

บทที่ 4

กฎหมายไทยที่สามารถนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ต

ในบทนี้จะกล่าวถึงบทบัญญัติในกฎหมายอาญาของไทยที่สามารถนำมาบังคับใช้กับการข่มขู่ทางอินเทอร์เน็ต โทษสำหรับการกระทำความผิดฐานข่มขู่ทางอินเทอร์เน็ต มาตรการอื่น ๆ ที่อาจนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ต และเปรียบเทียบบทบัญญัติฐานข่มขู่ทางอินเทอร์เน็ตในประเทศสหรัฐอเมริกา กับกฎหมายของประเทศไทย

4.1 บทบัญญัติในกฎหมายอาญาของไทยที่สามารถนำมาบังคับใช้

ในหัวข้อนี้จะศึกษาว่ามีบทบัญญัติในกฎหมายอาญาของไทยบทบัญญัติใดบ้างที่สามารถนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ตได้ โดยจะศึกษาพิจารณาถึงองค์ประกอบของการข่มขู่ทางอินเทอร์เน็ต กับบทบัญญัติในประมวลกฎหมายอาญา และบทบัญญัติในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

จากการศึกษาในบทที่ผ่านมาทำให้ทราบว่า การข่มขู่ทางอินเทอร์เน็ตมีองค์ประกอบดังนี้ คือ 1. ใช้หรือส่งอีเมลหรือการสื่อสารทางอิเล็กทรอนิกส์ ด้วยถ้อยคำข่มขู่ว่าจะทำร้ายร่างกายบุคคลใดบุคคลหนึ่ง หรือข่มขู่ว่าจะก่อให้เกิดความเสียหายหรือทำลายทรัพย์สินของบุคคลใดบุคคลหนึ่ง หรือกระทำการต่อบุตร พี่น้อง คู่สมรส หรือผู้อยู่ในอุปการะของบุคคลดังกล่าว 2. ใช้หรือส่งอีเมลหรือการสื่อสารทางอิเล็กทรอนิกส์ถึงบุคคลอื่นในลักษณะซ้ำ ๆ อย่างต่อเนื่อง 3. ส่งอีเมลหรือการสื่อสารทางอิเล็กทรอนิกส์ถึงบุคคลอื่นโดยรู้ว่าจะมีความนั้นเป็นเท็จ 4. ยินยอมรับรู้ให้มีการใช้อุปกรณ์ทางอิเล็กทรอนิกส์ซึ่งอยู่ในความควบคุมของตนเพื่อใช้กระทำการตามที่บัญญัติไว้ว่าการกระทำใดเป็นการกระทำความผิดฐานข่มขู่ทางอินเทอร์เน็ต 5. ใช้การสื่อสารทางอิเล็กทรอนิกส์ในการชักจูงให้บุคคลที่สามกระทำการอันละเมิดต่อกฎหมายแทนตน

6. สร้างและดำเนินการจัดการเว็บไซต์ที่มีข้อความข่มขู่ หรือรังควานผู้อื่น

ส่วนขององค์ประกอบภายในนั้น ผู้ที่กระทำการข่มขู่ทางอินเทอร์เน็ตจะต้องมีเจตนาดังนี้ คือ โดยเจตนาข่มเหง รบกวน ข่มขู่ ทำให้หวาดกลัว รังควาน หรือทำให้อับอาย

พิจารณาองค์ประกอบข้างต้นกับบทบัญญัติในกฎหมายอาญาของประเทศไทยได้ ดังนี้

4.1.1 ประมวลกฎหมายอาญา

เมื่อพิจารณาถึงลักษณะของการข่มขู่ทางอินเทอร์เน็ตดังที่ได้กล่าวมาแล้วนั้น บทบัญญัติในประมวลกฎหมายอาญาของไทยที่อาจนำมาปรับใช้เกี่ยวกับกับการข่มขู่ทางอินเทอร์เน็ตมี 3 มาตรา ได้แก่ มาตรา 309 และมาตรา 392

1. ประมวลกฎหมายอาญามาตรา 309 บัญญัติว่า “มาตรา 309 ผู้ใดข่มขืนใจผู้อื่นให้กระทำการใด ไม่กระทำการใด หรือจ่ายอมต่อสิ่งใด โดยทำให้กลัวว่าจะเกิดอันตรายต่อชีวิต ร่างกาย เสรีภาพ ชื่อเสียงหรือทรัพย์สินของผู้ถูกข่มขืนใจนั้นเองหรือของผู้อื่น หรือโดยใช้กำลังประทุษร้ายจนผู้ถูกข่มขืนใจต้องกระทำการนั้น ไม่กระทำการนั้นหรือจ่ายอมต่อสิ่งนั้น ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ

ถ้าความผิดตามวรรคแรกได้กระทำโดยมีอาวุธ หรือโดยร่วมกระทำความผิดด้วยกันตั้งแต่ห้าคนขึ้นไป หรือได้กระทำเพื่อให้ผู้ถูกข่มขืนใจทำ ถอน ทำให้เสียหาย หรือทำลายเอกสารสิทธิอย่างใด ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้ากระทำโดยอ้ำอานาจอั้งยี่หรือชองโจร ไม่ว่าอั้งยี่หรือชองโจรนั้นจะมีอยู่หรือไม่ ผู้กระทำต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองพันบาทถึงหนึ่งหมื่นสี่พันบาท”

2. ประมวลกฎหมายอาญามาตรา 392 บัญญัติว่า “ผู้ใดทำให้ผู้อื่นเกิดความกลัว หรือความตกใจ โดยการขู่เข็ญ ต้องระวางโทษจำคุกไม่เกินหนึ่งเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ”

4.1.1.1 ความผิดตามประมวลกฎหมายอาญามาตรา 309

การกระทำของผู้ใดจะเป็นการกระทำความผิดตามมาตรา 309 ได้นั้น ผู้กระทำต้องได้กระทำการครบทั้งองค์ประกอบภายนอกและภายในตามที่กฎหมายมาตรานี้บัญญัติไว้ ดังนี้

องค์ประกอบภายนอก

1. ข่มขืนใจผู้อื่นให้กระทำการใด ไม่กระทำการใด หรือจ่ายอมต่อสิ่งใด คือเป็นการบังคับใจผู้อื่นให้เขาต้องกระทำการใด ไม่กระทำการใด หรือจ่ายอมต่อสิ่งใด

การข่มขืนใจให้ผู้อื่นกระทำ หมายความว่า ให้เคลื่อนไหวร่างกาย การข่มขืนใจไม่ให้กระทำ หมายความว่า ไม่ให้กระทำ ส่วนการข่มขืนใจให้จ่ายอมต่อสิ่งใด ๆ หมายความว่า การข่มขืนใจไม่ให้ขัดขืนต่อการกระทำของผู้กระทำหรือของคนที่สาม

2. โดยทำให้กลัวว่าจะทำให้เกิดอันตรายต่อชีวิต ร่างกาย เสรีภาพ ชื่อเสียงหรือทรัพย์สินของผู้ถูกรุ้มนั้น หรือของผู้อื่น หรือโดยใช้กำลังประทุษร้าย การทำให้กลัวนั้นไม่ได้มีการจำกัดวิธีไว้ อาจทำได้ด้วยวาจา หนังสือหรือท่าทาง และการขู่เช่นนั้นจะเป็นการขู่ว่าจะทำอันตรายในปัจจุบัน หรือในอนาคตก็ได้ แต่ข้อสำคัญอยู่ที่การทำให้เขากลัวว่าจะเกิดอันตรายต่อเขา และแม้ว่าอันตรายที่ขู่จะมีอยู่จริงหรือไม่คิดจะทำตามที่ขู่จริง ๆ ก็ไม่สำคัญ ความสำคัญอยู่ที่การขู่ นั้นเป็นตัวการทำให้ผู้ที่ถูกขู่กลัวก็พอ¹

การทำให้กลัวว่าจะเกิดอันตรายต่อชีวิตคือทำให้กลัวว่าจะต้องตาย อันตรายแก่ร่างกายคือได้รับบาดเจ็บ อันตรายแก่เสรีภาพคือถูกจับถูกกักขัง ถูกห้ามพูดห้ามเขียน อันตรายแก่ชื่อเสียงคือถูกเปิดเผยความลับทำให้เสียชื่อเสียง หรืออันตรายแก่ทรัพย์สิน เช่น ถูกขู่ว่าจะเผาบ้าน หรือทำลายข้าวของ เป็นต้น ส่วนการข่มขืนใจผู้อื่นโดยใช้กำลังประทุษร้าย เช่น ทำร้ายเขาแล้วห้ามไม่ให้ทำหรือบังคับให้เขาทำ เป็นต้น

3. จนผู้ถูกรุ้มนั้นใจต้องกระทำการนั้น ไม่กระทำการนั้น หรือจำยอมต่อสิ่งนั้น

การทำให้กลัวนั้นจะทำให้เกิดความกลัวขึ้นทันทีหรือภายหลังที่ผู้ถูกรุ้มนั้นใจได้ไตร่ตรองไปบ้างแล้วก็ไม่เป็นข้อสำคัญ ความผิดสำเร็จเมื่อมีความกลัวเกิดขึ้นจนผู้ถูกรุ้มนั้นใจกระทำ ไม่กระทำ หรือจำยอมให้กระทำการตามที่ถูกรุ้มนั้นใจ

การทำให้กลัว เป็นการลงมือกระทำความผิดแล้ว ฉะนั้น ถ้าทำให้เขากลัวแล้วเขาไม่กลัว จึงไม่ยอมกระทำ ไม่ยอมที่จะไม่กระทำหรือไม่ยอมต่อสิ่งใด ๆ ตามที่ขู่ ผู้กระทำก็มีความผิดฐานพยายามตามมาตรา 80²

ความผิดตามมาตรานี้ต้องปรากฏว่าผู้กระทำไม่มีอำนาจกระทำได้ ดังนั้นถ้าเป็นการขู่ว่าจะทำตามสิทธิหรือทำตามอำนาจกฎหมายไม่ถือเป็นการขู่³

ส่วนขององค์ประกอบภายใน คือ เจตนาธรรมดา กล่าวคือ ผู้กระทำจะต้องทราบว่าการกระทำของตนเป็นการทำให้กลัวว่าจะเกิดอันตรายหรือการใช้กำลังประทุษร้าย และผู้กระทำประสงค์จะให้การกระทำดังกล่าวเป็นเหตุให้ผู้ถูกรุ้มนั้นใจกระทำ ไม่กระทำหรือจำยอมต่อสิ่งใด ๆ ตามที่ตนข่มขืนใจ หรือมิฉะนั้นย่อมเห็นได้ว่า ผู้ถูกรุ้มนั้นใจจะกระทำ ไม่กระทำหรือจำยอม

¹ ทวีเกียรติ มีนะกนิษฐ, คำอธิบายกฎหมายอาญาภาคความผิดและโทษ, พิมพ์ครั้งที่ 4 (กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2551), น. 264-267.

² หยุต แสงอุทัย, กฎหมายอาญา ภาค 2-3, พิมพ์ครั้งที่ 10 (กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2544), น. 220-224.

³ ทวีเกียรติ มีนะกนิษฐ, อ้างแล้ว เชิงอรรถที่ 1

ต่อสิ่งนั้น ๆ ถ้าผู้กระทำมีเจตนาเพียงล้อเล่น แต่ผู้ถูกข่มขืนใจสำคัญผิดว่าเป็นความจริง ผู้กระทำก็
ไม่มีความผิด⁴

ส่วนเหตุเพิ่มโทษมีดังนี้คือ ถ้าได้กระทำโดยมีอาวุธ หรือโดยร่วมกระทำความผิดด้วยกัน
ตั้งแต่ห้าคนขึ้นไป หรือโดยมีมูลเหตุชักจูงใจเพื่อให้ผู้ถูกข่มขืนใจทำ ถอน ทำให้เสียหาย หรือ
ทำลายเอกสารสิทธิอย่างใด ต้องระวางโทษหนักขึ้น

และผู้กระทำต้องรับโทษสูงขึ้นอีกถ้าได้กระทำโดยอ้างอำนาจอัยย์หรือช่องโหว่ ไม่ว่าจะอัยย์
หรือช่องโหว่นั้นจะมีอยู่หรือไม่

ส่วนโทษของมาตรานี้คือ ระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือ
ทั้งจำทั้งปรับ

เมื่อพิจารณาจากบทบัญญัติของมาตรา 309 แล้วจะเห็นได้ว่ามาตรานี้ไม่สามารถที่จะ
นำมาใช้บังคับกับการกระทำที่มีลักษณะของการข่มขู่ทางอินเทอร์เน็ตได้กล่าวคือ การข่มขู่ทาง
อินเทอร์เน็ตนั้นมีการกระทำอันเป็นการข่มขู่ แต่ไม่เข้าลักษณะของการข่มขืนใจให้กระทำการใด
ไม่กระทำการใด หรือจ่ายอมต่อสิ่งใด เมื่อขาดองค์ประกอบในส่วนนี้การข่มขู่ทางอินเทอร์เน็ตจึง
ไม่เป็นการกระทำความผิดตามมาตรา 309

4.1.1.2 ความผิดตามประมวลกฎหมายอาญามาตรา 392

การกระทำของผู้ใดจะเป็นการกระทำความผิดตามมาตรา 392 ได้นั้น ผู้กระทำต้องได้
กระทำการครบทั้งองค์ประกอบภายนอกและภายในตามที่กฎหมายมาตรานี้บัญญัติไว้ ดังนี้

องค์ประกอบภายนอก

1. ทำให้เกิดความกลัวหรือความตกใจ
2. โดยการขู่เข็ญ

ขู่เข็ญ คือ การแสดงว่าจะทำให้เกิดภัยแก่เขาซึ่งจะเป็นภัยที่เกิดขึ้นในทันทีหรือต่อไปใน
ภายหน้าก็ได้

ส่วนองค์ประกอบภายใน คือ เจตนารมณ์ คือเจตนาทำให้เกิดความกลัวหรือความ
ตกใจ ดังนั้นเพียงขู่เข็ญก็ผิดแล้ว

ความผิดตามมาตรานี้เป็นความผิดที่ต้องการผลซึ่งก็คือความกลัวหรือความตกใจ และ
เนื่องจากความผิดฐานนี้เป็นความผิดลหุโทษ ซึ่งมาตรา 105 บัญญัติว่า “ผู้ใดพยายามกระทำ

⁴ หยุด แสงอุทัย, อ้างแล้ว เชิงอรรถที่ 2

ความผิดลหุโทษ ผู้นั้นไม่ต้องรับโทษ” ดังนั้นจึงไม่มีการพยายามกระทำความผิดสำหรับความผิดฐานนี้ ดังนั้นในกรณีที่เกิดจึงไม่ต้องวินิจฉัยความผิดฐานนี้⁵

ส่วนโทษของมาตรานี้ คือ ระวังโทษจำคุกไม่เกินหนึ่งเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ

เมื่อพิจารณาจากบทบัญญัติของมาตรา 392 แล้วจะเห็นได้ว่ามาตรานี้สามารถที่จะนำมาใช้บังคับกับการกระทำที่มีลักษณะของการข่มขู่ทางอินเทอร์เน็ตได้กล่าวคือ การข่มขู่ทางอินเทอร์เน็ตนั้นมีการกระทำความผิดอันเป็นการข่มขู่ที่มีเจตนาให้ผู้ถูกข่มขู่เกิดความกลัว จึงเข้าองค์ประกอบทั้งภายนอกและภายในของมาตรา 392

จากการพิจารณามาตรา 309 และ มาตรา 392 ทำให้ทราบว่า มีเพียงบทบัญญัติมาตรา 392 เท่านั้นที่ใช้กับการข่มขู่ทางอินเทอร์เน็ตได้โดยตรง แต่เนื่องจากมาตรา 392 นั้นเป็นความผิดลหุโทษ จึงอาจมีปัญหาในเรื่องการนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ต กล่าวคือ

1. มาตรา 392 เป็นความผิดลหุโทษจึงไม่ได้มีการบัญญัติในเรื่องของการกระทำโดยมีเหตุฉกรรจ์เอาไว้ ซึ่งต่างจากบทบัญญัติในมาตรา 309 วรรคสองและวรรคสามที่มีการบัญญัติในเรื่องของเหตุฉกรรจ์ มีการเพิ่มโทษแก่ผู้กระทำความผิด
2. มาตรา 392 เป็นความผิดลหุโทษ ดังนั้นจึงไม่มีการพยายามกระทำความผิดสำหรับความผิดฐานนี้

4.1.2 บทบัญญัติในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

เมื่อพิจารณาถึงลักษณะของการข่มขู่ทางอินเทอร์เน็ตดังที่ได้กล่าวมาแล้วนั้น บทบัญญัติในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่อาจนำมาปรับใช้เกี่ยวกับกับการข่มขู่ทางอินเทอร์เน็ตมี ดังนี้คือ มาตรา 11 , มาตรา 14(1) , มาตรา 14(4) มาตรา 15 มาตรา 16 และมาตรา 17

4.1.2.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 11

⁵ คณิต ณ นคร, กฎหมายอาญาภาคความผิด, พิมพ์ครั้งที่ 8 (กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2545), น. 88-89.

บทบัญญัติมาตรา 11 ใช้กับการส่งข้อมูลคอมพิวเตอร์รบกวนการใช้คอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

มาตรา 11 บัญญัติว่า “ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท”

ความผิดตามมาตรา 11 นี้ คณะกรรมาธิการในการร่างกฎหมายได้เพิ่มเติมขึ้นมาใหม่เป็นการบัญญัติเอาผิดแก่การกระทำที่ไม่ถึงกับทำให้ระบบคอมพิวเตอร์ของบุคคลอื่นไม่สามารถทำงานตามปกติได้ แต่เป็นการทำให้เกิดการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข เช่นส่ง e-mail มากจนล้นระบบคอมพิวเตอร์ของบุคคลอื่นจนทำให้เกิดความยุ่งยากในการใช้ระบบคอมพิวเตอร์ของเขา ภาษาอังกฤษเรียกว่า “spamming”⁶

องค์ประกอบความผิดของมาตรานี้คือ

1. ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ความจริงแล้ว “จดหมายอิเล็กทรอนิกส์” หรือ e-mail ก็อยู่ในความหมายของ “ข้อมูลอิเล็กทรอนิกส์” อยู่แล้วตามนิยามศัพท์ แต่ที่มีการบัญญัติไว้โดยเฉพาะนั้นก็เพื่อให้เข้าใจในความหมายขององค์ประกอบความผิดฐานนี้
2. โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูล องค์ประกอบความผิดนี้สำคัญมากเพราะไม่ใช่เรื่อง “โดยมิชอบ” เหมือนกับความผิดตามมาตราอื่นๆ ในพระราชบัญญัตินี้ แต่เป็นเรื่องปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูล

การปกปิดหรือปลอมแปลงนี้ต้องเป็นเรื่องของ “แหล่งที่มาของการส่งข้อมูล” ซึ่งตรวจสอบได้โดย “ข้อมูลจราจรทางคอมพิวเตอร์” ได้แก่การปกปิดหรือปลอมแปลง IP address⁷ และหมายถึงการกระทำที่ทำให้ไม่สามารถตรวจสอบถึงแหล่งที่มาของการส่งข้อมูลและส่งผลให้ไม่อาจ

⁶ พรเพชร วิชิตชลชัย, คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 น. 16.

<http://www.etcommission.go.th/documents/laws/mnote/cc_act_exp.pdf>

⁷ IP Address หรือเลขที่อยู่ไอพี คือเลขที่อยู่อินเทอร์เน็ตโปรโตคอล เป็นเลขที่อยู่ซึ่งเป็นตัวเลขเฉพาะที่ใช้กับคอมพิวเตอร์ทางอินเทอร์เน็ต IP Address จะเป็นชุดของตัวเลขสี่ตัว แต่ละชุดจะอยู่ในช่วง 0-255 แยกจากกันโดยใช้จุด (เช่น 121.56.97.178) คอมพิวเตอร์ทุกตัวที่เชื่อมต่อกับคอมพิวเตอร์อินเทอร์เน็ตจะได้รับ IP Address เพื่อช่วยให้การส่งทางอินเทอร์เน็ต จาก หรือถึงคอมพิวเตอร์จากจุดหนึ่งไปยังจุดหมายปลายทางทำได้ถูกต้อง ผู้ให้บริการอินเทอร์เน็ตส่วนใหญ่จะเป็นผู้ควบคุม IP Address

ตรวจสอบได้ทางระบบข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น ไม่ใช่กรณีการปกปิดหรือปลอมแปลงโดยการไม่ใช่ชื่อจริง หรือการเปลี่ยนแปลงใช้ชื่อหรือใช้นามแฝง หรือใช้ email-address ที่ผิดไปหรือเปลี่ยนแปลงไปซึ่งยังตรวจสอบแหล่งที่มาของการส่งข้อมูลได้อยู่

3. อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข การรบกวนน่าจะมีความรุนแรงของการรบกวนพอสมควร และให้ใช้มาตรฐานของวิญญูชนเป็นระดับในการวัด⁸

ส่วนโทษของมาตรานี้คือ ระวังโทษปรับไม่เกินหนึ่งแสนบาท ส่วนโทษจำคุกนั้นไม่มี

เมื่อพิจารณาบทบัญญัตินี้กับการข่มขู่ทางอินเทอร์เน็ต จะพบว่ามืองค์ประกอบตรงกันในเรื่องของการส่งอีเมลไปยังผู้อื่นเท่านั้น แต่การข่มขู่ทางอินเทอร์เน็ตจะไม่ตรงกับองค์ประกอบของมาตรานี้ในเรื่องของการส่งอีเมลโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวกับการส่งโดยมีเจตนารบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข กล่าวคือการข่มขู่ทางอินเทอร์เน็ตที่ใช้อีเมลเป็นเครื่องมือในการกระทำความผิด เป็นการส่งโดยมีเจตนาที่จะข่มขู่ รังควานผู้รับอีเมลดังกล่าวให้เกิดความหวาดกลัวจากถ้อยคำที่ถูกส่งมากับอีเมลดังกล่าว แต่การส่งอีเมลตามมาตรา 11 นี้ มีเจตนาในการส่งเพื่อบกพรอนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุขเท่านั้น เมื่อเจตนาและองค์ประกอบของความผิดในการส่งอีเมลต่างกัน การข่มขู่ทางอินเทอร์เน็ตจึงไม่เป็นการกระทำความผิดตามมาตรา 11 ดังนั้นจึงไม่สามารถนำมาตรานี้มาบังคับใช้กับการข่มขู่ผ่านทางอีเมลได้

4.1.2.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14 (1)

มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

ความผิดตามมาตรา 14 (1) มืองค์ประกอบความผิด ดังนี้⁹

1. นำเข้าสู่ระบบคอมพิวเตอร์

การนำเข้าสู่ หมายถึงการนำข้อมูลคอมพิวเตอร์หรือโปรแกรมซอฟต์แวร์ต่างๆ เข้าสู่ระบบคอมพิวเตอร์

2. ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ

⁸ พรเพชร วิชิตชลชัย, อ่างแล้ว เชิงอรรถที่ 6

⁹ เฟิงอ้าง, น. 21-22.

ข้อมูลคอมพิวเตอร์ปลอม หมายถึงข้อมูลคอมพิวเตอร์ที่มีการเปลี่ยนแปลงแก้ไข ไม่ว่าจะการเปลี่ยนแปลงแก้ไขนั้นจะทั้งหมดหรือแต่เพียงบางส่วน ส่วนข้อมูลคอมพิวเตอร์เป็นเท็จนั้น น่าจะหมายถึงข้อมูลคอมพิวเตอร์ที่ไม่ใช่ของจริง

มาตรา 3 บัญญัติว่า “ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย“

ดังนั้น “ข้อมูลคอมพิวเตอร์” จึงหมายถึงข้อมูลทุกอย่างที่อยู่ในระบบคอมพิวเตอร์ รวมทั้งชุดคำสั่งด้วยหากอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ ส่วนที่บัญญัติให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์¹⁰ ด้วยนั้นก็เพื่อให้ครอบคลุมถึงข้อมูลประเภทอื่น ๆ ที่อาจสร้างด้วยวิธีการทางอิเล็กทรอนิกส์อื่น ๆ ในอนาคตที่ไม่ใช่เทคโนโลยีคอมพิวเตอร์ก็ได้

3. โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

องค์ประกอบนี้ไม่ใช่เจตนาพิเศษของผู้กระทำ แต่เป็นเรื่องที่จะต้องพิจารณาจากลักษณะของการกระทำในเรื่องของเจตนาด้วย

4. เจตนาตามประมวลกฎหมายอาญา มาตรา 59

เจตนาในที่นี้ต้องครอบคลุมองค์ประกอบทั้งสามประการข้างต้น กล่าวคือผู้กระทำต้องมีเจตนานำเข้าสู่ระบบคอมพิวเตอร์ ในขณะที่เดียวกันผู้กระทำต้องรู้ถึงข้อเท็จจริงในองค์ประกอบความผิดว่าเป็นข้อมูลคอมพิวเตอร์ปลอมหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จและต้องรู้ว่าการกระทำดังกล่าวเป็นการกระทำที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

มาตรา 14 (1) อาจนำมาปรับใช้กับการส่งอีเมลล์หรือการสื่อสารทางอิเล็กทรอนิกส์ถึงบุคคลอื่นโดยรู้ว่าข้อความนั้นเป็นเท็จ กล่าวคือ ผู้กระทำได้มีการส่งข้อความเท็จที่ถือว่าเป็นข้อมูลทางอิเล็กทรอนิกส์ผ่านทางอินเทอร์เน็ตโดยรู้ว่าข้อความที่ส่งนั้นน่าจะเกิดความเสียหายแก่เหยื่อ

¹⁰ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 “ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

4.1.2.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.2550 มาตรา 14 (4)

มาตรา 14 (4) “นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้”

ความผิดตามมาตรา 14 (4) มีองค์ประกอบความผิด ดังนี้¹¹

- (1) นำเข้าสู่ระบบคอมพิวเตอร์
- (2) ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

องค์ประกอบความผิดข้อนี้พิจารณาจากลักษณะของข้อมูลคอมพิวเตอร์เช่นกัน คือเป็นข้อมูลคอมพิวเตอร์ที่มีลักษณะอันลามก

คำว่า “ลามก” เป็นคำสามัญที่ไม่มีการนิยามศัพท์ แต่เป็นคำที่ใช้เป็นองค์ประกอบความผิดตามประมวลกฎหมายอาญา มาตรา 287 ซึ่งเป็นความผิดฐานเผยแพร่วัตถุอันลามก ดังนั้นข้อมูลคอมพิวเตอร์ใดจะเข้าองค์ประกอบความผิด “ลามก” หรือไม่ จึงใช้มาตรฐานเดียวกันกับความผิดตามประมวลกฎหมายอาญามาตรา 287 ดังกล่าว

- (3) ข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

การจะเป็นความผิดตามมาตรา 14 (4) นอกจากข้อมูลคอมพิวเตอร์นั้นมีลักษณะอันลามกแล้ว ยังต้องเป็นข้อมูลคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้อีกด้วย

มาตรานี้อาจนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ตได้ในบางกรณี เช่น ผู้กระทำได้สร้างเว็บไซต์ที่บุคคลใด ๆ ก็เปิดเข้าดูได้ โดยได้ลงภาพเปลือยของผู้หญิงคนหนึ่ง พร้อมชื่อที่อยู่ เบอร์โทรศัพท์ ของเหยื่อเอาไว้ แล้วลงข้อความเชิญชวนให้คนที่เข้าเว็บไซต์ติดต่อหรือไปหาเหยื่อ การกระทำได้กล่าวของผู้กระทำนั้นถือว่าเป็นการรังควานเหยื่อ หรืออาจเป็นการจู่โจมให้บุคคลอื่นกระทำการอันเป็นการละเมิดกฎหมายต่อเหยื่อก็ได้

ในกรณีตามตัวอย่างนั้น แม้จะดำเนินคดีเอาผิดกับผู้กระทำได้ แต่ความผิดดังกล่าวก็มาจากที่กฎหมายต้องการเอาผิดกับผู้ที่น่าภาพลามกเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปเข้าถึงได้ ไม่ได้มีเจตนารมณ์ที่จะเอาผิดกับผู้กระทำที่มีเจตนาอื่นอยู่เบื้องหลังการกระทำได้ ดังนั้น แม้จะปรับใช้กับการกระทำบางประการได้ แต่ก็ไม่สามารถยับยั้งผู้ที่มีเจตนาจะกระทำการข่มขู่ทางอินเทอร์เน็ตได้ เพราะผู้ใดคิดจะกระทำได้เสี่ยงไปใช้วิธีอื่นที่ไม่เป็นความผิดตามมาตรานี้ก็ได้อีก

¹¹ พรเพชร วิชิตชลชัย, อ้างแล้ว เจริญธรรมที่ 6, น. 23-24.

4.1.2.4 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
มาตรา 15

มาตรา 15 “ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตาม
มาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำ
ความผิดตามมาตรา 14”

มาตรา 15 เป็นการเอาผิดกับ “ผู้ให้บริการ” มีองค์ประกอบความผิด ดังนี้¹²

(1) ผู้ให้บริการ

ผู้ที่จะมีความผิดตามมาตรา 15 ต้องเป็น “ผู้ให้บริการ” ซึ่งมีนิยามศัพท์ไว้ในมาตรา 3 ผู้
ให้บริการจึงหมายถึงผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ตหรือให้สามารถติดต่อถึงกัน
โดยประการอื่นโดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ไม่ว่าจะเป็นการให้บริการในนามของตนเอง
หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น และยังหมายความรวมถึงผู้ให้บริการเก็บรักษา
ข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

(2) จงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14

บทบัญญัติมาตรานี้ใช้ถ้อยคำ “จงใจ” ซึ่งเป็นคำที่เพิ่มขึ้นมาจาก “เจตนา” โดยมี
เจตนารมณ์ที่จะเน้นให้เห็นว่า “จงใจ” นั้นหมายถึงต้องรู้ว่ามีกระทำความผิดตามมาตรา 14
เช่น มีการเตือนหรือแจ้งให้ทราบแล้วว่าข้อมูลคอมพิวเตอร์นั้นเป็นความผิดต่อกฎหมายตาม
บทบัญญัติมาตรา 14 เมื่อผู้ให้บริการยังปล่อยให้มีการเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็น
ความผิดในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ก็จะได้ถือว่าเป็นการจงใจสนับสนุน
หรือยินยอมให้มีการกระทำความผิด

(3) ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

ข้อนี้เป็นเรื่องที่ยกกฎหมายบัญญัติเอาผิดเฉพาะผู้ให้บริการที่กระทำความผิดในระบบ
คอมพิวเตอร์ที่อยู่ในความควบคุมของตนเท่านั้น

มาตรานี้สามารถนำมาปรับใช้ในกรณีที่มีบุคคลได้กระทำการอันเป็นการข่มขู่ทาง
อินเทอร์เน็ต แล้วการกระทำดังกล่าวเป็นความผิดตามมาตรา 14 แล้วเหยื่อหรือบุคคลใดก็ตาม
แจ้งผู้ให้บริการได้รู้ถึงการกระทำดังกล่าว แต่ผู้ให้บริการก็ไม่ได้ดำเนินการจัดการปล่อยให้มีการ
กระทำความผิดต่อไป ผู้ให้บริการก็จะมีผิดตามมาตรา 15

¹² เฟิงอ้วง, น. 25-26.

4.1.2.5 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

มาตรา 16

มาตรา 16 “ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย”

ความผิดตามมาตรา 16 นี้เป็นลักษณะของการดูหมิ่นหรือหมิ่นประมาทด้วยการตกแต่งภาพของบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด มีองค์ประกอบความผิด ดังนี้¹³

1. นำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้

หมายความว่า ผู้กระทำได้มีการกระทำอันเป็นการนำข้อมูลคอมพิวเตอร์เข้าสู่ระบบคอมพิวเตอร์ และระบบคอมพิวเตอร์นั้นเป็นระบบที่ประชาชนทั่วไปอาจเข้าถึงได้ ถ้าเป็นระบบคอมพิวเตอร์ของตนเองก็ไม่เป็นความผิด

2. ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด

องค์ประกอบความผิดข้อนี้ต้องเป็นข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น หมายถึงการแสดงผลข้อมูลคอมพิวเตอร์นั้นออกเป็นภาพของบุคคล และภาพนั้นอาจเกิดจากการสร้างขึ้นใหม่ หรือเป็นภาพที่มีอยู่แต่ได้มีการตัดต่อ เติมหรือดัดแปลง ซึ่งเป็นการทำด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด

คำว่า “วิธีการอื่นใด” ได้บัญญัติไว้เพื่อให้ครอบคลุมการเปลี่ยนแปลงแก้ไขข้อมูลคอมพิวเตอร์ที่เป็นภาพบุคคลนั้นด้วยวิธีการใดๆ ก็ได้ซึ่งจะมีผลทำให้เกิดการเปลี่ยนแปลงต่อข้อมูลคอมพิวเตอร์

3. โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

¹³ เฟิ่งอ้วง, น. 27.

องค์ประกอบความผิดข้อนี้ใช้ข้อความทำนองเดียวกับความผิดฐานหมิ่นประมาทตาม ประมวลกฎหมายอาญา มาตรา 326 แต่เพิ่มคำว่า “ได้รับความอับอาย” เข้าไปด้วย จึงมี ความหมายกว้างกว่าความผิดฐานหมิ่นประมาท

4. เจตนาตามประมวลกฎหมายอาญา มาตรา 59 หมายถึงเจตนาในการนำภาพบุคคลเข้าสู่ ระบบคอมพิวเตอร์

อย่างไรก็ดี ถ้าเป็นการนำเข้าสู่ข้อมูลคอมพิวเตอร์โดยสุจริตจะไม่ถือว่าเป็นความผิด

นอกจากนี้ ความผิดตามมาตรา 17 ยังเป็นความผิดอันยอมความได้ เนื่องจากเห็นได้ ชัดเจนว่าความเสียหายที่เกิดขึ้นนั้นเป็นความเสียหายเฉพาะบุคคล

บทบัญญัตินี้อาจนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ตได้ในกรณีของการสร้างและ ดำเนินการจัดการเว็บไซต์ที่รังควานผู้อื่น เช่น ผู้กระทำได้สร้างเว็บไซต์ขึ้นมาและได้นำภาพของเหยื่อที่ได้นำไปติดต่อกับภาพของผู้ที่เป็นโรคติดต่อร้ายแรง จนดูเหมือนเหยื่อกำลังเป็นโรคติดต่อ ร้ายแรง มาลงในเว็บไซต์ดังกล่าว เพื่อให้เหยื่อได้รับความอับอาย

จากการพิจารณาบทบัญญัติที่กล่าวมานั้น ทำให้ทราบว่าพระราชบัญญัติว่าด้วยการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์บางมาตราสามารถนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ต ได้ ถ้าการกระทำของผู้กระทำครบองค์ประกอบของความผิดตามที่ได้บัญญัติไว้

4.1.2.6 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 17

มาตรา 17 ไม่ใช่มาตราที่กำหนดฐานความผิดแต่อย่างใดแต่เป็นมาตราที่บัญญัติขึ้นเพื่อ ตอบสนองปัญหาเรื่องหลักดินแดน กล่าวคือ ลักษณะของการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ส่วนใหญ่นั้นจะมีผลเกิดขึ้นโดยไม่มีเขตแดน (borderless) โดยเฉพาะที่เกี่ยวข้องกับ การส่งข้อมูลคอมพิวเตอร์ ซึ่งไม่ว่าจะส่ง ณ ที่แห่งใดในโลกก็จะส่งผลที่สามารถเปิดระบบ คอมพิวเตอร์ได้ทั่วโลก จึงถือว่าเป็นอาชญากรรมที่ไร้พรมแดน¹⁴

การข่มขู่ทางอินเทอร์เน็ตเช่นเดียวกัน กล่าวคือ การข่มขู่ทางอินเทอร์เน็ตนั้นผู้กระทำจะ ข่มขู่ผ่านทางอีเมลหรือสื่อสารผ่านทางอิเล็กทรอนิกส์ หรือสร้างเว็บไซต์ขึ้นเพื่อใช้ในการข่มขู่ รังควาน การข่มขู่โดยวิธีการเช่นว่านั้น ผู้กระทำอาจอยู่ไกลจากผู้ถูกข่มขู่หลายพันไมล์ เช่น อยู่คน ละประเทศ หรือคนละทวีปก็ได้ จึงมีปัญหว่า ถ้าผู้ถูกข่มขู่อยู่ในประเทศไทย แต่ผู้ที่กระทำการ ข่มขู่อยู่ที่ประเทศสหรัฐอเมริกา จะดำเนินการฟ้องร้อง นำตัวผู้กระทำความผิดมารับโทษ หรือ จัดการกับผู้กระทำผิดอย่างไร

¹⁴ เฟิงอ้าง, น. 29.

พิจารณาได้ว่า การกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้นเป็นบทบัญญัติความผิดที่มีโทษทางอาญา ดังนั้นจึงต้องนำหลักกฎหมายความรับผิดในเรื่องหลักดินแดนตามที่บัญญัติไว้ในประมวลกฎหมายอาญามาใช้ด้วย ดังนี้

มาตรา 5 “ความผิดใดที่การกระทำแม้แต่ส่วนหนึ่งส่วนใดได้กระทำ ในราชอาณาจักรก็ดี ผลแห่งการกระทำเกิดในราชอาณาจักรโดยผู้กระทำประสงค์ให้ผลนั้นเกิดในราชอาณาจักร หรือโดยลักษณะแห่งการกระทำ ผลที่เกิดขึ้นควรเกิดในราชอาณาจักรหรือย่อมจะเล็งเห็นได้ว่าผลนั้นจะเกิดในราชอาณาจักรก็ดี ให้ถือว่าความผิดนั้นได้กระทำในราชอาณาจักร

ในกรณีการเตรียมการ หรือพยายามกระทำการใดซึ่งกฎหมายบัญญัติเป็นความผิด แม้การกระทำนั้นจะได้กระทำนอกราชอาณาจักร ถ้าหากการกระทำนั้นจะได้กระทำตลอดไปจนถึงขั้นความผิดสำเร็จ ผลจะเกิดขึ้นในราชอาณาจักร ให้ถือว่าการเตรียมการหรือพยายามกระทำความผิดนั้นได้กระทำในราชอาณาจักร”

ดังนั้น การกระทำความผิดเกี่ยวกับคอมพิวเตอร์โดยเฉพาะที่เกี่ยวกับข้อมูลคอมพิวเตอร์ไม่ว่าจะเป็นการเข้าถึง การเข้าแทรกแซง ทำลาย การนำเข้าสู่ระบบคอมพิวเตอร์ การเผยแพร่จนถึงแม้ว่าจะไม่ได้กระทำในประเทศไทย แต่ถ้าผลที่เกิดขึ้น คือผู้รับข้อมูลสามารถเปิดรับข้อมูลคอมพิวเตอร์นั้นในประเทศไทยได้ย่อมถือว่าผลแห่งการกระทำเกิดในประเทศไทย และถือว่าความผิดนั้นได้กระทำในประเทศไทยด้วย

เช่นเดียวกับกรณีที่มีการเตรียมการหรือความพยายามกระทำการใดๆ ที่พระราชบัญญัตินี้บัญญัติไว้เป็นความผิด แม้การเตรียมการหรือการพยายามนั้นจะได้กระทำนอกประเทศไทยแต่ถ้าหากกระทำไปตลอดแล้วผลจะเกิดในประเทศไทย ก็ถือว่าการเตรียมการหรือพยายามกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้กระทำในประเทศไทย

ดังที่ได้กล่าวมาแล้วว่าลักษณะของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ส่วนใหญ่ไม่ว่าจะกระทำ ณ ที่ใดในโลกก็มักจะเกิดผลในประเทศไทยด้วย ดังนั้นการส่งข้อมูลคอมพิวเตอร์ที่เป็นความผิดถึงแม้จะกระทำที่ประเทศอื่นแต่ผลของข้อมูลเกิดขึ้นในประเทศไทยก็ให้หลักตามประมวลกฎหมายอาญา มาตรา 6 ได้

นอกจากจะนำเรื่องหลักดินแดนในประมวลกฎหมายอาญามาใช้แล้ว พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ยังได้บัญญัติมาตรา 17 ขึ้น ดังนี้

มาตรา 17 “ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(1) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ

จะต้องรับโทษภายในราชอาณาจักร”

ดังนั้น ถ้ามาตราใดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 สามารถนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ตได้ และผู้ที่กระทำความผิดเป็นคนต่างด้าว แล้วผู้ที่ถูกข่มขู่คือคนไทย แล้วคนไทยได้มีการร้องขอให้ลงโทษ ผู้กระทำความผิดที่เป็นคนต่างด้าวจะต้องรับโทษในประเทศไทย

4.2 โทษสำหรับการกระทำความผิดฐานข่มขู่ทางอินเทอร์เน็ต

ประมวลกฎหมายอาญามาตรา 392 ได้กำหนดโทษสำหรับผู้กระทำความผิดไว้ดังนี้คือ “ระวางโทษจำคุกไม่เกินหนึ่งเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ” ส่วนพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14 (1) และ (4) ได้กำหนดโทษไว้ที่ “ระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ” ส่วนมาตรา 16 กำหนดว่า “ระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ” จึงพิจารณาได้ว่าบทบัญญัติของกฎหมายไทยที่สามารถนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ตได้โดยตรงอย่าง มาตรา 392 ของประมวลกฎหมายอาญานั้น กำหนดอัตราโทษไว้ต่ำมาก เนื่องจากเป็นเพียงความผิดลหุโทษเท่านั้น ส่วนบทบัญญัติในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14(1) , (4) และ 16 นั้นแม้ว่าจะมีการกำหนดอัตราโทษไว้ไม่ต่ำมาก แต่เนื่องจากมาตราทั้งสองอาจนำมาปรับใช้ได้ในบางกรณีเท่านั้น ผู้กระทำการข่มขู่ทางอินเทอร์เน็ตอาจใช้วิธีอื่นทำให้ไม่เป็นการกระทำความผิดตามที่ได้บัญญัติไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ก็ได้ เมื่อเป็นเช่นนี้ อัตราโทษตามมาตรา 392 ของประมวลกฎหมายอาญาจึงอาจไม่น่ากลัวพอสำหรับผู้ที่จะกระทำความผิดก็ได้

การที่กฎหมายที่มีอยู่และอาจนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ตได้โดยตรงมีอัตราโทษที่ค่อนข้างเบา ย่อมส่งผลให้ไม่สามารถยับยั้งหรือการป้องปรามบุคคลไม่ให้มีการกระทำการอันเป็นการข่มขู่ทางอินเทอร์เน็ตได้

4.3 มาตรการอื่น ๆ ที่อาจนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ต

เนื่องจากโทษที่กำหนดเอาไว้ในความผิดมาตราต่าง ๆ อาจจะไม่เพียงพอที่จะปกป้องคุ้มครองเหยื่อได้ หรือไม่อาจยับยั้งบุคคลไม่ให้กระทำการอันเป็นความผิดได้ เพราะมีอัตราโทษที่ไม่เหมาะสม การมีมาตรการอื่น ๆ มาใช้บังคับแก่กรณีดังกล่าวจึงเป็นการเพิ่มประสิทธิภาพในการให้ความคุ้มครองเหยื่อและหยุดหรือยับยั้งผู้กระทำไม่ให้กระทำการได้ มาตรการอื่น ๆ ที่อาจนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ตได้ เช่น การใช้วิธีการเพื่อความปลอดภัย มาตรการรอกอกลงโทษโดยมีการกำหนดเงื่อนไขในการคุมประพฤติ และมาตรการในการได้มาซึ่งพยานหลักฐาน

4.3.1 การใช้วิธีการเพื่อความปลอดภัย

วิธีการเพื่อความปลอดภัย หมายถึง วิธีการเพื่อให้สังคมปลอดภัยจากการกระทำความผิดของผู้กระทำความผิดในเวลาภายหลัง หรือเป็นวิธีการเพื่อความปลอดภัยเพื่อปฏิบัติต่อผู้ที่น่าจะกระทำความผิดขึ้นในอนาคต หรือเป็นวิธีการเพื่อให้สังคมปลอดภัยจากการกระทำความผิดซึ่งอาจเกิดขึ้นในอนาคตของผู้กระทำ¹⁵ ดังนั้น วิธีการเพื่อความปลอดภัยจึงเป็นมาตรการทางกฎหมายที่นำมาใช้เพื่อสนับสนุนการปรับปรุงแก้ไขตัวบุคคลที่มีลักษณะอันตรายเมื่อวิธีการลงโทษทางอาญาไม่ได้ผลเพียงพอ และเนื่องจากวิธีการเพื่อความปลอดภัยไม่ใช่โทษจึงสามารถนำมาใช้ได้อย่างกว้างขวาง และผู้ถูกใช้วิธีการนี้ก็ไม่ถือว่าได้รับโทษหรือถูกตัดสิทธิใดๆ¹⁶

ประมวลกฎหมายอาญา มาตรา 39 กำหนดวิธีการเพื่อความปลอดภัยไว้ 5 ประการ คือ กักกัน ห้ามเข้าเขตกำหนด เรียกประกันทัณฑ์บน คุมตัวไว้ในสถานพยาบาล ห้ามการประกอบอาชีพบางอย่าง

¹⁵ คณิต ณ นคร, กฎหมายอาญาภาคทั่วไป, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2547), น. 400.

¹⁶ ทวีเกียรติ มินะกนิษฐ, คำอธิบายกฎหมายอาญาภาคทั่วไป, พิมพ์ครั้งที่ 9 (กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2551), น. 243-244.

4.3.1.1 การกักกัน

มาตรา 40 แห่งประมวลกฎหมายอาญาบัญญัติว่า “กักกัน คือ การควบคุมผู้กระทำความผิดติดนิสัยไว้ในเขตกำหนดเพื่อป้องกันการกระทำความผิด เพื่อตัดนิสัย และเพื่อฝึกหัดอาชีพ”

จากบทบัญญัติข้างต้นพิจารณาได้ว่าการกักกันไม่สามารถนำมาปรับใช้กับผู้กระทำการข่มขู่ทางอินเทอร์เน็ตได้ เพราะการข่มขู่ทางอินเทอร์เน็ตนั้นอาศัยอีเมลหรือการสื่อสารทางอิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิด ซึ่งผู้กระทำสามารถใช้ผ่านคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์ใด ๆ ก็ได้ โดยที่ไม่ต้องไปถึงถึงตัวบุคคลที่ตกเป็นเหยื่อของการข่มขู่ ดังนั้นแม้ว่าจะถูกกักกันแต่ถ้าผู้กระทำมีคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์อยู่กับตัว ผู้กระทำก็สามารถกระทำความผิดได้ การกักกันผู้กระทำจึงไม่สามารถป้องกันให้เกิดการกระทำความผิดได้

4.3.1.2 การห้ามเข้าเขตกำหนด

มาตรา 44 แห่งประมวลกฎหมายอาญา บัญญัติว่า “ห้ามเข้าเขตกำหนด คือการห้ามมิให้เข้าไปในท้องที่หรือสถานที่ที่กำหนดไว้ในคำพิพากษา”

การห้ามผู้กระทำการข่มขู่ทางอินเทอร์เน็ตไม่ให้เข้าไปในท้องที่หรือสถานที่ใด ๆ ไม่ได้เป็นการป้องกันไม่ให้เกิดการกระทำความผิดได้ เนื่องจากการข่มขู่ทางอินเทอร์เน็ตนั้นผู้กระทำไม่จำเป็นต้องไปใกล้หรือประชิดตัวเหยื่อเพื่อกระทำการข่มขู่ เพราะสามารถใช้เครื่องคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการข่มขู่เหยื่อจากที่ใดก็ได้

4.3.1.3 การเรียกประกันทัณฑ์บน

การเรียกประกันทัณฑ์บน คือ การให้บุคคลทำทัณฑ์บนโดยกำหนดจำนวนเงินว่าจะไม่ก่อเหตุร้ายให้เกิดอันตรายแก่บุคคลหรือทรัพย์สินของผู้อื่นตลอดเวลาที่ศาลกำหนด

การเรียกประกันทัณฑ์บนเกิดได้ 2 กรณี คือ กรณีที่ยังไม่มีคดีอาญาเกิดขึ้น แต่ความปรากฏว่าบุคคลจะก่อเหตุร้ายให้เกิดอันตรายแก่บุคคลหรือทรัพย์สินของผู้อื่น กับกรณีในการพิจารณาคดีความผิดใดความผิดหนึ่งที่ศาลไม่ลงโทษผู้ถูกฟ้อง เพราะการกระทำนั้นยังไม่ถึงขั้นเป็นความผิดอาญา แต่มีเหตุอันควรเชื่อว่าผู้ถูกฟ้องน่าจะก่อเหตุร้ายให้เกิดอันตรายแก่บุคคลหรือทรัพย์สินของผู้อื่น¹⁷

การเรียกประกันทัณฑ์บนสามารถนำมาใช้กับการข่มขู่ทางอินเทอร์เน็ตได้เต็มที่ กล่าวคือ ในกรณีที่ผู้กระทำได้กระทำการข่มขู่เหยื่อผ่านทางอีเมลซ้ำ ๆ ว่าจะทำร้ายเหยื่อ ในกรณีเช่นนี้

¹⁷ คณิต ณ นคร, อ้างแล้ว เชิงอรรถที่ 15, น. 412-413.

แม้ว่าการทำร้ายเหยื่อยังไม่เกิดขึ้นจริง แต่เพื่อป้องกันไม่ให้ผู้ที่ข่มขู่ลงมือกระทำการตามที่ได้ข่มขู่ไว้ ก็อาจใช้วิธีเรียกประกันตัวแทนได้

การเรียกประกันตัวแทนนั้นต้องร้องขอโดยพนักงานอัยการ และหากศาลเห็นพ้องด้วยกับข้อเสนอของพนักงานอัยการศาลก็จะสั่งให้ทำประกันโดยกำหนดจำนวนเงินไม่เกินห้าหมื่นบาท ว่าผู้ประกันจะไม่ก่อเหตุร้ายตลอดเวลาที่ศาลกำหนด แต่ไม่เกินสองปีและศาลอาจสั่งให้มีประกันด้วยได้

เมื่อศาลได้สั่งเรียกประกันตัวแทนหรือสั่งให้มีประกันด้วยแล้ว ถ้าผู้ถูกเรียกประกันตัวแทนไม่ยอมปฏิบัติตาม ศาลมีอำนาจกักขังหรือห้ามเข้าเขตกำหนดเพื่อบังคับให้ปฏิบัติตามหรือเป็นการทดแทนได้ และถ้าผู้ทำประกันกระทำผิดประกัน ศาลมีอำนาจสั่งให้ชำระเงินไม่เกินจำนวนที่กำหนดไว้ในประกัน

จากที่กล่าวมาพิจารณาได้ว่าการเรียกประกันตัวแทนเป็นวิธีการเพื่อความปลอดภัยที่สามารถนำมาใช้กับการข่มขู่ทางอินเทอร์เน็ตได้ กล่าวคือ ให้ผู้ที่กระทำความผิดทำประกันโดยมีการกำหนดจำนวนเงินว่าจะไม่กระทำการข่มขู่ทางอินเทอร์เน็ตต่อผู้อื่นตลอดเวลาที่ศาลกำหนด

4.3.1.4 การคุมตัวไว้ในสถานพยาบาล

การคุมตัวไว้ในสถานพยาบาล หมายถึง การควบคุมบุคคลที่มีความบกพร่องทางจิตให้อยู่ในสถานพยาบาลเพื่อการบำบัดรักษาให้หายก่อนที่จะออกมาในสังคม ทั้งนี้เพื่อป้องกันมิให้ผู้บกพร่องทางจิตนั้นก่อเหตุร้ายหรือกระทำการอันเป็นอันตรายแก่ผู้อื่นหรือทรัพย์สินของผู้อื่นได้¹⁸

การคุมตัวไว้ในสถานพยาบาล จึงเป็นวิธีการเพื่อความปลอดภัยที่มีเนื้อหาสองประการคือ เป็น “วิธีการเพื่อความปลอดภัย” และในขณะเดียวกันก็เป็น “มาตรการบำบัดด้วย”

มาตรา 48 “ถ้าศาลเห็นว่า การปล่อยตัวผู้มีจิตบกพร่อง โรคจิต หรือจิตฟั่นเฟือน ซึ่งไม่ต้องการบำบัดหรือได้รับการลดโทษตามมาตรา 65 จะเป็นการไม่ปลอดภัยแก่ประชาชน ศาลจะสั่งให้ส่งไปคุมตัวไว้ในสถานพยาบาลก็ได้ และคำสั่งนี้ศาลจะเพิกถอนเสียเมื่อใดก็ได้”

การคุมตัวไว้ในสถานพยาบาลนี้อาจนำมาใช้กับผู้กระทำการข่มขู่ทางอินเทอร์เน็ตที่เป็นผู้มีจิตบกพร่อง โรคจิต หรือจิตฟั่นเฟือนได้ แต่หากผู้กระทำยังไม่ถึงขั้นเป็นผู้มีจิตบกพร่อง โรคจิต หรือจิตฟั่นเฟือน แต่อาจเป็นผู้มีปัญหาทางจิตที่ยังไม่รุนแรงมาก การคุมตัวไว้ในสถานพยาบาลก็ไม่สามารถนำมาใช้กับผู้กระทำที่กล่าวมาได้ จึงควรมีการนำผู้กระทำการข่มขู่ทางอินเทอร์เน็ตที่มี

¹⁸ วิจิตรา เลิศศิริกิจ, “ความผิดฐานเฝ้าติดตามและข่มขู่,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2550), น. 75.

พฤติกรรมเบี่ยงเบนหรือมีปัญหาทางสุขภาพจิตที่ยังไม่รุนแรงไปรับคำปรึกษาจาก นักจิตวิทยา หรือ จิตแพทย์

4.3.1.5 การห้ามประกอบอาชีพบางอย่าง

การห้ามประกอบอาชีพบางอย่าง เป็นมาตรการเพื่อคุ้มครองสาธารณชนจากการกระทำของบุคคลที่ในการประกอบอาชีพหรือวิชาชีพใดแล้วได้กระทำความผิดโดยอาศัยโอกาสจากการประกอบอาชีพหรือวิชาชีพนั้น หรือในการประกอบอาชีพหรือวิชาชีพใดแล้วได้กระทำความผิดเนื่องจากการประกอบอาชีพหรือวิชาชีพนั้น¹⁹

มาตรา 50 “เมื่อศาลพิพากษาให้ลงโทษผู้ใด ถ้าศาลเห็นว่าผู้นั้นกระทำความผิดโดยอาศัยโอกาสจากการประกอบอาชีพหรือวิชาชีพ หรือเนื่องจากการประกอบอาชีพหรือวิชาชีพ และเห็นว่าหากผู้นั้นประกอบอาชีพหรือวิชาชีพนั้นต่อไปอาจจะกระทำความผิดเช่นนั้นขึ้นอีก ศาลจะสั่งไว้ในคำพิพากษาห้ามการประกอบอาชีพหรือวิชาชีพนั้นเป็นเวลาไม่เกินห้าปีนับแต่วันพ้นโทษไปแล้วก็ได้”

การห้ามประกอบอาชีพบางอย่างอาจนำมาใช้กับการข่มขู่ทางอินเทอร์เน็ตได้ในกรณีที่ผู้กระทำการข่มขู่ได้อาศัยโอกาสจากการประกอบอาชีพของตนมากระทำการความผิด เช่น ผู้กระทำการข่มขู่เป็นผู้ให้บริการทางอินเทอร์เน็ต และไม่พอใจผู้รับบริการทางอินเทอร์เน็ตรายหนึ่งจึงอาศัยประโยชน์จากการให้บริการทางอินเทอร์เน็ตของตน ค้นข้อมูล ประวัติส่วนตัว ชื่อที่อยู่อีเมลของบุคคลดังกล่าว และดำเนินการข่มขู่บุคคลนั้นผ่านทางอีเมล หรือทางเว็บไซต์ที่ตนได้สร้างขึ้น

4.3.2 มาตรการรอกการลงโทษโดยมีการกำหนดเงื่อนไขเพื่อคุ้มครองความประพฤติ

ในการรอกการลงโทษ ศาลจะปล่อยตัวผู้กระทำความผิดไปเลย หรือจะปล่อยตัวผู้กระทำความผิดโดยกำหนดเงื่อนไขเพื่อคุ้มครองความประพฤติผู้กระทำความผิดก็ได้

มาตรา 56 “ผู้ใดกระทำความผิดซึ่งมีโทษจำคุก และในคดีนั้นศาลจะลงโทษจำคุกไม่เกินสามปี ถ้าไม่ปรากฏว่าผู้นั้นได้รับโทษจำคุกมาก่อน หรือปรากฏว่าได้รับโทษจำคุกมาก่อน แต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาท หรือความผิดลหุโทษ เมื่อศาลได้คำนึงถึงอายุ ประวัติ ความประพฤติ สติปัญญา การศึกษาอบรม สุขภาพ ภาวะแห่งจิต นิสัย อาชีพ และสิ่งแวดล้อมของผู้นั้น หรือสภาพความผิดหรือเหตุอันสมควรปรานีแล้ว เห็นเป็นการสมควร ศาลจะพิพากษาว่าผู้นั้นมีความผิดแต่รอกการกำหนดโทษไว้หรือกำหนดโทษแต่รอกการลงโทษไว้แล้วปล่อยตัวไป เพื่อให้

¹⁹ คณิต ญ นคร, อ้างแล้ว เชิงอรรถที่ 15, น.417-418.

โอกาสผู้นั้นกลับตัวภายในระยะเวลาที่ศาลจะได้กำหนด แต่ต้องไม่เกินห้าปีนับแต่วันที่ศาลพิพากษา โดยจะกำหนดเงื่อนไขเพื่อคุ้มครองความประพฤติของผู้นั้นด้วยหรือไม่ก็ได้

เงื่อนไขเพื่อคุ้มครองความประพฤติของผู้กระทำความผิดนั้น ศาลอาจกำหนดข้อเดียวหรือหลายข้อ ดังต่อไปนี้

(5) เงื่อนไขอื่นๆ ตามที่ศาลเห็นสมควรกำหนดเพื่อแก้ไข ฟื้นฟู หรือป้องกันมิให้ผู้กระทำความผิดกระทำหรือมีโอกาสดังกล่าวซ้ำอีก

การข่มขู่ทางอินเทอร์เน็ต ซึ่งอาจเป็นการกระทำความผิดตามมาตรา 392 แห่งประมวลกฎหมายอาญานั้น พิจารณาได้ว่าเป็นความผิดลหุโทษ ซึ่งศาลอาจให้การลงโทษก็ได้ ในกรณีเช่นว่าศาลอาจรอการลงโทษโดยมีการกำหนดเงื่อนไขเพื่อคุ้มครองความประพฤติของผู้กระทำด้วยก็ได้

4.3.3 มาตรการในการได้มาซึ่งพยานหลักฐาน

ปัญหาสำคัญประการหนึ่งของการข่มขู่ทางอินเทอร์เน็ตก็คือ การได้มาซึ่งพยานหลักฐาน เพราะผู้กระทำผิดที่ข่มขู่ผ่านทางอินเทอร์เน็ตแทนที่จะข่มขู่แบบธรรมดาทั่วไปนั้นก็เพื่อปกปิดร่องรอยของการกระทำของตนนั่นเอง ด้วยเหตุดังกล่าวจึงทำให้หาพยานหลักฐานยากขึ้น อย่างไรก็ตาม เพื่อจัดการกับปัญหาดังกล่าวจึงได้มีการบัญญัติให้อำนาจพนักงานเจ้าหน้าที่เป็นพิเศษในการจัดการให้ได้มาซึ่งหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 ดังนี้²⁰

มาตรา 18 “ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่าการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด และหาตัวผู้กระทำความผิด

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้”

อำนาจตาม (1) เป็นเรื่องทั่วไปในการรวบรวมพยานหลักฐานซึ่งอาจทำโดยวิธีการเรียกบุคคลมาให้ถ้อยคำ หรือให้บุคคลชี้แจงเป็นหนังสือ หรือให้ส่งเอกสารหรือวัตถุอื่นใด ซึ่งอำนาจตาม

²⁰ พรเพชร วิชิตชลชัย, อ้างแล้ว เชิงอรรถที่ 6, หน้า 32-38.

(1) นี่เป็นอำนาจที่เจ้าพนักงานฝ่ายปกครองและตำรวจชั้นผู้ใหญ่มียอยู่แล้วตามประมวลกฎหมายวิธีพิจารณาความอาญา ส่วน “ข้อมูล” นั้นหมายถึงข้อมูลทั่วไป เช่นเป็นข้อมูลที่เก็บไว้ในไฟล์ดิจิทัล แต่ไม่รวมถึงข้อมูลคอมพิวเตอร์

มาตรา 18(2) “เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง”

ผู้ให้บริการมีหน้าที่ตามมาตรา 26 ที่จะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน ดังนั้นหลักเกณฑ์และระยะเวลาในการเก็บรักษาจึงต้องพิจารณาจากมาตรา 26 ด้วย

นอกจากพนักงานเจ้าหน้าที่ที่มีอำนาจเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการแล้ว ก็ยังมีอำนาจเรียกจากบุคคลอื่นที่เกี่ยวข้องได้อีกด้วย

มาตรา 18(3) “สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่”

ข้อมูลเกี่ยวกับผู้ใช้บริการ เช่นข้อมูลรหัสประจำตัวผู้ใช้บริการ (user ID) ข้อมูลเกี่ยวกับบุคคลที่ใช้บริการซึ่งได้มีการลงทะเบียน (register) ไว้ เป็นต้น

มาตรา 18(4) “ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่”

การทำสำเนาข้อมูลคอมพิวเตอร์หรือข้อมูลจราจรทางคอมพิวเตอร์เมื่อไปกระทำจากระบบคอมพิวเตอร์ ถือว่าเป็นการล่วงล้ำเข้าไปในข้อมูลคอมพิวเตอร์ซึ่งหากบุคคลทั่วไปทำย่อมเป็นความผิด ดังนั้นพนักงานเจ้าหน้าที่จะกระทำได้อีกต่อเมื่อได้รับอนุญาตจากศาลก่อน

ส่วนข้อความที่ว่า “ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่” หมายถึง ในกรณีที่หากพนักงานเจ้าหน้าที่ได้ยึดหรืออายัดระบบคอมพิวเตอร์นั้นมาแล้ว ดังนั้นเมื่อได้ยึดหรืออายัดระบบคอมพิวเตอร์มาแล้วก็ย่อมใช้อำนาจทำสำเนาข้อมูลคอมพิวเตอร์ได้เลยโดยไม่จำเป็นต้องขออนุญาตต่อศาลอีก

มาตรา 18(5) “สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่”

การที่พนักงานเจ้าหน้าที่จะสั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่

พนักงานเจ้าหน้าที่จะต้องยื่นคำร้องขออนุญาตจากศาลที่มีเขตอำนาจและศาลได้มีคำสั่งอนุญาตก่อน

มาตรา 18(6) “ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูล คอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้”

มาตรา 18(7) “ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว”

การใช้อำนาจในการตรวจสอบและเข้าถึงข้อมูลคอมพิวเตอร์ตาม (6) พนักงานเจ้าหน้าที่อาจพบปัญหาซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลคอมพิวเตอร์ได้เนื่องจากมีรหัสลับป้องกันการเข้าถึงข้อมูลนั้น มาตรา 18(7) จึงให้อำนาจพนักงานเจ้าหน้าที่ในการดำเนินการถอดรหัสลับหรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

มาตรา 18(8) “ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้”

ถึงแม้ว่าพนักงานเจ้าหน้าที่จะได้ใช้อำนาจตามที่บัญญัติไว้ในข้อก่อน ๆ แล้ว เช่นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์หรือการถอดรหัสลับแล้วก็ตาม แต่บางครั้งก็อาจยังไม่ได้ข้อมูล เช่นไม่อาจถอดรหัสลับได้ มาตรา 18(8) จึงให้อำนาจพนักงานเจ้าหน้าที่ในการยึดอายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

การยึดระบบคอมพิวเตอร์ คือการนำระบบคอมพิวเตอร์มาอยู่ในความครอบครองของพนักงานเจ้าหน้าที่ ส่วนการอายัดระบบคอมพิวเตอร์น่าจะหมายถึงการที่พนักงานเจ้าหน้าที่สั่งระงับการใช้ระบบคอมพิวเตอร์นั้นและให้ระบบคอมพิวเตอร์นั้นอยู่ในความควบคุมของพนักงานเจ้าหน้าที่

การยึดหรืออายัดระบบคอมพิวเตอร์นอกจากจะต้องได้รับอนุญาตจากศาลแล้ว พนักงานเจ้าหน้าที่จะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้นให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอ

ขยายเวลายืดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยืดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยืดหรือถอนการอายัดโดยพลัน หนังสือแสดงการยืดหรืออายัดดังกล่าวเป็นไปตามที่กำหนดในกฎกระทรวง

นอกจากนี้ มาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ยังได้กำหนดหน้าที่และความรับผิดชอบของผู้ให้บริการด้วย กล่าวคือผู้ให้บริการมีหน้าที่ต้องเก็บรักษาข้อมูล การมีบทบัญญัติเช่นนี้ย่อมช่วยในการหาพยานหลักฐานด้วย

มาตรา 26 “ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่มีข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษา ข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถ ระบุตัว ผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลา ไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การ ใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่ รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท”

มาตรา 26 กำหนดให้ผู้ให้บริการมีหน้าที่ต้องเก็บรักษาข้อมูล 2 ประเภท คือ²¹

(1) ข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่มีข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์แต่อาจขยายออกไปได้กรณีที่ พนักงานเจ้าหน้าที่สั่งให้เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปี เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

(2) ข้อมูลผู้ให้บริการ หมายถึง ข้อมูลที่บันทึกถึงตัวตนของบุคคลในการเข้าใช้บริการทาง เครือข่ายของผู้ให้บริการ ไม่ว่าจะเป็นชื่อ สกุล รหัสเลขประจำตัว user name หรือ pin code ใดๆ ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลของผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้ เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การให้บริการสิ้นสุดลง

²¹ เฟิงอ้าง, น. 53.

สาเหตุหนึ่งของการที่ผู้กระทำการข่มขู่เลือกกระทำการข่มขู่ทางอินเทอร์เน็ตก็เพราะคิดว่าการข่มขู่ทางอินเทอร์เน็ตนั้นไม่ต้องเปิดเผยตัว ทำให้การดำเนินการหาตัวผู้กระทำความผิดมาลงโทษได้ยาก การที่กฎหมายกำหนดให้ผู้ให้บริการมีหน้าที่ต้องเก็บรักษาข้อมูลนั้นช่วยแก้ปัญหาดังกล่าวได้พอสมควร เพราะข้อมูลดังกล่าวอาจนำไปสู่การหาตัวผู้กระทำความผิดได้ แต่ถ้าไม่มีการเก็บข้อมูลดังกล่าวเอาไว้หลักฐานก็ย่อมไม่มี บทบัญญัติมาตรา 26 จึงมีความสำคัญมาก

4.4 เปรียบเทียบบทบัญญัติฐานข่มขู่ทางอินเทอร์เน็ตในประเทศสหรัฐอเมริกา กับกฎหมายของประเทศไทย

ในหัวข้อนี้จะเปรียบเทียบบทบัญญัติฐานข่มขู่ทางอินเทอร์เน็ตในประเทศสหรัฐอเมริกากับกฎหมายของประเทศไทยในเรื่องของการมีบทบัญญัติว่าด้วยการข่มขู่ทางอินเทอร์เน็ต บทบัญญัติใดบ้างที่สามารถนำมาใช้กับการข่มขู่ทางอินเทอร์เน็ต โทษสำหรับการข่มขู่ทางอินเทอร์เน็ต และมาตรการอื่น ๆ ที่อาจนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ต

4.4.1 เปรียบเทียบเรื่องการมีบทบัญญัติว่าด้วยการข่มขู่ทางอินเทอร์เน็ต

ในประเทศสหรัฐอเมริกานั้น ในหลายมลรัฐได้มีการบัญญัติความผิดฐานข่มขู่ทางอินเทอร์เน็ตเอาไว้ อย่างเช่น มลรัฐอิลลินอยส์ มลรัฐวอชิงตัน มลรัฐลุยเซียนา มลรัฐมิสซิสซิปปี มลรัฐนอร์ทคาโรไลนา และมลรัฐโรดไอแลนด์ เป็นต้น ส่วนมลรัฐอื่น ๆ ที่ไม่ได้มีการบัญญัติเรื่องการข่มขู่ทางอินเทอร์เน็ตเอาไว้โดยตรงก็จะให้นำความผิดฐานคุกคาม (harassment) หรือความผิดฐานเฝ้าติดตามและข่มขู่ (Stalking) มาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ต

ส่วนประเทศไทยในขณะนี้ยังไม่มีบทบัญญัติเรื่องการข่มขู่ทางอินเทอร์เน็ต

4.4.2 เปรียบเทียบเรื่องบทบัญญัติที่นำมาใช้กับการข่มขู่ทางอินเทอร์เน็ต

ในประเทศสหรัฐอเมริกานั้น ในหลายมลรัฐมีบทบัญญัติเรื่องการข่มขู่ทางอินเทอร์เน็ตไว้โดยเฉพาะ เมื่อมีการกระทำความผิดเกิดขึ้นจึงสามารถนำบทบัญญัตินี้ดังกล่าวมาบังคับใช้ได้ทันที กฎหมายการข่มขู่ทางอินเทอร์เน็ตที่มีการบัญญัติไว้นั้น มีการบัญญัติถึงคำจำกัดความของคำต่าง ๆ อย่างเช่น คำว่า “การสื่อสารทางอิเล็กทรอนิกส์” (Electronic communication) , “ไปรษณีย์

อิเล็กทรอนิกส์” (Electronic Mail) , “รังควาน” (Harass) เอาไว้โดยเฉพาะเพื่อที่จะได้ไม่ต้องมีปัญหากับการตีความ

นอกจากนี้ยังได้บัญญัติถึงการกระทำที่ถือว่าเป็นการข่มขู่ทางอินเทอร์เน็ตไว้ด้วยว่าต้องมีองค์ประกอบใดบ้าง โดยทั่วไปแล้วจะมีองค์ประกอบดังนี้ คือ

1. มีการใช้อีเมลล์หรือการสื่อสารทางอิเล็กทรอนิกส์อื่น ๆ ส่งถ้อยคำ รูปภาพ เสียง เครื่องหมาย หรือข้อมูลอื่น ๆ ข่มขู่บุคคลใดบุคคลหนึ่งเป็นการเฉพาะว่าจะทำอันตรายต่อร่างกายหรือก่อให้เกิดความเสียหายต่อทรัพย์สินของบุคคลที่กล่าวมาหรือสมาชิกในครอบครัวของบุคคลดังกล่าว และบางมลรัฐได้เพิ่มเรื่องการข่มขู่ว่าจะลงละเมิดทางเพศ หรือกักขังหน่วงเหนี่ยวเข้าไปด้วย
2. มีการส่งอีเมลล์ หรือการสื่อสารทางอิเล็กทรอนิกส์ถึงบุคคลใดบุคคลหนึ่ง โดยใช้ถ้อยคำที่เป็นเท็จในเรื่องการตาย การบาดเจ็บ การเจ็บป่วย การเสียโฉม การกระทำไม่เหมาะสม หรือการกระทำผิดทางอาญาของบุคคลที่ได้รับการสื่อสารนั้น ๆ หรือของสมาชิกในครอบครัวของบุคคลนั้น
3. ส่งอีเมลล์ หรือการสื่อสารทางอิเล็กทรอนิกส์จูงใจให้บุคคลอื่นกระทำการอันเป็นการละเมิดต่อกฎหมายโดยตรงต่อบุคคลใดบุคคลหนึ่งหรือสมาชิกในครอบครัวของบุคคลนั้น
4. สร้างและดำเนินการจัดการเว็บไซต์ที่บุคคลทั่วไปเข้าถึงได้ และในเว็บไซต์มีถ้อยคำข้อความในการข่มขู่บุคคลใดบุคคลหนึ่งว่าจะทำอันตรายต่อกายของบุคคลนั้น หรือลงข้อความจูงใจให้บุคคลอื่นกระทำการอันเป็นการละเมิดต่อกฎหมายโดยตรงต่อบุคคลนั้น
5. จะต้องมีการกระทำได้ที่กล่าวมาข้างต้นในลักษณะซ้ำ ๆ และต่อเนื่องในช่วงระยะเวลาหนึ่ง
6. บัญญัติให้บุคคลที่ยินยอมรับรู้ให้มีการใช้อุปกรณ์ทางอิเล็กทรอนิกส์ซึ่งอยู่ในความควบคุมของตนเพื่อใช้กระทำการข่มขู่ทางอินเทอร์เน็ตตามที่กล่าวมานั้นมีความผิด
7. การกระทำการข่มขู่ดังที่กล่าวมานั้นต้องเป็นการกระทำโดยมีเจตนาเพื่อข่มขู่ รังควาน ให้บุคคลใดบุคคลหนึ่ง เกิดความหวาดกลัว ทรมาน รู้สึกอับอาย

นอกจากจะบัญญัติว่าการกระทำใดเป็นการข่มขู่ทางอินเทอร์เน็ตแล้ว ยังมีการบัญญัติถึงการกระทำผิดซ้ำและการกระทำความผิดโดยมีเหตุฉกรรจ์เอาไว้ด้วย และในบางมลรัฐยังได้มีการบัญญัติถึงเหตุยกเว้นความผิดไว้ด้วย

ส่วนของประเทศไทยนั้นเนื่องจากไม่ได้มีบทบัญญัติเรื่องการข่มขู่ทางอินเทอร์เน็ตเอาไว้ จึงต้องพิจารณาว่ากฎหมายอาญาของไทยมีอยู่ในขณะนั้น มีบทบัญญัติใดบ้างที่สามารถนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ตได้ จากการพิจารณาพบว่าประมวลกฎหมายอาญาของไทย มาตรา 392 นั้นสามารถนำมาปรับใช้ได้ แต่มาตราดังกล่าวก็เป็นเพียงความผิดลหุโทษเท่านั้น จึงไม่ได้มีการบัญญัติถึงเรื่องการกระทำความผิดซ้ำ หรือการกระทำความผิดโดยมีเหตุฉกรรจ์

เอาไว้ด้วย ส่วนพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ก็มีบทบัญญัติที่อาจนำมาปรับใช้ได้บ้าง ไม่ว่าจะเป็นมาตรา 14(1) ,14(4) , 15 และ มาตรา 16 อย่างไรก็ดี เนื่องจากบทบัญญัติดังกล่าวไม่ได้บัญญัติขึ้นสำหรับการกระทำการอันเป็นการข่มขู่ทางอินเทอร์เน็ตโดยตรง แต่เป็นบทบัญญัติที่ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มาตราดังกล่าวที่อาจนำมาปรับใช้ได้ จึงไม่ครอบคลุมถึงการกระทำการอันเป็นการข่มขู่ทางอินเทอร์เน็ตได้ทั้งหมด

4.4.3 เปรียบเทียบเรื่องโทษสำหรับการข่มขู่ทางอินเทอร์เน็ต

ในประเทศสหรัฐอเมริกา นั้น โทษสำหรับการข่มขู่ทางอินเทอร์เน็ตนั้นแตกต่างกันไปตามแต่ละมลรัฐ บางมลรัฐกำหนดให้ความผิดฐานข่มขู่ทางอินเทอร์เน็ตนั้นเป็นความผิดอาญาไม่ร้ายแรง แต่ในบางมลรัฐก็ถือว่าเป็นความผิดอาญาร้ายแรง แต่ถ้าเป็นการกระทำผิดซ้ำ หรือเป็นการกระทำโดยมีเหตุกรรเจ้นั้นจะถือว่าเป็นความผิดอาญาร้ายแรง มีโทษจำคุก โทษปรับ หรือทั้งจำคุกทั้งปรับ

ส่วนประเทศไทยนั้นเนื่องจากไม่มีบทบัญญัติว่าด้วยการข่มขู่ทางอินเทอร์เน็ตโดยเฉพาะ จึงต้องนำบทบัญญัติในกฎหมายอาญาของไทยที่มีอยู่มาปรับใช้ บทบัญญัติที่นำมาปรับใช้ได้โดยตรงอย่างมาตรา 392 แห่งประมวลกฎหมายอาญานั้น เป็นความผิดลหุโทษ อัตราโทษที่กำหนดไว้จึงเบาบาง และไม่ได้มีการบัญญัติถึงการกระทำความผิดซ้ำ หรือการกระทำความผิดโดยมีเหตุกรรเจ้อไว้ด้วย

ส่วนบทบัญญัติในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่อาจนำมาปรับใช้ได้นั้น แม้ว่าแต่ละบทบัญญัติจะมีทั้งโทษปรับ และโทษจำคุก แต่เมื่อบทบัญญัติดังกล่าวไม่ได้ครอบคลุมถึงการกระทำการอันเป็นการข่มขู่โดยตรง ประสิทธิภาพในการยับยั้งไม่ให้กระทำผิด หรือกระทำผิดซ้ำได้อีกจึงอาจไม่ดีเท่าที่ควร

4.4.4 เปรียบเทียบมาตรการอื่น ๆ ที่อาจนำมาปรับใช้กับการข่มขู่ทางอินเทอร์เน็ต

ในสหรัฐอเมริกา นั้นมีมาตรการที่อาจนำมาช่วยเสริมประสิทธิภาพในการจัดการกับปัญหาการข่มขู่ทางอินเทอร์เน็ตหลายมาตรการด้วยกัน เช่น คำสั่งคุ้มครองหรือคำสั่งงดเว้นกระทำการ การใช้วิธีการเพื่อความปลอดภัย และการประเมินสภาพทางจิตของจำเลย มาตรการที่กล่าวมา

นั้นมีทั้งมาตรการที่เป็นการยับยั้งไม่ให้กระทำผิดซ้ำอีก รวมถึงเป็นมาตรการที่ช่วยคุ้มครองผู้ที่ตกเป็นเหยื่ออีกด้วย

สำหรับประเทศไทยนั้นมาตรการอื่นที่อาจนำมาปรับใช้นั้นได้แก่ วิธีการเพื่อความปลอดภัยประเภทของการเรียกประกันทัณฑ์บนเท่านั้น วิธีการอื่นอย่างการกักกัน หรือการห้ามเข้าเขตที่กำหนดนั้นไม่อาจนำมาใช้ได้ เนื่องจากลักษณะของการกระทำความผิดนั้นไม่จำเป็นต้องเข้าถึงตัวเหยื่อโดยตรง ส่วนมาตรการรอกการลงโทษโดยมีการกำหนดเงื่อนไขเพื่อคุ้มครองความปลอดภัยนั้นสามารถนำมาใช้ได้

