บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันนี้หน่วยงานต่างๆ จะต้องใช้ข้อมูลในการตัดสินใจแทบทุกเรื่อง ทำให้ต้องมีข้อมูลมากมาย จึงจำเป็นต้องอาศัยเทคโนโลยีสมัยใหม่ในการจัดการกับข้อมูลเหล่านั้น เทคโนโลยีสารสนเทศเป็นเครื่องมือชนิดหนึ่งที่สามารถช่วยจัดการกับข้อมูลให้เป็นระบบได้ โดยเฉพาะคอมพิวเตอร์ ไม่ว่าจะเป็นการจัดเก็บข้อมูล แยกแยะข้อมูล ประมวลผล (Process) วิเคราะห์ข้อมูลและทำรายงาน รวมถึงการสื่อสารโทรคมนาคมก็สามารถทำได้อย่างรวดเร็ว แต่ก็ใช่ว่าเทคโนโลยีสารสนเทศจะจัดการแก้ปัญหาได้ทุกเรื่อง เพราะการทำงานของคอมพิวเตอร์นั้นไม่ใช่จะทำงานได้โดยปราศจากความเกี่ยวข้องของมนุษย์ คอมพิวเตอร์จะทำงานได้นั้นจะต้องมีคำสั่งหรือชุดคำสั่งที่เรียกกันว่าโปรแกรม (Program) อันจะต้องอาศัยคนเราควบคุมการทำงานของคอมพิวเตอร์และข้อมูลในคอมพิวเตอร์

ขณะที่ข้อมูลเป็นสิ่งจำเป็นสำหรับกิจกรรมต่างๆ เสมือนองค์ประกอบพื้นฐานที่สามนอกจากสสารและพลังงาน ผลประโยชน์อันเกิดจากข้อมูลก็เพิ่มมากขึ้นเหมือนเงาตามตัว จึงทำให้เกิดการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ เช่น การเข้าถึงข้อมูลโดยปราศจากอำนาจ การแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ การลบและการทำลายข้อมูล ซึ่งเกิดขึ้นไม่เว้นแต่ละวัน การกระทำเหล่านี้ถือเป็นอาชญากรรมอย่างหนึ่งอันก่อให้เกิดความสูญเสียทางด้านทรัพย์สินมูลค่ามหาศาล และนับวันอาชญากรรมประเภทนี้จะมีมากขึ้น ตลอดจนมีการพัฒนารูปแบบการกระทำความผิดไปตามความก้าวหน้าของเทคโนโลยีสารสนเทศ จึงจำเป็นอย่างยิ่งที่จะต้องมีมาตรการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึงและเรียกใช้ข้อมูลโดยปราศจากอำนาจ การทำลายข้อมูลไม่ว่าจะกระทำโดยเจตนาหรือไม่ก็ตาม

มาตรการรักษาความปลอดภัยของข้อมูลที่กล่าวถึง จะต้องให้ความสำคัญกับสิ่งต่อไปนี้

1. ด้านกฎหมาย (Legal Issue) การมีมาตรการทางกฎหมายเป็นวิถีทางหนึ่งที่จัดการกับปัญหาอาชญากรรมคอมพิวเตอร์ ดังจะเห็นได้จากการที่หลายๆ ประเทศมีกฎหมายอาชญากรรมคอมพิวเตอร์ ซึ่งสามารถสรุปความผิดพื้นฐานจากกฎหมายของต่างประเทศ แบ่งเป็น 3 ประเภท ได้แก่ ประเภทแรกความผิดฐานเข้าถึงโดยปราศจากอำนาจหรือการกระทำเกินกว่าอำนาจแห่งการเข้าถึง ประเภทที่สองความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ และประเภทสุดท้ายคือความผิดฐานทำให้เสียหายหรือทำลายข้อมูล อีกทั้งบางประเทศยังมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งข้อมูลบางอย่างถือว่าเป็นสิ่งที่ไม่พึงเปิดเผย เช่น การที่มีประวัติเป็นผู้ถูกจำคุกหรือเป็นผู้ติดยาเสพติด การที่มีประวัติถูกสอบสวนทางวินัย หรือข้อมูลค่าจ้าง เงินเดือน การเปิดเผยข้อมูลประเภทนี้นอกจากผิดจรรยาบรรณแล้ว ยังจะต้องมีกฎหมายรับประกันสิทธิในการให้หรือใช้ข้อมูลอย่างไม่ถูกต้องด้วย

2. ด้านจรรยาบรรณ (Moral or Ethical Issue) เป็นการป้องกันการเข้าถึงและเรียกใช้ข้อมูลโดยไม่ได้รับอนุญาต เช่น การนำข้อมูลส่วนบุคคลไปทำร้ายกันทางงานอาชีพ ทางการเมือง ซึ่งเป็นการใช้ผิดวัตถุประสงค์ของการจัดเก็บข้อมูลไว้ในฐานข้อมูล

3. ด้านความลับของบริษัท (Corporate Secrecy) บริษัทต่างๆ จะมีข้อมูลบางอย่างที่เปิดเผยไม่ได้ เช่น กระบวนการผลิตสินค้า สูตรการผลิต ราคาประมูล สิ่งเหล่านี้ถ้ามีการเปิดเผยจะทำให้บริษัทขาดรายได้

4. ด้านการฉ้อฉลหรือการทำลาย (Fraud or Sabotage) สาเหตุหนึ่งที่ก่อให้เกิดการรั่วไหลของข้อมูลคือ พนักงานไม่พอใจบริษัทหรือพนักงานทุจริต

1.2 ขอบเขตของการวิจัยและวัตถุประสงค์การวิจัย

อาชญากรรมคอมพิวเตอร์ก่อให้เกิดความเสียหายและเป็นอันตรายแก่ระบบต่างๆ ของประเทศ ไม่ว่าจะเป็นระบบความมั่นคง เศรษฐกิจ สังคมและการเมือง อาชญากรรมคอมพิวเตอร์มีอยู่ด้วยกันหลายประเภท หนึ่งในจำนวนเหล่านั้นก็คือการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ ไม่ว่าจะเป็นการเข้าถึงโดยปราศจากอำนาจ การแก้ไขเปลี่ยนแปลงข้อมูล การลบและการทำลายข้อมูล บุคคลที่กระทำความผิดจะได้รับประโยชน์จากการกระทำเหล่านี้และยังก่อให้เกิดความไม่เชื่อถือข้อมูลของผู้ที่เกี่ยวข้องหรือประชาชนทั่วไป ซึ่งไม่ใช่แต่ประเทศไทยเท่านั้น ในต่างประเทศก็มีเหตุการณ์เหล่านี้เกิดขึ้นไม่เว้นแต่ละวัน

การวิจัยฉบับนี้ จะได้ทำการศึกษาอาชญากรรมคอมพิวเตอร์เฉพาะในแง่ที่อาชญากรกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ ซึ่งประกอบด้วยรูปแบบวิธีการต่างๆ ที่เกิดขึ้นกับข้อมูล และบางส่วนในการวิจัยได้ทำการศึกษารูปแบบวิธีการก่ออาชญากรรมลักษณะนี้ในต่างประเทศ ได้แก่ ประเทศสหรัฐอเมริกา และประเทศอังกฤษ ตลอดจนศึกษาถึงแนวทางและมาตรการรักษาความปลอดภัยของข้อมูล รวมถึงมาตรการทางกฎหมายอาญาของต่างประเทศที่ได้บัญญัติออกมาบังคับใช้ อันจะนำไปสู่แนวทางการบัญญัติกฎหมายและมาตรการต่างๆ เพื่อที่จะให้ความคุ้มครองแก่ข้อมูลในคอมพิวเตอร์ของประเทศไทย อันเป็นวัตถุประสงค์ของการวิจัยฉบับนี้

1.3 สมมุติฐาน

โดยปกติอาชญากรรมที่เกิดในปัจจุบันแม้จะรุนแรงแต่ก็มีรูปแบบไม่ซับซ้อน ไม่ยากในการปราบปราม แต่เนื่องจากนานาอารยประเทศได้มีการพัฒนาเทคโนโลยีมาอำนวยความสะดวกสำหรับการดำเนินชีวิตและการทำธุรกิจมากขึ้น อาชญากรจึงมีการพัฒนารูปแบบและอาศัยเทคโนโลยี โดยนำมาตรการใหม่ๆ มาใช้ ก่อให้เกิดปัญหาในการพิสูจน์ความผิด และสาเหตุหนึ่งที่ไม่อาจป้องกันอาชญากรรมดังกล่าวได้ก็คือ การขาดมาตรการรักษาความปลอดภัยของข้อมูลที่ได้มาจากเทคโนโลยีสมัยใหม่ แม้ว่าหลายหน่วยงานได้นำมาตรการป้องกันข้อมูลในรูปแบบต่างๆ มาใช้แล้วก็ตาม แต่ก็ไม่อาจยับยั้งอาชญากรรมประเภทนี้ได้ อีกทั้งมาตรการปราบปรามอันได้แก่ กฎหมายที่มีโทษทางอาญาซึ่งนำมาปรับใช้อยู่ในปัจจุบันยังมีช่องว่างในด้านการตีความ ก่อให้เกิดปัญหาทางกฎหมาย ดังนั้นจึงจำเป็นต้องมีมาตรการป้องกันและปราบปรามที่ชัดเจน อันจะต้องมีการบัญญัติกฎหมายเฉพาะเพื่อให้ครอบคลุมการกระทำความผิดในเรื่องนี้ได้อย่างเหมาะสม

1.4 วิธีดำเนินการวิจัย

เป็นการวิจัยแบบเอกสาร โดยการศึกษาวิเคราะห์ข้อมูลจากเอกสารเป็นหลัก

1.5 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1. เพื่อให้ทราบถึงลักษณะการจัดเก็บ การใช้ และการสื่อสารข้อมูลในคอมพิวเตอร์
2. เพื่อให้ทราบถึงความเสียหายต่อการลักลอบใช้ การแก้ไขเปลี่ยนแปลง การลบและการทำลายข้อมูลในคอมพิวเตอร์

3. เพื่อแสดงให้เห็นถึงแนวความคิดในการบังคับใช้กฎหมายที่มีโทษทางอาญา ในการลักลอบใช้ การแก้ไขเปลี่ยนแปลง การลบและการทำลายข้อมูลในคอมพิวเตอร์

4. เพื่อให้ทราบถึงแนวความคิดการบังคับใช้กฎหมายที่มีโทษทางอาญาของต่างประเทศ ในการลักลอบใช้ การแก้ไขเปลี่ยนแปลง การลบและการทำลายข้อมูลในคอมพิวเตอร์

5. เพื่อให้ทราบถึงแนวทางการปรับปรุงแก้ไขหรือเพิ่มบทบัญญัติกฎหมาย ในการรักษาความปลอดภัยของข้อมูลในคอมพิวเตอร์