บทที่ 6

บทสรุปและข้อเสนอแนะ

6.1 บทสรุป

อาชญากรรมคอมพิวเตอร์มีหลากหลายรูปแบบ การกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ถือเป็นอาชญากรรมคอมพิวเตอร์รูปแบบหนึ่ง การที่จะหามาตรการมาป้องกันการกระทำการดังกล่าวจำเป็นจะต้องมีความรู้พื้นฐานเกี่ยวกับเทคโนโลยีสารสนเทศ อันประกอบด้วยกระบวนการทำงานของคอมพิวเตอร์ การสื่อสารข้อมูล รวมถึงระบบสารสนเทศ เมื่อสามารถเข้าใจถึงสิ่งต่างๆ เหล่านี้แล้ว จึงจะมาทำการศึกษาถึงลักษณะหรือวิธีการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ ว่าสามารถเกิดขึ้นในขั้นตอนใดได้บ้าง และการกระทำความผิดในขั้นตอนนั้นๆ ถือเป็นอาชญากรรมหรือไม่ ซึ่งความหมายของอาชญากรรมมีนักกฎหมายและนักอาชญาวิทยาหลายท่านได้ให้คำจำกัดความไว้ แต่พอสรุปได้ว่าเป็นการกระทำความผิดที่เป็นการละเมิดกฎหมายอาญา โดยผู้กระทำมีเจตนาชั่วร้ายและขัดต่อหลักศีลธรรม ก่อให้เกิดความเสียหายต่อสังคม ดังนั้น ถ้าการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ที่ผู้กระทำมีเจตนาละเมิดกฎหมายอาญา และเข้าลักษณะดังกล่าวข้างต้นก็จะต้องถือว่าเป็นอาชญากรรม นอกจากจะเป็นอาชญากรรมแล้วการกระทำดังกล่าวยังเป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่งด้วย

การกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์มีด้วยกันหลายรูปแบบ โดยสามารถแบ่งออกได้ดังนี้

1. การลักลอบเข้าถึงและการใช้ข้อมูล หรือที่นิยมเรียกกันโดยทั่วไปว่าการเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access) รวมถึงกรณีที่ผู้กระทำได้กระทำนอกเหนืออำนาจที่ตนได้รับ เรียกว่าการกระทำเกินกว่าอำนาจแห่งการเข้าถึง (Exceeds Authorized Access) โดยสามารถแบ่งผู้กระทำการเข้าถึงโดยปราศจากอำนาจได้เป็น 2 จำพวก จำพวกแรกจะกระทำโดยไม่มีเจตนาชั่วร้าย ส่วนมากจะเป็นนักศึกษาที่ต้องการโอ้อวดหรือทดสอบความสามารถของตน บางครั้งจะให้คำแนะนำวิธีการป้องกันระบบให้ดีกว่าที่เป็นอยู่ อีกจำพวกหนึ่งจะกระทำโดยมีเจตนา

ชั่วร้าย มีวัตถุประสงค์เพื่อเข้าไปทำลาย ก่อให้เกิดความเสียหายแก่ระบบด้วยการลบแฟ้มข้อมูลต่างๆ หรือทำให้คอมพิวเตอร์ทำงานไม่ได้

2. การคัดลอกข้อมูลโดยปราศจากอำนาจ ผู้กระทำมีวัตถุประสงค์เพื่อจารกรรมข้อมูลโดยเฉพาะข้อมูลที่เป็นความลับ ข้อมูลทางการเงิน ข้อมูลทางด้านอุตสาหกรรม เช่น การคัดลอกหมายเลขบัตรเครดิตเพื่อนำไปจำหน่ายหรือเพื่อไปกระทำการอย่างอื่นต่อไป

3. การแก้ไขเปลี่ยนแปลงข้อมูล สามารถทำได้โดยการเพิ่มข้อมูล ตัดทอนข้อมูล หรือจำกัดข้อมูล โดยมากผู้กระทำในลักษณะนี้จะมีวัตถุประสงค์เพื่อการฉ้อโกง การแก้ไขเปลี่ยนแปลงข้อมูลสามารถกระทำได้ในแต่ละขั้นตอนการทำงานของคอมพิวเตอร์ ซึ่งการกระทำความผิดในบางขั้นตอนผู้กระทำไม่ต้องมีความรู้เกี่ยวกับเทคโนโลยีสารสนเทศ เพียงแต่มีโอกาสเข้าถึงข้อมูลก็สามารถที่จะทำการแก้ไขเปลี่ยนแปลงข้อมูลนั้นได้ แต่บางขั้นตอนผู้กระทำผิดจะต้องมีความรู้ความชำนาญทางด้านเทคโนโลยีสารสนเทศ เช่น การเขียนโปรแกรม หรือต้องมีความรู้ทางด้านเครือข่ายจึงจะสามารถกระทำความผิดได้

4. การลบและการทำลายข้อมูล ผู้กระทำความผิดจะมีวัตถุประสงค์หลักคือทำให้ข้อมูลเกิดความเสียหาย อาจจะมีสาเหตุมาจากความโกรธแค้นของพนักงาน เหตุผลทางการ หรือเหตุผลทางธุรกิจ แต่สาเหตุที่พบมากที่สุดคือการฉ้อโกงในรูปแบบต่างๆ โดยที่การลบหรือการทำลายข้อมูลเป็นส่วนหนึ่งของการฉ้อโกง

5. การก่อให้เกิดไวรัสคอมพิวเตอร์เพื่อทำลายข้อมูล มีผลเช่นเดียวกับการลบและการทำลายข้อมูล แต่ไวรัสคอมพิวเตอร์จะก่อให้เกิดผลเสียหายในวงกว้างกว่า เพราะไวรัสคอมพิวเตอร์บางชนิดไม่ได้ทำลายเฉพาะข้อมูลที่เฉพาะเจาะจงเท่านั้น แต่จะทำลายข้อมูลทั้งระบบ

ในด้านต่างประเทศนั้น ประเทศสหรัฐอเมริกาได้มีการบัญญัติกฎหมายอาชญากรรมคอมพิวเตอร์มาใช้บังคับเป็นครั้งแรกเมื่อปี ค.ศ. 1984 ต่อมาได้มีการแก้ไขและบัญญัติ The Computer Fraud and Abuse Act of 1986 มาใช้บังคับ ล่าสุดมีการแก้ไขเพิ่มเติมในปี ค.ศ. 1994 (ตามรายละเอียดในภาคผนวก) กฎหมายฉบับนี้ได้แบ่งความผิดออกเป็น 3 ฐาน คือ

1. ความผิดฐานเข้าถึงโดยปราศจากอำนาจ หมายถึงการกระทำโดยเจตนา เข้าไปสู่ สั่ง สื่อสารกับ ใส่ข้อมูลเข้าไปเก็บ ล้วงข้อมูลมาจาก หรืออีกนัยหนึ่งเป็นการเอาประโยชน์ใดๆ ของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์มาใช้ โดยที่ตนเองไม่มีอำนาจที่จะกระทำเช่นนั้น และในกรณีนี้รวมถึงการกระทำเกินกว่าอำนาจแห่งการเข้าถึงด้วย

2. ความผิดฐานแก้ไขเปลี่ยนแปลง หมายถึงการกระทำโดยเจตนาแก้ไขเปลี่ยนแปลงโปรแกรมหรือข้อมูลใดๆ ที่ได้มีการจัดเก็บอยู่ในคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

3. ความผิดฐานทำให้เสียหายหรือทำลาย หมายถึงการกระทำโดยเจตนาก่อให้เกิดความเสียหายหรือทำลายโปรแกรมหรือข้อมูลใดๆ ที่ได้มีการจัดเก็บอยู่ในคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

การที่ประเทศสหรัฐอเมริกาซึ่งเป็นผู้นำทางด้านเทคโนโลยีสารสนเทศ ไม่ว่าเป็นด้านการผลิต จำหน่าย หรือการใช้งาน ได้บัญญัติกฎหมายอาชญากรรมคอมพิวเตอร์มาใช้บังคับ แทนการแก้ไขเพิ่มเติมกฎหมายอื่นๆ ที่เกี่ยวข้อง ทำให้เห็นได้ว่าประเทศสหรัฐอเมริกาได้ตระหนักถึงปัญหาการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ที่เกิดขึ้น และได้ให้ความสำคัญกับอาชญากรรมประเภทนี้

สำหรับประเทศอังกฤษได้มีการบัญญัติกฎหมายอาญาเกี่ยวกับคอมพิวเตอร์ ฉบับแรกมาบังคับใช้คือ The Computer Misuse Act 1990 โดยก่อนที่จะบัญญัติกฎหมายฉบับนี้ ประเทศอังกฤษได้ทำการศึกษารูปแบบการบัญญัติกฎหมายของประเทศสหรัฐอเมริกา ในที่สุดก็ได้บัญญัติความผิดเกี่ยวกับคอมพิวเตอร์เป็น 3 ฐานความผิด คือ

1. ความผิดฐานเข้าถึงโดยปราศจากอำนาจ หมายถึงการกระทำให้คอมพิวเตอร์แสดงการทำงานใดๆ โดยมีเจตนาที่จะเข้าถึงโปรแกรมหรือข้อมูล ซึ่งเก็บไว้ในคอมพิวเตอร์โดยรู้อยู่แล้วว่าตนเองไม่มีอำนาจกระทำเช่นนั้น

2. ความผิดฐานเข้าถึงโดยปราศจากอำนาจโดยมีเจตนาที่จะกระทำ หรือเพื่อความสะดวกในการกระทำความผิดอื่นๆ หมายถึงการกระทำความผิดฐานนี้ต้องผ่านการกระทำความผิดฐานแรกเสียก่อน และการเข้าถึงนั้นมีเจตนากระทำหรือเพื่อความสะดวกในการกระทำความผิดอื่นๆ ที่มีความรุนแรงกว่า โดยไม่จำเป็นต้องพิสูจน์ว่าเจตนาที่จะกระทำความผิดหรือเพื่อความสะดวกในการกระทำความผิดนั้น ได้มีการกระทำความผิดอื่นๆ เกิดขึ้นหรือไม่

3. ความผิดฐานเปลี่ยนแปลงโดยปราศจากอำนาจ หมายถึงการเปลี่ยนแปลงโปรแกรมหรือข้อมูลที่เก็บอยู่ในคอมพิวเตอร์ ไม่ว่าจะเป็นการกระทำโดยการแทรก ตัดทอน แก้ไขเปลี่ยนแปลง หรือลบโปรแกรมหรือข้อมูลก็ตาม

จากฐานความผิดที่บัญญัติในกฎหมายฉบับนี้ จะเห็นได้ว่าประเทศอังกฤษมีแนวคิดในการคุ้มครองข้อมูลอย่างเคร่งครัดมาก ดังจะเห็นได้จากฐานความผิดที่หนึ่งและที่สองดังกล่าวข้างต้นนั้น มีเนื้อหาคุ้มครองข้อมูลอย่างเคร่งครัด อีกทั้งความผิดในฐานความผิดที่สองได้ลงโทษถึงการกระทำความผิดในอนาคตที่ยังไม่ได้กระทำไว้ด้วย และยังมุ่งการพิสูจน์ในส่วนของเจตนาร้าย (Mens Rea) เป็นหลักโดยได้ให้เหตุผลว่าการพิสูจน์ถึงเจตนาอันทุจริตในขณะกระทำความผิดนั้น เป็นเรื่องที่ง่ายกว่าการไปตีความของการกระทำว่ากระทำความผิดหรือไม่ กล่าวคือหากขณะที่กระทำการเข้าสู่ระบบประมวลผลด้วยจิตใจอันทุจริตแล้ว ถือว่ามีเจตนากระทำความผิดแล้ว ซึ่งหากพิสูจน์ถึงเรื่องการกระทำจะเป็นสิ่งที่ยากที่จะชี้ว่ากระทำความผิดหรือไม่ เพราะบางกรณีอาจมีการเข้าสู่ระบบโดยมีการกระทำทางกายภาพแต่อาจจะขาดเจตนาทางจิตใจที่เป็นการทุจริตก็ได้

สำหรับประเทศไทยนั้น ปัจจุบันยังไม่มีกฎหมายอาชญากรรมคอมพิวเตอร์ เมื่อมีการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์เกิดขึ้น ก็จะอาศัยการปรับใช้กับฐานความผิดในประมวลกฎหมายอาญา และความผิดตามพระราชบัญญัติที่มีลักษณะใกล้เคียงกัน เช่น

1. ความผิดฐานลักทรัพย์ ตามประมวลกฎหมายอาญามาตรา 334 มีสาระสำคัญที่ต้องพิจารณาอยู่สองส่วนด้วยกันคือ ส่วนแรกความหมายของคำว่า "ทรัพย์" เนื่องจากประมวลกฎหมายอาญาไม่มีบทนิยามของคำว่า "ทรัพย์" การที่จะวินิจฉัยว่าอะไรเป็นทรัพย์ จึงต้องถือตามประมวลกฎหมายแพ่งและพาณิชย์ ซึ่งได้นิยามคำว่า "ทรัพย์" ไว้ว่า หมายถึงวัตถุที่มีรูปร่าง เมื่อข้อมูลในคอมพิวเตอร์เป็นสิ่งที่ไม่มีรูปร่างจึงไม่อาจเป็นทรัพย์ตามคำนิยามนี้ และส่วนที่สองความหมายของคำว่า "เอาไป" ศาลฎีกาได้วางบรรทัดฐานไว้ว่าหมายถึงการพาทรัพย์เคลื่อนที่ไปจากการครอบครองของผู้อื่น ซึ่งเท่ากับว่ามีการกระทำอยู่สองประการ คือการแย่งการครอบครองประการหนึ่ง และการพาทรัพย์เคลื่อนที่ไปอีกประการหนึ่ง แม้ว่าข้อมูลจะสามารถเคลื่อนที่ได้โดยการอาศัยเครื่องมือบางอย่างก็ตาม แต่ข้อมูลไม่อาจเป็นทรัพย์หรือทรัพย์สินที่ถูกแย่งการครอบครองได้ เพราะทรัพย์หรือทรัพย์สินที่จะถูกแย่งการครอบครองได้นั้น จะต้องมีลักษณะพิเศษคือมีผู้ทรงสิทธิได้แต่เพียงผู้เดียว (Exclusive Right) รวมทั้งสามารถกีดกันผู้อื่นมิให้ยุ่งเกี่ยวได้ แต่ข้อมูลไม่ได้มีลักษณะเช่นนั้น ข้อมูลสามารถไหลไปได้อย่างเสรีตามลักษณะธรรมชาติของตนเอง (By Nature) และความหมายของการเอาไปในความผิดฐานลักทรัพย์จะต้องมีลักษณะสมมาตร กล่าวคือมีผู้ได้ฝ่ายหนึ่งและผู้เสียฝ่ายหนึ่ง แต่ลักษณะธรรมชาติของข้อมูลในคอมพิวเตอร์นั้นไม่มีอะไรเสียไปยังคงเหมือนเดิมทุกประการ เมื่อข้อมูลในคอมพิวเตอร์ไม่ได้เป็นทรัพย์และไม่สามารถถูกแย่งการครอบครองได้ จึงไม่อาจนำความผิดฐานลักทรัพย์มาปรับใช้กับการลักข้อมูลในคอมพิวเตอร์ได้

2. ความผิดฐานยักยอก ตามประมวลกฎหมายอาญามาตรา 352 องค์ประกอบสำคัญของความผิดตามมาตรานี้คือการ "เบียดบัง" ซึ่งมีความหมายเช่นเดียวกับคำว่า "เอาไป" ในความผิดฐานลักทรัพย์ อันมีลักษณะเป็นการตัดกรรมสิทธิ์ และจากเหตุผลที่กล่าวแล้วในความผิดฐานลักทรัพย์ไม่ว่าจะเป็นในส่วนของความหมายของคำว่าทรัพย์หรือลักษณะธรรมชาติของข้อมูล จึงสามารถกล่าวได้ว่าไม่อาจนำความผิดตามมาตรานี้ มาปรับใช้กับการยักยอกข้อมูลในคอมพิวเตอร์ได้

3. ความผิดฐานปลอมเอกสาร ตามประมวลกฎหมายอาญา มาตรา 264 บัญญัติถึงการทำเอกสารปลอม เติมหรือตัดทอนข้อความหรือแก้ไขด้วยประการใดๆ ในเอกสารที่แท้จริงเป็นความผิด ในเรื่องนี้แม้ว่าการทำเอกสารปลอม เติมหรือตัดทอนข้อความหรือแก้ไขด้วยประการใดๆ โดยวัตถุแห่งการกระทำต่อเป็นข้อมูลในคอมพิวเตอร์ หรือกล่าวอีกนัยหนึ่งเป็นการใช้คอมพิวเตอร์ในการกระทำความผิดฐานปลอมเอกสารก็ตาม แต่ก็ใช่ว่าวัตถุแห่งการกระทำต่อต้องเป็นข้อมูลในคอมพิวเตอร์เท่านั้น ด้วยเทคโนโลยีสารสนเทศในปัจจุบันผู้กระทำสามารถแก้ไขเปลี่ยนแปลงข้อมูลในขณะที่มีการสื่อสารข้อมูลได้โดยไม่ต้องแก้ไขที่ตัวข้อมูล แต่เป็นการแก้ไขเปลี่ยนแปลงสัญญาณทางอิเล็กทรอนิกส์ ซึ่งไม่อาจถือได้ว่าสิ่งเหล่านี้เป็นเอกสารตามความหมายของคำนิยามคำว่า "เอกสาร" มาตรา 1 (7) ได้ แม้ว่าภายหลังสัญญาณทางอิเล็กทรอนิกส์จะแปรสภาพมาอยู่ในรูปของข้อมูลก็ตาม ดังนั้น การที่จะนำความผิดฐานปลอมเอกสารมาปรับใช้ก็จะเกิดข้อขัดข้องดังกล่าวขึ้นได้

4. ความผิดฐานทำให้เสียทรัพย์ ตามประมวลกฎหมายอาญา มาตรา 358 บัญญัติถึงการทำให้เสียหาย ทำลาย ทำให้เสื่อมค่า หรือทำให้ไร้ประโยชน์แก่ทรัพย์ของผู้อื่นหรือผู้อื่นเป็นเจ้าของรวมอยู่ด้วยเป็นความผิด นอกจากประเด็นความหมายของคำว่า "ทรัพย์" ที่ได้กล่าวไว้แล้วในความผิดฐานลักทรัพย์ ยังมีอีกประเด็นที่จะต้องพิจารณาคือข้อมูลเป็นสิ่งที่ไม่มีรูปร่าง เช่นเดียวกับทรัพยสิทธิในอสังหาริมทรัพย์ แต่ต่างกันตรงที่ว่าทรัพยสิทธิไม่สามารถถูกทำลายได้ ทรัพยสิทธิจะสูญไปก็เนื่องมาจากทรัพย์ที่เป็นหลักฐานแห่งสิทธิถูกทำลาย แต่ข้อมูลสามารถถูกทำลายได้ จึงก่อให้ข้อสงสัยว่าการทำลายข้อมูลในคอมพิวเตอร์นั้น จะเป็นความผิดฐานทำให้เสียทรัพย์ได้หรือไม่ ในเรื่องนี้แม้จะยังไม่มีคำพิพากษาฎีกาออกมาเป็นบรรทัดฐาน แต่ในอนาคตหากศาลฎีกาวินิจฉัยว่าไม่เป็นความผิดฐานทำให้เสียทรัพย์ ก็จะทำให้ไม่สามารถนำความผิดฐานนี้มาปรับใช้เพื่อลงโทษผู้กระทำได้ ในทางกลับกันหากวินิจฉัยว่าเป็นความผิดฐานทำให้เสียทรัพย์ ก็จะเป็นการตีความที่ขัดต่อลายลักษณ์อักษรและเจตนารมย์ของกฎหมาย รวมทั้งขัดต่อหลักกฎหมายอาญา

5. ความผิดฐานบุกรุก ตามประมวลกฎหมายอาญา มาตรา 362 บัญญัติถึงการกระทำที่เป็นความผิดไว้สองประการ คือ กระทำการโดยเจตนาเข้าไปในอสังหาริมทรัพย์ของผู้อื่นเพื่อแย่งการครอบครอง และกระทำการโดยเจตนาเข้าไปในอสังหาริมทรัพย์ของผู้อื่นเพื่อรบกวน

การครอบครอง จะเห็นได้ว่าความผิดทั้งสองประการมุ่งเน้นไปที่อสังหาริมทรัพย์ แม้ว่าบางครั้งจะเรียกว่าความผิดประการที่สองว่าเป็นการก่อความเดือดร้อนรำคาญก็ตาม แต่การรบกวนหรือการก่อความเดือดร้อนรำคาญนั้น หมายถึงเฉพาะสิทธิในการครอบครองอสังหาริมทรัพย์เท่านั้นและไม่หมายรวมถึงทรัพยสิทธิต่างๆ เพราะทรัพยสิทธิไม่อยู่ในข่ายของความหมายคำว่า "เข้าไป" ได้ ในส่วนของการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์นั้น หากผู้กระทำความผิดได้เข้าไปอสังหาริมทรัพย์ของผู้อื่นโดยเจตนาเพื่อรบกวนการครอบครอง ก็จะต้องมีความผิดฐานบุกรุกแม้ว่าการเข้าไปนั้นจะยังไม่ได้กระทำอันตรายใดๆ ต่อข้อมูลก็ตาม แต่ด้วยความสามารถของเทคโนโลยีสารสนเทศในปัจจุบัน การกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ไม่จำเป็นต้องเข้าไปในอสังหาริมทรัพย์ของผู้อื่นก็สามารถกระทำความผิดได้ ดังนั้น การที่จะนำความผิดฐานบุกรุกมาปรับใช้กับการบุกรุกทางคอมพิวเตอร์นั้น จึงเกิดข้อติดขัดในกรณีที่ผู้กระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ไม่ได้เข้าไปในอสังหาริมทรัพย์ของผู้อื่น

6. ความผิดตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ก่อนที่จะมีประกาศใช้พระราชบัญญัติฉบับนี้ การให้ความคุ้มครองโปรแกรมคอมพิวเตอร์ยังมีความคลุมเครืออยู่ อันเนื่องมาจากความไม่ชัดเจนของคำนิยาม แต่หลังจากที่มีการประกาศใช้ทำให้การคุ้มครองโปรแกรมคอมพิวเตอร์มีความชัดเจนมากขึ้น โดยโปรแกรมที่ได้รับความคุ้มครองนั้นมิใช่มีเพียงแต่โปรแกรมชุดคำสั่งเท่านั้น แต่ยังรวมถึงโปรแกรมที่อยู่ในรูปของข้อมูลที่เก็บในลักษณะฐานข้อมูลด้วย ส่วนการพิจารณาว่าฐานข้อมูลจะได้รับความคุ้มครองหรือไม่ก็เป็นไปตามหลักเกณฑ์ของมาตรา 12 ตามพระราชบัญญัติฉบับนี้ อย่างไรก็ตามพระราชบัญญัติฉบับนี้ก็ยังมีปัญหาความไม่ชัดเจนของบทบัญญัติบางมาตรา เช่น คำนิยามคำว่า "ทำซ้ำ" นั้นจะรวมถึงการนำโปรแกรมหรือข้อมูลบรรจุลงในหน่วยความจำของเครื่องหรือไม่ ซึ่งปัญหานี้และปัญหาอื่นที่มีความไม่ชัดเจนของตัวบทบัญญัติคงจะต้องอาศัยการตีความของคำพิพากษาฎีกา และถ้าตีความออกมาในลักษณะที่เจ้าของโปรแกรมหรือข้อมูลเสียประโยชน์ก็จะมีแรงผลักดันให้มีการแก้ไขกฎหมาย ดังนั้น หากมีมาตรการมาคุ้มครองโปรแกรมหรือข้อมูล เพื่อป้องกันการละเมิดลิขสิทธิ์ก็น่าจะมีประโยชน์ไม่น้อย

7. ความผิดตามพระราชบัญญัติโทรเลขและโทรศัพท์ พ.ศ. 2477 เนื่องจากการใช้คอมพิวเตอร์ในเชิงเทคโนโลยีสารสนเทศมีเกี่ยวเนื่องกับการสื่อสาร จึงมักจะเกิดความผิดที่คาบเกี่ยวกับพระราชบัญญัติฉบับนี้ โดยมาตรา 24 บัญญัติถึง "การกระทำที่มิชอบด้วยกฎหมาย เพื่อล่วงรู้เนื้อหาในข่าวสาร โทรเลข โทรศัพท์" ซึ่งการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ไม่ใช่เป็นการโทรเลข หรือโทรศัพท์ พระราชบัญญัติฉบับนี้จึงครอบคลุมไปไม่ถึง ทำให้ต้องมีการแก้ไขเพิ่มเติม โดยให้มาตรา 24 ที่แก้ไขใหม่ มีเนื้อหาครอบคลุมถึงการกระทำผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ด้วยซึ่งก็น่าจะเป็นเรื่องที่ดี แต่การแก้ไขมาตราอื่นก็ยังมีขอบเขตที่จำกัดและอาจก่อให้เกิดปัญหาการตีความในอนาคต ดังที่ได้กล่าวไว้แล้วในหัวข้อ 5.3.2 และถ้ามีการตีความออก

มาว่ามาตรานั้นๆ ไม่ครอบคลุมถึงการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ ก็จะก่อให้เกิดข้อขัดข้องในการบังคับใช้

8. ความผิดตามพระราชบัญญัติวิทยุคมนาคม พ.ศ. 2498 เนื่องจากปัจจุบันมีการสื่อสารข้อมูลในเครือข่ายกันหลายรูปแบบ รูปแบบหนึ่งก็คือการสื่อสารวิทยุ โดยมีวิธีการคือส่งสัญญาณคลื่นแม่เหล็กไฟฟ้าผ่านอากาศไปยังเครื่องรับ ตามที่ได้กล่าวไว้แล้วในหัวข้อ 2.1.2.1 ดังนั้น เมื่อเกิดการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์เกิดขึ้น ก็เกิดความพยายามที่ปรับการกระทำดังกล่าวกับความผิดตามพระราชบัญญัติฉบับนี้ ซึ่งก็ไม่สามารถจะปรับได้ เพราะไม่ว่าจะเป็นการเข้าถึงโดยปราศจากอำนาจ การแก้ไขเปลี่ยนแปลงข้อมูล การลบและการทำลายข้อมูลไม่อยู่ในความหมายที่ว่าเป็นการรบกวนหรือขัดขวางต่อการวิทยุคมนาคม อันถือเป็นความผิดตามพระราชบัญญัติฉบับนี้แต่อย่างใด อีกทั้งการสื่อสารข้อมูลดังกล่าวก็ไม่ใช่วิธีการส่งหรือรับด้วยคลื่นแฮรตเซียน และข่าววิทยุคมนาคมก็ไม่อาจแปลความให้ครอบคลุมถึงข้อมูลในคอมพิวเตอร์ได้

6.2 ข้อเสนอแนะ

จากการวิเคราะห์กฎหมายที่มีโทษทางอาญาของไทยที่ใช้บังคับอยู่ ไม่ว่าจะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติที่กล่าวมาข้างต้น จะเห็นได้ว่ายังไม่เพียงพอต่อการแก้ไขปัญหาการกระทำความผิดที่ผู้กระทำได้มีการพัฒนารูปแบบ โดยอาศัยเทคโนโลยีใหม่ๆ มากระทำความผิด โดยเฉพาะความผิดที่เกี่ยวกับข้อมูลที่ได้มาจากเทคโนโลยีสมัยใหม่ ผู้วิจัยจึงขอเสนอแนะว่า ควรจะมีมาตรการรักษาความปลอดภัยของข้อมูล ดังนี้

1. การกำหนดแนวนโยบายแห่งชาติ รัฐควรจะมีการกำหนดแนวนโยบายเทคโนโลยีสารสนเทศแห่งชาติ ไว้ในแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ เพื่อที่ส่วนราชการจะได้ใช้เป็นแนวทางในการปฏิบัติ เช่น กำหนดให้มีการปฏิรูปกฎหมายเทคโนโลยีสารสนเทศ และถ้าจำเป็นก็ควรจัดให้มีหน่วยงานเฉพาะทางด้านเทคโนโลยีสารสนเทศ เพื่อจัดการกับปัญหาต่างๆ ได้ครบวงจร อีกทั้งเพื่อให้เป็นการสอดรับกับรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 ซึ่งได้กำหนดหลักการสำคัญไว้ใน หมวด 5 แนวนโยบายแห่งรัฐ โดยมาตรา 78 บัญญัติว่า "รัฐต้อง... พัฒนาเศรษฐกิจท้องถิ่นและระบบสาธารณูปโภคและระบบสาธารณูปการ ตลอดทั้งโครงสร้างพื้นฐานสารสนเทศในท้องถิ่นให้ทั่วถึง และเท่าเทียมกันทั่วประเทศ..."

2. มาตรการป้องกัน แต่ละองค์กรจะต้องมีการป้องกันระบบคอมพิวเตอร์ของตนให้ปลอดภัยจากการคุกคามของผู้ที่ไม่หวังดี มาตรการป้องกันมีมากมายหลายวิธี เช่น

มาตรการป้องกันทางนโยบายและการบริหาร มีกำหนดอำนาจหน้าที่และความรับผิดชอบอย่างชัดเจน เพื่อมิให้มีเกิดความผิดพลาดขึ้นได้ มีการถ่วงดุลอำนาจในตำแหน่งหรืองานที่สำคัญหรืองานที่มีผลประโยชน์มากๆ โดยให้มีบุคคลอื่นที่จะสามารถทำการตรวจสอบได้ ไม่ควรให้รับผิดชอบเพียงบุคคลคนเดียว อาจจะให้รับผิดชอบเป็นคณะบุคคล มีการกำหนดเป็นนโยบายหรือระเบียบการบริหารงาน และถ้าหากมีการฝ่าฝืนก็ต้องมีการลงโทษ

มาตรการป้องกันทางเทคนิค เช่น การป้องกันทางด้านกายภาพ โดยทำการจัดเก็บรักษาอุปกรณ์ หรือสื่อที่ใช้เก็บข้อมูล จัดให้มีระบบการป้องกันอัคคีภัยที่มีประสิทธิภาพ ดูแลรักษาสายสื่อสารที่ติดต่อกับระบบคอมพิวเตอร์ เพื่อป้องกันมิให้บุคคลภายนอกลักลอบเข้ามาในเครือข่ายโดยไม่ได้รับอนุญาต มีการกำหนดมาตรการการเข้าถึงข้อมูล เช่น การระบุตัวผู้ใช้ และรหัสผ่าน เพื่อเป็นการยืนยันว่าเป็นผู้ที่ใช้ระบบได้จริง การควบคุมโดยใช้ลักษณะทางชีวภาพ เช่น ตรวจลายนิ้วมือ ตรวจเสียง ตรวจเรตินาจากดวงตา ตรวจภาพถ่าย เป็นต้น จัดให้มีการแบ่งแยกประเภทผู้ใช้ประโยชน์จากฐานข้อมูลว่าเป็นผู้ใช้ในระดับใด มีการกำหนดเวลาการใช้งานของเครื่อง การกำหนดรหัสผ่านก่อนใช้เครื่อง มีการเข้ารหัสลับข้อมูลซึ่งเป็นการกำหนดวิธีการเปลี่ยนแปรรหัสของข้อมูลที่จัดเก็บอยู่ในระบบ ให้อยู่ในรูปที่ไม่สามารถอ่านให้เข้าใจได้สำหรับข้อมูลที่เป็นความลับ อีกทั้งต้องมีการสำรองข้อมูล ซึ่งเป็นวิธีการลดความเสียหายที่อาจเกิดขึ้นได้เมื่อข้อมูลนั้นสูญหายหรือถูกทำลาย และควรเก็บข้อมูลสำรองไว้ในที่ปลอดภัย มีการเขียนโปรแกรมหรือการใช้โปรแกรม เพื่อช่วยตรวจสอบระบบรักษาความปลอดภัยและป้องกันการเข้าถึงโดยปราศจากอำนาจ เช่น โปรแกรมสำหรับถอดรหัสผ่าน โปรแกรมที่จะทำการบันทึกรายละเอียดการขอใช้บริการต่างๆ โปรแกรมวิเคราะห์ปริมาณการใช้งานในเครือข่าย โปรแกรมตรวจสอบและรายงานให้ทราบถึงจุดอ่อนต่างๆ ของระบบคอมพิวเตอร์บนเครือข่าย การติดตั้งตัวป้องกันการบุกรุก (Firewall) และการติดตั้งตัวบริการแทน (Proxy)

3. มาตรการปราบปราม ซึ่งจะต้องมีการบัญญัติกฎหมายบังคับเฉพาะ (Specific Law) คือกฎหมายอาชญากรรมคอมพิวเตอร์ เพื่อใช้ป้องกันสังคมต่อการกระทำของอาชญากรที่กระทำต่อข้อมูล อุปกรณ์ที่เกี่ยวข้องกับการจัดเก็บข้อมูลและการส่งผ่านข้อมูล การบัญญัติกฎหมายอาชญากรรมคอมพิวเตอร์มาใช้บังคับเช่นเดียวกับบางประเทศ จะเป็นการขจัดปัญหาและอุปสรรคสำหรับคดีอาชญากรรมคอมพิวเตอร์ที่เมื่อเกิดขึ้นแล้วจะต้องปรับใช้กับกฎหมายอื่น โดยผู้วิจัยเห็นว่ากฎหมายฉบับนี้ จะต้องมีขอบเขตกว้างขวางพอที่จะครอบคลุมการกระทำความผิดทั้งหมด แต่ขอบเขตที่กว้างขวางนั้นจะต้องไม่รวมการกระทำที่เป็นเพียงแค่การผิดมารยาทหรือผิด

จรรยาบรรณเข้าไปด้วย อย่างไรก็ตามการบัญญัติกฎหมายก็ควรจะต้องคำนึงถึงความต้องการของสังคมด้วย เพราะอาจจะไปกระทบต่อสิทธิเสรีภาพของประชาชนที่ต้องสูญเสียไป อนึ่งจากการที่ผู้วิจัยได้ค้นคว้าหาข้อมูลสำหรับการทำวิจัยฉบับนี้ ทำให้ได้ทราบว่าปัจจุบันได้มีการจัดตั้งคณะอนุกรรมการเพื่อยกร่างกฎหมายอาชญากรรมคอมพิวเตอร์แล้ว และกฎหมายฉบับนี้เป็นหนึ่งในหกฉบับของโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ ซึ่งอยู่ในความรับผิดชอบของศูนย์เทคโนโลยีและคอมพิวเตอร์แห่งชาติ (The National Electronics and Computer Technology Center : NECTEC)

อย่างไรก็ตาม แม้จะมีมาตรการต่างๆ ออกมาใช้บังคับก็เป็นเพียงวิธีการหนึ่งสำหรับการแก้ปัญหาในเรื่องนี้เท่านั้น แต่ความรู้สำนึกและการมีจรรยาบรรณของคนต่างหากที่สามารถแก้ปัญหานี้ได้อย่างสิ้นเชิงและถาวร