CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 327/2026/NĐ-CP	*Hà Nội, ngày 19 tháng 8 năm 2026*

NGHỊ ĐỊNH
Quy định về phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng

Căn cứ Luật Tổ chức Chính phủ số 63/2025/QH15;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Theo đề nghị của Bộ trưởng Bộ Công an;

Chính phủ ban hành Nghị định quy định về phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Nghị định này quy định chi tiết Điều 14 Luật An ninh mạng, bao gồm các nội dung sau:

1. Biện pháp phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

2. Thẩm quyền của lực lượng chuyên trách bảo vệ an ninh mạng, cơ quan có thẩm quyền, trách nhiệm của doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng, chủ quản hệ thống thông tin, tổ chức, cá nhân trong phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

3. Cơ chế phối hợp trong phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

Điều 2. Đối tượng áp dụng

1. Lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền về phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

2. Chủ quản hệ thống thông tin, doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng Việt Nam.

3. Tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng Việt Nam.

Điều 3. Giải thích từ ngữ

Trong Nghị định này những từ ngữ dưới đây được hiểu như sau:

1. Nhà cung cấp dịch vụ là doanh nghiệp, tổ chức, cá nhân trong và ngoài nước cung cấp các sản phẩm, dịch vụ trên không gian mạng tại Việt Nam, gồm: dịch vụ viễn thông, Internet, dịch vụ lưu trữ, máy chủ, tên miền, mạng riêng ảo (Virtual Private Network), máy chủ trung gian (Proxy), dịch vụ điện toán đám mây (Cloud Computing), mạng xã hội, trang thông tin điện tử, các tổ chức tài chính, tổ chức tín dụng, chi nhánh ngân hàng nước ngoài tại Việt Nam, tổ chức cung ứng dịch vụ trung gian thanh toán, các sàn giao dịch chứng khoán, sàn giao dịch tài sản số, sàn thương mại điện tử trong phạm vi cung cấp, quản lý, vận hành trên không gian mạng, truyền hình số, trò chơi trực tuyến, trí tuệ nhân tạo, lượng tử, dịch vụ máy chủ ẩn danh và các loại sản phẩm, dịch vụ khác trên không gian mạng.

2. Tổ chức, cá nhân sử dụng dịch vụ là tổ chức, cá nhân sử dụng, đăng ký sử dụng các sản phẩm, dịch vụ trên không gian mạng của nhà cung cấp dịch vụ.

3. Cơ quan có thẩm quyền phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng gồm: Bộ, cơ quan ngang bộ, Ủy ban nhân dân các cấp trong phạm vi chức năng quản lý nhà nước được giao; cơ quan, tổ chức khác được giao nhiệm vụ theo quy định của pháp luật.

4. Địa chỉ mạng là thông tin, dữ liệu điện tử dùng để định danh, nhận diện và xác định vị trí của thiết bị, hệ thống thông tin hoặc tài khoản khi tham gia mạng máy tính, mạng viễn thông hoặc Internet, bao gồm nhưng không giới hạn ở địa chỉ IP, địa chỉ MAC, tên miền, số nhận dạng thiết bị, thông tin tài khoản, thông tin cổng kết nối, dữ liệu định tuyến và các thông tin kỹ thuật có liên quan khác.

5. Tình huống khẩn cấp trên không gian mạng là sự việc đang xảy ra hoặc có nguy cơ xảy ra ngay lập tức liên quan đến thông tin hoặc hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng mà nếu không được ngăn chặn, xử lý kịp thời có thể gây thiệt hại nghiêm trọng hoặc đặc biệt nghiêm trọng đối với an ninh quốc gia, trật tự, an toàn xã hội hoặc tính mạng, tài sản của cơ quan, tổ chức, cá nhân.

Điều 4. Nguyên tắc phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng

1. Bảo đảm sự quản lý thống nhất của Nhà nước; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng và trách nhiệm của các cơ quan, tổ chức, cá nhân trong phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

2. Tôn trọng, bảo vệ quyền con người, quyền và lợi ích hợp pháp của tổ chức, cá nhân; bảo đảm lợi ích của Nhà nước theo quy định của pháp luật.

3. Việc phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng phải tuân thủ quy định của Luật An ninh mạng và pháp luật có liên quan; bảo đảm chính xác, kịp thời, đúng thẩm quyền.

4. Hoạt động phối hợp giữa lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền với nhà cung cấp dịch vụ, chủ quản hệ thống thông tin đẩy mạnh hợp tác quốc tế trên cơ sở tôn trọng độc lập, chủ quyền, toàn vẹn lãnh thổ, bình đẳng và cùng có lợi, không can thiệp vào công việc nội bộ của quốc gia khác theo các điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

5. Bảo đảm việc áp dụng các biện pháp quản lý, ngăn chặn phải khách quan, đúng pháp luật và hạn chế tối đa tác động không cần thiết đến hoạt động sản xuất, kinh doanh hợp pháp của doanh nghiệp và các chủ thể tham gia không gian mạng.

6. Bộ Quốc phòng quản lý về an ninh mạng đối với nhiệm vụ quân sự, quốc phòng; Bộ Công an quản lý về an ninh mạng đối với các đơn vị quân đội có hoạt động dân sự, kinh tế theo thẩm quyền; đối với các nội dung giao thoa (nếu có), Bộ Công an và Bộ Quốc phòng thống nhất quy chế phối hợp.

Chương II
PHÒNG NGỪA, XỬ LÝ THÔNG TIN VÀ HÀNH VI SỬ DỤNG CÔNG NGHỆ THÔNG TIN, MẠNG MÁY TÍNH, MẠNG VIỄN THÔNG, PHƯƠNG TIỆN ĐIỆN TỬ XÂM PHẠM AN NINH QUỐC GIA, TRẬT TỰ, AN TOÀN XÃ HỘI TRÊN KHÔNG GIAN MẠNG

Điều 5. Biện pháp phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ và phối hợp xử lý thông tin xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng

1. Chủ quản hệ thống thông tin, nhà cung cấp dịch vụ có trách nhiệm tiến hành các biện pháp:

a) Định danh, xác thực điện tử đối với tổ chức, cá nhân sử dụng dịch vụ trước và trong quá trình cung cấp dịch vụ; phát hiện, ngăn chặn hoạt động của tài khoản số không chính chủ; quản lý địa chỉ mạng của tổ chức, cá nhân sử dụng dịch vụ Internet theo quy định;

b) Chấp hành quy định của pháp luật về bảo vệ bí mật nhà nước, thời hạn bảo quản, lưu trữ, cung cấp thông tin, dữ liệu điện tử phục vụ công tác phòng ngừa, xử lý thông tin và hành vi vi phạm trên không gian mạng;

c) Phối hợp, tạo điều kiện cho lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền thực hiện nhiệm vụ;

d) Thực hiện theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng về việc kết nối, xây dựng hệ thống liên thông với nền tảng kỹ thuật số; tiếp nhận, trả lời văn bản điện tử phục vụ công tác bảo đảm an ninh mạng và phòng ngừa, xử lý thông tin và hành vi vi phạm trên không gian mạng;

đ) Cung cấp thông tin, tài liệu, dữ liệu điện tử đầy đủ, chính xác, đúng thời hạn, bảo đảm bí mật cho lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền theo quy định của pháp luật;

e) Thực hiện ngay các biện pháp cần thiết theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền khi nhận được thông tin cảnh báo về an ninh mạng và hành vi vi phạm trên không gian mạng;

g) Báo cáo lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền trong thời hạn 24 giờ kể từ khi phát hiện hành vi tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội;

h) Tổ chức cung ứng dịch vụ thanh toán, trung gian thanh toán, tài sản số có trách nhiệm theo quy định của pháp luật nếu tiếp tục cung ứng dịch vụ cho

tài khoản số trong danh sách cảnh báo của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền.

2. Tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng phải phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng, cơ quan có thẩm quyền, chủ quản hệ thống trong việc xử lý thông tin xâm phạm an ninh quốc gia, trật tự, an toàn xã hội theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng quy định tại Điều 7 của Nghị định này.

3. Quá trình phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ thông tin xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng, chủ quản hệ thống thông tin, nhà cung cấp dịch vụ có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng, cơ quan có thẩm quyền theo quy định tại Chương IV của Nghị định này.

Điều 6. Biện pháp phòng ngừa, phát hiện và phối hợp xử lý hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng

1. Chủ quản hệ thống thông tin và nhà cung cấp dịch vụ có trách nhiệm chủ động triển khai biện pháp kỹ thuật, quản lý để kiểm soát thông tin trên hệ thống; kịp thời thông báo, phối hợp lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền xử lý khi phát hiện thông tin thuộc các nhóm nội dung quy định tại Điều 13 Luật An ninh mạng.

2. Chủ quản hệ thống thông tin, nhà cung cấp dịch vụ có trách nhiệm áp dụng biện pháp quản lý, biện pháp kỹ thuật để phòng ngừa, phát hiện hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng, bao gồm:

a) Rà soát, nhận diện, đánh giá nguy cơ, dấu hiệu, phương thức, thủ đoạn, công cụ, tài khoản số, hội, nhóm, kênh, trang, ứng dụng, nền tảng, hệ thống thông tin, tên miền, địa chỉ mạng, đường dẫn, dữ liệu điện tử có dấu hiệu bị lợi dụng để thực hiện hành vi vi phạm pháp luật trên không gian mạng;

b) Thiết lập, duy trì cơ chế kiểm tra, giám sát, cảnh báo, phát hiện sớm, tiếp nhận phản ánh, tố giác, kiến nghị của tổ chức, cá nhân về hành vi vi phạm pháp luật trên không gian mạng;

c) Ngăn ngừa việc lợi dụng tài khoản số, danh tính điện tử, phương tiện điện tử, hạ tầng kỹ thuật, dịch vụ số để thực hiện hành vi vi phạm pháp luật;

d) Tổ chức quản lý, phân quyền, kiểm soát truy cập, ghi nhận và lưu giữ nhật ký hệ thống, dữ liệu điện tử cần thiết theo quy định của pháp luật nhằm phục vụ phát hiện, xác minh, xử lý hành vi vi phạm và bảo vệ quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

đ) Rà soát, loại bỏ hoặc vô hiệu hóa trong phạm vi quản lý của mình các công cụ, phần mềm, ứng dụng, tài khoản, đường dẫn, dữ liệu, cấu hình kỹ thuật có dấu hiệu trực tiếp phục vụ việc thực hiện hành vi vi phạm pháp luật trên không gian mạng theo quy định của pháp luật;

e) Áp dụng biện pháp bảo vệ trẻ em, người chưa thành niên, người cao tuổi, người khuyết tật và những người có nguy cơ bị xâm hại, bị lợi dụng, gặp khó khăn trong việc tự bảo vệ quyền và lợi ích hợp pháp trên không gian mạng; chủ động cảnh báo nguy cơ bị lừa đảo, chiếm đoạt tài sản, làm nhục, vu khống, xâm phạm bí mật đời sống riêng tư, truyền bá nội dung vi phạm pháp luật và các hành vi xâm hại khác;

g) Tuyên truyền, phổ biến pháp luật, nâng cao nhận thức, kỹ năng phòng ngừa, phát hiện, ứng phó với hành vi vi phạm pháp luật trên không gian mạng cho người sử dụng dịch vụ, cán bộ quản trị, người vận hành hệ thống thông tin và các chủ thể có liên quan;

h) Thực hiện yêu cầu, hướng dẫn, cảnh báo của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền; phối hợp ngăn chặn nguy cơ phát sinh, lan rộng hoặc tái diễn hành vi vi phạm.

3. Khi phát hiện dấu hiệu hành vi vi phạm pháp luật trên không gian mạng, nhà cung cấp dịch vụ, chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan có trách nhiệm áp dụng ngay biện pháp cần thiết trong phạm vi quản lý của mình để hạn chế hậu quả, bảo toàn dữ liệu điện tử, bảo đảm không làm mất, sai lệch, hư hỏng, tổn hại dữ liệu điện tử và kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền theo quy định của pháp luật.

4. Tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng phải phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng, cơ quan có thẩm quyền, chủ quản hệ thống trong việc xử lý hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng quy định tại Điều 7 của Nghị định này.

5. Quá trình phòng ngừa, phát hiện hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng, chủ quản hệ thống thông tin, nhà cung cấp dịch vụ có trách nhiệm phối hợp với lực lượng chuyên trách bảo

vệ an ninh mạng, cơ quan có thẩm quyền theo quy định tại Chương IV của Nghị định này.

Điều 7. Biện pháp xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng

Việc xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng được lực lượng chuyên trách bảo vệ an ninh mạng thực hiện bằng việc áp dụng một hoặc một số biện pháp quy định tại khoản 1 Điều 5 Luật An ninh mạng, phù hợp với tính chất, mức độ vi phạm. Nhà cung cấp dịch vụ, chủ quản hệ thống thông tin, tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng vi phạm quy định của Nghị định này tùy theo tính chất, mức độ vi phạm và hậu quả gây ra theo quy định tại Nghị định quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân sẽ bị áp dụng các biện pháp sau đây:

1. Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến trong các trường hợp sau:

a) Thông tin được cung cấp, truyền đưa có nội dung xâm phạm an ninh quốc gia, phương hại nghiêm trọng đến trật tự, an toàn xã hội; kích động bạo lực, biểu tình, bạo loạn chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

b) Hoạt động thiết lập, cung cấp dịch vụ mạng viễn thông, Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến nhằm mục đích truyền đưa thông tin không phép hoặc trái phép;

c) Phát hiện hành vi lợi dụng hạ tầng mạng để xâm nhập, truy cập trái phép, sửa đổi, xóa bỏ trái phép thông tin, chiếm quyền điều khiển thiết bị số, có hành vi cản trở, gây gián đoạn hoạt động cung cấp dịch vụ của hệ thống thông tin;

d) Khi phát hiện thông tin, dịch vụ viễn thông xâm phạm an ninh quốc gia, chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam hoặc sử dụng trong các kịch bản bạo động, bạo loạn;

đ) Nhà cung cấp dịch vụ không triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hoặc không thực hiện việc ngăn chặn, loại bỏ thông tin vi phạm theo yêu cầu của cơ quan có thẩm quyền; tự ý thay đổi, hủy bỏ hoặc vô hiệu hóa trái phép các biện pháp kỹ thuật được xây dựng, sử dụng để bảo vệ thông tin thuộc bí mật nhà nước;

e) Nhà cung cấp dịch vụ không thực hiện ngăn chặn, ngừng cung cấp dịch vụ viễn thông, Internet hoặc không bố trí cổng kết nối kỹ thuật theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng; không chấp hành quyết định huy động một phần hoặc toàn bộ cơ sở hạ tầng viễn thông, Internet trong trường hợp xử lý tình huống nguy hiểm về an ninh mạng;

g) Trường hợp khác theo quyết định của lực lượng chuyên trách bảo vệ an ninh mạng.

2. Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật, tin giả 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 trong các trường hợp sau:

a) Thông tin có nội dung sai sự thật, xuyên tạc, gây ảnh hưởng đến hoạt động bình thường hoặc uy tín của cơ quan, tổ chức, chính quyền Nhân dân; xúc phạm danh dự, nhân phẩm, bí mật đời tư của cá nhân;

b) Thông tin nhằm cổ súy, vận động hoặc dụ dỗ người khác thực hiện hành vi xâm hại an ninh quốc gia, trật tự, an toàn xã hội;

c) Thông tin vi phạm quy định về bảo vệ trẻ em trên môi trường mạng;

d) Thông tin kích động dâm ô, đồi trụy, tội phạm, mê tín dị đoan; vi phạm thuần phong mỹ tục;

đ) Thông tin mang tính đe dọa, kích động mâu thuẫn, chia rẽ, lôi kéo tụ tập đông người trái pháp luật gây tác động tiêu cực đến an ninh quốc gia, trật tự, an toàn xã hội;

e) Thông tin giả mạo, sai sự thật nhằm mục đích lừa đảo, chiếm đoạt tài sản;

g) Thông tin giả mạo, sai sự thật khác trong các lĩnh vực tài chính, ngân hàng, thương mại, đầu tư, giao thông, xây dựng, khoa học công nghệ, nông, lâm, ngư nghiệp và các lĩnh vực khác có nội dung xâm phạm an ninh quốc gia, trật tự, an toàn xã hội;

h) Trường hợp doanh nghiệp cung cấp dịch vụ, chủ quản hệ thống thông tin không thực hiện yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng về xóa bỏ thông tin vi phạm chậm nhất là 24 giờ (đối với tình huống khẩn cấp là 06 giờ) hoặc để ngăn chặn hậu quả nghiêm trọng xảy ra, lực lượng chuyên trách bảo vệ an ninh mạng được phép truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật, tin giả 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;

i) Trường hợp khác theo quyết định của lực lượng chuyên trách bảo vệ an ninh mạng.

3. Phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền trong các trường hợp sau:

a) Chủ quản hệ thống thông tin không đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin do mình quản lý; không triển khai biện pháp quản lý, kỹ thuật phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ, xóa bỏ thông tin vi phạm pháp luật theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng;

b) Chủ quản hệ thống thông tin thiết lập mạng xã hội, trang thông tin điện tử có nội dung vi phạm pháp luật mà không có giấy phép hoặc vi phạm quy định về trách nhiệm của tổ chức, doanh nghiệp thiết lập mạng xã hội;

c) Nhà cung cấp dịch vụ không thực hiện thu hồi tên miền sau khi có đề nghị của lực lượng chuyên trách bảo vệ an ninh mạng;

d) Chủ quản hệ thống thông tin, nhà cung cấp dịch vụ không hợp tác, cản trở quá trình thanh tra, kiểm tra, xử lý vi phạm của lực lượng chuyên trách bảo vệ an ninh mạng;

đ) Chủ quản hệ thống thông tin, nhà cung cấp dịch vụ không triển khai các biện pháp xử lý tình huống nguy hiểm về an ninh mạng hoặc không chấp hành quyết định huy động một phần hoặc toàn bộ cơ sở hạ tầng viễn thông, Internet phục vụ bảo đảm an ninh mạng;

e) Tên miền bị sử dụng để phát tán mã độc, lừa đảo, chiếm đoạt tài sản, tấn công mạng;

g) Hệ thống thông tin bị sử dụng làm phương tiện thu thập, chiếm đoạt trái phép thông tin, xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của tổ chức, cá nhân khác; cản trở hoạt động cung cấp dịch vụ của hệ thống khác;

h) Hoạt động vận hành hệ thống thông tin, nền tảng ứng dụng phân tích dữ liệu lớn vi phạm quy định về xử lý, kinh doanh, mua bán trái phép dữ liệu cá nhân quy mô lớn;

i) Trường hợp khác theo quyết định của lực lượng chuyên trách bảo vệ an ninh mạng.

4. Yêu cầu thiết lập cơ chế kiểm soát nội dung để phòng ngừa tái phạm trong các trường hợp sau:

a) Nền tảng, hệ thống thông tin cho phép người dùng dễ dàng tạo, chia sẻ nội dung vi phạm nhưng chưa có biện pháp kiểm soát phù hợp; có nguy cơ cao tái diễn hành vi phát tán thông tin vi phạm nếu không thiết lập cơ chế kiểm soát;

b) Nhà cung cấp dịch vụ, chủ quản hệ thống thông tin không có hoặc không thực hiện quy trình kiểm duyệt, cảnh báo, phát hiện nội dung vi phạm;

c) Hệ thống thông tin có lỗ hổng bảo mật bị lợi dụng thực hiện hành vi phát tán mã độc hoặc thông tin độc hại trên diện rộng;

d) Chủ quản hệ thống thông tin quản lý, điều hành trang thông tin điện tử, mạng xã hội nhưng không triển khai biện pháp phòng ngừa, phát hiện, ngăn chặn, gỡ, xóa bỏ thông tin có nội dung vi phạm pháp luật;

đ) Chủ quản hệ thống thông tin không áp dụng biện pháp quản lý hoặc biện pháp kỹ thuật theo tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng để phòng, chống nguy cơ, khắc phục sự cố an ninh mạng;

e) Doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, Internet, chủ quản hệ thống thông tin để xảy ra nhiều lần hành vi đăng tải, chia sẻ, phát tán thông tin vi phạm pháp luật;

g) Lực lượng chuyên trách bảo vệ an ninh mạng đã áp dụng các hình thức xử phạt đối với hành vi cung cấp, phát tán thông tin vi phạm nhưng chủ quản hệ thống, nhà cung cấp dịch vụ chưa có quy trình quản lý nội dung, chưa có biện pháp kỹ thuật tự động kiểm duyệt nhằm phát hiện, ngăn chặn hành vi vi phạm tái diễn;

h) Nền tảng vi phạm quy định về bảo vệ trẻ em, không tích hợp các biện pháp ngăn ngừa trẻ em truy cập thông tin không có lợi trên môi trường mạng hoặc không có dấu hiệu cảnh báo đối với sản phẩm, dịch vụ công nghệ thông tin có nội dung không phù hợp với trẻ em;

i) Trường hợp khác theo quyết định của lực lượng chuyên trách bảo vệ an ninh mạng.

5. Ngăn chặn truy cập từ lãnh thổ Việt Nam đối với hệ thống thông tin vi phạm trong các trường hợp sau:

a) Chủ quản hệ thống thông tin đặt tại nước ngoài không tuân thủ yêu cầu gỡ bỏ thông tin vi phạm, không cung cấp dữ liệu phục vụ công tác điều tra của lực lượng chuyên trách bảo vệ an ninh mạng;

b) Hệ thống thông tin có dấu hiệu phát tán mã độc, chiếm quyền điều khiển thiết bị; thực hiện tấn công mạng hoặc khủng bố mạng từ lãnh thổ nước ngoài ảnh hưởng đến hạ tầng quốc gia;

c) Hệ thống thông tin phục vụ hành vi cung cấp, chia sẻ, phát tán thông tin trên không gian mạng có nội dung vi phạm pháp luật, gây ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội đã bị xử lý nhưng tiếp tục tái phạm; chủ quản hệ thống không tuân thủ yêu cầu ngăn chặn, gỡ bỏ, xóa bỏ thông tin trái pháp luật của lực lượng chuyên trách bảo vệ an ninh mạng;

d) Nền tảng xuyên biên giới cung cấp, chia sẻ, phát tán thông tin có nội dung chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, kích động bạo loạn, gây rối trật tự công cộng;

đ) Hệ thống thông tin bị lợi dụng thực hiện hoạt động gián điệp mạng, khủng bố mạng hoặc tấn công xâm nhập trái phép, phá hoại hệ thống thông tin quan trọng về an ninh quốc gia nhưng chủ quản hệ thống không có biện pháp kiểm soát hoặc khắc phục sự cố kỹ thuật;

e) Hệ thống thông tin đặt tại nước ngoài xử lý dữ liệu cá nhân của công dân Việt Nam không tuân thủ các quy định pháp luật Việt Nam; chủ quản hệ thống không chấp hành quyết định xử phạt hành chính của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền;

g) Doanh nghiệp nước ngoài khi cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam không đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam, không thực hiện nghĩa vụ lưu trữ dữ liệu theo quy định của pháp luật Việt Nam;

h) Trường hợp khác theo quyết định của lực lượng chuyên trách bảo vệ an ninh mạng.

6. Yêu cầu lưu trữ, cung cấp dữ liệu phục vụ điều tra, xử lý theo quy định của pháp luật trong các trường hợp sau:

a) Khi lực lượng chuyên trách bảo vệ an ninh mạng phát hiện dấu hiệu tội phạm hoặc vi phạm hành chính cần xác minh, làm rõ;

b) Khi cần thu thập, đối chiếu thông tin để bảo vệ quyền, lợi ích hợp pháp của tổ chức, cá nhân bị ảnh hưởng;

c) Khi dữ liệu liên quan đến hành vi phát tán thông tin vi phạm hoặc sử dụng hệ thống để thực hiện hành vi vi phạm pháp luật;

d) Khi dữ liệu là bằng chứng liên quan đến hành vi vi phạm pháp luật;

đ) Trường hợp khác theo quyết định của lực lượng chuyên trách bảo vệ an ninh mạng.

7. Tạm dừng giao dịch tài khoản thanh toán liên quan theo quy định của pháp luật trong các trường hợp sau:

a) Tài khoản thanh toán, ví điện tử hoặc phương thức hỗ trợ thanh toán được xác định là phương tiện nhận tiền, chi trả, luân chuyển dòng tiền có nguồn gốc từ các hoạt động vi phạm pháp luật;

b) Chủ tài khoản thanh toán sử dụng thông tin giả mạo, giấy tờ giả hoặc thuê, mượn tài khoản của người khác để thực hiện các giao dịch đáng ngờ trên không gian mạng;

c) Phát hiện hoạt động sử dụng tài khoản số để mua bán, giao dịch, quy đổi trái phép ngoại tệ, tài sản số;

d) Phát hiện hoạt động sử dụng không gian mạng can thiệp vào hoạt động giao dịch, thay đổi tài khoản nhận tiền để lừa đảo, chiếm đoạt tài sản;

đ) Phát hiện hoạt động sử dụng không gian mạng huy động vốn theo phương thức lừa đảo, chiếm đoạt tài sản;

e) Phát hiện hoạt động mở tài khoản số không đúng trình tự, thủ tục hoặc duy trì tài khoản bằng thông tin định danh giả mạo;

g) Nhà cung cấp dịch vụ không tạm dừng giao dịch hoặc phong tỏa tài khoản số khi phát hiện có sai sót, nhầm lẫn, bị lộ lọt thông tin hoặc khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng;

h) Trường hợp khác theo quyết định của lực lượng chuyên trách bảo vệ an ninh mạng.

8. Ngoài các biện pháp xử lý quy định tại Điều này, nhà cung cấp dịch vụ, chủ quản hệ thống thông tin, tổ chức, cá nhân vi phạm có thể bị xử lý theo quy định của pháp luật về xử lý vi phạm hành chính, pháp luật hình sự và pháp luật có liên quan. Đồng thời phải khắc phục hậu quả do hành vi vi phạm gây ra; thông báo, cảnh báo cho tổ chức, cá nhân sử dụng dịch vụ có nguy cơ bị ảnh hưởng; thực hiện biện pháp bảo vệ quyền, lợi ích hợp pháp của tổ chức, cá nhân bị xâm hại theo quy định của pháp luật.

9. Trường hợp hành vi vi phạm có liên quan đến nhiều chủ thể, nhiều nền tảng, nhiều hệ thống thông tin, nhiều loại tài khoản số, giao dịch điện tử hoặc có yếu tố nước ngoài, việc xử lý được thực hiện theo cơ chế phối hợp quy định tại Chương IV của Nghị định này và quy định pháp luật có liên quan.

10. Việc xử lý hành vi vi phạm trên không gian mạng phải gắn với yêu cầu bảo toàn chứng cứ điện tử, ngăn chặn tái phạm, đồng thời bảo đảm quyền

con người, quyền công dân, bí mật nhà nước, bí mật công tác, bí mật kinh doanh, dữ liệu cá nhân và quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân theo quy định của pháp luật.

11. Nhà cung cấp dịch vụ, chủ quản hệ thống thông tin có trách nhiệm cung cấp thông tin, dữ liệu điện tử theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền phục vụ phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng:

a) Chậm nhất 24 giờ đối với yêu cầu thông thường;

b) Chậm nhất 03 giờ đối với tình huống khẩn cấp.

Chương III
THẨM QUYỀN CỦA LỰC LƯỢNG CHUYÊN TRÁCH BẢO VỆ AN NINH MẠNG VÀ CƠ QUAN CÓ THẨM QUYỀN TRONG PHÒNG NGỪA, XỬ LÝ THÔNG TIN VÀ HÀNH VI SỬ DỤNG CÔNG NGHỆ THÔNG TIN, MẠNG MÁY TÍNH, MẠNG VIỄN THÔNG, PHƯƠNG TIỆN ĐIỆN TỬ XÂM PHẠM AN NINH QUỐC GIA, TRẬT TỰ, AN TOÀN XÃ HỘI TRÊN KHÔNG GIAN MẠNG

Điều 8. Tuyên truyền, giáo dục về phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng

1. Lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền triển khai các biện pháp tuyên truyền, giáo dục về phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng. Nội dung thông tin, tuyên truyền, giáo dục bao gồm:

a) Chủ trương, chính sách, pháp luật của Nhà nước về phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng;

b) Vị trí, vai trò, tầm quan trọng của công tác phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng;

c) Phương thức, thủ đoạn, nguy cơ và tác hại của thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng;

d) Kiến thức, kỹ năng, kinh nghiệm nhận diện, tự bảo vệ, phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng; kỹ năng ứng phó khi bị tấn công, xâm nhập trái phép vào hệ thống thông tin, cơ sở dữ liệu;

đ) Trách nhiệm của nhà cung cấp dịch vụ, chủ quản hệ thống thông tin, tổ chức, cá nhân trong phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng;

e) Các nội dung khác có liên quan theo yêu cầu của công tác phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

2. Hình thức thông tin, tuyên truyền, giáo dục:

a) Gặp gỡ, trao đổi, đối thoại, thảo luận trực tiếp;

b) Thông qua các phương tiện thông tin đại chúng, hệ thống thông tin trên không gian mạng;

c) Thông qua hoạt động tại các cơ sở giáo dục, đào tạo;

d) Thông qua các cuộc thi tìm hiểu pháp luật, sinh hoạt cộng đồng;

đ) Thông qua các tổ chức chính trị - xã hội;

e) Các hình thức khác phù hợp với quy định của pháp luật.

Điều 9. Thẩm quyền của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền trong áp dụng các biện pháp phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng

1. Lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền áp dụng các biện pháp quy định tại Điều 5, Điều 6 và Điều 7 của Nghị định này theo thẩm quyền được giao và theo quy định của pháp luật có liên quan. Tiến hành các biện pháp nghiệp vụ theo quy định của pháp luật, thu thập thông tin,

tài liệu, dữ liệu điện tử để xác minh, làm rõ thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng; lực lượng chuyên trách bảo vệ an ninh mạng trực tiếp thực hiện hoặc thực hiện theo yêu cầu của cơ quan nhà nước có thẩm quyền các biện pháp thu thập bí mật dữ liệu điện tử trong quá trình điều tra vụ án hình sự theo thủ tục tố tụng đặc biệt.

2. Kiểm tra, phát hiện, thu thập, phân tích, trích xuất dữ liệu điện tử để khai thác thông tin, tài liệu phục vụ công tác phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

3. Yêu cầu nhà cung cấp dịch vụ, chủ quản hệ thống thông tin, tổ chức, cá nhân sử dụng dịch vụ cung cấp thông tin, tài liệu, đồ vật, phương tiện điện tử, dữ liệu điện tử; bố trí mặt bằng, cổng kết nối, các điều kiện cần thiết khác khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng để triển khai các phương tiện, biện pháp kỹ thuật kiểm tra, giám sát, thu thập dữ liệu điện tử phục vụ công tác phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

4. Yêu cầu hoặc phối hợp với cơ quan nhà nước có thẩm quyền yêu cầu nhà cung cấp dịch vụ, chủ quản hệ thống thông tin chặn truy cập, vô hiệu hóa, đóng tài khoản số, phong tỏa, mở phong tỏa tài khoản số, tạm dừng giao dịch, hoạt động của tài khoản số, định danh, xác thực lại tài khoản số, tạm đình chỉ, đình chỉ hoạt động của trang thông tin điện tử, hệ thống thông tin, phương tiện điện tử, cung cấp dịch vụ, thu hồi giấy phép hoạt động theo quy định của pháp luật.

5. Lực lượng chuyên trách bảo vệ an ninh mạng thực hiện dò quét, phát hiện lỗ hổng bảo mật, yêu cầu nhà cung cấp dịch vụ, chủ quản hệ thống thông tin có biện pháp khắc phục nhằm đảm bảo an toàn thông tin, an ninh mạng đối với hệ thống thông tin.

6. Lực lượng chuyên trách bảo vệ an ninh mạng sử dụng phần mềm, thiết bị, phương tiện điện tử phục hồi dữ liệu điện tử bị xóa để phục vụ công tác phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

7. Thu giữ, tạm giữ đồ vật, tài liệu, phương tiện điện tử, dữ liệu điện tử, tài sản số liên quan đến hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng theo quy định của pháp luật.

8. Cảnh báo, yêu cầu nhà cung cấp dịch vụ cảnh báo thông tin về an ninh mạng, tổ chức, cá nhân, tài khoản thanh toán, ví điện tử, tài khoản chứng khoán và các loại tài khoản số khác nghi vấn liên quan đến hoạt động vi phạm pháp luật phục vụ công tác phòng ngừa, ngăn chặn tội phạm và các hành vi vi phạm pháp luật khác có sử dụng công nghệ cao.

9. Lực lượng chuyên trách bảo vệ an ninh mạng xây dựng, tạo lập, quản lý hệ thống kết nối với các nhà cung cấp dịch vụ, chủ quản hệ thống thông tin để trao đổi, cung cấp thông tin, yêu cầu thực hiện các biện pháp phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

Điều 10. Trách nhiệm của tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng

1. Chịu trách nhiệm trước pháp luật về nội dung thông tin do mình tạo lập, đăng tải, lưu trữ, truyền đưa, chia sẻ, phát tán trên không gian mạng.

2. Không được lợi dụng không gian mạng để tạo lập, đăng tải, chia sẻ, phát tán thông tin xâm phạm an ninh quốc gia, trật tự, an toàn xã hội hoặc thực hiện hành vi vi phạm pháp luật.

3. Không được sử dụng công nghệ thông tin, phương tiện điện tử, trí tuệ nhân tạo, phần mềm, công cụ kỹ thuật để giả mạo, xuyên tạc, lừa đảo, kích động, dụ dỗ, xúi giục, hướng dẫn hoặc tiếp tay cho hành vi vi phạm pháp luật.

4. Thực hiện yêu cầu gỡ bỏ, cải chính, chấm dứt phát tán, cung cấp thông tin, dữ liệu liên quan khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền.

5. Chủ động thông báo, tố giác đến lực lượng chuyên trách bảo vệ an ninh mạng hoặc cơ quan có thẩm quyền, nhà cung cấp dịch vụ, chủ quản hệ thống thông tin khi phát hiện thông tin hoặc hành vi vi phạm pháp luật trên không gian mạng.

6. Có trách nhiệm gỡ bỏ thông tin vi phạm thuộc phạm vi quản lý khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền; việc gỡ bỏ bao gồm xóa bỏ nội dung vi phạm, loại bỏ bản sao, đường dẫn và nội dung chia sẻ lại có liên quan.

7. Thời hạn thực hiện nghĩa vụ gỡ bỏ: chậm nhất là 24 giờ kể từ khi nhận được yêu cầu; tình huống khẩn cấp thực hiện trong thời hạn chậm nhất là 06 giờ; đồng thời có trách nhiệm thông báo kết quả thực hiện theo yêu cầu.

8. Áp dụng các biện pháp kỹ thuật cần thiết để ngăn chặn việc tiếp tục lan truyền thông tin vi phạm trong phạm vi do mình quản lý, bao gồm: vô hiệu hóa chức năng chia sẻ, sao chép, phát tán; ngăn chặn việc đăng tải lại; loại bỏ liên kết, dữ liệu dẫn tới nội dung vi phạm theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền.

9. Cung cấp thông tin, tài liệu, dữ liệu điện tử liên quan đến nội dung vi phạm theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền; bảo đảm dữ liệu chính xác, đầy đủ, đúng định dạng và trong thời hạn chậm nhất là 24 giờ, tình huống khẩn cấp chậm nhất là 03 giờ.

10. Không được lập, điều hành, duy trì hội, nhóm, kênh, trang, tài khoản trên không gian mạng nhằm mục đích thực hiện hành vi vi phạm pháp luật hoặc tiếp tay cho hành vi vi phạm pháp luật; ban hành và công khai quy tắc cộng đồng, nội quy quản lý; tổ chức kiểm duyệt nội dung phù hợp với quy mô hoạt động của hội, nhóm, kênh, trang, tài khoản trên không gian mạng; chủ động loại bỏ thành viên, nội dung, liên kết, công cụ, bài viết, tài khoản có dấu hiệu vi phạm pháp luật.

11. Khóa, loại bỏ tài khoản, yêu cầu nhà cung cấp dịch vụ khóa, loại bỏ tài khoản gắn với các thông tin đăng ký của tổ chức, cá nhân nếu phát hiện tài khoản bị sử dụng trái phép mà không do mình ủy quyền hoặc đang bị sử dụng vào mục đích vi phạm pháp luật.

Chương IV
PHỐI HỢP GIỮA LỰC LƯỢNG CHUYÊN TRÁCH BẢO VỆ AN NINH MẠNG, CƠ QUAN CÓ THẨM QUYỀN VỚI CHỦ QUẢN HỆ THỐNG THÔNG TIN, NHÀ CUNG CẤP DỊCH VỤ TRONG PHÒNG NGỪA, XỬ LÝ THÔNG TIN VÀ HÀNH VI SỬ DỤNG CÔNG NGHỆ THÔNG TIN, MẠNG MÁY TÍNH, MẠNG VIỄN THÔNG, PHƯƠNG TIỆN ĐIỆN TỬ XÂM PHẠM AN NINH QUỐC GIA, TRẬT TỰ, AN TOÀN XÃ HỘI TRÊN KHÔNG GIAN MẠNG

Điều 11. Nội dung phối hợp

1. Chia sẻ thông tin, dữ liệu, cảnh báo sớm về nguy cơ, phương thức, thủ đoạn, hạ tầng, công cụ, hội, nhóm, tài khoản, ứng dụng, nền tảng có dấu hiệu vi phạm.

2. Phối hợp rà soát, phát hiện, ngăn chặn, bóc gỡ hạ tầng kỹ thuật, tài khoản số, dòng tiền, công cụ, phần mềm, hệ thống, dữ liệu có liên quan đến hành vi vi phạm.

3. Chia sẻ cảnh báo, thông tin nguy cơ, dấu hiệu vi phạm; xác minh thông tin, tài khoản số, địa chỉ mạng, đường dẫn, dữ liệu điện tử và các thông tin liên quan phục vụ phòng ngừa, phát hiện, ngăn chặn hành vi vi phạm.

4. Phối hợp ngăn chặn, gỡ bỏ thông tin vi phạm; tạm dừng, hạn chế, khôi phục quyền truy cập, sử dụng dịch vụ hoặc giao dịch điện tử theo yêu cầu hợp pháp của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền, phù hợp với pháp luật chuyên ngành.

5. Phối hợp bảo toàn dữ liệu, nhật ký hệ thống, chứng cứ điện tử; khắc phục hậu quả, phục hồi hệ thống; tuyên truyền, cảnh báo người sử dụng; hỗ trợ đào tạo, tập huấn, diễn tập, kiểm tra kỹ thuật.

6. Trong tình huống khẩn cấp đe dọa xâm hại an ninh quốc gia, trật tự, an toàn xã hội, đe dọa tính mạng con người hoặc gây hậu quả đặc biệt nghiêm trọng, lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền được yêu cầu thực hiện ngay biện pháp cần thiết theo Nghị định quy định chi tiết trình tự, thủ tục áp dụng một số biện pháp bảo vệ an ninh mạng; yêu cầu phải được xác nhận, hoàn thiện hồ sơ theo quy định của pháp luật.

7. Phối hợp xác minh, truy vết tài khoản số, thiết bị, địa chỉ định danh thiết bị khi tham gia mạng Internet hoặc mạng nội bộ (IP), dữ liệu định danh, dữ liệu giao dịch, tài sản số, dòng tiền điện tử.

8. Phối hợp khắc phục hậu quả, bảo vệ bị hại, cảnh báo người sử dụng, ngăn ngừa tái diễn.

9. Phối hợp sơ kết, tổng kết, thống kê, đánh giá tình hình, kiến nghị sửa đổi, bổ sung chính sách, pháp luật.

Điều 12. Phương thức phối hợp

1. Bằng văn bản giấy hoặc văn bản điện tử, hệ thống dữ liệu dùng chung, nền tảng kỹ thuật số, đường dây nóng hoặc phương thức điện tử khác theo quy định.

2. Thông qua cơ chế kết nối, chia sẻ dữ liệu, danh sách cảnh báo, cơ chế xử lý tự động, bán tự động, nền tảng phối hợp liên ngành theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng.

3. Thông qua họp liên ngành, tổ công tác, kế hoạch phối hợp chuyên đề hoặc hình thức khác do lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền quyết định.

Điều 13. Phối hợp xử lý tình huống khẩn cấp

1. Khi phát hiện tình huống khẩn cấp trên không gian mạng, chủ quản hệ thống thông tin, nhà cung cấp dịch vụ, cơ quan, tổ chức, cá nhân có liên quan phải:

a) Áp dụng ngay biện pháp cần thiết để hạn chế hậu quả;

b) Thông báo ngay cho lực lượng chuyên trách bảo vệ an ninh mạng;

c) Bảo toàn hiện trạng hệ thống, dữ liệu, chứng cứ điện tử;

d) Chấp hành ngay yêu cầu phối hợp, yêu cầu kỹ thuật, yêu cầu ngăn chặn của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền.

2. Lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với cơ quan, tổ chức, doanh nghiệp có liên quan xử lý tình huống khẩn cấp; trường hợp vượt thẩm quyền thì báo cáo cấp có thẩm quyền xem xét, quyết định.

Điều 14. Trách nhiệm trong công tác phối hợp

1. Lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm chủ trì hướng dẫn, đôn đốc, kiểm tra, tiếp nhận, xử lý yêu cầu phối hợp; cung cấp thông tin cần thiết cho các chủ thể có liên quan trong phạm vi pháp luật cho phép.

2. Chủ quản hệ thống thông tin, nhà cung cấp dịch vụ và cơ quan, tổ chức có liên quan có trách nhiệm chỉ định đầu mối phối hợp; tổ chức tiếp nhận yêu cầu trong tình huống khẩn cấp theo chế độ thường trực 24/24 giờ; thực hiện và phản hồi kết quả xử lý trong thời hạn theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền.

3. Bộ Công an chủ trì, phối hợp với các bộ, ngành có liên quan hướng dẫn biểu mẫu, phương thức gửi, tiếp nhận, xác thực, phản hồi yêu cầu phối hợp bằng văn bản và phương thức điện tử; hướng dẫn cơ chế lưu vết, kiểm tra, giám sát, tổng hợp, thống kê phục vụ quản lý nhà nước.

4. Bộ Quốc phòng chủ trì, phối hợp với Bộ Công an và các bộ, ngành có liên quan hướng dẫn biểu mẫu, phương thức gửi, tiếp nhận, xác thực, phản hồi yêu cầu phối hợp bằng văn bản và phương thức điện tử; hướng dẫn cơ chế lưu vết, kiểm tra, giám sát, tổng hợp, thống kê phục vụ quản lý nhà nước đối với hệ thống thông tin quân sự.

Chương V
ĐIỀU KHOẢN THI HÀNH

Điều 15. Hiệu lực thi hành

Nghị định này có hiệu lực thi hành kể từ ngày 19 tháng 8 năm 2026.

Điều 16. Trách nhiệm thi hành

Các Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Chủ tịch Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Nghị định này.

Nơi nhận:
- Ban Bí thư Trung ương Đảng;
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các bộ, cơ quan ngang bộ;
- HĐND, UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng Dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan trung ương của các tổ chức chính trị - xã hội;
- VPCP: BTCN, các PCN, Trợ lý TTg, các Vụ, Cục, Công báo;
- Lưu: VT, CĐS (02) 19

TM. CHÍNH PHỦ
KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG

Phạm Gia Túc