SỰ CẦN THIẾT PHẢI CÓ LUẬT AN NINH MẠNG

★ PGS, TS NGUYỄN THỊ NGỌC HOA
Học viện Báo chí và Tuyên truyền
★ ThS BÙI THỊ LONG
Học viện Chính trị quốc gia Hồ Chí Minh

● *Tóm tắt: Nhằm tăng cường bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội; phòng ngừa, ứng phó với các nguy cơ đe dọa an ninh mạng; khắc phục hạn chế, yếu kém liên quan đến bảo vệ an ninh mạng, Kỳ họp thứ 5 (từ ngày 21-5-2018 đến ngày 15-6-2018), Quốc hội khóa XIV đã thông qua Luật An ninh mạng năm 2018 (sau đây gọi là Luật An ninh mạng). Không như một số luận điểm xuyên tạc của kẻ xấu, Luật hoàn toàn phù hợp với quy định của Hiến pháp năm 2013 về quyền con người, quyền cơ bản của công dân và bảo vệ Tổ quốc; bảo đảm sự phù hợp với thông lệ quốc tế*[1].

● *Từ khóa: Luật An ninh mạng, an ninh quốc gia.*

1. Luật An ninh mạng thể chế hóa đường lối, chủ trương của Đảng, là cơ sở pháp lý bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội

Luật An ninh mạng thể chế hóa đầy đủ, kịp thời chủ trương, đường lối của Đảng về an ninh mạng được nêu tại một số văn bản như:

- Nghị quyết số 13-NQ/TW ngày 16-1-2012 của 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 của Hội nghị Trung ương 8 khóa XI về chiến lược bảo vệ Tổ quốc trong tình hình mới.

- Chỉ thị số 46-CT/TW của Bộ Chính trị về tăng cường sự lãnh đạo của Đảng đối với công tác bảo đảm an ninh trật tự trong tình hình mới, trong đó khẳng định vấn đề an ninh mạng đang là vấn đề rất phức tạp, cần được chú trọng giải quyết đồng bộ, hiệu quả.

- Chỉ thị số 28-CT/TW của Ban Bí thư Trung ương Đảng và Chỉ thị số 15-CT/TTg của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng.

- Chỉ thị số 30-CT/TW của Bộ Chính trị ban hành 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 101/2016/NĐ-CP 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...

Cùng với quá trình hội nhập quốc tế, phát triển công nghệ thông tin, đặc biệt là cuộc cách mạng Công nghiệp 4.0, thực trạng, tình hình diễn ra trên không gian mạng đã đặt ra yêu cầu cấp thiết đối với công tác an ninh mạng trong bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội, cụ thể:

Thứ nhất, phòng ngừa, đấu tranh, làm thất bại hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, chống nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, tuyên truyền phá hoại tư tưởng, phá hoại nội bộ, phá hoại khối đại đoàn kết toàn dân tộc, kích động biểu tình, phá rối an ninh trên không gian mạng của các thế lực thù địch, phản động.

Thứ hai, phòng ngừa, ngăn chặn, ứng phó, khắc phục hậu quả của các hoạt động tấn công mạng, khủng bố mạng, phòng, chống chiến tranh mạng khi hoạt động tấn công mạng nhằm vào hệ thống thông tin nước ta gia tăng về số lượng và mức độ nguy hiểm, ảnh hưởng nghiêm trọng tới chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội. Trong khi đó, khủng bố mạng nổi lên như một thách thức toàn cầu, chiến tranh mạng là một trong những nguy cơ đe dọa an ninh quốc gia. Những vấn đề trên đòi hỏi phải chủ động phòng ngừa, ngăn chặn, ứng phó, có phương án và sự chuẩn bị sẵn sàng để kịp thời xử lý các tình huống xấu có thể xảy ra.

Thứ ba, phòng ngừa, ngăn chặn, loại bỏ tác nhân tiến hành hoạt động gián điệp mạng, sử dụng không gian mạng để chiếm đoạt thông tin, tài liệu bí mật nhà nước, đặc biệt là hoạt động xâm nhập, tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia; đồng thời, hạn chế và tiến tới chấm dứt tình trang đăng tải bí mật nhà nước trên mạng internet do chủ quan hoặc thiếu kiến thức an ninh mạng.

Thứ tư, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia và áp dụng các biện pháp cần thiết, tương xứng. Đây là hệ thống thông tin của các mục tiêu quan trọng quốc gia, cơ sở hạ tầng quan trọng quốc gia, cơ quan chứa đựng bí mật nhà nước, nếu bị tấn công, xâm nhập, phá hoại, chiếm đoạt thông tin có thể gây hậu quả nghiêm trọng, ảnh hưởng tới chủ quyền, lợi ích, an ninh quốc gia, gây rối loạn trật tự, an toàn xã hội nên cần có biện pháp bảo vệ chặt chẽ, tương xứng và ở mức độ cao hơn so với những mục tiêu cần bảo vệ ít quan trọng hơn. Việc bảo vệ những hệ thống thông tin này không chỉ bao gồm hoạt động kiểm tra, đánh giá quá trình vận hành, áp dụng các tiêu chuẩn an ninh mạng phù hợp, riêng biệt mà phải tiến hành hoạt động thẩm định ngay từ khi xây dựng hồ sơ thiết kế, vận hành hệ thống thông tin để sớm phát hiện, loại bỏ các nguy cơ đe dọa an ninh mạng.

Thứ năm, quy định và thống nhất thực hiện phòng ngừa, ứng phó nguy cơ, sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia. Hoạt động ứng cứu sự cố an toàn thông tin mạng theo quy định của Luật An toàn thông tin mạng hiện nay chỉ phát huy được vai trò bảo đảm 3 thuộc tính của thông tin là tính nguyên vẹn, tính bảo mật và tính khả dụng, chưa đáp ứng được yêu cầu bảo vệ quốc phòng, an ninh, trật tự, an toàn xã hội, xử lý sự cố, huy động lực lượng ứng phó, cũng như loại bỏ các tác nhân gây hại tồn tại sẵn bên trong hệ thống thông tin hoặc hành vi vi phạm pháp luật trên không gian mạng ảnh hưởng tới hệ thống thông tin quan trọng về an ninh quốc gia. Phòng ngừa, ứng phó nguy cơ, sự cố an

ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia là một quy trình thống nhất. Việc phân tích các sự cố an ninh mạng liên quan trực tiếp tới dấu vết hiện trường và các dấu hiệu phạm tội, góp phần vào công tác điều tra, xử lý hành vi vi phạm của cơ quan chức năng Bộ Công an, Bộ Quốc phòng. Do đó, thống nhất đầu mối trong giám sát, dự báo, ứng phó và diễn tập ứng phó khẩn cấp sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia là cấp bách, cần thiết, không trùng dẫm với ứng cứu sự cố an toàn thông tin mạng.

Thứ sáu, quy định về tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia. Tham khảo kinh nghiệm nước ngoài cho thấy, một số quốc gia trên thế giới đã xây dựng các bộ tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng để áp dụng cho các mục tiêu, đối tượng và yêu cầu bảo vệ an ninh mạng cụ thể. Ở nước ta, tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng được ban hành rộng rãi, được áp dụng chung cho toàn xã hội, mang tính phổ thông, đại chúng. Tuy nhiên, đối với hệ thống thông tin quan trọng về an ninh quốc gia, ngoài những tiêu chuẩn an toàn thông tin mạng, cần có những quy định về tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng ở mức độ cao hơn để đáp ứng yêu cầu đặt ra.

Thứ bảy, triển khai công tác bảo vệ an ninh mạng trong hệ thống cơ quan nhà nước từ Trung ương đến địa phương. Hiện nay, hệ thống thông tin của cơ quan nhà nước tồn tại nhiều lỗ hổng bảo mật không được khắc phục, nhận thức của cán bộ, nhân viên còn nhiều hạn chế, chưa nhận thức được mức độ cần thiết của công tác an ninh mạng. Trong khi đó, công nghệ thông tin đã được ứng dụng rộng rãi từ Trung ương đến địa phương, chính phủ điện tử và các hệ thống điều khiển, xử lý tự động đã xuất hiện ở mọi ngành, cấp, lĩnh vực. Hệ thống thông tin của cơ quan nhà nước đang là đối tượng của hoạt động tấn công mạng, xâm nhập mạng, gián điệp mạng; tình trạng đăng tải thông tin, tài liệu bí mật nhà nước trên mạng internet vẫn còn tồn tại. Do đó, tình hình thực tiễn đã đặt ra yêu cầu triển khai công tác bảo vệ an ninh mạng và lực lượng an ninh mạng từ Trung ương đến địa phương.

Thứ tám, đặt nền móng và triển khai công tác nghiên cứu, dự báo, phát triển các giải pháp bảo đảm an ninh mạng. Hiện nay, công tác này chưa được chú trọng, nhà nước cũng chưa có định hướng quản lý, bảo đảm an ninh mạng đối với các xu hướng công nghệ có khả năng thay đổi tương lai như cuộc cách mạng công nghiệp lần thứ 4, điện toán đám mây, dữ liệu lớn, dữ liệu nhanh. Tham khảo kinh nghiệm nước ngoài cho thấy, một số quốc gia đã xây dựng nhiều đạo luật chuyên ngành của an ninh mạng, tập trung nâng cao năng lực dự báo, chia sẻ thông tin và tăng cường năng lực an ninh mạng.

Thứ chín, thường xuyên kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thống thông tin của các bộ, ngành, địa phương. Mặc dù Chính phủ đã giao Bộ Công an chủ trì, phối hợp với các bộ, ngành liên quan triển khai nhiều kế hoạch kiểm tra, đánh giá thực trạng an ninh mạng tại hàng chục bộ, ngành, địa phương nhưng đây là hoạt động đột xuất, chưa được triển khai hằng năm, không tạo thành được trách nhiệm và ý thức kiểm tra, đánh giá an ninh mạng định kỳ. Trong khi đó, cơ quan chủ quản hệ thống thông tin chưa nhận thức rõ trách nhiệm của mình, chưa chủ động hoặc

triển khai các hoạt động bảo vệ an ninh mạng một cách chiếu lệ, hình thức. Để phòng ngừa, hạn chế nguy cơ an ninh mạng, cần xây dựng quy trình, cơ chế kiểm tra, đánh giá thực trạng an ninh mạng phù hợp, thống nhất trên phạm vi cả nước.

Thứ mười, xây dựng cơ chế chia sẻ thông tin, thông báo tình hình an ninh mạng để nâng cao nhận thức về an ninh mạng, chủ động phòng ngừa các nguy cơ an ninh mạng có thể xảy ra. Việc chia sẻ thông tin, thông báo tình hình an ninh mạng có thể được thực hiện bởi cơ quan chức năng để tổ chức, cá nhân nâng cao nhận thức, áp dụng biện pháp phòng tránh hoặc nghiên cứu, tham khảo.

2. Luật An ninh mạng là công cụ hữu hiệu phòng ngừa, ứng phó với các nguy cơ đe dọa an ninh mạng, bảo vệ an ninh của các cơ quan, tổ chức kinh tế, xã hội, chính trị

Một là, Luật An ninh mạng là công cụ hữu hiệu phòng ngừa, ứng phó với các nguy cơ đe dọa an ninh mạng như: i) Nguy cơ các thế lực phản động thông qua không gian mạng thực hiện âm mưu "diễn biến hòa bình", phá hoại tư tưởng, chuyển hóa chế độ chính trị nước ta. Trong bối cảnh toàn cầu hóa, hội nhập quốc tế và đặc biệt là sự phát triển mạnh mẽ của khoa học công nghệ, âm mưu này được triển khai dưới nhiều phương thức thức khác nhau. Không gian mạng trở thành môi trường lý tưởng cho âm mưu "diễn biến hòa bình", phá hoại tư tưởng, chuyển hóa chế độ chính trị nước ta, thông qua các hoạt động thúc đẩy "tự diễn biến", "tự chuyển hóa"; liên lạc, móc nối, chỉ đạo và thành lập tổ chức hoạt động chống phá; sử dụng không gian mạng để kích động biểu tình, gây rối an ninh, chuyển hóa chế độ chính trị ở nước ta. ii) Nguy cơ đối mặt với các cuộc tấn công mạng trên quy mô lớn, cường độ cao. Mục tiêu tấn công mạng là hạ tầng truyền dẫn vật lý (cáp truyền dẫn quốc tế, trục truyền dẫn nội bộ quốc gia...), hạ tầng dịch vụ lõi (router, thiết bị mạng...), hệ thống điều khiển tự động hóa (SCADA) của các cơ sở quan trọng về kinh tế, quốc phòng, an ninh... Tấn công mạng có thể diễn ra theo kiểu tự phát, đơn lẻ, theo các chiến dịch với mục đích khống chế và thu thập thông tin, khủng bố, đe dọa và tán phát các thông điệp xấu, phá hủy cơ sở hạ tầng trọng yếu quốc gia, hệ thống thông tin quan trọng về an ninh quốc gia, thậm chí là phục vụ chiến tranh. iii) Nguy cơ mất kiểm soát về an ninh, an toàn thông tin mạng. Nguy cơ này chịu tác động trực tiếp từ bốn yếu tố: Sự phụ thuộc vào hạ tầng và dịch vụ công nghệ, thiếu hụt nguồn nhân lực công nghệ thông tin chất lượng cao, ý thức người dùng hạn chế và bất cập, hạn chế, yếu kém trong quản lý nhà nước về an ninh, an toàn thông tin mạng.

Hai là, Luật An ninh mạng khắc phục hạn chế, yếu kém liên quan đến bảo vệ an ninh mạng ở nước ta trong thời gian qua:

Thứ nhất, chồng chéo trong thực hiện chức năng, nhiệm vụ bảo vệ an ninh mạng giữa các bộ, ngành chức năng; tồn tại cách hiểu chưa rõ ràng giữa an ninh mạng và an toàn thông tin mạng. Cần thống nhất nhận thức rằng, an ninh mạng bao gồm hoạt động bảo vệ an ninh quốc gia, trật tự, an toàn xã hội theo chức năng, nhiệm vụ của Bộ Công an; hoạt động tác chiến trên không gian mạng theo chức năng, nhiệm vụ của Bộ Quốc phòng và bảo đảm an toàn thông tin mạng theo chức năng, nhiệm vụ của Bộ Thông tin và Truyền thông. An toàn thông tin mạng là điều kiện cho bảo đảm an ninh mạng được thực thi có hiệu quả, bền vững.

Có nhiều nguyên nhân dẫn đến tồn tại, vướng mắc nêu trên, trong đó nguyên nhân chủ yếu là từ sự vướng mắc, bất cập được biểu hiện thông qua hai vấn đề: i) Do chưa có sự nhận thức thống nhất về an ninh mạng nên hiện nay, Bộ Công an thực hiện nhiệm vụ bảo vệ an ninh mạng đều dựa trên cơ sở quy định của Luật An ninh quốc gia, Luật Công an nhân dân và các văn bản dưới luật về bảo vệ an ninh quốc gia nói chung và nguyên tắc tổ chức, hoạt động, chức năng, nhiệm vụ, quyền hạn và chế độ, chính sách đối với lực lượng Công an nhân dân nói riêng; chưa có quy định cụ thể về an ninh mạng và chức năng, nhiệm vụ, quyền hạn của lực lượng an ninh mạng trong Công an nhân dân. ii) Qua rà soát hệ thống pháp luật của một số quốc gia trên thế giới (Anh, Mỹ, Nhật, Úc...) cho thấy, các quốc gia này không phân tách "cyber security" thành "an ninh mạng" và "an toàn thông tin mạng" như ở nước ta, mà thống nhất giao một đầu mối thực hiện chức năng quản lý nhà nước, căn cứ vào chức năng, nhiệm vụ của các bộ, ngành để có sự phân công phù hợp. Hai vấn đề trên đã dẫn tới công tác bảo vệ an ninh mạng chưa được triển khai trên tất cả các lĩnh vực, đối tượng mà không gian mạng bao phủ và hiện đang có ảnh hưởng sâu sắc.

Thứ hai, chưa có văn bản luật quy định về công tác an ninh mạng. Trong những năm qua, nước ta đã ban hành nhiều văn bản quy phạm pháp luật liên quan đến lĩnh vực công nghệ thông tin, viễn thông, internet nhưng chưa có văn bản quy phạm pháp luật quy định cụ thể về an ninh mạng nên chưa có đầy đủ căn cứ pháp lý để triển khai các biện pháp phòng ngừa, phát hiện, xử lý, đấu tranh với các nguy cơ đe dọa an ninh mạng, hành vi vi phạm pháp luật trên không gian mạng. Các quy định hiện nay về an toàn thông tin mạng chưa đủ sức răn đe, ngăn chặn các hành vi vi phạm trên không gian mạng; chưa đáp ứng được yêu cầu thực tiễn của công tác an ninh mạng đặt ra trong tình hình mới. Thực trạng này đã gây khó khăn, vướng mắc trong tổ chức, triển khai các phương án bảo đảm an ninh thông tin, an ninh mạng cũng như trong công tác phòng ngừa, đấu tranh ngăn chặn các hoạt động sử dụng internet để xâm phạm an ninh quốc gia, trật tự, an toàn xã hội.

3. Luật An ninh mạng bảo đảm sự phù hợp với quy định của Hiến pháp năm 2013 về quyền con người, quyền cơ bản của công dân

Luật An ninh mạng bảo đảm sự phù hợp với quy định của Hiến pháp năm 2013 về quyền con người, quyền cơ bản của công dân và bảo vệ Tổ quốc. Theo quy định tại khoản 2 Điều 14 của Hiến pháp năm 2013 thì 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[2]. Luật An ninh mạng sẽ quy định các biện pháp nghiệp vụ an ninh mạng, trong đó có một số biện pháp có khả năng ảnh hưởng tới quyền con người, quyền và nghĩa vụ cơ bản của công dân như giám sát an ninh mạng, hạn chế thông tin mạng... Do vậy, việc ban hành Luật An ninh mạng để bảo đảm quyền con người, quyền công dân theo quy định của Hiến pháp là cần thiết. Bên cạnh đó, việc ban hành Luật này cũng góp phần cụ thể hóa tinh thần và nội dung mới của Hiến pháp về bảo vệ Tổ quốc, đặc biệt là quy định "Tổ quốc Việt Nam là thiêng liêng, bất khả xâm phạm" và "mọi hành vi chống lại độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ, chống lại sự nghiệp xây dựng và bảo vệ Tổ quốc đều bị nghiêm trị".

Luật An ninh mạng bảo đảm sự phù hợp với thông lệ quốc tế. Qua nghiên cứu cho thấy, hiện đã có nhiều quốc gia trên thế giới ban hành các văn bản luật về an ninh mạng, điển hình như: Mỹ, Nhật, Trung Quốc, Anh, Úc, Cộng hòa Séc, Hàn Quốc... Riêng Mỹ đã ban hành tới 6 đạo luật chuyên ngành về các vấn đề về an ninh mạng là: Đạo luật Đánh giá Lực lượng An ninh mạng, Đạo luật Tăng cường An ninh mạng năm 2014, Đạo luật Bảo vệ An ninh mạng Quốc gia 2014, Đạo luật hiện đại hóa An ninh thông tin Liên bang năm 2014, Dự luật Chia sẻ thông tin An ninh mạng năm 2015, Dự luật Tăng cường Bảo vệ An ninh mạng Quốc gia năm 2015. Ngày 7-12-2015, Hội đồng và Nghị viện châu Âu đạt được sự thống nhất về các biện pháp thúc đẩy an ninh mạng tổng thể trong Liên minh châu Âu tại Chỉ thị An ninh thông tin và mạng (Network and Information Security) nhằm tăng cường các khả năng an ninh mạng của các quốc gia thành viên, tăng cường sự hợp tác của các quốc gia thành viên trong lĩnh vực an ninh mạng. Việc xây dựng, ban hành Luật An ninh mạng sẽ bảo đảm công tác an ninh mạng của nước ta có sự phù hợp nhất định với thông lệ quốc tế và bảo đảm các điều kiện hội nhập quốc tế về an ninh mạng.

Trên đây là vai trò và giá trị của Luật An ninh mạng trong việc bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội; phòng ngừa, ứng phó với các nguy cơ đe dọa an ninh mạng; khắc phục hạn chế, yếu kém liên quan đến bảo vệ an ninh mạng; thể chế hóa đầy đủ, kịp thời các chủ trương, đường lối của Đảng về an ninh mạng; bảo đảm sự phù hợp với quy định của Hiến pháp năm 2013 về quyền con người, quyền cơ bản của công dân và bảo vệ Tổ quốc; bảo đảm sự phù hợp với thông lệ quốc tế ❐

(1) Chính phủ: Tờ trình số 397/TTr-CP ngày 26-9-2017 của Chính phủ về dự án Luật An ninh mạng.
(2) Quốc hội: *Hiến pháp năm 2013.*

Tài liệu tham khảo

1. Các văn bản luật về an ninh mạng, điển hình như: Mỹ, Nhật, Trung Quốc, Anh, Úc, Cộng hòa Séc, Hàn Quốc...
2. Chỉ thị số 28-CT/TW của Ban Bí thư Trung ương Đảng và Chỉ thị số 15-CT/TTg của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng.
3. Chỉ thị số 30-CT/TW của Bộ Chính trị ban hành về phát triển và tăng cường quản lý báo chí điện tử, mạng xã hội và các loại hình truyền thông khác trên Internet.
4. Chỉ thị số 46-CT/TW của Bộ Chính trị về tăng cường sự lãnh đạo của Đảng đối với công tác bảo đảm an ninh trật tự trong tình hình mới, trong đó khẳng định vấn đề an ninh mạng đang là vấn đề rất phức tạp, cần được chú trọng giải quyết đồng bộ, hiệu quả.
5. Chính phủ: Tờ trình số 397/TTr-CP ngày 26-9-2017 của Chính phủ về dự án Luật An ninh mạng.
6. Nghị định 101/2016/NĐ-CP 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...
7. Nghị quyết số 13-NQ/TW ngày 16-1-2012 của 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.*
8. Nghị quyết số 28-NQ/TW của Hội nghị Trung ương 8 khóa XI *về chiến lược bảo vệ Tổ quốc trong tình hình mới.*
9. Quốc hội: *Hiến pháp năm 2013.*