บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

สังคมในปัจจุบันนี้เทคโนโลยีทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทในชีวิตประจำวันของผู้คนในสังคมเป็นอย่างมาก ความก้าวหน้าทางเทคโนโลยีเหล่านี้มีส่วนช่วยให้การดำเนินกิจกรรมต่าง ๆ เป็นไปอย่างรวดเร็วและสะดวกสบายมากยิ่งขึ้น หน่วยงานและองค์กรทั้งภาครัฐและเอกชนต่างยอมรับเอาคุณประโยชน์ของเทคโนโลยีนี้มาเพื่อประยุกต์ใช้ในการดำเนินงานกิจการต่าง ๆ ของแต่ละหน่วยงาน อาทิ รูปแบบการให้บริการที่เรียกว่า “E-Service” ของหน่วยงานภาครัฐ ซึ่งนำเอาเทคโนโลยีคอมพิวเตอร์มาใช้ในการให้บริการ ตัวอย่างที่เห็นได้ชัดคือ การให้บริการชำระภาษีผ่านทางอินเทอร์เน็ตสำหรับประชาชนทั่วไป (E-Revenue) ของกรมสรรพากร[1] การสำรองที่นั่งตั๋วโดยสารเครื่องบินผ่านทางอินเทอร์เน็ต (E-Booking)[2] รูปแบบการบริการธนาคารอิเล็กทรอนิกส์ (E-Banking) ซึ่งทำให้ลูกค้าของธนาคารสามารถทำธุรกรรมทางการเงินการธนาคารได้อย่างสะดวกและรวดเร็ว[3] ตัวอย่างเหล่านี้เป็นเพียงส่วนหนึ่งของการประยุกต์ใช้เทคโนโลยีคอมพิวเตอร์และเทคโนโลยีสารสนเทศเพื่อให้เกิดประโยชน์กับสังคมมากที่สุด

แต่อย่างไรก็ตาม การใช้งานเทคโนโลยีเหล่านี้ หากนำมาใช้ในแนวทางที่ไม่ถูกต้องและเหมาะสมแล้ว จะส่งผลกระทบและก่อให้เกิดความเสียหายแก่สังคมเป็นอย่างยิ่ง ดังเช่นข่าวสารที่ปรากฏตามสื่อต่าง ๆ ในยุคสมัยนี้ อาทิ “แฮกเกอร์รวมพลถล่มอินเทอร์เน็ตอาทิตย์นี้[4]” “แฮกเกอร์

---

[1] วศิน เพิ่มทรัพย์, ความรู้เบื้องต้นเกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศ, (กรุงเทพมหานคร: โปรวิชั่น, 2548), น.34.

[2] *เพิ่งอ้าง*, น.35.

[3] *เพิ่งอ้าง*, น.38.

[4] “แฮกเกอร์รวมพลถล่มอินเทอร์เน็ตอาทิตย์นี้,” <http://www.thaicleannet.com/modules.php?name=tcn_stories_view&sid=170>

เจาะระบบภัยออนไลน์ใกล้ตัว[5]" "มือดีลองของแฮกเว็บไอซีทีโพสต์รูปควายเย้ยผู้บริหาร[6]" "แฮกเกอร์ล่มเครือข่ายมือถือด้วย SMS[7]" "แฮกเกอร์เปลี่ยนหน้าเว็บราชการทั่วโลก[8]" "แฮกเกอร์เจาะระบบคอมพิวเตอร์เพื่อเปลี่ยนเกรดตัวเอง[9]" "แฮกเกอร์ชาวอังกฤษบุกรุกระบบคอมพิวเตอร์ของทหารสหรัฐอเมริกา[10]" "สหรัฐอเมริกาแจ้งกองปราบล่าโจรไฮเทคเจาะฐานทัพอากาศโจรกรรมข้อมูล[11]" "แฮกเกอร์เจาะระบบคอมพิวเตอร์โกงการเลือกตั้ง[12]" "ตำรวจอิตาลีจับแฮกเกอร์ซึ่งเจาะระบบเว็บไซต์สำคัญของสหรัฐอเมริกา[13]" และข่าวอื่น ๆ ทำนองเดียวกันนี้อีกมากมาย กรณีต่าง ๆ เหล่านี้ล้วนเป็นสัญญาณที่สะท้อนให้เห็นถึงรูปแบบใหม่ของปัญหาสังคมในยุคเทคโนโลยีสารสนเทศ

---

[5] "แฮกเกอร์เจาะระบบภัยออนไลน์ใกล้ตัว," <http://www.thairath.com/thairath1/2546/itdigest/feb/17/itdigest.asp>

[6] "มือดีลองของแฮกเว็บไอซีทีโพสต์รูปควายเย้ยผู้บริหาร," <http://www.police.go.th/policenews/show.php?news_id=269&cat=CRC1&id=135>, 20 พฤษภาคม 2546.

[7] "แฮกเกอร์ล่มเครือข่ายมือถือด้วย SMS," <http://www.arip.co.th/news.php?id=404507>

[8] "แฮกเกอร์เปลี่ยนหน้าเว็บราชการทั่วโลก," <http://www.police.go.th/policenews/show.php?news_id=155&cat=CRC1&id=99>, 23 มกราคม 2544.

[9] "แฮกเกอร์เจาะระบบคอมพิวเตอร์เพื่อเปลี่ยนเกรดตัวเอง," <http://www.police.go.th/policenews/show.php?news_id=188&cat=CRC1&id=107>, 26 พฤศจิกายน 2545.

[10] "แฮกเกอร์ชาวอังกฤษบุกรุกระบบคอมพิวเตอร์ของทหารสหรัฐอเมริกา," <http://www.police.go.th/policenews/show.php?news_id=134&cat=CRC1&id=87>, 17 พฤศจิกายน 2545.

[11] "สหรัฐอเมริกาแจ้งกองปราบล่าโจรไฮเทคเจาะฐานทัพอากาศโจรกรรมข้อมูล," <http://www.police.go.th/policenews/show.php?news_id=146&cat=CRC1&id=97>, 27 มกราคม 2542.

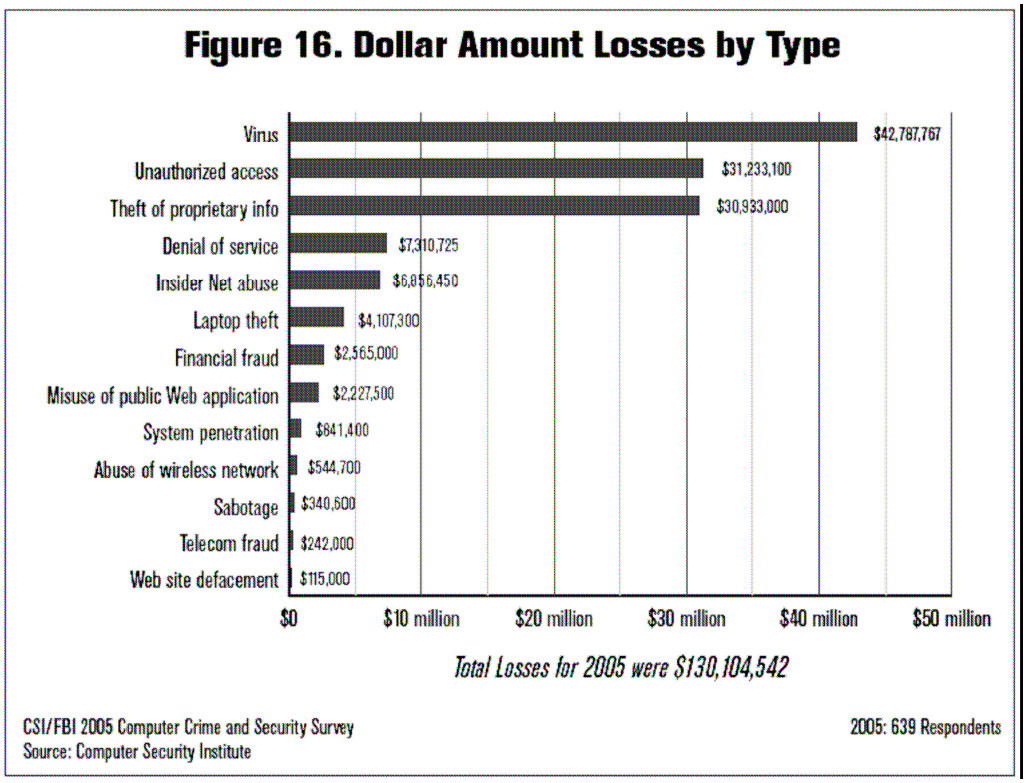
[12] "จับ แฮกเกอร์ เจาะระบบโกงการเลือกตั้งของมหาวิทยาลัย," <http://www.police.go.th/policenews/show.php?news_id=286&cat=CRC1&id=137>, 30 มิถุนายน 2546.

[13] "ตำรวจอิตาลีรวบแฮกเกอร์เจาะเว็บลับของทางการสหรัฐ," <http://www.police.go.th/policenews/show.php?news_id=23&cat=CRC1&id=15 >, 1 พฤศจิกายน 2545.

อาชญากรรมคอมพิวเตอร์ (Computer Crime) เป็นประเด็นที่ถูกหยิบยกขึ้นมาพิจารณาอย่างละเอียดถี่ถ้วนในช่วงระยะเวลาหลายปีที่ผ่านมา เนื่องจากเป็นปัญหาสังคมในมิติใหม่ซึ่งก่อให้เกิดความเสียหายทั้งต่อบุคคลและสังคมสารสนเทศเป็นอย่างมาก นอกจากนี้ยังสร้างความสูญเสียทางเศรษฐกิจคิดเป็นเงินจำนวนมหาศาล จากการสำรวจความเสียหายที่เกิดจากอาชญากรรมคอมพิวเตอร์ในปี ค.ศ. 2005 ซึ่งทำการสำรวจโดยสถาบันความปลอดภัยด้านคอมพิวเตอร์ (CSI : Computer Security Institute) และสำนักงานสืบสวนสอบสวนกลาง (FBI: Federal Bureau of Investigation) ของประเทศสหรัฐอเมริกา[14] ปรากฏผลออกมาว่า ความสูญเสียที่เกิดจากอาชญากรรมคอมพิวเตอร์ในปี ค.ศ. 2005 คิดเป็นเงินทั้งสิ้น 130,104,542 เหรียญสหรัฐ

ภาพที่ 1.1

การสำรวจความเสียหายที่เกิดจากอาชญากรรมคอมพิวเตอร์ในปี ค.ศ. 2005



[14] Lawrence A. Gordon, Martin P. Loeb,William Lucyshyn and Robert Richardson, “2005 CSI/FBI computer Crime and Security Survey,” <http://www.usdoj .gov/criminal/cybercrime/FBI2005.pdf>

ผลกระทบจากอาชญากรรมคอมพิวเตอร์ซึ่งก่อให้เกิดความเสียหายอย่างร้ายแรงต่อสังคมในยุคเทคโนโลยีสารสนเทศนี้มีที่มาของปัญหาเกิดจากฝีมือของบุคคลที่สังคมทั่ว ๆ ไปรู้จักในชื่อว่า “แฮกเกอร์” (hacker) ซึ่งมีความหมายในทำนองผู้ที่มีความรู้ความสามารถในด้านคอมพิวเตอร์เป็นพิเศษและนำความรู้ของตนมาใช้ในทางที่ผิด โดยวิธีการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจ หรือไม่ได้รับความยินยอมจากผู้ที่มีอำนาจ การสร้างชุดโปรแกรมที่เรียกว่า “ไวรัสคอมพิวเตอร์” “หนอน” (Worm) หรือ “ม้าโทรจัน” (Trojan Horse) เพื่อวัตถุประสงค์ในการทำลาย หยุดยั้งหรือควบคุมระบบการทำงานของคอมพิวเตอร์ของผู้อื่น หรือเพื่อการจารกรรมข้อมูลที่สำคัญของผู้อื่นผ่านทางระบบเครือข่ายคอมพิวเตอร์ พฤติกรรมของผู้กระทำผิดเหล่านี้ได้นำมาสู่รูปแบบของอาชญากรรมในมิติใหม่ที่เติบโตขึ้นท่ามกลางกระแสของเทคโนโลยีสารสนเทศซึ่งเชื่อมโยงข้อมูลสารสนเทศทุกพื้นที่ในโลกใบนี้ให้สามารถเข้าถึงได้อย่างสะดวกรวดเร็วและฉับไว

หลายประเทศต่างตระหนักถึงปัญหาอันเกิดจากพิษภัยของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบที่มีต่อสังคมในยุคเทคโนโลยีสารสนเทศ จึงมีการกำหนดมาตรการทางกฎหมายเพื่อดำเนินคดีและลงโทษผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบเหล่านี้[15] การลงโทษผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบไม่ได้มีวัตถุประสงค์เพียงเพื่อการทดแทนหรือการแก้แค้นผู้กระทำผิดเท่านั้น แต่ยังมีวัตถุประสงค์เพื่อยับยั้งไม่ให้มีการกระทำความผิดซ้ำอีก หรือยับยั้งผู้กระทำผิดคนอื่น ๆ ที่จะกระทำความผิดในลักษณะเช่นเดียวกันนี้มิให้เอาเป็นเยี่ยงอย่าง รวมทั้งแก้ไขฟื้นฟูให้ผู้กระทำผิดกลับตัวกลับใจสำนึกผิดในการกระทำที่ตนได้ทำลงไป พร้อมที่จะกลับคืนสู่สังคมในฐานะของพลเมืองดีต่อไป หากกระบวนการยุติธรรมสามารถปฏิบัติต่อผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบให้บรรลุผลตามวัตถุประสงค์ของการลงโทษดังกล่าวข้างต้นแล้ว จะทำให้สามารถแก้ไขปัญหาและควบคุมอาชญากรรมคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ

มาตรการทางอาญาสำหรับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศมีวิธีการหรือรูปแบบที่แตกต่างกันไป เช่น การจำคุก การปรับหรือชดใช้ค่าเสียหาย การริบอุปกรณ์คอมพิวเตอร์ การห้ามเข้าถึงคอมพิวเตอร์หรืออินเทอร์เน็ต หรือควบคุมการใช้งานคอมพิวเตอร์ การทำงานบริการสังคม เป็นต้น มาตรการต่าง ๆ เหล่านี้ ต่างมีข้อดีข้อเสียที่

---

[15] “ความปลอดภัยของเครือข่ายอินเทอร์เน็ต,” <http://www.police.go.th/pisc/cybercrime.pdf>

แตกต่างกันออกไป ดังนั้นการกำหนดมาตรการบังคับทางอาญาจึงต้องเหมาะสม สอดคล้องกับวัตถุประสงค์ในการลงโทษ เพราะหากมีการนำมาตรการทางอาญามาใช้โดยมิได้คำนึงถึงวัตถุประสงค์ในการลงโทษแล้ว ผู้กระทำความผิดจะไม่รู้สึกเข็ดหลาบ หรือสำนึกผิดในการกระทำของตน ในที่สุดจึงกลับไปกระทำความผิดในลักษณะเดียวกันนั้นอีก เหมือนเช่นในกรณีที่เคยเกิดขึ้นกับคดีแฮกเกอร์ชื่อดัง คือ นายเควิน เดวิด มิตนิก (Kevin David Mitnick) ซึ่งถูกดำเนินคดีและพิพากษาลงโทษตั้งแต่อายุ 17 ปี หลังจากพ้นโทษเขายังกลับไปเกี่ยวข้องกับการกระทำความผิดทางคอมพิวเตอร์มาตลอดระยะเวลา 16 ปี และถูกเจ้าหน้าที่จับกุมดำเนินคดีถึง 6 ครั้ง[16] กรณีนี้ทำให้เกิดคำถามตามมาว่า เหตุใดมาตรการทางอาญาสำหรับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบจึงไม่บรรลุตามวัตถุประสงค์ของการลงโทษและมาตรการบังคับทางอาญาวิธีการใดหรือรูปแบบใดที่เหมาะสมที่จะนำมาใช้กับผู้กระทำผิดในลักษณะนี้

ปัจจุบันประเทศไทยมีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้ว แต่อย่างไรก็ตามเนื่องด้วยกระบวนการยุติธรรมทางอาญาของไทยยังไม่เคยมีประสบการณ์เกี่ยวกับคดีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบเหมือนเช่นในต่างประเทศ ผู้เขียนจึงได้ศึกษาถึงรูปแบบของมาตรการทางอาญากรณีการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศ พร้อมทั้งวิเคราะห์ถึงข้อดี ข้อด้อยและความเป็นไปได้ในการนำมาตรการดังกล่าวมาปรับใช้กับกระบวนการยุติธรรมทางอาญาของไทย ทั้งนี้เพื่อให้เกิดความเหมาะสมกับสภาพตัวผู้กระทำผิดและพฤติการณ์แห่งคดีนั้นๆ อันจะส่งผลให้บรรลุซึ่งวัตถุประสงค์ในการลงโทษและสามารถควบคุม ป้องกันอาชญากรรมทางคอมพิวเตอร์ซึ่งเกิดจาก ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบได้อย่างแท้จริง

การศึกษาของผู้เขียนในครั้งนี้วางอยู่บนพื้นฐานของสมมติฐาน คือ การกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบมีสาเหตุของการกระทำผิดหรือมีแรงจูงใจในการกระทำความผิดที่แตกต่างจากอาชญากรในรูปแบบอื่น ดังนั้นมาตรการบังคับทางอาญาที่เหมาะสมสำหรับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบจึงควรมีความแตกต่างจากอาชญากรรูปแบบอื่นด้วย ในเบื้องต้นผู้เขียนจึงศึกษาถึงสาเหตุของการกระทำความผิดผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในแต่ละรูปแบบ ทั้งนี้เพื่อประโยชน์ในการนำมาตรการทางอาญาที่เหมาะสมกับลักษณะการกระทำผิดในแต่ละกรณีไปใช้ให้เกิดประสิทธิภาพทั้งในแง่ของ

---

[16] Tsutomu Shimomura and John Markoff, วิสามัญฯ แฮกเกอร์ (Take Down), แปลโดย Super U:-), (กรุงเทพมหานคร: สำนักพิมพ์มติชน, 2543), น.292-390.

การข่มขู่ยับยั้งและการแก้ไขฟื้นฟูผู้กระทำผิด และนอกจากนี้ยังศึกษาแนวความคิดและทฤษฎีการลงโทษรวมถึงรูปแบบและวิธีการในการใช้มาตรการทางอาญาสำหรับการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศ ซึ่งสามารถนำมาปรับใช้เป็นแนวทางในการพิจารณาวิเคราะห์ถึงความเหมาะสมและความเป็นไปได้ในการนำมาใช้กับกระบวนการยุติธรรมของไทย

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาสาเหตุของการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ รวมถึงความคิด ทัศนคติและแรงจูงใจในการกระทำความผิด ทั้งนี้เพื่อทำความเข้าใจสภาพภูมิหลังของผู้กระทำผิด และนำความรู้ที่ได้มาปรับใช้ในการวางมาตรการทางอาญาที่เหมาะสมกับผู้กระทำผิดในแต่ละรูปแบบเพื่อให้บรรลุผลทั้งในการข่มขู่ยับยั้งและการแก้ไขฟื้นฟูผู้กระทำผิด
2. เพื่อศึกษามาตรการบังคับทางอาญาสำหรับการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศ
3. เพื่อศึกษาแนวทางและความเป็นไปได้ในการกำหนดมาตรการทางอาญาสำหรับกรณีการกระทำความผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ ทั้งนี้เพื่อให้มีมาตรการทางอาญาสำหรับการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบที่สอดคล้องตามวัตถุประสงค์ของการลงโทษอย่างแท้จริง

1.3 สมมติฐานการศึกษา

การกำหนดโทษสำหรับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในประเทศไทยยังไม่เหมาะสมในการบรรลุวัตถุประสงค์ของการข่มขู่ยับยั้งและแก้ไขฟื้นฟูผู้กระทำผิด เนื่องจากยังมีมาตรการลงโทษที่ไม่หลากหลายเหมือนที่กำหนดในกฎหมายต่างประเทศ

1.4 ขอบเขตของการศึกษา

วิทยานิพนธ์ฉบับนี้จะศึกษาถึงสาเหตุและแรงจูงใจในการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ โดยจะศึกษาจากข้อมูลทางวิชาการและการวิจัยทั้งในด้านสังคมวิทยา จิตวิทยาและอาชญาวิทยา รวมทั้งศึกษาถึงบทบัญญัติความผิดและโทษที่เกี่ยวข้องกับการกระทำความผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบทั้งของไทยและต่างประเทศ รวมทั้งมาตรการทางอาญาในต่างประเทศที่ได้นำมาบังคับกับการกระทำผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ

1.5 วิธีการศึกษา

ศึกษาโดยวิธีการค้นคว้าวิจัยเอกสารเกี่ยวกับอาชญากรรมคอมพิวเตอร์ สาเหตุและแรงจูงใจในการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ บทบัญญัติและมาตรการบังคับทางอาญาสำหรับการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบทั้งของไทยและต่างประเทศ ทั้งนี้โดยศึกษาจากตำราทางวิชาการ วิทยานิพนธ์ บทความทั้งของไทยและต่างประเทศ นอกจากนี้ยังศึกษาจากข้อมูลทางสื่ออิเล็กทรอนิกส์ต่าง ๆ ได้แก่ ข้อมูลจากเว็บไซต์ในอินเทอร์เน็ต

1.6 ประโยชน์ของการศึกษา

1. ทำให้ทราบถึงสาเหตุและแรงจูงใจในการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ รวมถึงแนวความคิด ทัศนคติของผู้กระทำผิดที่มีต่อการกระทำความผิดทางคอมพิวเตอร์
2. ทำให้ทราบถึงรูปแบบหรือวิธีการในการบังคับทางอาญาสำหรับการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศ
3. ทำให้ทราบถึงแนวทางที่เหมาะสมและความเป็นไปได้ในการกำหนดมาตรการทางอาญาในประเทศไทยให้เหมาะสมกับการกระทำผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในแต่ละประเภท เพื่อให้สอดคล้องกับวัตถุประสงค์ในการลงโทษทั้งในด้านการข่มขู่ยับยั้งและการแก้ไขฟื้นฟูผู้กระทำผิด