TS. PHẠM VĂN LỢI
(Chủ biên)

TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN

(Sách chuyên khảo)

TP
NHÀ XUẤT BẢN TƯ PHÁP

TỘI PHẠM
TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN

MÃ SỐ: TPA - 07 - 08

137-2007/CXB/40-07/NXBTP

TS. PHẠM VĂN LỢI
(Chủ biên)

TỘI PHẠM
TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN

(Sách chuyên khảo)

NHÀ XUẤT BẢN TƯ PHÁP
HÀ NỘI - 2007

TẬP THỂ TÁC GIẢ

1. TS. Phạm Văn Lợi - Phó Viện trưởng Viện Khoa học pháp lý - Bộ Tư pháp (Chủ biên)

2. TS. Mai Anh - Giám đốc Trung tâm Thông tin - Bộ Khoa học và Công nghệ

3. TS. Nguyễn Minh Đức - Cục trưởng Cục Thống kê - Viện Kiểm sát nhân dân tối cao

4. TS. Trần Văn Hoà - Cục Cảnh sát kinh tế - Bộ Công an

5. TS. Trần Mạnh Đạt - Trưởng Ban Nghiên cứu tư pháp hình sự - Viện Khoa học pháp lý - Bộ Tư pháp

6. ThS. Nguyễn Văn Cương - Viện Khoa học pháp lý - Bộ Tư pháp

7. ThS. Trần Văn Đạt - Vụ Pháp luật hình sự, hành chính - Bộ Tư pháp

8. ThS. Nguyễn Văn Hiển - Viện Khoa học pháp lý - Bộ Tư pháp

9. ThS. Lê Tuấn Sơn - Cục Thi hành án dân sự - Bộ Tư pháp

10. ThS. Trịnh Tiến Việt - Khoa Luật - Đại học Quốc gia Hà Nội

11. CN. Phạm Văn Thiệu - Toà án nhân dân tối cao

12. CN. Võ Văn Tuyển - Vụ Pháp luật quốc tế - Bộ Tư pháp

13. CN. Nguyễn Mạnh Cường - Viện Khoa học pháp lý - Bộ Tư pháp

14. CN. Nguyễn Minh Khuê - Viện Khoa học pháp lý - Bộ Tư pháp

15. CN. Lê Thị Hồng Thương - Vụ Pháp chế - Bộ Công an

LỜI GIỚI THIỆU

Ngày nay, chúng ta đang chứng kiến và thụ hưởng những thành tựu to lớn của cuộc cách mạng khoa học kỹ thuật mới - cuộc cách mạng công nghệ thông tin. Mặc dù cuộc cách mạng này mới chỉ khởi đầu từ những năm cuối của thế kỷ XX, bắt nguồn bằng việc phát minh ra máy tính điện tử (Computer) và thực sự bùng phát khi mạng thông tin toàn cầu (Internet) được sử dụng rộng rãi, song đã được nhiều nhà khoa học dự báo là sẽ đưa xã hội loài người tiến vào một kỷ nguyên mới, một thời kỳ mới - nền kinh tế tri thức, một nền kinh tế được tiên đoán là sẽ phát triển mạnh mẽ gấp nhiều lần so với cuộc cách mạng công nghiệp trước đây. Thực tiễn đời sống xã hội trên thế giới và ngay cả ở Việt Nam chúng ta những năm vừa qua đã kiểm chứng cho dự báo này. Máy tính và công nghệ kỹ thuật số đi kèm đã và đang thay thế các công nghệ trước đây trên tất cả mọi lĩnh vực đời sống xã hội. Máy tính đã nhanh chóng hiện diện và được sử dụng rộng rãi trong hầu hết các lĩnh vực của đời sống xã

hội, với những mục đích sử dụng cũng hết sức đa dạng, từ sản xuất, kinh doanh, ứng dụng khoa học kỹ thuật cho đến mục đích giải trí đơn thuần.

Mới chỉ hình thành và phát triển vài thập kỷ, nhưng cuộc cách mạng mới này đã khiến cho nhiều ngành kinh tế, xã hội và văn hoá hoàn toàn phụ thuộc vào các công nghệ mới của nó, đặc biệt phải kể đến vai trò của máy tính điện tử và Internet. Công nghệ thông tin cũng hình thành một thế hệ mới, khác so với thế hệ cách đây chỉ vài thập kỷ ở chỗ phụ thuộc vào công nghệ thông tin, coi máy tính, Internet, E-mail, điện thoại di động, máy ảnh số, máy nghe nhạc số... là những công cụ không thể thiếu trong cuộc sống. Cuộc cách mạng cũng phát triển những khái niệm, thuật ngữ mới mà cách đây vài thập kỷ chưa được nhắc đến nhưng nay đã trở nên quen thuộc trong đời sống xã hội như: thư tín điện tử (E-mail), mạng thông tin toàn cầu (Internet), thông tin di động (Mobile Phone), thương mại điện tử (E-Commercial), công nghệ số (Digital Technology) công nghệ không dây (Wifi, Bluetooth), trò chuyện trên mạng (Chatting), trò chơi trên mạng (Game Online)...

Cũng như bất kỳ một thành tựu khoa học nào của

nhân loại, khi mà các thành tựu càng được ứng dụng rộng rãi trong đời sống xã hội thì càng dễ bị lợi dụng, sử dụng hoặc là mục tiêu của tội phạm. Các thành tựu do công nghệ thông tin đem lại cũng không nằm ngoài quy luật đó. Vì vậy, trong thế giới mà công nghệ thông tin đã tạo ra cho con người đã hình thành một khái niệm mới về tội phạm - tội phạm trong lĩnh vực công nghệ thông tin hay còn được biết đến với các tên khác nhau như: tội phạm mạng (Cyber Crimes), tội phạm máy tính hay tội phạm liên quan đến máy tính (Computer Crimes). Đây là những khái niệm mới không chỉ đối với Việt Nam mà còn đối với nhiều nước trên thế giới. Do vậy, ngay từ việc sử dụng thuật ngữ, việc đưa ra khái niệm, đặc điểm đến việc quy định những hành vi nguy hiểm cho xã hội nào cần phải tội phạm hoá cũng còn có nhiều ý kiến không đồng nhất. Chính vì vậy, thách thức mới hiện nay đối với các nhà xây dựng pháp luật cũng như các cơ quan thực thi pháp luật là việc đưa ra những quy định pháp luật phù hợp và các biện pháp khả thi để có thể phòng chống và đấu tranh một cách có hiệu quả loại tội phạm này trong giai đoạn hiện nay. Cuốn sách chuyên khảo "***Tội phạm trong lĩnh vực công nghệ***

***thông tin*"** tập trung phân tích khái niệm, những đặc điểm về tội phạm trong lĩnh vực công nghệ thông tin; thực trạng và giải pháp phòng chống loại tội phạm này ở nước ta và một số nước trên thế giới.

Xin trân trọng giới thiệu cùng bạn đọc!

Hà Nội, tháng 4 năm 2007

NHÀ XUẤT BẢN TƯ PHÁP

Chương I

KHÁI NIỆM, ĐẶC ĐIỂM CỦA TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN

I. KHÁI NIỆM, ĐẶC ĐIỂM CỦA TỘI PHẠM

Khái niệm tội phạm là một trong những vấn đề trọng tâm trong pháp luật hình sự của nhiều nước trên thế giới. Việc quan niệm cũng như điều chỉnh bằng pháp luật đối với những hành vi bị coi là tội phạm đều có tính lịch sử và phụ thuộc điều kiện chính trị, kinh tế, văn hoá, xã hội của mỗi quốc gia. Chính vì vậy, trên cơ sở xác định những hành vi bị coi là tội phạm, mỗi nước đều có những quy định pháp luật điều chỉnh tương ứng, phù hợp với điều kiện của mình.

Ở nước ta, việc xác định những hành vi bị coi là tội phạm được quy định trong Bộ luật Hình sự năm 1999. Điều 8 Bộ luật Hình sự năm 1999 quy định:

> *"1. Tội phạm là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự, do người có năng lực trách nhiệm hình sự thực*

hiện một cách cố ý hoặc vô ý, xâm phạm độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ Tổ quốc, xâm phạm chế độ chính trị, chế độ kinh tế, nền văn hoá, quốc phòng, an ninh, trật tự, an toàn xã hội, quyền, lợi ích hợp pháp của tổ chức, xâm phạm tính mạng, sức khoẻ, danh dự, nhân phẩm, tự do, tài sản, các quyền, lợi ích hợp pháp khác của công dân, xâm phạm những lĩnh vực khác của trật tự pháp luật xã hội chủ nghĩa.

2. Căn cứ vào tính chất và mức độ nguy hiểm cho xã hội của hành vi được quy định trong Bộ luật này, tội phạm được phân thành tội phạm ít nghiêm trọng, tội phạm nghiêm trọng, tội phạm rất nghiêm trọng và tội phạm đặc biệt nghiêm trọng.

3. Tội phạm ít nghiêm trọng là tội phạm gây nguy hại không lớn cho xã hội mà mức cao nhất của khung hình phạt đối với tội ấy là đến ba năm tù; tội phạm nghiêm trọng là tội phạm gây nguy hại lớn cho xã hội mà mức cao nhất của khung hình phạt đối với tội ấy là đến bảy năm tù; tội phạm rất nghiêm trọng là tội phạm gây nguy hại rất

lớn cho xã hội mà mức cao nhất của khung hình phạt đối với tội ấy là đến mười lăm năm tù; tội phạm đặc biệt nghiêm trọng là tội phạm gây nguy hại đặc biệt lớn cho xã hội mà mức cao nhất của khung hình phạt đối với tội ấy là trên mười lăm năm tù, tù chung thân hoặc tử hình.

4. Những hành vi tuy có dấu hiệu của tội phạm, nhưng tính chất nguy hiểm cho xã hội không đáng kể, thì không phải là tội phạm và được xử lý bằng các biện pháp khác".

Theo luật hình sự Việt Nam thì tội phạm phải là hành vi của con người - nguyên tắc hành vi trong luật hình sự Việt Nam. Những gì mới chỉ hình thành trong tư tưởng, chưa thể hiện ra bên ngoài bằng hành vi thì chưa thể là tội phạm. Chỉ qua hành vi của mình, con người mới có thể gây thiệt hại, gây ra sự nguy hiểm cho xã hội và những gì trong ý nghĩ, tư tưởng của con người cũng chỉ có thể được xác định qua chính những biểu hiện bên ngoài mà trước hết là qua các hành vi của họ. Với định nghĩa trên thì *hành vi bị coi là tội phạm được phân biệt với hành vi không phải là tội phạm qua các dấu hiệu sau:*

- Hành vi bị coi là tội phạm phải là hành vi nguy hiểm cho xã hội;

- Hành vi đó phải được quy định trong Bộ luật Hình sự;

- Hành vi đó phải do người có năng lực trách nhiệm hình sự thực hiện một cách cố ý hoặc vô ý.

Dấu hiệu "*nguy hiểm cho xã hội*" là dấu hiệu cơ bản, quan trọng nhất và quyết định những dấu hiệu khác của tội phạm. Nguy hiểm cho xã hội có nghĩa là gây ra hoặc đe doạ gây ra thiệt hại đáng kể cho các quan hệ xã hội được luật hình sự bảo vệ, đó là các quan hệ xã hội như: độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ Tổ quốc, chế độ chính trị, chế độ kinh tế, nền văn hoá, quốc phòng, an ninh, trật tự, an toàn xã hội, quyền, lợi ích hợp pháp của tổ chức, tính mạng, sức khoẻ, tự do, danh dự, nhân phẩm, sở hữu, các quyền và lợi ích hợp pháp khác của công dân...

Theo quy định thì hành vi nguy hiểm cho xã hội chỉ có thể bị coi là tội phạm nếu "*được quy định trong Bộ luật Hình sự*". Sự quy định này thể hiện nguyên tắc "*không ai bị kết án vì một hành vi mà lúc họ thực hiện luật pháp quốc gia hay quốc tế không coi là tội phạm*" được quy định tại khoản 2 Điều 11 Tuyên ngôn

toàn thế giới về nhân quyền của Liên hợp quốc. Việc khẳng định tội phạm phải được quy định trong Bộ luật Hình sự không những là cơ sở đảm bảo cho đường lối đấu tranh phòng, chống tội phạm được thống nhất, bảo đảm nguyên tắc pháp chế, bảo đảm quyền dân chủ của công dân không bị những hành vi xử lý tuỳ tiện, mà còn là động lực thúc đẩy cơ quan lập pháp kịp thời sửa đổi, bổ sung và hoàn thiện pháp luật hình sự phù hợp với tình hình chính trị, kinh tế, xã hội[1].

Hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự bị coi là tội phạm khi hành vi đó do người có năng lực trách nhiệm hình sự thực hiện một cách cố ý hoặc vô ý. Khẳng định này thể hiện "*nguyên tắc có lỗi*", bởi vì luật hình sự Việt Nam không thừa nhận việc quy tội khách quan, nghĩa là quy trách nhiệm cho con người chỉ căn cứ vào việc người đó đã thực hiện hành vi gây thiệt hại cho xã hội mà không căn cứ vào lỗi của họ. Chúng ta áp dụng hình phạt không phải để trừng trị hành vi mà để trừng trị người đã thực hiện tội phạm nhằm cải tạo, giáo dục họ. Mục

[1] Trường Đại học Luật Hà Nội: *Giáo trình Luật hình sự Việt Nam*, Nxb. Công an nhân dân, H.2005, tr. 48.

đích giáo dục, cải tạo chỉ có thể đạt được nếu hình phạt được áp dụng cho người có lỗi, đối với người không có lỗi, hình phạt không phát huy được tác dụng giáo dục, cải tạo[1]. Điều kiện để người thực hiện hành vi nguy hiểm cho xã hội có thể có lỗi (cố ý hoặc vô ý) khi thực hiện hành vi đó là họ phải là người có năng lực trách nhiệm hình sự, đó là năng lực nhận thức được ý nghĩa xã hội của hành vi và năng lực điều khiển hành vi theo đòi hỏi của xã hội. Người có năng lực trách nhiệm hình sự bị coi là có lỗi khi thực hiện hành vi đó là kết quả của sự tự lựa chọn và quyết định của chủ thể trong khi có đủ điều kiện quyết định thực hiện xử sự khác phù hợp với đòi hỏi của xã hội.

Cũng theo điều luật trên, tuy tội phạm có chung các dấu hiệu như đã trình bày, nhưng những hành vi phạm tội cụ thể có tính chất và mức độ nguy hiểm cho xã hội khác nhau. Vì vậy, theo khoản 2 Điều 8 Bộ luật Hình sự năm 1999, tội phạm được phân thành bốn loại khác nhau: tội phạm ít nghiêm trọng, tội phạm nghiêm trọng, tội phạm rất nghiêm trọng và tội phạm đặc biệt nghiêm trọng. Sự phân loại như vậy thể hiện

[1] Trường Đại học Luật Hà Nội: *Giáo trình Luật hình sự Việt Nam*, Nxb. Công an nhân dân, H.2005, tr. 47.

sự quy định về phân hoá trách nhiệm hình sự và là cơ sở thống nhất cho việc xây dựng các khung hình phạt cho các tội phạm cụ thể cũng như cho việc xây dựng trong luật hình sự và các ngành luật liên quan các quy định về sự phân hoá trong đường lối đấu tranh phòng, chống các loại tội phạm khác nhau.

Theo khoản 3 Điều 8 Bộ luật Hình sự năm 1999 thì các loại tội phạm được phân biệt với nhau bởi cả dấu hiệu về mặt nội dung chính trị, xã hội và cả dấu hiệu về mặt hậu quả pháp lý[1]. *Tội phạm nói chung* có *dấu hiệu về mặt nội dung chính trị, xã hội là tính nguy hiểm cho xã hội* và có *dấu hiệu về mặt hậu quả pháp lý là tính chịu hình phạt* thì các loại tội phạm cũng có những dấu hiệu đó nhưng với nội dung cụ thể khác nhau. Mức độ xác định tính nguy hiểm cho xã hội được xác định qua mức độ cao nhất của khung hình phạt. Ngoài ra, nhằm tránh việc xác định tội phạm một cách máy móc, khoản 4 Điều 8 Bộ luật Hình sự năm 1999 quy định: *những hành vi tuy có dấu hiệu của tội phạm, nhưng tính chất nguy hiểm*

[1] Uông Chu Lưu (Chủ biên): *Bình luận khoa học Bộ luật Hình sự Việt Nam năm 1999,* Nxb. Chính trị quốc gia, H. 2001, tr. 30-33.

cho xã hội không đáng kể, thì không phải là tội phạm và mức độ nguy hiểm đáng kể hay không đáng kể của hành vi tội phạm được xác định trên cơ sở tính chất của các quan hệ xã hội bị xâm hại; tính chất của hành vi khách quan, trong đó bao gồm cả tính chất của phương pháp, thủ đoạn, công cụ và phương tiện phạm tội; tính chất và mức độ thiệt hại gây ra hoặc đe doạ gây ra cho quan hệ xã hội bị xâm hại; tính chất mức độ lỗi; động cơ, mục đích của người phạm tội; nhân thân của người có hành vi phạm tội; hoàn cảnh kinh tế, chính trị, xã hội...[1]

Như vậy, khoản 1 Điều 8 Bộ luật Hình sự năm 1999 đã định nghĩa tội phạm một cách khoa học, thể hiện tập trung nhất quan điểm của Nhà nước ta về tội phạm. Định nghĩa này không những là cơ sở khoa học thống nhất cho việc xác định những tội phạm cụ thể trong Phần các tội phạm của Bộ luật Hình sự, mà còn là cơ sở cho việc nhận thức và áp dụng đúng đắn các điều luật quy định về từng tội phạm cụ thể[2].

---

[1] Trường Đại học Luật Hà Nội: *Giáo trình Luật hình sự Việt Nam*, Nxb. Công an nhân dân, H.2005, tr. 46.

[2] Trường Đại học Luật Hà Nội: *Giáo trình Luật hình sự Việt Nam*, Nxb. Công an nhân dân, H.2005, tr. 41.

II. KHÁI NIỆM VỀ TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN

Tội phạm trong lĩnh vực công nghệ thông tin (hay còn gọi là tội phạm mạng, tội phạm máy tính hay tội phạm liên quan đến máy tính...) có thể xác định là hành vi bị coi là tội phạm có liên quan đến lĩnh vực công nghệ thông tin. Việc điều chỉnh bằng pháp luật đối với tội phạm trong lĩnh vực công nghệ thông tin đã được quan tâm từ những năm 70 của thế kỷ trước. Năm 1977, Thượng nghị sĩ Ribikoff đã đệ trình Nghị viện Hoa Kỳ dự luật về tội phạm mạng - lúc bấy giờ mới chỉ gọi là tội phạm máy tính. Tuy nhiên, lúc đó dự luật này chưa được chấp nhận[1]. Năm 1983, khối OECD lập một nhóm chuyên gia nghiên cứu về tội phạm liên quan đến máy tính để đưa ra các đề xuất sửa đổi pháp luật hình sự của các quốc gia thành viên. Năm 1989, Hội đồng châu Âu cũng thông qua bản đề xuất danh mục các tội phạm được coi là tội phạm máy tính. Năm 1997, nhóm các nước công nghiệp phát triển G8 cũng thể hiện mối quan tâm của mình về vấn đề này bằng cách thông qua hệ nguyên tắc phòng,

[1] Stein Schjolberg - Chief Judge - Moss District Court, Norway http://www.mosstingrett.no/info/legal.html.

chống tội phạm máy tính. Năm 2001, Hội đồng châu Âu thông qua Công ước về tội phạm mạng. Hiện nay, nhiều quốc gia trên thế giới đã có văn bản quy phạm pháp luật quy định về tội phạm mạng. Đi tiên phong trong số đó có thể kể đến: Hoa Kỳ, Pháp, Đức, Anh, Bỉ, Canada, Nhật Bản...

Theo nghĩa chung nhất, theo những quy định pháp luật hình sự của một số nước về tội phạm mạng thì ***tội phạm mạng*** là hành vi vi phạm luật hình sự được thực hiện trên mạng máy tính (bao gồm mạng Internet). Điều này có nghĩa là, việc thực hiện tội phạm mạng luôn gắn với phương tiện là máy tính và gắn với những kiến thức, tri thức về máy tính. Máy tính có thể là phương tiện để thực hiện hành vi phạm tội nhưng cũng có thể là mục tiêu xâm hại của tội phạm. Tuy nhiên, cho đến nay, ở tầm quốc tế, chưa có định nghĩa chuẩn về tội phạm mạng. Cũng còn nhiều quan niệm khác nhau về việc liệu có nên coi tội phạm mạng là loại tội phạm hoàn toàn mới so với các tội phạm truyền thống hay không, và tương ứng với nó là một hệ thống các quy phạm pháp luật hình sự riêng để điều chỉnh.

Nhiều người cho rằng, tội phạm mạng, về bản

chất chỉ là hình thức biểu hiện mới của các tội phạm truyền thống. Chẳng hạn, các hành vi lấy mã số bí mật để truy cập vào tài khoản của người khác thực hiện hành vi mua bán chính là hành vi xâm phạm sở hữu thuộc các tội truyền thống như trộm cắp, lừa đảo, cưỡng đoạt tài sản. Các hành vi xâm phạm quyền sở hữu trí tuệ trên mạng Internet cũng có thể xử lý dựa trên các tội truyền thống liên quan đến quyền sở hữu trí tuệ[1]... Thông thường, đối với các tội phạm truyền thống này, trong yếu tố cấu thành tội phạm đều không coi phương tiện phạm tội là yếu tố bắt buộc của cấu thành tội phạm. Vì vậy, dù được thực hiện dựa vào máy tính, mạng Internet thì vẫn có thể áp dụng quy định về tội phạm truyền thống để xử lý. Chính vì thế, không nên chỉ vì liên quan đến máy tính, mạng máy tính - những phương tiện công nghệ mới - mà coi tội phạm mạng là loại tội phạm mới khác về chất so với các tội phạm truyền thống.

Ở một góc độ khác, nhiều người lại cho rằng, tội phạm mạng là loại tội phạm hoàn toàn mới, đòi hỏi có hệ thống quy phạm pháp luật hình sự riêng để điều

[1] Li, Xingan. Cybercrime: *An Introduction, Joensuu,* July 2005.

chỉnh. Tính mới của loại tội phạm này là ở chỗ: việc thực hiện các tội phạm này luôn gắn với các thiết bị công nghệ cao, đòi hỏi người thực hiện phải có kiến thức về máy tính. Việc điều tra, truy tố cũng phải do những người có kiến thức về máy tính thực hiện. Ngoài ra, người thực hiện tội phạm mạng thường không có mặt khi thiệt hại xảy ra. Mối quan hệ từ trước giữa người phạm tội và người bị xâm hại cũng thường không tồn tại[1]. Người bị thiệt hại thường không muốn tiết lộ với các cơ quan có thẩm quyền về việc mình bị xâm hại nhằm giảm tác động tiêu cực tới uy tín, an ninh mạng của mình. Ngoài ra, việc xử lý tội phạm mạng cũng đặt ra vấn đề xác định thẩm quyền tài phán của các cơ quan có thẩm quyền, đặt ra yêu cầu hợp tác quốc tế cao trong phòng, chống tội phạm vì loại tội này thường được thực hiện xuyên quốc gia.

Dưới góc độ luật thực định, nhiều quốc gia đã quy định những tội phạm mới nhằm xử lý bằng các biện pháp hình sự đối với một số hành vi xâm phạm quyền và lợi ích của người khác trên mạng Internet tương

[1] F. Lawrence Street & Mark P. Grant: *The Law of Internet* - 2004 (Lexis.com).

đối điển hình. Trong đó phải kể đến tội truy cập trái pháp luật vào dữ liệu máy tính của người khác; tội gây rối hoạt động của hệ thống máy tính của người khác; tội tạo và lan truyền vi rút máy tính... Ngoài ra, các hành vi lừa đảo qua mạng Internet; trộm cắp mật mã truy cập vào tài khoản tín dụng để chiếm đoạt tài sản của người khác; xâm phạm sở hữu trí tuệ trên mạng (nhất là xâm phạm bản quyền); xâm phạm bí mật riêng tư; phát tán, lan truyền văn hoá phẩm đồi truỵ... thì được xử lý theo các tội đã quy định trước đây trong pháp luật hình sự.

Từ những phân tích nêu trên về những dấu hiệu của tội phạm trong pháp luật hình sự và quan niệm về tội phạm mạng ở một số nước trên thế giới, có thể thấy: trước hết, *xét về bản chất thì tội phạm trong lĩnh vực công nghệ thông tin (tội phạm mạng) cũng có đầy đủ các tính chất, đặc điểm như mọi tội phạm truyền thống khác,* nghĩa là cũng được coi là những hành vi nguy hiểm cho xã hội, gồm 4 yếu tố cấu thành cơ bản của một tội phạm (khách thể, mặt khách quan, chủ thể và mặt chủ quan của tội phạm). *Điểm khác biệt với những tội phạm khác* là, đối với tội phạm trong lĩnh vực công nghệ thông tin thì công nghệ thông tin, máy tính và mạng máy tính có vai trò, mức độ nhất

định trong việc thực hiện, che giấu và gây ra những hậu quả xấu đối với xã hội của hành vi phạm tội [1]. Đánh giá một cách tổng thể có thể thấy rằng, đối với loại tội phạm trong lĩnh vực công nghệ thông tin, thì công nghệ thông tin, máy tính và mạng máy tính trong quá trình phạm tội có thể được thể hiện dưới nhiều góc độ khác nhau: *có thể là khách thể của tội phạm, có thể là công cụ phạm tội, có thể có vai trò như là chủ thể của tội phạm.*

Dưới góc độ là ***khách thể của tội phạm,*** hiểu theo nghĩa đơn giản nhất, máy tính và các thiết bị có liên quan là một loại tài sản có giá trị. Do vậy, nó có thể trở thành đối tượng xâm hại của các tội xâm phạm sở hữu như trộm cắp tài sản hay phá hoại tài sản. Hiểu theo một giác độ phức tạp hơn, máy tính với vai trò như là khách thể của tội phạm còn được thể hiện trong việc tội phạm cố tình phá hoại hay trộm cắp chúng nhằm xoá bỏ hoặc lấy cắp các thông tin mà nó chứa đựng.

Dưới góc độ là ***công cụ phạm tội,*** máy tính và

[1] Nguyễn Mạnh Toàn: *Đặc điểm và các dạng hành vi cơ bản của tội phạm tin học,* Tạp chí Nhà nước và Pháp luật, số 3/2002.

mạng Internet ngày càng được các loại tội phạm khác nhau sử dụng vì những khả năng ưu việt của chúng. Việc sử dụng máy tính và các thiết bị liên quan làm công cụ phạm tội cũng được chia ra làm hai loại: *thứ nhất,* máy tính được sử dụng như là công cụ để thực hiện các ***tội phạm truyền thống,*** *ví dụ:* tội đánh bạc, tội lừa đảo chiếm đoạt tài sản; *thứ hai,* máy tính, các phần mềm máy tính và các bí mật được lưu giữ trong máy tính được sử dụng như là miếng mồi để dụ dỗ những người nhẹ dạ cả tin. *Ví dụ,* trong một vụ việc diễn ra ở bang Florida của Mỹ, một tên tội phạm đã lừa đảo trên 50 triệu đô la của các nhà đầu tư với việc đưa ra thông tin rằng anh ta đang nghiên cứu một phần mềm mà có khả năng sẽ thu lợi rất lớn.

Còn *dưới góc độ* ***chủ thể của tội phạm,*** mặc dù chúng ta đều biết rằng, theo lý luận chung chỉ các cá nhân mới được coi là chủ thể của tội phạm, tuy nhiên, nếu xét về bản chất của vấn đề, tức là xét dưới góc độ đối tượng đã thực hiện hành vi phạm tội thì máy tính và mạng máy tính trong một số trường hợp cũng có thể được coi đã đóng vai trò như là một chủ thể của tội phạm. Trong trường hợp này, chính môi trường của máy tính, các tính năng của máy tính đã thực hiện các hành vi cấu thành tội phạm. Ví dụ cụ thể trong

trường hợp này là hành vi phát tán virút tin học. Người làm ra và phát tán virút tin học đôi khi chỉ chủ định phát tán trên một hoặc một số máy tính nhất định. Tuy nhiên, với tính năng phát tán qua mạng thông qua thư điện tử, các máy tính này đã tự động phát tán các virút này sang nhiều máy tính khác và gây ra hậu quả là hàng triệu máy tính có thể bị nhiễm virút trong thời gian rất ngắn.

Mặc dù chúng ta tạm chia vai trò của công nghệ thông tin và máy tính đối với từng quá trình diễn biến của tội phạm như trên, nhưng trên thực tiễn việc nhận thức về vấn đề này rất khác nhau ở từng quốc gia, từng khu vực và phụ thuộc vào trình độ phát triển khoa học, công nghệ của mỗi quốc gia, khu vực đó. Tuỳ thuộc vào nhận thức, khái niệm về tội phạm trong lĩnh vực công nghệ thông tin có thể rất rộng và cũng có thể là rất hẹp.

Tiếp cận ở phạm vi rộng, thì việc định nghĩa thế nào là tội phạm trong lĩnh vực công nghệ thông tin cần dựa trên vai trò của máy tính trong việc thực hiện hành vi phạm tội. Theo quan điểm này thì ***tội phạm trong lĩnh vực công nghệ thông tin*** bao gồm những tội phạm có sự liên can, dính líu của máy tính

tới tội phạm với ba vai trò:

+ Máy tính là mục đích của tội phạm;

+ Máy tính là công cụ phạm tội;

+ Máy tính là vật trung gian để cất giấu, lưu trữ những thứ đã chiếm đoạt được.

Theo quan điểm này thì rất nhiều các loại tội phạm truyền thống cũng dễ bị coi là tội phạm trong lĩnh vực công nghệ thông tin hay tội phạm máy tính, đặc biệt là những tội sử dụng máy tính, mạng máy tính làm công cụ, phương tiện phạm tội. *Ví dụ:* tội đánh bạc trên mạng, tội cung cấp các dịch vụ mại dâm trực tuyến, tội truyền bá văn hoá phẩm đồi truỵ trên mạng[1]. Một trong những định nghĩa rộng nhất về tội phạm máy tính hay tội phạm trong lĩnh vực công nghệ thông tin được Bộ Tư pháp Hoa Kỳ đưa ra là: "*Tội phạm trong lĩnh vực công nghệ thông tin là bất cứ các hành vi vi phạm pháp luật hình sự nào có liên quan đến việc sử dụng các hiểu biết về công nghệ máy tính trong việc phạm tội, điều tra hoặc xét xử*"[2].

---

[1] Nguyễn Mạnh Toàn: *Sđd*, tr. 31.

[2] Mohamed Chawki: *A Citical Look at the Regulation of Cybercrime*, Đại học Lyon III - Pháp, tr. 7.

Theo định nghĩa này thì bất cứ tội phạm nào cũng có thể được xếp vào loại tội phạm tin học vì chỉ cần trong quá trình điều tra các điều tra viên sử dụng máy tính để tìm kiếm thông tin cũng được coi là hành vi phạm tội trong lĩnh vực này.

Tuy nhiên, với quan điểm hiểu tội phạm trong lĩnh vực công nghệ thông tin theo phạm vi rộng như trên cũng gặp phải một vấn đề khó khăn. Đó là làm thế nào để cụ thể hoá các hành vi phạm tội cụ thể và từ đó xác định tội danh cụ thể cho các hành vi này. Đây là công việc không dễ dàng vì khi định tội danh, xét về bản chất thì nhiều tội danh lại trùng với các tội danh truyền thống như tội lừa đảo, đánh bạc...; điểm khác có chăng ở đây là việc sử dụng công cụ là mạng máy tính.

Tiếp cận ở phạm vi hẹp, có nhà nghiên cứu cho rằng, tội phạm trong lĩnh vực công nghệ thông tin chỉ là tội phạm được thực hiện và gây hậu quả trên môi trường, trên thế giới ảo do thành tựu của khoa học công nghệ tin học đem lại và nó hoàn toàn khác với các loại tội phạm truyền thống trước kia. Bộ luật Hình sự năm 1999 đã tiếp cận theo quan điểm này. Tuy nhiên, Bộ luật Hình sự năm 1999 mới chỉ đề cập

và quy định về 03 tội danh có liên quan đến công nghệ thông tin, đó là: Tội tạo ra và lan truyền, phát tán các chương trình virút tin học (Điều 224); Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử (Điều 225); Tội sử dụng trái phép thông tin trên mạng và trong máy tính (Điều 226). Tuy nhiên, trên thế giới hiện nay đã xuất hiện thêm nhiều hành vi được coi là tội phạm trong lĩnh vực công nghệ thông tin khác và được hiểu và tiếp cận theo phạm vi hẹp, *ví dụ:* Tội vào cửa bằng mật khẩu trộm cắp; Tội sao chụp bất hợp pháp các chương trình phần mềm; Tội đe doạ tấn công hệ thống máy tính... Phương pháp tiếp cận theo phạm vi hẹp có *ưu điểm* là định rõ được tội danh cần xử lý nhưng lại có *nhược điểm* là rất dễ bỏ lọt tội phạm, nhất là trong bối cảnh công nghệ thông tin đang phát triển với tốc độ rất nhanh như hiện nay. Một ví dụ điển hình là trên thế giới hiện nay đang tranh cãi về việc có coi hành vi trộm cắp, lừa đảo các tài sản mà người chơi có được khi tham gia các trò chơi trực tuyến là tội phạm hay không? Nếu nhìn dưới góc độ thế nào là tài sản theo quy định của pháp luật hiện hành, thì các *"tài sản"* ảo này là hoàn toàn không có giá trị vì nó thực chất

không phải là tài sản, nó chỉ là những thứ được tạo ra trong thế giới ảo do một phần mềm máy tính (những người xây dựng lên trò chơi trực tuyến) nghĩ ra. Tuy nhiên, nếu xét dưới góc độ các tài sản này là do người chơi đã bỏ nhiều công sức để tạo lập được, cùng với tính chất có thể *"chiếm hữu, sử dụng và định đoạt"* (sự chiếm hữu, sử dụng và định đoạt ở đây về thực chất cũng chỉ mang tính tương đối) và đặc biệt là những tài sản này có thể quy đổi hay xác định được bằng giá trị thực (có thể bán cho những người chơi khác) thì chúng lại thực sự cần được coi là một tài sản thực và cần được pháp luật bảo vệ trước những hành vi lừa đảo chiếm đoạt tài sản, trộm cắp tài sản giống như đối với các tài sản hữu hình khác.

Mặt khác, nếu chỉ coi tội phạm trong lĩnh vực công nghệ thông tin giới hạn trong phạm vi thế giới ảo, môi trường điện tử do công nghệ thông tin đem lại thì đối với những tội phạm truyền thống sử dụng thành tựu công nghệ thông tin, việc thực hiện hành vi phạm tội, việc truy tìm dấu vết, chính sách ngăn ngừa, đấu tranh đối với hành vi này sẽ không có gì khác so với các phương pháp xử lý truyền thống, trong khi về bản chất thì các hành vi phạm tội này lại khác hẳn. *Ví dụ,*

kẻ phạm tội tống tiền trên mạng trong và sau khi thực hiện hoàn toàn có thể xoá sạch toàn bộ dấu vết tội phạm bằng kỹ thuật công nghệ tin học nên đã gây không ít khó khăn cho hoạt động thu thập dấu vết nếu các phương pháp thu thập, bảo quản chứng cứ không thay đổi phù hợp[1].

Như vậy, mỗi quan điểm về tội phạm trong lĩnh vực công nghệ thông tin đều có những khiếm khuyết nhất định, vì vậy, trên thế giới hiện nay vẫn chưa có được một khái niệm về tội phạm trong lĩnh vực công nghệ thông tin đầy đủ được mọi người cùng nhất trí. Trong khuôn khổ cuộc họp lần thứ 10 của Đại hội đồng Liên hợp quốc về ngăn chặn và xử lý tội phạm được tổ chức tại thành phố Viên (Áo) từ ngày 10/10/2000 đến ngày 17/10/2000, một cuộc hội thảo đã được tổ chức để bàn về vấn đề tội phạm trong lĩnh vực công nghệ thông tin và việc định nghĩa về tội phạm này được đưa ra thành hai quan điểm:

Thứ nhất, theo nghĩa hẹp, ***tội phạm trong lĩnh vực công nghệ thông tin*** *là các hành vi phạm tội sử dụng máy tính và mạng máy tính với mục đích xâm*

[1] Nguyễn Mạnh Toàn: *Sđd*, tr. 31.

phạm đến an toàn của hệ thống máy tính và quy trình lưu trữ dữ liệu của hệ thống đó. Loại tội phạm theo định nghĩa này có thể được hiểu là loại tội phạm mới có quan hệ trực tiếp đến máy tính, mạng máy tính, làm ảnh hưởng và gây thiệt hại cho người sử dụng.

Thứ hai, theo nghĩa rộng, ***tội phạm trong lĩnh vực công nghệ thông tin*** *là các hành vi phạm tội sử dụng máy tính hoặc các phương pháp khác có liên quan đến máy tính, mạng máy tính, bao gồm các loại tội phạm như chiếm giữ bất hợp pháp và đe doạ hoặc làm sai lệch thông tin bằng phương pháp sử dụng mạng máy tính.* Loại tội phạm theo định nghĩa này là rất rộng, bao gồm nhiều loại hành vi của tội phạm truyền thống được thực hiện với sự trợ giúp của công cụ máy tính mà phổ biến hiện nay như các hành vi lừa đảo, trốn lậu cước viễn thông, mạo danh...

Như vậy, định nghĩa về tội phạm trong lĩnh vực công nghệ thông tin như nêu trên tuy chưa phải là định nghĩa hoàn chỉnh, tuy còn chung chung và sơ sài nhưng ý nghĩa quan trọng của nó là lần đầu tiên khái niệm thế nào là tội phạm trong lĩnh vực công nghệ thông tin (tội phạm mạng, tội phạm máy tính hay tội phạm liên quan đến máy tính) đã được các nước trên

thế giới thảo luận và đi tới nhất trí. Theo định nghĩa trên thì tội phạm trong lĩnh vực công nghệ thông tin là những tội phạm liên quan đến máy tính và các mạng thông tin. Định nghĩa này đã thừa nhận tội phạm trong lĩnh vực công nghệ thông tin bao gồm cả các tội phạm mới hình thành trong môi trường của công nghệ thông tin và cả những tội phạm truyền thống nhưng được thực hiện với sự giúp đỡ của các công nghệ thông tin mới.

III. CÁC ĐẶC ĐIỂM CỦA TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN

1. Khách thể của tội phạm

Trên cơ sở khái niệm về tội phạm trong lĩnh vực công nghệ thông tin được nêu ở phần trên, chúng ta có thể chia khách thể của tội phạm này thành hai loại:

Thứ nhất, tội phạm trong lĩnh vực công nghệ thông tin *xâm phạm, làm ảnh hưởng đến hoạt động bình thường của hệ thống máy tính, mạng máy tính và thiết bị liên quan.* Sự xâm phạm ở đây được hiểu theo nghĩa rộng, nghĩa là từ việc làm hỏng hóc, chiếm đoạt, làm sai lệch thông tin của máy tính, mạng máy tính, các thiết bị liên quan cũng như các thông tin

trong hệ thống máy tính và mạng máy tính. Các khách thể này rất đa dạng, từ chiếc máy tính đơn nhất, các thiết bị của mạng máy tính... đến các chương trình máy tính, các thông tin chứa đựng trong hệ thống máy tính và hệ thống mạng. Đây là nhóm khách thể của 03 tội danh về tin học trong Bộ luật Hình sự năm 1999 của nước ta.

Thứ hai, tội phạm trong lĩnh vực công nghệ thông tin *sử dụng máy tính và mạng máy tính như là công cụ để xâm phạm đến lợi ích chính đáng của cá nhân, pháp nhân, tổ chức, ảnh hưởng đến trật tự công cộng.* Đây là khách thể rất rộng và liên quan đến các tội phạm truyền thống nhưng đã sử dụng các thành tựu của công nghệ thông tin để thực hiện hành vi phạm tội. Với sự trợ giúp của khoa học kỹ thuật mới, các tội phạm này có thể gây ra những thiệt hại vô cùng nghiêm trọng về nhiều mặt cho hoạt động bình thường của các cơ quan nhà nước, các tổ chức và đời sống xã hội không chỉ giới hạn trong phạm vi một quốc gia.

2. Mặt khách quan của tội phạm

Các hành vi của tội phạm trong lĩnh vực công nghệ thông tin rất đa dạng và phức tạp. Các hành vi

này cũng phát triển, thay đổi không ngừng cùng với sự phát triển của các công nghệ mới. Hiện nay, theo Bộ luật Hình sự năm 1999 của nước ta thì có ba nhóm hành vi chính, đó là:

Nhóm thứ nhất, hành vi tạo ra và lan truyền, phát tán các chương trình vi rút qua mạng máy tính hoặc bằng các phương thức khác. ***Tạo ra các chương trình vi rút*** là hành vi sản xuất ra các chương trình virút tin học. ***Lan truyền các chương trình vi rút*** là hành vi truyền đi các chương trình virút tin học thông qua hệ thống (mạng) máy tính trong nước hoặc quốc tế (Internet). ***Phát tán các chương trình vi rút*** là hành vi truyền các chương trình vi rút tin học không thông qua hệ thống mạng máy tính mà bằng các sản phẩm phần mềm máy tính (Điều 224).

Nhóm thứ hai, hành vi vận hành, khai thác và sử dụng mạng máy tính điện tử trái với các quy định của Nhà nước. ***Vận hành mạng máy tính điện tử*** là hành vi khởi động, truy cập vào hệ thống mạng máy tính điện tử. ***Khai thác mạng máy tính điện tử*** là hành vi tìm kiếm nhằm rút ra hoặc ghi lại các thông tin cần thiết cho nhu cầu của mình từ các dữ liệu trong mạng máy tính điện tử. ***Sử dụng mạng máy tính***

điện tử là hành vi phát huy tính năng, công dụng của mạng máy tính điện tử nhằm khai thác các thông tin có trong các dữ liệu của máy tính (Điều 225).

Nhóm thứ ba, hành vi sử dụng thông tin trên mạng và trong máy tính hoặc đưa vào mạng máy tính các thông tin trái với các quy định của Nhà nước. Sử dụng trái phép thông tin trong các dữ liệu của máy tính không được phép của cơ quan nhà nước hoặc người có thẩm quyền. ***Đưa trái phép vào mạng máy tính các thông tin*** là hành vi đưa các thông tin vào trong các dữ liệu của máy tính không được phép của các cơ quan nhà nước hoặc người có thẩm quyền (Điều 226)[1].

Các nước thuộc Liên Xô cũ cũng có những quy định liên quan đến hành vi của tội phạm trong lĩnh vực công nghệ thông tin tương tự, tuy đôi chỗ có rộng hơn. Bộ luật Hình sự Liên bang Nga dành một chương (Chương 28) quy định về các tội phạm thông tin máy tính (Computer information crimes) gồm ba nhóm

[1] Phùng Thế Ván, Trần Văn Luyện, Phạm Thanh Bình, Nguyễn Đức Mai: *Bình luận khoa học Bộ luật Hình sự 1999*, Nxb. Công an nhân dân, H. 2001, tr. 413-487.

hành vi: thâm nhập vào hệ thống thông tin máy tính trái phép; sản xuất, sử dụng và phát tán các phần mềm máy tính có hại; vi phạm các quy định về vận hành mạng và hệ thống máy tính. Bộ luật Hình sự Belarus quy định các tội phạm này trong Chương 31 *"Các tội phạm về an toàn thông tin"*, trong đó quy định các nhóm hành vi: thâm nhập vào hệ thống thông tin máy tính trái phép; sửa đổi các thông tin của hệ thống máy tính; phá hoại thông tin máy tính; phát triển, sử dụng và phát tán các chương trình máy tính gây hại; vi phạm các quy định về vận hành mạng và hệ thống máy tính.

Theo tác giả Mohamed Chawki, Trường Đại học Tổng hợp Lyon III (Pháp)[1], thì *các nhóm hành vi sau đây có thể coi là mặt khách quan của loại tội phạm trong lĩnh vực công nghệ thông tin:*

- Xâm nhập trái phép vào các hệ thống máy tính và thông tin (hacking);

- Tạo ra, lan truyền và phát tán các virút tin học có hại;

[1] Mohamed Chawki: *A Critical look at the regulation of Cybercrime, tr.14-21.*

- Lừa đảo trên mạng (Online Fraud), bao gồm các hành vi: lấy cắp thông tin về tài khoản; giả mạo thông qua các thông tin lấy cắp được từ hệ thống máy tính; thay đổi dữ liệu hoặc các chương trình; lừa đảo đấu giá trực tuyến; giả mạo thư điện tử;

- Quấy rối tình dục và lăng mạ người khác trên mạng;

- Khủng bố mạng thông tin;

- Đe doạ trên mạng.

Như vậy, theo quan điểm của Mohamed Chawki thì rất nhiều các hành vi phạm tội truyền thống (như hành vi lừa đảo, khủng bố, tống tiền, quấy rối tình dục...) cũng có thể được coi là hành vi phạm tội về công nghệ thông tin nếu các hành vi này được thực hiện thông qua hệ thống máy tính.

Thông thường, các hành vi phạm tội của nhóm tội phạm về công nghệ thông tin cần phải gây ra hậu quả thiệt hại nhất định thì mới bị truy cứu trách nhiệm hình sự. Điều 224 Bộ luật Hình sự năm 1999 quy định nếu chỉ tạo ra các chương trình vi rút nhưng không lan truyền hoặc phát tán chúng, không gây ra hậu quả thiệt hại thì không cấu thành tội phạm.

3. Chủ thể của tội phạm

Cũng giống như các tội phạm truyền thống khác, chủ thể của tội phạm trong lĩnh vực công nghệ thông tin là *những cá nhân đủ độ tuổi theo luật định và có năng lực trách nhiệm hình sự.* Theo Bộ luật Hình sự năm 1999 thì công dân Việt Nam, người nước ngoài, người không có quốc tịch từ đủ 16 tuổi trở lên có năng lực trách nhiệm hình sự là chủ thể của tội phạm khi thực hiện hành vi phạm tội. Đối với các tội phạm trong lĩnh vực công nghệ thông tin, các chủ thể này thường là những người có hiểu biết về công nghệ máy tính, công nghệ mạng và đã lợi dụng những hiểu biết này để thực hiện hành vi phạm tội. Tuy nhiên, cũng có trường hợp chủ thể là những người không hiểu biết đầy đủ về các quy định liên quan đến vận hành, khai thác và sử dụng mạng máy tính điện tử dẫn đến những thiệt hại (*ví dụ:* Điều 225 Bộ luật Hình sự năm 1999 quy định về tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử). Một vấn đề nữa đáng lưu ý hiện nay đối với chủ thể của nhóm tội phạm này là tình trạng ngày càng "*trẻ hoá*" của các ***hacker***[1].

[1] Danh từ riêng đã trở thành thông dụng để chỉ những kẻ chuyên xâm nhập trái phép vào hệ thống máy tính thông qua mạng Internet.

Với sự phát triển của công nghệ thông tin và các chương trình phần mềm, giới trẻ luôn là thế hệ nhận biết nhanh nhạy những công nghệ mới, cộng với tính cách còn bồng bột, thích thể hiện mình nên rất dễ dẫn đến việc rơi vào con đường phạm tội với những động cơ và mục đích hết sức đơn giản, ngây thơ, chẳng hạn tạo ra và phát tán virút tin học gây hại chỉ để đùa vui, hoặc thâm nhập các trang thông tin chỉ để thể hiện khả năng của mình.

4. Mặt chủ quan của tội phạm

Các tội phạm trong lĩnh vực công nghệ thông tin, thông thường được thực hiện do lỗi cố ý. Trong ba tội danh có liên quan đến tội phạm trong lĩnh vực công nghệ thông tin được quy định tại Bộ luật Hình sự năm 1999 có một tội danh được thực hiện do lỗi vô ý do cẩu thả hoặc vô ý vì quá tự tin. Đó là tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử (Điều 225). Tuy nhiên, trong trường hợp lỗi vô ý, thì thường là những hành vi gây ra hậu quả thiệt hại nghiêm trọng. Tội phạm hoàn thành từ thời điểm xảy ra các thiệt hại. Trong trường hợp tuy hành vi vi phạm chưa gây ra hậu quả nghiêm trọng nhưng trước đó đã bị xử phạt hành chính về hành vi này mà

còn vi phạm thì hành vi vẫn cấu thành tội phạm.

Các yếu tố về động cơ, mục đích phạm tội của nhóm các tội phạm trong lĩnh vực công nghệ thông tin thường không phải là dấu hiệu bắt buộc của loại tội phạm này mà yếu tố quan trọng nhất để xác định tội phạm là hành vi phạm tội và hậu quả thiệt hại. Sở dĩ như vậy vì chúng ta thấy động cơ, mục đích của nhóm tội về công nghệ thông tin rất đa dạng và đôi khi động cơ, mục đích rất đơn giản nhưng lại gây ra những hậu quả rất nghiêm trọng. Do đó, đối với nhóm tội phạm này, chúng ta không thể coi động cơ, mục đích là dấu hiệu bắt buộc mà chỉ nên coi chúng như là những tình tiết tăng nặng và giảm nhẹ có liên quan mà thôi.

IV. SỰ KHÁC BIỆT GIỮA TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN VỚI TỘI PHẠM THÔNG THƯỜNG

Qua phân tích những đặc điểm của tội phạm trong lĩnh vực công nghệ thông tin ở phần trên, chúng ta đã thấy được phần nào sự khác biệt giữa nhóm các tội phạm trong lĩnh vực công nghệ thông tin với các nhóm tội phạm thông thường khác. Tựu trung lại có thể thấy *bốn đặc điểm khác biệt cơ bản* của tội phạm trong lĩnh vực công nghệ thông tin so với tội phạm

thông thường như sau:

Thứ nhất, có vai trò của máy tính, mạng máy tính và các thiết bị công nghệ thông tin có liên quan. Như phần đầu bài viết đã phân tích, một điểm khác biệt cơ bản giữa các tội phạm trong lĩnh vực công nghệ thông tin và tội phạm thông thường chính là ở vai trò của máy tính, mạng máy tính cũng như các thiết bị công nghệ thông tin khác có liên quan đến quá trình thực hiện tội phạm. Tất cả các tội phạm trong lĩnh vực công nghệ thông tin đều có liên quan không ít thì nhiều đến máy tính, mạng máy tính và các thiết bị công nghệ thông tin có liên quan. Máy tính, mạng máy tính vừa có thể là đối tượng của tội phạm, vừa có thể là môi trường và công cụ đắc lực để thực hiện hành vi phạm tội.

Thứ hai, về đặc điểm chủ thể: người phạm các tội về công nghệ thông tin hầu hết là những người thông minh, những người có tri thức và am hiểu về công nghệ mới. Phần lớn những người phạm tội là những người có hiểu biết vững vàng về công nghệ kỹ thuật số, máy tính và có kỹ năng khai thác sử dụng chúng thành thạo. Vì vậy, họ luôn thành công trong việc thực hiện hành vi phạm tội và gây rất nhiều khó khăn

cho các cơ quan tiến hành tố tụng, thường thì họ là những người trẻ tuổi, chưa từng bị pháp luật trừng trị và không hề có tiền án.

Thứ ba, về hậu quả thiệt hại: hậu quả của tội phạm trong lĩnh vực công nghệ thông tin thường rất nghiêm trọng. Một khi các hoạt động quản lý xã hội được máy tính hoá, hệ thống mạng, hệ thống thông tin được phổ biến rộng khắp trên tất cả các lĩnh vực của đời sống xã hội, thì hậu quả do tội phạm này gây ra sẽ nhanh chóng ảnh hưởng tới hầu hết các lĩnh vực của đời sống với tốc độ chóng mặt, gây ra các hậu quả khôn lường về kinh tế - xã hội. Theo thống kê không đầy đủ của các chuyên gia an ninh mạng của Hoa Kỳ thì nước này mỗi năm thiệt hại khoảng từ 550 triệu đến 13 tỷ đô la do các tội phạm trong lĩnh vực công nghệ thông tin gây ra[1]. Các chuyên gia của EU cũng chỉ ra rằng, trong vài năm gần đây, những nhóm hacker có tổ chức chuyên phá hoại và thay đổi các trang thông tin ngày càng lộng hành. Chúng không chỉ gây tổn thất về tài chính tới hàng tỉ đô la mỗi năm mà trong một số trường hợp, còn gây hại đến tính

[1] Mohamed Chawki: *A Critical look at the regulation of Cybercrime,* tr. 11.

mạng con người, chẳng hạn như việc tấn công vào các hệ thống điều khiển bệnh viện và không lưu. Ở Việt Nam, tuy loại tội phạm này chưa phát triển nhưng cũng đã gây ra thiệt hại rất lớn, nhất là trong lĩnh vực bảo hộ quyền sở hữu trí tuệ. Rất nhiều các phần mềm do các công ty trong nước sản xuất vừa đưa ra thị trường đã bị giới hacker bẻ khoá, đăng các ký hiệu đăng ký công khai trên mạng hoặc sang in đĩa chương trình lậu khiến các công ty phần mềm rất khó khăn trong việc thu hồi vốn và bảo vệ bản quyền.

Thứ tư, về tính chất của hành vi phạm tội: các hành vi phạm tội có liên quan đến công nghệ thông tin thường rất tinh xảo. Tính chất này được quy định do các đặc điểm sau:

- Tội phạm trong lĩnh vực công nghệ thông tin phá huỷ hoạt động của các đối tượng tồn tại dưới dạng vật thể (như chương trình máy tính hoặc dữ liệu), mà không phá huỷ máy tính hoặc mạng máy tính, mạng thông tin hay các linh kiện của chúng, nên *sự phá huỷ này không để lại các dấu vết của sự phá huỷ tồn tại dưới dạng vật thể*;

- Người phạm tội chỉ *thực hiện hành vi phạm tội trong thời gian rất ngắn*, chúng có thể thực hiện hành

vi phạm tội chỉ trong vòng một phần nghìn, thậm chí một phần triệu giây bằng các máy tính có tốc độ xử lý siêu tốc;

- *Người phạm tội không bị hạn chế về thời gian, không gian,* chúng có thể thực hiện hành vi phạm tội ở bất cứ khi nào, bất cứ đâu, thậm chí từ một nơi rất xa hiện trường hoặc từ nước ngoài;

- Việc điều tra thu thập dấu vết đối với loại tội phạm này là cực kỳ khó khăn, bởi vì, người phạm tội có thể xoá bỏ hoàn toàn các dấu vết của hành vi phạm tội với một chương trình xoá dấu vết đã được đặt sẵn khi các lệnh phạm tội được thực hiện[1].

Ngoài bốn đặc điểm khác biệt cơ bản kể trên, chúng ta cũng có thể thấy một số dấu hiệu khác biệt khác so với các nhóm tội phạm thông thường như: tính không biên giới của loại tội phạm này, tính chất ngày càng tăng về số lượng và hậu quả, tinh vi về cách thức tiến hành cùng với sự phát triển của cuộc cách mạng công nghệ thông tin... Nhận biết các dấu hiệu này giúp chúng ta dễ dàng hơn trong việc xác định

[1] Nguyễn Mạnh Toàn: *Đặc điểm và các dạng hành vi cơ bản của tội phạm tin học. Sđd.*

đúng các loại tội danh thuộc nhóm tội phạm về công nghệ thông tin để có những biện pháp ngăn ngừa và xử lý có hiệu quả.

Tóm lại, tội phạm trong lĩnh vực công nghệ thông tin là một nhóm tội phạm mới hình thành trong quá trình phát triển của cuộc cách mạng công nghệ thông tin vào cuối thế kỷ XX và được dự báo là sẽ phát triển rất nhanh vào thế kỷ này. Hầu hết các nước trên thế giới đều đã và đang ban hành những văn bản pháp luật hình sự để ngăn ngừa và trừng trị loại tội phạm này. Qua các quy định của Bộ luật Hình sự năm 1999 cho thấy, tội phạm trong lĩnh vực công nghệ thông tin đã được tội phạm hoá ở nước ta, cho dù nội dung còn hết sức khái quát cần phải được cụ thể hoá, chi tiết hoá từng hành vi cụ thể cũng như bổ sung thêm những hành vi phạm tội mới thì cuộc đấu tranh phòng chống loại tội phạm này mới thực sự đạt hiệu quả.

Chương II

TÌNH HÌNH TỘI PHẠM VÀ CÁC QUY ĐỊNH PHÁP LUẬT VỀ PHÒNG, CHỐNG TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN

I. TÌNH HÌNH TỘI PHẠM VÀ CÁC QUY ĐỊNH PHÁP LUẬT VỀ PHÒNG, CHỐNG TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN CỦA MỘT SỐ NƯỚC TRÊN THẾ GIỚI

1. Tình hình tội phạm trong lĩnh vực công nghệ thông tin của một số nước trên thế giới

Bên cạnh những thành tựu đạt được, chính công nghệ thông tin đã và đang làm nảy sinh những thách thức đối với đời sống xã hội, ngay cả ở các nước phát triển. Không phải ngẫu nhiên mà các chuyên gia máy tính đã nhận định "*thế kỷ XXI là thế kỷ của tội phạm máy tính*". Không như các loại vi phạm pháp luật thông thường khác, hành vi vi phạm pháp luật trong lĩnh vực công nghệ thông tin xâm hại tới rất nhiều quan hệ xã hội, nhiều lĩnh vực khác nhau như: ngân hàng, quân sự, an ninh, thương mại hay lĩnh vực văn

hoá. *Ví dụ,* xâm phạm tình dục trẻ em chưa thành niên, giả mạo trong thương mại điện tử, giả mạo trong thanh toán ngân hàng, phá hoại, các loại tấn công làm tê liệt các dịch vụ máy chủ, tấn công làm tắc nghẽn đường truyền, vi rút (đặc biệt các loại vi rút như Trojan, Java applets), đánh cắp mật khẩu, đổi tên miền và địa chỉ IP, nghe lén thông tin trên mạng, thư điện tử mạo danh, thư điện tử vô danh.

Thông báo của Trung tâm nghiên cứu chiến lược và quốc tế nêu rõ: "*Một loại tội phạm công nghệ cao xuyên quốc gia mới xuất hiện. Chúng đang tập hợp công nghệ máy tính hàng đầu nhằm phục vụ cho các hoạt động toàn cầu không biên giới của chúng, trong khi đó các hoạt động phòng, chống lại bị cản trở bởi biên giới không có trong bản đồ của không gian nối mạng*". Trên thực tế, về mặt công nghệ, các cơ quan hành pháp thường thua kém tội phạm sử dụng mạng từ 5 đến 10 năm. Hàng tháng, tội phạm có tổ chức xuyên quốc gia lại gia tăng các vụ trộm cắp trên mạng. Trên thế giới đã xảy ra hàng nghìn vụ xâm phạm mạng Internet. Sự tăng vọt của loại tội phạm này không chỉ báo hiệu sự gia tăng của loại tội phạm mới mà còn cho thấy sự nhận thức về mức độ nguy

hiểm tội ác cũng càng rõ hơn. Thiệt hại do những tên tin tặc gây ra không hề thua kém bất cứ loại tội phạm nào. Chỉ tính riêng trong lĩnh vực dịch vụ tài chính, ngân hàng ở Mỹ cũng đã tổn thất khoảng 2,4 tỷ đô la Mỹ trong mỗi năm do các vụ tấn công máy tính. Tháng 3/1997, ông Xandip Saula - Giám định viên và là nhà phối hợp chương trình kiểm soát ma tuý của Liên hiệp quốc đã tuyên bố rằng, Internet đã thực sự trở thành "*Viện thí nghiệm kín*" phục vụ cho hoạt động sản xuất các loại chất ma tuý tổng hợp. Theo tài liệu mà ông Xandip Saula viện dẫn thì trên mạng Internet hiện đang "*đầy ứ*" những công thức sản xuất chất ma tuý, đặc biệt là những công thức sản xuất các chế phẩm tổng hợp thế hệ mới. Chỉ riêng tháng 5/2000 vi rút "*I love you*" đã gây thiệt hại gần 10 tỷ đô la Mỹ. Theo nhận định của các chuyên gia máy tính thì chiến tranh mạng có thể làm ngưng trệ toàn bộ nền kinh tế của một đất nước và điển hình là vụ đột nhập gây thiệt hại lớn nhất vào các mạng chia rẽ dữ liệu nội bộ của hãng Microsoft ngày 25/10/2000. Người đột nhập mạng đã sử dụng một loại vi rút mang tên '*Trojan*' (Con ngựa thành Tơ-roa) nhằm chuyển tải mã chương trình Window. Hay nạn bạo lực trên mạng cũng đang là vấn đề cấp bách. Sách báo

khiêu dâm trẻ em cũng là vấn đề chưa thể kiểm soát nổi. Ngoài ra, trong lĩnh vực quân sự, máy tính cũng chính là một tác nhân làm thay đổi cục diện tình hình. Điều đó có thể thấy từ chiến tranh vùng Vịnh (Irắc), Mỹ đã cài đặt một loại vi rút đặc biệt vào một chiếc máy in trong hệ thống phòng không, làm rối loạn hệ thống chỉ huy của Irắc. Cuộc chiến tranh Côxôvô được coi là cuộc chiến tranh mạng đầu tiên. Ngay từ đầu cuộc chiến, Nam Tư đã áp dụng hàng loạt biện pháp "*chiến tranh mạng*" tấn công gây rối loạn, thậm chí làm tê liệt mạng và hệ thống thư điện tử của NATO. Cụ thể, với sự giúp đỡ của chuyên gia máy tính Nga, các "*hacker*" của Nam Tư đã tấn công gây rối loạn mạng máy tính quân sự của Hải quân Mỹ, 2.000 bức thư điện tử mỗi ngày cùng với việc cài đặt các loại vi rút máy tính để phá hoại, đã làm ngưng trệ các hoạt động trong hệ thống thư điện tử của NATO (Tổ chức quân sự Bắc Đại Tây Dương). Việc sử dụng một loại bom đặc biệt tấn công từ xa đã phá hoại, làm tê liệt hệ thống máy chủ trên mạng của NATO và làm cho nhiều hệ thống mạng của NATO buộc phải ngừng hoạt động. Một thời gian sau lại xuất hiện một loại vi rút mới với cái tên "*...red*" nhằm mục đích tấn công vào "*Nhà Trắng*" và tập đoàn Microsoft.

Hậu quả của cuộc tấn công này khó có thể lường hết được, nếu như không được ngăn chặn kịp thời...

Sức mạnh và tính năng ưu việt của công nghệ thông tin đem lại cho thế giới là vô cùng hữu ích mà không ai có thể phủ nhận được. Nhưng mặt khác, song hành với nó là những nguy cơ tiềm ẩn không nhỏ. Nguy cơ trước hết là vấn đề an ninh và độ tin cậy của các thông tin trên Internet. Theo đó, thông qua Internet, trên thế giới đã xảy ra nhiều vụ đánh cắp bí mật quốc gia, nhiều hoạt động trộm cắp, lừa đảo, rửa tiền, tuyên truyền tài liệu phản động, văn hóa phẩm đồi truỵ, phá hoại trang thiết bị... Chúng ta có thể lấy ví dụ: Nếu một vụ cướp ngân hàng để lấy đi một tỷ đồng là rất khó khăn và không dễ trót lọt, thì việc một người bằng kỹ thuật công nghệ thông tin đột nhập vào một hệ thống máy tính của một tập đoàn, một công ty có thể lấy đi hàng trăm tỷ một cách dễ dàng. Ngoài ra, nó còn có thể làm cho cả hệ thống máy tính ngừng làm việc hoặc bị tê liệt, phong tỏa dữ liệu và lấy trộm các bí mật thông tin, còn thiệt hại về tài sản thì không thể thống kê được, đặc biệt là vấn đề chi phí, tiền của khắc phục hậu quả do tội phạm gây ra. Điều này có thể thấy qua một số vụ việc dưới đây:

- Năm 1999, vi rút Cherbobyl xuất hiện, nó khiến

ổ cứng và dữ liệu của nạn nhân hoàn toàn không thể truy cập. Ở Mỹ, vi rút này chỉ tấn công một số ít máy, nhưng ở Trung Quốc thiệt hại do sự tấn công của vi rút Cherbobyl ước tính lên tới 291 triệu đô la Mỹ;

- Năm 2000, vi rút Lover Letter từ quê hương Phillippins đổ bộ sang châu Âu và châu Mỹ trong vòng 06 tiếng đồng hồ đã phá hoại từ 2,5 đến 3 triệu máy và đã gây thiệt hại ước tính là 8,7 tỷ đô la Mỹ. Theo nhận xét của các chuyên gia thì Phillippins được coi là thiên đường của tin tặc[1];

- Cũng trong năm 2000, Văn phòng tương lai ở Vương quốc Anh phát hiện hệ thống tài chính bị ngự trị bởi bọn tội phạm máy tính, đã phát hiện hơn 2,8 tỷ đô la Mỹ trong thẻ tín dụng bị lấy cắp liên quan đến những vụ giả mạo hay gian lận xuất phát từ mạng lưới Internet trong năm 1999, dự đoán mất 5,5 tỷ đô la Mỹ vào năm 2002, với những giao dịch lên tới 900 tỷ đô la Mỹ và 0,3% số tiền này bị mất cắp[2];

---

[1] *PC World VietNam,* tháng 12/2000, tr.1.

[2] Nông Xuân Trường: *Tội phạm tin học và các biện pháp đấu tranh chống tội phạm tin học tại Hàn Quốc.* Tạp chí Kiểm sát, số 10/2003, tr. 49.

- Năm 2001, tại Mỹ có khoảng 85% trang web của các tổ chức Chính phủ, các tập đoàn kinh tế và tổ chức đoàn thể khác bị hacker tấn công. Theo báo cáo của Cục Điều tra Liên bang Mỹ (FBI) và Uỷ ban Bảo mật máy điện toán Mỹ (CSI) thì thiệt hại do các hacker này gây ra ít nhất là 377 triệu đô la Mỹ. Cũng trong năm này, tại Malaysia tình trạng hacker tấn công vào các trang web của Chính phủ đã lên mức báo động, các chuyên gia quản lý mạng nước này cảnh báo có khoảng 700 website khác cũng có nguy cơ bị hacker xâm nhập[1];

- Ngày 7/5/2001, website của Ấn Độ cũng bị tấn công;

- Ngày 28/6/2001, tại Singapo, website của Đảng Cộng sản các dân tộc Singapo (NSP) bị hacker tấn công. Hơn 8000 địa chỉ trong danh sách e-mail của NSP bị tin tặc xóa sạch. Vụ tấn công này xảy ra ngay sau khi Chính phủ thông báo các website chính trị cần phải điều chỉnh để ngăn chặn những luồng thông tin phá hoại[2];

- Tháng 6/2002, hacker đã thâm nhập NASA và lấy cắp dữ liệu, gây thiệt hại gần một triệu đô la Mỹ[3];

---

[1] Theo Malay Mail ngày 04/3/2001.

[2] Theo AFP ngày 29/6/2001.

[3] Trang http://www.VnExpress.net ngày 29/6/2002, tr.1.

- Ngày 18/12/2003, 13 website của NASA lại trở thành mục tiêu tấn công của một nhóm hacker Brazil;

- Năm 2004 được coi là năm bùng nổ của tội phạm máy tính. Theo đó, số vi rút mới tăng hơn 50% đã phá vỡ hơn 100.000 rào chắn an ninh. Các nỗ lực xâm nhập máy tính kiểu đánh lừa người dùng mở file đính kèm thư điện tử đã tăng hơn 30% và cách tấn công cũng phức tạp hơn, nhưng đáng cảnh báo là sự gia tăng cái gọi là mạng máy tính kiểm soát từ xa (bom net) do bọn hacker lừa đảo sử dụng để thực hiện tội ác trên không gian điều khiển. Ngoài ra, đó là sự bùng nổ các website ngân hàng giả dùng để moi thông tin đăng ký (login) của khách hàng. Cổng web Lycos Eurrope cho biết số tin nhắn E-mail giả mạo bị phát hiện tăng 500%. Nhóm The Anti-Phishing Working chuyên chống tội phạm ngân hàng điện tử thống kê số vụ tấn công kiểu này tăng 30% mỗi tháng.

Những tháng đầu năm 2004, xuất hiện các vi rút đính kèm ác tính Netsky, Bagle và MyDoom nhưng sau đó các vi rút nguỵ trang kỹ hay sâu (worm) thống trị môi trường Internet. Bên cạnh đó, năm 2004 cũng là năm chứng kiến sự xuất hiện của dòng vi rút đầu tiên trên điện thoại di động. Nếu trong quá khứ, quấy

rối điện thoại di động chỉ tồn tại trong phòng thí nghiệm thì đầu tháng 6 năm 2004, vi rút Cabir đã xuất hiện và "*nhảy*" được từ điện thoại di động này sang điện thoại di động khác bằng cách lợi dụng công nghệ sóng ngắn Bluetooth, có game Mosquito trên điện thoại Symbian biết lén lút gửi tin nhắn theo các số lưu trong máy, tháng 10 năm 2004, vi rút Skulls Trojan có thể làm hỏng điện thoại di động[1]...

- Tác hại của tội phạm máy tính là rất lớn, theo các chuyên gia Australia thì hàng năm tội phạm máy tính gây thiệt hại cho nước này trên 11 triệu đô la Mỹ và chắc chắn con số thực tế còn cao hơn nhiều lần[2]...

Những vấn đề nêu trên cho thấy, mức độ nguy hiểm của loại tội phạm này không thua kém bất kỳ tội phạm nào khác và có sự gia tăng nhanh chóng về số lượng phạm tội trong từng năm. Cụ thể, ở Hồng Kông, năm 1998 mới chỉ có 38 trường hợp phạm tội, tới năm

---

[1] Trung Nguyên. *Năm 2004, năm bùng nổ tội phạm máy tính*. Tổng hợp từ Internet tháng 01/2005, tr.1-2. Http://www.tuoitre.com.vn ngày 16/01/2005.

[2] Tymothyhall. White collar crime in Australia. Dẫn theo: Dương Tuyết Miên & Nguyễn Ngọc Khanh. *Tội phạm vi tính*. Tạp chí Tòa án nhân dân, số 5/2000, tr.19.

2000 con số đó đã lên tới 368 trường hợp, năm 2004 có tới hơn 600 trường hợp phạm tội.

Tuy vấn đề tội phạm trên mạng ngày càng gia tăng và rất nguy hiểm nhưng hầu hết đều chưa bị trừng phạt. Năm 1998, trong số 419 vụ án tội phạm trong lĩnh vực công nghệ thông tin chuyển đến Uỷ viên công tố Liên bang Mỹ thì chỉ khởi tố được 83 vụ, những vụ còn lại đều bị đình chỉ vì thiếu bằng chứng. Có đến 40% vụ việc không được xử lý vì thiếu bằng chứng phạm tội, hoặc không có dấu hiệu vi phạm pháp luật rõ ràng.

2. Các quy định pháp luật về phòng, chống tội phạm trong lĩnh vực công nghệ thông tin của một số nước trên thế giới

Mục tiêu của an ninh tin học là nhằm bảo vệ các cơ sở hạ tầng thông tin trong nước, bao gồm cả khu vực tư nhân và khu vực Chính phủ có sử dụng máy tính và mạng máy tính. Do đó, việc coi trọng máy tính, sớm tìm ra các cách thức và phương pháp cũng như có đối sách phù hợp để bảo vệ an ninh tin học trong hiện tại và tương lai là nhiệm vụ chung của tất cả các quốc gia trên thế giới, đồng thời đó cũng là trách nhiệm riêng của từng nước trong hợp tác quốc

tế đấu tranh chống lại các tội phạm xuyên quốc gia, tội phạm quốc tế và hợp tác vì một nền an ninh chung của nhân loại.

Hiện nay, số lượng các vụ phạm tội trên mạng đang và sẽ tăng nhanh gấp bội nếu chúng ta không có các biện pháp đấu tranh phòng chống. Bởi lẽ, tội phạm trong lĩnh vực công nghệ thông tin có thể tiến hành các hoạt động tác động đến nhiều nơi trên thế giới với thời gian tính bằng phần trăm của giây và tốc độ lan truyền nhanh. Đối tượng chủ yếu mà tội phạm này tấn công là hệ thống thương mại điện tử, kinh doanh điện tử, hệ thống thanh toán - ngân hàng, hệ thống tự động bán hàng...

Trước thực trạng đó, hầu hết các nước trên thế giới đã có nhiều biện pháp khác nhau để phòng chống loại tội phạm này trên cả phương diện pháp lý và phương diện thực tiễn.

Về cơ sở pháp lý, nhiều nước trên thế giới đã ban hành các đạo luật riêng hoặc một số điều luật riêng trong Bộ luật Hình sự quy định về tội phạm trong lĩnh vực công nghệ thông tin để đấu tranh phòng chống. *Ví dụ:*

- Theo luật của Australia, hành vi phá hủy,

xóa bỏ hoặc làm thay đổi dữ liệu lưu trữ trong máy tính hoặc đưa thêm dữ liệu vào máy vi tính một cách bất hợp pháp có thể bị xử phạt đến 10 năm tù hoặc bị phạt đến 48 nghìn đô la Úc;

- Bộ luật Hình sự Nhật Bản đã dành một số điều luật quy định về các hành vi phạm tội liên quan đến lĩnh vực công nghệ thông tin, như: Điều 161-2 về tội làm giả dữ liệu điện từ và cung cấp dữ liệu ấy; Điều 234-2 về tội làm hư hại máy tính để cản trở nghiệp vụ; Điều 246-2 về tội lừa đảo bằng cách sử dụng máy tính... Trong đó, mức hình phạt nghiêm khắc là tù khổ sai đến 10 năm hoặc phạt tiền với mức cao;

- Bộ luật Hình sự Liên bang Nga đã dành riêng Chương 28 quy định về các tội phạm trong lĩnh vực thông tin máy tính với ba điều luật cụ thể liên quan đến nhóm tội phạm này, gồm: Điều 268 về tội sử dụng trái phép thông tin trong máy vi tính; Điều 269 về tội xây dựng, sử dụng và lan truyền các chương trình vi rút; Điều 270 về tội vi phạm các quy định về vận hành hệ thống hay mạng vi tính. Trong đó, hình phạt nặng nhất cho tội phạm

máy tính có thể đến 7 năm tù;

- Đạo luật về truyền thông điện tử của Hoa Kỳ quy định hành vi truy cập dịch vụ truyền thông điện tử trái phép là tội phạm. Đạo luật bí mật truyền thông điện tử coi hành vi chiếm đoạt thông tin điện tử, ngăn chặn hành động thông tin điện tử, tiết lộ thông tin điện tử chiếm đoạt được là tội phạm. Ngoài ra, luật về lạm dụng và lừa đảo thông qua máy tính quy định tội phạm đối với nhiều loại hành vi: truy cập thông tin bí mật trong hệ thống máy tính của Chính phủ; chiếm đoạt thông tin của các tổ chức tín dụng; truy cập trái phép vào hệ thống máy tính của Chính phủ; sử dụng máy tính để lừa đảo chiếm đoạt tài sản của người khác; chiếm đoạt hoặc chuyển nhượng mật mã truy cập vào các cơ sở dữ liệu;

- Bộ luật Hình sự của Canada cũng quy định tại Điều 342-1 về tội phạm trong lĩnh vực công nghệ thông tin như: Người nào sử dụng phương tiện máy tính gây rối loạn chức năng của hệ thống máy tính một cách trực tiếp hoặc gián tiếp, sử dụng hoặc cho người khác sử

dụng mã số truy cập để người này thực hiện hành vi gây rối loạn chức năng của hệ thống máy tính, thì bị phạt tù không quá 10 năm;

- Tại Braxin, Luật số 9.983 ngày 17/7/2000 đã tội phạm hoá hành vi đưa dữ liệu sai vào hệ thống thông tin, theo đó: Người nào đưa thông tin sai lạc vào hệ thống thông tin thì có thể bị phạt tù từ 02 đến 12 năm (Điều 313 - A); Người nào thay đổi trái phép hệ thống thông tin hoặc chương trình máy tính thì bị phạt tù từ 03 tháng đến 02 năm (Điều 313 - B);

- Tại Anh, Luật Chống lạm dụng máy tính năm 1990 coi các hành vi sau là tội phạm: ***Truy cập trái phép*** *(Người nào truy cập trái phép vào máy tính hoặc thực hiện các biện pháp để truy cập trái phép vào mạng máy tính thì bị phạt tù không quá 06 tháng - Điều 1);* ***Truy cập trái phép để thực hiện hành vi phạm tội*** *(Người nào truy cập trái phép vào hệ thống máy tính để thực hiện các hành vi phạm tội mà luật hình sự đã quy định thì bị phạt tù không quá 05 năm - Điều 2);* ***Thay đổi dữ liệu một cách trái phép*** *(Người nào thay đổi trái phép các*

dữ liệu được lưu trữ trong hệ thống máy tính hoặc ngăn cản người khác truy cập vào dữ liệu, làm ảnh hưởng xấu tới độ tin cậy của dữ liệu thì bị phạt tù đến không quá 05 năm - Điều 3);

- Tại Bỉ, Bộ luật Hình sự (sửa đổi năm 2000) quy định tại Điều 550(b) như sau: Người nào biết rằng mình không có quyền truy cập, mà truy cập vào hệ thống máy tính thì bị phạt tù từ 03 tháng đến 01 năm và bị phạt tiền từ 5.200 đến 50.000 Franc Bỉ hoặc một trong hai hình phạt này. Trường hợp hành vi này được thực hiện với mục đích lừa dối thì có thể bị phạt tù từ 06 tháng đến 02 năm; Người nào có ý định lừa dối hoặc có ý định gây thiệt hại cho người khác, mà lạm dụng quyền truy cập vào hệ thống máy tính thì có thể bị phạt tù từ 06 tháng đến 02 năm và phạt tiền từ 5.200 đến 20.000 Franc Bỉ hoặc một trong hai hình phạt này; Người nào nỗ lực thực hiện các hành vi bị cấm kể trên thì bị phạt tù từ 06 tháng đến 05 năm hoặc bị phạt tiền từ 5.200 đến 40.000 Franc Bỉ hoặc cả hai hình phạt trên; Người nào biết

rằng dữ liệu có được là do thực hiện các hành vi bị cấm kể trên mà lưu giữ, tiết lộ cho người khác hoặc sử dụng dữ liệu có được vào bất cứ mục đích gì thì bị phạt tù từ 06 tháng đến 03 năm hoặc bị phạt tiền từ 5.200 đến 20.000 Franc Bỉ hoặc cả hai hình phạt này;

- Tại Cộng hoà Pháp, Bộ luật Hình sự cũng quy định: Người nào truy cập trái phép hệ thống xử lý thông tin tự động thì bị phạt tù không quá 01 năm và bị phạt tiền không quá 100.000 Franc. Trường hợp dữ liệu bị xâm hại bởi hành vi này thì người thực hiện hành vi sẽ bị phạt không quá 02 năm và bị phạt tiền không quá 200.000 Franc (Điều 323-1); Hành vi gây rối sự vận hành của hệ thống xử lý thông tin tự động thì bị phạt tù không quá 03 năm và bị phạt tiền không quá 300.000 Franc (Điều 323-2); Hành vi đưa dữ liệu trái phép vào hệ thống xử lý thông tin tự động làm dữ liệu trong hệ thống xử lý thông tin bị xâm hại hoặc thay đổi thì bị phạt tù không quá 3 năm và bị phạt tiền không quá 300.000 Franc (Điều 323-3);

- Tại Cộng hoà Liên bang Đức, Bộ luật

Hình sự quy định các hành vi sau là tội phạm: Hành vi chiếm đoạt dữ liệu: (Người nào chiếm đoạt trái phép dữ liệu của người khác mà dữ liệu này được bảo hộ khỏi sự chiếm đoạt thì bị phạt tù không quá 03 năm - Điều 202a); Hành vi thay đổi dữ liệu (Người nào xoá, làm hỏng, làm cho không còn giá trị, thay đổi dữ liệu thì bị phạt tù không quá 02 năm - Điều 303a); Hành vi phá hỏng hệ thống máy tính (Người nào can thiệp trái phép vào quá trình xử lý dữ liệu quan trọng của doanh nghiệp hoặc cơ quan nhà nước bằng việc phá huỷ, làm hỏng, xoá, bỏ hệ thống máy tính hoặc vật mang dữ liệu thì bị phạt tù không quá 05 năm - Điều 303b).

- Tại Trung Quốc, Hội đồng Nhà nước đã ban hành Nghị định số 147 ngày 18/02/1994 về Quy chế an toàn thông tin máy tính quy định trách nhiệm xử phạt đối với hành vi vi phạm như sau: Tổ chức an ninh công cộng có thể cảnh cáo hoặc phạt tiền tới 5.000 nhân dân tệ đối với cá nhân và tới 15.000 nhân dân tệ đối với tổ chức trong trường hợp cá nhân, tổ chức đưa vi rút máy

tính hoặc các dữ liệu độc hại khác làm ảnh hưởng tới an ninh mạng thông tin. Tổ chức, cá nhân bán trái phép các sản phẩm bảo vệ an ninh máy tính sẽ bị phạt từ 01 đến 03 lần thu nhập bất hợp pháp. Thu nhập bất hợp pháp bị tịch thu (Điều 23);

- Công ước của Hội đồng châu Âu về tội phạm mạng năm 2001 thì coi các hành vi chống lại sự bí mật, tính toàn vẹn và sẵn có của dữ liệu máy tính và hệ thống máy tính là tội phạm mạng, bao gồm:

*+ **Truy cập trái pháp luật:** Là hành vi cố ý truy cập vào một phần hoặc toàn bộ hệ thống máy tính mà không có quyền truy cập (có thể đòi hỏi thêm điều kiện việc truy cập phải có mục đích thu thập dữ liệu máy tính hoặc mục đích không trung thực khác;*

*+ **Ngăn chặn bất hợp pháp:** Là hành vi cố ý ngăn chặn việc truyền tải dữ liệu máy tính từ hệ thống máy tính này sang hệ thống máy tính khác hoặc trong cùng một hệ thống của người không có quyền thực hiện hành vi này;*

*+ **Gây rối dữ liệu:** Là hành vi cố ý làm*

hỏng, xoá, làm giảm chất lượng dữ liệu máy tính của người không có quyền thực hiện hành vi này (có thể đòi hỏi theo điều kiện là đã gây ra hậu quả nghiêm trọng);

*+ **Gây rối hệ thống máy tính:** Là hành vi cố ý ngăn cản sự vận hành bình thường của hệ thống máy tính bằng việc đưa vào, truyền tải, làm hỏng, xoá, thay đổi dữ liệu máy tính;*

*+ **Lạm dụng các thiết bị:** Là hành vi cố ý chiếm hữu, sản xuất, bán, cho người khác sử dụng, nhập khẩu, phân phối thiết bị (bao gồm chương trình máy tính), mã số truy cập hoặc các dữ liệu tương tự được thiết kế với mục đích chủ yếu là thực hiện các hành vi bị cấm trong Công ước này.*

Ngoài ra, Công ước còn quy định cấm cả các hành vi như tuyên truyền văn hoá phẩm đồi truỵ trên Internet (nhất là các văn hoá phẩm liên quan đến lạm dụng tình dục trẻ em), các hành vi xâm phạm quyền sở hữu trí tuệ trên mạng Internet.

Về mặt thực tế, các nước trên thế giới cũng đã có các biện pháp cụ thể để đấu tranh phòng, chống tội

phạm trong lĩnh vực công nghệ thông tin, cụ thể là:

> *- Tổ chức Cảnh sát quốc tế (Interpol) đã thành lập nhiều nhóm an ninh mạng, phối hợp với đội ngũ chuyên gia mạng để chống các hình thức tội ác trong thế giới mạng. Các nhóm này đã phối hợp theo khu vực Mỹ, Âu, Phi và châu Á - Thái Bình Dương. Mỗi nhóm bao gồm những người đứng đầu Đội đặc nhiệm chống tội phạm công nghệ thông tin (Information Technology Crime Unit - ITCU) của mỗi quốc gia. Mặc dù các đội đặc nhiệm ITCU này ở mỗi quốc gia có nhiều khác biệt, nhưng Interpol vẫn liên tục tổ chức trao đổi thông tin, cập nhật tình hình tội phạm, chia sẻ kinh nghiệm và huấn luyện các kỹ năng tin học cần thiết để các nhóm chiến đấu với tội phạm tin học và chiến thắng thế giới ngầm trên Internet. Trong đó, nhóm phối hợp châu Á - Thái Bình Dương hình thành năm 1998 và Việt Nam trở thành thành viên từ năm 2002*[1].

[1] http://www.echip.com.vn/: *Tuyên chiến với tội phạm máy tính*, ngày 07/01/2006, tr.1.

Ngoài ra, cảnh sát toàn thế giới vừa cùng nhau cam kết tiến hành cuộc đọ sức thực sự chống lại tội phạm mạng. Từ ngày 15 đến ngày 17/9/2005, gần 200 chuyên gia đến từ châu Âu, Mỹ, Úc, Trung Quốc, Nhật Bản đã họp tại Strasbourg để bàn các giải pháp chống tội phạm mạng. Đặc biệt, Công ước của châu Âu về tội phạm mạng đã có hiệu lực từ ngày 01/7/2004 nhằm tăng cường hợp tác về vấn đề trên[1].

- Liên minh châu Âu cũng vừa thành lập Cục Bảo mật thông tin và mạng châu Âu (European Network and Information Security Agency - EINSA), một cơ quan giữ vai trò "Bộ Tổng tham mưu", điều hành cuộc chiến chống tội ác trên Internet. EINSA sẽ được cấp 24,3 triệu Euro để bắt đầu hoạt động vào năm 2004 với trụ sở chính đặt tại Brussels (Bỉ). Ngoài ra, châu Âu còn đề xuất thông qua một Hiệp định đa phương để chống tội phạm trên mạng với các quy định

---

[1] http://www.vietnamnet: *Cảnh sát mạng chống tội phạm mạng: Chạy đua với thời gian*, ngày 22/9/2004, tr.1.

cụ thể về bằng chứng điện tử để tăng cường hiệu quả của cuộc chiến tổng lực nhằm thanh lọc môi trường mạng. Cụ thể như sau:

+ Mỗi nước tham gia phải cấm tất cả các hoạt động phân phối phần mềm sử dụng cho các mục đích phạm pháp trực tuyến;

+ Buộc các nhà cung cấp dịch vụ Internet (ISP) phải bảo đảm cung cấp thông tin lưu trữ ngay khi cơ quan chống tội phạm có yêu cầu;

+ Cho phép nghe trộm qua mạng;

+ Việc phối hợp dẫn độ tội phạm máy tính, cho phép cảnh sát yêu cầu đồng nghiệp ở các quốc gia khác phối hợp thực hiện điều tra.

Nước Mỹ đã tỏ ra sốt sắng với Hiệp định này, tích cực thúc giục và hy vọng sớm thiết lập những tiêu chuẩn chống tội phạm quốc tế trong các vấn đề như: xâm phạm bản quyền, gian lận thương mại trực tuyến, khiêu dâm trẻ em, xâm nhập mạng trái phép[1].

[1] http://www.echip.com.vn/: *Tuyên chiến với tội phạm máy tính*, ngày 07/01/2006, tr.2.

Cũng tại nước Mỹ, ông John Ashcroft - Bộ trưởng Bộ Tư pháp đã tuyên bố: "Siêu xa lộ thông tin không phải là đường cao tốc để chuyển tải tội ác. Ngăn chặn tội ác trên Internet sẽ là ưu tiên hàng đầu của cơ quan công lực Liên bang". Đại diện Bộ Tư pháp đã tuyên bố như vậy trước khi triển khai một cuộc chiến tổng lực trên không gian điều khiển học. Cụ thể, Cục Điều tra Liên bang (FBI) đã phối hợp với 43 đơn vị của Bộ Tư pháp Mỹ, Uỷ ban Thương mại Liên bang (FTC), Cục Thanh tra bưu chính (PIS), Mật vụ, Cục Thuế quan và Nhập cư để triển khai một cuộc điều tra có tên gọi là "Chiến dịch càn quét thế giới mạng" (Operation Cyber Sweep). Sau hai tuần càn quét thế giới ngầm trên Internet, kết thúc giai đoạn đầu của chiến dịch, FBI đã bắt giam 130 tội phạm, thu hồi hơn 17 triệu đô la Mỹ. FBI còn xác định được danh sách của 125.000 nạn nhân đã bị thiệt hại tổng cộng khoảng 100 triệu đô la Mỹ[1].

[1] http://www.echip.com.vn/: *Tuyên chiến với tội phạm máy tính*, ngày 07/01/2006, tr.2.

Bên cạnh đó, tháng 12/2000 một cuộc Hội nghị quốc tế được tổ chức tại nước này với sự tham gia của 16 nước, bao gồm: Mỹ, Canada, Anh, Australia, Brazil, Đan Mạch, Phần Lan, Đức, Pháp, Nhật Bản, Hàn Quốc, Nga, Tây Ban Nha, Thụy Điển, Italia và Lucxambua. Hội nghị đã thành lập ra một cơ quan với tên gọi "Địa điểm liên lạc quốc tế về tội phạm công nghệ cao 24/24h" để hỗ trợ và phối hợp giữa các quốc gia thành viên trong việc phát hiện, điều tra và xử lý tội phạm tin học.

- Để đối phó với tội phạm công nghệ cao, Cảnh sát nước Anh đã áp dụng mọi biện pháp, trong đó có một biện pháp khá hữu hiệu là tìm ra những bằng chứng phạm tội của kẻ bị tình nghi từ chiếc ổ cứng máy tính.

Tại đất nước này đã sớm hình thành một Đội cảnh sát phòng, chống tội phạm riêng trong lĩnh vực công nghệ cao (NHTCU). Đội đặc nhiệm này có nhiệm vụ đấu tranh chống lại các tội phạm trực tuyến như hacker, lừa đảo, gieo rắc khiêu dâm trẻ em và bất kỳ hành vi phạm tội nào có liên quan đến máy tính.

Đội đặc nhiệm này sử dụng phần mềm EnCase là công cụ để đấu tranh, và phần mềm này đang được hơn 2.000 cơ quan an ninh trên toàn thế giới sử dụng. Phần mềm này đã giúp cho Điều tra viên tìm manh mối trong các ổ cứng mà họ tịch thu được của bọn tội phạm trong quá trình điều tra.

Ngoài ra, để đối phó có hiệu quả hơn, NHTCU còn hợp tác với một số cơ quan và hãng nghiên cứu và một trong số đó là hãng DataSec. Hãng này chuyên tìm kiếm và thu thập các bằng chứng về hoạt động của những người gieo rắc khiêu dâm trẻ em, phối hợp với cảnh sát và các nhà cung cấp dịch vụ Internet lần theo dấu vết, sau khi cảnh sát tịch thu được máy tính mà kẻ tình nghi sử dụng, nhiệm vụ của DataSec là tìm ra bằng chứng từ chiếc máy tính đó[1].

- Tại Hàn Quốc, trong quá trình đấu tranh phòng và chống tội phạm trong lĩnh vực công nghệ thông tin, các cơ quan tư pháp

[1] http://www.vietnamnet.vn/: *Tìm bằng chứng phạm tội trong ổ cứng máy tính*, ngày 08/6/2002, tr.1.

nước này đã phân tích để chỉ ra năm nhóm tội phạm loại này như sau[1]*:*

+ Nhóm tội phạm nói xấu, phá hoại thư tín dụng, lưu hành các lời nói đồn đại nhảm nhí hoặc những câu chuyện vô căn cứ bằng cách sử dụng hệ thống thông tin viễn thông;

+ Nhóm tội phạm lưu hành các tài liệu bị cấm như các tài liệu có nội dung đồi trụy, tấn công vào mạng máy tính;

+ Nhóm tội phạm sử dụng máy tính trái phép, gian lận thương mại điện tử;

+ Nhóm tội phạm tiết lộ và sử dụng thông tin cá nhân một cách bất hợp pháp; và

+ Nhóm tội phạm xâm nhập bất hợp pháp vào hệ thống máy tính bằng các hình thức như tin tặc, khủng bố trên mạng, lan truyền phát tán các vi rút tin học.

Tuy nhiên, trước tình hình gia tăng ngày càng nhiều của tội phạm trong lĩnh vực công nghệ thông tin, đồng thời phòng ngừa đối với

[1] Nông Xuân Trường: *Tội phạm tin học và các biện pháp đấu tranh chống tội phạm tin học tại Hàn Quốc*. Tạp chí Kiểm sát, số 10/2003, tr. 49-50.

loại tội phạm mới và tinh vi này, Hàn Quốc đã thành lập một hệ thống Cơ quan điều tra tội phạm công nghệ thông tin bao gồm:

+ Trung tâm chỉ huy ứng phó với tội phạm công nghệ thông tin;

+ Ban điều tra tội phạm công nghệ thông tin;

+ Đội điều tra tội phạm công nghệ thông tin.

Song song với việc hình thành một hệ thống Cơ quan điều tra tội phạm công nghệ thông tin với những nhiệm vụ và quyền hạn tương ứng, các cơ quan tư pháp nước này còn áp dụng đồng bộ và có hệ thống một số biện pháp sau để tăng cường công tác điều tra và chất lượng công tác điều tra đối với tội phạm công nghệ thông tin, cụ thể:

+ Tổ chức các khóa đào tạo cho các Điều tra viên, Công tố viên phụ trách điều tra tội phạm công nghệ thông tin. Hoạt động này do Viện Công tố tối cao và Viện Nghiên cứu - Đào tạo pháp vụ thuộc Bộ Tư pháp đảm nhiệm việc tổ chức tập huấn hoặc mời các chuyên gia giỏi các nước phát triển trên thế giới về đào tạo;

+ Thành lập Trung tâm Quản lý tội phạm trên mạng Internet (ICIC). Nhiệm vụ của tổ

chức này là bảo vệ cơ sở hạ tầng quốc gia và các hoạt động tư nhân trên mạng Internet, tiếp nhận, xử lý những lời đe dọa hoặc chống lại các cuộc tấn công vào cơ sở hạ tầng của Nhà nước;

+ Đầu tư trang thiết bị hiện đại nhất để phục vụ việc điều tra tội phạm công nghệ thông tin;

+ Thiết lập và giữ vững mối quan hệ chặt chẽ với Cơ quan an ninh thông tin Hàn Quốc, với các cơ sở đào tạo đại học, các viện nghiên cứu, các nhà cung cấp dịch vụ Internet trên đất nước để có thông tin và kiến thức chuyên ngành cập nhật, giảm bớt các nguy cơ có thể xảy ra trong công tác điều tra tội phạm công nghệ thông tin;

+ Tăng cường hợp tác quốc tế trong việc phát hiện, phòng ngừa và trấn áp tội phạm công nghệ thông tin.

- Ở Rumani, trong thời gian vừa qua do tội phạm trong lĩnh vực công nghệ thông tin ở nước này phát triển quá mạnh nên đã gây thiệt hại về nhiều mặt cho đời sống xã hội. Chính vì vậy, về mặt thực tế, để đấu tranh

phòng chống loại tội phạm này, Rumani đã có một số giải pháp sau:

+ Ban hành một đạo luật chống tội phạm tin học (được Quốc hội Rumani thông qua năm 2003);

+ Cơ quan cảnh sát Rumani thiết lập một bộ phận chuyên trách về tội phạm công nghệ thông tin, chuyên dò tìm manh mối của bọn tin tặc, theo dõi tín hiệu Internet từ những điểm có nghi ngờ và điều tra phân tích dữ liệu từ ổ cứng của bọn tội phạm;

+ Liên hệ, hợp tác mật thiết với nước ngoài, nhận sự hỗ trợ từ Interpol, từ FBI và các chuyên viên chống tội phạm công nghệ thông tin của Mỹ và Tây Âu;

+ Đào tạo các cán bộ an ninh chuyên trách chống tội phạm tin học[1].

- Riêng đối với các nước ASEAN, việc đấu tranh phòng, chống tội phạm công nghệ thông tin cũng được quan tâm thỏa đáng, cụ thể, các nước này đã thành lập Nhóm chống

---

[1] http://www.vinexco.com.vn: *Tội phạm kỹ thuật cao - khủng bố tin học*, ngày 20/10/2003, tr.2.

tội phạm công nghệ thông tin. Theo đó, Bộ trưởng viễn thông các quốc gia Đông Nam Á đã quyết định thiết lập một hệ thống cảnh báo sớm để theo dõi những kẻ khủng bố sử dụng mạng máy tính để gây bất ổn trong khu vực.

Đặc biệt, mỗi thành viên của các quốc gia ASEAN sẽ thành lập một nhóm chuyên gia tin học phản ứng nhanh (Computer Emergency Response Team - CERT) để "hỗ trợ việc ngăn ngừa, bảo vệ và giải quyết những mối đe dọa an ninh máy tính, đồng thời củng cố sự hợp tác trong khu vực". Trước hết, mỗi nhóm phải có ít nhất là 12 người, các nhóm này sẽ chia sẻ những thông tin liên quan đến hacker, các loại sâu và vi rút máy tính, đồng thời hợp tác chống lại những tội phạm mới trên mạng...

II. TÌNH HÌNH TỘI PHẠM VÀ CÁC QUY ĐỊNH PHÁP LUẬT VỀ PHÒNG, CHỐNG TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN Ở NƯỚC TA

1. Tình hình tội phạm trong lĩnh vực công nghệ thông tin ở nước ta

Cùng với xu thế hội nhập kinh tế, quốc tế toàn cầu,

ở nước ta tình hình vi phạm pháp luật trong lĩnh vực công nghệ thông tin cũng gia tăng một cách nhanh chóng trong mấy năm gần đây, đặc biệt là trong các lĩnh vực ngân hàng, bưu chính viễn thông, thương mại điện tử, văn hoá - nghệ thuật và sở hữu trí tuệ.

Trong lĩnh vực ngân hàng

- Lợi dụng chủ trương hiện đại hoá và tăng cường công tác giao dịch một cửa, một số cán bộ đã lợi dụng việc quản lý lỏng lẻo của ngành ngân hàng để lập chứng từ giả. Nguy hiểm hơn, chúng còn sử dụng phần mềm máy tính quản lý quá trình giao dịch, thanh toán... chiếm đoạt hàng tỷ đồng của Nhà nước. Điển hình là vụ Hoàng Văn Mạnh, lãnh đạo Phòng Kế toán tin học Chi nhánh Ngân hàng Đầu tư - Phát triển tỉnh Hưng Yên tự ý sửa phần mềm máy tính của hệ thống kế toán, chuyển tiền vào tài khoản cá nhân của y để tham nhũng với số tiền 1,08 tỷ đồng[1].

- Lợi dụng sơ hở trong việc triển khai hoạt động hệ thống máy rút tiền ATM, một số cán bộ kế toán ngân

[1] Trang vi tính của http://www.VnExpress.net.

hàng có thể truy cập vào mạng máy tính và thao tác trực tiếp trên máy tính, sau đó chuyển tiền từ tài khoản của khách hàng sang tài khoản của mình rồi thông qua máy ATM rút tiền tham ô. Điển hình là vụ Võ Sỹ Phượng, cán bộ Ngân hàng Nông nghiệp và Phát triển nông thôn chi nhánh quận Thanh Xuân - Hà Nội, ngày 18/3/2004 đã lợi dụng sơ hở của chương trình Korebank tự ý chuyển hai tài khoản gửi của hai khách hàng sang tài khoản của mình và vợ với tổng số tiền là 176.738.000 đồng (tiền gốc) để sử dụng vào mục đích cá nhân như chơi lô đề, cá cược bóng đá[1]...

- Ngoài ra, còn có việc giả mạo chữ ký của chủ tài khoản vào tài khoản "*ma*", rồi dùng thẻ ATM rút tiền tham ô. *Ví dụ,* vụ Trần Thị Bé Hạnh, giao dịch viên thuộc Phòng Kinh doanh dịch vụ Ngân hàng Vietcombank chi nhánh Cần Thơ, bằng thủ đoạn trên đã rút trên 100 triệu đồng để sử dụng vào mục đích cá nhân như chơi lô đề[2]...

- Do công tác kiểm tra, kiểm soát không chặt chẽ, một số nhân viên ngân hàng đã thông qua máy ATM

[1] Trang vi tính của http://www.VnExpress.net

[2] Trang vi tính của http://www.VnExpress.net.

hạch toán nhầm trong tài khoản khách hàng bằng cách thêm những số '0' như vụ nhân viên Ngân hàng Ngoại thương Hà Nội đã tự sửa 700.000 nghìn đồng thành 7.000.000 triệu đồng.

- Năm 2005 đã phát hiện được bảy vụ, đối tượng lợi dụng công nghệ thông tin và việc triển khai áp dụng công nghệ thông tin hỗ trợ hoạt động nghiệp vụ của các ngân hàng để lừa đảo chiếm đoạt tài sản (Vụ Đỗ Giang Nam, Giám đốc Công ty Tin học Phương Nam bằng thủ đoạn đột nhập vào hệ thống tin học của Ngân hàng Nông nghiệp và Phát triển nông thôn Việt Nam phát ra lệnh gửi tiền *"ảo"* từ chi nhánh Ngân hàng Nông nghiệp và Phát triển nông thôn Hải Phòng đến chi nhánh tại các tỉnh Ninh Bình, Thái Bình, Thanh Hoá để chiếm đoạt 1.432.000.000 tỷ đồng là một điển hình...)[1].

Trong lĩnh vực bưu chính viễn thông

Tại một số tỉnh, thành phố trong cả nước, thời gian

[1] Trang vi tính của http://www.VnExpress.net.

qua, đã phát sinh một loại tội phạm mới, đó là hành vi lắp đặt, thuê kênh riêng, sử dụng dịch vụ viễn thông; sử dụng thiết bị kỹ thuật công nghệ cao để trộm cắp tiền cước điện thoại viễn thông quốc tế với số lượng lớn, không những gây thiệt hại đặc biệt nghiêm trọng đến nền kinh tế, mà còn làm mất quyền kiểm soát về mặt an ninh thông tin của các cơ quan chức năng của Nhà nước. Loại tội phạm này đang có chiều hướng gia tăng và lan rộng.

Từ năm 1999 đến nay, lực lượng bảo vệ an ninh kinh tế và lực lượng An ninh điều tra đã phối hợp với ngành Bưu chính viễn thông phát hiện, bắt giữ và khởi tố, điều tra hơn 50 vụ phạm tội loại này với trên 100 bị can, kết thúc điều tra trên 20 vụ, tạm đình chỉ điều tra và xử lý hành chính 03 vụ do đối tượng chính bỏ trốn. Tuy nhiên, đến nay chưa phát hiện và làm rõ được vụ nào đối tượng phạm tội thông qua việc dùng thiết bị kỹ thuật trộm cắp cước viễn thông quốc tế để trực tiếp xâm hại đến an ninh quốc gia. Quá trình điều tra, xét xử loại tội này còn có nhiều vướng mắc, mặc dù đã xác định được loại tội phạm này có một số hành vi phạm tội đặc trưng như lén lút lắp đặt và sử dụng một số thiết bị viễn thông mới, chuyên dùng, có tính năng tác dụng lớn như nén, điều khiển và khuyếch đại

tín hiệu thu phát để chuyển lưu lượng điện thoại quốc tế từ nước ngoài về Việt Nam không qua sự kiểm soát cước quốc tế của ngành Bưu điện. Hệ thống thiết bị viễn thông do bọn tội phạm này thiết lập liên lạc trực tiếp với nước ngoài bằng cách thông qua kênh thuê riêng quốc tế hoặc thu nhận tín hiệu trực tiếp từ vệ tinh nước ngoài VSAT qua ăngten parabol và được kết nối với nhiều máy điện thoại loại cố định, vô tuyến cố định và di động Vinaphone, Mobiphone, Viettel... Thời gian qua, ở các tỉnh như Lạng Sơn, Quảng Ninh, Hà Giang đã phát hiện bốn vụ trộm cắp cước viễn thông quốc tế bằng việc lợi dụng sự chồng lấn sóng viễn thông tại các khu vực biên giới Việt - Trung và Trung Quốc - Liên bang Nga của hai loại điện thoại di động hoặc điện thoại kéo dài để thực hiện các cuộc gọi từ nước ngoài về Việt Nam. Bọn tội phạm đã chiếm đoạt tiền cước điện thoại quốc tế mà Nhà nước ta được hưởng theo thoả thuận độc quyền kinh doanh viễn thông giữa Việt Nam và nước ngoài; chúng chỉ phải thanh toán cước điện thoại nội hạt. Điển hình là vụ Chen Jen Chong người Đài Loan cấu kết với Lưu Hồ Hải người Trung Quốc, từ 18/12/2000 đến ngày 02/4/2001 đã thiết lập một hệ thống chuyển tải các cuộc gọi quốc tế trên 24 kênh từ nước ngoài vào Việt

Nam không qua sự kiểm soát, được hoà mạng trái phép qua 12 kênh điện thoại công cộng thuê bao của Bưu điện thành phố Hồ Chí Minh, chiếm đoạt hơn 3,5 tỷ đồng cước phí điện thoại quốc tế[1].

Thiệt hại về mặt kinh tế cho đến nay, qua công tác giám định và điều tra của Cơ quan An ninh điều tra, ước tính khoảng trên 30 triệu đô la Mỹ, hàng trăm tỷ đồng Việt Nam và khoảng 8,3 triệu phút viễn thông quốc tế chưa xác định được từ nước nào chuyển về Việt Nam (do đó không tính được thiệt hại quy ra tiền). Ngay với hình thức trộm cắp cước viễn thông quốc tế đơn giản bằng điện thoại kéo dài từ Trung Quốc sang như vụ ở Quảng Ninh, chỉ trong một thời gian ngắn, bọn tội phạm đã chiếm đoạt được 24.785 đô la Mỹ hoặc vụ Phạm Hoàng Hùng chiếm đoạt 18,031 tỷ đồng[2]...

Trong lĩnh vực thương mại điện tử

Về bản chất, cơ chế hoạt động cũng như các mô hình

[1] Trang An ninh kinh tế của http://www.cand.com.vn.

[2] Trang An ninh kinh tế của http://www.cand.com.vn.

thực hiện giao dịch thương mại điện tử như hoạt động giao dịch mua bán, trao đổi hàng hoá thông qua phương tiện điện tử trên thế giới nói chung và ở Việt Nam nói riêng cho thấy, đây là một lĩnh vực mới và vô cùng rộng lớn, các vi phạm pháp luật xảy ra đa dạng, phong phú, gây thiệt hại đáng kể về mặt vật chất cho các tổ chức, cá nhân như:

- ***Hành vi lừa đảo chiếm đoạt tài sản.*** Là việc kẻ lừa đảo lập một website, về mặt hình thức giống hệt như website của một số doanh nghiệp nổi tiếng và làm ăn có uy tín, tạo nên sự nhầm lẫn đối với khách hàng. Sau khi khách hàng thực hiện các giao dịch mua bán hàng hoá và chuyển tiền vào tài khoản theo chỉ dẫn, hàng hoá đã không được đem tới địa chỉ của người mua như yêu cầu, số tiền đó đã bị chiếm đoạt. Hành vi này chủ yếu xảy ra trong giao dịch diễn ra giữa hai nhóm đối tượng trong đó bên bán là doanh nghiệp và bên mua là cá nhân;

- ***Hành vi trộm cắp tài sản.*** Các doanh nghiệp kinh doanh văn hoá phẩm, báo chí, phim ảnh v.v... khi khách hàng có nhu cầu sử dụng một sản phẩm nào đó, *ví dụ,* đọc báo điện tử, xem phim, nghe ca nhạc v.v... thì khách hàng phải vào website của nhà

cung cấp sản phẩm, khai báo tên, tuổi, địa chỉ, số tài khoản thì mới cập nhật và khai thác được, số tiền phải trả tuỳ theo từng dữ liệu mà khách hàng khai thác. Tuy nhiên, trên thực tế một số trường hợp không cần có tài khoản nhưng vẫn có thể khai thác các dữ liệu mà không phải trả tiền;

- ***Hành vi lấy cắp thông tin của các doanh nghiệp.*** *Ví dụ:* một tập đoàn kinh tế A có trụ sở chính tại Mỹ, có các chi nhánh tại Anh, Pháp, Việt Nam v.v... Khi có một kế hoạch kinh doanh cụ thể, tập đoàn này không cần phải triệu tập đại diện tất cả các chi nhánh về trung tâm đầu não để phổ biến và triển khai kế hoạch (vì nếu làm như vậy sẽ rất tốn kém và quan trọng hơn là mất cơ hội trong kinh doanh), từ trung tâm, qua phương tiện điện tử có thể truyền tải toàn bộ nội dung kế hoạch đó đến từng chi nhánh và các nơi cần truyền tải ở các nước trên thế giới một cách nhanh chóng, chính xác, kịp thời. Trong quá trình chuyển tải thông tin từ trung tâm đến các chi nhánh, thông tin đã bị đánh cắp, kế hoạch đó bị lộ, lợi ích của doanh nghiệp bị thiệt hại, thậm chí có thể dẫn đến tình trạng phá sản;

- ***Hành vi vô ý làm lộ bí mật thông tin.*** Các chủ

thể tham gia giao dịch thương mại điện tử đều phải sử dụng một mạng thông tin nhất định để trao đổi những vấn đề cần thiết. Khi cần bảo mật những thông tin này, các chủ thể giao dịch có thể đăng ký sử dụng một dịch vụ bảo mật từ một nhà cung cấp dịch vụ nhất định (ví dụ mật mã), nhà cung cấp dịch vụ này có trách nhiệm bảo vệ các thông tin được giữ bí mật trong quá trình truyền đi một cách tuyệt đối. Tuy nhiên, trong quá trình thực hiện các thao tác nghiệp vụ, một số cá nhân thuộc nhà cung cấp dịch vụ quản lý đã vô ý làm lộ các thông tin nói trên cho một hoặc nhiều đối tượng khác làm thiệt hại cho các chủ thể tham gia giao dịch (ở đây chỉ xét trường hợp vô ý). Mặc dù lỗi hoàn toàn là vô ý nhưng hậu quả thiệt hại cho các chủ thể tham gia giao dịch đã xảy ra, ở một mức độ nhất định những cá nhân này phải chịu trách nhiệm hình sự bởi hành vi vô ý làm lộ bí mật thông tin thương mại điện tử của mình;

- ***Hành vi làm biến dạng các dữ liệu thương mại điện tử.*** Quá trình các cá nhân, tổ chức, doanh nghiệp đàm phán, trao đổi với nhau về một vấn đề nào đó liên quan đến hoạt động kinh doanh được thực hiện qua phương tiện điện tử, kẻ gian đã làm biến dạng các dữ liệu trên trước khi chúng được đưa

tới nơi cần truyền tải, dẫn đến tình trạng hiểu sai lệch nội dung và gây thiệt hại cho cá nhân, doanh nghiệp đó. Thực tiễn cho thấy có nhiều hình thức làm biến dạng các dữ liệu thông tin điện tử nói chung và dữ liệu thương mại điện tử nói riêng, trong đó hình thức tạo vi rút và sâu máy tính là một hình thức điển hình. Kể từ khi máy tính được đưa vào ứng dụng trong thương mại (1980) thì vi rút và sâu máy tính cũng xuất hiện, ngoài việc xuất hiện do các biến cố kỹ thuật thì việc tạo ra những vi rút với ý đồ phá hoại các chương trình phần mềm, nội dung các dữ liệu được truyền tải, lưu giữ của các cá nhân, tổ chức, gây thiệt hại rất lớn cho các tổ chức, cá nhân này cũng khá phổ biến. Theo kết quả nghiên cứu của Trường Đại học Bách khoa Hà Nội, số lượng máy tính của Việt Nam bị vi rút tấn công lên tới 95% và thiệt hại lên tới 390 tỷ đồng/năm. Theo ước tính của hãng dịch vụ mạng Sandvine, bất kỳ ngày nào cũng có từ 2% đến 12% lưu lượng thông tin mạng là những luồng có tính chất phá hoại;

- ***Hành vi tấn công từ chối dịch vụ.*** Là tên gọi chung của kiểu tấn công làm cho một hệ thống nào đó bị quá tải dẫn đến không thể cung cấp dịch vụ hoặc phải ngừng hoạt động. Để thực hiện việc tấn công từ

chối dịch vụ, kẻ tấn công tìm cách chiếm dụng và điều khiển nhiều máy tính hoặc mạng máy tính trung gian từ nhiều nơi để đồng loạt gửi ào ạt các gói tin với số lượng lớn, mục đích chiếm đoạt tài nguyên và làm ngập đường truyền của một mục tiêu xác định nào đó. Thậm chí hiện nay đã xuất hiện nhiều loại vi rút có chức năng tự động tấn công dịch vụ, hậu quả là làm cho hoạt động của hệ thống quá tải và không đáp ứng được yêu cầu hợp lệ nữa;

- ***Hành vi giả mạo chữ ký điện tử.*** Mặc dù khi sử dụng chữ ký điện tử, các chủ thể tham gia giao dịch thương mại điện tử đã phải đăng ký với một nhà cung cấp dịch vụ nhất định và sử dụng sản phẩm của họ. Tuy nhiên, chữ ký điện tử này hoàn toàn có thể bị giả mạo và gây thiệt hại cho doanh nghiệp.

Ví dụ, để xác nhận một sản phẩm nào đó là sản phẩm của doanh nghiệp, Giám đốc doanh nghiệp phải ký (bằng chữ ký điện tử) xác nhận, khẳng định sản phẩm đó. Khi đã đánh cắp được chữ ký điện tử, kẻ gian đã dùng chữ ký đó để xác nhận sản phẩm của mình (gần giống sản phẩm của doanh nghiệp nhưng chất lượng kém hơn).

Trong lĩnh vực văn hoá - nghệ thuật

Thế giới Internet là thế giới được quản lý một cách lỏng lẻo. Tính chất dễ dàng, thông thoáng, tốc độ trong cung cấp và tiếp cận thông tin trong mạng Internet đã trở thành con dao hai lưỡi. Ngoài các hành vi vi phạm đã được nêu ở trên thì chúng ta cũng đang phải đối đầu với nạn các hacker xây dựng các trang web sex để phát tán, cung cấp cho các đối tượng có nhu cầu xem hoặc tò mò xem. Ở nước ta hiện nay có hơn 10 trang web sex bằng tiếng Việt và có rất đông cổ động viên tham gia bởi vì chỉ cần ngồi một chỗ, dùng máy tính là có thể vào được các trang web này. Do vậy, các cổ động viên của các trang web sex không giới hạn độ tuổi tham gia. Một số đối tượng dùng Internet để đưa ảnh khiêu dâm, khiêu dâm trẻ em, tạo ảnh khoả thân đưa lên mạng để tấn công đời tư của người khác, mua bán dâm, kích dục thông qua chat tại các quán cà phê Internet mà máy tính có gắn webcam. Ngoài việc phát tán hình ảnh đời tư của người khác lên mạng, lợi dụng sự quảng cáo về các trang web sex, tội phạm mạng còn tải nội dung của các trang web sex này và ghi vào

đĩa CD để bán. Số lượng đĩa CD loại này đang được bán tràn lan và rất khó kiểm soát.

2. Nguyên nhân của tình trạng tội phạm trong lĩnh vực công nghệ thông tin ở nước ta

Theo thống kê của các trung tâm, cơ quan về an ninh mạng thì hiện nay khoảng 90% máy tính ở nước ta bị nhiễm vi rút, gây thiệt hại hàng chục tỷ đồng mỗi năm, làm ảnh hưởng trực tiếp đến việc phát triển kinh tế, tình hình an ninh trật tự, an ninh quốc gia. Ngoài các nguyên nhân của tội phạm nói chung thì nguyên nhân cơ bản dẫn đến hành vi phạm tội trong lĩnh vực công nghệ thông tin là:

Thứ nhất, người sử dụng máy tính chưa nhận thức và có ý thức đầy đủ về tầm quan trọng của vấn đề an ninh mạng, vì nhiều người hoặc nhiều doanh nghiệp cho rằng website của mình chỉ cần có firewall (bức tường lửa) là bảo đảm an toàn tuyệt đối. Nhưng thật ra, tính năng của bức tường lửa cũng chỉ bảo đảm được phần nào mức độ an toàn của hệ thống mạng, bức tường lửa có thể chỉ được ví như một chiếc khoá của ngôi nhà, cửa chính có thể đóng nhưng "*kẻ trộm*" có thể đột nhập từ cửa sổ, thậm chí từ lỗ thông hơi của ngôi nhà;

Thứ hai, tuỳ theo mục đích của người phạm tội mà

họ sẽ thực hiện những hành vi vi phạm trong các lĩnh vực tương ứng. Ví dụ, mục đích của tội phạm là kiếm tiền thì phải xâm nhập vào các trang website của ngân hàng, doanh nghiệp, trung tâm thương mại để lừa đảo, chiếm đoạt tài sản; còn mục đích của tội phạm là chính trị thì phải xâm nhập vào các trang website của Chính phủ để phá rối và tuyên truyền các tư tưởng xấu đến các trang website khác mà có nhiều người tham gia truy cập hàng ngày;

Thứ ba, một số người phạm tội do không hiểu biết về pháp luật. Đây là những đối tượng có kỹ năng hoặc mới khám phá được các kỹ thuật xâm nhập vào các website nhằm thể hiện sự hiểu biết của mình nhưng không biết được hậu quả hành vi của mình gây ra, làm tổn hại về vật chất, lẫn uy tín của các trang website đó.

3. Những khó khăn, vướng mắc trong quá trình điều tra, truy tố, xét xử

Trong công tác điều tra

Dấu vết của tội phạm trong lĩnh vực công nghệ thông tin rất mờ nhạt, khó xác định chứng cứ. Do

không có đủ phương tiện kỹ thuật, chuyên gia về công nghệ thông tin và cơ chế phối hợp quốc tế để truy tìm dấu vết điện tử, cho nên công tác điều tra chưa đạt hiệu quả. Hiện nay Cục Cảnh sát điều tra tội phạm kinh tế thuộc Bộ Công an được giao nhiệm vụ tiến hành phát hiện và điều tra tội phạm công nghệ cao, phục hồi, thu thập, giám định chứng cứ điện tử. Tuy nhiên, việc điều tra các loại tội phạm liên quan đến lĩnh vực này của cơ quan Điều tra các cấp còn hạn chế, chưa nhiều do cơ sở vật chất chưa được trang bị đầy đủ và đồng bộ, do vậy ảnh hưởng đến kết luận điều tra các vụ án liên quan đến lĩnh vực này.

Trong công tác truy tố

Do tính chất đặc thù của loại tội phạm này và do điều kiện thực tiễn của các cơ quan thực hành quyền công tố, việc truy tố các hành vi vi phạm pháp luật trong lĩnh vực công nghệ thông tin trong thời gian qua cũng hết sức khó khăn, bởi vì:

- Đây là loại tội mới, tội phạm chủ yếu lợi dụng những khả năng về công nghệ thông tin để phạm tội, do đó, hoạt động thường tinh vi xảo quyệt; việc phát

hiện ra tội phạm đã khó, việc xử lý bằng biện pháp hình sự đối với chúng lại càng khó hơn vì *các quy định của Bộ luật Hình sự đối với loại tội phạm này chưa cụ thể*. Nghiên cứu quy định tại các điều luật đối với các tội phạm về công nghệ thông tin trong Bộ luật Hình sự năm 1999 cho thấy, các quy định chỉ mang tính nguyên tắc chung rất dễ dẫn đến cách hiểu và vận dụng khác nhau trong thực tiễn, trong khi đó đến nay chưa có văn bản hướng dẫn áp dụng pháp luật của các cơ quan có thẩm quyền xác định được phạm vi của "*mạng máy tính*" mà người phạm tội đã lan truyền, phát tán các chương trình vi rút hoặc đưa vào mạng máy tính những thông tin trái với quy định của pháp luật; số lượng máy tính bị làm biến dạng, làm huỷ hoại các dữ liệu để có thể xử lý bằng hình sự theo khoản 1 của các điều luật này; hoặc các thuật ngữ "*gây hậu quả nghiêm trọng*" hoặc "*gây hậu quả rất nghiêm trọng*" hoặc "*đặc biệt nghiêm trọng*"... để xác định khung hình phạt sẽ truy tố, xét xử và quyết định hình phạt. Đây là những vấn đề rất dễ dẫn đến cách hiểu không thống nhất giữa các cơ quan tiến hành tố tụng và đưa đến sự vận dụng khác nhau;

- *Có thể nói các cơ chế của xã hội chưa thật sự vào cuộc để đấu tranh với loại tội phạm này,* thậm chí

ngay cả các cơ quan bảo vệ pháp luật cũng chưa có sự chuẩn bị sẵn sàng đấu tranh với chúng, trừ việc tội phạm hoá các hành vi của chúng. Vì thế, kinh nghiệm đấu tranh với loại tội phạm này của các cơ quan tiến hành tố tụng hầu như chưa có. Ngược lại với xu thế trên thì việc tin học hoá, phổ biến máy vi tính, mạng máy tính đang tăng nhanh trong tất cả các ngành, các lĩnh vực. Trước tình trạng đó, các cơ quan tiến hành tố tụng ở nước ta nếu không có sự chuẩn bị chu đáo trong việc đấu tranh với loại tội phạm này thì sự yếu kém trong hoạt động phòng, chống các tội phạm về công nghệ thông tin là điều không tránh khỏi. Nhu cầu tổ chức việc nghiên cứu, học tập những kiến thức về công nghệ thông tin và cả những kinh nghiệm đấu tranh với loại tội phạm này là rất cấp thiết;

- *Trình độ, khả năng về công nghệ thông tin của các Điều tra viên, Kiểm sát viên và Thẩm phán các cấp còn rất hạn chế.* Phần lớn lực lượng cán bộ này hiện nay có trình độ chuyên môn nghiệp vụ pháp lý sâu và cũng được đào tạo về tin học cơ bản. Nhưng kiến thức về tin học cơ bản đó chủ yếu chỉ để sử dụng trang thiết bị công nghệ thông tin phục vụ cho hoạt động nghiệp vụ và văn phòng; còn kiến thức chuyên sâu về công nghệ thông tin để có thể thực hiện nhiệm vụ phát hiện, điều tra,

truy tố, xét xử các tội phạm về công nghệ thông tin như những tội phạm mà Bộ luật Hình sự năm 1999 đã quy định còn rất hạn chế. Ngay cả khi đã phát hiện ra tội phạm, việc đấu tranh với người phạm tội để chỉ ra hành vi mà người phạm tội đó đã thực hiện là hành vi phạm tội cũng không phải là chuyện đơn giản. Trong khi đó, trước sự phát triển như vũ bão của công nghệ thông tin ngày nay, việc đào tạo nâng cao về công nghệ thông tin cho lực lượng này và ngay cả việc cập nhật có hệ thống của cơ quan quản lý nhà nước về những phát triển mới của công nghệ thông tin để phổ biến rộng rãi cũng chưa thực hiện được.

- *Về công tác nắm và quản lý tin báo tội phạm của ngành Kiểm sát nhân dân:* Hiện nay các tin báo tội phạm chủ yếu được lấy từ cơ quan Công an cùng cấp, chỉ có rất ít tin báo được tiếp nhận từ các cơ quan, tổ chức xã hội khác hoặc qua đơn tố cáo. Chất lượng một số tin báo và việc phân loại, xử lý các tin báo chưa chính xác. Do đó, còn để xảy ra tình trạng bỏ lọt tội phạm không bị xử lý trước pháp luật. Công tác phối kết hợp với các ngành có liên quan để nắm các thông tin về tội phạm còn ở mức độ thấp.

Mặt khác, đối tượng phạm tội, địa điểm phạm tội như trên đã nêu, không chỉ riêng là người Việt Nam

và hành vi phạm tội được thực hiện trên lãnh thổ của Việt Nam, mà người phạm tội có thể là người nước ngoài và thực hiện hành vi phạm tội ở bên ngoài lãnh thổ Việt Nam. Vì vậy, nếu có phát hiện ra người phạm tội thì việc điều tra, đấu tranh và xử lý chúng cũng không hề dễ dàng. Việc đấu tranh, xử lý các vụ việc loại này còn liên quan đến luật pháp quốc tế, luật pháp quốc gia mà người phạm tội là công dân, đến sự hoạt động của lực lượng Cảnh sát quốc tế, sự phối hợp của các cơ quan tư pháp quốc tế khác...

Trong công tác xét xử

Những hành vi phạm pháp nêu trên có những thủ đoạn mới, tinh vi, lợi dụng các tiến bộ của khoa học kỹ thuật. Bộ luật Hình sự năm 1999 đã bổ sung ba tội danh mới về công nghệ thông tin, song chưa có điều luật nào quy định cụ thể về các loại hành vi trên. Vướng mắc nhất trong quá trình xử lý các hành vi vi phạm là khi áp dụng các điều luật trong Bộ luật Hình sự hiện hành vào giải quyết, xử lý thì có nhiều ý kiến, quan điểm khác nhau về định tội danh. *Ví dụ,* trong quá trình xử lý những vụ việc trong lĩnh vực ngân

hàng và bưu chính viễn thông thì quan điểm của cơ quan Điều tra, Viện Kiểm sát không thống nhất về tội danh, sau đó lãnh đạo của ba ngành Công an, Viện Kiểm sát, Toà án đã nhiều lần trực tiếp nghe báo cáo và cuối cùng mới tạm thời thống nhất quan điểm xử lý về tội "*trộm cắp tài sản*" đối với hành vi lắp đặt, sử dụng trái phép thiết bị viễn thông để thu cước điện thoại quốc tế. Tuy nhiên, đến nay vẫn còn nhiều quan điểm khác nhau về tội danh, nhưng chưa có sự thống nhất; các cơ quan Công an, Viện Kiểm sát, Toà án vẫn chưa ban hành được thông tư liên tịch hướng dẫn chính thức về xác định tội danh trong quá trình điều tra, truy tố, xét xử đối với loại hành vi này. Dưới đây là những quan điểm khác nhau trong chính các cơ quan xét xử và của các luật gia ngoài ngành Toà án:

- Xác định tội danh của các hành vi dùng thẻ giả để rút tiền được nêu ở trên, có hai loại ý kiến sau:

Thứ nhất: Xác định việc dùng thẻ giả để rút tiền của người khác tại các ngân hàng là tội "*trộm cắp tài sản*"[1]

[1] Lê Đăng Doanh: *Về định tội danh đối với hành vi làm, sử dụng thẻ tín dụng giả hay các loại thẻ khác để mua hàng hoá hoặc rút tiền tại máy trả tiền tự động của các ngân hàng*, Tạp chí Toà án nhân dân, số 6/2006, tr. 24.

Điều 138 Bộ luật Hình sự năm 1999 quy định: "*Người nào trộm cắp tài sản của người khác có giá trị từ năm trăm nghìn đồng đến dưới năm mươi triệu đồng hoặc dưới năm trăm nghìn đồng nhưng gây hậu quả nghiêm trọng hoặc đã bị xử phạt hành chính về hành vi chiếm đoạt hoặc đã bị kết án về tội chiếm đoạt tài sản, chưa được xoá án tích mà còn vi phạm, thì bị phạt cải tạo không giam giữ đến ba năm hoặc phạt tù từ sáu tháng đến ba năm*". Về mặt khoa học, tội trộm cắp tài sản là hành vi lén lút chiếm đoạt tài sản đang có người khác quản lý. Nếu nhìn về mặt hình thức và đơn giản hoá hành vi phạm tội thì quan niệm này cho rằng, dữ liệu mật mã của thẻ tín dụng được xem như một chìa khoá để mở két bạc. Người trộm cắp thẻ tín dụng và làm thẻ tín dụng giả là quá trình "*chế tạo chìa khoá*". Nếu coi nơi trả tiền tự động của các ngân hàng chỉ là "*két đựng tiền*" thì việc dùng "*chìa khoá - thẻ tín dụng giả*" mở "*két bạc*" của ngân hàng - máy chi trả tiền mặt để lấy tiền hoặc lấy đồ thông qua việc mua bán có thể được coi là "*lén lút*" đối với người quản lý tài sản - các ngân hàng. Trường hợp người phạm tội sử dụng mật mã của thẻ tín dụng thật của người khác để mua hàng hoá qua trang web mua bán trực tuyến hoặc để rút tiền tại các máy rút tiền tự động của ngân

hàng làm cho số tiền trong tài khoản của người có thẻ tín dụng thật mất đi một số tiền nhất định mà người có số tiền đó không hay biết khi có việc chiếm đoạt xảy ra cũng là hành vi phạm tội *"trộm cắp tài sản"*.

Thứ hai: Xác định việc dùng thẻ giả để rút tiền của người khác tại các ngân hàng là tội *"lừa đảo chiếm đoạt tài sản"*[1]. Điều 139 Bộ luật Hình sự năm 1999 quy định: *"Người nào bằng thủ đoạn gian dối chiếm đoạt tài sản của người khác có giá trị từ năm trăm nghìn đồng đến dưới năm mươi triệu đồng hoặc dưới năm trăm nghìn đồng nhưng gây hậu quả nghiêm trọng hoặc đã bị xử phạt hành chính về hành vi chiếm đoạt hoặc đã bị kết án về tội chiếm đoạt tài sản, chưa được xoá án tích mà còn vi phạm, thì bị phạt cải tạo không giam giữ đến ba năm hoặc bị phạt tù từ sáu tháng đến ba năm"*. Vì hành vi dùng mật mã của thẻ tín dụng giả thực hiện việc mua bán trên mạng qua trang web mua bán trực tuyến diễn ra hoàn toàn công khai mà trung tâm quản lý mạng của ngân hàng đều biết có sự giao dịch đang được tiến hành. Trường hợp này không thể coi là hành vi *"lén lút"*

[1] Lê Đăng Doanh: *Tài liệu đã dẫn*, số 6/2006, tr. 26.

được. Hoặc người phạm tội dùng thẻ tín dụng giả, thanh toán trực tiếp với cơ sở bán hàng cũng diễn ra công khai trước mắt người bán hàng và do tin rằng thẻ tín dụng đó là thật nên mới giao hàng hoá cho người phạm tội. Do đó cũng không thể coi các trường hợp này là hành vi *"lén lút"* chiếm đoạt tài sản. Với những người dùng thẻ tín dụng giả tại các máy rút tiền tự động, về thực chất *"thẻ giả"* nhưng chứa đựng toàn bộ các thông tin dữ liệu như thẻ thật 100%. Do vậy mới làm cho cơ quan ngân hàng - máy rút tiền tự động tin là thẻ thật nên đã giao tiền. Với các trường hợp chiếm đoạt tài sản nêu trên thì việc xác định tội danh là *"trộm cắp tài sản"* cũng có những yếu tố bất hợp lý, không phản ánh đúng được bản chất của hành vi phạm tội.

Nếu đánh giá một cách tổng quát, người phạm tội bằng nhiều thủ đoạn gian dối để có được số mật mã của thẻ tín dụng thật của khách hàng và công đoạn cuối cùng là dùng thẻ tín dụng giả để rút tiền... hay mua hàng hoá qua mạng Internet đã thể hiện đầy đủ bản chất của tội lừa đảo, đó là *"bằng thủ đoạn gian dối chiếm đoạt tài sản..."*. Gian dối với chính người quản lý tài sản là các ngân hàng, các cơ sở phát hành

các loại thẻ tín dụng. Bởi do hành vi gian dối - làm thẻ tín dụng giả mới tạo nên sự nhầm lẫn của hệ thống máy tính - người quản lý tài sản đã được tự động hoá... Hơn nữa, về mặt chủ quan, người chiếm đoạt tài sản biết rõ hành vi rút được tiền của ngân hàng, hay mua được hàng hoá là kết quả của sự gian dối. Do vậy, có thể thấy sự thống nhất giữa mặt khách quan với yếu tố chủ quan của người phạm tội. Vì thế, loại ý kiến này cho rằng, định tội danh *"lừa đảo chiếm đoạt tài sản"* theo quy định tại Điều 139 Bộ luật Hình sự năm 1999 là phù hợp.

- Xác định tội danh của các hành vi lắp đặt, thuê kênh riêng, sử dụng dịch vụ viễn thông được nêu trên:

+ *Về việc xác định tội danh.*

Một là, truy tố, xét xử về tội *"kinh doanh trái phép"*. Những người theo quan điểm này dựa trên lập luận: Những hành vi trên thực chất là thực hiện dịch vụ truyền lưu lượng điện thoại từ nước ngoài vào Việt Nam. Theo điểm 7 Điều 4 Pháp lệnh Bưu chính viễn thông ngày 25/5/2002, đây là loại hình dịch vụ viễn thông quốc tế. Theo quy định tại Điều 5 Pháp lệnh này, các thành phần kinh tế được Nhà nước khuyến khích kinh doanh với đầy đủ các loại hình dịch vụ.

Thực tế hiện nay Nhà nước đã mở cửa thị trường viễn thông, cho phép nhiều doanh nghiệp tham gia cung cấp dịch vụ viễn thông, xoá bỏ độc quyền.

Để thực hiện hoạt động kinh doanh dịch vụ viễn thông quốc tế, các chủ thể phải có những điều kiện nhất định và phải được cơ quan quản lý về viễn thông cấp phép. Trong các vụ việc đã được khám phá, các đối tượng đã phải bỏ vốn đầu tư, bỏ công sức, mua sắm, lắp đặt trang thiết bị viễn thông để thu lợi nhuận. Đây thực chất là kinh doanh nhưng không xin phép mà lén lút kinh doanh nên được coi là kinh doanh trái phép.

Hành vi kinh doanh trái phép đó là nguy hiểm cho xã hội, đã thu được số tiền rất lớn. So với những hành vi kinh doanh thông thường khác, những hành vi này còn nguy hiểm hơn bởi chúng không chỉ xâm phạm đến trật tự quản lý kinh tế, mà còn xâm phạm đến an ninh lãnh thổ của Việt Nam, an toàn công cộng nơi xảy ra tội phạm. Do đó, cần truy tố, xét xử về tội "*kinh doanh trái phép*" theo Điều 159 Bộ luật Hình sự năm 1999.

Hai là, truy tố, xét xử về tội "*vi phạm các quy định về nghiên cứu, thăm dò, khai thác tài nguyên*" (Điều 172

Bộ luật Hình sự năm 1999). Những người theo quan điểm này lập luận: Bản chất của các hành vi đó là việc khai thác trái phép phổ tần số vô tuyến điện. Các đối tượng đã lợi dụng sự sơ hở trong quản lý dịch vụ viễn thông quốc tế, lợi dụng các tiến bộ khoa học kỹ thuật và sự thiếu thiết bị cũng như kinh nghiệm trong kiểm soát, phát hiện vi phạm của lực lượng chuyên ngành để khai thác và sử dụng trái phép phổ tần số vô tuyến điện nhằm thu lợi nhuận. Mà phổ tần số vô tuyến điện theo quy định của Nhà nước là tài nguyên cần được khai thác, sử dụng theo kế hoạch.

Ba là, truy tố, xét xử về tội "*sử dụng trái phép tài sản*" (Điều 142 Bộ luật Hình sự năm 1999). Những người có ý kiến này cho rằng: các hành vi trên đều có mục đích vụ lợi, đều khai thác, sử dụng phổ tần số vô tuyến điện là tài nguyên quốc gia, sử dụng cả mạng điện thoại công cộng. Phổ tần số vô tuyến điện và mạng điện thoại công cộng là phương tiện, tài sản mà người quản lý, sở hữu là những người đang được phép khai thác lợi ích của chúng. Qua việc sử dụng phổ tần số vô tuyến điện và mạng điện thoại công cộng, những người này đã thu những khoản lợi nhuận lớn, gây thất thu cho chủ thể được phép quản lý, khai thác,

gây hậu quả nghiêm trọng. Do đó, các hành vi này phạm tội "*sử dụng trái phép tài sản*" quy định tại Điều 142 Bộ luật Hình sự năm 1999.

Bốn là, truy tố, xét xử về tội "*trộm cắp tài sản*". Những người theo quan điểm này lập luận: Tần số vô tuyến điện được coi là quyền tài sản, do đó, là một dạng tài sản. Tài sản này đang có chủ, do Bộ Bưu chính Viễn thông quản lý. Các đối tượng đã lén lút lắp đặt các thiết bị viễn thông và sử dụng trái phép phổ tần số vô tuyến điện để chiếm đoạt cước điện thoại là phạm tội "*trộm cắp tài sản*". Nhà nước ta phải thuê vệ tinh địa tĩnh của nước ngoài để phát triển dịch vụ viễn thông trong nước. Giải tần số vô tuyến điện, quỹ đạo vệ tinh địa tĩnh thuộc chủ quyền của Việt Nam, là tài nguyên và tài sản của Nhà nước Việt Nam, đại diện là Tổng Công ty Bưu chính Viễn thông Việt Nam. Nhà nước ta phải bỏ tiền thuê phạm vi giải tần số vô tuyến điện, phạm vi giải tần số vô tuyến điện này ở trong mạng lưới viễn thông quốc gia. Khi sử dụng tần số vô tuyến điện thì phải trả tiền tương ứng với thời gian sử dụng. Số tiền này các đối tượng không trả cho cơ quan nhà nước mà chiếm đoạt, nghĩa là xâm phạm đến quyền sở hữu tài sản.

Năm là, có ý kiến cho rằng, những hành vi trên không thoả mãn đầy đủ dấu hiệu của một cấu thành tội phạm nào trong phần các tội phạm của Bộ luật Hình sự. Do đó, dù các hành vi này là nguy hiểm cho xã hội, nhưng cũng chỉ xử lý về hành chính, không được áp dụng tương tự quy định pháp luật hình sự để truy tố, xét xử vì Điều 2 Bộ luật Hình sự năm 1999 quy định: "*Chỉ người nào phạm một tội đã được Bộ luật Hình sự quy định mới phải chịu trách nhiệm hình sự*".

4. Các quy định pháp luật về phòng, chống tội phạm trong lĩnh vực công nghệ thông tin ở nước ta

Hành vi vi phạm pháp luật trong lĩnh vực công nghệ thông tin thường gây hậu quả rất nghiêm trọng. Các hành vi này không chỉ đơn thuần làm cho Nhà nước thất thu tiền mà còn đe doạ đến công tác đảm bảo an ninh, trật tự. Do đó, cuộc đấu tranh này nếu không được quan tâm đúng mức, thiếu chủ trương, chính sách đúng đắn, kịp thời và không thực hiện đồng bộ các giải pháp mang tính khả thi thì sẽ không đủ khả năng để ngăn chặn, đẩy lùi vi phạm pháp luật trong lĩnh vực công nghệ thông tin. Điều này chính là nhân tố góp phần gây mất ổn định chính trị - xã hội.

Trong Chiến lược phát triển kinh tế - xã hội tới

năm 2010 của Đại hội Đảng toàn quốc lần thứ IX đã đề ra mục tiêu phát triển công nghệ thông tin: "*Phát triển mạnh thương mại, nâng cao năng lực và chất lượng hoạt động để mở rộng thị trường trong nước và hội nhập quốc tế có hiệu quả... Phát triển thương mại điện tử, nhà nước, các hiệp hội, các doanh nghiệp phối hợp tìm kiếm, mở rộng thị trường cho sản phẩm Việt Nam*". Trong Chỉ thị số *58-CT/TW* ngày 17/10/2000 về việc đẩy mạnh ứng dụng và phát triển công nghệ thông tin phục vụ sự nghiệp công nghiệp hoá, hiện đại hoá, Bộ Chính trị cũng yêu cầu: "*Tập trung phát triển các dịch vụ điện tử trong các lĩnh vực tài chính (thuế, kho bạc, kiểm toán..., ngân hàng, hải quan, hàng không, thương mại, thương mại điện tử và các dịch vụ công cộng... đảm bảo các điều kiện cần thiết phù hợp với tiến độ hội nhập kinh tế khu vực và quốc tế*".

Quyết định số 246/2005/QĐ-TTg ngày 06/10/2005 của Thủ tướng Chính phủ về việc phê duyệt Chiến lược phát triển công nghệ thông tin và truyền thông Việt Nam đến năm 2010 và định hướng đến năm 2020 đề ra mục tiêu của chiến lược đến năm 2010 là "*Ứng dụng rộng rãi công nghệ thông tin và truyền thông trong các ngành, lĩnh vực trọng điểm của nền kinh tế.*

Hình thành, xây dựng và phát triển Việt Nam điện tử với công dân điện tử, Chính phủ điện tử, doanh nghiệp điện tử, giao dịch và thương mại điện tử để Việt Nam đạt trình độ trung bình khá trong khu vực ASEAN. Công nghiệp công nghệ thông tin và truyền thông trở thành ngành công nghiệp mũi nhọn có tốc độ tăng trưởng 20% - 25%/năm, đạt tổng doanh thu khoảng 6 - 7 tỷ USD vào năm 2010".

Định hướng phát triển đến 2015 và tầm nhìn đến 2020: "*Ứng dụng rộng rãi công nghệ thông tin và truyền thông trong mọi lĩnh vực, khai thác có hiệu quả thông tin và tri thức trong tất cả các ngành... Hình thành xã hội thông tin. Công nghiệp công nghệ thông tin và truyền thông có tốc độ tăng trưởng trên 20%/năm, đạt tổng doanh thu khoảng 15 tỷ USD*".

Tầm nhìn 2020: "*Với công nghệ thông tin và truyền thông làm nòng cốt Việt Nam chuyển đổi nhanh cơ cấu kinh tế - xã hội trở thành một nước có trình độ tiên tiến về phát triển kinh tế tri thức và xã hội thông tin, góp phần quan trọng thực hiện thắng lợi sự nghiệp công nghiệp hoá, hiện đại hoá đất nước*".

Nhận thức đúng đắn tầm quan trọng của cuộc đấu tranh chống vi phạm pháp luật nói chung và vi phạm

pháp luật trong lĩnh vực công nghệ thông tin nói riêng, thời gian qua Đảng và Nhà nước ta luôn quan tâm đến việc chỉ đạo công tác phòng ngừa và đấu tranh chống vi phạm pháp luật. Nhiều văn bản quan trọng thể hiện rõ tư tưởng chỉ đạo của Đảng và Nhà nước về cuộc đấu tranh này đã được ban hành và triển khai trên thực tiễn, cụ thể:

- Nghị định số 55/2001/NĐ-CP ngày 23/8/2001 của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ Internet (Nghị định số 55/2001/NĐ-CP) quy định như sau: "*Thông tin đưa vào lưu trữ, truyền đi và nhận đến trên Internet phải tuân thủ các quy định tương ứng của Luật Báo chí, Luật Xuất bản, Pháp lệnh Bảo vệ bí mật nhà nước và các quy định của pháp luật về sở hữu trí tuệ và quản lý thông tin trên Internet*" (Điều 6); "*Bí mật đối với các thông tin riêng trên Internet của tổ chức, cá nhân được bảo đảm theo quy định của Hiến pháp và pháp luật*" (Điều 8); Nghiêm cấm các hành vi "*gây rối, phá hoại hệ thống thiết bị và cản trở việc cung cấp, sử dụng các dịch vụ Internet; đánh cắp và sử dụng trái phép mật khẩu, khoá mật mã và thông tin riêng trên Internet của các tổ chức, cá nhân*" (Điều 11).

- Pháp lệnh số 43/2002/PL-UBTVQH10 ngày

25/5/2002 về bưu chính, viễn thông quy định một số điều về an toàn, an ninh, bảo đảm bí mật thông tin như sau:

> *"Bảo vệ an toàn mạng bưu chính, mạng viễn thông và an ninh thông tin là trách nhiệm của mọi tổ chức, cá nhân.*
>
> *Cơ quan, tổ chức, doanh nghiệp phải áp dụng các biện pháp bảo đảm an toàn mạng bưu chính, mạng viễn thông của mình và an ninh thông tin" (Điều 6);*
>
> *"Bí mật đối với thông tin riêng chuyển qua mạng bưu chính, mạng viễn thông của mọi tổ chức, cá nhân được bảo đảm theo quy định của pháp luật.*
>
> ...
>
> *Tổ chức, cá nhân vi phạm pháp luật nghiêm trọng, gây ảnh hưởng xấu đến quốc phòng, an ninh thì bị tạm đình chỉ hoặc đình chỉ cung cấp dịch vụ bưu chính viễn thông theo quy định của Chính phủ"(Điều 9).*

Pháp lệnh này quy định nghiêm cấm các hành vi:

> *"Phá hoại các công trình bưu chính, viễn*

thông hoặc cản trở hoạt động hợp pháp về bưu chính, viễn thông;

Thu trộm, nghe trộm tin trên mạng viễn thông; trộm cắp, sử dụng trái phép mật khẩu, khoá mật mã và thông tin riêng của tổ chức, cá nhân khác;

Cung cấp, sử dụng dịch vụ bưu chính, viễn thông hoặc sử dụng tần số vô tuyến điện và thiết bị vô tuyến điện, thiết bị bưu chính, viễn thông nhằm mục đích chống lại Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam, gây rối an ninh, trật tự, an toàn xã hội, vi phạm thuần phong mỹ tục của dân tộc, hoạt động buôn lậu hoặc có hành vi khác vi phạm pháp luật về bưu chính, viễn thông"(Điều 10).

- Nghị định số 160/2004/NĐ-CP ngày 03/9/2004 quy định chi tiết một số điều của Pháp lệnh Bưu chính, Viễn thông về viễn thông như sau:

"... Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn mạng viễn thông và an ninh thông tin;... thực hiện các yêu cầu về bảo đảm an toàn mạng viễn thông và an

ninh thông tin của các cơ quan nhà nước có thẩm quyền.

Bộ Bưu chính Viễn thông phối hợp với Bộ Công an và các cơ quan có liên quan hướng dẫn việc bảo đảm an toàn mạng viễn thông và an ninh thông tin trong hoạt động viễn thông" (Điều 3).

"Cơ quan, tổ chức, cá nhân tham gia hoạt động viễn thông phải... chịu trách nhiệm trước pháp luật về nội dung thông tin mà mình đưa vào, lưu trữ và truyền đi trên mạng viễn thông.

... Nghiêm cấm việc nghe trộm, thu trộm thông tin trên mạng viễn thông, trộm cắp, sử dụng trái phép mật khẩu, khoá mật mã và thông tin riêng của các tổ chức, cá nhân" (Điều 4).

- Ngày 16 tháng 12 năm 2004, Bộ Bưu chính Viễn thông đã ban hành Thông tư số 05/2004/TT-BBCVT hướng dẫn thực hiện một số điều về xử lý vi phạm hành chính và khiếu nại, tố cáo quy định tại Chương IV Nghị định số 55/2001/NĐ-CP của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ Internet. Tại

Mục II của thông tư này quy định 09 hành vi vi phạm trong lĩnh vực công nghệ thông tin bị xử lý hành chính như: không khai báo làm thủ tục cấp lại giấy phép cung cấp dịch vụ Internet bị mất hoặc bị hư hỏng; vi phạm quy định của Nhà nước về quản lý, truy cập, kết nối Internet trong việc sử dụng Internet; vi phạm các quy định của Nhà nước về an toàn, an ninh thông tin trên Internet trong việc sử dụng dịch vụ Internet; sử dụng quá hạn giấy phép cung cấp dịch vụ Internet; vi phạm các quy định của Nhà nước về tiêu chuẩn, chất lượng dịch vụ Internet trong việc cung cấp dịch vụ Internet; vi phạm các quy định của Nhà nước về giá, cước dịch vụ Internet trong việc cung cấp dịch vụ Internet; vi phạm các quy định của Nhà nước về quản lý tài nguyên Internet trong việc cung cấp và sử dụng dịch vụ Internet; vi phạm các quy định của Nhà nước về quản lý truy cập, kết nối Internet trong việc cung cấp dịch vụ Internet; vi phạm các quy định của Nhà nước về an toàn, an ninh thông tin trên Internet trong việc cung cấp dịch vụ Internet.

Theo quy định của Thông tư này, *những đối tượng có thể bị áp dụng các biện pháp xử phạt là:* tổ chức, cá nhân trong nước, tổ chức, cá nhân nước ngoài hoạt

động trong lĩnh vực Internet tại Việt Nam, bao gồm: doanh nghiệp cung cấp dịch vụ Internet; đơn vị cung cấp dịch vụ truy cập Internet dùng riêng; đại lý cung cấp dịch vụ Internet; tổ chức, cá nhân sử dụng dịch vụ truy cập, kết nối, ứng dụng Internet trong bưu chính, viễn thông; doanh nghiệp cung cấp dịch vụ bưu chính, viễn thông liên quan đến hoạt động Internet và các doanh nghiệp, đại lý cung cấp dịch vụ ứng dụng Internet khác và người sử dụng dịch vụ Internet khác không thuộc lĩnh vực bưu chính viễn thông như thông tin, thương mại, ngân hàng...

Với lĩnh vực quản lý tài nguyên Internet, nếu trong quá trình cung cấp và sử dụng dịch vụ Internet các tổ chức, cá nhân có các hành vi vi phạm như chuyển nhượng, cho thuê, bán lại tên miền, địa chỉ (IP) và số hiệu mạng Internet; sử dụng tên miền cấp cao khác tên miền "*.vn*" mà không thông báo cho cơ quan quản lý tài nguyên Internet; các cơ quan, tổ chức của hệ thống chính trị sử dụng tên miền khác tên miền cấp cao "*.vn*" hoặc không lưu giữ trong máy chủ có địa chỉ IP ở Việt Nam; báo điện tử không sử dụng tên miền cấp cao "*.vn*"; sử dụng tên miền để truyền bá các thông tin trái với quy định của pháp luật... đều bị xử phạt hành chính.

- Thông tư liên tịch số 02/2005/TTLT-BCVT-VHTT-CA-KHĐT ngày 14/7/2005 giữa Bộ Bưu chính Viễn thông, Bộ Văn hoá Thông tin, Bộ Công an, Bộ Kế hoạch và Đầu tư, về quản lý đại lý Internet hoạt động kinh doanh tại Việt Nam quy định đối tượng điều chỉnh của Thông tư bao gồm: doanh nghiệp cung cấp dịch vụ truy cập Internet, doanh nghiệp cung cấp dịch vụ ứng dụng Internet trong bưu chính, viễn thông, đại lý Internet và người sử dụng dịch vụ Internet tại đại lý.

Thông tư cũng quy định rõ: cấm các đối tượng này dùng Internet để lưu giữ tin, tài liệu, số liệu thuộc bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp luật nước ta quy định; sử dụng hoặc hướng dẫn người khác sử dụng công cụ hỗ trợ để truy cập vào các trang thông tin trên Internet (trang web) do cơ quan quản lý nhà nước có thẩm quyền cấm truy cập; gửi, lan truyền, phát tán vi rút tin học, chương trình phần mềm có tính năng lấy trộm thông tin, phá huỷ dữ liệu máy tính lên mạng Internet; làm rối loạn, cản trở hoạt động cung cấp, sử dụng dịch vụ Internet; lợi dụng dịch vụ Internet để chống lại Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam, gây rối loạn an ninh trật tự, xâm hại đến lợi ích của các cơ quan, tổ chức, cá nhân; vi phạm đạo đức,

thuần phong mỹ tục; xây dựng các trang Web, tổ chức các diễn đàn trên Internet có nội dung hướng dẫn, lôi kéo, kích động người khác thực hiện các hành vi trên; truy cập đến các nhà cung cấp dịch vụ Internet nước ngoài bằng việc quay số điện thoại trực tiếp.

- Ngày 29 tháng 11 năm 2005, Quốc hội thông qua Luật số 51/2005/QH11 về giao dịch điện tử. Luật này điều chỉnh về các hành vi giao dịch điện tử trong hoạt động của các cơ quan nhà nước; trong lĩnh vực dân sự, kinh doanh, thương mại... Điều 9 của Luật quy định về *các hành vi bị nghiêm cấm trong giao dịch điện tử gồm:* cản trở việc lựa chọn sử dụng giao dịch điện tử; cản trở hoặc ngăn chặn trái phép quá trình truyền, gửi, nhận thông điệp dữ liệu; thay đổi, xoá, huỷ, giả mạo, sao chép, tiết lộ, hiển thị, di chuyển trái phép một phần hoặc toàn bộ thông điệp dữ liệu; tạo ra hoặc phát tán chương trình phần mềm làm rối loạn, thay đổi, phá hoại hệ thống điều hành hoặc có hành vi khác nhằm phá hoại hạ tầng công nghệ về giao dịch điện tử; tạo ra thông điệp dữ liệu nhằm thực hiện hành vi trái pháp luật; gian lận, mạo nhận, chiếm đoạt hoặc sử dụng trái phép chữ ký điện tử của người khác. Luật này quy định một chương riêng (Chương VI) về an ninh, an toàn, bảo vệ, bảo mật trong giao dịch điện

tử, gồm 6 điều: Bảo đảm an ninh, an toàn trong giao dịch điện tử (Điều 44); Bảo vệ thông điệp dữ liệu (Điều 45); Bảo mật thông tin trong giao dịch điện tử (Điều 46); Trách nhiệm của tổ chức cung cấp dịch vụ mạng (Điều 47); Trách nhiệm của cơ quan, tổ chức, cá nhân khi có yêu cầu của cơ quan nhà nước có thẩm quyền (Điều 48); Quyền và trách nhiệm của cơ quan nhà nước có thẩm quyền (Điều 49).

- Bộ luật Hình sự năm 1999 đã dành 03 điều quy định các hành vi vi phạm pháp luật trong lĩnh vực này. Đó là:

"*Tội tạo ra và lan truyền các chương trình vi - rút tin học*" (Điều 224). Quy định này nhằm xử lý hình sự đối với bất cứ người nào có hành vi cố ý tạo ra và cố ý lan truyền, phát tán các chương trình vi rút qua mạng máy tính hoặc bằng phương thức khác để gây rối loạn hoạt động, phong toả hoặc làm biến dạng, làm huỷ hoại mạng máy tính điện tử;

"*Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử*" (Điều 225). Quy định này nhằm xử lý hình sự đối với những người sử dụng mạng máy tính mà có hành vi vi phạm các quy định về vận hành, khai thác, sử dụng tức là tác nghiệp

không đúng quy định hoặc đưa vào mạng những thông tin không đúng quy định dẫn đến hậu quả làm rối loạn hoạt động, phong toả hoặc làm biến dạng, làm huỷ hoại các dữ liệu của một hoặc nhiều máy tính;

"*Tội sử dụng trái phép thông tin trên mạng và trong máy tính*" (Điều 226). Quy định này nhằm xử lý hình sự những người không được phép sử dụng thông tin trên mạng và trong máy tính mà vẫn sử dụng hoặc được phép sử dụng những thông tin trên mạng nhưng không chấp hành theo đúng những quy định của pháp luật và quy định trong máy tính.

Để nâng cao hiệu quả của cuộc đấu tranh, trong những năm qua, chúng ta đã chú trọng thực hiện đồng bộ các giải pháp (tuy nhiên mới chỉ là bước đầu) nhằm thực hiện tốt hai nhiệm vụ: phát hiện, xử lý kịp thời vi phạm pháp luật và các biện pháp phòng ngừa có hiệu quả. Cụ thể, ngoài việc tăng cường xử lý bằng biện pháp hành chính và hình sự đối với vi phạm pháp luật trong lĩnh vực này, Nhà nước đã chú trọng đến việc hoàn thiện hệ thống pháp luật (Luật Công nghệ thông tin đã được trình Quốc hội xem xét, thông qua)... Việc tăng cường hiệu quả các biện pháp kinh tế - xã hội, tăng cường công tác tuyên truyền, giáo dục ý

thức pháp luật cho mọi đối tượng trong xã hội cũng được đặt ra thành yêu cầu cấp thiết, vì như nhận xét của một nhà chuyên môn thì: *"Về mặt chuyên môn, hacker rõ ràng là người có hiểu biết tốt về mạng, tuy nhiên đa phần là trẻ tuổi nên có tâm lý muốn thể hiện mình mà chưa nhận thức được cái nào nên làm, cái nào không nên làm. Chính vì vậy mà chúng ta cần có biện pháp giáo dục cho đối tượng này vào những việc nên làm..."*[1].

Qua nghiên cứu tình hình và các quy định pháp luật phòng, chống tội phạm trong lĩnh vực công nghệ thông tin ở nước ta, chúng tôi rút ra *một số nhận xét sau đây:*

- Các quy định pháp luật trong lĩnh vực này chưa nhiều và nằm rải rác ở các hình thức văn bản khác nhau như: bộ luật, luật, pháp lệnh, nghị định và các thông tư;

- Vi phạm trong lĩnh vực công nghệ thông tin rất đa dạng và xảy ra hầu như trong tất cả các lĩnh vực của đời sống xã hội và phức tạp với nhiều cấp độ khác

[1] Đỗ Xuân Thọ - Chủ tịch Hội tin học Việt Nam, Tổng Cục trưởng Tổng cục Khoa học kỹ thuật - Bộ Công an.

nhau, trong khi đó, Bộ luật Hình sự năm 1999 mới chỉ quy định 03 tội danh rất chung chung về lĩnh vực này;

- Thực tiễn điều tra, truy tố và xét xử những năm qua cho thấy, các tội được quy định trong Bộ luật Hình sự năm 1999 xét xử không nhiều, trong khi đó, các tội phạm liên quan trong lĩnh vực truyền thông và thương mại điện tử khá nhiều. Vì vậy, trong quá trình áp dụng pháp luật đã gây không ít khó khăn cho các cơ quan tiến hành tố tụng trong việc định tội danh;

- Một số vấn đề lý luận về chủ thể, vấn đề chứng cứ thực hiện hành vi phạm tội cũng như định lượng hậu quả do tội phạm trong lĩnh vực công nghệ thông tin gây ra còn gây nhiều tranh luận khác nhau. Vì vậy, cần phải có những nghiên cứu sâu hơn về những vấn đề này;

- Vai trò nòng cốt của cơ quan bảo vệ pháp luật chưa được phát huy nên chưa đáp ứng yêu cầu của cuộc đấu tranh. Trình độ nhận thức và hiểu biết về lĩnh vực này của cán bộ các cơ quan bảo vệ pháp luật còn hạn chế, dẫn đến bỏ lọt nhiều hành vi vi phạm pháp luật. Bởi đúng như tên gọi của nó: "*tội phạm công nghệ cao*", để đấu tranh phòng, chống loại tội phạm này, đòi hỏi những người làm công tác bảo vệ

pháp luật phải am hiểu sâu sắc về công nghệ thông tin. Hiện nay, một thực trạng đặt ra là, tuy có dấu hiệu vi phạm pháp luật về lĩnh vực này, nhưng do trình độ hiểu biết của Cơ quan điều tra quá hạn chế so với trình độ của kẻ phạm tội nên rất khó tìm ra đủ chứng cứ để xử lý. *Ví dụ,* người phạm tội mang theo các thiết bị sử dụng vào mục đích phạm tội ngang nhiên qua đường hải quan nhưng cơ quan Hải quan không phát hiện được vì không biết các phương tiện đó có thể sử dụng vào việc gì;

- Trang thiết bị, kỹ thuật của cơ quan bảo vệ pháp luật còn quá lạc hậu so với phương tiện của người phạm tội. Điều này cũng ảnh hưởng rất lớn tới kết quả điều tra, xử lý loại tội phạm này, đặc biệt là khi có yêu cầu trưng cầu giám định, bởi nội dung giám định về cơ bản là xác định tính năng kỹ thuật của các thiết bị, phương tiện mà đối tượng sử dụng để phạm tội. Điều này đòi hỏi số cán bộ làm công tác giám định phải am hiểu chuyên môn và có thiết bị, kỹ thuật hiện đại để thực thi công việc;

- Việc tăng cường hợp tác quốc tế trong đấu tranh chống vi phạm pháp luật nói chung và tội phạm nói riêng vẫn còn nhiều hạn chế. Hiện nay, do tác động

mạnh mẽ của quá trình giao lưu quốc tế trên nhiều lĩnh vực, đặc biệt là lĩnh vực công nghệ thông tin nên cuộc đấu tranh chống vi phạm pháp luật về công nghệ thông tin không còn là vấn đề của riêng mỗi quốc gia, mỗi khu vực mà trở thành vấn đề toàn cầu. Cuộc đấu tranh này nếu chỉ tiến hành đơn lẻ, không có sự hợp tác quốc tế chặt chẽ thì khó có thể đem lại hiệu quả cao.

Từ những vấn đề nêu trên cho thấy, để đấu tranh phòng, chống một cách có hiệu quả các hành vi vi phạm pháp luật trong lĩnh vực công nghệ thông tin, cần phải tiến hành đồng bộ hàng loạt các công việc cụ thể không chỉ đối với cơ quan quản lý, mà còn đối với cơ quan bảo vệ pháp luật.

Chương III

QUAN ĐIỂM VÀ GIẢI PHÁP ĐẤU TRANH PHÒNG, CHỐNG TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN Ở NƯỚC TA

Trong những năm qua, sự phát triển mạnh mẽ của công nghệ thông tin đã làm thay đổi cuộc sống của người dân, tạo cơ hội mới cho sự phát triển kinh tế - xã hội. Tuy nhiên, công nghệ thông tin cũng bộc lộ những mặt tiêu cực của nó, đặc biệt là trong xu thế hội nhập ngày càng mở rộng, các tiến bộ về khoa học kỹ thuật trong lĩnh vực này sẽ thâm nhập ngày càng nhiều vào Việt Nam. Sự thâm nhập này cũng đồng nghĩa với việc nảy sinh những phức tạp mới và tình hình vi phạm pháp luật trong lĩnh vực công nghệ thông tin trong thời gian tới sẽ có chiều hướng gia tăng. Từ đó, yêu cầu đặt ra là phải có các giải pháp đồng bộ để đấu tranh phòng, chống loại vi phạm pháp luật này một cách hiệu quả.

TỘI PHẠM
TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN

I. QUAN ĐIỂM ĐẤU TRANH PHÒNG, CHỐNG TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN

Những năm gần đây, Chính phủ đã có nhiều biện pháp cấp bách tăng cường bảo vệ an ninh, trật tự an toàn xã hội trong tình hình mới nhưng tình hình tội phạm ở nước ta vẫn có có xu hướng gia tăng và diễn biến phức tạp. Cơ cấu thành phần tội phạm có những thay đổi, đối tượng phạm tội là người lao động chiếm 70%, số thanh niên phạm tội chiếm tỷ lệ ngày càng cao. Đặc biệt là tình hình phạm tội có tổ chức như tham nhũng, xâm hại trẻ em, công nghệ thông tin... diễn biến phức tạp gây hậu quả nghiêm trọng, gây tâm lý bất an trong xã hội. Đứng trước thực trạng như vậy, ngày 31/7/1998 Chính phủ đã ban hành Nghị quyết số 09/1998/NQ-CP về tăng cường công tác phòng, chống tội phạm trong tình hình mới, theo đó chủ trương, biện pháp để chống lại tội phạm liên quan đến lĩnh vực công nghệ thông tin là "*...; tăng cường sự hợp tác quốc tế trong phòng, chống tội phạm theo nguyên tắc phù hợp với pháp luật hiện hành của nước ta và pháp luật quốc tế, phù hợp với các chương trình chống tội phạm của Liên hợp quốc và Tổ chức cảnh sát hình sự quốc tế Interpol*". Cụ thể hoá Nghị quyết, Thủ tướng Chính phủ đã ban hành Quyết định số

138/1998/QĐ-TTg ngày 31/7/1998 về việc phê duyệt Chương trình quốc gia phòng, chống tội phạm, với nội dung " *...; đấu tranh chống các loại tội phạm có tổ chức quốc tế...; tổ chức thực hiện hợp tác quốc tế trong lĩnh vực phòng, chống tội phạm, nhất là chống các tội phạm có tính quốc tế và tội phạm là người Việt Nam ở nước ngoài; xây dựng và hoàn thiện các văn bản quy phạm pháp luật về phòng, chống tội phạm đáp ứng đòi hỏi của thực tiễn*". Tiếp đó, ngày 02/6/2005 Bộ Chính trị đã ban hành Nghị quyết số 49/NQ-TW về Chiến lược cải cách tư pháp đến năm 2020 cho phù hợp với công tác lập pháp và chương trình cải cách hành chính, nhiệm vụ của Chiến lược là "... *Quy định là tội phạm đối với những hành vi nguy hiểm cho xã hội mới xuất hiện trong quá trình phát triển kinh tế - xã hội, khoa học, công nghệ và hội nhập quốc tế*" và "*Tổ chức thực hiện tốt các điều ước quốc tế mà Nhà nước ta đã tham gia. Tiếp tục ký kết hiệp định tương trợ tư pháp với các nước khác, trước hết là với các nước láng giềng, các nước trong khu vực và các nước có quan hệ truyền thống. Tăng cường sự phối hợp chung trong hoạt động phòng ngừa và đấu tranh chống tội phạm có yếu tố quốc tế và khủng bố quốc tế với các tổ chức Interpol, Aseanpol,... với cảnh sát các nước láng giềng và khu*

vực, với cảnh sát một số quốc gia có nhiều công dân Việt Nam sinh sống, lao động, học tập".

Như vậy, các nghị quyết của Đảng, Nhà nước ta đã thể hiện những quan điểm cơ bản tạo cơ sở cho việc đấu tranh phòng, chống tội phạm trong tình hình mới, trong đó có tội phạm trong lĩnh vực công nghệ thông tin. Những quan điểm về hợp tác quốc tế trong phòng, chống tội phạm; huy động sự tham gia của các nguồn lực xã hội; đề cao tính phòng ngừa; hoàn thiện pháp luật đã được thể hiện rõ nét trong quá trình đấu tranh phòng, chống tội phạm nói chung và tội phạm trong lĩnh vực công nghệ thông tin nói riêng.

II. CÁC GIẢI PHÁP ĐẤU TRANH PHÒNG, CHỐNG TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN

1. Về thiết chế

Vài năm trở lại đây, chúng ta dường như vui mừng trước sự phát triển như vũ bão của công nghệ thông tin trong nước mà quên đi những bất cập trong việc bảo mật thông tin và đảm bảo an ninh mạng. Thực chất, đây là vấn đề không mới và nhiều quốc gia đã gặp phải nhưng trong khi các quốc gia khác nhanh chóng khắc phục một cách hiệu quả thì Việt Nam lại

"*chậm chạp*" trong việc khắc phục những bất cập này. *Trước hết,* vấn đề này là do nhận thức, bởi một sai lầm rất phổ biến trong suy nghĩ của một số người có Website không đánh giá đúng giá trị bảo mật thông tin. Họ cho rằng thông tin trên website của họ không đáng giá, không thực sự quan trọng và cũng ít lượng truy cập nên không cần thiết phải làm bảo mật một cách chuyên nghiệp. Những người có website cũng không lường được rằng, có thể thông tin bình thường được đăng tải không thật quan trọng, nhưng nếu bị kẻ xấu lợi dụng, chẳng hạn như làm thay đổi, xuyên tạc thông tin, thì hậu quả sẽ vô cùng lớn... *Thứ hai,* công tác bảo mật hoặc an ninh mạng là rất quan trọng nhưng hiện nay chúng ta thiếu nguồn nhân lực. Tại một số trường đại học của nước ta chưa có hệ chính quy bậc đại học và sau đại học để đào tạo nguồn nhân lực cho công tác bảo mật hoặc an ninh mạng. Những người có khả năng trong lĩnh vực này hầu như là tự học hỏi, tự rèn luyện từ công việc thực tế và những người có chứng chỉ bảo mật học từ nước ngoài còn quá ít và chưa hẳn đã đáp ứng được nhu cầu công việc cụ thể trên hệ thống mạng ở nước ta. *Thứ ba,* để đối phó với tội phạm máy tính, hiện nay hầu hết các nước trên thế giới đều có các tổ chức cứu hộ khẩn cấp sự cố an

ninh máy tính (CERT). Các tổ chức này có nhiệm vụ theo dõi, nghiên cứu, thu thập và đưa ra các giải pháp về an ninh máy tính, nhằm bảo vệ người sử dụng máy tính, đảm bảo an ninh thông tin quốc gia, khắc phục sự cố cũng như tư vấn cho các doanh nghiệp, cơ quan thi hành pháp luật trong lĩnh vực công nghệ thông tin. Tuy nhiên, ở Việt Nam hiện nay chưa có một tổ chức chính thức nào đảm nhiệm vai trò như CERT. Từ trước đến nay, việc theo dõi, cảnh báo, cung cấp thông tin, công cụ khắc phục sự cố trong lĩnh vực an ninh mạng máy tính thường do nhóm viết phần mềm diệt vi rút BKAV của Trung tâm An ninh mạng thuộc Đại học Bách khoa Hà Nội (BKIS) tự nguyện đảm nhận. Điều này đang ngày càng trở nên bất cập khi tình hình an ninh máy tính và mạng diễn biến theo những chiều hướng phức tạp. Vì thế, việc thành lập một Trung tâm quốc gia về cứu hộ khẩn cấp các sự cố an ninh máy tính là một yêu cầu cấp bách nhằm tránh những hậu quả xảy ra trong tương lai. Chính vì vậy, Cục Cảnh sát kinh tế (Bộ Công an) đã được giao thành lập lực lượng cảnh sát đặc nhiệm trên mạng, nhằm chống tội phạm và xử lý các vụ việc có dấu hiệu tội phạm hình sự trên Internet. Tuy nhiên, chỉ riêng một lực lượng cảnh sát đặc nhiệm sẽ không thể làm hết mọi việc, bởi vì tội

phạm trên mạng khác với những loại tội phạm thông thường ở đặc điểm vô hình và không phân biệt biên giới, lãnh thổ. Vì vậy, chúng ta còn cần có những đơn vị tinh nhuệ của lực lượng cảnh sát phối hợp với các đơn vị an ninh mạng ngoài xã hội[1]. Đồng thời, việc thành lập lực lượng cảnh sát đặc nhiệm trên mạng là một bước đi cần thiết, nhưng chỉ để "*chống*" chứ chưa có được tính chất "*cảnh báo, phòng tránh*" hay "*cứu hộ*"[2]. *Chính vì vậy, yêu cầu cần thiết về thiết chế hiện nay là chúng ta phải thành lập một Trung tâm quốc gia về cứu hộ khẩn cấp các sự cố an ninh máy tính kiểu như CERT* và yêu cầu này cần được thể hiện bằng những chính sách cụ thể và rõ ràng của các cơ quan chuyên trách vì sự phát triển mạnh mẽ và an toàn của công nghệ thông tin ở nước ta.

2. Về thể chế

Ở nước ta hiện nay, hệ thống pháp luật và cơ quan thực thi pháp luật chưa đủ mạnh để đấu tranh có hiệu quả với các vi phạm trong lĩnh vực công nghệ thông tin. Vì vậy, những giải pháp về mặt thể chế là:

---

[1] Tạp chí Bưu điện, tháng 01/2004.

[2] Tạp chí Bưu điện, tháng 01/2004.

Một là, Trên cơ sở nghiên cứu kỹ Công ước của Hội đồng châu Âu về tội phạm mạng; Luật Mẫu về tội phạm máy tính và liên quan đến máy tính; Luật Mẫu về chứng cứ điện tử (phần Phụ lục), Việt Nam cần xây dựng đầy đủ các văn bản quy phạm pháp luật làm cơ sở để đấu tranh phòng, chống có hiệu quả tội phạm trong lĩnh vực công nghệ thông tin. Trước hết, cần sửa đổi, bổ sung Bộ luật Hình sự năm 1999. Theo chúng tôi nên có một chương riêng trong Bộ luật Hình sự về lĩnh vực này tương xứng với các chương khác như chương Tội phạm về ma tuý, Tội phạm về môi trường... Tại chương này, cần bổ sung một loạt các hành vi tội phạm trong lĩnh vực công nghệ thông tin mới phát sinh mà trước đây các nhà làm luật chưa dự liệu hết như:

- Hành vi lợi dụng công nghệ thông tin để tuyên truyền chống Nhà nước Việt Nam, kích động bạo lực, tuyên truyền chiến tranh xâm lược, phá hoại thuần phong mỹ tục, tiết lộ các thông tin thuộc bí mật Nhà nước;

- Hành vi xâm nhập trái phép, tấn công vào máy tính hoặc hệ thống máy tính;

- Hành vi làm thay đổi cơ sở dữ liệu máy tính mà

không được phép của chủ sở hữu;

- Hành vi làm cản trở trái phép hoạt động của máy tính, mạng máy tính;

- Hành vi sử dụng, chiếm đoạt, mua bán hoặc công khai hoá trái phép mã truy cập của máy tính;

- Hành vi sử dụng thiết bị kỹ thuật công nghệ cao hoặc lợi dụng sự chồng lấn sóng viễn thông ở một số vùng thuộc các tỉnh giáp biên giới chiếm đoạt tiền cước điện thoại viễn thông quốc tế với số lượng lớn;

- Hành vi sử dụng mạng máy tính để hoạt động phạm tội đánh bạc, cá độ, mại dâm;

- Hành vi sử dụng điện thoại đe doạ người khác, sử dụng điện thoại để tống tiền;

- Hành vi lợi dụng công nghệ thông tin và việc triển khai áp dụng công nghệ thông tin hỗ trợ hoạt động nghiệp vụ của các ngân hàng để lừa đảo chiếm đoạt tài sản;

- Hành vi thiết lập hệ thống thiết bị cung cấp dịch vụ Internet không đúng với các quy định ghi trong giấy phép;

- Hành vi vi phạm bí mật thông tin cho người sử dụng;

- Hành vi đấu nối trái phép máy tính vào mạng viễn thông công cộng;

- Hành vi kinh doanh trái phép dịch vụ Internet;

- Hành vi xâm phạm an toàn hệ thống an ninh mạng.

Hai là, xây dựng và ban hành các nghị định về xử lý vi phạm hành chính trong lĩnh vực công nghệ thông tin nhằm cụ thể hoá các hành vi vi phạm chưa đến mức bị coi là tội phạm trong lĩnh vực này một cách đầy đủ hơn, trong đó cần tăng nặng chế tài xử lý, nhất là phạt tiền, để nâng cao mức độ răn đe và ngăn chặn loại tội phạm này.

Ba là, trong thời gian chờ Bộ luật Hình sự năm 1999 được sửa đổi, bổ sung cần ban hành nghị định, thông tư hướng dẫn, giải thích cụ thể các tội phạm về máy tính trong Bộ luật Hình sự năm 1999. Cần có hướng dẫn đối với việc thực hiện các hành vi liên quan đến các tội khác ngoài 03 tội trong Bộ luật Hình sự năm 1999 nhưng sử dụng máy tính và mạng máy tính làm phương tiện phạm tội thì sẽ truy tố theo các tội liên quan.

Bốn là, bổ sung một số điều luật liên quan đến chứng cứ điện tử trong Bộ luật Tố tụng hình sự năm

2003, bởi vì hoạt động của loại tội phạm công nghệ cao cũng để lại những dấu vết trong các thiết bị điện tử mà chúng đã sử dụng để gây án hoặc xâm nhập trái phép. Thực chất đây là một loại chứng cứ mới, được tạo ra và lưu giữ lại trong máy tính một cách tự động, tồn tại dưới dạng những tín hiệu điện tử, kỹ thuật số, được lưu giữ lại trong các bộ nhớ của các thiết bị điện tử một cách tự động, khách quan theo lệnh của phần mềm đã được lập trình sẵn, có thể phát hiện, bảo quản và ghi lại hoặc in ra giấy để làm chứng cứ sử dụng trước Tòa án.

Chứng cứ điện tử là những chứng cứ được lưu giữ dưới hình thức điện tử hoặc kỹ thuật số trong máy tính hoặc trong các thiết bị điện tử có bộ nhớ. *Những chứng cứ điện tử có thể thu thập được để chứng minh hành vi phạm tội bao gồm:*

+ Những chứng cứ điện tử do máy tính tự động tạo ra như: "*cookies*", "*URL*", E-mail logs, web server logs...;

+ Những thông tin điện tử do con người tạo ra được lưu giữ trong máy tính hoặc các thiết bị điện tử khác, như các văn bản, bảng biểu, các hình ảnh, thông tin... được lưu giữ dưới hình thức điện tử, kỹ thuật số.

Để thu thập chứng cứ điện tử lưu ở máy tính và các thiết bị kỹ thuật số có bộ nhớ như máy fax, máy điện thoại, máy in, photocopy, máy định vị toàn cầu, máy nhắn tin, đĩa CD, đĩa mềm, USB, MP3... cũng như phục hồi lại những *"dấu vết điện tử"* và ghi lại dưới hình thức có thể đọc được, thì cần sử dụng những thiết bị kỹ thuật, công nghệ máy tính và phần mềm đặc biệt. Quy trình ghi, sao chụp chứng cứ điện tử phải được pháp luật công nhận để đảm bảo tính khách quan, nguyên vẹn, có thể kiểm chứng, giám định được của những chứng cứ điện tử được đưa ra làm bằng chứng trước Toà án.

Chứng cứ điện tử là một trong những hình thức biểu hiện mới của chứng cứ, có tính đặc thù (có thể sửa, chèn thêm, xoá, bị vi rút tấn công...). Do vậy, cần phải được nghiên cứu, bổ sung vào Bộ luật Tố tụng hình sự để đáp ứng yêu cầu đấu tranh phòng, chống loại tội phạm mới này, đặc biệt là quy định về thủ tục tố tụng hình sự đối với việc thu thập, bảo quản, phục hồi và giám định chứng cứ điện tử. Để đáp ứng yêu cầu này cần có những quy định cụ thể về mặt pháp lý cũng như về giải pháp kỹ thuật để có thể sử dụng chứng cứ điện tử làm bằng chứng chứng minh tội phạm, trong đó việc công nhận về mặt pháp lý những

công nghệ, thiết bị, phần mềm dùng để phát hiện, phục hồi, ghi, sao chép, in những chứng cứ điện tử và quy trình xác lập chứng cứ điện tử là rất quan trọng.

3. Về điều kiện đảm bảo

Ngoài yêu cầu về việc thành lập Trung tâm quốc gia về cứu hộ khẩn cấp các sự cố an ninh máy tính, trong khuôn khổ các dự án đầu tư trọng điểm quốc gia về công nghệ thông tin, năm 2003 Chính phủ đã phê duyệt quyết định đầu tư 49 tỷ đồng để nâng cấp Trung tâm An ninh mạng BKIS Đại học Bách khoa Hà Nội[1]. Sau khi triển khai, Trung tâm BKIS đã được trang bị một số lượng lớn các thiết bị mạng, thiết bị an ninh chuyên dụng, thiết bị kiểm định chất lượng mạng và phòng thí nghiệm an ninh mạng hiện đại hàng đầu khu vực, đạt chuẩn quốc tế. Với các trang thiết bị được đầu tư, các chuyên gia của Trung tâm có thể giả lập được mô hình của hầu hết các hệ thống mạng ở Việt Nam, nhờ đó luôn sẵn sàng tư vấn, giải pháp an ninh cho bất kỳ hệ thống mạng nào ở Việt Nam. Song song với quá trình tiếp nhận đầu tư,

[1] Trang vi tính của mạng http://www.vnn.vn.

Trung tâm đã đào tạo được một đội ngũ hơn 50 chuyên gia an ninh mạng. BKIS cũng đã xúc tiến và hiện là nhà tư vấn an ninh mạng cho hầu hết các cơ quan quan trọng của Chính phủ. Tuy nhiên, việc Chính phủ trang bị cơ sở vật chất, kinh phí cho Trung tâm An ninh mạng BKIS như vậy mới chỉ là bước đầu và yêu cầu trong thời gian tới cần phải có sự đầu tư hơn nữa về kinh phí để đào tạo nguồn nhân lực, cơ sở vật chất, trang thiết bị công nghệ thông tin thì mới xử lý được nguy cơ tấn công mạng diễn ra ngày càng tinh vi.

4. Các giải pháp khác

Thứ nhất, nâng cao hiệu quả hoạt động của cơ quan bảo vệ pháp luật, đặc biệt là đội ngũ cán bộ trong cơ quan bảo vệ pháp luật.

Thực tiễn cho thấy, các cơ quan bảo vệ pháp luật đóng vai trò quan trọng trong cuộc đấu tranh phòng, chống vi phạm pháp luật. Do đó, để đấu tranh có hiệu quả với vi phạm pháp luật nói chung và vi phạm pháp luật trong lĩnh vực công nghệ thông tin nói riêng, *chúng ta cần quan tâm đến một số vấn đề sau:*

- *Nâng cao năng lực của đội ngũ cán bộ trong cơ quan bảo vệ pháp luật.* Hoạt động phát hiện và xử lý

vi phạm pháp luật là một trong những hoạt động áp dụng pháp luật, hoạt động điều chỉnh pháp luật đối với các trường hợp cụ thể. Năng lực, trình độ cán bộ tham gia phát hiện và xử lý vi phạm pháp luật được nâng cao sẽ giúp họ áp dụng pháp luật một cách có hiệu quả. Trong giai đoạn hiện nay, bên cạnh việc tăng cường số lượng cán bộ, các cơ quan bảo vệ pháp luật cần đặc biệt chú trọng công tác sử dụng, đào tạo và bồi dưỡng cán bộ làm công tác phát hiện và xử lý vi phạm pháp luật trong lĩnh vực công nghệ thông tin. Do tính chất phức tạp của việc xử lý vi phạm pháp luật trong lĩnh vực công nghệ thông tin, đội ngũ cán bộ này ngoài việc nắm chắc kiến thức pháp lý, cần có sự hiểu biết những vấn đề về công nghệ thông tin như quản trị mạng, các ứng dụng công nghệ thông tin, giao dịch điện tử... Đồng thời, Nhà nước cần tạo điều kiện, hỗ trợ kinh phí, thời gian cho số cán bộ này theo học các lớp bồi dưỡng nghiệp vụ, ngoại ngữ, tin học để nâng cao trình độ chuyên môn và khả năng ứng dụng thành tựu khoa học - kỹ thuật trong lĩnh vực công nghệ thông tin;

- *Nâng cao hiệu quả các biện pháp xử lý vi phạm pháp luật trong lĩnh vực công nghệ thông tin.* Bởi xử

lý nghiêm minh mọi hành vi vi phạm pháp luật là một biện pháp quan trọng không chỉ có ý nghĩa răn đe, giáo dục đối với chủ thể vi phạm pháp luật mà còn có tác dụng ngăn ngừa khả năng phát sinh vi phạm pháp luật của các chủ thể khác trong xã hội, góp phần tạo lòng tin vào pháp luật cho nhân dân, nâng cao ý thức pháp luật trong cộng đồng. Việc xử lý vi phạm pháp luật nói chung và vi phạm pháp luật trong lĩnh vực công nghệ thông tin nói riêng cần bảo đảm nguyên tắc: mọi hành vi vi phạm pháp luật phải được xử lý nghiêm minh, trong đó cần tập trung tăng cường hiệu quả xử lý hành chính và xử lý hình sự.

Thứ hai, tăng cường công tác tuyên truyền, giáo dục ý thức pháp luật.

Giáo dục pháp luật là một trong những yếu tố quan trọng tác động tích cực đến việc phòng ngừa vi phạm pháp luật. Thông qua giáo dục pháp luật giúp mọi thành viên trong xã hội nhận thức đầy đủ tầm quan trọng, các giá trị xã hội của pháp luật, từ đó giúp họ tự giác lựa chọn hành vi xử sự đúng đắn. Đặc biệt, trong lĩnh vực công nghệ thông tin, đặc điểm về chủ thể vi phạm là những người có hiểu biết tốt về mạng, phần lớn là trẻ tuổi và nhiều người nước ngoài, do đó

cần có phương pháp tuyên truyền, giáo dục pháp luật thích hợp. *Ví dụ,* cung cấp các thông tin pháp luật liên quan bằng tiếng Việt và tiếng Anh trên mạng; đăng tải thường xuyên các hành vi bị pháp luật cấm trong lĩnh vực công nghệ thông tin, tổ chức các cuộc hội thảo, đàm thoại với mục đích tuyên truyền, giáo dục ý thức pháp luật.

Thứ ba, tăng cường sự phối hợp giữa cơ quan chuyên ngành với cơ quan thực thi pháp luật và hợp tác quốc tế trong phòng, chống tội phạm trong lĩnh vực công nghệ thông tin.

Việc đảm bảo an ninh, trật tự trong lĩnh vực công nghệ thông tin trong nước cần có sự phối hợp chặt chẽ giữa Bộ Bưu chính Viễn thông và Bộ Công an, vì đây là hai ngành chủ chốt thực hiện nhiệm vụ này, đặc biệt là trong quá trình điều tra các tội phạm trong lĩnh vực công nghệ thông tin. Do chứng cứ trong điều tra thường là các trang thiết bị kỹ thuật về công nghệ thông tin nên đòi hỏi phải có chuyên gia hiểu biết để phân tích, đánh giá chính xác mức độ thiệt hại của hành vi vi phạm... Vì vậy, nên chăng hai Bộ cần sớm phối hợp để có thể thành lập Trung tâm công nghệ cao hoặc các đơn vị chịu trách nhiệm chính về các vấn đề liên quan đến vi phạm

pháp luật trong lĩnh vực công nghệ thông tin.

Ngoài ra, trong những năm qua, vấn đề an ninh mạng đã được các quốc gia quan tâm và Diễn đàn hợp tác kinh tế châu Á - Thái Bình Dương (APEC) đã có những chương trình, kế hoạch đẩy mạnh hoạt động đảm bảo an ninh mạng nói chung và chống khủng bố trên mạng nói riêng. Hưởng ứng chương trình này, Việt Nam đã cung cấp thông tin về cơ sở hạ tầng thông tin quốc gia cho APEC và đang triển khai những hoạt động ban đầu (*Ví dụ:* Đề án của Bộ Giáo dục và Đào tạo trình Chính phủ thành lập Trung tâm ứng cứu khẩn cấp về máy tính quốc gia. Theo đề án này thì Trung tâm An ninh mạng của Trường Đại học Bách khoa Hà Nội sẽ thực thi chức năng này[1]. Tuy nhiên, để phòng chống tội phạm trong lĩnh vực công nghệ thông tin có hiệu quả, ngoài việc phát triển hệ thống mạng và đảm bảo an ninh mạng, chúng ta cần phải có đội ngũ cán bộ thực thi pháp luật được đào tạo về công nghệ thông tin để kịp thời phối hợp, hợp tác với các cơ quan, tổ chức hữu quan trong nước và quốc tế trong việc phát hiện và xử lý những hành vi vi phạm pháp luật trong lĩnh vực công nghệ thông tin.

[1] Trang vi tính của mạng http://www.vnn.vn.

Phụ lục

CÔNG ƯỚC CỦA HỘI ĐỒNG CHÂU ÂU VỀ TỘI PHẠM MẠNG

(Budapest ngày 23/11/2001)

LỜI NÓI ĐẦU

Các quốc gia thành viên Hội đồng châu Âu và các quốc gia ký tên dưới đây:

Lưu ý rằng mục đích của Hội đồng châu Âu là hướng tới sự thống nhất cao hơn giữa các quốc gia thành viên;

Thừa nhận giá trị của việc tăng cường hợp tác với các quốc gia khác tham gia Công ước;

Phúc đáp nhu cầu bức thiết về việc áp dụng một chính sách hình sự chung nhằm bảo vệ xã hội trước tội phạm mạng bằng việc xây dựng luật phù hợp và tăng cường hợp tác quốc tế;

Ý thức được những thay đổi to lớn từ quá trình số hóa, tin học hoá, sự hội tụ và toàn cầu hóa mạng máy tính;

Lo ngại về những rủi ro mà mạng máy tính và thông tin điện tử được sử dụng để thực hiện các hành vi phạm tội trong khi các chứng cứ liên quan đến tội phạm được lưu trữ và truyền tải bởi các mạng này;

Thừa nhận nhu cầu hợp tác giữa các nước với khu vực tư nhân trong việc chống tội phạm mạng và nhu cầu bảo vệ lợi ích hợp pháp trong việc sử dụng và phát triển công nghệ thông tin;

Tin tưởng rằng việc đấu tranh có hiệu quả với tội phạm mạng đòi hỏi sự hợp tác quốc tế nhanh, hiệu quả và không ngừng được tăng cường về các vấn đề hình sự;

Được thuyết phục rằng Công ước này là cần thiết để ngăn ngừa các hành vi chống lại sự bí mật, tính toàn vẹn và sẵn có của các hệ thống máy tính, mạng và dữ liệu máy tính, chống lại sự sử dụng sai lạc hệ thống, mạng và dữ liệu bằng việc tội phạm hóa các hành vi này, như được quy định trong Công ước, và việc áp dụng các quyền năng đầy đủ cho việc chống lại các hành vi phạm tội đó một cách hiệu quả, bằng việc hỗ trợ quá trình phát hiện, điều tra và truy tố ở cả cấp độ quốc gia, quốc tế và bằng việc cung cấp những sự dàn xếp giúp cho việc hợp tác quốc tế được nhanh và đáng tin cậy;

Ý thức sự cần thiết đảm bảo sự cân bằng hợp lý giữa lợi ích của việc thực thi pháp luật và việc tôn trọng các quyền con người cơ bản đã được ghi nhận trong Công ước năm 1950 về bảo vệ quyền con người và quyền tự do cơ bản của Hội đồng châu Âu, Công ước năm 1966 của Liên hợp quốc về các quyền dân sự và chính trị và các công ước khác về quyền con người trong đó có quyền bày tỏ ý kiến mà không bị sách nhiễu, quyền tự do tư tưởng, bao gồm quyền tự do tìm kiếm, tiếp nhận và phổ biến thông tin và tư tưởng thuộc mọi thể loại, không hạn chế về biên giới, và quyền tôn trọng bí mật đời tư;

Ý thức về quyền được bảo vệ các thông tin cá nhân đã được ghi nhận, chẳng hạn trong Công ước năm 1981 của Hội đồng châu Âu về bảo vệ cá nhân đối với việc tự động xử lý thông tin cá nhân;

Có cân nhắc đến Công ước năm 1989 của Liên hợp quốc về quyền trẻ em và Công ước năm 1999 của Tổ chức lao động quốc tế về các hình thức lao động tồi tệ đối với trẻ em;

Tính đến sự tồn tại của các Công ước của Hội đồng châu Âu về hợp tác trong lĩnh vực hình sự cũng như các công ước tương tự của các quốc gia thành viên

Hội đồng châu Âu và các quốc gia khác. Nhấn mạnh rằng Công ước này được xây dựng để bổ sung những Công ước đã nêu góp phần làm cho quá trình điều tra tội phạm, các thủ tục tố tụng hình sự liên quan đến hệ thống máy tính và dữ liệu máy tính được hiệu quả hơn và tạo khả năng cho việc thu thập chứng cứ dưới hình thức điện tử của tội phạm hình sự;

Chào đón những diễn tiến mới đây trong sự hiểu biết và hợp tác quốc tế về chống tội phạm mạng, bao gồm những biện pháp do Liên hợp quốc, các nước OECD, Liên minh châu Âu và G8 thực hiện;

Ghi nhớ đến các Đề xuất số R. (85) 10 của Hội đồng Bộ trưởng về việc áp dụng thực tế Công ước châu Âu về tương trợ trong lĩnh vực hình sự liên quan đến hành vi cản trở hoạt động viễn thông, Đề xuất số R. (88) 2 về vi phạm bản quyền trong lĩnh vực quyền tác giả và quyền kế thừa, Đề xuất số R. (87) 15 điều chỉnh việc sử dụng thông tin cá nhân trong lĩnh vực điều tra, Đề xuất số R. (95) 4 về việc bảo vệ thông tin cá nhân trong lĩnh vực dịch vụ viễn thông, với sự lưu ý đặc biệt tới dịch vụ điện thoại, cũng như Đề xuất số R. (89) 9 về tội phạm liên quan đến máy tính quy định các định hướng đối với nghị viện các nước về định

nghĩa một số loại tội phạm máy tính và Đề xuất số R (95) 13 về các vấn đề luật tố tụng hình sự của các nước liên quan đến công nghệ thông tin;

Dẫn chiếu đến Nghị quyết số 1 do Hội nghị Bộ trưởng Tư pháp châu Âu tại Kỳ họp số 21 (ngày 10 và 11/6/1997 tại Praha) có khuyến nghị rằng Hội đồng Bộ trưởng nên ủng hộ dự án về tội phạm mạng do Uỷ ban châu Âu về các vấn đề tội phạm (CDPC) thực hiện để làm cho các quy định pháp luật hình sự tương thích với nhau hơn và tạo khả năng sử dụng các phương tiện hiệu quả để điều tra các loại tội ấy, cũng như Nghị quyết số 3 được thông qua tại Kỳ họp số 23 của Hội nghị Bộ trưởng Tư pháp châu Âu (ngày 08 và 09/6/2000 tại Luân Đôn) trong đó khuyến khích các bên tham gia đàm phán theo đuổi các nỗ lực tìm ra các giải pháp phù hợp để tạo khả năng cho nhiều quốc gia nhất có thể trở thành thành viên của Công ước và ghi nhận nhu cầu đối với một hệ thống hợp tác quốc tế nhanh và hiệu quả, có tính đầy đủ các đòi hỏi cụ thể của cuộc chiến chống tội phạm mạng;

Dẫn chiếu đến Chương trình hành động do Nguyên thủ các quốc gia thuộc Hội đồng châu Âu thông qua nhân dịp Hội nghị thượng đỉnh lần 2 (tại Strasbourg ngày 10 và 11/10/1997) về phản ứng chung đối với sự

phát triển của công nghệ thông tin mới theo tiêu chuẩn và giá trị của Hội đồng châu Âu;

Đã đồng ý những điều sau đây:

Chương I

VIỆC SỬ DỤNG TỪ NGỮ

Điều 1. *Định nghĩa*

Trong Công ước này:

a) "*Hệ thống máy tính*" là bất cứ thiết bị hoặc nhóm thiết bị có liên hệ với nhau, thực hiện quá trình xử lý dữ liệu một cách tự động theo một chương trình định sẵn;

b) "Dữ liệu máy tính" là bất cứ sự thể hiện tình tiết thực tế, thông tin hoặc khái niệm theo một hình thức tương thích với việc xử lý trong hệ thống máy tính, bao gồm chương trình phù hợp với việc làm cho hệ thống máy tính thực hiện một chức năng nhất định;

c) "Nhà cung cấp dịch vụ" có nghĩa:

(i) Một tổ chức (công hoặc tư) cung cấp khả năng liên lạc thông qua hệ thống máy tính cho người sử dụng dịch vụ; và

(ii) Bất cứ tổ chức nào khác, thay mặt các tổ chức hoặc người sử dụng dịch vụ kể trên thực hiện việc xử

lý hoặc lưu trữ dữ liệu máy tính;

d) "Dữ liệu lưu thông" là bất cứ dữ liệu máy tính nào liên quan đến việc liên lạc qua hệ thống máy tính hoặc được tạo ra bởi hệ thống máy tính trong trường hợp hệ thống máy tính là một phần của chuỗi liên lạc, chỉ ra nguồn gốc, đích tới, lộ trình, thời gian, ngày, kích cỡ, thời hạn hoặc loại dịch vụ nền tảng của việc liên lạc.

Chương II

CÁC BIỆN PHÁP CẦN PHẢI THỰC HIỆN Ở CẤP QUỐC GIA

Mục 1

LUẬT HÌNH SỰ

Nhóm 1

Các tội phạm chống lại tính bí mật, toàn vẹn và sẵn có của dữ liệu máy tính và hệ thống máy tính

Điều 2. ***Truy cập bất hợp pháp***

Các quốc gia thành viên phải ban hành luật và các

biện pháp cần thiết khác quy định tội phạm trong luật quốc gia mình đối với các hành vi, được thực hiện một cách cố ý, truy cập toàn bộ hoặc một phần hệ thống máy tính mà không có quyền truy cập. Quốc gia thành viên có thể yêu cầu rằng chỉ coi là đã có hành vi phạm tội khi có hành vi vi phạm các biện pháp an ninh, với ý định chiếm đoạt dữ liệu máy tính hoặc các ý định không trung thực khác, hoặc có liên hệ với một hệ thống máy tính được kết nối với hệ thống máy tính khác.

Điều 3. ***Ngăn chặn bất hợp pháp***

Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để quy định tội phạm trong luật quốc gia mình đối với hành vi, được thực hiện một cách cố ý, ngăn chặn trong khi không có quyền ngăn chặn, bằng các biện pháp kỹ thuật việc truyền tải các dữ liệu máy tính không vì mục đích công, từ hoặc trong một hệ thống máy tính, bao gồm việc phát các tín hiệu điện từ từ hệ thống máy tính mang dữ liệu máy tính ấy. Quốc gia thành viên có thể yêu cầu rằng chỉ coi là đã có hành vi phạm tội khi hành vi ấy được thực hiện với ý định không trung thực, hoặc có liên quan đến một hệ thống máy tính được kết nối với hệ thống máy tính khác.

Điều 4. ***Gây rối dữ liệu***

1. Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để quy định tội phạm trong luật quốc gia mình đối với hành vi, được thực hiện một cách cố ý, làm hư hại, xóa, làm hỏng hoặc nén dữ liệu máy tính đối với người không có quyền làm việc ấy.

2. Quốc gia thành viên có thể bảo lưu quyền yêu cầu rằng hành vi mô tả trong khoản 1 phải gây ra thiệt hại nghiêm trọng.

Điều 5. ***Gây rối hệ thống***

Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để quy định tội phạm trong luật quốc gia mình đối với hành vi, được thực hiện một cách cố ý, cản trở nghiêm trọng hoạt động của hệ thống máy tính đối với người không có quyền làm việc này, bằng việc đưa vào, truyền tải, làm hư hỏng, xóa, làm suy giảm, thay thế hoặc nén dữ liệu máy tính.

Điều 6. ***Sử dụng sai lạc các thiết bị***

1. Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để quy định tội phạm trong luật quốc gia mình đối với hành vi, được thực hiện một cách cố ý, của người không có quyền thực hiện:

a) Sản xuất, bán, đề nghị sử dụng, nhập khẩu, phân phối hoặc bằng các cách thức khác cung cấp:

(i) Thiết bị, bao gồm chương trình máy tính, được thiết kế hoặc được điều chỉnh để thực hiện hành vi phạm tội nêu từ Điều 2 đến Điều 5; hoặc

(ii) Mã số truy cập của máy tính (password), mật mã truy cập hoặc dữ liệu tương tự mà nhờ mã số ấy toàn bộ hoặc một phần hệ thống máy tính có thể được truy cập với ý định sẽ sử dụng để thực hiện hành vi phạm tội quy định từ Điều 2 đến Điều 5;

b) Chiếm hữu các khoản mục nêu tại tiểu khoản (a.i) và (a.ii) kể trên với ý định cho người khác sử dụng để thực hiện các hành vi phạm tội quy định từ Điều 2 đến Điều 5. Quốc gia thành viên có thể bảo lưu quyền yêu cầu rằng phải chiếm hữu một số lượng nhất định các khoản mục kể trên thì mới bị truy cứu trách nhiệm hình sự.

2. Điều khoản này sẽ không được áp dụng để quy định trách nhiệm hình sự đối với hành vi sản xuất, bán, đề nghị sử dụng, nhập khẩu, phân phối hoặc bằng cách thức khác cung cấp hoặc chiếm hữu nêu tại khoản 1 Điều này mà không vì mục đích thực hiện hành vi phạm tội quy định từ Điều 2 đến Điều 5 của Công ước này, chẳng hạn thử nghiệm hoặc bảo vệ hợp

pháp hệ thống máy tính.

3. Quốc gia thành viên có quyền bảo lưu quyền không áp dụng khoản 1 Điều này với điều kiện là việc bảo lưu đó không liên quan đến việc bán, phân phối hoặc cung cấp các khoản mục nêu tại điểm (a.ii) của khoản 1 Điều này.

Nhóm 2

Các tội phạm liên quan đến máy tính

Điều 7. ***Hành vi giả mạo liên quan đến máy tính***

Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để quy định tội phạm trong luật quốc gia mình đối với hành vi, được thực hiện một cách cố ý, của người không được phép, đưa vào, thay đổi, xóa, hoặc nén dữ liệu máy tính, làm cho dữ liệu không còn chính xác với ý định rằng dữ liệu ấy sẽ được sử dụng cho các mục đích hợp pháp nếu nó là chính xác, bất kể dữ liệu có thể đọc hoặc nhận biết được trực tiếp hay không. Quốc gia thành viên có thể yêu cầu rằng chỉ coi là đã có hành vi phạm tội và phải chịu trách nhiệm hình sự khi hành vi ấy được thực hiện với

ý định lừa đảo hoặc các ý định không trung thực khác.

Điều 8. ***Lừa đảo liên quan đến máy tính***

Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để quy định tội phạm trong luật quốc gia mình đối với hành vi, được thực hiện một cách cố ý, của người không được phép, gây thiệt hại về tài sản cho người khác bằng cách:

a) Đưa vào, thay đổi, xóa hoặc nén dữ liệu máy tính;

b) Bất cứ hành vi gây rối nào đối với sự vận hành của hệ thống máy tính.

Với ý định lừa đảo hoặc không trung thực nhằm thu lợi, quyền lợi kinh tế mà không được phép, cho mình hoặc cho người khác.

Nhóm 3
Các tội phạm liên quan đến nội dung

Điều 9. ***Các tội phạm liên quan đến tài liệu khiêu dâm trẻ em***

1. Các quốc gia thành viên phải ban hành luật và

các biện pháp cần thiết khác để quy định tội phạm trong luật quốc gia mình đối với hành vi, được thực hiện một cách cố ý, của người không được phép:

a) Sản xuất tài liệu khiêu dâm trẻ em để phát tán qua hệ thống máy tính; hoặc

b) Đề nghị cung cấp hoặc cung cấp tài liệu khiêu dâm trẻ em qua hệ thống máy tính; hoặc

c) Phát tán hoặc truyền tải tài liệu khiêu dâm trẻ em qua hệ thống máy tính; hoặc

d) Mua tài liệu khiêu dâm trẻ em cho mình hoặc cho người khác thông qua hệ thống máy tính; hoặc

e) Sở hữu tài liệu khiêu dâm trẻ em trong hệ thống máy tính hoặc trong phương tiện lưu trữ dữ liệu máy tính.

2. Theo cách hiểu của khoản 1 Điều này: "*tài liệu khiêu dâm trẻ em*" bao gồm bất cứ tài liệu nào bằng hình ảnh mô tả:

a) Người chưa thành niên thực hiện hành vi tình dục; hoặc

b) Người giống người chưa thành niên thực hiện hành vi tình dục; hoặc

c) Hình ảnh thực tế diễn tả người chưa thành niên

thực hiện hành vi tình dục.

3. Theo cách hiểu của khoản 2 Điều này, "*người chưa thành niên*" là tất cả mọi người dưới 18 tuổi. Quốc gia thành viên có thể đưa ra giới hạn tuổi thấp hơn nhưng không được dưới 16 tuổi.

4. Quốc gia thành viên có quyền bảo lưu không áp dụng, toàn bộ hoặc một phần, các tiểu khoản d và e khoản 1, các tiểu khoản b và c khoản 2.

Nhóm 4
Các tội phạm xâm phạm quyền tác giả và quyền liên quan

Điều 10. ***Tội phạm xâm phạm quyền tác giả và các quyền liên quan***

1. Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để quy định tội phạm trong luật quốc gia mình đối với hành vi xâm phạm quyền tác giả, như được định nghĩa về quyền tác giả trong luật của quốc gia đó, phù hợp với các nghĩa vụ đã cam kết theo Luật Paris ngày 24/7/1971 sửa đổi, bổ sung Công ước Berne về bảo hộ các tác phẩm văn học

và nghệ thuật, Hiệp định về các khía cạnh thương mại của quyền sở hữu trí tuệ (TRIPS) và Công ước quyền tác giả của WIPO (Tổ chức sở hữu trí tuệ thế giới), trừ các quyền tinh thần quy định trong các công ước, khi hành vi này được thực hiện một cách cố ý, với quy mô có ý nghĩa về mặt thương mại và thông qua hệ thống máy tính.

2. Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để quy định tội phạm trong luật quốc gia mình đối với hành vi xâm phạm quyền liên quan, như được định nghĩa về quyền liên quan trong luật của quốc gia đó, phù hợp với các nghĩa vụ đã cam kết theo Công ước quốc tế bảo hộ người biểu diễn, nhà sản xuất chương trình và tổ chức phát thanh (Công ước Rome), Hiệp định TRIPS và Công ước về chương trình âm thanh và các buổi biểu diễn của WIPO, không tính đến các quyền tinh thần quy định trong các công ước, khi hành vi này được thực hiện một cách cố ý, với quy mô có ý nghĩa về mặt thương mại và thông qua hệ thống máy tính.

3. Quốc gia thành viên có quyền bảo lưu không quy định trách nhiệm hình sự theo khoản 1 và 2 của Điều này trong một số trường hợp nhất định, nếu như

có các biện pháp hiệu quả khác và sự bảo lưu đó không làm giảm nghĩa vụ quốc tế của quốc gia thành viên quy định trong các điều ước quốc tế nêu trong khoản 1 và 2 của Điều này.

Nhóm 5
Trách nhiệm bổ trợ và biện pháp chế tài

Điều 11. ***Nỗ lực và hỗ trợ thực hiện hành vi phạm tội***

1. Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để quy định tội phạm trong luật quốc gia mình đối với hành vi, được thực hiện một cách cố ý, trợ giúp hoặc khuyến khích việc thực hiện các hành vi phạm tội quy định từ Điều 2 đến Điều 10 Công ước này với ý định mong muốn tội phạm đó được thực hiện.

2. Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để quy định tội phạm trong luật quốc gia mình đối với hành vi, được thực hiện một cách cố ý, nỗ lực thực hiện một tội quy định

từ Điều 3 đến Điều 5, Điều 7, Điều 8 và Điều 9.1a và c của Công ước này.

3. Quốc gia thành viên có quyền bảo lưu không áp dụng một phần hoặc toàn bộ khoản 2 của Điều này.

Điều 12. ***Trách nhiệm của pháp nhân***

1. Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để đảm bảo rằng pháp nhân phải chịu trách nhiệm đối với các hành vi phạm tội quy định trong Công ước này, được bất cứ cá nhân nào thực hiện vì lợi ích của pháp nhân, nếu cá nhân ấy là đại diện hoặc một phần trong cơ quan của pháp nhân và nắm vị trí lãnh đạo trên cơ sở:

a) Thẩm quyền đại diện cho pháp nhân;

b) Thẩm quyền ra quyết định nhân danh pháp nhân;

c) Thẩm quyền thực hiện việc kiểm soát trong nội bộ pháp nhân.

2. Ngoài các trường hợp quy định tại khoản 1 Điều này, các quốc gia thành viên phải thực hiện các biện pháp cần thiết để đảm bảo rằng pháp nhân phải chịu trách nhiệm khi không thực hiện tốt việc giám sát hoặc kiểm soát của cá nhân đề cập trong khoản 1 làm

cho tội phạm quy định trong Công ước này được thực hiện bởi cá nhân hành xử theo thẩm quyền của mình vì lợi ích của pháp nhân.

3. Theo các nguyên tắc pháp lý của quốc gia thành viên, trách nhiệm của pháp nhân có thể là trách nhiệm hình sự, dân sự hoặc hành chính.

4. Trách nhiệm này được áp dụng mà không được làm sai lệch việc truy cứu trách nhiệm hình sự đối với các cá nhân đã thực hiện hành vi phạm tội.

Điều 13. ***Biện pháp chế tài và các biện pháp khác***

1. Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để đảm bảo rằng các tội phạm quy định từ Điều 2 đến Điều 11 Công ước này được trừng trị bởi hệ thống chế tài tương xứng, hiệu quả và có tác dụng răn đe, bao gồm cả việc tước quyền tự do cá nhân.

2. Các quốc gia thành viên phải đảm bảo rằng pháp nhân phải chịu trách nhiệm phù hợp với các quy định tại Điều 12 và bị áp dụng các biện pháp chế tài hình sự hoặc phi hình sự mang tính tương xứng, hiệu quả và có tính răn đe hoặc các biện pháp khác, bao gồm cả chế tài phạt tiền.

Mục 2
LUẬT TỐ TỤNG

Nhóm 1
Các quy định chung

Điều 14. ***Phạm vi các quy định tố tụng***

1. Các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để xác lập thẩm quyền và trình tự, thủ tục quy định trong Điều này phục vụ hoạt động điều tra hoặc tố tụng hình sự.

2. Trừ trường hợp được quy định cụ thể tại Điều 21, các quốc gia thành viên phải áp dụng các thẩm quyền và trình tự, thủ tục nêu tại khoản 1 Điều này đối với:

a) Các tội phạm quy định từ Điều 2 đến Điều 11 của Công ước này;

b) Các tội phạm khác được thực hiện thông qua hệ thống máy tính; và

c) Việc thu thập chứng cứ dưới hình thức điện tử đối với một tội phạm.

3. a) Quốc gia thành viên có quyền bảo lưu không áp dụng các biện pháp nêu tại Điều 20 chỉ đối với các

tội hoặc loại tội nêu cụ thể trong bảo lưu, với điều kiện là các tội ấy không bị hạn chế hơn so với các tội bị áp dụng các biện pháp nêu tại Điều 21. Quốc gia thành viên phải cân nhắc việc hạn chế những bảo lưu như vậy để tạo khả năng cho việc áp dụng một cách rộng rãi nhất các biện pháp nêu tại Điều 20.

b) Trường hợp quốc gia thành viên do những hạn chế trong pháp luật đang có hiệu lực tại thời điểm tham gia Công ước này mà không thể áp dụng các biện pháp nêu tại Điều 20 và Điều 21 đối với các liên lạc được truyền tải trong một hệ thống máy tính của nhà cung cấp dịch vụ mà:

(i) Đang hoạt động vì lợi ích của một nhóm các nhà sử dụng có tính chất đóng; và

(ii) Không sử dụng hệ thống liên lạc công cộng và không kết nối với hệ thống máy tính khác, bất kể là công cộng hay tư nhân,

Thì quốc gia đó có thể bảo lưu quyền không áp dụng các biện pháp đối với những loại liên lạc đó. Quốc gia thành viên có trách nhiệm cân nhắc việc hạn chế sự bảo lưu đó để tạo khả năng áp dụng một cách rộng rãi nhất các biện pháp được đề cập tại Điều 20 và Điều 21.

Điều 15. ***Điều kiện và biện pháp bảo vệ***

1. Quốc gia thành viên phải bảo đảm rằng việc thiết lập, thực thi và áp dụng các quyền năng và trình tự, thủ tục quy định trong điều này được tuân thủ theo các điều kiện và các biện pháp bảo vệ quy định trong luật của quốc gia mình, nhằm bảo vệ đầy đủ quyền con người và các quyền tự do, bao gồm các quyền phát sinh theo các nghĩa vụ mà quốc gia đã cam kết theo Công ước năm 1950 của Hội đồng châu Âu về bảo vệ quyền con người và các quyền tự do cơ bản, Công ước năm 1966 của Liên hợp quốc về các quyền dân sự và chính trị và các điều ước quốc tế khác về nhân quyền trong đó có quy định nguyên tắc tương xứng.

2. Các điều kiện và biện pháp bảo vệ đó, phù hợp từ giác độ bản chất các quyền năng và trình tự, thủ tục, bao gồm sự giám sát tư pháp hoặc giám sát độc lập khác, các căn cứ biện minh cho sự áp dụng, giới hạn của phạm vi và thời hạn của các quyền năng và trình tự, thủ tục đó.

3. Trong phạm vi phù hợp với lợi ích công cộng, đặc biệt là việc thực thi công lý một cách công bằng, quốc gia thành viên phải cân nhắc ảnh hưởng của các quyền năng và trình tự, thủ tục trong Điều này đối

với các quyền, trách nhiệm và lợi ích hợp pháp của các bên thứ ba.

Nhóm 2
Việc bảo quản khẩn cấp
các dữ liệu máy tính đã được lưu trữ

Điều 16. ***Bảo quản khẩn cấp các dữ liệu máy tính đã được lưu trữ***

1. Các quốc gia thành viên Công ước phải ban hành luật và các biện pháp cần thiết khác để tạo khả năng cho các cơ quan chức năng ra lệnh hoặc thực hiện các biện pháp tương tự để bảo quản khẩn cấp các dữ liệu máy tính nhất định, bao gồm cả dữ liệu lưu thông, đã được lưu trữ bởi hệ thống máy tính, nhất là khi có căn cứ để cho rằng dữ liệu máy tính này đặc biệt dễ bị mất hoặc thay đổi.

2. Trường hợp quốc gia thành viên Công ước đảm bảo hiệu lực của khoản 1 Điều này bằng quy định ra lệnh cho một người phải giữ gìn dữ liệu máy tính đã được lưu trữ thuộc sự chiếm hữu, quản lý của người đó, quốc gia thành viên Công ước phải ban hành luật

và các biện pháp cần thiết khác để quy định người này có nghĩa vụ giữ gìn và duy trì sự toàn vẹn của dữ liệu máy tính đó trong một thời gian cần thiết, không quá 90 ngày, để tạo khả năng cho các cơ quan chức năng có được các thông tin từ dữ liệu. Quốc gia thành viên có thể quy định việc gia hạn lệnh kể trên.

3. Quốc gia thành viên phải ban hành luật hoặc các biện pháp cần thiết khác buộc người giữ gìn dữ liệu máy tính đảm bảo sự bí mật về hành vi tố tụng đó trong một thời hạn được luật của quốc gia mình quy định.

4. Thẩm quyền và trình tự, thủ tục nêu tại Điều này sẽ được thực hiện như quy định tại Điều 14 và Điều 15.

Điều 17. ***Bảo quản khẩn cấp và tiết lộ một phần dữ liệu lưu thông***

1. Đối với dữ liệu lưu thông được bảo quản theo quy định tại Điều 16, quốc gia thành viên Công ước phải ban hành luật hoặc thực hiện các biện pháp cần thiết khác để:

a) Bảo đảm rằng việc bảo quản khẩn cấp dữ liệu lưu thông là sẵn có bất kể có bao nhiêu nhà cung cấp dịch vụ liên quan đến việc truyền tải liên lạc đó; và

b) Bảo đảm rằng việc tiết lộ nhanh chóng cho cơ

quan chức năng của quốc gia thành viên Công ước, hoặc người được chỉ định bởi cơ quan đó, một lượng dữ liệu lưu thông đủ để tạo khả năng cho quốc gia thành viên này nhận ra các nhà cung cấp dịch vụ và đường truyền liên lạc đó.

2. Thẩm quyền và trình tự, thủ tục đề cập trong Điều này sẽ được thực hiện như quy định tại Điều 14 và Điều 15.

Nhóm 3
Lệnh xuất trình

Điều 18. *Lệnh xuất trình*

1. Quốc gia thành viên Công ước phải ban hành luật hoặc các biện pháp cần thiết để trao thẩm quyền cho cơ quan chức năng ra lệnh:

a) Người trong lãnh thổ của mình đệ trình dữ liệu máy tính được yêu cầu thuộc sự chiếm hữu, quản lý của người đó hiện đang được lưu trữ trong hệ thống máy tính hoặc phương tiện lưu trữ dữ liệu máy tính; và

b) Nhà cung cấp dịch vụ đang cung cấp dịch vụ

trong lãnh thổ của mình đệ trình thông tin về người đăng ký dịch vụ có liên quan đến dịch vụ đó đang thuộc sự chiếm hữu, quản lý của nhà cung cấp dịch vụ.

2. Thẩm quyền và trình tự, thủ tục nêu tại điều này được thực hiện theo các quy định tại Điều 14 và Điều 15.

3. Trong Điều này, từ "*thông tin về người đăng ký dịch vụ*" được hiểu là bất cứ thông tin nào dưới hình thức dữ liệu máy tính hoặc các hình thức khác mà nhà cung cấp dịch vụ đang nắm giữ, có liên quan tới người đăng ký sử dụng dịch vụ nhưng không phải là dữ liệu lưu thông hoặc dữ liệu nội dung mà bằng thông tin ấy có thể xác định được:

a) Loại dịch vụ liên lạc được sử dụng, các quy định kỹ thuật được áp dụng và thời hạn cung cấp dịch vụ;

b) Thông tin nhận dạng của người đăng ký dịch vụ, địa chỉ bưu điện hoặc địa chỉ địa lý, điện thoại và số tiếp cận khác, thông tin về thanh toán và cách tính cước, được cung cấp theo thỏa thuận cung cấp dịch vụ;

c) Các thông tin khác tại địa điểm lắp đặt các phương tiện liên lạc, được cung cấp theo thỏa thuận cung cấp dịch vụ.

Nhóm 4
Khám xét và thu giữ dữ liệu máy tính đã được lưu trữ

Điều 19. ***Khám xét và thu giữ dữ liệu máy tính đã được lưu trữ***

1. Quốc gia thành viên Công ước phải ban hành luật hoặc các biện pháp cần thiết khác để trao thẩm quyền cho cơ quan chức năng thực hiện việc khám xét hoặc các biện pháp tương tự truy cập:

a) Hệ thống máy tính hoặc một phần của hệ thống máy tính và các dữ liệu máy tính được lưu trữ ở trong đó; và

b) Phương tiện lưu trữ dữ liệu máy tính trong đó dữ liệu máy tính có thể đã được lưu trữ thuộc lãnh thổ của quốc gia mình.

2. Quốc gia thành viên Công ước phải ban hành luật hoặc các biện pháp cần thiết khác để bảo đảm rằng, khi cơ quan chức năng thực hiện việc khám xét hoặc các biện pháp tương tự truy cập hệ thống máy tính nhất định hoặc một phần của hệ thống ấy phù

hợp với quy định tại khoản 1a Điều này và có căn cứ hợp lý để tin rằng dữ liệu mình cần tìm kiếm đang được lưu trữ trong hệ thống máy tính khác hoặc trong một phần của hệ thống máy tính khác thuộc lãnh thổ quốc gia mình mà dữ liệu ấy được tiếp cận một cách hợp pháp hoặc sẵn có đối với hệ thống máy tính đầu tiên, cơ quan chức năng sẽ có khả năng mở rộng một cách nhanh chóng việc khám xét hoặc các biện pháp tương tự để truy cập hệ thống máy tính khác.

3. Quốc gia thành viên Công ước phải ban hành luật hoặc các biện pháp cần thiết khác để trao thẩm quyền cho cơ quan chức năng thực hiện việc thu giữ hoặc các biện pháp tương tự khác bảo đảm an toàn cho dữ liệu máy tính đã được truy cập theo khoản 1 và khoản 2. Các biện pháp này bao gồm thẩm quyền thực hiện việc:

a) Thu giữ hoặc các biện pháp khác bảo đảm an toàn cho hệ thống máy tính hoặc một phần của hệ thống máy tính hoặc phương tiện lưu trữ dữ liệu máy tính;

b) Nhân bản hoặc giữ bản sao của dữ liệu máy tính này;

c) Duy trì sự toàn vẹn của dữ liệu máy tính được lưu trữ có liên quan;

d) Làm cho không truy cập được hoặc mang các dữ liệu máy tính này ra khỏi hệ thống máy tính đã được truy cập.

4. Quốc gia thành viên Công ước phải ban hành luật hoặc các biện pháp cần thiết khác để trao thẩm quyền cho cơ quan chức năng buộc bất cứ người nào biết về các hoạt động của hệ thống máy tính hoặc các biện pháp được áp dụng để bảo vệ dữ liệu máy tính cung cấp, một cách hợp lý, các thông tin cần thiết, để tạo khả năng cho việc áp dụng các biện pháp đề cập trong khoản 1 và khoản 2 Điều này.

5. Thẩm quyền và trình tự, thủ tục nêu tại Điều này được thực hiện theo quy định tại Điều 14 và Điều 15.

Nhóm 5

Thu thập dữ liệu máy tính trong thời gian thực

Điều 20. ***Thu thập dữ liệu máy tính trong thời gian thực***

1. Quốc gia thành viên Công ước phải ban hành luật hoặc các biện pháp cần thiết khác để trao thẩm

quyền cho cơ quan chức năng thực hiện:

a) Thu thập hoặc ghi lại, bằng cách áp dụng các biện pháp kỹ thuật trên lãnh thổ của quốc gia đó; hoặc

b) Hợp tác và hỗ trợ cơ quan chức năng trong việc thu thập và ghi lại dữ liệu lưu thông, trong thời gian thực, có gắn với các liên lạc đang được điều tra trong lãnh thổ quốc gia mình được truyền qua hệ thống máy tính.

2. Trường hợp quốc gia thành viên Công ước, vì các nguyên tắc đã được quy định trong luật quốc gia mình không thể áp dụng các biện pháp nêu tại khoản 1.a, quốc gia này phải áp dụng các biện pháp pháp lý hoặc biện pháp khác thay thế cần thiết để bảo đảm việc thu thập hoặc ghi lại trong thời gian thực dữ liệu lưu thông gắn với các liên lạc được truyền tải trong lãnh thổ quốc gia mình thông qua việc áp dụng các phương tiện kỹ thuật trên lãnh thổ đó.

3. Quốc gia thành viên Công ước phải ban hành luật hoặc các biện pháp cần thiết khác để quy định nghĩa vụ cho nhà cung cấp dịch vụ phải giữ bí mật đối với việc thực thi thẩm quyền quy định trong Điều này và bất cứ thông tin nào liên quan tới việc thực thi ấy.

4. Thẩm quyền và trình tự, thủ tục nêu tại Điều này

được thực hiện theo quy định tại Điều 14 và Điều 15.

Điều 21. ***Chặn dữ liệu nội dung***

1. Quốc gia thành viên phải ban hành luật hoặc các biện pháp cần thiết khác liên quan đến các loại tội phạm nghiêm trọng được quy định trong luật của quốc gia mình, để trao thẩm quyền cho các cơ quan chức năng thực hiện:

a) Thu thập hoặc ghi lại việc áp dụng các biện pháp kỹ thuật trên lãnh thổ của quốc gia ấy, và

b) Buộc nhà cung cấp dịch vụ, trong khả năng kỹ thuật của mình:

(i) Thu thập hoặc ghi lại thông qua việc áp dụng các phương tiện kỹ thuật trên lãnh thổ của quốc gia đó, hoặc

(ii) Hợp tác và hỗ trợ cơ quan chức năng thu thập hoặc ghi lại, dữ liệu nội dung, trong thời gian thực, của các liên lạc cụ thể trong lãnh thổ quốc gia mình được truyền tải qua hệ thống máy tính.

2. Trường hợp quốc gia thành viên Công ước, vì các nguyên tắc đã được quy định trong luật quốc gia mình, không thể áp dụng các biện pháp nêu tại khoản 1.a quốc gia này phải áp dụng các biện pháp pháp lý

hoặc biện pháp khác thay thế cần thiết để bảo đảm việc thu thập hoặc ghi lại trong thời gian thực dữ liệu nội dung gắn với các liên lạc được truyền tải trong lãnh thổ quốc gia mình thông qua việc áp dụng các phương tiện kỹ thuật trên lãnh thổ đó.

3. Quốc gia thành viên Công ước phải ban hành luật hoặc các biện pháp cần thiết khác để quy định nghĩa vụ cho nhà cung cấp dịch vụ phải giữ bí mật đối với việc thực thi thẩm quyền quy định trong Điều này và bất cứ thông tin nào liên quan tới việc thực thi ấy.

4. Thẩm quyền và trình tự, thủ tục nêu tại Điều này được thực hiện theo quy định tại Điều 14 và Điều 15.

Mục 3
THẨM QUYỀN TÀI PHÁN

Điều 22. *Thẩm quyền tài phán*

1. Quốc gia thành viên phải ban hành luật hoặc các biện pháp cần thiết khác để thiết lập thẩm quyền tài phán đối với bất cứ tội phạm nào quy định từ Điều 2 đến Điều 11 của Công ước khi tội phạm ấy được thực hiện:

a) Trong lãnh thổ quốc gia mình; hoặc

b) Trên tàu mang cờ hiệu của quốc gia mình; hoặc

c) Trên máy bay đăng ký theo luật của quốc gia mình; hoặc

d) Bởi công dân của quốc gia mình, nếu tội phạm bị trừng phạt theo luật hình sự nơi thực hiện hành vi hoặc khi tội phạm được thực hiện ngoài thẩm quyền tài phán của bất cứ quốc gia thành viên Công ước.

2. Quốc gia thành viên Công ước có quyền bảo lưu không áp dụng hoặc chỉ áp dụng trong một số trường hợp đặc biệt hoặc theo điều kiện nhất định quy tắc về thẩm quyền tài phán quy định từ khoản 1.b đến 1.d của Điều này hoặc bất cứ phần nào trong đó.

3. Quốc gia thành viên Công ước phải áp dụng các biện pháp cần thiết để thiết lập quyền tài phán đối với các tội phạm quy định tại khoản 1 Điều 24 Công ước, trong các trường hợp người bị cáo buộc là phạm tội đang có mặt trong lãnh thổ quốc gia mình và sẽ không dẫn độ người chỉ vì lý do quốc tịch của người đó sau khi có yêu cầu dẫn độ.

4. Công ước này không loại trừ bất cứ thẩm quyền tài phán về hình sự nào mà quốc gia thành viên Công ước thực hiện theo luật của quốc gia mình.

5. Trường hợp nhiều quốc gia thành viên Công ước

đều cho rằng mình có thẩm quyền tài phán đối với hành vi phạm tội quy định trong Công ước thì các quốc gia thành viên phải tham vấn với nhau, nếu thấy hợp lý, để xác định quốc gia hợp lý nhất nên tiến hành việc truy tố.

Chương III

HỢP TÁC QUỐC TẾ

Mục 1

CÁC NGUYÊN TẮC CHUNG

Nhóm 1
Các nguyên tắc chung liên quan đến hợp tác quốc tế

Điều 23. ***Các nguyên tắc chung liên quan đến hợp tác quốc tế***

Các quốc gia thành viên phải hợp tác với nhau, phù hợp với các quy định trong chương này, và thông qua việc áp dụng các văn bản quốc tế về hợp tác quốc tế trong lĩnh vực hình sự, các thỏa thuận hợp tác trên

cơ sở luật hợp nhất hoặc có đi có lại, và luật của quốc gia mình, với phạm vi rộng nhất có thể để phục vụ việc điều tra, tố tụng liên quan đến các tội phạm hình sự có liên quan đến hệ thống máy tính và dữ liệu máy tính, hoặc để thu thập chứng cứ dưới hình thức điện tử.

Nhóm 2
Các nguyên tắc liên quan đến việc dẫn độ

Điều 24. *Dẫn độ*

1. a) Điều luật này được áp dụng đối với việc dẫn độ giữa các quốc gia thành viên Công ước đối với các tội phạm được quy định phù hợp với các điều từ Điều 2 đến Điều 11 Công ước này với điều kiện tội phạm ấy bị trừng phạt về mặt hình sự theo pháp luật của cả hai quốc gia có liên quan với hình phạt tước đoạt tự do tối đa một năm trở lên hoặc bởi hình phạt nặng hơn.

b) Trường hợp các bên có thỏa thuận về mức hình phạt nhẹ hơn vẫn bị dẫn độ theo nguyên tắc luật hợp nhất hoặc nguyên tắc có đi có lại hoặc theo các hiệp định dẫn độ, bao gồm Công ước châu Âu về dẫn độ tội

phạm (ETS No. 24), thì các thỏa thuận này sẽ được ưu tiên áp dụng.

2. Các tội phạm được mô tả trong khoản 1 Điều này được hiểu bao gồm cả loại tội phạm có thể bị dẫn độ theo hiệp định dẫn độ đang tồn tại giữa các quốc gia thành viên Công ước.

3. Nếu một quốc gia thành viên Công ước quy định việc dẫn độ phải có điều kiện là có hiệp định dẫn độ với quốc gia thành viên Công ước khác, mà hiện tại giữa các quốc gia này chưa có hiệp định dẫn độ, thì quốc gia thành viên Công ước có thể coi Công ước này là cơ sở pháp lý cho việc dẫn độ đối với các tội phạm quy định tại khoản 1 Điều này.

4. Các quốc gia thành viên Công ước không quy định việc dẫn độ phải có điều kiện là có hiệp định dẫn độ với quốc gia thành viên Công ước khác thì các quốc gia này phải coi tội phạm quy định trong khoản 1 Điều này là tội phạm có thể bị dẫn độ giữa các quốc gia thành viên Công ước.

5. Việc dẫn độ phải tuân theo các điều kiện quy định bởi luật của quốc gia được yêu cầu dẫn độ hoặc bởi các hiệp định dẫn độ, bao gồm căn cứ mà quốc gia được yêu cầu dẫn độ từ chối việc dẫn độ.

6. Trường hợp việc dẫn độ đối với loại tội quy định tại khoản 1 Điều này bị từ chối chỉ vì lý do quốc tịch của người bị yêu cầu dẫn độ hoặc bởi quốc gia được yêu cầu dẫn độ cho rằng mình có quyền tài phán đối với tội phạm này thì quốc gia được yêu cầu dẫn độ phải đệ trình vụ việc, theo yêu cầu của quốc gia yêu cầu dẫn độ, lên cơ quan chức năng của mình để truy tố và phải thông báo kết quả giải quyết cuối cùng cho quốc gia yêu cầu dẫn độ biết trong thời hạn hợp lý. Cơ quan chức năng này phải ra quyết định và tiến hành điều tra, tố tụng theo cách thức tương tự với cách thức áp dụng đối với loại tội có bản chất tương tự theo luật của quốc gia mình.

7. a) Quốc gia thành viên Công ước, tại thời điểm ký kết hoặc khi ký thác văn bản phê chuẩn, chấp thuận, phê duyệt hoặc gia nhập, phải thông báo cho Tổng thư ký Hội đồng châu Âu tên và địa chỉ của cơ quan chức năng chịu trách nhiệm việc đưa và tiếp nhận yêu cầu dẫn độ hoặc tạm giữ trong trường hợp không có hiệp định.

b) Tổng thư ký Hội đồng châu Âu phải thiết lập và cập nhật bản đăng ký các cơ quan chức năng được chỉ định ở trên bởi quốc gia thành viên Công ước. Quốc

gia thành viên Công ước phải bảo đảm rằng các chi tiết trên bản đăng ký luôn luôn chính xác.

Nhóm 3
Nguyên tắc chung liên quan đến việc tương trợ tư pháp

Điều 25. ***Nguyên tắc chung liên quan đến việc tương trợ tư pháp***

1. Quốc gia thành viên Công ước phải đảm bảo cung cấp sự tương trợ tư pháp rộng lớn nhất có thể để phục vụ hoạt động điều tra hoặc tố tụng liên quan đến các tội phạm về hệ thống máy tính hoặc dữ liệu máy tính hoặc việc thu thập các chứng cứ dưới hình thức điện tử về các tội phạm.

2. Quốc gia thành viên Công ước phải ban hành luật và các biện pháp cần thiết khác để thực hiện các nghĩa vụ quy định từ Điều 27 đến Điều 35.

3. Các quốc gia thành viên Công ước, trong trường hợp khẩn cấp, có thể đưa ra các yêu cầu tương trợ tư pháp hoặc các liên lạc có liên quan bằng các phương tiện liên lạc nhanh, bao gồm fax hoặc thư điện tử,

trong phạm vi mà các biện pháp ấy đảm bảo mức độ hợp lý về an ninh và tính xác thực (bao gồm cả việc sử dụng mật mã khi cần thiết), với sự xác nhận chính thức sau đó, khi được yêu cầu bởi bên được yêu cầu tương trợ. Bên được yêu cầu tương trợ phải chấp nhận và phản hồi yêu cầu bằng phương thức liên lạc nhanh.

4. Trừ trường hợp được quy định cụ thể trong Chương này, tương trợ tư pháp phải được thực hiện theo các điều kiện quy định trong luật của quốc gia được yêu cầu tương trợ hoặc theo các hiệp định tương trợ tư pháp, bao gồm cả các căn cứ bên được yêu cầu tương trợ có thể từ chối sự hợp tác. Bên được yêu cầu tương trợ không được từ chối tương trợ tư pháp về các tội phạm đề cập từ Điều 2 đến Điều 11 chỉ với lý do là yêu cầu đó liên quan đến tội phạm được coi là tội phạm ngân sách.

5. Tuỳ trường hợp, phù hợp với quy định của Chương này, bên được yêu cầu tương trợ có thể buộc việc tương trợ tư pháp tuân theo các điều kiện về tội phạm kép. Điều kiện này được coi là thỏa mãn bất kể luật của các quốc gia có liên quan coi hành vi phạm tội có cùng một loại tội hay không, có cùng tên gọi hay không, miễn là hành vi đó bị coi là tội phạm bởi luật của cả quốc gia yêu cầu dẫn độ và quốc gia được

đề nghị dẫn độ.

Điều 26. ***Thông tin đột xuất***

1. Quốc gia thành viên Công ước có thể, trong phạm vi giới hạn luật quốc gia mình và không có yêu cầu trước, chuyển cho quốc gia thành viên Công ước khác các thông tin thu thập được trong quá trình điều tra của mình nếu như quốc gia này thấy việc tiết lộ thông tin ấy có thể giúp cho quốc gia tiếp nhận thông tin khởi động hoặc tiến hành điều tra hoặc hoạt động tố tụng về tội phạm quy định trong Công ước này hoặc có thể dẫn đến việc yêu cầu hợp tác bởi quốc gia đó theo quy định của Chương này.

2. Trước khi cung cấp thông tin đó, quốc gia cung cấp thông tin có thể yêu cầu thông tin đó phải được giữ bí mật hoặc chỉ được sử dụng theo các điều kiện nhất định. Nếu quốc gia tiếp nhận thông tin không thể tuân thủ với các yêu cầu đó, quốc gia này phải thông báo cho quốc gia dự định cung cấp thông tin để quốc gia dự định cung cấp thông tin cân nhắc liệu có nên cung cấp thông tin không. Nếu quốc gia tiếp nhận thông tin chấp nhận các điều kiện của việc cung cấp thông tin thì các điều kiện này sẽ có giá trị ràng buộc đối với quốc gia này.

Nhóm 4

Trình tự, thủ tục liên quan đến yêu cầu tương trợ tư pháp trong trường hợp không có điều ước quốc tế được áp dụng

Điều 27. ***Trình tự, thủ tục liên quan đến yêu cầu tương trợ tư pháp trong trường hợp không có điều ước quốc tế được áp dụng***

1. Trường hợp không có hiệp định tương trợ tư pháp hoặc các thỏa thuận về việc áp dụng luật thống nhất hoặc về việc áp dụng nguyên tắc có đi có lại điều chỉnh quan hệ giữa bên yêu cầu tương trợ và bên được yêu cầu tương trợ, các quy định từ khoản 2 đến khoản 9 của Điều này sẽ được áp dụng. Các quy định của Điều này sẽ không được áp dụng trong trường hợp có các hiệp định, thỏa thuận hoặc đạo luật đó tồn tại, trừ trường hợp các bên có liên quan thỏa thuận đồng ý áp dụng tất cả hoặc bất cứ phần nào trong Điều này thay thế cho các hiệp định, thỏa thuận hoặc đạo luật đó.

2. a) Quốc gia thành viên Công ước phải chỉ định một cơ quan chức năng ở trung ương chịu trách nhiệm

về việc gửi và trả lời các yêu cầu về tương trợ tư pháp, việc thực thi các yêu cầu đó hoặc chuyển cho cơ quan chức năng để thực thi;

b) Các cơ quan trung ương này sẽ liên lạc trực tiếp với nhau;

c) Quốc gia thành viên Công ước, tại thời điểm ký kết hoặc ký thác văn bản phê chuẩn, chấp thuận, phê duyệt hoặc xin gia nhập, phải thông báo cho Tổng thư ký Hội đồng châu Âu tên, địa chỉ của cơ quan được chỉ định phù hợp với khoản này;

d) Tổng thư ký Hội đồng châu Âu phải thiết lập và cập nhật một bản đăng ký các cơ quan trung ương được chỉ định bởi các quốc gia thành viên Công ước. Các quốc gia thành viên Công ước phải bảo đảm rằng các thông tin chi tiết mình cung cấp vào bản đăng ký của Hội đồng châu Âu là luôn luôn chính xác.

3. Các yêu cầu tương trợ tư pháp theo Điều này phải được thực thi phù hợp với các trình tự, thủ tục quy định bởi bên yêu cầu tương trợ trừ trường hợp không phù hợp với luật của quốc gia được yêu cầu tương trợ.

4. Quốc gia được yêu cầu tương trợ, bên cạnh các căn cứ từ chối quy định tại khoản 4 Điều 25, có thể từ

chối tương trợ nếu:

a) Yêu cầu liên quan đến tội phạm mà bên được yêu cầu tương trợ coi đó là tội phạm chính trị hoặc tội phạm liên quan đến tội phạm chính trị, hoặc;

b) Quốc gia này xét thấy việc thực thi yêu cầu đó có khả năng làm phương hại đối với chủ quyền, an ninh, trật tự công cộng hoặc các lợi ích thiết yếu khác.

5. Quốc gia được yêu cầu tương trợ có thể tạm hoãn thực hiện yêu cầu nếu như việc thực hiện yêu cầu có ảnh hưởng tiêu cực đến quá trình điều tra hình sự hoặc hoạt động tố tụng do các cơ quan chức năng tiến hành.

6. Trước khi từ chối hoặc tạm hoãn việc tương trợ tư pháp, quốc gia được yêu cầu tương trợ, khi thấy hợp lý và đã tham vấn với quốc gia yêu cầu tương trợ, phải cân nhắc xem liệu yêu cầu có thể được thực hiện một phần hoặc được thực hiện nhưng theo các điều kiện mà quốc gia này cho là cần thiết.

7. Quốc gia được yêu cầu tương trợ phải thông báo ngay cho quốc gia yêu cầu tương trợ về kết quả thực hiện việc tương trợ. Trường hợp từ chối hoặc tạm hoãn việc thực hiện yêu cầu thì phải nêu lý do. Quốc gia được yêu cầu tương trợ phải thông báo cho quốc gia

yêu cầu tương trợ về lý do làm cho không thể thực hiện được yêu cầu hoặc có khả năng trì hoãn một cách đáng kể việc thực hiện yêu cầu.

8. Quốc gia yêu cầu tương trợ có quyền yêu cầu quốc gia được yêu cầu tương trợ phải giữ bí mật đối với nội dung trong yêu cầu nêu trong Chương này ngoại trừ trường hợp phục vụ chính việc thực thi yêu cầu. Nếu quốc gia được yêu cầu tương trợ không thể tuân thủ được yêu cầu về việc giữ bí mật, quốc gia này phải thông báo ngay cho quốc gia yêu cầu tương trợ để quốc gia yêu cầu tương trợ sẽ quyết định liệu có nên tiếp tục yêu cầu tương trợ hay không.

9. a) Trong trường hợp khẩn cấp, yêu cầu tương trợ hoặc các liên lạc liên quan có thể gửi trực tiếp bởi cơ quan tư pháp của quốc gia yêu cầu tương trợ đến cơ quan tương ứng của quốc gia được yêu cầu tương trợ. Trong trường hợp ấy, bản sao của yêu cầu phải được gửi đồng thời cho cơ quan trung ương của quốc gia được yêu cầu thông qua cơ quan trung ương của quốc gia yêu cầu.

b) Bất cứ yêu cầu hoặc liên lạc được thực hiện theo khoản này đều có thể thực hiện thông qua Tổ chức Cảnh sát hình sự quốc tế (Interpol).

c) Trường hợp yêu cầu được thực hiện theo tiểu khoản 9.a của Điều này và cơ quan được yêu cầu không có khả năng xử lý yêu cầu, cơ quan này phải gửi tới cơ quan chức năng có thẩm quyền của quốc gia được yêu cầu và thông báo trực tiếp cho quốc gia yêu cầu về việc đó.

d) Yêu cầu hoặc liên lạc neu tai khoản này không liên quan đến các hành động cưỡng chế có thể được truyền tải trực tiếp bởi cơ quan chức năng của quốc gia yêu cầu đến cơ quan chức năng của quốc gia được yêu cầu.

e) Quốc gia thành viên Công ước, tại thời điểm ký kết hoặc ký thác văn bản phê chuẩn, chấp thuận, phê duyệt hoặc xin gia nhập, có thể thông báo cho Tổng thư ký Hội đồng châu Âu rằng, để đảm bảo tính hiệu quả, các yêu cầu được nêu trong khoản này phải được gửi tới cơ quan trung ương của mình.

Điều 28. ***Bí mật và hạn chế sử dụng***

1. Trường hợp không có hiệp định tương trợ tư pháp hoặc thỏa thuận trên cơ sở đạo luật thống nhất hoặc nguyên tắc có đi có lại đang có hiệu lực giữa quốc gia yêu cầu và quốc gia được yêu cầu thì các quy định trong Điều này sẽ được áp dụng. Các quy định trong

điều này không được áp dụng trong trường hợp các hiệp định, thỏa thuận hoặc đạo luật nêu trên tồn tại, trừ khi các quốc gia thành viên có liên quan thỏa thuận sẽ áp dụng tất cả hay một phần của Điều này thay thế cho các văn bản đó.

2. Quốc gia được yêu cầu có thể cung cấp thông tin hoặc tài liệu tương ứng với yêu cầu theo các điều kiện cụ thể là:

a) Thông tin hoặc tài liệu ấy phải được giữ bí mật nếu không thì sẽ không thực hiện yêu cầu tương trợ;

b) Thông tin hoặc tài liệu ấy không được sử dụng để điều tra hoặc tố tụng ngoài hoạt động điều tra hoặc tố tụng đã nêu trong yêu cầu.

3. Nếu quốc gia yêu cầu không thể tuân thủ điều kiện nêu tại khoản 2 thì quốc gia này phải thông báo ngay cho quốc gia được yêu cầu biết để quốc gia được yêu cầu cân nhắc liệu có cung cấp thông tin, tài liệu hay không. Trường hợp quốc gia yêu cầu chấp nhận các điều kiện thì các điều kiện này sẽ ràng buộc quốc gia này.

4. Quốc gia cung cấp thông tin hoặc tài liệu theo điều kiện nhất định nêu tại khoản 2 Điều này có quyền yêu cầu quốc gia nhận thông tin giải thích việc sử dụng thông tin, tài liệu đó theo các điều kiện đã đặt ra.

Mục 2
CÁC QUY ĐỊNH CỤ THỂ

Nhóm 1
Tương trợ tư pháp liên quan đến các biện pháp tạm thời

Điều 29. ***Bảo quản khẩn cấp dữ liệu máy tính được lưu trữ***

1. Quốc gia thành viên Công ước có thể yêu cầu quốc gia thành viên Công ước khác ra lệnh hoặc thực hiện biện pháp khác để có được sự bảo quản khẩn cấp các dữ liệu được lưu trữ bởi hệ thống máy tính đang nằm trên lãnh thổ quốc gia được yêu cầu. Liên quan tới việc ấy quốc gia yêu cầu có ý định gửi yêu cầu tương trợ tư pháp để khám xét hoặc các biện pháp tương tự khác truy cập, thu giữ hoặc các biện pháp tương tự khác bảo đảm an toàn, hoặc tiết lộ dữ liệu.

2. Yêu cầu bảo quản dữ liệu theo khoản 1 Điều này phải nêu rõ:

a) Cơ quan yêu cầu việc bảo quản dữ liệu;

b) Loại tội phạm đang được điều tra hoặc tố tụng

và bản tóm tắt các tình tiết có liên quan;

c) Dữ liệu máy tính đang được lưu trữ muốn được bảo quản và mối quan hệ của nó với tội phạm đang được điều tra, tố tụng;

d) Các thông tin sẵn có nhận diện người quản lý dữ liệu máy tính đang được lưu trữ hoặc địa điểm của hệ thống máy tính;

e) Sự cần thiết của việc bảo quản; và

f) Rằng quốc gia yêu cầu đang có ý định gửi yêu cầu tương trợ tư pháp để khám xét hoặc các biện pháp truy cập tương tự, thu giữ hoặc các biện pháp bảo đảm an toàn tương tự, hoặc tiết lộ dữ liệu máy tính đang được lưu trữ.

3. Khi nhận được yêu cầu từ quốc gia khác, quốc gia được yêu cầu phải thực hiện tất cả các biện pháp cần thiết để giữ gìn một cách nhanh chóng dữ liệu đã được chỉ định phù hợp với quy định trong luật quốc gia mình. Để đáp ứng yêu cầu, tội phạm kép không được coi là điều kiện để cung cấp sự bảo quản đó.

4. Quốc gia thành viên Công ước đòi hỏi phải có tội phạm kép là điều kiện để đáp ứng yêu cầu tương trợ tư pháp trong việc khám xét hoặc thực hiện các biện pháp tương tự để truy cập dữ liệu, thu giữ hoặc thực

hiện các biện pháp bảo đảm khác, hoặc tiết lộ dữ liệu máy tính đang được lưu trữ có thể, đối với các tội ngoài các tội quy định từ Điều 2 đến Điều 11 của Công ước này, bảo lưu quyền từ chối yêu cầu giữ gìn dữ liệu nêu trong Điều này trong các trường hợp quốc gia này có lý do hợp lý để tin rằng tại thời điểm tiết lộ, điều kiện tội phạm kép không thể đáp ứng.

5. Thêm vào đó, yêu cầu bảo quản dữ liệu chỉ có thể bị từ chối nếu:

a) Yêu cầu liên quan đến tội phạm mà quốc gia được yêu cầu coi đó là tội phạm chính trị hoặc tội phạm liên quan đến tội phạm chính trị, hoặc

b) Quốc gia được yêu cầu coi việc thực thi yêu cầu tương trợ có khả năng gây tổn thương tới chủ quyền, an ninh, trật tự công cộng hoặc các lợi ích thiết yếu khác.

6. Trường hợp quốc gia được yêu cầu thấy rằng việc giữ gìn dữ liệu không đảm bảo sự sẵn có của dữ liệu được cung cấp trong tương lai hoặc có khả năng làm lộ bí mật hoặc gây tổn hại tới hoạt động điều tra của quốc gia yêu cầu, quốc gia được yêu cầu phải thông báo ngay cho quốc gia yêu cầu để quốc gia yêu cầu cân nhắc có nên thực thi yêu cầu hay không.

7. Bất cứ sự giữ gìn dữ liệu nào được thực hiện

theo yêu cầu quy định tại khoản 1 Điều này phải được thực hiện trong thời hạn không ít hơn 60 ngày, để tạo khả năng cho quốc gia yêu cầu đệ trình bản yêu cầu khám xét hoặc các biện pháp tương tự khác để truy cập, thu giữ hoặc các biện pháp tương tự khác bảo đảm an toàn, hoặc tiết lộ dữ liệu. Sau khi nhận được yêu cầu đó, dữ liệu phải tiếp tục được giữ gìn chờ có quyết định về yêu cầu đó.

Điều 30. ***Tiết lộ nhanh dữ liệu lưu thông được bảo quản***

1. Trường hợp, trong quá trình thực thi yêu cầu theo quy định tại Điều 29 để giữ gìn dữ liệu lưu thông liên quan đến một liên lạc cụ thể, quốc gia được yêu cầu phát hiện thấy nhà cung cấp dịch vụ ở quốc gia khác có liên quan đến việc truyền tải liên lạc, quốc gia được yêu cầu sẽ nhanh chóng tiết lộ cho quốc gia yêu cầu lượng dữ liệu lưu thông đủ lớn để nhận ra nhà cung cấp dịch vụ đó và đường mà liên lạc được truyền tải.

2. Việc tiết lộ dữ liệu lưu thông nêu tại khoản 1 Điều này chỉ có thể bị từ chối nếu:

a) Yêu cầu liên quan đến tội phạm mà bên được yêu cầu tương trợ coi đó là tội phạm chính trị hoặc tội phạm liên quan đến tội phạm chính trị, hoặc

b) Quốc gia này xét thấy việc thực thi yêu cầu đó có khả năng làm thương tổn đối với chủ quyền, an ninh, trật tự công cộng hoặc các lợi ích thiết yếu khác.

Nhóm 2
Tương trợ tư pháp đối với thẩm quyền điều tra

Điều 31. ***Tương trợ tư pháp trong việc truy cập các dữ liệu máy tính được lưu trữ***

1. Quốc gia thành viên Công ước có quyền yêu cầu quốc gia thành viên Công ước khác tiến hành khám xét hoặc truy cập, thu giữ hoặc các bảo đảm tương tự, và tiết lộ dữ liệu lưu trữ bởi hệ thống máy tính trên lãnh thổ của quốc gia được yêu cầu, bao gồm cả dữ liệu đã được gìn giữ theo Điều 29.

2. Quốc gia được yêu cầu phải đáp ứng yêu cầu thông qua việc áp dụng các văn bản, thỏa thuận và luật quốc tế nêu tại Điều 23 và phù hợp với các quy định khác có liên quan trong Chương này.

3. Yêu cầu phải được đáp ứng một cách nhanh chóng nếu:

a) Có cơ sở để tin rằng dữ liệu liên quan là đặc biệt

dễ bị mất hoặc điều chỉnh; hoặc

b) Văn bản, thỏa thuận và luật đề cập tại khoản 2 có quy định về việc hỗ trợ nhanh chóng.

Điều 32. ***Truy cập xuyên biên giới đối với dữ liệu máy tính được lưu trữ với sự đồng ý hoặc khi được cung cấp một cách công khai***

Quốc gia thành viên có thể, ngay cả khi không có sự cho phép của quốc gia khác:

a) Tiếp cận một cách công khai dữ liệu máy tính được lưu trữ sẵn có (nguồn mở), bất kể dữ liệu này nằm ở khu vực địa lý nào; hoặc

b) Truy cập hoặc tiếp nhận, thông qua hệ thống máy tính ở trên lãnh thổ của mình, dữ liệu máy tính được lưu trữ đang nằm ở quốc gia thành viên Công ước, nếu quốc gia yêu cầu nhận được sự đồng ý một cách hợp pháp và tự nguyện của người đang có thẩm quyền hợp pháp tiết lộ dữ liệu cho quốc gia yêu cầu thông qua hệ thống máy tính đó.

Điều 33. ***Tương trợ tư pháp khi thu thập dữ liệu lưu thông trong thời gian thực***

1. Quốc gia thành viên Công ước phải tương trợ tư pháp đối với nhau trong việc thu thập dữ liệu lưu thông

trong thời gian thực có liên quan với liên lạc được điều tra trong lãnh thổ của mình được truyền tải qua hệ thống máy tính. Theo các quy định tại khoản 2 Điều này, sự tương trợ này sẽ được điều chỉnh bởi các điều kiện, trình tự và thủ tục quy định trong luật của các quốc gia.

2. Quốc gia thành viên Công ước phải cung cấp sự tương trợ tối thiểu là với các tội phạm mà việc thu thập dữ liệu là sẵn có trong hồ sơ vụ việc tương tự quốc gia mình đang tiến hành.

Điều 34. ***Tương trợ tư pháp đối với việc chặn dữ liệu nội dung***

Quốc gia thành viên phải tương trợ tư pháp đối với nhau trong việc thu thập hoặc ghi lại trong thời gian thực dữ liệu nội dung của các liên lạc đã chỉ định được truyền tải bởi hệ thống máy tính trong phạm vi cho phép theo hiệp định được áp dụng và luật của quốc gia mình.

Nhóm 3
Mạng lưới 24/7

Điều 35. ***Mạng lưới 24/7***

1. Quốc gia thành viên Công ước phải chỉ định một

(điểm liên lạc) hoạt động 24 giờ một ngày và 7 ngày trong tuần để cung cấp sự hỗ trợ kịp thời việc điều tra hoặc tố tụng đối với tội phạm liên quan đến hệ thống máy tính hoặc dữ liệu máy tính, thu thập chứng cứ dưới hình thức điện tử. Sự hỗ trợ ấy bao gồm hỗ trợ, hoặc, nếu được cho phép bởi luật và thực tiễn quốc gia, trực tiếp tiến hành các biện pháp sau đây:

a) Cung cấp các lời tư vấn kỹ thuật;

b) Bảo quản dữ liệu theo Điều 29 và Điều 30;

c) Thu thập chứng cứ, cung cấp thông tin pháp lý và địa điểm của bị can.

2. a) Điểm liên lạc của quốc gia thành viên Công ước phải có năng lực thực thi các liên lạc với điểm liên lạc của quốc gia thành viên Công ước khác một cách nhanh chóng.

b) Nếu điểm liên lạc chỉ định bởi quốc gia thành viên Công ước không phải là một bộ phận của cơ quan chức năng của quốc gia thành viên Công ước chịu trách nhiệm về việc hỗ trợ tư pháp quốc tế hoặc dẫn độ, điểm liên lạc phải đảm bảo rằng nó có thể điều phối với cơ quan chức năng kể trên một cách nhanh chóng.

3. Quốc gia thành viên Công ước phải bảo đảm sự

sẵn có của đội ngũ nhân sự được đào tạo và trang bị để hỗ trợ sự hoạt động của mạng lưới.

Chương IV

CÁC QUY ĐỊNH CUỐI CÙNG

Điều 36. ***Ký kết và có hiệu lực***

1. Công ước này được để mở cho việc ký kết bởi quốc gia thành viên Hội đồng châu Âu và quốc gia không phải thành viên Hội đồng châu Âu nhưng đã tham gia soạn thảo Công ước.

2. Công ước này phụ thuộc vào việc phê chuẩn, chấp thuận hoặc phê duyệt. Văn bản phê chuẩn, chấp thuận hoặc phê duyệt sẽ được lưu trữ bởi Tổng thư ký Hội đồng châu Âu.

3. Công ước này sẽ phát sinh hiệu lực vào ngày đầu tiên của tháng ngay sau khi hết thời hạn 03 tháng kể từ ngày 05 quốc gia, trong đó ít nhất là 03 quốc gia thành viên Hội đồng châu Âu, bày tỏ sự đồng ý ràng buộc bởi Công ước này phù hợp với các quy định tại khoản 1 và khoản 2 Điều này.

4. Đối với quốc gia bày tỏ sự đồng ý ràng buộc bởi Công ước sau thời điểm kể trên thì Công ước sẽ phát

sinh hiệu lực kể từ ngày đầu tiên của tháng kế tiếp thời điểm hết thời hạn 03 tháng kể từ ngày quốc gia bày tỏ đồng ý ràng buộc bởi Công ước phù hợp với các quy định tại khoản 1 và khoản 2 Điều này.

Điều 37. ***Gia nhập Công ước***

1. Sau khi Công ước có hiệu lực, Hội đồng Bộ trưởng của Hội đồng Châu Âu, sau khi tham vấn và nhận được sự đồng thuận tuyệt đối của các quốc gia thành viên Công ước, có thể mời bất cứ quốc gia nào không phải là thành viên Hội đồng châu Âu và không tham gia quá trình soạn thảo Công ước gia nhập Công ước này. Việc ra quyết định sẽ được tiến hành theo nguyên tắc biểu quyết theo đa số quy định tại Điều 20.d Luật Hội đồng châu Âu và bởi sự nhất trí tuyệt đối của các đại diện quốc gia thành viên có quyền tham gia Hội đồng Bộ trưởng.

2. Quốc gia muốn gia nhập Công ước theo khoản 1 Điều này, Công ước sẽ có hiệu lực vào ngày đầu tiên của tháng kế tiếp thời điểm hết thời hạn 03 tháng kể từ ngày Tổng thư ký Hội đồng châu Âu lưu trữ văn bản đề nghị gia nhập.

Điều 38. ***Áp dụng theo lãnh thổ***

1. Quốc gia thành viên Công ước, tại thời điểm ký

kết hoặc gửi lưu trữ văn bản phê chuẩn, chấp thuận, phê duyệt hoặc xin gia nhập, có quyền quy định vùng lãnh thổ mà Công ước sẽ được áp dụng.

2. Quốc gia thành viên Công ước, sau thời điểm kể trên, có thể, bằng việc ra tuyên bố gửi cho Tổng thư ký Hội đồng châu Âu, mở rộng việc áp dụng Công ước này đối với các vùng lãnh thổ khác được nêu trong tuyên bố. Đối với vùng lãnh thổ này, Công ước sẽ có hiệu lực kể từ ngày đầu tiên của tháng kế tiếp thời điểm hết thời hạn 03 tháng sau ngày Tổng thư ký Hội đồng châu Âu nhận được tuyên bố.

3. Các tuyên bố nêu tại 2 khoản kể trên về lãnh thổ được áp dụng Công ước có thể được rút lại bằng cách thông báo cho Tổng thư ký Hội đồng châu Âu. Việc rút lại tuyên bố này sẽ có hiệu lực kể từ ngày đầu tiên của tháng kế tiếp thời điểm hết thời hạn 03 tháng sau ngày Tổng thư ký Hội đồng châu Âu nhận được thông báo đó.

Điều 39. ***Áp dụng Công ước***

1. Mục đích của Công ước này là bổ sung các hiệp định hoặc thỏa thuận song phương hoặc đa phương giữa các quốc gia thành viên Công ước, bao gồm các quy định của:

- Công ước châu Âu về dẫn độ ngày 13/12/1957 (ETS No. 24);

- Công ước châu Âu về tương trợ tư pháp trong lĩnh vực hình sự ngày 20/4/1959 (ETS No. 30);

- Nghị định thư bổ sung Công ước về tương trợ tư pháp trong lĩnh vực hình sự ngày 17/3/1978 (ETS No. 99).

2. Nếu các quốc gia tham gia Công ước đã hoặc sẽ ký kết hiệp định hoặc thiết lập các quan hệ riêng về các vấn đề quy định trong Công ước này thì các hiệp định này sẽ được ưu tiên áp dụng giữa các quốc gia thành viên hiệp định. Tuy nhiên, các hiệp định này không được trái với mục tiêu và các nguyên tắc của Công ước này.

3. Không có quy định nào của Công ước này ảnh hưởng tới các quyền, nghĩa vụ và trách nhiệm khác của quốc gia thành viên Công ước.

Điều 40. ***Tuyên bố***

Bằng việc gửi văn bản thông báo cho Tổng thư ký Hội đồng châu Âu, quốc gia, tại thời điểm ký kết hoặc khi ký thác văn bản phê chuẩn, chấp thuận, phê duyệt hoặc gia nhập, quốc gia có thể tuyên bố rằng quốc gia mình tiếp nhận các khả năng yêu cầu các yếu

tố bổ sung quy định tại Điều 2, Điều 3, khoản 1.b Điều 6 , Điều 7, khoản 3 Điều 9 và khoản 9.e. Điều 27.

Điều 41. ***Điều khoản liên bang***

1. Quốc gia liên bang có thể bảo lưu các nghĩa vụ quy định tại Chương II của Công ước này phù hợp với các nguyên tắc cơ bản điều chỉnh mối quan hệ giữa chính quyền trung ương và chính quyền các bang hoặc các lãnh thổ tương tự với điều kiện điều này vẫn đảm bảo các hoạt động hợp tác quy định tại Chương III.

2. Khi đưa ra các bảo lưu như quy định tại khoản 1 Điều này, quốc gia liên bang không được áp dụng các điều khoản bảo lưu đó để loại trừ hoặc làm giảm một cách căn bản nghĩa vụ cung cấp các biện pháp quy định tại Chương II. Xét về tổng thể, quốc gia này phải đảm bảo năng lực thi hành pháp luật hiệu quả và đủ rộng đối với các biện pháp này.

3. Đối với các quy định của Công ước này mà việc áp dụng nó thuộc về thẩm quyền của chính quyền bang hoặc chính quyền lãnh thổ tương tự bang nhưng lại chưa được quy định trong Hiến pháp liên bang về việc phải có những biện pháp pháp lý, thì chính quyền liên bang phải thông báo cho các cơ quan chức năng của chính quyền bang về các quy định của Công ước

và khuyến khích các bang có các biện pháp phù hợp để đảm bảo hiệu lực của Công ước.

Điều 42. ***Bảo lưu***

Bằng việc gửi văn bản thông báo cho Tổng thư ký Hội đồng châu Âu, quốc gia, tại thời điểm ký kết hoặc khi ký thác văn bản phê chuẩn, chấp thuận, phê duyệt hoặc gia nhập, quốc gia có thể tuyên bố rằng quốc gia mình chấp nhận thực hiện các bảo lưu quy định tại khoản 2 Điều 4, khoản 3 Điều 6, khoản 4 Điều 9, khoản 3 Điều 10, khoản 3 Điều 11, khoản 3 Điều 14, khoản 2 Điều 22, khoản 4 Điều 29, và khoản 1 Điều 41. Ngoài các trường hợp trên, các quốc gia không được tuyên bố bảo lưu bất cứ quy định nào khác.

Điều 43. ***Việc rút lại bảo lưu***

1. Quốc gia thành viên Công ước đã tuyên bố bảo lưu theo quy định tại Điều 42 có quyền rút lại một phần hoặc tất cả các bảo lưu bằng cách gửi văn bản thông báo cho Tổng thư ký Hội đồng châu Âu. Việc rút lại bảo lưu đó có hiệu lực kể từ ngày Tổng thư ký Hội đồng châu Âu nhận được văn bản đề nghị rút lại bảo lưu. Trường hợp tuyên bố rút lại bảo lưu quy định rõ ngày phát sinh hiệu lực của việc rút lại bảo lưu mà

ngày đó sau ngày Tổng thư ký Hội đồng châu Âu nhận được văn bản đề nghị rút lại bảo lưu thì thời điểm có hiệu lực của việc rút lại bảo lưu là ngày mà văn bản đề nghị rút lại bảo lưu đã quy định.

2. Quốc gia thành viên Công ước đã tuyên bố bảo lưu theo quy định tại Điều 42 phải rút lại các bảo lưu, toàn bộ hoặc một phần, ngay khi điều kiện cho phép.

3. Tổng thư ký Hội đồng châu Âu có thể định kỳ đề nghị quốc gia thành viên Công ước đã tuyên bố bảo lưu theo quy định tại Điều 42 thông báo về khả năng rút lại các bảo lưu.

Điều 44. ***Sửa đổi***

1. Bất cứ quốc gia thành viên nào cũng có quyền đề nghị sửa đổi Công ước này. Đề nghị sửa đổi Công ước phải được Tổng thư ký Hội đồng châu Âu gửi cho tất cả các quốc gia thành viên Hội đồng châu Âu, các quốc gia không phải thành viên của Hội đồng nhưng có tham gia vào việc xây dựng Công ước này cũng như các quốc gia gia nhập Công ước hoặc được mời gia nhập Công ước, phù hợp với các quy định tại Điều 37.

2. Đề nghị sửa đổi của quốc gia thành viên phải được gửi cho Uỷ ban châu Âu về các vấn đề tội phạm (CDPC) và Uỷ ban này sẽ đệ trình lên Hội

đồng Bộ trưởng quan điểm của Uỷ ban về lời đề nghị sửa đổi này.

3. Hội nghị Bộ trưởng sẽ cân nhắc các đề nghị sửa đổi cũng như ý kiến của Uỷ ban châu Âu về các vấn đề tội phạm và sau khi tham vấn với các quốc gia thành viên của Công ước nhưng không phải là thành viên Hội đồng châu Âu, sẽ chấp thuận đề nghị sửa đổi.

4. Biên bản sửa đổi Công ước được Hội đồng Bộ trưởng thông qua phù hợp với khoản 3 của Điều này phải được gửi trước cho các quốc gia thành viên để được chấp nhận.

5. Bất cứ sự sửa đổi nào phù hợp với khoản 3 của Điều này sẽ phát sinh hiệu lực vào ngày thứ 13 sau khi tất cả các thành viên Công ước đã thông báo Tổng thư ký về việc chấp thuận của họ.

Điều 45. ***Giải quyết tranh chấp***

1. Uỷ ban châu Âu về các vấn đề tội phạm (CDPC) sẽ duy trì thông tin về việc giải thích và áp dụng Công ước này.

2. Trong trường hợp các quốc gia thành viên có tranh chấp về việc giải thích và áp dụng Công ước này, các quốc gia tranh chấp phải tiến hành thương

lượng hoặc thực hiện các phương thức giải quyết tranh chấp hòa bình khác, bao gồm cả việc đưa tranh chấp lên Uỷ ban châu Âu về các vấn đề tội phạm (CDPC), hoặc một Uỷ ban Trọng tài mà quyết định của Uỷ ban Trọng tài là chung thẩm và có giá trị thi hành đối với các bên, hoặc tới Tòa án công lý quốc tế (ICJ), theo sự thỏa thuận của các bên.

Điều 46. ***Tham vấn giữa các bên***

1. Các bên tham gia Công ước phải tham vấn một cách định kỳ và hợp lý nhằm:

a) Sử dụng và thực thi có hiệu quả Công ước này, bao gồm việc phát hiện các vấn đề có liên quan cũng như các tác dụng của các bản tuyên bố hoặc bảo lưu được thực hiện theo Công ước này;

b) Trao đổi thông tin về các diễn tiến pháp luật, chính sách hoặc công nghệ quan trọng liên quan đến tội phạm mạng và việc thu thập chứng cứ dưới hình thức điện tử;

c) Cân nhắc việc bổ sung hoặc sửa đổi Công ước.

2. Uỷ ban châu Âu về các vấn đề tội phạm (CDPC) có trách nhiệm giữ thông tin định kỳ kết quả của các hoạt động tham vấn nêu tại khoản 1.

3. Uỷ ban châu Âu về các vấn đề tội phạm (CDPC) có trách nhiệm, một cách hợp lý, thúc đẩy các hoạt động tham vấn nêu tại khoản 1 Điều này và thực hiện các biện pháp cần thiết để hỗ trợ các bên muốn bổ sung hoặc sửa đổi Công ước. Chậm nhất là 03 năm sau khi Công ước này có hiệu lực, Uỷ ban châu Âu về các vấn đề tội phạm (CDPC) phải: hợp tác với các bên tham gia Công ước, tiến hành hoạt động đánh giá lại các quy định của Công ước, và nếu cần thiết, đề nghị sửa đổi, bổ sung Công ước.

4. Trừ trường hợp Hội đồng châu Âu có nêu rõ, các chi phí phát sinh trong quá trình thực thi các quy định tại khoản 1 Công ước này sẽ do các bên tham gia Công ước tự chịu và theo cách thức mà các bên này tự quyết định.

5. Ban thư ký Hội đồng châu Âu sẽ hỗ trợ các bên tham gia Công ước trong việc thực thi các chức năng phù hợp với điều này.

Điều 47. ***Từ bỏ Công ước***

1. Quốc gia thành viên có thể tuyên bố từ bỏ Công ước vào bất cứ thời điểm nào bằng cách gửi thông báo cho Tổng thư ký Hội đồng châu Âu.

2. Việc từ bỏ đó sẽ có hiệu lực vào ngày đầu tiên

của tháng kế tiếp của thời điểm hết thời hạn 03 tháng sau ngày Tổng thư ký Hội đồng châu Âu nhận được thông báo từ bỏ Công ước.

Điều 48. ***Thông báo***

Tổng thư ký Hội đồng châu Âu phải thông báo các quốc gia thành viên của Hội đồng châu Âu, các quốc gia không phải là thành viên Hội đồng châu Âu nhưng đã tham gia xây dựng Công ước này cũng như các quốc gia gia nhập Công ước, hoặc được mời gia nhập Công ước:

a) Bất kỳ việc ký kết;

b) Việc cam đoan phê chuẩn, chấp thuận, thông qua hoặc gia nhập;

c) Ngày có hiệu lực của Công ước này phù hợp với các quy định tại Điều 36 và Điều 37;

d) Các tuyên bố quy định tại Điều 40 hoặc bảo lưu được thực hiện phù hợp với Điều 42;

e) Các hành vi khác, thông báo hoặc liên lạc liên quan đến Công ước này.

Với sự chứng kiến của những người ký dưới đây, đã được trao đầy đủ thẩm quyền để tiến hành ký Công ước này.

Làm tại Budapest, ngày 23 tháng 11 năm 2001, bằng tiếng Anh và tiếng Pháp, cả hai bản đều có giá trị pháp lý như nhau, bản gốc được lưu trữ tại Hội đồng châu Âu. Tổng thư ký Hội đồng châu Âu có trách nhiệm cung cấp các bản sao cho các quốc gia thành viên của Hội đồng châu Âu hoặc các quốc gia không phải thành viên Hội đồng châu Âu nhưng đã tham gia soạn thảo Công ước và bất cứ quốc gia nào được mời tham gia Công ước.

LUẬT MẪU VỀ TỘI PHẠM MÁY TÍNH VÀ LIÊN QUAN ĐẾN MÁY TÍNH CỦA CÁC NƯỚC THUỘC KHỐI THỊNH VƯỢNG CHUNG

(Anh, Australia, Newzland v.v.)

Đạo luật chống tội phạm máy tính, tội phạm liên quan đến máy tính và để tạo điều kiện thuận lợi cho việc thu thập chứng cứ điện tử.

Phần 1

GIỚI THIỆU

Tên gọi rút gọn

1. Đạo luật này có thể được trích dẫn với tên là Luật Tội phạm máy tính và liên quan đến máy tính.

Mục đích

2. Mục đích của đạo luật này là bảo vệ sự toàn vẹn của hệ thống máy tính, sự bí mật, toàn vẹn và sẵn có của dữ liệu, ngăn ngừa sự lạm dụng các hệ thống đó và tạo điều kiện thuận lợi cho việc thu thập và sử

dụng chứng cứ điện tử.

Các định nghĩa

3. Trong đạo luật này, trừ trường hợp quy định khác:

"*Dữ liệu máy tính*" là bất cứ sự thể hiện tình tiết thực tế, thông tin hoặc khái niệm theo một hình thức thích hợp với việc xử lý trong một hệ thống máy tính, bao gồm một chương trình phù hợp với việc làm cho hệ thống máy tính thực hiện một chức năng;

"*Phương tiện lưu trữ dữ liệu máy tính*" là bất cứ vật nào (ví dụ, một chiếc đĩa) mà thông tin chứa trong phương tiện ấy có thể được tái sản xuất mà có thể cần hoặc không cần sự trợ giúp của bất cứ vật nào khác;

"*Hệ thống máy tính*" là một thiết bị hoặc một nhóm các thiết bị có liên hệ với nhau, bao gồm Internet, thực hiện quá trình xử lý dữ liệu một cách tự động hoặc thực hiện chức năng khác theo một chương trình.

"*Nhà cung cấp dịch vụ*" có nghĩa:

a) Một tổ chức công hoặc tư cung cấp cho người sử dụng dịch vụ khả năng liên lạc thông qua một hệ thống máy tính; và

b) Bất cứ tổ chức nào khác, thay mặt các tổ chức

hoặc người sử dụng dịch vụ kể trên thực hiện việc xử lý hoặc lưu trữ dữ liệu máy tính.

"*Dữ liệu lưu thông*" là dữ liệu máy tính:

a) Có liên quan đến việc liên lạc bằng một hệ thống máy tính; và

b) Được sản sinh bởi một hệ thống máy tính nằm trong một chuỗi liên lạc; và

c) Chỉ ra nguồn gốc, đích, lộ trình, thời gian, ngày, kích cỡ, thời hạn hoặc loại dịch vụ nền tảng của việc liên lạc.

Quyền tài phán

4. Đạo luật này áp dụng đối với hành vi hành động hoặc không hành động xảy ra:

a) Trong lãnh thổ của [quốc gia ban hành đạo luật]; hoặc

b) Trên một chiếc tàu hoặc máy bay đăng ký ở [quốc gia ban hành đạo luật]; hoặc

c) Bởi người mang quốc tịch của [quốc gia ban hành đạo luật] ngoài quyền tài phán của bất cứ quốc gia nào; hoặc

d) Bởi người mang quốc tịch của [quốc gia ban

hành đạo luật] ngoài lãnh thổ của [quốc gia ban hành đạo luật], nếu hành vi của người đó cũng cấu thành tội phạm theo luật của quốc gia nơi hành vi phạm tội được thực hiện.

Lưu ý: Tội phạm mạng là loại tội thường có cơ sở lãnh thổ rộng lớn so với các tội phạm thông thường bởi tội phạm này tuy được thực hiện trong lãnh thổ một nước nhưng có thể có ảnh hưởng to lớn đối với quốc gia khác. Một số quốc gia có thể giải quyết vấn đề này thông qua việc phát triển các án lệ để giải thích thuật ngữ "thẩm quyền tài phán theo lãnh thổ" đủ rộng để bao hàm cả các hành vi "có mối liên hệ thực sự và quan trọng" đối với quốc gia đó mặc dù các yếu tố cấu thành tội phạm được thực hiện ở nơi khác. Ở một số quốc gia, các đạo luật thành văn trực tiếp quy định rằng luật này có thể áp dụng cho cả các hành vi thực hiện ở ngoài lãnh thổ nhưng có mối liên hệ quan trọng với quốc gia ấy. Dù tiếp cận theo cách nào thì điều quan trọng là các quốc gia cần cân nhắc vấn đề thẩm quyền tài phán một cách cẩn thận để đảm bảo rằng không có thiên đường nào

dành cho người thực hiện tội phạm mạng có thể thoát khỏi trách nhiệm.

Phần II

CÁC TỘI PHẠM

Truy cập bất hợp pháp

5. Người nào cố ý, và không có lý do hợp pháp, truy cập tất cả hoặc bất cứ phần nào của một hệ thống máy tính, thì phạm một tội và bị phạt tù không quá [thời hạn], hoặc bị phạt tiền không quá [mức tiền] hoặc bị cả hai.

Gây rối dữ liệu

6. 1) Người nào, cố ý hoặc vô ý, mà không có lý do hợp pháp, thực hiện bất cứ hành vi nào trong số các hành vi sau:

a) Tiêu hủy hoặc thay đổi dữ liệu; hoặc

b) Đưa ra các dữ liệu không có ý nghĩa, không có giá trị sử dụng hoặc không có hiệu lực; hoặc

c) Cản trở, ngăn chặn hoặc gây rối quá trình sử dụng hợp pháp dữ liệu; hoặc

d) Cản trở, ngăn chặn hoặc gây rối người khác

trong việc sử dụng hợp pháp dữ liệu; hoặc

e) Từ chối tiếp cận dữ liệu đối với người có quyền tiếp cận dữ liệu;

thì phạm một tội và bị phạt tù với thời hạn không quá [thời hạn] hoặc bị phạt tiền với mức không quá [số tiền], hoặc bị cả hai.

2) Khoản 1 kể trên được áp dụng bất kể hành vi gây ra tác dụng tạm thời hay lâu dài.

Gây rối hệ thống máy tính

7. 1) Người nào, cố ý hoặc vô ý, mà không có lý do hợp pháp:

a) Cản trở hoặc gây rối sự vận hành của một hệ thống máy tính; hoặc

b) Cản trở hoặc gây rối người đang sử dụng hoặc vận hành hợp pháp một hệ thống máy tính;

thì phạm một tội và bị phạt tù không quá [thời hạn], hoặc bị phạt tiền không quá [mức tiền], hoặc bị cả hai.

2) Trong việc áp dụng quy định tại khoản 1 Điều này, từ "*cản trở*", trong mối quan hệ với một hệ thống máy tính, bao gồm nhưng không chỉ giới hạn trong

các hành vi sau:

a) Cắt nguồn cung cấp điện đối với hệ thống máy tính; và

b) Tạo ra sự gây rối điện từ đối với hệ thống máy tính; và

c) Làm hư hại hệ thống máy tính bằng bất cứ phương tiện nào; và

d) Nạp, xóa hoặc thay đổi dữ liệu máy tính.

Ngăn chặn bất hợp pháp dữ liệu

8. Người nào, cố ý mà không có lý do hợp pháp, ngăn chặn bằng các phương tiện kỹ thuật:

a) Bất cứ sự truyền tải dữ liệu không công khai nào tới, từ hoặc trong một hệ thống máy tính; hoặc

b) Sự phát ra các tín hiệu điện từ mang dữ liệu từ hệ thống máy tính;

thì phạm một tội và bị phạt tù không quá [thời hạn] hoặc bị phạt tiền không quá [số tiền], hoặc bị cả hai.

Các thiết bị bất hợp pháp

9. 1) Một người sẽ bị coi là phạm một tội nếu người đó:

a) Cố ý hoặc vô ý, mà không có lý do hợp pháp, sản

xuất, bán, mời sử dụng, nhập khẩu, xuất khẩu, phân phối hoặc bằng các cách thức khác cung cấp:

(i) Thiết bị, bao gồm chương trình máy tính, được thiết kế hoặc được điều chỉnh để thực hiện hành vi phạm tội nêu tại Điều 5, 6, 7 hoặc 8; hoặc

(ii) Mã số truy cập của máy tính (password), mật mã truy cập hoặc dữ liệu tương tự mà nhờ mã số ấy toàn bộ hoặc một phần hệ thống máy tính có thể được truy cập;

b) Chiếm hữu các khoản mục nêu tại tiểu khoản (i) và (ii) với ý định cho người khác sử dụng để thực hiện các hành vi phạm tội quy định tại Điều 5, 6, 7 hoặc 8.

2) Người nào vi phạm quy định tại điều này thì bị phạt tù không quá [thời hạn] hoặc bị phạt tiền không quá [số tiền] hoặc bị phạt cả hai.

[Bản của Nhóm chuyên gia về khoản 3

3) Người nào sở hữu từ 2 khoản mục nêu tại tiểu khoản (i) hoặc (ii) trở lên thì được coi là sở hữu khoản mục với ý định sử dụng hoặc cho người khác sử dụng để thực hiện tội phạm nêu tại Điều 5, 6, 7 hoặc 8 trừ trường hợp chứng minh được điều ngược lại].

[Bản thay thế khoản 3 do Canada đề xuất

3) Người nào chiếm hữu nhiều hơn [số lượng] khoản mục nêu tại tiểu khoản (i) hoặc (ii), Tòa án có thể coi rằng người đó sở hữu khoản mục với ý định sử dụng hoặc cho người khác sử dụng để thực hiện tội phạm nêu tại Điều 5, 6, 7 hoặc 8 trừ trường hợp người này đưa ra được lý do hợp lý về mục đích của việc chiếm hữu đó].

Chú thích:

Khoản 3 là một quy định có tính tùy nghi. Đối với một số quốc gia, việc giả định như vậy có thể là rất hữu ích, nhưng đối với quốc gia khác thì có thể không có ý nghĩa lắm trong bối cảnh hành vi vi phạm cụ thể này. Các quốc gia cần cân nhắc trên cơ sở cân nhắc bối cảnh pháp lý cụ thể của mình xem liệu có nên đưa thêm khoản này vào không.

Tư liệu khiêu dâm trẻ em

10. 1) Người nào cố ý, thực hiện các hành vi sau đây:

a) Phát hành tài liệu khiêu dâm trẻ em qua hệ thống máy tính; hoặc

b) Sản xuất tài liệu khiêu dâm trẻ em để phát hành qua hệ thống máy tính; hoặc

c) Sở hữu tài liệu khiêu dâm trẻ em trong hệ thống máy tính hoặc trong phương tiện lưu trữ dữ liệu máy tính,

thì phạm một tội và bị phạt tù không quá [thời hạn] hoặc bị phạt tiền không quá [số tiền], hoặc cả hai.

Chú thích:

Pháp luật về tài liệu khiêu dâm có nội dung rất khác nhau trong các quốc gia thuộc khối Thịnh vượng chung. Vì thế, quy định cấm trong Luật mẫu chỉ giới hạn trong tài liệu khiêu dâm trẻ em vốn là đối tượng bị cấm tuyệt đối bởi pháp luật của tất cả các quốc gia. Tuy nhiên, các nước có thể mở rộng việc áp dụng điều cấm này đối với các loại tài liệu khiêu dâm khác theo quy định trong luật của quốc gia đó.

Chú thích:

Hình phạt tiền sẽ được áp dụng đối với các công ty nhưng mức tiền phạt có thể không đủ lớn. Vì thế, đối với các công ty, nên quy định mức phạt cao hơn. Khi đó, khoản 1

có thể quy định như sau:

"thì phạm một tội":

a) Trong trường hợp người phạm tội là cá nhân, thì bị phạt tiền không quá [mức tiền phạt] hoặc bị phạt tù không quá [thời hạn bị phạt tù];

b) Trong trường hợp người phạm tội là công ty, thì bị phạt tiền không quá [mức tiền phạt cao].

2) Có thể được miễn trừ trách nhiệm nêu tại khoản 1a hoặc 1c nếu như người bị truy tố chứng minh được rằng, tư liệu khiêu dâm trẻ em chỉ thuần túy sử dụng cho mục đích nghiên cứu khoa học, chữa trị bệnh hoặc thi hành pháp luật.

Chú thích:

Các quốc gia có thể muốn mở rộng hoặc thu hẹp các khả năng miễn trừ trách nhiệm quy định tại khoản 2, tùy thuộc vào bối cảnh cụ thể của mỗi quốc gia. Tuy nhiên, cần lưu ý để các khả năng miễn trừ trách nhiệm chỉ ở mức tối thiểu và tránh sử dụng loại ngôn ngữ có thể hiểu rộng một cách quá mức để

ngăn chặn khả năng sử dụng các căn cứ miễn trừ trách nhiệm ngay cả trong các trường hợp không thể chấp nhận được.

3) Trong Điều này:

"*Tài liệu khiêu dâm trẻ em*" bao gồm bất cứ tài liệu nào bằng hình ảnh mô tả:

a) Người chưa thành niên thực hiện hành vi tình dục; hoặc

b) Người giống người chưa thành niên thực hiện hành vi tình dục; hoặc

c) Hình ảnh thực tế diễn tả người chưa thành niên thực hiện hành vi tình dục.

"*Người chưa thành niên*" là người dưới [x] tuổi(*).

"*Phát hành*" bao gồm:

a) Phân phối, truyền tải, phát tán, lưu hành, giao nhận, trưng bày, cho mượn, trao đổi, bán, chào bán, cho thuê, đề nghị cho thuê, đề nghị dưới hình thức khác, hoặc cung cấp dưới bất cứ cách thức nào; hoặc

b) Chiếm hữu hoặc chiếm giữ, hoặc kiểm soát, vì

(*) Do pháp luật quốc gia quy định.

mục đích thực hiện hành vi nêu tại khoản (a); hoặc

c) In, chụp, nhân bản hoặc thực hiện bất cứ hành vi nào khác (bất kể cùng hoặc khác loại hoặc bản chất) với mục đích thực hiện hành vi nêu tại khoản (a).

Phần III

QUYỀN NĂNG TỐ TỤNG

Các định nghĩa cho phần này

Chú thích:

Vì tất cả các quốc gia đều đã quy định về thẩm quyền khám xét theo luật án lệ hoặc luật thành văn, mục đích của Điều 11 và Điều 12 là đưa ra các điểm sửa đổi cần thiết đối với các quy định về thẩm quyền khám xét hiện hành để đảm bảo rằng thẩm quyền đó bao gồm cả thẩm quyền khám xét và giữ đồ vật đối với hệ thống máy tính và dữ liệu máy tính.

Quy định về lệnh khám xét chung chỉ mang tính chất minh họa mà không có ý định đưa ra mô hình toàn diện về các quyền khám xét chung. Cùng một quy định nhưng được

xây dựng theo nhiều phương án khác nhau để các quốc gia với điều kiện khác nhau có thể được chọn lựa. Những phương án này được để trong dấu ngoặc kép và in nghiêng.

11. Trong phần này:

"*Vật*" bao gồm:

a) Hệ thống máy tính hoặc một phần trong hệ thống máy tính; và

b) Hệ thống máy tính khác, nếu:

(i) Dữ liệu máy tính từ hệ thống máy tính đó được cung cấp sẵn có đối với hệ thống máy tính đầu tiên đang bị khám xét; và

(ii) Có các căn cứ hợp lý để tin rằng các dữ liệu máy tính cần tìm kiếm được lưu trữ trong hệ thống máy tính khác; và

c) Phương tiện lưu trữ dữ liệu máy tính.

"*Thu giữ*" bao gồm:

a) Tạo hoặc giữ lại một bản sao dữ liệu máy tính, bao gồm cả việc sử dụng phương tiện tại hiện trường; và

b) Làm cho không thể truy cập được hoặc chuyển đi, dữ liệu máy tính trong hệ thống máy tính đã được

truy cập; và

c) Lấy một bản in đầu ra của dữ liệu máy tính.

Lệnh khám xét và thu giữ

12. Dựa trên cơ sở [lời cáo buộc có tuyên thệ] [lời tuyên thệ], Thẩm phán phụ trách vụ việc thấy có căn cứ hợp lý để [nghi ngờ] [tin tưởng] tồn tại vật hoặc dữ liệu máy tính ở một nơi mà vật hoặc dữ liệu máy tính đó:

a) Có vai trò quan trọng trong việc chứng minh hành vi phạm tội; hoặc

b) Đã bị một người chiếm hữu bằng hành vi phạm tội;

Thẩm phán [có thể] [phải] ra lệnh ủy quyền cho Điều tra viên (sỹ quan [thi hành pháp luật] [cảnh sát]) nếu như việc ra lệnh này là cần thiết để thâm nhập nơi khám xét và giữ vật hoặc dữ liệu máy tính.

Chú thích:

Nếu quy định hiện hành về khám xét và thu giữ có quy định về nội dung của lệnh khám, theo từng điều khoản hoặc mẫu, thì các quy định này cần được rà soát lại để đảm bảo rằng các quy định ấy cũng đề cập đến dữ liệu máy tính.

Cảnh sát hỗ trợ

13. 1) Người đang chiếm hữu hoặc kiểm soát phương tiện lưu trữ dữ liệu máy tính hoặc hệ thống máy tính thuộc đối tượng bị khám xét theo quy định tại Điều 12 phải cho phép và hỗ trợ người đang tiến hành việc khám xét nếu được yêu cầu, để:

a) Tiếp cận và sử dụng một hệ thống máy tính hoặc phương tiện lưu trữ dữ liệu máy tính nhằm khám xét bất cứ dữ liệu máy tính nào sẵn có hoặc đang ở trong hệ thống; và

b) Thu thập và sao chụp dữ liệu máy tính đó; và

c) Sử dụng các thiết bị để nhân bản; và

d) Thu thập các sản phẩm đầu ra có thể nhận biết được từ một hệ thống máy tính bằng một văn bản dưới dạng ngôn ngữ thông thường mà con người có thể đọc được.

2) Người nào không có lý do hợp pháp cho phép hoặc hỗ trợ người khác thực hiện một hành vi phạm tội thì bị phạt tù không quá [thời hạn] hoặc bị phạt tiền không quá [số tiền] hoặc bị cả hai.

Chú thích:

Các quốc gia có thể định nghĩa từ "hỗ trợ"

bao gồm việc cung cấp mã số truy cập máy tính, mã nguồn hoặc các thông tin cần thiết khác để truy cập một máy tính. Các định nghĩa đó cần được soạn thảo phù hợp với các quy định của Hiến pháp hoặc luật án lệ về bảo vệ khỏi sự tự buộc tội chính mình.

Biên bản và tiếp cận đối với dữ liệu bị thu giữ

14. 1) Nếu hệ thống máy tính hoặc dữ liệu máy tính đã bị chuyển đi hoặc đưa vào tình trạng không thể truy cập được, sau khi bị khám xét hoặc thu giữ theo quy định tại Điều 12 thì người đã ra lệnh khám xét, tại thời điểm khám xét hoặc ngay khi có thể sau thời điểm khám xét, phải:

a) Lập một danh mục những gì đã bị thu giữ hoặc bị đưa vào tình trạng không thể truy cập được, ghi rõ ngày và thời điểm bị thu giữ; và

b) Cung cấp một bản sao của danh mục đó cho:

(i) Người đang quản lý địa điểm bị khám xét; hoặc

(ii) Người quản lý hệ thống máy tính.

2) Phù hợp với quy định tại khoản 3, khi được yêu cầu, Điều tra viên hoặc người có thẩm quyền khác phải:

a) Cho phép người quản lý, kiểm soát hệ thống

máy tính hoặc người đại diện của người này truy cập và sao chép dữ liệu máy tính có trong hệ thống máy tính; hoặc

b) .Cung cấp cho người đó một bản sao dữ liệu máy tính.

3) Điều tra viên hoặc người có thẩm quyền khác có quyền từ chối việc truy cập hoặc sao chép nếu người này có lý do hợp lý để tin rằng việc cho phép truy cập hoặc cung cấp các bản sao chép:

a) Sẽ cấu thành một tội phạm; hoặc

b) Sẽ làm sai lệch:

(i) Hoạt động điều tra liên quan đến việc tiến hành thu giữ; hoặc

(ii) Các hoạt động điều tra khác đang được triển khai; hoặc

(iii) Bất cứ thủ tục tố tụng hình sự nào đang được tiến hành hoặc có thể được tiến hành liên quan tới các hoạt động điều tra này.

Cung cấp dữ liệu

15. Nếu được Điều tra viên chứng minh rằng dữ liệu máy tính nhất định, hoặc bản in của dữ liệu ấy

hoặc các thông tin khác là cần thiết cho việc điều tra tội phạm hoặc tố tụng hình sự thì Thẩm phán phụ trách vụ việc có thể ra lệnh:

a) Người trong lãnh thổ của [quốc gia ban hành luật] quản lý hệ thống máy tính phải lấy từ hệ thống máy tính ấy các dữ liệu máy tính hoặc bản in hoặc các sản phẩm đầu ra có thể nhận biết của dữ liệu đó; và

b) Nhà cung cấp dịch vụ Internet ở [quốc gia ban hành luật] phải cung cấp các thông tin về người đăng ký hoặc sử dụng dịch vụ; và

c) [Người trong lãnh thổ [quốc gia ban hành luật] truy cập được hệ thống máy tính phải xử lý và thu thập các dữ liệu máy tính từ hệ thống và cung cấp cho người được pháp luật quy định].

Chú thích:

Như đã lưu ý trong báo cáo của nhóm chuyên gia, có quốc gia áp dụng tiêu chuẩn chung cho lệnh về cung cấp chứng cứ như áp dụng cho lệnh khám xét tư pháp thông thường. Tuy nhiên, một số nước lại thấy việc sử dụng tiêu chuẩn thấp hơn là đủ bởi quá trình cung cấp dữ liệu ít mang tính áp chế so

với quá trình thực hiện lệnh khám xét tư pháp thông thường.

Chú thích:

Các quốc gia có thể cân nhắc xem liệu khoản c có phù hợp để quy định trong luật của mỗi quốc gia không, bởi lẽ, các quy định này có thể rất hữu dụng nhưng nó đòi hỏi việc xử lý và thu thập dữ liệu phải có lệnh của Tòa án, do đó nó có thể sẽ không phù hợp với một số nước.

Tiết lộ dữ liệu lưu thông đang lưu giữ

Phương án 1

16. Nếu có căn cứ hợp lý để tin rằng dữ liệu lưu trữ trong hệ thống máy tính là cần thiết cho hoạt động điều tra hình sự, Điều tra viên có thể, bằng văn bản, thông báo cho người quản lý hệ thống máy tính, yêu cầu người này tiết lộ đầy đủ các dữ liệu lưu thông về một liên lạc để nhận diện:

a) Các nhà cung cấp dịch vụ; và

b) Con đường liên lạc được truyền tải.

Phương án 2

16. Nếu Điều tra viên đề nghị và chứng minh được

rằng dữ liệu lưu trữ trong hệ thống máy tính là cần thiết cho hoạt động điều tra hình sự hoặc hoạt động tố tụng hình sự, Thẩm phán phụ trách vụ việc có thể lệnh cho người quản lý hệ thống máy tính tiết lộ các dữ liệu lưu thông về liên lạc đủ để nhận diện:

a) Nhà cung cấp dịch vụ; và

b) Con đường liên lạc được truyền tải.

Gìn giữ dữ liệu

17. 1) Nếu có căn cứ hợp lý để tin rằng:

a) Dữ liệu lưu trữ trong hệ thống máy tính là cần thiết cho hoạt động điều tra hình sự; và

b) Có rủi ro rằng dữ liệu đó có thể bị phá hủy hoặc làm cho không thể tiếp cận được,

thì Điều tra viên có thể, bằng văn bản, thông báo cho người quản lý hệ thống máy tính, yêu cầu người này đảm bảo rằng dữ liệu nêu trong thông báo được gìn giữ trong thời hạn tối đa là 07 ngày như đã nói trong thông báo.

2) Thời hạn này có thể gia hạn thêm 07 ngày nếu khi áp dụng biện pháp một cách đơn phương, [Thẩm phán] cho gia hạn đối với việc gìn giữ dữ liệu đó.

Chặn các liên lạc điện tử

18. Trên cơ sở [lời cáo buộc có tuyên thệ] [lời khai có tuyên thệ] có căn cứ hợp lý [để nghi ngờ] [tin tưởng] rằng nội dung của các liên lạc điện tử là cần thiết cho hoạt động điều tra hình sự, Thẩm phán phụ trách vụ việc [có thể] [phải]:

a) Ra lệnh nhà cung cấp dịch vụ Internet hiện đang cung cấp dịch vụ ở [quốc gia ban hành luật] thông qua việc áp dụng các biện pháp kỹ thuật thu thập, ghi lại, cho phép hoặc hỗ trợ cơ quan có thẩm quyền thu thập, ghi lại nội dung dữ liệu gắn với các liên lạc được truyền tải qua hệ thống máy tính; hoặc

b) Uỷ quyền cho Điều tra viên thu thập hoặc ghi lại dữ liệu đó thông qua việc áp dụng các biện pháp kỹ thuật.

Chặn các dữ liệu lưu thông

19. 1) Nếu có căn cứ hợp lý để tin rằng dữ liệu lưu thông liên quan tới một liên lạc cụ thể là cần thiết trong hoạt động điều tra hình sự, thì Điều tra viên có thể, bằng văn bản, thông báo cho người quản lý dữ liệu đó, yêu cầu người này:

a) Thu thập hoặc ghi lại dữ liệu lưu thông gắn với liên lạc đang được điều tra trong một khoảng thời

gian nhất định; và

b) Cho phép và hỗ trợ Điều tra viên thu thập hoặc ghi lại những dữ liệu đó.

2) Trên cơ sở [lời cáo buộc có tuyên thệ] [lời khai có tuyên thệ] có căn cứ hợp lý để [tin tưởng] rằng dữ liệu lưu thông là cần thiết cho việc điều tra hình sự, Thẩm phán [có thể/phải] uỷ quyền cho Điều tra viên thu thập hoặc ghi lại các dữ liệu lưu thông liên quan với liên lạc được điều tra trong một thời gian nhất định thông qua việc áp dụng các biện pháp kỹ thuật.

Chứng cứ

20. Trong hoạt động tố tụng liên quan đến hành vi vi phạm pháp luật của [quốc gia ban hành luật], tình tiết:

a) Có cáo buộc là hành vi gây rối hệ thống máy tính đã được thực hiện; và

b) Bằng chứng đã được sản sinh từ hệ thống máy tính đó,

không tự nó ngăn cản sự chấp nhận chứng cứ đó.

Sự bí mật và giới hạn trách nhiệm

21. 1) Nhà cung cấp dịch vụ tiết lộ mà không có thẩm quyền:

a) Tình tiết rằng một lệnh theo quy định tại Điều 13, 15, 16, 17, 18 và 19 đã được ban hành; hoặc

b) Bất cứ điều gì được thực hiện theo lệnh đó; hoặc

c) Bất cứ dữ liệu nào được thu thập hoặc ghi lại theo lệnh đó;

thì phạm một tội và bị phạt tù không quá [thời hạn] hoặc bị phạt tiền không quá [số tiền] hoặc bị phạt cả hai.

2) Nhà cung cấp dịch vụ Internet không phải chịu trách nhiệm về mặt dân sự hoặc hình sự theo luật của [quốc gia ban hành luật này] khi tiết lộ các dữ liệu hoặc thông tin theo quy định tại Điều 13, 15, 16, 18 hoặc 19.

LUẬT MẪU VỀ CHỨNG CỨ ĐIỆN TỬ CỦA CÁC NƯỚC THUỘC KHỐI THỊNH VƯỢNG CHUNG

(Anh, Australia, Newzland v.v.)

Đạo luật quy định việc công nhận về mặt pháp lý các biên bản điện tử và tạo điều kiện cho việc thừa nhận biên bản điện tử làm bằng chứng trong các thủ tục tố tụng.

Được ban hành bởi Nghị viện [tên của Nghị viện] nước ....[tên nước] như sau:

Tên gọi rút gọn

1. Đạo luật này có thể được trích dẫn với tên gọi là Luật Chứng cứ điện tử, (năm ban hành....)

Giải thích thuật ngữ

2. Trong đạo luật này:

"*Dữ liệu*" là sự trình bày thông tin hoặc ý niệm dưới bất cứ hình thức nào.

"*Biên bản điện tử*" là những dữ liệu được ghi hoặc

lưu giữ trên bất cứ phương tiện trung gian nào, bằng hệ thống máy tính hoặc các thiết bị tương tự mà có thể đọc hoặc nhận biết được bởi người, hệ thống máy tính hoặc các thiết bị tương tự khác. Biên bản điện tử bao gồm cả các bản trình bày, bản in hoặc các sản phẩm đầu ra khác từ dữ liệu đó.

"*Hệ thống biên bản điện tử*" bao gồm hệ thống máy tính hoặc các thiết bị tương tự mà nhờ đó dữ liệu được ghi hoặc lưu giữ và bất cứ thủ tục nào liên quan đến việc ghi và lưu giữ biên bản điện tử.

"*Thủ tục tố tụng*" được hiểu là thủ tục dân sự, hình sự và hành chính trước Tòa án, trước một cơ quan tài phán, một hội đồng hoặc uỷ ban.

Khả năng chấp nhận chung

3. Không có quy định nào trong bộ quy tắc về chứng cứ hiện hành được áp dụng để loại trừ việc thừa nhận tư cách chứng cứ của biên bản điện tử chỉ trên cơ sở rằng đó là một biên bản điện tử.

4. 1) Đạo luật này không làm thay đổi bất cứ quy tắc trong luật pháp hiện hành liên quan đến việc thừa nhận tư cách chứng cứ của biên bản, ngoại trừ các quy tắc liên quan đến việc chứng thực và chứng cứ tốt nhất.

Phạm vi của đạo luật

2) Tòa án có thể xem xét chứng cứ được viện dẫn theo quy định của Luật này trong việc áp dụng bất cứ quy định pháp luật hiện hành nào đối với việc thừa nhận tư cách chứng cứ của biên bản.

Chứng thực

5. Người sử dụng biên bản điện tử trong các thủ tục tố tụng có trách nhiệm chứng minh tính xác thực của biên bản điện tử bằng các chứng cứ chứng minh rằng biên bản điện tử đúng là cái mà người này xuất trình làm bằng chứng.

Việc áp dụng quy tắc chứng cứ tốt nhất

6. 1) Trong mọi thủ tục tố tụng, khi quy tắc chứng cứ tốt nhất được áp dụng đối với biên bản điện tử, quy tắc này sẽ được coi là thỏa mãn nếu chứng minh được sự toàn vẹn của hệ thống biên bản điện tử đã ghi hoặc lưu giữ dữ liệu.

2) Trong mọi thủ tục tố tụng, khi biên bản điện tử đã được in ra, bản in này đã được sử dụng một cách nhất quán và rõ ràng là biên bản chứa đựng thông tin, thì theo quy định của quy tắc chứng cứ tốt nhất,

bản in này sẽ được coi là biên bản.

Giả định về sự toàn vẹn

7. Trừ khi có bằng chứng chứng minh điều ngược lại, sự toàn vẹn của hệ thống biên bản điện tử ghi và lưu giữ các biên bản điện tử được giả định là tồn tại trong các thủ tục tố tụng:

a) Khi viện dẫn được chứng cứ chứng minh rằng hệ thống máy tính hoặc các thiết bị điện tử tương tự khác hoạt động bình thường, hoặc nếu không hoạt động bình thường nhưng sự toàn vẹn của biên bản không bị ảnh hưởng bởi sự không bình thường ấy, và không có căn cứ hợp lý khác để nghi ngờ sự toàn vẹn của biên bản.

b) Khi đã chứng minh được rằng biên bản điện tử được ghi hoặc lưu trữ bởi bên tham gia tố tụng có quyền lợi đối lập với bên xuất trình biên bản điện tử làm chứng cứ; hoặc

c) Khi đã chứng minh được rằng biên bản điện tử được người không tham gia tố tụng ghi hoặc lưu trữ trong quá trình kinh doanh thông thường của mình và sự ghi, lưu trữ biên bản ấy không chịu ảnh hưởng của bên xuất trình biên bản điện tử.

Các tiêu chuẩn

8. Trong việc quyết định công nhận hay không công nhận biên bản điện tử, việc xuất trình chứng cứ được thực hiện theo các tiêu chuẩn, thủ tục, thực tiễn ghi, lưu giữ biên bản điện tử trong các loại hình hoạt động có sử dụng, ghi hoặc lưu giữ biên bản điện tử và bản chất, mục đích của biên bản điện tử.

Chứng minh bằng bản tuyên thệ

9. Các vấn đề đề cập trong các điều 6, 7 và 8 có thể được xác lập bằng một bản tuyên thệ với cam kết rằng lời tuyên thệ đó là thuộc phạm vi hiểu biết hoặc niềm tin tốt nhất của người tuyên thệ.

Đối chất

10. 1) Người tuyên thệ nêu tại Điều 9 đã xuất trình chứng cứ có thể được đối chất bởi bên tham gia tố tụng có lợi ích đối lập với mình hoặc bên yêu cầu đưa ra bản tuyên thệ.

2) Khi được Tòa án cho phép, các bên tham gia tố tụng có thể đối chất với người được đề cập trong tiểu khoản 7c.

Thỏa thuận về sự thừa nhận biên bản điện tử

11. 1) Trừ trường hợp được pháp luật quy định

khác, Tòa án có thể thừa nhận biên bản điện tử theo sự cân nhắc của mình, nếu các bên tham gia tố tụng, ở bất cứ thời điểm nào, đã đồng ý một cách rõ ràng rằng việc thừa nhận đó là vấn đề không thể tranh cãi.

2) Không kể các quy định tại khoản 1 kể trên, thỏa thuận giữa các bên về việc thừa nhận một biên bản điện tử không mặc nhiên làm cho biên bản điện tử được thừa nhận trong việc buộc tội của tố tụng hình sự nếu tại thời điểm xác lập thỏa thuận, người bị buộc tội không được đại diện bởi luật sư.

Thừa nhận chữ ký điện tử

12. 1) Khi quy tắc chứng cứ yêu cầu phải có chữ ký hoặc có quy định về hệ quả pháp lý của việc không có chữ ký thì các chữ ký điện tử sẽ được coi là thỏa mãn quy tắc này và tránh được những hệ quả của việc không có chữ ký.

2) Chữ ký điện tử có thể được chứng minh bằng bất cứ cách thức nào, bao gồm cả bằng việc chứng minh rằng có một thủ tục cần thiết cho một người, khi tiến hành giao dịch, đưa ra một biểu tượng hoặc thủ tục an ninh để xác minh rằng biên bản điện tử là đúng của người đó.

DANH MỤC CÁC VẤN ĐỀ PHÁP LÝ CHỦ YẾU ĐƯỢC ĐỀ CẬP TRONG CUỐN SÁCH

(Được in đậm, nghiêng)

TÀI LIỆU THAM KHẢO

TIẾNG VIỆT

1. Chỉ thị số 58 - CT/TW ngày 17/10/2000 về việc đẩy mạnh ứng dụng và phát triển công nghệ thông tin phục vụ sự nghiệp công nghiệp hoá, hiện đại hoá.

2. Công ước của Hội đồng châu Âu về tội phạm mạng (Công ước Budapest ngày 23/11/2001).

3. Luật mẫu về tội phạm máy tính và liên quan đến máy tính (của Khối thịnh vượng chung).

4. Luật mẫu về chứng cứ điện tử (của Khối thịnh vượng chung).

5. Bộ luật Hình sự năm 1999.

6. Bộ luật Hình sự của một số nước (Nhật Bản, Liên bang Nga, Australia, Mỹ, Hàn Quốc, Rumani...).

7. Luật Tổ chức Viện Kiểm sát nhân dân năm 2002.

8. Pháp lệnh số 43/2002/PL-UBTVQH10 về bưu chính viễn thông.

9. Nghị định số 55/2001/NĐ-CP ngày 23/8/2001 về

quản lý, cung cấp và sử dụng dịch vụ Internet.

10. Nghị định số 160/2004/NĐ-CP ngày 03/9/2004 quy định chi tiết một số điều của Pháp lệnh Bưu chính viễn thông.

11. Nghị định số 55/2001/NĐ-CP của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ Internet.

12. Quyết định số 246/2005/QĐ-TTg của Thủ tướng Chính phủ về việc phê duyệt chiến lược phát triển công nghệ thông tin và truyền thông Việt Nam đến năm 2010 và định hướng đến năm 2020.

13. Thông tư số 05/2004/TT-BBCVT hướng dẫn thực hiện một số điều về xử lý vi phạm hành chính và khiếu nại, tố cáo quy định tại Chương IV Nghị định số 55/2001/NĐ-CP của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ Internet.

14. Thông tư liên tịch số 01/2001/TTLT-TCBĐ-BCA ngày 07/6/2001 của Tổng cục Bưu điện, Bộ Công an hướng dẫn việc bảo đảm an toàn mạng lưới và an ninh thông tin trong hoạt động bưu chính viễn thông.

15. Thông tư liên tịch số 02 ngày 14/7/2005 giữa Bộ Bưu chính Viễn Thông, Bộ Văn hoá thông tin, Bộ Kế hoạch và Đầu tư, Bộ Công an về quản lý đại lý Internet.

16. *Bình luận khoa học Bộ luật Hình sự năm 1999*, Nxb. Công an nhân dân, H. 2001;

17. Uông Chu Lưu (Chủ biên): *Bình luận khoa học Bộ luật hình sự năm 1999*, Nxb. Chính trị quốc gia, H. 2001.

18. Lê Đăng Doanh: *Về định tội danh đối với hành vi làm, sử dụng thẻ tín dụng giả hay các loại thẻ khác để mua hàng hoá hoặc rút tiền tại máy trả tiền tự động của các ngân hàng,* Tạp chí Toà án nhân dân, số 6/2006.

19. Mohamed Chawki: *A Citical Look at the Regulation of Cybercrime,* Đại học Lyon III, Pháp.

20. Nguyễn Mạnh Toàn, *Đặc điểm và các dạng hành vi cơ bản của tội phạm tin học,* Tạp chí Nhà nước và Pháp luật, số 3/2002.

21. Nông Xuân Trường: *Tội phạm tin học và các biện pháp đấu tranh chống tội phạm tin học tại Hàn Quốc,* Tạp chí Kiểm sát, số 10/2003, tr.49.

22. *PC World VietNam,* tháng 12/2000, tr. 1.

23. *Số chuyên đề về Luật hình sự một số nước trên thế giới,* Tạp chí Dân chủ và pháp luật (Bộ Tư pháp), năm 1998.

24. Tạp chí Bưu điện, tháng 1/2004.

25. Tạp chí Nhà nước và Pháp luật, số 03/2002.

26. Tạp chí Kiểm sát, số 10/2003.

27. Tài liệu của Dự án "*Tăng cường thông tin pháp luật tại Việt Nam giai đoạn 2001- 2004*".

28. Theo Malay Mail ngày 04/3/2001.

29. Theo AFP ngày 29/6/2001.

30. *Trung Nguyên. Năm 2004, năm bùng nổ tội phạm máy tính.* Tổng hợp từ Internet tháng 1/2005, tr.1-2, http://www.tuoitre.com.vn ngày 16/01/2005.

31. Tymothyhall. White collar crime in Australia. Dẫn theo: Dương Tuyết Miên & Nguyễn Ngọc Khanh. *Tội phạm vi tính,* Tạp chí Tòa án nhân dân, số 5/2000, tr.19.

32. Http://www.echip.com.vn: *Tuyên chiến với tội phạm máy tính,* ngày 07/01/2006, tr. 1,2.

33. Http://www.vietnamnet: *Cảnh sát mạng chống tội phạm mạng:* Chạy đua với thời gian, ngày 22/09/2004, tr. 1.

34. Http://www.vietnamnet.vn/. *Tìm bằng chứng phạm tội trong ổ cứng máy tính,* ngày 08/6/2002, tr. 1.

35. Http://www.vinexco.com.vn/. *Tội phạm kỹ thuật*

cao - khủng bố tin học, ngày 20/10/2003, tr. 2.

TIẾNG NƯỚC NGOÀI

36. F. Lawrence Street & Mark P. Grant - *The Law of Internet* - 2004 (Lexis.com).

37. Li, Xingan. Cybercrime: *An Introduction, Joensuu*, July 2005.

38. Stein Schjolberg-Chief Judge-Moss District Court,Norway www.mosstingrett.no/info/legal.html).

MỤC LỤC

Chương II

TÌNH HÌNH TỘI PHẠM VÀ CÁC QUY ĐỊNH PHÁP LUẬT VỀ PHÒNG, CHỐNG TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN 47

TP NHÀ XUẤT BẢN TƯ PHÁP

Địa chỉ: 58 - 60 Trần Phú - Ba Đình - Hà Nội, Địa chỉ cơ sở 2: 343 Đội Cấn - Ba Đình - Hà Nội
Điện thoại: 04. 8231135, 04. 7623693 - Phát hành: 080 48457, 04. 7629926
Biên tập: 04.7623970, 04. 7623692, 04. 7623695, 080 46864
Thiết kế - Chế bản: 080 48321, 04. 7623694 - Hành chính: 04. 7343606 - Kế toán: 04.7343604
Fax: 04. 7340981, 04. 7624197 - Email: nxbtp@moj.gov.vn - Website: http://nxbtp.moj.gov.vn

Chịu trách nhiệm xuất bản
NGUYỄN ĐỨC GIAO

Chịu trách nhiệm nội dung
TRƯƠNG QUANG VINH

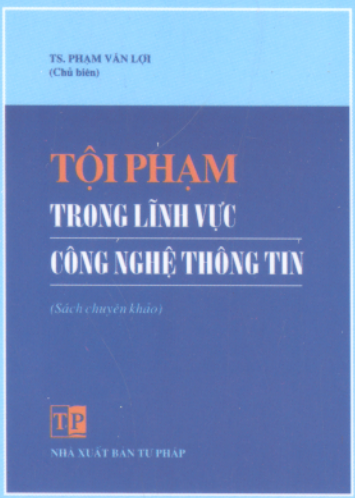
Biên tập
TRƯƠNG THU HÀ

Biên tập mỹ thuật
ĐẶNG VINH QUANG

Trình bày
NGUYỄN HUYỀN THANH

Sửa bản in
PHÒNG SỬA BÀI

In 1.000c, khổ 14,5x20,5cm, tại Công ty In và Văn hoá phẩm. Kế hoạch xuất bản số: 137-2007/CXB/40-07/NXBTP được Cục Xuất bản xác nhận đăng ký ngày 13/02/2007. In xong, nộp lưu chiểu tháng 4 năm 2007.



Giá: 26.000 đ