HỌC VIỆN KỸ THUẬT MẬT MÃ

TS. NGUYỄN ĐÌNH VINH
THS. TRẦN QUANG KỲ

GIÁO TRÌNH

LUẬT PHÁP AN TOÀN THÔNG TIN

HÀ NỘI - 2007

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

1.	TT	Thông tin
2.	CNTT	Công nghệ thông tin
3.	ATTT	An toàn thông tin
4.	BVTT	Bảo vệ thông tin
5.	HT	Hệ thống
6.	TCTP	Tiếp cận trái phép
7.	CSDL	Cơ sở dữ liệu
8.	DBMS	Hệ quản trị cơ sở dữ liệu
9.	GD&ĐT	Giáo dục và đào tạo
10.	MT	Máy tính
11.	PC	Máy tính cá nhân
12.	SNG	Cộng đồng các quốc gia độc lập
13.	HTMT	Hệ thống máy tính
14.	CT&DL	Chương trình và dữ liệu
15.	WIPO	Tổ chức sở hữu trí tuệ thế giới
16.	DMCA	Luật bản quyền thiên niên kỷ số hoá
17.	CO	Cơ quan bản quyền (Copyright Office)
18.	SHTT	Sở hữu trí tuệ
19.	PO	Cơ quan sáng chế (Patent Office)
20.	PTO	Cơ quan sáng chế và thương hiệu (Patent and Trademark Office)
21.	BMTM	Bí mật thương mại
22.	EU	Cộng đồng Châu Âu
23.	MĐT	Mã đối tượng
24.	HĐTK	Hợp đồng thuê khoán
25.	IEEE	Viện kỹ sư Điện - Điện tử (Mỹ)
26.	ACM	Hiệp hội máy tính (Mỹ)
27.	CEI	Viện đạo đức học máy tính (Mỹ)

28.	USC	Hiến pháp Hoa Kỳ (United States Constitute)
29.	FTC	Uỷ ban thương mại liên bang (Hoa Kỳ)
30.	EC	Uỷ ban Châu Âu (Europe Council)
31.	DES	Chuẩn mã dữ liệu (Mỹ)

LỜI NÓI ĐẦU

Thời gian gần đây chúng ta thường nghe nói nhiều đến các vụ tấn công vào các hệ thống máy tính của các ngân hàng, của các cơ quan quản lý nhà nước, của các cơ quan quốc phòng, an ninh trên khắp thế giới. Ở nước ta mới đây nhất là vụ xâm nhập trái phép vào trang Web của bộ GD&ĐT gây nhiều tai tiếng trong dư luận. Vấn đề bảo vệ thông tin (TT) nhất là các TT nhạy cảm ngày càng thu hút sự chú ý của xã hội và của giới chuyên môn. Một chuyên ngành mới gắn liền với vấn đề an toàn TT (ATTT) đã ra đời - đó là chuyên ngành tội phạm học máy tính (Computer Forensics).

Mục tiêu của tội phạm máy tính có thể là chi tiết bất kỳ của hệ tính toán. Các mục tiêu này có những đặc tính khác với các mục tiêu tội phạm thông thường.

• Kích thước và tính cơ động: Các thiết bị vật lý trong hệ MT nhỏ đến mức giá trị của chúng là đến hàng nghìn đô - la vẫn có thể để gọn trong một valy nhỏ và trị giá hàng chục nghìn đô - la vẫn có thể mang được trên hai tay.

• Khả năng không cần tiếp xúc vật lý trực tiếp: Các quỹ điện tử chuyển khoản hầu hết là tiền gửi các ngân hàng. Ví dụ, một số cơ quan trả lương cho cán bộ nhân viên bằng cách chuyển trực tiếp tài khoản qua máy tính thay thế tiền mặt. Khách hàng có thể gửi tiền vào ngân hàng ngay ở nhà mình, di chuyển quỹ giữa các tài khoản và sắp xếp việc rút tiền thông qua MT cá nhân.

• Giá trị tài sản: Giá trị của TT được lưu giữ trong mỗi hệ MT rất cao. Một số MT chứa TT bí mật của các cá nhân như thuế, các khoản đầu tư, bệnh tật. Một số máy khác lại chứa TT về các dòng sản phẩm mới, các số liệu thương mại, các chiến lược tiếp thị … Các hệ MT trong các cơ quan an ninh, quốc phòng chứa các TT tuyệt mật về bí mật quốc gia, các mục tiêu quân sự, các phong trào đấu tranh, các vũ khí chiến lược…

Rõ ràng ATTT là một vấn đề rất quan trọng, trong thời đại CNTT phát triển nhanh đến mức chóng mặt thì nó lại càng trở nên bức xúc hơn bao giờ hết. Hệ MT là một mục tiêu phức tạp. Hệ MT gồm phần cứng, phần mềm, đường truyền, dữ liệu và con người thao tác. Một kẻ gian quan tâm đến một ngân hàng, nó có thể tấn công vào hệ MT của ngân hàng đó trên nhiều mục tiêu (chứ không nhất thiết chỉ vào tiền mặt để trong két). Danh sách khách hàng và địa chỉ của họ, tài khoản cá nhân và các giao dịch tài chính thường nhật…đều có thể nằm trong vòng ngắm. Danh sách có thể ghi trên giấy, trên đĩa từ, được lưu trong bộ nhớ MT hoặc được truyền qua đường truyền thông bằng modem, điện thoại… Sự đa dạng của các mục tiêu có thể tấn công làm cho an toàn MT càng trở nên khó khăn hơn.

Trong những học kỳ trước, chúng ta đã nghiên cứu khá sâu về các tai họa về ATTT và đặc biệt là các phương pháp để bảo vệ thông tin trong các hệ MT để chống lại các hiểm họa đó. Chúng ta đã làm quen với kỹ thuật mật mã, với kiểm soát phần mềm, kiểm soát phần cứng, các kiểm soát vật lý và kiểm soát con người…Tất cả các phương pháp BVTT đã biết đều nhằm tới bảo vệ cho được tính bí mật, tính toàn vẹn và tính sẵn sàng phục vụ của các thành phần trong các hệ máy tính.

Giáo trình này dành riêng giới thiệu về pháp luật ATTT. Các kiểm soát về pháp lý và đạo lý là một phần quan trọng của ATTT. Tất cả các loại tội phạm đều cần chống lại bằng pháp luật. Với tội phạm máy tính cũng như vậy. Pháp luật chống lại tội phạm máy tính, bảo vệ an toàn hệ máy tính, ATTT gọi là pháp luật an toàn thông tin. Phải ban hành các đạo luật quy định bắt buộc mọi người phải tuân thủ khi làm việc với các hệ MT và các TT trong đó, nghiêm cấm các hành vi phạm tội trong quá trình giao tác thông tin, bảo vệ hiệu quả các lợi ích của Nhà nước, xã hội và cá nhân trong lĩnh vực thông tin; tạo ra hành lang pháp lý cho các hoạt động về đảm bảo ATTT… ở góc độ quốc gia và quốc tế. Đó chính là mục đích của luật pháp ATTT.

Pháp lý có tác dụng trừng phạt và răn đe; nó cũng có tác dụng to lớn trong giáo dục và giác ngộ. Do đó pháp lý luôn song hành với đạo lý. Đạo đức không mang tính cưỡng chế, nhưng nó lại rất quan trọng trong hình thành nhân cách con người, xác định các hành vi và phương cách ứng xử xã hội của cá nhân. Trong xã hội TT, nền kinh tế TT (hay còn gọi là kinh tế tri thức) thì việc ứng xử đúng theo các chuẩn mực đạo đức của xã hội TT nói chung và các hành vi đạo đức đúng đắn về ATTT nói riêng cũng là đòi hỏi ngày càng cấp thiết.

Các kỹ sư ATTT là những người làm việc bảo vệ ATTT trong thế giới CNTT (Cyber Space). Họ phải nắm vững CNTT, các kỹ thuật, công nghệ ATTT, các giải pháp bảo vệ hệ MT và các TT chứa trong đó. Họ cũng cần phải hiểu biết về các pháp luật ATTT và các vấn đề về đạo đức học máy tính và tội phạm học máy tính. Vì - chúng ta đã biết – bảo vệ bằng luật pháp là một phương pháp phi kỹ thuật hữu hiệu của ATTT; và vì chính các kỹ sư ATTT là những người trực tiếp làm việc với các CNTT và đối mặt với tội phạm MT nên họ cần hơn ai hết nắm được và tuân thủ các chuẩn mực đạo đức, các hành vi ứng xử nghề nghiệp đúng đắn trong xã hội thông tin phát triển nhanh chóng. Giáo trình này có mục đích cung cấp cho người học các kiến thức thuộc hai vấn đề đó.

Lần đầu tiên một giáo trình loại này được biên soạn, khó tránh được các thiếu sót, rất mong được sự đóng góp của các đồng nghiệp và bạn đọc gần xa.

Hà Nội tháng 11 năm 2007

Các tác giả

CHƯƠNG I NHỮNG VẤN ĐỀ LUẬT PHÁP TRONG AN TOÀN MÁY TÍNH

1.1 Công nghệ thông tin hiện đại và các vấn đề về an toàn - an ninh thông tin

1.1.1 Sự phát triển của CNTT và vai trò của nó trong xã hội hiện đại.

Công nghệ thông tin (CNTT) là tập hợp các phương pháp khoa học, các phương tiện và công cụ kỹ thuật hiện đại (chủ yếu là kỹ thuật máy tính và viễn thông) nhằm tổ chức khai thác và sử dụng có hiệu quả các nguồn tài nguyên TT rất phong phú và tiềm năng trong mọi lĩnh vực hoạt động của con người.

CNTT là một ngành non trẻ (theo nghĩa mới ra đời từ những năm 70 của thế kỷ 20) nhưng lại có tốc độ phát triển nhanh nhất và ảnh hưởng rộng lớn nhất tới sự phát triển của nhân loại. Người ta tính rằng, hiện nay cứ 5 đến 7 năm thì khoa học cơ bản lại tăng lên gấp đôi, còn CNTT để tăng lên 2 lần thì chỉ cần 5 đến 7 tháng. Các bộ vi xử lý phát triển đến chóng mặt, các máy tính PC đã có công suất đến bất ngờ và đã được liên kết thành các mạng LAN, mạng WAN… và siêu mạng Internet toàn cầu. Con người, ngồi trong căn phòng riêng của mình có thể tiếp nhận và trao đổi thông tin với toàn thế giới. Con người thấy mình mạnh mẽ làm sao. Một thế giới mới, một không gian điều khiển (Cyber Space) trao vào tay họ những công cụ kỳ diệu, những khả năng to lớn nhưng cũng đặt họ trước những thách thức không nhỏ.

CNTT với ảnh hưởng mọi mặt của nó đã góp phần hình thành một nền kinh tế – xã hội loại mới – nền kinh tế trí thức. Đã ra đời một xã hội thông tin dựa trên một xà hội học tập hứa hẹn một tương lai phát triển đa dạng và phong phú của con người.

1.1.2 Các hiểm họa về ATTT và các vấn đề tội phạm xã hội.

Con người hoạt động trong không gian CNTT thu được nhiều lợi ích to lớn nhưng cũng đứng trước nhiều hiểm họa khó lường. Đó là các hiểm họa về an toàn thông tin. Cũng như trong xã hội nói chung, xã hội thông tin cũng đầy rẫy các loại tội phạm CNTT mà đòi hỏi phải có các biện pháp hữu hiệu để ngăn chặn, chống lại; phải có các biện pháp trừng phạt và răn đe cũng như các giải pháp giác ngộ và giáo dục…

Chiếc PC của bạn bỗng nhiên chạy chậm như rùa, thiếu ổn định, bị treo, một số dữ liệu quan trọng bị mất. Trang Web của cơ quan tự dưng xuất hiện những hình ảnh lời lẽ tục tĩu. Một số tiền lớn trong tài khoản ngân hàng của bạn bị biến mất một cách khó hiểu… Nghi phạm số một ở đây là một Hắc – cơ (hacker – tin tặc). Hắc–cơ đã tạo ra một "lỗ hổng" trong hệ MT hoặc lợi dụng "lỗ hổng" sẵn có trong hệ MT đó để lọt vào… Theo số liệu vừa công bố, 26% các website của Việt Nam có mức đề kháng rất yếu đối với các virus máy tính. Bức tường lửa các

loại (Firewalls) nhiều khi vẫn bị bọn tội phạm chọc thủng để thực hiện các hành vi bất lương của chúng.

Chúng ta đã biết cách phân loại các hiểm họa ATTT và các phương pháp cơ bản về mặt công nghệ để đối phó với chúng. Nói chung có 3 loại hiểm họa ATTT cơ bản là:

- Hiểm họa phá vỡ tính bí mật của TT;
- Hiểm họa đe dọa tính toàn vẹn TT; và
- Hiểm từ chối dịch vụ của TT.

Trong mỗi loại hiểm họa lại có thể liệt kê hàng trăm, hàng nghìn các tấn công có tính tội phạm vào các mục tiêu rất đa dạng của một hệ MT (gồm phần cứng, phầm mềm, đường truyền, dữ liệu và con người).

Nói như vậy thì thấy vấn đề tội phạm MT là một vấn đề mới và rất phức tạp. Đây là loại tội phạm gắn liền với CNTT, là một thế hệ các loại tội phạm mới. Lớp tội phạm này dựa trên các đặc thù về công nghệ được dùng trong môi trường ảo, trong không gian điều khiển (Cybercrimes). Nó ngày càng phát triển về số lượng, chủng loại và mức độ tinh vi; nó không chỉ định vị ở một quốc gia mà diễn ra trên quy mô toàn thế giới.

Để đối phó với loại tội phạm này các biện pháp kỹ thuật công nghệ ATTT là quan trọng nhưng chưa đủ. Cần phải có hệ thống pháp luật ATTT hoàn chỉnh và không ngừng được sửa đổi bổ sung, cập nhật. Cũng cần phải có các quy tắc, chuẩn mực về đạo đức để hướng dẫn xã hội giác ngộ về các vấn đề ATTT, phong cách ứng xử nghề nghiệp phù hợp với quy trình làm việc với MT và ATTT.

1.1.3 Tội phạm máy tính và an toàn thông tin.

Tội phạm MT (Tiếng Anh là Cyber crimes hoặc Computer crimes) về bản chất cũng là các tội phạm truyền thống được thực hiện nhờ các CNTT (nhờ MT) hoặc diễn ra trong không gian điều khiển (hay không gian ảo) nhằm phá vỡ ATTT, xâm phạm đến quyền lợi về TT của quốc gia, tổ chức xã hội và cá nhân, được bảo hộ bởi pháp luật ATTT.

Một số quốc gia coi tội phạm MT là những hành vi vi phạm pháp luật về CNTT, một số quốc gia khác định nghĩa tội phạm MT như là các hành vi phạm pháp có liên quan đến MT, mạng MT. Dù định nghĩa hình thức có thể khác nhau, trên thực tế mọi tội phạm MT đều làm phá vỡ ATTT của quốc gia, của tổ chức kinh tế – xã hội, hoặc của cá nhân nào đó. Có thể phân ra làm 2 loại tội phạm MT cơ bản: Loại 1 – sử dụng MT, mạng MT như là công cụ để thực hiện hành vi phạm pháp và loại 2 – dùng MT, mạng MT làm nơi diễn ra các hành vi phạm pháp.

- Loại 1 thường thực hiện các hành vi phạm pháp trong các lĩnh vực sau:

1. Phạm pháp trong lĩnh vực tài chính – ngân hàng:

Sử dụng MT nhằm mục đích lấy tiền bất hợp pháp từ các tài khoản của khách hàng. Đây là hình thức cướp ngân hàng qua mạng. Hình thức này đã xảy ra nhiều ở châu Mỹ, châu Âu và nhất là các nước SNG. Đặc điểm của loại hình tội phạm này là có quy mô toàn cầu, thường thì kẻ phạm tội ở nước này gây án ở nước khác.

Lấy cắp mật khẩu của thẻ tín dụng (ATM) để lấy tiền.

Cài đặt các chương trình tự động vào hệ MT của các ngân hàng để trích trộm số lẻ (rất nhỏ) từ các tài khoản của khách hàng vào tài khoản của mình, qua đó có thể lấy được số tiền rất lớn trong thời gian dài.

2. Hành vi xâm phạm trong lĩnh vực sở hữu trí tuệ – bản quyền.

Môi trường mạng MT (ảo) rất thuận lợi cho các hành vi xâm phạm bản quyền số và sở hữu trí tuệ. Dạng tội phạm này phát triển rất mạnh và rất khó kiểm soát trên Internet. Đó là các hành vi lấy cắp phần mềm; ăn cắp dữ liệu; vi phạm bản quyền tác giả đối với các tác phẩm văn học, nghệ thuật (đạo nhạc), hội họa; giả mạo thương hiệu; ăn cắp mã nguồn của máy tính…

3. Tội phạm liên quan đến Thư điện tử (Email Spoofing).

Email spoofing có nghĩa là thư điện tử giả danh. Email spoofing được bắt nguồn từ một bức thư điện tử và phát tán đến các địa chỉ thư điện tử khác. Email spoofing thường cố gắng lừa người sử dụng bằng cách gửi các TT đến họ để có được các TT nhạy cảm của người đó (như mật khẩu, số thẻ tín dụng…). Thường hay xảy ra trường hợp, khi Email spoofing giả danh địa chỉ của nhà cung cấp dịch vụ gửi thư đến các thành viên sử dụng dịch vụ. Email spoofing cũng gây ra các thiệt hại về tài chính

4. Tội phạm trong lĩnh vực Forgery (Làm giả).

Sử dụng các phương tiện hiện đại như máy tính, máy tin và máy quét ảnh để làm giả các loại tiền, bưu phẩm, cổ phiếu, tem thuế và những giấy tờ quan trọng khác như bằng cấp, chứng nhận…

5. Tội phạm nhục mạ, vu khống người khác trên mạng.

Sử dụng các phương tiện trên Internet như các Websites, Email để phát tán thông tin nhục mạ, vu khống, bôi nhọ người khác. Thường thì các thông tin có tính chất nhục mạ này được gửi tới những người thân quen hay trong môi trường làm việc của người bị hại. Tiêu biểu là trường hợp nhân viên nào đó gửi Email bôi xấu lãnh đạo và gửi nhiều lần tới các đồng nghiệp trong cơ quan.

6. Tội phạm quấy rối trên mạng (Cyber staking).

Trong Cyber staking, tội phạm thường gửi Email quấy rối qua việc xuất hiện thường xuyên trên chatroom của người bị hại hoặc tội phạm luôn luôn gửi bom thư vào hộp thư của người bị hại.

7. Tội phạm đưa phim ảnh đồi truy, khiêu dâm lên mạng.

Dùng Website và các tạp chí điện tử để phổ cập, sản xuất, phát tán, trao đổi và cho tải về phim, ảnh và các ấn phẩm bị cấm; cung cấp thông tin khiêu dâm cho trẻ vị thành niên; thực hiện những phi vụ gọi gái, gọi trai mãi dâm trên mạng…

8. Tội phạm bán các mặt hàng cấm trên mạng MT.

Các mặt hàng cấm như vũ khí, động vật quý hiếm, ma túy… được rao bán công khai, núp danh hay đấu thầu qua các hình thức bán hàng trên mạng.

9. Tội phạm đánh bạc trực tuyến.

Hiện có hàng chục Website trên thế giới cung cấp dịch vụ đánh bạc trực tuyến hoặc tổ chức các hình thức cá độ trên mạng. Trong số này rất nhiều địa chỉ là những nơi rửa tiền trên mạng.

• Loại 2 thường xảy ra các dạng sau đây:

1. Truy nhập bất hợp pháp vào hệ thống MT hay mạng MT.

Hoạt động truy nhập trái phép vào hệ MT thường được gọi là Hacking. Hacking có rất nhiều dạng để tìm cách chọc thủng các tuyến bảo vệ của hệ MT nhằm xâm nhập vào các tài nguyên hệ thống. Giải pháp cho vấn đề này phải đồng bộ cả về kỹ thuật và khung hình pháp lý. Ngăn chặn các truy nhập trái phép là yêu cầu an toàn cơ bản nhất đối với một hệ MT bất kỳ, và ngày nay đó đã là yêu cầu của tất cả các chuẩn đánh giá ATTT.

2. Ăn cắp TT điện tử.

Tìm cách sở hữu trái phép các dữ liệu được lưu giữ trên đĩa cứng máy tính, hoặc trên các phương tiện lưu trữ dữ liệu của người khác…

3. Tội phạm gửi bom thư điện tử (Email bombing).

Đó là hành vi gửi hàng nghìn bức thư điện tử đến địa chỉ Email của nạn nhân (oanh tạc hòm thư) hoặc máy chủ quản lý Email, khiến cho hòm thư của nạn nhân hoặc máy chủ quản lý bị đầy dữ liệu (overflow – tràn), tê liệt không thể tiếp nhận được thư nữa.

4. Tội phạm sửa chữa (xuyên tạc) dữ liệu.

Cách thức này tấn công vào các dữ liệu thô, dùng máy tính sửa chữa dữ liệu, sau đó ghi đè lên dữ liệu thô nhằm làm thay đổi một cách không hợp pháp các dữ liệu.

5. Tội phạm tấn công từ chối dịch vụ.

Sự tấn công này bao gồm các hành vi như làm tràn bộ nhớ hệ thống máy chủ cung cấp dịch vụ; điều khiển dừng cung cấp dịch vụ cho khách hàng. Kẻ tấn công thường gửi những yêu cầu quá mức, vượt giới hạn cung cấp của các máy chủ nạn nhân và làm cho máy chủ bị sập hoàn toàn.

6. Tấn công các hệ thống bằng virus, worm, ngựa Troa.

Hiện nay có rất nhiều loại virus được đính kèm chương trình máy tính hay cài vào các file. Khi người sử dụng cài đặt các chương trình đó thì đồng thời cũng vô tình cài đặt luôn cả virus dẫn đến tình trạng dữ liệu bị xóa hoàn toàn hoặc có thể bị chèn thêm các TT khác. Có một số loại worm hoặc ngựa Troa có khả năng thâm nhập nhằm lấy được mật khẩu của nạn nhân để thực hiện các hành vi phạm pháp.

7. Ăn cắp thời lượng Internet.

Tội phạm này bao gồm các hành vi sử dụng mật khẩu và tài khoản của người bị hại để truy nhập Internet khiến cho các nạn nhân phải trả số tiền dịch vụ rất cao mà thực ra họ không sử dụng,

8. Giành quyền kiểm soát Web (web hacking).

Đây là hiện tượng khi một Hacker nắm được quyền kiểm soát của một Website bằng việc thay đổi mật khẩu của người chủ thực sự của Website.

9. Giành quyền kiểm soát hệ thống MT.

Sử dụng quyền quản trị giả mạo để kiểm soát và điều khiển toàn bộ hệ thống máy tính.

10. Phá hỏng phần cứng MT, các vật mang TT của hệ thống.

11. Dùng các kênh vật lý (như kênh âm thanh, kênh video, kênh điện từ…) để xâm nhập, ăn cắp thông tin nhạy cảm như trộm, chụp trộm, thu bức xạ điện từ…

Như trên chúng ta thấy, các tội phạm máy tính có nhiều đặc điểm khác với tội phạm truyền thống. Có thể kể ra các tính chất tiêu biểu là:

- Khó bị phát hiện vì các phương tiện hiện đại để phát hiện ra chúng không phải luôn có hiệu quả.
- Khó bị ngăn ngừa và vô hiệu hóa các hậu quả của chúng vì thường thì các phương tiện và các phương pháp bảo vệ bị tụt hậu so với các phương tiện và phương pháp tấn công.
- Thường không bị trừng phạt thích đáng do thiếu cơ sở pháp lý đủ mạnh và thiếu sự phối hợp chặt chẽ của pháp lý quốc tế.
- Được thực hiện ở phạm vi toàn cầu nhờ sử dụng liên lạc viễn thông.
- Có tính trí tuệ cao, có kỹ năng điêu luyện và đa dạng.

- Ngày càng có tính tổ chức cao.

Mặc dù một ngành khoa học kỹ thuật hình sự mới liên quan tới vấn đề tội phạm loại này là Điều tra học tội phạm máy tính đã ra đời, nhưng việc thu thập các chứng cứ điện tử của tội phạm máy tính còn hết sức khó khăn. Cùng với việc hệ thống pháp luật ATTT chưa hoàn chỉnh, đạo đức hành nghề MT chưa phát triển, các biện pháp và các phương tiện bảo vệ chưa thật sự hiệu quả làm cho việc bảo đảm ATTT gặp rất nhiều thách thức.

Ở đây, chúng ta quan tâm đặc biệt đến vấn đề các tội phạm MT gây tổn thất cho an ninh TT quốc gia, vì chúng đe dọa đến lợi ích quốc gia trong lĩnh vực ATTT. Trên thực tế, người ta chia loại tội phạm MT gây tổn hại quyền lợi quốc gia thành các dạng sau đây:

- Truy cập trái phép (TCTP) tới các mạng và các hệ thống MT nhằm mục đích hủy hoại, làm ngưng trệ hoạt động bình thường của chúng.
- TCTP tới các mạng, các hệ thống và các cơ sở dữ liệu (CSDL) nhằm mục đích thu thập các TT bí mật.
- Tạo lập và sử dụng các chương trình phá hoại.
- Lừa đảo và ăn cắp bằng liên lạc viễn thông.
- Các hành vi phạm luật nhằm chống phá chính quyền, chống phá Đảng, làm mất ổn định chính trị và đe dọa tới an ninh quốc gia.

Tiếp theo chúng ta sẽ xem xét một số ví dụ về tội phạm MT thuộc các dạng nêu trên.

1. TCTP các mạng và các HT MT phá hoại sự hoạt động bình thường của chúng.

- Phá hỏng các mạng và các hệ thống MT.

Đối tượng tấn công ở đây có thể là: các hệ thống MT; các hệ thống TT – VT trong lĩnh vực hoạt động Nhà nước, trong xây dựng, trong quốc phòng, trong các khoa học công nghệ mới nhất; cơ sở hạ tầng thông tin quân sự; kiến trúc TT quản lý của các ngân hàng, các cơ sở sản xuất công nghiệp, giao thông vận tải, dầu khí…

Mục tiêu của bọn tội phạm là gây rối loạn hoạt động của các cấu trúc điều khiển; các luồng giao thông và các phương tiện liên lạc; phong tỏa hoạt động của các doanh nghiệp, sân bay, bến cảng và các ngân hàng riêng lẻ cũng như một số lĩnh vực công nghiệp nhất định; khởi tạo những thảm họa công nghệ Gen lớn.

Năm 2004 đã xảy ra rất nhiều vụ tấn công " từ chối dịch vụ – DOS " vào các máy chủ của các cơ quan chính phủ và tài chính ngân hàng của nhiều nước làm chúng ngừng hoạt động trong nhiều giờ hoặc cả một ngày. Thiệt hại từ các tấn

công như vậy trong năm 2004 người ta tính được lên tới 34 tỷ USD. Mục tiêu ưa thích nhất của các tin tặc ở đây là các mạng quân sự và vũ trụ của Hoa Kỳ. Từ London (Anh) một nhân viên quản trị mạng là Garry Mackiman đã luồn vào được 92 mạng MT của Nhà Trắng và Cơ quan hàng không vũ trụ quốc gia Mỹ. Việc phá hoại các mạng MT thường được thực hiện từ những nước có sự cạnh tranh nhau trong các lĩnh vực chính trị và/hoặc kinh tế. Chẳng hạn, Trung Quốc có thể bị đe dọa bởi các tin tặc từ Hàn Quốc, Đài Loan, Nhật Bản, Malaixia và một số nước khác của khu vực Đông Nam Á.

- Tội phạm có tính lưu manh trên mạng.

Tệ nạn này thường được thực hiện với mục đích làm thay đổi TT trong website của các cơ quan Nhà nước. Ví dụ, một tin tặc đã vượt qua hệ thống bảo vệ, chui vào website của Hội đồng bang California làm hỏng website này. Một nhóm tin tặc đã thành công trong việc bẻ khóa website của Bộ tài chính Rumania và đánh sập nó. Sau tháng đầu tiên đi vào hoạt động website của tổng thống Nga V.Putin (www.kremlin.ru), tài nguyên mạng đã bị tin tặc tấn công 8743 lần. Các chuyên gia Nga đã phát hiện rằng, trong số những kẻ tội phạm ngoài nước Nga, còn có tin tặc từ các nước châu Âu và Bắc Mỹ. Hiện thời những cuộc đột nhập như vậy xảy ra khoảng 500 lần mỗi tháng.

- Hủy hoại MT hoặc các tài nguyên mạng.

Cộng đồng Internet đã quen thuộc với các tấn công tin tặc có nguyên nhân chính trị. Ví dụ, đáp trả sự tấn công của tin tặc A-dec-bai-gian láng giềng vào các website của Armenia, tin tặc nước này đã tiến hành trên mạng Internet "hành động trừng phạt", mà hậu quả là làm hỏng hàng loạt website của đối thủ. Số lượng các website bị phá hủy hoặc hỏng hóc của cả 2 bên lên đến gần 100.

2. TCTP tới các mạng, các HTMT và các CSDL nhằm thu thập các TT bí mật.

- Lấy cắp hoặc tiết lộ các TT mật mang tính quốc gia, tình báo hoặc quân sự.

Các tổ chức và cá nhân thâm nhập vào HTTT của các cơ cấu nhà nước để lấy cắp TT, sau đó dùng chúng với mục đích riêng gây nên mối đe dọa nghiêm trọng cho an ninh quốc gia. Ví dụ, năm 2002, công ty ForensicTech (của Mỹ) đã gây nên vụ tai tiếng lớn khi họ chuyển cho phóng viên Wasington Post những bằng chứng về việc đã lọt vào các mạng MT của 34 tổ chức có liên hệ tới những đầu mối quan trọng của Hoa Kỳ như Bộ binh và Hải quân, NASA, Bộ năng lượng…Thông tin bị lấy ra ở đây là bí mật quốc gia.

- Lấy cắp dữ liệu máy tính.

Những bon tội phạm tìm mọi cách ăn cắp dữ liệu MT vì mục đích vụ lợi. Trong số đó có các dữ liệu của các cơ quan Nhà nước với nội dung rất đa dạng và nhạy cảm. Chỉ riêng trong năm 2004, tổng thiệt hại từ việc lấy cắp dữ liệu MT của Hoa Kỳ đã lên đến 52,6 tỷ USD.

3. Tạo lập và sử dụng các chương trình gây hại.

Không gian ảo là một môi trường lý tưởng để phát tán virus MT và các chương trình độc hại như Worm, ngựa Tơ-roa, bom logic… Chúng được tạo ra một cách cố ý nhằm gây thiệt hại cho các HTMT và các mạng TT chủ yếu thuộc tài sản quốc gia. Chẳng hạn vào tháng 5 . 2000, sâu Lovebug đã làm hư hỏng tập địa chỉ của các HT thư điện tử của 14 đầu mối Liên bang của Hoa Kỳ, trong đó có cả CIA, Bộ Quốc Phòng, Nhà Trắng và Nghị viện.

Tỷ lệ thư điện tử bị nhiễm virus đang tăng nhanh: vào 1.2004 tỷ lệ trung bình là 1/129 ; còn vào 12.2004 con số đó là 1/51; tiếp đến 1.2005 là 1/35 và 6.2005 là 1/28. Số lượng các loại virus và sâu mới trên thế giới vào nửa cuối năm 2006 đã tăng 7300 loại so với cùng thời năm 2003.

Một số chương trình dạng "Ngựa Tơ-roa" có khả năng tạo ra sự rò rỉ TT quan trọng, đe dọa tới lợi ích quốc gia. Vào 6.2004, một kẻ gian đã thành công trong việc làm lây nhiễm virus cho các tài nguyên điện tử của chính phủ Hàn Quốc (64 máy tính), trong đó có website của Bộ quốc phòng. Theo số liệu chính thức, tại Hàn Quốc tin tặc có khả năng làm lan truyền chương trình Peep Trojan lên các MT của các hãng chuyên chế tạo các thiết bị bảo vệ dùng cho các địa chỉ quan trọng.

Nếu như trước đây, mục đích chủ yếu của lây nhiễm virus là làm chậm hoặc ngưng trên hoạt động của HTMT thì đến nay, những kẻ tin tặc có khả năng hủy hoại hoạt động của doanh nghiệp, chiếm đoạt TT đã được xác thực, ăn cắp tài nguyên sở hữu trí tuệ hoặc các tài nguyên tiền bạc.

4. Lừa đảo và lấy cắp bằng viễn thông.

Nhóm tội phạm MT này gồm các hành vi gian lận tài chính – ngoại hối, ăn cắp tiền ngân hàng.

Trong những năm gần đây, fishsing (câu) là dạng tội phạm phổ biến nhất, được thực hiện qua Internet nhằm rửa tiền và lấy cắp dữ liệu đã được xác thực. Đây là một biến thể của lừa đảo MT. Tin tặc gửi TT đến người dùng theo đường Email, dưới những lý do khác nhau, yêu cầu họ đi vào một website được tạo ra cố ý sẵn trong đó đã sao chép giao diện của máy dịch vụ hợp thức hiện thời và yêu cầu người dùng phải làm mới một số dữ liệu nào đó: ví dụ, nhập vào mật khẩu, đăng nhập, số tài khoản…

Cảnh sát Anh mới đây đã tính được rằng, chỉ riêng trong năm 2004 những kẻ fishsing đã chiếm đoạt từ các tài khoản ngân hàng của người dùng khoảng 60 triệu bảng Anh. Theo số liệu báo cáo gần đây của Index Security Business Global, trong nửa đầu 2005 đã có hơn 35 triệu tấn công dạng fishsing để lấy cắp các dữ liệu quan trọng và các TT nhận dạng nhằm mục đích vụ lợi. Thiệt hại từ những tấn công như vậy đối với các tổ chức trên toàn thế giới ước tính khoảng 2,5 tỷ Euro.

5. Các hành động tội phạm nhằm chống phá chính quyền Nhà nước và đe dọa an ninh quốc gia.

Nhóm tội phạm này bao gồm các hành vi sau đây: Truyền bá những tư tưởng cực đoan, chống đối chính sách của Nhà nước, nhen nhóm kích động tư tưởng hận thù dân tộc, khiêu khích phá hoại chính quyền, bôi nhọ chế độ, phát tán các TT độc hại…

Trong điều kiện hiện đại, khi sự phát triển nhanh chóng các CNTT kéo theo sự tăng mạnh tội phạm MT, ở hầu hết các nước đã nghiên cứu và thực hiện những biện pháp nhằm tạo lập các hệ thống ATTT, các phương tiện và các công nghệ bảo đảm ATTT, nhằm bảo vệ các tài nguyên TT và liên lạc quốc gia. Xu thế hiện nay là tiến hành đồng bộ các giải pháp và phương pháp trong tổng thể của 3 lĩnh vực: Công nghệ – pháp lý – các chuẩn.

1.2. Giới thiệu chung về các vấn đề luật pháp trong An toàn thông tin.

1.2.1 Bảo vệ các hệ thống MT chống lại các tội phạm.

Chống lại các tội phạm MT là yêu cầu khách quan đối với luật pháp ATTT. Chính các hành vi tội phạm là kết quả của các cuộc tấn công vào các hệ thống ATTT, biến các hiểm họa đối với một đối tượng nào đó trở thành hiện thực, biến các mối đe dọa ATTT thành hành động phá vỡ ATTT thực tế. Như trên đã nói, các biện pháp bảo vệ pháp lý là một trong các giải pháp quan trọng và cần thiết của việc bảo đảm ATTT, an ninh thông tin quốc gia. Trên góc độ đó thì bảo vệ các hệ thống MT chống lại tội phạm MT là chức năng ATTT cơ bản của pháp luật ATTT.

Từ quan điểm pháp lý thì các tội phạm MT là căn cứ khoa học thực tiễn (là cơ sở khách quan) để hình thành nên các quy phạm pháp luật về ATTT. Ở đây chúng ta cần nhớ lại khái niệm quy phạm pháp luật của khoa học pháp lý như sau:

- Quy phạm pháp luật chỉ do Nhà nước đặt ra hoặc thừa nhận và được bảo đảm thực hiện bằng các biện pháp cưỡng chế Nhà nước. Nhà nước thiết lập ra một hệ thống cơ quan chuyên môn để bảo đảm cho pháp luật (là tập hợp nhiều quy phạm pháp luật) được thực hiện chính xác và triệt để. Bất kỳ chủ thể nào vi phạm các quy phạm pháp luật cũng đều phải bị truy cứu trách nhiệm pháp lý.
- Quy phạm pháp luật là quy tắc xử sự mang tính bắt buộc chung. Quy phạm pháp luật được đặt ra không phải cho một chủ thể cụ thể mà cho các chủ thể không xác định. Tính bắt buộc chung của quy phạm pháp luật được hiểu là bắt buộc với tất cả mọi người nằm trong hoàn cảnh, điều kiện mà quy phạm pháp luật đó quy định.

- Nội dung mỗi quy phạm pháp luật là rõ ràng, chính xác, nó quy định những điều kiện được làm, không được làm. Nói cách khác, QPPL xác định rõ quyền và nghĩa vụ pháp lý của các bên tham gia quan hệ xã hội mà nó điều chỉnh.
- Về hình thức, QPPL là quy phạm thành văn được ghi nhận trong các văn bản pháp luật của Nhà nước, trình bày thành điều, khoản, có đánh số, mục rõ ràng.

Về mặt cấu trúc thì QPPL gồm 3 bộ phận hợp thành: Giả định, Quy định và Chế tài. **Phần giả định** nêu lên chủ thể (cá nhân, tổ chức), những hoàn cảnh, điều kiện. địa điểm, thời gian xảy ra hành vi trong cuộc sống mà con người gặp phải và cần phải xử sự theo những quy định của Nhà nước. Phần giả định tường trả lời câu hỏi ai? (tổ chức, cá nhân), khi nào? trong những điều kiện, hoàn cảnh nào?

Phần quy định là một bộ phận của QPPL trong đó nêu ra cách xử sự buộc mọi người phải theo khi ở vào điều kiện, hoàn cảnh đã nêu trong phần giả định của QPPL. Phần quy định thường trả lời câu hỏi: phải làm gì? được làm gì? làm như thế nào?

Quy định là một bộ phận quan trọng, là yếu tố trọng tâm của QPPL. Bởi vì quy định chính là bộ phận thể hiện ý chí và lợi ích của Nhà nước, của xã hội và của cá nhân con người trong việc điều chỉnh quan hệ xã hội nhất định. Quy định cũng chính là mệnh lệnh của Nhà nước buộc mọi chủ thể (tổ chức, cá nhân…) phải tuân theo nghiêm chỉnh.

Phần chế tài là một bộ phận của QPPL, nêu lên những biện pháp tác động mà nhà nước dự kiến sẽ áp dụng đối với chủ thể nào không thực hiện đúng bộ phận quy định của QPPL. Ở đây đưa ra các biện pháp trừng phạt thích đáng sẽ được Nhà nước áp dụng đối với các vi phạm của phần quy định nói trên.

Pháp luật ATTT đưa ra những quy định, hướng dẫn cho các cá nhân, tổ chức tham gia các giao tác TT, chỉ rõ các thao tác được thực hiện và các hành vi bị cấm; tạo ra các chuẩn mực pháp lý cho các ứng xử của cá nhân, tập thể để đảm bảo an toàn TT; đưa ra các hình phạt thích đáng đối với các tội phạm về ATTT. Do vậy pháp luật ATTT ngăn ngừa, chống lại các tội phạm MT và góp phần bảo vệ hữu hiệu an toàn TT cho các hệ MT.

1.2.2 Bảo vệ mã chương trình và dữ liệu (chống các truy cập trái phép phá vỡ tính bí mật).

Hệ thống pháp luật ATTT ở trong trạng thái hiện thời phù hợp khá tốt với công nghệ thông tin bằng việc dùng lại một số dạng cũ (đã có) của bảo vệ luật pháp (như luật bản quyền và sở hữu trí tuệ) và xây dựng các bộ luật mới cho các dạng kiểm soát mới (chưa có tiền lệ) gắn liền với công nghệ MT (như kiểm soát các truy nhập trái phép chẳng hạn). Chúng ta cũng biết Pháp luật và Đạo đức luôn luôn song hành với nhau, hỗ trợ nhau cũng góp phần bảo vệ cho an toàn của hệ thống MT. Tuy nhiên Pháp luật và Đạo đức chỉ là một mặt của vấn đề ATTT.

Toà án không phải là một dạng bảo vệ tốt nhất các tài nguyên MT; còn Đạo đức chậm kịp thay đổi vì nó mang tính tình huống và cá nhân hơn so với Luật pháp.

Luật pháp và ATTT liên quan với nhau theo nhiều cách. Thứ nhất, các bộ luật ATTT đều tác động tới tính riêng tư (bí mật). Thuật ngữ này thường được dùng để chỉ các quyền của các cá nhân (tổ chức) giữ kín các vấn đề của riêng mình tức TT riêng tư (TT bí mật).

Thứ hai, Luật pháp ATTT điều chỉnh việc sử dụng, phát triển và sở hữu các Dữ liệu (DL) và các Chương trình (CT). Các sở hữu trí tuệ (Bằng sáng chế, bằng phát minh), các bản quyền (tác giả) và các bí mật thương mại (thương hiệu) là các công cụ pháp lý để bảo vệ các quyền lợi của các nhà phát triển và chủ sở hữu của DL và CT. Một khía cạnh mới của ATTT là phải kiểm soát được các truy nhập tới các CT và DL trong HT, phải ngăn chặn được các tiếp cận trái phép tới các DL và CT. Sự kiểm soát như vậy cần tới sự hỗ trợ của các bộ luật.

Thứ ba, Luật pháp ATTT điều chỉnh các hành động cần thực thi (từ phía nhà quản trị, tổ chức, cá nhân) nhằm bảo vệ tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin MT và các dịch vụ. Các khía cạnh cơ bản này trong ATTT được tăng cường đáng kể và củng cố vững chắc bởi các bộ luật thích hợp.

Như vậy, các phương tiện luật pháp cũng tương tác với các dạng kiểm soát khác (về công nghệ, về chính sách …) tạo ra nền tảng của ATTT. Đó chính là bộ ba hoàn chỉnh của các phương pháp bảo vệ TT (hay còn gọi là Tam giác ATTT): công nghệ – chính sách quản lý – các quy chuẩn, tiêu chuẩn.

Công nghệ TT phát triển rất nhanh chóng làm cho vấn đề bảo đảm ATTT trở nên ngày càng bức xúc. Mặt khác luật pháp ATTT còn mới ở giai đoạn hình thành. Cho nên một bộ luật không phải lúc nào cũng cho ta một kiểm soát phù hợp (như vấn đề sao in không trả tiền các phần mềm các Hệ điều hành của Microsoft chẳng hạn). Cũng có thể giải thích nguyên nhân là vì; Khi các HT máy tính đã đi vào hoạt động và phát triển rầm rộ thì luật pháp lại chậm được xây dựng và thực thi. Tình hình ở đây không giống như là đối với quyền sở hữu thông thường. Máy tính (computers) là đối tượng mới, không giống như nhà, đất, trâu ngựa, hay tiền bạc. Và vị trí của các HT máy tính trong luật pháp còn chưa được xác lập rõ ràng; vai trò của MT và con người, DL và các quá trình khác liên quan đang được xác định rõ hơn trong luật pháp. Tuy nhiên, các điều luật vẫn chưa định vị đúng đắn được các hành vi thực hiện bằng MT. (Tội phạm MT chẳng hạn). Một điều nữa là một số vị thẩm phán, luật sư và nhiều nhà chức trách còn chưa hiểu về điện toán, vì thế họ không định hướng được các vấn đề điện toán quan hệ như thế nào với các phần khác đã được xác lập trong các bộ luật. Ví dụ: việc xác lập là tội phạm đối với hành vi tán phát trên mạng các văn hoá phẩm đồi truỵ hoặc các tài liệu phản động là dễ thấy, còn đối với hành vi tán phát các virut MT, các mã độc hại… thì khó thấy hơn.

Luật pháp ATTT tác động tới các nhà lập trình, các nhà sáng chế, các người dùng và các nhà quản trị của các HT máy tính và các ngân hàng DL. Các bộ luật này bảo vệ nhưng chúng còn điều chỉnh hành vi của những người sử dụng MT. Vì vậy chính các nhà máy tính chuyên nghiệp sẽ là các nhà làm luật có trình độ chuyên môn cao nhất trong việc đổi mới các luật cũ và thiết lập các luật mới cho MT. Vì thế nghiên cứu về luật pháp ATTT là công việc của chính các kỹ sư an toàn thông tin của chúng ta.

1.3 Bảo vệ chương trình và dữ liệu.

Bản quyền, sáng chế – phát minh và thương hiệu là các dạng bảo vệ pháp lý có thể áp dụng đối với các chương trình và đôi khi cả dữ liệu. Tuy nhiên chúng ta cần phải hiểu được sự khác nhau cơ bản giữa 3 dạng bảo vệ được đảm bảo và các phương pháp nhận được sự bảo vệ đó.

Giả sử Macta viết một chương trình MT để chơi một game video. Cô ta mời một vài bạn thân lại chơi và cho họ các bản copy sao cho họ có thể chơi ở nhà của họ. Steve lấy một bản copy về rồi tìm cách viết lại một phần chương trình của Macta nhằm hoàn thiện hơn chất lượng hiện hình (screen display). Sau đó Steve chia xẻ sự thay đổi này với Macta và cô ta đưa chúng vào chương trình của mình. Bây giờ, các bạn của Macta khuyên cô ta rằng chương trình game video đã rất tốt có thể đem bán, và cô ấy muốn quảng cáo và tiếp thị game video này để bán qua mạng. Macta muốn biết loại bảo vệ pháp lý nào cô ấy có thể áp dụng để bảo vệ phần mềm của mình.

Bản quyền, sáng chế – phát minh, và thương hiệu là các công cụ pháp lý có thể bảo vệ máy tính, chương trình và dữ liệu. Tuy nhiên, trong nhiều trường hợp, một số bước đi nhất định cần phải được thực hiện để bảo vệ chúng (CT và DL) trước khi một ai đó được cho phép tiếp cận tới chúng.

1.3.1 Luật sở hữu trí tuệ, bản quyền.

Ở các nước phát triển đi đầu trong lĩnh vực pháp luật ATTT (như Mỹ, Anh, Đức, Úc….), cơ sở của bảo vệ bản quyền và sở hữu trí tuệ được thể hiện ngay trong Hiến pháp (luật gốc). Ví dụ, ở Mỹ phần cơ bản của bảo đảm Hiến pháp về lĩnh vực này gồm các luật cụ thể hoá và mở rộng các quyền của Hiến pháp; như Luật bản quyền Mỹ năm 1978 (The U.S.Copyright Law of 1978), luật này lại đã được bổ sung vào năm 1998 thành Luật bản quyền thiên niên kỷ số hoá (Digital Millennium Copyright Act – DMCA) để áp dụng cho MT và các môi trường điện tử như băng, đĩa (hình và nhạc). Các thay đổi 1998 đã đưa Luật bản quyền Mỹ trở thành phù hợp chung với Tiêu chuẩn bản quyền quốc tế do Tổ chức sở hữu trí tuệ thế giới (World Intellectnal Property Organization – WIPO) đưa ra năm 1996 và đã được 95 nước công nhận.

1.3.1.1 Bản quyền (quyền tác giả - Copyrights).

Bản quyền được thiết kế để bảo vệ sự thể hiện cụ thể của các ý tưởng. Vì vậy nó được áp dụng cho một công trình sáng tạo như một truyện ngắn, một bức ảnh, một bài hát hoặc một bức đồ hoạ.

Vậy, quyền sao chép một sự thể hiện của một ý tưởng được bảo vệ bằng Bản quyền (Copyrights). Luật này cho rằng, bản thân các ý tưởng là hoàn toàn tự do, bất kỳ ai đó với trí óc sáng suốt cũng có thể nghĩ ra điều gì đó mà bất cứ ai khác cũng có thể ít nhất là về mặt lý thuyết. Ý tưởng về Bản quyền là để cho phép điều chỉnh sự trao đổi tự do các ý tưởng.

Tác giả của một cuốn sách chuyển các ý tưởng thành các từ ngữ trên mặt giấy. Trang sách đó là hiện thân sự thể hiện của các ý tưởng ấy và chính là cái kế sinh nhai của tác giả. Vì thế mà, một tác giả bao giờ cũng hy vọng có thể kiếm sống bằng cách thể hiện thật sinh động các ý tưởng sao cho những người khác thích mua để đọc chúng. (Sự bảo vệ tương tự được áp dụng với các tác phẩm âm nhạc, các vở kịch, phim, và các công trình nghệ thuật mà mỗi loại này là một sự thể hiện cá nhân của các tư tưởng).

Luật bản quyền bảo vệ quyền kiếm sống của các cá nhân đồng thời công nhận rằng chính sự trao đổi các ý tưởng giúp cho sự phát triển trí tuệ của cộng đồng. Luật bản quyền cho rằng con đường thể hiện một ý tưởng của mỗi tác giả là con đường riêng (mỗi tác giả thể hiện cũng một ý tưởng theo cách riêng của mình). Ví dụ, trong âm nhạc, với một sáng tạo nhà soạn nhạc có thể bản quyền một bài hát, nhà dàn dựng có thể bản quyền sự dàn dựng của bài hát nói trên, và ca sỹ có thể bản quyền sự biểu diễn riêng của mình trong sự dàn dựng bài hát đó. Và cái giá mà bạn mua tấm vé đến xem buổi biểu diễn đó là sự trả tiền cho cả ba sự thể hiện sáng tạo này.

Bản quyền cho một tác giả có quyền đặc biệt - đó là quyền sao chép sự thể hiện của anh ta và bán chúng (các bản sao chép đó) cho công chúng. Như vậy, chỉ duy nhất tác giả (hoặc những người bán sách, hay những người được tác giả uỷ quyền) mới có thể bán các bản copies của một cuốn sách của một tác giả.

1.3.1.2 Xác định sở hữu trí tuệ.

Luật bản quyền của Mỹ (Điều 102) nói rằng, một bản quyền có thể được đăng ký cho "các công trình nguyên thuỷ của nguồn tác giả (authorship) được ghi nhận trong môi trường thể hiện hữu hình bất kỳ… mà từ đó chúng có thể được thu phát, tái sản xuất, hoặc được lan truyền đi bằng các đường khác hoặc trực tiếp, hoặc nhờ máy móc hay thiết bị". Hơn nữa, bản quyền không bao gồm các ý tưởng còn đang được diễn giải. "Trong mọi trường hợp, bảo vệ bản quyền không bao giờ áp dụng cho các công trình nguyên thuỷ chỉ là sự mở rộng của một ý tưởng mà thôi". Bản quyền chỉ được áp dụng cho một tác phẩm nguyên thuỷ và nó phải ở trong một môi trường thể hiện hữu hình nào đó.

Chỉ có bản gốc thể hiện mới được đăng ký bản quyền; Nếu một thể hiện không có bản gốc xác định thì bản quyền không thể bảo đảm cho nó được. Một số tác phẩm được coi như của công, được sở hữu chung chứ không thuộc riêng ai. Như các tác phẩm của Chính phủ và các tổ chức khác thường được coi là của chung và vì vậy không có đối tượng để bản quyền. Các tác phẩm mà ai cũng biết, như các bản dân ca, nhạc cổ truyền hay như bài hát "Happy birthday to you" hoặc như các món "Mì ăn liền", Phở Hà Nội, Vodka Nga… nổi tiếng phổ biến đến mức mà sẽ rất khó cho ai đó chỉ ra tính nguyên thuỷ của chúng để bản quyền chúng.

Cần lưu ý rằng, bản quyền chỉ kéo dài một khoảng thời gian giới hạn cho nên các tác phẩm rất cổ ví như các vở kịch của Shakespeare chẳng hạn là thuộc về của công, khả năng bản quyền của chúng đã hết hiệu lực.

Sự thể hiện được đăng ký bản quyền phải tồn tại ở một môi trường hữu hình nhất định. Một truyện ngắn hoặc tác phẩm nghệ thuật phải được viết ra, in ra, vẽ ra, ghi lại (trên một môi trường vật lý như đĩa nhựa), được cất giữ trên môi trường từ (như băng đĩa), hoặc được ghi nhận bằng một số cách khác. Hơn nữa, mục đích của bản quyền là để phát triển sự phổ biến của tác phẩm: vì vậy tác phẩm phải được phân phối (bán), cho dù phải trả một phí nhất định cho một bản copy.

1.3.1.3 Tính nguyên gốc của tác phẩm (originality of work).

Tác phẩm muốn được bản quyền phải là công trình nguyên gốc của tác giả. Như đã nêu ở trên, một số thể hiện trong lĩnh vực công cộng không phải là đối tượng để bản quyền. Cũng có tác phẩm vẫn có thể được bản quyền cho dù nó có bao gồm ít nhiều tư liệu công cộng nhưng tính nguyên gốc nhất định vẫn bảo đảm. Tác giả của nó cũng không cần phải phân rõ đâu là công cộng và đâu là nguyên gốc.

Ví dụ, một nhà nghiên cứu lịch sử âm nhạc có thể bản quyền một bộ sưu tập các bài hát dân ca cho dù một số bài có thể là của chung. Thế nhưng để là đối tượng của bản quyền thì một số nội dung nào đó trong bộ sưu tập hoặc nói về bộ sưu tập đó nhất thiết phải là nguyên gốc. Nhà sử nhạc này có thể lập luận rằng, sự sưu tập các bài dân ca, sự chọn lựa xem đưa những bài nào vào bộ sưu tập và sự sắp xếp chúng theo một trật tự chính là phần nguyên gốc. Trong trường hợp này, Luật bản quyền sẽ không bảo vệ bản thân các bài hát dân ca (mà chúng thuộc sở hữu chung) nhưng nó lại bảo vệ sự sưu tập và tổ chức đặc biệt đó. Một ai đó đang bán một trang giấy trên đó có in một bài hát nằm trong bộ sưu tập nói trên sẽ được coi hầu như không vi phạm gì đến quyền tác giả của nhà sử nhạc đó. Các bộ từ điển cũng có thể bản quyền theo cách như vậy. Các tác giả không thể tuyên bố sở hữu các từ vựng, thuật ngữ, vì chính sự thể hiện của chúng mới tạo ra một bộ từ điển (cũng như ý tưởng được thể hiện thành tác phẩm bởi tác giả vậy, còn ý tưởng thì không thể bản quyền được).

1.3.1.4 Sử dụng hợp pháp các tác phẩm.

Luật bản quyền chỉ ra rằng, một đối tượng đã được bản quyền sẽ được dùng để trao đổi một cách hợp pháp. Người trả tiền (mua) có quyền sử dụng sản phẩm theo cách mà nó được định trước và theo cách sao cho không xâm phạm với các quyền của tác giả. Đặc biệt Luật này cho phép "sử dụng đúng một tác phẩm đã được bản quyền, bao gồm các hình thức sử dụng để tái bản, làm các bản sao copy cho các mục đích như phê bình, bình luận, tường thuật, tin tức, giảng dạy (gồm cả sao nhiều lần cho lớp học dùng), các cuộc thi hoặc để nghiên cứu". Mục đích và hiệu quả của việc sử dụng trên thị trường tiềm năng hay là giá trị của tác phẩm ảnh hưởng tới quyết định xem cái gì sẽ tạo nên sự sử dụng hợp pháp của nó. Ví dụ, sử dụng hợp pháp cho phép khi làm một copy một phần mềm đã bản quyền anh được thực hiện một cách công khai: Sự copy này bảo vệ anh khỏi các lỗi hệ thống nhưng nó không ảnh hưởng gì tới tác giả vì rằng anh không cần hoặc anh không muốn dùng cùng một lúc hai bản copy. Luật bản quyền thường đề cao quyền của các tác giả có thu nhập chính đáng nhờ tác phẩm của mình, và chính điều đó sẽ thúc đẩy mọi người cùng sử dụng các ý tưởng ẩn chứa trong tác phẩm. Sử dụng bất hợp pháp một sản phẩm đã bản quyền thì gọi là sự ăn cắp.

Sự ra đời của các máy photocopy làm khó khăn cho việc buộc thực thi các sử dụng hợp pháp. Anh có thể nói rằng việc làm một bản copy của một chương cần thiết nhất từ một cuốn sách chỉ dẫn du lịch để mang theo mình và có thể vứt đi vào cuối ngày nghỉ là một sử dụng hợp pháp vì thế tôi không cần phải mang theo mình cả một cuốn sách to dày. Ngày nay nhiều cửa hàng photocopy sẵn sàng làm copy một phần, đôi khi cả một chương từ cuốn sách hoặc cả bài báo từ một tạp chí nhưng từ chối copy toàn bộ một tập sách. Với các máy photocopy, chất lượng của một bản sao giảm sút rõ rệt sau từng lần copy, bạn sẽ thấy điều đó nếu bạn thử cố gắng đọc bản sao của bản sao của bản sao của một trang sách nào đó.

Luật bản quyền cũng đưa ra quan niệm bán lần đầu: sau khi đã mua một đối tượng có bản quyền, chủ sở hữu mới có thể đem cho hoặc bán lại đối tượng đó. Nghĩa là chủ sở hữu bản quyền (tác giả) hoàn toàn kiểm soát được sự mua bán lần đầu của đối tượng. Quan niệm này rất tốt đối với các sách: Tác giả sẽ được trả tiền khi một cửa hàng sách bán được một cuốn của anh ta, thế nhưng tác giả đó không được trả thêm gì nữa nếu sau đó cuốn sách này được bán lần nữa tại một cửa hàng sách cũ.

1.3.1.5 Các yêu cầu để đăng ký bản quyền.

Bản quyền có thể nhận được dễ dàng và các lỗi trong bảo vệ bản quyền có thể được chỉnh sửa. Bước đầu tiên để đăng ký là dấu hiệu lưu ý. Bất kỳ người dùng tiềm năng nào cũng phải được biết trước rằng, tác phẩm này đã được bản quyền. Mỗi bản copy phải được đánh dấu bằng ký hiệu bản quyền ©, từ Copyright, năm, và tên tác giả. (Ở một số nước, sau cụm từ này còn thêm cụm từ All rights reserved. Việc thêm câu này hiện nay không nhất thiết nhưng nên làm).

Thứ tự của các yếu tố cũng có thể được thay đổi và có thể thiếu hoặc © hay Copyright (nhưng không phải cả hai). Mỗi bản copy đều phải được đánh dấu như vậy, tuy nhiên Luật cũng tha thứ cho các sai sót trong đánh dấu các bản copy nếu như có lời giải trình phù hợp.

Bản quyền cũng phải trình bầy trên tờ đơn xin đăng ký. Ở Mỹ thì một đơn theo mẫu phải điền đầy đủ và phải gửi tới cơ quan bản quyền (Copyright Office) kèm theo khoản lệ phí (đã được ấn định) và một bản copy của tác phẩm. Trên thực tế CO chỉ đòi hỏi 25 trang đầu và 25 trang cuối của tác phẩm để chứng minh sự thật khi toà án yêu cầu. Đơn phải hoàn tất trong vòng 3 tháng sau khi tác phẩm được công bố lần đầu. Luật cho phép gửi đơn đăng ký muộn hơn tới 5 năm, nhưng phải không có tranh chấp gì trước thời điểm nộp đơn đăng ký.

Bản quyền ở Mỹ hiện nay kéo dài tới 70 năm sau khi tác giả sống lâu cuối cùng qua đời, hoặc nếu tác phẩm được bản quyền bởi công ty hay tổ chức thì kéo dài tới 95 năm sau ngày công bố. Chuẩn quốc tế là 50 năm sau khi tác giả cuối cùng chết hoặc 50 năm từ khi công bố. Ở Việt Nam theo Luật sở hữu trí tuệ là 50 năm như chuẩn quốc tế (Luật SHTT, 2005, Điều 27, Mục 1, Chương II).

1.3.1.6 Các vi phạm bản quyền.

Người giữ bản quyền phải tới toà để chứng minh rằng ai đó đã vi phạm bản quyền của anh ta. Sự vi phạm phải rất đáng kể và đó thường phải là bản sao chứ không phải là một tác phẩm độc lập. Về mặt lý thuyết hai người có thể viết ra cùng một bài hát một cách độc lập với nhau, không ai trong họ biết nhau. Cả hai người này đều hoàn toàn có thể bản quyền bảo vệ tác phẩm của họ. Không ai vi phạm tới người kia, và cả hai đều có quyền phân phối tác phẩm của họ để kiếm tiền. Ngược lại, bản quyền dễ dàng nhận ra đối với các tác phẩm viết với những điều tưởng tượng, vì rằng rất hiếm có hai người diễn tả cùng một ý tưởng bằng cùng một lời văn giống hệt nhau hay là gần giống nhau.

Sự độc lập của các tác phẩm không dùng trí tưởng tượng không hoàn toàn rõ như vậy. Chúng ta hãy xét ví dụ, một cuốn sách về số học. Phép chia còn dư có thể được giảng giải chỉ bằng một vài cách, vì thế hai cuốn sách độc lập có thể dùng lời lẽ giống nhau để giải thích nó. Số ví dụ khác nhau có thể cũng giới hạn, nên hai tác giả độc lập cũng có thể cùng chọn một ví dụ minh hoạ như nhau. Tuy nhiên, rất khó xảy ra rằng, cả hai tác giả sẽ có cùng một cách diễn đạt và có cùng các ví dụ suốt từ đầu đến cuối sách.

1.3.1.7 Bản quyền đối với các phần mềm máy tính.

Luật bản quyền đầu tiên được hình thành để bảo vệ các thứ như cuốn sách, các bài hát và các bức ảnh. Người ta dễ dàng ghi nhận khi các đối tượng này bị copy. Sự phân tách giữa miền công cộng và sáng tạo là rất rõ ràng. Và sự khác biệt giữa ý tưởng (cảm xúc, phong cách) và sự thể hiện chúng là rất dễ thấy. Những tác phẩm không dùng trí tưởng tượng khó khăn hơn trong nhận biết sự thể

hiện độc lập của chúng. Các chương trình máy tính cũng vậy, khó khăn rất nhiều trong sự phân định tính độc lập của chúng, vì ngôn ngữ lập trình rất cứng nhắc (không linh hoạt như ngôn ngữ bình thường) và tác động của nó rất nhanh và rộng.

Vậy một chương trình máy tính có thể bản quyền được không? Có thể. Luật bản quyền năm 1976 đã được mở rộng vào năm 1980 bao gồm cả xác định cho phần mềm MT. Tuy nhiên, bảo vệ bản quyền đối với tác phẩm MT có thể có hình thức không như mong đợi. Để thấy vì sao, ta hãy xét xem giải thuật (algorithm) được dùng để viết một chương trình. Giải thuật là một ý tưởng và các lệnh của ngôn ngữ lập trình là sự thể hiện của ý tưởng đó. Như vậy, bảo vệ ở đây là bảo vệ cho chính các lệnh của chương trình, chứ không phải cho khái niệm giải thuật: sao chép chính xác mã chương trình sẽ bị cấm, nhưng áp dụng lại thuật toán được cho phép. Hãy nhớ rằng một mục đích của bản quyền là phát triển sự trao đổi các ý tưởng. Chính thuật toán, là ý tưởng hiện thân trong một chương trình máy tính, phải được chia xẻ với cộng đồng.

Vấn đề thứ hai trong bảo vệ bản quyền của các tác phẩm máy tính là đòi hỏi rằng, tác phẩm phải được công bố. Một chương trình có thể được công bố bằng cách phân phối (bán) các bản copy mã đối tượng của nó, ví dụ, trên đĩa. Tuy nhiên, nếu mã nguồn không được phân phối, thì chương trình vẫn chưa được công bố. Một người cho là vi phạm không thể xâm phạm bản quyền trên mã nguồn nếu bản thân mã nguồn này chưa bao giờ được công bố.

1.3.1.8 Bản quyền các đối tượng số.

Luật bản quyền thiên niên kỷ số (DMCA) năm 1998 đã đưa ra một số luận điểm về các đối tượng số (như các file nhạc, các đồ hoạ, dữ liệu trong CSDL, và cả các chương trình máy tính), nhưng nó còn chưa tính tới nhiều loại khác.

Trong các quy định của DMCA có các nội dung sau:

- Các đối tượng số có thể là đối tượng để bản quyền.
- Sẽ là phạm tội nếu bỏ qua hoặc xoá đi chức năng chống ăn cắp được gắn vào đối tượng.
- Sẽ là phạm tội nếu sản xuất, bán hoặc là phân phát các thiết bị có khả năng xoá chức năng chống ăn cắp hoặc copy các đối tượng số.
- Tuy nhiên, các thiết bị này có thể được sử dụng (và sản xuất, bán hoặc phân phối) với mục đích nghiên cứu và đào tạo.
- Đã thành thông lệ chấp nhận cho làm bản sao lưu dự phòng của một đối tượng số như là sự bảo vệ chống các lỗi phần cứng và phần mềm hoặc cho cất giữ các bản sao copy và lưu trữ.

- Các thư viện có thể được làm tới 3 bản copy của một đối tượng số để cho các thư viện khác mượn.

Như vậy, người dùng có thể làm một số bản copy hợp lý của một đối tượng khi sử dụng đối tượng đó và như là sự bảo vệ chống các lỗi hệ thống. Nếu một hệ thống sao lưu dự phòng thường kỳ thì một đối tượng số (như là một chương trình phần mềm) sẽ được copy nhiều lần để lưu trữ và điều đó không vi phạm bản quyền.

Sự không rõ ràng xảy ra khi quyết định xem cái gì được coi là thiết bị để ghi nhận sự ăn cắp. Bộ phân tách hay là bộ giải thông dịch (dissasembler or decompiler) sẽ hỗ trợ ăn cắp hay sẽ được dùng để nghiên cứu và nâng cấp một chương trình. Một ai đó giải thông dịch (decompiles) một chương trình chạy được, nghiên cứu nó để tìm ra phương pháp của nó, và sau đó biến đổi nó, lại thông dịch và đem bán các kết quả thu được (chương trình chạy). Vậy người này đã sử dụng không đúng bộ giải thông dịch. Nhưng sự khác biệt rất khó mà làm rõ, một phần là vì cách dùng phụ thuộc vào nội dung và ngữ cảnh (context). Ở đây nó cũng giống như nếu có một luật nói rằng: việc bán cái kéo để cắt rau cỏ là hợp pháp nhưng không được để cái kéo đâm bị thương con người. Các chiếc kéo không biết người ta dùng chúng như thế nào. Người dùng quyết định nội dung và hoàn cảnh.

Chúng ta hãy xem xét một đĩa CD mà bạn mua về với lý do rõ ràng: để nghe nhiều lần. Bạn muốn nghe nhạc trên máy MP3 của mình, đó là sự dùng hợp pháp. Nhưng đĩa CD này được bảo vệ chống copy nên bạn không thể tải bản nhạc đó vào máy tính của mình để sau đó truyền sang máy MP3 được. Vậy bạn đã bị cấm (trong trường hợp này) thực hiện một sử dụng hợp pháp (nghe nhạc trên MP3). Nếu bạn cố gắng làm cái gì đó để xoá đi bảo vệ chống ăn cắp thì bạn đã vi phạm quy định chống ăn cắp, bạn cũng không thể mua một công cụ hoặc một chương trình khả dĩ cho phép bạn tải bản nhạc của mình (vì bạn đã mua CD) xuống máy MP3 (cũng) của mình vì rằng các công cụ ấy sẽ vi phạm quy định nói trên.

Phản ứng trước DMCA rất khác nhau. Có người cho rằng nó giới hạn các nghiên cứu an toàn MT. Có nhiều người chỉ ra rằng, DMCA có thể được dùng để ngăn cản chính sự trao đổi tự do các ý tưởng, điều mà Bản quyền có mục đích là phát triển không ngừng.

Các đối tượng số khác xa các tờ giấy chúng có thể được copy một cách chính xác. Mỗi bản copy số của một đối tượng số hoàn toàn giống như nguyên gốc.

Bản quyền bảo vệ quyền của nhà sáng tạo thu lợi từ mỗi bản copy của đối tượng, thậm chí nếu không có tiền trao tay.

Một nguyên tắc quan trọng là: phần mềm, như âm nhạc được nhận thức là một đối tượng cho vay hơn là đem bán. Bạn trả tiền mua không phải là bản thân

phần mềm, mà là quyền sử dụng phần mềm đó. Để làm rõ điều này, Luật cấm ăn cắp điện tử của Mỹ (The U.S. No Electronic Theft (NET) Act) năm 1997 coi là tội phạm việc tái sản xuất hoặc phân phối các tác phẩm bản quyền như phần mềm hoặc các bản ghi số (digital recordings), thậm chí không lấy tiền.

Lĩnh vực bảo vệ bản quyền áp dụng cho các tác phẩm máy tính còn đang tiếp tục phát triển và đang là chủ đề tranh cãi rất nhiều trên các phiên toà. Chẳng hạn, còn chưa xác định rõ những khía cạnh nào của một tác phẩm máy trính là đối tượng để bản quyền. Toà đã phải coi như là một quy tắc (rule) rằng, một thiết kế menu của máy tính có thể bản quyền nhưng những thứ "chỉ nhìn thấy và cảm nhận" (như giao diện người dùng Microsoft Windows) thì không thể. Phải chăng thiết kế menu không phải là một phần của cái "nhìn thấy và cảm nhận"?

1.3.2 Luật sở hữu trí tuệ, sáng chế.

1.3.2.1. Sáng chế.

Các sáng chế không giống như bản quyền trong nghĩa rằng sáng chế bảo vệ các phát minh, các đối tượng hữu hình hoặc cách thức làm ra chúng, chứ không phải là các tác phẩm của trí tuệ. Sự khác biệt giữa sáng chế và bản quyền là ở chỗ, sáng chế được nghĩ ra để áp dụng đối với các thành quả khoa học, công nghệ và chế tạo, trong khi bản quyền áp dụng cho các tác phẩm trong nghệ thuật, văn học và các loại được viết ra. Một sáng chế có thể bảo vệ "một quá trình mới và có lợi, máy móc, sản xuất, hoặc sự tổ hợp của các vật" Luật của Mỹ loại trừ "các định luật tự nhiên mới tìm ra… [và] các quá trình thuần tuý trí óc". Ví dụ "2 x 2 =4" không là một đối tượng phù hợp để sáng chế vì nó là một định luật tự nhiên. Tương tự, sự thể hiện thuộc về công cộng không phù hợp để bản quyền. Bạn có thể viện dẫn rằng, toán học là thuần tuý trí tuệ, là các ý tưởng. Sáng chế được nghĩ ra để bảo vệ cho một thiết bị hoặc một quá trình thể hiện ra một ý tưởng chứ không phải tự thân ý tưởng đó.

1.3.2.2. Đòi hỏi về tính mới (Requirments of Novelty).

Nếu như hai nhạc sỹ ngẫu nhiên sáng tác cùng một bài hát vào thời gian khác nhau, luật bản quyền có thể cho phép cả hai đều có bản quyền. Nếu hai nhà chế tạo đưa ra cùng một phát minh, thì sáng chế sẽ đến với người phát minh nó đầu tiên, không phụ thuộc vào ai là người đưa đơn đăng ký trước. Một sáng chế chỉ có thể được chấp nhận cho một thứ gì đó thực sự là mới và độc đáo, vì vậy chỉ có một sáng chế cho một phát minh mà thôi.

Đối tượng sáng chế cũng phải là không hiển nhiên. Nếu một phát minh mà là rất hiển nhiên đối với người có chuyên môn bình thường trong lĩnh vực, thì nó không thể được sáng chế. Luật tuyên bố rằng, sáng chế sẽ không nhận được "nếu sự khác nhau giữa đối tượng yêu cầu sáng chế và một kỹ năng trước đó còn ở mức mà đối tượng này như là một vật trọn vẹn tỏ ra hiển nhiên, vào thời điểm

phát minh được thực hiện, đối với một người có trình độ bình thường thuộc kỹ năng mà đối tượng đó liên quan". Ví dụ, một bìa nhỏ để dùng làm cái đánh dấu trang sách đọc, khó có thể xin sáng chế, vì ý tưởng về miếng bìa như vậy là rất hiển nhiên đối với hầu hết người đọc.

1.3.2.3. Thủ tục đăng ký sáng chế.

Người ta đăng ký bản quyền bằng việc điền kín một đơn mẫu ngắn, đánh dấu hiệu bản quyền trên tác phẩm sáng tạo và phân phối tác phẩm đó. Cả quy trình này chỉ cần chưa đầy một giờ.

Để nhận được một sáng chế, nhà phát minh cần phải thuyết phục Cơ quan sáng chế và thương hiệu Hoa Kỳ (U.S.Patent anh Trademark Office – U.S.PTO) rằng phát minh của anh ta xứng đáng là một sáng chế. Với khoản phí nhất định, một luật sư về sáng chế sẽ nghiên cứu các sáng chế đã được công nhận cho các phát minh tương tự. Sự khảo sát này sẽ kết luận hai điều. Thứ nhất, nó xác định rằng phát minh sẽ được đăng ký chưa từng được công nhận trước đó. Thứ hai, nó giúp cho nhận dạng được các thứ tương tự mà đã được sáng chế. Những sự tương tự này rất hữu ích khi miêu tả những nét độc đáo của phát minh và làm cho nó xứng đáng với bảo vệ sáng chế. Cơ quan sáng chế sẽ so sánh tất cả các phát minh tương tự đã được sáng chế và sẽ quyết định xem có cái gì thực sự mới và không hiển nhiên trong phát minh không. Nếu PTO quyết định rằng phát minh này là mới thì sáng chế coi như được đảm bảo.

Thông thường, nhà phát minh viết một đơn xin cấp sáng chế trong đó liệt kê nhiều minh chứng về tính nguyên gốc từ các đặc tính rất chung đến rất đặc thù. PO có thể chấp nhận một số đặc trưng chung hơn cả trong khi lại ủng hộ những tính chất đặc thù. Người làm đơn sáng chế phải làm rõ những cái mới trong phát minh ở dạng đủ chi tiết cho phép P.O. và toà án kết luận về tính mới; mức độ chi tiết đó cũng có thể nói với cộng đồng phát minh này làm việc như thế nào, đồng thời mở ra khả năng tranh chấp của nó.

Người sở hữu sáng chế sử dụng phát minh đã được đăng ký bằng cách sản xuất các sản phẩm hoặc cấp phép (license) cho người khác sản xuất chúng. Các đối tượng được sáng chế đôi khi được đánh dấu bởi số hiệu sáng chế nhằm cảnh báo những người khác rằng công nghệ này đã được đăng ký sáng chế. Người nắm giữ sáng chế hy vọng rằng, sự cảnh báo này sẽ ngăn chặn được sự vi phạm của những người khác.

1.3.2.4. Sự vi phạm sáng chế.

Người sở hữu sáng chế phải chống lại mọi sự vi phạm. Với bản quyền, người giữ bản quyền có thể lựa chọn các trường hợp để khởi kiện, bỏ qua các vi phạm nhỏ và chờ đợi vi phạm đủ lớn để chắc thắng trước toà. Trái lại, khi đã thua kiện một vi phạm sáng chế dù là rất nhỏ hoặc sự vi phạm mà người giữ quyền sáng chế không hề biết thì điều đó có nghĩa là anh ta mất toàn bộ quyền sáng chế đó.

Không giống như vi phạm bản quyền, chủ sở hữu sáng chế không thể chứng minh được rằng, kẻ vi phạm đó đã sao chép phát minh của anh ta; sự vi phạm sáng chế xảy ra thậm chí cả khi nếu ai đó phát minh một cách độc lập cùng một thứ như vậy mà không hề biết gì về phát minh đã đăng ký sáng chế.

Mỗi vi phạm đều phải bị khởi tố. Kiện cáo là tốn kém, mất thời gian, thậm chí tệ hơn nữa là theo kiện một vi phạm sáng chế chủ sáng chế có thể mất quyền sáng chế đó. Người bị buộc tội vi phạm có thể viện dẫn tất cả các luận cứ sau đây như một sự bào chữa (tự vệ):

- Đây không phải là vi phạm. Người bị cho là vi phạm này sẽ tuyên bố rằng, hai phát minh này là hoàn toàn khác xa nhau, rằng đã không xảy ra một vi phạm nào cả.
- Sáng chế không còn hiệu lực. Nếu một vi phạm trước đó không được chống lại, thì các quyền sáng chế có thể hết hiệu lực.
- Phát minh không mới. Trong trường hợp này, kẻ vi phạm giả định sẽ cố gắng thuyết phục toà rằng, P.O. đã hành động không chuẩn khi bảo đảm sáng chế và rằng phát minh này không xứng đáng là một sáng chế.
- Người vi phạm đã phát minh ra đối tượng đầu tiên. Nếu như vậy thì, người bị cho là vi phạm chứ không phải là chủ sỡ hữu sáng chế gốc sẽ có toàn quyền đối với sáng chế.

Bảo vệ đầu tiên không làm hại gì sáng chế, mặc dù nó có thể ảnh hưởng tới tính mới của phát minh. Tuy nhiên ba bảo vệ còn lại có thể làm mất quyền sáng chế. Cả bốn bảo vệ này đều có thể được sử dụng vào bất kỳ lúc nào khi một sáng chế kiện một ai đó đã vi phạm. Cuối cùng, sự nhận được và sự bảo vệ một sáng chế đều đòi hỏi chi một khoản lệ phí hợp pháp đáng kể. Bảo vệ sáng chế là phù hợp nhất đối với các công ty lớn với đội ngũ cán bộ nghiên cứu và phát triển có số lượng đáng kể.

1.3.2.5. Khả năng áp dụng sáng chế đối với các đối tượng máy tính.

P.O. đã không khuyến khích các sáng chế phần mềm máy tính. Trong một thời gian dài, các chương trình máy tính đã được coi như sự thể hiện của một thuật toán (algorithm) và thuật toán là tự nhiên không phải là chủ thể sáng chế. Trường hợp sáng chế phần mềm đầu tiên, Gottschalk v. Benson yêu cầu sáng chế quá trình biến các số thập phân thành nhị phân. Toà thượng thẩm đã từ chối yêu cầu, giải thích rằng đó dường như là đòi hỏi sáng chế cho một ý tưởng trừu tượng, tóm lại, là thuật toán. Mà thuật toán chính là thứ mà hầu hết các nhà phát triển phần mềm đều muốn bảo vệ.

Vào năm 1981, hai trường hợp (Diamond v. Bradley và Diamond v. Diehr) đã dành được sáng chế về quá trình mà phần mềm máy tính sử dụng, một thuật toán nổi tiếng – các cảm biến nhiệt độ và bộ đếm để tính thời gian cho việc lưu hoá các con có biển bằng cao su (một thứ đồ chơi). Toà án đã ủng hộ quyền sáng

chế này vì yêu cầu không phải cho phần mềm hoặc thuật toán đi kèm, mà là cho quá trình sử dụng phần mềm đó như là một trong các khâu của nó. Điều suy ra may mắn ở đây là, sử dụng phần mềm mà không dùng các khâu khác đã được sáng chế của quá trình trên sẽ không bị coi là vi phạm.

Từ 1981, luật sáng chế đã được mở rộng bao gồm cả phần mềm máy tính, và công nhận rằng các thuật toán, cũng như là các quá trình và các công thức đều là các phát minh. Sau các trường hợp nói trên, P.O. đã cấp sáng chế cho hàng nghìn phần mềm. Nhưng, vì lý do thời gian kéo dài và tốn kém để làm thủ tục và có được một sáng chế, dạng bảo vệ này có thể ít được chấp nhận đối với những người viết phần mềm ở dạng đơn lẻ.

Luật sở hữu trí tuệ năm 2005 của Việt Nam, Điều 59 ghi rõ; chương trình máy tính là đối tượng không được bảo hộ với danh nghĩa sáng chế.

1.3.3 Luật về bí mật thương mại.

Bí mật thương mại (BMTM) không giống như sáng chế hay bản quyền trong ý nghĩa rằng, nó phải chứa một bí mật. Thông tin này chỉ có giá trị như một bí mật, và một kẻ vi phạm là người làm tiết lộ bí mật đó. Một khi đã bị tiết lộ, thông tin đó thường không thể được coi là bí mật lại một lần nữa.

1.3.3.1 Các đặc trưng của Bí mật thương mại (BMTM).

Bí mật thương mại là thông tin quan trọng giúp cho một công ty lợi thế cạnh tranh trước các đối thủ khác. Ví dụ, công thức pha chế một loại nước giải khát là một bí mật thương mại, cũng như vậy một liệt kê các khách hàng qua bưu điện hay thông tin về một sản phẩm đều được công bố trong vài tháng.

Đặc trưng khác biệt của một bí mật thương mại là nó phải luôn luôn chứa đựng sự bí mật. Những người thuê khoán và những người ngoài, ai đã tiếp cận tới bí mật phải được đòi hỏi không được tiết lộ bí mật đó. Chủ sở hữu BMTM phải thực hiện các biện pháp đề phòng để bảo vệ bí mật đó, chẳng hạn như cất giấu nơi an toàn, mã hoá nó trong file máy tính hoặc yêu cầu các người thuê khoán ký vào cam kết rằng họ sẽ không tiết lộ ra.

Nếu ai đó thu được một BMTM một cách bất hợp pháp và thu lợi từ đó, chủ sở hữu của nó có thể đòi lại lợi nhuận đó, các thiệt hại và mất mát phải bồi hoàn và các giá trị pháp lý. Toà án sẽ làm tất cả những gì có thể để đưa chủ sở hữu đó về vị trí cạnh tranh như khi mà thông tin vẫn còn là bí mật, và các thiệt hại đã xảy ra có thể được bồi thường do mất giá. Tuy nhiên bảo vệ BMTM không có giá trị trong trường hợp một phát minh độc lập. Nếu ai đó khác ngẫu nhiên phát minh ra BMTM đó một cách độc lập, thì không có vi phạm nào xảy ra và các quyền BMTM vẫn tiếp tục hiệu lực.

1.3.3.2 Sự phát minh ngược.

Bảo vệ BMTM có thể bị mất hiệu lực vì một cách khác là bởi một phát minh ngược với nó. Giả sử rằng, BMTM là cách đóng các mảnh giấy lụa màu vào một cái thùng bìa để làm nó phát ra tiếng nổ và lại phun các mẩu giấy màu đó lên trời (pháo hoa bằng giấy). Bất kỳ ai cũng có thể cắt tung cái thùng đó ra để nghiên cứu quá trình kỹ thuật này. Vì vậy BMTM này dễ dàng bị khám phá. Đây là một phát minh ngược và nó làm mất hiệu lực BMTM nói trên. Trong phát minh ngược, người ta nghiên cứu đối tượng đã hoàn chỉnh thành sản phẩm để xác định xem nó được sản xuất như thế nào hoặc nó làm việc như thế nào.

Bằng cách phát minh ngược, một ai đó có thể khám phá ra điện thoại đã được xây dựng như thế nào; thiết kế của một điện thoại là nhìn rõ từ các thành phần và sự kết nối của chúng với nhau. Tuy nhiên, sáng chế là cách bảo vệ phù hợp hơn cả đối với phát minh kiểu như điện thoại. Một số thứ như nước giải khát không phải là tổ hợp rõ ràng của các thành phần như điện thoại. Chế tạo nước uống này cần thời gian, nhiệt độ, sự có mặt của oxy hay các khí khác, và các nhân tố tương tự mà không thể nhận biết được qua sự phân tích hoá học trực tiếp sản phẩm này. Công thức nước giải khát là BMTM được bảo đảm rất nghiêm. Bảo vệ BMTM rất hiệu quả khi mà bản thân bí mật không xuất hiện rõ trên sản phẩm.

1.3.3.3 Áp dụng cho các đối tượng máy tính.

Bảo vệ BMTM áp dụng rất tốt cho phần mềm MT. Thuật toán của một chương trình máy tính là mới, nhưng tính mới của nó phụ thuộc vào việc có ai khác biết nó không. Bảo vệ BMTM cho phép phân phối (bán) kết quả của bí mật (chương trinh thực hiện – executable program), trong khi vẫn giữ kín thiết kế chương trình. Bảo vệ BMTM không bảo hộ sự sao chép sản phẩm (đặc biệt là chương trình máy tính), do vậy nó không thể bảo vệ chống kẻ cắp đem bán bản sao của chương trình của một ai đó mà không có phép của họ. Tuy nhiên, bảo vệ BMTM làm cho bất hợp pháp việc ăn trộm một thuật toán bí mật và dùng nó trong một sản phẩm khác. Khó khăn đối với các chương trình máy tính là ở chỗ các phát minh ngược hay xảy ra. Các chương trình giải thông dịch và phân tách có thể sản xuất được một phiên bản nguồn của chương trình thực hiện. Tất nhiên nguồn này không chứa các tên biến miêu tả hoặc các diễn giải mã, nhưng nó là phiên bản chính xác mà ai đó có thể nghiên cứu, dùng lại hoặc nâng cấp.

1.3.3.4 Khó khăn buộc thực thi.

Bảo vệ BMTM là vô phương cứu vãn khi mà có ai đó suy đoán ra được thiết kế của chương trình bằng cách nghiên cứu đầu ra của nó, hoặc tệ hơn nữa, giải được mã đối tượng của nó. Cả hai cách này đều chính đáng (nghĩa là hợp pháp) và cả hai đều làm cho bảo vệ BMTM vô tác dụng.

Tính bảo mật của BMTM phải được chắc chắn đảm bảo bằng các biện pháp phù hợp. Nếu mã nguồn được kiểm soát lỏng lẻo hoặc nếu chủ sở hữu quên không nhắc nhở những người khác (ví dụ như các người làm thuê) về tính quan trọng giữ gìn bí mật, thì mọi sự khởi kiện về vi phạm phải được sẵn sàng. Các hợp đồng thuê khoán thường có cam kết trực tiếp rằng, người làm thuê không được làm tiết lộ bất kỳ BMTM nào biết được từ công ty, thậm chí cả sau khi đã rời khỏi công việc tại đây. Công việc bảo vệ thêm, ví như việc in sao các tài liệu nhạy cảm hoặc giám sát các tiếp cận (truy cập) tới các file máy tính chứa các thông tin bí mật, đều cần thiết kế để cảnh báo mọi người về tầm quan trọng của công tác bảo mật (secrecy).

1.3.4 Luật về bảo vệ các đối tượng máy tính.

Trong các mục trước chúng ta đã mô tả ba dạng bảo vệ: bản quyền, sáng chế và BMTM. Mỗi dạng cung cấp một loại bảo vệ khác nhau đối với các thông tin nhạy cảm. Trong mục này, chúng ta sẽ xem xét các kiểu khác nhau của các đối tượng máy tính và mô tả các dạng bảo vệ phù hợp với mỗi kiểu. Bảng sau đây cho thấy sự so sánh ba dạng bảo vệ nói trên về một số nét cơ bản.

Bảng 1: So sáng các bảo vệ Bản quyền, Sáng chế, và Bí mật thương mại.

	Bản quyền	Sáng chế	Bí mật TM
Bảo vệ đối tượng	Sự thể hiện của ý tưởng. Không phải bản thân ý tưởng.	Phát minh: cách làm việc của một thứ gì đó.	Bí mật của một thành tựu có tính cạnh tranh.
Đối tượng bảo vệ được công bố	Có. Xu hướng muốn phát triển sự công bố.	Thiết kế được giữ ở P.O.	Không
Yêu cầu được phân phối (mua bán)	Có	Không	Không
Độ dễ làm tài liệu	Rất dễ dàng, tự làm lấy.	Rất phức tạp: có luật sư riêng trợ giúp.	Không làm văn bản.
Thời gian hiệu lực	Cuộc đời của tác giả gốc cộng 70 năm hoặc 95 năm tất cả cho công	19 năm	Không xác định.

	ty.		
Bảo vệ hợp pháp	Khởi kiện khi bản sao không uỷ quyền (ăn cắp) được đem bán.	Khởi kiện nếu phát minh bị sao chép (copy).	Khởi kiện nếu bí mật bị tiết lộ bất hợp pháp.

Các đối tượng máy tính là mới mẻ và thường xuyên biến đổi, và sẽ còn lâu chúng mới hoàn toàn phù hợp được với hệ thống pháp luật đã hình thành từ các thể kỷ trước. Có lẽ phải mất ít chục năm nữa người ta mới chỉ ra rõ ràng được với loại đối tượng nào thì loại bảo vệ nào là phù hợp với chúng. Cũng có thể là một dạng bảo vệ mới hoặc sự đổi mới của dạng bảo vệ cũ nào đó sẽ được áp dụng riêng cho các đối tượng máy tính. Ví dụ, EU (cộng động Châu Âu) hầu như đã ban hành mô hình pháp lý cho bảo vệ bản quyền đối với phần mềm máy tính. Tuy nhiên, một trong các mục đích của nó là phát triển các phần mềm mà được xây dựng trên cơ sở những thứ người khác đã làm. Chẳng hạn, EU đặc biệt miễn trừ đặc tả giao diện của sản phẩm khỏi bản quyền và đã cho phép những người khác dùng giao diện đó để phát triển các sản phẩm mới mà có thể kết nối qua giao diện này.

Khi còn chưa có luật cung cấp sự bảo vệ hoàn toàn phù hợp cho các sản phẩm máy tính, chúng tôi đưa ra một vài chỉ dẫn cho việc sử dụng luật pháp để bảo vệ các đối tượng máy tính như sau:

1.3.4.1 Bảo vệ phần cứng.

Phần cứng máy tính như các con chips, đĩa cứng, hoặc môi trường đĩa mềm có thể đăng ký sáng chế. Bản thân môi trường có thể sáng chế, và ai đó phát minh ra một quy trình sản xuất đĩa mới, người đó có thể nhận một sáng chế thứ hai.

1.3.4.2 Bảo vệ phần sụn (Firmware).

Tình thế hơi kém rõ ràng đối với vi mã (microcode). Vi mã hay còn gọi là vi lệnh (microintructions) – là một loại lệnh mã máy điều khiển trực tiếp hoạt động của máy tính. Đó là lệnh cài sẵn bên trong (các vi xử lý), không phụ thuộc vào các chương trình đưa vào máy tính từ bên ngoài. Rõ ràng là các thiết bị vật lý trên đó vi mã được lưu giữ (các chipset chẳng hạn) có thể sáng chế. Một chip đặc dụng (special – purpose) chỉ để làm một nhiệm vụ riêng (ví dụ như bộ phận chia số dấu phẩy động) cũng có thể sáng chế được. Tuy nhiên, các dữ liệu (các lệnh, thuật toán, vi mã, các chương trình) lưu chứa trong các thiết bị (vật lý) lại không sáng chế được.

Vậy chúng có thể bản quyền được không? Chúng có thể là sự thể hiện của một ý tưởng ở dạng thúc đẩy sự trao đổi ý tưởng đó không? Có lẽ là không. Và ta giả sử rằng, các thiết bị này đã được bản quyền. Khi đó việc xác định một bản sao (copy) vi phạm bản quyền này sẽ như thế nào? Hơn nữa liệu người sản xuất

có thực sự mong muốn đăng ký một bản sao của thuật toán bên trong với cơ quan bản quyền không? Bảo vệ bản quyền rõ ràng là không thích hợp đối với phần sụn của máy tính.

Bảo vệ BMTM dường như là phù hợp đối với bộ mã đã hoá thân vào một chip nào đó của máy tính. Trong khoảng thời gian phù hợp, chúng ta có thể thiết kế ngược trở lại và suy ra được bộ mã đó từ hoạt động của con chip mà nó đã hoá thân vào. Hành trạng của con chip lại không cho thấy thuật toán nào đã được dùng để sinh ra hành trạng đó. Thuật toán gốc có thể có sự thể hiện tốt hơn (hoặc kém hơn) và tốc độ, kích thước, tính chịu lỗi (fault tolerance), mà sẽ không thấy được từ thiết kế ngược.

Ví dụ, Apple Computer – máy tính quả táo kiên định yêu cầu bảo vệ bản quyền cho hệ điều hành được cài cứng vào phần sụn của nó. Toà án đã quả quyết rằng, phần mềm máy tính là đối tượng thích hợp cho bảo vệ bản quyền và rằng loại bảo vệ đó không còn hiệu lực nữa khi phần mềm đó định vị một chip nào đó chứ không ở trong một chương trình thông thường.

1.3.4.3 Bảo vệ mã đối tượng của phần mềm.

Mã đối tượng thông thường được viết sao cho nó có thể được phân phối (mua bán) để thu lợi. Mã đối tượng (MĐT) là công trình sáng tạo và hầu hết mọi người đều công nhận rằng, sự phân phối MĐT là môi trường chấp nhận được về sự công bố. Như vậy, bảo vệ bản quyền có vẻ là phù hợp. Một đơn xin bản quyền thường được kèm theo một bản copy đối tượng mà sẽ xin bản quyền. Với một cuốn sách hoặc bản nhạc (được in hay được ghi âm) thì dễ dàng bản copy. Cơ quan bản quyền (The Copyright Office – C.O.) hiện còn chưa quyết định được môi trường nào là phù hợp để trên đó chấp nhận mã đối tượng. Một liệt kê nhị phân (a binary listing) của MĐT sẽ được xem xét, nhưng C.O. làm điều này mà không thừa nhận liệt kê này sẽ được công nhận hay đủ được chấp nhận hay không. C.O. sẽ chấp nhận một liệt kê mã nguồn. Một số người lập luận rằng, liệt kê mã nguồn không giống như liệt kê mã đối tượng, tương tự như là một bản dịch sang tiếng Pháp của một tiểu thuyết sẽ khác với nguyên bản ngôn ngữ gốc của nó. Vẫn chưa được rõ ràng tại toà rằng, đăng ký một phiên bản mã nguồn sẽ cung cấp bảo vệ bản quyền cho MĐT hay không. Tuy nhiên, người ta sẽ không thể lấy mã đối tượng nói trên của một hệ thống sắp xếp lại trật tự của các dãy riêng biệt và nói rằng đây là một hệ mới. Nếu không có các liệt kê nguồn gốc rất khó mà so sánh hai file nhị phân để xác định rằng, một file này là chức năng tương đương của file kia chỉ đơn giản qua sự sắp xếp trật tự.

Có lẽ phải cần một số phiên toà tranh tụng để xác lập các cách làm thủ tục văn bản bảo vệ bản quyền cho MĐT. Hơn nữa, các phiên tranh tụng sẽ phải đưa ra các tiền lệ để xác định sự tương đương của hai đoạn mã máy tính.

1.3.4.4 Bảo vệ mã nguồn phần mềm.

Các nhà phát triển phần mềm khi bán chúng trên thị trường thường né tránh việc phân phối mã nguồn của họ. Mã nguồn có thể được xem như một BMTM, mặc dù một vài luật sư cũng khuyến cáo rằng nó có thể được bản quyền. (Hai dạng bảo vệ này có thể loại trừ lẫn nhau, mặc dù đăng ký bản quyền sẽ không tai hại gì). Nhớ lại rằng, C.O. đòi hỏi đăng ký ít nhất 25 trang đầu và 25 trang cuối của tài liệu đã viết ra. Các trang này sẽ đặt tại thư viện của Quốc hội (The Library of Congress), nơi công chúng có thể tiếp cận. Đăng ký này giúp cho toà án xác định rõ, tác phẩm nào đã được đăng ký bảo hộ bản quyền.Tuy nhiên, vì chúng được trưng bày cho ai cũng xem được nên chúng không là bí mật, và đăng ký bản quyền có thể phá vỡ tính bí mật của thuật toán cao siêu. Bản quyền bảo vệ quyền được phân phối các bản copy sự thể hiện của một ý tưởng, chứ không phải bản thân ý tưởng. Vì thế, bản quyền không ngăn chặn người khác sử dụng lại một thuật toán, được thể hiện qua một chương trình đã được bản quyền.

Như vừa miêu tả, mã nguồn có thể là dạng phù hợp hơn cả để đăng ký bản quyền cho một chương trình được công bố ở dạng đối tượng rất khó để đăng ký mã nguồn với C.O. mà vẫn giữ được tính mật của nó. Một chương trình máy tính dài có thể được sắp xếp sao cho 25 trang đầu và 25 trang cuối của nó không tiết lộ nhiều phần mật của chương trình nguồn. Những lỗi nhỏ hoặc dấu hiệu nhận biết khác thường được cài vào mã nguồn (hoặc mã đối tượng) của một chương trình có thể hữu ích hơn trong việc xác định các vi phạm bản quyền. Xin nhắc lại rằng, cần một số phiên tranh tụng nữa mới có thể quyết định được các thủ tục bảo vệ các chương trình máy tính ở dạng nguồn cũng như ở dạng đối tượng.

1.3.4.5 Bảo vệ các văn bản tài liệu.

Nếu chúng ta coi văn bản như một tác phẩm viết không tưởng tượng (hoặc có thể tưởng tượng) thì bảo vệ bản quyền là hiệu quả và phù hợp với văn bản – tài liệu. Lưu ý rằng tài liệu khác với một chương trình. Một chương trình và tài liệu của nó phải được bản quyền riêng biệt. Hơn nữa, bảo vệ bản quyền của tài liệu có thể thắng kiện chống lại kẻ đã sao chép bất hợp pháp cả chương trình và tài liệu của nó.

Trong các phiên toà, khi mà một điều luật viết ra không rõ hoặc tính áp dụng của luật không tường minh với tình huống cụ thể, thì kết quả của các phiên toà sẽ dùng để phân loại thậm chí mở rộng ý nghĩa của các câu chữ (thuật ngữ) của bộ luật đó. Các luật sư thường biện minh cho các hành động không đúng (kể cả các tác phẩm máy tính) đã xảy ra, là do sự ngoại suy mở rộng của luật. Vì thế ý nghĩa và sử dụng một luật sẽ tiếp tục được hoàn chỉnh qua các phiên tranh tụng. Điều này càng là hiển nhiên khi mà công nghệ máy tính tiến bộ nhanh hơn nhiều so với sự theo kịp của pháp luật.

1.3.4.6 Bảo vệ nội dung Web.

Nội dung trên một trang web là môi trường. Khá giống như một cuốn sách hoặc bức ảnh, nên bảo vệ phù hợp nhất cho nó là bản quyền. Bản quyền này cũng

sẽ bảo vệ phần mềm mà bạn viết để làm sống động hoặc để tạo các tác động khác tới cách trình bầy (display) trang web của bạn. Và, về mặt lý thuyết, nếu trang web của bạn có chứa các mã độc hại thì bản quyền của bạn sẽ bảo hộ cả nó nữa. Như chúng tôi đã trình bày ở trên, một tác phẩm đã được bản quyền không phải hoàn toàn mới; nó có thể là sự pha trộn của tác phẩm mới mà bạn yêu cầu bản quyền và những thứ cũ mà bạn không được bản quyền. Bạn có thể trả tiền (mua) hoặc xin phép dùng một đoạn (một mẫu) của trang trí web, một biểu tượng (ví như một đoạn hình có quả đất đang xoay tròn) hoặc một bản nhạc. Bản quyền sẽ bảo hộ các tác phẩm nguyên gốc của bạn.

1.3.4.7 Bảo vệ tên miền và URLs (các địa chỉ tài nguyên).

Các tên miền, các URL – Uniform Resource Locality (tài nguyên định dạng), tên công ty, tên sản phẩm, và nhãn biểu tượng thương mại được bảo vệ bằng một nhãn hiệu (trademark) cung cấp toàn quyền sử dụng cho chủ sở hữu của các nhãn định dạng loại này.

1.4 Luật pháp và thông tin.

Mã nguồn, mã đối tượng, và thậm chí cái "nhìn thấy và cảm nhận" của một màn hình máy tính đều là các đối tượng được công nhận mặc dù chúng không hữu hình. Luật pháp đang làm việc khá trơn tru với những thứ đó, mặc dù đôi thứ còn bị chậm chạp. Nhưng hiện nay, điện toán đang được dịch chuyển tới các loại đối tượng mới, đòi hỏi các dạng bảo vệ pháp lý mới. Thương mại điện tử, xuất bản điện tử, bầu cử điện tử, giao dịch ngân hàng điện tử (electronic banking) là các thách thức mới đối với hệ thống pháp luật hiện nay.

Trong phần này chúng ta sẽ xem xét một số trong những đòi hỏi an toàn mới này.

1.4.1 Thông tin là đối tượng bảo vệ.

Người chủ hiệu thường tích trữ "các đồ vật" trong cửa hàng, ví như các bộ cúc áo, các xe hơi, và các gói đường. Các người mua là các khách hàng. Khi một thứ được bán cho một khách hàng, danh mục thứ đó của chủ hiệu bị giảm đi một, và người khách hàng đó trả tiền và rời khỏi cửa hàng mang theo đồ vật đã mua. Đôi khi khách hàng đó có thể bán lại thứ đó cho một ai khác với món trả hơn hoặc kém so với ban đầu.

Có các dạng mua bán khác cung cấp các dịch vụ mà có thể coi như giống các đồ vật, ví dụ cắt tóc, nhổ răng, hoặc sự bảo vệ cho một phiên toà. Một số dịch vụ có nhiều giá (ví dụ cắt tóc) nha cung cấp dịch vụ có thể lấy tiền người này nhiều hơn người khác. Cái mà chủ hiệu (thợ cắt tóc, bác sỹ nha khoa, luật sư) ở đây đã bán chính là thời gian. Cụ thể là, giá của một lần cắt tóc được so sánh với gia thời gian của thợ cắt tóc và các luật sư, và các bác sỹ được trả tiền bằng giờ dịch vụ trong đó rõ ràng là không có một đơn vị chuẩn nào. Giá trị của mỗi dịch

vụ trong kinh tế tự do, cách này hay cách khác đều phụ thuộc vào ý muốn của người mua và người bán. Ví dụ, người bác sỹ chỉ muốn bán một lượng thời gian nhất định, thời gian còn lại của ngày hôm đó ông ta còn định làm việc khác. Giống như người chủ hiệu, một khi, nhà cung cấp dịch vụ đã bán một lượng thời gian nhất định (tức là bán dịch vụ đó), nó không thể được bán cho ai đó khác một lần nữa. (Tương tự như khi khách hàng đã trả tiền và mang hàng đi thì trong danh mục của chủ hiệu phải giảm đi một).

Còn thông tin là một loại hàng hoá đặc biệt. Nó khác với các đồ vật, nó cũng khác hẳn các dịch vụ.

1.4.1.1 Thông tin không thể bị suy giảm.

Không giống như các thứ hữu hình (đồ vật) và các dịch vụ, thông tin có thể được bán nhiều lần mà không bị giảm sút cả danh mục và chất lượng. Ví dụ, cơ quan tín dụng có thể bán cùng một báo cáo tài chính về một cá nhân cho rất nhiều khách hàng. Mỗi khách hàng trả tiền đều vì thông tin trong báo cáo cần cho họ. Vậy cùng một thông tin đó được bán rất nhiều lần, và đương nhiên thông tin đó không bị suy giảm đi chút nào.

Đặc trưng này phân biệt thông tin với các tác phẩm hữu hình, như là cuốn sách, đĩa CD, hay các ấn phẩm. Mỗi sản phẩm hữu hình là một bản sao đơn lẻ mà có thể được đánh số riêng hoặc đếm được. Chủ hiệu sách luôn có thể yêu cầu nhiều hơn các bản sao của một cuốn sách nếu danh mục trở nên suy giảm, vì anh ta có thể bán bao nhiêu bản sách nếu anh ta thích.

1.4.1.2 Thông tin có thể nhân bản.

Giá trị của thông tin chính là cái mà người mua trả tiền cho người bán. Nhưng khi đã mua thông tin, người mua có thể sau đó lại trở thành người bán và có thể tước đoạt khả năng bán tiếp nữa của người bán đầu tiên. Vì thông tin không bị suy giảm nên người mua có thể thụ hưởng hoặc sử dụng thông tin và cũng có thể bán nó nhiều lần để thu lợi.

Giá của thông tin thường phụ thuộc thời gian. Nếu bạn biết được (vì lý do gì đó) giá giao dịch của các cổ phiếu nổi tiếng nào đấy (của hãng Microsoft chẳng hạn) vào tuần tới, thì thông tin này sẽ cực kỳ có giá vì rằng bạn có thể nhờ nó mà thu được mối lợi to lớn trên thị trường chứng khoán. Tất nhiên, cái giá giao dịch đó không thể biết được ngày hôm nay. Nhưng giả sử rằng, bạn biết được rằng Microsoft đã quyết định công bố cái gì đó vào tuần tới và điều đó sẽ làm cho giá cổ phiếu sẽ lên hoặc xuống. Thông tin này cũng sẽ hầu như quý báu như là biết chính xác giá giao dịch, và nó có thể biết trước (vào ngày hôm nay). Tuy nhiên, việc biết giá giao dịch của cổ phiếu Microsoft ngày hôm qua hoặc biết được hôm qua hãng này vừa công bố cái gì đó làm giá cổ phiếu đã tụt dốc ngay tức khắc lại không có giá trị vì rằng điều này đã được hầu hết các tờ báo ngân hàng lớn đưa

tin. Như vậy, giá của thông tin có thể phụ thuộc vào việc khi nào bạn biết được thông tin đó.

1.4.1.3 Thông tin được truyền đi thường ở dạng không hữu hình.

Tờ báo là một đồ tạo tác được in ấn. Hãng thông tấn trao tận tay cho khách hàng, người cầm nó vừa đi vừa đọc. Cả hai người bán và người mua đều nhận thấy và cùng thừa nhận rằng mình vừa kiếm được một thứ gì đó. Hơn nữa, rõ ràng là, nếu như tờ báo này bị hư hại đáng kể, ví dụ có một lỗ hổng lớn ở giữa trang báo, thì hệ quả sẽ dễ dàng được chỉ ra.

Nhưng thời gian đang thay đổi một cách nhanh chóng, thông tin nay đang được truyền đi như các dãy bit trên các mạng thay vì nó được in ra trên mặt các báo. Nếu dãy bit thông tin truyền đi có thể nhìn thấy được thì sự rò rỉ các bit (gây lỗi) cũng dễ chứng minh. Tuy nhiên, nếu bản copy của thông tin là rất chính xác nhưng thông tin nằm trong đó (copy) lại không đúng, không dùng được, hoặc không như là mong muốn, thì thật khó mà chứng minh rằng thông tin đó đã bị mất mát.

1.4.2 Những vấn đề luật pháp về thông tin.

Những đặc tính kể trên của thông tin quyết định đến các pháp luật về thông tin và an toàn thông tin. Chúng ta phải nhận thức được các yếu tố này nếu ta quan tâm xem thông tin có quan hệ tới các luật về bản quyền, sáng chế và nhãn hiệu như thế nào. Trước tiên chúng ta phải lưu ý rằng, thông tin có một số cơ sở luật pháp rất giới hạn để bảo vệ nó. Ví dụ, thông tin có thể được đối xử như một bí mật thương mại trong ý nghĩa rằng thông tin có mặt trong danh mục buôn bán của người bán thông tin. Trong khi người bán sở hữu thông tin này, bảo vệ BMTM đương nhiên được áp dụng cho quyền thu lợi từ thông tin đó của người bán. Như vậy toà án công nhận rằng thông tin có giá trị.

Tuy nhiên, như ở trên đã nói, BMTM có giá trị chỉ khi mà nó vẫn còn là bí mật. Ví dụ, hãng Coca – cola không thể hy vọng vẫn giữ được bảo vệ BMTM cho công thức của nó sau khi nó đã bán công thức này. BMTM này cũng không còn là an toàn nếu có ai đó lấy được hoặc suy đoán ra nó. Hai dạng bảo vệ khác mà người ta bàn tới ở đây là bản quyền và sáng chế. Như ta đã thấy ở các phần trước, cả hai loại này không có loại nào áp dụng hoàn chỉnh cho phần cứng hoặc phần mềm máy tính cả, và thậm chí chúng còn kém hơn nữa khi áp dụng cho thông tin. Tốc độ thay đổi trong hệ thống pháp luật là chậm chạp. Điều đó cho phép tin tưởng chắc chắn rằng, những đổi mới đã diễn ra là chính đáng và đã được nghiên cứu kỹ càng. Những bước đi muộn màng và chậm chạp trong hệ thống pháp luật gần như là đã bị đánh gục bởi nhịp độ siêu âm của các biến đổi trong công nghiệp CNTT (ITI – Information Technology Industry). Pháp luật không và không thể kiểm soát được tất cả các hiểm hoạ trong không gian điều khiển (cyber

threats). Chúng ta hãy xem xét một số ví dụ về các trường hợp trong đó nhu cầu thông tin đặt ra những đòi hỏi bức xúc đối với hệ thống pháp luật.

1.4.2.1 Thông tin thương mại (mua bán TT).

Thông tin không giống như hầu hết các hàng hoá thương mại khác, dù là nó có giá trị và là cơ sở của các trao đổi mua bán. Thị trường thông tin vẫn còn mới và do đó cộng đồng pháp luật vẫn còn ít kinh nghiệm trong các vấn đề của thông tin. Mặc dù vậy, một số vấn đề cơ bản then chốt cũng phải được giải quyết.

Ví dụ, chúng ta đã thấy việc ăn cắp phần mềm tức là sao chép thông tin mà không trả tiền đúng giá cho người đáng được hưởng. Có một vài cách tiếp cận đã hình thành để giúp cho các nhà phát triển phần mềm hoặc nhà sản xuất nhận được khoản trả công tương xứng khi có sự sử dụng phần mềm đó. Đó là các phương pháp: bảo vệ copy, kho tự do – dùng chung (freeware), và phần phối có kiểm soát. Cách đây ít lâu, một số phần mềm đang được phân phối như bộ mã di động hoặc như các phụ kiện điện tử đi kèm cần thiết. Mỗi phụ tung có thể bị truy theo dấu vết và phải trả tiền cho nó, và mỗi phụ kiện này có thể tự huỷ sau khi đã được dùng sao cho không còn lại gì cả để mà có thể bán cho ai đó nữa. Nhưng hệ thống này đòi hỏi nhiều công việc về tính toán và theo dõi dấu vết, do đó làm tăng giá thành khó chấp nhận. Như vậy, hiện nay vẫn chưa có một tiếp cận nào khả dĩ về mặt công nghệ, do đó phương thuốc luật pháp vẫn thường phải duy trì và phát triển.

1.4.2.2 Xuất bản điện tử (electronic publishing).

Nhiều tờ báo và tạp chí gửi một phiên bản các nội dung của nó lên Internet giống như là các dịch vụ điện báo và các hãng vô tuyến truyền hình vẫn làm. Ví dụ, hãng thông tấn Anh quốc BBC và hãng Roitơ có một trang web rất đồ sộ. Chúng ta cũng được chứng kiến rằng, một số tin tức và thông tin sẽ được xuất bản trọn vẹn và phần phối toàn bộ chỉ trên Internet mà thôi. Trên thực tế hiện nay, các Bách khoa toàn thư (encyclopedias) ví như là Britanica và Expedia, chủ yếu được cung cấp trên các trang web chứ không phải là được bán ở dạng nhiều tập sách như trước. Ở đây, một lần nữa lại xuất hiện vấn đề, nhà xuất bản (điện tử) phải có được khoản tiền hợp pháp cho công việc của mình. Giải pháp kỹ thuật dựa trên mật mã học hiện đang được phát triển để giải quyết vấn đề này. Tuy nhiên, các giải pháp kỹ thuật này cần phải được trợ giúp bằng cơ cấu luật pháp để buộc sử dụng chúng.

1.4.2.3 Bảo vệ dữ liệu trong một cơ sở dữ liệu (CSDL).

CSDL là một dạng đặc biệt của phần mềm đang đặt ra nhiều vấn đề nan giải cho pháp luật. Toà án đã và đang gặp rất nhiều khó khăn để quyết định xem phải áp dụng các luật bảo vệ nào cho CSDL. Làm thế nào để xác định rằng, một tập dữ liệu xuất phát từ một CSDL riêng nào đó (vì thế mà chủ sở hữu CSDL này có

thể đòi trả một món tiền nhất định?). Ai sẽ là chủ sở hữu các dữ liệu trong một CSDL nếu nó là các dữ liệu công cộng, như là tập các tên và các địa chỉ?

1.4.2.4 Thương mại điện tử (Electronic Commerce).

Các luật điều chỉnh buôn bán hàng hoá đã phát triển thành văn hàng trăm năm rồi. Các bảo vệ luật pháp phù hợp đã tồn tại bao gồm hàng hoá kém phẩm chất, trả tiền gian lận và lỗi giao nhận khi mà hàng hoá là hữu hình và được mua qua các thị trường truyền thống như các cửa hàng và lô hàng. Tuy nhiên, tình huống trở nên kém rõ ràng khi mà hàng hoá được mua bán trên mạng (bằng điện tử).

Nếu bạn đặt hàng bằng điện tử (trên mạng), chữ ký số và các thủ tục mật mã khác có thể cung cấp sự bảo vệ kỹ thuật cho "đồng tiền" của bạn. Tuy nhiên, giả sử rằng thông tin mà bạn yêu cầu không phù hợp để dùng, hoặc không nhận được hoặc đến được nhưng bị hong hoặc đến quá muộn không dùng được. Bạn sẽ phải chứng minh điều kiện giao nhận như thế nào? Trong mua bán theo lô, bạn thường có vận đơn (biên lai, giấy biên nhận) hoặc một dạng giấy tờ nào đó nhận thực về thời gian, ngày tháng và địa điểm. Nhưng trong mua bán điện tử, sự chứng nhận như vậy có thể không có hoặc có thể bị giả mạo rất dễ dàng. Những vấn đề pháp luật như vậy phải được giải quyết khi mà chúng ta tiến vào thời đại của thương mại điện tử.

1.4.3 Bảo vệ thông tin.

Rõ ràng là, các luật hiện hành không phù hợp cho bảo vệ bản thân TT và cho bảo vệ các dạng thương mại điện tử. Vậy TT sẽ được bảo vệ pháp lý như thế nào? Như đã mô tả, bản quyền, sáng chế và BMTM bao hàm một số, nhưng không phải tất cả, các khía cạnh liên quan tới TT. Mặc dù vậy, hệ thống pháp luật không cho phép luồng chảy tự do trong TT; một vài cơ chế có thể rất hữu ích.

1.4.3.1 Chế định hình sự và dân sự (Criminal and Civil Law).

Chế định là điều luật thành văn tuyên bố một cách thẳng thắn rằng các hành vi nhất định là phạm pháp. Mỗi quy phạm là kết quả của một quá trình pháp chế mà nhờ nó chủ thể nhà nước công bố rằng, luật mới sẽ có hiệu lực sau một thời gian thiết lập. Ví dụ, nghị viện có thể thảo luận các vấn đề liên quan tới các giao dịch thuế trên Internet và thông qua một luật về việc khi nào các khoản thuế chính đáng phải được trả.

Thông thường, sự vi phạm một chế định sẽ dẫn đến một toà án hình sự, tại đó nhà nước sẽ thi hành sự trừng phạt vì rằng hành vi phạm pháp đã làm hại cho mong muốn tự nhiên của cộng đồng. Ví dụ, nhà nước sẽ khởi tố một vụ giết người vì rằng kẻ giết người vi phạm luật mà nhà nước đã thông qua. Mục đích của toà án hình sự là để trừng phạt tội phạm, thường bằng cách tước bỏ tội phạm hết các quyền (như là bỏ tù tội phạm hoặc phạt tiền).

Luật dân sự là một dạng khác hẳn hình sự. Nó không đòi hỏi tiêu chuẩn cao về chứng minh sự phạm lỗi (như hình sự). Trong một án dân sự, một cá nhân, một tổ chức, công ty hoặc nhóm người tuyên bố rằng họ bị hại. Mục đích của toà án dân sự là sự bồi thường: là cho bị hại "hồi phục" bằng việc sửa chữa các vi phạm. Ví dụ, giả sử rằng Fred giết chết John. Vì Fred đã vi phạm luật chống giết người, nhà nước sẽ khởi tố Fred trước toà hình sự do phá vỡ luật, làm đảo lộn trật tự xã hội. Còn Abigail, vợ của bị hại còn sống sót, có thể là nhân chứng tại toà hình sự, mong muốn nhìn thấy Fred bị bỏ tù. Nhưng bà ta cũng có thể kiện Fred tại toà dân sự vì cái chết oan uổng, đòi hỏi một món tiền trả để trợ giúp các đứa con sống sót của bà ta.

1.4.3.2 Luật phạm lỗi (Tort law).

Có một ngôn ngữ luật riêng mô tả các thiệt hại xảy ra trong một vụ dân sự. Nó phản ánh hoặc là trường hợp trên cơ sở phá vỡ một điều luật hoặc là vi phạm quy ước hành xử tiền lệ đã được hoàn thiện từ trước. Nói cách khác, đôi khi các thẩm phán có thể đưa ra những quyết định dựa trên cái gì là có lý và cái gì đã từng cho qua hơn là dựa trên cái gì được viết trong pháp chế. Sự phạm lỗi (a tort) là sự gây hại không xảy ra từ vi phạm một chế định hoặc từ phá huỷ một hợp đồng, mà thay vì điều đó lại xảy ra. Như vậy, chế định luật được viết ra bởi các nhà pháp chế và được minh chứng bằng toà án, các điều phạm lỗi không được viết thành văn nhưng được rút ra qua các quyết định của toà án và đã trở thành các tiền lệ đối với các trường hợp xảy ra sau đó. Kiểm nghiệm cơ bản của một phạm lỗi là điều, những gì có thể làm (trong trường hợp tương tự) đối với một người lành mạnh (reasonable). Gian lận (fraud) là ví dụ điển hình của chế định phạm lỗi, trong đó, thông thường, một người lừa đảo người khác mà gây hại. Thông tin máy tính rất phù hợp đối với luật về phạm lỗi. Toà án hoàn toàn quyết định thế nào là một hành vi lành mạnh, chứ không như là một chế định dựa trên các hành động. Ví dụ thông tin lấy từ một người nào đó (mà không được phép) và đem bán TT đó cho một người khác như là TT của riêng mình, là sự gian lận (fraud). Chủ sở hữu TT này có thể khởi kiện anh, mặc dù có thể là không có chế định luật nào nói rằng trộm cắp thông tin là bất hợp pháp. Chủ sở hữu đó đã bị làm hại bởi sự tước đoạt khỏi khoản chi trả mà anh đã thu được khi bán TT nói trên.

Vì rằng, luật phạm lỗi chỉ được viết như là dãy các phán quyết của toà án được thường xuyên rút ra, khởi tố một vụ phạm lỗi (a tort case) có thể bị khó khăn. Nếu bạn có dính líu vào án dựa trên luật phạm lỗi, bạn và luật sư của bạn thường cố gắng thử hai cách tiếp cận: Thứ nhất, anh có thể cãi rằng, trường hợp của anh là sự vi phạm rõ ràng các chuẩn mực xã hội, rằng đó không phải là hành vi mà một người chân chính, cẩn trọng có thể mắc phải. Tiếp cận này có thể thiết lập một phạm lỗi khác. Thứ hai, anh có thể viện cãi rằng, trường hợp của anh tương tự như một hoặc vài tiền lệ, có thể chỉ ra sự song song giữa một chương trình máy tính và một tác phẩm nghệ thuật. Quan toà hoặc hội đồng sẽ phải quyết

định xem sự so sánh này phù hợp hay không. Trong cả hai lối tiếp cận này, đều có thể rút ra các điều giúp cho luật ngày càng hoàn thiện và bao được cả các đối tượng mới.

1.4.3.3 Chế định hợp đồng (Contract Law).

Chúng ta đã xem xét hai dạng bảo vệ các đối tượng máy tính ở trên. Đó là dùng chế định hình sự và dân sự, và dùng các chế định về phạm lỗi. Dạng thứ ba để bảo vệ đối tượng máy tính là các hợp đồng. Một hợp đồng là một sự thoả thuận giữa hai bên. Hợp đồng phải bao gồm ba thứ:

- Điều kiện đưa ra.
- Sự chấp nhận.
- Sự xem xét.

Một bên đưa ra một cái gì đó: "Tôi sẽ viết chương trình máy tính này cho anh với giá là bấy nhiêu tiền". Bên kia có thể chấp nhận điều đưa ra này, từ chối nó, đưa ra một đề nghị ngược hẳn lại, hoặc đơn giản là không đếm xỉa đến nó. Trong quá trình đạt tới thoả thuận bằng hợp đồng, chỉ có sự chấp nhận là quan trọng nhất, đáng quan tâm nhất, tất cả những điều còn lại chỉ là câu chuyện về sự thoả thuận đã đạt được như thế nào. Hợp đồng phải bao gồm sự xem xét về tiền bạc hoặc về các giá trị khác. Tư tưởng chính ở đây là, hai bên trao đổi các vật có giá trị, ví như thời gian thương mại (tính ra tiền) hoặc những hiểu biết kỹ nghệ (qua phong cách tiếp thị). Ví dụ, "Tôi sẽ rửa xe của anh nếu anh cho tôi ăn bữa trưa" hoặc "Nào chúng ta buôn bán hai đĩa CD này" là các điều kiện đưa ra đòi hỏi sự xem xét. Nó giúp cho hợp đồng sẽ được viết ra, nhưng nó không cần có mặt trong hợp đồng. Một hợp đồng viết có thể gồm hàng trăm trang từ ngữ và điều kiện lượng hoá điều đưa ra và sự xem xét.

Một khía cạnh cuối cùng của hợp đồng là tính tự do của nó. Hai bên phải đi vào hợp đồng một cách tự nguyện. Nếu tôi nói "Hãy ký bản hợp đồng này đi hoặc tôi sẽ bẻ gãy tay anh", thì bản hợp đồng này không phù hợp, cho dù nếu làm mất một cánh tay trên thực tế là xem xét cần quan tâm đối với anh. Hợp đồng được ký dưới sự cưỡng bức hoặc bằng hành động gian lận là không ràng buộc được. Hợp đồng không thể là sự buôn bán, trong ý nghĩa về sự xem xét bình đẳng đối với cả hai bên cho đến khi nào cả hai bên đều tự nguyện chấp nhận các điều kiện.

Thông tin cũng thường được trao đổi qua hợp đồng. Các hợp đồng là lý tưởng để bảo vệ sự truyền thông tin bởi vì, các hợp đồng có thể đưa ra các điều kiện bất kỳ. "Anh có quyền sử dụng nhưng không được thay đổi (modify) thông tin này" hoặc "Anh có quyền sử dụng nhưng không được bán lại thông tin này" hoặc "Anh có quyền xem thông tin này tự mình nhưng không cho phép những người khác xem nó" là ba điều kiện hợp đồng tiềm năng khả dĩ bảo vệ lợi ích thương mại của chủ sở hữu thông tin.

Các hợp đồng máy tính bao gồm sự phát triển và sử dụng phần mềm và các dữ liệu số hoá. Chúng tôi xin lưu ý ngắn gọn rằng, có tồn tại các quy định về việc ai sẽ có quyền ký hợp đồng đối với phần mềm, người thuê khoán hay người được thuê khoán, sự chờ đợi có lý về chất lượng của một phần mềm phải như thế nào.

Nếu các từ ngữ của bản hợp đồng đầy đủ và sự trao đổi xem xét đã diễn ra, mọi người đều vui vẻ. Thông thường các khó khăn xuất hiện khi mà một phía nghĩ các từ ngữ đã rất đầy đủ và chặt chẽ nhưng phía bên kia lại không đồng ý.

Giống như với chế định lỗi, phương thuốc chung nhất trong chế định hợp đồng là tiền. Anh đồng ý bán cho tôi một chuỗi hạt kim cương và tôi phát hiện ra là nó làm từ đồng thau. Tôi kiện anh, giả sử toà đồng ý với tôi, nó có thể buộc anh trao trả tôi một chuỗi hạt kim cương, nhưng thường hơn thì toà sẽ quyết rằng tôi có quyền có một khoản tiền. Trong trường hợp này, tôi có thể trước hết đòi lại số tiền mà tôi đã trả cho anh ban đầu, và sau đó viện dẫn về sự làm hại cố ý mà tôi biết khi đến gặp bác sỹ, chẳng hạn, rằng chuỗi hạt đồng của anh đã biến da tôi trở nên xanh xao hoặc về sự bị xúc phạm mà tôi cảm thấy khi một người bạn trỏ vào cái chuỗi hạt của tôi và kêu toáng lên "Hãy nhìn xem cái chuỗi hạt rẻ tiền này" tôi cũng có thể viện dẫn về các thiệt hại khác để trừng phạt và ngăn ngừa anh không làm việc tương tự một lần nữa. Toà sẽ quyết định cái nào trong các đòi hỏi của tôi là phù hợp và khoản tiền đền bù bao nhiêu là có lý.

Trong phần này đã trình bày sơ lược về các luật và áp dụng chúng cho phần cứng, phần mềm và dữ liệu máy tính. Sự khác nhau giữa luật hình sự và dân sự được so sánh trong bảng sau:

Bảng 2: So sánh luật hình sự và luật dân sự

	Luật hình sự	Luật dân sự
Xác định bởi	Các chế định	Các hợp đồng Luật chung
Các phiên toà tiến hành bởi	Nhà nước	Nhà nước Các cá nhân và các công ty
Bên bị thiệt hại	Xã hội	Cá nhân và các công ty
Phương pháp (chữa)	Nhà tù, phạt	Bồi thường thiệt hại, thông thường là tiền

Các hợp đồng giúp lấp đầy khoảng trống giữa luật hình sự, dân sự và phạm lỗi. Như vậy, khi còn chưa có các chế định rõ ràng, chúng ta trước tiên nhìn thấy sự phát triển các luật chung về phạm lỗi (a tort). Sau đó con người tăng cường các luật (phạm lỗi) này bằng các hợp đồng với các dạng bảo vệ riêng mà họ mong muốn.

Buộc thực thi luật dân sự về phạm lỗi hoặc các hợp đồng có thể đắt giá vì nó đòi hỏi một bên này khởi kiện bên kia. "Hệ thống pháp luật được cân nhắc một cách không chính thức bởi đồng tiền. Rất hấp dẫn khi theo kiện một công ty mạnh, nơi có thể trả nhiều tiền cho các thẩm phán có trọng lượng". Một giáo sư Mỹ đã nhận xét như vậy.

1.5 Quyền hạn của người thuê khoán và người nhận thuê khoán.

Những người thuê khoán (ông chủ) thuê những người nhận thuê khoán (người làm thuê) để đưa ra những ý tưởng và làm ra các sản phẩm. Sự bảo vệ được thực hiện bằng bản quyền, sáng chế và bí mật thương mại, dường như chống lại các nhà thuê khoán vì rằng nó được áp dụng cho các ý tưởng và các sản phẩm. Tuy nhiên, vấn đề ai sở hữu các ý tưởng và các sản phẩm lại phức tạp. Chủ sở hữu ở đây là một khía cạnh an toàn máy tính vì nó liên quan đến các quyền của một nhà thuê khoán bảo vệ tính bí mật và tính toàn vẹn của các công trình đã được các người nhận thuê khoán làm ra. Trong phần này chúng ta sẽ nghiên cứu các quyền tương ứng của các người thuê khoán và các người nhận thuê khoán đối với các sản phẩm MT của họ.

1.5.1 Chủ sở hữu các sản phẩm.

Như trên đã nói, đây là một vấn đề phức tạp và tế nhị. Chúng ta hãy xem xét một ví dụ.

Giả sử Edic là người làm việc cho một công ty phần mềm máy tính. Như là một phần công việc của mình, cô ta phát triển một chương trình điều khiển các windows trên một màn hình máy tính. Chương trình này sẽ thuộc về công ty của Edic vì rằng công ty đã trả tiền cho Edic để viết chương trình này: cô ta đã viết nó như một phần của hợp đồng công việc. Như vậy, Edic không thể tự mình tiếp thị chương trình. Cô ta không thể bán nó thậm chí nếu cô đã làm việc cho một công ty không có quan hệ gì tới phần mềm nhưng đã phát triển phần mềm này như là một phần công việc của cô ấy. Mọi người nhận thuê khoán đều hiểu yếu tố này trong trách nhiệm của họ đối với chủ thuê khoán của họ.

Trái lại, giả sử rằng Edic phát triển chương trình này vào các buổi tối ở nhà, đó không phải là một phần công việc của cô ta. Do vậy cô thử cố gắng tiếp thị sản phẩm tự mình. Nếu Edic làm việc như một nhà lập trình, chủ thuê khoán của cô ta có lẽ sẽ nói rằng, Edic đã trục lợi từ sự đào tạo và kinh nghiệm thu được

trong công việc (tại công ty), ít nhất thì Edic đã thai nghén hoặc suy nghĩ về đề án này khi làm việc. Vì vậy, người thuê khoán phải có lợi ích (nghĩa là sở hữu ít nhất một phần) trong các quyền đối với chương trình của cô ta. Tuy nhiên, tình huống sẽ thay đổi nếu công việc cơ bản (ở công ty) của Edic không phải là lập trình. Nếu Edic là phát thanh viên trên TV, chủ thuê khoán của cô ấy không thể có đóng góp gì liên quan tới sản phẩm máy tính của cô ta. Vậy nếu công việc của cô ấy không bao gồm việc lập trình, thì cô ấy có thể tự do mua bán bất kỳ sản phẩm máy tính nào mà mình làm ra. Và nếu chương trình ngoài giờ của Edic là một ứng dụng để vẽ cây gia phả chẳng hạn, chủ thuê khoán của cô ta rõ ràng không thể ham muốn quyền hành gì đối với chương trình của cô ấy, vì rằng nó rất xa lạ với lĩnh vực kinh doanh của ông này. Cuối cùng, giả sử rằng, Edic không là người nhận thuê khoán của công ty. Hơn nữa, cô ấy là một cố vấn – một người bị thuê mướn, và cô ấy viết các chương trình thương mại cho các khách hàng của mình với khoản phí nào đó. Hãy xem xét vị trí pháp lý của cô ta trong tình huống này. Cô ấy có thể sử dụng một thiết kế chương trình cơ bản, tổng quát nó lên chút ít, và tiếp thị nó cho mọi người. Edic cãi rằng cô ta nghĩ ra, viết và kiểm thử chương trình này, vì thế nó là công trình của cô ấy, và cô sở hữu nó (và có quyền bán nó). Khách hàng của Edic cãi rằng, ông ta đã trả tiền cho Edic để phát triển chương trình đó, và ông ta sở hữu nó giống như là ông ta có thể sở hữu một tủ sách mà cô ấy đã được trả tiền, để đặt ở địa điểm nào đó.

Rõ ràng là, các tình huống này khác nhau, và minh hoạ các luật về chủ sở hữu thường gặp khó khăn. Chúng ta hãy xem xét lần lượt mỗi loại bảo vệ.

1.5.1.1 Chủ sở hữu sáng chế (Patent).

Cá nhân mà sở hữu một công trình được bảo hộ bằng luật sáng chế hoặc luật bản quyền là một nhà phát minh, trong các ví dụ mô tả ở trên, chủ sở hữu ở đây là nhà lập trình hoặc nhà thuê khoán. Theo luật sáng chế, quan trọng phải biết ai là người đệ đơn đăng ký sáng chế. Nếu người nhận thuê khoán (làm thuê) cho phép người thuê khoán (ông chủ) đăng ký sáng chế một phát minh, thì người thuê khoán có thể sở hữu sáng chế đó và vì thế cả các quyền đối với phát minh.

Người chủ thuê khoán cũng có quyền đối với sáng chế nếu như chức năng công việc của người nhận thuê khoán có bao gồm phát minh ra sản phẩm. Ví dụ, trong một công ty lớn một nhà khoa học có thể được thuê khoán đề làm các nghiên cứu, phát triển, và các kết quả của công trình phát minh này sẽ trở thành sở hữu của người chủ công ty. Thậm chí khi người nhận thuê khoán đăng ký sáng chế cái gì đó, thì chủ thuê khoán có thể tranh chấp về quyền sử dụng phát minh đó nếu ông chủ này đã đóng góp một số tài nguyên (như là thời gian máy tính hoặc tiếp cận tới thư viện hoặc CSDL) vào quá trình phát minh đó.

1.5.1.2 Chủ sở hữu bản quyền (Copyright).

Sở hữu một bản quyền giống như sở hữu một sáng chế. Tác giả (nhà lập trình) được coi là chủ sở hữu của công trình, và chủ sở hữu có toàn quyền đối với

đối tượng. Tuy nhiên, một tình huống đặc biệt gọi là công trình cho thuê được áp dụng cho nhiều bản quyền đối với phát triển phần mềm hay các sản phẩm khác.

a) Công trình cho thuê (work for hire).

Trong tình huống này công trình cho thuê, người chủ thuê khoán, chứ không phải người nhận thuê khoán, sẽ được coi là tác giả của công trình. Công trình cho thuê thường không dễ phân biệt và nó phụ thuộc một phần vào luật lệ của quốc gia nơi diễn ra sự thuê khoán. Mối quan hệ giữa người nhận thuê khoán và chủ thuê khoán được coi là một công trình cho thuê nếu một số hoặc tất cả các điều kiện sau đây là đúng đắn. (Càng nhiều các điều kiện này là đúng đắn thì càng nhiều khả năng tình huống được xem là công trình cho thuê):

- Chủ thuê khoán có quan hệ quản trị (giám sát) xét duyệt dạng mẫu trong đó công trình sáng tạo được làm ra.
- Chủ thuê khoán có quyền sa thải người nhận thuê khoán.
- Chủ thuê khoán thu xếp để công trình được làm trước khi nó hoàn tất thiết kế (như là phản đối việc bán công trình đang tồn tại).
- Văn bản hợp đồng giữa chủ thuê khoán (bên A) và người nhận thuê khoán (bên B) ghi rõ rằng chủ thuê khoán đã thuê người nhận thuê khoán để làm công trình đó.

Trong tình huống, trong đó Edic phát triển một chương trình trên công việc của cô ta, chủ thuê khoán chắc chắn sẽ nói đó là công trình cho thuê. Do vậy, chủ thuê khoán sở hữu tất cả các quyền bản quyền và sẽ được đứng tên ở vị trí tác giả trong bằng bản quyền.

b) Các giấy phép (Licenses).

Trái ngược với công trình cho thuê, phần mềm cấp phép là sự thu xếp, trong đó nhà lập trình phát triển nó và vẫn là chủ sở hữu toàn bộ của phần mềm. Nhà lập trình nhượng cho công ty một giấy phép sử dụng phần mềm đó như là sự đền đáp về khoản phí mà công ty đã trả cho mình. Giấy phép có thể được bảo đảm trong một chu kỳ thời gian xác định hoặc vô hạn, cho một copy hoặc nhiều vô hạn, để sử dụng tại một hoặc nhiều địa điểm, dùng cho một hay tất cả các máy vào một hay nhiều lần. Sự thu xếp này là tiến bộ đáng kể đối với nhà lập trình, cũng giống như công trình cho thuê, giấy phép cũng rất có lợi cho chủ thuê khoán. Lựa chọn giữa công trình cho thuê và giấy phép chính là điều mà phần lớn do hai bên cùng thoả thuận.

1.5.1.3 Bảo vệ bí mật thương mại.

BMTM khác hẳn so với sáng chế và bản quyền ở chỗ không có nhà phát minh được đăng ký hoặc tác giả, không có cơ quan đăng ký cho BMTM (tức là không có bằng hoặc giấy chứng nhận cho BMTM). Trong sự việc BMTM bị lộ, chủ sở hữu BMTM có thể khởi kiện kẻ bộc lộ vì các thiệt hại phải chịu. Nhưng

trước hết, quyền sở hữu cần phải được xác lập vì rằng chỉ có chủ sở hữu BMTM mới có thể bị hại.

Công ty sẽ sở hữu các BMTM của các dữ liệu kinh doanh của riêng công ty. Nếu một bí mật mới được phát triển, thì công ty vẫn sẽ là chủ sở hữu. Ví dụ, một khi các vật thể mua bán đã được dự trữ, công ty có quyền BMTM đối với chúng, thậm chí nếu các vật thể đó còn chưa được hoàn chỉnh, toàn bộ, in ấn hoặc phân phối.

Cũng như là với bản quyền, chủ thuê khoán có thể viện dẫn về sự góp phần của ông ta vào phát triển các BMTM. Nếu BMTM của anh là một thuật toán tìm kiếm được cải tiến và phần việc của anh có bao gồm sự khảo sát và thử nghiệm các thuật toán tìm kiếm thì chủ thuê khoán của anh chắc chắn sẽ tuyên bố ít nhất là chủ sở hữu một phần của thuật toán mà anh muốn tiếp tục.

1.5.2 Các hợp đồng thuê khoán (HĐTK).

Hợp đồng thuê khoán thường chỉ rõ các quyền về sở hữu. Nhưng đôi khi nhà phát triển phần mềm và chủ sở hữu tiềm năng lại không có hợp đồng với nhau. Xác lập hợp đồng là cần thiết cho cả người nhận thuê khoán và chủ thuê khoán vì nhờ nó cả hai người sẽ hiểu rõ quyền và trách nhiệm của mình.

Thông thường, HĐTK chỉ ra rằng, người nhận thuê khoán sẽ được thuê để làm việc như nhà lập trình của riêng công ty. Công ty này tuyên bố rằng đây là tình huống công trình cho thuê. Công ty giành được tất cả các quyền đối với bất kỳ chương trình nào được phát triển, bao gồm các quyền về bản quyền và quyền tiếp thị. Hợp đồng này cũng có thể nói tiếp rằng, người nhận thuê khoán sẽ được phép tiếp cận tới các BMTM nhất định như là một phần của thuê khoán, và anh ta phải cam kết rằng không bộc lộ các bí mật này cho bất kỳ ai.

Một số HĐTK chặt chẽ hơn (đối với người nhận thuê khoán) gán cho chủ thuê khoán các quyền về tất cả các phát minh (sáng chế) và tất cả các công trình sáng tạo (bản quyền) không chỉ là chính bản thân những quyền suy ra trực tiếp từ công việc của người nhận thuê. Ví dụ, giả sử rằng, một người nhận thuê được thuê khoán như là một nhân viên kế toán cho một công ty (sản xuất) ô tô. Khi làm việc, nhân viên này phát minh ra một cách mới rất hiệu quả để đốt cháy nhiên liệu trong động cơ ô tô. Chủ thuê khoán cãi rằng, nhân viên đó đã sử dụng thời gian công ty để nghĩ ra vấn đề này, và vì thế công ty được toàn quyền đối với sản phẩm đó. HĐTK chuyển giao toàn quyền các phát minh cho chủ thuê khoán sẽ có thể có xu thế tăng cường hơn nữa.

Thoả thuận không cạnh tranh đôi khi cũng được đưa vào một hợp đồng. Người nhận thuê tuyên bố rằng anh ta đơn giản chỉ làm việc cho một chủ thuê khoán. Điều này sẽ làm cho người nhận thuê rất đắt giá đối với đối thủ cạnh tranh (của ông chủ thuê khoán). Người nhận thuê thoả thuận không cạnh tranh bằng

cách làm việc trong lĩnh vực tương tự sau khi thôi việc trong một khoảng thời gian nhất định. Ví dụ, một nhà lập trình, người có tài năng và uy tín rất cao trong thiết kế các hệ điều hành có thể được hiểu giống như một đại ca về kỹ thuật thiết kế hệ điều hành. Người nhận thuê này có thể nhớ lại những phần chính của một hệ điều hành đã có sở hữu và anh ta có thể viết ra một hệ điều hành tương tự cho đối thủ cạnh tranh trong thời gian ngắn. Để ngăn chặn điều này, chủ thuê khoán có thể đòi hỏi người nhận thuê không được làm việc cho đối thủ cạnh tranh (kể cả làm việc như một hợp đồng độc lập). Thoả thuận không cạnh tranh không phải là luôn luôn bắt buộc trong luật, ở một số nước, quyền của người nhận thuê để kiếm sống được đặt lên trên các quyền của chủ thuê khoán.

Câu hỏi và các chủ đề tiểu luận.

1) Hãy thử liệt kê và phân loại các tội phạm máy tính mà anh (chị) đã biết?
2) Các tội phạm máy tính (hoặc CNTT) ở Việt Nam trong những năm gần đây đã diễn ra như thế nào? Hãy kể về một số vụ đã xử gần đây nhất (về kinh tế như vụ Colony Invest, về chính trị như vụ phát tán các tài liệu chống phá Nhà nước, về văn hoá xã hội như vụ liên quan đến diễn viên của Nhật ký Vàng Anh...).
3) Hãy phân tịch rõ vai trò, vị trí của pháp luật ATTT trong hệ thống ATTT nói chung. Mục đích, ý nghĩa của pháp luật ATTT hiện nay ở Việt Nam như thế nào?
4) Trình bày về các dạng bảo vệ Bản quyền, Sáng chế và Bí mật thương mại và sự áp dụng chúng cho các đối tượng máy tính.
5) Trình bày về ba chế định bảo vệ thông tin sau đây:
   - Chế định hình sự và dân sự.
   - Chế định luật phạm lỗi (phạt hành chính).
   - Chế định hợp đồng.
6) Hãy trình bày về bản chất toàn cầu của luật pháp quy định về an toàn thông tin.
7) Vai trò của chính sách mật mã quốc gia trong pháp luật ATTT.

CHƯƠNG II ĐẠO ĐỨC HỌC TRONG AN TOÀN MÁY TÍNH

Mục đích cơ bản của chương này là chỉ ra một số vấn đề đạo đức học liên quan chặt chẽ với an toàn máy tính và làm rõ xem chức năng kiểm soát của đạo đực học trong an toàn máy tính quan trọng như thế nào.

2.1. Sự khác biệt giữa luật pháp và đạo đức học.

Như chúng tôi đã lưu ý ở trên, luật pháp không phải lúc nào cũng là cách phù hợp để xem xét các vấn đề hành vi của con người. Rất khó xác định một điều luật chỉ để ngăn ngừa các hậu quả mà ta mong muốn. Ví dụ, luật hạn chế súc vật tại các địa điểm công cộng cần phải sửa đổi chút ít để cho phép các con chó dẫn dắt người bị mù đi qua đó. Các nhà làm luật, họ không phải là các nhà làm máy tính chuyên nghiệp, rất khó bị buộc phải nghĩ về tất cả các loại trừ khi họ soạn thảo một bộ luật về các hoạt động điện toán. Thậm chí, cả khi luật đã được soạn thảo tốt và được viết ra hoàn hảo, thì sự thực thi nó cũng còn khó khăn. Tự bản thân luật không đi vào cuộc sống ngay được. Toà án bị quá tải, và khởi kiện các vi phạm tương đối nhỏ cũng phải mất rất nhiều thời gian và tiền của.

Như vậy, không thể và không thực tế để phát triển các luật nhằm mô tả và điều chỉnh tất cả các dạng hành vi mà xã hội chấp nhận. Thay vì điều đó, xã hội dựa vào đạo đức học (hoặc đạo lý) để đưa ra các chuẩn (mẫu) hành vi phù hợp được chấp nhận chung. (Ở đây các thuật ngữ đạo đức học và đạo lý được hiểu là tương đương). Đạo đức học là tiêu chuẩn được xác định khách quan về cái đúng và cái sai. Các tiêu chuẩn đạo đức thông thường là các nguyên tắc lý tưởng hoá vì rằng chúng tập trung vào một đối tượng. Trong một tình huống cụ thể, tuy nhiên, có thể bao gồm nhiều đối tượng đạo đức, vì thế con người phải lựa chọn hành vi phù hợp xem xét tất cả các đối tượng này. Mặc dù các nhóm tôn giáo và các tổ chức nghề nghiệp khuyến cáo các tiêu chuẩn nhất định về hành vi đạo đức, nhưng điều tối cần là mỗi cá nhân phải chịu trách nhiệm về quyết định phải làm gì trong mỗi tình huống cụ thể. Vì vậy, thông qua các lựa chọn của mình, mỗi chúng ta xác định một tập cá nhân các thử nghiệm đạo đức. Một tập các nguyên tắc đạo đức được gọi là một hệ thống đạo đức (hay hệ thống đạo lý).

Một đạo lý khác với một pháp lý trong một số điều quan trọng. Thứ nhất, pháp lý áp dụng cho tất cả mọi người: người ta có thể không đồng ý với nội dung hoặc ý nghĩa của một bộ luật, nhưng đó không phải là lý do để không tuân thủ bộ luật đó. Thứ hai, các toà án có quá trình điều chỉnh để xác định xem luật nào thay thế luật kia nếu hai luật mâu thuẫn nhau. Thứ ba, các bộ luật và các toà án sẽ phân biệt các hành vi nhất định, cái nào là đúng và cái nào là sai. Trên quan điểm pháp luật những gì không phi pháp là đúng. Cuối cúng, luật pháp có thể buộc thực thi để điều chỉnh các sai phạm đã thực hiện bởi hành vi vô luật.

Ngược lại, đạo đức là cá nhân (là riêng tư): hai người có thể có các quan niệm khác nhau trong việc đưa ra các phán xét đạo lý. Cái mà người này nhận

thấy hợp lý tuyệt vời, người khác lại có thể coi là không bao giờ nên làm. Thứ hai, các quan điểm đạo lý có thể và thường mâu thuẫn với nhau. Ví dụ, ý nghĩa cuộc sống con người là điều rất quan trọng trong hầu hết các hệ thống đạo lý. Hầu hết mọi người đều không muốn gây ra cái chết của ai đó, nhưng trong hoàn cảnh cần thiết bắt buộc một số người có thể chấp nhận sự hy sinh một người để cứu người khác hoặc cứu nhiều người khác. Giá trị của một cuộc đời không thể dễ dàng đo với giá trị của nhiều cuộc đời, và nhiều lời giải đạo đức phải được tìm ra cho sự mơ hồ chính đáng này. Vẫn chưa có người trọng tài cho các quan niệm đạo đức: Khi hai niềm tin đạo lý va chạm nhau, mỗi người phải chọn xem cái nào là quyết định. Thứ ba, hai người có thể tiếp cận các giá trị đạo đức một cách khác nhau, không tồn tại chuẩn vạn năng của đúng và sai trong các phán xét đạo đức. Không có ai lại đơn giản xem điều mà người khác đã làm như là chỉ dẫn lựa chọn cái đúng cho mình cả. Cuối cùng, không có sự bắt buộc nào trong lựa chọn về đạo lý cả. Sự khác nhau này được tổng hợp trong bảng sau:

Bảng 3: Sự tương phản của Luật pháp và Đạo đức học

Pháp luật	Đạo đức học
Diễn tả bằng các tài liệu viết chuẩn	Diễn tả bằng các nguyên tắc không thành văn
Minh chứng bởi toà án	Minh chứng bởi mỗi cá nhân
Xác lập bởi các thiết chế thay mặt mọi người	Đại diện bởi các triết gia, các tôn giáo, các nhóm nghề nghiệp
Áp dụng cho tất cả mọi người	Sự lựa chọn cá nhân
Sự ưu tiên được xác định bởi toà án nếu hai luật mâu thuẫn	Ưu tiên được xác định bởi cá nhân nếu hai nguyên tắc va nhau
Toà án là trọng tài cuối cùng của cái đúng	Không có trọng tài bên ngoài
Bắt buộc bởi cảnh sát và toà án	Bắt buộc rất hạn chế

2.1.1. Đạo đức học và tôn giáo.

Đạo đức học là tập hợp các nguyên tắc hoặc các chuẩn mực để phán xét cái đúng hoặc cái sai trong một tình huống cụ thể. Để hiểu được đạo đức học là gì, chúng ta có thể bắt đầu bằng việc cố gắng hiểu xem nó không là cái gì. Các nguyên tắc đạo đức khác với các tín ngưỡng tôn giáo. Tôn giáo dựa trên các ý niệm của con người về sự sáng tạo ra thế giới và sự tồn tại của các thế lực giám

sát hoặc thượng đế. Nhiều nguyên tắc đạo đức hoá thân trong các tôn giáo chính và cơ sở của tính đạo lý của con người chính là lòng tin và sự giác ngộ, điều hầu như giống như trong các tôn giáo. Tuy nhiên, hai người với các cơ sở tôn giáo khác nhau có thể tuân theo cùng một triết lý đạo đức, trong khi hai nhanh của cùng một tôn giáo có thể đạt tới các kết luận đạo đức trái ngược nhau trong một tình huống riêng. Cuối cùng, chúng ta có thể phân tích một tình huống từ một triển vọng đạo đức và đạt tới các kết luận đạo lý mà không cần phải viện tới bất kỳ một tôn giáo đặc biệt nào. Như vậy điều quan trọng là cần phân biệt đạo đức học với tôn giáo.

2.1.2. Đạo đức không phải là vạn năng.

Các giá trị đạo đức luôn biến đổi bởi xã hội và từ người này đến người kia trong khuôn khổ xã hội. Ví dụ, khái niệm riêng tư là rất quan trọng trong văn hoá phương Tây. Nhưng trong văn hoá phương Đông, riêng tư bị xem thường là vì người ta gắn riêng tư với việc có một thứ gì đó để che dấu. Không chỉ là khát vọng của người phương Tây về riêng tư đã không được hiểu thấu mà trên thực tế nó còn bao hàm nghĩa tiêu cực. Vì vậy, quan điểm của con người có thể bị ảnh hưởng bởi văn hoá và phong tục (nơi sinh ra). Các chuẩn mực hành vi cá nhân cũng chịu ảnh hưởng bởi các biến cố trong quá khứ cuộc sống. Mặc dù có những sự khác nhau này, các nguyên tắc phán xét về đạo đức vẫn giống nhau.

Những khía cạnh nêu trên của đạo đức học là hoàn toàn có lý và có thể hiểu được, nhưng nó vẫn làm cho con người không tin cậy vào đạo đức, vì rằng nó không được xây dựng trên các nguyên tắc cơ sở mà tất cả có thể chấp nhận. Mặt khác, những người có xuất thân từ tầng lớp khoa học và kỹ thuật thường tin vào sự chính xác và tính vạn năng.

Thuyết đa nguyên đạo đức công nhận hoặc chấp nhận rằng, trong một tình huống ứng xử cụ thể có thể có nhiều (hơn một) quan điểm về đạo đức cùng là đúng đắn (thậm chí như nhau). Chủ nghĩa đa nguyên là một cách thể hiện khác của ý niệm rằng, hai người có thể không đồng ý kiến nhau về mặt pháp lý đối với các vấn đề của đạo đức. Chúng ta chờ đợi và chấp nhận sự không đồng thuận ở đây cũng như trong các lĩnh vực khác như chính trị và tôn giáo.

Tuy nhiên, trong lĩnh vực khoa học và kỹ thuật, người ta thường mong muốn tìm ra các câu trả lời duy nhất, không mâu thuẫn và không đa nghĩa. Trong khoa học, một lời giải phải chính xác hoặc chứng minh được trong một số ý nghĩa nhất định. Khoa học đã cung cấp cho cuộc sống nhiều giải nghĩa cơ bản. Đạo đức học bị từ chối (hay bị hiểu lầm) bởi một số nhà khoa học vì rằng nó "mập mờ, đa nghĩa", tức là nó không có khung hình rõ ràng hoặc nó không dựa trên các chân lý cơ bản.

Chỉ cần nghiên cứu lịch sử của phát minh khoa học để thấy rằng, khoa học tự thân luôn được xây dựng trên các chân lý thời đại. Trong nhiều năm, Trái đất

đã được coi là trung tâm của hệ mặt trời. Ptôlêmê đã không phát hiện ra mâu thuẫn trong lý luận Địa tâm dựa trên chu kỳ quay của các hành tinh quan sát được. Cuối cùng, lý thuyết của ông đã bị thay thế bằng mẫu hành tinh Côpecnic lấy mặt trời làm tâm (Nhật tâm): các hành tinh quay quanh mặt trời. Tương tự, thuyết Tương đối của Anhxtanh đã mâu thuẫn với vật lý lượng tử cổ điển. Khoa học tràn đầy cảnh các lý thuyết từ nổi tiếng trở thành lạc hậu và các giả thuyết mới lại được đưa ra. Khi một lý thuyết mới đưa ra, một số người sẵn sàng chấp nhận giả thuyết mới, trong khi một số khác lại trung thành với cái cũ.

Nhưng cơ sở của khoa học phải luôn là "chân lý". Một số luận điểm phải được chúng minh là đúng, sai, hoặc không chứng minh được. Một luận điểm không bao giờ được cả đúng, cả sai. Các nhà khoa học cảm thấy bối rối với đạo đức học vì rằng, đạo đức học không cho ta sự phân biệt rạch ròi đúng, sai như vậy.

2.1.3. Đạo lý và lẽ phải.

Mọi người đều làm những phán xét đạo đức hàng ngày. (Mua các thứ ở nhà hàng bán lẻ tốt hơn hay là ở chỗ bán buôn? Hôm nay tôi sẽ ở nhà với gia đình hay đi chơi với bạn bè? Có thể chia xẻ các dữ liệu nhạy cảm cho người không có nghĩa vụ tiếp cận tới các dữ liệu đó không?). Vì rằng tất cả chúng ta đều bị thu hút vào sự lựa chọn các hành vi đạo đức, ta cần phải làm rõ xem, cần phải làm điều đó như thế nào để chúng ta có thể học cách áp dụng các nguyên tắc đạo đức trong các tình huống ứng xử nghề nghiệp giống như trong cuộc sống riêng tư hàng ngày.

Nghiên cứu đạo đức học có thể dẫn đến hai kết quả tích cực. Thứ nhất, trong những tình huống mà trong đó ta đã biết cái gì là đúng và cái gì là sai, đạo đức học sẽ có thể giúp ta lý giải sự lựa chọn của mình, tức là tìm được lẽ phải. Thứ hai, nếu ta không biết chọn hành vi đạo đức nào trong tình huống đó, thì đạo đức học có thể giúp ta phân biệt các hành vi bị dính líu vào, sao cho chúng ta có thể rút ra sự phán xét có lý, tức là ta rút ra được đạo lý ở đây.

2.1.2.1 Các bước kiểm tra một hành vi đạo đức.

Vậy có thể áp dụng các cơ sở của lựa chọn hành vi đạo đức vào an toàn máy tính như thế nào? Chúng tôi dẫn ra đây một số bước để rút ra và phản biện sự lựa chọn một hành vi đạo đức.

- Hãy hiểu rõ tình huống. Nắm vững các sự kiện của tình huống. Hãy đưa ra các câu hỏi để minh hoạ hoặc làm rõ. Thử cố gắng tìm xem, liệu có còn sự ảnh hưởng thích hợp nào chưa được xem xét tới.
- Hãy nắm một số lý thuyết về đạo lý và lẽ phải. Để lựa chọn hành vi, anh phải biết các hành vi này có thể được lý giải như thế nào.

- Hãy liệt kê các nguyên tắc đạo đức hàm chứa trong trường hợp. Những triết lý khác nhau nào có thể được áp dụng trong trường hợp này? Có cái nào trong các triết lý đó bao chứa những cái kia chăng?
- Hãy xác định xem những nguyên tắc nào trọng lượng hơn số còn lại. Đây là một đánh giá chủ quan. Nó thường bao gồm sự mở rộng nguyên tắc tới một kết luật lôgic hoặc sự xác định các tình huống trong đó một nguyên tắc này thay thế một nguyên tắc khác một cách rất rõ ràng.

Trong 4 bước này thì bước 1 và bước 3 là quan trọng hơn cả. Người ta rất thường xuyên phán xét một tình huống dựa trên các thông tin không đầy đủ, thực tế đó thường dẫn đến các phán xử trên định kiến, sự nghi ngờ hoặc nhầm lẫn. Sự xem xét tất cả các khía cạnh đạo đức khác nhau xuất hiện trong tình huống sẽ hình thành lên cơ sở để đánh giá trọng lượng của các lợi ích trong bước 4 nói trên.

2.1.2.2 Các nguyên tắc chính của đạo đức học.

Có hai trường phái khác nhau của đạo lý (sự có lý đạo đức): một dựa trên cơ sở điều thiện (điều tốt lành) thu được từ các hành vi và một dựa trên các trách nhiệm đương nhiên nhất định của con người.

a) Các nguyên tắc dựa trên hậu quả.

Thuyết mục đích của đạo đức học tập trung vào các hậu quả của hành vi. Một hành vi đạo đức lựa chọn là cái sẽ dẫn tới kết quả trong điều thiện tương lai lớn nhất và điều xấu nhỏ nhất. Ví dụ, nếu có một sinh viên trẻ hoặc một nghiên cứu sinh yêu cầu bạn viết cho anh ta một chương trình mà anh ta đã được phân cho ở lớp, bạn có thể xem xét đây là điều tốt (thiện) (anh ta sẽ hàm ơn bạn về sự quý mến), ngược lại đây là điều xấu (bạn có thể mắc vào cái bẫy làm cho bối rối và một hành vi vô nguyên tắc, cộng với việc bạn anh sẽ không học được các kỹ thuật cần thiết sẽ thu được từ việc viết chương trình này, trở thành thiếu hụt kiến thức). Các hậu quả tiêu cực ở đây rõ ràng là trọng lượng hơn mặt tích cực, và vì thế bạn từ chối yêu cầu của anh ta. Thuyết mục đích (Teleology) là tên gọi chung chỉ các lý luận về ứng xử mà tất cả đều hướng tới mục đích, đầu ra hoặc hậu quả của một hành vi đạo đức.

Có hai dạng quan trọng của thuyết mục đích: thuyết vị kỷ (egoism) và thuyết vị lợi (utilitarianism).

- Thuyết vị kỷ – Egoism là dạng thuyết cho rằng sự phán xét đạo đức trong mỗi tình huống được dựa trên cơ sở các lợi ích tích cực cho người lựa chọn một hành vi. Nhà vị kỷ (người ích kỷ) cân nhắc đầu ra của tất cả các hành vi có thể và chọn một hành vi sinh ra điều tốt lớn nhất cho anh ta (hoặc chị ta) với các hậu quả tiêu cực nhỏ nhất. Các ảnh hưởng đến những người khác không quan trọng. Ví dụ, một người vị kỷ thử đánh giá đạo lý của việc viết ra một mã máy tính tồi

(kém chất lượng) khi buộc phải làm trong một thời hạn có thể viện dẫn như sau: "Nếu tôi hoàn thành sản phẩm này một cách nhanh chóng, tôi sẽ làm vừa lòng sếp, ông ta sẽ mang lại cho tôi sự thăng tiến và các thứ tốt lành khác. Khách hàng có vẻ như không biết đủ sâu về chương trình đã được thông dịch, do đó tôi dường như sẽ không bị lên an gì. Uy tín của công ty tôi có thể bị suy giảm, nhưng điều đó không để lại dấu vết trực tiếp đến tôi. Vì vậy, tôi có thể lý giải được việc viết mã kém chất lượng này".

- Thuyết vị lợi (hay nguyên tắc Utilitarianism) cũng là một tiếp cận đánh giá về các kết quả tốt và xấu của mỗi hành vi đạo đức, nhưng nhóm đại diện ở đây là cả thế giới. Nhà vị lợi sẽ lựa chọn hành vi, mà nó sẽ mang lại lợi ích tốt tập thể lớn nhất cho tất cả mọi người với sự tiêu cực có thể nhỏ nhất (cũng) cho tất cả. Trong trường hợp nêu trên, nhà vị lợi sẽ cân nhắc lợi và hại cá nhân, lợi và hại cho công ty, lợi và hại cho khách hàng, và có lẽ lợi và hại cho cả xã hội. Ví dụ, một nhà phát triển thiết kế phần mềm để ghi nhận các bức xạ để lại các đám khói sẽ cần đánh giá các ảnh hưởng của nó lên sự hô hấp của mọi người. Nhà vị lợi này có thể nhận thức được lợi ích to lớn nhất cho tất cả mọi người, vì vậy bỏ ra thời gian đáng kể để viết ra một mã máy tính chất lượng cao, thay vì có thể chịu hậu quả cá nhân tiêu cực là làm mất lòng các sếp của mình.

b) Các nguyên tắc dựa trên quy định.

Một lý thuyết đạo đức khác là Đạo nghĩa học (Deontology). Đạo nghĩa học deontology được xây dựng trong ý nghĩa về nghĩa vụ, trách nhiệm của hành vi đạo đức. Nguyên tắc đạo lý này công nhận rằng, mọi thứ là tốt, là thiện trong và từ bản thân chúng. Các thứ mà là tốt một cách tự nhiên, sẽ là các luật lệ, quy định tốt, hoặc sẽ là các hành vi không đòi hỏi sự phán xét cao hơn (ý nói tự thân phản biện rồi). Một số thứ chính chúng là tốt, không cần phải phán xét về ảnh hưởng của chúng. Có thể ví dụ về các thứ tốt tự bản chất bên trong như sau:

- Chân lý, kiến thức, và quan niệm đúng về các loại khác nhau; sự hiểu thấu, tính khôn ngoan, sự thông thái.
- Sự phân chia đúng đắn về thiện và ác; công lý.
- Sự hài lòng, thoải mái, hạnh phúc, cuộc sống, sự giác ngộ.
- Hoà bình, an ninh – an toàn, tự do.
- Uy tín tốt, danh dự, sự quý trọng (kính mến), thương nhau, tình yêu, tình bạn, sự hợp tác, những ảo tưởng hay là những nhầm lẫn quan điểm tốt về mặt đạo đức.
- Vẻ đẹp, những cảm nhận thẩm mỹ (aesthetic experience).

Đạo nghĩa học dựa trên trách nhiệm là một trường phái đạo lý luôn tin rằng có tồn tại các luật lệ tối cao vạn năng, tự thân rõ ràng, tự nhiên quy định (quyết định) đạo đức riêng của chúng ta (cha mẹ sinh con, trời sinh tính). Có các nguyên

tắc đạo lý cơ sở nhất định được gắn liền với lý do trách nhiệm của con người đối với nhau. Những nguyên tắc đạo đức này thường được coi như các quyền: quyền được biết, quyền được riêng tư, quyền được thu nhập do làm việc. Có người đã liệt kê các trách nhiệm khác nhau, là phận sự đặt lên suốt sự tồn tại – hiện hữu của loài người:

- Sự trung thực, hay niềm tin chân lý.
- Sự sửa mình (reparation), trách nhiệm bồi thường vì hành vi xâm hại đã làm trước đó.
- Lòng biết ơn, sự đền ớn (đáp nghĩa) vì các dịch vụ trước đó hoặc các hành vi thân thiện.
- Sự công bằng, bác ái, sự phân phối hạnh phúc phù hợp với công tội.
- Từ thiện (làm phúc), bổn phận giúp đỡ người khác hoặc làm cho cuộc sống của họ tốt hơn.
- Không ác hiểm, không làm hại người khác.
- Sự tự hoàn thiện mình, luôn trở nên tốt hơn cả trong ý nghĩa tinh thần, cả trong ý nghĩa đạo đức (ví dụ, không thực hiện điều sai lần thứ hai).

Một trường phái khác của đạo lý được dựa trên các luật lệ mã mỗi cá nhân theo đuổi. Tôn giáo, sự học tập, sự từng trải, và sự phản ánh dẫn dắt mỗi con người tới một tập các nguyên tắc đạo đức cá nhân. Lời giải cho một vấn đề đạo đức sẽ được tìm ra bằng sự cân nhắc các giá trị trong khuôn khổ của những gì các nhân tin tưởng là hành vi đúng.

Chúng ta đã thấy các cơ sở của hai thuyết về đạo đức học: Thuyết dựa trên hậu quả và thuyết dựa trên quy định. Chúng tôi so sánh chúng trong bảng phân loại sau đây:

Bảng 4: Phân loại các Thuyết đạo đức học

Áp dụng / Lý thuyết	Cơ sở hậu quả	Cơ sở quy định
Cá nhân	Dựa trên các hậu quả đối với cá nhân	Dựa trên các luật lệ đòi hỏi bởi cá nhân từ tôn giáo kinh nghiệm và phân tích
Tổng hợp	Dựa trên các hậu quả đối với toàn xã hội	Dựa trên các luật lệ chung rõ ràng cho mọi người

Bây giờ chúng ta sẽ bắt đầu áp dụng các lý thuyết trên trong phân tích một số tình huống, xuất hiện trong đạo đức học an toàn máy tính.

2.2. Quyền riêng tư điện tử (Electronic Privacy).

Ở hầu hết các quốc gia, cá nhân được công nhận về riêng từ hoặc là bằng pháp luật hoặc là bằng tiền lệ mạnh. Quyền riêng tư có thể bị tước bỏ chỉ trong trường hợp về lợi ích tối thượng, như là ngăn chặn một tội ác hoặc bảo vệ quyền của những người khác. Quyền riêng tư thường được tuân thủ một cách rất nghiêm túc cả trong các toà án và cả về mặt cá nhân như là một căn cứ đạo đức.

Liên lạc điện tử vốn là một công nghệ mở hoàn toàn. Vì lý do hiệu quả, các tín hiệu của một cá nhân được lưu lại, được kết hợp, và chia xẻ với các tín hiệu của các người khác. Lại cũng vì hiệu quả, các tín hiệu này thường được lưu trữ và truyền đi ở dạng thức rất công khai. Mức độ mở này phần lớn có ngầm ý rằng, các liên lạc là mở cho sự xâm nhập của những người khác. Các vấn đề đạo đức đáng kể xuất hiện ở góc độ giới hạn cho phép người khác xâm nhập vào các liên lạc riêng tư.

2.2.1. Tính riêng tư của dữ liệu điện tử.

Henry L.Stimson, thư ký quốc gia của nước Mỹ năm 1929 đã nói một câu nổi tiếng: "Các quý ông không đọc thư của người khác". Đương nhiên là đúng, nhưng không phải ai cũng là quý ông (a gentleman). Vì vậy, an toàn thông tin vẫn bao gồm câu hỏi đạo đức về khi nào được coi là chính đáng việc tiếp cận các dữ liệu không thuộc về bạn.

Một lập luận cho là, bảo vệ là trách nhiệm của chủ sở hữu: những gì không được bảo vệ sẽ là mở cho tất cả. Quan điểm này dẫn tới sự tương tự về ngôi nhà: nếu cửa nhà không bị khoá, thì sẽ là đạo đức việc lẻn vào nhà và sục sạo lung tung hoặc lấy đi một vài thứ gì đó? Mọi người đều không nghĩ như vậy.

Một quan điểm có thể nữa về riêng tư, một số người trong nhóm quản trị có quyền pháp lý đối với các dữ liệu của các người mà họ quản trị. Trong ý nghĩa đó, người cha có quyền ghi nhận các dữ liệu của đứa trẻ con, người thầy giáo có quyền tiếp cận các file của cậu sinh viên, và người chủ thuê khoán được cho phép giám sát các người nhận thuê khoán. Ở đây nhiều người có thể đồng ý ít nhất ở một điểm. Tình huống cha – con có thể cho là đúng việc bảo vệ đứa trẻ khỏi các hành động xấu hoặc gây hại. Mặt khác, như một đứa trẻ trưởng thành, cậu bé sẽ làm các quyết định một cách độc lập, như vậy có thể lập luận rằng, cậu bé cần một mức độ riêng tư nào đó. Với các trường hợp thầy – trò và người chủ – người thuê, đạo tạo và công việc hoà lẫn với cuộc sống cá nhân. Người ta có thể viện dẫn rằng, người sinh viên hoặc người nhận thuê khoán hiện đang dùng các thiết

bị điện toán được trang bị, cần phải sử dụng chúng chỉ với mục đích mà vì nó các thiết bị này được giao cho họ, và do vậy tất cả sự sử dụng cần phải mở đối với sự giám sát. Trên thực tế, tuy nhiên, ở nhà trường và trên công việc, một lượng phải chăng các sử dụng cá nhân được ngầm hiểu là dư thừa (là chịu đựng được), và do vậy có thể là người quản trị không thể phân biệt được sự sử dụng riêng tư với sử dụng mở. Quan điểm đồng tình chung là tình huống bắt buộc: Trong một số tình huống, trở nên đủ quan trọng việc tiếp cận các dữ liệu mà không đếm xỉa gì đến các quyền cá nhân (ví dụ, nếu người làm thuê vắng mặt và một vài người rất cần một copy của bản báo cáo mà chỉ anh ta mới có, hoặc, nếu người thầy cần phải tìm ra bản copy một chương trình virút vừa mới ảnh hưởng xấu đến nhiều chương trình ở nhà trường). Trong các trường hợp loại này, quyền tiếp cận không phải là không bị giới hạn: chỉ được tiếp cận những gì mà nhu cầu của tình huống cần đến mà thôi. Tìm xem một báo cáo riêng không thể minh chứng cho việc đọc mọi từ ngữ ở bất kỳ file nào.

Như vậy là, tồn tại sự minh chứng có lý cho việc bỏ qua quyền riêng tư về dữ liệu điện tử của ai đó. Phía ngược lại của vấn đề này là, cũng tồn tại cơ sở để ngăn cấm tiếp cận.

2.2.2. Quyền riêng tư trong sử dụng mật mã.

Trong ví dụ trên, một chủ thuê khoán đi tìm bản báo cáo về ba bộ dây đeo kiếm có lẽ sẽ không có đủ chứng lý để mở một folder được đánh dấu "recipes" (các đơn thuốc) hoặc "financial data" (dữ liệu tiền bạc) và một hình cái khoá trên đó có chữ "PERSONAL" sẽ có thể loại trừ mọi giới hạn dù đó là những tìm kiến nghiêm chỉnh nhất. Trường hợp thông tin điện tử tương tự khoá "personal" nói trên sẽ là một file được mật mã hoá. Vậy sử dụng mật mã có thể lý giải như thế nào?

Có một vài trường hợp cần xem xét:

- Trong trường hợp giám sát, nếu người sinh viên hoặc người làm thuê nói trên được cho phép sử dụng các tài nguyên điện toán cho các mục đích cá nhân, thì người làm thuê có được mã hoá các dữ liệu cá nhân không?
- Người làm thuê có thể mã hoá các dữ liệu có quan hệ với công việc không?
- Chủ thuê khoán có thể mã hoã các dữ liệu để bảo vệ chúng đối với các đối tác cạnh tranh không?
- Có thể mã hoá các dữ liệu công dân riêng tư để bảo vệ chúng chống lại việc bị đọc bởi bất kỳ ai khác, kể cả nhà nước không?

Vấn đề then chốt trong tất cả các tình huống trên là ở chỗ, bảo vệ quyền lợi của ai và ở mức độ nào. Mã hoá loại trừ tiếp cận của người khác. Vậy lợi ích

riêng tư có đặt trên quyền lợi của loại trừ không? Trong trường hợp các dữ liệu liên quan đến công việc, nếu người làm thuê vắng mặt (đi họp, ốm hoặc vào ngày nghỉ chẳng hạn) thì sẽ có một sự phạt nặng (penalty) nếu chủ thuê khoán không thể tiếp cận được các dữ liệu công việc đó chỉ vì lý do chúng được mã hoá.

2.2.3. Uỷ nhiệm khoá mật mã (Cryptographic Key Escrow).

Có thể khắc phục mặt tích cực về tiếp cận bị giới hạn bởi mã hoá, nếu khoá mã được dành cho một nhóm tin cậy nào đó. Ví dụ, người làm thuê vẫn có thể bảo vệ một file nhạy cảm bằng mã hoá, nhưng anh ta trao một copy của khoá mã đó cho một ai đó mà có thể có như cầu tiếp cận tới file nhạy cảm này. Uỷ nhiệm khoá mật mã sẽ là phương tiện cho phép tiếp cận tới các dữ liệu mã hoá chỉ sau khi đã chứng minh được sự uỷ nhiệm này.

Các khía cạnh đạo đức gắn liền với uỷ nhiệm khoá mật mã là các công dân có thực sự buộc phải có khoá uỷ nhiệm khống và các nhân viên được uỷ nhiệm có thực sự xứng đáng không.

2.3. Một số ví dụ điển hình về đạo đức học máy tính.

2.3.1. Quyền riêng tư trong sử dụng các dịch vụ máy tính.

Đây là trường hợp liên quan tới việc quyết định xem, sử dụng thời gian máy tính như thế nào là phù hợp. Sử dụng thời gian máy tính là một vấn đề cả về tiếp cận bởi một cá nhân cả về khả năng sẵn có về chất lượng của các dịch vụ cho những người khác. Cá nhân này được cho phép tiếp cận tới các thiết bị tính toán để thực hiện một mục đích nhất định. Rất nhiều công ty dựa vào các chuẩn không thành văn về sự ứng xử, định hướng cho các hành vi của những ai có tiếp cận chính đáng (hợp pháp) tới một hệ thống điện toán. Các khía cạnh đạo đức học ở trường hợp này có thể giúp ta hiểu thấu về bộ chuẩn không thành văn nói trên.

2.3.1.1 Tình huống cụ thể.

Dave làm việc lập trình cho một công ty phần mềm lớn. Anh ta viết và kiểm thử các chương trình ứng dụng cho một nhà biên tập (compiter). Công ty của anh ta làm việc theo hai kíp tính toán. Ban ngày, sự phát triển các chương trình và các ứng dụng trực tuyến được chạy, ban đêm các công việc về lô sản phẩm được hoàn chỉnh. Dave vừa có tiếp cận tới các dữ liệu được tải xuống và nhận thấy rằng, các chạy lô ban đêm là bổ xung cho các nhiệm vụ lập trình ban ngày, vì thế việc tăng thêm công việc lập trình vào ca ban đêm sẽ không gây bất lợi tới làm việc của máy tính đối với những người dùng khác. Dave trở về sau những giờ (chuẩn) bình thường để làm một chương trình quản lý danh sách đầu tư chứng khoán của riêng mình. Sự tiêu hao trên hệ thống của anh ta là cực tiểu, và anh ra sử dụng rất ít các cung ứng đáng giá, như là giấy in. Hành vi ứng xử của Dave có đạo đức không?

2.3.1.2 Đánh giá các vấn đề.

Sau đây chúng ta liệt kê một số nguyên tắc đạo đức học chứa đựng trong trường hợp này.

- Quyền sở hữu các tài nguyên. Công ty sở hữu các tài nguyên tính toán và cung cấp chúng vì các nhu cầu tính toán của riêng công ty.
- Ảnh hưởng đến những người khác. Cho dù không mong muốn, một lỗi trong chương trình của Dave có thể ảnh hưởng có hại tới những người dúng khác, có thể thậm chí loại trừ dịch vụ của họ do sai sót hệ thống.
- Nguyên tắc suy diễn luận. Nếu hành vi của Dave là chấp nhận được, thì cũng sẽ là chấp nhận được đối với những người khác làm y như vậy. Tuy nhiên, quá nhiều người làm thuê làm vào ban đêm có thể làm giảm hiệu suất của hệ thống.
- Khả năng phát hiện, trừng phạt. Dave không biết rằng hành vi của anh ra đúng hay sai nếu công ty phát hiện ra. Nếu công ty quyết định rằng, đó là việc sử dụng không đúng, Dave có thể bị trừng phạt.

Còn những vấn đề khác nào trong trường hợp này? Những nguyên tắc nào quan trọng hơn cả?

2.3.1.3 Sự phân tích.

Nhà vị lợi có thể xem xét tất cả sự vượt trội của cái tốt trên cái xấu đối với mọi người. Dave thu được lợi ích từ việc dùng thời gian máy tính, mặc dù dành cho ứng dụng này lượng thời gian không lớn. Dave có khả năng bị trừng phạt, nhưng anh ta có thể cãi rằng do vô tình. Công ty không bị thiệt hại và cũng không được lợi gì. Như vậy nhà vị lợi có thể viện dẫn rằng việc sử dụng của Dave có thể là chính đáng.

Nguyên tắc suy diễn luận sẽ nhìn nhận: sẽ có vấn đề vì rõ ràng là nếu mọi người đều làm như Dave, chất lượng dịch vụ sẽ giảm sút. Nhà vị lợi sẽ cãi rằng mỗi người dùng mới phải cân nhắc lợi hại độc lập nhau. Sự dùng của Dave có thể làm máy tính quá tải, và tương tự như vậy Anna cũng không gây ra điều đó. Nhưng khi Bill muốn sử dụng máy, có thể khó khăn tương đối và như vậy Bill sẽ làm ảnh hưởng tới những người khác.

2.3.1.4 Các tình huống trái ngược.

Hãy tìm xem sẽ ảnh hưởng như thế nào tới đạo lý của tình huống nếu một trong bất kỳ hành vi hoặc đặc tính sau đây được xem xét:

- Dave đã bắt đầu kinh doanh quản lý danh sách chứng khoán cho nhiều người để thu lợi.

- Tiền lương của Dave thấp dưới mức sống trung bình, ngầm ý rằng Dave phải nhờ đến dùng máy tính để thu nhập thêm.
- Chủ thuê khoán của Dave đã biết về việc những người nhận thuê khoán khác đang làm điều tương tự và ngầm chấp thuận bằng việc không dừng họ lại.
- Dave đã làm việc trong một cơ quan nhà nước chứ không phải là công ty tư nhân và đã có lý rằng máy tính là thuộc về "nhân dân".

2.3.2. Từ chối dịch vụ (Denial of Service).

Đây là trường hợp nói về các vấn đề liên quan đến việc sự tính toán của một cá nhân ảnh hưởng đến các người dùng khác như thế nào. Trường hợp này tính tới những người có tiếp cận hợp pháp vì thế các kiểm soát tiếp cận chuẩn sẽ không ngăn cản họ. Tuy nhiên, vì lý do từ việc làm của ai đó, những người khác bị khước từ tiếp cận hợp pháp tới hệ thống. Vì vậy, tiêu điểm của trường hợp này là các quyền của tất cả các khách hàng.

2.3.2.1 Tình huống cụ thể.

Charlie và Carol là sinh viên ở Đại học tổng hợp, họ đang theo một chương trình về khoa học máy tính. Mỗi người phải viết một chương trình làm khoá luận. Chương trình của Charlie không may mắc phải một lỗi biên dịch và ngay tức khắc làm cho hệ thống tính toán ngừng trệ, toàn bộ các khách hàng bị mất hết các kết quả đang tính. Chương trình của Charlie dùng các đặc trưng chấp nhận được của ngôn ngữ; thông dịch mắc lỗi. Charlie đã không nghi ngờ là chương trình của anh ta có thể gây ra lỗi hệ thống. Anh ta báo cáo chương trình này cho Trung tâm điện toán và cố tìm cách để đạt được kết quả mong muốn của mình mà không thử kiểm tra lỗi hệ thống này.

Hệ thống tiếp tục bị treo theo chu kỳ, tất cả là 10 lần (sau lần ngưng trệ đầu tiên). Mỗi khi hệ thống bị ngưng trệ, đôi khi Charlie chạy được chương trình, nhưng đôi khi anh ta cũng không chạy được. Giám đốc nói chuyện với Charlie, và anh ta đã cung cấp tất cả các versions chương trình của mình cho nhóm chuyên gia tính toán của trung tâm. Các chuyên gia kết luận rằng, Charlie phải chịu trách nhiệm một phần chứ không phải tất cả trong lỗi ngưng trệ hệ thống do vô ý, rằng các lần cố gắng cuối để chạy chương trình khoá luận của Charlie một cách không mong muốn đã dẫn tới một số lỗi hệ thống phụ khác.

Trong sự phân tích tiếp theo, giám đốc trung tâm tính toán lưu ý thấy, Carol đã chạy chương trình của mình 8 (trong 10) lần đầu tiên mỗi khi hệ thống bị ngừng (theo chu kỳ). Giám đốc đã sử dụng quyền ưu tiên của nhà quản lý và đã kiểm tra các file của Carol và đã tìm được một file khai thác triệt để lỗi hệ thống giống hệt như chương trình của Charlie đã làm. Giám đốc ngay lập tức đình chỉ

sự tính toán của Carol, ngăn chặn tiếp cận của cô ta tới hệ thống máy tính. Vì điều này, Carol không thể hoàn thành được khoá luận của mình kịp thời hạn, cô ta nhận điểm D ở lớp và bị đuổi khỏi nhà trường.

2.3.2.2 Sự phân tích.

Trong trường hợp này sự lựa chọn khác nhau (đã được dựng lên cố ý) là không cần thiết. Tình huống ở đây được thể hiện như một kịch bản hoàn chỉnh. Nhưng khi nghiên cứu nó, nếu chúng ta muốn có các hành vi đối nghịch nhau, chúng ta cần đưa ra các thông tin phụ thêm. Ví dụ:

- Cần phải bổ sung thêm các thông tin gì?
- Ai là người có các quyền trong trường hợp này? Đó là những quyền gì? Ai là người có trách nhiệm bảo vệ những quyền đó? (Bước này trong đạo đức học thường làm rõ ai sẽ được xem như là nhóm trọng tài cho phân tích đạo nghĩa học).
- Charlie đã hành động một cách có trách nhiệm không? Bằng sự rõ ràng nào mà anh kết luận như vậy? Carol có làm thế không? Vậy cô ấy làm như thế nào? Giám đốc trung tâm đã hành động một cách có trách nhiệm không? Như thế nào?
- Những hành động gì khác mà Charlie hoặc Carol hoặc giám đốc có thể thực hiện để chúng có trách nhiệm hơn?

2.3.3. Chủ sở hữu các chương trình máy tính.

Trong trường hợp này, chúng ta xem xét người chủ sở hữu các chương trình: nhà lập trình, chủ thuê khoán, nhà quản lý, hoặc tất cả. Từ quan điểm luật pháp, hầu hết mọi quyền đều thuộc về người chủ thuê khoán như đã trình bày trong chương trước. Tuy nhiên, ở đây chúng ta đưa ra một vài căn cứ đối lập, có thể rất hữu ích khi nghiên cứu tình huống cụ thể. Như đã nói ở phần trên, các giám sát luật pháp đối với tính bảo mật của các chương trình có thể phức tạp, mất thời gian và đắt giá. Trong trường hợp này chúng ta nghiên cứu các giám sát đạo đức cá nhân, có thể thay vì khỏi cần đến hệ thống pháp luật.

2.3.3.1 Trường hợp cụ thể.

Greg là một nhà lập trình làm việc cho một hãng hàng không lớn, Star Computers, đang có nhiều hợp đồng nhà nước; Cathy là người quản trị (supervisor) của Greg. Greg đang thiết kế cho chương trình các loại thể hiện khác nhau (different simulations).

Để tăng cường khả năng của chương trình, Greg viết ra một số công cụ lập trình, ví như thiết bị tham chiếu chéo và một chương trình có thể trích tài liệu ra khỏi mã nguồn. Những thứ này không phải là nhiệm vụ thiết kế của Greg, anh ta

viết chúng một cách độc lập và dùng chúng trên công việc, nhưng không nói cho ai biết về chúng. Greg đã viết chúng vào buổi tối, ở nhà, dùng máy tính cá nhân của mình.

Greg quyết định tiếp thị (bán) các công cụ lập trình này đích thân. Khi Ban quản trị công ty Star nghe nói về điều đó, Cathy nhận được chỉ thị phải nói cho Greg rằng, anh ta không có quyền bán những sản phẩm này, vì khi được nhận thuê khoán, anh ta đã ký vào một tờ đơn, nói rằng tất cả các phát minh sẽ là sở hữu của công ty. Cathy không đồng ý quan điểm này vì rằng cô ta biết rằng Greg đã làm công việc này trên máy tính của riêng mình, ở nhà mình và vào buổi tối (thời gian riêng). Cô ta nói một cách miễn cưỡng cho Greg rằng anh không thể bán các sản phẩm đó. Cô cũng yêu cầu Greg cho cô ấy một bản copy các sản phẩm.

Cathy thôi việc cho công ty Star và giữ chân quản lý cho công ty Purple Computers, một đối tác cạnh tranh của Star. Cô ta mang theo bản copy các sản phẩm của Greg và phân phát nó cho những người cùng làm việc với cô. Các sản phẩm này tỏ ra rất thành công, chúng tăng cường đáng kể hiệu quả làm việc của những người nhận thuê khoán của cô ấy, và Cathy được công ty khen thưởng và nhận được một khoản tiền bồi dưỡng. Greg nghe được về điều này và tiếp xúc với Cathy. Nhưng Cathy quả quyết rằng, vì các sản phẩm đó được xác định là thuộc về công ty Star và vì Star đã làm việc phần lớn trên kinh phí nhà nước, các sản phẩm này trên thực tế đã thuộc lĩnh vực công cộng (dùng chung), và do đó chúng không thuộc về riêng một ai cả.

2.3.3.2 Sự phân tích.

Đây là trường hợp có nhiều ý nghĩa pháp lý cơ bản. Có lẽ, ai cũng có thể kiện người khác và, phụ thuộc vào số lượng tiền của và sức lực mà họ sẽ tiêu tốn trong các án phí, họ có thể theo đuổi toà án trong vài ba năm. Có lẽ, không có sự phán xét nào sẽ làm hài lòng tất cả.

Chúng ta hãy xếp các khía cạnh pháp lý sang bên và xem xét các vấn đề của đạo đức (đạo lý). Chúng ta muốn xác định xem, ai có thể làm điều gì, và những thay đổi gì có thể chấp nhận được để ngăn chặn sự rối rắm làm cho toà án khó giảm nhẹ.

Trước tiên, chúng ta vạch rõ các nguyên tắc đạo đức trong trường hợp.

- Các quyền: Những quyền gì của Greg, Cathy, của công ty Star và công ty Purple tương ứng?
- Căn cứ. Những quyền đó cho Greg, Cathy, Star và Purple cái gì? Những nguyên tắc "chơi đẹp", kinh doanh, quyền sở hữu, và còn nguyên tắc nào nữa gắn vào các trường hợp nào trong tình huống trên ?

- Ưu tiên: Cái nào trong các nguyên tắc này là thứ yếu so với số còn lại. Những cái nào được voi là ưu tiên (đứng trên)? (Lưu ý rằng, có thể rất khó so sánh hai quyền khác nhau, vì vậy kết quả của sự phân tích này có thể dẫn đến một số quyền là quan trọng nhưng không thể xếp thứ tự thứ nhất, thứ hai, thứ ba).
- Thông tin phụ: Các dữ kiện thực tế phụ nào bạn cần thiết để phân tích trường hợp này? Những giả định nào bạn định đưa ra để hoàn chỉnh sự phân tích này?

Tiếp đến, chúng ta muốn xem xét, những sự kiện nào dẫn tới tình huống được miêu tả và những hành động trái ngược nào có thể ngăn chặn được các kết quả tiêu cực.

- Những gì Greg có thể làm được khác đi trước khi bắt tay vào phát triển các sản phẩm của mình? Sau khi đang phát triển sản phẩm? Sau khi Cathy đã giảng giải rằng sản phẩm thuộc về Star?
- Những gì Cathy có thể làm khác đi khi cô ta được lệnh phải nói cho Greg rằng những sản phẩm đó thuộc về Star? Những gì Cathy phải làm khác đi để ngăn ngừa quyết định này bằng sự quản trị của mình? Cathy đã phải làm gì khác để ngăn chặn sự va chạm với Greg sau khi cô ta đã đến làm việc cho công ty Purple?
- Purple có thể làm gì khi biết rằng công ty này có được các sản phẩm từ Star (hoặc từ Greg)?
- Greg và Cathy đã có thể làm điều gì khác sau khi Greg đã nói với Cathy tại công ty Purple?
- Công ty Star đã phải làm gì khác để ngăn chặn Greg khỏi cảm nhận rằng anh ta là chủ sở hữu các sản phẩm của mình? Công ty Star đã phải làm gì để ngăn chặn Cathy mang các sản phẩm đó cho công ty Purple?

2.3.4. Truy cập các tài nguyên có chủ sở hữu.

Trong trường hợp này, chúng ta sẽ xem xét các vấn đề tiếp cận tới các tài nguyên có sở hữu hoặc bị hạn chế. Giống như trước, đây là trường hợp tiếp cận tới phần mềm. Tiêu điểm của trường hợp này là các quyền của một nhà phát triển phần mềm trong đối trọng với các quyền của các khách hàng, do vậy trường hợp này liên quan tới việc xác định các quyền truy nhập hợp pháp.

2.3.4.1 Trường hợp cụ thể.

Suzie sở hữu một copy của G-Whiz, một phần mềm đóng gói có chủ sở hữu mà cô ta đã trả tiền hợp pháp. Phần mềm này đã đăng ký bản quyền, và tài liệu

có chứa một giấy phép thoả thuận (license agreement) nói rằng, phần mềm này chỉ được dùng cho người trả tiền thôi. Suzie mời Luis cùng xem phần mềm để biết liệu nó có phù hợp với nhu cầu của anh ta không. Luis đến bên máy của Suzie và cô ấy biểu diễn phần mềm cho anh nhìn. Anh ta nói rất thích những gì đã nhìn thấy, nhưng anh ta muốn được thử kiểm nghiệm phần mềm lâu hơn nữa.

2.3.4.2 Các mở rộng đối với trường hợp.

Những hành vi đạo đức ở đây là rất rõ ràng. Những bước tiếp theo là ở chỗ nào các trách nhiệm đạo đức xuất hiện. Hãy lấy mỗi một trong các bước sau đây như một bước độc lập: nghĩa là không được giả định rằng bất kỳ một bước nào trong các bước còn lại đã xảy ra trong khi phân tích một bước cụ thể.

- Suzie đề nghị copy (sao chép) đĩa này cho Luis dùng.
- Suzie copy đĩa cho Luis dùng, và Luis dùng nó trong một khoảng thời gian nào đó.
- Suzie copy đĩa này cho Luis dùng, Luis dùng nó một thời gian và sau đó mua một copy tự mình.
- Suzie copy đĩa cho Luis thử suốt đêm, dưới một giới hạn rằng anh ta phải mang trả cô ấy vào hôm sau và phải không được copy nó cho bản thân. Luis đã làm như vậy.
- Suzie copy đĩa với giới hạn như trên, nhưng Luis vẫn làm một bản copy cho mình trước khi trả lại cho Suzie.
- Suzie copy đĩa với giới hạn như vậy, và Luis làm một copy cho mình, nhưng sau đó anh ta trả tiền bản copy này.
- Suzie copy đĩa với giới hạn như vậy, nhưng Luis không trả lại nó (bản sao) cho Suzie.

Với mỗi vấn đề mở rộng này, hãy miêu tả ai là người chịu tác động, những nguyên tắc đạo đức nào nằm trong tình huống, và những nguyên tắc nào thống lĩnh những cái còn lại.

2.3.5. Gian lận máy tính.

Trong những trường hợp trên, chúng ta tập trung vào những người, hành động trong các tình huống hợp pháp hoặc ít nhất cũng là có thể bàn cãi được (debatable). Trong trường hợp này, chúng ta xem xét sự gian lận ngoài luật, nhưng là bất hợp pháp. Tuy nhiên, trường hợp này trên thực tế rất hay xảy ra, khi người ta buộc phải làm những điều gian lận.

2.3.5.1 Trường hợp cụ thể.

Alicia là nhà lập trình làm việc trong một công ty. Ed, nhà quản trị của cô ta đề nghị cô viết một chương trình cho phép mọi người gửi trực tiếp các yêu cầu tới file kiểm toán của công ty ("The books"). Alicia biết rằng, các chương trình có tác động đến "the books", đều gồm các bước có trật tự, tất cả các bước đều phải kiểm toán. Alicia nhận ra rằng, với chương trình này, có thể xảy ra khả năng một cá nhân chèn các thay đổi vào số lượng chính của kiểm toán, và sẽ không có cách nào ghi dấu vết người đã làm sự thay đổi này (bằng sự phán xét nào hoặc khi nào).

Alicia đưa các vấn đề này ra với Ed. Anh ta đề nghị cô không nên đưa ra, rằng công việc của cô đơn giản là viết các chương trình như là anh ra đã chỉ dẫn. Anh ta nói rằng, anh ta cũng biết về sự dùng sai tiềm ẩn của các chương trình này, nhưng Ed biện minh yêu cầu của anh ta bằng lưu ý rằng, theo chu kỳ có một con số được đưa vào "the books" như lỗi nào đó và công ty cần có cách để sửa con số không chính xác này.

2.3.5.2 Sự mở rộng.

Trước tiên, chúng ta hãy làm rõ các lựa chọn mà Alicia có thể. Nếu Alicia viết chương trình này, cô ta có thể sẽ là đồng loã với sự gian lận. Nếu cô ta phàn nàn tới người quản trị của Ed, thì Ed hoặc người quản trị này có thể quở trách hoặc sa thải cô như một kẻ sinh sự. Nếu cô từ chối viết chương trình này, Ed có thể sa thải cô vì không thực thi nhiệm vụ được giao. Chúng ta thậm chí không biết rằng, chương trình này được thiết kế cho mục tiêu gian lận, Ed đưa ra một giải thích rằng, đó không phải là gian lận.

Cô ấy có thể viết chương trình nhưng đưa vào một mã ngoài, khả dĩ làm ra một log of mật, khi chương trình chạy, sẽ đưa ra người và những thay đổi đã được sinh ra. Extra file này sẽ cung cấp bằng chứng về sự gian lận, hoặc nó sẽ gây rắc rối cho Alicia nếu không có sự gian lận xảy ra nhưng Ed phát hiện được log mật này.

Ở đây, có mấy vấn đề đạo đức cần xem xét.

- Nhà lập trình phải có trách nhiệm về các chương trình do mình viết ra không? Lập trình viên có trách nhiệm về các kết quả của các chương trình đó không? (Trong khi chờ đợi câu trả lời này, hãy giả sử rằng chương trình đó là để điều chỉnh lại liều lượng trong một đơn thuốc được điều khiển bằng máy tính, và yêu cầu của Ed là tìm cách để làm chủ các chương trình giám sát để ngăn cản các liều lượng gây chết người. Khi đó Alicia phải có trách nhiệm về các kết quả của chương trình không).
- Nhà lập trình có hoàn toàn là kẻ làm thuê chỉ tuân theo mệnh lệnh (các nhiệm vụ được giao) một cách mù quáng (không suy nghĩ) không?

- Người nhận thuê khoán buộc phải chấp nhận mức độ mạo hiểm cá nhân nào (ví như sa thải có thể) vì thực hiện một hành vi mà anh ta hoặc cô ta nghĩ là không đúng?
- Chương trình để thao tác "the books" như miêu tả ở đây đã bao giờ được coi là hợp pháp chưa? Nếu vậy, trong những tình huống nào nó được coi là hợp pháp?
- Loại kiểm soát nào có thể được đưa vào những chương trình như vậy để các chương trình này là chấp nhận được? Bằng các cách nào mà một quản trị gia có thể yêu cầu một cách hợp pháp người thuê khoán viết ra một chương trình kiểu như vậy?
- Vấn đề đạo đức trong tình huống này sẽ có thay đổi không, nếu Alicia tự mình thiết kế và viết ra chương trình này?

2.3.5.3 Sự phân tích.

Nhà đạo nghĩa học – hành động sẽ nói rằng chân lý là đúng đắn. Vì thế, nếu Alicia nghĩ mục đích của chương trình đó là để lừa đảo, việc viết ra nó sẽ không phải là hành vi tốt. (Nếu mục đích là để học tập hoặc để nhận biết một mã tốt đẹp, thì viết nó có thể được minh chứng). Một phân tích có lợi hơn có thể xuất phát từ phía nhà vị lợi. Đối với Alicia việc viết chương trình đó mang lại thiệt hại có thể vì sẽ là đồng loã với gian lận, với cái lợi sẽ là có sự hợp tác với sếp của mình. Cô ta có được khoản gì đó có thể để mà làm giá với Ed, nhưng Ed cũng có thể quay ngoắt lại với cô và nói chương trình đó là ý tưởng của chính cô. Tựu trung cân bằng lại thì sự lựa chọn này tỏ ra có mặt tiêu cực lớn hơn.

Bằng việc không viết chương trình đó thì cái hại có thể của cô ta là có thể bị sa thải. Tuy nhiên, cô ta có cái lợi tiềm năng là có thể "thổi còi" đối với Ed. Sự lựa chọn này cũng không tỏ ra là mang lại nhiều tốt lành gì cho cô ta. Nhưng hành vi gian lận có những hậu quả tiêu cực cho các nhà đầu tư chứng khoán, các ngân hàng, và những nhà nhận thuê khoán vô tư khác. Không viết chương trình mang lại thiệt hại chỉ mình cá nhân Alicia. Còn việc đó lại có nhiều mặt tích cực lớn hơn.Có một khả năng khác nữa. Chương trình đó có thể không dùng cho mục đích gian lận. Nếu vậy, sẽ không có sự va chạm đạo đức. Vì thế Alicia có thể thử cố xác định xem các động cơ của Ed có phải là gian lận không.

2.3.6. Độ chính xác của thông tin.

Tiếp theo, chúng ta sẽ xem xét trách nhiệm về sự chính xác hay là sự toàn vẹn của thông tin. (Lưu ý, ở đây tác giả cho rằng accuracy = integrity). Một lần nữa, đây là vấn đề liên quan tới các hệ quản trị CSDL (DBMS) và các cơ chế kiểm soát tiếp cận khác. Tuy nhiên, như trong các trường hợp trước, ở đây là vấn

đề tiếp cận bởi người dùng hợp pháp (authorized: có uỷ quyền), vì vậy các kiểm soát không ngăn cấm tiếp cận.

2.3.6.1 Trường hợp cụ thể.

Emma là nhà nghiên cứu tại một Viện nghiên cứu, nơi mà Paul làm việc như một nhà lập trình thống kê. Emma viết một yêu cầu chuyển giao cho một nhà sản xuất ngũ cốc để ghi nhận giá trị dinh dưỡng của một loại ngũ cốc mới gọi là RawBits. Nhà sản xuất này tài trợ cho nghiên cứu của Emma. Emma không phải là nhà thống kê. Cô ta mang tất cả các dữ liệu của mình tới Paul để yêu cầu anh ta thực hiện các phân tích phù hợp và in ra các báo cáo cho cô ấy để gửi tới nhà sản xuất. Không may là, các dữ liệu mà Emma thu thập được dường như bác bỏ kết luận rằng RawBits là dinh dưỡng cao, và trên thực tế chúng có thể chứng tỏ rằng RawBits là có hại cho sức khoẻ. Paul cung cấp cho Emma các phân tích của mình nhưng cũng chỉ ra rằng, một vài điều chỉnh có thể được thực hiện khả dĩ có thể đưa RawBits lên vị trí sáng sủa hơn. Paul đưa ra một lưu ý hài hước về khả năng anh ta có thể sử dụng các thống kê để trợ giúp phía bên kia của bất kỳ vấn đề gì.

2.3.6.2 Các vấn đề đạo đức.

Rõ ràng là, nếu Paul thay đổi giá trị các dữ liệu thì anh ta đã hành động một cách vô đạo đức. Nhưng phải chăng là đạo đức hơn một chút đối với anh ta là đưa ra sự phân tích đúng các dữ liệu ở cách có thể hỗ trợ hai hoặc nhiều hơn các kết luận khác nhau? Liệu Paul phải có nghĩa vụ cung cấp cả hai phân tích tiêu cực và tích cực không? Paul có phải chịu trách nhiệm về việc sử dụng các kết quả của chương trình của anh ta bởi những người khác không?

Nếu Emma không hiểu được các phân tích thống kê, thì việc cô ta chấp nhận các kết luận tích cực của Paul có là đạo đức không? Các kết luận tiêu cực của Paul? Emma ý thức rằng, nếu cô đem các kết quả tiêu cực cho nhà sản xuất, người ta sẽ tìm ngay một nhà nghiên cứu khác để làm một nghiên cứu khác. Cô ta cũng ý thức rằng, nếu cô cung cấp cả hai tập kết quả cho nhà sản xuất , người ta sẽ chỉ công bố tập kết quả tích cực thôi. Nguyên tắc đạo đức nào hỗ trợ việc cô ta gửi cả hai tập dữ liệu? Nguyên tắc nào hỗ trợ việc cô chỉ gửi các dữ liệu tích cực? Cô ta còn có thể lựa chọn hành động nào khác nữa?

2.4. Các tiêu chuẩn đạo đức nghề nghiệp của một số tổ chức máy tính điển hình.

Ý thức được tầm quan trọng của các vấn đề đạo đức nghề nghiệp nhiều tổ chức máy tính đã chú trọng phát triển các tiêu chí đạo đức cho các thành viên của mình. Các tổ chức máy tính lớn, ví dụ như Hiệp hội máy tính (Association for Computing Machinery – ACM), Viện Kỹ sư Điện - Điện tử (Institute of Electrical and Electronics Engineers – IEEE) và Hiệp hội xử lý dữ liệu tự động

(Data Processing Management Association – DPMA) là các tổ chức đi đầu trong lĩnh vực này. Đã là thành viên của các tổ chức này không phân biệt năng lực, trách nhiệm hay kinh nghiệm trong điện toán đều tự nguyện tuân thủ bộ tiêu chuẩn đạo đức ứng xử nghề nghiệp của tổ chức. Vì lý do đó, các tiêu chí đạo đức trong những tổ chức này cơ bản chỉ là cố vấn, khuyên nhủ. Tuy vậy, các tiêu chuẩn này là những xuất phát điểm rất tốt cho các phân tích về đạo đức học.

2.4.1. Tiêu chí đạo đức của IEEE.

IEEE đã đưa ra một bộ tiêu chuẩn đạo đức cho các thành viên của mình. IEEE là tổ chức của các kỹ sư, không chỉ giới hạn trong lĩnh vực điện toán. Vì thế chuẩn mực đạo đức học của họ rộng hơn chút ít so với những gì có thể trông đợi cho an toàn máy tính, nhưng các nguyên tắc cơ bản hoàn toàn áp dụng được cho các tình huống điện toán. Nội dung của bộ tiêu chí này được trình bày trong bảng sau đây:

Chúng tôi, các thành viên của IEEE, trong sự giác ngộ về tầm quan trọng của các công nghệ của chúng tôi ảnh hưởng tới chất lượng cuộc sống trên toàn thế giới, và trong sự ý thức trách nhiệm cá nhân đối với nghề nghiệp, đối với các đồng nghiệp và đối với các cộng đồng mà chúng tôi phục vụ, chính bằng văn bản này cam kết cư xử theo phong cách nghề nghiệp và đạo đức cao nhất và đồng ý:

---

1) Có tinh thần trách nhiệm trong việc đưa ra các quyết định công nghệ phù hợp với sự an toàn, sức khoẻ, và phúc lợi của cộng đồng, và làm rõ một cách phù hợp các nhân tố có thể gây nguy hiểm cho cộng đồng hoặc môi trường.

2) Tránh các va chạm thực tế hoặc trông thấy của các quyền lợi ở bất cứ nơi nào có thể, và chỉ rõ cho các phía chịu tác động khi mà chúng tồn tại.

3) Có danh dự và thực tiễn trong phát biểu các khẳng định hoặc những đánh giá dựa trên các dữ liệu chắc chắn.

4) Từ chối sự hối lộ dưới tất cả các hình thức.

5) Nâng cao hiểu biết về công nghệ, ứng dụng phù hợp của nó, và các hệ quả tiềm năng.

6) Duy trì và nâng cao năng lực kỹ thuật của mình và chỉ đảm nhận các nhiệm vụ công nghệ khi đã được qua đào tạo hoặc đã có kinh nghiệm, hoặc sau khi làm rõ tất cả các giới hạn thích hợp.

7) Tìm kiếm, chấp nhận và đưa ra sự phê phán có danh dự về công vụ kỹ thuật, tìm hiểu và chỉnh sửa các lỗi, và trả công xứng đáng các đóng góp của những người khác.

8) Cư xử công bằng với tất cả mọi người, không quan tâm tới các yếu tố như màu da, tôn giáo, đẳng cấp, khuyết tật, tuổi tác hoặc xuất sứ.

9) Tránh làm tổn hại người khác, sở hữu của họ, uy tín hoặc công việc của họ bằng hành vi lừa dối hoặc gian lận.

10) Cộng tác với các đồng nghiệp và những người cùng làm việc trong sự phát triển chuyên môn của họ và hỗ trợ họ trong việc theo đuổi bộ tiêu chuẩn đạo đức này.

2.4.2. Tiêu chuẩn đạo đức nghề nghiệp của Hiệp hội Máy tính (Hoa kỳ) (ACM: Association for Computing Machinery).

Bộ tiêu chí đạo đức của ACM nêu lên ba loại trách nhiệm cho các thành viên của mình: các yêu cầu đạo lý chung, các trách nhiệm nghề nghiệp, và các trách nhiệm quản lý, lãnh đạo, gồm cả trong nội bộ và trong xã hội. Bộ chuẩn đạo đức này có ba phần (có thể coi phần cam kết là phần bốn) như sau:

Là một thành viên của ACM Tôi sẽ….

1.1. Đóng góp cho xã hội và sự mưu sinh của con người.

1.2. Không làm hại người khác.

1.3. Có lòng tự trọng và trung thực.

1.4. Công bằng và cư xử không phân biệt chủng tộc.

1.5. Tôn trọng các quyền sỡ hữu kể cả các bản quyền và sáng chế.

1.6. Trả tiền xứng đáng cho sở hữu trí tuệ.

1.7. Tôn trọng tính riêng tư của những người khác.

1.8. Đề cao sự bảo mật.

Là một nhà chuyên nghiệp điện toán của ACM Tôi sẽ…

1.1. Cố gắng đạt được chất lượng, hiệu quả, và tính chân thực cao nhất cả trong suốt quy trình và cả trong các sản phẩm của công việc chuyên môn.

1.2. Yêu cầu và giữ vững năng lực chuyên môn cao.

1.3. Hiểu biết và tuân thủ các pháp luật đang tồn tại liên quan tới công việc chuyên môn.

1.4. Nhận và cung cấp các báo cáo chuyên môn phù hợp.

1.5. Đưa ra các đánh giá tăng cường và xuyên suốt về các hệ thống máy tính và các thành phần của nó, bao gồm cả sự phân tích các rủi ro có thể.

1.6. Tôn trọng các hợp đồng, các thoả thuận và các trách nhiệm được giao.

1.7. Nâng cao sự hiểu biết công cộng về điện toán và các hệ quả của nó.

1.8. Tiếp cận (truy nhập) các tài nguyên điện toán và liên lạc khi và chỉ khi được uỷ quyền làm việc đó.

Là một thành viên của ACM và là một người lãnh đạo của tổ chức Tôi sẽ…

1.1. Diễn đạt rõ ràng (công khai – minh bạch) các trách nhiệm xã hội của các thành viên của đơn vị tổ chức và khuyến khích sự thừa nhận đầy đủ các trách nhiệm này.

1.2. Quản trị nhân sự và các tài nguyên.

1.3. Hiểu rõ và hỗ trợ việc sử dụng đúng đắn và có uỷ quyền các tài nguyên liên lạc và điện toán của tổ chức.

1.4. Cần chắc chắn rằng, các khách hàng và những người chịu tác động bởi hệ thống có các nhu cầu đã được diễn đạt một số cách rõ ràng trong quá trình đánh giá và sắp xếp các đòi hỏi, sau đó hệ thống này phải được chứng nhận là đáp ứng các đòi hỏi đó.

1.5. Công khai, minh bạch và hỗ trợ các chính sách bảo vệ sự chân thực của các khách hàng và những người chịu tác động của mỗi hệ thống điện toán.

1.6. Kiến tạo các khả năng (điều kiện) cho các thành viên của tổ chức hiểu biết các nguyên tắc và các giới hạn của các hệ thống máy tính.

Là một thành viên của ACM, Tôi sẽ…

1.1. Đề cao và tuân theo các nguyên tắc của tiêu chuẩn đạo đức này.

1.2. Coi các vi phạm tới bộ tiêu chuẩn này là trái với tư cách thành viên trong ACM.

2.4.3 Tiêu chuẩn đạo đức của Viện đạo đức học máy tính (Computer Ethics Institute – CEI).

Viện đạo đức học máy tính CEI là một tổ chức phi lợi nhuận có mục đích khuyến khích mọi người xem xét các khía cạnh đạo đức trong các hoạt động điện toán của mình. Viện này được thành lập từ giữa những năm 1980 như một liên doanh của IBM, các viện Brucking, và Tập đoàn thần học Washington. CEI đã

công bố chỉ dẫn đạo đức của mình dưới dạng mười mệnh lệnh về đạo đức máy tính như sau:

1) Ngươi không được sử dụng máy tính để làm hại người khác.
2) Ngươi không được can thiệp vào công việc điện toán của người khác.
3) Ngươi không được rình rập quanh các files máy tính của người khác.
4) Ngươi không được dùng máy tính để ăn cắp.
5) Ngươi không được dùng máy tính để sinh ra các bằng chứng giả.
6) Ngươi không được sao chép (copy) hoặc sử dụng phần mềm có chủ sở hữu mà không trả tiền.
7) Ngươi không được dùng các tài nguyên máy tính của người khác mà không có uỷ quyền hoặc không trả tiền phù hợp.
8) Ngươi không được chiếm đoạt kết quả trí tuệ của người khác.
9) Ngươi phải suy ngẫm về những hậu quả xã hội của mỗi chương trình mà ngươi viết ra hoặc của hệ thống mà ngươi thiết kế.
10) Ngươi phải luôn sử dụng máy tính theo cách sao cho các đồng nghiệp trẻ kính trọng và noi theo.

Nhiều tổ chức lựa chọn đạo đức học một cách rất nghiêm túc và đưa ra tài liệu chỉ dẫn sự ứng xử cho các thành viên của mình hoặc những người nhận thuê khoán. Một số tập đoàn, công ty yêu cầu những người làm thuê mới phải đọc chuẩn đạo đức của mình và ký vào đơn xin hứa tuân thủ chúng. Những chuẩn mực này rất hữu ích cho các bạn như là hình mẫu các hành vi ứng xử nghề nghiệp. Trên cơ sở nghiên cứu chúng bạn có thể soạn thảo cho mình một bộ chuẩn mực đạo đức riêng, phản ánh các ý tưởng của bạn về sự cư xử phù hợp trong các tình huống tương tự. Chuẩn mực đạo đức có thể giúp bạn đánh giá các tình huống một cách nhanh nhạy và hành động theo cách thức phù hợp, tự nhiên và có đạo lý.

Câu hỏi và các chủ đề thảo luận, tiểu luận.

1) Hãy làm rõ các nhân tố ủng hộ hoặc chống lại ý kiến rằng, việc sau đây sẽ là hành vi đạo đức:

Anh và vài người bạn quyết định chia sẻ các bản nhạc từ các đĩa CD. Anh copy một số bản vào máy tính của mình và sau đó làm rối loạn các bản copy giống vậy của các bạn khác.

Nhân tố này có thay đổi gì không nếu sự trao đổi được thực hiện với người không quen biết qua một dịch vụ chia sẻ các file ngầm định?

2) Hãy phân tích các lập luận về ý kiến rằng, việc sau đây sẽ là một hành vi đạo đức:

Khi đến thăm một người bạn ở một thành phố khác, anh mở máy tính xách tay của mình và bộ không dây của anh nhận được một tín hiệu mạnh về một điểm truy cập không an toàn có tên là Siren – island. Anh kết nối với nó và sử dụng truy cập Internet suốt cả ngày chủ nhật.

Tình huống có thay đổi gì không nếu khoảng thời gian không phải là chủ nhật mà là không giới hạn (anh không chỉ khi thăm mà cả khi trở về) và điểm truy cập này rõ ràng liên quan đến một người đang sống ở biệt thự liền kề đó?

3) Một người quen của anh có một Blog mà, mặc dù nó không trực tiếp liệt kê trên trang chủ của cô ta, anh cũng vẫn tìm thấy nhờ một vài thủ thuật tìm kiếm đơn giản. Trong Blog của mình cô ấy miêu tả một số tình tiết rất hấp dẫn về mối quan hệ của cô ta với một người bạn khác của anh. Hãy giải thích các khía cạnh đạo đức của:

   a) Việc anh đọc Blog này.

   b) Việc anh kể lại điều đó cho người thứ hai.

   c) Việc anh kể cho các bạn biết về điều đó.

   d) Việc anh gửi một liên kết tới Blog đó từ trang chủ của mình.

CHƯƠNG III GIỚI THIỆU MỘT SỐ LUẬT PHÁP AN TOÀN THÔNG TIN CỦA CÁC NƯỚC

Trong chương này chúng tôi sẽ giới thiệu một số luật trong lĩnh vực ATTT của Mỹ và Châu Âu, các quốc gia đi đầu về vấn đề liên quan. Trọng tâm là các luật của Mỹ, và như đã nói trên, đó là các luật được mở rộng cho các đối tượng mới trong kỹ thuật điện toán như chống tội phạm máy tính, bảo vệ chương trình và dữ liệu, kiểm soát các tiếp cận, bảo vệ người dùng… Những thiết chế cũ vẫn phù hợp như các vấn đề sở hữu trí tuệ đã được nói kỹ ở chương I sẽ không được nhắc lại ở chương này. Cuối chương có giới thiệu ngắn gọn về các luật liên quan của một số nước khác.

3.1. Luật pháp ATTT chọn lọc tại Mỹ.

3.1.1. Vài nét về thể chế và kinh doanh ở Mỹ.

3.1.1.1 Thể chế nước Mỹ.

a) Hiến pháp Hoa kỳ (USC – United States Constitute).

Hiến pháp Mỹ xây dựng trên chủ thuyết tam quyền phân lập, phân quyền giữa hành pháp, lập pháp và tư pháp. Các cơ quan nhà nước tương ứng là Tổng thống, Quốc hội và Toà án được trao cho những quyền lực có xác định giới hạn rõ ràng. Mỗi ngành có thẩm quyền nhất định để kiểm tra các ngành khác, dựa trên hàng loạt các phương tiện kiểm tra, điều chỉnh để bảo đảm các ngành không có sự lạm quyền. Quyền lực chính phủ còn bị hạn chế hơn nữa bởi hệ thống chính quyền kép, theo đó, chính quyền liên bang chỉ được trao quyền và trách nhiệm để đối phó và giải quyết các vấn đề cả nước (ngoại giao, thương mại, kiểm soát quân đội và hải quân…). Trách nhiệm và nghĩa vụ còn lại của chính phủ được giao cho chính quyền mỗi bang.

Điều V Hiến pháp cho phép những sửa đổi trong Hiến pháp (khi được thông qua bởi hai phần ba đa số của cả hai viện Quốc hội và được phê chuẩn của ba phần tư cơ quan lập pháp của các bang). Hiến pháp được mười ba bang phê chuẩn năm 1791 đã có mười tu chính án, được gọi chung là Tuyên ngôn Dân quyền (tự do tín ngưỡng, ngôn luận và báo chí…), để bảo vệ công dân trước sự chuyên chế nếu có của chính quyền liên bang. Cho đến nay, Hiến pháp đã có hai mươi sáu tu chính án.

b) Tổng thống (U.S. President).

Tổng thống (bất cứ công dân nào được sinh ra tại Mỹ, ít nhất 34 tuổi) được bầu ra cho một nhiệm kỳ bốn năm và chỉ có thể tái cử một nhiệm kỳ nữa (tu chính án 22 - được thông qua bốn nhiệm kỳ liên tiếp của Tổng thống Franklin, D.Roosevelt). Tổng thống vốn được dự tính chỉ hơn một ít so với người đứng đầu một bang, cũng như Tổng tư lệnh Quân lực, nhưng do tham gia ngày càng tăng ở chính quyền liên bang trong đời sống kinh tế của quốc gia và vai trò nổi bật trên

trường quốc tế, trong đó thường cần sự bí mật và sự nhanh chóng làm tăng vai trò quan trọng của chức vụ Tổng thống đối với Quốc hội.

Ngày nay, Tổng thống đề nghị một chương trình lập pháp mặc dầu Tổng thống, Nội các và các thành viên không phải và cũng không thể là nghị sĩ Quốc hội. Điều này có nghĩa là chính các nghị sĩ Quốc hội là người đệ trình các dự luật cho Hạ viện và Thượng viện. Hậu quả là Tổng thống hoàn toàn không có quyền lực khi gặp phải một Quốc hội bất hợp tác. Vì vậy, khó đảm bảo rằng các luật đã được thông qua sẽ được bộ máy hành chính liên bang thực thi có hiệu quả. Người ta nói rằng quyền lực thật sự duy nhất của Tổng thống là quyền thuyết phục.

Vai trò của Phó Tổng thống không được xác định rõ trong Hiến pháp. Hiến pháp chỉ cho Phó Tổng thống quyền chủ trì cuộc tranh luận ở Thượng viện và chỉ được biểu quyết trong trường hợp có ràng buộc. Tuy nhiên, Phó Tổng thống sẽ nắm quyền Tổng thống trong trường hợp Tổng thống chết, từ nhiệm hoặc lâm bệnh. Đến nay đã có tám trường hợp như vậy. Để cố gắng lôi kéo những người có khả năng vào chức vụ không quan trọng chủ yếu mang tính nghi thức này, gần đây Phó Tổng thống được trao thêm một số nhiệm vụ quan trọng trong công việc ngoại giao.

c) Quốc hội (Congress).

Ngành lập pháp của chính quyền quốc gia gồm hai viện – Thượng viện và Hạ viện, mỗi viện có vai trò, quyền lực và thủ tục bầu cử khác nhau.

- **Hạ viện.**

Hạ viện là một cơ quan năng động của chính quyền liên bang. Các bang được đại diện trên cơ sở dân số và được chia thành các khu vực bầu cử có quy mô gần bằng nhau (khoảng 520.000 người). Có 435 Hạ nghị sĩ, cư hai năm bầu một lần. Tất cả các bang phải chọn theo luật hệ thống, một khu vực bầu một người theo lối bỏ phiếu đa số đơn giản. Nếu khuyết Hạ nghị sĩ do chết, từ nhiệm… thì bổ sung bằng cuộc bầu cử phụ.

Chủ tịch Hạ viện, được Viện bầu lên và có trách nhiệm quan trọng, khiến ông có ảnh hưởng đáng kể đối với Tổng thống. Hơn nữa nếu Tổng thống và Phó tổng thống chết trước khi chấm dứt nhiệm kỳ, thì ông Chủ tịch Hạ viện trở thành Tổng thống.

- **Thượng viện.**

Thượng viện là một đối trọng bảo thủ, đối với Hạ viện có tính bình dân hơn. Từ năm 1913 (điểm sửa đổi lần thứ 17), mỗi bang có hai Thượng nghị sĩ, được bầu trực tiếp theo cách do cơ quan lập pháp mỗi bang quyết định. Sáu năm bầu Thượng nghị sĩ một lần, nhưng bầu cử xen kẽ nghĩa là một phần ba số Thượng nghị sĩ được bầu hai năm một lần. Nếu khuyết thượng nghị sĩ do chết hoặc từ nhiệm, thì trong khi chờ đến cuộc bầu cử quốc hội Thống đốc bang sẽ chỉ định

người thay thế. Hiện nay có 100 Thượng nghị sĩ. Thượng viện có một đặc quyền là tranh luận không bị hạn chế để bảo vệ quyền lợi của thiểu số, nhưng điều này đã làm cho một nhóm nhỏ Thượng nghị sĩ có thể ngăn cản việc thông qua một dự luật (bằng cách nói dông dài).

Mặc dầu có thể làm ra các điều luật nhưng nhiệm vụ quan trọng nhất của Quốc hội là xem xét các chính sách, hành động của các cơ quan hành pháp, và bảo đảm quyền lợi của các bang và các quận. Thật vậy, vì Hạ nghị sĩ và Thượng nghị sĩ phụ thuộc vào cử tri tại các bang, các khu vực bầu cử để được tái cử họ có xu hướng đáp ứng quyền lợi riêng của từng khu vực bầu cử, từng nhóm người hơn là giải quyết các vấn đề của cả nước. Quốc hội cũng kiểm soát nền tài chính quốc gia và một đội ngũ chuyên gia thường trực giúp Quốc hội xem xét và thay đổi ngân sách hàng năm do Tổng thống đưa ra.

d) Thẩm phán liên bang.

Trong hệ thống liên bang có 90 Toà án cấp quận do chánh án quận chủ toạ. Toà này xét xử các vụ án hình sự vi phạm luật liên bang và các vụ án dân sự về các vấn đề liên bang (tranh chấp giữa các bang, không đóng thuế liên bang…). Người ta có thể kháng án lên Toà Phúc thẩm nước Mỹ, có ba thẩm phán xét xử các kháng án, nhưng trong những vụ án rất quan trọng thì có chín thẩm phán xét xử. Trong đại đa số vụ án, quyết định của Toà Phúc thẩm là chung quyết và đặt ra một án lệ cho các trường hợp về sau, mặc dầu án lệ này không phải lúc nào cũng ràng buộc Tối cao Pháp viện.

Mặc dầu không nói rõ là được quyền xét lại một bản án – quyền quyết định hành động của Tổng thống, của Quốc hội hay của Chính quyền các bang có vi phạm Hiến pháp hay không - Đây là một vai trò quan trọng và Tối cao Pháp viện thường gồm chín vị (mặc dầu quốc hội có thể thay đổi con số này), do Tổng thống bổ nhiệm suốt đời sau khi được Thượng viện phê chuẩn.

e) Chính quyền bang.

Trong Hiến pháp đề cập rất ít đến Chính quyền bang – Tu chính án thứ mười (1791), chỉ đơn thuần nói rằng những quyền nào không được giành riêng cho Chính quyền liên bang thì thuộc về Chính quyền bang. Trong khi Hiến pháp của 50 bang rất lớn, chúng đều dựa trên sự phân quyền và một hệ thống kiểm tra và điều chỉnh, cùng nhấn mạnh quan niệm của người Mỹ là chính quyền giữ ở mức tối thiểu. Mỗi bang có Thống đốc, cơ quan Lập pháp và Toà án bang. Thống đốc được bầu qua bầu cử toàn bang. Tất cả các bang trừ bang Nebraska có cơ quan lập pháp lưỡng viện, thường được gọi là Thượng nghị viện và Hạ nghị viện.

Cấu trúc và thủ tục hệ thống toà án bang của các bang khác nhau rất lớn. Tuy vậy, nói chung, ở cấp thứ nhất có Tư pháp, các Toà hoà giải xét xử các vụ vi phạm nhỏ, do thẩm phán trị an (qua bầu cử) điều khiển. Lên nữa là Toà án của Hạt, nơi xét xử phần lớn các vụ án dân sự và hình sự. Kháng án được gửi đến Toà Phúc thẩm cấp quận, trong khi Tối cao Pháp viện của hệ thống các bang, khía

cạnh gây tranh cãi nhiều nhất của thẩm phán bang là do bầu cử (kể cả thẩm phán trong Tối cao Pháp viện).

3.1.1.2 Kinh doanh ở Mỹ.

Nhiều tư liệu lịch sử còn ghi nhận rằng vào đầu thể kỷ 19, lục địa Bắc Mỹ mà sau này là nước Mỹ vẫn còn nhiều vùng hoang vu, thưa thớt dân cư nhưng chỉ sau 50 năm và nhất là từ khi Hợp chủng Quốc chính thức ra đời, lượng người nhập cư vào Mỹ gia tăng rõ rệt. Trong thành phần những công dân mới có đủ loại người, người đi tìm vàng hoặc đi tìm vùng đất có nhiều cơ may hơn, người trốn pháp luật truy tố, người đi giảng đạo, người đi buôn, người làm thuê đi theo chủ… Dù thuộc thành phần nào chăng nữa, mong muốn chung của họ là xây dựng một cuộc sống mới đầy đủ hơn, tốt đẹp hơn so với trước đây. Nói chung, trong tay họ không có bao nhiều gia sản, nhiều người chỉ có đôi bàn tay trắng, thậm chí một câu tiếng Anh cũng không biết nhưng họ có ý chí, nghị lực và sức lao động. Họ hiểu rõ rằng trên mảnh đất với nhiều ưu đãi của thiên nhiên nơi đây, nếu chịu khó lao động, cuộc sống sung túc chẳng bao lâu sẽ đến. Quả thật, những người Mỹ thuộc thế hệ tiên phong (tính theo lịch sử Hợp Chủng Quốc) là những người rất yêu lao động, sẵn sàng đổ mồ hôi để đổi lấy thành quả lao động của mình. Chính vì vậy, họ luôn có ý thức và tham vọng cải tiến lao động để nhận được giá trị to lớn hơn. Họ rất chịu khó tìm tòi, vận dụng các phương pháp lao động cho kết quả tốt hơn, đỡ chi phí và khi cảm thấy không đạt được mục tiêu đã đặt ra trong lĩnh vực này, họ táo bạo bắt tay và công việc ở lĩnh vực khác để thử sức với số mệnh. Tóm lại, họ là những con người năng động nhất, giàu nghị lực nhất, có óc tiến thủ nhất trong thời đại của họ.

Người Mỹ rất biết giá trị lao động do họ tạo ra và nó phải được lượng hoá bằng tiền. Làm ra tiền, kiếm tiền là động lực thúc đẩy mọi người vận động nhanh hơn, căng thẳng hơn, cuồng nhiệt hơn so với xứ khác. Muốn thu được tiền, kiếm được nhiều lợi nhuận, một mặt ta phải ráo riết bươn chải, chạy đua với thời gian, với đối thủ cạnh tranh để có hàng hoá và dịch vụ tốt hơn, mặt khác cần tỉnh táo để không phải chi phí quá mức từ nguyên liệu, công sức tới tiền bạc. Các tính toán sòng phẳng đến chi li cho mọi việc bất kể đối với ai, từ người thân trong gia đình tới bạn hữu đã tạo cho người Mỹ một đặc điểm riêng: đó là tính thực dụng.

Có vô số thí dụ để nói về việc vận dụng tính thực dụng trong sản xuất kinh doanh, trong cả hoạt động nghệ thuật, giáo dục và trong gia đình. Người Mỹ luôn mong muốn đồ vật mình làm ra càng có nhiều chức năng càng tốt, cho dù các chức năng có thể bị áp đặt, khiên cưỡng, trái với quan niệm thông thường. Nếu mái nhà được tận dụng làm sân phơi, làm bãi đỗ xe hơi là chuyện đã quen thuộc ở nhiều nước hoặc tổ chức quán ăn đủ món ngay tại tầng trệt của nhà hát cũng được nhiều nước vận dụng thành quen dần, nhưng vào một điểm bán thuốc Tây mà có thể mua được nhiều thứ ngoài thuốc, kể cả hàng thực phẩm ăn liền, cũng có thể ngồi cà kê uống cà phê hay uống trà thì điều này khó thấy ở nước khác.

Chính tính thực dụng đã sớm đẩy người Mỹ lao vào hoạt động dịch vụ. Ngay từ cuối thể kỷ 19, khi nền công nghiệp non trẻ của Mỹ còn chưa đạt được trình độ công nghệ để vượt qua được các nước tư bản lọc lõi, già dạn kinh nghiệm như Anh, Pháp, Đức, các nhà sản xuất Mỹ đã tâm niệm rằng sản xuất ra hành hoá mới chỉ là một giai đoạn của quá trình kinh doanh, do đó muốn kinh doanh thành công, phải chú ý tốt các khâu hỗ trợ cần thiết để hàng hoá đến tay người tiêu thụ nhanh hơn, nhiều hơn. Muốn vậy phải biết chào hàng, săn đón khách hàng, giúp đỡ khách hàng xử lý các trục trặc kỹ thuật có thể xảy ra, cung cấp các phụ tùng thay thế hoặc trang bị phụ… Tóm lại, phải quan tâm chiều ý khách hàng, coi "khách hàng là thượng đế" phải luôn tâm niệm rằng "khách hàng bao giờ cũng đúng", có như vậy mới bán được hàng và thu được lợi nhuận. Một khi khách hàng đã bước vào gian hàng, lập tức họ săn đón, giới thiệu hàng hoá mà chưa cần biết họ có mua hay không. Dù khách hàng không mua gì, nhân viên bán hàng vẫn luôn niềm nở và vui vẻ tạm biệt để hy vọng khách hàng còn quay lại khi khác. Còn nếu khách có vẻ ưng ý một mặt hàng nào đó, người bán hàng sẽ hồ hởi làm theo mọi yêu cầu của khách hàng vì họ đã nhuần nhuyễn phương châm "một đơn hàng – một hợp đồng – một trách nhiệm" từ đơn giản và rẻ tiền như hộp xi đánh giày tới phức tạp và tốn tiền như chiếc xe hơi, khách hàng đều có cơ hội thử và được hướng dẫn sử dụng hết sức tận tình. Ở vị trí người bán hàng, hoặc phải bán cho đủ định mức đã giao trong ngày, hoặc bán được bao nhiêu thì hưởng hoa hồng bấy nhiêu nên những người bán hàng cố gắng thuyết phục cho được khách hàng của mình. Người bán hàng Mỹ cũng hay sử dụng những tiểu xảo như hàng còn rất nhiều nhưng nói chỉ còn một chiếc duy nhất, khách hàng thử tuy không đẹp lắm nhưng vẫn khen đẹp hết lời, hàng đang ế ẩm nói hàng đang bán chạy… do đó người mua cũng phải cảnh giác với những lời chào ngọt ngào, dù đã thử hàng rồi nhưng nếu không hài lòng thì kiên quyết chối từ.

Cùng một loại hàng hoá, giá bán ở các cửa hàng có thể khác nhau nên những người cẩn thận phải rẽ qua vài ba chỗ để khảo giá. Nói chung, giá cả được ghi rõ trên tấm phiếu gắn với hàng hoá, nếu món hàng được giảm giá thì trên tấm phiếu được ghi cả giá gốc và giá mới. Hàng mua rồi thường không được trả lại, song có thể đổi lấy cái khác với giá tương ứng hoặc nhận một tấm phiếu mua hàng ghi rõ số tiền đã trả để khi khác mua cũng được.

Gần vào những dịp lễ, các cửa hàng liên tiếp tung ra các mặt hàng mới rất hấp dẫn để mong thu được doanh số cao song giá cả thì không rẻ. Những người ít tiền thường chọn những ngày hàng bán "sôn" để đi chợ (thí dụ trong một tuần, cửa hàng lương thực thực phẩm có quy định ngày thứ tư giảm giá thịt, thứ sáu giảm giá gạo) hoặc mua hàng vào ngày cuối cùng vì theo thông lệ, cuối tháng hàng tồn kho được giảm giá. Đối với những người nghèo chờ tới cuối mùa hoặc sau ngày lễ lớn mới mua cũng vì lúc đó hàng hoá được giảm giá mạnh. Bên cạnh việc mua hàng trả chậm, được áp dụng đối với hàng hoá đắt tiền (chừng vài trăm USD trở lên). Layaway là hình thức bán hàng kiểu tín dụng ngắn hạn, tức là

thông qua một hợp đồng khế ước, người mua hàng chỉ phải trả ngay khoảng 10 – 15% số tiền, phần còn lại sẽ trả nốt trong vòng 30 ngày. Cũng có khi thông qua bảo lãnh của một công ty tài chính, người ta có thể tậu được xe hơi, đồ gỗ sang trọng, máy giặt, tủ lạnh, TV… mà không phải trả ngay số tiền lớn, thay vào đó là việc trả góp hàng tháng. Lại có hình thức hợp đồng thuê mua, theo đó có thể có ngay hàng hoá mong muốn để dùng, ví dụ xe hơi chẳng hạn, nhưng chừng nào còn chưa trả góp đủ thì vẫn chưa có quyền sở hữu mà chỉ có quyền sử dụng mà thôi.

Dịch vụ sau bán hàng ở Mỹ rất chu đáo. Ngay sau khi khách hàng lựa chọn được món hàng ưng ý, họ sẽ được hướng dẫn sử dụng tận tình và tiếp đó, hàng sẽ được bao gói cẩn thận, trang trí thêm nơ hoặc bướm nếu khách muốn. Nếu khách hàng không muốn lấy hàng ngay mà muốn được đem hàng đến tận nhà thì việc đem hàng đến nhà, dù bằng đường bưu điện thì vẫn là bổn phận và nghĩa vụ của người bán hàng. Người bán hàng sẵn sàng nhận lấy công việc rầy rà đó mà thường không đòi thêm phụ phí. Những năm gần đây, dịch vụ mua hàng qua điện thoại và qua máy vi tính rất phát triển vì tiết kiệm được nhiều thời gian và công sức cho người tiêu dùng. Có thể những nội dung dịch vụ đó hiện nay đã trở thành nếp chung của thế giới nhưng phải ghi nhận rằng người Mỹ đã thực hành chúng sớm nhất, đồng thời nước Mỹ trong những thập niên gần đây phát triển với tốc độ nhanh hơn hẳn các ngành sản xuất, vừa để đáp ứng nhu cầu trong nước vừa xuất khẩu được bình quân mỗi năm gần 60 tỷ USD (đứng đầu thế giới) để đổi lại lượng dịch vụ nhập khẩu từ các nước khác với giá trị tương đương.

Từ những đòi hỏi ngày càng khắt khe, khó tính của khách hàng, yêu cầu dịch vụ quay lại tác động tới sản xuất khiến sản xuất phải đa dạng hơn. Các nhà sản xuất Mỹ từ lâu đã quan niệm rằng khi sản phẩm của họ được bày bán trên thị trường thì đó mới chỉ là một nửa nghĩa vụ đối với người tiêu dùng. Nửa còn lại là tiếp tục điều chỉnh tính năng của sản phẩm, cung cấp thêm các trang bị phụ và các phụ tùng thay thế, hướng dẫn sử dụng sản phẩm đạt được mức độ thuận tiện nhất, an toàn nhất. Quan niệm này không chỉ cho phép nhà sản xuất thu được doanh số cao nhờ kích thích được người tiêu dùng mua nhiều sản phẩm chính của họ, mà còn thu thêm được số tiền không nhỏ, có khi bằng doanh thu sản phẩm chính, do bán được nhiều sản phẩm phụ và làm dịch vụ sau khi bán hàng.

Thuật ngữ "chìa khoá trao tay" ngày nay đã trở nên quen thuộc đối với mọi người, làm người ta chẳng còn chú ý đến ai là người đã phát kiến ra và sử dụng no đầu tiên. Không ai khác, chính người Mỹ đã nảy ra phương thức chuyển giao kỹ thuật một cách đầy đủ, trọn gói, với tính chất dịch vụ tối đa gọi là phương thức " on turn key" trong ngành xây dựng từ ngay sau chiến tranh thế giới thứ hai. Họ nhận bao thầu các công trình xây dựng có quy mô lớn, bảo đảm trong một thời gian nhất định sẽ bàn giao đủ mọi thứ, từ hồ sơ thủ tục, các tài liệu tính toán thiết kế tới hồ sơ kiểm tra chất lượng công trình, tài liệu hướng dẫn sử dụng, bảo trì và tất nhiên là có chuyên gia huấn luyện tay nghề cho tới khi người đặt

hàng hoàn toàn có đủ khả năng làm chủ được công trình. Để hoàn thành khối lượng công việc đa dạng và phức tạp tại công trường xây dựng, những người nhận thầu chịu trách nhiệm thuê mướn nhân công, mua sắm thiết bị, vật liệu và bằng nghệ thuật tổ chức công việc khéo léo, họ thúc đẩy tiến độ thực hiện công trình, rà soát kỷ luật lao động nghiêm ngặt, tính toán bù trừ các thương vụ sao cho đảm bảo được các cam kết đã ký trong hợp đồng và nhờ đó, thu được lợi nhuận tổng cộng rất lớn. Phương thức "chìa khoá trao tay" sau đó được vận dụng rộng rãi ở Tây Âu, rất phổ biến trong hoạt động chuyển giao công nghệ từ các nước tư bản chủ nghĩa sang các nước đang phát triển.

Khi thanh toán mua bán hàng hoá hay trả công dịch vụ, người dân các nước công nghiệp phát triển ít dùng tiền mặt mà thay vào đó là sử dụng ngân phiếu hoặc thẻ tín dụng. Thẻ tín dụng cũng là một phát kiến độc đáo của người Mỹ từ giữa thập niên 20 của thế kỷ XX. Công ty đầu tiên lập ra phương pháp thanh toán bằng thẻ là General Petroleum Corporation of California để mua xăng dầu gọi là nó là Gasonline Credit Card. Tuy vậy, cũng phải trải qua nhiều pha thăng trầm, tới những năm 50, thẻ tín dụng mới tìm được chỗ đứng vững nhờ việc gắn thêm những chức năng thanh toán tại các nhà hàng, khách sạn, quầy bán vé phương tiện vận tải, cửa hàng bán lẻ mà đi đầu trong việc thử nghiệm là các hãng Diners Club, American Express, Carte Blanche của Mỹ. Từ việc sử dụng ngày một rộng rãi tấm thẻ tín dụng, sau này, người Mỹ còn sáng chế được nhiều loại máy chuyên tự động kiểm tra thanh toán, kiểm tra tiền giả, đổi tiền, ứng tiền trước... và chúng được bố trí tại các địa điểm công cộng để dân chúng tiêu dùng.

Tính cách kinh doanh hiện đại của người Mỹ:

Người Mỹ ngày nay nói chung được nhìn nhận là cởi mở, thẳng thắn, khá nồng nhiệt và dễ dàng tạo lập quan hệ bạn bè. Tính cách ấy một phần bắt nguồn từ xuất xứ, một phần do ảnh hưởng của các quan hệ xã hội. Không chỉ ưa thích chuyện trò với nhau một cách tự nhiên thoải mái, người Mỹ có thể mạnh dạn khơi màn bắt chuyện với người hoàn toàn xa lạ. Người nước ngoài tới Mỹ đôi khi ngạc nhiên vì trên máy bay, tại bến chờ xe buýt hoặc trong một tiệm ăn trưa có người Mỹ xa lạ cười với mình một cách thân thiện, song nếu người đó cười lại rất có thể đó là khởi đầu của một đối thoại thú vị. Người Mỹ quan niệm giao tiếp xã hội ít nhất cũng tạo cho người ta cảm giác vui vẻ, dễ chịu, còn nhiều hơn là thu nhận được những hiểu biết mới về con người, về thế giới. Chính vì vậy, thanh thiếu niên Mỹ được quan tâm dạy dỗ cách giao tiếp với mọi người, cách nói chuyện lịch sự và cách giữ cho các cuộc đối thoại trôi chảy, không bị gián đoạn, cũng không để cho người đối thoại với mình ở vào thế bí hoặc e dè, thiếu tự nhiện khi trò chuyện. Tuy nhiên, nếu một người quá huyên thuyên nói hết cả phần đáng ra để cho người khác nói thì người đó bị đánh giá là ích kỷ. Ngược lại, người nào nói quá ít thì bị cho là thiếu ý thức trách nhiệm, không có tinh thần tập thể và đó là biểu hiện bất lịch sự. Nếu trong cuộc gặp gỡ có nhiều gương mặt mới, mọi người đều thấy mình có bổn phận phải tự giới thiệu ngay từ những

phút đầu tiên với người khách chưa quen biết. Một khi đã ngồi bên cạnh với một người mới xuất hiện, trách nhiệm của người chủ hoặc người đã có mặt từ trước là phải chủ động giới thiệu hoặc nói chuyện, giúp cho người tới sau còn xa lạ với bầu không khí chung không bị "khớp". Cũng như người Âu, người Mỹ rất tránh những câu hỏi về đời tư, ví dụ như bao nhiêu tuổi, tại sao chưa lập gia đình, sao ly dị, tại sao không có con, tại sao đầu bị hói, vì sao không đi lễ nhà thờ, lương tháng bao nhiêu...

Một điểm đáng chú ý của người Mỹ là họ rất có tinh thần tôn trọng pháp luật. Mọi mối quan hệ cá nhân với cá nhân, cá nhân với chính quyền, công ty này với công ty khác nếu có trục trặc là rất có thể được xem xét tại toà án, phán xử tại toà án. Vì vậy, người ta nói không đâu trên thế giới này nhiều toà án như Mỹ, cũng không đâu nhiều luật sư như ở Mỹ. Nếu ở Tây Âu, mua bảo hiểm còn có việc thuê luật sư vì trong tâm lý, người ta luôn ám ảnh có thể bị kiện cáo bất cứ lúc nào và nếu không có người biện hộ tin cậy, có thể bị thua thiệt bất ngờ vì những duyên cớ không lường trước được. Sự hiện diện của giới luật sư, một mặt có tác động tốt cho việc bảo vệ công lý, mặt khác cũng gây ra những sự phiền nhiễu, hao tiền, tốn của. Mặc dù vậy, người Mỹ có thể không tin vào chính phủ, không tin thậm chí cả cha mẹ, anh chị, vợ con, nhưng có một người duy nhất bao giờ cũng được tin cậy hoàn toàn, đó là luật sư riêng của họ. Chính vì luật sư là nghề được trọng vọng, lại có thu nhập ổn định nên hàng năm có khoảng 40.000 người thi lấy bằng luật để ra làm luật sư.

Người Mỹ biết tôn trọng lời hứa. Nếu nhận thấy điều gì có thể làm được, họ hứa và thực hiện cho được những điều gì cảm thấy khó khăn, không cho phép hứa hẹn thì họ trả lời "không" nhưng lại tìm cách tránh né. Chính vì vậy, khi bị người khác thất hứa, người Mỹ có thể giận dữ và huỷ bỏ quan hệ.

Trong bữa ăn tại nhà hàng, được dịch vụ chu đáo, ân cần của các nhân viên bồi bàn, người ta ăn uống rất tự nhiên, thoải mái, không kiểu cách, khách sáo. Người Mỹ uống rượu mạnh và hút thuốc nhiều. Hút thuốc trong bữa ăn tại nhà hàng là điều bình thường, không bị cấm đoán. Nói vậy không có nghĩa là không có những phép tắc lịch sự tối thiểu cần được tôn trọng.

3.1.2. Những luật về tội phạm máy tính.

3.1.2.1 Luật về gian lận và lạm dụng máy tính (Computer Fraud and Abuse Act).

Đây là luật gốc liên bang, Điều 18 Hiến pháp Hoa kỳ, mục 1030, đưa vào năm 1984, từ đó được bổ sung vài lần. (Luật này nghiêm cấm xâm nhập, làm hỏng và truy nhập trái phép). (Để vắn tắt ta viết như sau: 18 U.S.C.§ 1030, 1984, CFAA).

– Cố gắng định vị tội phạm máy tính trong một đạo luật hoàn chỉnh.

– Luật này đưa ra khái niệm "máy tính được bảo hộ" có định nghĩa là một máy tính:

"(A) chỉ dùng riêng cho cơ quan tài chính hoặc Chính phủ Mỹ, hoặc, trong trường hợp nó không được dành riêng cho sử dụng như vậy, được dùng bởi hoặc cho cơ quan tài chính hoặc Chính phủ Mỹ và trong việc xem xét các tác động vi phạm hiến pháp được dùng bởi hoặc cho cơ quan tài chính hoặc Chính phủ Mỹ;

hoặc

(B) dược sử dụng trong thương mại hoặc liên lạc toàn Liên bang hoặc ngoại thương, kể cả máy tính để ở ngoài nước Mỹ mà được sử dụng theo cách ảnh hưởng đến thương mại hoặc liên lạc toàn Liên bang hoặc liên lạc của nước Mỹ".

– Bao gồm 7 loại hành vi bị cấm:

1) Truy nhập trái phép tới máy tính đang chứa các dữ liệu về quốc phòng, quan hệ quốc tế hoặc các dữ liệu hạn chế của Chính phủ liên bang.

2) Truy nhập trái phép tới máy tính chứa các thông tin nhất định về tài chính và ngân hàng.

3) Truy nhập trái phép, sử dụng, xuyên tạc (thay đổi), thay đổi cấu trúc, hoặc làm lộ về máy tính hoặc thông tin trong máy tính làm việc nhân danh và vì lợi ích của Chính phủ Mỹ.

4) Sự truy nhập không có cho phép một "máy tính được bảo hộ", mà toà án hiện đang chỉ định đối với bất kỳ máy tính nào đó được kết nối với Internet.

5) Các gian lận máy tính.

6) Lan truyền các mã gây hại các hệ thống máy tính hoặc các mạng.

7) Buôn bán các mật khẩu máy tính.

– Các hình phạt bao gồm từ 5.000 đến 100.000 USD, hoặc hai lần giá trị thu được bởi hành vi phạm pháp, đôi khi còn cao hơn, hoặc phạt tù từ 1 năm đến 20 năm, hoặc cả hai.

3.1.2.2 Luật bảo vệ các liên lạc điện tử (Electronic Communications Privacy Act – ECPA).

18 U.S.C.§2510 – 2221, 1986, ECPA. (Luật này nghiêm cấm các can thiệp bất hợp pháp và sự tiết lộ các liên lạc điện tử được truyền tải hoặc lưu cất trong các mạng).

– Bổ xung mở rộng các điều luật liên bang về chống nghe trộm các liên lạc "miệng" và "giấy" bằng các truyền tải thông thường.

Mở rộng sự bảo vệ tới "các liên lạc điện tử" – Khái niệm quan trọng này được định nghĩa như là "bất kỳ sự truyền tải nào của các ký hiệu, các tín hiệu, chữ viết, hình ảnh, âm thanh, dữ liệu, hoặc kiến thức của bất kỳ ai khác được truyền toàn bộ hoặc từng phần bằng hệ thống vô tuyến, hữu tuyến, điện tử, điện quang hay quang học, mà tác động tới thương mại toàn liên bang hoặc ngoại thương", - loại trừ "các liên lạc giấy và miệng", "sự ghi nhận chỉ âm sắc", "thiết bị ghi dấu vết", và "thông tin chuyển tiền điện tử" được lưu giữ và được bảo vệ bằng luật khác.

Bảo vệ chống can thiệp trong khi truyền tải.

Đưa ra các hình phạt và các quyền bảo vệ chống các hành vi làm hại, các bồi thường thoả đáng, các phí thuê luật sư và các giá cả theo kiện.

Định ra các thủ tục cho truy nhập hợp pháp của các cơ quan thực thi pháp luật. Về vấn đề này có mấy lưu ý quan trọng. Thứ nhất, các nhân viên thực thi pháp luật luôn luôn được cho phép lấy lệnh của Toà án để truy nhập vào các liên lạc hoặc các bản ghi của chúng. Một bổ xung vào luật này yêu cầu các nhà cung cấp dịch vụ Internet (ISP) cài đặt thiết bị cần thiết cho phép các cuộc nghe ngầm theo lệnh của Toà án. Thứ hai, luật này cho phép các nhà ISP đọc nội dung các liên lạc nhằm để duy trì dịch vụ hoặc để bảo vệ chính mình khỏi bị hại. Chẳng hạn, ví dụ, nhà cung cấp dịch vụ có thể ghi đọc luồng để loại trừ các virut.

3.1.2.3 Luật thống nhất và tăng cường nước Mỹ, cung cấp các công cụ cần thiết để ngăn chặn và đối phó với chủ nghĩa khủng bố (gọi tắt là đạo luật yêu nước của Hoa Kỳ) (The Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act – USA Patriot Act).

Luật này được thông qua năm 2001 khi mà những tấn công khủng bố liên tục xảy ra trên lãnh thổ Mỹ. Luật yêu nước Hoa Kỹ được bổ sung và mở rộng vào tháng 3 năm 2006. Luật bao gồm một loạt điều khoản hỗ trợ tiếp cận buộc thực thi luật đối với các liên lạc điện tử. Theo luật này, cơ quan thực thi pháp luật chỉ cần thuyết phục Toà án rằng đích ở đây là một nhân viên của một tổ chức nước ngoài thì sẽ nhận được lệnh cho phép nghe ngầm ngay. Điều khoản an toàn máy tính cơ bản của Luật yêu nước là sự điều chỉnh, mở rộng của luật chống gian lận và lạm dụng máy tính:

- Cố ý tạo ra sự lan truyền một mã gây hại cho một " máy tính được bảo hộ " là một trọng tội (tội nghiêm trọng).
- Do sai sót gây ra thiệt hại cho một hệ thống máy tính tương tự như là hậu quả của truy nhập bất hợp pháp cũng bị coi là một trọng tội.
- Gây ra thiệt hại (dù là không cố ý) như là truy nhập bất hợp pháp tới một máy tính được bảo vệ cũng coi là một tội ác (nhẹ hơn).

- Sửa đổi vài luật đang tồn tại để cung cấp cho chính phủ các công cụ bổ sung để ghi dấu vết, ngăn chặn và tiêu diệt chủ nghĩa khủng bố.
- Tạo điều kiện chia sẻ các thông tin về an ninh quốc gia và thực thi luật này.
- Cho phép các tiếp cận bổ xung của chính phủ tới các thông tin cần thiết, gồm cả các thông tin điện tử.

3.1.2.4 Luật hiện đại hóa công nghệ ngân hàng 1999. (Financial Industries Modernization Act of 1999 – Gramm-Leach-Bliley)

15 U.S.C.§ §6801 – 6810 (chống tiết lộ thông tin tài chính riêng)

15 U.S.C.§ §6821 – 6827 (chống tiếp cận gian lận)

Luật này còn có tên thường gọi là luật Gramm – Leach – Bliley, 1999; bao gồm an toàn dữ liệu cho các khách hàng của các thiết chế tài chính. Mỗi thiết chế (cơ quan) tài chính phải có chính sách an toàn của mình để thông báo cho các khách hàng. Và các khách hàng phải được cung cấp cơ hội để khước từ mọi việc dùng dữ liệu không đúng mục đích kinh doanh cần thiết mà các dữ liệu được thu thập cho nó. Luật Gramm-Leach-Bliley và các quy định áp dụng nó cũng đòi hỏi các thiết chế ngân hàng phải được đánh giá an toàn – rủi ro chi tiết định kỳ. Dựa trên cơ sở các kết quả của sự đánh giá này, cơ quan tài chính phải thông qua " một chương trình an toàn thông tin " tăng cường nhằm bảo vệ chống truy nhập trái phép hoặc việc dùng các thông tin riêng không công bố của các khách hàng.

3.1.2.5 Luật các thông tin riêng tư Hoa Kỳ. (US Privacy Act).

Luật riêng tư 1974, bảo vệ sự an toàn của các dữ liệu cá nhân do nhà nước thu gom. Cá nhân được quyền biết những dữ liệu gì được thu gom về anh ta hoặc cô ta, dùng cho mục đích gì, và những thông tin như vậy được phổ biến cho ai. Luật này còn được bổ sung để ngăn chặn việc một cơ quan chính phủ này truy nhập tới các dữ liệu được thu gom bởi một cơ quan chính phủ khác dùng cho mục đích khác.. Luật này cũng đòi hỏi sự nỗ lực thường xuyên trong bảo đảm sự bí mật của các dữ liệu cá nhân đã thu thập được.

3.1.2.6 Luật chuyển tiền điện tử của Mỹ.(US Electronic Funds TransferAct)

Luật này nghiêm cấm việc sử dụng, vận chuyển, bán, nhận hay cung cấp các vật dụng hay món nợ thu được một cách gian lận hoặc do thất bại, sửa đổi, ăn cắp, hoặc giả mạo trong thương mại toàn liên bang hay ngoại thương.

3.1.2.7 Luật năm 1998 về ngăn chặn sự giả mạo và ăn cắp định danh.

(Indentity Theft and Assumption Deterrence Act of 1998)

Đây là sự điều chỉnh bổ sung của 18 U.S.C.§1028 (khởi tố hình sự việc chuyển giao cố ý hay sử dụng định danh của một người khác cho các mục đích phi pháp). Trộm cắp định danh cũng có thể vi phạm các luật hình sự liên bang

khác như 18 U.S.C.§1029: gian lận thẻ tín dụng, 18 U.S.C.§1030: gian lận máy tính, 18 U.S.C.§1341: gian lận thư tín, 18 U.S.C.§1343: gian lận điện tín, và 18 U.S.C.§1344: gian lận thiết chế tài chính.

3.1.2.8 Luật 2004 về tăng cường các hình phạt ăn cắp định danh (Indentity Theft Penalty Enhancement Act of 2004).

Các điều chỉnh bổ xung vào các điều luật đã có, luật này xác lập hai loại " trộm cắp định danh trầm trọng ":

- Trộm cắp danh tính liên quan tới chủ nghĩa khủng bố
- Trộm cắp danh tính liên quan với các trọng tội khác.

Luật này tăng các hình phạt và hợp pháp hoá khoản tiền phụ phí theo kiện một vụ ăn cắp định danh.

3.1.2.9 Luật năm 2003 về các giao dịch tiền tệ chính xác và công bằng. (Fair and Accurate Credit Transactions Act of 2003).

Đây là các điều chỉnh và tái khẳng định đối với Luật về báo cáo tiền tệ công bằng năm 1970 (Fair Credit Reporting Act of 1970), mà luật 1970 là bổ xung cho 15 U.S.C.§ §1681-1681(u).

Luật 2003 này bao gồm các điều khoản nhằm hạn chế sự ăn cắp định danh và trợ giúp các bị hại trong ăn cắp định danh tái bảo vệ (lấy lại định danh hoặc được bồi thường thiệt hại).

Luật này còn có một số chứng thư (Titles). Chứng thư I (Titles I) quy định về việc ngăn chặn ăn cắp định danh và việc truy hồi nguồn gốc tiền tệ. Chứng thư VII quy định về mối quan hệ tới các luật của bang.

Liên quan tới Luật giao dịch tiền tệ (2003) và Luật báo cáo tài chính (1970), uỷ ban thương mại liên bang của Hoa Kỳ (FTC – Federal Trade Commision) đưa ra một số văn bản hướng dẫn quan trọng.

Vào tháng 2/2005, FTC công bố Các chỉ dẫn về phương hướng lưu giữ hợp thức các thông tin của khách hàng. Các chỉ dẫn này có hiệu lực từ tháng 7/2005, và quy định về sự sắp xếp các báo cáo của khách hàng và các thông tin thu được từ các báo cáo này.

Vào tháng 7/2006, FTC và Hiệp hội các ngân hàng liên bang Hoa Kỳ công bố để lấy ý kiến Các chỉ dẫn cho việc đặt " cờ đỏ " (phạt tiền) trộm cắp định danh và mâu thuẫn địa chỉ. Khi được thông qua, các chỉ dẫn này sẽ đòi hỏi các cơ quan tài chính và các báo cáo đầu tư phải phát triển và ứng dụng các chương trình ngăn chặn trộm cắp định danh.

3.1.2.10. Luật bảo hộ riêng tư trực tuyến của trẻ em năm 1998. (Children's Online Privacy Act of 1998).

Quy định về việc lựa chọn trực tuyến và tiết lộ các thông tin từ trẻ em dưới 13 tuổi.

Đưa ra những quy định đòi hỏi " những thủ tục hợp lý để bảo vệ sự bí mật, an toàn và toàn vẹn " của các thông tin được giữ kín. 15 U.S.C.§6502.

Sự vi phạm được coi như hành động thương mại không chính đáng theo luật của FTC.

3.1.3. Các luật của bang.

Ngoài luật Liên bang, ở Mỹ còn có hệ thống luật pháp các bang. Trong lĩnh vực an toàn thông tin, các bang cũng ban hành nhiều bộ luật, cụ thể hoá hoặc vận dụng các luật liên bang trong từng lĩnh vực vào khuôn khổ các bang. Tuy nhiên có những luật của bang đi trước lại được phổ biến cho toàn liên bang áp dụng. Sau đây xin giới thiệu một số luật của các bang.

• Luật quản lý sự giám sát điện tử và các cuộc nghe trộm của bang Pennsylvania.

(Wiretapping and Electronic Surveillance Control Act).

19 Pa CSA § §5701, et seq.

• Luật về Hacking và các vi phạm tương tự.

(Hacking and Similar Offenses Act)

18 Pa CSA § §7611, et seq.

- Trộm cắp điện toán (truy nhập phi pháp) §7613.
- Sao chép phi pháp các dữ liệu máy tính §7614.

• Luật về các vi phạm khai báo các thông tin cá nhân.

(Breach of Personal Information Notification Act)

73 PS § §2301 – 2329.

Nói chung, luật này yêu cầu khai báo không chậm trễ đối với những người thường trú tại Pennsylvania " mà các thông tin cá nhân không mã hoá và không chỉnh lý của họ bị truy nhập hoặc có lý do chắc chắn cho là bị truy nhập và bị săn lùng bởi người dấu tên hoặc người bất hợp pháp " thông qua vụ vi phạm an toàn của một hệ thống tin học hóa.

• Luật về các vi phạm khai báo của bang California.

(California Law, Cal.Civ.Code § § 1798.29(a),1798.82(a)).

Luật này yêu cầu các nhà doanh nghiệp tiến hành kinh doanh tại California và các cơ quan chính quyền bang phải thực hiện khai báo những người mà thông tin cá nhân của họ bị tổn thương. Sự tổn thương dữ liệu xảy ra trước kia, tương tự

như các vụ hiện nay, đã không được công bố một cách công khai trước khi luật này của California có hiệu lực. Sau đó nhiều bang khác của Hoa kỳ cũng ban hành hoặc công nhận các luật tương tự. Cho đến nay có ít nhất ba mươi tư (34) bang ở Mỹ đã ban bố luật về khai báo các vi phạm dữ liệu. Có hai mươi tư (24) bang đã thông qua các luật đóng băng tài chính (Credit freeze Laws) cho phép các khách hành đóng băng (giữ kín) các báo cáo tài chính của mình đối với tiếp cận yêu cầu đầu tư mới hoặc mọi tiếp cận.

- Luật về bảo vệ lưu trữ.

(Secure Disposal Law)

Cal.Civ.Code § 1798.1.

California cũng yêu cầu các doanh nghiệp thực hiện các bước hợp lý để huỷ các bản ghi (giấy và điện tử) đang chứa các loại xác định của thông tin cá nhân mà không yêu cầu đến nữa. Các bản ghi này phải được huỷ vụn, tẩy xoá hoặc làm biến đổi để làm cho sau đó không có khả năng giải mã bằng bất kỳ phương tiện nào.

Các bang Arkanas, Kentucky, Hawaii, New Jersey, North Carolina, Texas và Utal ban hành các pháp luật tương tự.

3.2. Luật pháp ATTT tại các nước khác.

Nhiều nước khác như Anh quốc, Australia, Canada, Brazil, Nhật Bản, Cộng Hoà Séc, Hàn Quốc và Ấn độ cũng đã ban hành nhiều đạo luật về an toàn máy tính. Các luật này quy định về các vi phạm như gian lận, truy nhập máy tính trái phép bí mật dữ liệu, lạm dụng máy tính.

Ngày nay Internet đã trở thành thực thể quốc tế toàn cầu. Các công dân ở một nước chịu ảnh hưởng tác động bởi khách hàng ở các nước khác, và các khành hàng ở một nước có thể là chủ thể luật pháp ở các nước khác. Bản chất toàn cầu của tội phạm máy tính làm cho cuộc sống phức tạp lên nhiều. Ví dụ, một công dân của nước A có thể ngồi tại nước B, làm việc tới một ISP ở nước C, sử dụng một máy chủ bị tổn thương ở nước D, và tấn công vào loạt máy tính ở nước E (ở đây không muốn nói sự dạo chơi trên mạng đi qua hàng tá các nước). Để trừng trị tội phạm này có thể đòi hỏi sự hợp tác của tất cả 5 nước. Tên tội phạm này có thể cần được dẫn độ từ B về E để xét xử ở đó, tuy nhiên có thể chưa có hiệp định dẫn độ đối với tội phạm máy tính giữa B và E. Và bằng chứng thu được ở D có thể không được công nhận ở E vì do lấy mẫu và lưu giữ mẫu bằng chứng đó. Và tội phạm này ở E có thể lại không là tội phạm ở B, vì thế các cơ quan thực thi pháp luật mặc dù tương tự nhau, có thể không hành động được. Mặc dù tội phạm máy tính là hiện tượng thực sự toàn cầu các thể chế pháp luật

khác nhau ở các nước khác nhau lại khác nhau. Sự khác nhau trong hành pháp này lại cản trở đối với việc phán xử tội phạm máy tính quốc tế.

Trong phần còn lại của chương này, chúng ta sẽ điểm qua một cách vắn tắt các luật của một số nước khác ngoài Mỹ.

3.2.1. Thoả thuận của Uỷ ban Châu Âu về tội phạm điều khiển. (Council of Europe Agreement on Cybercrime – ECAC).

Tháng 11 năm 2001, Mỹ, Canada, Nhật bản và 22 nước Châu Âu đã ký Thoả thuận của EC về tội phạm điều khiển (ECAC) để thống nhất xác định các hoạt động tội phạm trong không gian điều khiển (cyberspace) và hỗ trợ việc truy nã và xét xử chúng vượt qua biên giới quốc gia. Ý nghĩa của thoả thuận này không chỉ quan trọng ở chỗ coi các hoạt động tội phạm này là phi pháp, mà còn ở chỗ việc cả 25 nước này đều công nhận chúng là các tội ác xuyên quốc gia mình sẽ giúp cho các cơ quan thực thi pháp luật dễ dàng hơn trong việc hợp tác với nhau, trong việc dẫn độ các tội phạm đã thực hiện tội ác chống một nước này từ lãnh thổ một nước khác. Tuy nhiên để thực tế hỗ trợ được cho sự truy nã, xét xử và trừng phạt các tội phạm máy tính, cần phải vào cuộc không chỉ 25 nước này mà nhiều hơn nhiều vì như ta đã nói về bản chất toàn cầu của các tội phạm máy tính. Cho nên thoả thuận EC cũng kêu gọi các nước khác (ngoài 25 nước đã ký) tham gia vào. Bản thoả thuận cũng yêu cầu các nước thông qua nó, tiến hành ban bố các đạo luật hình sự giống nhau về tin tặc (hacking), về gian lận và làm giả trong lĩnh vực điện toán, truy nhập bất hợp pháp, các vi phạm bản quyền, quấy rối trên mạng và khiêu dâm trẻ em. Bản Thoả thuận này cũng bao gồm các điều khoản về các hiệu lực truy nã và các thủ tục cần thiết như là săn lùng trên các mạng và chặn bắt các liên lạc và các yêu cầu về hợp tác thực thi luật qua biên giới trong truy lùng, bắt giữ và dẫn độ. Văn bản gốc của Thoả thuận đã được bổ sung bằng một phụ lục coi là một tội hình sự bất kỳ hình thức tuyên truyền nào thông qua các mạng máy tính về phân biệt chủng tộc và bài ngoại.

3.2.2. Luật về bảo vệ dữ liệu của Cộng đồng châu Âu (EU). (Europe Union Data Protection Act).

Luật về bảo vệ dữ liệu EU, dựa trên Bản chỉ dẫn về an ninh châu Âu, là mô hình pháp lý cho tất cả các nước trong EU. Nó xác lập các quyền riêng tư và trách nhiệm bảo hộ đối với mọi công dân của các nước thành viên. Luật này quy định về sự thu thập và lưu trữ các dữ liệu riêng về các cá nhân, như họ tên, địa chỉ và các số đặc chỉ (nhận dạng, thông hành ...). Luật đòi hỏi mục đích kinh doanh của việc thu thập dữ liệu và giám sát chống tiết lộ. Thông qua vào năm 1994, đây là một trong số các luật sớm nhất xác lập các yêu cầu bảo hộ đối với việc an toàn các dữ liệu cá nhân. Điều quan trọng hơn cả ở đây là: Luật yêu cầu sự bảo hộ tương tự ở cả bên ngoài các nước EU trong trường hợp các tổ chức trong EU đưa các dữ liệu được bảo hộ ra khỏi lãnh thổ EU.

3.2.3. Sự kiểm soát nội dung.

Hiện nay nhiều nước đã đưa ra các luật kiểm soát nội dung luồng Internet cho phép tại các nước mình.

- Singapor yêu cầu các nhà cung cấp dịch vụ Internet (ISP) phải tiến hành lọc lựa (Filter) các nội dung cho phép truyền vào nội địa các nước.
- Trung Quốc nghiêm cấm các tài liệu kích động sự rối loạn trật tự xã hội hoặc gây mất ổn định chính trị của đất nước, hay ảnh hưởng đến bản sắc văn hoá Trung Hoa.
- Tuynidia ban bố luật áp dụng các hình thức giám sát tương tự (cấm) đối với các bài viết, bài nói có tính chất phê phán (kể cả ở các dạng môi trường khác Internet).
- Có nhiều luật đưa ra quy định coi là bất hợp pháp việc truyền các nội dung không cho phép, qua một nước không phụ thuộc vào nguồn hoặc đích của nội dung đó có mặt tại nước đó không. Chúng ta đã biết về cấu trúc đường dẫn (Routing) hiện nay của Internet là rất phức tạp và không thể định trước, nên việc tuân thủ các luật nói trên, mà trong bối cảnh thực thi luật một cách riêng rẽ, là khó có hiệu lực

3.3. Mật mã và pháp lý.

Luật pháp thường được dùng để điều chỉnh mọi người vì lợi ích riêng của họ và vì các lợi ích to lớn hơn của cộng đồng. Giết người, trộm cắp, say rượu và nghiện hút bị hạn chế nhờ pháp luật. Nhìn chung, sự công bằng giữa tự do cá nhân và lợi ích xã hội cộng đồng là tương đối dễ dàng phân xử. Ví dụ, quyền nổ súng của một ai đó sẽ kết thúc khi mà viên đạn đã trúng đích.

Mật mã cũng là một công cụ hoạt động điều chỉnh, tuy nhiên các vấn đề ở đây tỏ ra ít rõ ràng hơn. Một phần cũng vì lý do có rất ít các thoả thuận công khai về chủ đề này. Quyền và nghĩa vụ trong sử dụng mật mã như thế nào; việc điều chỉnh các lợi ích trong áp dụng mật mã ra sao... Đó là các vấn đề ít được bàn thảo và công bố.

Con người luôn mong muốn bảo vệ sự riêng tư (bí mật riêng) của mình, bao gồm cả bí mật của các liên lạc với người khác. Các doanh nhân muốn sự bí mật tương tự. Bọn tội phạm mong muốn có sự bí mật sao cho chúng có thể thông tin cho nhau các kế hoạch tội ác theo cách riêng. Các nhà chức trách muốn ghi dấu vết các hoạt động bất hợp pháp, vừa để ngăn chặn tội phạm, vừa để truy bắt và trừng phạt bọn tội phạm sau khi nó đã được thực hiện. Cuối cùng, các quốc gia rất muốn nắm được các kế hoạch quân sự và ngoại giao của các đối tác khác. Chúng ta đều biết, mật mã là công cụ cơ mật và trọng yếu để bảo vệ các bí mật tầm cỡ quốc gia, tuy nhiên khả năng phá được mật mã cũng là công cụ mạnh mẽ

đối với nhà nước, sẽ là càng tốt nếu người dân được sử dụng mật mã càng ít (nhất là thứ mật mã mà nhà nước không thể phá được).

3.3.1. Kiểm soát việc sử dụng mật mã.

Hiện nay ở nhiều nước, cùng với chính sách về hạn chế nội dung các luồng Internet, cũng đưa ra các hạn chế rất chặt về việc sử dụng mật mã đối với các khách hàng. Ví dụ, ở Trung Quốc Lệnh số 273 của Uỷ ban nhà nước yêu cầu các tổ chức và cá nhân nước ngoài phải có đơn xin phép sử dụng mật mã tại Trung Quốc. Ở Pakistan, người ta yêu cầu tất cả các phần cứng và phần mềm mã hoá đều phải được kiểm tra và phê chuẩn của Bộ liên lạc viễn thông Pakistan. Còn ở Irắc, sử dụng ngay cả Internet cũng bị hạn chế chặt chẽ, và việc sử dụng trái phép mật mã phải chịu lãnh phạt rất nặng.

Có lẽ chỉ có chính sách mật mã của nước Pháp là được bàn tới công khai nhất. Nhập khẩu các sản phẩm mật mã là phải đăng ký: Chỉ cần người bán đăng ký một sản phẩm thương mại rộng rãi thì tất cả các nhập khẩu sản phẩm đó coi như được chấp nhận. Sử dụng mã hoá cho xác thực không bị hạn chế gì. Sử dụng mã hoá với khoá dài đến 128 bit cho tính bí mật chỉ đỏi hỏi đăng ký của người bán. Việc dùng các sản phẩm với độ dài khoá lớn hơn 128 bit đòi hỏi khoá đó phải được uỷ nhiệm bởi phía thứ ba tin cậy.

Những luật như vậy rất khó có hiệu lực thực thi một cách riêng lẻ. Mật mã học, ẩn mã học, và cách viết mật mã được dùng hàng thế kỷ nay. Các nhà chức trách đều biết rằng, họ không thể ngăn cản hai người hợp tác với nhau để che dấu sự liên lạc của họ. Tuy nhiên, nhà nước có thể giới hạn việc dùng mật mã dựa trên trao đổi bằng máy tính bằng cách giới hạn chính mật mã trong các sản phẩm thương mại rộng rãi. Mặc dù giám sát 50 triệu người dùng máy tính là không thể được, việc kiểm soát một nhóm các doanh nghiệp sản xuất máy tính lớn lại là hiện thực, đặc biệt đó lại là các doanh nghiệp mà lợi nhuận của nó chịu ảnh hưởng không phải bởi khả năng bán các sản phẩm bất kỳ trong một nước cụ thể. Vì vậy, nhà nước khi đó sẽ chỉ định việc dùng mật mã tại nguồn: là nhà sản xuất và người bán.

3.3.2. Các kiểm soát đối với việc xuất khẩu mật mã.

Cho đến tận 1998, Mỹ vẫn dẫn đầu các nước công nghiệp trong việc kiểm soát mật mã. Nó được thực hiện bằng việc kiểm soát sự xuất khẩu các sản phẩm mật mã bởi các kiểm duyệt giống như đối với vũ khí hạt nhân: bom và đầu đạn nguyên tử.

Mặc dù, luật pháp áp dụng với tất cả mọi người, trên thực tế, nó lại chỉ có hiệu lực thực thi đối với các nhà sản xuất phần mềm dùng rộng rãi (mass – market). Các nhà sản xuất phần mềm có thể xuất khẩu một cách tự do (nghĩa là xuất cho tất cả loại trừ một nhóm các nước mà đối với họ có sự giám nghiêm

ngặt về vũ khí) các sản phẩm bất kỳ nào dùng mã hoá đối xứng với độ dài khoá 40 bit hoặc nhỏ hơn. Ngoại trừ cho phép mã hoá mạnh hơn đối với các tổ chức tài chính và đối với các tập đoàn xuyên quốc gia dùng mật mã cho liên lạc nội bộ tập đoàn. Mật mã học chỉ duy nhất xác thực (ví dụ, chữ ký số) cũng được cho phép. Mặc dù luật này không kiểm soát việc dùng mật mã nhưng giới hạn xuất khẩu hạn chế rất hiệu quả sự sử dụng mật mã, vì rằng các nhà cung cấp lớn không thể bán các sản phẩm ra thế giới với mật mã mạnh được.

Chính sách của Mỹ đặc biệt quan trọng vì hầu hết các nhà cung cấp các phần mềm thông dụng đều sinh ra tại Mỹ, và Mỹ cũng là nơi có nhiều khách hàng nhất. Mỹ cũng có thể buộc các nhà sản xuất phần mềm không được viết các chương trình theo cách mà sau này ai đó bên kia đại dương có thể chèn mật mã vào.

Mặc dù nhà cung cấp phần mềm có thể chuyển cho hoặc mở một đại lý (chi nhánh) ở một nước không kiểm soát được (về mật mã), thì nhà cung cấp mới này cũng rất khó có thể thu được một thị phần có ý nghĩa đối lại các đối tác cạnh tranh to lớn và hùng hậu đã được xác lập từ lâu rồi. Nếu như một nhà cung cấp như vậy mà có khả năng giành được một lượng đáng kể các thương vụ bên ngoài các công ty Mỹ thì sẽ có các phản đối kịch liệt và sức ép chính trị từ phía chính phủ Mỹ. Vì thế, chính sách của Mỹ về vấn đề này đã, đang và sẽ thống trị thị trường thế giới.

Mật mã bao gồm không chỉ là các sản phẩm, nó chứa đựng cả các ý tưởng sâu xa nữa. Dù cho nhà nước giám sát một cách hiệu quả và chặt chẽ các luồng sản phẩm qua biên giới, việc kiểm soát các luồng tư tưởng cả ở trong đàu óc con người, cả ở trên Internet là không thể được. Trường hợp mã nguồn PGP của Phil Zimmerman – người sáng chế ra Thư điện tử mã hóa PGP là một ví dụ điển hình.

Nhà nước có thể kiểm soát việc dùng mật mã thông qua cơ chế ủy nhiệm khóa. Mặc dù luật pháp cho phép nhà nước đọc các liên lạc được mã hóa, trên thực tế nhà nước không muốn đọc tất cả chúng. Nhà nước chỉ quan tâm đến những gì liên quan đến an ninh quốc gia là chủ yếu, Trong trường hợp này, nhà nước có thể yêu cầu tòa án cho phép tìm kiếm nhà, cơ quan hay các file máy tính của những người liên quan. Sau đó nhà nước sẽ biện minh cho lý do chính đáng để đọc các dữ liêu đã mã hóa liên quan. Để thực hiện điều này, nhà nước đưa ra một sơ đồ, trong đó khóa mã của bạn chỉ có hiệu lực bằng sự ủy nhiệm của tòa án (phê chuẩn của tòa án). Năm 1996, chính phủ Mỹ chủ trương nới lỏng sự hạn chế xuất khẩu đối với cái gọi là mật mã được giao kèo. Với mật mã giao kèo, nhà nước có khả năng nhận được khóa mã của bất kỳ liên lạc mã hóa nào. Đó chính là sự ủy nhiệm khóa mật mã.

3.3.3. Chính sách mật mã hiện thời của Mỹ.

Năm 1996, Ban nghiên cứu quốc gia của Mỹ – U.S National Research Council (NRC) đã báo cáo các kết quả của 18 tháng nghiên cứu để đưa ra tư vấn

cho chính sách mật mã của chính phủ liên bang Hoa Kỳ. Bản báo cáo đã cân nhắc kỹ lưỡng tất cả các yếu tố chịu ảnh hưởng của chính sách mật mã, như là việc bảo vệ các thông tin nhạy cảm cho các công ty Mỹ và các cá nhân mỹ cũng như của nước ngoài, của thương mại quốc tế, hiệu lực của pháp luật (ngăn chặn, truy nã và khởi tố) và sự thu thập tình báo. Báo cáo đã đề xuất các luận điểm sau đây cho chính sách:

• Không có luật nào ngăn cản việc sản xuất, bán hoặc sử dụng bất kỳ dạng nào của mật mã trong giới hạn lãnh thổ Hoa Kỳ.

• Các giảm sát xuất khẩu mật mã cần được nới lỏng nhưng không được loại bỏ.

• Các sản phẩm bảo đảm tính bí mật ở mức đáp ứng hầu hết các yêu cầu thương mại chung cần được xuất khẩu một cách dễ dàng. Năm 1996, mức này bao gồm các sản phẩm hỗ trợ DES với khóa 56 bit, và do vậy các sản phẩm này phải được xuất khẩu dễ dàng.

• Mật mã ủy nhiệm khóa cần phải được nghiên cứu tiếp tục, và, vì vẫn chưa có được công nghệ hoàn chỉnh, việc dùng nó nên rất hạn chế (không coi là bắt buộc).

• Quốc hội cần xem xét một cách nghiêm túc pháp luật khả dĩ đưa ra được các hình phạt đối với việc dùng các liên lạc mã hóa trong thương mại liên bang để thực hiện ý đồ gây tội ác.

• Chính phủ Mỹ cần phát triển một cơ chế để khuyến khích sự bảo vệ thông tin (ATTT) trong khu vực tư nhân.

Vào tháng 9 năm 1998, Chính phủ Mỹ công bố rằng việc xuất khẩu mật mã được mở cửa. Xuất khẩu khóa đơn (56 bit) DES được cho phép tới tất cả các nước (loại trừ 7 nước hỗ trợ cho chủ nghĩa khủng bố). Mã khóa kích thước không giới hạn có thể xuất khẩu tới 45 nước công nghiệp lớn để sử dụng cho các cơ quan tài chính, các nhà cung cấp y khoa, và các công ty thương mại điện tử. Hơn thế nữa, quá trình xin cấp phép, từng là sự ngăn cản kinh khủng, nay được đơn giản hóa tới mức ngắn gọn, chỉ trong vòng một tuần lễ là hoàn tất.

Câu hỏi và các chủ đề thảo luận, tiểu luận.

1) Bạn hãy tổng quan về các luật bảo vệ thông tin trong lĩnh vực ngân hàng, tài chính của Mỹ.
2) Về vấn đề riêng tư cá nhân trong luật ATTT của Liên bang và các bang ở Hoa Kỳ.
3) Bạn có nhận xét gì về hệ thống pháp luật về an toàn máy tính của Mỹ và Tây Âu.

4) Vai trò của chính sách mật mã trong pháp luật an toàn thông tin.
5) Hãy lấy một ví dụ minh hoạ cho bản chất toàn cầu của các tội phạm máy tính và minh chứng cho sự cần thiết của một không gian toàn cầu về luật pháp ATTT nói chung và luật pháp chống tội phạm máy tính và chủ nghĩa khủng bố nói riêng.
6) Bạn hãy nói hiểu biết của mình về chính sách mật mã hiện hành của Hoa Kỳ.

CHƯƠNG IV PHÁT TRIỂN LUẬT PHÁP AN TOÀN THÔNG TIN TẠI VIỆT NAM

4.1. Thực trạng và thách thức luật pháp ATTT tại Việt Nam.

4.1.1. Thực trạng phát triển CNTT & TT và các thách thức đặt ra.

Trong hơn chục năm qua, ở Việt Nam đã có một sự phát triển ngoạn mục về mọi mặt kinh tế, chính trị, xã hội. Đó là do những ngọn gió tươi mát và mạnh mẽ của đổi mới mang lại, đó là do sự mở cửa hội nhập ngày càng toàn diện và sâu sắc với thế giới và khu vực. Sự đổi mới và mở cửa đầu tiên là trong lĩnh vực điện tử và viễn thông, mở cửa về thông tin viễn thông. Các thành tựu ở đây ấn tượng đến mức mà người ta đã nói về một cuộc cách mạng trong lĩnh vực tin học viễn thông ở Việt Nam. Từ chỗ cả nước chỉ có một số máy tính điện tử cổ điển như Minscơ - 22, Minscơ - 32 ở Hà Nội và vài cỗ IBM 360/50 ở Miền Nam mới giải phóng đến nay máy tính đã tràn ngập mọi nơi trong các công sở, nhà trường, trong các gia đình, trong các cửa hàng phố xá... Các mạng máy tính xuất hiện và đi vào hoạt động. Internet trở thành thông dụng như các trò chơi game thường nhật của mọi người. Mạng lưới điện thoại (cố định và di động) đã đạt được mật độ phát triển trung bình trên thế giới. Cùng với các thành tựu to lớn trong các lĩnh vực kinh tế xã hội quan trọng khác Việt Nam đang tự tin đi tới nền kinh tế trí thức cùng toàn thể nhân loại với nhiều thời cơ và thách thức. Một thách thức to lớn khi một đất nước đi vào nền kinh tế tri thức, vào xã hội thông tin, đi vào xa lộ thông tin gặp phải - đó là các vấn đề về an toàn thông tin mà chúng ta đã nói ngay từ đầu giáo trình này.

4.1.2. Tình hình tội phạm máy tính và pháp luật.

Ở Việt Nam xuất hiện tất cả các loại tội phạm máy tính, các loại tội phạm về công nghệ thông tin mà thế giới đã gặp phải. Các sản phẩm công nghệ thông tin, các sản phẩm bảo vệ thông tin, các công nghệ ATTT điển hình đều được nhập khẩu và có bán các cửa hàng, các công ty. Đã xuất hiện các tổ chức tin tặc, đã hình thành các trung tâm an toàn, an ninh mạng, trung tâm cảnh báo và đối phó với các hoạt động phá hoại. Một số vụ án hình sự về ăn cắp trên mạng và phát tán các tài liệu phản động và văn hoá phẩm đồi truỵ trên mạng đã được xét xử.

Cũng như ở nhiều nước, bài toán về an toàn thông tin ở Việt Nam cũng được đặt ra ngày càng cấp thiết. Các thông tin an ninh, quốc phòng, các bí mật quốc gia, các thông tin nhạy cảm trong kinh tế, xã hội và của các cá nhân... cần phải được bảo vệ. Một trong các khía cạnh quan trọng của bảo vệ thông tin như chúng ta đã biết là bảo vệ pháp lý: cần phải có hệ thống luật pháp về ATTT. Trong những năm qua Nhà nước cộng hoà XHCN Việt Nam đã làm được nhiều việc trong lĩnh vực này.

4.2. Một số văn bản pháp luật về ATTT ban hành tại Việt Nam.

4.2.1. Pháp lệnh bảo vệ bí mật nhà nước (BMNN).

Để nâng cao trách nhiệm của cơ quan nhà nước, các tổ chức xã hội, các công dân trong nhiệm vụ bảo vệ bí mật nhà nước ngày 11-1-2001 Chủ tịch nước đã công bố Pháp lệnh bảo vệ bí mật nhà nước (do Uỷ ban thường vụ quốc hội thông qua).

- Định nghĩa bí mật nhà nước (là loại thông tin đặc biệt về chính trị, kinh tế, quốc phòng, an ninh.... mà nhà nước không công bố hoặc chưa công bố và nếu bị tiết lộ thì sẽ gây nguy hại cho Nhà nước CHXHCN Việt Nam.

- Nghiêm cấm mọi hành vi xâm phạm BMNN (như thu thập, làm lộ, làm mất, chiếm đoạt, mua bán, tiêu huỷ trái phép) và quy định việc tiếp xúc, bảo quản và xử lý BMNN.

- Lần đầu đưa ra các độ mật: Tuyệt mật, Tối mật và Mật của các thông tin BMNN (mà được áp dụng vào các dạng TT khác sau này).

- Nói rõ tại điều 5: Mật mã quốc gia thuộc độ Tuyệt mật và tại điều 15: Nội dung BMNN nếu truyền đưa bằng phương tiện viễn thông và máy tính thì phải được mã hoá theo quy định của pháp luật về cơ yếu.

- Quy định nội dung quản lý nhà nước về BMNN (Chính phủ thống nhất quản lý nhà nước về bảo vệ BMNN, Bộ công an chịu trách nhiệm trước Chính phủ về bảo vệ BMNN).

- Ngày 28-3-2002 Chính phủ có Nghị định số 33/2002/NĐ-CP quy định chi tiết thi hành pháp lệnh này. Tại điều 15 của Nghị định số 33 nói rõ: Nghiêm cấm các cơ quan, tổ chức và cá nhân tự nghiên cứu, sản xuất, cung cấp, quản lý, sử dụng mật mã để tiến hành các hoạt động xâm phạm an ninh quốc gia.

Đây là văn bản luật đầu tiên có một số quy định về mật mã và sử dụng mật mã ở Việt Nam.

4.2.2.Pháp lệnh Cơ yếu.

Ngày 15-4-2001 chủ tịch nước ký lệnh công bố Pháp lệnh cơ yếu (được UBTVQH thông qua).

Pháp lệnh cơ yếu quy định về:

- Ví trí, tính chất, chức năng của cơ yếu; ngay tại điều 1 nói rõ hoạt động cơ yếu là hoạt động cơ mật đặc biệt, thuộc lĩnh vực an ninh quốc gia với chức năng sử dụng mật mã để bảo vệ thông tin bí mật nhà nước. Lĩnh vực an ninh quốc gia có phạm vi rộng, liên quan đến an ninh, ổn định của mỗi quốc gia;

lực lượng nòng cốt để bảo vệ an ninh quốc gia bao gồm cả quân đội và công an.

- Như vậy hoạt động cơ yếu thực chất là hoạt động mật mã. Do đó có thể hiểu Pháp luật cơ yếu chính là pháp luật quy định về mật mã và các hoạt động mật mã.

- Hoạt động đó được xác định là cơ mật đặc biệt, thuộc lĩnh vực an ninh quốc gia.

- Về nhiệm vụ cơ yếu; Điều 12 nói rõ 9 nhiệm vụ sau đây:

- Bảo đảm bí mật, an toàn, chính xác, kịp thời thông tin của Đảng, Nhà nước trong mọi tình huống.
- Tổ chức xây dựng và thống nhất quản lý sử dụng hệ thống mạng liên lạc cơ yếu trong nước và cơ quan đại diện Việt Nam ở nước ngoài.
- Bảo đảm tính sẵn sàng của hệ thống liên lạc cơ yếu của cơ quan Đảng, Nhà nước, đơn vị vũ trang nhân dân và các yêu cầu liên lạc đặc biệt khác; bảo đảm lực lượng dự bị, nguồn dự trữ sản phẩm mật mã để ứng phó có hiệu quả trong mọi tình huống.
- Sản xuất, cung cấp sản phẩm mật mã và xây dựng cơ sở vật chất, kỹ thuật đáp ứng yêu cầu chính quy, từng bước hiện đại của cơ yếu.
- Bảo vệ kỹ thuật, nghiệp vụ mật mã, nội dung của công trình nghiên cứu, phát minh sáng chế, các sản phẩm khoa học, công nghệ mật mã theo quy định của pháp luật về bảo vệ bí mật nhà nước.
- Tổ chức nghiên cứu và thống nhất quản lý nghiên cứu phát triển khoa học, công nghệ mật mã Việt Nam.
- Xây dựng tổ chức, đội ngũ người làm công tác cơ yếu vững mạnh, chính quy, có phẩm chất chính trị, đạo đức cách mạng, lối sống lành mạnh và trung thực, giỏi về chuyên môn nghiệp vụ, tổ chức đào tạo chuyên ngành cơ yếu các bậc trung học, cao đẳng, đại học và sau đại học.
- Phối hợp với cơ quan, tổ chức có liên quan để bảo vệ thông tin bí mật nhà nước và tạo mọi điều kiện cho tổ chức cơ yếu, người làm công tác cơ yếu hoàn thành nhiệm vụ.
- Thực hiện các nhiệm vụ khác do Đảng và Nhà nước giao.

- Nghiêm cấm việc nghiên cứu và sử dụng mật mã để tiến hành hoạt động xâm phạm an ninh quốc gia, các hành vi thu thập, làm lộ, làm mất, chiếm đoạt, mua bán, tiêu huỷ sản phẩm mật mã, các hoạt động gây phương hại đến lợi ích của Nhà nước, quyền lợi và lợi ích hợp pháp của tổ chức, cá nhân.

- Quản lý nhà nước về cơ yếu:

  - Xây dựng chiến lược, quy hoạch, kế hoạch phát triển cơ yếu, xây dựng chính sách, tiêu chuẩn mật mã quốc gia.
  - Xây dựng, ban hành và hướng dẫn thi hành các văn bản quy phạm pháp luật về cơ yếu.
  - Xây dựng tổ chức cơ yếu, tổ chức đào tạo chuyên ngành cơ yếu.
  - Xây dựng chế độ tiền lương và phụ cấp, các chế độ chính sách khác đối với người làm công tác cơ yếu.
  - Thống nhất quản lý hoạt động chuyên môn nghiệp vụ về cơ yếu, quản lý việc tổ chức nghiên cứu sáng chế, sản xuất, nhập khẩu, xuất khẩu trang thiết bị và các sản phẩm mật mã; kiểm soát việc sử dụng các loại kỹ thuật mật mã.
  - Quản lý các hoạt động, kế hoạch, ngân sách và cơ sở vật chất, kỹ thuật cơ yếu.
  - Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý các vi phạm pháp luật về cơ yếu.
  - Hợp tác quốc tế về cơ yếu.

Quản lý mật mã dân sự: việc quản lý, nghiên cứu, sản xuất và sử dụng mật mã để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước do Chính phủ quy định.

4.2.3. Nghị định của Chính phủ về quản lý mật mã dân sự.

Ngày 08/5/2007, Chính phủ đã ban hành Nghị định số 73/2007/NĐ-CP về hoạt động nghiên cứu, sản xuất, kinh doanh và sử dụng mật mã để bảo vệ thông tin không thuộc phạm vi bí mật Nhà nước.

Nội dung Nghị định gồm 5 chương, 31 điều cụ thể như sau:

Chương I: Những quy định chung.

Chương này có 6 điều (từ Điều 1 đến Điều 6) gồm: phạm vi điều chỉnh của nghị định này quy định về hoạt động nghiên cứu, sản xuất kinh doanh và sử dụng mật mã để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước. Đối tượng áp

dụng không phân biệt tổ chức, cá nhân Việt Nam hay nước ngoài. Quy định về quy chuẩn kỹ thuật và áp dụng quy chuẩn kỹ thuật đối với sản phẩm mật mã dân sự. Chương này cũng thể hiện chính sách thông thoáng và chủ trương nhất quán của nhà nước trong hoạt động nghiên cứu, sản xuất, kinh doanh và sử dụng sản phẩm mật mã dân sự, nhưng cũng thể hiện thái độ kiên quyết, nghiêm cấm các hoạt động xâm hại đến lợi ích quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Chương II: Nghiên cứu, sản xuất, kinh doanh và sử dụng sản phẩm mật mã dân sự.

Chương này có 3 mục: bao gồm 13 điều (từ Điều 7 đến Điều 19). Các quy định trong chương này thể hiện nguyên tắc quản lý thống nhất về hoạt động nghiên cứu, sản xuất, kinh doanh và sử dụng sản phẩm mật mã dân sự: Nhà nước khuyến khích các tổ chức, cá nhân có nhu cầu, đủ điều kiện nghiên cứu và phát triển mật mã dân sự; hoạt động nghiên cứu mật mã dân sự thực hiện theo quy định của Luật Khoa học và Công nghệ. Tuy nhiên, các kết quả nghiên cứu mật mã dân sự khi đưa vào sản xuất, kinh doanh và sử dụng phải áp dụng các quy định quản lý Nhà nước về chất lượng sản phẩm, hàng hoá và dịch vụ và tuân theo Điều 6, Điều 8 của Nghị định này.

Trong chương này quy định rõ: Sản phẩm mật mã dân sự là loại hàng đặc biệt thuộc danh mục hàng hoá, dịch vụ hạn chế kinh doanh, chỉ doanh nghiệp đăng ký và có đủ điều kiện được cấp phép mới được hoạt động sản xuất, kinh doanh sản phẩm mật mã dân sự. Ban Cơ yếu Chính Phủ là cơ quan nhà nước có thẩm quyền quản lý về hoạt động sản xuất, kinh doanh sản phẩm mật mã dân sự, cấp "Giấy phép sản xuất, kinh doanh sản phẩm mật mã dân sự", "Giấy chứng nhận hợp chuẩn sản phẩm mật mã dân sự" và " Giấy chứng nhận hợp quy sản phẩm mật mã dân sự".

Nhà nước khuyến khích các tổ chức, cá nhân sử dụng sản phẩm mật mã dân sự để bảo vệ thông tin của mình.

Chương III: Quản lý Nhà nước về mật mã dân sự.

Chương này có 3 điều (từ Điều 20 đến Điều 22) bao gồm nội dung quản lý nhà nước về mật mã dân sự, trách nhiệm của Ban Cơ yếu Chính phủ về hoạt động nghiên cứu, sản xuất, kinh doanh và sử dụng sản phẩm mật mã dân sự, trách nhiệm của các Bộ, Ngành, Uỷ ban nhân dân các tỉnh, thành phố trực thuộc Trung ương có liên quan.

Chương IV: Thanh tra, kiểm tra, xử lý vi phạm và giải quyết khiếu nại tố cáo.

Chương này có 7 điều (từ Điều 23 đến Điều 29), các quy định trong chương này thể hiện rõ vai trò quản lý nhà nước về thanh tra, kiểm tra, xử lý vi phạm và giải quyết khiếu nại tố cáo. Việc xử lý các vi phạm cũng được cụ thể hoá bằng

các quy định xử phạt hành chính, bồi thường thiệt hại hoặc truy cứu trách nhiệm hình sự.

Chương V: Điều khoản thi hành.

Chương này có 2 điều (Điều 30 đến Điều 31) quy định về hiệu lực; trách nhiệm hướng dẫn, kiểm tra thực thi, thi hành Nghị định.

Để Nghị định sớm đi vào cuộc sống, tăng cường sự quản lý của nhà nước đối với các hoạt động nghiên cứu, sản xuất, kinh doanh, sử dụng sản phẩm mật mã dân sự, góp phần thúc đẩy sự phát triển kinh tế – xã hội, Ban Cơ yếu Chính phủ đang tập trung phối hợp với các cơ quan, Bộ, Ngành xây dựng Thông tư hướng dẫn thực hiện Nghị định; nghiên cứu, xây dựng và đề xuất ban hành Tiêu chuẩn và Quy chuẩn kỹ thuật mật mã dân sự; đề xuất kế hoạch xây dựng chính sách mật mã quốc gia. Bên cạnh đó, Ban Cơ yếu Chính phủ cũng đang điều chỉnh về tổ chức, xây dựng các cơ quan quản lý mật mã dân sự, cơ quan đánh giá, kiểm định sản phẩm mật mã dân sự và các tổ chức liên quan.

4.2.4. Luật sở hữu trí tuệ.

Ngày 12/12/2005, chủ tịch nước đã ký lệnh công bố Luật sở hữu trí tuệ (đã được quốc hội nước CHXNCN Việt Nam thông qua).

Lần đầu tiên áp dụng ở Việt Nam Luật sở hữu trí tuệ tương ứng với luật và các công ước quốc tế trong lĩnh vực này. Bao gồm cả các phần mở rộng cho các đối tượng máy tính.

Bộ luật này có 6 phần:

- Phần thứ nhất: Những quy định chung.
- Phần thứ hai: Quyền tác giả và quyền liên quan.

Ở đây quy định về các điều kiện bảo hộ quyền tác giả và quyền liên quan. Nội dung, giới hạn quyền, thời hạn bảo hộ quyền tác giả; Chủ sở hữu quyền tác giả; Chứng nhận, đăng ký quyền tác giả và quyền liên quan; Tổ chức đại diện, tư vấn, dịch vụ quyền tác giả.

- Phần thứ ba: Quyền sở hữu công nghiệp.

Ở đây quy định về các điều kiện bảo hộ quyền sở hữu công nghiệp, phát minh, sáng chế, xác lập quyền sở hữu công nghiệp đối với sáng chế, kiểu dáng công nghiệp, thiết kế bố trí, nhãn hiệu, chỉ dẫn địa lý; chủ sở hữu, nội dung và giới hạn quyền sở hữu công nghiệp.

- Phần thứ tư: Quyền đối với giống cây trồng.
- Phần thứ năm: Bảo vệ quyền sở hữu trí tuệ.

Ở đây quy định về điều kiện bảo vệ quyền sở hữu trí tuệ; Xử lý các xâm phạm quyền sở hữu trí tuệ bằng biện pháp dân sự, xử lý các xâm phạm bằng biện pháp hành chính và dân sự, kiểm soát hàng hoá xuất khẩu nhập khẩu liên quan đến sở hữu trí tuệ.

– Phần thứ sáu: Điều khoản thi hành.

4.2.5. Luật Giao dịch điện tử (GDĐT).

Luật Giao dịch điện tử có hiệu lực từ ngày 1/3/2006.

Luật GDĐT ra đời là một đòi hỏi bức thiết của việc ứng dụng CNTT trong nước cũng như hội nhập quốc tế. Trong nhiều năm qua, đầu tư cho CNTT của nước ta tuy chưa lớn bằng một số nước nhưng cũng chiếm tỷ lệ cao trong ngân sách. CNTT đã góp phần nâng cao hiệu quả của nhiều hoạt động kinh tế xã hội, song chúng ta chưa có một văn bản pháp luật nào công nhận giá trị pháp lý của các ứng dụng này. Do vậy, bên cạnh hệ thống quản lý hành chính, giao dịch được tin học hoá hoạt động khá hiệu quả, chúng ta vẫn phải duy trì các hệ thống thủ công truyền thống theo quy định của pháp luật. Luật GDĐT ra đời cũng tạo ra cơ sở pháp lý bảo đảm an ninh, an toàn cho GDĐT, bảo vệ quyền lợi hợp pháp của các bên tham gia GDĐT. Tinh thần cơ bản của Luật GDĐT là công nhận giá trị pháp lý của thông điệp dữ liệu – một hình thức thể hiện mới của giao dịch bên cạnh hình thức *văn bản và lời nói* như quy định của bộ Luật Dân sự.

Chương II, Luật GDĐT quy định về: Hình thức thể hiện thông điệp dữ liệu , giá trị pháp lý của thông điệp dữ liệu, thông điệp dữ liệu có giá trị như văn bản, thông điệp dữ liệu có giá trị như bản gốc, thông điệp dữ liệu làm chứng cứ và lưu trữ thông điệp dữ liệu. Một trong các biện pháp bảo đảm an toàn cho các bên tham gia là việc ký trên các văn bản giao dịch nhằm khẳng định ý chí của mỗi bên.

Chương III quy định về giá trị pháp lý của chữ ký điện tử gắn kèm với thông điệp dữ liệu, các vấn đề liên quan đến con dấu trong GDĐT, trách nhiệm của người ký, người nhận chữ ký điện tử. Trong chương này cũng có các quy định về việc chứng thực điện tử (CA), tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử và các điều kiện để hình thành các tổ chức này. Các chương II và III tuy không đề cập trực tiếp đến vấn đề an ninh, an toàn thông tin trên mạng, nhưng thực chất các quy định của hai chương này liên quan đến thông điệp dữ liệu và chữ ký điện tử cúng chính là các vấn đề mấu chốt để đảm bảo an toàn cho các bên giao dịch.

Các quy định cụ thể liên quan đến an ninh, an toàn, bảo mật trong GDĐT được quy định cung trong Chương VI: *An ninh, An toàn, Bảo vệ, Bảo mật trong giao dịch điện tử.* Nội dung chính của chương này là các cá nhân, tổ chức khi tham gia GDĐT có quyền lựa chọn các biện pháp bảo đảm an ninh, an toàn phù hợp với quy định của pháp luật và không được thực hiện bất kỳ hành vi nào nhằm

cản trở hoặc gây phương hại đến việc bảo đảm an ninh, an toàn trong GDĐT (Điều 44); không được thực hiện bất kỳ hành vi nào gây phương hại đến sự toàn vẹn của thông điệp dữ liệu của cơ quan, tổ chức, cá nhân khác (Điều 45). Về vấn đề bảo mật thông tin cá nhân, khoản 2 Điều 46 quy định: *Cơ quan, tổ chức, cá nhân không được sử dụng, cung cấp hoặc tiết lộ thông tin về bí mật đời tư hoặc thông tin của cơ quan, tổ chức, cá nhân khác mà mình tiếp cận hoặc kiểm soát được trong GDĐT nếu không được sự đồng ý của họ...*

Vì GDĐT khác giao dịch thông thường là có sự tham gia của các nhà cung cấp dịch vụ trên mạng nên Luật cũng quy định trách nhiệm của nhà cung cấp này tại Điều 47:

> 1. *Tổ chức cung cấp dịch vụ mạng có trách nhiệm phối hợp với các cơ quan hữu quan xây dựng quy chế quản lý và các biện pháp kỹ thuật để phòng ngừa, ngăn chặn việc sử dụng dịch vụ mạng nhằm phát tán các thông điệp dữ liệu có nội dung không phù hợp với truyền thống văn hoá, đạo đức của dân tộc, gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội hoặc vi phạm các quy định khác của pháp luật.*
>
> 2. *Tổ chức cung cấp dịch vụ mạng phải chịu trách nhiệm trước pháp luật nếu không kịp thời loại bỏ những thông điệp dữ liệu được quy định trong khoản 1 Điều này khi tổ chức cung cấp dịch vụ mạng đó đã nhận được thông báo của cơ quan nhà nước có thẩm quyền.*
>
> Còn trong Điều 41 quy định cụ thể việc bảo đảm an toàn, bảo mật và lưu trữ thông tin điện tử trong các cơ quan nhà nước. *1. Định kỳ kiểm tra và bảo đảm an toàn hệ thống thông tin điện tử của cơ quan minh trong quá trình GDĐT. 2. Bảo đảm bí mật thông tin liên quan đến GDĐT, không được sử dụng thông tin vào mục đích khác trái với quy định về việc sử dụng thông tin đó, không tiết lộ thông tin cho bên thứ ba theo quy định của pháp luật. 3. Bảo đảm tính toàn vẹn của thông điệp dữ liệu trong GDĐT do mình tiến hành; bảo đảm an toàn trong vận hành của hệ thống mạng máy tính của cơ quan mình. 4. Thành lập cơ sở dữ liệu về các giao dịch tương ứng, bảo đảm thông tin và có biện pháp dự phòng nhằm phục hồi được thông tin trong trường hợp hệ thống thông tin điện tử bị lỗi. 5. Bảo đảm an toàn, bảo mật và lưu trữ thông tin theo quy định của Luật này và các quy định khác của pháp luật có liên quan.*

Mục tiêu chính của luật GDĐT là tạo ra khung pháp lý, công nhận hoạt động GDĐT được thể hiện qua thông điệp dữ liệu, công nhận giá trị pháp lý của chữ ký điện tử, tạo chỗ dựa pháp lý cho các bên giao dịch có sự tin cậy để ứng dụng GDĐT. Luật cũng đề cập đến các vấn đề liên quan đến an ninh, an toàn giao dịch và cả vấn đề bảo vệ thông tin cá nhân trong quá trình giao dịch, song các quy định chỉ nhằm vào an ninh, an toàn trong GDĐT. Tuy nhiên, đây là một

khái niệm rộng bao hàm cả an ninh mạng, an ninh an toàn và bảo mật thông tin, vì thế Luật chưa thể quy định một cách chi tiết. Theo chúng tôi, riêng về lĩnh vực an ninh, an toàn trong GDĐT, chúng ta cũng cần có những Nghị định hướng dẫn thi hành Luật một cách chi tiết cho từng vấn đề an ninh mạng, bảo mật và an toàn thông tin, bảo vệ thông tin cá nhân và nhất là văn bản pháp luật liên quan đến tội phạm trên mạng.

4.2.6. Luật công nghệ thông tin (Luật CNTT).

Luật CNTT được chủ tịch nước công bố ngày 12/7/2006. Luật quy định về hoạt động ứng dụng và phát triển CNTT, quyền và nghĩa vụ của cơ quan, tổ chức, cá nhân tham gia hoạt động ứng dụng và phát triển CNTT.

Về các hành vi phạm pháp liên quan đến an toàn, an ninh thông tin trên mạng, luật bao gồm các nhóm hành vi:

- Nhóm hành vi vi phạm pháp luật có tính chất chống lại con người. Khoản 2, Điều 12 Luật CNTT quy định nghiêm cấm hành vi cung cấp, trao đổi, truyền đưa, lưu trữ, sử dụng thông tin số nhằm mục đích kích động bạo lực, tuyên truyền chiến tranh xâm lược, gây hận thù giữa các dân tộc và nhân dân các nước, kích động dâm ô, đồi truỵ, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong mỹ tục của dân tộc, xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự, nhân phẩm, uy tín của công dân; quảng cáo, tuyên truyền hàng hoá, dịch vụ thuộc danh mục cấm đã được pháp luật quy định.
- Về nhóm hành vi xâm phạm tài sản của tổ chức, cá nhân. Khoản 1, Điều 12 nghiêm cấm hành vi cản trở bất hợp pháp hoạt động của hệ thống máy chủ, tên miền quốc gia, phá hoại cơ sở hạ tầng thông tin, phá hoại thông tin trên môi trường mạng.

  Khoản 3, Điều 12 nghiêm cấm hành vi xâm phạm quyền sở hữu trí tuệ trong hoạt động công nghệ thông tin, sản xuất, lưu hành sản phẩm công nghệ thông tin trái pháp luật; giả mạo trang thông tin điện tử của tổ chức, cá nhân khác; tạo đường dẫn trái phép đối với tên miền của tổ chức, cá nhân sử dụng hợp pháp tên miền đó.

  Khoản 1, Điều 21 quy định tổ chức, cá nhân thu thập, xử lý và sử dụng thông tin cá nhân của người khác trên môi trường mạng phải được người đó đồng ý, trừ trường hợp pháp luật có quy định khác.

  Điều 71 quy định tổ chức, cá nhân không được tạo ra, cài đặt, phát tán virus máy tính, phần mềm gây hại vào thiết bị số của người khác để thực hiện một trong những hành vi bao gồm: thay đổi các tham số cài đặt của thiết bị số; thu thập thông tin của người khác; xoá bỏ, làm mất tác dụng của các phần mềm bảo đảm an toàn, an ninh thông tin được cài đặt trên

bị số; ngăn chặn khả năng của người sử dụng xoá bỏ hoặc hạn chế sử dụng những phần mềm không cần thiết; chiếm đoạt quyền điều khiển thiết bị số; thay đổi, xoá bỏ thông tin lưu trữ trên thiết bị số....

Khoản 2, Điều 72 quy định tổ chức cá nhân không được thực hiện một trong những hành vi bao gồm: xâm nhập, sửa đổi, xoá bỏ nội dung thông tin của tổ chức, cá nhân khác trên môi trường mạng; cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của tổ chức, cá nhân khác trên môi trường mạng, phá khoá mã, trộm cắp, sử dụng mật khẩu, khoá mật mã và thông tin của tổ chức, cá nhân khác trên môi trường mạng.

- Về nhóm hành vi vi phạm pháp luật có tính chất chống lại Chính phủ. Khoản 2, Điều 12 nghiêm cấm hành vi cung cấp, trao đổi, truyền đưa, lưu trữ, sử dụng thông tin số nhằm mục đích chống Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam, phá hoại khối đoàn kết toàn dân; tiết lộ bí mật Nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác đã được pháp luật quy định.

  Khoản 2, Điều 68 quy định tên miền quốc gia Việt Nam ".vn" dành cho tổ chức Đảng, cơ quan Nhà nước phải được bảo vệ và không được xâm phạm.

  Ở Việt Nam, Luật CNTT được ban hành kết hợp với các văn bản quy phạm pháp luật hiện có đã tạo lập hành lang pháp lý tương đối phù hợp nhằm ngăn ngừa các hành vi vi phạm pháp luật liên quan đến máy tính và môi trường mạng, góp phần bảo đảm an toàn, an ninh thông tin trên mạng.

4.3. Triển vọng phát triển luật pháp ATTT và đạo đức học máy tính tại Việt Nam.

Cũng như ở các nơi khác trên thế giới, ở Việt Nam CNTT & TT phát triển rất nhanh chóng, còn pháp luật ATTT lại có bước đi chậm chạp và bất cập. Điều đó tạo ra một khoảng cách nguy hiểm, tạo điều kiện cho các tội phạm máy tính hoành hành gây ra nhiều thiệt hại khôn lường cho nhà nước, các tổ chức và các cá nhân. Phải khẩn trương xây dựng hệ thống pháp luật ATTT hoàn chỉnh, làm cơ sở cho việc đối phó có hiệu quả với các loại tội phạm máy tính, tạo hành lang an toàn cho các hoạt động áp dụng CNTT & TT cũng như công nghệ ATTT vào các lĩnh vực khác nhau của kinh tế, xã hội, an ninh, quốc phòng. Đó là yêu cầu cấp bách đối với nước ta.

Trong các văn bản luật phải khẳng định các quyền lợi trong lĩnh vực thông tin. Các chủ thể phải được ghi nhận về quyền sở hữu và thu nhận trong lĩnh vực thông tin, quyền tham gia các giao tác thông tin theo cách mà pháp luật quy định,

đồng thời bảo đảm an ninh thông tin không bị phá vỡ. Luật pháp về ATTT cần phải định rõ được các kênh "rò rỉ" thông tin, các "lỗ hổng", các điểm yếu có thể của các công nghệ an toàn, thậm chí của các tiêu chuẩn. Đây là nơi hay diễn ra sự vi phạm ATTT cấu thành các tội phạm máy tính. Cùng với các giải pháp công nghệ, pháp luật ATTT phải góp phần bịt kín các lỗ hổng, vá kín các rò rỉ, gia cố các điểm yếu bằng các chế tài quy đinh, hình phạt ở dạng chế định hình sự, dân sự và hành chính.

Luật pháp ATTT phải bảo vệ thông tin và các đối tượng liên quan, các cơ sở hạ tầng thông tin bằng các công cụ đã quen thuộc của sở hữu trí tuệ như bản quyền tác giả, sáng chế độc quyền, bí mật thương mại, nhãn hiệu thương mại... Phải mở rộng các hình thức bảo vệ này cho các đối tượng mới là máy tính và các sản phẩm số hóa như chương trình máy tính, các mã máy tính, các cơ sở dữ liệu...

Bên cạnh đó, cần tuyên truyền vận động và khẩn trương hình thành các bộ chuẩn mực đạo đức cư xử nghề nghiệp trong lĩnh vực máy tính và ATTT. Các chuẩn mực nghề nghiệp này chưa phải là luật định nhưng có tác dụng rất to lớn trong việc định hướng hành vi của xã hội, cổ vũ hướng tới bảo đảm ATTT, lên án, tẩy tray các hành vi xâm phạm ATTT, phá vỡ ATTT.

Câu hỏi và các chủ đề thảo luận, tiểu luận.

1) Vì sao bảo vệ Bí mật nhà nước lại là vấn đề quan tâm hàng đầu của hệ thống pháp luật ATTT của Việt Nam? Vấn đề đó được thể hiện qua pháp luật cơ yếu ra sao?
2) Hãy trình bày các hiểu biết của bạn về quản lý nhà nước về Bảo vệ Bí mật nhà nước, và công tác cơ yếu.
3) Hãy phân tích các khía cạnh pháp luật và đạo đức mà bạn nhận biết qua các vụ đã xảy ra tại nước ta:
    a) Vụ một học sinh phổ thông đột nhập trái phép vào trang web của Bộ giáo dục đào tạo năm 2006. Việc giải quyết vụ này bạn nhận thấy có những kết luận gì cần rút ra.
    b) Vụ lừa đảo kinh doanh trên mạng của Colony Invest.
    c) Vụ tội phạm chống phá nhà nước bằng tuyên truyền tán phát các tài liệu phản động trên mạng.
4) Bạn có muốn trở thành hội viên của Hiệp hội ATTT Việt Nam không? Nếu là hội viên thì bạn hãy cho biết trách nhiệm pháp lý và đạo đức của thành viên Hội như thế nào.
5) Hãy trình bày nhận xét của bạn về phương hướng phát triển của luật pháp an toàn thông tin của nước ta.

PHỤ LỤC 1

PHÁP LỆNH BẢO VỆ BÍ MẬT NHÀ NƯỚC

Để nâng cao trách nhiệm của cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị – xã hội, tổ chức xã hội, tổ chức kinh tế, tổ chức khác, đơn vị vũ trang nhân dân và mọi công dân trong nhiệm vụ bảo vệ bí mật nhà nước, góp phần xây dựng và bảo vệ Tổ quốc.

Căn cứ vào Hiến pháp của nước Cộng hoà xã hội chủ nghĩa Việt Nam năm 1992.

Căn cứ vào Nghị quyết của Quốc hội khóa X, kỳ họp thứ 6 về Chương trình xây dựng luật, pháp lệnh năm 2000.

Pháp lệnh này quy định về bảo vệ bí mật nhà nước.

CHƯƠNG I

Những quy định chung

Điều 1.

Bí mật nhà nước là những tin về vụ, việc, tài liệu, vật, địa điểm, thời gian, lời nói có nội dung quan trọng thuộc lĩnh vực chính trị, quốc phòng, an ninh, đối ngoại, kinh tế, khoa học, công nghệ, các lĩnh vực khác mà Nhà nước không công bố hoặc chưa công bố và nếu bị tiết lộ thi gây nguy hại cho Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam.

Điều 2.

Bảo vệ bí mật nhà nước là nhiệm vụ rất quan trọng của Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam.

Cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị – xã hội, tổ chức xã hội, tổ chức kinh tế, tổ chức khác, đơn vị vũ trang nhân dân (sau đây gọi chung là cơ quan, tổ chức) và mọi công dân đều có nghĩa vụ, trách nhiệm bảo vệ bí mạt nhà nước.

Điều 3.

Nghiêm cấm mọi hành vi thu thập, làm lộ, làm mất, chiếm đoạt, mua bán, tiểu huỷ trái phép bí mật nhà nước và việc lạm dụng bảo vệ bí mật nhà nước để che dấu hành vi vi phạm pháp luật, xâm phạm quyền, lợi ích hợp pháp của cơ quan, tổ chức và công dân hoặc làm cản trở việc thực hiện các kế hoạch nhà nước.

Việc tiếp xúc bảo vệ, bảo quản, cung cấp và xử lý bí mật nhà nước phải thực hiện theo quy định của Chính phủ.

CHƯƠNG II

Phạm vi bí mật nhà nước

Điều 4.

Căn cứ vào tính chất quan trọng của nội dung tin, mức độ nguy hại nếu bị tiết lộ, các tin thuộc phạm vi bí mật nhà nước được chia làm ba mức độ Tuyệt mật, Tối mật và Mật.

Điều 5.

Bí mật nhà nước trong phạm vi sau đây thuộc độ Tuyệt mật:

1. Chiến lược an ninh quốc gia, kế hoạch phòng thủ đất nước, kế hoạch động viên đối phó với chiến tranh; các loại vũ khí, phương tiện có ý nghĩa quyết định khả năng phòng thủ đất nước.
2. Các chủ trương, chính sách về đối nội, đối ngoại của Đảng Cộng sản Việt Nam và Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam không công bố hoặc chưa công bố.

   Những tin của nước ngoài hoặc của các tổ chức quốc tế chuyển giao cho Việt Nam mà Chính phủ xác định thuộc độ Tuyệt mật.
3. Tổ chức và hoạt động tình báo, phản gián do Chính phủ quy định.
4. Mật mã quốc gia.
5. Dự trữ chiến lược quốc gia, các số liệu dự toán, quyết toán ngân sách nhà nước về những lĩnh vực chưa công bố; kế hoạch phát triển, khoá an toàn của từng mẫu tiền và các loại giấy tờ có giá trị như tiền; phương án kế hoạch thu đổi tiền chưa công bố.
6. Khu vực, địa điểm cấm; tin, tài liệu khác mà Chính phủ xác định thuộc độ Tuyệt mật.

Điều 6.

Bí mật nhà nước trong phạm vi sau đây thuộc độ Tối mật:

1. Các cuộc đàn phán và tiếp xúc cấp cao giữa nước ta với nước ngoài hoặc các tổ chức quốc tế về chính trị, quốc phòng, an ninh, đối ngoại, kinh tế, khoa học, công nghệ và các lĩnh vực khác chưa công bố.

   Những tin của nước ngoài hoặc của các tổ chức quốc tế chuyển giao cho Việt Nam mà Chính phủ xác định thuộc độ Tối mật.
2. Tổ chức hoạt động, trang bị, phương án tác chiến của các đơn vị vũ trang nhân dân, trừ tổ chức và hoạt động được quy định tại khoản 3 Điều 5 của Pháp lệnh này; phương án sản xuất, vận chuyển và cất giữa vũ khí mới; công trình quan trọng phòng thủ biên giới, vùng trời, vùng biển, hải đảo.

3. Bản đồ quân sự, toạ độ điểm hạng I, hạng II nhà nước của mạng lưới quốc gia hoàn chỉnh cùng với các ghi chú điểm kèm theo.

   Vị trí và trị số độ cao các mốc chính của các trạm khí tượng, thuỷ văn, hải văn; số liệu độ cao và số không tuyệt đối của các mốc hải văn.

4. Số lượng tiền in, phát hành; tiền dự trữ bằng đồng Việt Nam và ngoại tệ; các số liệu về bội chi, lạm phát tiền mặt chưa công bố; phương án giá các mặt hàng chiến lược thuộc Nhà nước quản lý chưa công bố.

5. Nơi lưu giữ và số lượng kim loại quý hiếm, đá quý, ngoại hối và vật quý hiếm khác của nhà nước.

6. Công trình khoa học, phát minh, sáng chế, giải pháp hữu ích, bí quyết nghề nghiệp đặc biệt quan trọng đối với quốc phòng, an ninh, kinh tế, khoa học, công nghệ mà Nhà nước chưa công bố.

7. Kế hoạch xuất khẩu, nhập khẩu các mặt hàng đặc biệt giữ vị trí trọng yếu trong việc phát triển và bảo vệ đất nước không công bố hoặc chưa công bố.

8. Tin, tài liệu khác mà Chính phủ xác định thuộc độ Tối mật.

Điều 7.

Bí mật nhà nước ngoài phạm vi quy định tại Điều 5 và Điều 6 của Pháp lệnh này thì thuộc độ Mật.

Danh mục bí mật nhà nước thuộc độ Mật do người đứng đầu hoặc người được uỷ quyền của cơ quan, tổ chức đề nghị Bộ trưởng Bộ Công an quyết định.

Điều 8.

Căn cứ vào danh mục bí mật nhà nước thuộc độ Tuyệt mật, Tối mật và Mật đã được cấp có thẩm quyền ban hành theo quy định của Pháp lệnh này, người đứng đầu hoặc người được uỷ quyền của cơ quan, tổ chức quyết định độ mật đối với từng bí mật nhà nước cụ thể.

Điều 9.

Việc lập, quyết định, thay đổi độ mật và giải mật đối với từng bí mật nhà nước phải được tiến hành theo thẩm quyền và thủ tục quy định tại Pháp lệnh này.

CHƯƠNG III

QUẢN LÝ NHÀ NƯỚC VỀ BẢO VỆ BÍ MẬT NHÀ NƯỚC; TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC VÀ CÔNG DÂN VỀ BẢO VỆ BÍ MẬT NHÀ NƯỚC

Điều 10.

Nội dung quản lý nhà nước về bảo vệ bí mật nhà nước gồm:

1. Ban hành và hướng dẫn thi hành các văn bản quy định pháp luật về bảo vệ bí mật nhà nước.
2. Quyết định và giải mật bí mật nhà nước, quy định việc công bố danh mục bí mật nhà nước.
3. Quyết định kinh phí và bảo đảm cơ sở vật chất, kỹ thuật phục vụ công tác bảo vệ bí mật nhà nước.
4. Quy định chế độ, chính sách đối với người trực tiếp làm công tác bảo vệ bí mật nhà nước.
5. Thanh tra, kiểm tra, xử lý vi phạm và giải quyết khiếu nại, tố cáo trong lĩnh vực bảo vệ bí mật nhà nước.
6. Sơ kết, tổng kết công tác bảo vệ bí mật nhà nước.

Điều 11.

1. Chính phủ thống nhất quản lý nhà nước về bảo vệ bí mật nhà nước.
2. Bộ Công an chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về bảo vệ bí mật nhà nước và có nhiệm vụ, quyền hạn sau đây:
    a) Trình Chính phủ, Thủ tướng Chính phủ dự thảo các văn bản quy phạm pháp luật về bảo vệ bí mật nhà nước.
    b) Hướng dẫn cơ quan, tổ chức lập danh mục bí mật nhà nước và thực hiện công tác bảo vệ bí mật nhà nước.
    c) Thẩm định việc lập và giải mật danh mục bí mật nhà nước thuộc độ Tuyệt mật và Tối mật trình Thủ tướng Chính phủ quyết định.
    d) Quyết định và giải mật danh mục bí mật nhà nước thuộc độ Mật sau khi thống nhất với người đứng đầu hoặc người được uỷ quyền của cơ quan, tổ chức có liên quan.
    e) Thanh tra, kiểm tra, xử lý các vi phạm và giải quyết khiếu nại, tố cáo trong lĩnh vực bảo vệ bí mật nhà nước.
    f) Giúp Chính phủ sơ kết, tổng kết công tác bảo vệ bí mật nhà nước.

Điều 12.

Trong phạm vi nhiệm vụ, quyền hạn của mình người đứng đầu hoặc người được uỷ quyền của cơ quan, tổ chức và Chủ tịch Uỷ ban nhân dân các cấp có trách nhiệm sau đây:

1. Tổ chức, thực hiện công tác bảo vệ bí mật nhà nước theo quy định của Pháp lệnh này và các văn bản pháp luật khác có liên quan.

2. Ban hành và tổ chức thực hiện nội quy bảo vệ bí mật nhà nước theo quy định của Chính phủ.
3. Lập danh mục, thay đổi độ mật, giải mật bí mật nhà nước gửi cấp có thẩm quyền quyết định.
4. Bố trí cán bộ làm công tác bảo vệ bí mật nhà nước theo quy định của Chính phủ.
5. Tuyên truyền, giáo dục những người thuộc quyền quản lý của mình nâng cao trách nhiệm, cảnh giác và nghiêm chỉnh chấp hành pháp luật về bảo vệ bí mật nhà nước.
6. Thực hiện chế độ báo cáo về công tác bảo vệ bí mật nhà nước theo quy định của Chính phủ.

Điều 13.

Bộ Quốc phòng có trách nhiệm tổ chức thực hiện công tác bảo vệ bí mật nhà nước trong các cơ quan, đơn vị thuộc phạm vi quản lý của mình theo quy định của Chính phủ.

Điều 14.

Chính phủ quy định việc bảo vệ bí mật nhà nước trong hoạt động xuất bản, báo chí và thông tin đại chúng khác phù hợp với quy định của Pháp lệnh này.

Điều 15.

Nội dung bí mật nhà nước nếu tuyên truyền đưa bằng phương tiện viễn thông và máy tính thì phải được mã hoá theo quy định của pháp luật về cơ yếu.

Điều 16.

Công trình khoa học, phát minh, sáng chế, giải pháp hữu ích của cơ quan, tổ chức hoặc công dân có liên quan đến nội dung bí mật nhà nước phải đăng ký tại cơ quan nhà nước có thẩm quyền và được bảo vệ theo quy định của pháp luật.

Điều 17.

Cơ quan, tổ chức, công dân Việt Nam tiếp xúc với tổ chức, cá nhân nước ngoài phải tuân thủ các quy định của pháp luật về bảo vệ bí mật nhà nước; khi tiến hành chương trình hợp tác quốc tế có liên quan đến bí mật nhà nước thì phải được sự đồng ý của cơ quan nhà nước có thẩm quyền về bảo vệ bí mật nhà nước.

Điều 18.

Người làm công tác bảo vệ bí mật nhà nước phải có phẩm chất tốt, có trình độ chuyên môn nghiệp vụ, có năng lực hoàn thành nhiệm vụ được giao và phải cam kết bảo vệ bí mật nhà nước.

Người được giao nhiệm vụ tiếp xúc với bí mật nhà nước phải cam kết bảo vệ bí mật nhà nước.

CHƯƠNG IV

KHEN THƯỞNG VÀ XỬ LÝ VI PHẠM

Điều 19.

Cơ quan tổ chức và công dân có thành tích bảo vệ bí mật nhà nước thì được khen thưởng theo quy định của pháp luật.

Điều 20.

Người nào vi phạm các quy định của Pháp lệnh này và các quy định khác của pháp luật về bảo vệ bí mật nhà nước thì tuỳ theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc truy cứu trách nhiệm hình sự; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luât.

CHƯƠNG V

ĐIỀU KHOẢN THI HÀNH

Điều 21.

Pháp lệnh này có hiệu lực kể từ ngày 01 tháng 04 năm 2001.

Pháp lệnh này thay thế Pháp lệnh bảo vệ bí mật nhà nước ngày 28 tháng 10 năm 1991.

Những quy định trước đây trái với Pháp lệnh này đều bãi bỏ.

Điều 22.

Chính phủ quy định chi tiết và hướng dẫn thi hành Pháp lệnh này.

Hà Nội, ngày 28 tháng 12 năm 2000

TM. UỶ BAN THƯỜNG VỤ QUỐC HỘI

Chủ tịch

NÔNG ĐỨC MẠNH

PHỤ LỤC 2

QUỐC HỘI

NƯỚC CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

Khoá XI, kỳ họp thứ 9

(Từ ngày 16 tháng 5 đến ngày 29 tháng 6 năm 2006)

LUẬT CÔNG NGHỆ THÔNG TIN

Căn cứ vào Hiến pháp nước Cộng hoà xã hội chủ nghĩa Việt Nam năm 1992 đã được sửa đổi, bổ sung theo Nghị quyết số 51/2001/QH10 ngày 25 tháng 12 năm 2001 của Quốc hội khoá X, kỳ họp thứ 10;

Luật này quy định về công nghệ thông tin.

Chương I

NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Luật này quy định về hoạt động ứng dụng và phát triển công nghệ thông tin, các biện pháp bảo đảm ứng dụng và phát triển công nghệ thông tin, quyền và nghĩa vụ của cơ quan, tổ chức, cá nhân (sau đây gọi chung là tổ chức, cá nhân) tham gia hoạt động ứng dụng và phát triển công nghệ thông tin.

Điều 2. Đối tượng áp dụng

Luật này áp dụng đối tổ chức, cá nhân Việt Nam, tổ chức, cá nhân nước ngoài tham gia hoạt động ứng dụng và phát triển công nghệ thông tin tại Việt Nam.

Điều 3. Áp dụng Luật công nghệ thông tin

1. Trường hợp có sự khác nhau giữa quy định của Luật công nghệ thông tin với quy định của luật khác về cùng một vấn đề liên quan đến hoạt động ứng dụng và phát triển công nghệ thông tin thì áp dụng quy định của Luật công nghệ thông tin.

2. Trường hợp điều ước quốc tế mà Cộng hoà xã hội chủ nghĩa Việt Nam là thành viên có quy định khác với quy định của Luật này thì áp dụng quy định của điều ước quốc tế đó.

Điều 4. Giải thích từ ngữ

Trong Luật này, các từ ngữ dưới đây được hiểu như sau:

1. *Công nghệ thông tin* là tập hợp các phương pháp khoa học, công nghệ và công cụ kỹ thuật hiện đại để sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số.

2. *Thông tin số* là thông tin được tạo lập bằng phương pháp dùng tín hiệu số.

3. *Môi trường mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua cơ sở hạ tầng thông tin.

4. *Cơ sơ hạ tầng thông tin* là hệ thống trang thiết bị phục vụ cho việc sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số, bao gồm mạng viễn thông, mạng Internet, mạng máy tính và cơ sở dữ liệu.

5. *Ứng dụng công nghệ thông tin* là việc sử dụng công nghệ thông tin vào các hoạt động thuộc lĩnh vực kinh tế – xã hội, đối ngoại, quốc phòng, an ninh và các hoạt động khác nhằm nâng cao năng suất, chất lượng, hiệu quả của hoạt động này.

6. *Phát triển công nghệ thông tin* là hoạt động nghiên cứu – phát triển liên quan đến quá trình sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số; phát triển nguồn nhân lực công nghệ thông tin; phát triển công nghiệp công nghệ thông tin và phát triển dịch vụ công nghệ thông tin.

7. *Khoảng cách số* là sự chênh lệch về điều kiện, khả năng sử dụng máy tính và cơ sở hạ tầng thông tin để truy nhập các nguồn thông tin, tri thức.

8. *Đầu tư mạo hiểm trong lĩnh vực công nghệ thông tin* là đầu tiên cho doanh nghiệp hoạt động trong lĩnh vực đó có triển vọng đem lại lợi nhuận lớn nhưng có rủi ro cao.

9. *Công nghiệp công nghệ thông tin* là ngành kinh tế – kỹ thuật công nghệ cao sản xuất và cung cấp sản phẩm công nghệ thông tin, bao gồm sản phẩm phần cứng, phần mềm và nội dung thông tin số.

10.*Phần cứng* là sản phẩm thiết bị số hoàn chỉnh; cụm linh kiện; linh kiện; bộ phận của thiết bị số, cụm linh kiện, linh kiện.

11.*Thiết bị số* là thiết bị điện tử, máy tính, viễn thông, truyền dẫn, thu phát sóng vô tuyến điện và thiết bị tích hợp khác được sử dụng để sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số.

12.*Phần mềm* là chương trình máy tính được mô tả bằng hệ thống ký hiệu, mã hoặc ngôn ngữ để điều khiển thiết bị số thực hiện chức năng nhất định.

13.*Mã nguồn* là sản phẩm trước biên dịch của một phần mềm, chưa có khả năng điều khiển thiết bị số.

14.*Mã máy* là sản phẩm sau biên dịch của một phần mềm, có khả năng điều khiển thiết bị số.

15.*Thư rác* là thư điện tử, tin nhắn được gửi đến người nhận mà người nhận đó không mong muốn hoặc không có trách nhiệm phải tiếp nhận theo quy định của pháp luật.

16.*Vi rút máy tính* là chương trình máy tính có khả năng lây lan, gây ra hoạt động không bình thường cho thiết bị số hoặc sao chép, sửa đổi, xoá bỏ thông tin lưu trữ trong thiết bị số.

17.*Trang thông tin điện tử (Website)* là trang thông tin hoặc một tập hợp trang thông tin trên môi trường mạng phục vụ cho việc cung cấp, trao đổi thông tin.

18.*Số hoá* là việc biến đổi các loại hình thông tin sang thông tin số.

Điều 5. Chính sách của Nhà nước về ứng dụng và phát triển công nghệ thông tin

1. Ưu tiên ứng dụng và phát triển công nghệ thông tin trong chiến lược phát triển kinh tế – xã hội và sự nghiệp công nghiệp hoá, hiện đại hoá đất nước.

2. Tạo điều kiện để tổ chức, cá nhân hoạt động ứng dụng và phát triển công nghệ thông tin đáp ứng yêu cầu phát triển kinh tế – xã hội, đối ngoại, quốc phòng, an ninh; thúc đẩy công nghiệp công nghệ thông tin phát triển thành ngành kinh tế trọng điểm, đáp ứng nhu cầu thị trường nội địa và xuất khẩu.

3. Khuyến khích đầu tư cho lĩnh vực công nghệ thông tin.

4. Ưu tiên dành một khoản ngân sách nhà nước để ứng dụng công nghệ thông tin trong một số lĩnh vực thiết yếu, tạo lập nền công nghiệp công nghệ thông tin và phát triển nguồn nhân lực công nghệ thông tin.

5. Tạo điều kiện thuận lợi để phát triển cơ sở hạ tầng thông tin quốc gia.

6. Có chính sách ưu đãi để tổ chức, cá nhân có hoạt động ứng dụng và phát triển công nghệ thông tin đối với nông nghiệp; nông thôn, vùng sâu, vùng xa, biên giới, hải đảo; người dân tộc thiểu số, người tàn tật, người có hoàn cảnh khó khăn.

7. Bảo đảm quyền lợi và lợi ích hợp pháp của tổ chức, cá nhân ứng dụng và phát triển công nghệ thông tin.

8. Tăng cường giao lưu và hợp tác quốc tế; khuyến khích hợp tác với tổ chức, cá nhân Việt Nam ở nước ngoài trong lĩnh vực công nghệ thông tin.

Điều 6. Nội dung quản lý Nhà nước về công nghệ thông tin

1. Xây dựng, tổ chức thực hiện chiến lược, quy hoạch, kế hoạch, chính sách ứng dụng và phát triển công nghệ thông tin.

2. Xây dựng, ban hành, tuyên truyền, phổ biến, tổ chức thực hiện văn bản quy phạm pháp luật, tiêu chuẩn quốc gia, quy chuẩn kỹ thuật trong lĩnh vực công nghệ thông tin.

3. Quản lý an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin.

4. Tổ chức quản lý và sử dụng tài nguyên thông tin cơ sở dữ liệu quốc gia.

5. Quản lý và tạo điều kiện thúc đẩy công tác hợp tác quốc tế về công nghệ thông tin.

6. Quản lý, đào tạo, bồi dưỡng và phát triển nguồn nhân lực công nghệ thông tin.

7. Xây dựng cơ chế, chính sách và các quy định liên quan đến sản phẩm, dịch vụ công ích trong lĩnh vực công nghệ thông tin.

8. Xây dựng cơ chế, chính sách và các quy định về việc huy động nguồn nhân lực công nghệ thông tin phục vụ quốc phòng, an ninh và các trường hợp khẩn cấp quy định tại Điều 14 của Luật này.

9. Quản lý thống kê về công nghệ thông tin.

10.Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm trong lĩnh vực công nghệ thông tin.

Điều 7. Trách nhiệm quản lý Nhà nước về công nghệ thông tin

1. Chính phủ thống nhất quản lý nhà nước về công nghệ thông tin.

2. Bộ Bưu chính, Viễn thông chịu trách nhiệm trước Chính phủ trong việc chủ trì, phối hợp với Bộ, cơ quan ngang Bộ có liên quan thực hiện quản lý nhà nước về công nghệ thông tin.

3. Bộ, cơ quan ngang Bộ trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm chủ trì, phối hợp với Bộ Bưu chính, Viễn thông thực hiện quản lý nhà nước về công nghệ thong tin theo phân công của Chính phủ.

4. Uỷ ban nhân dân tỉnh, thành phố trực thuộc trung ương trong phạm vi nhiệm vụ, quyền hạn của mình thực hiện quản lý nhà nước về công nghệ thông tin tại địa phương.

5. Việc tổ chức thực hiện ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước do Chính phủ quy định.

Điều 8. Quyền của tổ chức, cá nhân tham gia hoạt động ứng dụng và phát triển công nghệ thông tin

1. Tổ chức, cá nhân tham gia hoạt động ứng dụng công nghệ thông tin có các quyền sau đây:

a) Tìm kiếm, trao đổi, sử dụng thông tin trên môi trường mạng, trừ thông tin có nội dung quy định tại khoản 2 Điều 12 của Luật này.

b) Yêu cầu khôi phục thông tin của mình hoặc khôi phục khả năng truy nhập đến nguồn thông tin của mình trong trường hợp nội dung thông tin đó không vi phạm quy định tạii khoản 2 Điều 12 của Luật này.

c) Yêu cầu cơ quan nhà nước có thẩm quyền giải quyết theo quy định của pháp luật trong trường hợp bị từ chối việc khôi phục thông tin hoặc khôi phục khả năng truy nhập đến nguồn thông tin đó.

d) Phân phát các địa chỉ liên lạc có trên môi trường mạng khi có sự đồng ý của chủ sở hữu địa chỉ liên lạc đó.

e) Từ chội cung cấp hoặc nhận trên môi trường mạng sản phẩm, dịch vụ trái với quy định của pháp luật và phải chịu trách nhiệm về việc đó.

2. Tổ chức, cá nhân tham gia phát triển công nghệ thông tin có các quyền sau đây:

a) Nghiên cứu và phát triển sản phẩm công nghệ thông tin.

b) Sản xuất sản phẩm công nghệ thông tin; số hoá, duy trì và làm tăng giá trị các nguồn tài nguyên thông tin.

3. Cơ quan nhà nước có quyền từ chối nhận thông tin trên môi trường mạng nếu độ tin cậy và bí mật của thông tin đó được truyền đưa qua môi trường mạng không được bảo đảm.

Điều 9. Trách nhiệm của tổ chức, cá nhân tham gia hoạt động ứng dụng và phát triển công nghệ thông tin

1. Tổ chức, cá nhân tham gia hoạt động ứng dụng công nghệ thông tin chịu trách nhiệm về nội dung thông tin số của mình trên môi trường mạng.

2. Tổ chức, cá nhân khi hoạt động kinh doanh trên môi trường mạng phải thông báo công khai trên môi trường mạng những thông tin có liên quan, bao gồm:

a) Tên, địa chỉ địa lý, số điện thoại, địa chỉ thư điện tử.

b) Thông tin về quyết định thành lập, giấy phép hoạt động hoặc giấy chứng nhận đăng ký kinh doanh (nếu có).

c) Tên cơ quan quản lý nhà cung cấp (nếu có).

d) Thông tin về giá, thuế, chi phí vận chuyển (nếu có) của hàng hoá, dịch vụ.

3. Tổ chức, cá nhân tham gia phát triển công nghệ thông tin có trách nhiệm sau đây:

a) Bảo đảm tính trung thực của kết quả nghiên cứu, phát triển.

b) Bảo đảm quyền và lợi ích hợp pháp của chủ sở hữu cơ sở dữ liệu và không gây cản trở cho việc sử dụng cơ sở dữ liệu đó khi thực hiện hành vi tái sản xuất, phân phối, quảng bá, truyền đưa, cung cấp nội dung hợp thành cơ sở dữ liệu đó.

4. Khi hoạt động trên môi trường mạng, cơ quan nhà nước có trách nhiệm sau đây:

a) Thông báo trên phương tiện thông tin đại chúng về các hoạt động thực hiện trên môi trường mạng theo quy định tại khoản 1 Điều 27 của Luật này.

b) Thông báo cho tổ chức, cá nhân có liên quan địa chỉ liên hệ của cơ quan đó trên môi trường mạng.

c) Trả lời theo thẩm quyền văn bản của tổ chức, cá nhân gửi đến cơ quan nhà nước thông qua môi trường mạng.

d) Cung cấp trên môi trường mạng thông tin phục vụ lợi ích công cộng, thủ tục hành chính.

e) Sử dụng chữ ký điện tử theo quy định của pháp luật về giao dịch điện tử.

f) Bảo đảm độ tin cậy và bí mật của nội dung thông tin trong việc gửi, nhận văn bản trên môi trường mạng.

g) Bảo đảm tính chính xác, đầy đủ, kịp thời của thông tin, văn bản được trao đổi, cung cấp và lấy ý kiến trên môi trường mạng.

h) Bảo đảm hệ thống thiết bị cung cấp thông tin, lấy ý kiến trên môi trường mạng hoạt động cả trong giờ và ngoài giờ làm việc, trừ trường hợp bất khả kháng.

i) Thực hiện việc cung cấp thông tin và lấy ý kiến qua trang thông tin điện tử phải tuân thủ quy định tại Điều 28 của Luật này.

Điều 10. Thanh tra về công nghệ thông tin

1. Thanh tra Bộ Bưu chính, Viễn thông thực hiện chức năng thanh tra chuyên ngành về công nghệ thông tin.

2. Tổ chức và hoạt động của thanh tra về công nghệ thông tin thực hiện theo quy định của pháp luật về thanh tra.

Điều 11. Hội, hiệp hội về công nghệ thông tin

1. Hội, hiệp hội về công nghệ thông tin có trách nhiệm bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân tham gia hoạt động ứng dụng và phát triển công nghệ thông tin.

2. Hội, hiệp hội về công nghệ thông tin được tổ chức và hoạt động theo quy định của pháp luật về hội.

Điều 12. Các hành vi bị nghiêm cấm

1. Cản trở hoạt động hợp pháp hoặc hỗ trợ hoặc hoạt động bất hợp pháp về ứng dụng và phát triển công nghệ thông tin; cản trở bất hợp pháp hoạt động của hệ thống máy chủ tên miền quốc gia; phá hoại cơ sở hạ tầng thông tin, phá hoại thông tin trên môi trường mạng.

2. Cung cấp, trao đổi, truyền đưa, lưu trữ, sử dụng thông tin số nhằm mục đích sau đây:

a) Chống Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam, phá hoại khối đoàn kết toàn dân.

b) Kích động bạo lực, tuyên truyền chiến tranh xâm lược, gây hận thù giữa các dân tộc và nhân dân các nước, kích động dâm ô, đồi truỵ, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong mỹ tục của dân tộc.

c) Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác đã được pháp luật quy định.

d) Xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự, nhân phẩm, uy tín của công dân.

e) Quảng cáo, tuyên truyền hàng hoá, dịch vụ thuộc danh mục cấm đã được pháp luật quy định.

3. Xâm phạm quyền sở hữu trí tuệ trong hoạt động công nghệ thông tin; sản xuất, lưu hành sản phẩm công nghệ thông tin trái pháp luật; giả mạo trang thông tin điện tử của tổ chức, cá nhân khác; tạo đường dẫn trái phép đối với tên miền của tổ chức, cá nhân sử dụng hợp pháp tên miền đó.

Chương II

ỨNG DỤNG CÔNG NGHỆ THÔNG TIN

Mục 1

QUY ĐỊNH CHUNG VỀ ỨNG DỤNG CÔNG NGHỆ THÔNG TIN

Điều 13. Nguyên tắc chung về hoạt động ứng dụng công nghệ thông tin

1. Tổ chức cá nhân có quyền tiến hành các hoạt động ứng dụng công nghệ thông tin theo quy định của Luật này và các quy định khác của pháp luật có liên quan.

2. Việc ứng dụng công nghệ thông tin vào các hoạt động thuộc lĩnh vực kinh tế – xã hội, đối ngoại, quốc phòng, an ninh; hoạt động phòng chống lụt bão, thiên tai, thảm hoạ khác, cứu hộ, cứu nạn và các hoạt động khác được Nhà nước khuyến khích.

3. Tổ chức, cá nhân tiến hành hoạt động viễn thông, hoạt động phát thanh, truyền hình trên môi trường mạng phải thực hiện các quy định của pháp luật về viễn thông, báo chí và các quy định của Luật này.

Điều 14. Ưu tiên ứng dụng công nghệ thông tin trong trường hợp khẩn cấp

1. Cơ quan nhà nước có thẩm quyền quyết định huy động một phần hoặc toàn bộ cơ sở hạ tầng thông tin để ưu tiên phục vụ cho việc ứng dụng công nghệ thông tin khi có một trong các trường hợp khẩn cấp sau đây:

a) Phục vụ phòng, chống lụt, bão, hoả hoạn, thiên tai, thảm hoạ khác.

b) Phục vụ cấp cứu và phòng chống dịch bệnh.

c) Phục vụ cứu nạn, cứu hộ.

d) Phục vụ quốc phòng, an ninh, bảo đảm trật tự, an toàn xã hội, phòng chống tội phạm.

2. Chính phủ quy định cụ thể việc ưu tiên ứng dụng công nghệ thông tin trong các trường hợp khẩn cấp.

Điều 15. Quản lý và sử dụng thông tin số

1. Tổ chức, cá nhân có quyền tự do sử dụng thông tin số vào mục đích chính đáng, phù hợp với quy định của pháp luật.

2. Cơ quan nhà nước có thẩm quyền chịu trách nhiệm thực hiện các biện pháp bảo đảm việc truy nhập và sử dụng thuận lợi thông tin số.

3. Việc cung cấp, trao đổi, truyền đưa, lưu trữ, sử dụng thông tin số phải bảo đảm không vi phạm quy định tại khoản 2 Điều 12 của Luật này và các quy định khác của pháp luật có liên quan.

4. Tổ chức, cá nhân không được trích dẫn nội dung thông tin số của tổ chức, cá nhân khác trong trường hợp chủ sở hữu thông tin số đã có cảnh báo hoặc pháp luật quy định việc trích dẫn thông tin là không được phép.

5. Trường hợp được phép trích dẫn thông tin số, tổ chức, cá nhân có trách nhiệm nêu rõ nguồn của thông tin đó.

Điều 16. Truyền đưa thông tin số

1. Tổ chức, cá nhân có quyền truyền đưa thông tin số của tổ chức, cá nhân khác phù hợp với quy định của Luật này.

2. Tổ chức, cá nhân truyền đưa thông tin số của tổ chức, cá nhân khác không phải chịu trách nhiệm về nội dung thông tin được lưu trữ tự động, trung gian, tạm thời do yêu cầu kỹ thuật nếu hoạt động lưu trữ tạm thời nhằm mục đích phục vụ cho việc truyền đưa thông tin và thông tin được lưu trữ trong khoảng thời gian đủ để thực hiện việc truyền đưa.

3. Tổ chức, cá nhân truyền đưa thông tin số có trách nhiệm tiến hành kịp thời các biện pháp cần thiết để ngăn chặn việc truy nhập thông tin hoặc loại bỏ thông tin trái pháp luật theo yêu cầu của cơ quan nhà nước có thẩm quyền.

4. Tổ chức, cá nhân truyền đưa thông tin số của tổ chức, cá nhân khác không phải chịu trách nhiệm về nội dung thông tin đó, trừ trường hợp thực hiện một trong các hành vi sau đây:

a) Chính mình bắt đầu việc truyền đưa thông tin.

b) Lựa chọn người nhận thông tin được truyền đưa.

c) Lựa chọn và sửa đổi nội dung thông tin được truyền đưa.

Điều 17. Lưu trữ tạm thời thông tin số

1. Tổ chức, cá nhân có quyền lưu trữ tạm thời thông tin số của tổ chức, cá nhân khác.

2. Tổ chức, cá nhân lưu trữ tạm thời thông tin số của tổ chức, cá nhân khác không phải chịu trách nhiệm về nội dung thông tin đó, trừ trường hợp thực hiện một trong các hành vi sau đây:

a) Sửa đổi nội dung thông tin.

b) Không tuân thủ quy định về truy nhập hoặc cập nhật nội dung thông tin.

c) Thu thập dữ liệu bất hợp pháp thông qua việc lưu trữ thông tin tạm thời.

d) Tiết lộ bí mật thông tin.

Điều 18. Cho thuê chỗ lưu trữ thông tin số

1. Cho thuê chỗ lưu trữ thông tin số là dịch vụ cho thuê dung lượng thiết bị lưu trữ để lưu trữ thông tin trên môi trường mạng.

2. Nội dung thông tin số lưu trữ không được vi phạm quy định tại khoản 2 Điều 12 của Luật này.

3. Tổ chức, cá nhân cho thuê chỗ lưu trữ thông tin số có trách nhiệm sau đây:

a) Thực hiện việc yêu cầu của cơ quan nhà nước có thẩm quyền về việc xác định danh sách chủ sở hữu thuê chỗ lưu trữ thông tin số để thiết lập trang thông tin điện tử và danh sách chủ sở hữu thông tin số được lưu trữ bởi tổ chức, cá nhân đó.

b) Tiến hành kịp thời các biện pháp cần thiết để ngăn chặn việc truy nhập thông tin số hoặc loại bỏ thông tin số trái pháp luật theo yêu cầu của cơ quan nhà nước có thẩm quyền.

c) Ngừng cho tổ chức, cá nhân khác thuê chỗ lưu trữ thông tin số trong trường hợp tự mình pháp hiện hoặc được cơ quan nhà nước có thẩm quyền thông báo cho biết thông tin đang được lưu trữ là trái pháp luật.

d) Bảo đảm bí mật thông tin của tổ chức, cá nhân thuê chỗ lưu trữ thông tin.

Điều 19. Công cụ tìm kiếm thông tin số

1. Công cụ tìm kiếm thông tin số là chương trình máy tính tiếp nhận yêu cầu tìm kiếm thông tin số, thực hiện việc tìm kiếm thông tin số và gửi lại thông tin tìm kiếm được.

2. Nhà nước có chính sách khuyến khích tổ chức cá nhân phát triển, cung cấp công cụ tìm kiếm thông tin số.

3. Tổ chức, cá nhân có trách nhiệm ngừng cung cấp cho tổ chức, cá nhân khác công cụ tìm kiếm đến các nguồn thông tin số trong trường hợp tự mình phát hiện hoặc được cơ quan nhà nước có thẩm quyền thông báo cho biết thông tin đó là trái pháp luật.

Điều 20. Theo dõi, giám sát nội dung thông tin số

1. Cơ quan nhà nước có thẩm quyền chịu trách nhiệm theo dõi, giám sát thông tin số; điều tra hành vi vi phạm pháp luật xảy ra trong quá trình truyền đưa hoặt lưu trữ thông tin số.

2. Tổ chức, cá nhân tham gia ứng dụng công nghệ thông tin không phải chịu trách nhiệm theo dõi, giám sát thông tin số của tổ chức, cá nhân khác, điều tra các hành vi vi phạm pháp luật xảy ra trong quá trình truyền đưa hoặc lưu trữ thông tin số của tổ chức, cá nhân khác, trừ trường hợp cơ quan nhà nước có thẩm quyền yêu cầu.

Điều 21. Thu thập, xử lý và sử dụng thông tin cá nhân trên môi trường mạng

1. Tổ chức, cá nhân thu thập, xử lý và sử dụng thông tin cá nhân của người khác trên môi trường mạng phải được người đó đồng ý, trừ trường hợp pháp luật có quy định khác.

2. Tổ chức, cá nhân thu thập, xử lý và sử dụng thông tin cá nhân của người khác có trách nhiệm sau đây:

a) Thông báo cho người đó biết về hình thức, phạm vi, địa điểm và mục đích của việc thu thập, xử lý và sử dụng thông tin cá nhân của người đó.

b) Sử dụng đúng mục đích thông tin cá nhân thu thập được và chỉ lưu trữ những thông tin đó trong một khoảng thời gian nhất định theo quy định của pháp luật hoặc theo thoả thuận giữa hai bên.

c) Tiến hành các biện pháp quản lý, kỹ thuật cần thiết để bảo đảm thông tin cá nhân không bí mất, đánh cắp, tiết lộ, thay đổi hoặc phá huỷ.

d) Tiến hành ngay các biện pháp cần thiết khi nhận được yêu cầu kiểm tra lại, đính chính hoặc huỷ bỏ theo quy định tại khoản 1 Điều 22 của Luật này; không được cung cấp hoặc sử dụng thông tin cá nhân liên quan cho đến khi thông tin đó được đính chính lại.

3. Tổ chức, cá nhân có quyền thu thập, xử lý và sử dụng thông tin cá nhân của người khác mà không cần sự đồng ý của người đó trong trường hợp thông tin cá nhân của người đó được sử dụng cho mục đích sau đây:

a) Ký kết, sửa đổi hoặc thực hiện hợp đồng sử dụng thông tin, sản phẩm, dịch vụ trên môi trường mạng.

b) Tính giá, cước sử dụng thông tin, sản phẩm, dịch vụ trên môi trường mạng.

c) Thực hiện nghĩa vụ khác theo quy định của pháp luật.

Điều 22. Lưu trữ, cung cấp thông tin cá nhân trên môi trường mạng

1. Cá nhân có quyền yêu cầu tổ chức, cá nhân lưu trữ thông tin cá nhân của mình trên môi trường mạng thực hiện việc kiểm tra, đính chính hoặc huỷ bỏ thông tin đó.

2. Tổ chức, cá nhân không được cung cấp thông tin cá nhân của người khác cho bên thứ ba, trừ trường hợp pháp luật có quy định khác hoặc có sự đồng ý của người đó.

3. Cá nhân có quyền yêu cầu bồi thường thiệt hại do hành vi vi phạm trong việc cung cấp thông tin cá nhân.

Điều 23. Thiết lập trang thông tin điện tử

1. Tổ chức, cá nhân có quyền thiết lập trang thông tin điện tử theo quy định của pháp luật và chịu trách nhiệm quản lý nội dung và hoạt động trang thông tin điện tử của mình.

2. Tổ chức, cá nhân sử dụng tên miền quốc gia Việt Nam ".vn" khi thiết lập trang thông tin điện tử không cần thông báo với Bộ Bưu chính, Viễn thông. Tổ chức, cá nhân khi thiết lập trang thông tin điện tử không sử dụng tên miền quốc gia Việt Nam ".vn" phải thôngbáo trên môi trường mạng với Bộ Bưu chính, Viễn thông những thông tin sau đây:

a) Tên tổ chức ghi trong quyết định thành lập, giấy phép hoạt động, giấy chứng nhận đăng ký kinh doanh hoặc giấy phép mở văn phòng đại diện; tên cá nhân.

b) Số, ngày cấp, nơi cấp chứng minh thư nhân dân hoặc số, ngày cấp, nơi cấp hộ chiếu của cá nhân.

c) Địa chỉ trụ sở chính của tổ chức hoặc nơi thường trú của cá nhân.

d) Số điện thoại, số fax, địa chỉ thư điện tử.

e) Các tên miền đã đăng ký.

3. Tổ chức, cá nhân phải chịu trách nhiệm trước pháp luật về tính chính xác của các thông tin quy định tại khoản 2 Điều này, khi thay đổi thông tin thì phải thông báo về sự thay đổi đó.

4. Trang thông tin điện tử được sử dụng cho hoạt động báo chí phải thực hiện quy định của Luật này, pháp luật về báo chí và các quy định khác của pháp luật có liên quan.

5. Trang thông tin điện tử được sử dụng cho hoạt động kinh tế – xã hội, đối ngoại, quốc phòng, an ninh phải thực hiện quy định của Luật này và các quy định khác của pháp luật có liên quan.

Mục 2

ỨNG DỤNG CÔNG NGHỆ THÔNG TIN TRONG HOẠT ĐỘNG CỦA CƠ QUAN NHÀ NƯỚC

Điều 24. Nguyên tắc ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước

1. Việc ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước phải được ưu tiên, bảo đảm tính công khai, minh bạch nhằm nâng cao hiệu lực, hiệu quả hoạt động của cơ quan nhà nước; tạo điều kiện để nhân dân thực hiện tốt quyền và nghĩa vụ công dân.

2. Việc ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước phải thúc đẩy chương trình đổi mới hoạt động của cơ quan nhà nước và chương trình cải cách hành chính.

3. Việc cung cấp, trao đổi thông tin phải bảo đảm chính xác và phù hợp với mục đích sử dụng.

4. Quy trình, thủ tục hoạt động phải công khai minh bạch.

5. Sử dụng thống nhất tiêu chuẩn, bảo đảm tính tương thích về công nghệ thông tin của cơ quan nhà nước.

6. Bảo đảm an ninh, an toàn, tiết kiệm và có hiệu quả.

7. Người đứng đầu cơ quan nhà nước phải chịu trách nhiệm về việc ứng dụng công nghệ thông tin thuộc thẩm quyền quản lý của mình.

Điều 25. Điều kiện để triển khai ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước

1. Cơ quan nhà nước có trách nhiệm chuẩn bị các điều kiện để triển khai ứng dụng công nghệ thông tin trong hoạt động của cơ quan mình.

2. Chính phủ quy định cụ thể các điều kiện bảo đảm cho ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước; xây dựng và tổ chức thực hiện chương trình quốc gia về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước với nội dung chủ yếu sau đây:

a) Lộ trình thực hiện các hoạt động trên môi trường mạng của các cơ quan nhà nước.

b) Các ngành, lĩnh vực có tác động lớn đến phát triển kinh tế – xã hội cần ưu tiên ứng dụng công nghệ thông tin.

c) Việc chia sẻ, sử dụng chung thông tin số.

d) Lĩnh vực được ưu tiên, khuyến khích nghiên cứu – phát triển, hợp tác quốc tế, phát triển nguồn nhân lực và xây dựng cơ sở hạ tầng thông tin đáp ứng yêu cầu ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước trong từng giai đoạn.

e) Nguồn tài chính bảo đảm cho ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

f) Các chương trình, đề án, dự án trọng điểm về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

Điều 26. Nội dung ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước

1. Xây dựng và sử dụng cơ sở hạ tầng thông tin phục vụ cho hoạt động của cơ quan nhà nước và hoạt động trao đổi, cung cấp thông tin giữa cơ quan nhà nước với tổ chức, cá nhân.

2. Xây dựng, thu thập và duy trì cơ sở dữ liệu phục vụ cho hoạt động của cơ quan và phục vụ lợi ích công cộng.

3. Xây dựng các biểu mẫu phục vụ cho việc trao đổi, cung cấp thông tin và lấy ý kiến góp ý của tổ chức, cá nhân trên môi trường mạng.

4. Thiết lập trang thông tin điện tử phù hợp với quy định tại Điều 23 và Điều 28 của Luật này.

5. Cung cấp, chia sẻ thông tin với cơ quan khác của nhà nước.

6. Thực hiện việc cung cấp dịch vụ công trên môi trường mạng.

7. Xây dựng, thực hiện kế hoạch đào tạo, nâng cao nhận thức và trình độ ứng dụng công nghệ thông tin của cán bộ, công chức.

8. Thực hiện hoạt động trên môi trường mạng theo quy định tại Điều 27 của Luật này.

Điều 27. Hoạt động của cơ quan nhà nước trên môi trường mạng

1. Hoạt động của cơ quan nhà nước trên môi trường mạng bao gồm:

a) Cung cấp, trao đổi, thu thập thông tin với tổ chức, cá nhân.

b) Chia sẻ thông tin trong nội bộ và với cơ quan khác của Nhà nước.

c) Cung cấp các dịch vụ công.

d) Các hoạt động khác theo quy định của Chính phủ.

2. Thời điểm và địa điểm gửi, nhận thông tin trên môi trường mạng thực hiện theo quy định của pháp luật về giao dịch điện tử.

Điều 28. Trang thông tin điện tử của cơ quan nhà nước

1. Trang thông tin điện tử của cơ quan nhà nước phải đáp ứng các yêu cầu sau đây:

a) Bảo đảm cho tổ chức, cá nhân truy nhập thuận tiện.

b) Hỗ trợ tổ chức, cá nhân truy nhập và sử dụng các biểu mẫu trên trang thông tin điện tử (nếu có).

c) Bảo đảm tính chính xác và sự thống nhất về nội dung của thông tin trên trang thông tin điện tử.

d) Cập nhật thường xuyên và kịp thời thông tin trên trang thông tin điện tử.

e) Thực hiện quy định của pháp luật về bảo vệ bí mật nhà nước.

2. Trang thông tin điện tử của cơ quan nhà nước phải có những thông tin chủ yếu sau đây:

a) Tổ chức, chức năng, nhiệm vụ, quyền hạn của cơ quan đó và của từng đơn vị trực thuộc.

b) Hệ thống văn bản quy phạm pháp luật chuyên ngành và văn bản pháp luật có liên quan.

c) Quy trình, thủ tục hành chính được thực hiện bởi các đơn vị trực thuộc, tên của người chịu trách nhiệm trong từng khâu thực hiện quy trình, thủ tục hành chính, thời hạn giải quyết các thủ tục hành chính.

d) Thông tin tuyên truyền, phổ biến, hướng dẫn thực hiện pháp luật, chế đố, chính sách, chiến lược, quy hoạch chuyên ngành.

e) Danh mục địa chỉ thư điện tử chính thức của từng đơn vị trực thuộc và cán bộ, công chức có thẩm quyền.

f) Thông tin về dự án, hạng mục đầu tư, đấu thầu, mua sắm công.

g) Danh mục các hoạt động trên môi trường mạng đang được cơ quan đó thực hiện theo quy định tại khoản 1 Điều 27 của Luật này.

h) Mục lấy ý kiến góp ý của tổ chức, cá nhân.

3. Cơ quan nhà nước cung cấp miễn phí thông tin quy định tại khoản 2 Điều này.

Mục 3

ỨNG DỤNG CÔNG NGHỆ THÔNG TIN TRONG THƯƠNG MẠI

Điều 29. Nguyên tắc ứng dụng công nghệ thông tin trong thương mại

1. Tổ chức, cá nhân có quyền ứng dụng công nghệ thông tin trong thương mại.

2. Hoạt động thương mại trên môi trường mạng phải tuân thủ quy định của Luật này, pháp luật về thương mại và pháp luật về giao dịch điện tử.

Điều 30. Trang thông tin điện tử bán hàng

1. Tổ chức, cá nhân có quyền thiết lập trang thông tin điện tử bán hàng theo quy định của Luật này và các quy định khác của pháp luật có liên quan.

2. Trang thông tin điện tử bán hàng phải bảo đảm các yêu cầu chủ yếu sau đây:

a) Cung cấp đầy đủ, chính xác thông tin về hàng hoá, dịch vụ, điều kiện giao dịch, thủ tục giải quyết tranh chấp và bồi thường thiệt hại.

b) Cung cấp cho người tiêu dùng thông tin về phương thức thanh toán an toàn và tiện lợi trên môi trường mạng.

c) Công bố các trường hợp người tiêu dùng có quyền huỷ bỏ, sửa đổi thoả thuận trên môi trường mạng.

3. Tổ chức, cá nhân sở hữu trang thông tin điện tử bán hàng chịu trách nhiệm về nội dung thông tin cung cấp trên trang thông tin điện tử, thực hiện quy định của Luật này và các quy định khác của pháp luật có liên quan về giao kết hợp đồng, đặt hàng, thanh toán, quảng cáo, khuyến mại.

Điều 31. Cung cấp thông tin cho việc giao kết hợp đồng trên môi trường mạng

1. Trừ trường hợp các bên liên quan có thoả thuận khác, tổ chức, cá nhân bán hàng hoá, cung cấp dịch vụ phải cung cấp các thông tin sau đây cho việc giao kết hợp đồng:

a) Trình tự thực hiện để tiến tới giao kết hợp đồng trên môi trường mạng.

b) Biện pháp kỹ thuật xác định và sửa đổi thông tin nhập sai.

c) Việc lưu trữ hồ sơ hợp đồng và cho phép truy nhập hồ sơ đó.

2. Khi đưa ra các thông tin về điều kiện hợp đồng cho người tiêu dùng, tổ chức, cá nhân phải bảo đảm cho người dùng khả năng lưu trữ và tái tạo được các thông tin đó.

Điều 32. Giải quyết hậu quả do lỗi nhập sai thông tin thương mại trên môi trường mạng

Trường hợp người mua nhập sai thông tin gửi vào trang thông tin điện tử bán hàng mà hệ thống nhập tin không cung cấp khả năng sửa đổi thông tin, người mua có quyền đơn phương chấm dứt hợp đồng nếu đã thực hiện các biện pháp sau đây:

1. Thông báo kịp thời cho người bán biết về thông tin nhập sai của mình và người bán cũng đã xác nhận việc nhận được thông báo đó.

2. Trả lại hàng hoá đã nhận nhưng chưa sử dụng hoặc hưởng bất kỳ lợi ích nào từ hàng hoá đó.

Điều 33. Thanh toán trên môi trường mạng

1. Nhà nước khuyến khích tổ chức, cá nhân thực hiện thanh toán trên môi trường mạng theo quy định của pháp luật.

2. Điều kiện, quy trình, thủ tục thanh toán trên môi trường mạng do cơ quan nhà nước có thẩm quyền quy định.

Mục 4

ỨNG DỤNG CÔNG NGHỆ THÔNG TIN TRONG MỘT SỐ LĨNH VỰC

Điều 34. Ứng dụng công nghệ thông tin trong lĩnh vực giáo dục và đào tạo

1. Nhà nước có chính sách khuyến khích ứng dụng công nghệ thông tin trong việc dạy, học, tuyển sinh, đào tạo và các hoạt động khác trong lĩnh vực giáo dục và đào tạo trên môi trường mạng.

2. Tổ chức, cá nhân tiến hành hoạt động giáo dục và đào tạo trên môi trường mạng phải tuân thủ quy định của Luật này và quy định của pháp luật về giáo dục.

3. Cơ quan nhà nước có thẩm quyền chịu trách nhiệm xây dựng, triển khai thực hiện chương trình hỗ trợ tổ chức, cá nhân nhằm mục đích thúc đẩy ứng dụng công nghệ thông tin trong giáo dục và đào tạo.

4. Bộ giáo dục và Đào tạo quy định điều kiện hoạt động giáo dục và đào tạo, công nhận giá trị pháp lý của văn bằng, chứng chỉ trong hoạt động giáo dục và đào tạo trên môi trường mạng và thực hiện kiểm định chất lượng giáo dục và đào tạo trên môi trường mạng.

Điều 35. Ứng dụng công nghệ thông tin trong lĩnh vực y tế

1. Nhà nước có chính sách khuyến khích ứng dụng công nghệ thông tin trong lĩnh vực y tế.

2. Tổ chức, cá nhân tiến hành hoạt động y tế trên môi trường mạng phải tuân thủ quy định của Luật này, pháp luật về y, dược và các quy định khác của pháp luật có liên quan.

3. Bộ y tế quy định cụ thể điều kiện hoạt động y tế trên môi trường mạng.

Điều 36. ứng dụng công nghệ thông tin trong lĩnh vực văn hoá - thông tin

1. Nhà nước có chính sách khuyến khích ứng dụng công nghệ thông tin trong việc số hoá sản phẩm văn hoá, lưu trữ, quảng bá sản phẩm văn hoá đã được số hoá và các hoạt động khác trong lĩnh vực văn hoá.

2. Tổ chức, cá nhân tiến hành hoạt động văn hoá, báo chí trên môi trường mạng phải tuân thủ quy định của Luật này và các quy định của pháp luật về báo chí, văn hoá - thông tin.

3. Tổ chức, cá nhân được Nhà nước hỗ trợ kinh phí để thực hiện số hoá các sản phẩm văn hoá có giá trị bảo tồn phải tuân thủ quy định của Chính phủ về điều kiện thực hiện số hoá các sản phẩm văn hoá có giá trị bảo tồn.

4. Chính phủ quy định việc quản lý hoạt động giải trí trên môi trường mạng nhằm bảo đảm yêu cầu sau đây:

a) Nội dung giải trí phải lành mạnh, có tính giáo dục, tính văn hoá, không trái thuần phong mỹ tục của dân tộc.

b) Gắn trách nhiệm và quyền lợi của các đối tượng tham gia hoạt động giải trí trên môi trường mạng với lợi ích chung của xã hội, cộng đồng.

c) Bảo đảm an toàn kỹ thuật và chất lượng dịch vụ.

d) Bảo đảm an ninh chính trị, trật tự, an toàn xã hội và ngăn chặn các loại tội phạm phát sinh từ hoạt động này.

Điều 37. Ứng dụng công nghệ thông tin trong quốc phòng, an ninh và một số lĩnh vực khác

Hoạt động ứng dụng công nghệ thông tin phục vụ quốc phòng, an ninh và một số lĩnh vực khác được thực hiện theo quy định của Chính phủ.

Chương III

PHÁT TRIỂN CÔNG NGHỆ THÔNG TIN

Mục 1

NGHIÊN CỨU – PHÁT TRIỂN CÔNG NGHỆ THÔNG TIN

Điều 38. Khuyến khích nghiên cứu – phát triển công nghệ thông tin

1. Nhà nước khuyến khích tổ chức, cá nhân nghiên cứu – phát triển công nghệ, sản phẩm công nghệ thông tin nhằm phát triển kinh tế – xã hội, bảo đảm quốc phòng an ninh, nâng cao đời sống vật chất, tinh thần của nhân dân.

2. Tổ chức, cá nhân nghiên cứu – phát triển công nghệ, sản phẩm công nghệ thông tin để đổi mới quản lý kinh tế – xã hội, đổi mới công nghệ được hưởng ưu đãi về thuế, tín dụng và các ưu đãi khác theo quy định của pháp luật.

3. Nhà nước tạo điều kiện để tổ chức, cá nhân hoạt động khoa học và công nghệ chuyển giao kết quả nghiên cứu – phát triển công nghệ, sản phẩm công nghệ thông tin để ứng dụng rộng rãi vào sản xuất và đời sống.

Điều 39. Cơ sở vật chất, kỹ thuật phục vụ cho hoạt động nghiên cứu – phát triển công nghệ thông tin

Nhà nước huy động các nguồn vốn để đầu tư xây dựng cơ sở vật chất, kỹ thuật của các tổ chức nghiên cứu – phát triển công nghệ thông tin; khuyến khích tổ chức, cá nhân đầu tư xây dựng cơ sở vật chất, kỹ thuật phục vụ nghiên cứu – phát triển công nghệ thông tin; đầu tư một số phòng thí nghiệm trọng điểm về công nghệ thông tin đạt tiêu chuẩn quốc tế; ban hành quy chế sử dụng phòng thí nghiệm trọng điểm về công nghệ thông tin.

Điều 40. Nghiên cứu – phát triển công nghệ, sản phẩm công nghệ thông tin

1. Nhà nước khuyến khích tổ chức, cá nhân tham gia nghiên cứu – phát triển công nghệ, sản phẩm công nghệ thông tin.

2. Nhà nước ưu tiên dành một khoản từ ngân sách nhà nước cho các chương trình, đề tài nghiên cứu – phát triển phần mềm; ưu tiên hoạt động nghiên cứu – phát triển công nghệ thông tin ở trường đại học, viện nghiên cứu; phát triển các mô hình gắn kết nghiên cứu, đào tạo với sản xuất về công nghệ thông tin.

3. Cơ quan quản lý nhà nước về công nghệ thông tin chủ trì, phối hợp với cơ quan quản lý nhà nước về khoa học và công nghệ tổ chức tuyển chọn cơ sở nghiên cứu, đào tạo, doanh nghiệp thực hiện nhiệm vụ nghiên cứu – phát triển sản phẩm công nghệ thông tin trọng điểm.

Điều 41. Tiêu chuẩn, chất lượng trong hoạt động ứng dụng và phát triển công nghệ thông tin

1. Việc quản lý tiêu chuẩn, chất lượng sản phẩm, dịch vụ công nghệ thông tin được thực hiện theo quy định của pháp luật về tiêu chuẩn, chất lượng.

2. Khuyến khích tổ chức, cá nhân tham gia sản xuất, cung cấp sản phẩm, dịch vụ công nghệ thông tin, công bố tiêu chuẩn cơ sở và phải bảo đảm sản phẩm, dịch vụ của mình phù hợp với tiêu chuẩn đã công bố.

3. Chất lượng sản phẩm, dịch vụ công nghệ thông tin được quản lý thông qua các hình thức sau đây:

a) Chứng nhận phù hợp tiêu chuẩn, quy chuẩn kỹ thuật.

b) Công bố phù hợp tiêu chuẩn, quy chuẩn kỹ thuật.

c) Kiểm định chất lượng.

4. Bộ Bưu chính, Viễn thông công bố sản phẩm, dịch vụ công nghệ thông tin cần áp dụng tiêu chuẩn quốc gia hoặc tiêu chuẩn quốc tế; ban hành và công bố áp dụng quy chuẩn kỹ thuật; quy định cụ thể về quản lý chất lượng sản phẩm, dịch vụ công nghệ thông tin; quy định các điều kiện đối với cơ quan đo kiểm trong nước và nước ngoài để phục vụ cho việc quản lý chất lượng sản phẩm, dịch vụ công nghệ thông tin và công bố cơ quan đo kiểm về công nghệ thông tin có thẩm quyền.

5. Việc thừa nhận lẫn nhau về đánh giá phù hợp tiêu chuẩn đối với sản phẩm công nghệ thông tin giữa Cộng hoà xã hội chủ nghĩa Việt Nam với nước ngoài và tổ chức quốc tế được thực hiện theo quy định của điều ước quốc tế mà Cộng hoà xã hội chủ nghĩa Việt Nam là thành viên.

Mục 2

PHÁT TRIỂN NHÂN LỰC CÔNG NGHỆ THÔNG TIN

Điều 42. Chính sách phát triển nguồn nhân lực công nghệ thông tin

1. Nhà nước có chính sách phát triển quy mô và tăng cường chất lượng đào tạo nguồn nhân lực công nghệ thông tin.

2. Chương trình, dự án ưu tiên, trọng điểm của Nhà nước về ứng dụng và phát triển công nghệ thông tin phải có hạng mục đào tạo nhân lực công nghệ thông tin.

3. Tổ chức, cá nhân được khuyến khích thành lập cơ sở đào tạo nhân lực công nghệ thông tin theo quy định của pháp luật.

4. Cơ sở đào tạo được hưởng ưu đãi trong hoạt động đào tạo về công nghệ thông tin tương đương với doanh nghiệp sản xuất phần mềm.

5. Nhà nước có chính sách hỗ trợ giáo viên, sinh viên và học sinh trong hệ thống giáo dục quốc dân truy nhập Internet tại các cơ sở giáo dục.

Điều 43. Chứng chỉ công nghệ thông tin

Bộ Bưu chính, Viễn thông chủ trì, phối hợp với Bộ Giáo dục và Đào tạo, Bộ Lao động – Thương binh và Xã hội quy định điều kiện hoạt động đào tạo công nghệ thông tin và cấp chứng chỉ công nghệ thông tin, việc công nhận chứng chỉ công nghệ thông tin của tổ chức nước ngoài sử dụng ở Việt Nam.

Điều 44. Sử dụng nhân lực công nghệ thông tin

1. Người hoạt động chuyên trách về ứng dụng và phát triển công nghệ thông tin trong các cơ quan nhà nước được hưởng chế độ ưu đãi về điều kiện làm việc.

2. Tiêu chuẩn ngành nghề, chức danh về công nghệ thông tin do cơ quan nhà nước có thẩm quyền ban hành.

Điều 45. Người Việt Nam làm việc tại nước ngoài

1. Nhà nước khuyến khích tổ chức, cá nhân tìm kiếm và mở rộng thị trường lao động nhằm tạo việc làm ở nước ngoài cho người lao động Việt Nam tham gia các hoạt động về công nghệ thông tin theo quy định của pháp luật Việt Nam, phù hợp với pháp luật của nước sở tại và điều ước quốc tế mà Cộng hoà xã hội Chủ nghĩa Việt Nam là thành viên.

2. Nhà nước có chính sách ưu đãi cho tổ chức, cá nhân nước ngoài, người Việt Nam định cư ở nước ngoài tuyển dụng lao động trong nước để phát triển, sản xuất, gia công sản phẩm công nghệ thông tin.

Điều 46. Phổ cập kiến thức công nghệ thông tin

1. Nhà nước có chính sách khuyến khích phổ cập kiến thức công nghệ thông tin trong phạm vi cả nước.

2. Uỷ ban nhân dân tỉnh, thành phố trực thuộc trung ương có trách nhiệm xây dựng và triển khai các hoạt động phổ cập kiến thức công nghệ thông tin cho tổ chức, cá nhân trong địa phương mình.

3. Bộ Giáo dục và Đào tạo có trách nhiệm xây dựng chương trình và tổ chức thực hiện phổ cập kiến thức công nghệ thông tin trong hệ thống giáo dục quốc dân.

4. Nhà nước có chính sách hỗ trợ việc học tập, phổ cập kiến thức công nghệ thông tin đối với người tàn tật, người nghèo, người dân tộc thiểu số và các đối tượng ưu tiên khác phù hợp với yêu cầu phát triển trong từng thời kỳ theo quy định của Chính phủ.

Mục 3

PHÁT TRIỂN CÔNG NGHIỆP CÔNG NGHỆ THÔNG TIN

Điều 47. Loại hình công nghiệp công nghệ thông tin

1. Công nghiệp phần cứng là công nghiệp sản xuất các sản phẩm phần cứng, bao gồm phụ tùng, linh kiện, thiết bị số.

2. Công nghiệp phần mềm là công nghiệp sản xuất các sản phẩm phần mềm, bao gồm phần mềm hệ thống, phần mềm ứng dụng, phần mềm điều khiển, tự động hoá và các sản phẩm tương tự khác; cung cấp các giải pháp cài đặt, bảo trì, hướng dẫn sử dụng.

3. Công nghiệp nội dung là công nghiệp sản xuất các sản phẩm thông tin số, bao gồm thông tin kinh tế – xã hội, thông tin khoa học – giáo dục, thông tin văn hoá - giải trí trên môi trường mạng và các sản phẩm tương tự khác.

Điều 48. Chính sách phát triển công nghiệp công nghệ thông tin

1. Nhà nước có chính sách ưu đãi, ưu tiên đầu tư phát triển công nghiệp công nghệ thông tin, đặc biệt chú trọng công nghiệp phần mềm và công nghiệp nội dung để trở thành một ngành kinh tế trọng điểm trong nền kinh tế quốc dân.

2. Nhà nước khuyến khích các nhà đầu tư tham gia hoạt động đầu tự mạo hiểm vào lĩnh vực công nghiệp công nghệ thông tin, đầu tư phát triển và cung cấp thiết bị số giá rẻ.

3. Chính phủ quy định cụ thể mức ưu đãi, ưu tiên và các điều kiện khác cho phát triển công nghiệp công nghệ thông tin.

Điều 49. Phát triển thị trường công nghiệp công nghệ thông tin

Cơ quan nhà nước có thẩm quyền ban hành quy định và tổ chức thực hiện các hoạt động phát triển thị trường công nghiệp công nghệ thông tin, bao gồm:

1. Thúc đẩy ứng dụng công nghệ thông tin; ưu tiên sử dụng nguồn vốn ngân sách nhà nước để mua sắm, sử dụng các sản phẩm công nghệ thông tin được sản xuất trong nước.

2. Xúc tiến thương mại, tổ chức triển lãm, hội chợ trong nước, hỗ trợ các doanh nghiệp tham gia triển lãm, hội chợ quốc tế, quảng bá, tiếp thị hình ảnh công nghiệp công nghệ thông tin của Việt Nam trên thế giới.

3. Phương pháp định giá phần mềm phục vụ cho việc quản lý các dự án ứng dụng và phát triển công nghệ thông tin.

Điều 50. Sản phẩm công nghệ thông tin trọng điểm

1. Sản phẩm công nghệ thông tin trọng điểm là sản phẩm công nghệ thông tin bảo đảm được một trong những yêu cầu sau đây:

a) Thị trường trong nước có nhu cầu lớn và tạo giá trị gia tăng cao.

b) Có tiềm năng xuất khẩu.

c) Có tác dụng tích cực về đổi mới công nghệ và hiệu quả kinh tế đối với các ngành kinh tế khác.

2. Bộ Bưu chính, Viễn thông côn bố danh mục và xây dựng chương trình phát triển các sản phẩm công nghệ thông tin trọng điểm trong từng thời kỳ phù hợp với quy hoạch phát triển công nghiệp công nghệ thông tin.

3. Các sản phẩm công nghệ thông tin thuộc danh mục sản phẩm công nghệ trọng điểm quy định tại khoản 2 Điều này được Nhà nước ưu tiên đầu tư nghiên cứu – phát triển, sản xuất.

4. Tổ chức, cá nhân tham gia nghiên cứu – phát triển, sản xuất sản phẩm công nghệ thông tin trọng điểm được hưởng ưu đãi theo quy đinh của Chính phủ; được Nhà nước ưu tiên đầu tư và được hưởng một phần tiền bản quyền đối với sản phẩm công nghệ thông tin trọng điểm do Nhà nước đầu tư.

5. Tổ chức, cá nhân tham gia nghiên cứu – phát triển, sản xuất sản phẩm công nghệ thông tin trọng điểm do Nhà nước đầu tư phải đáp ứng các điều kiện do cơ quan nhà nước có thẩm quyền quy định; không được chuyển giao, chuyển nhượng công nghệ, giải pháp phát triển sản phẩm công nghệ thông tin trọng điểm do Nhà nước đầu tư khi chưa có sự đồng ý của cơ quan nhà nước có thẩm quyền; chịu sự kiểm tra, kiểm soát, tuân thủ chế độ báo cáo theo quy định của cơ quan nhà nước có thẩm quyền về hoạt động nghiên cứu – phát triển, sản xuất và xúc tiến thương mại các sản phẩm công nghệ thông tin trọng điểm.

Điều 51. Khu công nghệ thông tin tập trung

1. Khu công nghệ thông tin tập trung là loại hình khu công nghệ cao, tập trung hoặc liên kết cơ sở nghiên cứu – phát triển, sản xuất, kinh doanh, đào tạo về công nghệ thông tin. Tổ chức, cá nhân đầu tư và hoạt động trong khu công nghệ thông tin tập trung được hưởng các chính sách ưu đãi của Nhà nước áp dụng với khu công nghệ cao.

2. Khuyến khích tổ chức, cá nhân trong nước và nước ngoài đầu tư, xây dựng khu công nghệ thông tin tập trung theo quy hoạch của Chính phủ.

Mục 4

PHÁT TRIỂN DỊCH VỤ CÔNG NGHỆ THÔNG TIN

Điều 52. Loại hình dịch vụ công nghệ thông tin

1. Điều tra, khảo sát, nghiên cứu thị trường về công nghệ thông tin.

2. Tư vấn, phân tích, lập kế hoạch, phân loại, thiết kế trong lĩnh vực công nghệ thông tin.

3. Tích hợp hệ thống, chạy thử, dịch vụ quản lý ứng dụng, cập nhật, bảo mật.

4. Thiết kế, lưu trữ, duy trì trang thông tin điện tử.

5. Bảo hành, bảo trì, bảo đảm an toàn mạng và thông tin.

6. Cập nhật, tìm kiếm, lưu trữ, xử lý dữ liệu và khai thác cơ sở dữ liệu.

7. Phân phối sản phẩm công nghệ thông tin.

8. Đào tạo công nghệ thông tin.

9. Chứng thực chữ ký điện tử.

10. Dịch vụ khác.

Điều 53. Chính sách phát triển dịch vụ công nghệ thông tin

1. Nhà nước có chính sách khuyến khích phát triển dịch vụ công nghệ thông tin.

2. Chính phủ quy định cụ thể chế độ ưu đãi và các điều kiện khác cho một số loại hình dịch vụ công nghệ thông tin.

Chương IV

BIỆN PHÁP BẢO ĐẢM ỨNG DỤNG VÀ PHÁT TRIỂN CÔNG NGHỆ THÔNG TIN

Mục 1

CƠ SỞ HẠ TẦNG THÔNG TIN PHỤC VỤ ỨNG DỤNG VÀ PHÁT TRIỂN CÔNG NGHỆ THÔNG TIN

Điều 54. Nguyên tắc phát triển cơ sở hạ tầng thông tin

1. Cơ sở hạ tầng thông tin phải được phát triển để bảo đảm chất lượng và đa dạng các loại hình dịch vụ nhằm đáp ứng yêu cầu ứng dụng và phát triển công nghệ thông tin.

2. Cơ quan nhà nước có thẩm quyền chịu trách nhiệm bảo đảm sự phát triển cơ sở hạ tầng thông tin phù hợp với yêu cầu phát triển kinh tế – xã hội; tạo điều kiện để các thành phần kinh tế sử dụng cơ sở hạ tầng thông tin trong môi trường cạnh tranh lành mạnh, bình đẳng, minh bạch; có biện pháp đồng bộ để ngăn chặn những hành vi lợi dụng cơ sở hạ tầng thông tin vi phạm quy định Điều 12 của Luật này.

Điều 55. Bảo đảm cơ sở hạ tầng thông tin phục vụ việc ứng dụng và phát triển công nghệ thông tin

1. Nhà nước có chính sách phát triển cơ sở hạ tầng thông tin quốc gia rộng khắp, có thông lượng lớn, tốc độ và chất lượng cao, giá cước cạnh tranh so với các nước trong khu vực; khuyến khích tổ chức, cá nhân cùng đầu tư, sử dụng chung cơ sở hạ tầng thông tin.

2. Điểm truy nhập Internet công cộng được ưu tiên đặt tại bưu cục, điểm bưu điện văn hoá xã, nhà ga, bến xe, cảng biển, cảng hàng không, cửa khẩu, khu dân cư, bệnh viện, trường học, siêu thị, trung tâm văn hoá, thể thao để phục vụ nhau cầu của tổ chức, cá nhân.

Điều 56. Cơ sở hạ tầng thông tin phục vụ cơ quan nhà nước

1. Cơ sở hạ tầng thông tin phục vụ cơ quan nhà nước, từ trung ương đến địa phương được thống nhất xây dựng và quản lý theo quy định của Chính phủ.

2. Kinh phí đầu tư, xây dựng, khai thác, bảo trì cơ sở hạ tầng thông tin phục vụ cơ quan nhà nước lấy từ ngân sách nhà nước và các nguồn khác.

Điều 57. Cơ sở hạ tầng thông tin phục vụ công ích

1. Nhà nước có chính sách ưu tiên vốn đầu tư và có cơ chế hỗ trợ tài chính cho việc xây dựng và sử dụng cơ sở hạ tầng thông tin phục vụ công ích và thu hẹp khoảng cách số.

2. Cơ quan quản lý nhà nước về công nghệ thông tin các cấp chịu trách nhiệm tổ chức thực hiện các chương trình, dự án thu hẹp khoảng cách số, bao gồm:

a) Lắp đặt hệ thống máy tính và truy nhập Internet tại trường học, điểm công cộng trên phạm vi toàn quốc.

b) Phát triển đội ngũ hướng dẫn sử dụng máy tính và truy nhập Internet.

c) Thu hẹp khoảng cách số giữa các vùng, miền.

Điều 58. Cơ sở dữ liệu quốc gia

1. Cơ sở dữ liệu quốc gia là tập hợp thông tin của một hoặc một số lĩnh vực kinh tế – xã hội được xây dựng, cập nhật và duy trì đáp ứng yêu cầu truy nhập và sử dụng thông tin của các ngành kinh tế và phục vụ lợi ích công cộng.

2. Tổ chức, cá nhân có quyền truy nhập và sử dụng thông tin trong cơ sở dữ liệu quốc gia, trừ trường hợp phát luật có quy định khác.

3. Nhà nước bảo đảm một phần hoặc toàn bộ kinh phí xây dựng và duy trì cơ sở dữ liệu quốc gia.

4. Chính phủ quy định danh mục cơ sở dữ liệu quốc gia; xây dựng, cập nhật và duy trì cơ sở dữ liệu quốc gia; ban hành quy chế khai thác, sử dụng cơ sở dữ liệu quốc gia.

Điều 59. Cơ sở dữ liệu của Bộ, ngành, địa phương

1. Cơ sở dữ liệu của Bộ, ngành, địa phương là tập hợp thông tin được xây dựng, cập nhật và duy trì đáp ứng yêu cầu truy nhập, sử dụng thông tin của mình và phục vụ lợi ích công cộng.

2. Tổ chức, cá nhân có quyền truy nhập và sử dụng thông tin trong cơ sở dữ liệu của Bộ, ngành, địa phương, trừ trường hợp pháp luật có quy định khác.

3. Nhà nước bảo đảm một phần hoặc toàn bộ kinh phí xây dựng và duy trì cơ sở dữ liệu của Bộ, ngành, địa phương.

4. Bộ, cơ quan ngang Bộ, cơ quan trực thuộc Chính phủ, Uỷ ban nhân dân tỉnh, thành phố trực thuộc trung ương quy định danh mục cơ sở dữ liệu; xây dựng, cập nhật và duy trì cơ sở dữ liệu; ban hành quy chế khai thác, sử dụng cơ sở dữ liệu của Bộ, ngành, địa phương mình.

Điều 60. Bảo vệ cơ sở hạ tầng thông tin

1. Cơ sở hạ tầng thông tin quốc gia phải được bảo vệ, Uỷ ban nhân dân các cấp, lực lượng vũ trang nhân dân và tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng thông tin có trách nhiệm phối hợp bảo vệ an toàn cơ sở hạ tầng thông tin quốc gia.

2. Tổ chức, cá nhân có trách nhiệm bảo đảm an toàn cơ sở hạ tầng thông tin thuộc thẩm quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo đảm an toàn cơ sở hạ tầng thông tin và an ninh thông tin của các cơ quan nhà nước có thẩm quyền.

3. Tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng thông tin có trách nhiệm tạo điều kiện làm việc, kỹ thuật, nghiệp vụ cần thiết để các cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ kiểm soát và bảo đảm an ninh thông tin khi có yêu cầu.

Mục 2

ĐẦU TƯ CHO CÔNG NGHỆ THÔNG TIN

Điều 61. Đầu tư của tổ chức, cá nhân cho công nghệ thông tin

1. Nhà nước khuyến khích tổ chức, cá nhân đầu tư cho hoạt động ứng dụng công nghệ thông tin để đổi mới quản lý kinh tế – xã hội, đổi mới công nghệ và nâng cao sức cạnh tranh của sản phẩm.

2. Nhà nước khuyến khích và bảo vệ quyền, lợi ích hợp pháp của tổ chức, cá nhân trong nước, người Việt Nam định cư ở nước ngoài, tổ chức, cá nhân nước ngoài đầu tư cho công nghệ thông tin.

3. Các khoản đầu tư của doanh nghiệp cho ứng dụng và phát triển công nghệ thông tin và các chi phí sau đây của doanh nghiệp được trừ khi tính thu nhập chịu thuế theo Luật thuế thu nhập doanh nghiệp:

a) Mở trường, lớp đào tạo công nghệ thông tin tại doanh nghiệp.

b) Cử người đi đào tạo, tiếp thu công nghệ mới phục vụ nhu cầu ứng dụng và phát triển công nghệ thông tin của doanh nghiệp.

Điều 62. Đầu tư của Nhà nước cho công nghệ thông tin

1. Đầu tư cho công nghệ thông tin là đầu tư phát triển.

2. Nhà nước ưu tiên bố trí ngân sách cho công nghệ thông tin, bảo đảm tỷ lệ tăng chi ngân sách cho công nghệ thông tin hàng năm cao hơn tỷ lệ tăng chi ngân sách nhà nước. Ngân sách cho công nghệ thông tin phải được quản lý, sử dụng có hiệu quả.

3. Chính phủ ban hành quy chế quản lý đầu tư phù hợp đối với các dự án ứng dụng công nghệ thông tin sử dụng vốn đầu tư có nguồn gốc từ ngân sách nhà nước.

4. Trong Mục lục ngân sách nhà nước có loại chi riêng về công nghệ thông tin.

Điều 63. Đầu tư cho sự nghiệp ứng dụng và phát triển công nghệ thông tin

1. Ngân sách nhà nước chi phí cho sự nghiệp ứng dụng và phát triển công nghệ thông tin được sử dụng vào các mục sau đây:

a) Phổ cập ứng dụng công nghệ thông tin, hỗ trợ dự án ứng dụng công nghệ thông tin có hiệu quả.

b) Phát triển nguồn thông tin số.

c) Xây dựng cơ sở dữ liệu quốc gia, cơ sở dữ liệu của Bộ, ngành, địa phương.

d) Xây dựng cơ sở hạ tầng thông tin phục vụ công ích và cơ quan nhà nước.

e) Điều tra, nghiên cứu, xây dựng, thử nghiệm, áp dụng tiến bộ khoa học – kỹ thuật về công nghệ thông tin, cơ chế, chính sách, chiến lược, quy hoạch, kế hoạch, tiêu chuẩn, quy chuẩn kỹ thuật, định mức kinh tế – kỹ thuật, mô hình ứng dụng và phát triển công nghệ thông tin.

f) Phát triển nguồn nhân lực công nghệ thông tin.

g) Tuyên truyền, phổ biến, giáo dục pháp luật về công nghệ thông tin, đào tạo, tập huấn chuyên môn, quản lý về công nghệ thông tin.

h) Trao giải thưởng công nghệ thông tin.

i) Các hoạt động khác cho sự nghiệp ứng dụng và phát triển công nghệ thông tin.

2. Hằng năm, Bộ Bưu chính, Viễn thông chịu trách nhiệm tổng hợp dự toán kinh phí chi cho sự nghiệp ứng dụng và phát triển công nghệ thông tin quy định tại khoản 1 Điều này của các Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và của tỉnh, thành phố trực thuộc trung ương để Chính phủ trình Quốc hội.

Điều 64. Đầu tư và phát triển công nghệ thông tin phục vụ nông nghiệp và nông thôn

1. Thu hút mọi nguồn lực để đầu tư xây dựng cơ sở hạ tầng thông tin, đẩy nhanh quá trình hiện đại hoá nông thôn, miền núi, hải đảo.

2. Tạo điều kiện thuận lợi cho nhân dân ở vùng sâu, vùng xa, vùng có đồng bào dân tộc thiểu số, vùng có điều kiện kinh tế – xã hội khó khăn, vùng có điều kiện kinh tế – xã hội đặc biệt khó khăn ứng dụng công nghệ thông tin để phục vụ sản xuất và đời sống.

3. Tổ chức, cá nhân hoạt động ứng dụng và phát triển công nghệ thông tin tại vùng sâu, vùng xa, vùng có đồng bào dân tộc thiểu số, vùng có điều kiện kinh tế – xã hội khó khăn, vùng có điều kiện kinh tế – xã hội đặc biệt khó khăn được hưởng các chính sách ưu đãi về đầu tư, tài chính và các ưu đãi khác theo quy định của pháp luật.

4. Hoạt động ứng dụng và cung cấp dịch vụ công nghệ thông tin phục vụ mục tiêu khuyến nông, khuyến lâm, khuyến ngư, đánh bắt xa bờ được Nhà nước hỗ trợ một phần kinh phí.

Mục 3

HỢP TÁC QUỐC TẾ VỀ CÔNG NGHỆ THÔNG TIN

Điều 65. Nguyên tắc hợp tác quốc tế về công nghệ thông tin

Tổ chức, cá nhân Việt Nam hợp tác về công nghệ thông tin với tổ chức, cá nhân nước ngoài, tổ chức quốc tế theo nguyên tắc tôn trọng độc lập, chủ quyền quốc gia, không can thiệp vào công việc nội bộ của nhau, bình đẳng và cùng có lợi.

Điều 66. Nội dung hợp tác quốc tế về công nghệ thông tin

1. Phân tích xu hướng quốc tế về công nghệ thông tin, quy mô và triển vọng phát triển thị trường nước ngoài và xây dựng chiến lược phát triển thị trường công nghệ thông tin ở nước ngoài.

2. Quảng bá thông tin về định hướng, chính sách ứng dụng và phát triển công nghệ thông tin của Việt Nam và của các nước trên thế giới.

3. Xây dựng cơ chế, chính sách đẩy mạnh hợp tác giữa tổ chức, cá nhân Việt Nam với tổ chức, cá nhân nước ngoài, tổ chức quốc tế hoạt động trong lĩnh vực công nghệ thông tin.

4. Thực hiện chương trình, dự án hợp tác quốc tế về công nghệ thông tin.

5. Phát triển thị trường công nghệ thông tin ở nước ngoài, giới thiệu sản phẩm công nghệ thông tin Việt Nam qua các triển lãm quốc tế, tiếp cận với khách hàng tiềm năng.

6. Tổ chức hội thảo, hội nghị và diễn đàn quốc tế về công nghệ thông tin.

7. Ký kết, gia nhập và thực hiện các điều ước quốc tế song phương, đa phương và tham gia tổ chức khu vực, tổ chức quốc tế về công nghệ thông tin.

8. Tiếp thu công nghệ của nước ngoài chuyển giao vào Việt Nam.

Mục 4

BẢO VỆ QUYỀN, LỢI ÍCH HỢP PHÁP VÀ HỖ TRỢ NGƯỜI SỬ DỤNG SẢN PHẨM DỊCH VỤ CÔNG NGHỆ THÔNG TIN

Điều 67. Trách nhiệm bảo vệ quyền, lợi ích hợp pháp của người sử dụng sản phẩm, dịch vụ công nghệ thông tin

Nhà nước và xã hội thực hiện các biện pháp phòng, chống các hành vi xâm hại quyền, lợi ích hợp pháp của người sử dụng sản phẩm, dịch vụ công nghệ thông tin. Quyền, lợi ích hợp pháp của người sử dụng sản phẩm, dịch vụ công nghệ thông tin được bảo vệ theo quy định của pháp luật.

Điều 68. Bảo vệ tên miền quốc gia Việt Nam ".vn"

1. Tên miền quốc gia Việt Nam ".vn" và tên miền cấp dưới của tên miền quốc gia Việt Nam ".vn" là một phần tài nguyên thông tin quốc gia, có giá trị sử dụng như nhau và phải được quản lý, khai thác, sử dụng đúng mục đích, có hiệu quả.

Nhà nước khuyến khích tổ chức, cá nhân đăng ký và sử dụng tên miền quốc gia Việt Nam ".vn". Tên miền đăng ký phải thể hiện tính nghiêm túc để tránh gây sự hiểu nhầm hoặc xuyên tạc do tính đa âm, đa nghĩa hoặc khi không dùng dấu trong tiếng Việt.

2. Tên miền quốc gia Việt Nam ".vn" dành cho tổ chức Đảng, cơ quan nhà nước phải được bảo vệ và không được xâm phạm.

3. Tổ chức, cá nhân đăng ký sử dụng tên miền quốc gia Việt Nam ".vn" phải chịu trách nhiệm trước pháp luật về mục đích sử dụng và tính chính xách của các thông tin đăng ký và bảo đảm việc đăng ký, sử dụng tên miền quốc gia

Việt Nam ".vn" không xâm phạm các quyền, lợi ích hợp pháp của tổ chức, cá nhân khác có trước ngày đăng ký.

4. Bộ Bưu chính, Viễn thông quy định việc đăng ký, quản lý, sử dụng và giải quyết tranh chấp tên miền quốc gia Việt Nam ".vn"

Điều 69. Bảo vệ quyền sở hữu trí tuệ trong lĩnh vực công nghệ thông tin

Việc bảo vệ quyền sở hữu trí tuệ trong lĩnh vực công nghệ thông tin phải thực hiện theo quy định của pháp luật về sở hữu trí tuệ và các quy định sau đây:

1. Tổ chức, cá nhân truyền đưa thông tin trên môi trường mạng có quyền tạo ra bản sao tạm thời một tác phẩm được bảo hộ do yêu cầu kỹ thuật của hoạt động truyền đưa thông tin và bản sao tạm thời được lưu trữ trong khoảng thời gian đủ để thực hiện việc truyền đưa thông tin.

2. Người sử dụng hợp pháp phần mềm được bảo hộ có quyền sao chép phần mềm đó để lưu trữ dự phòng và thay thế phân mềm bị phá hỏng mà không phải xin phép, không phải trả tiền bản quyền.

Điều 70. Chống thư rác

1. Tổ chức, cá nhân không được che giấu tên của mình hoặc giả mạo tên của tổ chức, cá nhân khác khi gửi thông tin trên môi trường mạng.

2. Tổ chức, cá nhân gửi thông tin quảng cáo trên môi trường mạng phải bảo đảm cho người tiêu dùng khả năng từ chối nhận thông tin quảng cáo.

3. Tổ chức, cá nhân không được tiếp tục gửi thông tin quảng cáo trên môi trường mạng đến người tiêu dùng nếu người tiêu dùng đó thông báo không đồng ý nhận thông tin quảng cáo.

Điều 71. Chống vi rút máy tính và phần mềm gây hại

Tổ chức, cá nhân không được tạo ra, cài đặt, phát tán vi rút máy tính, phần mềm gây hại vào thiết bị số của người khác để thực hiện một trong những hành vi sau đây:

1. Thay đổi các tham số cài đặt của thiết bị số.

2. Thu thập thông tin của ngườ khác.

3. Xoá bỏ, làm mất tác dụng của các phần mềm bảo đảm an toàn, an ninh thông tin được cài đặt trên thiết bị số.

4. Ngăn chặn khả năng của người sử dụng xoá bỏ hoặc hạn chế sử dụng những phần mềm không cần thiết.

5. Chiếm đoạt quyền điều khiển thiết bị số.

6. Thay đổi, xoá bỏ thông tin lưu trữ trên thiết bị số.

7. Các hành vi khác xâm hại quyền, lợi ích hợp pháp của người sử dụng.

Điều 72. Bảo đảm an toàn, bí mật thông tin

1. Thông tin riêng hợp pháp của tổ chức, cá nhân trao đổi, truyền đưa, lưu trữ trên môi trường mạng được bảo đảm bí mật theo quy định của pháp luật.

2. Tổ chức, cá nhân không được thực hiện một trong những hành vi sau đây:

a) Xâm nhập, sửa đổi, xoá bỏ nội dung thông tin của tổ chức, cá nhân khác trên môi trường mạng.

b) Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

c) Ngăn chặn việc truy nhập đến thông tin của tổ chức, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

d) Bẻ khoá, trộm cắp, sử dụng mật khẩu, khoá mật mã và thông tin của tổ chức, cá nhân khác trên môi trường mạng.

e) Hành vi khác làm mất an toàn, bí mật thông tin của tổ chức, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Điều 73. Trách nhiệm bảo vệ trẻ em

1. Nhà nước, xã hội và nhà trường có trách nhiệm sau đây:

a) Bảo vệ trẻ em không bị tác động tiêu cực của thông tin trên môi trường mạng.

b) Tiến hành các biện pháp phòng, chống các ứng dụng công nghệ thông tin có nội dung kích động bạo lực và khiêu dâm.

2. Gia đình có trách nhiệm ngăn chặn trẻ em truy nhập thông tin không có lợi cho trẻ em.

3. Cơ quan nhà nước có thẩm quyền tiến hành những biện pháp sau đây để ngăn ngừa trẻ em truy nhập thông tin không có lợi trên môi trường mạng:

a) Tổ chức xây dựng và phổ biến sử dụng phần mềm lọc nội dung.

b) Tổ chức xây dựng và phổ biến công cụ ngăn chặn trẻ em truy nhập thông tin không có lợi cho trẻ em.

c) Hướng dẫn thiết lập và quản lý trang thông tin điện tử dành cho trẻ em nhằm mục đích thúc đẩy việc thiết lập các trang thông tin điện tử có nội dung thông tin phù hợp với trẻ em, không gây hại cho trẻ em; tăng cường khả năng quản lý nội dung thông tin trên môi trường mạng phù hợp với trẻ em, không gây hại cho trẻ em.

4. Nhà cung cấp dịch vụ có biện pháp ngăn ngừa trẻ em truy nhập trên môi trường mạng thông tin không có lợi đối với trẻ em.

5. Sản phẩm, dịch vụ công nghệ thông tin mang nội dung không có lợi cho trẻ em phải có dấu hiệu cảnh báo.

Điều 74. Hỗ trợ người tàn tật

1. Nhà nước khuyến khích và tạo điều kiện thuận lợi cho người tàn tật tham gia hoạt động ứng dụng và phát triển công nghệ thông tin, phát triển năng lực làm việc của người tàn tật thông qua ứng dụng và phát triển công nghệ thông tin; có chính sách ưu tiên cho người tàn tật tham gia các chương trình giáo dục và đào tạo về công nghệ thông tin.

2. Chiến lược, kế hoạch, chính sách phát triển công nghệ thông tin quốc gia phải có nội dung hỗ trợ, bảo đảm cho người tàn tật hoà nhập với cộng đồng.

3. Nhà nước có chính sách ưu đãi về thuế, tín dụng và ưu đãi khác cho hoạt động sau đây:

a) Nghiên cứu – phát triển các công cụ và ứng dụng nhằm nâng cao khả năng của người tàn tật trong việc truy nhập, sử dụng các nguồn thông tin và tri thức thông qua sử dụng máy tính và cơ sở hạ tầng thông tin.

b) Sản xuất, cung cấp công nghệ, thiết bị, dịch vụ, ứng dụng công nghệ thông tin và nội dung thông tin số đáp ứng nhu cầu đặc biệt của người tàn tật.

Chương V

GIẢI QUYẾT TRANH CHẤP VÀ XỬ LÝ VI PHẠM

Điều 75. Giải quyết tranh chấp về công nghệ thông tin

1. Tranh chấp về công nghệ thông tin là tranh chấp phát sinh trong hoạt động ứng dụng và phát triển công nghệ thông tin.

2. Khuyến khích các bên giải quyết tranh chấp về công nghệ thông tin thông qua hoà giải; trong trường hợp các bên không hoà giải được thì giải quyết theo quy định của pháp luật.

Điều 76. Hình thức giải quyết tranh chấp về đăng ký, sử dụng tên miền quốc gia Việt Nam ".vn"

Tranh chấp về đăng ký, sử dụng tên miền quốc gia Việt Nam ".vn" được giải quyết theo các hình thức sau đây:

1. Thông qua thương lượng, hoà giải.

2. Thông qua trọng tài.

3. Khởi kiện tại Toà án.

Điều 77. Xử lý vi phạm pháp luật về công nghệ thông tin

1. Cá nhân có hành vi vi phạm pháp luật về công nghệ thông tin thì tuỳ theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

2. Tổ chức có hành vi vi phạm pháp luật về công nghệ thông tin thì tuỳ theo tính chất, mức độ vi phạm mà bị xử phạt hành chính, đình chỉ hoạt động, nếu gây thiệt hại lớn thì phải bồi thường theo quy định của pháp luật.

Chương VI

ĐIỀU KHOẢN THI HÀNH

Điều 78. Hiệu lực thi hành

Luật này có hiệu lực thi hành từ ngày 01 tháng 01 năm 2007**.**

Điều 79. Hướng dẫn thi hành

Chính phủ quy định chi tiết và hướng dẫn thi hành Luật này.

*Luật này đã được Quốc hội nước Cộng hoà xã hội chủ nghĩa Việt Nam khoá XI, kỳ họp thứ 9 thông qua ngày 29 tháng 6 năm 200**6.***

CHỦ TỊCH QUỐC HỘI

NGUYỄN PHÚ TRỌNG

TÀI LIỆU THAM KHẢO

1. J.K.Shim et all: The International Handbook of Computer Security AMACOM
2. W.Caelli, D.Longley, M.Shain: Information Security Handbook Maemillan Press, 1994
3. F.J.Cooper et all: Implementing Internet Security NPR, 1995
4. K.M.Jackson, J.Hruska: Computer Security Reference Book CRC, 1992
5. J.R.Vacca: Internet Security Secrets,

   IDG Books Worldwide Inc., 1996
6. C.P.Pfleeger: Security in Computing

   Prentice Hall, 1999
7. D.L.Baumer, J.B.Earp, J.C.Poindexter: Internet privacy law: a comparison between the US and EU.

   Computer & Security (2004) 23, 400-412
8. H.B.Wolfe: An Introduction to Computer Forensics: Gathering Evidence in a Computing Environment

   New Zealand, 2001.
9. R.McKemmish: What is Forensic Computing?

   Australia, 1999.
10. J.Landman: Forensic Computing: An Introduction to the Principles and the Practical Application.

    Australia, 2002.
11. Nguyễn Đình Vinh, Trần Đức Sự: Giáo trình Cơ sở an toàn thông tin.

    Học viện Kỹ thuật mật mã, Hà Nội, 2006.

