Những vấn đề về pháp luật và qui chế trong nền kinh tế thông tin

Rodolfo Noel S. Quimbo

Tháng 5/2003

Nhóm công tác e-ASEAN UNDP-APDIP

LỜI NÓI ĐẦU

Một trong nhiều thách thức mà các nước trong khu vực Châu Á-Thái Bình Dương ngày nay đang phải đối mặt là việc chuẩn bị sẵn sàng cho xã hội và chính phủ của họ trong bối cảnh toàn cầu hoá và cách mạng thông tin truyền thông. Các nhà hoạch định chính sách, doanh nhân, các nhà hoạt động của các tổ chức phi chính phủ (NGO), các học giả, và thường dân đang ngày càng quan tâm tới nhu cầu xây dựng xã hội trở nên cạnh tranh trong nền kinh tế thông tin đang phát triển.

Nhóm công tác e-ASEAN và Chương trình phát triển thông tin châu Á Thái Bình Dương của UNDP (UNDP-APDIP) có chung niềm tin rằng với công nghệ thông tin và truyền thông (ICT), các nước có thể đối mặt với các thách thức của kỷ nguyên thông tin. Với ICT, họ có thể vươn tới một tầm cao mới trong sự nghiệp phát triển kinh tế, xã hội và chính trị. Chúng tôi hy vọng rằng trong việc thực hiện bước nhảy vọt này, các nhà hoạch định chính sách, những người lập kế hoạch, nghiên cứu viên, những người triển khai kế hoạch, các nhà bình luận và những người khác sẽ thấy các quyển sách khoa học thường thức điện tử (e-primers) về xã hội thông tin, kinh tế thông tin và tổ chức xã hội này là bổ ích.
E-primers có mục đích giúp cho người đọc hiểu biết rõ ràng về những thuật ngữ, định nghĩa, xu hướng và những vấn đề khác nhau gắn liền với kỷ nguyên thông tin. E-primers được viết với ngôn ngữ đơn giản, dễ hiểu bao gồm các ví dụ, trường hợp tiêu biểu, các bài học thu được và những thực hành tốt nhất giúp các nhà xây dựng kế hoạch và những người ra quyết định trong việc nêu lên những vấn đề thích hợp và xây dựng chính sách chiến lược phù hợp trong nền kinh tế thông tin.

E-primers bao gồm những phần sau:

- Kỷ nguyên thông tin
- Net, Web và Cơ sở hạ tầng thông tin
- Thương mại điện tử và kinh doanh điện tử
- Những vấn đề về pháp luật và qui chế trong nền kinh tế thông tin
- Chính phủ điện tử
- Công nghệ thông tin và truyền thông (ICT) và giáo dục
- Gen, công nghệ và chính sách: Giới thiệu tới công nghệ sinh học

Các tài liệu trên có thể tìm thấy trên mạng qua địa chỉ www.eprimers.org và www.apdip.net

Sách khoa học thường thức E-primers này do UNDP-APDIP thực hiện, nhằm tạo ra một môi trường thúc đẩy ICT qua việc cải tổ chính sách và ủng hộ tại khu vực châu Á Thái Bình Dương và qua nhóm công tác e-ASEAN, một sáng kiến ICT vì sự phát triển của mười nước thành viên của Hiệp hội các quốc gia Đông Nam Á. Chúng tôi hoan nghênh ý kiến của các bạn về những chủ đề và vấn đề mớâcm theo đó nội dung của E-primers có thể hữu dụng.

Cuối cùng, chúng tôi xin cảm ơn những người viết bài, các nhà nghiên cứu, những người đóng góp ý kiến và nhóm công tác - những người đã thực hiện và tham gia đóng góp đối với quyển sách E-primers này .

Roberto R. Romulo
Chủ tịch (2000-2002)
Nhóm công tác e-ASEAN UNDP-APDIP
Manila. Philippines

Shahid Akhtar
Điều phối viên chương trình
Kuala Lumpur, Malaysia
www.apdip.net

GIỚI THIỆU

Khi mà phạm vi ảnh hưởng của Internet như một mạng truyền thông được mở rộng tới các giao dịch trong lĩnh vực thương mại, các cơ quan lập pháp trở nên quan tâm hơn việc điều chỉnh những giao dịch đó và hoạt động của những chủ thể tham gia. Các vấn đề nẩy sinh từ một thực tế ngày càng phức tạp của Internet đã đặt ra câu hỏi phải có những quy định pháp luật mới trong lĩnh vực này. Những đòi hỏi pháp lý như vậy bao quát nhiều khía cạnh, từ vấn đề tự điều chỉnh cho tới vấn đề về chủ quyền lãnh thổ quốc gia.

Quyển sách này nhằm giúp những nước đang phát triển xác định những vấn đề cần quan tâm để xây dựng một khung khổ pháp lý phù hợp cho Thương mại điện tử (TMĐT), và những khung khổ pháp lý và thể chế tương ứng khác liên quan như vấn đề cạnh tranh, bí mật riêng tư, bảo vệ người tiêu dùng, việc truy cập/cơ hội bình đẳng và sở hữu trí tuệ.

Quyển sách này cũng sẽ thảo luận về một số vấn đề mà những nước đang phát triển trong Khu vực Châu Á - Thái Bình Dương phải đối mặt; về sự thất bại hay chậm trễ trong việc đưa ra những chính sách hoặc xây dựng cơ sở pháp lý phù hợp để tham gia vào nền kinh tế thế giới.

I. PHÁP LUẬT VÀ INTERNET

Trong bối cảnh công nghệ phát triển với một tốc độ nhanh chóng, pháp luật cần phải được xây dựng để kịp thời điều chỉnh những hiện tượng xã hội mới phát sinh. Việc thiếu khung khổ pháp lý, trong nhiều hệ thống xét xử, để điều chỉnh những vấn đề liên quan tới hiệu lực pháp lý của các giao dịch điện tử, là rào cản rất lớn đối với sự phát triển của TMĐT. Có một thực tế rằng, rất nhiều quy định pháp lý, liên quan tới hợp đồng và những giao dịch thương mại khác, đưa ra đòi hỏi tài liệu phải ở dạng văn bản, được ký hoặc dưới hình thức bản gốc.

Thực tế, trong những giao dịch TMĐT, thông điệp dữ liệu, tài liệu hoặc hợp đồng được giao kết bằng phương thức số hoá đã tạo nên một giao dịch điện tử hoàn chỉnh.

Để giải quyết vấn đề hóc búa này, Uỷ Ban của Liên Hợp quốc về pháp luật thương mại quốc tế (UNCITRAL) đã soạn thảo một luật mẫu về TMĐT, Luật Mẫu này có thể được sử dụng như một hướng dẫn phục vụ các chính phủ trong quá trình xây dựng pháp luật về TMĐT cho riêng họ.

Luật Mẫu UNCITRAL đưa ra những nguyên tắc gì ?

Luật Mẫu được soạn thảo dựa trên những nguyên tắc cơ bản sau đây:

1. *Tương đương thuộc tính*: truyền thông điện tử được coi có những thuộc tính tương đương việc trao đổi tài liệu ở dạng văn bản. Một khi có những tiêu

chuẩn xác định, tài liệu điện tử có thể được coi có giá trị pháp lý như tài liệu ở dạng văn bản.

2. *Tự do thoả thuận hợp đồng*: các bên trong một hợp đồng có thể thoả thuận hình thức hợp đồng ở dạng thông điệp dữ liệu. Tuy nhiên, điều này không dẫn tới việc thay đổi những điều khoản cơ bản của hợp đồng.

3. *Tôn trọng việc sử dụng tự nguyên phương thức truyền thông điện tử*. Các bên có thể tự do lựa chọn việc tham gia một giao dịch điện hay không. Điều này không mang tính bắt buộc.

4. *Giá trị pháp lý của hợp đồng và tính ưu việt của những quy định pháp lý về hình thức hợp đồng*. Những đòi hỏi đối với hợp đồng để có giá trị pháp lý và khả năng được thi hành phải được tôn trọng.

5. *Áp dụng về mặt hình thức hơn là quan tâm tới nội dung*. Luật phải được áp dụng đối với hình thức hợp đồng, mà không đề cập tới nội dung, trên cơ sở phải thoả mãn những đòi hỏi pháp lý nhất định.

6. *Pháp luật về bảo về người tiêu dùng phải đi trước*. Pháp luật bảo vệ người tiêu dùng có thể phải được hình thành trước những quy định của Luật Mẫu.

Luật Mẫu đảm bảo cho cái gì ?

Luật Mẫu nhằm đưa ra sự bảo vệ đầy đủ về mặt pháp lý cho những tổ chức, cá nhân mong muốn tham gia TMĐT. Nó đảm bảo rằng những giao dịch TMĐT được thừa nhận giá trị pháp lý và nếu cần thiết thì sẽ có những hành động thích hợp được tiến hành để tăng cường khả năng thi hành cho những giao dịch được cam kết bằng phương tiện điện tử.

II. XÉT XỬ VÀ XUNG ĐỘT PHÁP LUẬT

Có người đã nói rằng: "*Trong nhiều năm, một trong những vấn đề pháp lý khó nhất về Internet liên quan tới đặc tính quan trong nhất của phương tiện truyền thông, đó là tính không bị giới hạn về mặt không gian*". Đặc tính trên đã tạo nên tính cách mạng cho truyền thông và thương mại, nó cũng đã dẫn tới rất nhiều tranh chấp và vụ án. Và, một điểm rất khó khi giải quyết những vụ án như thế là việc xác định nơi tiến hành giao dịch. [1]

Khi nào thì xẩy ra xung đột pháp luật ?

Một người dân ở Manila quyết định kiện một bác sĩ ở Manila vì đã làm ông ta bị thương, người dân này có thể kiện tại Toà Manila. Những toà án ở Manila có thẩm quyền xét xử đối với vị bác sĩ kia. Nhưng nếu người bị thiệt hại sau đó chuyển tới Hà Nội và quyết định đưa vụ việc ra toà ở đó, Bác sĩ ở Manila sẽ có quyền phản đối và có cơ sở pháp lý để khẳng định không có toà nào ở Hà Nội có thẩm quyền xét xử vụ việc liên quan tới ông ta.

Đó là một vụ việc đơn giản. Nhưng nếu xem xét một vụ việc liên quan tới một website nội dung đồi truỵ có trụ sở tại Hồng Kông, đặt máy chủ tại Caribbean và đăng ký trang web tại Hà Lan trong khi người chủ lại là công dân quốc tịch Anh. Trang Web đó có phạm vi trên toàn thế giới. Nếu có lời cáo buộc về tính khiêu dâm của trang web thì ai sẽ bị kiện và sẽ bị kiện ở đâu ?

Một vụ việc thứ 3, giả sử A ở Hà Nội và ký một hợp đồng vận chuyển máy móc với B ở Yangon. Nếu B không chuyển hàng hoá thì A sẽ kiện ở toà nào ? Nếu A kiện vụ việc ra toà vì đã không thực hiện đúng hợp đồng tại toà án ở Hà Nội, Toà án tại Hà Nội sẽ có thẩm quyền giải quyết theo căn cứ nào ?

Những ví dụ trên cho thấy thẩm quyền xét xử không được xác định giống nhau trong môi trường mạng Internet.

Quy định về thẩm quyền xét xử thế nào ?

Tại Mỹ, có nhiều cách xác định thẩm quyền xét xử của toà án đối với những hành vi trên mạng:

1. *Đã tới một bang*. Toà án có thể có quyền xét xử đối với một bị cáo ở ngoài phạm vi của Bang, miễn rằng, khi tới bang đó, người này đã bị triệu tập hoặc toà án đã gửi lệnh triệu tập do có người kiện. Đây là trường hợp đã được áp dụng cho một lập trình viên người Nga bị kiện bởi những nhà xuất bản sách điện tử (Adobe). Trong khi tới Nevada, anh ta đã nhận được một thông báo và sau đó bị bắt giữ.

2. *Gây thiệt hại trên một bang*. Một doanh nghiệp hoạt động trong lĩnh vực Internet có thể cũng chịu thẩm quyền xét xử do việc gây thiệt hại trên một bang khác. Nguyên tắc này được rút ra từ một số vụ việc mà toà án ở bang khác đã có quyền xét xử đối với những công dân không ở bang đó, khi họ gây một tai nạn rồi bỏ đi. Nếu một người sử dụng Internet để gây thiệt hại ở một bang, người gây thiệt hại có thể bị kiện tới toà án của Bang có thiệt hại xẩy ra. Trong những trường hợp mà quan hệ giữa hành động và thiệt hại là không rõ ràng, toà án cũng có thể tìm chứng cứ rằng hoạt động đó được thực hiện có chủ ý tại nơi bang đó hoặc rằng người gây thiệt hại đã có mối liên hệ với bang đó. [2]

3. *Liên hệ nhỏ nhất*. Một doanh nghiệp hoặc một người, có liên quan tới một bang cụ thể, có thể bị toà án bắt giữ dù doanh nghiệp hoặc người đó không có trụ sở hoặc sống tại bang đó. Thông thường, căn cứ xác định là sự lui tới thường xuyên; khoản lợi nhuận mà hàng hoá, dịch vụ bán được trên bang đó; hoặc liên quan tới một số hoạt động nhất định tại Bang đó. Ví dụ, những trang web chỉ quảng cáo mà không thực sự chào bán một loại sản phẩm, dịch vụ nào, có thể được coi là không có mối liên hệ nhỏ nhất được đòi hỏi cho phép toà án có quyền xét xử. Nhưng những trang web quảng cáo và chào bán hàng hoá, dịch vụ và sau đó nhận chào mua hàng từ Bang đó, doanh nghiệp có trang web như vậy có thể bị coi là thoả mãn đòi hỏi pháp lý để toà án tại Bang đó có thẩm quyền xét xử.

4. *Ảnh hưởng*. Khi hành vi của một người trên mạng, mặc dù được bắt nguồn từ một bang, đã tạo ra hoặc gây nên thiệt hại trên một bang khác, toà án của Bang có thiệt hại xẩy ra đó có quyền xét xử đối với bị cáo. Ví dụ: một vụ việc đã được đưa ra toà bởi Hiệp hội kiểm soát bảo san DVD chống lại những người tạo DeCCS[3] (*một phần mềm phá mã hệ thống bảo vệ việc sao chép, để cho phép những ổ ghi CDROM có thể đọc được DVDs*). Vấn đề là liệu toà án California có thẩm quyền xét xử đối với người vi phạm, một sinh viên ở Indiana và sau đó chuyển sang sống tại Texas. Toà án thụ lý đã cho rằng những toà án tại California có thẩm quyền xét xử, dẫn chiếu tới một vụ việc của Toà án tối cao Hoa Kỳ liên quan tới một thiếu niên 17 tuổi đã bị buộc tội vu cáo (phỉ báng). Phim ảnh và công nghiệp máy tính của California đã bị ảnh hưởng bởi hành vi của thiếu niên 17 tuổi trên, lúc đó đang sống tại Indiana. Quyết định này đã mở rộng quyền xét xử đối với những vụ việc trên mạng. Nếu một toà án khác dựa vào những tiêu chí của toà án California, bất cứ một trang web nào của có thể bị đưa ra toà dù trang web đó có tạo ảnh hưởng hay không. Luật sư trưởng của Minnesota đã đưa ra tuyên bố đáng lưu ý sau: "*Cảnh báo tới mọi người sử dụng và nhà cung cấp dịch vụ Internet: những người sống ngoài Minnesota truyền gửi thông tin qua Internet phải biết rằng thông tin được phát tán tại Minnesota sẽ nằm trong quyền xét xử của toà án tại Minnesota do vi phạm luật hình sự và dân sự của Bang*".

Tại sao cần những quy định pháp luật về xét xử ?

Do bản chất quốc tế của Internet, cần phải hình thành các quy định pháp luật điều chỉnh một hợp đồng được lập, thực hiện hoặc tiến hành trực tuyến. Nhiều vấn đề phức tạp có thể nẩy sinh khiến việc xác định pháp luật điều chỉnh sẽ trở nên khó khăn. Trong bối cảnh hiện tại, nhà kinh doanh phải xác định được quy định pháp luật hiện hành nào được áp dụng và đảm bảo rằng chúng được thể hiện trong pháp luật địa phương nơi có trang web. Điều này sẽ loại bỏ trường hợp không xác định được trách nhiệm cũng như khả năng khó thực thi của hợp đồng mà họ đã tham gia. Tốt hơn, khi tiến hành những giao dịch trực tuyến, trước tiên, các bên phải thoả thuận những cơ chế pháp luật được áp dụng, có vậy khi một tranh chấp nẩy sinh, vấn đề về thẩm quyền xét xử (pháp luật và toà án nào) sẽ được giải quyết.

III. THỪA NHẬN PHÁP LÝ ĐỐI VỚI DỮ LIỆU VÀ CHỮ KÝ ĐIỆN TỬ

Trong một hội thảo của APEC về TMĐT đầu năm 1998[4], môi trường chính sách không đảm bảo, cùng với những vấn đề khác, được các nước thành viên coi là một cản trở lớn nhất đối với sự phát triển của TMĐT. Và cản lớn nhất bắt nguồn từ thực tế rằng pháp luật hiện hành thường đưa ra những tài liệu ở dạng văn bản, phải có chữ ký viết tay, và việc tạo và lưu trữ bản gốc bằng giấy tờ.

Lấy trường hợp các quy định của Luật pháp Phillipines về việc hình thành và thực hiện hợp đồng làm ví dụ. Bộ luật dân sự Phillippine, được ban hành năm 1950, quy định rằng một hợp đồng là sự thống nhất giữa hai bên, theo đó một bên rằng buộc

quyền và nghĩa vụ của mình đối với bên kia để cung cấp một vật hoặc thực hiện một dịch vụ. Có rất nhiều vấn đề phát sinh như: Những cái gì xẩy ra sau đó nếu một bên lập trình một máy tính để đưa ra những cam kết, ví dụ trên E-bay chẳng hạn ? Khi nào thì anh ta không thực hiện những gì được giới hạn trong pháp luật hiện hành ? Có nên có sự thống nhất giữa các bên trong việc này ? Cho rằng hợp đồng giữa E-bay và người đó là có hiệu lực, nó có khả năng được thi hành không ?

Một vấn đề khác liên quan tới Quy chế về hành vi vi phạm ở Hoa Kỳ. Quy chế đòi hỏi rằng những hợp đồng nhất định, như thoả thuận mua bán hàng hoá ở một mức giá không thấp hơn 500 pesos (khoảng 10 đô), hoặc, không tính tới trường hợp khác, một thoả thuận thuê hơn một năm hoặc bán một bất động sản phải được thực hiện ở dạng văn bản. Những hợp đồng không ở dạng văn bản, mặc dù có hiệu lực, không được toà án chập nhận. Những quy định của toà án cũng đòi hỏi tài liệu ở dạng văn bản mà không ở dạng điện tử.

Rõ ràng cần có sự thay đổi trong những hệ thống pháp luật không cho phép thừa nhận giá trị pháp lý của tài liệu và chữ ký ở dạng điện tử, từ đó đưa ra sự đảm bảo rằng toà án sẽ cho phép những tài liệu ở dạng điện tử là chứng cứ trong những vụ việc hoặc tranh chấp.

Những nước nào đã ban hành luật về thương mại điện tử ?

Tại Đông Á, Hồng Kông đã ban hành Pháp lệnh giao dịch điện tử (có hiệu lực từ ngày 7/4/2000, được ban hành ngày 7/1/2000), văn bản này quy định về chữ ký số và bản ghi điện tử. Văn bản luật này được áp dụng rộng rãi cho mọi hoạt động truyền thông. Luật về chữ ký điện tử và Tổ chức chứng thực điện tử của Nhật Bản (có hiệu lực vào ngày 1/4/2001, được ban hành ngày 25/5/2000) đề cập tới chữ ký điện tử và được áp dụng phổ biến cho hoạt động truyền thông. Luật Cơ bản của Hàn Quốc về TMĐT cũng quy định về chữ ký số và được áp dụng phổ biến cho truyền thông.

Tại Đông Nam Á, Malaysia đã ban hành Luật về Chữ ký điện tử năm 1997, có hiệu lực từ ngày 1/10/1998. Luật Giao dịch điện tử của Singapore năm 1998 (được ban hành ngày 29/6/1998) quy định cả chữ ký điện tử và chữ ký số cũng như bản ghi điện tử và được áp dụng cho truyền thông. Tương tự, Luật TMĐT của Thái Lan (được thông qua dự thảo 2 và 3 vào Tháng 10/2000) bao quát về chữ ký điện tử và được áp dụng chủ yếu cho truyền thông. Trong Đạo luật TMĐT của Phillipines năm 2000 (được ban hành ngày 14/6/2000) điều chỉnh về chữ ký điện tử, giao dịch điện tử, và tội phạm liên quan tới TMĐT. Luật giao dịch điện tử của Brunei (được ban hành tháng 11/2000) bao quát hợp đồng điện tử cũng như chữ ký điện tử và chữ ký số.

Đạo luật công nghệ thông tin của Ấn Độ năm 2000 (ban hành ngày 9/6/2000, được thông qua bởi cơ quan lập pháp ngày 17/5/2000 và được thi hành từ tháng 10/2000) quy định về chữ ký số và bản ghi điện tử, và được áp dụng cho mọi hoạt động truyền thông.

Có những phương pháp điều chỉnh pháp luật nào đối với chứng thực điện tử ?

Không dễ để phân loại những quy định pháp luật về xác thực điện tử vì tồn tại rất nhiều khác biệt. Tuy nhiên, một cách chung nhất thì có 3 phương pháp điều chỉnh sau đây: [5]

- Phương pháp điều chỉnh chữ ký số;
- Phương pháp điều chỉnh hai nhánh;
- Phương pháp điều chỉnh tối thiểu.

Bảng 1. Ba cách quy định về xác thực điện tử

		Trung lập về công nghệ	Công nghệ cụ thể	Ví dụ	Định nghĩa
Phương pháp điều chỉnh chữ ký số	Các quy định kỹ thuật	-	+	Germany	Đưa ra tiêu chuẩn kỹ thuật cho chữ ký số (không có hậu quả pháp lý rõ ràng)
	Các quy định pháp lý	-	+	Utah, Italy	Thừa nhận pháp lý đối với chữ ký số dưới những điều kiện nhất định
	Các quy định tổ chức	-	+	Nhật Bản, Hà Lan	Đưa ra những đòi hỏi đối với tổ chức chứng thực
Phương pháp điều chỉnh hai nhánh		+	+/-	UNCITRAL (chữ ký điện tử), EU, Singapore	Thừa nhận pháp lý (an toàn) đối với chữ ký điện tử dưới những điều kiện nhất định
Phương pháp điều chỉnh tối thiểu		+	-	UNCITRAL (thương mại điện tử), Victoria (Australia)	Đối xử bình đẳng giữa chữ ký điện tử và chữ ký viết tay

Nguồn: "Tổng hợp", tiếp cận trong pháp luật xác thực điện tử; sẵn có trên trang web: http://rechten.uvt.nl/simone/Ds-art4.htm#sy2

Phương pháp điều chỉnh chữ ký số là gì ?

Phương pháp điều chỉnh chữ ký số đưa ra những quy định về kỹ thuật chữ ký số. Xây dựng pháp luật theo phương pháp này thực chất là xây dựng pháp luật về chữ ký số vì nội dung điều chỉnh chính là việc sử dụng chữ ký số. Theo phương pháp điều chỉnh này, có 3 cách quy định sau:

1. *Cách quy định kỹ thuật*. Cách quy định này nhằm xác định những tiêu chuẩn kỹ thuật của chữ ký số bằng phương tiện pháp lý. Cách quy định này không đề cập tới hậu quả pháp lý, mặc dù những hậu quả pháp lý đó có thể hoàn toàn xảy ra do việc sử dụng chữ ký số phù hợp với pháp luật liên quan.

2. *Cách quy định pháp lý*. Cách quy định này nhằm tạo cho cơ sở pháp lý cho chữ ký số tương tự với chữ ký viết tay. Mục đích chung của những quy định pháp luật này là đảm bảo an toàn pháp lý cho việc sử dụng chữ ký số. Thông

thường, pháp luật dạng này cũng bao gồm cả những quy định về Hạ tầng mã khoá công khai (PKI).

3. Cách quy định tổ chức. Cách quy định này không đề cập tới những tiêu chuẩn kỹ thuật của chữ ký số hay đưa ra thừa nhận phá lý rõ ràng cho chữ ký chữ ký số. Cách quy định này đưa ra mô hình tổ chức cho cơ quan chứng thực (CAs) và việc sử dụng chứng chỉ số liên quan tới việc ứng dụng chữ ký số. Mục đích là thúc đẩy niềm tin vào giao dịch điện tử bằng cách đảm bảo rằng cơ quan chứng thực là đáng tin cậy và an toàn.[6]

Phương pháp điều chỉnh hai nhánh là gì ?

Một phương pháp điều chỉnh thứ hai được gọi là phương pháp điều chỉnh hai nhánh, vì dựa vào sự kết hợp để quy định về xác thực điện tử. Theo phương pháp này, các nhà lập pháp tìm cách làm cho pháp luật của họ tồn tại lâu hơn bằng cách không đưa những đòi hỏi về công nghệ nhất định mà chỉ dự đoán những tiến bộ của công nghệ. Theo đó, Phương pháp này xây dựng những đòi hỏi pháp lý thấp nhất đối với xác thực điện tử và tạo hiệu lực pháp lý cao nhất đối với những kỹ thuật xác thực điện tử nhất định. Các công nghệ có được giá trị pháp lý cao hơn này chính là chữ ký điện tử an toàn.[7]

Phương pháp điều chỉnh tối thiểu là gì ?

Phương pháp điều chỉnh này không đưa ra những công nghệ cụ thể và vì thế nhắm tới mục tiêu trung lập về mặt công nghệ. Cách điều chỉnh này đưa ra đề cập tới những chức năng mà một chữ ký điện tử phải có để được sử dụng trong các giao dịch thương mại; những mức độ đáng tin cậy khác nhau phù hợp mục đích sử dụng của chữ ký điện tử. Vì phương pháp điều chỉnh này dựa vào chức năng tương ứng của chữ ký, vì vậy nó còn được gọi là phương pháp điều chỉnh theo chức năng. [8]

Phương pháp điều chỉnh nào ?

Thực tiễn thương mại đang thay đổi không ngừng và chúng ta không biết sẽ có những thay đổi gì về mặt công nghệ ứng dụng trong thương mại điện tử. Vì vậy, có thể không khôn ngoan khi ban hành những quy định pháp lý chi tiết và xác định những cách thức kinh doanh đặc thù, như mô hình PKI, vì khả năng tồn tại của chúng là không chắc chắn.

Theo cách nhìn này, phương pháp điều chỉnh chữ ký số có vẻ không phù hợp, mặc dù những nhà lập pháp và hành pháp đi theo phương pháp điều chỉnh này có thể có những lý do hợp lý (như tính chắc chắn pháp lý, tính đáng tin cậy đối với những vấn đề pháp lý).

Phương pháp điều chỉnh hai nhánh cũng tương tự như vậy, nhưng ở một mức độ thấp hơn, Phương pháp này nhằm đạt được hai mục đích: thứ nhất là tránh trường hợp phải thay đổi pháp luật thường xuyên bằng những quy định mở đối với những công nghệ mới; và thứ hai là đưa ra những tiêu chuẩn cho chữ ký điện tử an toàn

(bao gồm cả chữ ký số). Phương pháp điều chỉnh hai nhánh thường liên quan tới các vấn đề và tính huống chưa xác định (ví dụ như Cơ quan chứng thực, trách nhiệm, chất lượng tập chung chủ yếu vào những kỹ thuật nhất định).

Tóm lại, cả phương pháp điều chỉnh chữ ký sô và hai nhánh trong nhiều trường hợp chỉ tập chung vào chữ ký, mà không đề cập tới những đòi hỏi mẫu trong một tổng thể.

Phương pháp điều chỉnh tối thiểu theo như Luật Mẫu UNCITRAL đưa ra giải pháp nhậy cảm nhất đối với những nhà lập pháp muốn giải quyết vấn đề bằng việc đưa ra đòi hỏi mẫu trong pháp luật của họ. Theo Phương pháp điều chỉnh này, những đòi hỏi pháp lý mẫu được đề cập tới một cách tổng thể. Hơn thế, Phương pháp điều chỉnh tối thiểu cho phép đề cập tới những chức năng khác nhau mà kỹ thuật có thể thực hiện được trong hệ thống pháp luật quốc gia, đồng thời tạo cơ sở cho những tiến bộ kỹ thuật và công nghệ mới. Nhiều luật mới ban hành ở nhiều nước dựa trên Phương pháp điều chỉnh này đã thừa nhận những lợi thế của Phương pháp điều chỉnh tối thiểu, Luật Mẫu về thương mại điện tử là một ví dụ chứng minh. [9]

IV. SÁNG CHẾ, BÍ MẬT THƯƠNG MẠI VÀ SỞ HỮU TRÍ TUỆ

Trong nền kinh tế thông tin, việc sở hữu và bảo vệ các ý tưởng có ý nghĩa đặc biệt quan trọng. Những ý tưởng bản thân chúng đã là hàng hoá. Ý tưởng cũng đem lại tính cạnh tranh hơn cho người sở hữu nó trong thời đại thông tin. Vì thế, cần thiết rằng chế độ pháp lý cho việc bảo vệ ý tưởng cần được hình thành. Việc thiếu một hệ thống pháp luật như vậy sẽ không chỉ làm kìm hãm sự phát triển mà còn ngăn cản sự thịnh vượng của nền kinh tế thông tin.

Thông tin được sử dụng thế nào trên Internet ?

Ngày nay, mạng Internet hoạt động chủ yếu với chức năng truyền tải dữ liệu và thông tin giữa những hệ thống mạng. Thông thường, dữ liệu và thông tin truyền gửi được tập hợp và thu thập bởi những người quản trị mạng để hình thành một tài liệu sơ lược về những người sử dụng. Tài liệu sơ lược này sau đó sẽ được sử dụng đối với những sản phẩm và dịch vụ phù hợp với nhu cầu khách hàng, cũng như dự đoán được những cách thức mua hàng của họ. Có những trường hợp tài liệu thu thập được có thể được bán hoặc chia sẻ với những công ty khác. Thường có những tập đoàn lớn dựa vào thu nhập từ việc bán thông tin cá nhân của của khách hàng. Gần như mọi công ty hiện đại trên thế giới ngày nay đều sử dụng thông tin cá nhân ở một mức độ nào đó. Tuy nhiên, một số công ty phụ thuộc vào thu nhập này nhiều hơn những công ty khác. Trong số những công ty nổi tiếng phụ thuộc gần như và việc bán thông tin cá nhân phải kể đến DoubleClick, công ty này đã phân phối những quảng cáo trực tuyến, và thu từ những công ty khác như Equifa và Experian[10].

Một điều quan trọng cần phải nhớ là buôn bán những thông tin cá nhân đã phát tiển từ trước khi có Internet. Một trong những công ty hàng đầu đã khám phá ra giá trị

của thông tin cá nhân là Polk, được thành lập năm 1870. Sản phẩm ban đầu của Polk là danh mục những doanh nghiệp có trụ sở tại Michigan, được tổ chức bởi một nhà ga xe lửa. ý tưởng này là tạo điều kiện dễ dàng hơn cho những khách hàng sống gần một nhà ga xe lửa có thể mua hàng ở gần đó. Trong thế kỷ 20, Polk trở thành một công ty hàng đầu trong lĩnh vực bán những thông tin về danh sách đăng ký xe máy. Polk đã sử dụng những danh sách đó để liên hệ với người sở hữu xe ôtô nhân danh ngành sản xuất thiết bị giao thông và tạo lợi nhuận bằng cách kết nối người sản xuất và thiết kế xe với nhau với những thông tin chung, và sau đó bán thông tin đó cho những nhà nghiên cứu thị trường muốn sử dụng những thông đó để xác định lối sống, thu nhập và những thuộc tính khác giúp quyết định việc mua bất kỳ một sản phẩm nào đó. [11]

Thông tin có phải là đối tượng của quyền sở hữu không ?

Cá nhân coi thông tin riêng tư là tài sản cá nhân của mình và mọi việc sử dụng mà không có sự đồng ý của họ sẽ bị coi là ăn cắp thông tin cá nhân. Vì vậy, một số học giả đã cho rằng dữ liệu và thông tin, những thông tin cá nhân cụ thể, phải có được quyền tài sản và sự bảo vệ tương ứng vì thế việc sử dụng chúng có thể mang giá trị vật chất nhất định.

Đây là sự khác biệt cơ bản với cơ chế pháp luật hiện hành. Hiện tại, việc ăn cắp bí mật cá nhân được bảo vệ bởi những quy định pháp lý. Một người xâm phạm bí mật cá nhân của người khác có thể bị kiện. Nếu DoubleClick theo dõi khách hàng bằng cách thiết lập chế độ cookies trong thiết bị máy tính lưu trữ và nếu nhiều khách hàng cảm thấy bí mật cá nhân của họ bị xâm phạm thì DoubleClick có thể bị dính lứu đến một vụ kiện. Một chế độ tài sản cho phép kiểm soát và tạo quyền lực cho cá nhân có quyền sở hữu, chế độ này hỏi phải thoả thuận với người sở hữu trước khi trao đổi. Trong một chế độ tài sản, người có quyền sở hữu có thể thoả thuận mức giá, nhưng trong một chế độ trách nhiệm, toà án sẽ làm như vậy.[12]

Chế độ tài sản có vẻ phù hợp hơn trong bối cảnh việc vi phạm thông tin cá nhân trên Internet ngày càng nhiều. , mặc dù có thể xẩy ra tranh chấp nhiều hơn. Việc coi thông tin là đối tượng của quyền sở hữu và có cơ chế bảo vệ đủ để giải quyết việc sử dụng trái phép thông tin. Tuy nhiên, đây có thể là những vấn đề trong tương lại.

Bí mật thương mại là gì ?

Bí mật thương mại là bất kỳ một công thức, mẫu, thiết bị vật lý, ý tưởng, quá trình, sự biên tập thông tin hoặc những thông tin khác mà :

- cung cấp cho người sở hữu thông tin lợi thế so sách trên thị trường; và
- được sử dụng theo cách có thể ngăn ngừa việc tiết lộ công khai hoặc những việc đối thủ cạnh tranh biết về nó, ngoại trừ trường hợp có được thông tin đó một cách bất hợp pháp.

Trong thực tế, bí mật thương mại và những ý tưởng được tiết lộ, sao chụp hoặc được bán cho những đối thủ cạnh tranh, tạo cho người sở hữu chúng những lợi thế

cạnh tranh không nhỏ. Điều này cũng đúng trên môi trường mạng và có lẽ còn dễ hơn.

Những bí mật thương mại bị xâm hại thế nào ?

Bí mật thương mại có thể bị xâm hại hoặc thông qua việc ăn cắp trái phép thông tin hoặc từ việc vi phạm những thoả thuận về giữ bí mật. Trường hợp ăn cắp trái phép thông tin có thể xây ra đối với những mẫu gián điệp cũ hoặc những dạng gián điệp mới như tin tặc. Trong trường hợp vi phạm những thoả thuận về giữ bí mật, nghĩa vụ giữ bí mật đã đã không được thực hiện, như trường hợp một người làm công cho một công ty không được có hành vi đi ngược lại quyền lợi của công ty.[13]

Có cách để bảo vệ bí mật thương mại không ?

Nhằm nhấn mạnh nhu cầu bảo vệ bí mật, và để đảm bảo những dấu hiệu tồn tại của một nghĩa vụ như vậy, theo truyền thống, hầu hết những công ty công nghệ cao đều đòi hỏi người lao động phải ký kết một bản thoả thuận về giữ bí mật.

Một người sở hữu bí mật thương mại có thể đảm bảo cho quyền chống lại người khác đã ăn cắp thông tin bí mật bằng cách đề nghị toà án đưa ra một lệnh (được gọi là một huấn thị) nhằm trách việc tiết lộ thông tin sau này. Nó cũng có thể tập hợp những thiệt hại về mặt kinh tế như là kết quả của hành vi tiết lộ và sử dụng bí mật thương mại.

Sau đây là ví dụ về một vụ xâm phạm bí mật thương mại liên quan tới Wal-Mart và Amazon.com. Tháng 11/1998, Wal-Mart đã khởi kiện tại Arkansas chống lại Amazon.com "*nhằm dừng ngay lập tức việc Amazon.com bán hệ thống thông tin tuyệt mật bởi và việc những người khác sử dụng hội viên cũ của Wal-Mart*". Toà án thu lý ban đầu đã quyết định rằng vụ kiện cần được đưa ra toà tại Bang Washington, trụ sở của Amazon.com.

Tháng 1/1999, Wal-Mart một lần nữa đã kiện Amazon.com và người bảo trợ cho Amazon là Drugstore.com, nhưng lần này tại toà án ở Washington. Theo cáo buộc, Amazon đã thuê 15 cán bộ kỹ thuật quan trọng của Wal-Mart vì kiến thức của họ về hệ thống bán lẻ trên mạng. Trưởng phòng Thông tin của Amazon đã đóng vai trò như phó giám đốc của hệ thống thông tin tại Wal-Mart trước khi được thuê bởi Amazon vào năm 1997. Vào tháng 3/1999, Amazon đã kiện lại Wal-Mart dựa trên cáo buộc rằng Wal-Mart đã thực hiện hành vi cạnh tranh không lành mạnh và can thiệp một cách có ý thức vào hoạt động của Amazon.com". Đây là một trong những vụ án phức tạp nhất trong lĩnh vực này. Vụ kiện chấm dứt bằng việc các bên đã đi tơi một thoả thuận vào tháng 4/1999.[14]

Quyền sở hữu bí mật thương mại được kiểm chứng thế nào ?

Để thắng trong một vụ kiện liên quan tới bí mật thương mại, một người sở hữu bí mật thương mại phải chứng tỏ rằng thông tin được coi là bí mật đã thực sự là một bí mật thương mại. Một lần nữa, thoả thuận giữ bí mật thường là cách tốt nhất để

làm chuyện này. Thêm vào đó, người sở hữu bí mật thương mại phải chứng tỏ rằng thông tin mà bị cáo có được đã được thu thập một cách bất hợp pháp (nếu bị cáo bị buộc tội sử dụng bí mật vì mục đích thương mại) hoặc được tiết lộ một cách bất hợp pháp hoặc có vẻ như vậy (nếu bị cáo bị buộc tội tiết lộ thông tin).

Có trường hợp bí mật bị tiết lộ theo những quy định pháp luật không ?

Tuy nhiên, trường hợp bí mật thương mại được phát hiện ra một cách độc lập, tức là không bằng việc sử dụng những biện pháp phi pháp, thì người phát hiện ra bí mật thương mại đó vẫn có thể nó. Ví dụ, hành vi phân tích một sản phẩm có được một cách hợp pháp và xác định đó là bí mật thương mại.

Một số công ty phần mềm đã tiết lộ bí mật thương mại của họ một cách cố ý nhằm tìm ra những khiếm khuyết của sản phẩm phần mềm, với mục đích cho để người khác đặt hàng những giải pháp cho những khiếm khuyến này. Ví dụ, Netscape đã xuất bản mã nguồn của mình sau khi phát hiện ra rằng chương trinh máy tính của mình có những khiếm khuyến về an toàn mà có thể bị khai thác bởi tin tặc. Người xây dựng Netscape đã hy vọng rằng với việc tiết lộ hoặc gửi mã nguồn, những người phát triển phần mềm khác có thể xem xét kỹ lưỡng nó, và tìm ra dấu hiệu chạy không chuẩn, và cung cấp những đường dẫn mà người sử dụng Netscape có thể tải xuống miễn phí.

Bằng sáng chế phương thức kinh doanh là gì ?

Bằng sáng chế phương thức kinh doanh là một loại bằng sáng chế được biết như những bằng sáng chế tiện ích được sử dụng để bảo vệ những phát minh, công thức hoá học, hoặc những khám pháp khác. Phương pháp kinh doanh được coi như một quá trình bởi vì nó không phải là những vật thể vật chấp như những phát minh cơ khí hay cấu trúc hoá học khác.[15]

Tháng 7/1998, một toà án liên bang đã quy định rằng những luật về bảo hộ bằng sáng chế nhằm bảo vệ bất cứ phương pháp nào, dù có dựa trên máy tính hay không, miễn là phương pháp đó tạo ra một kết quả hữu ích, cụ thể và hữu hình.[16]

Một số ví dụ về bằng sáng chế phương thức kinh doanh:

- Bằng sáng chế "**1-click**" rất nổi tiếng của Amazon.com (U.S. Patent No. 5,960,411) ngày 28/9/1999, được cấp cho "*một hệ thống và phương pháp nhằm đưa ra một chào mua hàng qua mạng Internet*". Bằng sáng chế được quản lý chủ yếu đối với cách thức thông tin về người sử dụng được lưu trữ trên website, sau đó, người sử dụng có thể đặt hàng từ nó với một nhắp chuột vào đường liên kết với một mặt hàng.
- Bằng sáng chế "**Đấu giá đặt sẵn**" của Priceline (U.S. No. 5,794,207), được cấp cho một "*phương thức và bộ máy của hệ thống mạng thương mại chạy trên cơ chế bảo mật được thiết kế để tạo sự phù hợp với những chào mua hàng có điều kiện*". Tháng 11/1999, Priceline.com đã kiện Khách sạn Price Matcher của

Microsoft về vi phạm Bản quyền sáng chế đối với Phương thức kinh doanh Đấu giá đặt sẵn.

- Bằng sáng chế "**Quảng cáo DoubleClick**" (U.S.No.5,948,061), cấp cho "*một phương pháp truyền gửi, nhắm đích, và đo lường việc quảng cáo qua mạng*". Tháng 11/1999, DoubleClick đã kiện Công tyL90 tại Virginia vì đã sử dụng phương pháp này để truyền gửi quảng cáo trên mang Internet.
- Băng sáng chế "**Mua hàng bằng giỏ hàng điện tử**" (U.S. 5,715,314), cấp cho "*Hệ thống bán hàng qua mạng*".

Bằng sáng chế phương pháp kinh doanh có thể được sử dụng một cách hiệu quả chống lại những kẻ cạnh tranh chủ yếu. Ví dụ, tháng 9/1999 Amazon.com đã thành công trong việc buộc BarnesandNoble.com ngừng việc sử dụng hệ thống bán hàng one-click và buộc Công ty đó sử dụng một hệ thống đặt hàng phức tạp hơn.

Có những quy định pháp lý gì về thủ tục xin cấp bằng sáng chế ?

Toà án Hoa Kỳ vừa mới đưa ra phán quyết rằng Cơ quan quản lý bằng sáng chế có quyền cấp bằng sáng chế về giải pháp thương mại nếu thoả mãn thủ tục thử nghiệm ba tầng đối với bằng sáng chế. Đó là, sáng chế phải:

1. *Hữu ích*. Một doanh nghiệp chỉ cần chứng minh rằng một phương thức hoặc phần mềm có thể tạo ra những giá trị hữu hình cụ thể. Ví dụ, Bằng Sáng chế Amazon 1-click tạo ra kết quả hữu hình là một vụ mua bán được tiến hành.

2. *Mới*. Phương pháp hoặc phần mềm đó phải mới. Điều này có nghĩa là nó phải có một khía cạnh ứng dụng nào đó khác với một vài cách đã được biết từ trước.

3. *Không dễ dàng tạo ra được*. Phương pháp hoặc phần mềm phải không dễ tạo ra được, có nghĩa là một ai đó khi đã có kỹ năng bình thường trong lĩnh vực công nghệ cụ thể cũng không thể dễ dàng nghĩ ra nó. Ví dụ, một nhà kinh tế tạo ra một phương pháp tránh thuế bằng việc sử dụng một thẻ tín dụng để mượn tiền từ một tài khoản 40l(k). Phương pháp này không tồn tại trước đây và khác về chất với những phương pháp tránh thuế trước đó. Khi mà phương pháp này mới và không dễ tạo ra đối với những kế toán hoặc chuyên gia thuế, nhà kinh tế có quyền đòi hỏi được cấp bằng sáng chế cho nó.

Internet có ảnh hưởng gì đối với sở hữu trí tuệ ?

Đặc tính không biên giới của Internet, đặc biệt là thương mại điện tử, đưa ra câu hỏi liên quan tới khả năng áp dụng hệ thống pháp luật truyền thống trong việc tăng cường pháp luật về sở hữu trí tuệ. Như đã đề cập trước đó, hệ thống pháp luật truyền thống được xây dựng trên những khái niệm về chủ quyền và lãnh thổ.

Ngược lại, Internet thương không thể bị giới hạn bởi biên giới lãnh thổ. Vì vậy, Internet thường được miêu tả như một "***chiếc máy sao chụp***"lớn nhất thế giới.

Nhờ vào những khả năng và đặc tính của công nghệ kỹ thuật số, thương mại điện tử có thể có những ảnh hưởng rất lớn đối với hệ thống quyền tác giả và những quyền

liên quan, và phạm vi của quyền tác giả và những quyền liên quan tới lượt mình có thể ảnh hưởng nhất định tới thương mại điện tử. Nếu những quy định pháp luật không được đưa ra và được áp dụng một cách phù hợp, ciệc xác định những nguyên lý cơ bản của quyền tác giả và những quyền liên quan cũng sẽ khó thực hiện. Trên Internet, một người có thể tạo ra số lượng bản sao không giới hạn của một chương trình, bản nhạc, tác phẩm nghệ thuật, sách hay phim ảnh ở một thời điểm nào đó, và không làm ảnh hưởng lớn tới chất lượng. Thực tế, không có sự khác biệt giữa bản gốc và bản copy. Và bản sao có thể được truyền gửi tới những khu vực khác trên thế giới chỉ trong một vài phút. Kết quả là có thể làm mất đi thị trường truyền thống của những tác phẩm này.

Tại sao sản phẩm số hoá dễ bị vi phạm bản quyền ?

Đặc tính của những tác phẩm số hoá khiến chúng dễ bị ăn cắp bản quyền. Vì vậy, việc tải về một phần mềm, cuốn sách điện tử, hoặc âm nhạc trên mạng bằng chiếc máy tính để bàn tại nhà là rất dễ dàng và thuận tiện.

Đây là nguyên nhân tại sao thương mại điện tử thường liên quan tới việc bán và cấp phép sở hữu trí tuệ, và tiềm năng đầy đủ của nó sẽ không được thực hiện nếu sản phẩm sở hữu trí tuệ không được bảo vệ một cách đầy đủ. Nhà cung cấp nội dung và những người sở hữu khác của quyền sở hữu trí tuệ sẽ không để lơi ích của mình bị đe doạ trừ phi một cơ chế bảo hộ phù hợp, ở mức quốc tế hoặc quốc gia, được hình thành để bảo đảm những điều khoản theo đó tác phẩm của họ được đưa ra.

Công nghiệp âm nhạc và phim ảnh đã có hành đồng chống lại hành vi vi phạm bản quyền đối với việc sử dụng mp3, một công nghệ tổng hợp, tích hợp âm nhạc cho phép có thể tải về được một cách dễ dàng. Bên cạch sự thành công trong việc chống lại Napster, gần đây, đã có quyết định cấm một wetsite (2600.com) phát tán phần mềm để đổi mã số DVD. Trong vụ việc này, 2600.com đã bị kiện do trang Web này đã phát tán phần mềm đổi mã số nhằm bảo vệ DVDs khỏi bị sao chép, website này cũng đã tạo đường liên kết tới hơn 500 website khác trên toàn thế giới cũng có phần mềm tương tự. Thẩm phán ra phán quyết chống lại 2600.com, cho rằng "*nguyên đơn đã bị thiệt hại nghiêm trọng do việc sử dụng chương trình có nguy cơ làm giảm thu nhập của các studio từ việc bán và cho thuê DVDs và làm mất động lực đối với việc hình thành những sáng kiến nhiều tiêm năng, mới và sáng tạo cho việc phân phối những tác phẩm phim hoạt hình ở dạng số hoá, như phim ảnh theo đặt hàng trên Internet*".[17]

Tháng 5/2002. Audiogalaxy.com, một dang công ty hoạt động giống Napster, đã tạo thuận lợi và khuyến khích việc mua bán trái phép hàng triệu bản sao những bài hát, đã bị đưa ra toà bởi Hiệp hội công nghiệp ghi âm của Mỹ (RIAA) và Hiệp hội những nhà xuất bản âm nhạc quốc gia (NMPA) vì vi phạm bản quyền bán buôn tác phẩm âm nhạc.[18] Sau vụ kiện một tháng, Audiogalaxy.com đã phải đồng ý để một hệ thống lọc đòi hỏi sự cho phép của những người viết, phát hành và/hoặc những công ty ghi âm trước khi bài hát được chia sẻ trên mạng Internet.

“Copyleft” là gì ?

Copyleft là "*một thông báo bản quyền cho phép việc tái phân phát và sửa đổi một cách giới hạn, miễn rằng mọi bản sao và những sản phẩm của nó vẫn được phép*"[20]. Copyleft là phương pháp để tạo một chương trình phần mềm miễn phí. Phần mềm miễn phí dạng này cho phép người sử dụng chạy, sao, phân phối, nguyên cứu, thay đổi hoặc nâng cấp phần mềm. Tương ứng, nó tạo cho người sử dụng tự do: (1) chay chương trình cho bất kỳ mục đích nào; (2) nghiên cứu cách để chương trình chạy và làm nó phù hợp với những nhu cầu của người sử dụng; (3) tái phân phối những bản sao cho người khác; và (4) nâng cấp chương trình và phát tán chương trình được nâng cấp đó ra công chúng.

“GPL” là gì ?

GPL là từ viết tắc của Giấy phép phổ biến công cộng (General Public License). Trong khi giấy phép cho hầu hết phần mềm ngăn cản việc chia sẻ và thay đổi chương trình, một phần mềm GPL tạo cho người sử dụng tự do chia sẻ và thay đổi. Theo GPL, người sử dụng được tự do nhận hoặc đề nghị mã nguồn, thay đổi chương trình hoặc sử dụng chương trình đó, hoặc một phần của nó, trong một phần mềm miễn phí mới hoặc được nâng cấp. Một phần mềm GPL, tuy nhiên, phải thoả mãn điều kiện là việc hưởng quyền chia sẻ và thay đổi được chuyển giao cho những người nhận và sử dụng sau đó. [22]

Có những vấn đề cơ bản gì về bảo vệ quyền sở hữu trí tuệ trên Internet ?

Vấn đề cơ bản nhất là phải xác định được phạm vi bảo vệ trong môi trường số hoá, đó là, làm thế nào định nghĩa quyền, và những ngoài lệ và giới hạn gì được cho phép. Những vấn đề quan trong khác bao gồm làm thế nào quyền được đảm bảo thi hành và được quản lý trong môi trường này; ai trong dây truyền phát tán những tài liệu vi phạm có thể chịu trách nhiệm pháp lý đối với việc vi phạm; và những vấn đề về thẩm quyền xét xử và luật áp dụng.

Có những sáng kiến quốc tế nào nhằm bảo vệ sở hữu trí tuệ trên Internet ? Có những điều ước quốc tế nào quy định về Internet ?

Tổ chức sở hữu trí tuệ thế giới WIPO, với 179 nước thành viên, chịu trách nhiệm hình thành khung khổ pháp luật và chính sách ở mức độ quốc tế để tăng cường việc tạo ra và bảo vệ quyền sở hữu trí tuệ. Mục đích cao nhất của nó là đạt được mức thăng bằng phù hợp trong pháp luật, cung cấp quyền đầy đủ và hiệu quả trong phạm vi hợp lý và trong những ngoại lệ phù hợp. Từ khi việc mua bán sản phẩm có bản quyền, đặc tính và tín hiệu âm đã trở nên một yếu tố quan trọng trong thương mại điện tử toàn cầu, những người có quyền sở hữu nên được bảo vệ một cách hợp pháp trong khả năng của mình để bán và cấp phép cho sở hữu của họ trên Internet phù hợp với những giới hạn và những ngoại lệ tương ứng nhằm bảo vệ việc sử dụng vì lợi ích của cộng đồng.

WIPO đã có 23 hiệp định quốc tế liên quan tới những khía cạnh khác nhau của việc bảo vệ sở hữu trí tuệ.

Theo Công ước Berne, công ước lớn nhất về bản quyền tác giả quốc tế, việc bảo vệ bản quyền bao quát mọi sản phẩm văn học và nghệ thuật. Thuận ngữ này bao gồm những dạng khác nhau của sự sáng tạo, như sản phẩm viết, cả tiểu thuyết lẫn không phải tiểu thuyết, bao gồm những văn bản kỹ thuật và khoa học và chương trinh máy tính; cơ sở dữ liệu gốc do việc lựa chọn và sắp xết nội dung của nó; tác phẩm âm nhạc; tác phẩm nghe nhìn; tác phẩm nghệ thuật , bao gồm bản vẽ và tranh vẽ; và ảnh chụp. Những quyền liên quan được bảo vệ bao gồm việc đóng góp của những người thêm vào giá trị của tác phẩm văn học nghệ thuật khi được đưa ra công chúng, bao gồm những nghệ sĩ biểu diễn như diễn viên, nghệ sĩ múa, ca sĩ và nhạc công; những người tạo ra tín hiệu âm, bao gồm đĩa CD; và những tổ chức truyền thanh.

Tương tự, năm 1996 WIPO đã thông qua 2 Hiệp định: **Hiệp định Quyền tác giả** WIPO (WCT) và **Hiệp định về ghi âm và trình diễn** (Performances and Phonograms Treaty(WPPT). thường được coi là những hiệp định về Internet, những hiệp định này tìm cách đưa ra những vấn đề về định nghĩa và phạm vi quyền trong môi trường số hoá, và một số thách thức của việc đảm bảo thực thi và cấp phép trực tuyến. Hiệp định WTC và WPPT cũng đã làm rõ phạm vi kiểm soát của người nắm giữ quyền khi tác phẩm nghệ thuật, biểu diễn và ghi âm được đưa ra công chúng để tải về hoặc được truy cập tới trên mạng Internet. Dạng truyền gửi này khác với phát thanh, trong đó tài liệu không được lựa chọn và chuyển đi bằng một thiết bị truyền tín hiệu vật lý giống như máy phát thanh tới nhóm những người nghe. Hơn nữa, nó được truyền đi một cách tương tác, đó là theo yêu cầu từ những người sử dụng cá nhân, tại thời điểm và địa điểm do họ lựa chọn. Những hiệp định đòi hỏi rằng một quyền đặc biệt được cấp để kiểm soát những hành vi tuyên truyền ra công chúng như vậy, trong khi dành cho các nước quyền quyết định xem phải sắp xếp quyền đó như thế nào trong hệ thống pháp luật quốc gia.

Các hiệp định trên đã có hiệu lực từ tháng 3 và tháng 5 năm 2002. Những quy định của cả hai hiệp định đã được trên cơ sở đồng thuận bởi 100 quốc gia. Ngay nay, chúng cũng đóng vai trò như tài liệu hướng dẫn và những quy định mẫu cho pháp luật quốc gia. Nhằm để những hiệp định trên được áp dụng thực sự trong môi trường mạng, chúng phải được thể hiện trong pháp luật của nhiều nước trên thế giới. WIPO vì thế đang tiến hành những hoạt động nhằm thúc đẩy việc áp dụng các hiệp định đó và để đưa ra lời khuyên đối với các chính phủ về việc thực thi và thông qua.

Tại sao cần những sáng kiến như vậy ?

Những vấn đề về thi hành và cấp phép không mới, nhưng chúng đã thay đổi ở nhiều khía cạnh và ở mức độ cấp thiết khi những tác phẩm được khai thác trên hệ thống kỹ thuật số. Nhằm bảo vệ về mặt pháp lý trở nên có ý nghĩa, người giữ quyền phải có quyền kiểm tra và dừng việc phát tán những bản sao số hoá không được phép, mà do đặc tính của môi trường số hoá, những tác phẩm dạng này có thể bị

phát tán rất nhanh và với số lượng lớn, ở khoảng cách xa tới không thể tượng tượng nổi. Hơn nữa, đối với thương mại điện tử, để phát triển ở mức độ cao nhất, cần phải xây dựng những hệ thống hỗ trợ việc cấp phép trực tuyến đáng tin cậy.

V. TRANH CHẤP VỀ TÊN MIỀN

Tên miền là gì ?

Tên miền là địa chỉ của công ty trên mạng Internet và tương đương với địa chỉ kinh doanh trong thế giới thực. Vì ngày có càng nhiều công ty sử dụng Internet, số lượng những tranh chấp phát sinh từ việc sử dụng tên miền tăng càng nhanh.

Tên miền được chia phân chia theo những cấp khác nhau. Cấp cao nhất xuất hiện sau dấu chấm (.) trong tên miền. Ví dụ trong tên miền "microsoft.com", mức tên miền cao nhất là .com, tên miền cấp một phổ biến nhất, chỉ ra rằng tên miền được sở hữu bởi một công ty thương mại. Những tên miền cũng phổ biến khác là .org (cho những tổ chức phi lợi nhuận), .net (cho những tổ chức liên quan tới mạng và và Internet), .edu (cho các trường đại học), và .gov (cho cơ quan chính phủ). Tách biệt với những tên miền chung này, mỗi quốc gia có một tên miền cấp một. Ví dụ, .ca chỉ tên miền của Canada, và .ie chỉ tên miền của Irac.

Tranh chấp về tên miền có thể nẩy sinh như thế nào ?

Tranh chấp về tên miền liên quan tới những tên miền cấp hai, chúng đề cập tới tên liên kề phía bên trái của tên miền cấp cao nhất trong địa chỉ Internet. Ví dụ, trong tên miền "www.microsoft.com" , tên miền cấp hai là Microsoft.

Hai tên miền cấp hai giống hệt nhau không thể cùng tồn tại dưới cùng một tên miền cập một. Ví dụ, mặc dù Công ty Delta Faucet và Delta Airlines đều muốn đặt tên miền là "delta.com", nhưng chỉ có một công ty có thể có tên miền delta. Không may cho cả Công ty Delta Faucet và Delta Airlines, Công ty đã đặt tên miền là delta.com là Công ty tài chính Delta của Woodbury, có trụ sở tại Newyork. (Delta Airlines sử dụng tên miền deltaairlines.com trong khi công ty Delta Faucet sử dụng tên miền là Deltafaucet.com).

Một số ví dụ điển hình về tranh chấp về tên miền:

- **Mcdonalds.com**: tên miền này đã bị đăng ký bởi một cá nhân viết bài cho tạp chí Wired, người này đã viết một câu chuyện về giá trị tên miền. Trong bài báo của mình, tác giả đã yêu cầu liên lạc với mình tại địa chỉ ronald@mcdonalds.com với đề nghị liên quan tới tên miền đó. Để dành lại tên miền MacDonalds, tác giả đã yêu cầu Công ty Mcdonalds phải có một khoản đóng góp từ thiện.
- **Micros0ft.com**: Công ty Zero Micro Software, đã đăng ký tên miền micros0ft.com (với số không thay thế chữ o), nhưng việc đăng ký này đã bị đình chỉ sau khi Microsoft kiện công ty này.

- **Mtv.com**: tên miền MTV trước tiên đã bị đăng ký bởi Công ty Adam Curry cho trò chơi video MTV. MTV đầu tiên đã không quan tâm tới tên miền này trên Internet. Nhưng khi Adam Curry từ bỏ MTV, Công ty đã muốn kiểm soát tên miền. Sau khi vụ kiện ở liên bang được tiến hành, tranh chấp đã được giải quyết.
- **Taiwan.com**: Tổ chức thông tin Trung Quốc ở lục địa Xinhua đã được phép đăng ký tên miền taiwan.com, trong sự bất bình của chính phủ Đài loan.

Người nào kiểm soát tên miền ? và Những vụ tranh chấp về tên miền sẽ được giải quyết thế nào ?

Trước Tháng 12/1999, một công ty có tên Network Solutions Inc (NSI) hầu như là cơ quan duy nhất quản lý việc đăng ký tên miền cấp hai cho những tên miền cấp một thông dụng, bao gồm tên miền .com, .net, và .org. NSI đã đưa ra chính sách độc tài đối với tên miền và đã có quyền kiểm soát rất lớn đối với tên miền được đăng ký, và cách thức giải quyết những vụ tranh chấp. Nhằm trách việc phải giải quyết tranh chấp về tên miền, NSI đã ban hành chính sách thứ tự ưu tiên về thời gian. Theo cơ chế này, người nào đăng ký tên miền trước thì sẽ có giá trị trước. Nếu tên miền vẫn chưa bị đăng ký thì người đăng ký sẽ được phép. Chính sách này giờ đã bị thay đổi bởi Chính sách giải quyết tranh chấp về tên miền thống nhất do ICANN (Tổ chức Internet cho việc đánh số và xác định tên đăng ký) và được sử dụng bởi tất cả những người đăng ký tin tưởng. Theo chính sách mới này, một người sở hữu thương nhãn có thể đưa ra một thủ tục hành chính tương đối đơn giản để kiểm tra sự tồn tại của tên miền. Muốn được đăng ký, người sở hữu thương nhãn phải chứng minh rằng:

1. Người đó sở hữu một nhãn mác (hoặc được đăng ký hoặc chưa được đăng ký) giống hệt hoặc tương tự tền miền cấp hai được đăng ký;
2. Bên đăng ký tên miền không có quyền hoặc lợi ích hợp pháp đối với tên miền; và
3. Tên miền được đăng ký và sử dụng vì mục đích xấu.

Những người tranh chấp về tên miền có thể tới toà án để kiện. Tại Mỹ, Đạo luật bảo vệ người tiêu dùng chống lại những hành vi vi phạm trên mạng tháng 11/1999 đã quy định thủ tục dễ dàng hơn cho cá nhân và công ty để kiện trong những trường hợp có tên hoặc thương nhãn tương tự (tới mức gây nhầm lẫn). Tuy nhiên, họ phải chứng minh rằng người nắm giữ tên miền có mục đích xấu.

Một phần của Đạo luật trên liên quan tới những cá nhân nổi tiếng. Phần cho phép cá nhân kiện theo thủ tục dân sự chống lại người đăng ký tên họ như một tên miền cấp hai cho mục đích bán tên miền đó để kiếm lợi bất chính. Ví dụ trường hợp vụ tên miền juliaroberts.com. Một cá nhân đã có ý định bán tên miền này cho nữ diễn viên Julia Roberts sau khi đã đăng ký nó. Để chứng minh mục đích xấu của người đăng ký, toà án đưa ra quy định rằng tên miền phải được chuyển giao cho người sử dụng hợp pháp nó.

Có tổ chức quốc tế nào giải quyết những vụ tranh chấp ?

WIPO vừa mới thiết lập một cơ quan trọng tài và trung tâm hoà giải, được mô tả trên trang web của WIPO là "*được chấp nhận trên toàn thế giới là cơ quan hàng đầu trong lĩnh vực giải quyết tranh chấp tên miền*". Từ tháng 9/1999, Trung tâm này đã giải quyết những vụ việc liên quan tới tên miền cấp một như .com, .org, .net.

Sau quyết định của ICANN ngày 16/11/2000 cho phép 7 tên miền cấp một mới, WIPO đã làm việc với những người vận hành tên miền cấp một mới để xây dựng cơ chế giải quyết tranh chấp liên quan tới tên miền cho những tên miền của họ. Trung tâm cũng đã chỉ định cung cấp dịch vụ giải quyết tranh chấp cho những tên miền này.

Thêm vào đó, Trung tâm cũng giải quyết cả những thủ tục tranh chấp về Tên miền cấp một theo mã quốc gia, như .ph cho Phillippines hoặc th cho Thái Lan.

VI. VẤN ĐỀ BẢO VỆ BÍ MẬT THÔNG TIN VỀ NGƯỜI TIÊU DÙNG

Những tiến bộ trong công nghệ thông tin và quản lý dữ liệu tạo ra khả năng có một nền kinh tế dựa trên mạng Internet mới và thịnh vượng. Hệ thống thông tin và truyền thông mới cho phép tập hợp, chia sẻ và phát triển những khối lượng thông tin với tốc tộ và tính hiệu quả không thể dự liệu được. Những công nghệ này cũng đặt ra nguy cơ đối với thông tin bí mật. Tổ chức, cá nhân ngày nay, bằng những phương tiện, phương pháp mới, có khả năng xâm phạm bí mật cá nhân của người khác và dưới một phương thức rất khó cản trở.

Bí mật riêng tư là gì ?

Thông tin bí mật cá nhân có một ý nghĩa quan trọng, "*đó là sự đòi hỏi của một cá nhân để kiểm soát được những điều kiện theo đó thông tin cá nhân - những thông tin cho phép nhận dạng ra cá nhân đó - bị truy cập, tiết lộ và sử dụng*". [23]

Bí mật cá nhân bị tiết lộ được định nghĩa tương tự như "*khả năng của cá nhân để chọn cho mình thời gian, hoàn cảnh, và mức độ theo đó thái độ, niềm tin, cử chỉ và ý kiến được chia sẻ cùng hoặc từ chối chia sẻ cùng người khác.*" [24]

Tại sao phải bảo về bí mật riêng tư ?

Quyền có bí mật cá nhân là quyền cơ bản trong một xã hội dân chủ. Việc bị nắm giữ, dù là nhỏ nhất, một phần thông tin về chính mình thông qua Internet có nghĩa là đã mất đi quyền tự do cơ bản. Hơn nữa, càng nhiều người khác biết về những chi tiết về đời sống của một người thì khả năng người đó bị ảnh hưởng, can thiệp hoặc phán xét sẽ càng lớn.

Việc biết và kiểm soát khả năng tiết lộ thông tin cá nhân ; việc truyền gửi và sử dụng thông tin cá nhân là chìa khoá để bảo vệ tính riêng tư.

Có trường hợp bảo vệ bí mật riêng tư quá mức ?

Một trong những vẫn vấn đề gây nhiều tranh luận là liệu một cơ chế quá nghiêm khác nhằm bảo vệ việc tiết lộ thông tin riêng tư có thể gây cản trở đối với thương mại. Việc đòi hỏi sự đồng ý của một người trước khi dữ liệu cá nhân có người đó bị sử dụng có thể ngăn cản sự phát triển của thương mại, thường được dựa trên nguyên tắc "*thông tin tốt hơn có nghĩa là thị trường tốt hơn*". Nếu thị trường có thể xác định chính xác những người khác hàng, việc tạo sự phù hợp giữa những người mua và người bán có thể được tiến hành.

Một vấn đề gây tranh luận khác là sự cần thiết phải trung thực. Những nghĩa vụ pháp lý và đạo đức của việc tiết lộ gắn liên với một mối quan hệ, đòi hỏi việc mở rộng mà bí mật thông tin có thể ngăn cản.

Những thách thức nào đối với việc bảo vệ bí mật thông tin được đặt ra ? Làm sao có thể sử dụng hợp pháp thông tin được đảm bảo ?

Tìm ra sự thăng bằng giữa nhu cầu pháp lý để thu thập thông tin và nhu cầu bảo vệ bí mật riêng tư đã trở thành một thách thức lớn. Những hướng dẫn sau đây của OECD có thể được cân nhắc như những đòi hỏi cơ bản nhất đối với việc sử dụng hoặc xử lý hợp pháp những thông tin trực tuyến :

- *Nguyên tắc bảo vệ bí mật thông tin*. Thông tin cá nhân có thể dành được, bị tiết lộ, và sử dụng chỉ theo những cách tôn trọng bí mật cá nhân.
- *Nguyên tắc toàn vẹn thông tin*. Thông tin cá nhân phải không bị thay đổi hoặc huỷ đi một cách trái phép.
- *Nguyên tắc chất lượng thông tin*. Thông tin phải chính xác, đúng thời gian, hoàn thiện và liên quan tới mục đích mà nó được cung cấp hoặc sử dụng.
- *Nguyên tắc giới hạn thu thập*. Dữ liệu cá nhân phải có được bằng phương tiện hợp pháp và trong trường hợp thích hợp, với kiến thức và sự thống nhất về đối tượng dữ liệu.
- *Nguyên tắc cụ thể mục đích*. Dữ liệu cá nhân cần phải được bảo vệ một cách hợp lý chống lại những nguy cơ giống như mất hoặc việc truy cập trái phép, việc phá huỷ, sử dụng, thay đổi hoặc tiết lộ dữ liệu.
- *Nguyên tắc không che đậy*. Cần có một chính sách cởi mở phù hợp với sự phát triển, thực tiễn và chính sách đối với dữ liệu cá nhân.
- *Nguyên tắc trách nhiệm giải trình*. Người kiểm soát dữ liệu có trách nhiệm tạo sự phù hợp với những biện pháp dựa trên những nguyên tắc được nêu trên.

Có những hướng dẫn khác về bảo vệ dữ liệu không ?

Liên minh Châu Âu đã ban hành Chỉ thị 95/46/EC, nó đã thành lập một khung khổ pháp lý đê đảm bảo sự tự do trao đổi dữ liệu cá nhân, trong khi cho phép những nước thành viên EU việc đưa ra những quy định riêng đối với việc thi hành Chỉ thị này. Việc trao đổi tự do dữ liệu là đặc biệt quan trọng đối với mọi dịch vụ với một

cơ sở khách hàng lớn và phụ thuộc vào việc xử lý dữ liệu cá nhân, như việc bán hàng từ xa và dịch vụ tài chính. Thực tế, ngân hàng và công ty bảo hiểm phải xử lý một khối lượng lớn dữ liệu cá nhân, bên cạnh những thứ khác, về những vấn đề máng tính nhậy cảm cao như tín dụng và giá trị tín dụng. Nếu mỗi nước thành viên đã có hệ thống quy định riêng của mình về bảo vệ dữ liệu (ví dụ về cách thức làm sao chủ thể dữ liệu có thể xác minh thông tin về họ), việc cung cấp những dịch vụ qua biên giới , nhất là thông qua những siêu xa lộ thông tin, sẽ không thể thực hiện được và cơ hội thị trường đặc biệt có giá trị này sẽ bị mất.
Chỉ thị cũng nhằm mục đích thu hẹp sự khác biệt giữa những luật bảo vệ dữ liệu của quốc gia ở mức cần thiết để rời bỏ những rào cản đối với tự do dữ liệu cá nhân trong EU. Nhờ vào đó, bất cứ người nào mà dữ liệu được xử lý trong Cộng đồng Châu Âu sẽ có thể được tạo một mức độ bảo vệ quyền tương đương, đặc biệt đối với quyền bí mật cá nhân, bất luận ở nước thành viên nào, nơi mà việc xử lý được tiến hành.

Người tiêu dùng có thể được bảo vệ thế nào trong các giao dịch thương mại điện tử ?

Tháng 12/1999, OECD đã ban hành Bản hướng dẫn về bảo vệ người tiêu dùng trong bối cảnh thương mại điện tử để giúp bảo vệ người tiêu dùng khi tiến hành mua bán trên mạng, và từ đó khuyến khích họ :

- kinh doanh trung thực ; tiến hành quảng cáo và tiến hành nghiên cứu thị trường;
- có thông tin rõ ràng về nhận dạng của một doanh nghiệp trực tuyến, hàng hoá và dịch vụ được chào và điều khoản của giao dịch ;
- quá trình minh bạch cho việc xác định các giao dịch ;
- cơ chế thanh toán an toàn;
- cơ chế giải quyết tranh chấp và đền bù phù hợp, đúng hạn và hợp lý; bảo vệ bí mật cá nhân; và giáo dục người tiêu dùng và doanh nghiệp.

Bảng 2. Hướng dẫn của OECD về bảo vệ người tiêu dùng

A. Bảo vệ minh bạch và hiệu quả

Người tiêu dùng tham gia vào thương mại điện tử phải được hưởng chế độ bảo vệ minh minh bạch và hiệu quả không thấp hơn mức độ bảo vệ được đưa ra trong những hình thức thương mại khác.

B. Thông lệ thị trường, quảng cáo và kinh doanh trung thực

Doanh nghiệp tham gia thương mại điện tử phải quan tâm đúng mức tới những lợi ích của người tiêu dùng và hành động phù hợp với những thông lệ thị trường, quảng cáo và kinh doanh trung thực.

C. Tiết lộ bí mật trực tuyến

I. Thông tin về doanh nghiệp

Doanh nghiệp tham gia TMĐT với khách hàng phải cung cấp thông tin dễ tiếp cận, rõ ràng và chính xác về chính mình đủ để cho phép ở mức thấp nhất.

II. Thông tin về hàng hoá hoặc dịch vụ

Doanh nghiệp tham gia TMĐT với khách hàng cần cung cấp những thông tin dễ tiếp cận và chính xác về miêu tả hàng hoá, dịch vụ được chào; đủ để người tiêu dùng ra quyết định có nên tham gia giao dịch hay không và theo cách tạo khả năng cho người tiêu dùng lưu trữ một bản ghi đầu đủ về thông tin đó.

III. Thông tin về giao dịch

Doanh nghiệp tham gia TMĐT phải cung cấp đầy đủ thông tin về những điều kiện và chi phí kèm theo giao dịch để khiến người tiêu dùng có thể ra quyết định về việc có nên tham gia giao dịch đó không.

IV. Quá trình xác nhận

Để tránh việc gây nhầm lẫn liên quan tới ý định của khách hàng khi mua hàng, khách hàng phải có thể, trước khi đưa ra lệnh mua, nhận dạng chính xác những hàng hoá hoặc dịch vụ mà người đó mong muốn mua; nhận dạng những sai sót hoặc thay đổi của chào hàng; thể hiện một sự đồng ý với đây đủ thông tin và tự nguyện khi mua hàng; và lưu trữ một bản ghi đầy đủ và chính xác về giao dịch.

V. Thanh toán

Người tiêu dùng cần được cung cấp cơ chế thanh toán an toàn, dễ sử dụng và được thông tin về mức độ an toàn của cơ chế đó.

Giải quyết tranh chấp và bồi thường

Người tiêu dùng phải được cung cấp khả năng truy cập có ý nghĩa tới việc giải quyết tranh chấp và đền bù đúng thời gian mà không chịu chi phí quá đáng.

Bảo vệ bí mật

TMĐT B2C cần được tiến hành phù hợp với những nguyên tắc bảo vệ bí mật được thừa nhận như được đưa ra trong Hướng dẫn của OECD điều chỉnh bảo vệ bí mật riêng tư và việc trao đổi qua biên giới của dữ liệu cá nhân (1980). Cũng tính tới tuyên bố hội nghị bộ trưởng của OECD về bảo vệ bí mật cá nhân trên mạng toàn

cầu (1998), để cung cấp khả năng bảo vệ người tiêu dùng một cách phù hợp và hiệu quả.

Giáo dục và nâng cao nhận thức

Chính phủ, doanh nghiệp và đại diện người tiêu dùng cần phối hợp với nhau để tuyền truyền cho người tiêu dùng về thương mại điện tử, hỗ trợ việc ra quyết định với đầy đủ thông tin bở người tiêu dùng khi tham gia vào thương mại điện tử, và tăng cường nhận thức của doanh nghiệp và người tiêu dùng về cơ chế bảo vệ người tiêu dùng được áp dụng cho hoạt động trực tuyến của họ.

Nguồn: Tổ chức phát triển và hợp tác kinh tế, Hướng dẫn về Bảo vệ người tiêu dùng trong bối cảnh thương mại điện tử (2000); có sẵn trên trang web: http://www1.oecd.org//publications/e-book/9300023E.PDF

Các hướng dẫn của OECD sẽ được sử dụng thế nào ?

Hướng dẫn của OECD được thiết kế như một công cụ trung lập về mặt công nghệ để giúp đại diện các chính phủ, doanh nghiệp và người tiêu dùng bằng cách đưa ra những hướng dẫn thực tế để giúp hình thành và duy trì niềm tin của khách hàng vào thương mại điện tử. Hướng dẫn này đưa ra những khía cạnh cơ bản của thương mại điện tử B2C và phản ánh những quy định pháp luật đang hiện hành đối với khách hàng trong những hình thức truyền thống hơn của thương mại. Họ nhấn mạnh tầm quan trọng của việc minh bạch hoá và tiết lộ thông tin và sự cần thiết có sự hợp tác giữa các chính phủ, doanh nghiệp và người tiêu dùng ở mức quốc gia và quốc tế.

Hướng dẫn nhằm cung cấp những nguyên tắc để giúp :

- Chính phủ xem xét, và (nếu cần thiết) tạo sự phù hợp, hình thành khuôn mẫu và thi hành chính sách và sáng kiến khách hàng trong thương mại điện tử.
- Doanh nghiệp, người tiêu dùng và những tổ chức tự quản khác, bằng việc đưa ra hướng dẫn về những đặc điểm cơ bản của việc bảo vệ khách hàng mà có thể được cân nhắc trong quá trình phát triển và thi hành những cơ chế tự quản.
- tổ chức kinh doanh và người tiêu dùng, bằng việc vạch ra những sự tiết lộ thông tin cơ bản và những thực tiễn kinh doanh điển hình mà họ có thể cung cấp hoặc mong chờ ở trên mạng.

Xem xét thế nào về vấn đề xét xử và bồi thường cho người tiêu dùng ?

Hướng dẫn của OECD đã đề cập theo chiều sâu những vấn đề liên quan tới thẩm quyền xét xử, những luật được áp dụng và khả năng tiếp cận tới việc bồi thường. Vì bản chất rộng và sâu của những vấn đề trên, những câu hỏi làm sao chúng có thể được đưa ra một cách tốt nhất trong bối cạnh thương mại điện tử không phải chỉ duy nhất đối với việc bảo vệ người tiêu dùng. Tuy nhiên, tiềm năng của Ỉnternet làm tăng số lượng giao dịch B2C qua biên giới tạo đòi hỏi một điều quan trọng rằng lợi ích của khách hàng được tính tới một cách đầy đủ.

Hướng dẫn trên của OECD cho thấy tính phức tạp của vấn đề và thực tế vẫn còn thiếu sự đồng thuận quốc tế về những vấn đề này. Hướng dẫn thừa nhận rằng moi giao dịch qua biên giới giữa doanh nghiệp và người tiêu dùng nằm trong khung khổ pháp lý về quyền xét xử và luật áp dụng, nhưng thương mại điện tử đặt ra những thách thức mới cho khung khổ pháp lý đó. Hướng dẫn đòi hỏi cần phải làm nhiều việc hơn nữa trong để đưa ra những vấn đề này và đảm bảo rằng lợi ích của người tiêu dùng được bảo vệ khi hình thành những quy định mới.

Hướng dẫn trên cũng đề cập tới tầm quan trọng của việc tạo khả năng tiếp cận của khách hàng đối với những thủ tục bồi thường hợp lý, đúng thời gian và tiện lợi ; và khuyến khích xây dựng những cơ chế giải quyết tranh chấp thay thế hiệu quả. Việc khởi kiện để giải quyết một tranh chấp thường rất tốn phí, khó khăn và mất nhiều thời gian. Những vấn đề như vậy có thể càng phức tạp hơn đối với những tranh chấp mạng tính quốc tế. Trong những hình thức thương mại khác, sự phát triển của những cơ chế giải quyết tranh chấp thay thế hiệu quả có thể giúp tránh được những thủ tục phức tạp hiện hành, để giải quyết những khiếu nại của người tiêu dùng một cách nhanh chóng, dễ dàng và hợp lý, và thiết lập những cơ chế giải quyết tranh chấp trực tuyến hiệu quả nhằm tạo dựng niềm tin cho người tiêu dùng.

Chính phủ có cần can thiệp vào vấn đề bảo vệ người tiêu dùng và bí mật riêng tư hay không ? Khu vực tư nhân có thể đóng vai trò gì ?

Cuối cùng, vấn đề bảo vệ người tiêu dùng và bí mật cá nhân là vấn đề của cả khu vực chính phủ và khu vực tư nhân. Chính phủ phải đảm bảo rằng có đủ luật cho phép bảo vệ người tiêu dùng; khu vực tư nhân phải thi hành chế độ bảo vệ bí mật cá nhân có ý nghĩ, thân thiện và tự điều chỉnh. Cho tới khi người sử dụng tin tưởng rằng việc truyền thông và dữ liệu của họ là an toàn khỏi việc bị ngăn chặn và việc sự dụng trái phép, có vậy mới khuyến khích họ sử dụng Internt vì mục đích thương mại. Chỉ với niềm tin của khách hàng mới có thể giúp thương mại điện tử phát triển.

VII. TỘI PHẠM TRÊN MẠNG

Có thể có tội phạm trên mạng được không ?

Mạng Internet có tiềm năng trở thành một trong những thành tựu lớn nhất của loài người. Viễn thông, hệ thống ngân hàng, tiện ích công cộng và hệ thống xử lý khẩn cấp đều hoạt động trên mạng. Nhưng có những người sử dụng Internet vào mục đích xấu. Trong lịch sử tồn tại rất ngắn của Internet, chúng ta đã chứng kiến rất nhiều hành vi phạm tội. Mặc dù thường rất khó để xác định những động cơ của những hành vi vi phạm trên mạng này, hậu quả của chúng là khiến người ta giảm niềm tin vào hệ thống Internet.

Nguy cơ tăng mạnh những hành vi vi phạm trên mạng lớn tới nỗi mà Cơ quan điều tra liên bang của Hoa Kỳ (FBI) đã tiến hành một số bước chuẩn bị cho cuộc chiến chống lại tội phạm trên mạng và khủng bố trên mạng và coi đó là mối quan tâm đáng ưu tiên số 3 sau chống khủng bố và chống chiến tranh du kích. Thêm vào đó,

FBI đã thay đổi định hướng nhằm tập chung vào việc tuyển dụng chuyên gia và hình thành một dạng cơ quan mới có nhiều kinh nghiệm trong thế giới Công nghệ thông tin.

Tội phạm máy tính hoặc tội phạm trên mạng là gì ?

"**Tội phạm máy tính**" hay tội phạm trên mạng đề cập tới một hành vi vi phạm liên quan tới việc sử dụng máy tính. Tội phạm trên mạng có thể được phân thành những nhóm lớn sau: Tội phạm trên mạng chống lại con người, tài sản và chính phủ.

Tội phạm trên mạng chống lại con người bao gồm việc truyền gửi những văn hoá phẩm đồi truỵ hoặc quấy rối tình dục qua sử dụng một máy tính như e-mail.

Tội phạm trên mạng chống lại tài sản bao gồm việc xâm phạm máy tính bất hợp pháp qua không gian trên mạng, mang tính phá hoại hệ thống máy tính, truyền gửi những chương trình gây hại, và sở hữu những thông tin máy tính bất hợp pháp. Hành vi xâm nhập và bẻ khoá nằm trong số những hành vi nguy hiểm nhất của loại tội phạm trên mạng cho tới nay. Việc tạo và truyền bá những chương trình máy tính gây hại hoặc virus trong hệ thống máy tính là một dạng khác của tội phạm trên mạng chống lại tài sản. Sao chụp phần mềm bất hợp pháp cũng là một dạng đặc biệt của tội phạm trên mạng thuộc nhóm này.

Một ví dụ điển hình khác của tội phạm trên mạng chống lại chính phủ là khủng bố trên mạng, trong đó không gian ảo bị sử dụng bởi cá nhân và tổ chức để đe doạ chính phủ và khủng bố người dân của một nước. Loại tội phạm này có hình thức của những cá nhân xâm nhập vào một trang web của cơ quan chính phủ hoặc quân đội.

Có những ví dụ điển hình gì về tội phạm trên mạng ?

1. *Gửi bom thư (Mail bombing)*: liên quan tới việc gửi rất nhiều thông điệp và nhiều lần nhằm vào một người nhận xác. Hộp thư của người nhận vì thế tràn ngập những bức thư vớ vẩn.
2. *Gửi phát tán thư (Spamming)*: thường được sử dụng như một công cụ cho xúc tiến thương mại. Loại này nhắm vào nhiều người nhận và làm ngập những hội thư này với các thông điệp vớ vẩn.
3. *Liên kết danh sách (List Linking)*: liên quan tới việc đăng ký một địa chỉ e-mail trong nhiều danh sách gửi mai.
4. *Lừa đảo (Spoofing)*: là giả mạo nhận dạng của người gửi e-mail và giả tạo để lừa người nhận rằng e-mail được bắt nguồn từ một người gửi mail giả định nào đó.
5. *Kết nối không được sự đồng ý*: là tìm đưa một nội dung website lên một trang web khác mà không được sự đồng ý của trang web đó.
6. *Từ chối dịch vụ*: là một nỗ lực trái phép nhằm ngăn cản người sử dụng hợp pháp của một dịch vụ khỏi việc sử dụng dịch vụ đó.

7. *Bẻ khoá là hành vi truy cập một* cách trái phép vào một hệ thống và phá huỷ hệ thống đó, gây nên những thiệt hại nhất định.

Trong mội trường mạng, nạn nhân thường phải nhận rất nhiều thông điệp với nội dung đe doạ.

Phạm vi của tội phạm trên mạng ?

Tội phạm trên mạng không bị giới hạn bởi phạm vi lãnh thổ hoặc thẩm quyền xét xử của một quốc gia. Nếu không bị kiểm tra hoặc trừng phạt, tội phạm trên mạng sẽ ảnh hưởng tới sự phát triển của thương mại điện tử. Thêm vào đó, có sự di chuyển nhanh chóng các loại hình tội phạm truyền thống vào thế giới ảo như nạn mại dâm trẻ em, lừa dối, làm giả, xuyên tạc, ăn cắp sở hữu trí tuệ, ăn cắp thông tin và tiền...

Những quy định pháp lý nào cần có để ngăn ngừa, nắm bắt và buộc tội những tội phạm trên mạng ?

Những quy định liên quan tới trộm cắp cần phải được xem xét lại. Trong nhiều hệ thống xét xử hoặc trong thế giới thực, việc trộm cắp liên quan tới việc lấy một thứ hoặc tước quyền sở hữu của một nạn nhân. Giải quyết thế nào đối với trường hợp một người truy cập mà không được phép vào một phai của người khác và sau đó sao lại file đó ? Trong trường hợp này, nó có thể được cho rằng việc trộm cắp không xẩy ra vì vật đó đã bị sao lại mà không bị lấy đi. Làm rõ sự việc này là vụ việc tại nước Mỹ nơi có quy định pháp luật liên quan tới truyền gửi tài sản ăn cắp giữa các bang chỉ đề cập tới những đồ vật hữu hình và không áp dụng đối với đồ vật vô hình.

1. *Những thách thức về mặt cộng nghệ*: trong khi có thể lần theo dấu vêt theo một đường dẫn điện tử, nhiệm vụ trở nên rất khó khăn vì kỹ năng và công nghệ cho phép dấu tên khi tiến hành hành vi vi phạm.

2. *Những thách thức về mặt pháp lý*: pháp luật và những công cụ pháp lý khác chống lại tội phạm đi sau sự thay đổi nhanh chóng của công nghệ.

3. *Thách thức về mặt nguồn lực*: điều này đề cập tới vấn đề thiếu những chuyên gia, hoặc thiếu ngân sách cho những công nghệ mới cũng như cho việc đào tạo con người.

Những hoạt động nào đang được thực hiện nhằm ngăn ngừa và buộc tội tội phạm trên mạng ?

Đạo luật gian lận và lợi dụng máy tính (18 USC 1030); 18 USC 2701 trừng phạt việc truy cập trái pháp luật tới nhưng kho truyền thông được lưu trữ; 18 USC 2702 ngăn cấm việc tiết lộ cho bất kỳ người nào những nội dung truyền thông một kho lưu trữ dữ liệu điện tử; và 18 USC 2703 cho phép việc tiết lộ cho chính phủ đối với những nội dung của truyền thông điệp tử nhưng chỉ theo lệnh của toà án.

Sau vụ khủng bố ngày 11/9/2001, Hạ viện Hoa Kỳ đã ban hành Đạo luật ái quốc USA. Đây là một đạo luật bao quát nhằm tới việc chống lại nguy cơ khủng bố, bao

gồm cả khủng bố trên mạng. Đạo luật mới này tạo quyền lực cho những cơ quan thi hành pháp luật trong và ngoài nước có thể giúp phát hiện và ngăn cản hành vi khủng bố. Đạo luật ái quốc đã mở rộng những phương pháp truyền thống như theo dõi nghe trộm điện thoại, truy nã tìm kiếm, giấy đòi ra hầu toà để tạo khả năng dễ hơn cho việc thi hành pháp luật của Hoa Kỳ và của cơ quan điều tra nhằm chống lại khủng bố. Ví dụ, Chính phủ Hoa Kỳ giờ có thể theo dõi hành vi truy cập trang web của người mỹ để nói với toà án rằng việc theo dõi không dẫn tới thông tin liên quan tới việc điều tra tội phạm.

Đạo luật ái quốc cũng tương tự, có 2 thay đổi về lượng thông tin mà chính phủ có thể có được liên quan tới người sử dụng từ những nhà cung cấp dịch vụ của họ. Điều 212 của Luật này cho phép Nhà cung cấp dịch vụ cung cấp tự nguyện mọi thông tin không có nội dung cho việc thi hành pháp luật mà không cần bất kỳ yêu cầu nào từ toà án. Thứ 2, Điều 210 và 211 đã mở rộng những bản ghi mà chính phủ có thể tìm thấy với một lệnh của toà để bao gồm những bản ghi về thời gian hội họp, những địa chỉ mạng được đăng ký hiện thời, phương tiện và nguồn thanh toán, bao gồm cả thẻ tín dụng hoặc số tài khoản.

Có hay không những nỗ lực liên chính phủ chống lại tội phạm trên mạng ?

Hội đồng Châu Âu đã thông qua một Công ước về tội phạm trên mạng, Công ước này đã đưa ra những loại tội phạm sau:

1. Tội phạm chống lại tính đáng tin cậy, toàn vẹn và sự sẵn sàng của dữ liệu và hệ thống, như việc truy cập trái phép, sự ngăn chặn trái pháp luật, can thiệp vào hệ thống và dữ liệu bằng những thiết bị trái pháp luật;
2. Những tội phạm liên quan tới máy tính như làm hàng giả liên quan tới máy tính và những hành vi giả mạo liên quan tới máy tính;
3. Những tội phạm liên quan tới nội dung như tuyền truyền tài liệu khiêu dâm trẻ em; và
4. Tội phạm liên quan tới bản quyền tác giả.

Công ước cũng khuyến khích các thành viên tham gia vào những nỗ lực chung, thông qua hỗ trợ lẫn nhau, thoả thuận về dẫn độ và những biện pháp khác nhằm chống lại tội phạm trên mạng. Kêu gọi hợp tác quốc tế là rất quan trong trong bối cảnh tội phạm trên mạng vượt ra ngoài sự kiểm soát của mỗi quốc gia.

Tương tự, Diễn đàn Hợp tác Kinh tế Châu Á - Thái Bình Dương đã tiến hành những chương trình hoạt động sau đây để chống lại sự phát triển của tội phạm trên mạng:

- lập tức ban hành pháp luật hỗ trợ lẫn nhau và những thoả thuận về nội dung và thủ tục liên quan tới an toàn trên mạng;
- bao quát như những nội dung được thể hiện trong Công ước về tội phạm trên mạng của Châu Âu;
- hỗ trợ lẫn nhau giữa những nền kinh tế trong việc phát triên khả năng đánh giá nguy cơ;

- những hướng dẫn về an toàn và kỹ thuật có thể được chính phủ và những tổ chức xã hội sử dụng trong nỗ lực chống lại tội phạm trên mạng; và
- mở rộng chương trình đối với những nền kinh tế và người tiêu dùng lên quan tới an toàn trên mạng.

Những nước thành viên của Hiệp hội các nước Đông Nam Á (ASEAN) đã thống nhất tạo một trung tâm hợp tác an toàn mạng ASEAN với mục đích giúp đỡ giải quyết những vụ việc trên mạng và khủng bố trên mạng. Nhóm phản ứng lại những biến cố bất thường cũng sẽ được thành lập trong khu vực ASEAN nhằm phục vụ hệ thống cảnh báo chống lại viruses. Những nước ASEAN sẽ tập chung vào việc tăng cường hạ tầng Công nghệ thông tin và truyền thông phù hợp nhằm thu hút nhiều nhà đầu tư hơn nữa.

Có những động thái nào nhằm chống lại tội phạm trên mạng ở những nước đang phát triển ?

Tại Phillipines, Đạo luật Thương mại điện tử cũng đưa ra những hình phạt đối với việc truy cập và bẻ khoá trái phép, cũng như việc phát tán những chương trình viuses.

Đạo luật tội phạm trên mạng của Malaysia năm 1997 đưa ra những hình phạt đối với việc truy cập trái phép vào những tà liệu máy tính, truy cập trái phép với mục đích phạm tội, chỉnh sửa trái phép nội dung của một máy tính, và truyền thông sai trái.

Đạo luật lam dụng máy tính của Singapore trừng phạt việc truy cập đối với tài liệu máy tính, truy cập với mục đích phạm tội hoặc tạo thuận lợi cho phạm tội, sửa đổi trái phép tài liệu máy tính, sử dụng trái phép hoặc ngăn cản dịch vụ máy tính, cản trở trái phép việc sử dụng máy tính, và tiết lộ trái phép việc truy cập vào hệ thống mật mã.

Tại Ấn độ, Đạo luật Công nghệ thông tin năm 2000 ngăn cản việc trục lợi từ những nguồn tại liệu của máy tính và việc bẻ khoá.

Vấn đề gì được coi là quan trọng nhất để chống lại tội phạm trên mạng ?

Một điều được cho là một công cụ tốt nhất chống lại việc truy cập không gian ảo và tội phạm ảo vẫn là việc ngăn ngừa. Có rất nhiều công nghệ có thể được sử dụng đối với nhiều người giúp ngăn ngừa các hành vi tấn công trên mạng như bức tường lửa, công nghệ mã khoá, và hệ thống hạ tầng mã khoá công khai.

Bên cạnh pháp luật, những nguồn lực khác cũng cần phải được cung cấp cho những cơ quan thực thi pháp luật để họ có thể có được công cụ, thiết bị và những kiến thức cần thiết giúp bảo vệ thành công hệ thống mạng khỏi những sự vi phạm trên. Pháp luật chống lại tội phạm trên mạng sẽ không có ý nghĩa gì nến cơ quan thực thi pháp luật không có được đào tạo cần thiết để thậm trí có khả năng vận hành một máy tính. Thẩm phán cũng phải được đào tạo.

Hơn nữa, tham vấn, hợp tác và phối hợp giữa những chính phủ và khu vực tư nhân là rất quan trọng, nhằm tạo sự hài hoà hoá một cách hoàn thiện nhất có thể những biện pháp, thực tiễn, và thủ tục sẽ được sử dụng để chống lại vấn đề trên. Việc hài hoà hoá hệ thống pháp luật trên phạm vị quốc tế, khu vực và quốc gia là cần thiết để đối mặt với những thách thức mang tính quốc tế.

Tổ chức, cá nhân nào cần tham gia việc chống lại tội phạm trên mạng ?

An toàn và bí mật không phải chỉ thuộc về trách nhiệm của chính phủ. Cần thiết sự tham gia của khu vực tư nhân để thi hành những chính sách gần gũi với người sử dụng và họ có thể tự tiến hành.

Chính phủ sẽ phải làm việc cùng những luật sự (người hướng dẫn luật) trên mạng khác để phát triển những giải pháp phù hợp đối với những vấn đề liên quan tới tội phạm trên mạng mà chúng có thể được phát hiện một cách đầy đủ bởi khu vực tư nhân.

Môt nhiệm vụ vô cùng khó khăn để tăng sự hiểu biết ở mọi mức độ của xã hội – trong chính phủ, khu vực tư nhân, trong nhân dân và thậm trí ở mỗi cá nhân – về nhu cầu cho, và mục đích của, an toàn và bảo vệ bí mật và việc ngăn ngừa và kiểm soát tội phạm trên mạng. Sự hiểu biết về tội phạm được tiến hành trên mạng và những biện pháp có thể chống lại chúng cũng rất cần thiết. Cuối cùng và có lẽ là quan trọng nhất, một điều thiết yếu là chúng ta phải có được sự đồng thuận đối với việc sử dụng đúng đắn và có đạo đức về máy tính và hệ thống thông tin.

VIII. KIỂM DUYỆT HOẶC NHỮNG QUY ĐỊNH VỀ NỘI DUNG

Quy định về nội dung là gì ?

Quy định về nội dung đề cập tới những quy định pháp luật của một chính phủ liên quan tới:

- Kiểm duyệt thông tin và truyền thông trên Internet; và
- Kiểm soát hay cố gắng kiểm soát việc tiếp cận tới những trang web có vấn đề trên Internet.

Các quốc gia có chính sách và pháp luật về nội dung như thế nào ?

Nhiều chính phủ tìm cách phát hiện và kiểm soát thông tin trên Interrnet không tuân theo luật pháp của nước họ và có hại hoặc không phù hợp với trẻ vị thành niên. Thông tin như vậy có rất nhiều, từ những tuyên ngôn về chính trị đến những tài liệu kích động hay xúi dục thù hằn sắc tộc, hay những tài liệu về khiêu dâm.

Chính sách của chính phủ đối với việc kiểm duyệt Internet có thể được chia thành bốn nhóm vấn đề sau:

1. Chính sách khuyến khích hình thành cơ chế tự điều tiết trên Internet hoặc sử dụng các chương trình sàng lọc, ngăn chặn. Phương thức này đã được Liên hiệp Anh, Canada, và nhiều nước Tây Âu khác sử dụng. New Zealand cũng đang áp dụng phương thức này. New Zealand đã áp dụng việc phân loại các thông tin ngoài luồng một cách hiệu quả. Các nước trên đã xây dựng được các văn bản pháp luật điều chỉnh nội dung bất hợp pháp trên Interrnet, ví dụ như khiêu dâm trẻ em và kích động phân biệt chủng tộc. Các quốc gia này cũng có cơ chế phân biệt thông tin không phù hợp với trẻ vị thành niên những vẫn có giá trị trên Internet, những thông tin này được kiểm soát để trẻ vị thành niên không thể tiếp cận được. Một số quốc gia khuyến khích việc sử dụng và phát triển những công nghệ tạo điều kiện cho người sử dụng Internet kiểm soát chính bản thân cũng như việc truy cập Internet của con cái họ.
2. Luật hình sự áp dụng đối với những người cung cấp nội dung không phù hợp với trẻ vị thành niên trên mạng. Chính sách này được áp dụng tại một số Bang ở Australia và đã được thử nghiệm tại Mỹ. Những quốc gia này xây dựng những bộ luật điều chỉnh các nội dung bất hợp pháp, trong đó hình thành các hình thức chế tài tương ứng với các loại tội phạm truyền bá thông tin trái pháp luật trên Internet.
3. Ngăn chặn việc tiếp cận tới những nguồn thông tin bất hợp pháp. Chính sách này được cụ thể hoá trong pháp luật của Australia và Trung Quốc, A Rập Xê út, Việt Nam, và những nước khác. Một số quốc gia yêu cầu nhà cung cấp dịch vụ Internet ngăn chặn những tài liệu không phù hợp trong khi những quốc gia khác chỉ cho phép truy cấp những tài liệu Internet bị cấm thông qua những điểm truy cập do chính phủ kiểm soát.
4. Ngăn cấm việc truy cập Internet tại các điểm dịch vụ Internet công cộng. Một số quốc gia như Trung Quốc đưa ra biện pháp ngăn cấm việc truy cập Internet công cộng hoặc yêu cầu những người sử dụng Internet đăng ký với cơ quan có thẩm quyền của chính phủ trước khi được phép truy cập những thông tin bị cấm.

Những nước phát triển có quy định về nội dung thông tin trên Internet không ?

Câu trả lời là có. Tại Australia, các biện pháp kiểm duyệt được thể hiện trong pháp luật liên bang và của từng bang. Chế độ kiểm duyệt của Australia là một hệ thống được thành lập nhằm áp dụng đối với những người làm chủ nội dung thông tin, bao gồm những nhà cung cấp dịch vụ Internet, nhưng không bao gồm những nhà cung cấp nội dung thông tin. Chính phủ Australia yêu cầu các nhà cung cấp nội dung thông tin xoá bỏ những thông tin bất hợp pháp từ dịch vụ của họ (Web, Usenet, FTP, vv…), cơ quan của chính phủ sẽ gửi các khuyến cáo về việc tồn tại những thông tin bất hợp pháp tới nhà cung cấp nội dung. Tuy nhiên, pháp luật Australia không đòi hỏi các nhà cung cấp dịch vụ Internet ngăn chặn việc truy cập đối với nội dung không thuộc về Australia. Thay vào đó, cơ quan chuyên trách sẽ thông báo cho những nhà cung cấp phần mềm ngăn chặn những nội dung thông tin không thuộc về Australia để bổ sung vào danh sách cần quản lý của họ. Với những người sử dụng Internet tại Australia thì luật pháp không yêu cầu họ sử dụng phần mềm

ngăn chặn. Thêm vào đó, Australia cũng xây dựng luật hình sự liên bang và của từng bang để điều chỉnh hành vi vi phạm của những nhà cung cấp nội dung thông tin. Các quy định pháp luật này tạo điều kiện truy tố những người sử dụng Internet truy cập hoặc xử lý những nguồn thông tin bất hợp pháp hoặc không phù hợp với trẻ vị thành niên. Thẩm quyền xét xử các vụ việc liên quan tới vi phạm dạng này có khác nhau trong từng điều luật của mỗi bang.

Tại Pháp, chính phủ đã xây dựng những quy định pháp luật điều chỉnh việc truyền bá thông tin kỳ thị chủng tộc. Tháng 5/2000, toà án tại Pháp đã đưa ra phán quyết yêu cầu Công ty Yahoo của Mỹ phải có biện pháp ngăn chặn những người pháp sử dụng Internet để truy cập vào trang web bán đấu giá những kỷ vật gợi về chủ nghĩa phát xít và nạn phân biệt chủng tộc. Yahoo đã thừa nhận rằng không thể có biện pháp kỹ thuật nào ngăn chặn việc những người sử dụng Internet tại Pháp truy cập vào những trang web có nội dung về chủ nghĩa quốc xã và rằng trang web của Pháp tuân theo luật của Pháp về việc cấm quảng cáo những kỷ vật về chủ nghĩa quốc xã. Tháng 11 năm 2001, một toà án của Mỹ đã đã ra phán quyết rằng Yahoo không phải tuân theo yêu cầu của toà án Pháp liên quan tới việc truy cập những trang web của Mỹ. Toà án này viện cớ rằng Bộ luật sửa đổi đầu tiên của Mỹ bảo vệ nội dung thông tin thuộc về sở hữu của những công ty Mỹ khỏi những quy định của các quốc gia khác liên quan tới quyền tự do ngôn luận.

Vào giữa thập niên 90, những nhà cung cấp dịch vụ Đức ngăn chặn sự truy cập một số nội dung Internet không thuộc Đức mà chứa đựng những nội dung bất hợp pháp theo luật pháp của Đức, đặc biệt là việc tuyên truyền phân biệt chủng tộc và khiêu dâm trẻ em. Vào tháng 7 năm 2000, có nguồn tin cho biết chính phủ Đức đã ngừng những nỗ lực ngăn chặn việc truy cập vào những nội dung không thuộc về Đức nhưng cảnh sát sẽ tiếp tục ngăn chặn những thông tin bất hợp pháp được tạo ra trong nước. Năm 2001 và 2002, Chính phủ Đức thông báo về việc một số trang web của Mỹ không tuân thủ các quy định của pháp luật Đức. Bộ về Gia đình, Người cao tuổi, Phụ nữ và Trẻ em của Đức cũng thông báo về việc có những trang web nước ngoài đã truyền bá những thông tin trái với Công ước về Phổ biến ấn phẩm và những loại hình Truyền thông nguy hại đến đạo đức của lớp trẻ. Cơ quan này sau đó đưa ra yêu cầu phải có hình thức chế tài đối với những trang Web trên toàn thế giới có chứa đựng các nội dung về khiêu dâm, bạo lực, khích động chiến tranh, phân biệt chủng tộc, phát xít… Chính phủ Đức đã đề nghị chủ các trang web trên loại bỏ các thông tin bất hợp pháp ra khỏi trang web của họ hoặc phải hình thành cơ chế kiểm soát việc truy cấp tới những nguồn thông tin này.

Chính sách của Anh và Mỹ đối với việc kiểm duyệt nội dung trên Internet ?

Nước Anh vẫn chưa ban hành luật cụ thể điều chỉnh việc truy cập Internet và dường như không có ý định làm điều này. Tháng 9 năm 1996, một tổ chức phi chính phủ có tên UK Internet Watch Foundation (IWF) đã được thành lập với sự trợ giúp của hiệp hội các nhà cung cấp dịch vụ với mục đích đưa ra các biện pháp

loại bỏ các thông tin độc hại trên Internet, đặc biệt là những tài liệu khiêu dâm trẻ vị thành niên. IWF được thành lập sau khi Cảnh sát thành phố London đề nghị tất cả các nhà cung cấp dịch vụ Internet kiểm duyệt các thông tin trên mạng, nếu không sẽ tiến hành truy tố những nhà cung cấp dịch vụ Internet nào có thông tin bất hợp pháp trên hệ thống mạng của họ.

IWF vận hành một đường dây nóng để tạo điều kiện cho những thành viên trong cộng đồng thông báo về những tài liệu khiêu dâm trẻ em hoặc những tài liệu bất hợp pháp trên internet. Khi IWF nhận được báo cáo thì IWF sẽ xem xét và đưa ra quyết định liệu những tài liệu này có tiềm ẩn sự bất hợp pháp không. Sau đó, IWF sẽ cố gắng xác định nguồn gốc của những tài liệu này và thông báo tới cảnh sát Anh hoặc những cơ quan thi hành pháp luật thích hợp ở nước ngoài. IWF cũng đề nghị những nhà cung cấp dịch vụ của Anh loại bỏ những thông tin độc hại khỏi dịch vụ của họ; và nếu những họ không thực hiện yêu cầu thì sẽ phải đứng trước nguy cơ bị truy tố.

Tháng 2 năm 2002, IWF tuyên bố rằng họ sẽ loại bọ những thông tin mang tính phân biệt chủng tộc hoặc xúi dục phạm tội và rằng Bộ nội vụ đã cung cấp cho IWF bản hướng dẫn bổ sung các quy định áp dụng luật liên quan tới nạn phân biệt chủng tộc trên Internet - những tài liêu làm bùng phát ngọn lửa phân biệt chủng tộc trên internet.

Năm 1996, Chính phủ Mỹ bắt đầu thúc đẩy việc kiểm duyệt Internet khi thông qua luật Viễn thông trong sạch (Communication Decency Act: CDA), luật này hình sự hoá việc gửi bất cứ thông điệp "khiếm nhã" nào trên mạng Internet. Tháng 6/1996, một toà án tại Philadelphia đã phủ nhận CDA vì cho rằng luật này không phù hợp với hiến pháp và đi ngược lại tự do ngôn luận. Toà án này cũng đã đưa ra điều luật rằng Internet là "*một thị trường tự do lý tưởng*" và nên xem Internet như là truyền hình. Một trong những phán quyết có nội dung: "*Internet có thể được coi như một cuộc đối thoại bất tận trên toàn thế giới. Chính phủ không thể thông qua CDA ngắt lời những cuộc đối thoại này. Do Internet có tính năng ưu việt là tạo ra quyền tự do ngôn luận cho nên Internet xứng đáng được Chính phủ bảo vệ* ".

Một quy định pháp luật khác về nội dung Internet cũng không được áp dụng là Luật bảo hộ Internet đối với trẻ em (CIPA: Children's Internet Protectin Act), được Liên Bang Hoa Kỳ thông qua tháng 12/2000. Luật này buộc ngừng việc tài trợ cho hoạt động sử dụng các chương trình ngăn chặn những thiết bị đầu cuối mà cả người trưởng thành và trẻ vị thành niên đang sử dụng tại thư viện công cộng. Một toà án liên bang đã phủ nhận thẳng thừng CIPA với lý do rằng những chương trình ngăn cản không thể kiểm duyệt một cách hiệu quả những tài liệu "*có hại cho trẻ vị thành niên*". Toà án gọi phần mềm này là "*công cụ đần độn*", và nói thêm rằng "*những nhà sản xuất phải đối mặt với nhiều vấn đề tương tự và rằng những người bán phần mềm kiểm duyệt này nhiều vô kể*".

Trong Vụ khủng bố ngày 11/9 tại New York và Washington, bọn khủng bố được giả thiết là đã sử dụng Internet để liên lạc với nhau và chuẩn bị kế hoạch hành động. Điều này dẫn đến việc đòi hỏi phải có những biện pháp an toàn gắt gao và những quy định nghiêm khắc đối với Internet. Một ít phút sau khi vụ khủng bố xảy ra, cơ quan FBI đã viếng thăm một số cơ quan đầu não của những nhà cung cấp dịch vụ Internet tiếng tăm, bao gồm Hotmail, AOL và Earthlink để thu thập chi tiết những tin nhắn mà bọn khủng bố có thể gửi cho nhau qua email. Việc giám sát những tài liệu trên Internet được hợp pháp hoá vào ngày 24/10/2001 với việc ban hành đạo luật USA Patriot (Đạo luật nước Mỹ ái quốc). Phương pháp ngăn chặn bọn khủng bố này khẳng định rằng nhà cầm quyền đã sẵn sàng để FBI cài đặt chương trình Carnivore vào thiết bị của các nhà cung cấp dịch vụ Inernet với mục đích giám sát dòng chảy của những tin nhắn email và kiểm duyệt hoạt động của những trang Web mà bị tình nghi là có sự dích lứu với thế lực bên ngoài. Điều này thực hiện được chỉ dưới sự cho phép của một toà án đặc biệt.

Những nước đang phát triển nào có quy định điều chỉnh nội dung Internet ?

Tháng 9 năm 1996, Trung Quốc đã ban bố việc cấm truy cập một số trang Web cụ thể thông qua việc sử dụng hệ thống màng lọc để ngăn chặn việc tuyên truyền những thông tin không trong sạch. Những trang bị cấm bao gồm Western news outlets (Tin tức phương Tây), những trang bình luận về Đài loan, những trang của những người chống đối Trung Quốc và những trang về tình dục. Một nghiên cứu của trường đại học Luật chỉ ra rằng Trung Quốc là nước kiểm duyệt Internet mạnh mẽ nhất trên thế giới, thường xuyên từ chối sự truy cập của người sử dụng đối với 19.000 trang Web mà chính phủ cho rằng có những thông tin không lành mạnh. Nghiên cứu đã thử nghiệm truy cập từ nhiều điểm khác nhau ở Trung Quốc trong vòng sáu tháng, và nhận thấy rằng Bắc Kinh đã ngăn chặn hàng ngàn những tin tức phổ biến, những trang về chính trị và tôn giáo, cùng với những trò giải trí và giáo dục khác. Trung Quốc cũng không cho phép người sử dụng truy cập đến những trang tôn giáo phương Tây tầm cỡ. Những trang về tin tức cũng bị ngăn chặn. Trong số những trang người sử dụng gặp vấn đề trong khoảng thời gian thử nghiệm có những trang thuộc về phát thanh công cộng quốc gia như*: The Los Angeles Times,The Washington Post, và tạp chí Time.*

Các điểm truy cập Internet ở Ả Rập Xê Út chịu sự giám sát bởi một trung tâm kiểm soát của chính phủ từ năm 1999, khi mà truy cập Internet lần đầu tiên được đưa vào sử dụng. Từ trung tâm này, chính phủ ngăn chặn việc truy cập nội dung Internet rõ ràng không phù hợp với công dân nước họ, ví dụ như những thông tin cho là nhạy cảm với tôn giáo và chính trị, những trang khiêu dâm…Theo thông báo của tờ Thời báo New York ngày 19/11/2001 thì hàng tháng, hơn 7000 trang bị đưa vào danh sách cần kiểm duyệt và trung tâm kiểm soát nhận được hơn 100 yêu cầu mỗi ngày để loại bỏ việc kiểm soát một số trang đặc thù khỏi danh sách bởi những trang này bị mô tả không đúng sự thật do việc sử dụng phần mềm ngăn chặn thương mại của Mỹ.

Cơ quan Phát thanh Singapore (SAB) đã quy định nội dung Internet như là nội dung của dịch vụ phát thanh từ tháng 7 năm 1996. Trên cơ sở Kế hoạch Đăng ký loại Thông tin, Những người cung cấp nội dung Internet và những Nhà cung cấp dịch vụ cần tự động đăng ký. Việc đăng ký yêu cầu tuân theo những Điều kiện Đăng ký Phân loại và Mã Sử dụng Internet, nó bao gồm việc xác định những "*tài liệu cấm*". Tóm lại, "*tài liệu cấm*" là những tài liệu rõ ràng "*mang tích chống lại lợi ích công cộng, đạo đức công cộng, trật tự công cộng, an toàn công cộng, sự hoà hợp dân tộc, và những vấn đề không phù hợp với luật pháp Singapore*". SBA có quyền áp dụng hình phạt, bao gồm việc phạt tiền, với những người phải đăng ký.

SBA đưa ra cách tiếp cận hơi cứng rắn đối với việc quy định các dịch vụ trên Internet. Ví dụ như, những người đăng ký nếu bị phát hiện vi phạm quy định thì họ sẽ có một cơ hội để sửa chữa trước khi cơ quan có thẩm quyền xử lý. Những người sử dụng Internet ở Singapore truy cập tất cả những tài liệu có giá trị sử dụng trên Internet, ngoại trừ một số trang Web mà tính bất hợp pháp hiện hữu rõ ràng và nội dung Internet không bị SBA kiểm duyệt sơ bộ; và những nhà cung cấp dịch vụ cũng không bị yêu cầu kiểm soát nội dung Internet mà họ cung cấp. SBA chủ yếu quan tâm đến vấn đề khiêu dâm, bạo lực và kích động phân biệt chủng tộc, tôn giáo. Phạm vi hoạt động của SBA chỉ nhắm tới kiểm soát việc cung cấp những tài liệu đến khu vực công cộng. Đối với những liên lạc mang tính riêng tư, ví dụ như email và Internet Relay Chat giữa những cá nhân hay tổ chức, thì không phải nhiệm vụ của họ.

Những nước nào không điều chỉnh về nội dung ?

Tháng 8 năm 1998, Uỷ ban Viễn thông và Phát thanh - Truyền hình Canada (Canadian Radio-Television and Telecommunications Commission: CRTC) đã đưa ra cuộc bàn luận công khai về vai trò mà CRTC đúng ra đã phải có để hình thành những quy định đối với các vấn đề cần quan tâm như khiêu dâm trực tuyến, những phát biểu cực đoan và "*nội dung của Canada*" trên trang Web. Sau đó, tháng 5 năm 1999, CRTC đã đưa ra một tin với tiêu đề "*CRTC Sẽ không Quy định gì về Internet*". Nội dung tin này cho biết rằng "*sau khi tiến hành những cuộc phỏng vấn chuyên sâu, CRTC đã đưa ra kết luận rằng hình thức truyền thông mới trên internet sẽ đạt được những mục đích của Đạo luật truyền thông một cách đầy triển vọng, có tính cạnh tranh cao cũng như sẽ có được sự thành công mà không cần đến những quy định kiểm duyệt. CRTC cho rằng nỗ lực hình thành các quy định điều chỉnh lĩnh vực truyền thông mới của Canada có thể đẩy ngành công nghiệp này mất đi những thuận lợi cạnh tranh trên thị trị trường thế giới*."

Tương tự như vậy, Đan Mạch không có luật sử phạt đối với việc cung cấp những tài liệu không phù hợp với lứa tuổi vị thành niên trên Internet. Hoặc cũng không có bất cứ đề nghị nào về việc soạn thảo một bộ luật về vấn đề này. Thảo luận về việc bảo vệ vị thành niên đối với những nội dung không lành mạnh đang mở ra một vấn đề xoay quanh việc sử dụng thiết bị kiểm duyệt thông tin tại các thư viện công cộng.

Cũng như vậy, Nauy cũng không có quy định pháp luật điều chỉnh việc kiểm duyệt nội dung trên "*phương tiện truyền thông đại chúng mới (Internet)*". Nhưng thay vào đó, những nỗ lực trong vấn đề này là hướng đến thông báo tới đại chúng về sự phát triển của Internet thông qua Hội đồng Phân loại Phim Na Uy, Hội đồng này đôi khi xuất bản những báo cáo về sự tiến bộ của công nghệ và tác động của chúng đối với xã hội.

Việc kiểm soát nội dung trên Internet có tương tự việc kiểm soát nội dung trên máy điện thoại, đài hoặc tivi không ?

Công trả lời là chưa hẳn. Việc quy định về truyền thông qua phát thanh và truyền hình dựa trên cơ sở học thuyết "*sự khan hiếm*", học thuyết này cho rằng việc kiểm duyệt nội dung của chính phủ xác định vai trò của chính phủ trong việc quy định tần xuất phát đối với hình ảnh khan hiếm. Tuy nhiên, Internet không phải là nguồn thông tin "*khan hiếm*" vì mọi người có thể kết nối máy tính của mình với Internet mà không cần đến sự cho phép của chính phủ. Hoặc cũng không phải là nơi phải xin phép chính phủ để hoạt động. Hơn nữa, việc quản lý đối với điện thoại, phát thanh và truyền hình tỏ ra đơn giản hơn vì nhà nước có thể dễ dàng tìm cách chuyển "kênh" thông tin đến một địa điểm mà trẻ em hoặc đối tượng không được phép khó thể tiếp cận được.

Có nên kiểm duyệt thông tin trên Internet không ?

Internet là công cụ phát triển nhanh và rộng nhất đối với truyền thông đại chúng và cung cấp thông tin trên toàn thế giới. Nó có thể được sử dụng để cung cấp một lượng lớn thông tin tới bất cứ đâu trên thế giới với một chi phí cực rẻ. Vấn đề ở đây là thông tin có thể là "tốt" hay "xấu". Trong 10 năm trở lại đây, đã dấy lên sự quan tâm đến vấn đề nội dung có hại trên Internet, bao gồm nội dung về tình dục và bạo lực, hướng dẫn chế tạo bom, hoạt động khủng bố, và khiêu dâm trẻ em.

Rồi sao nữa? Phải chăng chính phủ nên tính đến việc sàng lọc thông tin? Hoặc những cá nhân nên được phép quyết định cho chính bản thân mình cái gì là có hại? Câu hỏi này không dễ trả lời vì nó liên quan tới sự cân bằng tế nhị giữa tự do ngôn luận, tự do thông tin của cá nhân và quyền của chính phủ được ngăn chặn những gì nguy hại đến công dân nước mình.

Bảng 2 tóm tắt về tính hai mặt của kiểm duyệt nội dung thông tin trên Internet.

Vấn đề tự kiểm duyệt thì thế nào ?

Quy định về bản thân ít có giá trị hơn so với những yêu cầu truyền thống và những quy định pháp luật về kiểm soát. Trước tiên, những đòi hỏi pháp lý về kiểm soát không thích hợp với những thay đổi nhanh chóng của công nghệ trong kỷ nguyên đổi mới. Thứ hai, với những quy định tự điều chỉnh thì các cấp chính quyền không cần phải mở rộng bộ máy củng cố quyền lực một cách mạnh mẽ. Đối với người sử dụng (doanh nghiệp, người tiêu dùng), việc tự điều chỉnh có vẻ phù hợp hơn, nó đòi

hỏi tính tự nguyên của người sử dụng và tạo cho họ quyền được tự bảo vệ chính mình.

Việc tự kiểm duyệt có thể hiệu quả thế nào ?

Cần có những quy định pháp luật mới đảm bảo rằng nội dung Internet và hành vi của các nhà cung cấp dịch vụ Internet phù hợp với những nguyên tắc xã hội. Toàn xã hội cần quan tâm tới vấn đề này và xây dựng một hệ thống quy định đáng tin cậy. Ví dụ, cần thiết lập các đòi hỏi đối với các nhà cung cấp dịch vụ Internet, bắt buộc họ phải loại bỏ những nội dung bất hợp pháp khi nhận được thông báo rằng những nội dung này đang tồn tại trong dịch vụ của họ. Thủ tục để đưa ra thông báo và loại bỏ nội dung cần được quy định cụ thể.

Bảng 3. Kiểm duyệt hay không kiểm duyệt

Kiểm duyệt	Không kiểm duyệt
Việc cho phép tự do ngôn luận trên Internet sẽ gây ra những tác hại không nhỏ đối với toàn xã hội. Lợi ích của việc không kiểm duyệt nội dung sẽ không thể so sánh với những thiệt hại mà các thông tin độc hại có thể gây ra, ví dụ như những thông tin khiêu dâm trẻ vị thành niên, thông tin khích động bạo lực, cổ động chiến tranh…	Kiểm duyệt nhìn chung là một tai hoạ và nên tránh áp dụng. Thông tin khiêu dâm trẻ em đã có những điều luật thích hợp điều chỉnh. Việc tự do ngôn luận có ý nghĩa tiêu cực của nó nhưng chỉ biện pháp tốt nhất là nên vạch trần và đấu tranh với nó. Mặt khác, những nhóm người này sẽ luôn bị xã hội lên án
Internet là một công cụ truyền thông đầy sức mạnh, vì vậy cần tới kiểm duyệt để điều chỉnh mọi hoạt động vi phạm nếu có. Nó cũng giống như truyền hình cần được kiêm duyệt mạnh mẽ hơn sách, báo. Internet có thể tích hợp nhiều chức năng của truyền hình, báo chí, truyền thanh… vì vậy cần thiết lập những chế độ kiểm duyệt phù hợp như đối với từng loại hình phương tiện thông tin truyền thống.	Việc kiểm duyệt đối với Internet sẽ không còn thích hợp như kiểm duyệt đối với báo chí và truyền hình, vì Internet sẽ trở thành một phương tiện thông tin đại chúng, tích hợp nhiều loại hình giải trí khác nhau. Xã hội rồi sẽ phụ thuộc rất lớn vào Internet vì vậy cần phải được sự bảo hộ tương tự. Khi những người sáng lập ra Hiến pháp Mỹ tuyên bố về tự do báo chí, họ đã quan tâm tới báo in, vì đó là phần cơ bản và có quyền lực nhất của truyền thông lúc bấy giờ. Ngày nay, họ chắc sẽ phải quan tâm đến việc ngăn chặn việc kiểm duyệt đối truyền thông bằng phát thanh và Internet bởi chúng là phương tiện cơ bản để phân phối thông tin.
Mặc dù việc kiểm duyệt là rất khó khăn, tuy nhiên chính phủ cần tìm ra những biện pháp phù hợp, ví dụ như đê ngăn chặn việc mua bán những phim bạo lực hay khiêu dâm, vì vấn đề này ảnh hưởng sâu sắc tới nền tảng đạo đức xã hội. Một khó khăn khác cần tính tới khi tiến hành kiểm duyệt, đó là việc cung cấp thông tin nặc danh trên Internet. Điều này đã tiếp tay cho những kẻ truyền bá thông tin khiêu dâm hoặc bất hợp pháp khác. Một số quốc gia Châu Á đã đưa ra quy định đòi hỏi việc đăng ký trước khi đăng tải nội dung lên Internet. Với một hệ thống như vậy, nếu mọi người chấp nhận, thì nó là một giải pháp tương đối là đơn giản để tăng cường việc kiểm soát đối với những nội dung thực sự không có lợi.	Dù không tính tới việc hạn chế quyền tự do ngôn luận thì kiểm duyệt cũng sẽ khó thực hiện được. Các chính phủ có thể kiểm duyệt được thông tin được đăng tải trên phạm vi quốc gia mình nhưng không thể kiểm soát những tài liệu của nước ngoài. Sẽ rất khó để tìm ra giải pháp ngăn chặn việc truy cập thông tin độc hại trên trang Web của Mỹ từ nước Anh hay Thuỵ Điển. Cũng có thể là những công dân của những nước này lại đăng tải những tài liệu độc hại và gửi lên những trang web có tên miền ở nước ngoài, như vậy vấn đề trở nên càng phức tạp hơn. Mặt khác, tự do ngôn luận trong một số trường hợp cũng cần có sự nặc danh để bảo vệ tác giả.

Tại một số quốc gia đã hình thành các quy định pháp luật kiểm soát việc sản xuất các tài liệu độc hại. Các quy định pháp luật này đưa ra chế tài đối với tác giả các tài liệu trên. Những nhà cung cấp dịch vụ Internet có thể phải chịu trách nhiệm pháp lý nếu họ trợ giúp việc cung cấp những thông tin độc hại như hướng dẫn chế tạo bom, khiêu dâm, và những thông tin tương tự như vậy.	Những nhà cung cấp dịch vụ chắc chắn không thể quyết định sáng suốt được cái gì có thể và cái gì không thể đưa lên Internet. Vì lợi nhuận, họ có thể đưa lên Internet bất kỳ loại thông tin nào.
Các vấn đề về bảo vệ trẻ em; chống khủng bố, tội phạm, phân biệt chủng tộc… mang tính quốc tế. Vì vậy, cần thông qua hợp tác quốc tế và những công ước quốc tế để điều chỉnh. Cần phải hợp pháp hoá việc kiểm duyệt những nơi tạo ra sự nguy hại cho người khác thông qua những bài phát biểu hay tác phẩm nghệ thuật… Những thông tin dạng trên rõ ràng có thể gây sự nguy hại đối với các nhóm người khác nhau trong xã hội. Các biện pháp này có thể giúp loại bỏ nhiều thông tin độc hại.	Không nên áp dụng việc kiểm duyệt độc đoán và hà khắc, cần thiết đưa ra các quy định nhằm nâng cao nhận thức của những người kinh doanh về trách nhiệm của họ đối với người sử dụng Internet. Các bậc phụ huynh có thể sử dụng những phần mềm kiểm soát thông tin đối với trẻ.

Nguồn: Matt Butt,"Tổng hợp: Chính phủ có nên kiểm duyệt những nội dung trên mạng Internet" (ngày 3/11/2000);

Nhà cung cấp dịch vụ có thể soạn một hợp đồng với người sử dụng trong đó có những điều khoản quy định về việc cung cấp nội dung thông tin. Điều này phù hợp với những quy định pháp luật và tránh cho họ khỏi trách nhiệm pháp lý. Lợi ích lớn cho những người kinh doanh khi thực hiện điều này là việc tạo được lòng tin với khách hàng và giúp kinh doanh hiệu quả.

Để có thể hoạt động hiệu quả, cơ chế kiểm duyệt phải là sản phẩm được đảm bảo bởi những cơ quan tự điều tiết. Những cơ quan này phải có tính đại diện rộng và khả năng tiếp cận tới những cơ quan liên quan. Tuỳ thuộc vào sự cho phép của cấp có thẩm quyền, những cơ quan này có đặc quyền thúc đẩy hoạt động của họ. Để tự điều chỉnh có hiệu quả thì những cơ quan như vậy phải tư vấn khách hàng hoặc người dân. Nếu không có sự tham gia của người sử dụng, thì cơ chế tự điều tiết sẽ không phản ánh chính nhu cầu của người sử dụng, và sẽ không hiệu quả trong việc đưa ra những tiêu chuẩn để thúc đẩy, từ đó dẫn tới thất bại trong việc tạo lập lòng tin.

Chính phủ có vai trò gì đối với việc tự kiểm duyệt ?

Các cấp có thẩm quyền cần có chính sách hỗ trợ cho việc tự kiểm duyệt. Các chính sách hỗ trợ này có thể dưới những hình thức đơn giản và không can thiệp vào quá trình tự kiểm duyệt.

Mặc dù việc tự kiểm duyệt có những ý nghĩa nhất định. Tuy nhiên, bản thân hình thức này không thể đảm bảo rằng những người truyền bá thông tin độc hại có tehẻ bị bắt và trừng phạt. Tuy nhiên cơ chế tự kiểm duyệt có thể giúp đảm bảo rằng những kẻ phạm tội không sử dụng Internet để gây ra thiệt hại. Chính phủ thông qua

giáo dục và những thông tin công cộng để nâng cao nhận thức cho người sử dụng về cơ chế tự kiểm duyệt, ví dụ như cung cấp công cụ giúp sàng lọc và ngăn chặn những nội dung không phù hợp hay gửi những thắc mắc về nội dung Internet qua đường dây nóng.

Chính phủ cần tập trung vào hiệu quả kiểm duyệt thông qua việc cho phép nhà kinh doanh đảm nhận số lượng công việc mà họ có thể đảm nhận. Cuối cùng, nhà kinh doanh có được lợi ích to lớn khi tạo ra lòng tin đối với người sử dụng cũng như nhà cung cấp dịch vụ.

Vậy sự phân định ranh giới giữa việc tự hình thành các quy định trong kinh doanh và viêc chính phủ đặt ra các quy định là ở đâu? Rõ ràng, chính phủ phải đảm bảo rằng luật pháp được tôn trọng trong không gian máy tính (cyberspace), ví dụ như với mục đích bảo vệ sở hữu trí tuệ và ngăn chặn tội phạm. Về phía những người kinh doanh, họ phải chấp nhận vai trò chính yếu của chính phủ trong việc thiết lập chính sách Internet. Nói chung, các nhà nhà kinh doanh có quyền đề nghị chính phủ cởi bỏ những quy định kiềm chế đối với những khu vực mà không có chứng cứ rõ ràng rằng việc kinh doanh sẽ có tác động tiêu cực đến xã hội hay những quyền cơ bản của con người.

Vấn đề trao quyền cho người sử dụng cuối cùng thì thế nào ?

Công nghệ sàng lọc nội dung có thể tạo cho người sử dụng khả năng chọn lựa những nội dung mà họ và con cái họ có thể truy cập. Với chức năng sử dụng thông minh, công nghệ này có thể giúp chuyển việc kiểm soát hay trách nhiệm về những nội dung độc hại từ phía chính phủ, các cơ quan kiểm duyệt và những người có chức năng giám sát sang các tổ chức, cá nhân. Vì vậy, cần khuyên khích việc hình thành các công cụ sàng lọc nội dung Internet hiệu quả, ví dụ như hệ thống cho phép theo dõi, cập nhật và phân loại các thông tin trong một khoảng thời gian nào đó là rất cần thiết.

Một hệ thống sàng lọc thông tin hiệu quả giúp nhận biết được nhiều giá trị quan trọng: người sử dụng cuối cùng tự quản lý; tôn trọng tự do bày tỏ, đa dạng trong tư tưởng, sự minh bạch; tôn trọng sự riêng tư, thao tác và sự tương thích. Hơn nữa, hệ thống này phải làm nổi bật tính thân thiện khi giao tiếp với người sử dụng, từ đó khuyến khích việc sử dụng những đặc điểm này và đưa ra sự lựa chọn về khả năng của người sử dụng cuối cùng. Những tổ chức thuộc nhóm ba nên được khuyến khích để phát triển và cung cấp công cụ sàng lọc thông tin miễn phí. Những nhà kinh doanh nên thúc đẩy việc sử dụng các hệ thống sàng lọc nội dung thông tin; hướng dẫn cho khách hàng về cách thức để sàng lọc; và tạo ra sự dễ dàng cho các bậc phụ huynh, giáo viên, và những người khách quan tâm đến những người trưởng thành để chọn lựa, lắp đặt và làm tương thích bộ lọc phù hợp với thiết bị của họ. Những yêu cầu điều tiết đối với những người cung cấp dịch vụ để bảo vệ hay sàng lọc nội dung thì nên tránh. Chính phủ hay những cơ quan kiểm duyệt có thể cung cấp bộ lọc nhưng không nên kiểm soát việc sử dụng của họ.

Tương tự như vậy, cần có những thiết bị truyền thông kỹ thuật và có tổ chức để đảm bảo rằng người sử dụng có thể phản hồi lại đối với những nội dung trên Internet mà họ nhận thấy cần phải chú ý đến. Những "*đường dây nóng*" này đảm bảo rằng, trong trường hợp cần thiết và phù hợp, hành vi hiệu quả có thể được triển khai để xua tan những mối bận tâm. Công việc đánh giá tính hợp pháp hay bất hợp pháp của một dữ liệu cụ thể là rất khó khăn đối với những nhà cung cấp dịch vụ, vì vậy cần kết hợp với công việc của đường dây nóng. Để có được chức năng này, các đường dây nóng cần có một môi trường và luật điều chỉnh để tạo điều kiện cho cho việc kiểm soát những nội dung có vấn đề hoặc bất hợp pháp. Cần thiết hình thành các quy định pháp lý đối với việc cài đặt phần mềm một cách có tổ chức và những thủ tục của đường dây nóng và bảo vệ những đường dây này khỏi tội phạm hay trách nhiệm pháp lý dân sự trong quản lý kinh doanh của những đường dây này ("bến cảng an toàn").

Những vấn đề gì cần được cân nhắc khi lựa chọn một cơ chế kiểm duyệt cụ thể ?

Dù thế nào đi chăng nữa, khi đưa ra những quy định kiểm duyệt nội dung thông tin thì cần tính rằng những quy định này sẽ không kìm hãm sự phát triển của công nghệ. Hệ thống các quy định này cần dựa trên cơ chế quản lý của chính phủ và cơ chế tự quản lý của những tổ chức, cá nhân kinh doanh, đây có thể là giải pháp đúng đắn đối với việc kiểm duyệt nội dung trong thời đại thông tin.

Bởi Internet có tính toàn cầu, nên cần có một mạng lưới quốc tế về đường dây nóng được quy định bởi một hiệp định khung, hiệp định này bao gồm những tiêu chuẩn cơ bản nhất đối với việc chuyển giao những nội dung cần quan tâm và quy định về trao đổi thông tin giữa các đường dây nóng. Cơ chế giúp phát hiện nhanh chóng các thông tin độc hại của các nhà cung cấp dịch vụ ở các khu vực khác nhau. Cơ chế này cũng giúp loại bỏ các thủ tục ngoại giao phức tạp về hợp tác quốc tế.

Cuối cùng, cần có chiến lược giáo dục và đào tạo, giúp nâng cao nhận thức về tầm quan trọng của kiểm duyệt. Công nghiệp Internet nên có đường dây trực tuyến và chương trình ngoại tuyến để nâng cao nhận thức về cơ chế tự kiểm duyệt, ví dụ như những hệ thống sàng lọc thông tin và đường dây nóng. Trường học cũng nên cung cấp những kỹ năng cần thiết cho trẻ để hiểu được lợi ích và những giới hạn của những thông tin trực tuyến sao cho có thể tự kiểm soát bản thân đối với nội dung Internet có vấn đề. Internet là một môi trường tương tác cho phép có sự truyền gửi và phản hồi thông tin, các thực tiễn trên Internet không ngừng thay đổi, vì vậy hệ thống pháp luật và cơ chế kiểm duyệt cũng phải thay đổi theo nhằm kiểm soát có hiệu quả môi trường trên Internet. [35]

THAM KHẢO

Pháp luật không gian điều khiển và thương mại điện tử. Baumer, David và J. Carl Poindexter. McGraw-Hill/Irwin. 2001.
Web: thiết kế sơ khai và số phận sau cùng của mạng truy cập toàn cầu cho nhà đầu tư. Berners-Lee, Tim. Harper San Francisco. 1999.
Pháp luật về truyền thông trong thời đại Internet. Xuất bản lần 1. Morgan Kaufmann. Black, Sharon K. 2001.
Chứng cứ số hoá và tội phạm máy tính. Academic Press. Casey, Eoghan. 2000.
Luật không gian điều khiển: văn bản và án lệ. Xuất bản lần 1. South-Western. College Pub. Ferrera, Gerald R. et al. 2000.
Luật không gian điều khiển: quan điểm quốc gia và quốc tế. Girasa, Rosario.
Pháp luật và chính sách về Internet. Xuất bản lần 1. Hiller, Janine and Ronnie Cohen. Prentice Hall. 2002.
Tìm sự bảo hộ bằng sáng chế không khó: làm sao để tìm được bằng sáng trên trên mạng và trong thư viện. Xuất bản lần thứ 2. Hitcock, David. Nolo Press.
Hướng dẫn Gigalaw đối với pháp luật về Internet. Random House. Isenberg, Doug. 2002.
Bộ luật và những quy định khác về không gian điều khiển. Lessig, Lawrence. 1999. New York: Basic Books.
Tương lại của ý tưởng: số phận chung trong một thế giới được kết nối. New York: Random House.
Bản quyền số hoá. Litman, Jessica. 2001. Amherst, NY: Prometheus Books.
Nguồn mở: giấy tờ không được uỷ quyền. Rosenberg, Donald K. (2000). John Wiley & Sons.
Phần mềm miễn phí, xã hội miễn phí: những bài viết chọn lựa của Richard Stallman. Stallman, Richard, Lawrence, Lessig and Joshua Gay. (2002).
Bản quyền tác giả và việc vi phạm bản quyền tác giả: sự xuất hiện của sở hữu trí tuệ và cách thức đe doạ sự sáng tạo. Vaidhyanathan, Siva. 2001. New York University Press.

GHI CHÚ

[1] Doug Isenberg, Hướng dẫn Gigalaw đối với luật về Internet (Random House, 1985).
[2] EDIAS Software Intern. V. BAGIS Intern., Ltd., 947 F. Supp. 412 (D. Ariz. 1996)
[3] DVD Copy Control Association, Inc. v. Andrew Thomas McLaughlin et al., Case No. CV 786804 (Superior Court of the State of California, County of Santa Clara).
[4] Richard, Taylor, Diễn đàn APEC và Chính sách về Thương mại điện tử: ảnh hưởng của Hoa Kỳ đối với thương mại điện tử thế giới; có sẵn trên trang web http://ww.ist.psu.edu/iip/Publication/
Taylor/ITS98rt3.pdf
[5] Cách tiếp cận với pháp luật xác thực điện tử; có sẵn trên trang web
http://rechten.uvt.nl/simone/Ds-art4.htm#_Toc468692769
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Ibid.
[10] Paul Scholtz, "Kinh tế học về thông tin cá nhân" First Monday 5, 9 (September 2000), [báo điều tử] http://www.firstmonday.dk/issues/issue5_9/sholtz/#s4
[11] Ibid.
[12] Ibid.
[13] "Bí mật thương mại"; có sẵn trên trang web http://www.cerebalaw.com/tradesec.htm
[14] James Hollander, "Amazon.com và Wal-Mart giải quyết vụ án về thương mại điện tử nổi tiếng" E-Commerce Times (5/4/1999), [báo điện tử]
http://www.ecommercetimes.com/news/articles/990405-1.shtml
[15] "Bằng sáng chế kinh doanh trên Internet," có sẵn trên trang web của http://www.nolo.com/lawcenter/ency/article.cfm/objectID/C2DBFF26-7097-4B7B-AE36DA00499851EE
[16] State Street Bank & Trust Co. v. Signal Financial Group, Inc. 149 F.3d 1368 (Fed. Cir.1998) cert denied 119 S. Ct. 851 (1999); có sẵn trên http://www.kuesterlaw.com/saris.htm
[17] Jennifer Hampton, "*Hollywood mong muốn chiến thắng trong in vụ vi vi phạm bản quyền đĩa DVD*", E-Commerce Times (18/8/2000), có sẵn trên trang web
http://www.ecommercetimes.com/news/articles2000/000818-6.shtml
[18] "Những nhà viết nhạc, nhà xuất bản âm nhac và công nghiệp ghi âm đã đưa Audiogalaxy.com ra toà vì xâm phạm quyền tác giả", Recording Industry Association of America Press Releases (24/5/2002); có trên trang web http://www.riaa.com/PR_story.cfm?id=520
[19] Susan Rush, "Audiogalaxy và Công nghiệp âm nhạc: vụ việc không được giải quyết," Broadbandweek.com (18/6/2002); có trên trang web
http://www.broadbandweek.com/news/020617/020618_content_Agalaxy.htm
[20] http://www.dsl.org/copyleft/
[21] http://www.gnu.org/philosophy/free-sw.html
[22] http://www.evolt.org/article/GNU_GPL/17/137/
[23] Những nguyên tắc cho việc cung cấp và sử dụng thông tin cá nhân; http://iitf.doc.gov/
ipc/ipc/ipc-pubs/niiprivprin_final.html
24 Irving J. Sloan, Law of Privacy in a Technological Society (Oceana Publications, 1986).
[25] Margaret N. Uy, "Bí mật riêng tư, chúng ta đã chuẩn bị cho điều đó ? (Phần 1)", e-Legal 1:2.
[26] "Hội đồng đã thông qua Chỉ thị về bảo vệ dữ liệu cá nhân", European Commission Press Release: IP/95/822 (July 25, 1995);
http://www.privacy.org/pi/intl_orgs/ec/dp_EC_press_release.txt
[27] OECD, Hướng dẫn cho bảo vệ ngươi tiêu dùng trong bối cảnh TMĐT (2000); có trên http://www1.oecd.org/publications/e-book/9300023E.PDF
[28] Janet Reno, 5/4/2000
[29] Giới hạn điện tử, "Phân tích EFF về những quy định về Luật ái quốc của Mỹ liên quan tới hoạt động trực tuyến" (31/11/2001); có trên trang web
http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html
[30] "Tội phạm trên mạng," Cyberlaw India FAQs;
http://www.cyberlawindia.com/cyberindia/cybfaq.htm#cybercrime
[31]US v. Brown, 925 F.2nd 1301, 1308, 10th Circ. 1991
[32] http://eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_analysis.html
[33] Jonathan Wallace, "Bảo vệ trao đổi thông tin trên thế giới: quyết định CDA là một thắng lợi ngọt ngào - Phần I;" http://www.spectacle.org/cda/decision.html

[34] "Toà án liên bang phản đối việc kiểm duyệt trong thư viện," Press Release (31/5/2002); có trên trang web http://www.aclu.org/news/2002/n053102a.html
[35] Center for Democracy & Technology, "Nguyên tắc CDT;" http://www.cdt.org/mission/principles.shtml

Về tác giả

Rodolfo Noel S. Quimbo là luật sư làm việc trong Phòng làm việc của Nghị sĩ Juan M. Flavier.
Ông tốt nghiệp tại trường đại học Philipin chuyên khoa Luật và Tiếng Anh.
Ông đã viết một số bài báo và giảng bào về pháp luật TMĐT tại Philippin và trong khu vực ASEAN

Lời cám ơn

Tôi muốn cảm ơn những người sau
Kimi, vì tình yêu, lòng kiên nhẫn và tình bạn
Senator Juan M. Flavier, sếp của tôi vì sự động vin và thời gian để viết
Romy and Lydia Quimbo, vì sự động viên tôi quay lại trường học
Emmanuel Lallana and Jaime Faustino, vì giới thiệu tôi tới nghiên cứu chính sách thương mại điện tử
Ramon J. Navarra Jr. and Renato N. Bantug Jr., những người cùng nghiên cứu và là người bạn thân thiết nhất
Greta, luôn vẫy đuôi khi tôi về nhà
Pavan Duggal, Advocate, Toà án tối cao Ấn độ cho việc xem xét bản dự thảo và
Borro, Bheng, Rommel, Pids, Angie, Percy, Celia, Jean, Winnie, Rene, Didith, Philip, Cynthia, Bong, Perry, and Bats, and Katch, Shelah, Patricia, đồng nghiệp và bạn bè