ความรับผิดทางอาญาเกี่ยวกับโปรแกรมเรียกค่าไถ่ในกฎหมายว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์
Criminal liability on the Ransomware program under Law on computer-related crime

ปรมินทร์ แสงศักดิ์สิทธารถ[1*]
[1]คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม
2410/2 ถนนพหลโยธิน จตุจักร กรุงเทพมหานคร 10900
*E-mail: ramin_ut62@hotmail.com

บทคัดย่อ

วิทยานิพนธ์ฉบับนี้มุ่งเพื่อศึกษาความหมาย รูปแบบ และผลกระทบในการกระทำโปรแกรมเรียกค่าไถ่ข้อมูลทางคอมพิวเตอร์ โดยทำการศึกษาจากกฎหมายของประเทศไทยและกฎหมายของต่างประเทศที่เกี่ยวข้องกับการกระทำในลักษณะละเมิดสิทธิของผู้อื่น โดยการใช้โปรแกรมเรียกค่าไถ่ข้อมูลทางคอมพิวเตอร์ แม้ว่ากฎหมายในประเทศไทยที่เกี่ยวข้องกับการเรียกค่าไถ่ข้อมูลทางคอมพิวเตอร์ ถือเป็นการกระทำที่กระทบสิทธิส่วนบุคคล เสรีภาพ และส่งผลกระทบต่ออารมณ์ความรู้สึกสภาพจิตใจของผู้เสียหาย อีกทั้งยังสร้างความเสียหายต่อองค์กรของรัฐและความมั่นคงของประเทศซึ่งอาจนำไปสู่ภยันตรายร้ายแรงและอาชญากรรมอื่น ๆ ตามมา ด้วยเหตุที่ประเทศไทยยังไม่มีบทบัญญัติกฎหมายในการนำมาปรับใช้กับการกระทำโปรแกรมเรียกค่าไถ่ข้อมูลทางคอมพิวเตอร์ได้ จึงเป็นการสมควรที่รัฐจะเห็นความสำคัญในการปรับปรุงกฎหมายที่มีอยู่ เพราะบางกรณีการกระทำความผิดที่เกิดขึ้นก็ไม่มีบทบัญญัติองค์ประกอบความผิดที่กฎหมายนั้น ๆ กำหนด ทำให้ไม่สามารถเอาผิดกับผู้กระทำความผิดได้

ในการศึกษาผู้วิจัยมีข้อเสนอแนะว่า ควรบัญญัติให้การกระทำความผิดเกี่ยวกับการใช้โปรแกรมเรียกค่าไถ่ข้อมูลทางคอมพิวเตอร์มีความรับผิดทางอาญาโดยตรง โดยการเพิ่มฐานความผิดใหม่ไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 อีกทั้งควรกำหนดเพิ่มโทษให้ผู้กระทำความผิดได้รับโทษที่หนักขึ้นด้วย ไม่ควรกำหนดโทษความผิดฐานโปรแกรมเรียกค่าไถ่เป็นเพียงความผิดลหุโทษ และหามาตรการทางกฎหมายเพื่อให้สอดคล้องกับอาชญากรรมในยุคปัจจุบันให้มีความทันสมัยมากยิ่งขึ้น

คำสำคัญ: โปรแกรมเรียกค่าไถ่ มัลแวร์ ความรับผิดทางอาญา

Abstract

This thesis aims at studying meaning, form and impact of ransoming computer data under Thai laws and foreign laws in relation to infringement of other people's rights by use of Ransomware program. In taking into account of Thai laws in relation to ransoming computer data, this kind of act is actually perceived as a deprivation of personal rights and liberty, an impact on damaged person's state of mind and a cause of damage to state agencies and national security by leading to occurrence of other severe perils and crimes. Whereas existing Thai laws are still lack of provisions to be applicable to this act of ransoming computer data, the related government agency would rather revise the laws under the fact that, in some circumstances, none of element or provisions of law can be applicable to take legal action against the offenders.

The researcher has certain suggestions to provide an offense and direct criminal liability in use of ransomware program to ransom computer data by adding such new offense in the Computer-related Crime Act B.E. 2550 (2007) as amended by the Computer-related Crime Act (No. 2) B.E. 2560 (2017).In addition, the culprit of this kind of offense deserves harsher penalty. Such offending use of ransomware program should not be merely misdemeanor and any up-to-date legal measure should be sought to be conformity with current developed nature of crime.

Keywords: Ransomware, Malware and Criminal Liability

1. บทนำ

สังคมปัจจุบันมีความรวดเร็วในการเผยแพร่ข้อมูลข่าวสาร เป็นยุคของสังคมและเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่มีการพัฒนาอย่างรวดเร็วเพราะมีการนำสารสนเทศทางด้านคอมพิวเตอร์เข้ามาใช้ในระบบที่รู้จักกันดีคืออินเทอร์เน็ต (Internet) ทำให้สามารถจัดเก็บ ประมวลผลข้อมูลได้แม่นยำและรวดเร็ว ด้วยประสิทธิภาพดังกล่าวทำให้ประชาชน หน่วยงาน องค์กร สถาบันการเงิน หันมาใช้คอมพิวเตอร์เป็นจำนวนมาก ในปัจจุบันรัฐบาลของประเทศไทยก็ได้ประกาศนโยบายประเทศไทย 4.0 ผลักดันให้ไอทีเข้ามาเป็นโครงสร้างพื้นฐานของประเทศ การพัฒนาไอทีจึงเป็นสิ่งจำเป็นเพื่อที่จะให้ประชาชนมีคุณภาพชีวิตที่ดีขึ้น แต่อีกมุมมองหนึ่งอาจกล่าวว่าการพัฒนาเป็นสิ่งที่ไม่จำเป็น เพราะคุณภาพชีวิตอย่างสมัยโบราณเป็นคุณภาพชีวิตที่ดีกว่าคุณภาพชีวิตสมัยปัจจุบัน แต่ถ้าหากสนใจจะพัฒนาก็จะต้องใช้ไอทีอย่างหนีไม่พ้น (ศรีศักดิ์ จามรมาน, 2549: 1)

การใช้สารสนเทศที่ถูกต้องย่อมมีผลดีกับคุณภาพชีวิตของประชาชน แต่ในอีกด้านกลับถูกใช้เป็นเครื่องมือในการกระทำความผิดจนกลายเป็นอาชญากรรมคอมพิวเตอร์ (Computer Crime) ซึ่งเป็นรูปแบบหนึ่งในกลุ่มของอาชญากรรมทางเศรษฐกิจ (Economic Crimes) หรือที่รู้จักกันในชื่อ “White Collar Crimes” หรืออาชญากรรมเสื้อคอปก ความผิดสำคัญๆ ของอาชญากรรมประเภทนี้ ได้แก่ การเข้าไปในระบบโดยปราศจากอำนาจ (Computer Hacking) การกระทำความผิดโดยเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ (Computer Manipulation) การก่อวินาศกรรมคอมพิวเตอร์ (Computer Sabotage) การละเมิดลิขสิทธิ์ซอร์ฟแวร์ และการข่มขู่กรรโชกรีดไถ (Ransom) ทางคอมพิวเตอร์ เป็นต้น (สาวตรี สุขศรี, 2552: 193 - 194) อาชญากรรมประเภทนี้มีการพัฒนารูปแบบที่ซับซ้อนมากขึ้นเรื่อย ๆ จนกลายเป็นปัญหาของนานาประเทศ ส่งผลกระทบต่อระบบเศรษฐกิจโดยรวม โดยเฉพาะอย่างยิ่งในกลุ่มธุรกิจการเงิน นอกจากนี้ยังรวมถึงการกระทำความผิดในด้านอื่น ๆ ที่กฎหมายคุ้มครอง เช่น สร้างความเสียหายต่อสาธารณะ ความมั่นคง รวมทั้งการพัฒนาทางสังคมของประเทศ

ปัจจุบันมีการระบาดอย่างแพร่หลายของโปรแกรมคอมพิวเตอร์ในลักษณะของ การกรรโชกข้อมูลทางคอมพิวเตอร์จากโปรแกรมมัลแวร์ CryptoLocker, WannaCry และ BadRabbit ซึ่งได้สร้างมูลค่าในสกุลเงินดิจิทัล (บิตคอยน์: Bitcoin) ให้กลุ่มอาชญากรอย่างมหาศาล แต่ก็สร้างความหายนะแก่สังคมและเศรษฐกิจเป็นอย่างมากเช่นกัน จากสถิติการโจมตีของโปรแกรมเรียกค่าไถ่ กลุ่มเป้าหมายได้แก่ โรงพยาบาล คลินิก ที่มีสุขภาพและชีวิตของมนุษย์เป็นสิ่งต่อรอง องค์กรที่ใช้คอมพิวเตอร์เป็นกิจวัตรประจำก็เป็นกลุ่มเสี่ยง เช่น ธุรกิจส่งออก สถาบันการศึกษา ตลาดหลักทรัพย์และการธนาคาร เป็นต้น ทั่วโลกเรียกชื่อมัลแวร์นี้ว่า “Ransomware” หรือ “โปรแกรมเรียกค่าไถ่”

โปรแกรมเรียกค่าไถ่สามารถทำเงินให้กลุ่มอาชญากรที่เห็นผลโดยชัดเจน รูปแบบวิธีการก็มีการพัฒนาไปพร้อมกับวิวัฒนาการเทคโนโลยีคอมพิวเตอร์และอินเตอร์เน็ต แต่การพัฒนากฎหมายกลับไล่ตามรูปแบบอาชญากรรมนั้นได้อย่างล่าช้า กฎหมายเดิมที่มีอยู่ก็มีช่องว่างไม่อาจใช้บังคับได้ครอบคลุม จึงกลายเป็นปัญหาที่หลายประเทศต้องให้ความสำคัญปรับปรุงกฎหมายของตนให้สอดคล้องกับการกำหนดฐานความผิดแบบใหม่ ๆ ซึ่งในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 ก็เช่นกัน เดิมกฎหมายได้กำหนดความรับผิดเฉพาะในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์เท่านั้น แต่ยังมีการกระทำความผิดต่าง ๆ ตามมา เช่น การเปลี่ยนแปลง การทำลาย หรือแม้แต่การจับข้อมูลเป็นตัวประกัน ซึ่งยังไม่มีนิยามและการกำหนดฐานความผิดที่ครอบคลุม ดังนั้นควรจะต้องมีการกำหนดกฎเกณฑ์ให้เหมาะสมในปัญหาดังกล่าว

2. วัตถุประสงค์การวิจัย

งานวิจัยนี้มุ่งเน้นที่จะศึกษาแนวความคิดหลักการ และทฤษฎีของกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์เกี่ยวกับโปรแกรมเรียกค่าไถ่ตามกฎหมายประเทศไทยกับมาตรฐานสากลของต่างประเทศ อีกทั้งยังศึกษาสภาพปัญหาเกี่ยวกับการกระทำที่เป็นโปรแกรมเรียกค่าไถ่ข้อมูลทางคอมพิวเตอร์ เพื่อกำหนดความรับผิดทางอาญาเกี่ยวกับโปรแกรมเรียกค่าไถ่ในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ให้เหมาะสมกับประเทศไทย

3. วัสดุอุปกรณ์และวิธีดำเนินการวิจัย

การศึกษานี้ใช้ระเบียบวิจัยเชิงคุณภาพ โดยการวิจัยเอกสารเป็นหลัก (Documentary Research) และ

วิเคราะห์ข้อมูลจากหนังสือ บทความ เอกสาร วารสาร กฎหมายที่เกี่ยวกับความรับผิดทางอาญาที่เกิดจากโปรแกรมเรียกค่าไถ่ ตามกฎหมายว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ ตลอดจนข้อมูลทางกฎหมายจากเว็บไซต์อินเตอร์เน็ตที่เกี่ยวกับบทบัญญัติทางกฎหมายต่าง ๆ รวมถึงคำอธิบาย บทความ หรือข้อคิดเห็นต่างๆ โดยศึกษาเปรียบเทียบระหว่างหลักกฎหมายของต่างประเทศกับหลักกฎหมายของประเทศไทย

4. ผลการวิจัย

4.1 ปัญหาทางกฎหมายเกี่ยวกับโปรแกรมเรียกค่าไถ่ ในกฎหมายว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ หลักการกระทำความผิดทางคอมพิวเตอร์หรืออาชญากรรมคอมพิวเตอร์อาจถูกแบ่งออกเป็น 2 ประเภทคือ อาชญากรรมที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการก่ออาชญากรรม และอาชญากรรมที่มีข้อมูลหรือระบบคอมพิวเตอร์เป็นเป้าหมายของผู้กระทำความผิด ในยุคแรกอาจหมายความถึงการกระทำที่ส่งผลกระทบต่อความเป็นส่วนตัว (Privacy) และก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยในสังคม ซึ่งไม่เกี่ยวข้องกับเศรษฐกิจเลย แต่นับจากช่วงปี ค.ศ. 1970 เป็นต้นมา อาชญากรรมคอมพิวเตอร์ได้เป็นส่วนหนึ่งของอาชญากรรมเศรษฐกิจ สิ่งที่กฎหมายต้องการจะให้ความคุ้มครองก็ถูกขยายจากข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัว เพื่อไปคุ้มครองป้องกันเศรษฐกิจและความมั่นคงของประเทศ และต่อมาได้เกิดหลักการกระทำความผิดทางคอมพิวเตอร์ในรูปแบบอื่น ๆ อีกหลายอย่างตามมา ได้แก่

1) การแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ (Computer Manipulation)

2) การเจาะระบบและการเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access) ซึ่งมีรูปแบบการเจาะระบบคอมพิวเตอร์ (Computer Hacking) และมีอีกรูปแบบหนึ่งที่ทุกคนควรให้ความสนใจคือ “สงครามไซเบอร์ (Cyber War)” ซึ่งเป็นอาชญากรรมคอมพิวเตอร์ด้านความมั่นคงของชาติ เพื่อการโจรกรรมทางไซเบอร์ การเจาะเข้าระบบทำลายเว็บไซต์ การโฆษณาชวนเชื่อทางอินเทอร์เน็ต การรวบรวมและการล้วงความลับข้อมูล การรบกวนเครื่องมือและอุปกรณ์ การโจมตีโครงสร้างระบบคอมพิวเตอร์และเครือข่ายพื้นฐานที่สำคัญ เป็นต้น

3) การขโมย คัดลอก และการใช้ซอร์ฟแวร์โดยมิได้รับอนุญาต ซึ่งการกระทำความผิดรูปแบบนี้ในช่วงแรกส่วนใหญ่มุ่งที่ซอร์ฟแวร์ส่วนบุคคล เนื่องจากมีเอกชนไม่กี่รายที่มีงบประมาณในการลงทุนเรื่องโปรแกรมคอมพิวเตอร์ต่างๆ ซึ่งโปรแกรมสำหรับเครื่องคอมพิวเตอร์จะต้องสั่งซื้อจากเจ้าของลิขสิทธิ์เท่านั้น แต่ต่อมาเมื่อมีผู้ใช้คอมพิวเตอร์มากขึ้นความต้องการโปรแกรมพื้นฐานก็มีมากขึ้นด้วย โปรแกรมจึงกลายเป็นเป้าหมายของผู้กระทำความผิด เพราะโปรแกรมที่มีลิขสิทธิ์ส่วนใหญ่จะมีราคาแพง อาชญากรที่มีอุปกรณ์เครื่องมือจึงมีการคัดลอกโปรแกรมเหล่านั้น

4) การก่อวินาศกรรมทางอินเตอร์เน็ต (Computer Sabotage) และการข่มขู่ทางอินเทอร์เน็ต (Computer Expressing) ซึ่งส่วนใหญ่มักมีเป้าหมายที่เป็นการกระทำต่อคอมพิวเตอร์ส่วนบุคคล โดยการปล่อยไวรัส (Virus) มัลแวร์ (Malware) หรือหนอนคอมพิวเตอร์ (Worm) ให้ไปทำลายระบบหรือข้อมูลคอมพิวเตอร์ที่ต้องการเท่านั้น นอกจากนี้การก่อวินาศกรรมคอมพิวเตอร์ ยังนำมาซึ่งความผิดอีกรูปแบบหนึ่งคือ การข่มขู่ทางอินเตอร์เน็ต (Computer Expressing) ที่เกิดขึ้นในรูปแบบเดียวกัน มีลักษณะของการข่มขู่ กรรโชก หรือรีดไถ (Ransom) โดยผู้เสียหายจะถูกข่มขู่ผ่านทางจดหมายอิเล็กทรอนิกส์ ให้ต้องยินยอมกระทำการอย่างหนึ่งอย่างใด มิเช่นนั้นระบบคอมพิวเตอร์จะถูกบล็อกหรือทำให้ใช้งานไม่ได้ จากนั้นจึงข่มขู่ให้เหยื่อจ่ายเงินเพื่อแลกกับการถอดรหัสดังกล่าว ซึ่งในการศึกษานี้จะมุ่งศึกษากรณีดังกล่าว ที่ผ่านมาได้มีผู้ใช้งานคอมพิวเตอร์ของหน่วยงานภาครัฐ ภาคเอกชนหรือองค์กรต่างๆ ถูกโจมตีด้วยโปรแกรมเรียกค่าไถ่ (Ransomware) ตัวอย่างเช่น ข่าวการแพร่กระจายไวรัส Ransomware mssecsvc.exe ภายในมหาวิทยาลัยราชภัฏรำไพพรรณี เมื่อวันที่ 19 พฤศจิกายน 2560 โดยหน่วยงานที่พบการแพร่โปรแกรมคือ หน่วยงานธุรการ หน่วยงานการเงิน หน่วยงานการเจ้าหน้าที่และนิติกร หน่วยงานอาคารสถานที่และบริการ ฯลฯ (ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏรำไพพรรณี, 2561) ซึ่งในต่างประเทศมีผู้เสียหายหลายรายที่ต้องยินยอมจ่ายค่าไถ่ ซึ่งอาจจะเป็นเงินหรือทรัพย์สินอื่น ๆ เพื่อแลกกับข้อมูลสำคัญของตนที่โดนเข้ารหัสไว้ ปัจจุบันยังไม่สามารถที่จะจับกุมได้หรือจับได้เพียงไม่กี่ราย โดยมีสถิติจาก Solutionary ซึ่งเป็นบริษัทด้านความปลอดภัยในเครือ NTT Group รายงานการโจมตีของ Ransomware ที่ตรวจพบในช่วงกลางปี พ.ศ.2559 พบว่าหน่วยงานด้านสาธารณสุขเป็นหน่วยงานที่ถูกโจมตี

มากที่สุดถึง 88% รองลงมาคือหน่วยงานด้านการศึกษา 6% และหน่วยงานด้านการเงิน 4% (Help Net Security,2559) นับว่าเป็นปัญหาภัยคุกคามบนโลกยุคเทคโนโลยีสารสนเทศที่สร้างความเสียหายอย่างร้ายแรง อีกทั้งยังไม่พบวิธีการกู้คืนไฟล์จากการถูกโจมตีด้วยวิธีการนี้

การโจมตีด้วยโปรแกรมเรียกค่าไถ่ส่วนใหญ่จะมาทางอีเมล์หลอกลวงที่แนบไฟล์ Ransomware ไว้ โดยเนื้อหาในอีเมล์จะดึงดูดให้ผู้อ่านอยากคลิกเข้าไปอ่าน ตัวอย่างเช่น อีเมล์แจ้งเลขที่ใบสั่งซื้อสินค้า (Order ID) หากผู้ใช้ไม่เปิดไฟล์ที่แนบมาก็อาจจะทำให้สูญเสียโอกาสทางการค้าได้ หรือในองค์กรทางการแพทย์มีการ Copy Icon หลอกว่าเป็นข้อมูลของคนไข้ แต่ถ้าผู้ใช้คลิกเปิดไฟล์โดยไม่ระมัดระวัง ก็จะตกเป็นเหยื่อของ Ransomware ทันที

การโจมตีสถาบันการศึกษาที่เคยพบจะใช้วิธี “Social Engineering” เป็นการหลอกผู้ใช้งานให้ดาวน์โหลดโปรแกรมมาติดตั้งในเครื่อง เช่น ในขณะที่ใช้งานระบบลงทะเบียนเรียนออนไลน์ของมหาวิทยาลัย พบว่ามี Pop-Up ขึ้นมาบอกว่า ให้ดาวน์โหลดโปรแกรมเสริมมาติดตั้งเพื่อให้สามารถลงทะเบียนได้สะดวก และรวดเร็วขึ้น ทั้งๆ ที่โปรแกรมนี้ไม่มีอยู่จริง หากผู้ใช้งานหลงเชื่อและทำการดาวน์โหลดมาติดตั้ง ไฟล์ต่างๆ ก็จะโดนจับเป็นตัวประกันทันที หรือมีไฟล์แนบที่มากับอีเมล์จะเป็น zip file หากแตกไฟล์ออกมาก็จะพบไฟล์นามสกุล .doc, .xls, .ppt หรือไฟล์อื่นๆ ที่เราคุ้นเคย แต่ถ้าสังเกตดีๆ จะพบว่านามสกุลของไฟล์จริงๆ แล้วเป็น .exe เรียกเทคนิคการตั้งชื่อไฟล์แบบนี้ว่า “Double Extensions”

Ransomware นั้นเป็นที่รู้จักกันมานานหลายปีแล้ว และได้สร้างปัญหาและความเสียหายไปหลายประเทศทั่วโลก จากการศึกษากฎหมายในประเทศไทยมีเพียงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ.2560 เท่านั้นที่จะถูกนำมาใช้แก้ปัญหา แต่ผู้วิจัยเห็นว่าไม่เพียงพอที่จะสามารถแก้ไขปัญหาการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่ทางคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ โดยการศึกษาพบว่ามีปัญหาการกระทำความผิดของโปรแกรมเรียกค่าไถ่ตามกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ดังต่อไปนี้

4.1.1 การไม่มีกฎหมายบัญญัติในเรื่องการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่ทางคอมพิวเตอร์

ประเด็นแรกที่จะต้องพิจารณาคือ กฎหมายที่ใช้ควบคุมปัญหาการกระทำผิดเกี่ยวกับโปรแกรมค่าไถ่คอมพิวเตอร์นั้นมีบัญญัติไว้เพื่อการบังคับใช้หรือไม่ ซึ่งในประเทศไทยก่อนที่จะมีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ไม่สามารถที่จะนำตัวผู้กระทำมาลงโทษได้ เนื่องจากมีปัญหาว่ากฎหมายไม่ได้บัญญัติว่าข้อมูลในคอมพิวเตอร์ เป็น “ทรัพย์” และกฎหมายอาญาที่มีอยู่ในขณะนั้นก็ไม่สามารถนำมาปรับใช้กับเรื่องดังกล่าวได้ เนื่องจากไม่อาจกล่าวว่าการเข้าถึงข้อมูลของผู้อื่นโดยมิชอบแล้วกระทำการอย่างอื่นต่อไปจะเป็นความผิดเกี่ยวกับทรัพย์ได้ ดังนั้นการล็อคข้อมูลและการข่มขู่กรรโชกเพื่อความต้องการอย่างหนึ่งอย่างใดเกี่ยวกับข้อมูลคอมพิวเตอร์อาจไม่ถือว่าเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่อย่างใด จึงต้องอาศัยการเทียบเคียงกฎหมายใกล้เคียงเกี่ยวกับการกระทำความผิดในการเรียกค่าไถ่ทางคอมพิวเตอร์ ได้แก่ ประมวลกฎหมายอาญา และประมวลกฎหมายวิธีพิจารณาความอาญา พิจารณาความหมายคำนิยาม ค่าไถ่ (Ransom) หมายความว่า ทรัพย์สินหรือประโยชน์ที่เรียกเอา หรือให้เพื่อแลกเปลี่ยนเสรีภาพของผู้ถูกเอาตัวไป ผู้ถูกหน่วงเหนี่ยว หรือผู้ถูกกักขัง (พจนานุกรมฉบับราชบัณฑิตยสถาน, 2554) ส่วนในทางกฎหมายอาญาโดยทั่วไป คำว่า “ค่าไถ่” พบว่ามีบัญญัติไว้ดังนี้

มาตรา 1 (13) “ค่าไถ่” หมายความว่า ทรัพย์สินหรือประโยชน์ที่เรียกเอา หรือให้เพื่อแลกเปลี่ยนเสรีภาพของผู้ถูกเอาตัวไป ผู้ถูกหน่วงเหนี่ยว หรือผู้ถูกกักขัง

เมื่อวิเคราะห์จากนิยาม“ทรัพย์สิน หรือประโยชน์ที่เรียกเอา” คำว่า “ประโยชน์” จะเป็นประโยชน์อะไรก็ได้ไม่จำเป็นว่าจะต้องต้องเป็นประโยชน์ในลักษณะที่เป็นทรัพย์สิน และ “ที่เรียกเอาหรือให้เพื่อแลกเปลี่ยนเสรีภาพ” จะต้องมีเจตนาพิเศษ เพื่อแลกเปลี่ยนเสรีภาพด้วย จึงจะถือว่าเป็นค่าไถ่

มาตรา 314 ผู้ใดเพื่อให้ได้มาซึ่งค่าไถ่

(1) เอาตัวเด็กอายุไม่เกินสิบห้าปีไป

(2) เอาตัวบุคคลอายุกว่าสิบห้าปีไป โดยใช้อุบายหลอกลวง ข่มเข็ญ ใช้กำลังประทุษร้าย ใช้อำนาจครอบงำผิดคลองธรรมหรือใช้วิธีข่มขืนใจด้วยประการอื่นใด หรือ

(3) หน่วงเหนี่ยวหรือกักขังบุคคลใด...
จากบทบัญญัติตามมาตรา 313 จะเห็นว่า การกระทำมี 3 กรณีคือ

1) เอาตัวเด็กอายุไม่เกิน 15 ปีไป ซึ่งกรณีนี้จะต้องเป็นกรณีที่เด็กอายุไม่เกิน 15 ปี เท่านั้น และไม่ว่าเด็กจะสมัครใจไปด้วยหรือไม่ก็ตาม ก็เป็นความผิดตามอนุมาตรานี้

2) เอาตัวบุคคลอายุกว่า 15 ปีไป โดยใช้อุบายหลอกลวง ขู่เข็ญใช้กำลังประทุษร้าย ใช้อำนาจครอบงำ ผิดคลองธรรมหรือใช้วิธีข่มขืนใจด้วยประการอื่นใด สรุปได้ว่าผู้ที่ถูกเอาตัวไปจะต้องมีอายุเกิน 15 ปี และต้องไม่สมัครใจไปด้วย

3) หน่วงเหนี่ยวหรือกักขังบุคคลใด (ตามมาตรา 310) เป็นกรณีที่ผู้ถูกระทำไม่ได้สมัครใจไปด้วย ซึ่งผู้ถูกกระทำตาม (3) นี้จะเป็นเด็ก หรือเป็นบุคคลมีอายุเกินกว่า 15 ปีก็ได้ และอาจจะไม่มีการเอาตัวไป คงมีแต่การหน่วงเหนี่ยวหรือกักขังก็ได้

โดยการกระทำทั้ง 3 กรณีนั้นมีเจตนาพิเศษคือ “เพื่อให้ได้มาซึ่งค่าไถ่” ดังนั้นค่าไถ่ในกรณีทั่วไปตามประมวลกฎหมายอาญาทั้งมาตรา 1 และมาตรา 313 จึงเป็นการกระทำกับตัวบุคคลเท่านั้น กฎหมายยังให้ความคุ้มครองไม่ครอบคลุมถึงทรัพย์อย่างอื่น

มาตรา 337 ความผิดฐานกรรโชกซึ่งองค์ประกอบความผิดตามมาตรานี้ คือ

1) ผู้กระทำผิดต้องต้องข่มขืนใจให้ยอมให้หรือยอมจะให้ ขู่จะทำร้ายในเวลานั้น หรืออาจขู่ว่าจะทำร้ายในอนาคตก็ได้ ต้องใช้กำลังประทุษร้ายหรือขู่เข็ญว่าจะทำอันตรายต่อร่างกาย

2) ผู้กระทำผิดอาจทำอันตรายต่อร่างกาย เสรีภาพ ชื่อเสียง หรือทรัพย์สินของผู้ถูกขู่เข็ญหรือของบุคคลที่สาม

3) ผู้กระทำผิดมุ่งต่อทรัพย์คือวัตถุมีรูปร่างรวมถึงประโยชน์ในลักษณะที่เป็นทรัพย์สินด้วย

แต่ในกรณีของการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่นั้น ผู้กระทำความผิดไม่จำเป็นต้องข่มขืนใจให้เหยื่อยินยอม หรือใช้กำลังทางร่างกายข่มขู่จะทำอันตรายแก่ผู้เสียหายแต่อย่างใด กล่าวคือผู้กระทำความผิดเพียงแค่ใช้คำสั่งโปรแกรมแจ้งข้อความข่มขู่ไปยังผู้เสียหาย เมื่อผู้เสียหายเห็นข้อความจะยอมทำตามหรือไม่นั้นก็ไม่อาจรู้ แต่หากผู้เสียหายไม่ทำตามก็จะได้รับคำสั่งให้ทำลายข้อมูลในเครื่องคอมพิวเตอร์ทันที และองค์ประกอบที่ผู้กระทำความผิดมีจุดประสงค์ต่อทรัพย์ที่มีรูปร่างซึ่งก็คือเงินหรือทรัพย์สินอื่นใด แต่เงินในรูปแบบที่ถูกเรียกเอาจะเป็นสกุลเงินดิจิทัล เช่น Bitcion ซึ่งไม่ใช่สกุลเงินสากลที่มีใช้ในปัจจุบัน แต่เป็นสกุลเงินสมมติในโลกอินเทอร์เน็ต และใช้กันอย่างแพร่หลายในธุรกิจมืดที่เป็นปัญหาอีกประเด็นหนึ่ง ดังนั้นการเทียบเคียงประมวลกฎหมายอาญา ในฐานความผิดกรรโชกทรัพย์ตามมาตรา 337 จึงใช้ในกรณีการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่ไม่ได้ อีกทั้งผู้กระทำความผิดบางรายอาจเรียกเอาทรัพย์สินหรือเงินอย่างใดอย่างหนึ่ง แต่ในประเด็นข้อมูลทางคอมพิวเตอร์ถือเป็นทรัพย์หรือไม่นั้น ตามแนวคำพิพากษาศาลฎีกาที่ 5161/2547 กรณีการขโมยข้อมูลคอมพิวเตอร์ ก็ไม่ถือเป็นความผิดฐานลักทรัพย์แต่อย่างใด

การที่ประเทศไทยไม่มีกฎหมายที่เหมาะสม ในเรื่องการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่ทางคอมพิวเตอร์นั้น จึงเกิดเป็นปัญหาว่าความก้าวหน้าของเทคโนโลยีในปัจจุบันที่ทำให้ข้อมูลต่างๆ จากที่มีรูปร่างจับต้องได้ เช่น กระดาษ โมเดล เป็นต้น ได้แปรเปลี่ยนเป็นข้อมูลแบบดิจิทัล เป็นพลังงานรูปแบบอื่น ซึ่งไม่มีรูปร่างและสัมผัสไม่ได้ด้วยกายมนุษย์ธรรมดาทั่วไป ต้องใช้เครื่องมือที่เป็นเทคโนโลยีจึงจะช่วยให้สัมผัสได้ และมูลค่าของข้อมูลก็แตกต่างกันไป เมื่อเกิดปัญหาว่าข้อมูลในคอมพิวเตอร์ถือเป็นทรัพย์หรือไม่ ใครคือผู้ปกป้องข้อมูลเหล่านั้น และสกุลเงินดิจิทัลที่เรียกเอาเป็นค่าไถ่จะถือว่าเป็นทรัพย์ด้วยหรือไม่ เมื่อเกิดการกระทำละเมิดจะดำเนินการกับใคร ผู้วิจัยจึงมีความเห็นว่าประเทศไทยจำเป็นต้องมีการบัญญัติกฎหมายมารองรับการกระทำความผิดดังกล่าวขึ้นมาโดยเฉพาะ เพื่อเป็นการอุดช่องว่างของกฎหมายและป้องกันผู้กระทำความผิดอาศัยใช้ช่องว่างของกฎหมายมากระทำความผิด

ในส่วนของกฎหมายสากลทางกลุ่มสหภาพยุโรป (European Union: EU) ได้มีการจัดตั้งกรรมาธิการผู้เชี่ยวชาญด้านอาชญากรรมทางคอมพิวเตอร์ขึ้นตั้งแต่ปี ค.ศ. 1985 เพื่อกำหนดแนวทางในการบัญญัติกฎหมายให้ครอบคลุมถึงลักษณะการกระทำที่สมควรบัญญัติเป็นความผิด ซึ่งมีอย่างน้อย 8 ฐานความผิด ได้แก่ การปลอมแปลงทางคอมพิวเตอร์ การฉ้อโกงทางคอมพิวเตอร์การเข้าถึงโดยมิชอบ การดักข้อมูลการทำลายข้อมูลคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ การรบกวนการทำงานของคอมพิวเตอร์หรือระบบคมนาคม และการทำซ้ำลายพิมพ์วงจรโดยมิชอบ และยังมีความผิดอื่นที่กำหนดให้เป็นทางเลือกที่จะ

บัญญัติเป็นกฎหมายภายใน 4 ฐานความผิด ได้แก่ การเปลี่ยนแปลงข้อมูลหรือโปรแกรมคอมพิวเตอร์ การจารกรรมทางคอมพิวเตอร์ การใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยมิชอบ และการใช้โปรแกรมคอมพิวเตอร์ที่ได้รับการคุ้มครองโดยมิชอบ เป็นต้นต่อมาสภายุโรป (Council of Europe) ได้จัดทำอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime ETS No. 185) โดยมีวัตถุประสงค์ที่สำคัญ 3 ประการ คือ

1) เพื่อให้กฎหมายสารบัญญัติภายในประเทศต่างๆ ที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มีความสอดคล้องและเป็นไปในทิศทางเดียวกัน

2) เพื่อให้กฎหมายวิธีพิจารณาความอาญาตามกฎหมายภายในให้อำนาจที่จำเป็นเพื่อการสืบสวนสอบสวนและฟ้องร้องการกระทำความผิดที่ได้กระทำโดยระบบคอมพิวเตอร์ ตลอดจนการรวบรวมพยานหลักฐานที่อยู่รูปข้อมูลอิเล็กทรอนิกส์

3) เพื่อเร่งให้เกิดความร่วมมือระหว่างประเทศที่รวดเร็วและบรรลุเป้าหมายของอนุสัญญา

สำหรับมาตรการทางกฎหมายนั้น คณะกรรมาธิการยุโรปได้นำเสนอโครงร่างที่ว่าด้วย Council Framework Decision on Attacks Against Information Systems เมื่อปี พ.ศ. 2545 โดยมีวัตถุประสงค์เพื่อนำเสนอการก่ออาชญากรรมทางคอมพิวเตอร์รูปแบบใหม่ๆ และข้อเสนอในการบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์ภายในกลุ่มประเทศสมาชิกเพื่อให้มีความสอดคล้องกัน โดยเนื้อหาในส่วนของโครงร่างดังกล่าวนี้มาจากการศึกษาเปรียบเทียบ Convention on Cybercrime ของสภายุโรป เช่น การกำหนดความผิดฐานการเข้าถึงระบบสารสนเทศโดยมิชอบ (Illegal access to Information Systems) ความผิดฐานรบกวนระบบสารสนเทศโดยมิชอบ (Illegal interference with Information Systems) ที่ประเทศสมาชิกจะต้องปฏิบัติให้เป็นไปตามข้อเสนอ

จากการศึกษาบทบัญญัติกฎหมายที่เกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์เกี่ยวกับโปรแกรมเรียกค่าไถ่ในต่างประเทศนั้น พบว่ามี 2 รูปแบบ ได้แก่

ก. การบัญญัติในลักษณะแก้ไขเพิ่มเติมในประมวลกฎหมายอาญา เช่น

1) สหพันธ์สาธารณรัฐเยอรมนี โดยฝ่ายนิติบัญญัติเห็นว่าการกระทำความผิดที่แม้จะเกิดขึ้นบนอินเทอร์เน็ตหรือที่เกี่ยวข้องกับคอมพิวเตอร์ เช่น ความผิดเกี่ยวกับการหมิ่นประมาท การทำให้เสียหายต่อสิทธิ หรือความลับส่วนบุคคล ความผิดเหล่านี้ก็ยังสามารถใช้กฎหมายอาญาทั่วไปมาปรับใช้กับข้อเท็จจริงเพื่อลงโทษได้ ทั้งนี้เพราะความผิดเหล่านั้นยังมีองค์ประกอบความผิดเช่นเดียวกับการกระทำความผิดดั้งเดิมอยู่ เพียงแต่มีการเปลี่ยนแปลงองค์ประกอบความผิดไปบางส่วนเท่านั้น

2) ประมวลกฎหมายอาญาของมลรัฐแคลิฟอร์เนีย (California Penal Code) มีวัตถุประสงค์เพื่อบัญญัติประมวลกฎหมายอาญาความผิดเกี่ยวกับคอมพิวเตอร์และการฉ้อโกง โดยมาตรา 502 ให้ความคุ้มครองบุคคล ธุรกิจ และหน่วยงานราชการจากการปลอมแปลง การรบกวน การทำลาย และการเข้าถึงจากการสร้างข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ อีกทั้งยังสามารถนำบทบัญญัติในคดีแพ่งข้อหาละเมิดและบทบัญญัติทางอาญาเพื่อชดเชยความเสียหายตามรัฐบัญญัติมลรัฐแคลิฟอร์เนียการเข้าถึงข้อมูลและการกระทำการทุจริตทางคอมพิวเตอร์ และได้กำหนดถึงการกระทำที่เป็นการรบกวน การทำลาย ทำให้เสียหาย รวมถึงการใช้ชุดข้อมูลเรียกค่าไถ่ไว้โดยชัดเจนในมาตรา 502 (C)

ข. การบัญญัติเป็นกฎหมายเฉพาะ เช่น

1) สาธารณรัฐสิงคโปร์ มีรัฐบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ.1990 (Computer Misuse Act 1990) ซึ่งคัดลอกมาจากอังกฤษ บทบัญญัติที่เกี่ยวข้องกับโปรแกรมเรียกค่าไถ่ มี 2 กรณีคือ ความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจเพื่อจะกระทำหรืออำนวยความสะดวกในการกระทำความผิดอื่น กับความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์

2) สหพันธรัฐมาเลเซีย ถือเป็นประเทศแรกๆในทวีปเอเชียตะวันออกเฉียงใต้ที่มีพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ ค.ศ. 1997 (Computer Crime Act 1997) ใช้บังคับ กฎหมายฉบับนี้กำหนดเฉพาะฐานความผิดที่ว่าด้วยอาชญากรรมคอมพิวเตอร์โดยแท้ หรือความผิดที่อาชญากรอาศัยความรู้ความสามารถด้านเทคโนโลยีคอมพิวเตอร์กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ การออกกฎหมายดังกล่าวมีวัตถุประสงค์เพื่อกำหนดฐานความผิดและบทลงโทษเกี่ยวกับการใช้คอมพิวเตอร์ไปในทางที่ผิด ทั้งนี้ได้ครอบคลุมไปถึงเรื่องการเข้าถึงทรัพยากรคอมพิวเตอร์โดยไม่ได้

รับอนุญาต การเข้าถึงโดยไม่ได้รับอนุญาตโดยมีเจตนาเพื่อการโจมตี และการแก้ไขดัดแปลงข้อมูลในคอมพิวเตอร์โดยไม่ได้รับอนุญาต

สำหรับประเทศไทยใช้การบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์ในรูปแบบที่สอง คือ บัญญัติเป็นกฎหมายเฉพาะโดยมีชื่อว่า พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 จะเห็นได้ว่าแม้รูปแบบการบัญญัติกฎหมายของแต่ละประเทศจะแตกต่างกัน แต่หลักการกำหนดฐานความผิดนั้นมักจะคล้ายคลึงกัน ทั้งนี้ในต่างประเทศก็คำนึงถึงลักษณะของการใช้คอมพิวเตอร์ในการกระทำความผิดเป็นสำคัญ กฎหมายที่ออกมาใช้บังคับจึงมีลักษณะที่ใกล้เคียงกัน ภายหลังจากที่ใช้บังคับพระราชบัญญัติดังกล่าวในระยะเวลาหนึ่ง ปรากฏว่าหลายภาคส่วนเสนอให้มีการทบทวนหลักการของกฎหมาย อันเนื่องมาจากประเด็นปัญหาการบังคับใช้กฎหมายในทางปฏิบัติทั้งทางข้อเท็จจริงและข้อกฎหมาย สาเหตุเพราะผลจากพัฒนาการทางเทคโนโลยีสารสนเทศและรูปแบบการกระทำความผิดที่เปลี่ยนแปลงไปอย่างรวดเร็ว การบังคับใช้กฎหมายและการตีความที่คลาดเคลื่อนไปจากเจตนารมณ์ พนักงานเจ้าหน้าที่ไม่เพียงพอและขาดการประสานงานอย่างมีประสิทธิภาพ ความล่าช้าในการตรากฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ อาจมีสาเหตุจากระบบงานราชการที่ยุ่งยาก ซับซ้อน ต้องผ่านหลายหน่วยงาน หลายขั้นตอนจึงทำให้ขาดความต่อเนื่อง อีกทั้งการคัดลอกกฎหมายต่างประเทศมาโดยมิได้คำนึงถึงความแตกต่างทางภูมิประเทศ ศาสนา วัฒนธรรม และความเจริญก้าวหน้าทางเทคโนโลยีที่ไม่เท่ากันแล้วย่อมจะเกิดปัญหาเมื่อนำมาใช้อย่างแน่นอน รวมถึงการขาดหลักกฎหมายที่เอื้อต่อการประสานความร่วมมือระหว่างประเทศ อันส่งผลกระทบต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อีกทั้งยังกระทบต่อความเชื่อมั่นในการลงทุนประกอบการในประเทศไทย ซึ่งส่งผลกระทบต่อเศรษฐกิจโดยรวมของประเทศอีกด้วย การกำหนดความรับผิดที่เกี่ยวกับโปรแกรมเรียกค่าไถ่ ซึ่งฐานความรับผิดตามกฎหมายที่มีในปัจจุบันนั้นยังไม่ครอบคลุมกับองค์ประกอบความผิดที่อาชญากรได้กระทำไป หากพิจารณากฎหมายของต่างประเทศแล้ว ในประเทศที่มีการพัฒนากฎหมายอย่างต่อเนื่องอย่างสหรัฐอเมริกาได้บัญญัติความรับผิดที่เกี่ยวกับการเรียกค่าไถ่ข้อมูลทางคอมพิวเตอร์ไว้ใน Computer Fraud and Abuse Act มาตรา 1030 (A) (7) และมลรัฐแคลิฟอร์เนียยังได้แก้ไขใน California Penal Code มาตรา 502 (C) ให้มีความชัดเจนยิ่งขึ้น เพื่อประสิทธิภาพในการบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพสูงสุด

ผู้วิจัยเห็นว่าควรที่จะต้องทำการศึกษาตัวอย่างกฎหมายจากหลายๆ ประเทศที่บังคับใช้ไปก่อนแล้ว เพื่อนำมาปรับให้เข้ากับบริบทของประเทศไทย ซึ่งการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่ ถือว่าเป็นเรื่องใหม่ในสังคมไทยและในกระบวนการยุติธรรมของประเทศไทยด้วย ซึ่งในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 ก็ยังไม่มีบทบัญญัติที่บัญญัติว่าการกระทำความผิดดังกล่าวมีความผิด ซึ่งผู้วิจัยเห็นว่าควรที่จะมีการแก้ไขพระราชบัญญัติดังกล่าว โดยการแยกการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่ทางคอมพิวเตอร์ออกมาเป็นอีกหมวดหนึ่งโดยเฉพาะ และกำหนดบทลงโทษผู้กระทำความผิดไว้ด้วย เช่นเดียวกับรัฐบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ของสาธารณรัฐสิงคโปร์

4.1.2 การปฏิบัติงานตามอำนาจของพนักงานสอบสวนเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์จากปัญหาการไม่มีกฎหมายบัญญัติ ในเรื่องการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่ทางคอมพิวเตอร์นั้นส่งให้เกิดผลกระทบต่ออำนาจของพนักงานสอบสวน ในเรื่องอำนาจของพนักงานเจ้าหน้าที่และเขตอำนาจสอบสวนกรณีความผิดที่เกี่ยวพันกันหลายท้องที่ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 19 พนักงานสอบสวนในท้องที่หนึ่งท้องที่ใดที่เกี่ยวข้องจะมีอำนาจสอบสวน ดังนั้นเมื่อเป็นความผิดที่เกี่ยวพันกันหลายท้องที่แล้ว พนักงานที่มีอำนาจสอบสวนจึงมีด้วยกันหลายท้องที่ แต่พนักงานผู้รับผิดชอบสรุปสำนวนส่งพนักงานอัยการต้องมีเพียงท้องที่เดียวเท่านั้น กล่าวคือหากจับผู้ต้องหาได้พนักงานผู้รับผิดชอบสรุปสำนวน คือพนักงานท้องที่ที่จับได้ แต่หากจับผู้ต้องหายังไม่ได้พนักงานผู้รับผิดชอบสรุปสำนวนคือพนักงานสอบสวนท้องที่ที่พบการกระทำผิด หากพนักงานสอบสวนผู้รับผิดชอบไม่เป็นไปตามที่มาตรา 19 กำหนดจะทำให้เกิดผลเสียแก่คดีได้โดยถือว่าไม่ได้มีการสอบสวนคดีนั้นโดยชอบ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 120 มีผลทำให้พนักงานอัยการไม่มีอำนาจฟ้องศาลต้องยกฟ้อง

ในประเด็นปัญหาอำนาจเจ้าหน้าที่ในการสืบสวนการที่จะพิจารณาว่าพนักงานสอบสวนท้องที่ใดจะเป็นพนักงานสอบสวนผู้รับผิดชอบ จึงต้องพิจารณาว่า “ผู้ต้องหาถูกจับหรือยังไม่ถูกจับ” ก่อน แต่ส่วนใหญ่แล้วผู้วิจัยเห็นว่าภาระจะตกอยู่แก่พนักงานสอบสวนซึ่งท้องที่ที่พบการกระทำผิด เพราะว่าในความจริง หากเกิดการกระทำความผิดในเรื่องดังกล่าวแล้วส่วนมากจะจับกุมตัวผู้กระทำความผิดไม่ค่อยได้ เช่น ในกรณีความผิดเกิดนอกราชอาณาจักร ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 20 วางหลักไว้ว่า ถ้าความผิดซึ่งมีโทษตามกฎหมายไทยได้กระทำลงนอกราชอาณาจักรไทย ให้อัยการสูงสุดหรือผู้รักษาการแทนเป็นพนักงานสอบสวนผู้รับผิดชอบ หรือจะมอบหมายหน้าที่นั้นให้พนักงานอัยการหรือพนักงานสอบสวนคนใดเป็นผู้รับผิดชอบทำการสอบสวนแทนก็ได้ และในกรณีที่อัยการสูงสุดหรือผู้รักษาการแทนมอบหมายให้พนักงานสอบสวนคนใดเป็นผู้รับผิดชอบทำการสอบสวน อัยการสูงสุดหรือผู้รักษาการแทนจะมอบหมายให้พนักงานอัยการคนใดทำการสอบสวนร่วมกับพนักงานสอบสวนก็ได้

4.1.3 การรับฟังพยานหลักฐานเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์

อีกปัญหาหนึ่งที่ได้รับผลกระทบเช่นกัน คือ เรื่อง “พยานหลักฐานเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์” ซึ่งส่วนใหญ่เป็นสิ่งที่มองไม่เห็นจับต้องไม่ได้ (Intangible) และปรากฏอยู่เพียงชั่วเวลาใดเวลาหนึ่งเท่านั้น สาเหตุเพราะพยานหลักฐานในอาชญากรรมทางคอมพิวเตอร์เป็นเพียงคลื่นกระแสไฟฟ้าหรือข้อมูลทางคอมพิวเตอร์ และปัญหาอีกประการหนึ่งที่มากับพยานหลักฐานคือระยะเวลาที่ผู้กระทำผิดใช้ในการก่ออาชญากรรมมีระยะเวลาสั้นมาก ซึ่งนอกจากพยานหลักฐานทางกายภาพแล้ว การสืบสวนคดีต้องเสาะหาร่องรอยของข้อมูลดิจิทัลที่มักจะเปลี่ยนแปลงได้ง่ายและมีอายุสั้น โดยเฉพาะในกรณีของโปรแกรมเรียกค่าไถ่นั้น ส่วนใหญ่อาชญากรจะตั้งเวลาเพื่อให้ผู้เสียหายดำเนินการตามความต้องการไว้ไม่นาน แล้วโปรแกรมจะถูกตั้งคำสั่งให้ทำลายตัวเองพร้อมกับข้อมูล เพื่อให้ยากในการติดตามแกะรอย อีกทั้งข้อมูลบางชนิด เช่น ข้อมูลเอกสาร ไม่ได้ถูกเก็บไว้อย่างถาวร ข้อมูลดังกล่าวอาจอยู่ในหน่วยความจำของระบบคอมพิวเตอร์ในช่วงระยะเวลาสั้น ๆ เท่านั้น และต่อมาก็จะถูกบันทึกอัดทับข้อมูลโดยข้อมูลอื่น ๆ

ผู้วิจัยเห็นว่า การเก็บรักษาข้อมูลขององค์กรต่าง ๆ นั้น จะมีประโยชน์ต่อการสืบเสาะแกะรอยอาชญากรรมบนอินเตอร์เน็ตของหน่วยงานที่บังคับใช้กฎหมาย และในบางประเทศได้ออกระเบียบ กฎหมายบังคับให้มีการเก็บรักษาข้อมูลในขอบเขตที่กำหนดไว้ เช่น สาธารณรัฐเกาหลีใต้ที่มีหน่วยงานกลางดูและความมั่นคงของระบบข้อมูล (Cyber Security) ที่สำคัญ ซึ่งจะไม่เกี่ยวกับข้อมูลส่วนบุคคลทั่วไป เนื่องจากเกี่ยวข้องกับสิทธิและเสรีภาพของประชาชน พนักงานสอบสวนต้องพึ่งพาบันทึกประวัติ (Historical Record) ที่แสดงข้อมูลว่ามีการติดต่อจากไหนไปไหน เมื่อไร และโดยใคร บางโอกาสผู้บังคับใช้กฎหมายอาจต้องแกะรอยการติดต่อสื่อสารในทางลับ ๆ ด้วยเช่นกัน จะเห็นว่าในกระบวนการสืบสวนนั้นจำเป็นที่จะต้องสร้างพื้นฐานเกี่ยวกับบุคลากรที่เป็นพนักงานเจ้าหน้าที่ให้มีความรู้ความเชี่ยวชาญด้านเทคโนโลยี และจำนวนมากขึ้น สามารถทำการสืบสวนแกะรอยอาชญากรรมบนระบบอินเตอร์เน็ตได้อย่างรวดเร็ว และสามารถตอบโต้กับการกระทำใหม่ๆ ของอาชญากรได้

4.2 แนวทางการกำหนดคำนิยามและองค์ประกอบของการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่

การก่ออาชญากรรมโจมตีข้อมูลในอินเทอร์เน็ตเป็นเรื่องที่เกิดขึ้นจริง เนื่องจากการกระทำความผิดสามารถทำได้ง่ายดาย สะดวกสบาย และรวดเร็ว ที่สำคัญคือผู้กระทำผิดเป็นอาชญากรในที่มืดโดยไม่ต้องเปิดเผยตัวตน ไม่มีใครรู้จัก และยากต่อการตามจับตัว ในปัจจุบันประเทศไทยก็มีอาชญากรรมดังกล่าวเกิดขึ้น แต่ก็มิได้เป็นที่รู้จักกันมากนัก เนื่องจากอาชญากรรมประเภทนี้ไม่ได้มีการกระทำซึ่งส่อให้เห็นถึงความร้ายแรง ความป่าเถื่อนอย่างชัดเจนเหมือนอาชญากรรมทั่ว ๆ ไป ไม่ว่าจะเป็นการฆ่า ทำร้ายร่างกาย ลักทรัพย์ วิ่งราวทรัพย์ และกรรโชกทรัพย์ เป็นต้น แต่อาชญากรรมประเภทนี้มักจะส่งผลกระทบทางด้านชีวิตความเป็นอยู่ การทำงาน อารมณ์ และจิตใจของผู้เสียหายมากกว่า ซึ่งนับว่าเป็นเรื่องที่น่ากังวลเป็นอย่างมาก เพราะอารมณ์และจิตใจเป็นสิ่งที่อยู่ภายใน ยากต่อการที่บุคคลภายนอกจะสังเกตเห็นได้ว่าเป็นอย่างไร จนบางครั้งจะทำให้เกิดภาวะซึมเศร้า เก็บกด และหากเป็นการสูญเสียข้อมูลที่สำคัญในชีวิตไปอาจนำไปสู่การฆ่าตัวตายได้ในที่สุด กล่าวได้ว่าสิ่งเหล่านี้ถือเป็นภัยเงียบที่ยังมองไม่เห็น ทำให้หลายๆ คนยังไม่มีความกระตือรือร้นที่จะเห็นถึงอันตรายจาก

อาชญากรรมประเภทนี้ การเรียกค่าไถ่ทางคอมพิวเตอร์นั้น ทำให้บุคคลดังกล่าวเกิดผลกระทบในการทำงานที่เกี่ยวข้องกับคอมพิวเตอร์ จะเห็นได้ว่าไม่มีผลกระทบกับชีวิต ร่างกาย หรือทรัพย์สิน แต่กระทบถึงการดำรงชีวิต การทำงาน สภาพอารมณ์จิตใจ ความเครียด และความกังวล เป็นต้น

กฎหมายที่ใช้บังคับอยู่ในประเทศไทยปัจจุบันนั้น สามารถนำมาปรับใช้กับโปรแกรมเรียกค่าไถ่ได้ในบางกรณีเท่านั้น โดยต้องเทียบเคียงเป็นเรื่องๆ ไป ซึ่งบางกรณียังไม่มีความเสียหายหรือมีความเสียหายพิเศษตามที่กฎหมายให้ความคุ้มครองไว้ ผู้เสียหายก็ไม่สามารถเอาผิดกับผู้กระทำความผิดได้ แตกต่างจากสหรัฐอเมริกาและสหพันธ์สาธารณรัฐเยอรมนีที่มีการบัญญัติให้การเรียกค่าไถ่ข้อมูลและโปรแกรมเรียกค่าไถ่มีความรับผิดทางอาญาเป็นความผิดเฉพาะไว้แล้ว ดังนั้นผู้วิจัยจะวิเคราะห์แนวทางที่สามารถนำกฎหมายต่างประเทศมาเป็นแบบอย่างและปรับใช้อย่างเหมาะสมในกฎหมายของประเทศไทย

4.2.1 การกำหนดคำนิยามของการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่

เนื่องจากโปรแกรมเรียกค่าไถ่ถือเป็นเรื่องใหม่ และเป็นถ้อยคำค่อนข้างใหม่ในกฎหมายจึงจำเป็นต้องให้ความหมายของคำดังกล่าวให้ชัดเจน ซึ่งสามารถพิจารณาได้ดังนี้

“Ransomware” มาจากคำว่า “Ransom” รวมกับคำว่า “Ware” ซึ่งเป็นคำย่อของคำว่า “Software”

“Ransom” อาจหมายความว่า จำนวนเงินที่เรียกร้องในการแลกเปลี่ยนสำหรับคน (หรือบางครั้งก็เป็นสัตว์) ที่ได้ถูกจับเป็นเชลย หรือ หมายความว่า จำนวนเงินที่เรียกร้องในการแลกเปลี่ยนสำหรับบุคคลบางคน หรือบางสิ่งที่ถูกจ่าย แต่ตามศัพท์บัญญัติราชบัณฑิตยสถาน นิยามคำว่า “Ransom” หมายถึง จำนวนเงินที่เรียกร้องในการแลกเปลี่ยนสิ่งหนึ่งสิ่งใดหรือหมายถึงค่าไถ่

“Software (ซอฟต์แวร์)” หมายถึง ลำดับขั้นตอนการทำงานที่เขียนขึ้นด้วยชุดคำสั่งของคอมพิวเตอร์ ชุดคำสั่งเหล่านี้ทำงานตามลำดับเป็นโปรแกรมคอมพิวเตอร์ เพราะว่าคอมพิวเตอร์ทำงานตามคำสั่ง การทำงานพื้นฐานเป็นการกระทำกับข้อมูลที่เป็นตัวเลขฐานสอง ซึ่งใช้แทนข้อมูลที่เป็นตัวเลข ตัวอักษร รูปภาพ หรือแม้แต่เป็นเสียงพูดก็ได้ ดังนั้นนิยามคำว่า “Software” หมายถึงชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงาน โดยโปรแกรมที่ใช้สั่งงานคอมพิวเตอร์นั้น มีทั้งโปรแกรมที่ใช้งานกันตามปกติทั่วไปกับโปรแกรมที่มีความประสงค์ร้าย หรือแต่ก่อนเรียกกันว่า “ไวรัสคอมพิวเตอร์”

ดังที่กล่าวมานั้น ในพระราชบัญญัติอาชญากรรมทางคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 ผู้วิจัยเห็นว่าควรมีการเสนอให้แก้ไขในมาตรา 21 คือความหมายของคำว่า “ชุดคำสั่งไม่พึงประสงค์” ควรให้มีความหมายที่ครอบคลุมโปรแกรมประสงค์ร้ายทุกชนิด เพราะมิฉะนั้นแล้วคนที่ใช้ Worm หรือ Trojan โจมตีคนอื่นอาจจะไม่มีความผิด เพราะว่า Worm Trojan ไม่ใช่ Virus จะเห็นได้ว่าการกำหนดขอบเขตนิยามของกฎหมายให้หมายความถึงชุดคำสั่งโดยทั่วไปอาจไม่ครอบคลุมไปถึงระบบอื่นๆ ที่มีคุณสมบัติของโปรแกรมแตกต่างกัน แล้วการบังคับใช้กฎหมายก็จะขาดประสิทธิภาพและมีขอบเขตที่แคบไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้ อีกทั้งควรแก้ไขคำนิยามในมาตรา 3 โดยเพิ่มคำว่า “โปรแกรมเรียกค่าไถ่ (Ransomware) หมายถึง สิ่งแปลกปลอมในคอมพิวเตอร์ที่ล็อคระบบคอมพิวเตอร์ไว้ หรือสิ่งที่นำเข้าไปในคอมพิวเตอร์ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ โดยไม่ได้รับอนุญาตให้เข้าถึงจากผู้ที่ได้รับอนุญาตให้เข้าถึงคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์หรือข้อมูลใด ๆ ภายใต้สถานการณ์ที่มีการจัดวาง หรือบอกให้กระทำการใดๆ ซึ่งแสดงความต้องการให้ชำระเงินหรือความต้องการอื่นๆ เพื่อเป็นค่าไถ่ข้อมูลและลบสิ่งข้อมูลในคอมพิวเตอร์ออกไป (รวมทั้งให้สามารถเข้าถึงคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลเครือข่ายได้) มิฉะนั้นจะได้รับผลกระทบจากสิ่งแปลกปลอมนั้น” เช่นเดียวกันกับในสหรัฐอเมริกาที่มีกฎหมายที่ใช้ดำเนินคดีกับอาชญากรรมคอมพิวเตอร์ที่เกี่ยวข้องโดยตรง ได้แก่ California Penal Code : Comprehensive Computer Data Access And Fraud Act ได้ให้คำนิยาม “Ransomware” หรือ “โปรแกรมเรียกค่าไถ่” ไว้ในมาตรา 502 (B) (16) เพื่อเป็นการป้องกันปัญหาในเรื่องการตีความกฎหมายในประเทศไทยได้

4.2.2 การกำหนดองค์ประกอบในการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่

จากกระบวนการทำงานของโปรแกรม พบว่าขั้นตอนการทำงานของโปรแกรมเรียกค่าไถ่ ประกอบด้วยฐานความผิด 4 ส่วน สามารถอธิบายได้ ดังต่อไปนี้

ขั้นตอนที่ 1 การเข้าถึง (Access) และการหลอกลวง (Phishing)

ขั้นตอนที่ 2 การล็อกหรือการปิดกั้น (Obstruction) และทำให้ข้อมูลสูญหาย (Damaging)

ขั้นตอนที่ 3 การข่มขู่ (Intimidate) หรือกรรโชกเรียกค่าไถ่ (Ransom) และ

ขั้นตอนที่4 การทำลายข้อมูล (Information Destruction)

หากพิจารณาจากฐานความผิดแล้ว กล่าวได้ว่าความผิดของโปรแกรมเรียกค่าไถ่นั้นเป็นความผิดในตัวเอง (Mala Inse) กล่าวคือแม้ว่าผู้กระทำจะมิได้มีมูลเหตุจูงใจเพื่อก่อให้เกิดความเสียหาย หรือการกระทำดังกล่าวจะยังมิได้ก่อให้เกิดความเสียหายก็ตาม ทั้งนี้เพราะเห็นว่าการกระทำดังกล่าวนั้นสามารถก่อให้เกิดการกระทำผิดฐานอื่น ๆ หรือฐานที่ใกล้เคียงค่อนข้างง่ายและอาจก่อให้เกิดความเสียหายอย่างร้ายแรง อีกทั้งการพิสูจน์มูลเหตุจูงใจทำได้ค่อนข้างยาก

นอกจากนี้เพื่อไม่ให้ฐานความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่มีความหมายแคบมากเกินไป จึงควรกำหนดให้โปรแกรมเรียกค่าไถ่ที่จะมีโทษทางอาญานั้นไม่ต้องเป็นความผิดในกรณีที่ได้ละเมิดหรือฝ่าฝืนระบบการรักษาความมั่นคงหรือปลอดภัยที่มีการป้องกันโดยเฉพาะเท่านั้น โดยผู้วิจัยเห็นว่าโปรแกรมเรียกค่าไถ่ที่กระทำกับระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ผู้เป็นเจ้าของอาจไม่ได้มีการป้องกันโดยเฉพาะนั้น อันมิใช่เป็นการแสดงว่าเจ้าของไม่ได้หวงห้ามหรือไม่มีเจตนาที่จะป้องกันระบบคอมพิวเตอร์และข้อมูลในคอมพิวเตอร์ไว้โดยเฉพาะ แต่ในเบื้องต้นอาจจะยังไม่รู้เท่าทันความผิดดังกล่าว

เมื่อกล่าวถึงสาเหตุที่ต้องกำหนดองค์ประกอบในการกระทำความผิดแล้ว สิ่งที่ต้องพิจารณาต่อไปคือการกำหนดองค์ประกอบความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ว่ามีองค์ประกอบเช่นใด โดยจะเริ่มจากองค์ประกอบภายนอกก่อน ดังนี้

4.2.2.1 องค์ประกอบความผิดภายนอก

ในแนวทางการพิจารณาความผิดฐานการใช้โปรแกรมเรียกค่าไถ่นั้น ผู้วิจัยเห็นว่าควรเทียบเคียงแบบอย่างจากสหรัฐอเมริกา ตามมาตรา 1030 (A) (7) ที่อาจแยกองค์ประกอบได้ ดังนี้

องค์ประกอบข้อที่ 1 มีเจตนาที่จะรีดไถเงินหรือสิ่งอื่น ๆ ที่มีค่า ซึ่งคำว่า “เจตนา” กับ “รีดไถหรือเรียกค่าไถ่” นั้นได้กล่าวมาแล้ว ส่วนนิยามคำว่า “เงิน” หรือ “สิ่งอื่น ๆ ที่มีค่า” ควรคำนึงถึงสกุลเงินอื่น ๆ ซึ่งเป็นสกุลเงินในระบบดิจิทัลด้วย เพราะในอาชญากรรมคอมพิวเตอร์กรณีใช้โปรแกรมเรียกค่าไถ่นั้นอาชญากรอาจจะเรียกค่าไถ่ที่เป็นสกุลเงินระบบดิจิทัล อีกทั้งควรกำหนดให้ข้อมูลในระบบดิจิทัลและสกุลเงินดังกล่าว มีค่าในลักษณะของทรัพย์รูปแบบหนึ่งที่แปรเปลี่ยนไปตามยุคสมัยและกาลเวลา

องค์ประกอบข้อที่ 2 มีผลถึงในการสื่อสารระหว่างมลรัฐหรือระหว่างประเทศ นั่นคือจะต้องคำนึงถึงสถานที่ประกอบความผิด ซึ่งอาชญากรจะกระทำความผิดที่ใดก็ได้ในโลก แต่เมื่อมีความผิดเกิดขึ้นในประเทศไทยแล้วจะต้องรับผิดตามกฎหมายบัญญัติ

องค์ประกอบข้อที่ 3 จะต้องเป็นภัยคุกคามต่อความเสียหายให้แก่คอมพิวเตอร์ที่มีการป้องกัน ซึ่งในประเด็นเรื่องมาตรการป้องกันเฉพาะของเครื่องคอมพิวเตอร์นั้น มีความจำเป็นอย่างยิ่งเพื่อไม่ให้ผลักภาระให้เจ้าหน้าที่อย่างเดียว ผู้ใช้งานคอมพิวเตอร์ควรจะต้องมีความกระตือรือร้นที่จะป้องกันข้อมูลของตัวเองด้วย แต่อย่างไรก็ตามการกระทำความผิดนั้นๆ ต้องมีการกระทำผ่านช่องทางอินเทอร์เน็ตและการสื่อสารอิเล็กทรอนิกส์

ดังนั้นการสื่อสารผ่านทางเครื่องมืออิเล็กทรอนิกส์ในปัจจุบัน ทั้งผ่านทางสัญญาณอินเทอร์เน็ต สัญญาณโทรศัพท์ สัญญาณวิทยุ การใช้คอมพิวเตอร์ในการส่งอีเมล์ โต้ตอบผ่านทางกระดานสนทนา โซเชียลมีเดียต่าง ๆ การใช้โทรศัพท์พูดคุยเชื่อมต่ออินเทอร์เน็ต แอพพลิเคชั่นต่างๆ ไม่ว่าจะเป็นไลน์ (LINE) วอทแอพ (Whatsapp) วีแชท (Wechat) เป็นต้น สิ่งเหล่านี้หากมีการส่งสารถึงบุคคลอื่นล้วนแล้วแต่เป็นการสื่อที่สามารถเชื่อมต่อกับโปรแกรมเรียกค่าไถ่ได้ทั้งสิ้น และดูเหมือนว่าโปรแกรมเรียกค่าไถ่นี้จะไม่ได้หยุดอยู่แค่คอมพิวเตอร์หรือโทรศัพท์มือถือเท่านั้น เพราะมีแนวโน้มจะเข้าถึงอุปกรณ์ทุกอย่างที่สามารถเชื่อมต่ออินเตอร์เน็ตไม่ว่าจะเป็น โทรทัศน์ Smart Watch หรือแม้กระทั่งรถยนต์ที่ใช้ WIFI ก็อาจตกเป็นเป้าหมายได้เช่นกัน

ในสหรัฐอเมริกาแต่ละมลรัฐได้มีการบัญญัติลักษณะการกระทำที่ถือว่าเป็นการคุกคามล่วงละเมิดผู้อื่นแตกต่างกันออกไป เช่น มลรัฐมิสซูรีกำหนดให้กระทำการติดต่อสื่อสารในลักษณะที่เป็นการละเมิดผู้อื่นอันมีความผิดอาญา ซึ่งทำให้บุคคลอื่นนั้นเกิดความกลัว หรือมีการข่มขู่ หรือทำให้ผู้อื่นเกิดความรำคาญใจ เกิดความทุกข์ในอารมณ์ มลรัฐมิชิแกนกำหนดให้การโพสต์ข้อความที่มีจุดมุ่งหมายให้ผู้เสียหายเกิดความกลัว รู้สึกถูก ข่มขู่หรือเกิดความกังวล ขัดขืนใจ มลรัฐเวอร์มอนต์ได้กำหนดให้บุคคลใดมีเจตนาที่จะทำให้ผู้อื่นหวาดกลัว ข่มขู่หรือทำให้รำคาญ โดยการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ทางโทรศัพท์หรือด้วยวิธีการอื่นใด เป็นต้น จะเห็นได้ว่าหลักกฎหมายในสหรัฐอเมริกาแต่ละมลรัฐไม่มีการกำหนดลักษณะการกระทำที่แน่นอนชัดเจน ทั้งนี้เมื่อเปรียบเทียบกับการกระทำผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่นั้น ผู้วิจัยเห็นว่าสามารถกระทำได้หลากหลายวิธี ไม่ว่าจะเป็นการส่งอีเมล์ การโพสต์ข้อความ รูปภาพ หรือวิดิโอลงโซเชียลมีเดีย หรือการสนทนากันผ่านทางการสนทนาโต้ตอบแบบทันที (Instant Messages) เป็นต้น

4.2.2.2 องค์ประกอบความผิดภายใน

การกระทำความผิดที่ต้องมีโทษทางอาญานั้น นอกจากจะต้องครบองค์ประกอบภายนอกแล้วจะต้องพิจารณาถึงองค์ประกอบภายในด้วย ซึ่งขึ้นอยู่กับเจตนาของผู้กระทำความผิด และพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 ซึ่งการพิจารณาการกระทำความผิด จะต้องพิจารณาถึงองค์ประกอบภายในด้วย โดยองค์ประกอบภายในนั้น ตามประมวลกฎหมายอาญา มาตรา 59 ได้แยกเป็นการกระทำโดยเจตนา และการกระทำโดยประมาท โดยพิจารณาดังนี้

กรณีกระทำโดยเจตนา ตามประมวลกฎหมายอาญา มาตรา 59 โดยหลักแล้วองค์ประกอบภายในของความผิดอาญา คือเจตนา โดยเมื่อพิจารณาความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่และความผิดเกี่ยวกับคอมพิวเตอร์ในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 จะเห็นได้ว่าไม่มีถ้อยคำใดบ่งชี้เป็นพิเศษ จึงต้องถือตามหลักกฎหมายอาญาตามมาตรา 59 ว่าการที่จะเป็นการกระทำความผิดตามมาตรา 5 - 16 นั้นต้องเป็นการกระทำโดยเจตนา ดังนั้นแนวทางการพิสูจน์เจตนาในความรับผิดของโปรแกรมเรียกค่าไถ่นั้นไม่แตกต่างจากเจตนาในประมวลกฎหมายอาญาแต่อย่างใด ซึ่งเจตนาตามมาตรา 59 นี้ เป็นเจตนากระทำความผิดตามที่กฎหมายบัญญัติให้เป็นความไม่ดีอยู่ในตัวอยู่แล้ว ไม่จำเป็นต้องพิจารณาถึงมูลเหตุจูงใจอันเป็นความสำนึกส่วนตัวโดยทั่วไปแต่อย่างใด ดังนั้นในแนวทางการบัญญัติความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่ก็เช่นเดียวกัน จะต้องพิจารณาเพียงว่าการกระทำความผิดดังกล่าวมีเจตนาที่เรียกค่าไถ่หรือไม่เท่านั้น ถึงแม้ผู้ที่ใช้โปรแกรมเรียกค่าไถ่จะไม่มีเจตนาร้ายที่ประสงค์ต่อร่างกายโดยอ้างว่าต้องการเงินเพียงอย่างเดียว ก็ไม่เป็นข้อแก้ตัวให้พ้นจากความผิดในการใช้โปรแกรมเรียกค่าไถ่ได้ และเมื่อการใช้โปรแกรมเรียกค่าไถ่เป็นองค์ประกอบความผิดภายใน จึงไม่ใช่การกระทำความผิดโดยไม่รู้ผิดชอบตามประมวลกฎหมายอาญามาตรา 65 ที่มีหลักว่า การกระทำความผิดในขณะไม่สามารถรู้ผิดชอบ หรือไม่สามารถบังคับตนเองได้ เพราะมีจิตบกพร่อง โรคจิตหรือจิตฟั่นเฟือน ผู้นั้นไม่ต้องรับโทษสำหรับความผิดนั้น

กรณีเจตนาตามหลักกฎหมายของต่างประเทศ จากการศึกษาการกระทำความผิดฐานใช้โปรแกรมในลักษณะข่มขู่ รีดไถเพื่อให้ได้เงินของสหรัฐอเมริกา พบว่าได้มีการบัญญัติถึงองค์ประกอบความผิดภายในคือเรื่องของเจตนาของผู้กระทำความผิดไว้ กล่าวคือผู้กระทำความผิดจำเป็นต้อง “รู้” หรือ “โดยรู้” ว่าการกระทำดังกล่าวจะทำให้เหยื่อเกิดความรู้สึกสูญเสียโกรธ รำคาญ เกิดความหดหู่ เกิดความทุกข์ รู้สึกถูกข่มขู่ กรรโชก รีดไถ เป็นต้น

สำหรับองค์ประกอบภายในเรื่องเจตนา ที่สหรัฐอเมริกาบัญญัติให้เป็นความรับผิดทางอาญาฐานความผิดเกี่ยวกับคอมพิวเตอร์และการสื่อสารทางอิเล็กทรอนิกส์ล้วนแต่กำหนดให้การกระทำโดย “เจตนา” เป็นความผิด ตัวอย่างเช่น มลรัฐอิลลินอยส์บัญญัติว่า “การแสดงความคิดเห็น คำร้องขอ คำแนะนำหรือข้อเสนอแนะที่มีลักษณะหยาบคายและเป็นการกระทำที่มีเจตนา กระทำละเมิดหรือรุกรานผู้อื่น” มลรัฐอินเดียนา บัญญัติว่า “บุคคลใดมีเจตนาที่จะก่อความรังควาญรบกวนหรือทำให้บุคคลอื่นเกิดความตกใจ โดยไม่มีเจตนาของการสื่อสารที่ถูกต้องตามกฎหมาย....” และบางมลรัฐได้มีการบัญญัติเจตนาพิเศษไว้ เช่น มลรัฐมอนทาน่า กำหนดว่า “การใช้การสื่อสารทางอิเล็กทรอนิกส์ที่จะพยายามที่จะรีดไถเงินหรือสิ่งอื่นใดที่มีค่าจากบุคคลใดบุคคลหนึ่งหรือไปรบกวนการสื่อสารโดยการกระทำซ้ำๆ รบกวนความสงบหรือสิทธิความเป็นส่วนตัวของบุคคลใน

สถานที่ที่การสื่อสารจะได้รับ” ซึ่งเจตนาพิเศษของบทบัญญัตินี้คือการใช้เครื่องคอมพิวเตอร์และเครื่องมือสื่อสารอิเล็กทรอนิกส์ในการรีดไถเงินหรือสิ่งอื่นใด อันเป็นการรบกวนความสงบหรือสิทธิความเป็นส่วนตัวอันบุคคลพึงจะได้รับ

ผู้วิจัยเห็นว่า หากนำเรื่องเจตนามาบัญญัติในความผิดของโปรแกรมเรียกค่าไถ่นั้น ควรกำหนดไว้เป็นเรื่องของเจตนาพิเศษในเรื่องเงินหรือทรัพย์สินอื่นๆ เพราะถึงแม้ผู้กระทำความผิดอาจไม่คาดคิดว่าการกระทำนั้นๆ ของตนจะส่งผลกระทบร้ายแรงต่อเหยื่อถึงขั้นชีวิต เช่น การใช้โปรแกรมเรียกค่าไถ่ในโรงพยาบาลที่มีผลทำให้ผู้ป่วยเสียชีวิต เป็นต้น ดังนั้นแค่ผู้กระทำความผิดรู้หรือโดยรู้ ว่าการกระทำที่ตนเองได้กระทำลงไปนั้นจะทำให้เหยื่อได้รับความเดือดร้อน ก็เพียงพอที่จะเป็นความผิดแล้ว ในหลักของความประมาทตามประมวลกฎหมายอาญา มาตรา 59 บัญญัติว่า กระทำโดยประมาท ได้แก่ กระทำความผิดมิใช่โดยเจตนา แต่กระทำโดยปราศจากความระมัดระวังซึ่งบุคคลในภาวะเช่นนั้นจักต้องมีตามวิสัยและพฤติการณ์ และผู้กระทำอาจใช้ความระมัดระวังเช่นว่านั้นได้แต่หาได้ใช้ให้เพียงพอไม่ ซึ่งตามหลักแล้วการกระทำใดที่ไม่มีกฎหมายกำหนดให้ต้องรับผิดในการกระทำโดยประมาท แม้ผู้กระทำผิดกระทำครบองค์ประกอบภายนอกแล้วหากแต่เป็นการกระทำโดยประมาท ผู้กระทำก็ไม่ต้องรับผิด เพราะไม่มีกฎหมายบัญญัติให้เป็นความผิดแต่อย่างใด ในเรื่องความรับผิดในการใช้โปรแกรมเรียกค่าไถ่ก็เช่นกัน หากบทบัญญัติทางกฎหมายไม่ได้กำหนดให้การใช้โปรแกรมเรียกค่าไถ่เป็นการกระทำโดยประมาทในความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 แล้ว ดังนั้นการใช้โปรแกรมเรียกค่าไถ่โดยประมาทจึงไม่เป็นความผิด

5. สรุปและข้อเสนอแนะ

จากการศึกษาสภาพปัญหาของโปรแกรมเรียกค่าไถ่ในประเทศไทย พบว่ามีสภาพปัญหาที่เกิดขึ้นดังต่อไปนี้

1) ปัญหาเกี่ยวกับข้อกฎหมาย ซึ่งกฎหมายที่จะใช้ควบคุมการกระทำผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่นั้นไม่มีบัญญัติไว้ และกฎหมายอาญาที่มีอยู่ก็ไม่สามารถนำมาปรับใช้ได้ ซึ่งฐานความรับผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มี ยังไม่ครอบคลุมกับองค์ประกอบความผิดที่อาชญากรได้กระทำไป เมื่อพิจารณาเปรียบเทียบกับกฎหมายของต่างประเทศแล้ว ในประเทศที่มีการพัฒนากฎหมายอย่างต่อเนื่อง เช่น สหรัฐอเมริกาและสหพันธ์สาธารณรัฐเยอรมนี ได้บัญญัติความรับผิดที่เกี่ยวกับการใช้คำสั่งคอมพิวเตอร์ในการรีดไถ หรือกรรโชกเอาเงิน ซึ่งมีลักษณะคล้ายกับโปรแกรมค่าไถ่คอมพิวเตอร์ไว้ อีกทั้งปัญหาความล่าช้าในการตรากฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ ที่มีสาเหตุจากระบบงานราชการที่ยุ่งยากซับซ้อน หรือแม้แต่ระบบการพิจารณาในสภา ที่มีการเปลี่ยนรัฐบาลกันบ่อยๆ ทำให้การตรากฎหมายขาดความต่อเนื่อง และไม่ทันรูปแบบของการกระทำความผิดที่แปรเปลี่ยนพัฒนาไปตามเทคโนโลยี

2) ปัญหาอำนาจของพนักงานสอบสวนในการสืบสวนจับและกุมผู้กระทำผิด ในกรณีความผิดที่เกี่ยวพันกันหลายท้องที่จะมีปัญหาในเรื่องอำนาจของพนักงานสืบสวน และปัญหาเรื่องของ “พยานหลักฐาน” ในคดีเกี่ยวกับความผิดทางคอมพิวเตอร์ ซึ่งส่วนใหญ่เป็นสิ่งที่มองไม่เห็น จับต้องไม่ได้ และปรากฏอยู่เพียงชั่วเวลาใดเวลาหนึ่งเท่านั้น อีกทั้ง “ระยะเวลา” ที่ผู้กระทำผิดใช้ในการก่ออาชญากรรมมีระยะเวลาสั้นมาก โดยเฉพาะในกรณีของโปรแกรมเรียกค่าไถ่ที่ส่วนใหญ่อาชญากรจะตั้งเวลาเพื่อให้เหยื่อดำเนินการตามความต้องการไว้ไม่นาน แล้วโปรแกรมจะถูกตั้งคำสั่งให้ทำลายตัวเองพร้อมกับข้อมูลเพื่อให้ยากในการติดตามแกะรอย รวมทั้งในกระบวนการสืบสวนนั้น จำเป็นที่จะต้องสร้างบุคลากรให้เพียงพอและมีความรู้ความเชี่ยวชาญด้านเทคโนโลยีสามารถพัฒนาตามทันอาชญากรรมรูปแบบใหม่ ๆ ได้

เมื่อผู้วิจัยได้ศึกษาเนื้อหาอย่างละเอียดแล้ว มีข้อเสนอแนะ ดังต่อไปนี้

1) การที่ประเทศไทยไม่มีกฎหมายที่เหมาะสมในเรื่องการกระทำความผิดเกี่ยวกับการเรียกค่าไถ่ทางคอมพิวเตอร์นั้น ผู้วิจัยจึงเห็นว่าประเทศไทยควรที่จะต้องแก้ไขเพิ่มเติมใน พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 โดยการแยกการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่ทางคอมพิวเตอร์ออกมาเป็นอีกหมวดหนึ่งโดยเฉพาะ และกำหนดบทลงโทษผู้กระทำความผิดไว้ด้วย เช่นเดียวกับรัฐบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ของสาธารณรัฐสิงคโปร์ เพื่อให้กฎหมายมีความทันสมัยมากยิ่งขึ้นและควรศึกษาการกระทำความผิดเกี่ยวกับโปรแกรมเรียกค่าไถ่ให้มีรูปแบบ

ที่ทันสมัย เพื่อเป็นการอุดช่องว่างของกฎหมายและป้องกันการใช้ช่องว่างของกฎหมายเพื่อใช้ในการกระทำความผิด

2) การกำหนดคำนิยามของโปรแกรมเรียกค่าไถ่นั้นใน พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 ยังมิได้มีการบัญญัติคำนี้ลงในคำนิยามในมาตรา 3 ซึ่งผู้วิจัยเห็นควรให้บัญญัติเพิ่มเติม คำว่า “โปรแกรมเรียกค่าไถ่ (Ransomware)” เช่นเดียวกันกับในสหรัฐอเมริกามีกฎหมายที่ใช้ดำเนินคดีกับอาชญากรรมคอมพิวเตอร์ที่เกี่ยวข้องโดยตรง เพื่อเป็นการป้องกันการตีความในกฎหมาย อีกทั้งควรมีการเสนอให้แก้ไขในมาตรา 21 ในความหมายของคำว่า “ชุดคำสั่งไม่พึงประสงค์” ควรให้มีความหมายที่ครอบคลุมโปรแกรมประสงค์ร้ายทุกชนิด หากกำหนดขอบเขตนิยามของกฎหมายไม่ครอบคลุมไปถึงระบบอื่น ๆ แล้วการบังคับใช้กฎหมายก็จะขาดประสิทธิภาพและมีขอบเขตที่แคบไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้

นอกจากนี้ รัฐควรจัดตั้งศูนย์บริการรับเรื่องร้องเรียนเพื่อให้ประชาชนสามารถร้องเรียนถึงพฤติกรรมที่ไม่เหมาะสมในการใช้งานบนอินเทอร์เน็ต ซึ่งรวมถึงการใช้โปรแกรมเรียกค่าไถ่ เพื่อให้สามารถรวบรวมลักษณะของการกระทำความผิดและความเสียหายที่เกิดขึ้นเพื่อศึกษาหาแนวทางในการป้องกันการกระทำความผิดที่เหมาะสมกับประเทศไทยต่อไป อีกทั้งควรจัดทำคำแนะนำและอบรมเจ้าหน้าที่ผู้ใช้บังคับกฎหมาย ผู้ให้บริการอินเทอร์เน็ตรวมถึงประชาชนทั่วไปถึงวิธีที่ควรปฏิบัติในการใช้งานบนอินเทอร์เน็ตเพื่อป้องกันโปรแกรมเรียกค่าไถ่ (Ransomware) ไม่ว่าทางใดเพื่อการป้องกันประชาชนจากการตกเป็นผู้ถูกกระทำจากโปรแกรมเรียกค่าไถ่ทางคอมพิวเตอร์

6. บรรณานุกรม

คำพิพากษาศาลฎีกาที่ 5161/2547.

ประมวลกฎหมายวิธีพิจารณาความอาญา.

ประมวลกฎหมายอาญา.

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560.

ศรีศักดิ์ จามรมาน. (2549). **การใช้เทคโนโลยีสารสนเทศเพื่อพัฒนาระบบการบริการและนโยบายสวัสดิการสังคมไทย.** เอกสารประกอบการสัมมนาเชิงปฏิบัติการ, คณะสังคมสงเคราะห์ศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

สาวตรี สุขศรี. (2552). **วิวัฒนาการเทคโนโลยีข้อมูลข่าวสาร: อาชญากรรมคอมพิวเตอร์กับปัญหาที่เกิดขึ้นในทางกฎหมาย.** วารสารนิติศาสตร์. 38(2): 193-194.

California Penal Code SB 1137.

Criminal Code (Strafgesetzbuch, StGB).

Computer Crime Act (Malaysia) 1997.

Computer Misuse Act (Singapore) 1990.

Criminal Code (Strafgesetzbuch, StGB))

ฐานข้อมูลออนไลน์

พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554. **ค่าไถ่.** www.royin.go.th/dictionary/. เข้าถึงเมื่อ 14 มีนาคม 2561.

ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏรำไพพรรณี.**แจ้งข่าวการแพร่กระจายไวรัส Ransomware mssecsvc.exe ภายในมหาวิทยาลัย.** www.rbru.ac.th/th/news/index.php?p=nSearch&typenews=&keyword=ransomware. เข้าถึงเมื่อ 14 มีนาคม 2561.

Help Net Security. **88% of all ransomware is detected in the healthcare industry.** www.helpnetsecurity.com/2016/07/27/ransomware-healthcare-industry. เข้าถึงเมื่อ 14 มีนาคม 2561.