chức năng nhằm phát hiện, đấu tranh phòng, chống các tội phạm sử dụng công nghệ cao, thường xuyên bồi dưỡng, bổ sung và nâng cao kiến thức chuyên môn, nghiệp vụ cùng kiến thức tin học, ngoại ngữ cho cán bộ thực thi công tác.

Thứ tư, tiếp tục hoàn thiện hệ thống chính sách, pháp luật về phòng, chống tội phạm công nghệ cao, trong đó chú trọng cần nghiên cứu sửa đổi, bổ sung Bộ luật hình sự, Bộ luật tố tụng hình sự, pháp luật về các biện pháp phòng, chống tội phạm công nghệ cao và một số đạo luật có liên quan khác. Tiếp tục mở rộng quan hệ đối ngoại và tăng cường hợp tác quốc tế về phòng, chống tội phạm sử dụng công nghệ cao. Trong thời đại Cách mạng công nghiệp 4.0 và sự phát triển vượt trội của công nghệ thông tin và trí tuệ nhân tạo, công nghệ phát triển đã khiến cho những giao dịch được thực hiện không cần giấy tờ như trước đây. Việc tạo ra các tiêu chuẩn mới về tốc độ, hiệu quả và độ chính xác trong thông tin liên lạc, đã trở thành công cụ quan trọng để thúc đẩy đổi mới sáng tạo và tăng năng suất tổng thể. Bên cạnh đó, máy tính được sử dụng rộng rãi để lưu trữ dữ liệu bảo mật về chính trị, xã hội, kinh tế hoặc thông tin cá nhân đã mang lại lợi ích to lớn cho xã hội. Không gian mạng trở thành

một phần của lãnh thổ quốc gia, một phần không gian sống của con người. Cùng với đó, sự phát triển nhanh chóng của công nghệ internet và máy tính trên toàn cầu đã dẫn đến sự phát triển của các hình thức tội phạm xuyên quốc gia, đặc biệt là tội phạm liên quan đến internet. Những tội phạm này hầu như không có ranh giới và có thể ảnh hưởng đến bất kỳ quốc gia nào trên toàn cầu. Do đó, cần nâng cao nhận thức và ban hành khung khổ pháp luật cần thiết ở tất cả các quốc gia để phòng ngừa các tội phạm sử dụng công nghệ cao.

Mạng xã hội ra đời tạo một bước ngoặt lớn trong giao tiếp gián tiếp. Với sự hấp dẫn của mình, mạng xã hội trở thành một bộ phận không thể thiếu trong đời sống của giới trẻ Việt Nam hiện đại. Bên cạnh những tác động tích cực, mạng xã hội dường như cũng làm cho một bộ phận giới trẻ cô đơn hơn. Chính điều này là nguy cơ khiến cho họ trở thành đối tượng tấn công của các tội phạm sử dụng công nghệ cao. Tội phạm sử dụng công nghệ cao gắn liền với sự bùng nổ của công nghệ thông tin và viễn thông. Cùng với xu thế mới của thời đại, tội phạm sử dụng công nghệ cao sẽ tiếp tục gia tăng. Chính vì vậy, cần tổ chức thực hiện một cách đồng bộ các giải pháp cơ bản trên đây nhằm nâng cao hiệu quả cuộc đấu tranh phòng, chống loại tội phạm này.

CỦNG CỐ AN TOÀN THÔNG TIN MẠNG THÔNG QUA VIỆC XÁC ĐỊNH TRÁCH NHIỆM CỦA CHỦ THỂ XỬ LÝ DỮ LIỆU

TS. NGUYỄN THỊ HOA*

Ngày nay, internet đã trở thành một phần của cuộc sống và xu hướng phát triển có thể nói là vượt qua sự tưởng tượng của con người¹. Nhờ có internet mà không gian mạng đã được hình thành và phát triển. Sự phát triển mạnh mẽ của hoạt động mạng cũng kéo theo một lỗ hổng đó là vấn đề về bảo đảm an ninh mạng. Một nghiên cứu đã chỉ ra rằng, an ninh mạng được xem là một vấn đề xã hội phức tạp vì hai lý do: *thứ nhất*, mạng internet là một nền tảng kỹ thuật không an toàn; *thứ hai*, do công nghệ thay đổi một cách nhanh chóng nên có thể tạo ra rất nhiều lỗ hổng cần phải khắc phục².

1. Khái niệm về an toàn thông tin

Khi xem xét về vấn đề này thì một nghiên cứu chỉ ra rằng, vấn đề an toàn thông tin thực tế là bảo vệ các thông tin khỏi sự

* Trường Đại học Luật Thành phố Hồ Chí Minh.

1. Xem Ionut-Daniel Barbu & Cristian Pasrariu: “Information security analyst profile”, 3 Int’l. J. Info. Sec. & Cybercrime 29, 2014.

2. Xem Jennifer Chandler: “Information security, contract and liability”, 84 CHI.-KEN L. Rev 841, 2010.

tiếp cận, sử dụng, công bố, cắt dán, tìm đọc, sửa đổi, theo dõi, lưu trữ hoặc phá hủy mà không được phép¹. Cách hiểu trên cũng đã được đưa vào trong Luật an toàn thông tin mạng của Việt Nam, theo đó tại khoản 1, Điều 3 của luật này quy định rằng “An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin”. Với quy định nêu trên thì vấn đề an toàn thông tin được đặt ra không chỉ để bảo vệ thông tin cá nhân - thông tin gắn với việc xác định danh tính của một người cụ thể - mà còn bảo vệ tất cả các thông tin khi được đưa lên hệ thống thông tin trên mạng. Việc bảo đảm an ninh ở đây được hiểu là thông tin trên mạng được bảo vệ để bảo đảm tính nguyên vẹn và không bị sử dụng, tiết lộ, cắt dán, sửa đổi hoặc phá hoại, theo dõi hoặc lưu trữ trái phép. Do đó, việc bảo đảm an toàn thông tin mạng sẽ đòi hỏi sự tham gia và trách nhiệm của rất nhiều chủ thể từ khâu đầu vào của thông tin đến vấn đề bảo đảm an toàn cho hệ thống vận hành, lưu trữ, truyền tải thông tin... Vậy, câu hỏi đặt ra là làm thế nào để có thể bảo đảm an ninh thông tin tốt nhất? Để trả lời cho câu hỏi này thì cần phải tìm hiểu đâu là nguyên nhân chính hoặc chủ yếu dẫn đến mất an toàn thông tin.

2. Nguyên nhân chủ yếu dẫn đến mất an toàn thông tin

Để tìm ra nguyên nhân thực sự của các sự cố mất an toàn thông tin mạng, cần làm rõ thực trạng của việc mất an ninh mạng hiện nay.

1. Xem Ionut-Daniel Barbu & Cristian Pasrariu: “Information security analyst profile”, 3 Int'l. J. Info. Sec. & Cybercrime 29, 2014.

a) Thực trạng mất an toàn thông tin mạng tại Việt Nam

Liên quan đến vấn đề này, một đoạn trích mang tính thời sự trên báo *Nhân Dân* rất đáng quan tâm như sau: “Theo báo cáo An ninh Website trong 9 tháng đầu năm 2020 của CyStack (công ty chuyên về lĩnh vực an ninh mạng), số cuộc tấn công vào các trang mạng tại Việt Nam là 3.041 vụ, xếp thứ 18 trong các quốc gia được khảo sát. Trong số này có nhiều website là trang chủ, cổng thông tin điện tử của các cơ quan, tổ chức nhà nước. Có thể dẫn ra một số sự vụ đáng chú ý như: năm 2016, tin tặc tấn công Hãng hàng không quốc gia Vietnam Airlines; năm 2018, tấn công website của Ngân hàng Thương mại cổ phần Ngoại thương Việt Nam (Vietcombank). Gần đây, theo thông tin từ Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an), một ngân hàng đã bị tin tặc tấn công gây tổn thất lên đến 44 tỷ đồng. Theo thống kê trên trang zone-h.org (nơi tin tặc thường khoe chiến tích), nhiều website tên miền Việt Nam vẫn đang bị nhóm Cuộc cách mạng của người Maroc (Morrocan Revolution) chiếm quyền kiểm soát. Thông tin trên cũng được chính Trung tâm Giám sát an toàn không gian mạng quốc gia (Cục An toàn thông tin - Bộ Thông tin và Truyền thông) xác nhận khi đơn vị này cho biết: Từ đầu năm 2021 đã có 163 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam”¹.

Ngoài ra, mới đây nhất, chúng ta cũng đã nghe đến rất nhiều vụ tấn công mạng, có thể kể đến như vụ việc

1. <https://nhandan.vn/binh-luan-phe-phan/bao-dam-an-toan-thong-tin-truoc-yeu-cau-chuyen-doi-so-636216/>, truy cập ngày 21/8/2021.

Ngân hàng MSB bị lộ 2 triệu dữ liệu khách hàng¹ hoặc vụ thông tin cá nhân của hơn 10.000 người bị rao bán bởi chủ thể có tài khoản “Ox1337xO”². Vậy, câu hỏi đặt ra đầu là nguyên nhân dẫn đến các sự cố mất an toàn thông tin mạng nêu trên?

b) Nguyên nhân của các sự cố mất an toàn thông tin mạng

Để tìm câu trả lời cho các sự cố mất an toàn thông tin mạng, cần tìm hiểu cách thức mà các loại tội phạm mạng đang thực hiện để có thể gây hại cho người dùng.

Theo nghiên cứu của Bộ Thông tin và Truyền thông thì cứ mỗi phút trên toàn cầu có khoảng 10.000 vụ tấn công mạng và từ đó đã đưa ra nhận định rằng “không ai sống trong môi trường mạng mà không có rủi ro bị tấn công”³. Theo cảnh báo của Tổ chức Cảnh sát hình sự quốc tế - Interpol thì tội phạm mạng đang không ngừng gia tăng với các phương thức mới và kỹ thuật hiện đại⁴. Mới đây nhất, Interpol cũng đã công bố khuyến cáo về tình hình tội phạm công nghệ thông tin năm 2021 tại khu vực châu Á⁵, trong đó có nêu các cách thức tội phạm mạng thường xuyên xảy ra như sau:

1. https://www.mic.gov.vn/mic_2020/Pages/TinTuc/146254/Ngan-hang-so--Xoay-chuyen-thach-thuc-thanh-co-hoi-but-toc.html, truy cập ngày 19/8/2021.

2. <https://vnisa.org.vn/ba-he-luy-voi-cac-nan-nhan-cua-vu-lo-thong-tin-10-000-nguoi-viet/>, truy cập ngày 19/8/2021.

3. “Trở thành cường quốc về an ninh mạng để có hòa bình”, <https://www.mic.gov.vn>, truy cập ngày 18/8/2021.

4. Xem <https://www.interpol.int>, truy cập ngày 18/8/2021.

5. Xem “Asean cyberthreat Assessment 2021-Key cyberthreat trends outlook from the Asean cybercrime operations Desk”, Interpol: [file:///Users/macbook/Downloads/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final%20\(1\).pdf](file:///Users/macbook/Downloads/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final%20(1).pdf), truy cập ngày 19/8/2021.

- Loại hình tội phạm mạng về làm mất an toàn hệ thống thư điện tử doanh nghiệp (Business e-mail compromise) là rất đáng quan tâm. Cụ thể, nhóm tội phạm mạng hướng mục tiêu đến các doanh nghiệp có các giao dịch chuyển khoản hoặc có nhà cung cấp ở nước ngoài hoặc nhiều nước khác nhau vì họ hay có địa chỉ email của các nhân viên chịu trách nhiệm chăm sóc khách hàng được công bố trên mạng hoặc các nhân viên cao cấp trong lĩnh vực tài chính hoặc liên quan đến hoạt động chi trả thông qua chuyển khoản. Những chủ thể này sẽ bị lừa đảo thông qua các công cụ như keylogger - một phần mềm nhỏ gọn có khả năng ghi lại mọi phím bấm mà người dùng đã bấm trên bàn phím để có được thông tin; hoặc thông qua việc mạo danh các chủ thể uy tín để gửi các tin nhắn (phishing) để người tiếp nhận tin tưởng thực hiện giao dịch theo yêu cầu.

- Loại tội phạm mạng thông qua phishing cũng có thể thực hiện bằng cách sử dụng email xác thực của một tổ chức kinh doanh hợp pháp để thay đổi người nhận từ đó lấy được những thông tin nhạy cảm như thẻ tín dụng, tài khoản ngân hàng. Các email giả mạo yêu cầu người nhận nhấp chuột vào đường dẫn (link) liên kết để cập nhật hồ sơ cá nhân của họ hoặc thực hiện một giao dịch. Sau đó, liên kết sẽ đưa nạn nhân đến một trang web giả mạo mà các thông tin được nhập sẽ được chuyển trực tiếp đến kẻ lừa đảo.

- Ngoài ra, có thể kể đến loại tội phạm dùng một mã độc (ransomware) để ngăn chặn hoặc hạn chế người dùng truy cập vào hệ thống mạng nào đó bằng cách khóa màn hình hoặc khóa tệp của người dùng nhằm đòi tiền chuộc. Có rất nhiều mã độc hiện đại, nổi bật có thể kể đến là loại mã độc

(crypto-ransomware) sẽ mã hóa một số tệp nhất định trên các hệ thống bị nhiễm và buộc người dùng phải trả tiền chuộc thông qua việc thanh toán trực tuyến (online) để có thể có được mật mã giải mã độc.

- Cách thức thứ tư mà tội phạm mạng hay sử dụng là đánh chặn dữ liệu của hoạt động thương mại điện tử để ăn trộm dữ liệu khách hàng từ các kho dữ liệu trực tuyến. Công cụ mà tội phạm sử dụng trong trường hợp này tương tự như một tài khoản tín dụng trực tuyến có khả năng quét các máy thanh toán ATM với một cách làm nổi bật nhất là thông qua công cụ theo dõi (JS-sniffer) mà tội phạm mạng cài vào website để lấy cắp dữ liệu người dùng như số thẻ thanh toán, tên, địa chỉ và mật mã thẻ.

- Cách thức năm của hoạt động tội phạm đó là cung cấp dịch vụ phục vụ cho tội phạm mạng (thường được gọi là Crimeware-as-a Service -CaaS). CaaS cho phép các tội phạm mạng với các nền tảng riêng của mình bán hàng hoặc cung cấp dịch vụ cho các tội phạm mạng khác thiếu kiến thức mạng nhưng có tiền để hỗ trợ cho các cuộc tấn công mạng.

- Cách thức cuối cùng được nhắc đến đó là việc xâm nhập của tội phạm mạng vào chính hệ thống thông tin mạng bị lỗi (fraud) của nạn nhân. Khi các loại tiền ảo phát triển thì hệ thống tội phạm cũng đã xâm nhập vào lĩnh vực này bằng cách kiếm tiền điện tử từ phần cứng của nạn nhân còn gọi là (Cryptojacking). Cụ thể, những kẻ tấn công mạng sẽ chạy một phần mềm đào tiền điện tử trên phần cứng máy tính của nạn nhân mà không được sự đồng ý của chủ thể này. Khi đó, tội phạm sẽ có được tiền điện tử để thu lợi nhuận còn

nạn nhân chịu chi phí điện gia tăng khiến máy chóng bị hư hỏng mà không biết.

Cũng trong báo cáo này, Interpol đã công bố số liệu: trong thời gian dịch bệnh Covid-19 diễn ra thì 59% tội phạm mạng đến từ phishing/scam/fraud; malware/ransomware là 36%; miền độc hại (malicious domains) là 22% và tin giả (fake news) là 14%.

Từ diễn biến về tình hình tội phạm mạng nêu trên có thể hiểu rằng nguyên nhân dẫn đến mất an toàn thông tin mạng chủ yếu là vì vấn đề kết cấu hạ tầng mạng không bảo đảm và tội phạm mạng có thể xâm nhập bất kỳ đâu từ các máy tính cá nhân đến các máy tính của doanh nghiệp hay cơ quan, tổ chức. Việc không bảo đảm kết cấu hạ tầng mạng này có thể do hai nguyên nhân - khách quan và chủ quan. Do đó, biện pháp đầu tiên và trước nhất để bảo đảm an toàn thông tin mạng đó là hoàn thiện kết cấu hạ tầng mạng. Đối với từng cá nhân cụ thể, nếu như kết cấu hạ tầng mạng của họ không bảo đảm thì sẽ gây thiệt hại cho chính bản thân mỗi người và thiệt hại có thể không trầm trọng so với thiệt hại từ các doanh nghiệp bị tấn công. Về vấn đề này thì ông Lê Quang Hà, Giám đốc sản phẩm Công ty An ninh mạng Viettel nhận định rằng, trường hợp lộ lọt số lượng lớn thông tin người dùng thường không phải xuất phát từ cá nhân riêng lẻ mà từ hệ thống lưu trữ, xử lý thông tin khách hàng của các tổ chức, doanh nghiệp¹. Ngoài ra, theo khuyến cáo của Phòng Thương mại quốc tế (ICC) thì hệ thống thông tin của các doanh nghiệp là tâm điểm cho các

1. Xem <https://vnisa.org.vn/ba-he-luy-voi-cac-nan-nhan-cua-vu-lo-thong-tin-10-000-nguoi-viet/>, truy cập ngày 19/8/2021.

hành vi phạm tội trong lĩnh vực an toàn thông tin¹. Vậy, câu hỏi đặt ra là có trách nhiệm của các tổ chức, doanh nghiệp hoặc người lao động của các chủ thể này khi để lộ thông tin cá nhân của khách hàng hay không?

3. Giải pháp hoàn thiện khung pháp lý để bảo đảm an toàn thông tin

Tìm kiếm giải pháp hoàn thiện cơ chế bảo đảm an toàn thông tin tại Việt Nam sẽ thuyết phục và hiệu quả hơn thông qua nghiên cứu kinh nghiệm của các nước phát triển.

a) Kinh nghiệm của nước ngoài nhằm bảo đảm an toàn thông tin mạng

Từ những phân tích ở trên cho thấy, các tổ chức, doanh nghiệp thường là đối tượng tấn công mạng và gây hậu quả nghiêm trọng đến các cá nhân và nền kinh tế. Liên quan đến việc mất an toàn thông tin thì một trong những thông tin mà xã hội rất quan tâm đó là thông tin về bí mật cá nhân. Trên cơ sở đó, Liên minh châu Âu đã ban hành Quy tắc số 2016/679, ngày 27/4/2016 liên quan đến việc bảo vệ các cá nhân trước việc xử lý các dữ liệu cá nhân và sự lưu thông tự do các dữ liệu cá nhân đó, và bãi bỏ Chỉ thị số 95/46/CE (được gọi tắt là Quy chế chung về bảo vệ dữ liệu cá nhân - GDPR) tại Điều 5 đặt ra những điều kiện để bảo đảm dữ liệu cá nhân. Trong đó, đáng chú ý tại điểm f, khoản 1, Điều 5 quy định: “Dữ liệu cá nhân cần phải được xử lý theo cách nhằm

1. Xem “Guide ICC de la cybersécurité à l'intention des entreprises” 2015: <https://iccwbo.org/content/uploads/sites/3/2016/11/ICC-Cyber-Security-Guidelines-for-Business-French-version.pdf>, truy cập ngày 21/8/2021.

bảo đảm an toàn phù hợp cho dữ liệu cá nhân trong đó có bao gồm việc bảo vệ chống lại các việc xử lý dữ liệu cá nhân không được cho phép hoặc bất hợp pháp cũng như chống lại việc đánh mất hoặc phá hoại hay bất kỳ thiệt hại nào mang tính tai nạn bằng việc trang bị về kỹ thuật cũng như tổ chức một cách phù hợp (với tính toàn vẹn và tính bí mật của dữ liệu)". Để bảo đảm cho việc thực hiện nghĩa vụ trên thì khoản 2, Điều 5 GDPR quy định rằng "Chủ thể được giao nhiệm vụ xử lý dữ liệu có trách nhiệm tôn trọng các quy định tại khoản 1 nêu trên và phải có năng lực chỉ ra rằng mình đã thực hiện trách nhiệm đó".

Tại Pháp, quy định này cũng đã được luật hoá tại Điều 35 Luật số 2018-493, ngày 20/6/2018 liên quan đến bảo vệ dữ liệu cá nhân, trong đó khẳng định việc xử lý dữ liệu cá nhân cần phải tuân thủ các quy định của GDPR nêu trên. Thực tế thì trước khi có quy định của GDPR, từ năm 2004, tại Điều 34 Luật thông tin và tự do được sửa đổi bởi Luật số 2004-801, ngày 06/8/2004 thì quy định về trách nhiệm của chủ thể xử lý thông tin cá nhân đã được đặt ra. Quy định này là sự luật hóa án lệ của Tòa án Pháp đã xét xử trước đó và cũng nhiều lần áp dụng tương tự từ sau khi luật nêu trên được ban hành. Cụ thể, Tòa án Pháp đã không ít lần quy trách nhiệm cho các doanh nghiệp trong việc để lộ dữ liệu, trong đó có dữ liệu cá nhân. Vụ việc đáng chú ý có thể kể đến là phán quyết của Tòa án tối cao của Pháp đã từng áp dụng quy định của Bộ luật hình sự tại Điều 226-16 và 226-17 quy định về phạt do lỗi bất cẩn cũng như cố ý trong quá trình xử lý dữ liệu cá nhân khi không tôn trọng những điều kiện tiên quyết trong quá trình

xử lý theo quy định của pháp luật có thể bị phạt 5 năm tù và phạt tiền lên tới 300.000 Euro. Trong vụ việc này, Tòa án tối cao đã ủng hộ quan điểm của Tòa phúc thẩm Paris tuyên phạt hai nhân viên của Công đoàn đa ngành của các dược sĩ trong lĩnh vực lao động của vùng Aix (gọi tắt là SIMTPA) tổng số tiền phạt là 80.000 franc vào năm 2002. Lý do tuyên phạt là do hai nhân viên của SIMTPA đã có thiếu sót trong việc thực hiện các biện pháp để bảo đảm an toàn cho dữ liệu cá nhân khi được giao nhiệm vụ xử lý dữ liệu. Cụ thể, hai nhân viên này đã không khóa hồ sơ dữ liệu bằng cách tạo mật mã để lưu trữ thông tin nhằm ngăn cản sự tiếp cận của người thứ ba¹.

Hướng giải quyết của Tòa án tối cao nêu trên và các quy định của pháp luật của Pháp cũng như của Liên minh châu Âu cũng được áp dụng tiếp sau đó không chỉ đối với việc bảo vệ dữ liệu cá nhân mà còn liên quan đến việc bảo vệ thông tin của các cơ quan, tổ chức khác. Cụ thể, vụ việc tại Tòa phúc thẩm Paris sau đó vào năm 2013 liên quan đến Văn phòng quốc gia về an toàn vệ sinh thực phẩm, môi trường và lao động (gọi tắt là ANSES). Những dữ liệu của chủ thể này đã bị lấy đi bởi các chủ tài khoản được xác định có địa chỉ tại Thụy Điển và Panama. Sau đó, các thông tin này được đưa lên mạng mà một chủ thể khác tại Pháp là Olivier có tài khoản tên Bluetouff tiếp cận được. Các thông tin lấy được đã được Oliver sử dụng làm cơ sở cho các lập luận trong bài nghiên cứu của mình và đã công bố bài báo. Sau đó, chủ thể này còn theo đường dẫn xâm nhập được mạng nội bộ của

1. Xem Cass. Ch. Crim. N. 99-82.136, 30 Octobre 2001.

ANSES và lấy được rất nhiều dữ liệu, chỉ khi đến phần dữ liệu đòi hỏi mật mã thì Olivier mới nhận ra rằng mình đã vào một trang mạng bí mật không nên vào và dừng lại tại đó. Khi đọc bài nghiên cứu được công bố bởi Olivier, ANSES đã nhận ra những số liệu nghiên cứu của cơ quan mình đã bị đánh cắp nên đã khởi kiện ra Tòa án Paris yêu cầu tuyên phạt Olivier về tội ăn trộm với số tiền phạt là 5.000 Euro kèm mức án tù treo. Tuy nhiên, Tòa phúc thẩm Paris cho rằng không có cơ sở để cho rằng Olivier phạm tội ăn trộm vì việc chủ thể này tiếp cận được thông tin là do lỗi của ANSES trong việc thực hiện các biện pháp cần thiết để bảo vệ sự toàn vẹn của dữ liệu và ngăn ngừa sự tiếp cận không được phép của bên thứ ba¹.

Từ các vụ việc trên và quy định pháp luật của Pháp và Liên minh châu Âu cho thấy các nước này đề cao vai trò bảo đảm thông tin của các chủ thể xử lý dữ liệu là rất thuyết phục. Vì nếu ngay tại khâu xử lý dữ liệu mà các chủ thể có trách nhiệm đã áp dụng các biện pháp cần thiết để bảo quản dữ liệu thì nguy cơ việc dữ liệu bị lộ và đánh cắp hay bị tiếp cận trái phép sẽ giảm thiểu đi rất nhiều. Do đó, đây chính là một cách làm rất khoa học đáng để chúng ta quan tâm. Vậy, câu hỏi đặt ra là Việt Nam có quy định của pháp luật về vấn đề này hay không?

a) Hoàn thiện pháp luật Việt Nam về bảo đảm an toàn thông tin

Tại Việt Nam, liên quan đến vấn đề bảo đảm an toàn thông tin, theo ông Nguyễn Ngọc Cường, Phó Cục trưởng

1. Xem C.A. Paris, Ch. 10, No. 13/04833, 5 février 2014.

Cục An ninh mạng và Phòng, chống tội phạm công nghệ cao cho rằng: “Tình trạng lộ bí mật nhà nước, lộ dữ liệu cá nhân trên không gian mạng tiếp tục được phát hiện tại nhiều cơ quan, đơn vị, doanh nghiệp. Nhiều hệ thống thông tin còn bọc lộ sơ hở, lỗ hổng trong cơ chế bảo mật do không được quan tâm và đầu tư đúng mức”¹. Và cũng theo ông Nguyễn Ngọc Cường thì một số văn bản quy phạm pháp luật có đề cập khía cạnh bảo vệ dữ liệu cá nhân nhưng chưa đầy đủ và thiếu chế tài đủ mạnh để xử lý vi phạm. Qua nghiên cứu thực tế của Việt Nam, vấn đề an ninh mạng thực sự đáng báo động mà chưa nhận được sự đánh giá đúng từ phía cơ quan áp dụng pháp luật. Có thể đó là lý do dẫn đến tình trạng như nhận định của ông Võ Đỗ Thắng, Giám đốc Trung tâm an ninh mạng Athena cho rằng, mặc dù có rất nhiều sai phạm trong việc để lộ thông tin nhưng “cho tới thời điểm hiện nay, hầu như chưa có trường hợp nào doanh nghiệp phải chịu trách nhiệm về việc để lộ thông tin cá nhân khách hàng, cho dù tình trạng thông tin cá nhân bị rò rỉ đã xảy ra rất nhiều trong ngành hàng không, thông tin di động, địa ốc, bảo hiểm nhân thọ”. Vậy đâu là sự chưa đầy đủ của pháp luật Việt Nam về vấn đề này?

Trách nhiệm của chủ thể xử lý dữ liệu trước khi có sự cố xảy ra. Khi nghiên cứu các quy định của pháp luật có liên quan, chúng tôi nhận thấy pháp luật của chúng ta chưa phù hợp, đặc biệt là đối với các doanh nghiệp, tổ chức chủ quản

1. <https://tinnhanhchungkhoan.vn/lo-thong-tin-ca-nhan-rao-ban-tren-mang-doanh-nghiep-phai-chiu-trach-nhiem-post250674.html>, truy cập ngày 20/8/2021.

xử lý dữ liệu cá nhân. Điển hình là quy định của chúng ta chỉ đặt ra trách nhiệm mang tính khuyến khích mà không đặt ra nghĩa vụ và chế tài để buộc các chủ thể liên quan phải thực hiện. Ví dụ, tại khoản 3, Điều 16 Luật an toàn thông tin mạng quy định “Tổ chức, cá nhân xử lý thông tin cá nhân phải xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin cá nhân của tổ chức, cá nhân mình”, nhưng quy định này không thể hiện rõ là “các biện pháp bảo vệ thông tin cá nhân” đó phải phù hợp và tương xứng với dữ liệu cũng như nguy cơ rủi ro.

Hơn nữa, luật cũng không quy định về trách nhiệm do cấu thả hoặc bất cẩn mà để lộ dữ liệu của các chủ thể này. Khi nghiên cứu các văn bản khác thì tại Điều 159 Bộ luật hình sự chỉ quy định về trách nhiệm cho chủ thể “cố ý” làm thất lạc thông tin mà không quy định đối với lỗi vô ý, cấu thả. Điều này là hoàn toàn khác đối với pháp luật của Pháp, trong đó Bộ luật hình sự nước này tại Điều 226-16 cho phép truy cứu trách nhiệm hình sự đối với cả lỗi “bất cẩn” (không phải cố ý) của chủ thể xử lý thông tin dẫn đến để lộ thông tin cá nhân thông qua việc không thực hiện các biện pháp cần thiết để bảo vệ sự toàn vẹn và chống lại việc tiếp cận không được phép đối với thông tin. Nếu chúng ta cho rằng, Việt Nam đã có quy định xử phạt hành chính về hành vi cấu thả dẫn đến để lộ thông tin cá nhân thì chế tài xử phạt cũng không đáng kể. Cụ thể, Nghị định số 15/2020/NĐ-CP, ngày 03/02/2020 của Chính phủ 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 (sau đây gọi tắt là Nghị định số 15/2020/NĐ-CP) tại điểm đ, khoản 3,

Điều 102 chỉ xử phạt 20.000.000 đồng đối với hành vi “Không thực hiện các biện pháp quản lý, kỹ thuật cần thiết để bảo đảm thông tin cá nhân không bị mất, đánh cắp, tiết lộ, thay đổi hoặc phá hủy khi thu thập, xử lý và sử dụng thông tin cá nhân của người khác trên môi trường mạng”. Nếu so sánh chế tài áp dụng giữa Việt Nam và Pháp thì có thể thấy chế tài phạt của chúng ta không có tính răn đe, ngăn ngừa hành vi phạm tội.

Trách nhiệm của chủ thể xử lý dữ liệu khi có sự cố mất an toàn thông tin. Ngoài quy định về chế tài áp dụng cho việc phòng ngừa sự cố mất an toàn thông tin thì chúng ta cũng cần lưu ý đến quy định về xử lý đối với sự cố an toàn thông tin. Lấy kinh nghiệm từ nước ngoài, ví dụ như khoản 1, Điều 33 GDPR của Liên minh châu Âu quy định rằng “khi có sự vi phạm đối với dữ liệu cá nhân, chủ thể chịu trách nhiệm về xử lý thông tin cá nhân phải thông báo về sự vi phạm này đối với cơ quan nhà nước có thẩm quyền trong thời hạn sớm nhất có thể và trễ nhất là 72 giờ kể từ ngày biết về sự cố trừ trường hợp sự cố liên quan không thể nào ảnh hưởng đến quyền và tự do của cá nhân”.

Tại Việt Nam, vấn đề về ứng phó đối với sự cố an toàn thông tin hiện nay được quy định bởi Thông tư số 20/2017/TT-BTTTT, ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc áp dụng cho cơ quan, tổ chức, cá nhân liên quan đến hoạt động điều phối, ứng cứu sự cố an toàn thông tin mạng nhưng chủ yếu quy định về quyền hạn và trách nhiệm của tổ chức tham gia ứng cứu sự cố thông tin mà không có quy định về chế tài khi vi phạm. Đối với các

doanh nghiệp kinh doanh thương mại điện tử, chúng ta có Nghị định số 52/2013/NĐ-CP, ngày 16/5/2013 của Chính phủ về thương mại điện tử, trong đó Điều 69 quy định nghĩa vụ công bố chính sách bảo vệ thông tin của người tiêu dùng nhưng không quy định về việc chính sách đó phải “tương xứng” với thông tin cũng như với nguy cơ rủi ro. Khoản 3, Điều 72 Nghị định nêu trên cũng quy định về nghĩa vụ của đơn vị lưu trữ phải thông báo về trường hợp hệ thống thông tin bị tấn công trong vòng 24 giờ sau khi phát hiện sự cố. Do đó, nếu các doanh nghiệp này không thông báo về sự cố an toàn thông tin có thể bị xử phạt hành chính nhưng mức phạt cũng không mang tính chất răn đe, cụ thể theo quy định tại điểm a, khoản 2, Điều 78 Nghị định số 15/2020/NĐ-CP quy định phạt tiền từ 20.000.000 đồng đến 30.000.000 đồng đối với hành vi “không báo cáo với cơ quan điều phối quốc gia khi tiếp nhận thông tin, phát hiện sự cố đối với hệ thống thông tin trong phạm vi quản lý”. Ngay cả khi áp dụng quy định xử phạt này thì cũng không rõ đây là trách nhiệm của doanh nghiệp có sử dụng mạng (chủ thể xử lý dữ liệu) hay áp dụng đối với tổ chức cung ứng dịch vụ mạng.

Từ những phân tích nêu trên cho thấy, pháp luật của Việt Nam liên quan đến an ninh mạng hiện nay còn rải rác, chưa thực sự đầy đủ và hiệu quả để bảo vệ quyền và lợi ích hợp pháp của các chủ thể khi tham gia vào các nền tảng mạng.

Trên đây chỉ là một trong những vấn đề bất cập trong hệ thống pháp luật bảo đảm an ninh mạng của Việt Nam hiện nay. Ngoài ra, cần lưu ý rằng, “tội phạm mạng là không có biên giới, nguy cơ và các cuộc tấn công mạng có thể đến từ

bất kỳ đâu và bất kỳ lúc nào”¹. Do đó, việc bảo đảm an ninh mạng không chỉ đòi hỏi chúng ta phải hoàn thiện kết cấu hạ tầng mạng cũng như khung pháp lý trong hệ thống pháp luật nội địa của quốc gia mình, mà còn phải gia tăng hợp tác quốc tế trong lĩnh vực này để có thể phòng, chống tội phạm mạng một cách tốt nhất. Đây cũng là một vấn đề cần quan tâm khi mà hiện nay, tại khu vực Đông Nam Á cũng như châu Á vẫn chưa có được một điều ước quốc tế chung để các nước thành viên phối hợp và hỗ trợ nhau trong phòng, chống tội phạm mạng.

1. <https://www.interpol.int/fr/Infractions/Cybercriminalite/Reponse-aux-cybermenaces>, truy cập ngày 22/8/2021.

NGUYÊN TẮC CẤM SỬ DỤNG VŨ LỰC VÀ ĐE DỌA SỬ DỤNG VŨ LỰC TRONG PHÁP LUẬT QUỐC TẾ VỚI HÀNH VI TẤN CÔNG MẠNG

TS. NGUYỄN THỊ THU TRANG*

NGUYỄN ĐAN CHI**

VÕ MINH THU***

DƯƠNG THỊ HOÀI THƯƠNG****

Tại Điều 2 (4) Hiến chương Liên hợp quốc về nguyên tắc cấm sử dụng vũ lực và đe dọa sử dụng vũ lực được thể hiện rõ: Pháp luật quốc tế cấm các quốc gia là thành viên của Liên hợp quốc sử dụng vũ lực và đe dọa sử dụng vũ lực với mục đích xâm phạm đến phạm vi lãnh thổ và nền độc lập chính trị của quốc gia khác hoặc trái với mục đích của Hiến chương Liên hợp quốc đề ra. Đây là một trong bảy nguyên tắc cơ bản của Luật quốc tế. Ngoài Điều 2 (4) Hiến chương Liên hợp quốc, nguyên tắc này còn được pháp điển hóa trong Hiệp ước Kellogg-Briand năm 1928, Tuyên bố của Đại hội đồng Liên hợp quốc năm 1970 và tại các điều ước quốc tế song phương và đa phương khác.

*, **, ***, **** Trường Đại học Kinh tế - Luật, Đại học Quốc gia Thành phố Hồ Chí Minh.

Với sự phát triển mạnh mẽ của khoa học công nghệ, một vấn đề phát sinh đó là các cuộc tấn công mạng xảy ra khắp nơi trên thế giới.

1. Khái niệm và ảnh hưởng của tấn công mạng

Hướng dẫn Tallinn về luật pháp quốc tế áp dụng cho chiến tranh mạng định nghĩa: “Tấn công mạng là hoạt động mạng, mang tính tấn công hay phòng thủ với mục đích gây thiệt hại về người và tài sản”¹. Còn T. Ivanjko và cộng sự cho rằng, tấn công mạng là cuộc tấn công trong không gian mạng với mục đích làm ảnh hưởng đến hệ thống máy tính hay mạng, đồng thời cũng ảnh hưởng đến các hệ thống vật lý khác². Điều 2 (8) Luật an ninh mạng Việt Nam năm 2018 định nghĩa rằng, tấn công mạng là hành vi phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử bằng không gian mạng, công nghệ thông tin hay các phương tiện điện tử khác. Như vậy, khái niệm tấn công mạng ở Việt Nam có điểm giống và khác so với những quan điểm đã viện dẫn ở trên. Nhìn chung, đây là hành vi xâm nhập, tác động tiêu cực trên không gian

1. The International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence: “*Tallinn Manual on the International Law applicable to Cyber warfare*”, Cambridge University Press, New York, the United State of America, 2013, p.92.

2. Xem I. Duić, V. Cvrtić & T. Ivanjko: *International cyber security challenges*, Croatian Radiotelevision, University of Applied Sciences Vrnjačka Banja, Zagreb, Croatia, 2017, p.1527.

mạng nhằm phá hoại hệ thống máy tính, mạng lưới, cơ sở dữ liệu, phương tiện điện tử với mục đích: (a) tuyên truyền hoặc lừa dối; (b) gây gián đoạn một phần hoặc toàn bộ máy tính, hệ thống máy tính hoặc mạng lưới được nhắm mục tiêu vào kết cấu hạ tầng vật lý do máy tính vận hành liên quan đến; (c) gây thiệt hại vật lý đến máy tính, hệ thống máy tính và mạng lưới¹.

Những vụ việc tấn công mạng đã “chạm tay” đến hầu hết mọi lĩnh vực trọng yếu trên khắp thế giới như: y tế, dịch vụ tài chính, giao thông vận tải, cung cấp nước, thực phẩm, nông nghiệp, năng lượng,... Từ thực tế hiện nay cho thấy, tấn công mạng đã thực sự là một mối đe dọa lớn trong nhiều lĩnh vực đối với các quốc gia, đơn cử như một số vụ việc:

Với hoạt động hàng không, vào chiều 29/7/2016, một cuộc tấn công mạng vào hệ thống thông tin của Tổng Công ty Hàng không Việt Nam với những câu chữ và hình ảnh xúc phạm Việt Nam và Philíppin, xuyên tạc các nội dung về Biển Đông. Vụ việc này không chỉ gây thiệt hại đối với ngành hàng không Việt Nam, mà còn ảnh hưởng đến quan hệ ngoại giao giữa Việt Nam với Trung Quốc và Philíppin.

Với hoạt động cung cấp nhiên liệu, ngày 07/5/2021 vừa qua, công ty vận hành hệ thống đường ống dẫn xăng/dầu lớn nhất nước Mỹ - Colonial Pipeline đã bị gián đoạn hoạt động bởi một vụ tấn công mạng, buộc họ phải đóng cửa toàn bộ mạng lưới cung cấp nhiên liệu từ các nhà máy lọc dầu của Mỹ. Vụ tấn công này được thực hiện thông qua phần mềm

1. Xem Oona A. Hathaway, Rebecca Crootof, P. Levitz, H.Nix & Julia Spiegel: *The Law of Cyber-Attack*, California Law Review, 2012.

Ransomware - một virus mã hóa độc hại rất được ưa chuộng trong các cuộc tấn công mạng suốt 5 năm trở lại đây¹.

Với hoạt động cung cấp lương thực, ngày 30/5/2021, hệ thống máy chủ và mạng máy tính của công ty cung cấp thịt lớn nhất thế giới JBS đã bị đánh sập bởi một cuộc tấn công mạng, khiến các hoạt động của họ ở Ôxtrâyli và khu vực Bắc Mỹ phải tạm ngừng, gây ra nhiều rắc rối cho thị trường thịt của châu Âu và châu Mỹ².

Với hoạt động quản lý hành chính, vào ngày 06/7/2021, mọi hoạt động dịch vụ xã hội của huyện Anhalt-Bitterfeld thuộc bang Sachsen-Anhalt của Đức đã bị đình trệ khi toàn bộ hệ thống quản lý hành chính của huyện bị tin tặc tấn công³.

Với hoạt động y tế, trong bối cảnh đại dịch Covid-19 diễn biến phức tạp và lây lan trên diện rộng, một làn sóng tin tặc tấn công mạng được cho là bắt đầu xuất hiện vào tháng 10/2020 đang gia tăng mạnh mẽ. Cụ thể, số vụ tấn công nhằm vào các cơ sở y tế trên toàn thế giới tăng 45%, cao gấp 2 lần mức tăng của các vụ tấn công mạng trên mọi lĩnh vực trong cùng một thời gian⁴.

1. Xem Văn Khoa: “Hệ thống đường ống nhiên liệu lớn nhất của Mỹ bị tấn công mạng “bất thường”, <https://thanhnien.vn>, truy cập ngày 31/7/2021.

2. Xem Ban thời sự: “Công ty sản xuất thịt lớn nhất thế giới bị tấn công mạng”, <https://vtv.vn>, truy cập ngày 31/7/2021.

3. Xem BT: “Đức lần đầu tiên ban bố tình trạng thảm họa mạng”, <https://www.antv.gov.vn>, truy cập ngày 31/7/2021.

4. Theo báo cáo của Công ty công nghệ Checkpoint Technologies của Ixraen: “Gia tăng tấn công mạng nhằm vào bệnh viện trên khắp thế giới”, <https://hanoimoi.com.vn>, truy cập ngày 31/7/2021.

Những vụ tấn công mạng vào các lĩnh vực trọng yếu đã thực sự gây ra nhiều khó khăn, tổn thất và thiệt hại đối với các nước, và tổn hại nặng nề nhất chính là nền kinh tế quốc gia. Mới đây, thông tin từ Báo cáo Viện tội phạm học Ôxtrâyliia cho biết mỗi năm người dân Ôxtrâyliia đã phải tốn 2,6 tỷ USD vào việc ngăn chặn tội phạm mạng và xử lý hậu quả của các cuộc tấn công mạng¹. Bên cạnh đó, những nguy hiểm tiềm ẩn đằng sau các vụ việc tấn công mạng có quy mô lớn chính là sự can thiệp của tin tặc vào hoạt động chính trị của các quốc gia. Đây có lẽ sẽ là vấn đề đáng được quan tâm và bảo vệ chặt chẽ nhất hiện nay, bởi chính trị là “đầu não” của một đất nước. Gần đây nhất vào chiều 06/7/2021, một cuộc tấn công mạng đã nhắm vào các trang thông tin điện tử của tổng thống, cơ quan an ninh và các cơ quan khác của Ucraina². Hay như cáo buộc gần đây của Mỹ và các nước đồng minh gồm NATO, EU, Anh, Canada, Ôxtrâyliia, Niu Dilân và Nhật Bản cho rằng Trung Quốc tấn công vào máy chủ Microsoft Exchange, nhằm đánh cắp thông tin và thực hiện hoạt động gián điệp mạng; theo Ngoại trưởng Mỹ Anthony, hành vi tấn công mạng của Trung Quốc là “mối đe dọa lớn đối với an ninh quốc gia” của các nước này³.

1. Xem Thông tấn xã Việt Nam: “Australia: Tội phạm mạng gây thiệt hại hàng tỷ USD mỗi năm”, <http://baovanhoa.vn>, truy cập ngày 01/8/2021.

2. Xem “Trang thông tin điện tử của cơ quan an ninh Ukraine bị tấn công”, <https://vietnamnet.vn>, truy cập ngày 01/8/2021.

3. Xem “Mỹ và một loạt đồng minh tố Trung Quốc tiến hành tấn công mạng”, <https://cand.com.vn>, truy cập ngày 01/8/2021.

2. Cơ sở áp dụng nguyên tắc cấm sử dụng vũ lực và đe dọa sử dụng vũ lực đối với hành vi tấn công mạng

Trên cơ sở quan điểm của các quốc gia là thành viên của Liên hợp quốc, các chuyên gia chính phủ do Đại hội đồng Liên hợp quốc thành lập đã đưa ra báo cáo về mối đe dọa trên không gian mạng. Theo đó, báo cáo cho rằng việc áp dụng luật pháp quốc tế nói chung và Điều 2 (4) Hiến chương Liên hợp quốc nói riêng là một điều rất cần thiết để duy trì hòa bình, ổn định an ninh thế giới và thúc đẩy phát triển môi trường công nghệ thông tin và truyền thông (Information and Commuication Technology - ICT) cởi mở, an toàn và dễ tiếp cận¹. Tuy nhiên, để áp dụng Điều 2 (4) Hiến chương Liên hợp quốc trong các hành vi tấn công trên không gian mạng cần phải đáp ứng đủ ba điều kiện sau:

Thứ nhất, các hành vi tấn công mạng phải do quốc gia tiến hành, hành vi của cá nhân hay nhóm vũ trang sẽ không nằm trong điều khoản này ngay cả khi hành vi của nó gây ra thiệt hại tương đương bởi các quốc gia gây ra. Tuy nhiên nếu hành vi tấn công của cá nhân hoặc pháp nhân mà quốc gia hiện diện đã biết hoặc phải biết hành vi đó thì phải thực hiện biện pháp ngăn ngừa, và nếu các quốc gia “hậu thuẫn” cho các cuộc tấn công thực hiện bởi nhóm người đó thì quốc gia phải chịu trách nhiệm pháp lý².

1. Xem United Nations General Assembly Doc A/68/98 (2013): *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Xem toàn văn tại <https://digitallibrary.un.org/record/753055>, truy cập ngày 20/7/2021.

2. Xem Nguyễn Tiến Đức và Trần Thị Thu Thủy: “Tấn công mạng và nguyên tắc cấm sử dụng vũ lực trong pháp luật quốc tế”, Tạp chí *Luật học*, tháng 8/2018.

Thứ hai, hành vi tấn công mạng phải tương đương “mối đe dọa” hoặc “sử dụng vũ lực” theo Điều 2 (4) Hiến chương Liên hợp quốc.

Thứ ba, mối đe dọa hoặc sử dụng vũ lực phải được thực hiện trong bối cảnh thiết lập “quan hệ quốc tế”. Việc tham chiếu đến “quan hệ quốc tế” trong Điều 2 (4) Hiến chương Liên hợp quốc đòi hỏi rằng tấn công mạng không chỉ tác động tới một quốc gia mà có thể chống lại quốc gia thứ ba. Do vậy, một quốc gia không bị coi là vi phạm bởi điều khoản này nếu như thực hiện tấn công mạng đối với các chủ thể phi nhà nước trong lãnh thổ của quốc gia này ngay cả khi có thể dẫn đến mối đe dọa hoặc sử dụng vũ lực. Nói cách khác, chủ thể bị tác động bởi hành vi tấn công mạng phải là quốc gia - chủ thể của luật quốc tế.

Theo quan điểm của Marco Roscini, để xác định hành vi tấn công mạng có thuộc phạm vi điều chỉnh của Điều 2 (4) Hiến chương Liên hợp quốc hay không, cần dựa vào các cách tiếp cận sau¹:

Thứ nhất, dựa trên công cụ, phương tiện để thực hiện hành vi (chẳng hạn như các loại vũ khí truyền thống): Cách tiếp cận này đã bị chỉ trích vì chỉ tập trung vào các công cụ được xác định bởi các đặc điểm vật lý của chúng và sẽ dẫn đến không thể kết luận các cuộc tấn công mạng là sử dụng vũ lực theo Điều 2 (4) Hiến chương Liên hợp quốc ngay cả khi chúng dẫn đến thiệt hại vật chất.

Thứ hai, dựa vào mục tiêu: Quan điểm này cho rằng các hoạt động mạng đạt đến mức độ “vũ lực” khi chúng tiến hành

1. Xem Marco Roscini: *Cyber Operations as a Use of Force*, University of Westminster, Research Paper No.16-05, 2015, p.7-9.

nhắm vào hạ tầng trọng điểm của quốc gia (National Critical Infrastructure - NCI), bất kể ảnh hưởng của chúng đối với hạ tầng đó hoặc bản chất của hoạt động đó là gì. Tuy nhiên, nếu theo cách tiếp cận này thì hành vi tấn công mạng được xác định là quá rộng, bởi vì mức độ tác động tới NCI là khác nhau. Ngoài ra, NCI gồm những gì cũng chưa được quy định rõ ràng.

Thứ ba, dựa trên tác động của hành vi: Các hình thức sử dụng vũ lực có tác động phá hoại trực tiếp đến tài sản con người. Do đó, bất kỳ hoạt động mạng nào gây ra hoặc có khả năng gây ra một cách hợp lý dẫn đến hậu quả gây tổn hại thường được tạo ra bởi vũ khí động năng sẽ là “sử dụng vũ lực”¹. Rõ ràng, với quan điểm này, sử dụng vũ lực bằng “tấn công mạng” được coi là “sử dụng vũ lực” khi sự phá hoại là “trực tiếp” đến con người và tài sản. Đây là quan điểm được ủng hộ nhiều nhất. Tuy nhiên, quan điểm này lại không xét đến việc phụ thuộc của xã hội hiện đại vào máy tính, hệ thống và mạng lưới máy tính và xã hội chịu tác động “gián tiếp” khi hạ tầng máy tính bị vô hiệu hóa mà không cần phải phá hủy chúng. Vì vậy, cách tiếp cận này bộc lộ điểm bất cập chính là “tác động trực tiếp” không phải là đặc điểm vốn có, cần thiết trong sử dụng vũ lực².

1. Xem Daniel B. Silver: “Computer Network Attack as a Use of Force under Article 2 (4) of the United Nations Charter”, *International Law Studies*, 76, 2002, p.92-93.

2. Ví dụ như trong Tuyên bố của Đại hội đồng Liên hợp quốc về định nghĩa hành động gây hấn (*Aggression*) được coi là hành động xâm lược, không chỉ là các vụ đánh bom, xâm lược mà còn là các hành động gián tiếp như vi phạm đóng quân, phong tỏa hải quân, cho phép các quốc gia khác sử dụng lãnh thổ với mục đích gây hấn. Xem thêm tại: Definition of Aggression, General Assembly Resolution 3314 (XXIX), 14 December 1974.

Rõ ràng, cả ba cách tiếp cận trên đều bộc lộ những điểm chưa phù hợp khi áp dụng nguyên tắc cấm dùng vũ lực và đe dọa dùng vũ lực đối với hành vi tấn công mạng. Do đó, việc áp dụng nguyên tắc này phù hợp hơn khi xác định “vũ trang” bằng cách tham chiếu đến các công cụ được sử dụng. Điều này phù hợp với ý nghĩa của từ “vũ trang” theo Từ điển Black’s Law: “Vũ trang có nghĩa là được trang bị vũ khí hay những điều liên quan đến việc sử dụng vũ khí”¹. Không như những sự tấn công đơn thuần, “tấn công vũ trang” yêu cầu phải có hai yếu tố đồng thời: việc sử dụng vũ khí và ý định cưỡng bức. Vì thế, việc quốc gia sử dụng vũ khí nhưng không nhằm ý định cưỡng bức quốc gia khác thì không thuộc phạm vi điều chỉnh tại Điều 2 (4) Hiến chương Liên hợp quốc nhưng nó lại vi phạm các quy tắc khác, chẳng hạn như nguyên tắc tôn trọng chủ quyền của quốc gia khác. Trong Từ điển Black’s Law định nghĩa “vũ khí” là một công cụ dùng để chiến đấu, tấn công, phòng thủ hoặc bất kỳ thứ gì được sử dụng hoặc được thiết kế để làm bị thương, đánh bại kẻ thù². Một số nhà bình luận luật học cũng cho rằng vũ khí là bất kỳ công cụ, phương tiện, thiết bị,... nào nhằm gây thiệt hại về vật chất hoặc tinh thần cho đối phương³. Nhóm tác giả nhận thấy rằng đặc điểm chung của các định nghĩa trên là: hậu quả của bạo lực đều do công cụ tạo ra. Vì vậy, vũ khí nên được xác định dựa vào hậu quả nó gây ra,

1, 2. Black’s Law Dictionary (4th edition, West Publishing CO. 1968), p.138, 1764.

3. Xem Marco Roscini: Cyber Operations as a Use of Force, *Tlđđ*, no.5, p.11.

chứ không phải thông qua cơ chế, phương thức mà chúng gây ra thiệt hại.

Câu hỏi thứ nhất cần giải quyết đó là: Hành vi tấn công mạng có phải là tấn công vũ trang theo Điều 2 (4) Hiến chương Liên hợp quốc hay không? Trong kết luận tư vấn về mối đe dọa vũ khí hạt nhân, Tòa án công lý quốc tế (ICJ) cho rằng: các Điều 2 (4), 51 và 42 Hiến chương Liên hợp quốc có giá trị áp dụng với hành vi sử dụng vũ lực bất kể loại vũ khí nào được sử dụng để gây thiệt hại¹. Một số quốc gia đã đưa các công nghệ mạng vào học thuyết quân sự của họ và đề cập không gian mạng là lĩnh vực chiến tranh thứ năm và đã thành lập các đơn vị quân đội có chuyên môn cụ thể về mạng². Đồng thời họ cũng có nhận xét rằng, tác động phá hoại của các hành vi tấn công mạng này lại có sức “công phá” gây ra hậu quả nghiêm trọng tương đương với các tác động vật lý thông thường³. Vì thế, chúng ta nên xem không gian mạng như một phương tiện chiến tranh mới; nói cách khác là một vũ khí gây thiệt hại không hơn không kém so với các loại vũ khí khác. Do đó, tấn công mạng được xem là hình thức tấn công vũ trang.

1. Xem Nguyễn Tiến Đức và Trần Thị Thu Thủy: “Tấn công mạng và nguyên tắc cấm sử dụng vũ lực trong pháp luật quốc tế”, *Tlđđ*.

2. Ví dụ như Trung Quốc, Nhật, Ôxtrâylia, Hoa Kỳ, Anh, Hà Lan,... xem Marco Roscini, *Cyber Operations as a Use of Force*, *Tlđđ*, no.5, p.3-4.

3. Tiêu biểu là vụ nổ đường ống dẫn khí đốt của Liên Xô ở Siberia vào tháng 6/1982 do một quả bom logic được cài vào hệ thống điều khiển máy tính của Cơ quan tình báo Trung ương Mỹ (CIA). Xem thêm Hoàng Phú: “Vụ nổ đường ống dẫn dầu khí đốt xuyên Siberia của Liên Xô vào năm 1982 là tai nạn hay phá hoại?”, truy cập ngày 24/7/2021.

Câu hỏi thứ hai cần giải quyết đó là: Mức độ phá hoại như thế nào của một cuộc tấn công mạng mới được xem là vi phạm Điều 2 (4) Hiến chương Liên hợp quốc? Trong Điều 2 (4) Hiến chương Liên hợp quốc không có từ ngữ nào cho rằng việc sử dụng vũ lực nên được phân biệt theo hậu quả. Như đã phân tích ở trên, Điều 2 (4) Hiến chương Liên hợp quốc cấm bất kỳ hành vi nào liên quan đến các cuộc tấn công xâm phạm chủ quyền lãnh thổ của quốc gia khác bất kể mức độ tấn công và mục đích của chúng. Rõ ràng, mức độ phá hoại không phải là yếu tố để xác định hành vi tấn công mạng là vi phạm Điều 2 (4) Hiến chương Liên hợp quốc. Có thể nói, nếu việc sử dụng vũ khí (mạng) tấn công, gây tổn hại và ảnh hưởng đến nhà nước thì được xem là sử dụng vũ lực hoặc đe dọa sử dụng vũ lực.

Tóm lại, khi một cuộc tấn công mạng được tiến hành bởi một quốc gia với ý định cưỡng bức nhằm chống lại quốc gia khác thì có khả năng được xem là sử dụng vũ lực theo Điều 2 (4) Hiến chương Liên hợp quốc. Tuy nhiên không phải bất cứ hoạt động trên không gian mạng trái phép nào cũng được coi là “tấn công mạng” bởi vì còn có hành vi “khai thác mạng”. Khai thác mạng là hành động truy cập trái phép vào máy tính, hệ thống máy tính hoặc mạng để thu thập thông tin nhưng không làm ảnh hưởng đến chức năng của hệ thống truy cập hay làm hỏng, sửa đổi, xóa dữ liệu trong đó. Mục tiêu của khai thác mạng là để có thông tin từ một mạng máy tính mà người dùng không biết, đây được xem như là hình thức gián điệp hiện đại¹. Sự khác biệt chính giữa tấn công

1. Gián điệp được xem là một hình thức bất hợp pháp trong quy định pháp luật của hầu hết các quốc gia, nhưng đối với pháp luật quốc tế thì không.

mạng và khai thác mạng là về bản chất mục đích của hành vi thực hiện: mục đích của tấn công mạng là phá hoại, còn mục đích khai thác mạng là thu được thông tin không bị phá hủy¹. Khai thác trên mạng có thể xâm phạm chủ quyền của một quốc gia khi việc này đòi hỏi bắt buộc phải xâm nhập trái phép vào kết cấu hạ tầng mạng nằm trên lãnh thổ của quốc gia đó. Khai thác mạng về bản chất không thể dẫn đến vi phạm nguyên tắc cấm dùng vũ lực và đe dọa dùng vũ lực bởi vì hành vi này không liên quan đến việc “sử dụng vũ khí”, hoàn toàn trái ngược với các cuộc tấn công mạng như đã trình bày.

3. Áp dụng nguyên tắc cấm sử dụng vũ lực và đe dọa sử dụng vũ lực đối với hành vi tấn công mạng - Sự cần thiết và liên hệ với Việt Nam

a) Sự cần thiết

Giả thuyết thứ nhất, nhìn từ góc độ thiệt hại mà những cuộc tấn công mạng gây ra, khả năng rất lớn những cuộc tấn công này sẽ châm ngòi xung đột dẫn đến chiến tranh. Bởi lẽ kinh tế, hành chính, chính trị, lương thực, y tế và năng lượng, nhiên liệu là sinh tồn, là an nguy và hưng thịnh của mỗi quốc gia. Nếu một trong những lĩnh vực đó của quốc gia này bị tấn công và hủy hoại bởi lực lượng tin tặc của một quốc gia khác, thì chiến tranh là điều không thể tránh khỏi. Nếu thật sự có chiến tranh, đó không phải là những cuộc chiến tranh truyền thống mà là “chiến tranh mạng”, như lời

1. See Joseph N. Madubuike - Ekwe: “Cyberattack and the Use of Force in International Law”, Beijing Law Review, 12, (2021), pp.631-649.

của nguyên Thứ trưởng Bộ Quốc phòng Hoa Kỳ, William Lynn: “Trong thế kỷ XXI, bit và byte có sức đe dọa tương đương với súng đạn và bom mìn”¹. Như vậy, trong thời đại hiện nay, tấn công mạng chính là hình thức được “ưa chuộng” để thực hiện sử dụng vũ lực mà không cần vũ khí nhưng lại để lại hậu quả nghiêm trọng. Căn cứ vào nội dung của các quy định pháp luật quốc tế về hành vi tấn công mạng chính là cơ sở để áp dụng nguyên tắc cấm sử dụng vũ lực và đe dọa sử dụng vũ lực.

Ở một giả thuyết khác, có thể lý giải rằng: Chính phủ các nước hiện nay rất khó để phát động chiến tranh bằng phương thức truyền thống, bởi sẽ vấp phải nhiều rào cản dư luận, mặt khác còn gây thiệt hại lớn về người và tài sản. Vì thế, khi Cách mạng công nghiệp lần thứ tư diễn ra với sự phát triển mạnh mẽ của không gian mạng và công nghệ hiện đại, tiên tiến, những xung đột dần chuyển hướng đến cuộc chiến “không khói súng”. Những cuộc chiến đó được ví như là Digital Pearl Harbor (trận Trân Châu Cảng trên mạng) nhằm ám chỉ về những cuộc tấn công mạng âm thầm và tinh vi bất ngờ xảy ra nhờ sự hỗ trợ của mã độc mà đối phương không hề biết². Vì vậy, khi chiến tranh bùng nổ sẽ gây ra những ảnh hưởng rất lớn đối với một quốc gia, đặc biệt là quốc gia có sự phát triển và phụ thuộc nhiều vào công nghệ số.

1. Intelligence and Security Committee: *Annual Report 2009 - 2010*, p.16, <http://isc.independent.gov.uk/committee-reports/annual-reports>, truy cập ngày 14/7/2021.

2. Xem Chí Thiện: “Những vụ chiến tranh mạng nổi tiếng”, <https://baophapluat.vn>, truy cập ngày 14/7/2021.

Nếu có chiến tranh mạng thực sự, thì áp dụng nguyên tắc cấm sử dụng vũ lực và đe dọa sử dụng vũ lực đối với các hành vi tấn công mạng là hợp lý. Bởi vì, những cuộc tấn công mạng dù được thực hiện trên không gian mạng nhưng lại có ảnh hưởng và gây thiệt hại trên thực tế của đối phương.

Nhận thức được ảnh hưởng nghiêm trọng của tấn công mạng đến an ninh quốc gia, các nước đã ban hành những quy định pháp luật nhằm trừng phạt và răn đe đối với chủ thể thực hiện hành vi này, ví dụ: Ôxtrâyliia xây dựng hành lang pháp lý vững chắc với các đạo luật về tội phạm mạng; Xingapo đã có Dự luật về an ninh mạng; Hoa Kỳ xây dựng hệ thống bảo mật thông tin mạnh mẽ và có hiệu quả nhất thế giới với 4 đạo luật về an ninh mạng,... Có thể thấy việc áp dụng nguyên tắc cấm sử dụng vũ lực và đe dọa sử dụng vũ lực đối với các hành vi tấn công mạng hiện nay là cần thiết. Bởi đó là cơ sở để củng cố và làm chặt chẽ hơn pháp luật của các quốc gia, đồng thời tạo nên quy định chung về cơ chế cấm thực hiện các hoạt động sử dụng vũ lực và đe dọa sử dụng vũ lực thông qua tấn công mạng trong quan hệ quốc tế.

b) Liên hệ với Việt Nam

Đối mặt với khó khăn và vấn đề tấn công mạng, Chính phủ Việt Nam đã nhìn nhận và nỗ lực xây dựng hành lang pháp lý nhằm ngăn ngừa, phòng, chống mối họa từ “tấn công mạng” bằng việc thông qua Luật an ninh mạng vào năm 2018. Luật an ninh mạng năm 2018 vừa là cơ sở pháp lý để xử lý các hành vi phạm tội, vừa bảo vệ hệ thống thông tin mạng quốc gia và phòng, chống tấn công mạng.

Tuy nhiên là một quốc gia đang phát triển, ngày càng hội nhập và tham gia sâu rộng vào không gian mạng toàn cầu, Việt Nam không tránh khỏi trở thành nạn nhân của các cuộc tấn công mạng. Tính đến tháng 6/2021, nước ta đã xảy ra 718 cuộc tấn công mạng vào các hệ thống thông tin theo thống kê của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCC) thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông¹. Bên cạnh đó, từ tháng 12/2019 cho đến nay, dịch bệnh Covid-19 diễn ra phức tạp ngày càng nghiêm trọng, hầu hết mọi lĩnh vực đều hoạt động trực tuyến, hàng loạt các cơ sở giáo dục, các doanh nghiệp, cơ quan, tổ chức,... đều sử dụng internet để quản lý, học tập và làm việc từ xa thông qua các phần mềm. Chính điều này đã tạo điều kiện cho các tội phạm tấn công mạng và ăn cắp dữ liệu của người dùng².

Để phòng ngừa và ngăn chặn các cuộc tấn công mạng, Việt Nam cần tích cực đẩy mạnh hợp tác song phương và đa phương với các quốc gia khác trong hoạt động phòng, chống tấn công mạng. Bởi rằng, chỉ Việt Nam thôi là chưa đủ, Việt Nam cần thêm những “người bạn” quốc tế cùng nhau chung tay bảo vệ an ninh thế giới và an ninh của chính quốc gia mình. Bên cạnh đó, Việt Nam là một quốc gia yêu chuộng hòa bình, không tham chiến và gây hấn với các quốc gia khác

1. Xem BT: “Số vụ tấn công mạng tại Việt Nam tăng mạnh”, <http://baochinhphu.vn>, truy cập ngày 26/7/2021.

2. Xem Lâm Thảo: “Toàn cảnh an ninh mạng Việt Nam 2020: Tổn thất hơn 1 tỷ USD do virus máy tính”, <https://nhandan.vn>, truy cập ngày 26/7/2021.

dù là không gian thực hay không gian mạng¹. Việt Nam nêu rõ quan điểm tôn trọng và tuân theo quy định của pháp luật quốc tế. Quan điểm của Việt Nam cần được thể hiện rõ: nguyên tắc cấm sử dụng vũ lực và đe dọa sử dụng vũ lực là nguyên tắc cơ bản của luật pháp quốc tế, thì nguyên tắc này cũng có giá trị áp dụng đối với các hành vi của quốc gia tiến hành trên không gian mạng như đã phân tích ở trên. Với tư cách là một thành viên của Liên hợp quốc, nếu có những hành vi tấn công mạng của các nước khác gây thiệt hại đến lợi ích quốc gia, Việt Nam sẽ lên án và có phương án xử lý theo quy định của luật pháp quốc tế.

1. Xem Nguyễn Tiến Đức và Trần Thị Thu Thủy: “Tấn công mạng và nguyên tắc cấm sử dụng vũ lực trong pháp luật quốc tế”, *Tlđđ*.

QUY ĐỊNH PHÁP LUẬT VỀ THÔNG TIN CÁ NHÂN VÀ KIẾN NGHỊ

ThS. NGUYỄN THỊ HỒNG HẠNH*

Ngày nay, nhân loại đang sống trong một “xã hội thông tin” mà ở đó việc trao đổi thông tin không giới hạn, xã hội càng văn minh thì vai trò thông tin càng trở nên quan trọng, là đòn bẩy để thúc đẩy nền kinh tế phát triển. Trước thách thức đó, Nhà nước ta không ngừng hoàn thiện các quy chế pháp lý để quản lý thông tin, quy định về quyền tiếp cận thông tin.

1. Khái niệm quyền tiếp cận thông tin

Trước hết, “quyền tiếp cận thông tin” được định nghĩa là quyền cơ bản của công dân, quyền này bao gồm quyền tìm kiếm thông tin và tiếp nhận thông tin. Quyền này chỉ được bảo đảm khi cơ quan nhà nước thực hiện nghĩa vụ của mình trong việc cung cấp thông tin khi có yêu cầu, cũng như công khai thông tin ngay cả khi không có yêu cầu, trừ những trường hợp ngoại lệ do pháp luật quy định¹. Ngoài ra, quyền

* Trường Đại học Luật Thành phố Hồ Chí Minh.

1. Xem Vũ Thị Tố Chinh: *Pháp luật về quyền tiếp cận thông tin của công dân trong quản lý nhà nước*, Luận văn Thạc sĩ Luật học, 2012.

tiếp cận thông tin còn là cơ sở, điều kiện để thực hiện các quyền dân sự, chính trị, kinh tế khác như quyền học tập, quyền tự do kinh doanh, quyền nghiên cứu khoa học, kỹ thuật, phát minh, sáng chế, quyền được hưởng chế độ bảo vệ sức khỏe. Ngày 06/4/2016, Luật tiếp cận thông tin năm 2016 đã được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIII, kỳ họp thứ 11 thông qua. Điều 2 của luật này đã đưa ra khái niệm *“Tiếp cận thông tin là việc đọc, xem, nghe, ghi chép, sao chép, chụp thông tin”*. Trên thế giới, khái niệm “quyền tiếp cận thông tin” ở mỗi quốc gia là khác nhau nhưng nhìn chung, các quốc gia đều thừa nhận quyền tiếp cận thông tin là quyền cơ bản của con người, cho phép công dân nước đó có quyền tiếp cận các văn bản của các cơ quan nhà nước trừ một số lĩnh vực mật theo quy định của luật. Ngoài ra, quyền tiếp cận thông tin ở Việt Nam hiện nay còn được quy định tại Điều 25 Hiến pháp năm 2013: *“Công dân có quyền tự do ngôn luận, tự do báo chí, tiếp cận thông tin, hội họp, lập hội, biểu tình”*. Thực tế khi triển khai quyền này, về phía chủ thể có thẩm quyền khi nhận được yêu cầu cung cấp thông tin thì thường có tâm lý né tránh do không biết quyền hạn của mình đến đâu và việc cung cấp thông tin có hợp pháp không. Hiện nay, do nhu cầu về thông tin là rất lớn, chúng ta có cách mạng thông tin, môi trường thông tin, cơ chế thông tin, công cụ thông tin... Việc thông tin bị bung bít, không công khai trước công chúng tạo hệ lụy rất lớn, đó là tình trạng lạc hậu, nghèo đói, bất bình đẳng, thiếu dân chủ của một quốc gia, nghiêm trọng hơn là tình trạng tham nhũng, quan liêu, của quyền dẫn đến khiếu nại, tố cáo tràn lan,

làm suy giảm niềm tin của nhân dân với chính quyền¹. Vì vậy, quy định của pháp luật về quyền tiếp cận thông tin là hết sức cần thiết và có vai trò to lớn trong công tác đấu tranh, phòng, chống tham nhũng, tăng cường hiệu quả quản lý nhà nước, góp phần xây dựng nhà nước dân chủ, của nhân dân, do nhân dân, vì nhân dân.

Luật tiếp cận thông tin năm 2016 đã quy định về thông tin được phép tiếp cận là những thông tin công khai rộng rãi và những thông tin được cung cấp theo yêu cầu.

Thứ nhất, thông tin phải được công khai, bao gồm:

Văn bản quy phạm pháp luật; văn bản hành chính có giá trị áp dụng chung; điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên, thỏa thuận quốc tế mà Việt Nam là một bên; thủ tục hành chính, quy trình giải quyết công việc của cơ quan nhà nước.

Thông tin phổ biến, hướng dẫn thực hiện pháp luật, chế độ, chính sách đối với những lĩnh vực thuộc phạm vi quản lý của cơ quan nhà nước.

Dự thảo văn bản quy phạm pháp luật theo quy định của pháp luật về ban hành văn bản quy phạm pháp luật; nội dung và kết quả trưng cầu ý dân, tiếp thu ý kiến của nhân dân đối với những vấn đề thuộc thẩm quyền quyết định của cơ quan nhà nước được đưa ra lấy ý kiến nhân dân theo quy định của pháp luật; đề án và dự thảo đề án thành lập, giải thể, nhập, chia đơn vị hành chính, điều chỉnh địa giới hành chính.

1. Xem Vũ Thị Tố Chinh: *Pháp luật về quyền tiếp cận thông tin của công dân trong quản lý nhà nước, Tlđd.*

Chiến lược, chương trình, dự án, đề án, kế hoạch, quy hoạch phát triển kinh tế - xã hội của quốc gia, địa phương; quy hoạch ngành, lĩnh vực và phương thức, kết quả thực hiện; chương trình, kế hoạch công tác hằng năm của cơ quan nhà nước.

Thông tin về dự toán ngân sách nhà nước; báo cáo tình hình thực hiện ngân sách nhà nước; quyết toán ngân sách nhà nước; dự toán, tình hình thực hiện, quyết toán ngân sách đối với các chương trình, dự án đầu tư xây dựng cơ bản sử dụng vốn ngân sách nhà nước; thủ tục ngân sách nhà nước.

Thông tin về phân bổ, quản lý, sử dụng nguồn vốn hỗ trợ phát triển chính thức và nguồn viện trợ phi chính phủ theo quy định; thông tin về quản lý, sử dụng các khoản cứu trợ, trợ cấp xã hội; quản lý, sử dụng các khoản đóng góp của nhân dân, các loại quỹ.

Thông tin về danh mục dự án, chương trình đầu tư công, mua sắm công và quản lý, sử dụng vốn đầu tư công, tình hình và kết quả thực hiện kế hoạch, chương trình, dự án đầu tư công; thông tin về đấu thầu; thông tin về quy hoạch, kế hoạch sử dụng đất; giá đất; thu hồi đất; phương án bồi thường, giải phóng mặt bằng, tái định cư liên quan đến dự án, công trình trên địa bàn.

Thông tin về hoạt động đầu tư, quản lý, sử dụng vốn nhà nước tại doanh nghiệp; báo cáo đánh giá kết quả hoạt động và xếp loại doanh nghiệp; báo cáo giám sát tình hình thực hiện công khai thông tin tài chính của doanh nghiệp và cơ quan nhà nước đại diện chủ sở hữu; thông tin về tổ chức và hoạt động của doanh nghiệp nhà nước.

Thông tin về sản phẩm, hàng hóa, dịch vụ có tác động tiêu cực đến sức khỏe, môi trường; kết luận kiểm tra, thanh tra, giám sát liên quan đến việc bảo vệ môi trường, sức khỏe của cộng đồng, an toàn thực phẩm, an toàn lao động;

Thông tin về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức của cơ quan và của đơn vị trực thuộc; nhiệm vụ, quyền hạn của cán bộ, công chức trực tiếp giải quyết các công việc của nhân dân; nội quy, quy chế do cơ quan nhà nước ban hành.

Báo cáo công tác định kỳ; báo cáo tài chính năm; thông tin thống kê về ngành, lĩnh vực quản lý; cơ sở dữ liệu quốc gia ngành, lĩnh vực; thông tin về tuyển dụng, sử dụng, quản lý cán bộ, công chức, viên chức; thông tin về danh mục và kết quả chương trình, đề tài khoa học.

Thông tin liên quan đến lợi ích công cộng, sức khỏe của cộng đồng.

Thông tin về thuế, phí, lệ phí¹.

Thứ hai, thông tin được cung cấp theo yêu cầu, bao gồm:

Thông tin trong thời hạn công khai nhưng chưa được công khai.

Thông tin hết thời hạn công khai theo quy định của pháp luật.

Thông tin đang được công khai nhưng vì lý do bất khả kháng người yêu cầu không thể tiếp cận được.

Thông tin liên quan đến bí mật kinh doanh, đời sống riêng tư, bí mật cá nhân, bí mật gia đình đủ điều kiện cung cấp theo quy định tại Điều 7 của luật.

1. Điều 17 Luật tiếp cận thông tin năm 2016.

Thông tin liên quan đến đời sống, sinh hoạt, sản xuất, kinh doanh của người yêu cầu cung cấp thông tin nhưng không thuộc loại thông tin quy định tại Điều 17 và khoản 2, Điều 23 của luật.

Ngoài thông tin quy định tại các khoản 1, 2 và 3, Điều 23, căn cứ vào nhiệm vụ, quyền hạn, điều kiện và khả năng thực tế của mình, cơ quan nhà nước có thể cung cấp thông tin khác do mình tạo ra hoặc nắm giữ¹.

Qua phân tích trên có thể thấy rằng hoạt động quản lý của bộ máy nhà nước về bản chất luôn chứa đựng thông tin và liên quan trực tiếp đến người dân. Thông tin trong lĩnh vực quản lý ảnh hưởng đến đời sống xã hội, có sức ảnh hưởng lớn đối với các chủ thể chịu sự tác động. Chính vì vậy, Luật tiếp cận thông tin đã quy định quyền và nghĩa vụ của công dân trong việc tiếp cận thông tin, phạm vi và trách nhiệm cung cấp thông tin của các cơ quan nhà nước, cách thức tiếp cận thông tin của công dân, chi phí tiếp cận thông tin là cơ sở cho quyền được tiếp cận thông tin thực thi. Như vậy, quyền được thông tin là một trong những quyền cơ bản của công dân được pháp luật bảo vệ và ghi nhận.

Thứ ba, thông tin công dân không được tiếp cận:

Thông tin trong quản lý nhà nước rất rộng nhưng không phải thông tin nào công dân cũng có thể tiếp cận. Có những thông tin trong quản lý thuộc bí mật nhà nước không thể công khai, vì pháp luật tôn trọng quyền tiếp cận thông tin của công dân nhưng cũng không tách rời lợi ích của nhà nước, lợi ích công cộng:

1. Điều 23 Luật tiếp cận thông tin năm 2016.

Thông tin thuộc bí mật nhà nước, bao gồm những thông tin có nội dung quan trọng thuộc lĩnh vực chính trị, quốc phòng, an ninh quốc gia, đối ngoại, kinh tế, khoa học, công nghệ và các lĩnh vực khác theo quy định của luật.

Khi thông tin thuộc bí mật nhà nước được giải mật thì công dân được tiếp cận theo quy định của luật này.

Thông tin mà nếu để tiếp cận sẽ gây nguy hại đến lợi ích của Nhà nước, ảnh hưởng xấu đến quốc phòng, an ninh quốc gia, quan hệ quốc tế, trật tự, an toàn xã hội, đạo đức xã hội, sức khỏe của cộng đồng; gây nguy hại đến tính mạng, cuộc sống hoặc tài sản của người khác; thông tin thuộc bí mật công tác; thông tin về cuộc họp nội bộ của cơ quan nhà nước; tài liệu do cơ quan nhà nước soạn thảo cho công việc nội bộ¹.

Ở đây, khái niệm “bí mật nhà nước” có thể xem là giới hạn lớn nhất của quyền này, gây khó khăn lớn nhất cho việc thực thi quyền cũng như trong Luật tiếp cận thông tin ở nước ta. Do “bí mật nhà nước” là những tin về vụ, việc, tài liệu, vật, địa điểm, thời gian, lời nói có nội dung quan trọng thuộc lĩnh vực chính trị, quốc phòng, an ninh, đối ngoại, kinh tế, khoa học, công nghệ, các lĩnh vực khác mà Nhà nước không công bố hoặc chưa công bố và nếu bị tiết lộ thì gây nguy hại cho Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam², nên những thông tin liên quan đến bí mật nhà nước là những thông tin rất quan trọng, ảnh hưởng đến quốc gia, nếu bị tiết lộ sẽ gây hậu quả khó lường.

1. Điều 6 Luật tiếp cận thông tin năm 2016.

2. Điều 1 Pháp lệnh bảo vệ bí mật nhà nước năm 2000.

2. Các quy định pháp luật về thông tin cá nhân

Thông tin cá nhân của một chủ thể là thông tin bao gồm: *họ tên, ngày sinh, địa chỉ nơi ở, địa chỉ nơi làm việc, số điện thoại cá nhân, thư điện tử, số tài khoản ngân hàng, số thẻ tín dụng, số chứng minh nhân dân, thông tin trong hồ sơ y tế, v.v.*¹. Những thông tin này có thể trở thành nguồn dữ liệu có giá trị mang tính thương mại, dân sự thông qua các hoạt động truyền thông, tiếp thị, quảng cáo. Vì vậy, các đối tác chiến lược luôn muốn khai thác thông tin cá nhân của khách hàng để đạt được các mục tiêu mong muốn. Tuy nhiên, để bảo đảm quyền riêng tư, các cá nhân không muốn thông tin cá nhân của mình bị khai thác và sử dụng không đúng mục đích. Chính vì vậy, mỗi chủ thể mong muốn kiểm soát và bảo vệ thông tin cá nhân của mình bằng các phương thức khác nhau. Thuật ngữ “thông tin cá nhân” đã được quy định trong Luật được năm 2005 và yêu cầu bảo mật thông tin cá nhân trong lĩnh vực hàng không đã được đề cập trong Luật hàng không dân dụng năm 2006. Tuy nhiên, đến năm 2016 Luật công nghệ thông tin năm 2006 mới quy định cụ thể về bảo vệ thông tin cá nhân trong môi trường mạng. Tại khoản 1, Điều 21 Luật công nghệ thông tin đã quy định tổ chức, cá nhân “thu thập, xử lý và sử dụng thông tin cá nhân của người khác trên môi trường mạng phải được người đó đồng ý trừ trường hợp pháp luật có quy định khác”. Điều này có nghĩa là khi thu thập, xử lý và sử dụng thông tin cá nhân của người khác, chủ thể thực hiện hành vi này có trách

1. Xem <http://lapphap.vn/pages/tintuc/printpage.aspx?tintucID=210631>.

nhiệm “Thông báo cho người đó biết về hình thức, phạm vi, địa điểm và mục đích của việc thu thập, xử lý và sử dụng thông tin cá nhân của người đó”¹. Ngoại lệ cho việc thu thập, xử lý và sử dụng thông tin cá nhân của người khác mà không cần sự đồng ý của người đó được đặt ra “trong trường hợp thông tin cá nhân đó được sử dụng cho mục đích sau đây: a) Ký kết, sửa đổi hoặc thực hiện hợp đồng sử dụng thông tin, sản phẩm, dịch vụ trên môi trường mạng; b) Tính giá, cước sử dụng thông tin, sản phẩm, dịch vụ trên môi trường mạng; c) Thực hiện nghĩa vụ khác theo quy định của pháp luật”². Tiếp theo đó, khoản 1, Điều 22 Luật công nghệ thông tin quy định quyền của các chủ thể trong việc kiểm tra, đính chính hoặc hủy bỏ thông tin cá nhân do chủ thể khác lưu trữ: “cá nhân có quyền yêu cầu tổ chức, cá nhân lưu trữ thông tin cá nhân của mình trên môi trường mạng thực hiện việc kiểm tra, đính chính hoặc hủy bỏ thông tin đó”. Tại khoản 2, khoản 3, Điều 22 Luật công nghệ thông tin quy định “tổ chức, cá nhân không được cung cấp thông tin cá nhân của người khác cho bên thứ ba, trừ trường hợp pháp luật có quy định khác hoặc có sự đồng ý của người đó” và “cá nhân có quyền yêu cầu bồi thường thiệt hại do hành vi vi phạm trong việc cung cấp thông tin cá nhân”.

Từ các quy định trên có thể thấy rằng việc “thu thập, xử lý, sử dụng, chuyển nhượng thông tin cá nhân” của bất cứ tổ chức, cá nhân nào trên môi trường mạng đều phải bảo đảm theo quy định của pháp luật. Chủ thể thông tin cá nhân có

1. Điểm a, khoản 2, Điều 21 Luật công nghệ thông tin năm 2006.

2. Khoản 3, Điều 21 Luật công nghệ thông tin năm 2006.

một số quyền nhất định đối với tổ chức, cá nhân thu thập, xử lý, sử dụng và chuyển nhượng thông tin cá nhân. Tuy nhiên, Luật công nghệ thông tin chỉ quy định nghĩa vụ pháp lý đối với việc thu thập, xử lý, lưu trữ, chuyển nhượng thông tin cá nhân trong môi trường mạng, để lại một khoảng trống pháp lý đối với việc bảo vệ thông tin cá nhân không ở trên môi trường mạng (tức là ở môi trường vật lý - môi trường offline). Thêm vào đó, thuật ngữ chủ thể thông tin cá nhân hoặc chủ thể dữ liệu (data subject) chưa được sử dụng trong đạo luật này¹.

Bàn về bảo vệ thông tin cá nhân còn được quy định trong Luật bảo vệ quyền lợi người tiêu dùng năm 2010 về bảo vệ thông tin của người tiêu dùng. Theo đó, người tiêu dùng được bảo đảm an toàn, bí mật thông tin của mình khi tham gia giao dịch, trừ trường hợp cơ quan nhà nước có thẩm quyền yêu cầu². Trường hợp thu thập, sử dụng, chuyển giao thông tin của người tiêu dùng thì tổ chức, cá nhân kinh doanh hàng hóa, dịch vụ có trách nhiệm: a) Thông báo rõ ràng, công khai trước khi thực hiện với người tiêu dùng về mục đích hoạt động thu thập, sử dụng thông tin của người tiêu dùng; b) Sử dụng thông tin phù hợp với mục đích đã thông báo với người tiêu dùng và phải được người tiêu dùng đồng ý; c) Bảo đảm an toàn, chính xác, đầy đủ khi thu thập, sử dụng, chuyển giao thông tin của người tiêu dùng; d) Tự mình hoặc có biện pháp để người tiêu dùng cập nhật, điều chỉnh thông tin khi phát hiện thấy thông tin đó không chính xác; đ) Chỉ được

1. Khoản 3, Điều 21 Luật công nghệ thông tin năm 2006.

2. Điều 6, Luật bảo vệ quyền lợi người tiêu dùng năm 2010.

chuyển giao thông tin của người tiêu dùng cho bên thứ ba khi có sự đồng ý của người tiêu dùng, trừ trường hợp pháp luật có quy định khác¹.

Bộ luật dân sự năm 2015 đã bổ sung quy định về “*quyền về đời sống riêng tư*” ngoài quy định về “*bí mật cá nhân*” và “*bí mật gia đình*” trong Bộ luật dân sự năm 1995 và năm 2005². Theo Điều 38, Bộ luật dân sự quy định *Quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình*: “1. Đời sống riêng tư, bí mật cá nhân, bí mật gia đình là bất khả xâm phạm và được pháp luật bảo vệ; 2. Việc thu thập, lưu giữ, sử dụng, công khai thông tin liên quan đến đời sống riêng tư, bí mật cá nhân phải được người đó đồng ý, việc thu thập, lưu giữ, sử dụng, công khai thông tin liên quan đến bí mật gia đình phải được các thành viên gia đình đồng ý, trừ trường hợp luật có quy định khác; 3. 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; 4. Việc bóc mở, kiểm soát, thu giữ thư tín, điện thoại, điện tín, cơ sở dữ liệu điện tử và các hình thức trao đổi thông tin riêng tư khác của người khác chỉ được thực hiện trong trường hợp luật quy định; 5. Các bên trong hợp đồng không được tiết lộ thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình của nhau mà mình đã biết được trong quá trình xác lập, thực hiện hợp đồng, trừ trường hợp có thỏa thuận khác”.

Một trong những đạo luật quan trọng về an ninh thông tin cá nhân là Luật an toàn thông tin mạng năm 2015 quy

1. Điều 6, Luật bảo vệ quyền lợi người tiêu dùng năm 2010.

2. Điều 38, Bộ luật dân sự năm 2015.

định bảo vệ thông tin cá nhân áp dụng đối với cơ quan, tổ chức, cá nhân Việt Nam và nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động an ninh thông tin mạng tại Việt Nam. Trong Luật an toàn thông tin mạng, lần đầu tiên thuật ngữ thông tin cá nhân được giải thích là “thông tin gắn với việc xác định danh tính của một người cụ thể”¹. Luật này cũng giải thích thuật ngữ “chủ thể thông tin cá nhân là người được xác định từ thông tin cá nhân đó”² đồng thời cũng quy định về “nguyên tắc bảo vệ thông tin cá nhân trên mạng” (Điều 16), “thu thập và sử dụng thông tin cá nhân” (Điều 17), “cập nhật, sửa đổi và hủy bỏ thông tin cá nhân” (Điều 18), yêu cầu “bảo đảm an toàn thông tin cá nhân trên mạng” (Điều 19) và “trách nhiệm của cơ quan quản lý nhà nước trong bảo vệ thông tin cá nhân trên mạng” (Điều 20).

3. Bất cập của pháp luật hiện hành về bảo vệ thông tin cá nhân

Hiện nay, pháp luật về bảo vệ thông tin cá nhân ở Việt Nam có những điểm bất cập sau:

Một là, khái niệm về thông tin cá nhân còn chưa thống nhất giữa các văn bản quy phạm pháp luật, trong Luật an toàn thông tin mạng đã đưa khái niệm về thông tin cá nhân, còn Nghị định số 52/2013/NĐ-CP, ngày 16/5/2013 của Chính phủ về thương mại điện tử lại quy định: “Thông tin cá nhân là các thông tin góp phần định danh một cá nhân cụ thể, bao gồm tên, tuổi, địa chỉ nhà riêng, số điện thoại, thông tin y tế,

1. Khoản 15, Điều 3 Luật an toàn thông tin mạng năm 2015.

2. Khoản 16, Điều 3 Luật an toàn thông tin mạng năm 2015.

số tài khoản, thông tin về các giao dịch thanh toán cá nhân và những thông tin khác mà cá nhân mong muốn giữ bí mật. Thông tin cá nhân trong Nghị định này không bao gồm thông tin liên hệ công việc và những thông tin mà cá nhân đã tự công bố trên các phương tiện truyền thông”¹. Trong khi Luật bảo vệ quyền lợi người tiêu dùng năm 2010 sử dụng từ “thông tin của người tiêu dùng”² để chứa đựng thông tin cá nhân của người tiêu dùng, thì Luật an toàn thông tin mạng và Nghị định số 52/2013/NĐ-CP lại dùng cụm từ “*thông tin cá nhân*”.

Hai là, Nghị định số 185/2013/NĐ-CP, ngày 15/11/2013 của Chính phủ Quy định xử phạt vi phạm hành chính trong hoạt động thương mại, sản xuất, buôn bán hàng giả, hàng cấm và bảo vệ quyền lợi người tiêu dùng (được sửa đổi, bổ sung bởi Nghị định số 124/2015/NĐ-CP). Nghị định số 185/2013/NĐ-CP đã đưa ra khái niệm “hàng giả” gồm hàng hóa không có giá trị sử dụng, công dụng; có giá trị sử dụng, công dụng không đúng với nguồn gốc bản chất tự nhiên, tên gọi của hàng hóa; có giá trị sử dụng, công dụng không đúng với giá trị sử dụng, công dụng đã công bố hoặc đăng ký³. Tiếp theo, tại Điều 11 quy định hình thức phạt tiền đối với hành vi buôn bán hàng giả không có giá trị sử dụng,

1. Khoản 13, Điều 3 Nghị định số 52/2013/NĐ-CP của Chính phủ về thương mại điện tử.

2. Điều 6 Luật bảo vệ quyền lợi người tiêu dùng năm 2010.

3. Khoản 8, Điều 3 Nghị định số 185/2013/NĐ-CP, ngày 15/11/2013 của Chính phủ Quy định xử phạt vi phạm hành chính trong hoạt động thương mại, sản xuất, buôn bán hàng giả, hàng cấm và bảo vệ quyền lợi người tiêu dùng.

công dụng, đồng thời đưa ra biện pháp khắc phục hậu quả là buộc tiêu hủy tang vật đối với hành vi vi phạm. Nghị định số 15/2020/NĐ-CP, ngày 03/02/2020 của Chính phủ 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 đã quy định về mức phạt tiền đối với việc thực hiện hành vi vi phạm thu thập thông tin cá nhân trái phép nhưng biện pháp khắc phục hậu quả thì lại không khác so với Nghị định số 185/2013/NĐ-CP. Nghị định số 185/2013/NĐ-CP quy định: “Phạt tiền từ 20.000.000 đồng đến 30.000.000 đồng đối với một trong các hành vi sau: a) Sử dụng không đúng mục đích thông tin cá nhân đã thỏa thuận khi thu thập hoặc khi chưa có sự đồng ý của chủ thể thông tin cá nhân; b) Cung cấp hoặc chia sẻ hoặc phát tán thông tin cá nhân đã thu thập, tiếp cận, kiểm soát cho bên thứ ba khi chưa có sự đồng ý của chủ thể thông tin cá nhân; c) Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác”¹ và nếu “Vi phạm các quy định về thay đổi họ tên, địa chỉ người nhận; chuyển tiếp, chuyển hoàn, rút lại bưu gửi; bưu gửi không có người nhận” thì biện pháp khắc phục hậu quả là buộc hoàn trả cước thu không đúng đối với hành vi vi phạm². Như vậy, giữa

1. Khoản 2, Điều 84 Nghị định số 15/2020/NĐ-CP, ngày 03/02/2020 của Chính phủ 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.

2. Điều 11 Nghị định số 15/2020/NĐ-CP, ngày 03/02/2020 của Chính phủ 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.

Nghị định số 185/2013/NĐ-CP và Nghị định số 15/2020/NĐ-CP tuy không có quá nhiều khác biệt về mức phạt tiền đối với việc thực hiện cùng một hành vi vi phạm (thu thập thông tin cá nhân trái phép) nhưng biện pháp khắc phục hậu quả thì lại không hoàn toàn giống nhau¹.

4. Kiến nghị

Để tăng cường các biện pháp bảo vệ thông tin cá nhân, xin đề xuất một số giải pháp sau:

Một là, ban hành Luật bảo đảm quyền được thông tin của công dân nhằm phòng, chống tham nhũng, lãng phí theo tinh thần Nghị quyết số 04-NQ/TW, ngày 21/8/2006 của Ban Chấp hành Trung ương Đảng (khóa X) về tăng cường sự lãnh đạo của Đảng đối với công tác phòng, chống tham nhũng, lãng phí đã đề ra chủ trương, giải pháp: “Bảo đảm công khai, minh bạch trong hoạt động của các cơ quan, tổ chức, đơn vị. Thực hiện nghiêm các quy định về công khai, minh bạch; bổ sung quy định bảo đảm minh bạch quá trình ra quyết định, bao gồm cả chính sách, văn bản quy phạm pháp luật và quyết định giải quyết một vụ việc cụ thể của cơ quan nhà nước các cấp”.

Hai là, Bộ luật dân sự nên sửa đổi quy định việc bồi thường thiệt hại đối với chủ thể có hành vi vi phạm theo hướng tạo điều kiện thuận lợi cho chủ thể thông tin bị xâm hại quyền lợi có thể khởi kiện đòi bồi thường thiệt hại.

1. Điều 11, Nghị định số 15/2020/NĐ-CP, ngày 03/02/2020 của Chính phủ 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.

Ba là, tăng cường các cơ quan quản lý nhà nước về bảo vệ thông tin cá nhân, quy định về thẩm quyền của cơ quan này trong việc xử lý các hành vi vi phạm trong bảo vệ thông tin cá nhân.

MỤC LỤC

| | Trang |
|--|-------|
| <i>Lời Nhà xuất bản</i> | 5 |
| - Quan điểm của Đảng và Nhà nước về bảo vệ chủ quyền quốc gia trên không gian mạng và bảo đảm an ninh mạng | 9 |
| Đồng chí NGUYỄN TRỌNG NGHĨA | |
| <i>Bí thư Trung ương Đảng,</i> | |
| <i>Trưởng Ban Tuyên giáo Trung ương</i> | |
| - Một số kinh nghiệm của Quân đội về chỉ đạo, tổ chức đấu tranh phản bác các quan điểm sai trái, thù địch trên không gian mạng | 25 |
| Trung tướng TRỊNH VĂN QUYẾT | |
| <i>Ủy viên Trung ương Đảng,</i> | |
| <i>Phó Chủ nhiệm Tổng cục Chính trị</i> | |
| <i>Quân đội nhân dân Việt Nam</i> | |
| - Bàn về chủ quyền quốc gia trên không gian mạng - Những yêu cầu bảo đảm các chỉ số an ninh, an toàn trong bối cảnh hiện nay | 39 |
| Thượng tướng, PGS.TS. NGUYỄN VĂN THÀNH | |
| <i>Phó Chủ tịch Hội đồng Lý luận Trung ương</i> | |

- Xuất bản sách lý luận, chính trị phục vụ sự nghiệp bảo vệ chủ quyền quốc gia trong tình hình mới 62
PGS.TS. PHẠM MINH TUẤN
Giám đốc - Tổng Biên tập
Nhà xuất bản Chính trị quốc gia Sự thật
- Nguy cơ, thách thức đặt ra đối với nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng trong tình hình mới 78
Thiếu tướng, TS. PHẠM VIỆT TRUNG
Phó Tư lệnh - Tham mưu trưởng
Bộ Tư lệnh tác chiến không gian mạng,
Bộ Quốc phòng
- Nâng cao ý thức làm chủ và bảo vệ không gian mạng của cán bộ, đảng viên hiện nay 92
PGS. TS. LÊ VĂN LỢI
Phó Giám đốc Học viện Chính trị quốc gia Hồ Chí Minh
- Bảo đảm an toàn thông tin trong truyền thông xã hội ở Việt Nam hiện nay 107
PGS.TS. VŨ TRỌNG LÂM
Phó Tổng Biên tập Tạp chí Cộng sản
TS. VŨ THỊ HƯƠNG
Nhà xuất bản Chính trị quốc gia Sự thật
- Tăng cường đấu tranh trên không gian mạng bảo vệ vững chắc nền tảng tư tưởng của Đảng 123
ThS. PHẠM THỊ THỊNH
Phó Giám đốc - Phó Tổng Biên tập
Nhà xuất bản Chính trị quốc gia Sự thật
- Mạng xã hội: Lợi ích và các mối đe dọa an ninh 139
ThS. NGUYỄN HOÀI ANH
Phó Giám đốc - Phó Tổng Biên tập
Nhà xuất bản Chính trị quốc gia Sự thật

- Tăng cường hợp tác quốc tế bảo vệ chủ quyền quốc gia trên không gian mạng 151

Thiếu tướng, PGS. TS. VŨ CƯỜNG QUYẾT
Viện trưởng Viện Chiến lược quốc phòng,
Bộ Quốc phòng

- Tính nhân bản tự nhiên - Phương pháp tiếp cận giá trị chung của quyền con người và chủ quyền quốc gia trong tư tưởng Hồ Chí Minh 163

TS. VÕ VĂN BÉ
Nhà xuất bản Chính trị quốc gia Sự thật
 ThS. PHAN DUY ANH
Trường Đại học Bách khoa,
Đại học Quốc gia Thành phố Hồ Chí Minh

- Những thách thức đối với việc bảo vệ chủ quyền quốc gia trên không gian mạng 178

Đại tá, TS. NGUYỄN CÔNG XUÂN
Viện Chiến lược quốc phòng,
Bộ Quốc phòng

- Ứng xử của các quốc gia trên không gian mạng: Tăng cường hợp tác và đấu tranh trên mặt trận ngoại giao 192

TS. CHU MINH THẢO
Viện Nghiên cứu chiến lược ngoại giao,
Bộ Ngoại giao

- Về chủ quyền không gian mạng trong quan hệ quốc tế của Trung Quốc và kinh nghiệm tham khảo cho Việt Nam 208

TS. NGUYỄN VIỆT LÂM
Phái đoàn đại diện thường trực Việt Nam
tại Liên hợp quốc, New York, Hoa Kỳ

- Nâng cao “sức đề kháng” với các luận điệu của các thế lực thù địch 230
- PGS. TS. NGUYỄN MINH TUẤN
Học viện Chính trị quốc gia Hồ Chí Minh
- Định hướng, giải pháp bảo vệ nền tảng tư tưởng của Đảng trên môi trường mạng xã hội ở Việt Nam hiện nay 241
- PGS. TS. MAI ĐỨC NGỌC
Học viện Chính trị quốc gia Hồ Chí Minh
- Ý nghĩa của việc sử dụng internet và mạng xã hội có trách nhiệm 258
- PGS. TS. NGUYỄN XUÂN TOÀN
Đại học Quốc gia Hà Nội
- Hoạt động xuất bản góp phần tuyên truyền, giáo dục nâng cao nhận thức về bảo vệ chủ quyền quốc gia trên không gian mạng 277
- ThS. PHẠM THỊ NGỌC BÍCH
ThS. NGUYỄN THỊ THÚY
Nhà xuất bản Chính trị quốc gia Sự thật
- Bảo đảm an toàn thông tin trong quá trình chuyển đổi số của doanh nghiệp 290
- Tập đoàn Công nghiệp - Viễn thông Quân đội (Viettel)*
- Mối quan hệ giữa an toàn thông tin và quá trình chuyển đổi số quốc gia 304
- ThS. ĐINH VĂN KẾT
*Cục An toàn thông tin,
Bộ Thông tin và Truyền thông*
- Nâng cao nhận thức của sinh viên đối với Luật an ninh mạng năm 2018 318
- LÊ MỘNG THƠ
*Trường Đại học Bách Khoa,
Đại học Quốc gia Thành phố Hồ Chí Minh*

- Những vấn đề đặt ra về bảo đảm an ninh kinh tế số của Việt Nam 328

Thượng tá, TS. HOÀNG MINH HUỆ
*Cục Khoa học, Chiến lược và Lịch sử Công an,
 Bộ Công an*
- Bảo vệ quyền về đời sống riêng tư trên môi trường không gian mạng theo pháp luật Việt Nam, kinh nghiệm quốc tế và kiến nghị hoàn thiện pháp luật 345

CAO HỒNG QUÂN
*Trường Đại học Bách khoa,
 Đại học Quốc gia Thành phố Hồ Chí Minh*

LÊ NHẬT HỒNG
Trường Đại học Luật Thành phố Hồ Chí Minh
- Thực trạng pháp luật Việt Nam về quyền bảo vệ thông tin cá nhân trên không gian mạng 362

HỒ BẢO
Trường Đại học Luật Thành phố Hồ Chí Minh
- Chủ thể dữ liệu, chủ thể kiểm soát dữ liệu và chủ thể xử lý dữ liệu trong pháp luật về bảo vệ dữ liệu cá nhân 379

ThS. NGUYỄN TẤN HOÀNG HẢI
 TRẦN VÕ KIỀU ANH
 HOÀNG THỊ KHÁNH HIỀN
 NGUYỄN PHẠM THANH HOA
Trường Đại học Luật Thành phố Hồ Chí Minh
- Quy định của pháp luật và vai trò của Nhà nước trong việc bảo đảm thi hành các quy định về an toàn, an ninh thông tin 392

ThS. NGUYỄN THANH QUYÊN
 ThS. HUỲNH THỊ HỒNG NHIÊN
Trường Đại học Luật Thành phố Hồ Chí Minh

- Quy định của pháp luật Việt Nam về an ninh mạng -
so sánh với pháp luật của một số quốc gia trên thế giới 410
ThS. NGUYỄN TRUNG DƯƠNG
Trường Đại học Luật Thành phố Hồ Chí Minh
- Pháp luật Việt Nam về giới hạn quyền tự do biểu đạt
trên không gian mạng 425
ThS. VŨ LÊ HẢI GIANG
Trường Đại học Luật Thành phố Hồ Chí Minh
- Giáo dục, nâng cao nhận thức cho sinh viên về bảo vệ
chủ quyền quốc gia trên không gian mạng 441
ThS. LÊ VŨ XUÂN UYÊN
*Học viện Chính trị khu vực II,
Học viện Chính trị quốc gia Hồ Chí Minh*
- Cô đơn trên mạng và nguy cơ bị tội phạm công nghệ cao
tấn công trong giới trẻ ở Việt Nam hiện nay 454
ThS. NCS. PHAN DUY ANH
*Trường Đại học Bách khoa,
Đại học Quốc gia Thành phố Hồ Chí Minh*
- Củng cố an toàn thông tin mạng thông qua việc xác
định trách nhiệm của chủ thể xử lý dữ liệu 466
TS. NGUYỄN THỊ HOA
Trường Đại học Luật Thành phố Hồ Chí Minh
- Nguyên tắc cấm sử dụng vũ lực và đe dọa sử dụng
vũ lực trong pháp luật quốc tế với hành vi tấn công mạng 482
TS. NGUYỄN THỊ THU TRANG
NGUYỄN ĐAN CHI
VŨ MINH THU
DƯƠNG THỊ HOÀI THƯƠNG
*Trường Đại học Kinh tế - Luật,
Đại học Quốc gia Thành phố Hồ Chí Minh*
- Quy định pháp luật về thông tin cá nhân và kiến nghị 498
ThS. NGUYỄN THỊ HỒNG HẠNH
Trường Đại học Luật Thành phố Hồ Chí Minh

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT

Số 6/86 Duy Tân, Cầu Giấy, Hà Nội, ĐT: 080 49221, Fax: 080 49222

Email: suthat@nxbctqg.vn, Website: www.nxbctqg.org.vn

Sách điện tử: www.stbook.vn, www.thuviencoso.vn

BẢO ĐẢM **CHỦ QUYỀN QUỐC GIA** **TRÊN KHÔNG GIAN MẠNG**

KỶ YẾU HỘI THẢO KHOA HỌC CẤP QUỐC GIA
TẬP 1



MÃ ĐỊNH DANH
CUỐN SÁCH



9 786045 772362



8935279135998

SÁCH NHÀ NƯỚC ĐẶT HÀNG