|  |  |
| --- | --- |
| **CHÍNH PHỦ**Số:/TTr-CP | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM****Độc lập - Tự do - Hạnh phúc***Hà Nội, ngày tháng năm 2025* |

# TỜ TRÌNH

**Dự thảo**

**Đề nghị xây dựng dự án Luật An ninh mạng**

Kính gửi: Quốc hội

Căn cứ quy định Luật Ban hành văn bản quy phạm pháp luật, Chính phủ báo cáo Quốc hội về đề xuất xây dựng dự án Luật An ninh mạng, như sau:

**I. SỰ CẦN THIẾT BAN HÀNH VĂN BẢN**

**1. Về cơ sở chính trị**

Trong bối cảnh Cách mạng công nghiệp lần thứ tư đang làm thay đổi mọi mặt của đời sống, với tầm nhìn chiến lược, Đảng và Nhà nước ta nhận thức rõ tầm quan trọng của không gian mạng. Các văn kiện, Nghị quyết của Đảng và Nhà nước gần đây tiếp tục đề ra nhiều chủ trương, định hướng quan trọng cho việc hoàn thiện thể chế về việc xác lập, bảo vệ chủ quyền quốc gia trên không gian mạng, như: Nghị quyết số 29-NQ/TW ngày 25/7/2018 của Bộ Chính trị 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 51-NQ/TW ngày 05/9/2019 của Bộ Chính trị về Chiến lược bảo vệ an ninh quốc gia, Nghị quyết số 44-NQ/TW ngày 24/11/2023 về Chiến lược bảo vệ Tổ quốc trong tình hình mới, Nghị quyết số 57-NQ/TW về Đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia, Nghị quyết số 68-NQ/TW về phát triển kinh tế tư nhân. Một số quan điểm chỉ đạo trọng tâm sau:

- Xây dựng không gian mạng quốc gia an toàn, lành mạnh, rộng khắp, tạo điều kiện thuận lợi cho phát triển kinh tế, văn hóa, xã hội, tăng cường quốc phòng, an ninh, mở rộng quan hệ hợp tác quốc tế,… góp phần thực hiện thắng lợi sự nghiệp xây dựng và bảo vệ Tổ quốc.

- An ninh mạng có vị trí đặc biệt quan trọng, là nhiệm vụ trọng yếu thường xuyên, vừa cấp bách, vừa lâu dài của cả hệ thống chính trị, của toàn dân, của các cấp, các ngành dưới sự lãnh đạo của Đảng, sự quản lý thống nhất của Nhà nước, trong đó lực lượng Công an nhân dân, Quân đội nhân dân giữ vai trò nòng cốt.

- Tăng cường bảo vệ an toàn, an ninh mạng các hệ thống thông tin quan trọng quốc gia và các hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, phát hiện và đấu tranh ngăn chặn các hoạt động xâm phạm an ninh quốc gia trên không gian mạng; khắc phục điểm yếu, lỗ hổng bảo mật, nguy cơ mất an toàn, an ninh mạng, an ninh thông tin.

- Phát triển không gian mạng an toàn, minh bạch và bền vững, sự phối hợp chặt chẽ giữa các cơ quan nhà nước, doanh nghiệp và người dân để tạo ra một môi trường mạng lành mạnh, vừa thúc đẩy đổi mới sáng tạo vừa đảm bảo an ninh quốc gia.

- Bảo vệ an ninh quốc gia, an ninh con người, an ninh kinh tế, an ninh mạng; giữ vững an ninh chính trị, trật tự, an toàn xã hội…”.

- Bảo đảm chủ quyền quốc gia trên không gian mạng; bảo đảm an ninh mạng, an ninh dữ liệu, an toàn thông tin của tổ chức và cá nhân là yêu cầu xuyên suốt, không thể tách rời trong quá trình phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia.

- Người dân, doanh nghiệp được tự do kinh doanh trong những ngành nghề pháp luật không cấm. Quyền kinh doanh chỉ có thể bị hạn chế vì lý do quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, đạo đức xã hội, môi trường và sức khoẻ của cộng đồng và phải được quy định trong luật

**2. Về cơ sở pháp lý**

Trong những năm qua, Việt Nam đã đạt được những thành tựu quan trọng trong việc bảo vệ không gian mạng quốc gia. Một trong những thành tựu nổi bật là việc xây dựng khung pháp lý vững chắc. Luật An ninh mạng năm 2018, Luật An toàn thông tin mạng năm 2015 là nền tảng quan trọng để bảo vệ không gian mạng và xử lý tội phạm mạng.

Ngày 19/02/2025, Quốc hội ban hành Nghị quyết số 190/2025/NQ-QH15 quy định về xử lý một số vấn đề liên quan đến sắp xếp tổ chức bộ máy nhà nước; Thông báo kết luận số 04/TB-BCĐTKNQ18 ngày 12/01/2025 của Ban Chỉ đạo Chính phủ tại Phiên họp thứ 9 thống nhất điều chỉnh một số nhiệm vụ của các Bộ, ngành về Bộ Công an, trong đó có nhiệm vụ bảo đảm an toàn thông tin mạng từ Bộ Thông tin và Truyền thông về Bộ Công an; Nghị định số 02/2025/NĐ-CP ngày 18/02/2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Công an; ngày 28/02/2025, Bộ Công an và Bộ Thông tin và Truyền thông tổ chức Lễ bàn giao công tác quản lý nhà nước về bảo đảm an toàn thông tin mạng từ Bộ Thông tin và Truyền thông về Bộ Công an; Quyết định số 1133/QĐ-BCA ngày 26/02/2025 của Bộ trưởng Bộ Công an phê duyệt Đề án tiếp nhận chức năng, nhiệm vụ bảo đảm an toàn thông tin mạng từ Bộ Thông tin và Truyền thông về Bộ Công an.

**3. Về cơ sở thực tiễn**

***a) Hạn chế, bất cập trong thi hành quy định về an ninh mạng giữa Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018***

Về bản chất công nghệ, an toàn thông tin mạng là một phần của an ninh mạng, nên hai vấn đề này thực sự có nhiều điểm tương đồng nhau, cụ thể: (1) Mục tiêu chính: Cả hai đều nhắm tới mục đích bảo vệ dữ liệu và hệ thống khỏi các mối đe dọa và tấn công. (2) Phương pháp: Đều sử dụng các biện pháp kỹ thuật và quy trình để đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của thông tin và hệ thống. (3) Kiểm soát truy cập: Áp dụng các biện pháp kiểm soát truy cập nhằm đảm bảo chỉ những người có quyền mới được truy cập vào các tài nguyên và thông tin. (4) Phát hiện và ngăn chặn: Cả hai lĩnh vực đều triển khai các giải pháp nhằm phát hiện và ngăn chặn các mối đe dọa từ bên ngoài và bên trong. (5) Đào tạo và nhận thức: Cả an toàn thông tin mạng và an ninh mạng đều chú trọng vào việc nâng cao nhận thức và đào tạo người dùng về các biện pháp bảo mật và cách phòng tránh các rủi ro bảo mật. (6) Cùng thực hiện chức năng quản lý nhà nước đối với thông tin, dữ liệu và hệ thống thông tin. Cùng thực hiện thanh tra, kiểm tra trên cùng một hệ, loại đối tượng, doanh nghiệp. Điều này khiến phát sinh nhiều mâu thuẫn, trùng dẫm trong khi triển khai công tác thực tế.

Cùng được bắt nguồn từ thuật ngữ “Cyber security”, hay còn gọi là an ninh mạng: trong khi Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao tập trung vào phạm vi rộng hơn là việc phòng ngừa, phát hiện, điều tra, xử lý, bảo vệ cơ sở hạ tầng không gian mạng, các hệ thống máy tính, hệ thống mạng, dữ liệu khỏi các mối đe dọa, bảo vệ an ninh quốc gia trên không gian mạng, trật tự an toàn xã hội thì Cục An toàn thông tin chỉ tập trung vào đảm bảo tính bảo mật, toàn vẹn và khả dụng của thông tin và hệ thống, gọi là “an toàn thông tin” - “safety information”.

Nhìn vào thực tiễn hiện nay, Việt Nam đang thực hiện cuộc cách mạng số với rất nhiều yếu tố thuận lợi về thể chế chính trị, kinh tế, xã hội, khoa học công nghệ để đưa đất nước bứt phá, bước vào kỷ nguyên vươn mình giàu mạnh. Việt Nam là một trong những quốc gia có tốc độ phát triển và ứng dụng Internet cao nhất thế giới, đứng đầu khu vực Đông Nam Á về số lượng tên miền quốc gia; có ngành công nghiệp thông tin có thứ hạng cao trong khu vực và trên thế giới; cơ sở hạ tầng số phát triển nhanh, cơ sở hạ tầng dữ liệu và mạng lưới trung tâm dữ liệu đang được cải thiện; Chính phủ điện tử dần toàn diện; dân số trẻ, có trình độ học vấn, tỷ lệ người dân dùng điện thoại thông minh và sử dụng các ứng dụng, dịch vụ trên không gian mạng, nhất là mạng xã hội ở mức cao. Đặc biệt, Việt Nam thường xuyên đứng trong danh sách 10 quốc gia có lưu lượng dữ liệu xuyên biên giới lớn nhất thế giới.

Đại hội XIII đã xác định: “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. Trong thực tiễn thời gian qua cho thấy, không gian mạng đã và đang làm thay đổi phương thức hoạt động, tổ chức cách thức tiến hành chiến tranh, can dự/can thiệp của các nước; cũng như nhiều khía cạnh khác của hoạt động an ninh, quân sự, tình báo, tội phạm. Tác chiến mạng đã trở thành một loại hình tác chiến hiện đại; an ninh mạng là ưu tiên hàng đầu trong chiến lược an ninh quốc gia của nhiều nước trên thế giới; thậm chí đã được sử dụng là lực lượng, chiến thuật tiên phong, mở đường cho hoạt động quân sự truyền thống; là vũ khí quan trọng để tiến hành âm mưu, ý đồ cách mạng sắc màu, cách mạng đường phố”.

Thực tiễn công tác bảo vệ an ninh mạng thời gian qua đã cho thấy, không gian mạng đang đặt ra nhiều nguy cơ, thách thức mới, đan xen, phức tạp đối với an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân, tác động trực tới cả công tác bảo đảm an ninh mạng và an toàn thông tin mạng, nổi lên là:

Thứ nhất, hoạt động tấn công mạng, gián điệp mạng và lộ, mất bí mật nhà nước tại Việt Nam diễn ra ngày càng phức tạp, ảnh hưởng nghiêm trọng đến an ninh quốc gia. Tin tặc sử dụng nhiều thủ đoạn tinh vi, không ngừng nâng cấp, cải tiến các dòng mã độc để tiến hành các chiến dịch tấn công mạng nhằm vào các cơ quan, tổ chức, doanh nghiệp của Việt Nam. Mục tiêu chủ yếu nhằm vào hệ thống mạng thông tin của các cơ quan Trung ương và các tập đoàn, doanh nghiệp quan trọng. Mục tiêu tấn công không chỉ nhằm thu thập thông tin tình báo, bí mật nhà nước, đặc biệt là các chủ trương, chính sách đối ngoại, an ninh, quốc phòng của Việt Nam mà còn chuẩn bị sẵn để tiến hành các hành động tình báo, phát động các cuộc tấn công phá hoại khi cần thiết. Hàng năm, Cục A05 phát hiện trên 2.600 trang/cổng TTĐT của Việt Nam (có tên miền “.vn”) bị tin tặc tấn công, thay đổi giao diện hoặc chèn tập tin; hàng chục vụ lộ tài liệu bí mật nhà nước với hàng trăm đầu tài liệu; hàng trăm TB dữ liệu của các bộ, ban, ngành, địa phương bị tin tặc chiếm đoạt, trong đó có nhiều tài liệu bí mật nhà nước. Một số cơ quan, đơn vị mặc dù đã được kiểm tra, cảnh báo về các nguy cơ gây mất an ninh mạng, lộ mất bí mật nhà nước, nhưng vấn để xảy ra tình trạng tiếp diễn.

Thứ hai, việc kiểm soát, quản trị và bảo vệ dữ liệu chưa tương xứng với giá trị và mức độ khai thác, sử dụng dữ liệu trong nền kinh tế số, xã hội số. Dữ liệu cá nhân đang được khai thác, sử dụng, tạo ra giá trị thặng dư một cách tự do, thiếu nguyên tắc và sự quản lý, dẫn tới thực trạng lộ, lọt, mua bán, xâm phạm dữ liệu cá nhân diễn ra phổ biến, ngày càng nghiêm trọng, kéo theo gia tăng các loại tội phạm mạng, tội phạm lừa đảo chiếm đoạt tài sản. Một số đường dây chiếm đoạt, mua bán dữ liệu quy mô lớn tại Việt Nam đã bị phát hiện, đấu tranh, xử lý. Số lượng dữ liệu cá nhân bị thu thập, mua bán trái phép phát hiện được lên tới hàng nghìn GB dữ liệu, trong đó có nhiều dữ liệu cá nhân nội bộ, nhạy cảm.

Thứ ba, hoạt động phá hoại tư tưởng, chống đối trong nước nhằm từng bước chuyển hóa chế độ chính trị ở nước ta diễn ra mạnh mẽ. Hàng năm, A05 rà soát, phát hiện hơn 7.500 nguồn khởi phát thông tin xấu độc, thu hút hơn 83 triệu lượt tiếp cận, tương tác thông tin, tập trung công kích, chống phá. Các hội nhóm “trái chiều”, bảo hiểm, bất động sản bị các tổ chức phản động lưu vong kích động, đã tổ chức tập trung đông người “đòi quyền lợi” và hoạt động chống phá nhân các sự kiện, ngày lễ lớn của đất nước.

Thứ tư, hoạt động sử dụng công nghệ cao để thực hiện hành vi phạm tội, xâm phạm TTATXH diễn ra ngày càng phức tạp, gây bức xúc trong xã hội, gây thiệt hại lớn về tài sản cho người dân, nhất là hoạt động lừa đảo, chiếm đoạt tài sản, đánh bạc và tổ chức đánh bạc, truyền bá văn hóa phẩm đồi trụy, mua bán vũ khí, vật liệu nổ, ma túy, bằng cấp giả. Đặc biệt, các nhóm tội phạm người nước ngoài có xu hướng dịch chuyển sang địa bàn Việt Nam để thực hiện hành vi phạm tội với nhiều thủ đoạn hoạt động mới tinh vi hơn, tập trung ở các tỉnh, thành phố lớn, khu du lịch, vùng ven biển có vị trí chiến lược, thiết yếu về an ninh quốc phòng như TP. Hồ Chí Minh, Hải Phòng, Quảng Ninh, Nha Trang, Đà Nẵng... Một số đối tượng người Trung Quốc còn móc nối, cấu kết với đối tượng người Việt Nam để lừa đảo, lôi kéo người Việt Nam sang Campuchia phạm tội sử dụng công nghệ cao, dưới hình thức giới thiệu “việc nhẹ, lương cao”. Năm 2024, đã xảy ra hơn 600 vụ lừa đảo tại 56 địa phương; với thủ đoạn được các đối tượng triệt để sử dụng là gọi điện, nhắn tin làm quen trên các trang mạng xã hội để hứa hẹn tặng quà, giả danh cơ quan thực thi pháp luật như: Công an, Viện Kiểm sát, Tòa án... yêu cầu người bị hại nộp tiền để lừa đảo, chiếm đoạt tài sản. Tội phạm tổ chức đánh bạc và đánh bạc trên mạng tiếp tục được phát hiện với số tiền đánh bạc lên tới hàng nghìn tỷ đồng.

Bối cảnh và tình hình trên đã đặt ra yêu cầu cấp bách là tiếp tục nhanh chóng hoàn thiện thể chế, chính sách pháp luật làm nền tảng vững chắc để thực hiện công tác quản lý nhà nước trên lĩnh vực an ninh mạng, đấu tranh phòng, chống tội phạm mạng, tội phạm sử dụng công nghệ cao, tội phạm xâm phạm dữ liệu cá nhân. Đặc biệt, theo tinh thần Nghị quyết số 18-NQ/TW ngày 25/10/2017 về một số vấn đề tiếp tục đổi mới, sắp xếp tổ chức bộ máy của hệ thống chính trị tinh gọn, hoạt động hiệu lực, hiệu quả và thực hiện Đề án tiếp nhận chức năng, nhiệm vụ bảo đảm an toàn thông tin mạng từ Bộ Thông tin và Truyền thông về Bộ Công an, công tác rà soát, đồng bộ hệ thống chính sách pháp luật trong lĩnh vực an ninh mạng, an toàn thông tin mạng là hết sức cần thiết để ổn định hoạt động của bộ máy bảo đảm thông suốt, không gián đoạn, góp phần bảo vệ an ninh mạng hiệu quả, toàn diện, thống nhất.

***b) Tạo cơ sở pháp lý cho tổ chức, triển khai các biện pháp bảo vệ an ninh mạng đối với các hệ thống thông tin quan trọng quốc gia theo chức năng, nhiệm vụ của lực lượng công an***

Theo quy định tại Luật An toàn thông tin mạng năm 2015, hệ thống thông tin quan trọng quốc gia là hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia”. Luật An ninh mạng năm 2018 đã dành riêng một chương (Chương II) để quy định về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia. Tại Chương này, Luật đã lý giải rõ hơn về hệ thống thông tin quan trọng về an ninh quốc gia, theo đó, hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng. Luật An toàn thông tin mạng phân loại hệ thống thông tin thành 5 cấp độ thì 03 cấp độ liên quan tới hệ thống thông tin quan trọng về an ninh quốc gia theo Luật An ninh mạng, 02 cấp độ chung còn lại thì thuộc đối tượng bảo vệ của an ninh mạng vì là thành phần của cơ sở hạ tầng không gian mạng quốc gia.

Nghị định số 53/2022/NĐ-CP của Chính phủ ngày 15/8/2022 quy định chi tiết một số điều của Luật An ninh mạng (Điều 3) một lần nữa khẳng định hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thống tin của cơ quan nhà nước và tổ chức chính trị của nước Cộng hòa xã hội chủ nghĩa Việt Nam. Những hệ thống này khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ tác động, gây hậu quả, thiệt hại nghiêm trọng đến an ninh thông tin, an ninh quốc gia, ảnh hưởng trực tiếp đến hoạt động, sự an toàn, ổn định, phát triển của hệ thống thông tin và chính trị, kinh tế - xã hội của đất nước.

Trong bối cảnh Việt Nam đang thực hiện chủ trương chuyển đổi số, xây dựng Chính phủ điện tử, phát triển kinh tế số, xã hội số, bảo đảm an ninh mạng đối với các hệ thống thông tin quan trọng về an ninh quốc gia trở thành nhiệm vụ quan trọng, cần quan tâm lãnh đạo, chỉ đạo, góp phần bảo đảm tuyệt đối an toàn trong xây dựng, hoạt động, nâng cấp, mở rộng các hệ thống thông tin quan trọng về an ninh quốc gia. Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia là nhiệm vụ của toàn Đảng, toàn dân, của tất cả các ngành, các cấp; trong đó, lực lượng Công an nhân dân đóng vai trò nòng cốt. Trong Công an nhân dân, lực lượng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thực hiện vai trò chủ động, tích cực của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia, được giao nhiệm vụ chủ trì, phối hợp với các đơn vị nghiệp vụ khác ở cả trong và ngoài ngành Công an tổ chức, triển khai các biện pháp, công tác bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Mặc dù, đã có nhiều quy định của pháp luật được ban hành và tổ chức triển khai trong thực tế nhằm bảo vệ an ninh mạng các hệ thống thông tin quan trọng về an ninh quốc gia. Tuy nhiên, hệ thống văn bản pháp luật về bảo đảm an toàn, an ninh mạng chưa đồng bộ, hiệu lực thi hành chưa cao. Các quy định của pháp luật về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia vẫn còn những hạn chế, bất cập nhất định, đó là:

(1) Danh mục hệ thống thông tin quan trọng về an ninh quốc gia chưa được ban hành để có căn cứ pháp lý xác định cụ thể, rõ ràng những hệ thống thông tin cần tập trung nguồn lực bảo vệ. Trong khi, Danh mục hệ thống thông tin quốc gia không bổ sung thêm hệ thống nào từ lúc Quyết định số 632/QĐ-TTg ngày 10/5/2017 của Thủ tướng Chính phủ được ban hành.

(2) Chưa có quy định về lực lượng chuyên trách bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia tại công an các đơn vị, địa phương. Nghị định số 53/2022/NĐ- CP của Chính phủ mới xác định lực lượng chuyên trách bảo vệ an ninh mạng trong lực lượng Công an là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an. Việc quy định như vậy đã vô tình làm giảm khả năng chủ động tác chiến, ứng phó trên không gian mạng của lực lượng Công an tại các đơn vị, địa phương.

(3) Một số quy định về xử phạt hành chính còn chưa thống nhất giữa các văn bản quy phạm pháp luật; một số quy định về công tác nghiệp vụ cơ bản của lực lượng Công an chưa phù hợp khi triển khai với đối tượng là hệ thống thông tin quan trọng về an ninh quốc gia (nhất là công tác điều tra cơ bản).

(4) Các điều ước quốc tế, hiệp định song phương, đa phương, các văn bản quy định về hợp tác giữa Việt Nam với các quốc gia, vùng lãnh thổ, giữa Bộ Công an với các cơ quan chuyên trách bảo vệ an ninh mạng của nước ngoài, với doanh nghiệp cung cấp dịch vụ qua biên giới vào Việt Nam còn ít, chưa thực sự tạo cơ chế, điều kiện để huy động tối đa mọi nguồn lực trong nước, nước ngoài phục vụ bảo vệ an ninh mạng các hệ thống thông tin quan trọng về an ninh quốc gia.

Từ tình hình trên, cần sớm hoàn thiện pháp luật về an ninh mạng đối với các hệ thống thông tin quan trọng về an ninh quốc gia theo chức năng, nhiệm vụ của lực lượng công an, trong đó quy định lực lượng chuyên trách, chủ lực bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an. Đồng thời, xác định lực lượng Công an tại các đơn vị, địa phương cũng là một trong những thành tố của lực lượng chuyên trách bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; (3) Bổ sung quy định tăng thêm trách nhiệm của công an các tỉnh, thành phố trực thuộc trung ương, nhất là phòng an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao của cơ quan công an các địa phương trong triển khai các biện pháp nghiệp vụ chuyên biệt bảo vệ an ninh HTTT quan trọng quốc gia.

***c) Cắt giảm thủ tục hành chính cải thiện môi trường kinh doanh sản phẩm, dịch vụ an ninh mạng***

Trong những năm qua, thực tiễn triển khai Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018 đã bộc lộ một số hạn chế nhất định, ảnh hưởng đến môi trường kinh doanh và hiệu quả quản lý nhà nước. Cụ thể, mặc dù hai luật này có mục tiêu và phạm vi điều chỉnh khác nhau, nhưng trong quá trình áp dụng lại xuất hiện nhiều quy định trùng lặp hoặc giao thoa, đặc biệt là trong lĩnh vực quản lý sản phẩm, dịch vụ an toàn thông tin mạng và an ninh mạng. Điều này dẫn đến việc doanh nghiệp, tổ chức phải thực hiện nhiều thủ tục hành chính tương tự nhau tại các cơ quan quản lý khác nhau, làm tăng chi phí tuân thủ và kéo dài thời gian đưa sản phẩm, dịch vụ ra thị trường.

Ví dụ, nhiều doanh nghiệp khi đăng ký chứng nhận hoặc công bố hợp quy đối với sản phẩm an toàn thông tin mạng vừa phải tuân thủ quy định của Luật An toàn thông tin mạng, vừa phải đáp ứng thêm yêu cầu về an ninh mạng theo Luật An ninh mạng. Sự thiếu đồng bộ này không chỉ làm nảy sinh thủ tục chồng chéo mà còn gây khó khăn trong việc xác định cơ quan đầu mối xử lý hồ sơ và giải quyết thủ tục hành chính.

Ngoài ra, môi trường pháp lý chưa thực sự rõ ràng và minh bạch khiến nhiều doanh nghiệp, đặc biệt là doanh nghiệp nhỏ và vừa, e ngại khi đầu tư vào lĩnh vực sản phẩm, dịch vụ an toàn thông tin mạng và an ninh mạng. Điều này phần nào cản trở mục tiêu phát triển ngành công nghiệp an toàn thông tin mạng trong nước, vốn đang rất cần thiết trước các nguy cơ, thách thức ngày càng gia tăng trên không gian mạng.

Việc hợp nhất hai Luật thành một Luật duy nhất là giải pháp căn cơ nhằm khắc phục những hạn chế nêu trên. Luật hợp nhất sẽ loại bỏ các quy định trùng lặp, làm rõ phạm vi, trách nhiệm của các cơ quan quản lý nhà nước, đồng thời thiết kế lại các quy trình, thủ tục hành chính theo hướng đơn giản, tinh gọn và hiệu quả hơn. Khi đó, doanh nghiệp chỉ cần thực hiện một bộ thủ tục nhất quán, rõ ràng, giảm bớt thời gian và chi phí không cần thiết. Bên cạnh đó, môi trường pháp lý ổn định và minh bạch hơn sẽ khuyến khích các doanh nghiệp mạnh dạn đầu tư, đổi mới và phát triển sản phẩm, dịch vụ an toàn thông tin mạng và an ninh mạng, góp phần nâng cao năng lực bảo vệ không gian mạng quốc gia, đồng thời thúc đẩy phát triển kinh tế số.

**Như vậy**:

(1) Việc xây dựng dự án Luật An ninh mạng trên cơ sở hợp nhất Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018 là hết sức cần thiết nhằm đáp ứng yêu cầu bảo vệ chủ quyền không gian mạng quốc gia, bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội, bảo vệ quyền và lợi ích hợp pháp của các cơ quan, tổ chức, cá nhân khi tham gia không gian mạng.

(2) Việc xây dựng dự án Luật An ninh mạng phù hợp với chủ trương quan trọng, đúng đắn của Đảng, Nhà nước, khắc phục được một số hạn chế, bất cập trong công tác quản lý nhà nước về an ninh mạng trong thời gian qua.

**II. MỤC ĐÍCH, QUAN ĐIỂM CHỈ ĐẠO XÂY DỰNG LUẬT**

**1. Mục đích**

- Bảo đảm tính thống nhất, đồng bộ của hệ thống pháp luật, loại bỏ sự chồng chéo, mâu thuẫn giữa hai luật hiện hành, tạo khung pháp lý rõ ràng, minh bạch, đáp ứng yêu cầu quản lý và bảo vệ không gian mạng.

- Nâng cao hiệu quả của hoạt động bảo đảm an ninh mạng, kết hợp chặt chẽ các biện pháp bảo vệ hệ thống thông tin, dữ liệu cá nhân, phòng chống tấn công mạng với các giải pháp bảo đảm an ninh quốc gia trên không gian mạng.

- Tạo điều kiện thuận lợi cho tổ chức, doanh nghiệp và cá nhân trong việc tuân thủ pháp luật, giảm thiểu thủ tục hành chính, đồng thời bảo vệ quyền lợi hợp pháp, thúc đẩy môi trường số an toàn, phát triển kinh tế số bền vững.

- Hoàn thiện cơ chế phòng thủ, giám sát, cảnh báo và ứng phó với các nguy cơ, sự cố an ninh mạng, bảo vệ hệ thống thông tin quan trọng quốc gia, tăng cường năng lực phòng ngừa và khắc phục hậu quả của các cuộc tấn công mạng.

- Đáp ứng yêu cầu hội nhập quốc tế, phù hợp với các cam kết, chuẩn mực quốc tế về an ninh mạng, thúc đẩy nghiên cứu, phát triển công nghệ và nâng cao năng lực cạnh tranh của Việt Nam trong lĩnh vực an ninh mạng.

**2. Quan điểm**

Một là, bảo đảm chủ quyền, an ninh quốc gia và trật tự, an toàn xã hội trên không gian mạng; Tạo cơ sở pháp lý vững chắc để bảo vệ lợi ích quốc gia, phòng ngừa, phát hiện, đấu tranh và xử lý các mối đe dọa từ không gian mạng, góp phần giữ vững ổn định chính trị, bảo vệ hệ thống chính trị, quốc phòng, an ninh và sự phát triển bền vững của đất nước.

Hai là, tạo lập môi trường mạng an toàn, lành mạnh, bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân; Quy định rõ trách nhiệm của các bên liên quan trong việc bảo vệ dữ liệu cá nhân, thông tin quan trọng, ngăn chặn các nội dung xấu độc, tin giả, thông tin sai lệch nhằm bảo đảm niềm tin số và sự phát triển lành mạnh của không gian mạng Việt Nam.

Ba là, nâng cao năng lực phòng thủ và ứng phó với các nguy cơ, thách thức từ không gian mạng; Quy định cơ chế giám sát, cảnh báo sớm và phương án ứng phó hiệu quả với các cuộc tấn công mạng, đảm bảo an ninh mạng cho các hệ thống thông tin quan trọng quốc gia.

Bốn là, thúc đẩy nghiên cứu, phát triển và làm chủ công nghệ an ninh mạng; khuyến khích tổ chức, cá nhân nghiên cứu, phát triển các sản phẩm, dịch vụ, công nghệ an ninh mạng nội địa, góp phần bảo đảm an ninh mạng quốc gia, nâng cao năng lực cạnh tranh, tiến tới tự chủ trong lĩnh vực an ninh mạng.

Năm là, tăng cường hợp tác quốc tế và huy động sự tham gia của toàn xã hội trong bảo đảm an ninh mạng; Hợp tác quốc tế trên cơ sở tôn trọng chủ quyền quốc gia, tuân thủ luật pháp quốc tế và các điều ước quốc tế mà Việt Nam là thành viên; Huy động sự tham gia của cơ quan nhà nước, tổ chức, doanh nghiệp và người dân trong công tác bảo vệ an ninh mạng, phát triển không gian mạng an toàn, lành mạnh và rộng khắp.

**III. PHẠM VI ĐIỀU CHỈNH, ĐỐI TƯỢNG ÁP DỤNG**

**1. Phạm vi điều chỉnh**

Luật này quy định về hoạt động bảo đảm an ninh mạng nhằm bảo vệ chủ quyền không gian mạng quốc gia, bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội, bảo vệ quyền và lợi ích hợp pháp của các cơ quan, tổ chức, cá nhân khi tham gia không gian mạng.

**2. Đối tượng áp dụng**

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 các hoạt động trên không gian mạng tại Việt Nam.

**3. Tên gọi của Luật**

Việc hợp nhất Luật An toàn thông tin mạng năm 2015, Luật An ninh mạng năm 2018 và lấy tên là Luật An ninh mạng xuất phát từ nhiều lý do. Trước hết, Luật An ninh mạng có phạm vi điều chỉnh rộng hơn, không chỉ tập trung vào bảo vệ thông tin mà còn bao quát các vấn đề về bảo vệ an ninh quốc gia và trật tự an toàn xã hội trên không gian mạng, trong khi Luật An toàn thông tin mạng chủ yếu liên quan đến khía cạnh kỹ thuật và bảo vệ thông tin mạng, hệ thống tin. Bên cạnh đó, an ninh mạng là lĩnh vực mang tính chiến lược, gắn với chủ quyền và an ninh quốc gia, nên việc đặt tên theo hướng này thể hiện sự ưu tiên cao trong chính sách pháp luật của Nhà nước trong giai đoạn hiện tại. Ngoài ra, trong bối cảnh các mối đe dọa trên không gian mạng ngày càng phức tạp, nhiều quốc gia cũng đang tập trung xây dựng pháp luật theo hướng toàn diện về an ninh mạng. Việc sử dụng tên gọi “Luật An ninh mạng” còn giúp tạo sự thống nhất, dễ hiểu và thuận tiện cho người dân, doanh nghiệp khi tiếp cận và thực thi pháp luật.

**IV. BỐ CỤC, NỘI DUNG CƠ BẢN CỦA DỰ THẢO LUẬT**

1. **Bố cục, nội dung cơ bản của dự thảo Luật**

Với phạm vi điều chỉnh như trên, bố cục của dự thảo Luật An ninh mạng gồm 08 chương, 58 điều. Cụ thể như sau:

Chương I. Những quy định chung (gồm 10 điều: từ Điều 1 đến Điều 10);

Chương II. Hoạt động bảo đảm an ninh mạng (gồm 03 mục, 18 điều: từ Điều 11 đến Điều 28);

Chương III. Phòng, chống tội phạm sử dụng công nghệ cao (gồm 06 điều: từ Điều 29 đến Điều 34);

Chương IV. Tiêu chuẩn, quy chuẩn an ninh mạng (gồm 03 điều: từ Điều 35 đến Điều 37);

Chương V. Sản phẩm, dịch vụ an ninh mạng (gồm 02 mục, 05 điều: từ Điều 38 đến Điều 42);

Chương VI. Điều kiện bảo đảm an ninh mạng (gồm 09 điều: Điều 43 đến Điều 51);

Chương VII. Quản lý nhà nước về an ninh mạng (gồm 05 điều: Điều 52 đến Điều 56);

Chương VIII. Điều khoản thi hành (gồm 02 điều: từ Điều 57 và Điều 58).

1. **Nội dung cơ bản của dự thảo văn bản**

***2.1. Những quy định chung***

Chương này quy định về phạm vi điều chỉnh; đối tượng áp dụng; giải thích từ ngữ; chính sách của Nhà nước về an ninh mạng; nguyên tắc bảo vệ an ninh mạng; biện pháp bảo vệ an ninh mạng; bảo vệ không gian mạng quốc gia; hợp tác quốc tế về an ninh mạng; các hành vi bị nghiêm cấm về an ninh mạng và xử lý vi phạm pháp luật về an ninh mạng. Trong đó:

- Phạm vi điều chỉnh của Luật là quy định về hoạt động bảo đảm an ninh mạng nhằm bảo vệ chủ quyền không gian mạng quốc gia, bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội, bảo vệ quyền và lợi ích hợp pháp của các cơ quan, tổ chức, cá nhân khi tham gia không gian mạng, bao gồm: bảo vệ thông tin mạng, bảo vệ hệ thống thông tin, phòng ngừa, xử lý hành vi xâm phạm an ninh mạng, phòng chống tội phạm mạng, tội phạm sử dụng công nghệ cao, tiêu chuẩn, quy chuẩn an ninh mạng, sản phẩm, dịch vụ an ninh mạng, điều kiện bảo đảm an ninh mạng, quản lý nhà nước về an ninh mạng và trách nhiệm của các chủ thể trong việc tuân thủ quy định pháp luật về an ninh mạng.

- Định nghĩa các từ, cụm từ được sử dụng trong Luật An ninh mạng nhằm đảm bảo cách hiểu thống nhất, chẳng hạn như: an ninh mạng, không gian mạng, hệ thống thông tin, tội phạm sử dụng công nghệ cao... Đây là nội dung rất quan trọng để xác định nội hàm, phạm vi của Luật An ninh mạng. Cụ thể, trong dự thảo Luật An ninh mạng dự kiến định nghĩa như sau:

*“An ninh mạng là sự bảo đảm an toàn, ổn định, bền vững của thông tin, hệ thống thông tin, không gian mạng và phòng, chống các hoạt động trên không gian mạng 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”.*

*“Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian”.*

- Để đảm bảo an ninh mạng dự thảo Luật có quy định về các nguyên tắc, biện pháp bảo vệ an ninh mạng, bảo vệ không gian mạng và các hành vi bị nghiêm cấm về an ninh mạng

***2.2. Hoạt động bảo đảm an ninh mạng***

Chương này quy định về các hoạt động bảo vệ thông tin mạng; bảo vệ hệ thống thông tin; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng. Trong đó:

- Về hoạt động bảo vệ thông tin mạng bao gồm: phân loại, quản lý gửi thông tin trên mạng; trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo vệ thông tin mạng; bảo đảm an ninh thông tin trên không gian mạng. Đây là quy định được kế thừa từ Luật An toàn thông tin mạng năm 2015 và bổ sung nội dung “bảo đảm an ninh thông tin” từ Luật An ninh mạng năm 2018.

- Quy định về bảo vệ hệ thống thông tin, trong đó có phân loại cấp độ hệ thống thông tin, nhiệm vụ bảo vệ hệ thống thông tin, biện pháp bảo vệ hệ thống thông tin, giám sát an ninh hệ thống thông tin, trách nhiệm của chủ quản hệ thống thông tin, kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng quốc gia, bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế, triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương.

- Quy định về phòng ngừa, xử lý hành vi xâm phạm an ninh mạng kế thừa các nội dung từ Luật An ninh mạng năm 2018 và bổ sung thêm các nội dung: phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại; ngăn chặn xung đột thông tin trên mạng từ Luật An toàn thông tin năm 2015.

***2.3. Phòng, chống tội phạm sử dụng công nghệ cao***

Chương này quy định về hoạt động phòng ngừa, phát hiện, xử lý tội phạm sử dụng công nghệ cao, trách nhiệm của cơ quan, tổ chức, doanh nghiệp và cá nhân trong phòng, chống tội phạm sử dụng công nghệ cao. Đây là nội dung mới được xây dựng trên cơ sở việc tội phạm mạng sử dụng công nghệ cao để tiến hành lừa đảo hiện nay.

***2.4. Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng***

Chương này quy định về hoạt động quản lý tiêu chuẩn, quy chuẩn trong lĩnh vực an ninh mạng. Kế thừa nội dung về quản lý tiêu chuẩn, quy chuẩn tại Luật An toàn thông tin mạng năm 2015. Trong đó, bổ sung thêm quy định về nhãn an ninh mạng.

*“Nhãn an ninh mạng là chứng nhận do Bộ Công an cấp cho sản phẩm, dịch vụ an ninh mạng hợp chuẩn, hợp quy khi doanh nghiệp, cá nhân có yêu cầu. Chính phủ quy định cụ thể về nhãn an ninh mạng”.*

***2.5. Sản phẩm, dịch vụ an ninh mạng***

Chương này quy định về hoạt động kinh doanh, xuất nhập, khẩu sản phẩm, dịch vụ an ninh mạng và giao trách nhiệm theo thẩm quyền cho Chính phủ và các bộ, ngành quy định chi tiết về điều kiện, trình tự thủ tục cấp phép kinh doanh sản phẩm dịch vụ an ninh mạng.

***2.6. Điều kiện bảo đảm an ninh mạng***

Chương này quy định về hoạt động nghiên cứu, phát triển an ninh mạng; nâng cao năng lực tự chủ về an ninh mạng; lực lượng bảo vệ an ninh mạng; bảo đảm nguồn nhân lực bảo vệ an ninh mạng; tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng; giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng; phổ biến kiến thức về an ninh mạng; kinh phí bảo vệ an ninh mạng và Văn bằng, chứng chỉ đào tạo về an ninh mạng.

***2.7. Quản lý nhà nước về an ninh mạng***

Chương này quy định về trách nhiệm và nội dung quản lý nhà nước về an ninh mạng trên cơ sở kế thừa các nội dung về quản lý nhà nước về an toàn thông tin tại Luật An toàn thông tin mạng năm 2015 và quản lý nhà nước về an ninh mạng tại Luật An ninh mạng năm 2018.

***2.8. Điều khoản thi hành***

Chương này quy định về hiệu lực và quy định chuyển tiếp, thay thế các quy định có hiện hành có liên quan tại Luật An toàn thông tin mạng năm 2015; Luật An ninh mạng năm 2018 và các văn bản quy phạm pháp luật khác.

**V. QUÁ TRÌNH LẬP HỒ SƠ ĐỀ NGHỊ XÂY DỰNG LUẬT**

**1**. Thực hiện Nghị quyết Chính phủ số 169/NQ-CP ngày 11/6/2025 về việc bổ sung dự án Luật An ninh mạng vào Chương trình lập pháp Quốc hội năm 2025; Tờ trình Chính phủ số 531/TTr-CP ngày 18/6/2025 về việc đề nghị bổ sung dự án Luật An ninh mạng vào Chương trình lập pháp năm 2025; y kiến của Ủy ban Quốc phòng và An ninh của Quốc hội tại công văn số /UBQPAN15 ngày / /2025 về rà soát, đề xuất bổ sung nhiệm vụ lập pháp mới của Chính phủ, giao Chính phủ xây dựng Luật An ninh mạng theo trình tự, thủ tục rút gọn, trình cho ý kiến và thông qua tại kỳ họp thứ 10 (tháng 10/2025), căn cứ quy định tại Luật Ban hành văn bản quy phạm pháp luật năm 2025; Bộ Công an đã chuẩn bị dự thảo hồ sơ đề nghị xây dựng Luật An ninh mạng theo quy định của Luật Ban hành văn bản quy phạm pháp luật.

**2.** Ngày / /2025, Bộ Tư pháp đã tổ chức Hội đồng thẩm định đối với hồ sơ đề nghị xây dựng Luật Bảo vệ dữ liệu cá nhân.

**3.** Ngày / /2025, Bộ Công an có Tờ trình Chính phủ số /TTr-BCA-A05 về hồ sơ đề nghị xây dựng Luật An ninh mạng.

**4**. Ngày / /2025, Thường trực Chính phủ đã họp cho ý kiến và nhất trí đối với hồ sơ đề nghị xây dựng Luật An ninh mạng.

**5**. Ngày / /2025, Chính phủ đã họp cho ý kiến và nhất trí đối với hồ sơ đề nghị xây dựng Luật An ninh mạng.

**VI. DỰ KIẾN NGUỒN LỰC, ĐIỀU KIỆN BẢO ĐẢM CHO VIỆC THI HÀNH LUẬT SAU KHI ĐƯỢC QUỐC HỘI THÔNG QUA**

**1.** Bộ Công an chủ trì, phối hợp với các bộ, ngành, địa phương, tổ chức, cá nhân có liên quan xây dựng Luật An ninh mạng.

**2**. Công tác quản lý nhà nước về an toàn, an ninh mạng, nay là an ninh mạng, đã được tổ chức thực hiện chuyên nghiệp, bài bản kể từ khi Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018 có hiệu lực, các cơ quan quản lý nhà nước đều có bố trí cán bộ, kinh phí cho công tác này và đã có kinh nghiệm tổ chức thực hiện. Vì vậy, nguồn lực dự kiến cho việc thực hiện Luật An ninh mạng không phát sinh lớn.

- Về nhân lực: Cơ bản không phát sinh so với hiện hành. Đối với Trung ương, Bộ Công an sẽ chịu trách nhiệm trước Chính phủ về việc tổ chức triển khai thi hành Luật và không làm phát sinh thêm tổ chức mới mà chỉ trên cơ sở các đơn vị đã có kiện toàn lại trong nhiệm kỳ mới và đội ngũ cán bộ sẵn có để tổ chức thực thi các nhiệm vụ quản lý nhà nước được giao trong Luật. Đối với địa phương, các Công an tỉnh, thành phố trực thuộc Trung ương sẽ bảo đảm thực hiện tốt chức năng quản lý nhà nước về an ninh mạng tại địa phương, kế thừa chức năng quản lý nhà nước về an toàn thông tin từ Sở Thông tin và Truyền thông trước đây.

- Về xây dựng các văn bản hướng dẫn thi hành Luật: Các cơ quan có thẩm quyền ban hành các văn bản được giao trong Luật bảo đảm phù hợp với quy định của pháp luật khác có liên quan.

- Về tuyên truyền, phổ biến, đào tạo nội dung của Luật: Các Bộ, ngành liên quan và các tỉnh thành phố trực thuộc Trung ương trong phạm vi chức năng, nhiệm vụ thực hiện tuyên truyền, phổ biến cho các tổ chức, cá nhân và tập huấn cho đội ngũ cán bộ trực tiếp thực hiện quản lý nhà nước về an ninh mạng hiểu biết đầy đủ về các quy định của Luật để thực hiện kịp thời.

- Về triển khai thi hành Luật khi có hiệu lực thi hành: Các Bộ, ngành liên quan và các cơ quan quản lý nhà nước liên quan ở các tỉnh, thành phố trực thuộc Trung ương trong phạm vi chức năng, nhiệm vụ triển khai thực hiện và theo dõi, giám sát, thanh tra, kiểm tra, sơ kết, tổng kết, đánh giá tình hình thực thi Luật theo thời gian định kỳ hoặc đột xuất.

**VII. THỜI GIAN DỰ KIẾN TRÌNH QUỐC HỘI XEM XÉT, THÔNG QUA**

Dự kiến thời gian trình Quốc hội cho ý kiến và thông qua: Kỳ họp thứ 10, Quốc hội khóa XV (tháng 10/2025).

Hồ sơ trình kèm theo gồm:

*a) Tờ trình Quốc hội;*

*b) Dự thảo Luật An ninh mạng;*

*c) Báo cáo đánh giá tác động của chính sách;*

*d) Báo cáo giải trình, tiếp thu ý kiến góp ý; bản chụp ý kiến góp ý; bảng tổng hợp ý kiến tham gia góp ý.*

Trên đây là Tờ trình đề nghị xây dựng dự án Luật An ninh mạng, Chính phủ trình Quốc hội xem xét, quyết định./.

|  |  |  |
| --- | --- | --- |
| ***Nơi nhận:***- Như trên;- Thủ tướng, các Phó Thủ tướng CP;- Các Bộ: Công an, Tư pháp;- VPCP: BTCN, các PCN, Trợ lý TTg; các Vụ: KSTT, NC, PL, QHĐP;- Lưu: VT, PL (2). |  | **TM. CHÍNH PHỦTUQ. THỦ TƯỚNGBỘ TRƯỞNG BỘ CÔNG AN** **Đại tướng Lương Tam Quang** |