มาตรการทางกฎหมายเกี่ยวกับการคุกคามทางอินเตอร์เน็ต (Cyberstalking)

Legislative Measures on Cyberstalking

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต มหาวิทยาลัยกรุงเทพ
พ.ศ. 2550

มาตรการทางกฎหมายเกี่ยวกับการคุกคามทางอินเตอร์เน็ต (Cyberstalking)

Legislative Measures on Cyberstalking

โดย

นางสาวรักข์ษิตา โพธิ์พิทักษ์กุล

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต มหาวิทยาลัยกรุงเทพ
พ.ศ. 2550

บัณฑิตวิทยาลัย
มหาวิทยาลัยกรุงเทพ

สารนิพนธ์

โดย

นางสาวรักข์ษิตา โพธิ์พิทักษ์กุล

เรื่อง

มาตรการทางกฎหมายเกี่ยวกับการคุกคามทางอินเตอร์เน็ต

ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต

อาจารย์ที่ปรึกษา _____
(ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ)

อาจารย์ที่ปรึกษาร่วม _____
(อาจารย์อำนาจ เนตยสุภา)

กรรมการผู้ทรงคุณวุฒิ _____
(รองศาสตราจารย์ ดร.พันธุ์ทิพย์ กาญจนจิตรา สายสุนทร)

ชื่องานวิจัยภาษาไทย : มาตรการทางกฎหมายเกี่ยวกับการคุกคามทางอินเตอร์เน็ต
ชื่องานวิจัยภาษาอังกฤษ : Legislative Measures on Cyberstalking
ชื่อผู้วิจัยภาษาไทย : นางสาวรักข์ษิตา โพธิ์พิทักษ์กุล
ชื่อผู้วิจัยภาษาอังกฤษ : Miss Raksita Popitakkul
ชื่อคณะ : คณะนิติศาสตร์
สาขา : กฎหมายธุรกิจระหว่างประเทศและธุรกรรมทางอิเล็กทรอนิกส์
ชื่อสถาบัน : มหาวิทยาลัยกรุงเทพ
รายชื่อที่ปรึกษา : ผู้ช่วยศาสตราจารย์ ดร. อรรยา สิงห์สงบ
รายชื่อที่ปรึกษาร่วม : อาจารย์อำนาจ เนตยสุภา
ปีการศึกษา : 2550
คำสำคัญ : คุกคาม อินเตอร์เน็ต

บทคัดย่อ

อินเตอร์เน็ตเป็นเครื่องมือสื่อสารที่มีประสิทธิภาพและเป็นที่นิยมอย่างมากในปัจจุบัน ซึ่งมีทั้งคุณและโทษในขณะเดียวกัน และจากลักษณะที่ไม่จำเป็นต้องเปิดเผยตัวของอินเตอร์เน็ตจึงมีความพยายามในการใช้อินเตอร์เน็ตเพื่อก่ออาชญากรรมในรูปแบบที่พัฒนาตามความก้าวหน้าของเทคโนโลยี “การคุกคามทางอินเตอร์เน็ต ” (Cyberstalking)เป็นอาชญากรรมรูปแบบใหม่ที่เปลี่ยนแปลงไปจากการคุกคามแบบธรรมดา จากการศึกษากฎหมายการคุกคามทางอินเตอร์เน็ตของประเทศสหรัฐอเมริกาพบว่ากฎหมายในแต่ละมลรัฐนั้นมีองค์ประกอบของการกระทำความผิดไม่แตกต่างกันเท่าใดนัก องค์ประกอบของการกระทำความผิดนั้นประกอบด้วย 1. มีการใช้หรือส่งการสื่อสารทางอิเล็กทรอนิกส์ 2. มีการข่มขู่ ข่มขวัญ หรือรังควาน 3. มีเจตนาทำให้เหยื่อนั้นเกิดความกลัวเกี่ยวกับความปลอดภัยในชีวิตและทรัพย์สิน หรือความกลัวว่าจะเกิดภยันตรายกับคนใกล้ชิดหรือคนในครอบครัวของเหยื่อ และในแต่ละมลรัฐก็บัญญัติอัตราโทษของความผิดดังกล่าวไว้ไม่เท่ากัน บางมลรัฐถือว่าการคุกคามทางอินเตอร์เน็ตเป็นความผิดฐานเบาสำหรับการกระทำความผิดครั้งแรก บางมลรัฐถือว่าเป็นความผิดร้ายแรงและต้องรับโทษหนักขึ้น หากมีการกระทำซ้ำ สำหรับบางมลรัฐที่มิได้บัญญัติกฎหมายการคุกคามทางอินเตอร์เน็ตไว้โดยเฉพาะก็จะนำกฎหมายเกี่ยวกับการคุกคาม (Stalking Law) มาใช้เทียบเคียงเพื่อลงโทษผู้กระทำความผิด

สำหรับประเทศไทยมีเพียงกฎหมายอาญามาตรา 326 มาตรา 328 และมาตรา 392 ที่สามารถนำมาปรับใช้ลงโทษผู้กระทำความผิดหากแต่บทลงโทษนั้นไม่รุนแรงพอที่จะยับยั้งหรือปราบปราม ผู้กระทำความผิด และนอกจากนี้ยังมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.....(ฉบับสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ) ซึ่งเป็นกฎหมายที่มีอัตราโทษ

สูงกว่าแต่ก็ยังไม่ครอบคลุมถึงการกระทำความผิดในลักษณะของการคุกคามทางอินเตอร์เน็ต

ดังนั้นจึงมีความจำเป็นที่ต้องศึกษาพฤติกรรมลักษณะของการคุกคามทางอินเตอร์เน็ต เพื่อหามาตรการทางกฎหมายที่เหมาะสมสำหรับประเทศไทยต่อไป

Abstract

The Internet is a worldwide, publicly accessible series of interconnected computer networks that can bring about both positive and negative effects. Regarding the concealed aspect of the Internet, there is a high tendency of cyber crimes to take place in accordance with rapid advancement of technology. Cyberstalking has become the most recent criminal threat which has gigantic difference comparing to those common menaces. According to the study of the U.S. Cyber Crime Law, it indicates that states and cities in the country rely on the similar basis of violation ranging from sending and receiving information on electronic communications, generating hazardous threats or menaces, having an intention to torture over one's life and treasury. Admittedly, each state has different levels of prosecution. In some states, the first violation of conducting the Internet threats is quite moderate while harsh punishment will come into action for the next illegal uses. Moreover, some states have no certain Cyber Crime Law, particularly the Stalking Law, for prosecuting those violators.

Thailand has legislated section 326, 328, and 392 in the penal code to penalize cyber terrorists, but still the punishment is weak. However, Thailand Cyber Crime Law B.E. 2550 and Personal Data Protection Law reportedly have higher level of punishment but they are not identified to completely relate to the violation of the Internet threats. It is therefore significant to study an overall aspect of the Internet threats in order to legislate the proper Internet Law for the country.

กิตติกรรมประกาศ

ผู้เขียนขอกราบขอบพระคุณ อาจารย์อำนาจ เนตยสุภา ที่ได้กรุณารับเป็นที่ปรึกษาสารนิพนธ์ โดยอาจารย์ได้สละเวลาอันมีค่าในการให้ความรู้ คำแนะนำ ตลอดจนแนวทางต่าง ๆ ในการทำสารนิพนธ์จนสำเร็จ ผู้เขียนขอกราบขอบพระคุณอาจารย์อย่างสูงไว้ ณ ที่นี้

กราบขอบพระคุณพ่อแม่ที่สนับสนุนในการศึกษาตลอดมา และคอยเป็นกำลังใจที่สำคัญที่สุดและเป็นแรงผลักดันให้ผู้เขียนบรรลุผลในการทำสารนิพนธ์ฉบับนี้

สุดท้าย ขอบคุณพี่ ๆ น้อง ๆ ร่วมคณะที่ผลัดกันให้กำลังใจ คอยไถ่ถามความคืบหน้าตลอดช่วงเวลาที่ทำสารนิพนธ์นี้ โดยเฉพาะคุณพฤกษาและคุณพันทิวาที่คอยดูแลและให้กำลังใจเป็นพิเศษรวมทั้งผู้ที่มิได้เอ่ยนามไว้ ณ ที่นี้ อีกทั้งพี่ ๆ น้อง ๆ และเพื่อนร่วมงานที่คอยดูแลงานให้ในช่วงเวลาที่ผู้เขียนทำสารนิพนธ์ฉบับนี้ให้สำเร็จลุล่วงด้วยดี

รักข์ษิตา โพธิ์พิทักษ์กุล

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญ (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีได้พัฒนาก้าวหน้าอย่างไร้พรมแดน โดยสังเกตจากการที่ประชาชนส่วนใหญ่สามารถติดต่อสื่อสารกันอย่างง่ายดายและทั่วโลก ซึ่งอินเตอร์เน็ตเป็นปัจจัยสำคัญในการก่อให้เกิดการพัฒนา แม้ว่าอินเตอร์เน็ตที่มี ส่วนสำคัญในชีวิตของผู้คนปัจจุบันและก่อให้เกิดประโยชน์มากมายจากการใช้อินเตอร์เน็ตในทางกลับกันการใช้อินเตอร์เน็ตของคนบางกลุ่มยังไม่เหมาะสมกับความเจริญในปัจจุบัน

การนำประสิทธิภาพของอินเตอร์เน็ตมาใช้เพื่อเป็นประโยชน์ต่อชีวิตประจำวันมีมากมาย เช่น การติดต่อสื่อสารกันในรูปแบบของจดหมายอิเล็กทรอนิกส์ การพูดคุยโต้ตอบกันโดยที่ต่างฝ่ายอยู่คนละที่ การหาข้อมูลความรู้ การใช้ประโยชน์ทางด้านธุรกิจ และแม้แต่การดำเนินชีวิตประจำวัน ส่วนมากมักใช้อินเตอร์เน็ตในส่วนที่เป็นประโยชน์ แต่ใช่ว่าคุณประโยชน์ของอินเตอร์เน็ตจะไม่ส่งผลก ระทบ เพราะยังมีบางส่วนใช้อินเตอร์เน็ตผิดวัตถุประสงค์ เช่น การใช้ก่อความรำคาญ เดือดร้อน หรือถึงขั้นที่ต้องดำเนินการทางกฎหมาย เช่น การหมิ่นประมาทบนอินเตอร์เน็ต หรือการก่ออาชญากรรมทางคอมพิวเตอร์ เช่น การนำภาพไม่พึงประสงค์นำมาเผยแพร่ต่อสาธารณชนโดยที่สร้างความเ สียหายต่อผู้ที่ถูกกระทำ ปัญหาที่เกิดขึ้นจากอินเตอร์เน็ตที่ได้กล่าวมาแล้วในขณะนี้สร้างความเดือดร้อนต่อผู้ใช้อินเตอร์เน็ตเป็นอย่างมากผู้ที่เกี่ยวข้องทั้งในส่วนของภาครัฐและของเอกชนก็ดีได้ร่วมกันสร้างมาตรการเพื่อรองรับกับปัญหาต่าง ๆ ที่เกิดขึ้นมา แต่เนื่องจากก ารพัฒนาอย่างไม่หยุดยั้งของระบบอินเตอร์เน็ตทำให้มาตรการต่าง ๆ เป็นการป้องกันปัญหาที่ปลายเหตุ

ปัญหาอย่างหนึ่งที่สร้างความเดือดร้อนต่อผู้ใช้อินเตอร์เน็ตอย่างต่อเนื่องก็คือปัญหาการคุกคามทางอินเตอร์เน็ตซึ่งปัจจุบันก่อให้เกิดผลเสียและยังสามารถสร้างปัญหาขึ้นอย่างทวีคูณซึ่งปัญหาดังกล่าวสร้างความเสียหายเดือดร้อนจากการถูกคุกคามของเหยื่อเป็นอย่างมาก ในการศึกษาครั้งนี้ ผู้ศึกษาได้กำหนดประเด็นปัญหาในเรื่องปัญหาการคุกคามทางอินเตอร์เน็ต (Cyberstalking) ออกเป็น 3 ประเภท คือ ปัญหาคุกคามผ่านทางจดหมายอิเล็กทรอนิกส์ และปัญห าคุกคามบนเว็บบอร์ดสาธารณะ และปัญหาการคุกคามทางห้องสนทนาสด อันการคุกคามดังกล่าวก่อให้เกิดความเดือดร้อนรำคาญต่อผู้ถูกคุกคามจนอาจจะกลายเป็นปัญหาอาชญากรรมชนิดใหม่ที่ผิดต่อกฎหมาย ซึ่งในประเทศไทยปัจจุบันอัตราการใช้อินเตอร์เน็ตมีจำนวนมากและยังไม่มีมาตรการหรือกฎ หมายที่สามารถรองรับและควบคุมการคุกคามทางอินเตอร์เน็ต ซึ่งในประเทศไทยมีเพียงประมวลกฎหมายแพ่งและ

พาณิชย์ว่าด้วยความรับผิดเพื่อละเมิด มาตรา 420 ประมวลกฎหมายอาญามาตรา 392 ซึ่งมีบทลงโทษเพียงจำคุกไม่เกินหนึ่งเดือน ปรับไม่เกินหนึ่งพันบาทหรือทั้งจำทั้งปรับ ซึ่งเป็นบทลงโทษที่ไม่รุนแรง จึงเป็นการสมควรที่จะมีการศึกษาเพื่อหาแนวทางแก้ไขปรับปรุงกฎหมายที่เหมาะสม เพื่อให้เท่าทันกับรูปแบบการกระทำความผิดที่พัฒนาเปลี่ยนแปลงไป

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อเข้าใจปัญหาและรูปแบบการคุกคามทางอินเตอร์เน็ต
2. ศึกษาถึงผลกระทบที่เกิดขึ้นจากการคุกคามทางอินเตอร์เน็ต
3. ศึกษาถึงขอบเขตและองค์ประกอบความผิดเกี่ยวกับการคุกคามทางอินเตอร์เน็ตของประเทศสหรัฐอเมริกาโดยเฉพาะกฎหมายของมลรัฐมิสซิสซิปปี้
4. เพื่อศึกษาถึงสภาพบังคับของกฎหมายอาญาของไทยว่าสามารถนำมาใช้บังคับกับความผิดเกี่ยวกับการคุกคามทางอินเตอร์เน็ตได้เพียงพอหรือไม่
5. เพื่อทราบถึงแนวทางแก้ไขและปรับปรุงกฎหมายอาญาของไทยให้มีมาตรการที่เหมาะสมต่อไป

1.3 สมมติฐานของการศึกษา

การถูกคุกคามทางอินเตอร์เน็ตโดยบุคคลไม่พึงประสงค์ ก่อให้เกิดความเดือดร้อนรำคาญและถือเป็นการละเมิดสิทธิส่วนบุคคลบนเครือข่ายอินเตอร์เน็ตจนบางครั้งก่อให้เกิดปัญหาอาชญากรรม อันเป็นการยากต่อการควบคุมและป้องกันความเสียหาย จึงควรมีมาตรการออกมาป้องกันและลงโทษผู้กระทำผิดโดยการออกกฎหมายเพื่อเป็นการปรามผู้คุกคามและลงโทษต่อไป

1.4 ขอบเขตของการศึกษา

ศึกษาเฉพาะกรณีปัญหาการคุกคามทางอินเตอร์เน็ตผ่านทางจดหมายอิเล็กทรอนิกส์ เว็บบอร์ด และห้องสนทนาสดที่เกิดขึ้นในประเทศไทยและกฎหมายไทยที่เกี่ยวข้อง โดยศึกษามาตรการทางกฎหมายในประเทศที่มีความก้าวหน้าทางเทคโนโลยีเฉพาะประเทศสหรัฐอเมริกา เพื่อนำมาเปรียบเทียบกับกฎหมายไทยที่มีอยู่ เพื่อเสนอแนะแนวทางที่เหมาะสมในการพัฒนาแก้ไขและปรับปรุงกฎหมายต่อไป

1.5 วิธีการศึกษา

วิธีการดำเนินการวิจัยเป็นการวิจัยเอกสาร การรวบรวมข้อมูลที่ค้นคว้าจากหนังสือ อินเตอร์เน็ต กฎหมายต่างประเทศ (เฉพาะ ประเทศ สหรัฐอเมริกา มลรัฐ มิสซิสซิปปี้) บทความ สื่อสารสนเทศอื่นที่เกี่ยวข้อง

1.6 นิยามศัพท์

“อินเตอร์เน็ต ” (Internet) คือ เครือข่ายของการสื่อสารข้อมูลขนาดใหญ่ อันประกอบด้วยเครือข่ายคอมพิวเตอร์จำนวนมาก เชื่อมโยงแหล่งข้อมูลจากองค์กรต่าง ๆ ทั่วโลกเข้าด้วยกัน

“แชทรูม ” (Chat Room) คือ ห้องสนทนาใช้เพื่อการสนทนาผ่านเครือข่ าย อินเตอร์เน็ตโดยทันทีทันใด

“เว็บบอร์ด ” (Webboard) คือ เป็นพื้นที่จัดสรรไว้บนเครือข่ายคอมพิวเตอร์เพื่อสามารถตั้งคำถาม (กระทู้) และตอบคำถามจากบุคคลทั่วไป อาจเป็นการเข้าถึงพื้นที่สนทนาโดยตรงหรือการสมัครสมาชิก วิธีการโดยการตั้งคำถามทิ้งไว้ (Post)โดยรอผู้ที่ส นใจเข้ามาตอบ หรือแสดงความคิดเห็น (เสมือนเป็นการทำประชาพิจารณ์)

“สแปมเมล ” (Spam Mail) คือ จดหมายอิเล็กทรอนิกส์ หรือ อีเมล์ที่มีลักษณะเป็นการโฆษณา ซึ่งมักจะมีอยู่มากมายในวันหนึ่ง ๆ อีเมล์ลักษณะนี้มักจะถูกส่งไปหาคนจำนวนมาก รวมทั้งเมลลิ่งลิสต์ (Mailing List) และนิวส์กรุ๊ป (Newsgroup) ด้วย การหลีกเลี่ยงจดหมายหรือ อีเมล์ประเภทนี้สามารถทำ ได้โดยการไม่ประกาศหมายเลขอีเมล์ ของตนลงในอินเตอร์เน็ตง่าย ๆ (เช่น ไม่ใส่หมายเลขอีเมล์ ลงไปในเว็บบอร์ดสาธารณะ) ไม่สมัครบริการบนอินเตอร์เน็ตกับเว็บไซต์ใด ๆ โดยที่ไม่แน่ใจว่าเว็บไซต์ นั้น ๆ จะเก็บหมายเลข อีเมล์ของเราเอาไว้เป็นความลับและไม่นำไปขายหรือมอบให้กับบุคคลที่สาม

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้เข้าใจปัญหาและรูปแบบการคุกคามทางอินเตอร์เน็ต
2. ทำให้ทราบถึงผลกระทบที่เกิดขึ้นจากการคุกคามทางอินเตอร์เน็ต
3. ทำให้ทราบถึงขอบเขตแล ะองค์ประกอบความผิดเกี่ยวกับการคุกคามทางอินเตอร์เน็ตของประเทศสหรัฐอเมริกาโดยเฉพาะกฎหมายของมลรัฐมิสซิสซิปปี้
4. ทำให้ทราบถึงสภาพบังคับของกฎหมายอาญาของไทยว่าสามารถนำมาใช้บังคับกับความผิดเกี่ยวกับการคุกคามทางอินเตอร์เน็ตได้เพียงพอหรือไม่
5. ทำให้ทราบถึงแนวทางแก้ไขและปรับปรุงกฎหมายอาญาของไทยให้มีมาตรการที่เหมาะสมต่อไป

บทที่ 2
การกระทำความผิดเกี่ยวกับการคุกคามทางอินเตอร์เน็ต

2.1 นิยามการจำแนกประเภทของการคุกคาม (Stalking)

2.1.1 ความหมายและประเภทของการคุกคาม (Stalking)

ตามพจนานุกรมฉบับราชบัณฑิ ตยสถาน พ.ศ. 2542 ได้ให้ความหมายของคำว่า “คุกคาม” ว่าหมายถึง แสดงด้วยกิริยาหรือวาจาให้หวาดกลัว ทำให้หวาดกลัว เช่น ภัยคุกคาม ในบทกลอนใช้คำว่า คุกก็มี เช่น ไปขู่ไปคุก ไปรุกรุมตี. (สมุทรโฆษ)

ตามพจนานุกรม (Black ’s Law Dictionary 8th Edition) ได้ให้ความหมายของคำว่า Stalking ไว้ว่าหมายถึง การติดตามผู้อื่นอย่างลับ ๆ การกระทำความผิดโดยการติดตามหรืออยู่ใกล้ผู้อื่น โดยมากมักไม่ให้ผู้นั้นรู้ตัว ซึ่งมีจุดประสงค์เพื่อรบกวนหรือคุกคามผู้นั้น หรือเพื่อกระทำความผิดอย่างอื่นต่อไป เช่นทำร้ายหรือทุบตี นิยามตามกฎหมายบางฉบับรวมถึงองค์ประกอบที่ว่า ผู้ที่ถูกติดตามต้องรู้สึกอึดอัดรำคาญใจ หวาดกลัว หรือเป็นทุกข์กังวลถึงความปลอดภัยของตนหรือของผู้อื่นที่ตนต้องรับผิดชอบโดยมีเหตุอันควร บางนิยามกำหนดว่า การกระทำเช่นการโทรศัพท์ไปหาผู้อื่นแล้วไม่ยอมพูดก็ถือเป็นการคุ กคามด้วยเช่นกัน[1]

คำว่า Stalking ซึ่งโดยทั่วไปแล้วความหมายของคำว่า Stalking คือ การสะกดรอยติดตามไล่ล่าสัตว์ แต่คำดังกล่าวได้ถูกนำมาใช้ในการให้คำนิยามพฤติกรรมของบุคคลที่มีลักษณะคุกคามมีการกระทำทางกายภาพที่สื่อให้เห็นถึงการกระทำที่เป็นความผิด ซึ่งการคุกคามอยู่ในรูปแบบ ต่าง ๆ ที่ก่อให้เกิดความกลัว และปรา กฏอยู่ในรูปแบบที่เป็นการกระทำซ้ำ ๆ เช่น ได้รับการติดต่อจากผู้ที่ไม่เป็นที่พึงประสงค์ (ไม่ว่าโดยทางจดหมายหรือการสื่อสารในรูปแบบอื่น) สังเกตพฤติกรรมของบุคคลอื่นอย่างใกล้ชิดสำหรับช่วงระยะเวลาหนึ่ง หรือติดต่ อกับสมาชิกในครอบครัว เพื่อน หรือเพื่อนร่วมงานของเหยื่อหรือเป้าหมาย และรวมถึงการคุกคามทางอินเตอร์เน็ต ซึ่งในที่นี้ผู้ที่ทำการคุกคามจะเรียกว่า “ Stalker ”

---

[1] Bryan A. Garner, Black ’s Law Dictionary, 8th ed. (St. Paul : Minn West ,2004),p. 1440

โดยทั่วไปแล้วคำจำกัดความทางกฎหมายของคุกคามหรือ Stalking นั้น ประกอบด้วย 3 องค์ประกอบ ดังนี้[2]

(1) รูปแบบ (การกระทำในช่วงระยะเวลาหนึ่ง) ของการล่วงล้ำทางพฤติกรรมซึ่งขึ้นอยู่กับความไม่พอของบุคคลอื่น
(2) การคุกคามขู่เข็ญที่ไม่ชัดเจนหรือที่ชัดเจน ซึ่งจะถูกนำมาพิสูจน์ให้เห็นในทางรูปแบบของการล่วงล้ำทางพฤติกรรม
(3) เป็นผลของการล่วงล้ำทางพฤติกรรม คือบุคคลนั้นรู้ สึกว่าถูกคุกคามขู่เข็ญเกิดความกลัวอย่างมีเหตุผล

ในทางการแพทย์ได้ให้คำจำกัดความคำว่า Stalking ว่า “เป็นรูปแบบที่ผิดปกติหรือเป็นรูปแบบที่ใช้เวลานานของการคุกคามขู่เข็ญหรือการรบกวนต่อบุคคลใดบุคคลหนึ่งโดยเฉพาะโดยตรง ”[3] และรูปแบบของการคุกคามขู่เข็ญหรือ การรบกวนก็ได้มีการให้คำจำกัดความว่า “เป็นการกระทำที่ปรากฏชัดแจ้งเกินหนึ่งครั้ง ในลักษณะของการติดตามหรือไล่ตามซึ่งขัดต่อความประสงค์ของเหยื่อ และเหยื่อมีความรู้สึกว่าถูกรบกวน”[4]

ในทางจิตเวชศาสตร์ (Psychiatry) ได้นำคำว่า Stalking มาใช้ โดยหมายถึงกลุ่มของพฤติกรรมใด ๆ ก็ตามที่บุคคลหนึ่งใช้เพื่อสร้างความเดือดร้อนรำคาญ หรือก่อให้เกิดความเสียหายกับบุคคลที่ตกเป็นเป้าหมายโดยลักษณะของพฤติกรรมเหล่านี้จะเกิดขึ้นซ้ำ ๆ บ่อยๆ และดำเนินไปอย่างช้า ๆ ค่อยเป็นค่อยไป (Mullen , Pathe & Stuart, 1999)[5] เพื่อมุ่งคว ามประสงค์ที่จะก่อให้เหยื่อนั้นเกิดความหวาดกลัว (Goode,1995)[6] เช่น การสะกดรอยตามเหยื่อ การโทรศัพท์พูดจาข่มขู่ ใช้ถ้อยคำลามกหยาบคาย และรวมไปถึงการทำลายทรัพย์สินของเหยื่อด้วย

---

[2] วิจิตรา เลิศหิรัญกิจ, “ความผิดฐานเฝ้าติดตามและข่มขู่ Stalking,” (วิทยานิพนธ์ปริญญามหาบัณฑิตคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์,2550),หน้า 6.

[3] เรื่องเดียวกัน, หน้า 7.

[4] เรื่องเดียวกัน, หน้า 8.

[5] จอมพล พิทักษ์สันตโยธิน, “การตามรังควานบนอินเตอร์เน็ต(Cyberstalking)กับความผิดทางอาญาในสหรัฐอเมริกาและสหราชอาณาจักร,” วารสารวิชาการมนุษย์ศาสตร์และสังคมศาสตร์ 13, (กันยายน –ธันวาคม 2548): 51-65.

[6] เรื่องเดียวกัน.

จากการศึกษา ของนักจิตวิทยา พบสถิติว่า ประมาณ ร้อยละ 25 นั้นคุกคามเฉพาะตัวเหยื่อ และร้อยละ 8 คุกคามถึงบุคคลที่สาม และ ร้อยละ 33 คุกคามทั้งตัวเหยื่อและคุกคามบุคคลที่สามด้วย นอกจากนี้ทรัพย์สินที่เสียหายและเป็นเป้าหมายที่นิยมมากที่สุดของเหยื่อ คือ รถ และร้อยละ 36 ของผู้คุกคามนั้นเข้าถึงและทำร้ายเหยื่อ แต่ ร้อยละ 6 นั้นทำร้ายถึงบุคคลที่สาม [7] เมื่อพิจารณาจากสถิติดังกล่าวจึง ทำให้เราเล็งเห็นได้ว่าการคุกคามนั้นสามารถสร้างความเสียหายให้แก่ชีวิตและทรัพย์สินของเหยื่อได้ มิใช่เพียงแค่การรุกล้ำเข้าถึงสิทธิส่วนตัวของบุคคลหนึ่งบุคคลใดที่ตกเป็นเหยื่อเท่านั้น การคุกคามจึงกลายเป็นปัญหาที่อาจทวีความรุนแรงมากขึ้นหากไม่มาตรการทางกฎหมายหรือมาตรการทางสังคมมาแก้ไขปัญหาการคุกคามดังกล่าวนี้

จากการยอมรับสิทธิมนุษยชนการใช้สิทธิต่าง ๆ สามารถรับรองให้กระทำได้ตามกฎหมายแต่ต้องอยู่ในขอบเขตของการกระทำที่ไม่ผิดต่อกฎหมายและต้องไม่ละเมิดสิทธิหน้าที่ หรือความเป็นอยู่ของบุคคลอื่น ดังนั้น เมื่อทุกคนต่างก็ดำเนินชีวิตของตนเองภายใต้สิทธิที่กฎหมายรองรับก็ทำให้สังคมอยู่อย่างปกติสุข แต่ในปัจจุบันการดำรงชีวิตของบุคคลในสังคมต่างเปลี่ยนแปลงไปเพื่อความอยู่รอด ชีวิตของคนในสังคมอาจเกิดความกดดัน ความสับสนในพฤติกรรมของตนเอง จนอาจทำให้เกิดการรุกรานหรือรุกล้ำสิทธิของคนในครอบครัว ผู้ร่วมงานตลอดจนคนในสังคม บางครั้งอาจมีการรุกรานหรือรุกล้ำสิทธิของผู้อื่นนั้นจนอาจจะถึงขั้นที่เกิดการคุกคามบุคคลอื่น แต่หากการกระทำนั้นเป็นการกระทำที่ไม่ส่งผลกระทบต่อบุคคลอื่นเท่าใด นักก็อาจจะทำการแก้ไขหรือไกล่เกลี่ยกันไม่ให้เกิดปัญหา แต่หากมีผลกระทบคุกคามถึงสิทธิส่วนตัวความเป็นอยู่ในชีวิตประจำวัน สภาวะทางจิตใจ สภาพอารมณ์ ทรัพย์สิน ตลอดจนร่างกายและชีวิตแล้ว ย่อมถือว่าเป็นภัยคุกคามที่ผู้กระทำควรได้รับโทษตามกฎหมาย

[7] Mullen et al., 1999. “Study of Stalker” Internet. http://ajp.psychiatryonline.org/cgi/content/full.156/8/1244.

2.1.2 รูปแบบของการคุกคาม

การคุกคามอาจจะเกิดขึ้นโดยที่ผู้เสียหายหรือเหยื่ออาจจะไม่ทราบด้วยซ้ำว่าเกิดขึ้น และพวกที่ชอบคุกคามส่วนใหญ่มักจะคิดว่าผู้เสียหายหรือเหยื่อชอบการกระทำของผู้กระทำการคุกคาม หรือในบางรายคิดว่าเป็นการช่วยเหลือเหยื่อ ซึ่งแตกต่างจากการกระทำความผิดทางอาญาทั่วไปที่มีการกระทำผิดเพียงครั้งเดียว แต่การคุกคามจะเกิดในรูปแบบที่ต่อเนื่องและมีหลายการกระทำ หรือมีการทำซ้ำ ๆกัน นอกจากนี้การกระทำดังกล่าวนั้นจะถูกกฎหมายโดยตัวของมันเอง เช่น การโทรศัพท์ หรือส่งของขวัญ หรือการส่ง อีเมล์ พวกที่ชอบคุกคามนั้นมักจะมองเหยื่อเป็นสิ่งของชิ้นหนึ่งซึ่งทำให้เหยื่อรู้สึกโกรธ เกลียด บุคคลที่ชอบคุกคามอย่างไร้ความปราณี นอกจากนี้พวกชอบคุกคามมักจะคิดว่าตนเองนั้นสามารถทำอย่างไรกับเหยื่อก็ได้ โดยจะมองว่าเหยื่อเป็นพวกอ่อนแอ พึ่งตนเองไม่ได้ทำให้พวกที่ชอบคุกคามคิดว่ าเหยื่อเหล่านี้ต้องการความช่วยเหลือ หรือบางครั้งพวกชอบคุกคามจะคิดว่าเป็นการสมควรอย่างยิ่งที่จะต้องลงโทษเหยื่อตามที่พวกเขาเห็นสมควร นอกจากนี้แล้วพวกคุกคามมักจะทำให้เหยื่อนั้นตกอยู่ในความหวาดกลัวหรือวิตกกังวลว่าจะเกิดอันตรายกับตัวเหยื่อหรือครอบครัวรวมถึงคนใกล้ชิดของเหยื่อ ผู้คุกคามเหล่านี้จะรู้สึกมีอำนาจที่ได้ควบคุมเหยื่อ

นักจิตวิทยามักจะจัดกลุ่มของพวกคุกคามไว้เป็นสองประเภท[8] คือ

1. พวกที่เป็นโรคจิต หลายคนที่มีพฤติกรรมคุกคามบุคคลอื่นมักจะมีประวัติเป็นผู้ป่วยทางจิตมาก่อน เช่น อาการจิตหลงผิด หรือเป็นพวกแยกจากบุคคลอื่น โรคบุคคลมีหลายพฤติกรรม เช่น ต่อต้านสังคม ไม่สามารถเข้ากับสังคมได้ หรือเป็นพวกที่ไม่มีสังคมเข้าสังคมไม่เก่ง หรือคิดว่าสังคมนั้นไม่ยอมรับตนเอง จนทำให้เกิดการปลีกตัวออกจากสังคม มีอาการเบื่อโลก หรือหวาดระแวงไม่ไว้ใจสังคม ไม่ไว้ใจคนในสังคม หรือคนรอบข้าง

2. พวกที่ไม่ได้เป็นโรคจิตหรือพวกที่ไม่เคยมีประวัติป่วยทางจิต พวกที่ชอบคุกคามกลุ่มนี้มักจะทำการคุกคามโดยมีอิทธิพลมาจากปัจจัยทางจิตหลายประการเช่นกัน เช่น ความโกรธ ความเกลียด ความหมกหมุ่น ความอิจฉา และการถูกปฏิเสธ

[8] Wikipedia, the free encyclopedia. “Stalking” Internet. http://enwikipedia.org/wiki/stalking.

2.1.3 ลักษณะของบุคคลที่สามารถเป็นผู้คุกคาม[9]

พวกคุกคามส่วนใหญ่แล้วมักจะเป็นพวกที่แยกตัวหรือเป็นพวกที่โดดเดี่ยวหรือเกิดจากพวกที่เสียเปรียบในสังคม อย่างไรก็ตามบุคคลเหล่านี้อาศัยอยู่ในทุกที่ของสังคม บ่อยครั้งที่การกระทำความผิดของบุคคลเหล่านี้ถูกกระตุ้นจากบาดแผลความสูญเสียในชีวิต เช่น ปัญหาความสัมพันธ์ หรือการหย่าร้าง การถูกเลิกจ้าง ความสูญเสียหรือขาดความมั่นใจของเด็ก หรือครอบครัวที่มีปัญหา ส่วนมากพวกคุกคามไม่ใช่พวกโรคจิต และจากการศึกษาเปรียบเทียบ [10] พวกคุกคามที่เป็นโรคจิตและไม่ได้เป็นโรคจิตแล้วพบว่า ร้อยละ 63 ของกลุ่มตัวอย่างนั้นได้รับความเจ็บปวดจากสภาวะจิตใจในแบบธรรมดา เช่น ความกดดัน ความสับสนในพฤติกรรมของตนเอง และจากการวิจัยของผู้เชี่ยวชาญด้านจิตวิทยาซึ่งใช้เกณฑ์ที่แตกต่างกัน พบว่าส่วนมากคือ ผู้คุกคามที่มีความสับสนในพฤติกรรมของตนเอง นอกจากนี้บุคคลที่สามารถจะกลายเป็นผู้คุกคามได้ คือ

1. อดีตคนรัก โดยส่วนมากพวกคุกคามเหล่านี้มักจะเคยมีความสัมพันธ์ เคยรักเหยื่อมาก่อน และส่วนมากก็จะเป็นอดีตคนรักที่กลายเป็นเหยื่อเป็นเป้าหมายของพวกคุกคามนี้ ไม่ว่าจะเคยมีความสัมพันธ์กันในระยะเวลาสั้น ๆ หรือยาวนาน

2. สมาชิกในครอบครัว พวกคุกคามอาจจะมีเป้าหมายคือ บุคคลในครอบครัว เช่น ญาติหรือพี่น้อง เนื่องจากพวกคุกคามเหล่านี้เป็นพวกคุกคามที่มีความแค้นใจ ได้รับการปฏิเสธจากคนในครอบครัว หรือเคยถูกทำให้ขายหน้า เสื่อมเสียเกียรติ หรือในอดีตได้รับการล่วงละเมิดจากคนในครอบครัว

3. เพื่อน หรือคนคุ้นเคย เหยื่ออาจจะถูกคุกคามจากคนที่แสวงหาความใกล้ชิดในเชิงชู้สาว หรือคนที่เข้าสังคมไม่เก่ง ซึ่งคนเหล่านี้มักจะมีแรงจูงใจโดยอยากที่จะมีความสัมพันธ์ในเชิงชู้สาวกับเหยื่อ เหยื่ออาจจะถูกคุกคามจากพวกที่มีความแค้นใ จ หรือเพื่อนบ้านรอบข้างที่มีปัญหากับเหยื่อในเรื่องเสียงดัง เรื่องต้นไม้ที่เกะกะ หรือเรื่องสัตว์เลี้ยง

4. คนคุ้นเคยในที่ทำงาน ในการศึกษาตัวผู้คุกคาม พบว่าร้อยละ 23 นั้นมีความสัมพันธ์กับเหยื่อในทางหน้าที่การงาน ส่วนมากจะเป็นพวกปฏิบัติงานทางการแพทย์ หรือพวกคุกคามที่เป็นหัวหน้าเหยื่อ ลูกจ้างผู้ชาย ผู้ให้บริการ หรือลูกค้า หรือคนอื่น ๆ ที่แสดงตัวในที่ทำงานของเหยื่อ และอาจมีพฤติกรรมที่อาจจะทำกับเหยื่อโดยตรง เช่น

---

[9] P. E. Mullen, Type of Stalker and Stalking Patterns. Internet. http://www.sexual harassmentsupport.org/TypesofStalker.html.

[10] Mullen et al., 1999. “Study of Stalker” Internet. http://ajp.psychiatryonline.org/cgi/content/ful.156/8/1244.

คุกคามทางเพศ ล่วงละเมิดทางกาย ทำให้เสียชื่อเสียง โจรกรรม หรือแม้กระทั่งฆาตกรรม บ่อยครั้งความรุนแรงของพวกคุกคามในสถานที่ทำงาน คือ พวกที่มีประวัติในการทำงานที่ไม่ดี มีอัตราการละเว้นหรือไม่มาทำงานสูง และมีประวัติการข่มขู่หรือเผชิญหน้ากับคนที่ตนเองแค้นใจ หรือไม่พอใจในสถานที่ทำงาน กระทรวงยุติธรรมของสหรัฐอเมริกาพบว่าในระหว่างปี ค.ศ. 1992-1996 มากกว่า 2 ล้านคนประสบอาชญากรรมความรุนแรงในสถานที่ทำงาน ซึ่งได้แก่

a. จำนวน 1.5 ล้านคนที่ถูกทำให้เสียชื่อเสียง
b. 51,000 คน ถูกข่มขืนกระทำชำเรา
c. 84,000 คน ถูกโจรกรรม
d. มากกว่า 1,000 คน ถูกฆาตกรรม

บ่อยครั้งที่เหยื่อจะไม่บอกเพื่อนร่วมงานหรือหัวหน้า งานเกี่ยวกับคนที่คุกคามเพราะ เหยื่อกลัวการโต้ตอบด้วยกำลังจากผู้คุกคามหรือผู้คุกคามที่เป็นลูกจ้างหรือนายจ้าง เหยื่อจึงมักคิดว่าไม่มีใครเชื่อหรือรู้สึกลำบากใจกับสถานการณ์แบบนี้

แพทย์ พยาบาล หรือนักจิตวิทยา หรือผู้ให้บริการด้านสุขภาพอาจจะกลายมาเป็นเป้าหมายของการคุกคามโดยตัวลูกค้าหรือตัวผู้ป่วย (หรือโดยวิธีอื่นรอบ ๆ ตัว) ครูอาจารย์อาจจะถูกคุกคามโดยนักเรียน (หรือโดยวิธีอื่นรอบ ๆ ตัว) นักจิตวิทยาเป็นส่วนหนึ่งที่มีความเสี่ยงในการกลายเป็นเป้าหมายของผู้คุกคามเพราะนักจิตวิทยาต้องติดต่อกับคนอื่นทั่วไปและต้องติดต่อกับพวกที่มีสภาวะทางจิต

5. คนแปลกหน้า บุคคลกลุ่มนี้มักจะเป็นพวกแสวงหาความใกล้ชิด หรือเป็นพวกที่ไม่มีความสามารถในการเข้าสังคม บางครั้งรวมถึงพวกที่มีพฤติกรรมไล่ล่าหรือพวกที่มีความแค้นใจด้วย คนกลุ่มนี้จะซ่อนลักษณะตัวตนของตนเองกับเหยื่อเอาไว้ใ นครั้งแรกและจะเปิดเผยหลังจากคุกคามเหยื่อในช่วงระยะเวลาหนึ่งเพื่อให้ได้ใกล้ชิดกับเหยื่อมากขึ้น ครั้งแรกเหยื่ออาจจะได้รับการยกย่องและปฏิบัติอย่างสุภาพเมื่อผู้คุกคามเข้าใกล้ เหยื่ออาจจะตอบตกลงในการนัดครั้งแรกกับผู้คุกคามหลังจากที่ได้รับคำเชิญ สิ่งนี้จึงกล ายเป็นผลกระทบที่ไม่ได้เกิดจากความตั้งใจในการกระตุ้นผู้คุกคาม ทำให้ผู้คุกคามคิดว่าได้มีการแลกเปลี่ยนความรักให้แก่กันและกันแล้ว

6. เพศ ผู้คุกคามส่วนมากแล้วจะเป็นผู้ชาย อย่างไรก็ตามผู้หญิงก็สามารถกลายเป็นผู้คุกคามได้เช่นเดียวกัน ผู้หญิงมักจะเป็นเหยื่อของ ใครคนหนึ่งซึ่งรู้จักพวกเธอบ่อยครั้งจะเป็นผู้มีติดต่อกันทางหน้าที่การงาน และเป็นจำนวนน้อยที่ผู้ชายจะถูกติดตามด้วยผู้ชาย ในขณะที่ผู้หญิงจะเป็นเป้าหมายของผู้หญิงด้วยกัน ส่วนมากผู้คุกคามที่เป็นหญิงมักจะเป็นพวกที่แสวงหาความใกล้ชิดและต้องการพิสูจน์ความสัม พันธ์ของตนเอง ในขณะที่ผู้ชายนั้นมักจะแสวงหาความใกล้ชิดเพื่อฟื้นฟูความสัมพันธ์ของตนเอง ผู้หญิงนั้น

อาจจะใช้ความรุนแรงเช่นเดียวกับผู้ชายและไม่มีความโน้มเอียงในความแตกต่างในเรื่องเพศที่เกี่ยวกับระยะเวลาในการคุกคาม ดังนั้น ขณะที่สิ่งรอบข้างและแรงจูงใจในการคุกค ามจะแตกต่างกัน หากแต่พฤติกรรมการรุกล้ำสิทธิและศักยภาพความรุนแรงที่เกิดจากการคุกคามนั้นสร้างความเสียหายไม่แตกต่างกัน

2.1.2 ลักษณะของบุคคลที่ตกเป็นเหยื่อ

บุคคลที่สามารถตกเป็นเหยื่อนั้นแบ่งออกได้ ดังนี้[11]

1. บุคคลที่มีชื่อเสียง (Celebrities)

บุคคลที่มีชื่อเสียงนั้นสามารถตกเป็นเป้าหมายและกลายเป็นเหยื่อ เนื่องจากเสน่ห์หรือแรงดึงดูดใจที่มีอยู่มาก และชีวิตความเป็นอยู่ที่มีชื่อเสียงในสังคม จากความชื่นชอบและความมีชื่อเสียงเป็นที่รู้จักในสังคมนั้น การแสดงความพึงพอใจอาจเป็นแค่เพียงการส่งจดหมายในฐานะคนที่มีความ นิยมชมชอบ แต่บางครั้งการแสดงความพึงพอใจของคนบางประเภทนั้นมีมากกว่าปกติมีความต้องการที่จะติดต่อบุคคลที่มีชื่อเสียงเหล่านั้น เช่น ดารา นักร้อง นักแสดง บุคคลกลุ่มนี้อาจจะถูกติดต่อหรือติดตามได้ง่าย นอกจากนี้บุคคลที่มีบุคลิกลักษณะพิเศษ เช่น เพื่อนบ้านหญิงที่มีความสวย หรือบุคคลที่มีชื่อเสียงแต่เป็นคนที่น่ารังเกียจก็อาจจะตกเป็นเหยื่อของการคุกคามได้เช่นเดียวกัน

2. บุคคลธรรมดาทั่วไป

บุคคลธรรมดาทั่วไปก็สามารถถูกคุกคามได้เช่นเดียวกันโดยไม่จำเป็นต้องมีชื่อเสียง เนื่องจากบุคคลธรรมดานั้นอาจถูกคุ กคามได้จากคนแปลกหน้า อดีตแฟนเก่า หรือถูกคุกคามจากนายจ้างหรือเพื่อนร่วมงานที่มีความอิจฉาริษยา หรือลูกค้าที่มาติดต่องาน

ดังนี้จึงเห็นได้ว่าบุคคลทุกคนสามารถตกเป็นเป้าหมายและกลายเป็นเหยื่อได้ ไม่ว่าจะเป็นคนที่มีชื่อเสียงหรือคนธรรมดาทั่วไป นอกจากนี้แล้วโดยส่ วนมากผู้หญิงมักจะเป็นเหยื่อมาก กว่าผู้ชาย และผู้ชายก็มีแนวโน้มหรือพฤติกรรมที่จะเป็นผู้คุกคามมากกว่าผู้หญิง แต่ไม่ว่าจะเป็นหญิงหรือชายก็สามารถเป็นเหยื่อหรือเป็นผู้คุกคามได้เช่นเดียวกัน

[11] วิจิตรา เลิศหิรัญกิจ, ความผิดฐานเฝ้าติดตามและข่มขู่ Stalking ,หน้า 13.

ในการศึกษาบุคคลที่มีพฤติกรรมคุกคามโดยนักจิตวิทยา Mullen (2000)[12] ได้ระบุลักษณะบุคคลที่มีพฤติกรรมคุกคามไว้ 6 แบบ ดังนี้[13]

1. พวกคุกคามที่ถูกปฏิเสธ (Rejected Stalkers) คือพวกที่มีพฤติกรรมที่จะคุกคามบุคคลอื่นด้วยการแก้ไข แก้แค้น เปลี่ยนแปลง การปฏิเสธที่ตนเองได้รับ เช่นจากการหย่า แยกทาง หรือถูกจำกัด

2. พวกคุกคามอันเกิดจากความไม่พอใจ (Resentful Stalkers) ติดตามด้วยความพยาบาทเพราะความแค้นใจที่มีต่อเหยื่อ โดยมีแรงจูงใจจากความต้องการที่จะทำให้เหยื่อเกิดความหวาดกลัวและความเครียด

3. พวกแสวงหาความใกล้ชิด (Intimacy Seekers) ทำเพื่อจะได้ใกล้ชิด มีความสัมพันธ์เชิงชู้สาวกับเหยื่อ โดยบุคคลเหล่านี้คิดว่าเหยื่อคือบุคคลที่ฟ้ากำหนดให้มาอยู่คู่กัน

4. พวกคุกคามที่มีพฤติกรรมเพื่อการมีเพศสัมพันธ์ (Eroto-manic Stalker) โดยบุคคลเหล่านี้มักจะคิดว่าเหยื่อนั้นหลงรักกับตนหรืออาจจะหลอกตัวเองว่าตนมีบางสิ่งลึกซึ้ งกับคนดังหรือดาราเป็นต้น

5. บุคคลที่ไม่มีความสามารถ (Incompetent-Suitor) เข้าสังคมไม่เก่ง มีพฤติกรรมคุกคามเหยื่อที่เป็นที่ชื่นชอบของคนในสังคม

6. พวกคุกคามที่มีพฤติกรรมแบบล่าเหยื่อ (Predatory Stalker) คือจะวางแผนและเตรียมการคุกคามเหยื่อโดยส่วนมากจะทำเพื่อการมีเพศสัมพันธ์กับเหยื่อ

2.1.5 ผลกระทบจากปัญหาการคุกคาม[14]

การคุกคามนั้นถือเป็นรูปแบบหนึ่งของการทำร้ายจิตใจโดยการบุกรุกเข้าไปสู่ชีวิตของเหยื่อโดย มีไม่ความสัมพันธ์ใด ๆ กับตัวเหยื่อ และการคุกคามไม่ได้เกิดขึ้นจากเหตุการณ์เดียว หากแต่เป็นขั้นตอนที่เกิดขึ้ นอย่างต่อเนื่องกันการคุกคามจะทำให้เหยื่อเกิดความกลัว หรือทำให้เหยื่อนั้นอยู่ในภาวะที่เสี่ยงต่ออันตรายจนอาจจะทำให้เหยื่อนั้นเป็นโรคจิต นอกจากนั้นยังอาจเป็นอันตรายต่อร่างกาย ซึ่งปัญหาการคุกคามนอกจากจะมี

---

[12] P. E. Mullen, Type of Stalker and Stalking Patterns. Internet. http://www.sexual harassmentsupport.org/TypesofStalker.html.

[13] Ibid.

[14] Wikipedia, the free encyclopedia. “Stalking” internet. http://en.wikipedia.org/wiki/ stalking.

ความผิดทางกฎหมายแล้วยังส่งผลกระทบต่อเหยื่อเป็นอย่า งมากไม่ว่าจะมีผลทางด้านอารมณ์ จิตใจ และการใช้ชีวิตประจำวัน และที่สำคัญความปลอดภัยในชีวิตและทรัพย์สินไม่ว่าจะเป็นของเหยื่อเองหรือของบุคคลที่มีความสัมพันธ์ใกล้ชิดกับเหยื่อ ซึ่งสามารถแยกได้ดังนี้

ผลกระทบต่ออารมณ์และสภาพจิตใจของเหยื่อ[15]

1. ปฏิเสธและสงสัยในตนเอง (เหยื่อไม่มีความเชื่อว่าจะเกิดสิ่งใดขึ้นกับตนและสงสัยการรับรู้ของผู้อื่น)
2. โทษตัวเอง
3. รู้สึกผิดละอาย หรือเสียหน้า
4. หงุดหงิด รำคาญใจ
5. มีความมั่นใจต่ำ
6. โมโห รู้สึกรุนแรงต่อผู้คุกคาม
7. ตกใจสับสน
8. ไม่มีความปลอดภัยและระวังตัวตลอดเวลา
9. อารมณ์เปลี่ยนแปลงบ่อยมากอย่างไม่มีเหตุผล
10. หมดความเชื่อมั่นและไว้ใจในบุคคลอื่น
11. ลดความสามารถในการทำงานหรือเรียน
12. มีปัญหาในการมีความสัมพันธ์กับบุคคลอื่น
13. แยกตัวไม่ติดต่อกับใคร
14. นึกถึงแต่อดีต สะเทือนใจ
15. รู้สึกอยากฆ่าตัวตาย

ผลกระทบต่อสภาพร่างกาย[16]

1. เกิดฝันร้ายและนอนไม่หลับ
2. มีปัญหาเรื่องเพศสัมพันธ์
3. เหนื่อยล้า
4. ส่งผลกระทบต่อโรคลมในกระเพาะอาหาร
5. น้ำหนักลดลงอย่างรวดเร็ว
6. ปวดหัว วิงเวียน ร่างกายไม่แข็งแรง เจ็บป่วยง่าย

---

[15] Wikipedia, the free encyclopedia. “Stalking” internet. http://en.wikipedia.org/wiki/stalking.

[16] Ibid.

7. หัวใจเต้นแรงและเหงื่อออก
8. อาจรักษาตนเองหรือความเครียดด้วยเหล้าหรือยาเสพติด

2.2 ปัญหาและผลกระทบจากการคุกคามทางอินเตอร์เน็ต (Cyberstalking)

2.2.1 ความหมายของการคุกคามทางอินเตอร์เน็ต

ตามพจนานุกรม (Black 's Law Dictionary 8th Edition) ได้ให้ความหมายของคำว่า Cyberstalking ไว้ว่า การข่มขู่ คุกคาม หรือรบกวนบุคคลอื่นโดยใช้จดหมายอิเล็กทรอนิกส์ (อีเมล์) จำนวนหนึ่งส่งผ่านทางอินเตอร์เน็ต โดยเฉพาะ อย่างยิ่งเมื่อมีเจตนาจะทำให้ผู้รับเกิดความกลัวว่าจะเกิดการกระทำที่ผิดกฎหมาย อันตราย หรือความเสียหายแก่ผู้รับหรือคนในครอบครัวหรือคนในบ้านของผู้รับ[17]

อินเตอร์เน็ตเป็นเครื่องมือที่มีพลังมีก้าวหน้าทางเทคโนโลยีสูงนำมาซึ่งยุคแห่งข้อมูลสมัยใหม่ แต่หากถูกนำมาใช้อย่างผิด ๆ ก็อาจเป็นอันตรายอย่างร้ายแรงและอาจถึงตายได้ เช่น การได้รับข้อความที่ว่า

" ต้องการนักเขียนหญิง ซึ่งไม่มีข้อจำกัดในจินตนาการและแฟนตาซี ชื่นชอบการมีเพศสัมพันธ์ทั้งแบบกลุ่มและแบบรุนแรง ..... หากสนใจ แวะมาได้ที่ .....(ที่อยู่).... โทร. ได้ทั้งกลางวันและกลางคืนที่เบอร์ ..... เราสัญญาว่า คุณจะได้ทุกอย่างที่คุณฝันถึง ตอบโฆษณานี้ถ้าคุณจริงจังเท่านั้น "[18] หรือ ข้อความที่ปรากฏอยู่ใน อีเมล์ว่า "ฉันเป็นฝันร้ายที่สุดของคุณ ปัญหาทั้งหลายกำลังจะเริ่มขึ้น "[19] หรือเมื่อผู้หญิงคนหนึ่งพบว่าเว็บไซต์หนึ่งมีข้อความดังต่อไปนี้ปรากฏอยู่ และพบว่า ตัวเธอเองเป็นผู้หญิงที่ปรากฏอยู่ในข้อความที่ว่านี้ " ตอนนี้ฉันซึมเศร้ามาก อืมมม ...เหมือนเป็นการฆ่าตัวตายสำหรับฉัน รถชน? กรีดข้อมือ? สองสามวันต่อมา ฉันถามตัวเองว่า "ทำไมฉันจะไม่ฆ่าเธอด้วยนะ"[20]

ข้อความทั้งหมดนี้เป็นตัวอย่างของการคุกคามทางอินเตอร์เน็ต (Cyberstalking) โดยทั่วไปการคุกคาม (Stalking) คือ พฤติกรรมการรังควานและข่มขู่ซ้ำ ๆ และด้วยความก้าวหน้าทางเทคโนโลยีก็มีอาชญากรรมชนิดใหม่นี้เกิดขึ้น คือ การคุกคามทาง

---

[17] Bryan A. Garner, Black 's Law Dictionary, 8th ed. p.415.

[18] Naomi H. Goodno, "Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws," The Berkeley Electronic Press ,(2006) : 1- 62.

[19] Ibid.

[20] Ibid., p. 2.

อินเตอร์เน็ต การคุกคามทางอินเต อร์เน็ตจะเกี่ยวข้องกับการใช้อินเตอร์เน็ต อีเมล์ หรือการติดต่อสื่อสารทางอิเล็กทรอนิกส์โดยวิธีอื่นในการคุกคามหรือรังควานข่มขู่บุคคลอื่น และการใช้เทคโนโลยีทางอิเล็กทรอนิกส์ก็ทำให้ผู้คุกคาม (Stalker) มีช่องทางในการข่มขู่คุกคามหรือตามรังควานเหยื่อของตนเพิ่มขึ้น

ปัญหาการคุกคามทางอินเตอร์เน็ต (Cyberstalking) คือ การคุกคามหรือรุกล้ำสิทธิส่วนบุคคลในวิธีการที่ก่อให้เกิดความกลัวต่อเหยื่อทางอิเล็กทรอนิกส์ ปัญหาการรบกวนและการคุกคามนั้นมีหลายรูปแบบด้วยกันบนโลกของอินเตอร์เน็ตแต่สิ่งที่เหมือนกันของปัญหาการคุ กคามในรูปแบบธรรมดาและการคุกคามทางอินเตอร์เน็ต (Cyberstalking)นั่นคือมีการเคลื่อนไหวตลอดเวลาของการคุกคามและมีความต้องการที่จะควบคุมเหยื่อหรือผู้เสียหายจนกว่าการกระทำของตนนั้นจะบรรลุผล ผู้กระทำการคุกคามโดยส่วนใหญ่แล้วจะเป็นผู้ชายมากกว่าผู้หญิงและผู้เสี ยหายหรือเหยื่อจะเป็นผู้หญิงมากกว่าผู้ชาย ในหลาย ๆ กรณีที่ผู้คุกคามและผู้เสียหายหรือเหยื่อนั้นเคยมีความสัมพันธ์กันมาก่อน และการคุกคามทางอินเตอร์เน็ตนั้นก็จะเริ่มขึ้นเมื่อผู้เสียหายหรือเหยื่อนั้นพยามทำการตัดความสัมพันธ์ อย่างไรก็ตามการคุกคามทางอินเตอร์ เน็ตอาจจะเกิดขึ้นจากคนแปลกหน้า จากการให้ข้อมูลส่วนบุคคลผ่านทางอินเตอร์เน็ต ทำให้เกิดการคุกคามทางอินเตอร์เน็ตโดยวิธีการเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับตัวของเหยื่ออย่างง่ายดายเพียงการคลิ๊กเม้าส์ไม่กี่ครั้ง

การคุกคามทางอินเตอร์เน็ตนั้นไม่มีการติดต่อกันทางกา ยภาพจนอาจทำให้เกิดความเข้าใจในทางที่ผิดว่ามีความรุนแรงน้อยกว่าการถูกคุกคามธรรมดา ซึ่งเป็นความเข้าใจในทางที่ผิดเมื่ออินเตอร์เน็ตได้กลายมาเป็นส่วนสำคัญในการใช้ชีวิตของเรา ผู้คุกคามจึงอาศัยข้อได้เปรียบของการติดต่อสื่อสารที่ง่ายของระบบอินเตอร์เน็ตในการเข้าถึ งข้อมูลส่วนบุคคล และคุณลักษณะพิเศษบางประการของการติดต่อสื่อสารกันทางอินเตอร์เน็ตที่ส่งเสริมให้เกิดการคุกคามทางอินเตอร์เน็ต เนื่องจากผู้คุกคามนั้นไม่ต้องการเผชิญหน้ากับตัวเหยื่อ จึงส่งการติดต่อสื่อสารที่มีลักษณะรบกวนหรือคุกคามไปยังเหยื่อ นอกจากนี้การคุกคามทางอินเตอร์เน็ตนั้นทำให้ผู้คุกคามนั้นอยู่ในตำแหน่งที่ได้เปรียบกว่าการคุกคามแบบธรรมดา เนื่องจากตัวผู้คุกคามอาจอยู่คนละประเทศ คนละเมือง หรืออยู่ที่ทำงานถัดไป และผู้กระทำการคุกคามอาจเป็นเพื่อนเก่าหรือคนรักเก่า หรือคนแปลกหน้าก็ได้ รวมถึงการคุกคามที่เกิดจากเด็กวัยรุ่นที่ต้องการล้อเล่นเท่านั้น นอกจากนี้การที่ไม่สามารถระบุได้ถึงแหล่งที่มาของการรบกวนหรือการคุกคามทางอินเตอร์เน็ตอาจเป็นเหตุร้ายกับตัวผู้ถูกคุกคามหรือเหยื่อ ทั้งนี้จากสภาพของการที่ไม่เปิดเผย ไม่สามารถระบุตัวตนหรือแหล่งที่มา

ของการคุกคามอาจก่อใ ห้เกิดการกระทำความผิดที่มีลักษณะต่อเนื่อง และบางรายอาจพยายามกระทำการคุกคามเหยื่อหรือทำการรุกรานผู้เสียหายถึงที่บ้านหรือที่ทำงาน

ปัญหาการคุกคามทางอินเตอร์เน็ตกลายเป็นปัญหาที่เพิ่มมากขึ้นและทวีความรุนแรงมากขึ้นเนื่องจากโลกของอิเล็กทรอนิกส์หรือบนโลกของอินเ ตอร์เน็ตนั้นไม่มีขอบเขต ปัญหาดังกล่าวได้ปรากฏเด่นชัดและเพิ่มมากขึ้นในประเทศสหรัฐอเมริกาซึ่งเป็นประเทศที่มีความก้าวหน้าทางด้านเทคโนโลยีคอมพิวเตอร์และโลกของอินเตอร์เน็ต ผู้ให้บริการอินเตอร์เน็ตบางรายในประเทศสหรัฐอเมริกาได้รวบรวมสถิติและประเภทของการร้อง เรียนเกี่ยวกับการรบกวนหรือการคุกคามสมาชิก รวมถึงหน่วยงานที่บังคับใช้กฎหมายก็ได้รวบรวมปัญหาการคุกคามทางอินเตอร์เน็ตที่เพิ่มมากขึ้น ดังนี้[21]

ประการแรก จากการสำรวจการใช้ความรุนแรงต่อผู้หญิงนั้นได้ระบุว่าการคุกคามเป็นเหตุการณ์ที่ทำให้ผู้เสียหายหรือเหยื่อนั้ นเกิดความกลัวในระดับสูง ผู้หญิง 1 ใน 12 คน (8.2 ล้านคน) และผู้ชาย 1 ใน 45 คน (2 ล้านคน) ในสหรัฐอเมริกาได้เคยถูกคุกคามมาก่อนในชีวิต และร้อยละ 1 ของผู้หญิงทั้งหมดและร้อยละ 0.4 ของผู้ชายทั้งหมดถูกคุกคามในระหว่างรอบ 12 เดือนที่ผ่านมา นอกจากนี้ผู้หญิงจะถูกคุกคามมากกว่าผู้ชาย โดย 4 ใน 5 ของผู้เสียหายหรือเหยื่อนั้นจะเป็นผู้หญิง โดยที่ผู้ชายจะเป็นผู้คุกคามมากกว่า และจากการสำรวจร้อยละ 87 ของผู้คุกคามที่ผู้เสียหายระบุไว้ในการสำรวจคือ ผู้ชาย และผู้หญิงจะถูกคุกคามโดยคนแปลกหน้ามากกว่าผู้ชายถึง 2 เท่าและ 8 ครั้งของผู้เสียหายหรือเหยื่อถูกคุกคามโดยคนใกล้ชิด

ประการที่สอง การรวบรวมหลักฐานจากหน่วยงานต่าง ๆที่เป็นผู้บังคับใช้กฎหมายระบุว่าการคุกคามทางอินเตอร์เน็ตเป็นปัญหาที่รุนแรงและกำลังขยายตัวจากระดับมลรัฐไปสู่ระดับรัฐบาลกลาง ประเด็นต่าง ๆมากมายได้นำขึ้นสู่สำนั กงานอัยการของสหรัฐอเมริกาโดยหน่วยงานสอบสวนสืบสวนของกรมตำรวจประเทศสหรัฐอเมริกาหรือ FBI และได้เริ่มต้นทำการศึกษากรณีการคุกคามทางอินเตอร์เน็ตหรือ Cyberstalking โดยการศึกษาของสำนักงานอัยการประจำแขวงลอสแองเจิลสิสได้ประมาณการว่า อีเมล์หรือการติดต่อโดยสื่ออิเล็กท รอนิกส์อื่น ๆ นั้นเป็น ปัจจัยต่อการเกิดการคุกคามประมาณ ร้อยละ 20 จาก 600 กรณี และหัวหน้าหน่วยการกระทำความผิดทางเพศในสำนักงานอัยการแขวงแมนฮัตตันยัง

---

[21] U.S the Attorney General, 1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry, A Report from the Attorney General to the Vice President. Internet. http://www.usdj.gov/criminal/cybercrime/cyberstalking.htm.

ได้ประมาณว่าประมาณ ร้อยละ 20 ของคดีที่ได้รับการสะสางและจัดการนั้นจะเกี่ยวข้องกับการคุกคามทางอิเล็กทรอนิกส์ นอ กจากนี้หน่วยงานเทคโนโลยีและการตรวจสอบคอมพิวเตอร์ของสำนักงานตำรวจกรุงนิวยอร์กระบุว่า ร้อยละ 40 ของคดีเกี่ยวข้องกับการรบกวนและการคุกคามทางอินเตอร์เน็ต และทั้งหมดนี้ได้เกิดขึ้นในรอบ 3-4 ปีที่ผ่านมา

ประการที่สาม ผู้ให้บริการอินเตอร์เน็ตยังได้รับข้อร้องเรีย นจำนวนมากขึ้นเกี่ยวกับพฤติกรรมการรบกวนและการคุกคามทางอินเตอร์เน็ต ผู้ให้บริการอินเตอร์เน็ตหลักรายหนึ่งระบุว่าได้รับการร้องเรียนประมาณ 15 ครั้งต่อเดือนเกี่ยวกับการคุกคามทางอินเตอร์เน็ตหรือCyberstalking

ประการสุดท้าย การศึกษาเกี่ยวกับผู้เสียหายทางเพศของวิ ทยาลัยหญิง โดยนักวิจัยของมหาวิทยาลัยซินซินเนติได้รวบรวมโดยการสุ่มสอบถามทางโทรศัพท์จำนวน 4,446 คน โดยการสอบถามได้กระทำขึ้นในระหว่างปี 2539 ถึง ปี 2540 โดยการตรวจสอบเหตุการณ์ว่าเคยถูกติดตามหรือคุกคามโดยวิธีการเฝ้ามอง ติดตาม โทรศัพท์ เขียนหรือส่ง อีเมล์หรือมีการติดต่อโดยวิธีอื่นอันทำให้เกิดความกลัวเกิดความวิตกกังวลต่อความปลอดภัยบ้างหรือไม่ พบว่าผู้หญิงจำนวน 581 คน (ร้อยละ 13.1) ถูกคุกคามและเกิดเหตุการณ์มากถึง 696 เหตุการณ์และบางเหตุการณ์เกิดขึ้นมากกว่า 1 ครั้ง ซึ่งเป็นผู้หญิงจำนวน ร้อยละ 15 ที่ประสบเหตุมากกว่า 1 ครั้ง และในเหตุการณ์ทั้งหมด 696 ครั้ง ดังกล่าวพบว่ามี 166 ครั้งที่คุกคามทาง อีเมล์ หรือคิดเป็น ร้อยละ 24.7 ดังนั้นการถูกคุกคามของผู้หญิงในมหาวิทยาลัยจึงมีความเกี่ยวข้องหรือถือได้ว่าเป็นการคุกคามทางอิเล็กทรอนิกส์หรือการใช้อินเตอร์เน็ตเป็นเครื่องมือในการคุกคาม

จากปัญหาดังกล่าวข้างต้นนั้นทำให้เล็งเห็นได้ว่าการคุกคามทางอินเตอร์เน็ตนั้นจะทวีความรุนแรงและขยายตัวมากขึ้นตามความเจริญก้าวหน้าทางด้านเทคโนโลยี นอกจากนี้ไม่ว่าจะเป็นเพศหญิงหรือเพศชายนั้นก็สามารถตกเป็นเหยื่อของการคุกคามได้เช่นเดียวกัน เพียงแต่ปริมาณของการถูกคุกคามนั้นจะเกิดขึ้นกับเหยื่อที่เป็นเพศหญิงมากกว่าเพศชาย และการคุกคามทางอินเตอร์เน็ตนั้นมีด้วยกันหลายรูปแบบด้วยกันตามความเจริญก้าวหน้าทางด้านเทคโนโลยีด้านคอมพิวเตอร์และอินเตอร์เน็ตจึงเป็นการสมควรอย่างยิ่งที่ควรจะได้ศึกษาถึงรูปแบบของการคุกคามทางอินเตอร์เน็ตต่อไป

2.2.2 รูปแบบของการคุกคามทางอินเตอร์เน็ต

โดยทั่วไปการคุกคามทางอินเตอร์เน็ตหรือ Cyberstalking ปรากฏได้หลายรูปแบบ แตกต่างกันไปตามลักษณะของการใช้งานอินเตอร์เน็ต โดยผู้คุกคามนั้นมักจะมุ่งหรือประสงค์ต่อเหยื่อโดยการใช้ระบบออนไลน์ ทั้งหลายไม่ว่าจะเป็นการใช้กระดานสนทนา (Webboard) ห้องแชท (Chat Room) การส่งสแปมเมล (Spam Mail) โดยผู้คุกคามเหล่านี้จะคุกคามผ่านการสนทนา หรือส่งเมล หรือไวรัส โดยทำการส่งข้อความหรือรูปแบบลักษณะดังกล่าวอย่างต่อเนื่อง หรือซ้ำ ๆ กัน หรือวิธีที่เกิดขึ้น นบ่อย ๆ ที่ปรากฏในการคุกคาม คือการลงข้อความ(Post)ในทางเสียหายหรือใส่ร้ายตามกระดานสนทนาต่าง ๆ ต่อบุคคลที่สามซึ่งสามารถเข้าถึงข้อความที่ปรากฏอยู่บนกระดานสนทนา หรือ เพื่อจะทำให้เกิดการโต้ตอบจากเหยื่อ หรือทำให้เหยื่อติดต่อกลับมาหาตน เมื่อได้รับการโต้ตอบห รือได้รับการติดต่อจากเหยื่อแล้ว ผู้คุกคามก็จะพยายามตามแกะรอย IP Address[22] ของเหยื่อเพื่อที่จะได้ทราบว่าเหยื่อมีที่อยู่หรือมีที่ทำงานที่ใด

การคุกคามทางอินเตอร์เน็ตนั้นเกิดขึ้นง่ายกว่าการคุกคามในรูปแบบธรรมดา เพราะอุปกรณ์ทางอิเล็กทรอนิกส์ต่าง ๆ เช่น อีเมล์ (E-Mail) อินเตอร์เน็ต (Internet) หรือห้องสนทนาสด (Chat Room) ต่าง ๆ เหล่านี้ได้อำนวยความสะดวกให้กับผู้ไม่หวังดีที่จะติดต่อเพื่อทำการคุกคามเหยื่อ โดยบุคคลหนึ่งซึ่งเป็นผู้คุกคามสามารถส่ง อีเมล์ ผ่านทางอินเตอร์เน็ตให้กับคนเป็นจำนวนร้อย ๆ คนเพียงแค่การ คลิ๊กหรือการกดปุ่มหนึ่งครั้งซึ่งเป็นการประหยัดเวลากว่าการส่งจดหมายหรือการโทรศัพท์หลายเท่าตัว หรือผู้คุกคามหนึ่งคนนั้นสามารถทำการคุกคามเหยื่อหรือผู้เสียหายได้เป็นจำนวนร้อย ๆ คน เพียงแค่การกดปุ่มหนึ่งครั้งเช่นกัน วิธีการคุกคามทางอิเล็กทรอนิกส์นั้นส่วนใหญ่มี ปัจจัยที่แปรผันมาจากการใช้ประโยชน์ทางอินเตอร์เน็ตใน ปัจจุบัน ซึ่งผู้ศึกษาได้แยกรูปแบบการศึกษาที่เกิดจากการคุกคามทางอินเตอร์เน็ตออกเป็น 3 รูปแบบ คือ

[22] IP Address ย่อมาจาก Internet Protocal Address หมายเลขประจำเครื่องคอมพิวเตอร์บนเครือข่ายอินเตอร์เน็ต เนื่องจากการสื่อสารระหว่างคอมพิวเตอร์แยกจากกันจำเป็นต้องมีหลายเลขประจำเครื่องที่ไม่ซ้ำกัน องค์กร Internet NIC (Internet Network Information Center) สหรัฐอเมริกาเป็นผู้รับผิดชอบในการลงทะเบียน และกำหนดหมายเลขดังกล่าว IP Address ประกอบด้วยเลข (0 – 255) จำนวน 4 ชุด โดยคั่นด้วยเครื่องหมายจุด เช่น 205.184.56.1 เป็นต้น.

1. การคุกคามผ่านทางจดหมายอิเล็กทรอนิกส์ (E-Mail Stalking)

การคุกคามผ่านทางจดหมายอิเล็กทรอนิกส์ (E-Mail Stalking) คือ การส่งจดหมายอิเล็กทรอนิกส์หรือ อีเมล์ อันไม่พึงประสงค์อันมีเนื้อหาไม่สมควรหรือใช้ถ้อยคำที่ไม่สุภาพหยาบคาย หรืออาจจะเป็นรูปภาพหรือข้อความต่าง ๆ ที่มีลักษณะลามกอนาจาร น่ารังเกียจ หรือข้อความอันมีลักษณะข่มขู่ในรูปแบบต่าง ๆ รวมทั้งการส่ง อีเมล์ที่มีไวรัสคอมพิวเตอร์แอบแฝง ซึ่งการกระทำดังกล่าวเป็นการคุกคามที่สร้างความเดือดร้อนรำคาญ หรือความหวาดกลัวแก่ผู้ตกเป็นเหยื่อ ซึ่งการคุกคามในลักษณะนี้เป็นลักษณะของการกระทำที่จำกัดอยู่เฉพาะเหยื่อและความเป็นส่วนตัวเท่านั้น

การคุกคามผ่านทางจดหมายอิเล็กทรอนิกส์หรืออีเมล์นั้นมีข้อน่าสังเกตว่า หากการส่งไวรัสหรืออีเมล์ขยะ (Junk Mail) ที่เป็นการชักจูงทางการตลาดนั้นหาใช่เป็นการคุกคามไม่[23] แต่จะต้องประกอบด้วยพฤติกรรมที่มีการส่งจดหมายอิเล็กทรอนิกส์หรืออีเมล์นั้นอย่างต่อเนื่อง นอกจากนี้ยังจะต้องมีจุดประสงค์เพื่อการข่มขู่ หรือขู่ขวัญจึงจะถือว่าเป็นการคุกคามผ่านทางจดหมายอิเล็กทรอนิกส์หรืออีเมล์เช่นเดียวกับวิธีการคุกคามทั่วไปที่จะต้องมีองค์ประกอบดังกล่าว เช่นการส่งใบเชิญการเป็นสมาชิกหนังสือโป๊ผ่านทางจดหมายอิเล็กทรอนิกส์หรืออีเมล์หลายหนหลายครั้งโดยที่ผู้รับนั้นไม่พึงประสงค์

การคุกคามผ่านทางจดหมายอิเล็กทรอนิกส์หรือ อีเมล์นั้นมีรูปแบบที่ใกล้เคียงกับการคุกคามในรูปแบบเดิม ๆ คือการคุกคามผ่านทางจดหมายอิเล็กทรอนิกส์หรือ อีเมล์นั้นมีลักษณะคล้ายกับการคุกคามทางโทรศัพท์ คือมีการคุกคามโดยตรงและเป็นการคุกคามต่อความเป็นส่วนตัวของเหยื่อห รือผู้เสียหาย หากแต่การคุกคามผ่านทางจดหมายอิเล็กทรอนิกส์นั้นมีการส่งและการแพร่ขยายที่กว้างขวางกว่าและคุกคามได้มากจำนวนกว่าเท่านั้น แต่ยังมีข้อโต้แย้งว่าการคุกคามผ่านทางจดหมายอิเล็กทรอนิกส์นั้นยังไม่มีความน่ากลัวหรือแพร่กระจายได้มากเท่ากับการคุกคามโดยวิ ธีทางโทรศัพท์ซึ่งเป็นวิธีการคุกคามในรูปแบบเดิม เนื่องจากการคุกคามผ่านทางจดหมายอิเล็กทรอนิกส์นั้นผู้รับจดหมายอิเล็กทรอนิกส์นั้นสามารถทำการลบจดหมายทิ้งโดยที่ยังไม่ได้อ่านจดหมายดังกล่าวได้หรืออาจทำการป้องกันหรือ Block จดหมายที่ส่งเข้ามาในตู้รับจดหมาย อย่างไรก็ตามไม่ว่าจะมีการป้องกันหรือทำการลบจดหมายทิ้งหรือไม่ การคุ กคามผ่านทางจดหมายอิเล็กทรอนิกส์ ก็ยังถือว่าเป็นการคุกคาม เพราะทำให้เกิดการรบกวนต่อความเป็นส่วนตัวของบุคคล ไม่ว่าจะเป็นการโทรศัพท์หรือการส่งจดหมายหรือ อีเมล์ต่างเข้าสู่กล่องจดหมายก็ตาม

---

[23] Emma Ogilvie, “Trends & Issues in crime and criminal justice” Australian Institue of Criminalogy, September 2000 ,No.166. Internet. http://www.aic.gov.au.

การติดตามตัวผู้คุกคามผ่านทางจดหมายอิเล็กทรอนิกส์หรือ อีเมล์นั้นสามารถแกะรอยและระบุตัวบุคคลได้เช่นเดียวกับการส่งจดหมาย ทำให้กรณีของจดหมายหรือ อีเมล์นั้นไม่เกี่ยวข้องกับความซับซ้อนทางเทคโนโลยีเพียงแต่เป็นรูปแบบหนึ่งในการสื่อสารเพื่อทำการคุกคามบุคคลอื่นเท่านั้น เนื่องจากในปัจจุบันมีระบบการป้องกัน อีเมล์ที่ไม่พึงประสงค์ รวมถึงความก้าวหน้าทางเทคโนโลยีที่สามารถระบุตัวตนหรือสถานที่ของผู้ส่ง อีเมล์ได้ จึงทำให้ความยุ่งยากในการตรวจสอบหรือสืบหาตัวผู้ที่ทำการคุกคามในรูปแบบนี้ไม่มีปัญหาเท่าที่ควร

2. การคุกคามโดยผ่านทางเว็บบอร์ด (Webboard Stalking)

การคุกคามโดยการใช้เว็บบอร์ดเป็นเครื่องมือได้ถูกจำกัดความให้เป็นการคุกคามในสื่อชนิดใหม่ ซึ่งมีความแตกต่างจากการคุกคามผ่านทางจดหมายอิเล็กทรอนิกส์หรืออีเมล์ที่ถูกเปรียบเทียบให้เป็นการคุกคามในรูปแบบเดิมเพียงแต่เป็นการสื่อสารแนวใหม่เท่านั้น พวกนักคุกคามทั้งหลายมักจะใช้การลงข้อความบนเว็บบอร์ดเป็นเครื่องมือในการทำลายชื่อเสียง หรือทำให้เหยื่อตกอยู่ในอันตราย ซึ่งเป็นการกระทำที่เปิดเผยต่อสาธารณชนมากกว่าที่จะทำต่อความเป็นส่วนตัวของบุคคล หรือตัวเหยื่อ ในเชิงที่ก่อความเสียหาย หรือก่อความอับอายให้กับเหยื่อ เช่น ตัวอย่างที่เกิดขึ้นในประเทศสหรัฐอเมริกา ผู้หญิงคนหนึ่งถูกคุกคามจากแฟนเก่าของเธอเป็นเวลาหลายปี โดยแฟนเก่าของเธอนั้นจะคอยติดตามเว็บไซต์ที่เธอได้เข้าไปสนทนาหรือเว็บไซต์ที่เธอเข้าไปเล่นอยู่เรื่อย ๆ และระหว่างนั้นก็จะลง (Post) ข้อความที่เป็นการให้ร้ายเธอเสมอ จนท้ายที่สุดก็ได้นำภาพของเธอไปตัดต่อกับภาพลามกอนาจารต่าง ๆ และนำภาพของเธอนั้นไปลงตามเว็บไซต์ต่าง ๆ และหญิงสาวเช่นกันที่ถูกคุกคามเป็นเวลาถึง 6 เดือน โดยเริ่มจากการลงข้อความข่มขู่ว่าจะฆ่าและข่มขืนเธอและท้ายที่สุดก็นำภาพขอ งเธอตัดต่อและลงในอินเตอร์เน็ต ทั้งสองกรณีดังกล่าวข้างตนทำให้เห็นได้ชัดเจนว่าการคุกคามในรูปแบบดังกล่าวนี้ไม่ได้เป็นการคุกคามต่อความเป็นส่วนตัวของบุคคลอย่างที่เคยมีมาอีกต่อไปเหมือนอย่างเช่น การโทรศัพท์ การส่งอีเมล์ข่มขู่หรือการการกระทำในรูปแบบอื่น ๆ ต่อเหยื่อ “ในชีวิตจริงการคุกคามนั้นผู้กระทำมีจุดประสงค์เพื่อเรียกความสนใจจากเหยื่อของตน เพื่อให้เหยื่อรู้หรือทราบว่าตนนั้นอยู่ที่ไหนอย่างไรแต่การคุกคามบนอินเตอร์เน็ตนั้นได้เปลี่ยนความคิดดังกล่าวไปอย่างสิ้นเชิง เพราะผู้กระทำหาได้อยู่ใกล้กับเหยื่อไม่ อาจจะอยู่ไกลออกไปถึง 200 ไมล์ก็เป็นได้ จึงไม่มีความจำเป็นต้องให้เหยื่อทราบว่าตนอยู่ที่ใด เป็นการเปิดเผยข้อมูลต่อสาธารณชนเท่านั้นเพื่อให้เหยื่อสนใจตน”(Gilbert)[24]

[24] Ibid.

จากกรณีตัวอย่างทั้งสองข้างต้นนั้นอาจจะมองว่าเป็นการกระทำที่ร้ายแรงและน่าหวาดกลัวแต่การกระทำดัง กล่าวอาจถูกมองได้ว่ายังแตกต่างจากคำว่าการคุกคามอย่างแท้จริง เพราะว่าการคุกคามโดยการใช้อินเตอร์เน็ตเป็นเครื่องมือนั้นเป็นการกระทำที่ทำให้เกิดความกลัวและความหวาดหวั่นทางอารมณ์เท่านั้น ซึ่งยังมิได้พิจารณาเป็นความผิดทางอาญาอย่างจริงจังเท่ากับการคุกคามจนเกิดการทำร้ายร่างกาย

3. การคุกคามผ่านทางห้องสนทนา (Chat Room Stalking)

การคุกคามประเภทนี้เป็นลักษณะของการคุกคามโดยการติดต่อกับเหยื่อโดยตรงโดยการส่งข้อความโต้ตอบทันที (Instant Messaging) ซึ่งอาจจะเป็นข้อความที่เป็นการข่มขู่ หรือหยาบคาย หรือรูปภาพที่มีลักษณะลามกอนาจารส่งให้กับผู้รับซึ่งเป็นเหยื่อเพื่อให้เหยื่อนั้นเกิดความเครียดเกิดความหวาดกลัว ลักษณะของการติดต่อกันทางห้องสนทนาคล้ายกับการติดต่อผ่านทางจดหมายอิเล็กทรอนิกส์ที่จำกัดอยู่เฉพาะเหยื่อและความเป็นส่วนตัว แต่แตกต่างกันตรงที่การติดต่อผ่านห้อง สนทนาเป็นการติดต่อกันโดยทันทีในเวลานั้น ๆ แต่ในปัจจุบันนี้การติดต่อผ่านทางห้องสนทนานี้ได้ถูกเปลี่ยนแปลงและพัฒนาโปรแกรมขึ้น ได้มีโปรแกรมสนทนาในรูปแบบใหม่คือ โปรแกรมเมสเซนเจอร์จากไมโครซอฟท์ และเป็นที่นิยมกันมาก มักถูกเรียกสั้น ๆ ว่า “เอ็มเอสเอ็น”[25] (MSN) หรือ “เอ็ม” ซึ่งโปรแกรมนี้สามารถดาวน์โหลดได้จากอินเตอร์เน็ตทั่วไป และผู้ใช้สามารถเชื่อมต่อคอมพิวเตอร์เข้ากับอินเตอร์เน็ตเพื่อใช้บริการโปรแกรมนี้ในการสนทนาส่งข้อความได้ทันที ซึ่งการเข้าใช้บริการโปรแกรมนี้ ผู้ใช้บริการก็อาจถูกคุกคามได้ในลักษณะเดียวกัน

ดังนั้น จึงทำให้เกิดคำถามว่าหากการกระทำที่เป็นลักษณะของการคุกคามที่เกิดบนโลกของอินเตอร์เน็ตแล้วจะไม่สามารถนำมาเปรียบเทียบกับโลกแห่งความจริงได้เพราะการคุกคามที่เกิดขึ้นบนโลกของอินเตอร์เน็ตนั้นมีผลกระทบเพียงด้านอารมณ์เท่านั้นและไม่ถือว่าเป็นกา รกระทำผิดอาญา ซึ่งในความเป็นจริงบางครั้งพฤติกรรมการคุกคามบนโลกของอินเตอร์เน็ตก็อาจจะถือเป็นลักษณะการกระทำของบุคคลที่ได้กระทำการเช่นนั้นในโลกแห่งความจริง

[25] Wikipedia , the free encyclopedia “MSN” internet.. http//wikipedia.org.wiki.msn.

2.2.3 ลักษณะการคุกคามทางอินเตอร์เน็ต

2.2.3.1 ทำการคุกคามด้วยตนเองโดยการติดต่อเหยื่อโดยตรง เป็นการคุกคามซึ่งลักษณะโดยส่วนใหญ่จะเป็นการส่ง อีเมล์จากตนเองถึงเหยื่อโดยตรง เพื่อสร้างความหวาดกลัวให้แก่ผู้ที่ตกเป็นเหยื่ออย่างเฉพาะเจาะจง หรือทำการพูดคุยโต้ตอบกับเหยื่อผ่านทางห้องสนทนากับเหยื่อ กรณีเช่นนี้การกระทำอาจจะเป็นลักษณะของการข่มขู่เหยื่อ การส่งข้ อความหยาบคาย ภาพลามกอนาจาร โดยจุดประสงค์ที่มุ่งต่อการควบคุมและสร้างความหวาดกลัวต่อเหยื่อและคงหมายรวมถึงการอ้างจะทำร้ายบุคคลที่มีความสัมพันธ์ใกล้ชิดต่อเหยื่อ นอกจากนี้การคุกคามดังกล่าวนั้นยังส่งผลต่อสภาวะหรือสภาพจิตใจของเหยื่อ ทำให้เหยื่อเกิดความหวาดระแวง รู้สึกหวาดกลัวถึงอันตรายต่อการดำเนินชีวิตในภาวะปกติวิสัยของเหยื่อ

2.2.3.2 ทำการคุกคามโดยการยุยง ปลุกปั่นให้ร้ายเหยื่อต่อบุคคลที่สามอันก่อให้เกิดการเกลียดชัง โดยการใช้ข้อความที่เป็นการให้ร้ายเหยื่อให้ผู้อื่นเข้าใจผิด กรณีของการคุกคามในลักษณะนี้ ส่วนใหญ่จะเป็นกรณีเรื่องของการให้ร้าย ใส่ความ สร้างความเสื่อมเสียสร้างความน่าอับอายให้เกิดขึ้นกับเหยื่อ หรือทำให้เหยื่อถูกดูหมิ่นเกลียดชัง และนอกจากนี้ผู้คุกคามอาจกระทำการปลอมเป็นเหยื่อเพื่อทำให้บุคคลที่สามเข้าใจผิดคิดว่าตนเองคือเหยื่อ สร้างความเสียหาย ต่อเหยื่อ เช่น การเข้าไปลงข้อความบนเว็บบอร์ดว่าเหยื่อต้องการมีเพศสัมพันธ์กับทุกคนโดยการอ้างชื่อ ที่อยู่ หมายเลขโทรศัพท์ที่ติดต่อของเหยื่อลงไปในข้อความดังกล่าวด้วย เพื่อเป็นการลวงให้บุคคลที่สามนั้นเข้าใจผิดว่าเป็นความต้องการของตัวเหยื่อ นอกจากนี้อาจจะสร้ างเหตุการณ์ขึ้นมาในทางที่เป็นเรื่องละเอียดอ่อนในสังคม เช่น การเมือง ศาสนา ความชอบที่เป็นกระแส เพื่อให้บุคคลอื่นที่เข้ามาอ่านข้อความดังกล่าวเกลียดชังเหยื่อและที่สำคัญอาจทวีความรุนแรงจนกระทั่งเป็นการลวงให้บุคคลที่สามนั้นกระทำการคุกคามเหยื่อ ซึ่งส่งผลกระทบที่ รุนแรงให้กับตัวผู้ที่เป็นเหยื่อ และเป็นการสร้างความเข้าใจผิดให้กับบุคคลที่สาม เกิดการลวงให้บุคคลที่สามก่ออาชญากรรมแทนตนเอง

2.2.4 ผลกระทบจากปัญหาการคุกคามทางอินเตอร์เน็ต

จากพฤติกรรมการคุกคามทางอิเล็กทรอนิกส์ไม่ว่าจะเป็นการคุกคามผ่านทาง อีเมล์หรือการคุกคามโดยการใช้อินเตอร์เน็ตเป็นเครื่องมือล้วนส่งผลกระทบต่อตัวผู้ที่ตกเป็นเหยื่อด้วยกันทั้งสิ้น ไม่ว่าจะเป็นผลกระทบต่อสภาพร่างกายหรือสภาพจิตใจรวมถึงสภาพอารมณ์

ของเหยื่อ ในกรณีที่เกิดผลกระทบสถานเบาก็เป็นเพียงแค่การสร้างความเดือดร้อนรำคาญให้กับตัวเหยื่อ เช่นกรณีของการส่งสแปมเมล (Spam Mail) ให้กับเหยื่อในคราวละจำนวนมาก ๆ และบ่อยครั้งมักจะเกิดโดยการส่งจากบุคคลคนเดียว หรืออาจส่ง สแปมเมลเพื่อการชักจูงทางการตลาด เพื่อการโฆษณา หรือขายสินค้า หรือการส่งข้อความ ที่ลักษณะของการติดไวรัสมากับเมล นั้น ๆ เพื่อให้ผู้รับเมลนั้นติดไวรัส ผลที่เกิดขึ้นคือการทำให้ผู้รับเมลนั้นเสียเวลาในการลบ อีเมล์ที่ไม่ต้องการนี้ทิ้งจากกล่องจดหมายส่วนตัว หรือทำให้เครื่องคอมพิวเตอร์หรือ อีเมล์ของเหยื่อนั้นติดไวรัส การคุกคามทางอินเตอร์เน็ตในลักษณะนี้นั้นยัง ถือว่ามีผลกระทบแค่สถานเบากับผู้ที่ ตกเป็นเหยื่อ คือการสร้างความเดือดร้อนรำคาญและเสียเวลาเท่านั้น แต่ถ้าหากว่าบุคคลหนึ่งได้รับข้อความ อีเมล์ครั้งแล้วครั้งเล่าจากบุคคลหนึ่งซึ่งไม่เปิดเผยตนว่าเป็นใคร แต่ดูเหมือนกับว่าคน ๆนั้นจะรู้จักชีวิตส่วนตัวของผู้รับเป็นอย่างดี ตัวอย่างเช่น “ฉันเป็นฝันร้ายที่สุดของคุณ ปัญหาทั้งหลายกำลังจะเริ่มขึ้น”[26] หากข้อความเหล่านี้ปรากฏขึ้นใน อีเมล์ของบุคคลที่เป็นผู้รับเมลแล้วย่อมก่อให้เกิดความวิตกกังวลหรือความหวาดกลัวกับผู้รับ อีเมล์ประเภทนี้ด้วยกันทั้งสิ้น เหยื่ออาจจะเกิดความกลัวถึงอันตรายที่จะเกิดขึ้นตามคำข่มขู่หรือคุกคามที่ปรากฏอยู่ในอีเมล์ เช่น คดีที่นักศึกษาคนหนึ่งถูกตั้งข้อหาจากการส่ง อีเมล์ให้กับนักศึกษาเอเชียกลุ่มหนึ่ง และมีข้อความปรากฏใน อีเมล์ว่า “ผมจะหาตัวพวกคุณ และจะฆ่าพวกคุณทิ้งซะ” และลงท้ายข้อความว่า “ คนเกลียดพวกเอเชีย ”[27] ซึ่งข้อความเหล่านี้ นั้นหากปรากฏอยู่ในอีเมล์ของผู้รับนั้นย่อมทำให้ผู้รับ อีเมล์นั้นตกเป็นเหยื่อ และตกอยู่ในความหวาดกลัวถึงอันตรายที่อาจจะเกิดขึ้นกับตนเอง คนใกล้ชิด หรือคนในครอบครัว

การคุกคามทางอินเตอร์เน็ตนั้นนอกจากจะทำให้ผู้ที่ตกเป็นเหยื่ออยู่ในความเครียดหวาดกลัว หรื อหวาดระแวงถึงภัยอันตรายที่อา จจะเกิดขึ้นกับตัวเองแล้ว ผลกระทบที่อาจจะเกิดขึ้นกับตัวเหยื่อ คือเหยื่อได้รับความอับอาย เสื่อมเสียชื่อเสียง หรือถูกดูหมิ่นเกลียดชังจากคนทั่วไป เนื่องจากการคุกคามทางอินเตอร์เน็ตนั้นบางครั้งเป็นการคุกคามที่เปิดเผยต่อสาธารณชนทั่วไปทำให้บุคคลที่สามหรือคนทั่วไปนั้นสามารถเข้าถึงหรือรับรู้ได้

ผลกระทบที่ร้ายแรงที่สุด คือการคุกคามทางอินเตอร์เน็ตที่นำพาไปสู่การคุกคามที่เกิดขึ้นในโลกแห่งความเป็นจริง เช่น คดีที่เกิดขึ้นในมลรัฐแคลิฟอร์เนีย ในเดือนมกราคม 2542 จำเลยในคดีได้รังควานและคุกคามผู้หญิงวัย 28 ปีรายหนึ่งโดยการเข้าไปเว็บบอร์ด

---

[26] Naomi H. Goodno, “Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws,” p. 1.

[27] Emma Ogilvie, Trends & Issues in crime and criminal justice. Australian Institue of Criminalogy, September 2000 ,No.166. Internet. http://www.aic.gov.au.

สาธารณะ และห้องสนทนาหลายหน และแอบอ้างว่าตนเองเป็นหญิงสาวผู้นั้นมาลงข้อความว่าหญิงผู้ตกเป็นเหยื่อนั้นมีความปรารถนาทางเพศในลักษณะอยากให้ชายแปลกหน้ามาข่มขืนกระทำชำเรา พร้อมทั้งได้ลงชื่อ ที่อยู่ และหมายเลขโทรศัพท์ติดต่อซึ่งเป็นของหญิงสาวที่เป็นเหยื่อไว้ด้วย การกระทำดังกล่าวของจำเลยรายนี้เป็นผลให้มีผู้ชายแปลกหน้า อย่างน้อย 6 คนมาเคาะประตูบ้านเธอกลางดึก เพื่อขอมีเพศสัมพันธ์ในลักษณะที่ได้ลงข้อความไว้บนอินเตอร์เน็ต นอกจากนี้ยังมีโทรศัพท์อีกจำนวนมากโทรมาเพื่อขอมีเพศสัมพันธ์ในลักษณะนี้ การคุกคามทางอินเตอร์เน็ตในลักษณะเช่นนี้ได้สร้างความเดือดร้อนแก่หญิงสาวผู้เป็นเหยื่อ ซึ่งตัวเธอเองนั้นไม่รู้เลยว่ามีการแอบอ้างเป็นตัวเธอและมีการลงข้อความพร้อมทั้งรายละเอียดที่สามารถติดต่อเธอได้อยู่บนอินเตอร์เน็ต ในที่สุดจำเลยในคดีดังกล่าวนั้นได้ถูกจำคุกเป็นเวลา 6 ปี[28]

นอกจากนี้จากรูปแบบของการคุกคามทางอินเตอร์เน็ตนั้นสามารถทำให้บุคคลที่สามที่ไม่ได้มีส่วนเกี่ยวข้องทำการคุกคามผู้อื่นแทน เช่นการส่ง อีเมล์รุนแรง (Hate E-Mail) ในนามของเหยื่อโดยให้เบอร์โทรศัพท์และที่อยู่ ตัวอย่างเช่น ส่งถึง “กลุ่มซาตาน คนติดยา และคนทำธุรกิจสื่อลามกอนาจาร ” เหยื่อรายนี้ได้ค้นพบว่ามีเหตุการณ์เช่นนี้เกิดขึ้น เมื่อเธอได้รับโทรศัพท์ข่มขวัญจากชายคนหนึ่งซึ่งอาศัยอยู่ห่างไปเพียงระยะทาง 20 นาทีจากบ้านของเธอ ว่า “เธอควรจะหาปืนเอาไว้ เพราะครั้งหน้าที่เราจะอ่านเรื่องของเธอมันจะอยู่ในรายงานของตำรวจ ” แท้ที่จริงแล้วผู้คุกคามทางอินเตอร์เน็ตของเหยื่อ คือคนที่เหยื่อทำธุรกิจด้วย[29]

จากกรณีที่เกิดขึ้นข้างต้นนี้ทำให้เล็งเห็นได้ว่าผลกระทบที่เกิดจากการคุกคามทางอินเตอร์เน็ตนั้นในลักษณะดังกล่าวนั้น มีการคุกคามที่รุนแรง มิใช่เพียงแค่การคุกคามที่ในสถานเบาที่สร้างความเดือดร้อนรำคาญ ความเครียด ความวิตกกังวลแก่สภาพจิตใจหรือสภาพอารมณ์ของผู้ที่เป็นเหยื่อเท่านั้น หากแต่เป็นการคุกคามที่อาจก่อให้เกิดอันตรายต่อเหยื่อ เกิดการทำร้ายร่างกายจนอาจถึงแก่ชีวิต มากที่สุด และมิใช่เพียงการคุกคามที่เกิดบนโลกของอินเตอร์เน็ตที่เกิดผลกระทบต่อสภาพอารมณ์และจิตใจของเหยื่อเพียงอย่างเดียวเท่านั้น แต่การคุกคามทางอินเตอร์เน็ตที่สามารถขยายผลมาสู่โลกแห่งความเป็นจริงได้ นอกจากนี้ปัญหาการคุกคามทางอินเตอร์เน็ตนั้นเป็นการคุกคามที่ไม่สามารถบ่งบอกหรือระบุตัวตนของผู้คุกคามได้ และการกระทำการคุกคามดังกล่าวนั้นก็

---

[28] Naomi H. Goodno, “Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws,” p.10.

[29] Ibid.

เป็นการคุกคามทางเครือข่ายอินเตอร์เน็ตที่ไม่มีลักษณะของการกระทำทางกายภาพ ซึ่งการคุกคามทางอินเตอร์เน็ตก็อาจจะมีผลกระทบอารมณ์และสภาพจิตใจของเหยื่อรวมถึงผลกระทบที่เกิดต่อสภาพร่ างกายของเหยื่อเหมือนการถูกคุกคามธรรมดาที่ผู้ศึกษาได้นำเสนอไว้แล้วข้างต้น

2.3 ความแตกต่างระหว่างการคุกคามทางอินเตอร์เน็ตและการคุกคามทั่วไป

จากการศึกษาการคุกคามทั่วไปและการคุกคามทางอินเตอร์เน็ตนั้น ทำให้เห็นว่าการคุกคามทางอินเตอร์เน็ตนั้นเหมือนกับการคุกคามทั่วไปเนื่องจากมีความคล้ายคลึงกันทั้งเนื้อหาและเจตนาซึ่งรวมถึงความต้องการของผู้คุกคามที่มีความต้องการที่จะใช้อำนาจบังคับเหยื่อ ควบคุมเหยื่อ และพฤติกรรมข่มขู่คุกคามก็จะนำไปสู่พฤติกรรมที่รุนแรงมากขึ้น อย่างไรก็ตามแม้ว่าจะมีความคล้ายคลึงกันก็ ตาม แต่การคุกคามทางอินเตอร์เน็ตก็แตกต่างจากการคุกคามทั่วไป ใน 4 ลักษณะ[30] ซึ่งความแตกต่างเหล่านี้มีความสำคัญเพราะเป็นเหตุผลที่ทำให้กฎหมายปราบปรามการคุกคามทั่วไปไม่สามารถดำเนินการครอบคลุมถึงการคุกคามทางอินเตอร์เน็ตได้ ดังนี้

2.3.1 ผู้คุกคามทางอินเตอร์เ น็ตสามารถคุกคามข่มขู่เหยื่อหลายรายอย่างรวดเร็วและส่งข้อมูลได้อย่างกว้างขวาง แม้ว่าความแตกต่างนี้จะชัดเจน แต่ก็ถือว่าเป็นสิ่งสำคัญเนื่องจากอินเตอร์เน็ตเป็นระบบการสื่อสารที่ไม่มีขอบเขต บุคคลสามารถส่งข้อความหนึ่งๆ ได้ทันทีโดยไม่ทราบว่าข้อความนั้นมาจากใคร ในขณะนี้เว็บไซต์ อินเตอร์เน็ต อีเมล์ ห้องสนทนา (Chat Room) กระดานข่าวอิเล็กทรอนิกส์ การส่งข้อความโต้ตอบทันที (Instant Messaging) และเครื่องมือสื่อสารทางเว็บไซต์อื่นๆ ได้ทำให้ผู้คุกคามทางอินเตอร์เน็ตสามารถส่งข้อความข่มขู่คุกคามได้อย่างรวดเร็ว บรรดาข้อความหรือรูปภาพต่าง ๆ ที่ส่งให้ทางอินเตอร์เน็ตก็สามารถส่งผ่านถึงกลุ่มคนจำนวนมาก ๆ และขยายเป็นวงกว้างกว่าการสื่อสารเพื่อข่มขู่โดยการคุกคามทั่วไปนอกจากนี้วิธีการดังกล่าวนั้นถือเป็นวิธีที่มีประสิทธิภาพและราคาต้นทุนต่ำ ตัวอย่างเช่น ผู้คุกคามทั่วไปอาจจะข่มขู่เหยื่อโดยการโทรศัพท์ถึงเหยื่อหลาย ๆ ครั้ง แต่ในการโทรศัพท์แต่ละครั้ง ผู้คุกคามจะต้องลงมือกระทำและใช้เวลา พฤติกรรมการคุกคามนี้สามารถสร้างผลกระทบที่รุนแรงขึ้นหากกระทำผ่านทางอินเตอร์เน็ต เนื่องจากในการส่ง อีเมล์เพียงครั้งเดียวผู้คุกคามสามารถส่งข้อคว ามถึงเหยื่อซ้ำ ๆเป็นพันๆ ครั้งโดยการอาศัยระบบและอุปกรณ์ของคอมพิวเตอร์ นอกจากนี้ ผู้คุกคามทางอินเตอร์เน็ตยังสามารถสร้างเว็บไซต์เพื่อลงคำข่มขู่หรือคุกคาม ดังนั้น แทนที่

[30] Ibid., p. 5.

จะส่งจดหมายข่มขู่เหยื่อ ผู้คุกคามสามารถส่งคำข่มขู่ให้โลกได้รู้ โดยการลงข้อความเหล่า นี้ไว้บนเว็บไซต์ ทำให้มีการข่มขู่คุกคามอย่างต่อเนื่อง ซึ่งการกระทำดังกล่าวนั้นทำให้เกิดการละเมิดความเป็นส่วนตัวของบุคคลและทำให้การคุกคามทางอินเตอร์เน็ตรุนแรงขึ้น

2.3.2 ผู้คุกคามทางอินเตอร์เน็ตสามารถที่จะอยู่ไกลจากเหยื่อ ผู้คุกคามทั่วไปมักจะอยู่ใกล้กับเหยื่อ หรือในบริเวณเดียวกันแต่ผู้คุกคามทางอินเตอร์เน็ตสามารถใช้อินเตอร์เน็ตคุกคามเหยื่อไม่ว่าเหยื่อจะอยู่ที่ไหน เหยื่อจึงไม่มีทางที่จะหนีพ้นผู้คุกคามได้ และการที่อินเตอร์เน็ตสามารถเข้าถึงบุคคลอย่างไม่มีข้อจำกัดทำให้การคุกคามบุคคลทางอินเตอร์เน็ตต่างจากการคุกคามทั่วไป 3 กรณีดังนี้[31]

(1) อินเตอร์เน็ตนั้นเป็นวิธีที่ถูกและสะดวกสำหรับผู้คุกคามทางอินเตอร์เน็ตในการติดต่อเหยื่อจากที่ไหนก็ได้ ผู้คุกคามสามารถคุกคามเหยื่อข้ามเมือง รัฐ หรือกระทั่งข้ามประเทศ ตราบเท่าที่มีการเข้าถึงอินเตอร์เน็ต ซึ่งถือว่าการสื่ อสารทางอินเตอร์เน็ตนั้นน่าจะเป็นสื่อที่มีราคาถูกกว่าโทรศัพท์และรวดเร็วกว่าไปรษณีย์

(2) ที่อยู่ของผู้คุกคามในอินเตอร์เน็ตไม่จำเป็นต้องเปิดเผยก็ได้ ซึ่งส่งผลให้เหยื่ออยู่ในสภาวะวิตกจริต เกิดความหวาดระแวง หวาดกลัวว่าผู้คุกคามเขาหรือเธอเป็นเพื่อนบ้าน หรืออยู่ในประเทศเพื่อนบ้าน

(3) สถานที่ตั้งหรือสถานที่อยู่ของผู้คุกคามทางอินเตอร์เน็ตก็สามารถก่อให้เกิดปัญหาเกี่ยวกับเรื่องเขตอำนาจศาลได้ เนื่องจากการคุกคามทางอินเตอร์เน็ตสามารถกระทำข้ามรัฐ หรือข้ามประเทศได้อย่างง่ายดาย อัยการอาจเผชิญกับปัญหาเรื่องเขตอำนาจศาลในการบังคับใช้กฎหมายได้

2.3.3 เป็นการยากที่จะเปิดเผยตัวผู้คุกคามทางอินเตอร์เน็ต ยังมีความเข้าใจผิดว่าการคุกคามทางอินเตอร์เน็ตนั้นอันตรายน้อยกว่าการคุกคามทั่วไป เนื่องจากการคุกคามทางอินเตอร์เน็ตนั้นไม่เกี่ยวข้องกับการติดต่อทางกายภาพ [32] แต่ในความเป็นจริงแล้วการคุกคามทางอินเตอร์เน็ตนั้นอันตรายกว่าการคุกคามแบบทั่วไป เนื่องจากอินเตอร์เน็ตเปิดโอกาสให้ผู้ที่อยากจะคุกคามบุคคลอื่นแต่ไม่อยากแสดงตนว่าตนเองคือผู้คุกคาม นอกจากนี้ยังไม่อยากที่จะคุกคามโดยวิธีทั่วไปก็สามารถใช้อินเตอร์เน็ตนั้นส่งข้อความข่มขู่คุกคามเหยื่อแทน

อินเตอร์เน็ตได้ถูกทำขึ้นให้สามารถทำลายความยับยั้งชั่งใจของบุคคล ความสามารถในการส่งข้อความข่มขู่คุกคามหรือรังควานเหยื่อ ทำให้ผู้คุกคามสามารถ

---

[31] Ibid., p. 6.

[32] Ibid., p. 7.

กระทำความผิด เอาชนะความลังเลใจ ความไม่เต็มใจ หรือความกลัวที่จะเผชิญหน้ากับเหยื่อ และอาจทำให้ผู้ก ระทำผิดคุกคามไม่กลัวการกระทำผิดเหล่านี้ นอกจากนี้การไม่เปิดเผยในอินเตอร์เน็ตยังส่งผลให้ผู้คุกคามทางอินเตอร์เน็ตสามารถติดตามและสืบการใช้อินเตอร์เน็ตของเหยื่อได้เป็นระยะเวลานานโดยที่เหยื่อนั้นอาจจะไม่รู้ตัว

มีนักวิชาการท่านหนึ่งได้อธิบายไว้ว่า “ผ้าคลุมที่ปิดบังโฉมหน้า” ในอินเตอร์เน็ตทำให้ผู้คุกคามทางอินเตอร์เน็ต “ มีข้อได้เปรียบ ”[33] และเป็นการยากที่จะชี้ตัว หาที่อยู่ และจับกุมผู้คุกคามได้ และผู้คุกคามสามารถใช้เทคโนโลยีในการปลดเครื่องหมายซึ่งสามารถชี้ตัวผู้คุกคามออกได้[34]

2.3.4 ผู้คุกคามทางอินเตอร์เน็ตสา มารถปลอมเป็นเหยื่อได้ง่าย ต่างจากการคุกคามโดยทั่วไป ผู้คุกคามทางอินเตอร์เน็ตสามารถแสดงตนเป็นเหยื่อและก่อความวุ่นวายหรือให้ร้าย ทำให้เหยื่อถูกดูหมิ่นเกลียดชังในอินเตอร์เน็ต โดยการส่ง อีเมล์ปลอม ลงประกาศข้อความในกระดานข่าวต่าง ๆ และก้าวร้าวผู้สนทนาใน ห้องสนทนา หรือลงประกาศข้อความที่เป็นการเสียหาย เหยื่อก็จะถูกห้ามการลงประกาศในกระดานข่าว ถูกกล่าวหาในการกระทำที่ไม่เหมาะสม และได้รับข้อความข่มขู่จากผู้ที่ถูกก้าวร้าวโดยผู้คุกคามเหยื่อโดยใช้ชื่อเหยื่อเป็นกำบัง

ตัวอย่างเรื่องจริงที่เกิดขึ้นกับ Jane Hitchcock[35] ซึ่งถูกคุกคามทางอินเตอร์เน็ตโดยเจ้าของบริษัทแห่งหนึ่ง หลังจากที่เธอร้องเรียนการให้บริการของบริษัทแห่งนี้ บริษัทแห่งนี้เป็นผู้คุกคามเธอและผู้คุกคามได้ใช้ชื่อ Hitchcock ลงประกาศข้อคิดเห็นที่ดุเดือดในเว็บไซต์และส่ง อีเมล์ในชื่อของเธอเพื่อที่จะทำให้คนอื่นโกรธแล้วกลับมาข่มขู่เธอ และผู้คุกคามเองก็ยังส่ง อีเมล์ ที่มีข้อความข่มขวัญถึงเธอเป็นพัน ๆ ฉบับเป็นเวลากว่าปี นอกจากนี้ผู้คุกคามยังส่ง อีเมล์ข่มขู่และคุกคามคนใกล้ตัวและคนใกล้ชิดของ Hitchcock คือผู้คุกคามยังส่ง อีเมล์ข่มขวัญสามีและเจ้านายของเธอ เป็นพัน ๆ ฉบับเช่นกันและบางครั้งก็ส่งในชื่อของ Hitchcock เองซึ่งในที่สุดก็ทำให้อีเมล์ ของบุคคลที่ได้รับข้อความข่มขู่คุกคามเหล่านี้เต็มและทำให้ใช้งานไม่ได้ การกระทำของผู้คุกคามทางอินเตอร์เน็ตดังกล่าวร้ายแรงถึงขนาดทำให้ Hitchcock ต้องถูกย้ายออก แต่ก็ไม่ได้เป็นการหยุดผู้คุกคามได้แต่อย่างไร ผู้คุกคามได้ค้นพบเธอในอินเตอร์เน็ตและเริ่มการคุกคามข่มขู่อีก จนกระทั่ง Hitchcock ได้ดำเนินการฟ้องศาลแต่ผู้คุกคามดังกล่าวไม่ได้ถูกตัดสินให้มีความผิดทางอาญา

---

[33] Ibid., p. 8.

[34] Ibid.

[35] Ibid.

2.3.5 ผู้คุกคามทางอินเตอร์เน็ตก่อให้เกิดการข่มขู่ คุกคามโดยบุคคลที่สามที่ไม่ได้มีส่วนเกี่ยวข้อง การที่ผู้คุกคามสามารถทำให้บุคคลที่สามทำการคุกคามข่มขู่เหยื่ออาจจะเป็นสิ่งที่น่าหวาดกลัวที่สุดและ เป็น ลักษณะพิเศษเฉพาะของการคุกคามทางอินเตอร์เน็ต ยกตัวอย่างเช่น[36] ในมลรัฐแคลิฟอร์เนีย จำเลยวัย 58 ปี ใช้อินเตอร์เน็ตในการชักจูงการข่มขืนหญิงวัย 28 ปีคนหนึ่งที่ปฏิเสธรับรักจากจำเลยผู้นั้น จำเลยได้ทำความหวาดกลัวให้เหยื่อโดยการปลอมเป็นเหยื่อในห้องสนทนาในอินเตอร์เน็ต พร้อมทั้งลงประกาศเบอร์โทรศัพท์และที่อยู่ของเหยื่อ และลงข้อความว่า เหยื่อจินตนาการที่จะถู ก ข่มขืน เนื่องจากข้อความเหล่านี้ มีผู้ชายอย่างน้อย 6 คนมาหาเธอที่บ้านและแสดงความจำนงว่าเขาต้องการข่มขืนเธอ เช่นเดียวกันกับ Hitchcock ที่ประสบกับการคุกคามทางอินเตอร์เน็ตในลักษณะคล้าย ๆกัน เมื่อผู้คุกคามเธอลงโฆษณาเบอร์โทรศัพท์และที่อยู่ของเธอในเว็บไซต์ alt-sex ซึ่งใช้ลงประกาศหาการมีเพศสัมพันธ์แบบซาดิสต์

นอกจากนี้ยังมีรูปแบบ ของการหลอกให้บุคคลที่สามที่ไม่ได้มีส่วนเกี่ยวข้องทำการคุกคามผู้อื่นแทน คือ ผู้คุกคามส่งอีเมล์รุนแรง (Hate E-Mail) ในนามของเหยื่อโดยให้เบอร์โทรศัพท์และที่อยู่ เช่น ส่งถึง “กลุ่มซาตาน คนติดยา และคนทำธุรกิจสื่ออนาจาร ” เหยื่อรายดังกล่าวค้นพบว่ามีเหตุการณ์นี้ขึ้น เมื่อเธอได้รับโทรศัพท์ข่มขวัญจากชายผู้หนึ่งซึ่งอาศัยเพียง 20 นาทีจากบ้านของเธอว่า “เธอควรจะหาปืนเอาไว้ เพราะครั้งหน้าที่เราจะอ่านเรื่องของเธอมันจะอยู่ในรายงานของตำรวจ ”[37] แท้ที่จริงผู้คุกคามทางอินเตอร์เน็ตของเหยื่อคือ คนที่เหยื่อทำธุรกิจด้วย แต่ผู้คุกคามก็ไม่มีความผิดทางอาญา

ท้ายสุด อินเตอร์เน็ตก็ทำให้การคุกคามทั่วไปที่น่าหวาดกลัวอยู่แล้วนั้นดูน่าหวาดกลัวมากยิ่งขึ้นอีก โดยการที่ผู้คุกคามสามารถใช้อินเตอร์เน็ตคุกคามได้ ตลอดยี่สิบสี่ชั่วโมง การต่ออินเตอร์เน็ตที่รวดเร็วทันใจ การส่งข้อความซ้ำ ๆได้อย่างมีประสิทธิภาพ และการไม่เปิดเผยแหล่งที่อยู่หรือแหล่งที่มาของผู้คุกคาม นอกจากนี้ ผู้คุกคามยังสามารถแสดงตนเป็นบุคคลอื่นได้ อีกทั้งโอกาสในการกระทำของผู้คุกคามก็ไม่มีขอบเข ต เช่นเดียวกับอินเตอร์เน็ต

จากการศึกษาทั้งหมดข้างต้น ผู้ศึกษานั้นเห็นว่าการคุกคามโดยทั่วไปและการคุกคามทางอินเตอร์เน็ตนั้นถือเป็นอาชญากรรมชนิดหนึ่งที่มีความรุนแรง และสามารถสร้างความเสียหายได้ไม่ต่างกัน และไม่ว่าจะเป็นเพศหญิงหรือเพศชายก็สามารถตกเป็น เหยื่อและกลายเป็นผู้คุกคามได้เท่า ๆ กัน เพียงแค่ว่ารูปแบบของการกระทำความผิดในการ

---

[36] Ibid., p. 9.

[37] Ibid., p. 10.

คุกคามนั้นได้แตกต่างและพัฒนาไปจากเดิมตามความก้าวหน้าทางเทคโนโลยี ดังนั้นจึงเป็นการสมควรอย่างยิ่งที่จะต้องทำการศึกษาถึงมาตรการทางกฎหมายของต่างประเทศและของประเทศไทยที่มีอยู่ว่าเพียงพอหรือไม่ในการแก้ไขปัญหาหรือมาตรการทางกฎหมายที่มีอยู่นั้นเพียงพอหรือไม่ในการลงโทษหรือปราบปรามผู้กระทำความผิด

บทที่ 3
มาตรการทางกฎหมายเกี่ยวกับการคุกคามทางอินเตอร์เน็ต (Cyberstalking)

3.1 ที่มาของ กฎหมายการคุ กคามทางอินเตอร์เน็ต Cyberstalking ในประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาซึ่งเป็นประเทศต้นกำเนิดของอินเตอร์เน็ต ได้เผชิญกับปัญหาการคุกคามซึ่งทวีความรุนแรงและพัฒนาไปในรูปแบบใหม่ที่อาศัยอินเตอร์เน็ตเป็นปัจจัย หน่วยงานบังคับใช้กฎหมายของประเทศสหรัฐอเมริกา จึงได้พยามศึกษาปัญหาที่เกิดขึ้น เช่น สำนักงานอัยการแขวงลอสแองเจิลลิสพบว่า อีเมล์และการติดต่อสื่อสารทางอิเล็กทรอนิกส์อื่นเป็นปัจจัยต่อการติดตามและคุกคามประมาณ ร้อยละ 20 และหัวหน้าหน่วยการกระทำความผิดทางเพศในสำนักงานอัยการแขวงแมนฮัตตันได้ประมาณว่า ร้อยละ 20 ของคดีที่ได้รับการสอบสวนจัดการจะเกี่ยวข้องกับการคุกคามทางอินเตอร์เน็ต แล ะหน่วยงานเทคโนโลยีและการตรวจสอบค อมพิวเตอร์ของสำนักงานตำรวจกรุงนิวยอร์กประมาณว่า ร้อยละ 40 ของคดีนั้นเกี่ยวข้องกับการรบกวนและการคุกคามทางอิเล็กทรอนิกส์ และทั้งหมดนี้ได้เกิดขึ้นภายในระยะเวลา 3 - 4 ปีที่ผ่านมา[38]

ในขณะที่การคุกคามทางอินเตอร์เน็ตเป็นปรากฏการณ์ใหม่เช่นเดียวกับอินเตอร์เน็ต การคุกคามทั่วไปก็ถือว่าเป็นอาชญากรรมที่เพิ่งเริ่มเกิดมาไม่นานนี้ โดยทั่วไปจุดประสงค์ของผู้คุกคามคือ ใช้อำนาจ “บังคับ” เหยื่อโดยทำให้เ หยื่อหวาดกลัวและบ่อยครั้งพฤติกรรมดังกล่าวนำไปสู่การใช้กำลังทางร่างกาย มลรัฐแคลิฟอร์เนียได้ออกกฎหมายควบคุมปราบปรามการคุกคามฉบับแรกในปี ค.ศ. 1990 เพื่อปราบปรามการคุกคามทั่วไป หลังจากเกิดเหตุฆาตกรรม Rebecca Schaeffer ดาราโทรทัศน์เรื่อง “My Sister Sam” เนื่องจาก Schaeffer ไม่สามารถหยุดแฟนคนหนึ่งที่คลั่งไคล้เธอและคุกคามเธอเป็นเวลากว่า 2 ปี การคุกคามรุนแรงขึ้นเป็นลำดับ และแฟนผู้นั้นได้ทำร้ายร่างกายเธอและฆ่าเธอในที่สุด[39]

---

[38] U.S the Attorney General, 1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry, A Report from the Attorney General to the Vice President . Internet. http://www.usdj.gov/criminal/cybercrime/cyberstalking.htm.

[39] Naomi H. Goodno, “Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws,” The Berkeley Electronic Press ,(2006) : 1- 62.

จากนั้นไม่นานมลรัฐอื่นและรัฐบาลกลางของสหรัฐอเมริกาก็ได้ดำเนินรอยตามมลรัฐแคลิฟอ ร์เนียในการออกกฎหมายปราบปรามการคุกคามเพื่อปิดช่องว่างของกฎหมายฝ่ายนิติบัญญัติได้เล็งเห็นความจำเป็นในการหยุดผู้คุกคามก่อนที่จะได้พัฒนาไปเป็นการข่มขู่คุกคามและรังควานร้ายแรงซึ่งมีผลกับความปลอดภัยของบุคคล นอกจากนี้กฎหมายปราบปรามการคุกคามก็มีจุดประสงค์เพื่ อ “กำจัดพฤติกรรมซึ่งขัดขวางการใช้ชีวิตปกติของเหยื่อ และป้องกันพฤติกรรมเหล่านั้นไม่ให้กลายเป็นความรุนแรง ” กฎหมายที่เกี่ยวข้องกับการคุกคามทั่วไปเป็นทั้งกฎหมายเชิงป้องกันและเชิงรุก เนื่องจากกฎหมายเหล่านี้มีจุดประสงค์เพื่อ “ทำการคุกคามบางประเภทให้เป็นคว ามผิดอาญา เพื่อป้องกันไม่ให้ผู้คุกคามกระทำการที่รุนแรงและร้ายแรงมากขึ้น”

แม้ว่าจะมีการตรากฎหมายเหล่านี้ขึ้น การคุกคามทั่วไปก็ยังเป็นปัญหาสำคัญในประเทศสหรัฐอเมริกา แต่ละปีมีคนเกือบห้าแสนคนที่ถูกคุกคาม และประมาณ ร้อยละ 85 ก็เป็นคนธรรมดาที่ไม่ได้มีชื่อเสียงหรือเป็นที่รู้จักทั่วไป[40] การคุกคามทั่วไปส่งผลกระทบที่สำคัญกับเหยื่อ โดยทำให้เกิดความเครียดหลังจากความหวาดกลัว ความซึมเศร้า และสภาพโศกเศร้าทางอารมณ์อย่างรุนแรง และส่งผลกระทบถึงสภาพร่างกาย ในขณะที่การคุกคามทั่วไปและการคุกคามทางอินเตอร์เน็ตมี จุดประสงค์คล้ายกัน คือ การบังคับข่มขวัญเหยื่อ แต่แตกต่างในพฤติกรรมในวิธีการที่ผู้คุกคามทางอินเตอร์เน็ตใช้ในการบรรลุจุดประสงค์ดังกล่าว

รัฐบาลกลางของประเทศสหรัฐอเมริกา และหน่วยงานทางด้านกฎหมายรวมถึงเจ้าหน้าที่ผู้บังคับใช้กฎหมายได้ตระหนักถึงภัยและผลกระทบอั นเกิดจากการคุกคามดังกล่าวที่มีต่อความสงบสุข และชีวิตส่วนตัวของประชาชน จึงได้ออกมาตรการทางกฎหมายต่าง ๆ ทั้งระดับรัฐบาลกลางและกฎหมายในระดับมลรัฐออกมาเพื่อจัดการกับปัญหาการคุกคามดังกล่าว ซึ่งล่าสุดนั้นมีเพียง 6 มลรัฐเท่านั้นที่ออกกฎหมายเกี่ยวกับการคุกคามทางอินเตอร์เน็ต (Cyberstalking) โดยเฉพาะเพื่อจัดการกับปัญหาดังกล่าว

กฎหมายในประเทศสหรัฐอเมริกานั้นมีทั้งกฎหมายในระดับมลรัฐ (State Laws) และกฎหมายในระดับรัฐบาลกลาง (Federal Laws) ซึ่งโดยส่วนใหญ่แล้วแต่ละมลรัฐนั้นได้นำเอาบทบัญญัติที่มีอยู่เกี่ยวกั บการคุกคาม (Stalking) มาปรับใช้เทียบเคียงกับกรณีที่เกิดขึ้น

---

[40] U.S the Attorney General, 1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry, A Report from the Attorney General to the Vice President August 1999. Internet. http://www.usdj.gov/criminal/cybercrime/cyberstalking.htm.

3.2 กฎหมายเกี่ยวกับการคุกคามทางอินเตอร์เน็ต (Cyberstalking)ในประเทศสหรัฐอเมริกา

3.2.1 กฎหมายในระดับรัฐบาลกลาง (Federal Law) นั้นได้บัญญัติมาตรการไว้ดังนี้

(1) Interstate Communication Act , 18 U.S.C. S. 875 (c)[41] บทบัญญัติในพระราชบัญญัติการสื่อสารระหว่างรัฐฉบับดังกล่าวนี้ได้บัญญัติให้การส่งผ่านการสื่อสารใด ๆ ในเชิงพาณิชย์ระหว่างรัฐหรือต่างประเทศอันเป็นการก่ออันตรายให้กับบุคคลอื่นนั้นต้องโทษปรับและจำคุกไม่เกินห้าปีหรือทั้งจำทั้งปรับ ซึ่งบทบัญญัติดังกล่าวได้รวมถึงการส่งผ่านการสื่อสารในรูปแบบของไปรษณีย์อิเล็กทรอนิกส์ด้วย[42]

(2) Federal Phone Harassment Statue , 47 U.S.C. S. 223 (a) (1) (c)[43] พระราชบัญญัติการคุกคามทางโทรศัพท์ บทบัญญัตินี้ให้การใช้โทรศัพท์หรือเครื่องมือสื่อสารใด ๆ ก็ตาม ระหว่างรัฐ หรือระหว่างประเทศในการก่อกวน สร้างความรำคาญ รบกวน คุกคาม หรือข่มขู่บุคคลอื่นเป็นความผิดต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับ หรือทั้งจำทั้งปรับ

ดังนั้นการคุกคามทางอินเตอร์เน็ตโดยการสร้างความรำคาญให้แก่ เหยื่อ โดยวิธีการส่งสแปมเมล ก็สามารถที่จะนำบทบัญญัติดังกล่าวมาปรับใช้ได้[44]

---

[41] “Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five year, or both”

[42] จอมพล พิทักษ์สันตโยธิน, “การตามรังควานบนอินเตอร์เน็ต(Cyberstalking)กับความผิดทางอาญาในสหรัฐอเมริกาและสหราชอาณาจักร,” วารสารวิชาการมนุษย์ศาสตร์และสังคมศาสตร์ 13, (กันยายน –ธันวาคม 2548) : 51-65.

[43] “(a) Prohibited acts generally Whoever - (1) in interstate or foreign communications –(c) makes a telephone call or utilizes a telecommunications device , whether or not conversation ensues , without disclosing his identify and with intent to annoy , abuse , threaten , or harass any person at the call number or who receives the communications ;shall be fined under title 18 or imprisoned not more than two years, or both.

[44] จอมพล พิทักษ์สันตโยธิน, “การตามรังควานบนอินเตอร์เน็ต(Cyberstalking)กับความผิดทางอาญาในสหรัฐอเมริกาและสหราชอาณาจักร,” วารสารวิชาการมนุษย์ศาสตร์และสังคมศาสตร์ ,หน้า 59.

(3) Federal Interstate Stalking Punishment and Prevention Act , 18 U.S.C. S.2261A[45]

บทบัญญัติดังกล่าวนั้นได้กำหนดให้การกระทำความผิดสำหรับบุคคลใด ๆที่ได้กระทำข้ามรัฐโดยการก่อให้เกิดความเสียหาย หรือเป็นก ารคุกคามบุคคลอื่น ให้ตกอยู่ในความกลัวว่าจะถูกเอาชีวิตหรือถูกทำร้ายจนเสียชีวิตนั้นถือเป็นความผิด

(4) บทบัญญัติมาตรา 18 U.S.C. 2425[46] บทบัญญัตินี้ได้ออกมาสมัยที่นาย บิล คลินตัน เป็นประธานาธิบดี ในช่วงปี พ .ศ. 2541 ซึ่งได้กำหนดความผิดอาญาแก่ผู้ซึ่งเจตนาใช้การสื่อสารในเชิงพาณิชย์ระหว่างรัฐ หรือระหว่างประเทศเพื่อชี้ชวนหรือเสนอหรือกระทำการล่อลวงผู้ที่อายุต่ำกว่า 16 ปี ให้มีส่วนร่วมในกิจกรรมทางเพศที่ผิดกฎหมาย ต้องโทษจำคุกไม่เกินห้าปี หรือปรับ หรือทั้งจำทั้งปรับ[47]

เมื่อพิจารณากฎหมายในระดั บรัฐบาลกลางแล้วเห็นได้ว่าบทบัญญัติทางกฎหมายของรัฐบาลนั้นยังไม่ครอบคลุมการกระทำความผิดเกี่ยวกับการคุกคามทางอินเตอร์เน็ต (Cyberstalking) ได้อย่างจริงจังและเพียงพอ จึงทำให้แต่ละมลรัฐนั้นจำเป็นต้องออกกฎหมายมาเพื่อลงโทษผู้กระทำความผิด เนื่องจากความผิดดังกล่าวนั้ นสร้างความเสียหายเป็นภัยอันตรายกับผู้ที่ตกเป็นเหยื่อ

---

[45] Rose Hunter, Cyberstalking, Law and the Internet. Internet. http//gsu.edu/lawand/papers/fa01/hunter/.

[46] “Whoever, using the mail or any facility or means of interstate or foreign commerce , or within the special maritime and territorial jurisdiction of the United State , knowingly initiates the transmission of the name . address , telephone number ,social security number ,or electronic mail address of another individual , knowing that such other individual has not attained the age of 16 years , with the intent to entice , encourage, offer ,or solicit any person to engage in any sexual activity for which any person can be charged with a criminal offense , or attempts to do so , shall be fined under this title , imprisoned not more than five years , or both.”

[47] จอมพล พิทักษ์สันตโยธิน, “การตามรังควานบนอินเตอร์เน็ต(Cyberstalking)กับความผิดทางอาญาในสหรัฐอเมริกาและสหราชอาณาจักร,” วารสารวิชาการมนุษย์ศาสตร์และสังคมศาสตร์ ,หน้า 59

3.2.2 กฎหมายในระดับมลรัฐ (State Law) ในประเทศสหรัฐอเมริกา

ในการศึกษาครั้งนี้ผู้ศึกษาจะได้พิจารณากฎหมาย Cyberstalking ในสหรัฐอเมริกา ซึ่งปัจจุบันได้มีการบัญญัติกฎหมายในเรื่องดังกล่าวทั้งหมดเพี ยง 6 มลรัฐ คือ Louisiana Washingon D.C. Illinois Rhode island Missisippi และ North Carolina ส่วนมลรัฐที่เหลือทั้งหมดนั้นใช้กฎหมายที่เกี่ยวกับการคุกคาม (Stalking Law) มาใช้เทียบเคียงลงโทษผู้กระทำความผิดฐาน Cyberstalking ซึ่งผู้ศึกษาจะได้ทำการศึกษากฎหมายของมลรัฐมิสซิสซิปปี้เป็นหลัก หากมลรัฐอื่นใน 6 มลรัฐที่กล่าวมาบัญญัติแตกต่างกัน ผู้ศึกษาจะนำมากล่าวเอาไว้ด้วย และจากนี้ผู้ศึกษาจะใช้คำว่า Cyberstalking เพื่อจะได้ความทั้งหมดของการคุกคามทางอินเตอร์เน็ต และการศึกษาครั้งนี้ผู้ศึกษาได้ทำการวิเคราะห์และแยกประเด็นของการกระทำความผิดอาญาโดยการคุกคามทางอินเตอร์เน็ต ดังนี้

3.3 องค์ประกอบของความผิดฐาน Cyberstalking[48]

(1) องค์ประกอบในเรื่องของเจตนา (The "Intentional" Mens Rea Requirement) เช่นเดียวกับอาชญากรรมทั้งหลาย การคุกคามทั่ว ไปประกอบด้วยองค์ประกอบของ "เจตนา" Mens Rea และ "การกระทำ" Actus Reus โดยทั่วไปผู้คุกคามต้อง "กระทำการใด ๆ ซ้ำ ๆ " หรือ "การกระทำต่อเนื่อง " (องค์ประกอบของการกระทำ) course of conduct "อย่างจงใจหรือตั้งใจ " (องค์ประกอบของเจตนา) ซึ่งทำให้เหยื่อนั้นหวาดกลัว หรือผู้คุกคามควรจะรู้ว่าการกระทำดังกล่าวจะทำให้เหยื่อกลัวในความปลอดภัยของตน แม้ว่ากฎหมายของแต่ละรัฐจะมีความแตกต่างกันอยู่มาก แต่กฎหมายส่วนใหญ่ของรัฐต่าง ๆ ในสหรัฐอเมริกาก็จะบัญญัติองค์ประกอบในเรื่องของเจตนาเอาไว้

องค์ประกอบในเรื่องเจตนานี้ควรเป็นอ งค์ประกอบในการพิจารณาการคุกคามทางอินเตอร์เน็ต Cyberstalking เช่นกัน จุดประสงค์หลักของกฎหมาย Cyberstalking คือเพื่อหยุดบุคคลไม่ให้ทำให้บุคคลอื่นเกิดความหวาดกลัวอย่างตั้งใจ ดังนั้นผู้คุกคามทางอินเตอร์เน็ต หรือ Cyberstalker จะต้องกระทำการใด ๆ "อย่างตั้งใจ" ที่จะทำให้เหยื่อเกิดความกลัวในความปลอดภัยของตนเอง

(2) องค์ประกอบเรื่องของการกระทำ มี "การกระทำต่อเนื่อง" ที่ทำให้วิญญูชน (reasonable person) เกิดความหวาดกลัวในความปลอดภัยของตน

---

[48] Naomi H. Goodno, "Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws," p.12.

ในการพิจารณาว่า “การกระทำ” ใดควรจะเป็นความผิดอาญา ควรจะพิจารณา 2 กรณีดังนี้

(2.1) กฎหมายการคุกคามทั่วไปส่วนใหญ่จะกำหนดให้การกระทำที่เป็นความผิดต้อง “ทำซ้ำๆ” กัน หมายความว่า ผู้คุกคามจะทำผิดกฎหมายก็ต่อเมื่อได้กระทำการใด ๆ ที่ทำให้เหยื่อเกิดความหวาดกลัวมากกว่าหนึ่งครั้ง ซึ่งก็เป็นการเหมาะสมที่จะกำหนดให้ผู้คุกคามทางอินเตอร์เน็ตหรือ Cyberstalker ต้องกระทำการซ้ำ ๆ อาทิเช่น การส่งอีเมล์ที่มีข้อความข่มขู่มากกว่าหนึ่งครั้ง หรือลงข้อความซึ่งทำให้บุคคลอื่นถูกข่มขู่คุกคามหรือรังควาน ข่มขู่เหยื่อในเว็บไซต์มากกว่าหนึ่งครั้ง เป็นต้น

(2.2) ชนิดของการกระทำ ที่เป็นความผิดอาญาของการคุกคามทั่วไป (Stalking) มีอยู่ 3 ประเภท คือ

2.2.1 การกระทำซึ่งมีการอยู่ใกล้เหยื่อ

2.2.2 มีการกระทำที่สื่อถึงการข่มขู่ทางวาจาหรือมีข้อความหรือคำขู่ที่สามารถเชื่อมโยงไปยังการกระทำ กล่าวคือ เป็น “คำขู่ที่น่าจะเป็นจริง” (Credible threat)

2.2.3 การกระทำที่ทำให้ “วิญญูชนทั่วไป” เกิดความหวาดกลัวในความปลอดภัยของตนเองหรือเกิดอาการซึมเศร้าทางอารมณ์อย่างรุนแรง ซึ่งการกระทำที่อาศัยเกณฑ์ของวิญญูชนทั่วไปนี้ทำให้กฎหมายนั้นสามารถครอบคลุม Cyberstalking ได้อย่างทั่วถึง เนื่องจากกฎหม ายนั้นมุ่งไปที่ผลกระทบต่อเหยื่อจากการกระทำของผู้กระทำผิด เช่น ความรู้สึกหวาดกลัว หรือตื่นตระหนกของเหยื่อ

3.3.1 องค์ประกอบในส่วนของการกระทำภายนอก (Actus Reus)

กฎหมาย Cyberstalking ของมลรัฐมิสซิสซิปปี้ (MISS.CODE.ANN.S. 97-45-15) มาตรา 97-45-15 บัญญัติว่า “ (1) บุคคลกระทำการอย่างหนึ่งอย่างใดต่อไปนี้ถือเป็นความผิดทางกฎหมาย

(a) ใช้อีเมล์หรือการสื่อสารทางอิเล็กทรอนิกส์ด้วยถ้อยคำหรือภาษาข่มขู่ที่จะทำร้ายร่างกายบุคคลใดบุคคลหนึ่ง หรือบุตร พี่น้อง สามีหรือภรรยา หรือผู้อยู่ในความอุปการะของบุคคลนั้น หรือข่มขู่ ที่จะทำลายทรัพย์สินของบุคคลใดบุคคลหนึ่ง หรือเพื่อจุดประสงค์ขู่เข็ญให้ได้มาซึ่งเงินหรือของมีค่าอื่นจากบุคคลใดบุคคลหนึ่ง

(b) ส่งอีเมล์หรือการสื่อสารทางอิเล็กทรอนิกส์ถึงบุคคลอื่นซ้ำ ๆไม่ว่าการกระทำจะนำไปสู่การสนทนาหรือไม่ เพื่อข่มขู่ ข่มขวัญ หรือรังควานบุคคล ใดบุคคลหนึ่ง

(c) ส่งอีเมล์หรือการสื่อสารทางอิเล็กทรอนิกส์ถึงบุคคลอื่นโดยรู้ว่าถ้อยคำนั้นเป็นเท็จเกี่ยวกับเรื่องการตาย การบาดเจ็บ การเจ็บป่วย พิการ การกระทำไม่เหมาะสม หรือการกระทำผิดทางอาญาของบุคคลที่ได้รับการสื่อสารนั้น ๆ หรือของสมาชิกในครอบครัวของบุคคลนั้ นโดยมีเจตนาข่มขู่ ข่มขวัญ หรือรังควาน

(d) ยินยอมรับรู้ให้มีการใช้อุปกรณ์การสื่อสารทางอิเล็กทรอนิกส์ ซึ่งอยู่ในความควบคุมของตน เพื่อใช้กระทำการตามที่ห้ามไว้ในมาตรานี้[49]

จากกฎหมาย Cyberstalking ของมลรัฐมิสซิสซิปปี้ พอที่จะสามารถอธิบายถึงการกระทำที่ถือว่าเป็นการกระทำความผิดฐาน Cyberstalking ผู้กระทำจะต้องมีการกระทำดังนี้

(1) ใช้หรือส่งอีเมล์หรือการสื่อสารทางอิเล็กทรอนิกส์ ด้วยถ้อยคำข่มขู่ที่จะทำร้ายร่างกาย หรือข่มขู่ที่จะทำลายทรัพย์สิน ซึ่งในกฎหมายของมลรัฐมิสซิสซิปปี้มิได้ให้คำจำกัดความคำว่า “อีเมล์” เอาไว้ มีเพียงมลรัฐหลุย ส์เซียน่าและมลรัฐนอร์ทคาโรไลน่าที่ให้ความหมายเอาไว้เหมือนกัน ดังนี้ กฎหมายของหลุยส์เซียน่า มาตรา 40.3 (a)(2) “อีเมล์ ” หมายความว่าการถ่ายทอดข้อมูลหรือการสื่อสารผ่านทางอินเตอร์เน็ต คอมพิวเตอร์ เครื่องโทรสาร วิทยุติดตามตัว โทรศัพท์เคลื่อนที่ เครื่องบันทึกวีดีโอ หรือ

---

[49] MISS.CODE.ANN.S. 97-45-15 (1) It is unlawful for a person to:

(a) Use in electronic mail or electronic communication any words or language threatening to inflict bodily harm to any person or to that person's child, sibling, spouse or dependent, or physical injury to the property of any person, or for the purpose of extorting money or other things of value from any person.

(b) Electronically mail or electronically communicate to another repeatedly, whether or not conversation ensues, for the purpose of threatening, terrifying or harassing any person.

(c) Electronically mail or electronically communicate to another and to knowingly make any false statement concerning death, injury, illness, disfigurement, indecent conduct, or criminal conduct of the person electronically mailed or of any member of the person's family or household with the intent to threaten, terrify or harass.

(d) Knowingly permit an electronic communication device under the person's control to be used for any purpose prohibited by this section.

วิธีทางไฟฟ้าอื่น ๆ ซึ่งส่งถึงบุคคลใดบุคคลหนึ่งโดยใช้ที่อยู่หรือหมายเลขที่อยู่ที่จำเพาะเจาะจง และบุคคลผู้นั้นได้รับการสื่อสารดังกล่าว”[50]

และคำว่า “การสื่อสารทางอิเล็กทรอนิกส์” กฎหมายของมลรัฐมิสซิส ซิปปี้มิบัญญัติคำจำกัดความเอาไว้ แต่ในมลรัฐหลุย ส์เซียน่าและมลรัฐนอร์ทคาโรไลน่าได้ให้คำจำกัดความเหมือนกันในกฎหมายของมลรัฐหลุย ส์เซียน่าบัญญัติไว้ในมาตรา 40.3 (a)(1) ว่า “การสื่อสารทางอิเล็กทรอนิกส์” หมายความว่า การส่งผ่านโดยทั้งหมดหรือเพียงส่วนใดส่วนหนึ่งของเครื่องหมาย สัญญาณ ข้อเขียน รูปภาพ เสียง ข้อมูล หรือข่าวกรองในลักษณะใดก็ตามทางระบบสาย ระบบวิทยุ ระบบคอมพิวเตอร์ ระบบแม่เหล็กไฟฟ้า ระบบการแผ่รังสีของคลื่นแม่เหล็กไฟฟ้า หรือระบบโฟโต้ออปติคอล[51]

กฎหมายของมลรัฐวอชิงตันบัญญัติไว้ในมาตรา 9.61.260 (5) ว่า “การสื่อสารทางอิเล็กทรอนิกส์” หมายถึง การส่งผ่านข้อมูลทางสายวิทยุ เคเบิลออปติเคิล คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่น ๆโดย การสื่อสารทางอิเล็กทรอนิกส์หมายรวมถึงแต่ไม่จำกัดเพียงอีเมล์ การสื่อสารทางอินเตอร์เน็ต การบริการวิทยุติดตามตัว และกา รส่งข้อความทางอิเล็กทรอนิกส์[52]

และกฎหมายของมลรัฐอิลลินอยส์ 720 ILCS 5/12-7.5. (b) บัญญัติว่า “การสื่อสารอิเล็กทรอนิกส์” หมายถึง การส่งผ่านโดยทั้งหมดหรือเพียงส่วนใดส่วนหนึ่งของเครื่องหมาย สัญญาณ ข้อเขียน เสียง ข้อมูล หรือข่าวกรองในลักษณะใดก็ตาม ท าง ระบบสาย ระบบวิทยุ ระบบแม่เหล็กไฟฟ้า ระบบการแผ่รังสีของคลื่นแม่เหล็กไฟฟ้า

---

[50] LA. REV. STAT. ANN. S. 40.3 A. For the purposes of this Section, the following words shall have the following meanings:

(2) "Electronic mail" means the transmission of information or communication by the use of the Internet, a computer, a facsimile machine, a pager, a cellular telephone, a video recorder, or other electronic means sent to a person identified by a unique address or address number and received by that person.

[51] LA. REV. STAT. ANN. S. 40.3 A. For the purposes of this Section, the following words shall have the following meanings:

(1) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, transmitted in whole or in part by wire, radio, computer, electromagnetic, photoelectric, or photo-optical system.

[52] WASH.REV.CODE.ANN. RCW 9.61.260 (5) For purposes of this section, "electronic communication" means the transmission of information by wire, radio, optical cable, electromagnetic, or other similar means. "Electronic communication" includes, but is not limited to, electronic mail, internet-based communications, pager service, and electronic text messaging.

หรือระบบโฟโต้ออปติคอล “การสื่อสารอิเล็กทรอนิกส์” หมายรวมถึง การส่งผ่านข้อมูลจากคอมพิวเตอร์เครื่องหนึ่งไปยังคอมพิวเตอร์เครื่องหนึ่งด้วย[53]

นอกจากการส่งอีเมล์หรือการสื่อสารทางอิเล็กทรอนิกส์ด้วยถ้อยคำหรือภาษาข่มขู่ที่จะทำร้ายร่างกายหรือข่มขู่ที่จะทำลายทรัพย์สินแล้ว ในกฎหมายของมลรัฐวอชิงตันได้บัญญัติไว้มากกว่าการส่งถ้อยคำหรือภาษาข่มขู่ไว้ด้วย คือ การใช้คำพูด รูปภาพ หรือภาษาที่เลวทราม หยาบโลน ลามก หรืออนาจาร หรือเป็นการ กระทำที่ทำให้คิดไปในทางหยาบโลน หรือลามก[54] ซึ่งในกฎหมายของมลรัฐอื่น ๆ ไม่ได้บัญญัติละเอียดเหมือนมลรัฐวอชิงตัน

(2) ส่งอีเมล์หรือการสื่อสารทางอิเล็กทรอนิกส์ถึงบุคคลอื่นซ้ำ ๆ

ในกฎหมายของมลรัฐมิสซิสซิปปี้มิได้บัญญัติว่าการกระทำซ้ำ ๆ นั้นจะต้องกระทำกี่ครั้งแต่ในกฎหมายของมลรัฐอิลลินอยส์ได้บัญญัติเอาไว้ใน 720 ILCS 5/12-7.5. (a) ว่า “บุคคลกระทำการคุกคามทางอินเตอร์เน็ตเมื่อบุคคลนั้น แสดงว่ารู้และปราศจากเหตุอันควรทางกฎหมาย โดยอย่างน้อยในสองคราวอย่างชัดเจน รังควานบุคคลอื่นผ่านทางการสื่อสารอิเล็กทรอนิกส์ ” ในมลรัฐอิลลินอยส์ได้กำหนดเอาไว้ว่า “โดยอย่างน้อยสองคราว อย่างชัดเจน” ส่วนในกฎหมายของมลรัฐวอชิงตันได้บัญญัติเพิ่มจากการกระทำซ้ำ ๆ ไว้ว่า “ไม่เปิดเผย ”[55] และในมลรัฐโร้ดไอร์แลนด์ได้กำหนดว่า มีการกระทำ (Course of Conduct) ที่ต่อเนื่องให้เห็นเป็นระยะเวลาหนึ่ง[56]

---

[53] 720 ILCS 5/12-7.5. (b) As used in this Section:

"Harass" means to engage in a knowing and willful course of conduct directed at a specific person that alarms, torments, or terrorizes that person.

"Electronic communication" means any transfer of signs, signals, writings, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electronmagnetic, photoelectric, or photo-optical system. "Electronic communication" includes transmissions by a computer through the Internet to another computer.

[54] WASH.REV.CODE.ANN. RCW 9.61.260 (1) (a) Using any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act;

[55] WASH.REV.CODE.ANN. RCW 9.61.260 (1) (b) Anonymously or repeatedly whether or not conversation occurs; or

[56] RI. GEN. LAW S. 11-52-4.2 (a) ..... "Course of conduct" means a pattern of conduct composed of a series of acts over a period of time, evidencing a continuity of purpose.

(3) ส่งอีเมล์หรือการสื่อสารทางอิเล็กทรอนิกส์โดยรู้ว่าข้อความนั้นเป็นเท็จ

กฎหมายของมลรัฐมิสซิสซิปปี้นั้นได้กำหนดว่าการส่ง อีเมล์ หรือการสื่อสารทางอิเล็กทรอนิกส์ที่เป็นเท็จ เช่นเรื่องการตาย การเจ็บป่วย หรือการกระทำความผิดทางอาญาของผู้ที่ได้รับการสื่อสารหรือสมาชิกในครอบครัว กฎหมายถือว่าเป็นความผิด แต่ในกฎหมายของมลรัฐอิลลินอยส์ มลรัฐวอชิงตัน และมลรัฐโร้ดไอร์แลนด์มิได้บัญญัติถึงการส่งข้อความอันเป็นเท็จให้กับผู้รับการสื่อสารหรือคนในครอบครัวว่าเป็นการกระทำความผิดฐาน Cyberstalking คงมีเพียงมลรัฐนอร์ทคาโรไลน่า และมลรัฐหลุย ส์เซียน่าที่บัญญัติให้การกระทำในลักษณะดังกล่าวเป็นความผิดเหมือนมลรัฐมิสซิสซิปปี้

(4) ยินยอมรับรู้ให้ใช้อุปกรณ์อิเล็กทรอกนิส์ซึ่งอยู่ในความครอบครองของตนเพื่อกระทำการตาม (1) ถึง (3)

บทบัญญัติของกฎหมายมลรัฐมิสซิสซิปปี้นี้เป็นบทบัญญัติที่เอาผิดกับบุคคลที่รู้เห็นเป็นใจในการกระทำความผิดด้วยอาจจะถือได้ว่าเป็นผู้สนับสนุนให้มีการกระทำความผิดโดยการยินยอมให้ใช้อุปกรณ์อิเล็กทรอนิกส์ที่อยู่ในความครอบครองไปใช้กระทำความผิด ซึ่งในกฎหมายของมลรัฐวอชิงตัน มลรัฐโร้ดไอร์แลนด์ และมลรัฐอิลลินอยส์ไม่ได้กล่าวถึงการกระทำผิดในลักษณะดังกล่าวของผู้ครอบครองอุปกรณ์อิเล็กทรอนิกส์

3.3.2 องค์ประกอบภายใน (Mens Rea) หรือเจตนาในการกระทำความผิด

องค์ประกอบภายในส่วนของ Mens Rea ผู้ที่กระทำ Cyberstalking นั้นจะต้องมีเจตนาที่จะกระทำซึ่งตามกฎหมายของมลรัฐมิสซิสซิปปี้ นั้นได้บัญญัติไว้ว่า “โดยเจตนาข่มขู่ ข่มขวัญ หรือรังควาน”

แต่ในกฎหมายของมลรัฐอิลลินอยส์บัญญัติในส่วนของ Mens Rea ไว้ว่า “(a) บุคคลกระทำการคุกคามทางอินเตอร์เน็ตเมื่อบุคคลนั้น แสดงว่ารู้และปราศจากเหตุอั นควรทางกฎหมาย โดยอย่างน้อยในสองคราวอย่างชัดเจน รังควานบุคคลอื่นผ่านทางการสื่อสารอิเล็กทรอนิกส์...”

ในกฎหมายของมลรัฐอิลลินอยส์ได้ให้คำจำกัดความคำว่า “รังควาน” หมายถึง มีส่วนร่วมอย่างแสดงว่ารู้หรือจงใจในการกระทำที่เจาะจงไปยังบุคคลใดโดยเฉพาะเพื่อจะทำให้บุคคลนั้นตระหนก ทรมาน หรือตื่นตกใจ[57]

---

[57] 720 ILCS 5/12-7.5. (b) As used in this Section:

"Harass" means to engage in a knowing and willful course of conduct directed at a specific person that alarms, torments, or terrorizes that person.

Cyberstalking นั้น ผู้กระทำต้องมีองค์ประกอบในส่วนของ Mens Rea ไม่ว่าโดยจงใจ โดยเจตนาข่มขู่ ข่มขวัญหรือรังควาน ซึ่ง Cyberstalking ผู้กระทำนั้นรู้ถึงการกระทำนั้นและได้กระทำการนั้นซ้ำ ๆ ซึ่งนอกจากนี้ในกฎห มายของมลรัฐมิสซิสซิปปี้ได้บัญญัติเรื่องเจตนาพิเศษไว้ด้วย “เพื่อจุดประสงค์ขู่เข็ญให้ได้มาซึ่งเงินหรือของมีค่าอื่นจากบุคคลใดบุคคลหนึ่ง”[58]

3.4 เหตุที่กฎหมายยกเว้นความผิด

กฎหมาย Cyberstalking ของบางมลรัฐจะมีข้อยกเว้น คือการกระทำที่ครบองค์ประกอบของ Cyberstalking แต่กฎหมายไม่ถือเป็นความผิดฐาน Cyberstalking ซึ่งข้อยกเว้นนี้บางรัฐก็บัญญัติเอาไว้ต่างกัน หรือบางรัฐก็ไม่ได้บัญญัติข้อยกเว้นนี้เอาไว้

ในกฎหมายของมลรัฐมิสซิสซิปปี้ มาตรา 97-45-15 (3) บัญญัติว่า “มาตรานี้ไม่บังคับใช้กับการกระทำที่สงบ ปร าศจากความรุนแรง หรือมิได้เป็นการข่มขวัญโดยมีเจตนาเพื่อแสดงความคิดเห็นทางการเมือง หรือเพื่อให้ข้อมูลที่ถูกกฎหมายแก่บุคคลอื่น โดยห้ามตีความมาตรานี้กระทบการกระทำที่ได้รับความคุ้มครองภายใต้รัฐธรรมนูญ ซึ่งรวมถึงการพูด การประท้วง หรือการรวมกลุ่ม ”[59] ซึ่งบท บัญญัติดังกล่าวนี้เหมือนบทบัญญัติของมลรัฐนอร์ทคาโรไลน่า (มาตรา 14-196.3. (e)) ส่วนกฎหมายของมลรัฐหลุย ส์เซียน่า มาตรา 40.3 E บัญญัติไว้ว่า “ มาตรานี้ไม่ได้ใช้กับการกระทำที่สงบปราศจากความรุนแรง หรือมิได้เป็นการข่มขวัญโดยมีเจตนาเพื่อแสดงความเห็นทางการเมืองหรือให้ข้อมูลที่ถูกกฎหมายแก่บุคคลอื่น”[60]

---

[58] MISS.CODE.ANN.S. 97-45-15 (1) It is unlawful for a person to:
(a) Use in electronic mail or electronic communication any words or language threatening to inflict bodily harm to any person or to that person's child, sibling, spouse or dependent, or physical injury to the property of any person, or for the purpose of extorting money or other things of value from any person.

[59] MISS.CODE.ANN.S. 97-45-15 (3) This section does not apply to any peaceable, nonviolent, or nonthreatening activity intended to express political views or to provide lawful information to others. This section shall not be construed to impair any constitutionally protected activity, including speech, protest or assembly.

[60] LA. REV. STAT. ANN. S. 40.3 E. This Section does not apply to any peaceable, nonviolent, or nonthreatening activity intended to express political views or to provide lawful information to others.

3.5 การกระทำความผิดฐาน Cyberstalking โดยมีเหตุฉกรรจ์

การกระทำความผิดฐาน Cyberstalking นั้นถ้ามีเหตุฉกรรจ์ตามที่กฎหมายกำหนดอยู่เกิดขึ้นด้วยผู้กระทำความผิดฐาน Cyberstalking โดยมีเหตุฉกรรจ์นั้นต้องได้รับโทษเ พิ่มขึ้นจากการกระทำความผิดฐาน Cyberstalking โดยไม่มีเหตุฉกรรจ์ด้วย เนื่องจากผู้กระทำ Cyberstalking นั้น ได้กระทำการอื่นนอกเหนือไปจากพฤติกรรม Cyberstalking เช่น มีการทำร้ายร่างกายเหยื่อจริงตามที่ข่มขู่ หรือมีการข่มขู่ว่าจะฆ่าและมีการฆ่าเกิดขึ้นจริง ซึ่งการกระทำดังกล่าวนั้นทำให้เหยื่อได้รับอันตรายแล้ว หรือน่าจะทำให้เหยื่อนั้นได้รับอันตรายทางกายจากการข่มขู่จริง ๆ ซึ่งในแต่ละมลรัฐก็ได้แบ่งแยกระดับ (Degree) ของการลงโทษเอาไว้ ถ้ามีเหตุหรือพฤติกรรมใดตามที่กฎหมายกำหนดก็จะต้องได้รับโทษหนักขึ้น เหตุฉกรรจ์ที่กฎหมายบัญญัติไว้ได้แก่

3.5.1 การกระทำความผิดฐาน Cyberstalking ที่กระทำซ้ำ

กฎหมายของมลรัฐมิสซิสซิปปี้ได้บัญญัติเรื่องของการกระทำผิดซ้ำไว้ในมาตรา 97-45-15 (b)(iv) ว่า “บุคคลนั้นเคยได้ถูกตัดสินว่าฝ่าฝืนมาตรานี้หรือกฎหมายที่คล้ายคลึงกันอย่างมากของรัฐอื่น เขตปกครองย่อยของรัฐอื่น หรือสหพันธรัฐ”[61]

กฎหมายของมลรัฐโร้ดไอร์แลนด์ มาตรา 11-52-4.2 บัญญัติว่า “การกระทำครั้งที่สองหรือครั้งถัดไปตามอนุมาตรา (a) นี้ถือเป็นความผิดอาญาฐานหนักต้องโทษจำคุกไม่เกิน 2 ปี ปรับไม่เกิน 6,000 ดอลล่าร์ หรือทั้งจำทั้งปรับ”[62]

กฎหมายของมลรัฐวอชิงตันแก้ไขเพิ่มเติมมาตรา 9.61.260 (3) บัญญัติว่า “การคุกคามทางอินเตอร์เน็ตถือเป็นความผิดอาญาร้ายแรงประเภท C หากมีข้อหนึ่งข้อใดต่อไปนี้ (a) “ผู้ลงมือกระทำเคยถูกตัดสินว่ากระทำความผิดเกี่ยวกับการรังควาน ดังที่นิยามไว้ในมาตรา 9A.46.060 ต่อเหยื่อรายเดิมหรือต่อสมาชิกในครอบครัวของเหยื่อรายเดิม.....”[63]

---

[61] MISS.CODE.ANN.S. 97-45-15 (b) (iv) The person has been previously convicted of violating this section or a substantially similar law of another state, a political subdivision of another state, or of the United States.

[62] RI. GEN. LAW S. 11-52-4.2 (b) A second or subsequent conviction under subsection (a) of this section shall be deemed a felony punishable by imprisonment for not more than two (2) years, by a fine of not more than six thousand dollars ($6,000), or both.

[63] WASH.REV.CODE.ANN. RCW 9.61.260 (3) Cyberstalking is a class C felony if either of the following applies:

(a) The perpetrator has previously been convicted of the crime of harassment, as defined in

ในกฎหมายของมลรัฐหลุย ส์เซียน่า มาตรา 40.3 (C)(2) บัญญัติว่า “หากมีการกระทำความผิดเป็นครั้งที่สองเกิดขึ้นในช่วงเวลา 7 ปี หลังจากการกระทำความผิดฐานคุกคามทางอินเตอร์เน็ตครั้งแรก ผู้กระทำความผิดต้องถูกจำคุกไม่น้อยกว่า 180 วัน แต่ไม่เกิน 3 ปี และอาจถูกปรับไม่เกิน 5,000 ดอลล่าร์ หรือทั้งจำทั้งปรับ [64] และมาตรา 40.3 (C)(3) บัญญัติว่า “หากมีการกระทำผิดเป็นครั้งที่สามหรือครั้งถัดมาเกิดขึ้นในช่วงเวลา 7 ปี หลังจากการกระทำความผิดคุกคามครั้งก่อนห น้า ผู้กระทำความผิดต้องถูกจำคุกไม่น้อยกว่า 2 ปีแต่ไม่เกิน 3 ปี และอาจถูกปรับไม่เกิน 5,000 ดอลล่าร์ หรือทั้งจำทั้งปรับ”[65] ในกฎหมายของมลรัฐหลุย ส์เซียน่าบัญญัติแตกต่างจากกฎหมายของมลรัฐอื่น คือ ได้บัญญัติเงื่อนไขของระยะเวลาในการกระทำซ้ำและจะต้องรับโทษหนั กขึ้นคือการกระทำครั้งที่สองนั้นเกิดขึ้นภายในระยะเวลา 7 ปี หลังจากการกระทำความผิดครั้งแรก

ส่วนกฎหมายของมลรัฐอิลลินอยส์ 720 ILCS 5/12-7.5. (C) บัญญัติว่าการวางโทษ การคุกคามทางอินเตอร์เน็ตถือเป็นความผิดอาญาร้ายแรงประเภท 4 (Class 4 Felony) การลงโทษครั้งที่สองหรือครั้งต่อ ๆ มา สำหรับการคุกคามทางอินเตอร์เน็ตถือเป็นความผิดอาญาร้ายแรงประเภท 3 (Class 3 Felony)[66]

3.5.2 การกระทำความผิดฐาน Cyberstalking ในระหว่างที่ศาลมีคำสั่งห้ามชั่วคราว

กฎหมายของมลรัฐมิสซิสซิปปี้ได้บัญญัติเกี่ยวกับการกระทำความผิด Cyberstalking ในระหว่างที่คำสั่งของศาลมีผลบังคับใช้อยู่ โดยโทษที่จะลงแก่ผู้กระทำความผิดก็สูงขึ้นด้วย ตามมาตรา 97-45-15 (b) บัญญัติว่า “บุคคลนั้นมีความผิดอาญาฐาน

RCW 9A.46.060, with the same victim or a member of the victim's family or household .....”

[64] LA. REV. STAT. ANN. S. 40.3 (C) (2) Upon a second conviction occurring within seven years of the prior conviction for cyberstalking, the offender shall be imprisoned for not less than one hundred and eighty days and not more than three years, and may be fined not more than five thousand dollars, or both.

[65] LA. REV. STAT. ANN. S. 14:40.3 C. (3) Upon a third or subsequent conviction occurring within seven years of a prior conviction for stalking, the offender shall be imprisoned for not less than two years and not more than five years and may be fined not more than five thousand dollars, or both.

[66] 720 ILCS 5/12-7.5. (c) Sentence. Cyberstalking is a Class 4 felony. A second or subsequent conviction for cyberstalking is a Class 3 felony.

หนัก ต้องโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 10,000 ดอลล่าร์ หรือทั้งจำทั้งปรับ หากกระทำการอย่างใดอย่างหนึ่งต่อไปนี้[67]

(i) การกระทำความผิดฝ่าฝืนคำสั่งควบคุมการกระทำของบุคคลและบุคคลนั้นได้รับแจ้งคำสั่งควบคุมนั้นแล้วหรือการลงข้อความฝ่าฝืนคำสั่งห้ามหรือคำสั่งห้ามในชั้นต้น[68]

(ii) การกระทำความผิดฝ่าฝืนเงื่อนไขการภาคทัณฑ์ เงื่อนไขการพันโทษโดยมีทัณฑ์บน เงื่อนไข การปล่อยตัวก่อนพิจารณาคดี เงื่อนไขการปล่อยตัวระหว่างอุทธรณ์โดยมีประกัน[69]

กฎหมายของมลรัฐโร้ดไอร์แลนด์ มาตรา 11-52-4.3 (a) บัญญัติว่า “เมื่อศาลที่มีอำนาจตัดสินคดีมีคำสั่งควบคุมหรือห้ามการกระทำของบุคคล โดยห้ามบุคคลหนึ่งรังควานบุคคลอีกผู้หนึ่ง และต่อมาบุคคลที่ถูกสั่งห้ามได้กระทำความผิดอาญาตามมาตรา 11-52-4.2 ต่อบุคคลที่ศาลมีคำสั่งคุ้มครอง บุคคลที่ฝ่าฝืนคำสั่งมีความผิดอาญาฐานหนักต้องโทษจำคุกไม่เกินสองปีหรือปรับไม่เกิน 6,000 ดอลล่าร์ หรือทั้งจำทั้งปรับ[70]

---

[67] MISS.CODE.ANN.S. 97-45-15 (b) If any of the following apply, the person is guilty of a felony punishable by imprisonment for not more than five (5) years or a fine of not more than Ten Thousand Dollars ($10,000.00), or both:

[68] MISS.CODE.ANN.S. 97-45-15 (b)(i) The offense is in violation of a restraining order and the person has received actual notice of that restraining order or posting the message is in violation of an injunction or preliminary injunction

[69] MISS.CODE.ANN.S. 97-45-15 (b) (ii) The offense is in violation of a condition of probation, a condition of parole, a condition of pretrial release or a condition of release on bond pending appeal.

[70] RI. GEN. LAW S. 11-52-4.3 (a) Whenever there is a restraining order or injunction issued by a court of competent jurisdiction enjoining one person from harassing another person, and the person so enjoined is convicted of the crime as set forth in section 11-52-4.2 for actions against the person protected by the court order or injunction, he or she shall be guilty of a felony which shall be punishable by imprisonment for not more than two (2) years, or by a fine of not more than six thousand dollars ($6,000), or both.

และมาตรา 11-52-4.3 (b) บัญญัติว่า “การกระทำครั้งที่สองหรือครั้งถัดไปตามอนุมาตรา (a) ของมาตรานี้ต้องโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 10,000 ดอลล่าร์ หรือทั้งจำทั้งปรับ”[71]

ในกฎหมายของมลรัฐวอชิงตันแก้ไขเพิ่มเติมมาตรา 9.61.260 (3) บัญญัติว่า “การคุกคามทางอินเตอร์เน็ตถือเป็นความผิดอาญา ร้ายแรงประเภท C หากมีข้อหนึ่งข้อใดต่อไปนี้ (a) “ผู้ลงมือกระทำเคยถูกตัดสินว่ากระทำความผิดเกี่ยวกับการรังควาน ดังที่ได้นิยามไว้ในมาตรา 9A.46.060 ต่อเหยื่อรายเดิมหรือต่อสมาชิกของเหยื่อรายเดิม หรือต่อบุคคลที่ได้มีการเจาะจงระบุไว้โดยเฉพาะในคำสั่งห้ามมิให้ติดต่อ หรือคำสั่ งห้ามมิให้รังควานภายในรัฐนี้หรือรัฐใด ๆ หรือ....”[72]

3.5.3 การกระทำความผิดฐาน Cyberstalking โดยใช้ความรุนแรง

การกระทำความผิดฐาน Cyberstalking โดยมีการกระทำที่เป็นการใช้ความรุนแรงด้วยนั้นถือว่าเป็นการคุกคามทางอินเตอร์เน็ตโดยมีเหตุฉกรรจ์ และการกระ ทำความผิดก่อให้เกิดคำขู่ที่น่าเชื่อ (Credible Threat) ว่าจะเกิดขึ้นจริง ซึ่งการข่มขู่ในลักษณะดังกล่าวนั้นมีลักษณะที่ทำให้เหยื่อนั้นเกิดความกลัวว่าจะมีการกระทำตามที่ข่มขู่จริง หรือนอกจากการคุกคามทางอินเตอร์เน็ตในรูปแบบปกติแล้ว การคุกคามหรือการส่งคำขู่ นั้นอาจรุนแรงขึ้นเป็นการคุกคามทางกายภาพ หรือเหยื่ออาจจะเชื่อว่าจะมีการทำร้ายร่างกายจริง ๆ หรือการข่มขู่ว่าจะฆ่า โดยกฎหมายของมลรัฐอิลลินอยส์ได้บัญญัติเอาไว้ชัดเจนคือ 720 ILCS 5/12-7.5. (a)(1) “ ในเวลาใด ๆ สื่อสารการข่มขู่ว่าจะทำร้ายร่างกายในทันทีหรือใ นอนาคต ล่วงเกินทางเพศ หรือกักขังหน่วงเหนี่ยว .....” 720 ILCS 5/12-7.5. (a)(2) “ทำให้

---

[71] RI. GEN. LAW S. 11-52-4.3 (b) A second or subsequent conviction under subsection (a) of this section shall be punishable by imprisonment for not more than five (5) years, by a fine of not more than ten thousand dollars ($10,000), or both.

[72] WASH.REV.CODE.ANN. RCW 9.61.260 (3) Cyberstalking is a class C felony if either of the following applies:

(a) The perpetrator has previously been convicted of the crime of harassment, as defined in RCW 9A.46.060, with the same victim or a member of the victim's family or household or any person specifically named in a no-contact order or no-harassment order in this or any other state; or

บุคคลนั้นหรือสมาชิกในครอบครัวของบุคคลนั้นมีความกลัวโดยสมเหตุผลว่าจะมีการทำร้ายร่างกายในทันทีหรือในอนาคต การล่วงเกินทางเพศ การกักขังหรือหน่วงเหนี่ยว”[73]

ในกฎหมายของมลรัฐวอชิงตันบัญญัติว่า “ผู้ลงมือกระทำเกี่ยวข้องกับการกระทำที่ห้ามไว้ในอนุมาตรา (1)(c) ของมาตรานี้ โดยข่มขู่ที่จะฆ่าบุคคลนั้น หรือบุคคลอื่น ๆ[74]

จากบทบัญญัติของกฎหมายนี้จะเห็นว่านอกจากผู้ทำการ Cyberstalking จะต้องมีการข่มขู่ ข่มขวัญ หรือรังค วานแล้ว ในกรณีที่มีเหตุฉกรรจ์ผู้กระทำจะต้องมีการข่มขู่ว่าจะทำร้ายร่าง ข่มขู่ว่าจะฆ่า หรือกักขังหน่วงเหนี่ยวและได้ลงมือกระทำตามที่ข่มขู่เหยื่อเช่นนั้นจริง

3.6 โทษสำหรับการกระทำความผิดฐาน Cyberstalking

โทษที่จะลงสำหรับการกระทำความผิดฐาน Cyberstalking นั้น คือ โทษจำคุก โทษปรับ หรือทั้งจำทั้งปรับเป็นไปตามพฤติกรรมและความรุนแรงของผู้กระทำความผิด ซึ่งในแต่ละมลรัฐนั้นโทษจะแตกต่างกัน บางมลรัฐบัญญัติให้การกระทำความผิดครั้งแรกเป็นเพียงแค่ความผิดฐานเบา คือจำคุกไม่เกินหนึ่งปี แต่สำหรับบางมลรัฐแม้จะเป็นก ารกระทำความผิดในครั้งแรกก็ถือว่าเป็นการกระทำความผิดร้ายแรงมีโทษจำคุกมากกว่าหนึ่งปีแต่ไม่เกินสามปี (Class 4 Felony) โดยอัตราโทษทั้งความผิดฐานเบาและความผิดร้ายแรงนั้นบางมลรัฐก็มีอัตราโทษที่เหมือนกัน บางมลรัฐก็มีอัตราโทษที่แตกต่างกันออกไป โดยทั้งควา มผิดฐานเบาและความผิดร้ายแรงนั้นแต่ละมลรัฐเองก็มีระดับขั้น (Degree) ของความรุนแรงที่แตกต่างกันแล้วแต่ว่ามลรัฐนั้นจะกำหนดอัตราโทษไว้เท่าใด

---

[73] 720 ILCS 5/12-7.5. (a) A person commits cyberstalking when he or she, knowingly and without lawful justification, on at least 2 separate occasions, harasses another person through the use of electronic communication and:
(1) at any time transmits a threat of immediate or future bodily harm, sexual assault, confinement, or restraint and the threat is directed towards that person or a family member of that person, or
(2) places that person or a family member of that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint.

[74] WASH.REV.CODE.ANN. RCW 9.61.260 (2)(b) The perpetrator engages in the behavior prohibited under subsection (1)(c) of this section by threatening to kill the person threatened or any other person.

อย่างไรก็ดีผู้ที่กระทำความผิดฐาน Cyberstalking ซ้ำ โทษที่ได้รับก็จะเพิ่มขึ้น ในกรณีที่มีการกระทำตามที่ข่มขู่ไว้จ ริง เช่น การทำร้ายร่างกาย กักขังหน่วงเหนี่ยว หรือการฆ่าเหยื่อซึ่งถือว่าเป็นเหตุฉกรรจ์โทษที่ได้รับก็จะหนักมากขึ้นกว่าโทษฐาน Cyberstalking เช่น โทษสำหรับมลรัฐมิสซิสซิปปี้บทลงโทษคือ จำคุกไม่เกินสองปี ปรับไม่เกิน 5,000 ดอลล่าร์หรือทั้งจำทั้งปรับ หากการกระทำนั้นเป็นการฝ่าฝืนข้อห้ามตามที่กฎหมายกำหนดไว้ อาทิเช่น การกระทำความผิดโดยฝ่าฝืนคำสั่งควบคุมการกระทำของบุคคลนั้นและบุคคลนั้นได้รับแจ้งคำสั่งควบคุมนั้นแล้ว หรือการลงข้อความฝ่าฝืนคำสั่งหรือคำสั่งห้ามในชั้นต้น หรือการกระทำความผิดฝ่าฝืนเงื่อนไข การภาคทัณฑ์ เงื่อนไขการพ้นโทษโดยมีทัณฑ์บน เงื่อนไขการปล่อยตัวก่อนการพิจารณาคดี หรือเงื่อนไขการปล่อยตัวระหว่างอุทธรรณ์โดยมีประกัน เป็นต้น ก็จะต้องได้รับโทษหนักขึ้น คือโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกิน 10,000 ดอลล่าร์ หรือ หรือทั้งจำทั้งปรับ[75]

และจากการศึกษากฎหมาย Cyberstalking ของมลรัฐมิสซิสซิปปี้นั้นพบว่ากฎหมายนั้นไม่ได้บัญญัติในเรื่องของสถานที่ที่ถือมีว่ากระทำความผิดฐาน Cyberstalking ไว้ เนื่องจาก Cyberstalking นั้นสามารถกระทำข้ามรัฐได้ ผู้คุกคามอาจจะอยู่คนละรัฐกับเหยื่อ ผู้คุกคามอา จจะอยู่ที่มลรัฐอิลลินอยส์แล้วทำการส่ง อีเมล์คุกคามให้กับเหยื่อที่อยู่ในมลรัฐมิสซิสซิปปี้ จะถือว่ามีการกระทำความผิดฐาน Cyberstalking ที่ใด

ปัญหาดังกล่าวนั้นมีเพียงมลรัฐนอร์ทคาโรไลน่า มลรัฐหลุย ส์เซียน่า และมลรัฐวอชิงตัน สามรัฐจากทั้งหมด หกรัฐที่มีกฎหมาย Cyberstalking แล้วได้บัญญัติกฎหมายเพื่อป้องกันปัญหาดังกล่าว

ในกฎหมาย Cyberstalking ของ มลรัฐนอร์ทคาโรไลน่า มาตรา 14-196.3 (C) นั้นถือว่า “การกระทำความผิดซึ่งกระทำโดยการใช้ อีเมล์หรือการสื่อสารทางอิเล็กทรอนิกส์ให้ถือว่าเกิดขึ้นในสถานที่ที่ อีเมล์หรือการสื่อสารอิเล็กทรอนิกส์ถูกส่งครั้งแรก ได้รับครั้ง

---

[75]MISS.CODE.ANN.S. 97-45-15 (a) Except as provided herein, the person is guilty of a felony punishable by imprisonment for not more than two (2) years or a fine of not more than Five Thousand Dollars ($5,000.00), or both.

(b) If any of the following apply, the person is guilty of a felony punishable by imprisonment for not more than five (5) years or a fine of not more than Ten Thousand Dollars ($10,000.00), or both:

(i) The offense is in violation of a restraining order and the person has received actual notice of that restraining order or posting the message is in violation of an injunction or preliminary injunction.

(ii) The offense is in violation of a condition of probation, a condition of parole, a condition of pretrial release or a condition of release on bond pending appeal.

แรกในรัฐนี้ หรือถูกอ่านครั้งแรกโดยบุคคลใดก็ตามในรัฐนี้ ”[76] ส่วนกฎหมายของมลรัฐหลุยส์เซียน่ามาตรา 40.3 D นั้นบัญญัติว่า “การกระทำความผิดใดตามมาตรานี้ซึ่งกระทำโดยการใช้อีเมล์หรือการสื่อสารอิเล็กทรอนิกส์ใ ห้ถือว่าการกระทำเกิดขึ้นในสถานที่ที่ อีเมล์หรือการสื่อสารอิเล็กทรอนิกส์ถูกส่งครั้งแรก ได้รับครั้งแรก หรือถูกอ่านครั้งแรก ”[77] ซึ่งทั้งสองรัฐนั้นบัญญัติเอาไว้คล้ายกันต่างกัน แค่เพียงในมลรัฐนอร์ทคาโรไลน่า การถูกส่งได้รับหรือถูกอ่านครั้งแรกกระทำโดยบุคคลในมลรัฐนอร์ทคาโรไลน่า ส่วนกฎหมายของมลรัฐวอชิงตันมาตรา 9A.61.260 (4) กำหนดว่า “ความผิดใด ๆ ที่กระทำภายใต้มาตรานี้อาจถือได้ว่ากระทำ ณ สถานที่ซึ่งได้มีการทำการสื่อสาร หรือสถานที่ที่ได้รับการสื่อสาร”[78]

3.7 มาตรการอื่น ๆ ทางกฎหมายที่อาจจะนำมาใช้ได้กับ Cyberstalking

นอกจากบทลงโทษทางกฎหมายแล้วในประเทศสหรัฐอเมริกายังมีมาตรการอื่น ๆ ทางกฎหมายที่สามารถนำมาใช้กับการกระทำผิดฐาน Cyberstalking เพื่อเป็นการป้องกันเหยื่อจากผู้คุกคามหรือเป็นการคุ้มครองเหยื่อในเบื้องต้นมิให้เหยื่อได้รับผลร้ายที่รุนแรงมากกว่าการข่มขู่ ข่มขวัญ หรือรังควาน มาตรการอื่นทางกฎหมายได้แก่

---

[76] NC.GEN.STAT.ANN. 14-196.3 (c) Any offense under this section committed by the use of electronic mail or electronic communication may be deemed to have been committed where the electronic mail or electronic communication was originally sent, originally received in this State, or first viewed by any person in this State.

[77] LA. REV. STAT. ANN. S. 40.3 D. Any offense under this Section committed by the use of electronic mail or electronic communication may be deemed to have been committed where the electronic mail or electronic communication was originally sent, originally received, or originally viewed by any person

[78] WASH.REV.CODE.ANN. RCW 9.61.260 (4) Any offense committed under this section may be deemed to have been committed either at the place from which the communication was made or at the place where the communication was received.

3.7.1 คำสั่งคุ้มครองหรือคำสั่งงดเว้นกระทำการ (Protective or Restraining Order)[79]

คำสั่งคุ้มครองหรือคำสั่งงดเว้นกระทำการคือคำสั่งจากศาล คำสั่งนี้สามารถป้องกันบุคคลจากการถูกรังควาน ทำร้ายร่ างกาย การรุกรานทางเพศ หรือการคุกคามบุคคลอื่น คำสั่งคุ้มครองเป็นการป้องกันอาชญากรรมก่อนที่จะเกิดขึ้น

หากบุคคลไม่มีความสัมพันธ์ในครอบครัว จะขอคำสั่งคุมครองหรือคำสั่งงดเว้นกระทำการได้เฉพาะในกรณีที่ถูกคุกคาม และคำสั่งคุ้มครองหรือคำสั่งงดเว้นกระทำการนั้ นจะไม่ใช้ในกรณีการทะเลาะเบาะแว้งระหว่างเพื่อนบ้าน

คำสั่งคุ้มครองหรือคำสั่งงดเว้นกระทำการนั้นเป็นคำสั่งที่ให้ผู้รับคำสั่งคุ้มครองนั้นไม่

1. เข้าไปในทรัพย์สิน
2. ทำร้ายร่างกาย ทุบตี
3. ข่มขู่ที่จะฆ่าหรือทำให้ได้รับบาดเจ็บ
4. รบกวนในสถานที่ทำงาน
5. ติดต่อทางโทรศัพท์
6. ซื้อหรือเป็นเจ้าของอาวุธปืน
7. ส่งจดหมาย (รวมถึงอีเมล์)

3.7.1.1 ประเภทของคำสั่งคุ้มครองหรือคำสั่งงดเว้นกระทำการ

(1) Restraining Personal Protective Order (สำหรับเหยื่อที่มีความสัมพันธ์กันในครอบครัว)

คำสั่งคุ้มครองหรือคำสั่งงดเว้นกระทำการประเภทนี้เหยื่อจะต้องแสดงความสัมพันธ์ เช่น เป็นสามีหรือภรรยา หรือเคยเป็นสามีหรือเคยเป็นภรรยา หรือเหยื่อจะต้องแสดงว่าใครคือคนที่เหยื่อมีลูกด้วย หรือเหยื่อกำลังมีความสัมพันธ์อยู่กับใคร

(2) Stalking Personal Protection Order (สำหรับเหยื่อที่ถูกคุกคาม)

คำสั่งคุ้มครองคุ้มครองประเภทนี้เหยื่อไม่ต้องแสดงความสัมพันธ์ใด ๆ กับผู้รับคำสั่งคุ้มครอง อย่างไรก็ตามเหยื่อต้องแสดง (a) แบบของพฤติกรรม (b) มีการกระทำอย่างน้อยที่สุดสองคราวชัดเจนที่เป็นเหตุให้วิญญูช นรู้สึกว่าถูกคุกคาม สะพรึงกลัว ถูกข่มขู่ ถูก

[79] What is personal Protection Order ? Internet. http://www.msu.edu/safe/facts/ppo.htm.

ขู่เข็ญ หรือถูกรุกรานทางเ พศ (c) สิ่งที่เกิดขึ้นนั้นมีสาเหตุที่แท้จริงจากการที่เหยื่อรู้สึก ว่าตนเองนั้นถูกคุกคามข่มขู่ขู่เข็ญ หรือถูกรุกรานทางเพศ

วิธีการขอคำสั่งคุ้มครองหรือคำสั่งงดเว้นกระทำการ

ไปยังศาล circuit court ที่เหยื่อมีภูมิลำเนาอยู่และร้องขอคำร้องขอคำสั่งคุ้มครองซึ่งในคำร้องจะระบุคำแนะนำไว้ นอกจากนี้เหยื่ออาจจะต้องระบุวัน เวลา พยานผู้รู้เห็น เอกสารต่าง ๆ ที่สนับสนุนว่าทำไมเหยื่อจะต้องได้รับความคุ้มครอง เมื่อศาลพิจารณาแล้วหากเห็นว่าควรได้รับความคุ้มครองศาลก็จะออกคำสั่งคุ้มครองให้ เหยื่อก็จะได้รับสำเนาคำ สั่งคุ้มครอง ผู้ที่จะต้องปฏิบัติตามคำสั่งศาลก็จะต้องได้รับแจ้งถึงคำสั่งศาลดังกล่าว โดยใครเป็นผู้นำส่งคำสั่งคุ้มครองดังกล่าวก็ได้ ในบางพื้นที่ตำรวจจะเป็นผู้แจ้งถึงคำสั่งคุ้มครองให้ทราบ คำสั่งคุ้มครองนั้นจะมีผลบังคับใช้เมื่อผู้พิพากษานั้นได้ลงนามในคำสั่ง

ในมลรัฐแคลิฟอร์เนียคำสั่งงดเว้นกระทำการเป็นคำสั่งของศาลที่ลงนามโดยผู้พิพากษา คำสั่งงดเว้นกระทำการมี 4 ประเภทที่ประชาชนสามารถร้องขอได้ ได้แก่[80]

1. คำสั่งคุ้มครองฉุกเฉิน (Emergency Protective Order : EPO) คำสั่งงดเว้นกระทำการนี้กำหนดขึ้นโดยการบังคับของกฎหมาย มีระยะเวลาใช้ได้ 5 วัน

2. คำสั่งงดเว้นการใช้ความรุนแรงในครอบครัวชั่วคราว (Domestic violence Temporary Restraining Order :TRO/DRVO) สามารถทำให้เป็นคำสั่งถาวรโดยมีระยะเวลา 1 ปีถึง 3 ปี

3. คำสั่งคุ้มครองทางอาญา (Criminal Protective Order) คำสั่งห้ามพบปะหรือติดต่อ (No contact order) คำสั่งนี้ต้องดำเนินการขอที่สำนักงานอัยการเขต และอัยการจะพิจารณาและส่งเรื่องไปยังผู้พิพากษาเพื่อพิจารณา ส่วนมากจะเป็นคดีเกี่ยวกับการคุกคาม

4. คำสั่งงดเว้นการรบกวนทางแพ่ง (Civil Harassment Restraining Order : CHO) คำสั่งนี้เป็นคำสั่งทางแพ่ง เพื่อคุ้มครองผู้ที่ได้รับคำสั่งจาก

4.1 การก่อความรำคาญ การรบกวน การจู่โจม การติดตาม การรบกวนความสงบของผู้ที่ได้รับการคุ้มครอง

---

[80] วิจิตรา เลิศหิรัญกิจ, “ความผิดฐานเฝ้าติดตามและข่มขู่ Stalking,” (วิทยานิพนธ์ปริญญามหาบัณฑิตคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์,2550),หน้า 44.

4.2 การติดต่อโดยตรงหรือโดยอ้อมกับผู้ที่ได้รับการคุ้มครองไม่ว่า โดยส่วนตัว โดยทางโทรศัพท์ หรือโดยทางอิเล็กทรอนิกส์

4.3 การเข้าใกล้ผู้ได้รับความคุ้มครองในระยะ 100 หลา ในที่ทำงาน ที่อยู่อาศัย หรือโรงเรียน

การร้องขอคำสั่งคุ้มครองนี้เหยื่อไม่จำเป็นต้องไปฟ้องคดีต่อศาลก่อน เพียงแค่ไปยื่นคำร้องต่อศาลและให้ศาลพิจารณาคำร้องเท่านั้น

3.7.2 วิธีการเพื่อความปลอดภัย ซึ่งศาลที่พิจารณาคดีอาจกำหนดคำสั่งให้งดเว้นการติดต่อกับเหยื่อ ซึ่งบางมลรัฐได้บัญญัติเรื่องนี้ไว้และบางมลรัฐก็ไม่ได้บัญญัติเรื่องนี้ไว้[81]

กฎหมายของมลรัฐแคลิฟอร์เนียมาตรา 646.9 (k) “ศาลที่พิพากษาตัดสินคดีควรพิจารณาออกคำสั่งงดเว้นกระทำการติดต่อกับเหยื่อ ใ ห้จำเลยงดเว้นการติดต่อด้วยวิธีการต่าง ๆ กับเหยื่อซึ่งอาจมีผลบังคับนานถึงสิบปี ตามที่ศาลจะเห็นสมควร ซึ่งเป็นเจตนาของฝ่ายนิติบัญญัติที่ว่าระยะเวลาของคำสั่งงดเว้นกระทำการให้ขึ้นอยู่กับความร้ายแรงของข้อเท็จจริงต่าง ๆ ที่ปรากฏต่อศาล ความเป็นไปได้ของการใช้ความรุนแรงในอนาคต และความปลอดภัยของเหยื่อและครอบครัวที่ใกล้ชิดของเขาหรือเธอ[82]

3.7.3 วิธีการเพื่อความปลอดภัย กรณีที่ศาลสั่งคุมประพฤติ ผู้ที่ถูกตัดสินว่ามีความผิดฐานคุกคาม ศาลจะกำหนดเงื่อนไขการคุมประพฤติให้ผู้นั้นปฏิบัติตาม[83] เช่นในกฎหมายของ มลรัฐแคลิฟอร์เนียมาตรา 646.9 (j) “ถ้าให้มีการคุมประพฤติ หรือการบังคับโทษจำคุกหรือการกำหนดโทษให้รอไว้ สำหรับผู้ที่ถูกตัดสินว่ามีความผิดภายใต้มาตรานี้ควรจะมีเงื่อนไขในการคุมประพฤติที่ให้ผู้นั้นเข้าไปร่วมรับคำปรึกษาตามที่ศาลได้กำหนดให้

---

[81] เรื่องเดียวกัน, หน้า 45.

[82] California Penal Code S.646.9 (k) “The sentencing court also shall consider issuing an order restraining the defendant from any contact with the victim , that may be valid for up to 10 years, as determined by the court. It is the intent of the Legislature that the length of any restraining order be based on the seriousness of the facts before the court, the probability of future violations, and the safety of the victim and his or her immediate family.”

[83] วิจิตรา เลิศหิรัญกิจ, ความผิดฐานเฝ้าติดตามและข่มขู่ Stalking ,หน้า 47.

อย่างไรก็ตามขึ้นอยู่กับเหตุที่เหมาะสมศาลอาจจะเห็นว่าไม่ควรกำหนดให้มีความจำเป็นต้องให้คำปรึกษา[84]

กฎหมายของมลรัฐมิชิแกนมาตรา 750.411 h (3) บัญญัติว่า "ศาลอาจจะให้บุคคลที่ถูกตัดสินว่ากระทำความผิดฝ่าฝืนมาตรานี้คุมประพฤติเป็นระยะเวลาไม่เกินห้าปี ถ้ามีการสั่ งให้คุมประพฤติ ศาลอาจจะเพิ่มเงื่อนไขการคุมประพฤติอื่น ๆ ที่ชอบด้วยกฎหมาย และสั่งให้จำเลยทำตามดังต่อไปนี้

(a) หยุดหรือเลิกคุกคามบุคคลในช่วงระยะเวลาของการคุมประพฤติ

(b) หยุดหรือเลิกติดต่อกับเหยื่อของการกระทำความผิด

(c) นำไปประเมินเพื่อตัดสินว่ามีความจำเป็นต้องรักษาทา งจิต การรับคำปรึกษาทางจิตหรือทางสังคม ถ้าศาลได้ตัดสินแล้วว่าเหมาะสม ก็ให้เขาได้รับการรักษาทางจิต รับคำปรึกษาทางจิตหรือสังคม โดยให้เขาเสียค่าใช้จ่ายเอง"[85]

3.7.4 การประเมินสภาพทางจิตของจำเลย ในบางมลรัฐนั้นกฎหมายได้กำหนดให้ศาลควรทำการประเมินสภาพจิตใจของจำเลยก่อน เพื่อจะได้เป็นประโยชน์แก่ตัวจำเลย

กฎหมายของมลรัฐแคลิฟอร์เนียมาตรา 646.9 (m) บัญญัติว่า "ศาลควรพิจารณาถึงว่าจำเลยจะได้รับประโยชน์จากการบำบัดรักษาตามมาตรา 2684 ถ้าพิจารณาแล้วว่ามีความเหมาะสมศาลควรต้องเสนอแนะกรมราชทัณฑ์ให้ทำหนังสือรับรองต ามที่ได้บัญญัติไว้

---

[84] California Penal Code S.646.9 (j) "if probation is granted , or the execution or imposition of sentence is suspended, for any person convicted of this section , it shall be condition of probation that the person participate in counseling , as designated by the court. However , the court , upon a showing of good cause , may find that the counseling requirement shall not be imposed."

[85] Michigan 750.411h (3) "The court may place an individual convicted of violating this section on probation for a term of not more than 5 years. If a term of probation is order , the court may , in addition to any other lawful condition of probation , order the defendant to do any of the following ; (a) Refrain from stalking any individual during the term of probation.

(b) Refrain from having any contact with the victim of offense.

(c) Be evaluated to determine the need for psychiatric , psychological , or social counseling and if , determined appropriate by court , to receive psychiatric , psychological , or social counseling at his or her owm expense."

ในมาตรา 2684 ตามหนังสือรับรองจำเลยควรต้องถูกนำมาประเมินและส่งตัวยัง โรงพยาบาลที่เหมาะสมเพื่อบำบัดรักษาตามมาตรา 2684"[86]

จะเห็นได้ว่ากฎหมายของประเทศสหรัฐอเมริกานั้นมีความแตกต่างกันในแต่ละมล รัฐ ไม่ว่าจะเป็นบทลงโทษ หรือรายละเอียดในแต่ละบ ทบัญญัติของกฎหมาย แต่โดยรวม แล้วกฎหมายของประเทศสหรัฐอเมริกาจะมีองค์ประกอบหลักที่คล้าย ๆ กัน คือ กฎหมาย Cyberstalking นั้นจะมีการข่มขู่ ข่มขวัญ หรังควาน และการกระทำนี้เกิดขึ้นซ้ำ ๆ ในช่วงระยะเวลาหนึ่ง และทำให้ผู้ที่ถูกคุกคามหรือเหยื่อนั้นเกิดควา มกลัวว่าจะเป็นอันตราย ต่อชีวิตและทรัพย์สินของตนเองหรือของสมาชิกในครอบครัว

บทลงโทษนั้นมีทั้งโทษจำคุก โทษปรับ หรือทั้งจำทั้งปรับ โดยอัตราโทษ จะ เป็นไปตามที่กฎหมายของแต่ละมลรัฐบัญญัติเอาไว้ บางมลรัฐถือว่าเป็นความผิดฐานเบา สำหรับการกระทำความผิดครั้งแรก บางมล รัฐถือว่าเป็นความผิดร้ายแรง และหากมีการ กระทำความผิดซ้ำโทษที่ได้รับก็จะรุนแรงขึ้น นอกจากโทษจำคุก โทษปรับแล้ว กฎหมาย ประเทศสหรัฐอเมริกายังมีมาตรการทางกฎหมายอื่นเช่น คำสั่งคุ้มครองชั่วคราว คำสั่งงด เว้นกระทำการ หรือการให้ศาลประเมินสภาพจิตใจ ซึ่งมาตรการเหล่ านี้เป็นมาตรการ สำหรับการคุกคามทั่วไป ซึ่งอาจนำมาปรับใช้ได้กับผู้กระทำความผิดฐาน Cyberstalking ด้วยเช่นกัน โดยมีจุดประสงค์เดียวกันคือการคุ้มครองเหยื่อจากความรุนแรงที่อาจจะเกิดขึ้น

3.8 กฎหมายไทยที่นำมาใช้กับการคุกคามทางอินเตอร์เน็ต

ปัญหาการคุกคามทางอิ นเตอร์เน็ต (Cyberstalking) นั้นเป็นรูปแบบการคุกคาม แนวใหม่ที่อาศัยเทคโนโลยีเป็นเครื่องช่วย พฤติกรรมการคุกคามในรูปแบบเดิมได้ เปลี่ยนแปลงไป เช่น วิธีการรบกวน การทำให้ตื่นตกใจ ทำให้เกิดความกลัวว่าจะเกิด อันตรายต่อร่างกาย ชีวิต และทรัพย์สิน ทำให้ได้รับ ความเดือดร้อนรำคาญ เช่นการส่ง อีเมล์ จำนวนมาก ๆ โดยมีข้อความที่เป็นการข่มขู่ หยาบคาย หรือรูปภาพลามก อนาจาร โดยการกระทำดังกล่าวนั้นเป็นการกระทำซ้ำ ๆ อย่างต่อเนื่องในช่วงระยะเวลา หนึ่ง รวมถึงการลงข้อความหรือรูปภาพบนเว็บบอร์ดสาธารณะที่เป็นการให้ร้ายผู้ ที่เป็น เหยื่อหรือทำให้เหยื่อได้รับความอับอาย ถูกดูหมิ่นเกลียดชัง การคุกคามทาง

---

[86] California Penal Code S.646.9 (m) "The court shall consider whether the defendant would benefit from treatment pursuant to Section 2684. Upon the certification , the defendant shall be evaluated and transferred to the appropriate hospital for treatment pursuant to Section 2684."

อินเตอร์เน็ตหรือ Cyberstalking นั้นจะเป็นพฤติกรรมที่ขยายวงกว้างมากขึ้นและทวีความรุนแรงมากขึ้น หากไม่มีมาตรการทางกฎหมายมาคอยควบคุมหรือกำหนดโทษ เนื่องจากพฤติกรรมแรกนั้นอาจเ ป็นเพียงแค่การสร้างความเดือดร้อนรำคาญ หรือแค่ทำให้ตื่นตกใจเท่านั้น แต่ถ้าพฤติกรรมดังกล่าวยังคงมีอยู่และดำเนินต่อไปโดยไม่มีการหยุดยั้ง พฤติกรรมการคุกคามทางอินเตอร์เน็ตดังกล่าวก็มิได้จำกัดเฉพาะการคุกคามบนโลกของอินเตอร์เน็ตเท่านั้น หากแต่อาจจะเป็นการคุ กคามเหยื่อในโลกแห่งความเป็นจริงด้วยเช่นกัน ซึ่งการคุกคามดังกล่าวอาจเป็นการคุกคามเหยื่อจนเป็นอันตรายต่อร่างกายหรือชีวิตของเหยื่อ หรือร้ายแรงจนกระทั่งถึงการฆาตกรรมเหยื่อในโลกของความเป็นจริง

เมื่อพิจารณาจากพฤติกรรมและลักษณะของการกระทำที่เป็นการคุกคามทางอินเตอร์เน็ตแล้ว กฎหมายของไทยจะสามารถนำมาบังคับใช้กับพฤติกรรมการคุกคามทางอินเตอร์เน็ตได้มากน้อยเพียงใด จึงควรนำมาพิจารณาเพื่อป้องกันเหยื่อและหยุดยั้งพฤติกรรมการคุกคามทางอินเตอร์เน็ตที่จะทวีความรุนแรงมากขึ้นจนกลายเป็นการคุกคามที่เป็นอันตรายต่อร่างกาย ชีวิตและทรัพย์สินของเหยื่อ

บทบัญญัติของกฎหมายที่เกี่ยวข้องกับกรณีปัญหาการคุกคามทางอินเตอร์เน็ต ปัจจุบันประเทศไทยยังไม่มีบทบัญญัติเฉพาะเรื่องปัญหา Cyberstalking หากมีกรณีปัญหาเกิดขึ้นการจะลงโทษผู้กระทำความผิดนั้นสามารถเทียบเคียงกฎหมาย ดังต่อไปนี้

ประมวลกฎหมายอาญา

3.8.1 ประมวลกฎหมายอาญามาตรา 326 บัญญัติไว้ว่า “ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สาม โดยประการที่น่าจะให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ”

(1) องค์ประกอบกายนอกของความผิด[87]

(1.1) ใส่ความ คำว่า “ใส่ความ” นั้น หมายถึงการกล่าวยืนยันข้อเท็จจริงถึงบุคคอื่น จะเท็จหรือจะจริงก็เป็นการใส่ความทั้งนั้น แต่จะเป็นการกล่าวยืนยันข้อเท็จจริงและเป็นการใส่ความได้ จะต้องเป็นเหตุก ารณ์หรือกรณีที่เกิดขึ้นในอดีตหรือปัจจุบัน การใส่ความนี้จะเป็นการกระทำโดยการกล่าวด้วยวาจา ลายลักษณ์อักษรหรือ

[87] หยุด แสงอุทัย,กฎหมายอาญาภาค 2-3 ,พิมพ์ครั้งที่ 8 แก้ไขเพิ่มเติม (กรุงเทพมหานคร: สำนักพิมพ์ธรรมศาสตร์,2540),หน้า 242.

โดยประการอื่น เช่นการเขียนรูปการ์ตูนก็ไม่สำคัญ ข้อสำคัญคือบุคคลอื่นนั้นสามารถทราบความหมายของการใส่ความได้

(1.2) ผู้อื่น หมายความถึงบุคคลโดยเจาะจงตัว แยกพิจารณาดังนี้

(1.2.1) บุคคลธรรมดา ซึ่งหมายความว่าบุคคลคนเดียวหรือหลายคนก็ได้ แต่จะต้องนับตั้งแต่มีสภาพบุคคลตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 15

(1.2.2) นิติบุคคล นิติบุคคลก็อยู่ในความหมายของคำว่า “ผู้อื่น” และการหมิ่นประมาทนิติบุคคลย่อมเป็นความผิดตามมาตรานี้เหมือนหมิ่นประมาทบุคคลธรรมดา

(1.3) การใส่ความจะต้องเป็นการใส่ความต่อบุคคลที่สาม หมายความว่าเป็นการใส่ความต่อบุคคลอื่น ซึ่งบุคคลนั้นมิใช่ตัวผู้ถูกใส่ความเอง บุคคลที่สามนี้จะต้องอยู่ในฐานะที่เข้าใจข้อความที่ใส่ความ

(1.4) โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นหรือถูกเกลียดชัง คำว่า “ชื่อเสียง” หมายความรวมถึงค่าหรือราคาที่มนุษย์มีต่อเพื่อนมนุษย์ด้วยกันในทางศีลธรรม (ในทางจิตใจ) หรือในทางสังคม การทำให้เสียชื่อเสียงหมายความถึงการทำให้ค่าหรือราคาที่มีอยู่หมดไป หรือลดน้อยถอ ยลง เช่นการกล่าวหาว่า นาง ก. เป็นชู้กับสามีคนอื่น มีเพศสัมพันธ์กับชายไม่เลือกหน้า ย่อมทำให้ค่าหรือราคาของนาง ก. ที่มีต่อเพื่อนมนุษย์ในศีลธรรม (ในทางจิตใจ) และในสังคมลดน้อยถอยลงเนื่องจากสังคมไทยไม่นิยมผู้หญิงมีชู้กับสามีผู้อื่น

(2) องค์ประกอบภายในของความผิด[88]

องค์ประกอบภายใน คือ เจตนาธรรมดา บทบัญญัติมาตรานี้นั้นสามารถนำมาปรับใช้กับการคุกคามทางอินเตอร์เน็ตได้ เนื่องจากการคุกคามทางอินเตอร์เน็ตนั้นสามารถกระทำได้โดยการเผยแพร่ข้อความ ลงข้อความอันเป็นเท็จหรือการใส่ความบนเว็บบอร์ดสาธารณะ หรือการลงข้อความ แสดงความคิดเห็นที่รุนแรง หรือข้อความที่เป็นการใส่ความเหยื่อทำให้เหยื่อนั้นถูกเกลียดชังหรือทำให้เหยื่อนั้นได้รับความเสียหาย ความอับอับอาย หรือเดือดร้อนรำคาญ หรืออาจจะรุนแรงถึงขั้นถูกคุกคามต่อชีวิตและทรัพย์สินของเหยื่อ โดยที่เหยื่อนั้นอาจจะรู้ตัวหรือไม่รู้ตัว

3.8.2 ประมวลกฎหมายอาญามาตรา 328 บัญญัติว่า “ถ้าความผิดฐานหมิ่นประมาทได้กระทำโดยการโฆษณาด้วยเอกสาร ภาพวาด ภาพระบายสี ภาพยนตร์ ภาพหรือตัวอักษรที่ทำให้ปรากฏไม่ว่าด้วยวิธีการใด ๆ แผ่นเสียง หรือ สิ่งบันทึกเสียง บันทึกภาพ หรือบันทึกอักษ ร กระทำโดยการกระจายเสียง หรือการกระจายภาพ หรือ

[88] เรื่องเดียวกัน.

โดยกระทำการป่าวประกาศด้วยวิธีอื่น ผู้กระทำต้องระวางโทษจำคุกไม่เกินสองปี และปรับไม่เกินสองแสนบาท”

(1) องค์ประกอบภายนอกของความผิด[89]

(1.1) กระทำความผิดฐานหมิ่นประมาท

(1.2) ได้กระทำโดยการโฆษณา ด้ว ยเอกสาร ภาพวาด ภาพระบายสี ภาพยนตร์ ภาพหรือตัวอักษรที่ทำให้ปรากฏด้วยวิธีใด ๆ แผ่นเสียงหรือสิ่งบันทึกเสียง หรือบันทึกอักษร กระทำโดยการกระจายเสียงหรือกระจายภาพหรือโดยทำการป่าวประกาศด้วยวิธีการอื่น ๆ

คำว่า “ความผิดฐานหมิ่นประมาท ” ในมาตรานี้หมายถึง การกระทำความผิดตามมาตรา 326 และมาตรา 327 เพราะทั้งสองมาตรานี้เรียกชื่อการกระทำว่า “ความผิดฐานหมิ่นประมาท”[90]

ส่วนความหมายของคำว่า “เอกสาร ” นั้นเป็นไปตามประมวลกฎหมายอาญา มาตรา 1(7) คำว่า “โฆษณา” หมายความถึงการกระทำให้แพร่หลาย

การป่าวประกาศ ” หมายความว่า ป่าวประกาศแก่ประชาชน เช่น พูดด้วยลำโพงต่อหน้าคนทั่ว ๆไป

(2) องค์ประกอบภายในของความผิด

องค์ประกอบภายใน คือ เจตนาธรรมดา ความผิดตามมาตรานี้นั้นสามารถนำมาปรับใช้ได้กับการคุกคามทางอินเตอร์เน็ต ซึ่งถือว่าการคุกคามทางอินเตอร์เน็ตนั้นถือว่าเข้าองค์ประ กอบภายนอกของการกระทำความผิดฐานหมิ่นประมาทตามมาตรา 328 เนื่องจากการคุกคามทางอินเตอร์เน็ตโดยวิธีการแพร่ข้อความอันเป็นเท็จหรือการลงข้อความหรือรูปภาพใด ๆ อันเป็นการให้เหยื่อนั้นได้รับความเสียหาย ได้รับความเดือดร้อนรำคาญ หรือได้รับความอับอาย ถูกดูหมิ่นห รือเกลียดชังตามความผิดฐานหมิ่นประมาทตามมาตรา 326 แล้ว ผู้คุกคามทางอินเตอร์เน็ตอาจได้รับโทษหนักขึ้นตามมาตรา 328 เนื่องจากถือว่าผู้คุกคามนั้นได้กระทำโดยการวิธีที่จะแพร่หลายไปยังคนจำนวนมาก การคุกคามทางอินเตอร์เน็ตนั้นแม้กระทำเพียงครั้งเดียวแต่สามารถเผย แพร่และแพร่หลายไปยังบุคคลทั่ว ๆไปที่สามารถเข้าถึงข้อมูลจากอินเตอร์เน็ตได้

---

[89] เรื่องเดียวกัน, หน้า 248.

[90] เรื่องเดียวกัน.

3.8.3 ประมวลกฎหมายอาญามาตรา 392 บัญญัติว่า “ผู้ใดทำให้ผู้อื่นเกิดความกลัวหรือความตกใจโดยการขู่เข็ญต้องระวางโทษจำคุกไม่เกินหนึ่งเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ”

(1) องค์ประกอบภายนอกของความผิด

(1.1) ทำให้เกิดความกลัวหรือความตกใจ

(1.2) โดยการขู่เข็ญ ขู่เข็ญ คือแสดงว่าจะทำให้เกิดภัยแก่เขา จะเป็นภัยที่เกิดขึ้นในทันทีต่อไปหรือต่อไปภายหน้าก็ได้ อาจทำโดยกิริยา วาจาโดยตรง หรือโดยเข้าใจเช่นนั้น ซึ่งต้องทำให้ผู้ถูกขู่ทราบถึงการขู่ว่าจะทำร้ายนั้น[91]

(1.3) การกระทำความผิดตามมาตรานี้ต้องเกิดผล คือ กลัวหรือตกใจ แต่ต้องไม่เกิดผลต่อไปถึงให้ทำอะไรดังมาตรา 309 ถ้าขู่แล้วไม่กลัวไม่ตกใจก็ไม่ลงโทษฐานพยายาม เพราะยกเว้นตามมาตรา 105 โดยผู้เสียหายกลัวหรือไม่ดูที่ พฤติการณ์ แม้จะบอกว่าไม่กลัวก็ตาม และการขู่เข็ญนั้นแม้จะไม่สามารถทำร้ายได้จริง ถ้าเกิดผลคือ ผู้ถูกขู่กลัวก็เป็นความผิด[92]

(2) องค์ประกอบภายในของความผิด

องค์ประกอบภายในคือ เจตนาธรรมดา มาตรานี้จำต้องมีเจตนา และหมายถึง ทำให้เกิดความกลัวเฉย ๆ ไม่ได้ บังคับให้ทำ ให้งดเว้นกระทำหรือให้จำยอมต่อสิ่งใด ซึ่งจะเป็นความผิดตามมาตรา 309 เช่น ขู่เข็ญว่าจะฆ่าเขาเสียให้ตายเพราะเกลียดเขา เพียงที่ขู่เข็ญก็เป็นความผิดตามมาตรานี้แล้ว[93]

บทบัญญัติในมาตรานี้สามารถนำมาปรับใช้ได้กับพฤติกรรมการคุกคามทางอินเตอร์เน็ ต เนื่องจากผู้กระทำนั้นไม่จำเป็นต้องมีการข่มขืนใจให้ผู้ถูกคุกคามนั้นกระทำการ ไม่กระทำการ หรือจำยอมต่อสิ่งใดเนื่องจากการคุกคามทางอินเตอร์เน็ตนั้นเหยื่ออาจได้รับการข่มขู่เพียงอย่างเดียวจนทำให้เกิดความกลัว เช่นการส่ง อีเมล์มาให้กับเหยื่อโดยมีข้อความขู่ว่ าจะทำร้ายร่างกาย หรือส่งข้อความว่าจะทำร้ายคนใกล้ชิดหรือคนในครอบครัว หรือข้อความใด ๆ ตลอดจนรูปภาพต่าง ๆ ที่อาจก่อให้เกิดความกลัวต่อเหยื่อ ซึ่งมีการส่ง อีเมล์มาเพื่อคุกคามเหยื่อหลาย ๆ ครั้งนั้นไม่จำต้องให้เหยื่อกระทำการหรือไม่กระทำการ หรือจำยอมต่อสิ่งใ ด เพียงแค่การส่งข้อความผ่านทาง อีเมล์ให้กับเหยื่อ

---

[91] จิตติ ติงศภัทิย์,กฎหมายอาญา ภาค2 ตอน2 และภาค3,พิมพ์ครั้งที่ 6 (กรุงเทพมหานคร: จิรรัชการพิมพ์,2545),หน้า 1234.

[92] วิจิตรา เลิศหิรัญกิจ, ความผิดฐานเฝ้าติดตามและข่มขู่ Stalking ,หน้า 60.

[93] หยุด แสงอุทัย,กฎหมายอาญาภาค 2-3 ,พิมพ์ครั้งที่ 8 แก้ไขเพิ่มเติม,หน้า 378.

จนกระทั่งเหยื่อนั้นเกิดความกลัวก็ถือได้ว่ากระทำความผิดตามมาตราดังกล่าว

นอกจากนี้บทบัญญัติตามมาตรา 392 ก็สามารถนำมาปรับใช้กับการคุกคามผ่านทางห้องสนทนาสดหรือ Chat Room รวมถึงการคุกคามผ่านการสื่อสารในระบบโ ปรแกรมเมสเซนเจอร์ของไมโครซอฟท์หรือที่เรียกกันว่า "เอ็มเอสเอ็น"[94] (MSN) หรือ "เอ็ม" ได้เช่นเดียวกัน เนื่องจากการคุกคามประเภทนี้เป็นลักษณะของการคุกคามโดยการติดต่อกับเหยื่อโดยตรงโดยการส่งข้อความโต้ตอบทันที (Instant Messaging) ซึ่งอาจจะเป็นข้อความที่เป็นการข่มขู่ หรือหยาบคาย หรือรูปภาพที่มีลักษณะลามกอนาจารส่งให้กับผู้รับซึ่งเป็นเหยื่อเพื่อให้เหยื่อนั้นเกิดความเครียดเกิดความหวาดกลัว ตื่นตกใจ ลักษณะการคุกคามทางห้องสนทนาสดคล้ายกับการคุกคามทางผ่านทาง อีเมล์ที่จำกัดอยู่เฉพาะตัวเหยื่อแต่แตกต่างกันตรงที่การคุกคามทางห้องสนทนาสดหรือการคุกคามทางระบบโปรแกรมเอ็มเอสเอ็นนั้นเป็นการคุกคามในเวลาที่ได้มีการสนทนากันหรือโดยทันทีในเวลานั้น ๆ

บทบัญญัติในมาตราดังกล่าวนี้เป็นการกระทำที่ไม่จำเป็นต้องมีองค์ประกอบในเรื่องของระยะเวลาเข้ามาเกี่ยวข้อง [95] การกระทำตามที่กฎหมายบัญ ญัติไว้ตามมาตรา 392 เพียงครั้งเดียวก็มีความผิดและไม่จำเป็นต้องกระทำซ้ำ ๆ อย่างต่อเนื่อง คือเป็นความผิดฐานเฉพาะ แม้มีการกระทำผิดและเป็นการกระทำที่ซ้ำ ๆ ก็ไม่มีบทบัญญัติให้รับโทษหนักขึ้น นอกจากนี้หากการกระทำความผิดไม่ครบองค์ประกอบตามที่กฎหมายบัญญัติไว้ ก็ไม่สามารถลงโทษผู้กระทำความผิดได้ แต่กฎหมายCyberstalking ของประเทศสหรัฐอเมริกาเช่นมลรัฐอิลลินอยส์นั้นมีองค์ประกอบในเรื่องของระยะเวลาเข้ามาเกี่ยวข้อง คือต้องมีการกระทำอย่างน้อย 2 ครั้ง

3.8.4 การพยายามกระทำความผิด

ตามประมวลกฎหมายอาญาความผิดฐานหมิ่นประมาทตา มมาตรา 326 และมาตรา 328 นี้ไม่มีการพยายามกระทำความผิด และการกระทำความผิดตามมาตรา 392 นั้นเป็นการกระทำความความผิดลหุโทษ ซึ่งบทบัญญัติที่ใช้แก่ความผิดลหุโทษมาตรา 105 บัญญัติว่า "ผู้ใดพยายามกระทำความผิดลหุโทษ ผู้นั้นไม่ต้องรับโทษ " ดังนั้นจึงไม่มีการพิจารณาเรื่องของการพยายามกระทำความผิด

เนื่องจากพฤติกรรมการคุกคามทางอินเตอร์เน็ตนั้นเป็นพฤติกรรมที่เกิดขึ้นอย่างต่อเนื่องซ้ำ ๆ กันในช่วงระยะเวลาหนึ่ง หากการลงโทษผู้กระทำความผิดนั้นไม่สามารถหยุดหรือยับยั้งตัวผู้กระทำความผิดได้ ผู้กระทำนั้นอาจจะไ ม่หลาบจำยังคงมีพฤติกรรม

---

[94] Wikipedia , the free encyclopedia "MSN" internet. http//wikipedia.org.wiki.msn.

[95] วิจิตรา เลิศหิรัญกิจ, ความผิดฐานเฝ้าติดตามและข่มขู่ Stalking ,หน้า 60.

คุกคามทางอินเตอร์เน็ตแก่เหยื่ออีก จึงมีบทบัญญัติประมวลกฎหมายอาญามาตรา 92 และมาตรา 93 ที่สามารถนำมาใช้เพื่อเพิ่มโทษแก่ผู้กระทำความผิดซ้ำ

3.8.5 ประมวลกฎหมายอาญามาตรา 92 บัญญัติว่า "ผู้ใดต้องคำพิพากษาถึงที่สุดให้ลงโทษจำคุ ก ถ้าและได้กระทำความผิดซ้ำอีก ในระหว่างที่ยังจะต้องรับโทษอยู่ก็ดี ภายในเวลาห้าปีนับแต่วันพ้นโทษก็ดี หากศาลจะพิพากษาลงโทษครั้งหลังถึงจำคุก ก็ให้เพิ่มโทษที่จะลงแก่ผู้นั้นหนึ่งในสามของโทษที่ศาลกำหนดสำหรับความผิดครั้งหลัง"

กรณีที่ผู้ต้องคำพิพากษาถึงที่สุดใ ห้ลงโทษจำคุก ได้กระทำความผิดฐานใดฐานหนึ่งอีก ในระหว่างที่ต้องรับโทษอยู่ก็ดี หรือภายในเวลาห้าปีนับแต่วันพ้นโทษก็ดี ถ้าในคดีหลังลงโทษถึงจำคุก ให้ศาลเพิ่มโทษหนึ่งในสาม โดยคำนวณจากโทษที่จะลงในความผิดครั้งหลัง มิใช่โทษที่กำหนดไว้ในกฎหมาย ดังนี้ ถ้าจำเล ยเคยถูกศาลพิพากษาลงโทษจำคุกแต่ให้รอการลงโทษไว้ เมื่อไม่มีการถูกจำคุก ย่อมไม่มีวันที่จำเลยพ้นโทษที่จะนับเวลาห้าปี นับแต่วันพ้นโทษเพื่อเ ป็นเหตุเพิ่มโทษในคดีหลัง ตามมาตรา 92 ได้ และแม้จำเลยจะกระทำผิดภายในห้าปีนับแต่วันพ้นกำหนดการลงโทษก็ตามจึงเพิ่มโทษจำเ ลยไม่ได้[96]

มาตรา 92 กำหนดว่าต้องมีคำพิพากษาถึงที่สุดให้จำคุก แต่ส่วนมากผู้กระทำความผิดฐานหมิ่นประมาทนั้น หากกระทำความผิดครั้งแรกหรือไม่เคยกระทำความผิดใด ๆ มาก่อนศาลมักจะรอการลงโทษสำหรับโทษจำคุกและลงโทษปรับ และมาตรา 92 นี้ก็ไม่สามารถนำมาใช้ลงโทษผู้กระ ทำความผิดที่ศาลลงโทษปรับเพียงอย่างเดียว ซึ่งกรณีของความผิดลหุโทษตามมาตรา 392 ซึ่งมีโทษจำคุกไม่เกินหนึ่งเดือนหรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ ส่วนใหญ่แล้วศาลมักจะปรับเพียงอย่างเดียวเนื่องจากเห็นว่าเป็นความผิดเล็กน้อยเท่านั้น

3.8.6 ประมวลกฎหมายอาญามาตรา 93 บัญญัติว่า " ผู้ใดต้องคำพิพากษาถึงที่สุดให้ลงโทษจำคุก ถ้าและได้กระทำผิดอย่างหนึ่งอย่างใดที่จำแนกไว้ในอนุมาตราต่อไปนี้ ซ้ำในอนุมาตราเดียวกันอีกในระหว่างที่ยังจะต้องรับโทษอยู่ก็ดี ภายในเวลาสามปีนับแต่วันพ้นโทษก็ดี ถ้าความผิดครั้งแรกเป็นความผิดซึ่งศาลพิพากษาลงโทษจำคุกไม่น้อยกว่าหกเดือน หากศาลจะพิพากษาลงโทษครั้งหลังถึงจำคุก ก็ให้เพิ่มโทษที่จะลงแก่ผู้นั้นกึ่งหนึ่งของโทษที่ศาลกำหนดสำหรับความผิดครั้งหลัง

(1) ความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร ตามที่ได้บัญญัติไว้ในมาตรา

---

[96] ทวีเกียรติ มีนะกนิษฐ์, หลักกฎหมายอาญาภาคทั่วไป,พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม (กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2546),หน้า 114.

107 ถึงมาตรา 137

(2) ความผิดต่อเจ้าพนักงานตามที่บัญญัติไว้ในมาตรา 136 ถึงมาตรา 146

(3) ความผิดต่อตำแหน่งหน้าที่ราชการ ตามที่ได้บัญญัติไว้ในมาตรา 147 ถึงมาตรา 166

(4) ความผิดต่อเจ้าพนักงานในการยุติธรรม ตามที่ได้บัญญัติในมาตรา 167 ถึงมาตรา 192 และมาตรา 194

(5) ความผิดต่อตำแหน่งหน้าที่ในการยุติธรรม ตามที่ได้บัญญัติไว้ในมาตรา 200 ถึงมาตรา 204

(6) ความผิดเกี่ยวกับความสงบสุขของประชาชน ตามที่ได้บัญญัติไว้ในมาตรา 209 ถึง มาตรา 216

(7) ความผิดเกี่ยวกับการก่อให้เกิดภัยอันตรายต่อประชาชนตามที่บัญญัติไว้ในมาตรา 217 ถึงมาตรา 224 มาตรา 226 ถึงมาตรา 234 และมาตรา 236 ถึงมาตรา 238

(8) ความผิดเกี่ยวกับเงินตรา ตามที่บัญญัติไว้ในมาตรา 240 ถึงมาตรา 249 ความผิดเกี่ยวกับดวงตราแสตมป์และตั๋วตามที่บัญญัติไว้ในมาตรา 250 ถึงมาตรา 261 และความผิดเกี่ยวกับเอกสาร ตามที่บัญญัติไว้ในมาตรา 264 ถึงมาตรา 269

(9) ความผิดเกี่ยวกับการค้า ตามที่บัญญัติไว้ในมาตรา 270 ถึงมาตรา 275

(10) ความผิดเกี่ยวกับเพศ ตามที่บัญญัติไว้ในมาตรา 276 ถึงมาตรา 285

(11) ความผิดต่อชีวิต ตามที่บัญญัติไว้ในมาตรา 288 ถึงมาตรา 290 และมาตรา 294 ความผิดต่อร่างกาย ตามที่บัญญัติไว้ในมาตรา 295 ถึงมาตรา 299 ความผิดฐานทำให้แท้งลูกตามที่บัญญัติไว้ในมาตรา 301 ถึงมาตรา 303 และความผิดฐานทอดทิ้งเด็กคนป่วยเจ็บหรือคนชรา ตามที่บัญญัติไว้ในมาตรา 306 ถึงมาตรา 308

(12) ความผิดต่อเสรีภาพ ตามที่บั ญญัติไว้ในมาตรา 309 มาตรา 310 และมาตรา 312 ถึงมาตรา 320

(13) ความผิดเกี่ยวกับทรัพย์ ตามที่บัญญัติไว้ในมาตรา 334 ถึงมาตรา 365

กรณีของมาตรา 93 คือ กรณีที่ผู้กระทำความผิด ต้องคำพิพากษาถึงที่สุดให้ลงโทษจำคุกไม่น้อยกว่าหกเดือน และได้กระทำความผิ ดอย่างหนึ่งอย่างใดทั้งในอนุมาตราเดียวกันอีกในระหว่างที่ยังต้องรับโทษอยู่ หรือภายในเวลาสามปีนับแต่วันพ้นโทษและในคดีหลังศาลพิจารณาลงโทษถึงจำคุก

เหตุเพิ่มโทษนี้เป็นการเพิ่มโทษเฉพาะในบางความผิดที่ระบุไว้ในอนุมาตราเดียวกันเท่านั้นดังที่กล่าวข้างต้น

การใช้ม าตรา 93 เพื่อเพิ่มโทษแก่ผู้กระทำความผิดนั้นต้องเป็นไปตามหลักเกณฑ์ตามที่มาตรานี้กำหนดไว้ ถ้าไม่เป็นไปตามหลักเกณฑ์ดังกล่าวก็ไม่สามารถเพิ่มโทษแก่ผู้กระทำความผิดซ้ำได้ ดังนั้น Cyberstalking เมื่อไม่เป็นความผิดตามมาตรา 93 (1) ถึง (13) เมื่อผู้กระทำ ความผิดกระทำความซ้ำขึ้นมาอีกก็ไม่สามารถเพิ่มโทษที่จะลงแก่ผู้กระทำความผิดซ้ำนั้นได้ เช่น ผู้ที่มีพฤติกรรม Cyberstalking และได้รับโทษตามมาตรา 392 ซึ่งโทษตามมาตรา 392 ไม่เป็นความผิดที่กำหนดเอาไว้ในมาตรา 93 (1) ถึง (13) ถ้าผู้นั้นได้กระทำความผิดซ้ำ ขึ้นมาอีกก็ไม่สามารถเพิ่มโทษสำหรับการกระทำความผิดในครั้งหลังได้

3.9 โทษตามบทบัญญัติในกฎหมายอาญา

ตามประมวลกฎหมายอาญามาตรา 326 มาตรา 328 และมาตรา 392 โทษที่จะนำมาลงกับผู้กระทำความผิด คือ โทษจำคุกและโทษปรับ โดยอัตราโทษนั้นแตกต่างกัน คือ จำคุกไม่เกินสองปี ปรับไม่เกินสองแสนบาท หรือทั้งจำทั้งปรับ สำหรับความผิดฐานหมิ่นประมาทที่ได้กระทำด้วยการโฆษณาหรือวิธีอื่นใดตามมาตรา 328 และจำคุกไม่เกินหนึ่งเดือน ปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ เมื่อพิจารณาบทบัญญัติโทษที่จะลงแก่ผู้คุกคาม ทางอินเตอร์เน็ตซึ่งเข้าข่ายลักษณะของการหมิ่นประมาทเหยื่อแล้วจะได้รับโทษจำคุก และโทษปรับมากกว่า ซึ่งมาตรา 392 นั้นเป็นเพียงแค่ลหุโทษ ซึ่งมีโทษไม่รุนแรงพอที่จะยับยั้งพฤติกรรมของผู้คุกคามได้และส่วนมากโทษที่จะลงนั้นเป็นแค่เพียงโทษปรับเท่านั้น ซึ่งโทษปรั บนั้นก็เป็นเพียงแค่โทษปรับที่มีจำนวนน้อ ย ผู้กระทำความผิดก็จะไม่เกรงกลัว

3.10 พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550[97]

มาตรา 14 บัญญัติไว้ว่า “ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

---

[97] โปรดดูภาคผนวก.

1. องค์ประกอบภายนอกของมาตรา 14 (1)

1.1 นำข้อมูลคอมพิวเตอร์เข้าสู่ระบบคอมพิวเตอร์

“ข้อมูลคอมพิวเตอร์ ” ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ .ศ. 2550 มาตรา 3 ให้ความหมายว่า “ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือ สิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย”

1.2 ข้อมูลคอมพิวเตอร์นั้นเป็นข้อมูลปลอมไม่ว่าทั้งหมดหรือบางส่วน

1.3 โดยประการที่น่าจะเกิดความเสียหาย

2. องค์ประกอบภายในของความผิด

องค์ประกอบภายใน คือ เจตนาธรรมดา ความผิดตามมาตรา 14 (1) นี้เป็นการกระทำความผิดในรูปแบบของการนำข้อความอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ มีการบิดเบือนข้อมูล หรือมีการเผยแพร่ข้อมูลอันเป็นเท็จเพื่อกระทำการคุกคามเหยื่อหรือทำให้เหยื่อนั้นได้รับความหวาดกลัวต่ออันตรายที่อาจจะเกิดขึ้นต่อชีวิตและทรัพ ย์สินของตนเอง เช่นการส่งอีเมล์แจ้งเหยื่อว่ามีการตายของบุคคลในครอบครัว หรือมีการลงข้อความอันป็นเท็จเกี่ยวกับตัวเหยื่อทำให้เหยื่อได้รับความเสียหาย

มาตรา 14 บัญญัติไว้ว่า “ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลใด ๆ ที่มีลักษณะ อันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

1. องค์ประกอบภายนอกของมาตรา 14 (4)

1.1 นำข้อมูลคอมพิวเตอร์เข้าสู่ระบบคอมพิวเตอร์

1.2 เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์

1.3 ข้อมูลนั้นมีลักษณะลามกและประชาชนทั่วไปนั้นสามารถเข้าถึงได้

2. องค์ประกอบภายในของความผิด

องค์ประกอบภายใน คือ เจตนาธรรมดา ความผิดตามมาตรา 14 (4) แห่งพระราชบัญญัติฉบับดังกล่าวนั้นสามารถนำมาใช้ลงโทษ ได้หากเกิด การคุกคามทางอินเตอร์เน็ตในลักษณะของการคุกคามโดยวิธีของ การเผยแพร่รูปที่มีลักษณะลามกอนาจารหรือภาพที่ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน โดย ภาพลามก

อนาจารเหล่านี้ผู้คุกคามได้ส่งให้กับเหยื่อ หรือผู้คุกคามอาจนำภาพลามกอนาจารต่าง ๆ ไปลง (Post) บนเว็บบอร์ดสาธารณะ และผู้คุกคามอาจลวงให้ประชาชนทั่วไปเข้าใจว่าผู้ที่นำภาพลามกอนาจาร ไปลงบนเว็บบอร์ดหรือเว็บไซต์ต่าง ๆ นั้นเป็นฝีมือของเหยื่อ ซึ่งแท้จริงแล้วการกระทำดังกล่าวเป็นฝีมือของผู้คุกคาม ๆ อาจจะลงภาพลามกอนาจารบนเว็บไซต์ต่าง ๆ และใ ห้ข้อมูลส่วนตัวต่าง ๆ ของเหยื่อ เอาไว้ เช่น ชื่อ ที่อยู่ หรือเบอร์โทรศัพท์ ทำให้เหยื่อได้รับความเสียหาย ซึ่งอัตราโทษจำคุกในความผิดมาตราดังกล่าวนี้มีอัตราโทษสูงสุด คือ ห้าปี เป็นอัตราโทษที่สูงกว่าความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา มาตรา 328 ซึ่งมีอัตราโทษจำคุกไม่เกินสองปี หากนำความผิดตามพระราชบัญญัติดังกล่าวมาใช้อาจจะได้ผลในการลงโทษผู้กระทำความผิดฐาน Cyberstalking มากกว่าประมวลกฎหมายอาญามาตรา 328

มาตรา 16 บัญญัติว่า “ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่ น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรั บไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ .....”

1. องค์ประกอบภายนอก

1.1 นำเข้าข้อมูลภาพของผู้อื่นสู่ระบบคอมพิวเตอร์ซึ่งประชาชนทั่วไปอาจเข้าถึงได้

1.2 สร้าง ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด

2. องค์ประกอบภายใน

องค์ประกอบภายใน คือ เจตนาธรรมดา ความผิดตามมาตรานี้นั้นเป็นบทลงโทษผู้คุกคามเหยื่อ โดยวิธีการตัดต่อรูปภาพของผู้เสียหาย หรือเหยื่อเข้าลักษณะของลามกอนาจาร หรือขัดต่อความสงบหรือศีลธรรมอันดีของประชาชนและนำภาพดังกล่าวของเหยื่อนั้นไปเผยแพร่บนอินเตอร์เน็ต ทำให้เห ยื่อได้รับความเสียหายหรือการส่งต่อภาพดังกล่าวต่อ ๆ กัน ก็ถือว่ามีความผิดตามมาตราดังกล่าวของร่างพระราชบัญญัติ ฉบับนี้ ตัวอย่างที่เกิดขึ้นในประเทศสหรัฐอเมริกา ผู้หญิงคนหนึ่งถูกคุกคามจากแฟนเก่าเป็นเวลาหลายปีโดยแฟนเก่าของเธอจะคอยติดตามเว็บไซต์สนทนาที่เธอเล่ นอยู่เรื่อย ๆ และในระหว่างนั้นก็จะลง (Post)ข้อมูลที่เป็นการให้ร้ายเธอเสมอ ๆ จนในที่สุดได้นำภาพเธอตัดต่อ

เข้ากับภาพลามกต่าง ๆ และนำไปลง (Post)ตามเว็บไซต์และกรณีหญิงสาวคนหนึ่งถูกคุกคามเป็นเวลาหกเดือน โดยเริ่มจากการลง (Post) ข้อความข่มขู่ว่าจะฆ่าเธอและข่มขืนเธอจนท้ายที่สุดก็นำภาพตัดต่อของเธอไปลงตามอินเตอร์เน็ต[98] หากการกระทำในลักษณะดังกล่าวเกิดขึ้นในประเทศไทย มาตรา 16 ของพระราชบัญญัติฉบับนี้ สามารถนำมาลงโทษผู้กระทำความผิดได้ ซึ่งอัตราโทษของมาตรานี้มีโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาทหรือทั้ง จำทั้งปรับ หากเกิดการกระทำความผิดในลักษณะดังกล่าวบทลงโทษตาม พระราชบัญญัติ นี้สามารถ จะลงโทษผู้กระทำความผิดได้มากกว่าและมีประสิทธิภาพมากกว่าเนื่องจาก มีลักษณะของการกระทำตามที่กฎหมายฉบับดังกล่าวถือว่าเป็นความผิดและมีอัตราโทษสูงกว่าประมวลกฎหมายอาญามาตรา 328

3.11 ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ .ศ. ...(ฉบับสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ)[99]

มาตรา 48 บัญญัติไว้ว่า “ผู้ใดกระทำการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิชอบด้วยกฎหมาย หรือให้ผู้อื่นเสียหาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามความในวรรคหนึ่งเป็นการเผยแพร่ข้อมูลโดยเฉพาะเจาะจงหรือโดยเปิดเผยซึ่งข้อมูลดังกล่าว ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

1. องค์ประกอบภายนอก

1.1 กระทำการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคล

1.2 เผยแพร่ข้อมูลโดยเฉพาะเจาะจงหรือโดยเปิดเผยซึ่งข้อมูล

2. องค์ประกอบภายใน คือเจตนาพิเศษ เพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิชอบด้วยกฎหมาย หรือให้ผู้อื่นเสียหาย ความผิดตาม มาตรา นี้หากผู้คุกคามนำข้อมูลส่วนบุคคลของเหยื่อไปใช้หรือกระทำการใด ๆ อันทำให้เหยื่อเสียหาย ถือว่ามีความผิดตามมาตรานี้ และจะต้องได้รับโทษหนักขึ้นหากทำการเผยแพร่ข้อมูลโดยเฉพาะเจาะจงของเหยื่อ เช่น ที่อยู่ เบอร์โทรศัพท์ หมายเลขประกันสังคม หมายเลขประจำตัวประชาชน ที่ทำงาน ตำแหน่งหน้าที่การงาน

---

[98] Emma Ogilvie, Trends & Issues in crime and criminal justice. Australian Institue of Criminalogy, September 2000 ,No.166. Internet. http://www.aic.gov.au.

[99] โปรดดูภาคผนวก.

3.12 โทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ .ศ. 2550 และร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ .ศ.....(ฉบับสำนักงานคณะกรรมข้อมูลข่าวสารของราชการ)

โทษตามพระราชบัญญัติว่าด้วยก ารกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นเมื่อเปรียบเทียบกับโทษตามประมวลกฎหมายอาญาแล้ว หาก Cyberstalking ปรากฏในรูปแบบของการคุกคามที่มีลักษณะของการเผยแพร่บนอินเตอร์เน็ตแล้วโทษตามพระราชบัญญัติฉบับดังกล่าวจะมีอัตราโทษที่มากกว่ากฎหมายอาญาความผิดฐานหมิ่นประมาท มาตรา 328 อัตราโทษสูงสุดไม่เกินสองปี โทษปรับสำหรับพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ.2550 จะน้อยกว่าคือปรับตั้งแต่ หกหมื่นถึงหนึ่งแสนบาท ส่วนกฎหมายอาญามาตรา 328 ปรับไม่เกินสองแสนบาท ถึงแม้ว่าอัตราโทษปรับของกฎหมายอาญาจะมากกว่าแต่ ลักษณะการกระทำความผิดนั้นหากผู้กระทำความผิดนั้นถูกลงโทษแค่ปรับซึ่งอาจจะถูกปรับน้อยหรืออาจจะถูกปรับมากก็ไม่สามารถทำให้ผู้กระทำความผิดนั้นหลาบจำได้เท่ากับโทษจำคุก

ส่วนโทษตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ .ศ..... โทษตามร่างพระราชบัญญัติดังกล่ าวนั้นสามารถลงโทษครอบคลุมทั้งผู้ที่มีหน้าที่ดูแลควบคุมข้อมูลส่วนบุคคล รวมทั้งผู้ที่นำข้อมูลไปแสวงหาประโยชน์ส่วนตน หรือเพื่อให้ผู้อื่นได้รับผลประโยชน์ เมื่อพิจารณาอัตราโทษจำคุกและโทษปรับแล้วถือว่าเป็นบทลงโทษที่อาจจะยับยั้งการกระทำความผิดหรือลงโทษผู้ก ระทำความผิดได้พอสมควร คืออัตราโทษขั้นต่ำจำคุกไม่เกินสามปี ปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

นอกจากนี้ร่างพระราชบัญญัติดังกล่าวยังได้กล่าวถึงความรับผิดทางแพ่งสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ครอบครองหรือควบคุมดูแลข้อมูลส่วนบุคคลเอาไว้ด้วย คือ

มาตรา 47 “ผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ครอบครองหรือควบคุมดูแล ข้อมูลส่วนบุคคลใดกระทำการเกี่ยวกับข้อมูลส่วนบุคคลอันก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือแก่บุคคลอื่นที่เกี่ยวข้องต้ องชดใช้ค่าสินไหมทดแทนเพื่อการนั้น ไม่ว่าจะเป็นการกระทำโดยจง ใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่จะพิสูจน์ได้ว่าการกระทำนั้นเกิดจากเหตุสุดวิสัย เป็นการกระทำตามกฎหมายหรือตามคำสั่งของเจ้าหน้าที่ปฏิบัติตามอำนาจหน้าที่ตามกฎหมาย หรือ เกิดเพราะการกระทำหรือละเว้นการกระทำของบุคคลที่เกี่ยวข้องหรือเจ้าของข้อมูลส่วนบุคคล

ค่าสินไหมทดแทนตามความในวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายที่เจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นที่เกี่ยวข้องแล้วแต่กรณีได้จ่ายไปตามความจำเป็นแก่การป้องกันความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นด้วย”

ซึ่งมาตราดังกล่าวนั้นไม่ได้ทำให้ความรับผิดของผู้ ประมวลข้อมูลส่วนบุคคล ผู้ครอบครองหรือควบคุมดูแลข้อมูลส่วนบุคคล นั้นหลุดพ้นไปด้วย ต้องดำเนินการชดใช้ค่าสินไหมทดแทนเว้นแต่จะพิสูจน์ได้ว่าการกระทำนั้นเกิดจากเหตุสุดวิสัย หรือได้กระทำตามกฎหมายหรือคำสั่งของเจ้าหน้าที่ที่ปฏิบัติตามอำนาจหน้าที่ของตน หรือความเ สียหายนั้นเกิดจากการกระทำหรือการละเว้นการกระทำของเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องนั้นเอง เพียงแต่ปัญหาค่าสินไหมทดแทนนั้น อาจจะมีปัญหาในเรื่องของการกำหนดว่าควรจะเป็นเท่าใด และค่าสินไหมทดแทนนั้นควรจะวัดจากอะไร เนื่องจากความเสียหายที่เกิดขึ้นนั้นบ่อยครั้งที่เกิดความเสียหายขึ้นแก่ชื่อเสียง จิตใจ มิได้เกิดความเสียหายต่อร่างกายหรือทรัพย์สินที่สามารถกำหนดค่าสินไหมทดแทนได้ง่ายกว่า ซึ่งปัญหาดังกล่าวนั้นจะพบได้บ่อยในประเทศไทย

จากที่ได้กล่าวมาว่าลักษณะของ Cyberstalking นั้นมีลักษณะพฤติกรรมที่เกิดขึ้นซ้ำ ๆ แ ละมีหลายการกระทำ เช่น การข่มขู่ การรังควาน การรบกวน หรือการก่อความรำคาญ โดยทำให้เกิดความกลัวหรือตื่นตกใจ และการข่มขู่ ข่มขวัญ หรือรังควานนั้นบางครั้งเป็นการข่มขู่ว่าจะทำร้ายร่างกาย ทำลายทรัพย์สินของเหยื่อ

เมื่อพิจารณาถึงลักษณะพฤติกรรมของ Cyberstalking แล้วเห็นว่าบทบัญญัติของกฎหมายในประมวลกฎหมายอาญามาตรา 326 มาตรา 328 และมาตรา 392 เป็นสามมาตราที่สามารถนำมาเป็นบทลงโทษผู้กระทำความผิดฐาน Cyberstalking ได้ หากแต่ผู้กระทำความผิดได้กระทำการอื่นเช่น ข่มขู่ว่าจะฆ่าแล้วมีการฆ่า ก็ต้องนำมาตรา 288 มาใช้ด้วย ในบทบัญญัติของทั้งสามมาตรานั้นมีบทลงโทษเพียงเล็กน้อย มาตรา 392 นั้นเป็นบทลหุโทษที่จำคุกไม่เกินหนึ่งเดือน ปรับไม่เกินหนึ่งพันบาท ไม่น่าจะสามารถยับยั้งหรือลงโทษผู้กระทำความผิดให้เข็ดหลาบ นอกจากนี้พฤติกรรมของ Cyberstalking นั้นต้องมีการกระทำ ซ้ำ ๆ ในช่วงระยะเวลาหนึ่ง ดังนั้น หากแม้ว่าผู้กระทำความผิดนั้นถูกศาลพิพากษาลงโทษว่ากระทำความผิดแล้วยังกลับมากระทำความผิดอีก กฎหมายของไทยก็มีบทบัญญัติเพิ่มโทษในมาตรา 92 และมาตรา 93 แต่ตามกฎหมายมาตรา 92 และมาตรา 93 นั้น ไม่อาจที่จะนำมาใช้ลงโทษผู้ กระทำความผิดที่ศาลลงโทษปรับเพียงอย่างเดียว เนื่องจากมาตรา 392 นั้นเป็นบทลหุโทษที่ศาลมักจะลงโทษปรับเพียงอย่างเดียว เพราะเห็นว่าเป็นความผิดเล็กน้อย ส่วนมาตรา 93 นั้นจะเพิ่มโทษได้ก็ต่อเมื่อเป็นไปตามบทบัญญัติของกฎหมายซึ่งจะเพิ่มโทษได้ต้องเป็นไปตามมาตรา 93 (1) ถึง (13) เมื่อมาตรา 326 มาตรา 328 และมาตรา 392 มิได้อยู่ในบทบัญญัติมาตรา 93(1) ถึง (13) ก็ไม่สามารถเพิ่มโทษตามมาตรา 93 ได้

ส่วนพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ .ศ. 2550 นั้นอาจจะใช้ได้แค่เพียงการเผยแพร่ภาพลามก อนาจาร และเผยแพร่ภาพที่ได้ตัดต่อ เติม หรือดัดแปลงโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีอื่น ๆ เท่านั้น หาก เป็นข้อความที่มีลักษณะเป็นการคุกคาม หรือข้อความที่ เป็นเท็จหรือใส่ร้ายเหยื่อ พระราชบัญญัติฉบับดังกล่าวนั้นไม่ครอบคลุมถึง ซึ่งบทลงโทษตามพระราชบัญญัติ ฉบับดังกล่าวมีอัตราโทษที่สูงกว่าแต่ก็ไม่ได้บัญญัติถึงการกระทำความผิดที่เกี่ยวกับ Cyberstalking โดยแท้จริงแล้วพระราชบัญญัติฉบับดังกล่าวน่าจะออกมาเพื่อแก้ปัญหา Cyberstalking ได้ แต่ปรากฏว่าพระราชบัญญัติฉบับดังกล่าวไม่เอื้ออำนวยต่อการนำมาใช้ลงโทษผู้กระทำความผิดฐาน Cyberstalking ได้ครอบคลุมเต็มที่

ในส่วนของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ .ศ. .. (ฉบับสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ) เป็นกฎหมายที่ลงโทษผู้นำข้อมูลส่วนบุคคลของผู้อื่นหรือ บุคคลที่เป็นเหยื่อ ไปใช้ในการคุกคาม หรือนำไปเปิดเผย เพื่อให้ตนหรือผู้อื่นได้รับประโยชน์หรือเพื่อให้เจ้าของข้อมูลนั้นได้รับความเสียหาย ร่างพระราชบัญญัติดังกล่าวถือได้ว่าเป็นกฎหมายที่คุ้มครองสิทธิส่วนบุคคลในการไม่เปิดเผยข้อมูล และให้ลงโทษผู้ที่นำข้อมูลไปใช้ในการคุกคามด้วย ซึ่งถือว่าเป็นกฎหมายที่ต้องการคุกคามความเป็นส่วนตัวได้ในระดับหนึ่ง ปัญหามีเพียงว่าร่างพระราชบัญญัติดังกล่าวนั้นยังไม่ประกาศใช้ จึงทำให้ผู้ที่ถูกเผยแพร่ข้อมูลส่วนบุคคลอาจตกเป็นเหยื่อและกฎหมายไม่สามารถลงโทษหรือดำเนินการเรียกค่าเสียหายใด ๆ จากผู้กระทำความผิดได้

บทที่ 4
บทวิเคราะห์กฎหมายประเทศสหรัฐอเมริกาและกฎหมายของประเทศไทย

4.1 บทวิเคราะห์กฎหมายประเทศสหรัฐอเมริกา

จากการศึกษาปัญหา Cyberstalking ในประเทศสหรัฐอเมริกานั้นพบว่า ปัญหาดังกล่าวนั้นเกิดขึ้นมาจากปัจจัยการขยายตัวของเส้นทางข้อมูลข่าวสารหรืออินเตอร์เน็ตที่เกิดขึ้นอย่างรวดเร็ว อินเตอร์เน็ตและเทคโนโลยีการติดต่อสื่อสารอื่น ๆ ได้เข้ามามีส่วนสำคัญต่อชีวิตประจำวันในสังคมทั่วทุกมุมโลก เพื่อเป็นการส่งเสริมการพาณิชย์ พัฒนาการศึกษา และการรักษาสุขภาพ นำการมีส่วนร่วมในระบบประชาธิปไตยในประเทศสหรัฐอเมริกาและทั่วโลก ช่วยอำน วยความสะดวกในการติดต่อสื่อสาร แต่เนื่องจากลักษณะเทคโนโลยีประเภทนี้มีค่าใช้จ่ายที่ถูก ง่ายต่อการใช้ และมีเอกลักษณ์ที่เป็นธรรมชาติคือการไม่เปิดเผย ทำให้ง่ายต่อการฉ้อโกง การหลอกลวง การล่วงละเมิดทางเพศ และปัญหาดังกล่าวได้ขย ายวงกว้างมากขึ้นจนกลายเป็ นปัญหาอาชญากรรมที่เรียกว่า “การคุกคามทางอินเตอร์เน็ต” หรือ Cyberstalking

การคุกคามทางอินเตอร์เน็ตนั้นอาจจะทำให้เห็นว่าเป็นการคุกคามที่ไม่มีลักษณะการคุกคามทางกายภาพเข้ามาเกี่ยวข้อง เช่นการเข้าทำร้ายร่าง กายของเหยื่อ จนเกิดความเข้าใจผิดว่าการคุกคามทาง อินเตอร์เน็ตนั้นมีความรุนแรงน้อยกว่าการถูกคุกคามทางกายภาพหรือการคุกคามแบบทั่วไป เมื่ออินเตอร์เน็ตได้กลายมาเป็นส่วนหนึ่งของการใช้ชีวิตส่วนบุคคล ง่ายต่อการใช้และไม่มีลักษณะของการเผชิญหน้า ไม่เกี่ยวกับกับบุคคลและลักษณะพิเศษของอินเตอร์เน็ตจึงทำให้เกิดก ารส่งเสริมการติดตามและการคุกคามทางอินเตอร์เน็ต อาจมีการติดต่อสื่อสารในลักษณะที่เป็นการรบกวนและคุกคาม เช่น ส่งอีเมล์โทรศัพท์ไปยังเหยื่อ และท้ายที่สุดอาจมีการติดตามหรือการคุกคามทางกายภาพ ปัญหา Cyberstalking อาจนำไปสู่พฤติกรรมที่รุนแรงขึ้น รวมถึงการคุกคามที่รุนแรงขึ้นเช่นกัน

นอกจากนี้พฤติกรรมการคุกคามที่เกิดขึ้นนั้นอาจจะไม่ใช่เกิดจากการคุกคามที่เกิดขึ้นโดยตัวของผู้คุกคามเอง หากแต่เป็นการคุกคามที่เกิดขึ้นจากบุคคลที่สาม ซึ่งผู้คุกคามนั้นอาจจะทำให้บุคคลที่สามนั้นกลายเป็นเครื่องมือในการคุกคามเหยื่อแท นตนเอง เช่น ผู้คุกคามอาจนำข้อความที่เข้าลักษณะของการต่อต้านหรือล่อลวงไปลงบนกระดานข้อความสาธารณะภายใต้ชื่อ หมายเลขโทรศัพท์ หรือที่อยู่ติดต่อ หรือ อีเมล์ของเหยื่อไว้ทำให้บุคคลอื่น ๆ ที่เข้าถึงข้อมูลดังกล่าวนั้นติดต่อกลับไปยังเหยื่อผู้เคราะห์ร้ายนั้น ปัญหา

ดังกล่าวนั้นทำให้ยากในการบังคับใช้กฎหมายเพื่อระบุตำแหน่งและจับกุมผู้กระทำความผิด[100]

ดังนั้น จากการศึกษากฎหมายของประเทศสหรัฐอเมริกาโดยรวมทั้งหมดแล้วนั้น พบว่ายังคงมีปัญหาซึ่งสามารถแยกพิจารณาได้ดังนี้[101]

(1) ปัญหาข้อกำหนดให้มีการกระทำที่อยู่ในระยะที่ใกล้กับเหยื่อ

ในปัจจุบันมีเพียงกฎหมายไม่กี่รัฐที่ควบคุมการคุกคามทั่วไปที่กำหนดว่า จำเลยจะต้องกระทำการใดๆที่มีการติดตามเหยื่อทางร่างกาย แต่เนื่องจากลักษณะของการคุกคามทางอินเตอร์เน็ตทำให้ผู้คุกคามสามารถอยู่ในที่ที่ห่างไกลจากเหยื่อได้ ดังนั้นกฎหมายที่กำหนดปัจจัยดังกล่าวก็ไม่สามารถแก้ปัญหานี้ได้

ตัวอย่างของปัญหาดังกล่าวเกิดขึ้นเมื่อปี ค.ศ. 1996 ในรัฐจอร์เจีย โดยผู้คุกคามได้ลงประกาศข้อความที่หยาบคายในเว็บไซต์และได้ให้เบอร์โทรศัพท์และที่อยู่ที่บ้านของเธอและโฆษณาว่า เหยื่อเป็นโสเภณี มีคนหลายคนโทรศัพท์หาเหยื่ อเพื่อตอบข้อความนั้นหรือกระทั่งบุกไปที่บ้านของเธอและรังควานเธออย่างไม่ได้ตั้งใจ ตามกฎหมายของรัฐจอร์เจียในขณะนั้น (กฎหมายได้ถูกแก้ไขแล้วในปัจจุบัน) ผู้คุกคามทางอินเตอร์เน็ตถูกตัดสินว่า ไม่ได้กระทำความผิดใดๆเนื่องจากการกระทำของผู้คุกคามไม่ได้เกี่ยวข้องกับการ ติดตามคุกคามเหยื่อทางร่างกาย

(2) ปัญหาข้อกำหนดให้มีการข่มขู่ที่น่าเชื่อได้ว่าจะเกิดขึ้นจริง (Credible Threat) กฎหมายควบคุมการคุกคามของหลายรัฐกำหนดว่า ผู้กระทำผิดจะต้องข่มขู่เหยื่อในลักษณะที่น่าเชื่อได้ว่าจะเกิดขึ้นจริง โดยทั่วไปการข่มขู่ที่น่าเชื่อว่ าจะเกิดขึ้นจริงจะประกอบด้วย “คำขู่โดยวาจาหรือข้อความ ” ประกอบกับ “ความสามารถในการกระทำตามคำขู่ ” เพื่อทำให้เหยื่อหวาดกลัว ซึ่งการกำหนดให้ความผิดทางอาญาต้องประกอบด้วยปัจจัยทั้งสองเรื่องทำให้เกณฑ์การพิจารณาไม่เพียงพอต่อการควบคุมการคุกคามทางอินเตอร์เน็ตด้วยเหตุ ผล 4 ข้อ ดังนี้

---

[100] U.S the Attorney General, 1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry, A Report from the Attorney General to the Vice President August 1999. Internet. http://www.usdj.gov/criminal/cybercrime/cyberstalking.htm.

[101] Naomi H. Goodno, “Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws,” The Berkeley Electronic Press ,(2006) : 1- 62.

(2.1) การกำหนดให้มีการข่มขู่ที่ชัดแจ้งก่อให้เกิดปัญหาช่องว่างในการพิจารณาลงโทษการกระทำซึ่งไม่ได้เป็นการข่มขู่ที่ชัดเจน แต่ยังสามารถทำให้วิญญูชนทั่วไปหวาดกลัวได้ เนื่องจากโดยทั่วไป ผู้คุกคามจะไม่ข่มขู่เหยื่ออย่างเปิดเผยแต่จะมี "การกระทำต่อเนื่อง" ซึ่งเมื่อพิจารณาโดยรวมแล้วทำให้วิญญูชนทั่วไปเกิดความหวาดกลัวได้ แต่การกระทำไม่ได้ถือว่าเป็นการข่มขู่ที่โจ่งแจ้ง

ยกตัวอย่างเช่น ผู้คุกคามทั่วไปอาจจะหลบอยู่ข้างหลังพุ่มไม้เพื่อมองเหยื่อ ลอบตามเหยื่อ โทรศัพท์ถึงเหยื่อแล้ววางสายทันที และส่งกุหลาบสี ดำให้เหยื่อ ซึ่งการกระทำดังกล่าวในแต่ละครั้งไม่ถือเป็นการข่มขู่อย่างชัดแจ้ง จึงไม่น่าจะเป็นไปตามข้อกำหนดให้มี "การข่มขู่ที่น่าเชื่อได้ว่าจะเกิดขึ้นจริง " ในกรณีของการคุกคามทางอินเตอร์เน็ต กฎหมายที่กำหนดให้มีองค์ประกอบดังกล่าวไม่สามารถครอบคลุมถึงการสื่อสารอิ เล็กทรอนิกส์ที่เป็นการรังควานเหยื่อแต่ไม่ถือเป็นการข่มขู่จริง อาทิเช่น การส่งข้อความทาง อีเมล์เป็นพัน ๆ ข้อความ เป็นต้น

ประเด็นปัญหาเกี่ยวกับเกณฑ์การข่มขู่ที่น่าจะเกิดจริงนี้กำลังอยู่ในระหว่างพิจารณาคดีการคุกคามทั่วไป มลรัฐหนึ่งได้แทนที่เกณฑ์การข่มขู่ที่ น่าจะเกิดขึ้นจริงด้วย "เกณฑ์วิญญูชน" เนื่องจากปัญหาเหล่านี้จะชัดเจนขึ้นเมื่อปรับใช้กฎหมายกับกรณีการคุกคามทางอินเตอร์เน็ต ในคดี Iowa v. Limbrecht ศาลตระหนักถึงการเปลี่ยนแปลงของกฎหมายและกล่าวว่า การตัดสินลงโทษการคุกคามในคดีจะเปลี่ยนแปลงหรือไม่นั้นขึ้นอยู่ กับว่า จะใช้เกณฑ์การพิจารณาใดในการตัดสิน จำเลยในคดีเป็นนักโทษเรือนจำซึ่งหลงใหลใน Stacy Corey หญิงสาวซึ่งทำงานในเรือนจำนั้น จำเลยมักจะใช้สายตาจ้องมองเธอและกล่าวเท็จกับนักโทษคนอื่นว่าจำเลยมีความสัมพันธ์ทางเพศกับ Corey จนทำให้เธอต้องลาออกและย้ายออก แต่จำเล ยก็ยังมีความหลงใหลคลั่งไคล้ในตัวเธอและหลังจากที่จำเลยพ้นโทษออกมา จำเลยค้นพบที่อยู่ใหม่ของ Corey และส่งจดหมายถึงสามีของ Corey กล่าวหาว่า Corey มีเพศสัมพันธ์กับนักโทษหลายคนในเรือนจำตอนที่เธอทำงานที่นั่น จำเลยขับรถผ่านหน้าบ้าน Corey หลายครั้งซึ่งทำให้เกิดการ สอบสวนและพิจารณาลงโทษจำเลยในข้อหาคุกคาม จำเลยอุทธรณ์ต่อคำพิพากษาโดยโต้แย้งว่า จำเลยมิได้ข่มขู่ Corey อย่างโจ่งแจ้ง ศาลรับทราบข้อเท็จจริงดังกล่าว และปฏิเสธที่จะยอมรับข้อโต้แย้งนั้น เพราะหากยอมรับ ก็จะเป็นการกลับไปใช้กฎหมายเก่าซึ่งกำหนดให้มีองค์ประกอบเกณ ฑ์การข่มขู่ที่น่าจะเกิดจริง

(Credible Threat)[102] ภายใต้กฎหมายฉบับแก้ไขซึ่งใช้เกณฑ์วิญญูชนแทน ศาลเห็นว่าการกระทำของจำเลยก่อให้เกิดความหวาดกลัวไม่น้อยไปกว่าการข่มขู่อย่างชัดแจ้ง

ในคดี Limbrecht ยังคงเป็นข้อถกเถียงกันในคดีการคุกคามทั่วไปว่า เกณฑ์การข่มขู่ที่น่าจะเกิดจริง (Credible Threat) เป็นเกณฑ์การตัดสินที่เหมาะสมหรือไม่ ปัญหาดังกล่าวเป็นปัญหาที่สำคัญในคดี Cyberstalking เนื่องจากอินเตอร์เน็ตทำให้ผู้คุกคามสามารถกระทำการข่มขวัญต่อเนื่องได้ง่ายและรวดเร็วกว่าผู้คุกคามทั่วไปที่ไม่ใช้อินเตอร์เน็ต ในคดี Limbrecht ผู้คุกคามส่งจดหมายสองฉบับในช่วงเวลาหนึ่งเดือน ในขณะที่ Cyberstalker สามารถส่งข้อความข่มขู่ทาง อีเมล์ได้เป็นร้อยหรือเป็นพันฉบับ (จดหมายในลักษณะเดียวกับในคดี Limbrecht) ภายในเวลาหนึ่งชั่วโมง ซึ่งภายในระยะเวลาไม่กี่วันหรือสัปดาห์ก็สามารถทำให้เกิดค วามวุ่นวายในชีวิตประจำวันของเหยื่อได้ หากไม่มีการข่มขู่ที่ชัดแจ้งในข้อความทาง อีเมล์เหล่านั้น เหยื่อก็ไม่สามารถพิสูจน์ได้ว่า มีการข่มขู่ที่น่าจะเกิดขึ้นจริง การข่มขู่อย่างโจ่งแจ้งโดยปกติจะเป็นวาจาหรือข้อความซึ่งอาจทำให้เกิดปัญหาในกรณี Cyberstalking การข่มขู่ทางวาจากำหนดให้ผู้คุกคามต้องอยู่ใกล้เหยื่อ ซึ่งไม่ครอบคลุมถึงหลาย ๆ กรณีของ Cyberstalking และการคุกคามโดยการเขียนไม่ได้ครอบคลุมถึงการสื่อสารทางอิเล็กทรอนิกส์ซึ่งทำให้เกิดปัญหาได้ เช่น อีเมล์ แชทรูมหรือการส่งข้อความฉับพลัน (Instant Messenger)[103]

(2.2) เป็นปัญหาซึ่งเกี่ยวกับการรับข้อความข่มขู่ในคดี Cyberstalking “ คำขู่ ” (Threat) สื่อโดยนัยว่า มีการสื่อสารโดยตรงจากผู้คุกคามถึงเหยื่อ แต่ผู้คุกคามทางอินเตอร์เน็ต (Cyberstalker) สามารถลงประกาศข้อความที่น่าหวาดกลัวอย่างง่ายดายโดยไม่จำเป็นต้องติดต่อกับเหยื่ อโดยตรงและเหยื่อก็ไม่จำเป็นต้องได้รับข้อความเหล่านั้นโดยตรง Cyberstalker สามารถเผยแพร่ข้อความคุกคามรังควานเหยื่อโดยการลงในเว็บไซต์ หรือกระดานข่าวพูดคุยต่าง ๆ ดังนั้น ในการคุกคามทางอินเตอร์เน็ต ผู้คุกคามสามารถคุกคามรังควานเหยื่อโดยไม่ต้องใช้ความพยายาม ใด ๆ เพียงแค่การใช้สื่อที่สามารถเข้าถึงได้ทั่วโลก และการกระทำนี้ก็ไม่ได้น่ากลัวน้อยไปกว่าการข่มขู่ที่จริงแต่อย่างใด

---

[102] IOWA CODE ANN. S.708.11(1)(a)(West 1993) (defining a “credible threat” as “a threat made with the intent to place a reasonable person in like circumstances in fear of death or bodily injury , coupled with the apparent ability to carry out of threat.”)

[103] Naomi H. Goodno, “Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws,” p.17.

ตัวอย่างเช่น ในคดีหนึ่งซึ่งผู้คุกคามได้ทำเว็บไซต์ขึ้นเพื่อลงข้อความเกี่ยวกับเหยื่อ Amy Boyer[104] ผู้คุกคามเป็นเพื่อนร่วมชั้นเรียนกับเธอ ซึ่งเขียนเรื่องแฟนตาซีต่างๆ เกี่ยวกับ Boyer และข้อความเกี่ยวกับชีวิตประจำวันของเธอโดยที่เธอไม่รู้ตัว เช่น เธอใส่อะไรในวันไหน สถานที่ที่เธอไปมา หรือว่าเธอกำลังทำอะไร และลงประกาศในเว็บไซต์นั้น การลงประกาศดำเนินเรื่อยมาเป็นระยะเวลาประมาณ 2 ปีและจบลงเมื่อผู้คุกคามฆาตกรรม Boyer และฆ่าตัวตายตาม ทั้ง Boyer และครอบครัวไม่ทราบเกี่ยวกับข้อความเหล่านี้ในเว็บไซต์ จนกระทั่งหลังการฆาตกรรม ถึงแม้ว่าคดีนี้จะไม่ได้มีการพิจารณาในชั้นศาล แต่ก็น่าจะเป็นไปได้ยากที่จะสามารถพิสูจน์ว่ามีการข่มขู่ที่น่าเชื่อได้ว่าจะเกิดจริง เนื่องจากข้อความไม่ได้ถูกส่งให้เธอโดยตรง จึงเป็นไปได้ยากที่จะกล่าวว่า ผู้คุกคามได้ทำการข่มขู่เธอโดยตรง

(2.3) ปัญหาองค์ประกอบของการข่มขู่ที่น่าจะเกิดขึ้นจริงกำหนดให้เหยื่อในคดีคุกคามทางอินเตอร์เน็ตต้องพิสูจน์ว่า ผู้คุกคามมีความสามารถชัดเจนในการทำให้คำขู่นั้นเกิดขึ้นจริง สมมติว่า ถ้าผู้คุกคามส่งข้อความมาจากประเทศอื่น การพิสูจน์ก็คงเป็นปัญหา เหยื่ออาจจะต้องพิสูจน์ว่า ผู้คุกคามมีความสามารถพอที่จะเดินทางข้ามประเทศเพื่อกระทำตามคำขู่นั้น การกำหนดองค์ประกอบดังกล่าวนั้นจึงไม่มีความจำเป็นและสร้างความยากลำบากในการพิสูจน์ข้อเท็จจริงของเหยื่อ

ในความเป็นจริง เหยื่ออาจจะไม่รู้เลยว่า ผู้คุกคามนิรนามอยู่ที่ใด รู้เพียงว่าเขาอาจจะเป็นเพื่อนบ้านของเธอ เป็นเพื่อนร่วมงาน หรืออยู่อีกประเทศหนึ่ง ซึ่งทำให้การพิสูจน์ว่าผู้คุกคามสามารถทำตามคำขู่ได้นั้นยากขึ้น อินเตอร์เน็ตอนุญาตให้มีการส่งข้อความทางอิเล็กทรอนิกส์โดยไม่ต้องเปิดเผยนามผู้ส่ง ซึ่งทำให้ผู้คุกคามสามารถซ่อนตัวจากความเป็นจริงและจากเหยื่อได้และเหยื่อที่ถูกคุกคามโดยบุคคลนิรนามก็ไม่สามารถรู้ได้ถึงนิสัยและจุดประสงค์ของบุคคลนั้น และเมื่อเหยื่อไม่สามารถรู้ว่าผู้คุกคามเป็นใคร อยู่ที่ไหน นิสัยใจคอเป็นอย่างไร ก็เป็นการยากมากๆหรือแทบจะเป็นไปไม่ได้ที่เหยื่อจะสามารถพิสูจน์ได้ว่าผู้คุกคามมีความสามารถพอที่จะกระทำการตามคำขู่ได้หรือไม่

(2.4) การพิสูจน์การข่มขู่ที่น่าเชื่อได้ว่าจะเกิดขึ้นจริงในคดีการคุกคามทางอินเตอร์เน็ตนั้น ไม่สามารถครอบคลุมถึงกรณีที่ผู้คุกคามทางอินเตอร์เน็ตลวงให้บุคคลที่สามข่มขู่เหยื่ออย่างไม่ได้ตั้งใจแทนตน เช่น หากผู้คุกคามใช้ชื่อของเหยื่อลงประกาศข้อความเชิญชวนให้มีการข่มขืนหมู่ ก็ไม่มีข้อพิสูจน์ของการข่มขู่ที่ชัดแจ้ง หรือมีการข่มขู่จากผู้คุกคามถึงเหยื่อโดยตรง

---

[104] Ibid., p. 18.

โดยสรุป กฎหมายต่าง ๆ ที่มีความพยายามจะรวมการคุกคามทางอินเตอร์เน็ตไว้ในกฎหมายควบคุมการคุกคามทั่วไป และ กฎหมายที่ควบคุมการคุกคามทางอินเตอร์เน็ตโดยตรง หากกฎหมายดังกล่าวมีข้อกำหนดการพิสูจน์การข่มขู่ที่น่าเชื่อได้ว่าจะเกิดขึ้นจริงแล้วก็ไม่สามารถครอบคลุ มแง่มุมต่างๆในคดี Cyberstalking ได้ เนื่องจากกฎหมายเหล่านั้นมุ่งไปที่การกระทำของผู้คุกคาม แต่ในคดี Cyberstalking การพิสูจน์ตามเกณฑ์วิญญูชนน่าจะเหมาะสมกว่า เนื่องจากจะมุ่งไปที่ความหวาดกลัวของเหยื่อซึ่งเกิดขึ้นจากการที่ผู้คุกคามตั้งใจข่มขู่รังควานเหยื่อ

(3) การพิสูจน์ตามเกณฑ์วิญญูชน (Reasonable Standard) หรือเกณฑ์ที่เหมาะสม กฎหมายที่ใช้เกณฑ์วิญญูชนในการพิสูจน์ความผิดเรื่องการคุกคามถือเป็นวิธีการที่ถูกต้อง เนื่องจากเกณฑ์การพิสูจน์ดังกล่าวไม่ได้กำหนดให้มีการพิสูจน์ว่าผู้คุกคามต้องอยู่ใกล้เหยื่อ นอกจากนั้นเกณฑ์การพิสูจน์ตามเกณฑ์วิญญูชนยังแก้ปัญหาที่เกิดขึ้นจากเกณฑ์การพิสูจน์การข่มขู่ที่น่าเชื่อได้ว่าจะเกิดจริง (Credible Threat) เกณฑ์วิญญูชนไม่ได้กำหนดให้ผู้คุกคามต้องส่งข้อความข่มขู่ที่ชัดแจ้งถึงเหยื่อโดยตรง และไม่ได้กำหนดให้เหยื่อต้องพิสูจน์ว่าผู้คุ กคามมีความสามารถที่จะกระทำการตามคำขู่หรือไม่ ในทางกลับกันความสำคัญของคดีมุ่งไปที่เหยื่อและการพิจารณาว่าเหยื่อมีเหตุผลพอหรือไม่ที่จะกลัวในความปลอดภัยของตน ซึ่งเป็นเหตุมาจากการกระทำของผู้คุกคามทางอินเตอร์เน็ต

การแยกแยะความแตกต่างระหว่างกฎหมายที่กำหนดให้ มีการพิสูจน์การข่มขู่ที่น่าเชื่อว่าจะเกิดขึ้นจริง (Credible Threat) และการพิสูจน์ตามเกณฑ์วิญญูนนั้นต้องการการตีความที่ละเอียดรอบคอบ ตัวอย่างเช่น กฎหมายการคุกคามของมลรัฐเดลาแวร์จะถือว่าเป็นความผิดอาญาหาก “บุคคลหนึ่งกระทำการต่อเนื่องโดยตรงกับบุคคลหนึ่งบุ คคลใดโดยเฉพาะ ซึ่งการกระทำนั้นทำให้เกิดความหวาดกลัวได้อย่างมีเหตุผล ” เมื่อพิจารณาผิวเผินแล้วเหมือนว่ากฎหมายจะไม่ได้กำหนดเรื่องของการพิสูจน์การข่มขู่ที่น่าเชื่อว่าจะเกิดขึ้นจริง (Credible Threat) เอาไว้ และก็ไม่ได้หมายความว่ากฎหมายฉบับดังกล่าวมุ่งเน้นที่ความกลัวของเหยื่อ เมื่อพิจารณาต่อไป “การกระทำต่อเนื่อง ” หมายรวมถึง การรักษาระยะใกล้กันระหว่างตัวเหยื่อกับผู้คุกคาม การสื่อสารคำขู่ทางวาจาและข้อความหรือการขู่ซึ่งเป็นนัยมาจากการกระทำ (เกณฑ์นี้เทียบได้กับ “การข่มขู่ที่น่าจะเกิดขึ้นจริง ”) ดังนั้นแม้ในตัวกฎหมายจะมีคำว่า “วิญญูชน” ปรากฏอยู่ แต่เมื่อพิจารณาอย่างละเอียดแล้วกฎหมายดังกล่าวกลับใช้เกณฑ์ “การข่มขู่ที่น่าจะเกิดขึ้นจริง” (Credible Threat)

(4) การลวงให้บุคคลที่สามคุกคามเหยื่อแทนตนเองเป็นความผิดอาญา

การลวงบุคคลที่สามให้คุกคามเหยื่อ แทนนั้นเป็นหนึ่งในความแตกต่างอย่างชัดเจนระหว่างการคุกคามทางอินเตอร์เน็ต (Cyberstalking) กับการคุกคามทั่วไป (Stalking) ในขณะนี้มีเพียงมลรัฐเดียวเท่านั้นคือ มลรัฐโอไฮโอ ที่ทำให้การกระทำดังกล่าวเป็นความผิดอาญา เพื่อไม่ให้ผู้คุกคามและเหยื่อเกิดความสับสนว่ าการกระทำนี้เป็นโทษทางอาญาหรือไม่ กฎหมายลงโทษการคุกคามทางอินเตอร์เน็ตจึงควรห้ามการใช้อินเตอร์เน็ตเพื่อทำให้บุคคลอื่นกระทำการใด ๆ อันจะทำให้วิญญูชนทั่วไปเกิดความหวาดกลัวในความปลอดภัยของตน

(5) ปัญหาจากการบังคับใช้ Interstate Communication Act,18 U.S.C. S. 875 (c)

พระราชบัญญัติฉบับดังกล่าวบัญญัติให้การส่งผ่านการสื่อสารใด ๆ ในเชิงพาณิชย์ระหว่างรัฐหรือต่างประเทศอันเป็นการก่ออันตรายให้กับบุคคลอื่นนั้นต้องโทษปรับและจำคุกไม่เกินห้าปีหรือทั้งจำทั้งปรับ ซึ่งกฎหมายฉบับดังกล่าวนี้ได้กำหนดว่า “การสื่อสารใด ๆ” หมายรวมถึง การข่มขู่ที่สื่อสารคมน าคมข้ามรัฐผ่านทางโทรศัพท์ อีเมล์ เพจเจอร์ หรืออินเตอร์เน็ต กฎหมายฉบับนี้ประสบความสำเร็จในการดำเนินคดีกับผู้คุกคามที่ใช้อินเตอร์เน็ตในการส่งข้อความข่มขู่ทางอีเมล์[105]

อย่างไรก็ตาม ข้อกำหนดที่ว่าการสื่อสารจะต้องประกอบด้วย “การข่มขู่” นี้เองเป็นส่วนที่ทำให้กฎหมายฉบับนี้ขาดความสมบูรณ์ เนื่องจากกฎหมายดังกล่าวมีความคล้ายคลึงกับข้อกำหนดของ “การข่มขู่ที่น่าจะเกิดขึ้นจริง ” (Credible Threat) ดังนั้น กฎหมายก็จะไม่สามารถปรับใช้กับผู้คุกคามที่ใช้อินเตอร์เน็ตในการมุ่งที่จะคุกคามหรือรัง ควานผู้อื่นแต่มิได้ใช้การข่มขู่อย่างเฉพาะเจาะจง

เช่นในคดี United States v Alkhabaz[106] คดีนี้จำเลยส่งข้อความทาง อีเมล์จำนวนมากเกี่ยวกับการจินตนาการทางเพศอย่างรุนแรงเกี่ยวกับผู้หญิงและเด็กไปให้คนรู้จัก และสุดท้ายจำเลยได้ลงเรื่องเกี่ยวกับการทรมานที่มีลักษณะโ จ่งแจ้งในห้องสนทนา ซึ่งเหยื่อที่ถูกข่มขืนทรมานนั้นมีชื่อเดียวกันกับเพื่อนร่วมชั้นเรียนของจำเลย ศาลตัดสินว่าจำเลย

---

[105] United State v. Kammersell, 196 F.3d 1137 (10th Cir.1999) (upholding the defendant’ s conviction even though the defendant sent the e-mail messages to the victim who was in the same state because the e-mail message was sent via interstate telephone lines.)

[106] Naomi H. Goodno, “Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws,” p. 30.

ไม่ได้กระทำความผิดขัดต่อมาตรา 875 (c) เนื่องจากจำเลยมิได้กระทำ "การสื่อสารที่ประกอบไปด้วยการข่มขู่อย่างแท้จริง"

เนื่องจากกฎหมายฉบับนี้จำกั ดอยู่เพียงกรณีที่การคุกคามทางอินเตอร์เน็ตมีการข่มขู่อย่าง "แท้จริง" คือ มีลักษณะเป็นไปได้เท่านั้น ทำให้กฎหมายมิได้ครอบคลุมถึงเหตุการณ์หลายๆ อย่างที่ผู้คุกคามกระทำการอย่างจงใจที่จะรังควานเหยื่อ แต่ปราศจากการข่มขู่อย่างชัดแจ้ง

(6) ปัญหาจาก Federal Phone Harassment Statue , 47 U.S.C. S. 223 พระราชบัญญัติการคุกคามทางโทรศัพท์ กฎหมายฉบับนี้ตราขึ้นในปี 1934 ซึ่งเป็นเวลาที่โทรศัพท์เป็นเทคโนโลยีใหม่ในการสื่อสารเหมือนกับอินเตอร์เน็ตในปัจจุบัน พระราชบัญญัตินี้ระบุว่า การใช้โทรศัพท์โดยเปิดเผยนามหรือไม่ก็ต าม หรือการใช้ "เครื่องมือสื่อสารใด ๆ" "เพื่อที่จะก่อให้เกิดความรำคาญ ล่วงละเมิด รังควาน หรือข่มขู่บุคคล " เป็นความผิดทางอาญา ต้องโทษจำคุกไม่เกินสองปี และเมื่อไม่นานมานี้ ในเดือนมกราคม 2006 รัฐบาลกลางได้แก้ไขคำจำกัดความของ "เครื่องมือสื่อสาร ใด ๆ" ได้ถูกเปลี่ยนให้ครอบคลุมถึง "อุปกรณ์หรือซอฟแวร์ใด ๆ ที่ถูกใช้ทำให้เกิดการสื่อสาร หรือการสื่อสารใด ๆ ที่ถูกส่งผ่านทางอินเตอร์เน็ตไม่ว่าทั้งหมดหรือบางส่วน" แต่การแก้ไขกฎหมายดังกล่าวก็ไม่สามารถแก้ไขปัญหาของ Cyberstalking ได้เนื่องจากบทบัญญัติของกฎหมายฉบับดังกล่าวนั้นจะถือว่าเป็น Cyberstalking และเป็นความผิดทางอาญาก็ต่อเมื่อนามของผู้คุกคามนั้นเป็นความลับ และ กฎหมายฉบับดังกล่าวก็สามารถปรับใช้ได้เฉพาะกับการคุกคามที่สื่อสารโดยตรงจากผู้คุกคามถึงตัวเหยื่อเท่านั้น กฎหมายฉบับดังกล่าวยังไม่สามารถจัดการได้กับพฤติกรรมการคุกคามและทำให้เหยื่อสะพรึงกลัวทางอ้อม เช่นการลงข้อความลงบนเว็บบอร์ด กระดานข่าว หรือการทำเว็บไซต์ซึ่งทำให้เหยื่อหวาดกลัว หรือเป็นการยั่วยุบุคคลที่สามให้คุกคามเหยื่อ นอกจากนี้บทลงโทษของกฎหมายฉบับดังกล่าวนั้นอัตราโทษสูงสุดเพียงสองปี แต่กฎหมายการคุกคามทั่วไปในระดับของรัฐบาลกลางนั้นโทษคือจำคุกห้าปีถึงตลอดชีวิต ซึ่งอัตราโทษสูงสุดของ Cyberstalking นั้นยังอยู่ในอัตราโทษที่ต่ำ

(7) ปัญหาจาก Federal Interstate Stalking Punishment and Prevention Act , 18 U.S.C. S.2261A

กฎหมายฉบับนี้ออกมาในปี ค.ศ. 1996 และเป็นกฎหมายของสหพันธรัฐฉบับแรกที่ใช้จัดการปัญหาการคุกคามโดยเฉพาะ และในเวลานั้นก็มุ่งแก้ปัญหาการคุกคามทั่วไป ในตอนแรกกฎหมายฉบับนี้มีปัจจัยหลัก 3 ข้อ ได้แก่ (1) จำเลยจะต้อง "เดินทางข้าม

เส้นแบ่งเขตรัฐ" และ (2) "การกระทำต่อเนื่อง" อย่างตั้งใจ โดยใช้ "ไปรษณีย์หรือเครื่องมือใดๆที่ใช้อำนวยความสะดวกทางการค้าระหว่างรัฐหรือกับต่างประเทศ " (3) โดยการกระทำดังกล่าวทำให้บุคคลตกอยู่ใน " ความกลัวตาย " หรือ "กลัวที่จะได้รับบาดเจ็บ " และเมื่อไม่นานมานี้ก็ได้มีการแก้ไขกฎหมายดังกล่ าวสองครั้งเพื่อให้สามารถปรับใช้กฎหมายกับการคุกคามทางอินเตอร์เน็ตได้

ครั้งแรกในปี ค.ศ. 2000 ซึ่งแก้ไขหลักการเกี่ยวกับการใช้อำนาจศาล ก่อนหน้านี้กฎหมายฉบับนี้ใช้ได้แต่ในกรณีที่ผู้คุกคามต้องเดินทางข้ามเส้นแบ่งเขตรัฐ ซึ่งเป็นปัญหาในกรณีของ Cyberstalking เนื่องจากตัว Cyberstalker นั้นสามารถรังควานหรือคุกคามเหยื่อโดยไม่ต้องก้าวออกจากบ้านของตนเอง

ครั้งที่สองในปี ค.ศ. 2006 ได้มีการแก้ไขกฎหมายฉบับดังกล่าวโดยเพิ่มข้อความ "ใช้การสื่อสารตอบโต้ทางคอมพิวเตอร์ใดๆ" อันก่อให้เกิด "ความรุนแรงอันตรายทางจิตใ จ" เป็นความผิดทางอาญา ซึ่งการแก้ไขกฎหมายฉบับดังกล่าวนั้นได้พยามแก้ไขปัญหาหลาย ๆ ด้านที่เกิดจากกฎหมายระดับรัฐบาลกลางฉบับอื่น โดยกฎหมายฉบับดังกล่าวมิได้มีเงื่อนไขการพิสูจน์ "การข่มขู่ที่น่าจะเกิดจริง " (True / Credible Threat) แต่รับหลักเกณฑ์การวัด "ความกลัวที่อยู่บนพื้นฐานของเหตุผล " (Reasonable Fear)[107] หรือ "อันตรายทางอารมณ์ที่รุนแรง" (Substantial Emotional Harm) ของเหยื่อ นอกจากนี้กฎหมายฉบับดังกล่าวก็ไม่ได้เจาะจงที่จะปราบปราม อีเมล์ที่ไม่เปิดเผยชื่อของผู้ส่งเท่านั้นด้วย

อย่างไรก็ตามกฎหมา ยฉบับดังกล่าวก็ยังไม่สามารถจัดการกับปัญหา Cyberstalking ได้อย่างครบถ้วน เนื่องจากกฎหมายดังกล่าวยังมีช่องว่างอยู่ คือ กฎหมายฉบับดังกล่าวนั้นไม่ได้ครอบคลุมถึงกรณีที่ผู้คุกคามนั้นแสร้งหรือปลอมเป็นตัวเหยื่อ และยุยงให้บุคคลที่สามรังควานหรือทำการคุกคามเหยื่อโ ดยที่บุคคลที่สามนั้นไม่รู้ เช่น การลงข้อความบนกระดานข่าวชวนให้มีเพศสัมพันธ์โดยใช้ชื่อของเหยื่อเพื่อที่จะหลอกให้บุคคลที่สามเข้าใจผิดและทำการตอบรับข้อความนั้นโดยการคุกคามถึงตัวเหยื่อ

(8) ปัญหาความไม่ครอบคลุมของบทบัญญัติมาตรา 18 U.S.C. 2425

เนื่องจากบทบัญญัติดังกล่าวนี้จะมีบทลงโทษกับ Cyberstalking ที่นำไปสู่การมีกิจกรรมทางเพศที่ผิดกฎหมาย แต่บทบัญญัตินี้มุ่งคุ้มครองเฉพาะเด็กที่อายุต่ำกว่า 16 ปี โดยไม่มีการกล่าวถึงเหยื่อหรือผู้เสียหายที่อายุมากกว่า 16 ปี และที่สำคัญบทบัญญัติมาตรา 18 U.S.C. 2425 นี้จะลงโทษกับกรณีที่การสื่อสารนั้นมีเจตนาที่จะชักชวนล่อลวงสู่

[107] Ibid., p.36

กิจกรรมทางเพศที่ผิดกฎหมายเท่านั้น กฎหมายฉบับนี้ไม่ได้รวมถึงการคุกคามหรือรังควานโดยใช้อินเตอร์เน็ตเป็นเครื่องมือแต่ไม่ได้นำไปสู่กิจกรรมทางเพศแต่อย่างใด

(9) ปัญหาของกฎหมายระดับมลรัฐ (State Law)ไม่มีการกล่าวถึง Cyberstalking

กฎหมายระดับมลรัฐบางฉบับนั้นไม่ได้กล่าวถึงปัญหาของ Cyberstalking เลย ตัวอย่างที่ชัดเจนที่สุด คือ กฎหมายที่กำหนดให้มีองค์ประกอบการติดตามทางกายภาพ เช่น ในมลรัฐนิวยอร์กจะต้องมีการทำร้ายร่างกายจนได้รับบาดเจ็บ [108] หรือมีการถืออาวุธ[109] ในมลรัฐคอนเนคติกัตต้องมีองค์ประกอบทางกายภาพ คือ มีการติดตามหรือดักรอ[110] ส่วนมลรัฐไอโอว่าต้องมีการติดตามทางกายภาพในระยะใกล้หรือมีการขู่ [111] และในมลรัฐแมรี่แลนด์นั้นต้องมีการเข้าหาหรือติดตามบุคคลอื่น[112]

ในกฎหมายบางฉบับก็มิได้กล่าวถึงเรื่องของ Cyberstalking เพราะยังขาดความชัดเจนว่ากฎหมายดังกล่าวนั้นครอบคลุมถึงการสื่อสารทางอิเล็กทรอนิกส์หรือไม่ เช่นมลรัฐอาร์คันซอ[113] มลรัฐคอนเนคติกัต และแขวงโคลัมเบีย [114] เช่น บางมลรัฐมีกฎหมายที่เกี่ยวกับการคุกคามทางโทรศัพท์แต่ไม่ได้เฉพาะเจาะจงว่าครอบคลุมถึงการสื่อสารทางอิเล็กทรอนิกส์ ซึ่งกฎหมายเหล่านี้ไม่สามารถนำมาใช้จัดการกับการคุกคามทางอินเตอร์เน็ตได้

(10) กฎหมายของมลรัฐกล่าวถึงเรื่อง Cyberstalking เพียงบางแง่มุมเท่านั้น คือ

(10.1) บางมลรัฐพยายามที่จะแก้กฎหมายเกี่ยวกับการคุกคามทั่วไปที่มีอยู่ให้ครอบคลุมถึง การคุกคามผ่านการสื่อสารทางอิเล็กทรอนิกส์ ชนิดของการสื่อสารทางอิเล็กทรอนิกส์ที่กฎหมายเหล่านี้ครอบคลุมถึงนั้นมีลักษณะที่แตกต่างกัน ในขณะที่บางรัฐเพียงเติมข้อความ “การสื่อสารทางอิเล็กทรอนิกส์ ” ลงไปในกฎหมายที่มีอยู่ เช่นในมลรัฐ

---

[108] N.Y. PENAL LAW S. 120.60 (McKinney 2005)

[109] N.Y. PENAL LAW S. 120.55 (McKinney 2005)

[110] CONN.GEN.STAT.ANN. S. 53-a 181e (West 2005)

[111] IOWA CODE ANN. S. 708.11 (West 2005)

[112] MD. CODE ANN.,CRIM. LAW 3-802 (West 2005)

[113] ARK. CODE ANN. S. 5-71-229 (West 2005)

[114] D.C. CODE S.22-404 (2005)

จอร์เจีย ได้ระบุว่า “การติดต่อ” หมายถึง การสื่อสารใด ๆ รวมถึงแต่ไม่จำกัดการสื่อสารทางคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ[115]

นอกจากนี้กฎหมายของหลาย ๆ มลรัฐ ได้ระบุเฉพาะเจาะจงว่าการสื่อสารดังกล่าวรวมถึงลักษณะใดบ้าง เช่น อีเมล์ การสื่อสารทางคอมพิวเตอร์ หรือการสื่อสารผ่านทางระบบเครือข่าย อาทิเช่น กฎหมายอาญาของมลรัฐแคลิฟอร์เนีย [116] ได้บัญญัติรวมถึงคอมพิวเตอร์ในความหมายที่เกี่ยวกับอุปกรณ์สื่อสารทางอิเล็กทรอนิกส์ เป็นต้น ซึ่งถือว่าเป็นสัญญาณที่ดีที่หลาย ๆ รัฐได้ใส่ใจกับปัญหาอาชญากรรมรูปแบบใหม่ แต่ผลที่ เกิดขึ้นนั้น คือ ความหลากหลายของกฎหมาย และความไม่เพียงพอ รวมถึงขาดความชัดเจนทั้งในแง่คำจำกัดความ เงื่อนไข การป้องกัน และบทลงโทษ

การแก้ไขกฎหมายปัจจุบันที่เกี่ยวกับการคุกคามโดยให้ครอบคลุมถึงการสื่อสารทางอิเล็กทรอนิกส์นั้นถือว่าเป็นแนวทางที่ถูกต้องแต่ ก็ยังไม่เพียงพอ เช่น กฎหมายการปราบปรามการคุกคามของมลรัฐนิวยอร์กจะครอบคลุมการ สื่อสารทางอิเล็กทรอนิกส์ แต่ในขณะนี้สภานิติบัญญัติกำลังเสนอร่างกฎหมายที่มุ่งปราบปรามการคุกคามทางอินเตอร์เน็ตโดยตรงโดยทำให้การคุกคามดังกล่าวนั้นเป็นความผิดอาญาร้ายแรง [117] จากตัวอย่างดังกล่าวนี้ทำให้เห็นว่าการแก้ไขกฎหมายที่เกี่ยวข้องกับการคุกคามที่มีอยู่อาจจะไม่เพียงพอที่จะแก้ไขปัญหา Cyberstalking ได้และยิ่งกว่านั้นในขณะที่กฎหมายบางตัวครอบคลุมถึงการสื่อสารทางอิเล็กทรอนิกส์ แต่ภาษาที่ปรากฏในตัวกฎหมายนั้นชี้ให้เห็นว่ากฎหมายครอบคลุ มเฉพาะข้อความที่ส่งตรงให้กับเหยื่อเท่านั้น เช่น อีเมล์ที่ส่งตรงจาก Cyberstalker สู่เหยื่อ แต่กฎหมายไม่ครอบคลุมการส่ง อีเมล์ในรูปลักษณะอื่น ๆ ซึ่งกฎหมายดังกล่าวอาจจะตัดคดี Cyberstalking บางคดีออกไปเลยก็ว่าได้ เช่น คดีของ BOYER[118] ผู้คุกคามได้ตั้งเว็ บไซต์ขึ้นมาโดยทั้งเว็บไซต์นั้นได้ทำให้กับเหยื่อเพื่อการติดตามเหยื่อในทุกฝีก้าว แต่ก็ไม่เคยได้ส่งอีเมล์ไปหาเหยื่อโดยตรง และกฎหมายดังกล่าวยังไม่รวมถึงกรณีที่ผู้คุกคามลวงให้บุคคลที่สามเป็นผู้คุกคามแทน

---

[115] GA. CODE ANN. S. 16-5-90 (West 2005) (“contact” means “any communication including but not limited to communication by computer , computer network , or by any other electronic device.”)

[116] CAL. PENAL CODE S. 646.9 (West 2005)

[117] Naomi H. Goodno, “Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws ,” p. 23.

[118] Ibid., p. 24.

(10.2) ในกฎหมายที่เกี่ยวกับการคุกคามทั่วไปกำหนดให้มีเงื่อนไขของการข่มขู่ที่น่าจะเกิดขึ้นจริง (Credible Threat Requirement) หรืออะไรที่ใกล้เคียงกัน มีกฎหมายหลายฉบับกำหนดว่าการสื่อสารอิเล็กทรอนิกส์ระหว่างผู้คุกคามและเหยื่อจะต้องรวมถึงการข่มขู่อย่างเฉพาะเจาะจง ซึ่งเหมือนกับการใช้เกณฑ์การข่มขู่ที่ น่าจะเกิดขึ้นจริง (Credible Threat) บางกฎหมายนั้นเหมือนมีการใช้มาตรฐานของวิญญูชน หากแต่ศึกษาในรายละเอียดจะพบว่ามีการระบุเอาไว้ว่าจะต้องมีการข่มขู่ที่เป็นได้เกิดขึ้น (Credible Threat Requirement) เช่นในมลรัฐอลาสก้า [119] มลรัฐแคลิฟอร์เนีย [120] มลรัฐเดลาแวร์[121] มลรัฐไอโอว่า [122] มลรัฐเมนน์ [123] มลรัฐแมสซาชูเซท [124] มลรัฐนอร์ทดาโกต้า[125] มลรัฐยูท่าห์[126] และมลรัฐไวโอมมิ่ง[127]

(11) กฎหมายของมลรัฐที่ออกมาแก้ไขปัญหา Cyberstalking ยังไม่ครอบคลุมเพียงพอ

เดือนสิงหาคม ปี ค.ศ. 2006 มีเพียง 6 รัฐเท่านั้น คือ มลรัฐวอชิงตัน มลรัฐหลุยส์เซียน่า มลรัฐมิสซิสซิปปี้ มลรัฐนอร์ทคาโรไลน่า มลรัฐอิลลินอยส์ และมลรัฐโร้ดไอร์แลนด์ ที่มีกฎหมายเกี่ยวกับ Cyberstalking แต่กฎหมายนี้ก็ยังมีลักษณะที่ยังไม่สามารถแก้ไขปัญหาได้อย่างเพียงพอ เช่นกฎหมายของมลรัฐอิลลินอยส์นั้นไม่ได้บัญญัติหรือกล่าวถึงเรื่องของการลวงให้บุคคลที่สาม นั้นทำการคุกคามหรือรังควานเหยื่อ ส่วนกฎหมายของมลรัฐหลุยส์เซียน่าและมลรัฐนอร์ทคาโรไลน่าก็มีลักษณะเหมือนกัน คือ การคุกคามหรือรังควานทางอิเล็กทรอนิส์จะต้องมีการส่งข้อความไปยังบุคคลอื่น เช่นเดียวกันกับกฎหมายของมลรัฐมิ สซิสซิปปี้ที่กำหนดให้ผู้คุกคามนั้นต้องส่ง อีเมล์ไปหาเหยื่อโดยเฉพาะเจาะจง ซึ่งทำให้การระบุเช่นว่านั้นไม่สามารถแก้ไขปัญหาการลวงบุคคลที่สามให้ทำการคุกคามเหยื่อและปัญหาที่ว่าข้อความไม่เคยถูกส่งไปหาเหยื่ออย่างเช่นคดีของ Boyer ที่ข้อความอันน่าสะพรึงกลัวต่าง ๆ ได้ปรากฏอยู่บนเว็บไซต์ แต่ไม่เคยได้ถูกส่งไปให้กับเหยื่อเลย

---

[119] ALA. CODE S. 13A-6-90 (2005)

[120] D.C. CODE S.22-404 (2005)

[121] DEL. CODE ANN. tit. 11, S.1312A (2005)

[122] N.Y. PENAL LAW S. 120.55 (McKinney 2005)

[123] ME. RVE. STAT. ANN. tit. 17-A S. 210-A (2) (2005)

[124] MASS. GEN. LAWS ANN. ch 265, S.43 (West 2005)

[125] N.D. CENT. CODE. S.12.1-17-07 (2005)

[126] UTAH CODE ANN. S. 76-5-106.5 (West 2005)

[127] WYO.STAT. ANN. S. 6-2-506 (a)(ii)(2005)

(12) ปัญหาการขอคำสั่งศาลเพื่อทำการปกป้องเหยื่อ

จากการเขียนหรือร่างกฎหมายควบคุมปราบปรามการคุกคามทางอินเตอร์เน็ตทำให้เหยื่อประสบความยากลำบากในการขอคำสั่งศาลที่ห้ามมิให้ผู้คุกคามเข้าใกล้เหยื่อ เนื่องจากคำจัดความของ “การคุกคาม” โดยทั่วไปจะใช้ประกอบการออกคำสั่งปกป้องเหยื่อ ดังนั้นเมื่อถ้อยคำในกฎหมายมิได้ครอบคลุมถึงการคุกคามทางอินเตอร์เน็ต ก็อาจจะเป็นการยากที่ศาลจะออกคำสั่งปกป้องเหยื่อ และการได้มาซึ่งคำสั่งก็ยังอาจหมายถึงการได้มาซึ่งข้อมูลที่หา ยากหรือหาไม่ได้เลยอันเนื่องมาจากลักษณะที่ไม่เปิดเผยนามของผู้คุกคามนั่นเอง เช่นการยื่นคำร้องในมลรัฐอินเดียน่า เหยื่อจะต้องรู้ (1) ชื่อและที่อยู่ที่ถูกต้องของผู้คุกคามทางอินเตอร์เน็ต (2) วันเกิดหรือเลขที่ประกันสังคม (3) ที่อยู่ปัจจุบันที่ถูกต้อง ลักษณะการไม่เปิดเผยตัวของอินเตอร์เน็ตอาจทำให้เป็นการยากภายใต้กฎหมายนี้ในการได้มาซึ่งข้อมูลทั้งหมด ดังนั้นเหยื่อของการคุกคามทางอินเตอร์เน็ตอาจจะไม่สามารถที่จะได้มาซึ่งการดูแลป้องกันจากการคุกคามเช่นว่า เช่นเดียวกันในกฎหมายของมลรัฐเวอร์จิเนียก็กำหนดไว้ว่า ศาลสามารถออกคำสั่งปกป้องเหยื่อจากผู้คุกคามได้หลังจากที่มีการตัดสินคดีเกี่ยวกับการคุกคามแล้ว หรือมิฉะนั้นเหยื่อจะต้องพิสูจน์โดยใช้หลักฐานที่มีน้ำหนักเพียงพอในการพิสูจน์ว่าผู้ลงมือหรือผู้กระทำการนั้นมีความผิดในการคุกคาม ซึ่งหลักดังกล่าวนี้ก่อให้เกิดปัญห าในกรณีของ Cyberstalking เนื่องจากเป็นการยากที่กฎหมายของเวอร์จิเนียจะครอบคลุมได้ถึงผู้คุกคามทางอินเตอร์เน็ต และครอบคลุมถึงการลวงบุคคลที่สามให้กระทำการคุกคามเหยื่อแทนตน เนื่องจากกฎหมายของเวอร์จิเนียนั้นยังไม่มีความชัดเจนว่ากฎหมายนั้นครอบคลุมถึงการสื่อสารทางอิเล็กทรอนิกส์หรือไม่[128]

ดังนั้นเหยื่อของ Cyberstalking อาจจะต้องรอจนกระทั่งผู้คุกคามถูกดำเนินคดีอย่างเป็นทางการก่อนที่จะได้รับคำสั่งศาลเพื่อคุ้มครองตนเอง

โดยสรุป มีอย่างน้อยสองแนวทางในการออกกฎหมายเพื่อแก้ไขช่องว่างทางกฎหมายระดับมลรัฐ ข้อความและภาษาในกฎหมายที่บัญญัติการกระทำของผู้คุกคามควรกำหนดเกณฑ์ที่เป็นรูปธรรม (Objective) ซึ่งมุ่งเน้นไปที่ความหวาดกลัวของเหยื่อมากกว่าที่จะเป็นเกณฑ์ที่เป็นนามธรรม (Subjective) ที่มุ่งเน้นการกระทำของผู้คุกคาม [129] ดังนั้นกฎหมายที่จะจัดการการคุกคามทางอินเตอร์เน็ตจึง ควรจะใช้เกณฑ์สำหรับวิญญูชน อีกช่องทางหนึ่งสำหรับการแก้ไขปัญหาคือ การบัญญัติกฎหมายที่กำหนดให้การหลอกลวงบุคคลที่สามทำการคุกคามหรือรังควานเหยื่อแทนผู้คุกคามเป็นความผิดอาญา

---

[128] VA. CODE. ANN. S. 18.2-60.3 (West 2005)

[129] Naomi H. Goodno, “Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws,” p. 37.

(13) ปัญหาในการทำให้การคุกคามทางอินเตอร์เน็ต Cyberstalking เป็นความผิดอาญาในประเทศสหรัฐอเมริกา

(13.1) ประเด็นการพิจารณาเกี่ยวกับรัฐธรรมนูญ[130]

กฎหมายการปราบปรามการคุกคามทางอินเตอร์เน็ตควรจะตีความได้กว้างเพื่อการนำมาปรับใช้ได้อย่างมีประสิทธิภาพ แต่ไม่ควรกว้างเกินไปจนกระทบกับเสรีภาพในการพูดซึ่งได้รับการป้องกันภายใต้ First Amendment ดังนั้นการตีความกฎหมาย Cyberstalking ที่มีอยู่และการเปลี่ยนแปลงกฎหมายที่เกี่ยวข้องกับการคุกคามนั้นควรจะเกี่ยวข้องกับการกระทำที่นำมาซึ่งพฤติกรรมการคุกคามและข่มขู่[131] และกฎหมายที่เกี่ยวกับ Cyberstalking ควรมุ่งเน้นที่พฤติกรรมที่มีพื้นฐานจากการกระทำที่ มีเจตนาเฉพาะเจาะจง เช่นการส่งอีเมล์ซ้ำแล้วซ้ำเล่า (ระเบิดอีเมล์) หรือการใช้ภาษาหยาบคายลามกด้วยเจตนาคุกคามรังควานเหยื่อ

(13.2) ปัญหาการขาดแคลนข้อมูลเกี่ยวกับการคุกคามทางอินเตอร์เน็ต ในประเทศสหรัฐอเมริกานั้นมีหลายหน่วยงานที่ดำเนินการเกี่ยวกับ การจัดการคุกคามซึ่งในแต่ละมลรัฐเองนั้นได้รับข้อมูลทางสถิติที่แตกต่างกันไป เฉพาะเขตที่มีหน่วยงานที่ดูแลเรื่องอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะเท่านั้นที่รายงานสถิติเกี่ยวกับการคุกคามทางอินเตอร์เน็ต นอกจากนี้เหตุที่หน่วยงานทั้งหลายขาดข้อมูลเกี่ยวกับ Cyberstalking ก็เป็นเพราะเหยื่อจากการถูกคุกคามทางอินเตอร์เน็ตหลายรายไม่ได้แจ้งหรือให้ข้อมูลกับหน่วยงานทางกฎหมาย และอีกส่วนหนึ่งเป็นเพราะหน่วยงานทางกฎหมายไม่มีบุคลากรที่ได้รับการฝึกฝนเกี่ยวกับเรื่องนี้อย่างเพียงพอ แต่ในทางตรงกันข้ามหน่วยงานที่ไม่แสวงหากำไรเช่น องค์กร CyberAngles องค์กรที่ไม่แสวงหากำไรที่คอยช่วยเหลือเหยื่อจากการถูกคุกคามทางอินเตอร์เน็ตได้ให้ข้อมูลประมาณการว่ามีผู้คุกคามทางอินเตอร์เน็ต หรือ Cyberstalker จำนวน 63,000 คนในประเทศสหรัฐอเมริกา และ 474,000 คนทั่วโลก[132]

จากการศึกษาวิเคราะห์ปัญหาจากม าตรการทางกฎหมายของสหรัฐอเมริกาพบว่า แม้ประเทศสหรัฐอเมริกาจะมีบทบัญญัติของกฎหมายเรื่อง Cyberstalking แต่ประเทศสหรัฐอเมริกาเอง ก็ยังไม่สามารถให้คำจำกัดความของ Cyberstalking ได้เป็นหนึ่งเดียวกัน และมีเพียงแค่ 6 มลรัฐเท่านั้นที่บัญญัติกฎหมาย Cyberstalking ออกมา ส่วนมลรัฐอื่น ๆ

---

[130] Ibid., p.39.

[131] AM. Civil Liberties Union v. Reno , 521 U.S. 844 (1997) (holding that the Internet is an important tool for protected speech activities)

[132] Naomi H. Goodno, “Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws ,” p. 41.

ก็ใช้ลักษณะการเทียบเคียงกฎหมาย Stalking Law ที่มีอยู่หากมีการกระทำความผิดเกิดขึ้น นอกจากนี้แม้บางมลรัฐเองจะมีกฎหมายเกี่ยวกับ Cyberstalking ออกมาแต่กฎหมายก็ไม่ได้บัญญัติครอบคลุมปัญหาที่เกิดขึ้น เช่น ปัญหาของการลวงบุคคลที่สามให้คุกคามเหยื่อแทน หรือบางมลรัฐเองการพิจารณาองค์ประกอบของความผิดนั้นผู้เสียหายหรือเหยื่อนั้นต้องพิสูจน์ให้ได้ว่า ผู้คุกคามนั้นสามารถกระทำการคุกคามได้ตามที่ข่มขู่ไว้จริง และที่สำคัญคือบางครั้งผู้ที่เป็นเหยื่อไม่รู้ด้วยซ้ำว่าใครคือผู้คุกคาม หรือผู้คุกคามนั้นอยู่ที่ไหน ซึ่งในเรื่องของไซเบอร์การพิสูจน์ถึงการกระทำนั้นเป็นเรื่องยาก จึงเห็นได้ว่าแม้ในประเทศที่มีกฎหมายเฉพาะเกี่ยวกับ Cyberstalking เองก็ไม่ได้แก้ไขปัญหาดังกล่าวได้ครอบคลุมทั้งหมด ผู้ศึกษาเห็นว่าเราจึงควรศึกษากฎหมายของไทยที่มีอยู่ว่าเพียงพอที่จะรองรับหรือแก้ไขปัญหาเฉพาะหน้าที่อาจเกิดขึ้นได้มากน้อยเพียงใดเพื่อเป็นการนำมาปรับปรุงแก้ไขหรือจำเป็นต้องมีการบัญญัติกฎหมายเกี่ยวกับ Cyberstalking ออกมาเป็นการเฉพาะอย่างประเทศสหรัฐอเมริกา

4.2 บทวิเคราะห์กฎหมายไทยที่นำมาใช้กับการคุกคามทางอินเตอร์เน็ต

เมื่อศึกษาปัญหาการคุกคามทางอินเตอร์เน็ตที่เกิดขึ้นแล้วนั้น ทำให้เห็นว่าสำหรับประเทศไทยนั้นยังไม่มีกฎหมายที่ออกมาเพื่อปัญหาการคุกคามทางอินเตอร์เป็นกฎหมายเฉพาะอย่างประเทศสหรัฐอเมริกา ซึ่งบทบัญญัติของกฎหมายของประเทศไทยที่สามารถนำมาปรับใช้ได้กับการคุกคามทางอินเตอร์ เน็ต คือ ประมวลกฎหมายอาญามาตรา 326 328 และ 392 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ .ศ. 2550 และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .....

สำหรับประเทศไทยการคุกคามทางอินเตอร์เน็ตถือเป็นอาชญากรรมแนวใหม่ที่แฝงมากับอิน เตอร์เน็ต และเป็นการเปลี่ยนรูปแบบของการกระทำความผิดตามความเจริญก้าวหน้าทางด้านเทคโนโลยีที่เปลี่ยนแปลงไป ดังนั้นจากการศึกษากฎหมายของไทยโดยรวมแล้วพบว่ายังคงมีปัญหาที่ต้องพิจารณาว่ากฎหมายที่มีอยู่แล้วในปัจจุบันจะสามารถรองรับกับปัญหาการคุกคามทางอินเตอร์เน็ตได้เพียงใด

ในปัจจุบันการกระทำหรือการดำเนินการต่าง ๆ บนโลกของอินเตอร์เน็ตที่สร้างความเสียหายให้กับบุคคลและสังคมนั้นถือเป็นความผิดหรือไม่ ทำให้ปัญหาที่ตามมาคือรูปแบบของการกระทำต่าง ๆ ที่เกิดขึ้นนั้นกฎหมายที่จะนำมาใช้จะมีผลครอบคลุม หรือลงโทษผู้กระทำความผิดได้หรือไม่ ซึ่งปัญหาที่จะควรนำมาพิจารณาก็คือ

4.2.1 ปัญหาการปรับใช้กฎหมายของไทยกับปัญหาการคุกคามทางอินเตอร์เน็ต

1. ประมวลกฎหมายอาญา

กฎหมายที่มีอยู่มีบทลงโทษที่เหมาะสมกับปัญหาที่เกิดขึ้นหรือไม่ สำหรับกฎหมายอาญาที่สามารถนำมาปรับใช้ได้คือ มาตรา 326 328 และ 392 ในความเป็นจริงแล้วพฤติกรรมของการคุกคามทางอินเตอร์เน็ตที่เกิดขึ้นนั้นหากเป็นการคุกคามที่ไม่รุนแรงหรือคุกคามต่อการใช้ชีวิตประจำวันหรือคุกคามถึงความปลอดภัยต่อชีวิตและทรัพย์สินของเหยื่อแล้ว การคุก คามทางอินเตอร์เน็ตอาจเป็นเพียงแค่การสร้างความเดือดร้อนรำคา ญให้กับผู้ถูกคุกคามหรือเหยื่อเท่านั้น ดังนั้นกฎหมายที่จะนำมาลงโทษผู้กระทำความผิดได้ก็มีเพียงกฎหมายอาญามาตรา 392 คือความผิดลหุโทษ ซึ่งอัตราโทษที่กฎหมายกำหนดไว้คือ จำคุกไม่เกินหนึ่งเดือน ปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ เมื่อพิจารณาถึงโทษของการ กระทำความผิดแล้วจะเห็นว่าเป็นอัตราโทษที่ต่ำไม่สามารถทำให้ผู้กระทำความผิดเกิดความเกรงกลัว หรือเกิดความยับยั้งชั่งใจในการกระทำความผิดได้

1.2 กฎหมายที่มีอยู่นั้นเหมาะสมหรือไม่กับส ภาพของสังคมในปัจจุบัน และสามารถ สะท้อนกลับต่อการพัฒนาการกระทำความผิดในรูปแบบให ม่ ๆ ได้หรือไม่ เนื่องจากมีการใช้อินเตอร์เน็ตเป็นเครื่องมือในการกระทำความผิด โดยอาศัยคุณสมบัติพิเศษของอินเตอร์เน็ต คือ การไม่เปิดเผยตัวของอินเตอร์เน็ตในการประกอบอาชญากรรมต่าง ๆ ทำให้ยากแก่การที่จะจับกุมตัวผู้กระทำความผิด และเมื่อพิจารณาความเสียหายที่เกิดขึ้ น จากการคุกคามนั้นสร้างความเสียหายได้อย่างมากมายมหาศาล แต่กฎหมายที่มีอยู่นั้นไม่เหมาะสมกับการกระทำความผิดที่เปลี่ยนแปลงไปและมีรูปแบบขององค์ประกอบการกระทำความผิดที่เปลี่ยนแปลงไป ซึ่งทำให้กฎหมายที่มีอยู่ไม่สามารถลงโทษผู้กระทำความผิดได้เต็มที่เหมาะสมกับควา มเสียหายที่เกิดขึ้น นอกจากนี้ทำให้เกิดช่องว่างทางกฎหมาย เมื่อองค์ประกอบในการกระทำความผิดได้เปลี่ยนแปลงไปตามความเจริญก้าวหน้าทางเทคโนโลยี จึงทำให้พฤติกรรมของการกระทำความผิดบางอย่างนั้นไม่เป็นความผิดตามกฎหมายอีกต่อไป เมื่อขาดองค์ประกอบในการกระทำความผิดแ ล้วจึงไม่สามารถลงโทษผู้กระทำความผิดได้ จึงทำให้กฎหมายที่มีอยู่ในปัจจุบันไม่มีประสิทธิภาพเพียงพอในการลงโทษผู้กระทำความผิด

1.3 บทบัญญัติของกฎหมาย เช่นกฎหมายอาญามาตรา 392 เองนั้นเป็นกฎหมายที่ได้บัญญัติตั้งแต่ ปี พ .ศ. 2499 ซึ่งในอดีตนั้นยังไม่ปราก ฏสภาพปัญหาดังเช่นในปัจจุบัน จึงทำให้การบัญญัติโทษทางกฎหมายนั้นไม่มีความรุนแรงแต่เมื่อสภาพปัญหาที่เกิดขึ้นได้เปลี่ยนแปลงไปตามความก้าวหน้าทางเทคโนโลยีจึงทำให้กฎหมายมาตรา

ดังกล่าวนี้กลายเป็นกฎหมายเก่าที่ไม่สามารถป้องกันและลงโทษผู้กระทำความผิดให้เกิดความเกรงกลัวได้ ดังนั้นจึงเป็นการสมควรที่จะต้องแก้ไขบทลงโทษให้มากขึ้นเพื่อเป็นการยับยั้งการกระทำความผิดและลงโทษผู้กระทำความผิดให้เข็ดหลาบ

1.4 กฎหมายที่มีอยู่นั้นสามารถนำมาใช้ได้ในลักษณะของการเทียบเคียงเพื่อลงโทษผู้กระทำความผิดเท่านั้น เนื่องจากยังไม่มีกฎหมายที่บัญญัติเกี่ยวกับการคุกคามทางอินเตอร์เน็ตไว้เป็นการเฉพาะที่สามารถนำมาลงโทษผู้กระทำความผิดได้ และการคุกคามทางอินเตอร์เน็ตนั้นไม่มีลักษณะของการกระทำทางกายภาพซึ่งอาจทำให้เกิดความรำคาญเท่านั้นจึงทำให้กฎหมายอาญามาตรา 392 นั้นไม่สามารถนำมาลงโทษผู้กระทำความผิดได้เต็มที่ และการกระทำบางอย่างซึ่งอาจถือได้ว่าเป็นการคุกคามแบบหนึ่ง เช่น การส่งสแปมเมลให้กับบุคคลใดบุคคลหนึ่งกฎหมายไม่ถือว่า เป็นการกระทำความผิดแต่อย่างใด จึงทำให้ผู้กระทำความผิดนั้นไม่ต้องได้รับโทษ

1.5 การกระทำความผิดนั้นหากอยู่ในรูปแบบของการลวงให้บุคคลที่ สามทำการคุกคามเหยื่อแทนอย่างเช่นกรณีที่เกิดขึ้นในประเทศสหรัฐอเมริกาแล้วกฎหมายอาญาของไทยที่มีอยู่บัญญัติไม่ครอบคลุมถึงการกระทำความผิดในลักษณะดังกล่าว ซึ่งหากเกิดการกระทำในลักษณะนี้แล้วกฎหมายอาญาของไทยก็ยังไม่สามารถลงโทษผู้กระทำความผิดได้ เช่นเดียวกันกับประ เทศสหรัฐอเมริกาที่กฎหมายยังไม่ได้บัญญัติให้การกระทำในรูปแบบนี้เป็นความผิดอาญายกเว้นเพียงมลรัฐเดียว คือ โอไฮโอ ที่บัญญัติให้เป็นความผิดอาญา

2. ประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยลักษณะละเมิด มาตรา 420

การคุกคามทางอินเตอร์เน็ตนอกจากจะเป็นการรุกล้ำสิทธิ ส่วนตัวของบุคคลแล้วยังเป็นการกระทำที่สามารถสร้างความเสียหายให้กับผู้ที่ตกเป็นเหยื่อได้ไม่มากก็น้อย ตั้งแต่การสร้างความเดือดร้อนรำคาญให้กับผู้ที่ตกเป็นเหยื่อ รบกวนการใช้ชีวิตประจำวันอย่างปกติสุข จนถึงการสร้างความอันตรายให้แก่ร่างกายหรือทรัพย์สินหรือมีกา รคุกคามจนถึงแก่ชีวิต ซึ่งผู้ที่ตกเป็นเหยื่อนั้นไม่สามารถดำรงชีวิตได้อย่างคนปกติทั่วไป ซึ่งบางครั้งผู้ที่เป็นเหยื่อนั้นไม่สามารถทราบได้ว่าผู้ที่คุกคามตนเองนั้นเป็นใคร ทำให้ส่งผลกระทบต่อจิตใจกับเหยื่อ ซึ่งถือว่าเป็นการกระทำละเมิด เหยื่ออาจจะอาศัยมาตร า 420 ในเรื่องของการทำละเมิดเรียกร้องค่าเสียหายที่เกิดขึ้น หากแต่ค่าเสียหายที่เรียกร้องนั้นจะต้องเป็นค่าเสียหายที่เกิดขึ้นจริงจากการถูกคุกคาม

บางครั้งการคุกคามที่เกิดขึ้นนั้นมิได้เป็นอันตรายต่อร่างกาย ชีวิต หรือทรัพย์สิน หากการคุกคามที่เกิดขึ้นนั้นส่งผลกระทบต่อจิตใจกับผู้ที่เป็นเหยื่อไม่สามารถดำรงชีวิตหรือใช้ชีวิตได้อย่างคนปกติทั่วไป สร้างความลำบากต่อเหยื่อ ๆ อาจจะต้องเสียค่าใช้จ่ายในการป้องกันตนเองจากการถูกคุกคามไม่ว่าโดยวิธีใดวิธีหนึ่ง

ดังนั้นในส่วนของการเรียกร้องค่าเสียหายในกรณีที่ถูกคุกคามแล้ว เกิดความเสียหายแก่จิตใจกฎหมายยังไม่สามารถระบุหรือตีราคาเป็นค่าความเสียหายที่เกิดขึ้นกับจิตใจได้ เนื่องจากประเทศไทยยังไม่มีการกำหนดค่าเสียหายในเชิงลงโทษ (Punitive Damages) ดังเช่นต่างประเทศ จึงทำให้การเรียกร้องค่าเสียหายเพื่อเป็นการชดเชยความเสียหายให้กับเหยื่อนั้นจึงเป็นการยาก

3. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550[133]

พระราชบัญญัติฉบับดังกล่าว เป็นพระราชบัญญัติที่ออกมาเฉพาะเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งมีการประกาศในราชกิจจานุเบกษาเมื่อวันที่ 18 มิถุนายน 2550 และให้มีผลบังคับใช้หลังจากประกาศในราชกิจจานุเบกษาแล้ว 30 วัน

พระราชบัญญัติฉบับดังกล่าวแบ่งออกเป็น 2 หมวด โดยหมวดแรกกำหนดเกี่ยวกับฐานความผิดและบทลงโทษเกี่ยวกับคอมพิวเตอร์มี 13 มาตรา คือตั้งแต่มาตรา 5 ถึงมาตรา 17 โดยมาตรา 5 ถึงมาตรา 12 เป็นบทบัญญัติที่กำหนดลักษณะของการกระทำความผิดซึ่งกระทบโดยตรงต่อการรักษาความลับ (Confidentiality) ความครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

สำหรับการกระทำความผิดที่กระทบต่อการรักษาความลับเช่นการเข้าถึงระบบคอมพิวเตอร์ของบุคคลอื่นซึ่งมีมาตรการป้องกันการเข้าถึงไว้ (มาตรา 5) การล่วงรู้มาตรการการป้องกันการเข้าถึงระบบคอมพิวเตอร์ การเข้าถึงข้อมูลของบุคคลอื่น (มาตรา 7) หรือการดักข้อมูลคอมพิวเตอร์ (มาตรา 8)

ส่วนการกระทำความผิดที่กระทบต่อความครบถ้วน ของระบบคอมพิวเตอร์ เช่น การรบกวนการทำงานของข้อมูลคอมพิวเตอร์ด้วยการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมข้อมูลคอมพิวเตอร์ (มาตรา 9) เป็นต้น

สำหรับการกระทำความผิดที่กระทบต่อสภาพพร้อมใช้งานตามปกติของระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ เช่นกา รกระทำความผิดด้วยการป้อนชุดคำสั่งหรือโปรแกรมคอมพิวเตอร์ที่ไม่พึงประสงค์ เช่น ไวรัส เพื่อให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้ตามปกติ (มาตรา 10) รวมถึงการส่งจดหมายอิเล็กทรอนิกส์ (Spam Mail) ที่เป็นการรบกวนการใช้งานของคนทั่วไป (มาตรา 11) อย่างไรก็ตามสำหรับการรบกวนระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้นมีการกำหนดบทโทษหนักขึ้นด้วยกรณี การกระทำความผิดก่อให้เกิดความเสียหายแก่ข้อมูลคอมพิวเตอร์หรือกระทบต่อความมั่นคงความปลอดภัยของของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ การ

---

[133] โปรดดูภาคผนวก.

บริการสาธารณะ หรือการกระ ทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ หรือการกระทำดังกล่าวก่อให้เกิดอันตรายแก่ร่างกายหรือชีวิตประชาชน ผู้กระทำความผิดในลักษณะดังกล่าวจะต้องได้รับโทษหนักขึ้น

นอกจากนั้น ยังได้มีการกำหนดฐานความผิดสำหรับการจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นเพื่อใช้เป็นเครื่องมือในการกระทำความผิดที่กล่าวมาข้างต้น เช่นการจงใจหรือเจตนาเผยแพร่ไวรัสที่ใช้ในการก่อให้เกิดความเสียหายหรือทำลายข้อมูลคอมพิวเตอร์ หรือชุดคำสั่งหรือชุดคำสั่งที่เรียกว่า Spy Ware เพื่อใช้โจรกรรมความลับทางการค้า เป็นต้น (มาตรา 13)

ส่วนพระราชบัญญัติตั้งแต่มาตรา 14 ถึงมาตรา 17 นั้นจะเป็นลักษณะของการกระทำความผิดที่เกี่ยวเนื่องกับการใช้คอมพิวเตอร์ในทางมิชอบเพื่อกระทำความผิดในลักษณะต่าง ๆ เช่นการปลอมแปลงข้อมูลคอมพิวเตอร์ การเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จซึ่งก่อให้เกิดความตื่นตระหนกกับประชาชน การเผยแพร่ข้อมูลอันมีลักษณะลามก การกระทำความผิดของผู้ให้บริการที่มิได้ลบข้อมูลคอมพิวเตอร์อันไม่เหมาะสม การตัดต่อภาพทำให้บุคคลเสียหาย เป็นต้น

ส่วนหมวดที่สองจะกำ หนดเกี่ยวกับพนักงานเจ้าหน้าที่ มีทั้งสิ้น 13 มาตรา ตั้งแต่ มาตรา 18 ถึงมาตรา 30 โดยกำหนดอำนาจของพนักงานเจ้าหน้าที่และคุณสมบัติของเจ้าพนักงานเอาไว้ ดังนี้

อำนาจของพนักงานเจ้าหน้าที่

พนักงานเจ้าหน้าที่มีอำนาจสั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวให้ แก่พนักงานเจ้าหน้าที่ทำสำเนาข้อมูลคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่ต้องสงสัย ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ถอดรหัสข้อมูลคอมพิวเตอร์ เรียกข้อมูลจราจรทางคอมพิวเตอร์และยึดหรืออายัดระบบคอมพิวเตอร์ (มาตรา 18) ทั้งนี้การใช้อำนาจดังกล่าวจะต้องกระทำ เท่าที่จำเป็นเพื่อป้องกันและปราบปรามการกระทำความผิดตามพระราชบัญญัติเท่านั้น (มาตรา 19)

นอกจากนี้ในปัจจุบันได้มีการพัฒนาชุดคำสั่งหรือโปรแกรมไม่พึงประสงค์มากมาย เช่น ไวรัส (Virus) เวิร์ม (Worm) สปายแวร์ (Spyware) และอื่น ๆเป็นจำนวนมากมาย ซึ่งเป็นการพั ฒนาตามความก้าวหน้าทางเทคโนโลยี การพัฒนาดังกล่าวนั้นมีทั้งคุณและโทษในขณะเดียวกัน การแก้ไขปัญหาและป้องกันปัญหาจึงไม่สามารถดำเนินการได้โดยง่ายพระราชบัญญัติฉบับดังกล่าวจึงได้กำหนดอำนาจของพนักงานเจ้าหน้าที่เอาไว้ให้อำนาจพนักงานเจ้าหน้าที่ในการสั่งห้ามจำหน่าย เผยแพร่ หรืออาจกำหนดเงื่อนไขการใช้

หรือมีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งดังกล่าวด้วยก็ได้ แต่ด้วยลักษณะที่เป็นคุณของชุดคำสั่งที่ไม่พึงประสงค์นั้นจึงทำให้มีข้อยกเว้นว่า การใช้อำนาจของพนักงานเจ้าหน้าที่ในการสั่งการกับชุดคำสั่งไม่พึงประสงค์นั้นมิให้รวมถึง ชุดคำสั่งที่พัฒนาขึ้นมาเพื่อแก้ปัญหาหรือป้องกันชุดคำสั่งดังกล่าว โดยให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีและการสื่อสารมีอำนาจในการประกาศว่าชุดคำสั่งใดบ้างเป็นชุดคำสั่งไม่พึงประสงค์ (มาตรา 21)

การตรวจสอบการใช้อำนาจ

ในการใช้อำนาจของพนักงานเจ้าหน้าที่ในการตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานในการกระทำความผิด หรือการสืบสวนหาตัวผู้กระทำความผิด และการเรียกข้อมูลจราจรคอมพิวเตอร์อันเป็นการบันทึกการเข้าออกจากระบบของผู้ใช้บริการที่ผู้ให้บริการเก็บรักษาไว้อันเป็นหลักฐานสำคัญในการสืบหาตัวผู้กระทำความผิด ซึ่งไม่รวมถึงข้อมูลที่บุคคลติดต่อกัน (มาตรา 18 (2)) พนักงานเจ้าหน้าที่ต้องบันทึกรายละเอียดการดำเนินการและเหตุผลในการดำเนินการ รายงานต่อศาลที่มีเขตอำนาจหรือศาลอาญาภายใน 48 ชั่วโมงนับแต่เวลาลงมือดำเนินการ ทั้งนี้ศาลมีอำนาจใช้ดุลพินิจที่จะสั่งระงับการดำเนินการดังกล่าวได้หากเห็นว่าเกินความจำเป็น (มาตรา 19 วรรคสาม)

นอกจากนี้พระราชบัญญัติฉบับดังกล่าวได้ให้อำนาจพนักงานเจ้าหน้าที่ในการรวบรวมพยานหลักฐานหาตัวผู้กระทำความผิด โดยเฉพาะอย่างยิ่งการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรคอมพิวเตอร์ (มาตรา 18 (6)) ซึ่งอาจกระทบความเป็นส่วนตัว ความลับทางการค้า หรือการติดต่อสื่อสาร จึงต้องมีการควบคุมการใช้อำนาจของพนักงานเจ้าหน้าที่ โดยพระราชบัญญัติฉบับดังกล่าวกำหนดห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรคอมพิวเตอร์หรือข้อมูลของผู้ให้บริการให้กับบุคคลหนึ่งบุคคลใด (มาตรา 22 วรรคหนึ่ง) เว้นแต่เพื่อประโยชน์ในการดำเนินคดีตามพระราชบัญญัติ การใช้อำนาจในทางมิชอบของพนักงานเจ้าหน้าที่ และการกระทำตามคำสั่งศาลในการพิจารณาคดี (มาตรา 22 วรรคสอง)

คุณสมบัติของเจ้าพนักงานหน้าที่

พระราชบัญญัติได้กำหนดให้เจ้าหน้าที่ต้องมีคุณสมบัติพิเศษ คือ มีความรู้ความชำนาญด้านคอมพิวเตอร์ผ่านหลักสูตรที่รัฐมนตรีว่าการกระทรวงเทคโนโลยีและการสื่อสารกำหนด (มาตรา 28)

หน้าที่ของผู้ให้บริการในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

สิ่งสำคัญในการหาตัวผู้กระทำความผิด คือ ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งถือเป็นพยานหลักฐานที่สำคัญ ในพระราชบัญญัติฉบับดังกล่าวจึงกำหนดให้ผู้ให้บริการเก็บข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวไว้ไม่น้อยก ว่า 90 วัน และในกรณีที่จำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกิน 90 วันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษก็ได้ อีกทั้งผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้อบ ริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บไว้เป็นเวลาไม่น้อยกว่า 90 วันนับตั้งแต่การใช้บริการสิ้นสุดลง (มาตรา 26) หากผู้ให้บริการใดไม่ปฏิบัติตามหน้าที่ที่กำหนดไว้ต้องระวางโทษตามที่กฎหมายกำหนด (มาตรา 26 วรรคสี่)

สำหรับปัญหาการคุกคามทางอินเตอร์เน็ตนั้น พระราชบัญญัติฉบับดังกล่าวสามารถนำมาใช้แก้ปัญหาการคุกคามทางอินเตอร์เน็ตได้แค่พียงบางประเด็นเท่านั้นตามมาตรา 14 (1) (4) เนื่องจากตามพระราชบัญญัติฉบับดังกล่าวนั้นมิได้บัญญัติถึงการคุกคามทางอินเตอร์เน็ต ไว้เป็นการเฉพาะ มาตราดังกล่าวบัญญัติเฉพาะกรณีการนำเข้า สู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลอันเป็นเท็จ เช่น การส่งอีเมล์ให้กับเหยื่อในเรื่องการตาย การบาดเจ็บ หรือการกระทำที่ไม่เหมาะสม หรือกรณีของการลงข้อความอันเป็นเท็จที่สร้างความเสียหายให้กับเหยื่อ หรือการลงข้อความต่าง ๆที่ไม่จริงเกี่ยวกับเหยื่อทำให้เหยื่อได้รับความเสียหายเป็นอันตรายต่อร่างกาย ชีวิตหรือทรัพย์สิน ก็สามารถนำมาตรา 14 (1) มาใช้เนื่องจากการลงข้อความอันเป็นเท็จหรือข้อความที่อาจทำให้เหยื่อนั้นได้รับความเสียหายถูกดูหมิ่นเกลียดชังต่าง ๆ เหล่านี้นั้น เป็ นการคุกคามที่กระทำได้ง่ายและสามารถสร้างความเสียหายได้ในวงกว้าง เนื่องจากอินเตอร์เน็ตนั้นไม่จำกัดเฉพาะบุคคล หรือกลุ่มคน เท่านั้น หรือการส่งภาพลามกอนาจาร หากผู้กระทำความผิดนั้นต้องการที่จะคุกคามเหยื่อโดยการส่งภาพลามกอนาจาร หรือนำรูปของเหยื่อไปตัดต่อกับรูปลามกอนาจารต่าง ๆ แล้วส่งให้กับเหยื่อหรือทำการลง (Post) ภาพลามกอนาจารนั้นลงบนเว็บไซต์ต่าง ๆ เพื่อให้เหยื่อนั้นได้รับความอับอายหรือถูกดูหมิ่นเกลียดชัง ก็สามารถนำมาตรานี้มาปรับใช้เทียบเคียงและลงโทษผู้กระทำความผิดได้เช่นเดียวกัน

4. ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ[134].....

ในปัจจุบันประเทศไทยมีการคุ้มครองส่วนบุคคลโดยบทบัญญัติของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ .ศ. 2540 แต่เนื่องจากใช้บังคับเฉพาะในหน่วยงานของรัฐเท่านั้น ไม่ครอบคลุมถึงข้อมูลส่วนบุคคลที่อยู่ในภาคเอกชน เช่นข้อมูลในธนาคารพ าณิชย์ ข้อมูลในโรงพยาบาลเอกชน ข้อมูลของพนักงานลูกจ้างบริษัทห้างร้านเอกชนต่าง ๆ บรรดาข้อมูลลูกค้าหรือข้อมูลทางกิจกรรมทางธุรกิจ หรือข้อมูลการเป็นสมาชิกบัตรต่าง ๆ นอกจากนี้ในปัจจุบันปัญหาการล่วงละเมิดข้อมูลส่วนบุคคลมีอยู่เป็นจำนวนมาก โดยเฉพาะการนำไปใช้ ประโยชน์ เปิดเผยหรือเผยแพร่จนทำให้ได้รับความเสียหาย ดังนั้นเพื่อเป็นการคุ้มครองและลดช่องว่างของกฎหมายที่มีอยู่ จึงควรมีกฎหมายที่มีลักษณะเป็นกลาง เพื่อขยายขอบเขตการคุ้มครองสิทธิเสรีภาพให้ครอบคลุมข้อมูลส่วนบุคคลทั้งหมดโดยเฉพาะ

ในหลายประเทศตระหนักถึงคว ามสำคัญและความจำเป็นในการออกกฎหมายหรือแนวทางต่าง ๆ ในการให้ความคุ้มครองข้อมูลส่วนบุคคลความเป็นส่วนตัวของประชาชนทั้งในระดับประเทศและความร่วมมือระหว่างประเทศ ฉะนั้นประเทศไทยจึงมีความจำเป็นที่จะต้องบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยมีเหตุผลสำคัญ คือ[135]

(1) ในปัจจุบันสังคมไทยยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ทำให้ไม่มีหลักประกันในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐาน ในขณะที่หลายประเทศในแถบยุโรป อเมริกาใต้ ได้มีบทบั ญญัติกฎหมายเพื่อมาคุ้มครองข้อมู ลส่วนบุคคลและเยียวยาความเสียหายอันเกิดจากการละเมิดความเป็นส่วนตัว

(2) จัดสร้างกลไกในการปกป้องข้อมูลส่วนบุคคล รักษาดุลยภาพของการคุ้มครองข้อมูลส่วนบุคคลในความเป็นส่วนตัว (Right of Privacy) เสรีภาพในการไหลเวียนของข้อมูลข่าวสาร (Free Flow of Information) และความมั่นคงของประเทศ (National Security) เพื่อเป็นโครงสร้างพื้นฐานสารสนเทศที่มั่นคงในยุคแห่งข้อมูลข่าวสาร และในการปกครองระบอบประชาธิปไตย เนื่องจากเป็นกฎหมายที่อยู่บนพื้นฐานเทคโนโลยีสารสนเทศ จึงมีความจำเป็นที่จะต้องอาศัยผู้เชี่ยวชาญในเทคโนโลยีดังกล่าว

(3) เพื่อสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ ในปัจจุบันการพัฒนาการ

---

[134] โปรดดูภาคผนวก.

[135] วิจารณ์ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ....., http://gotoknow.org/blog/LA641/64031.

ทางเทคโนโลยีสารสนเทศมีความก้าวหน้าอย่างรวดเร็ว ทำให้มีการนำเอาเทคโนโลยีมาประยุกต์ใช้ให้เกิดประโยชน์กับเศรษฐกิจและสังคมมากมาย โดยเฉพาะการประมวลผลข้อมูลส่วนบุคคลอันสามารถทำได้อย่างสะดวกรวดเร็ว จึงมีความจำเป็นที่จะต้องออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีการใช้อันอย่างแพร่หลายในยุคสังคมสารสนเทศ

สาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล[136]

หลักการประมวลผลข้อมูล

ร่างพระราชบัญญัติฉบับนี้ได้กำหนดวิธีการประมวลผลข้อมูลส่วนบุคคล สามารถกระทำได้โดยวิธีการอิเล็กทรอนิกส์ วิธีการอัตโนมัติ หรือวิธีการอื่นใดซึ่งหมายถึงวิธีที่มิใช่วิธีการทางอิเล็กทรอนิกส์ ในการจัดเก็บรวบรวม บันทึก จัดหมวดหมู่ โดยจะกระทำมิได้เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลและภายใต้วัตถุประสงค์การประมวลผล

ผู้ควบคุมข้อมูล

ร่างพระราชบัญญัตินี้ได้กำหนดใ ห้ผู้ควบคุมข้อมูลมีหน้าที่ต้องเก็บรวบรวมข้อมูลเท่าที่จำเป็นวัตถุประสงค์ที่จะใช้หรือเปิดเผย ข้อมูลที่จะใช้หรือเปิดเผยจะต้องถูกต้องครบถ้วน การเก็บรวบรวมข้อมูลต้องมีการกำหนดวัตถุประสงค์อย่างใดอย่างหนึ่งที่แน่นอนชัดเจน ในกรณีที่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลแตกต่างไปจากวัตถุประสงค์ที่เก็บรวบรวมข้อมูลไม่สามารถกระทำได้ เว้นแต่ได้รับความยินยอมของเจ้าของข้อมูลหรือผู้แทน หรือโดยอำนาจของกฎหมาย รักษาความปลอดภัยข้อมูลส่วนบุคคล ต้องเปิดเผยข้อมูลทั่วไปเกี่ยวกับการเก็บรวบรวม การเก็บรักษา และการใช้ข้อมูลส่วนบุคคล ยอมรับสิทธิในการเข้าถึงและสิทธิในการแก้ไขข้อมูลของเจ้าของข้อมูลส่วนบุคคล

การประมวลผลข้อมูล

ร่างพระราชบัญญัตินี้ได้กำหนดให้มีการประมวลผลโดยชอบ และกำหนดวัตถุประสงค์ ขอบเขต ระยะเวลา ฯลฯ โดยชัดแจ้ง นอกจากนี้ยังกำหนดให้พยายามที่จัดเก็บข้อมูลโดยตรงจากเจ้ าของข้อมูล รวมถึงการประมวลผลโดยมิได้รับความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้งจะกระทำมิได้เว้นแต่มีกฎหมายอื่นกำหนดเป็นการเฉพาะผูกพันตามสัญญาเพื่อการวิจัย ฯ

การคุ้มครองเจ้าของข้อมูล

ร่างพระราชบัญญัตินี้ได้กำหนดสิทธิของเจ้าของข้อมูล คือสิทธิในการรับทราบรายละ เอียดบางประการ เช่น สิทธิในการรับแจ้งวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล สิทธิในการเข้าถึงเพื่อตรวจสอบและแก้ไขข้อมูลส่วนบุคคลของตนเอง สิทธิในการร้องเรียนต่อคณะกรรมการและการเรียกร้องค่าเสียหาย

---

[136] เรื่องเดียวกัน.

ความปลอดภัยของข้อมูลที่มีการประมวลผล

ร่างพระราชบัญญัติ ฉบับนี้กำหนดให้ข้อมูลส่วนบุคคลต้องได้รับการประมวลผล จัดเก็บและควบคุมโดยคำนึงถึงมาตรฐานทางเทคโนโลยี และมาตรการความปลอดภัยอย่างเหมาะสม โดยต้องเป็นขั้นต่ำที่คณะกรรมการประกาศกำหนด และการประมวลผลสิ้นสุดลงเมื่อผู้ประมวลผลหยุดการประมวลผลและผู้ควบคุมได้แจ้งให้คณะกรรมการทราบ

การเปิดเผยข้อมูลโดยทั่วไปและการเปิดเผยข้อมูลเฉพาะเจาะจง

ร่างพระราชบัญญัตินี้ได้กำหนดมิให้เปิดเผยข้อมูลส่วนบุคคลที่มีการประมวลผลโดยทั่วไปและโดยเฉพาะเจาะจง โดยปราศจากความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง เว้นแต่เข้ากรณียกเว้นที่สามารถกระทำได้

ข้อมูลห้ามประมวลผล

ร่างพระราชบัญญัติกำหนดให้ข้อมูลบางประเภทไม่สามารถประมวลผลได้เว้นแต่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและได้รับอนุญาตจากคณะกรรมการ

การส่งและโอนข้อมูลไปประเทศอื่น

ร่างพระราชบัญญัตินี้ได้กำหนดให้การส่งหรือโอนข้อมูลส่วนบุ คคลไปนอกราชอาณาจักรนั้นจะกระทำมิได้ เว้นแต่ผู้ควบคุมจะแจ้งให้คณะกรรมการทราบ และห้ามส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศที่มิได้มีบทบัญญัติในการให้ความคุ้มครองข้อมูลส่วนบุคคล ยกเว้นว่าจะได้รับความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้งหรือเพื่อประโยชน์สาธารณะ

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ร่างพระราชบัญญัติกำหนดให้มีคณะกรรมการที่เรียกว่าคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีคุณวุฒิหลายสาขา กำหนดคุณสมบัติของคณะกรรมการ และการพ้นจากตำแหน่งของคณะกรรมการ รวมถึงอำนาจหน้าที่ของคณะกรรมการ เช่นการกำหนดนโยบาย การ ประมวลผล มาตรฐานการประมวลผล ตรวจสอบการดำเนินงานให้เป็นไปตามพระราชบัญญัติ และปฏิบัติการอื่นใดเพื่อให้เป็นไปตามพระราชบัญญัตินี้

การร้องเรียนและการอุทธรณ์

เป็นการกำหนดหลักเกณฑ์เกี่ยวกับการอุทธรณ์หรือเรียกร้องต่อคณะกรรมการ ในกรณีที่หน่วยงานดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลแล้วก่อความเสียหายต่อเจ้าของข้อมูลรวมทั้งกำหนดให้คณะกรรมการวางหลักเกณฑ์เพิ่มได้

บทกำหนดโทษ

เป็นการวางหลักเกณฑ์ที่เกี่ยวข้องกับความรับผิดทางแพ่งและทางอาญา ในกรณีที่เกิดความเสียหายขึ้นจากการดำเนินการที่มิชอบหรือฝ่าฝืนบทบัญญัติที่กฎหมายกำหนด

สำหรับร่างพระราชบัญญัติฉบับดังกล่าวนั้นสามารถนำมารองรับปัญหาการคุกคามทางอินเตอร์เน็ ตในรูปแบบของการนำข้อมูลต่าง ๆ ที่เป็นข้อมูลส่วนบุคคลไปลงบนเว็บบอร์ดเพื่อเป็นการให้ข้อมูลเสมือนเจ้าตัวเป็นผู้กระทำการเอง หรือการลงข้อมูลต่าง ๆ ที่สามารถระบุตัวได้ว่าเหยื่อเป็นผู้กระทำการนั้น ๆ ความรับผิดตามร่างพระราชบัญญัติฉบับดังกล่าวนั้นมิได้จำกัดเฉพาะตัวบุคคลธรรมดาเท่านั้นหากแต่องค์กรต่าง ๆที่เป็นผู้ควบคุมดูแลเก็บข้อมูลก็ต้องเป็นผู้รับผิดชอบด้วยเช่นกัน ซึ่งร่างพระราชบัญญัติฉบับดังกล่าวได้กำหนดหลักการเปิดเผยข้อมู ลทั่วไปและเฉพาะเจาะจงไว้โดยหลักแล้วจะไม่สามารถเปิดเผยข้อมูลที่มีการประมวลผลได้ หากปราศจากความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง ซึ่งหมายความว่าสามารถเปิดเผยข้อมูลได้เพียงเฉพาะที่ได้รับความยินยอมจากเจ้าของข้อมูล ซึ่งร่างพระราชบัญญัติฉบับดังกล่าวมิได้กำหนด ว่าต้องให้ความยินยอมเป็นลายลักษณ์อักษร เพียงแต่ให้ความยินยอมโดยชัดแจ้งก็พอที่จะเปิดเผยข้อมูลได้ การไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรนั้นทำให้การพิสูจน์การละเมิดสิทธิส่วนบุคคลเป็นไปด้วยความลำบากเนื่องจากขาดหลักฐานที่ใช้ในการพิสูจน์การกระทำความผิด เพราะหากมีการให้ความยินยอมกันเป็นลายลักษณ์อักษรแล้วเอกสารการให้ความยินยอมดังกล่าวจะกลายเป็นพยานเอกสารที่มีน้ำหนักในการพิจารณาคดี นอกจากนี้บทบัญญัติในร่างพระราชบัญญัติฉบับนี้ยังบัญญัติเรื่องความรับผิดทางแพ่งเอาไว้ในกรณีมีการเรียกร้องค่าสินไหมทดแทนซึ่งถือเป็น วิธีหนึ่งในการเยียวยาผู้ที่ได้รับความเสียหาย แต่มีข้อสังเกตคือค่าสินไหมทดแทนนั้นคำนวณจากอะไร ซึ่งส่วนใหญ่แล้วค่าสินไหมทดแทนตามกฎหมายไทยจะคำนวณจากความเสียหายที่เกิดขึ้นจริง และกฎหมายไทยก็ยังไม่มีเรื่องของการกำหนดค่าเสียหายในเชิงลงโทษจึงเป็นการยากหากจะคำนว ณค่าสินไหมทดแทนกรณีที่เกิดความเสียหายต่อชื่อเสียงของเหยื่อ

4.2.2 ปัญหาเรื่องเขตอำนาจศาล

การกระทำความผิดบนอินเตอร์เน็ตมีลักษณะไร้พรมแดนเกี่ยวพันกันได้หลายประเทศ ตัวผู้กระทำความผิดหรือผู้คุกคาม ตัวเหยื่อ และสถานที่ของการกระทำความผิดนั้นไม่มีความจำเป็ นที่จะต้องอยู่ในประเทศเดียวกัน ทำให้เกิดปัญหา ว่าความผิดนั้นเกิดขึ้นในประเทศใด และการพิจารณาคดีจะขึ้นอยู่กับศาลของประเทศใด

ในส่วนเขตอำนาจศาลในการดำเนินคดีตามกฎหมายอาญาของประเทศต่าง ๆ นั้นจะมีหลัก 4 ประการ คือ 1. หลักดินแดน (Territorial Principle) 2. หลักบุคคล (Nationality Principle) 3. หลักความมั่นคงแห่งรัฐ (Protective Principle) และ

4. หลักอำนาจลงโทษสากล (Universal Principle) ซึ่งตามกฎหมายของไทยได้บัญญัติให้ศาลไทยมีอำนาจในการพิจารณาคดีโดยอาศัยหลักทั้ง 4 ประการ ดังต่อไปนี้[137]

(1) หลักดินแดน (Territorial Principle) ตามประมวลกฎหมายอาญามาตรา 4 มาตรา 5 และมาตรา 6 สิ่งกำหนดในการใช้กฎหมาย คือ สถานที่ในการกระทำความผิด การกระทำความผิดเกิดขึ้นในรัฐใดย่อมตกอยู่ภายใต้กฎหมายของรัฐนั้น ๆ ไม่ว่าผู้กระทำความผิดหรือผู้เสียหายจะมีสัญชาติใด ด้วยเหตุ ที่กฎหมายอาญาบัญญัติเพื่อให้เกิดความสงบสุขและความปลอดภัยในพื้นที่ จึงบังคับใช้กับการกระทำความผิดในทุกประเภทในราชอาณาจักร

(2) หลักบุคคล (Nationality Principle) ตามประมวลกฎหมายอาญามาตรา 8 และมาตรา 9 สิ่งที่กำหนดในการใช้กฎหมาย คือ สัญชาติของบุคคล กฎหมายข องรัฐใดย่อมใช้บังคับและคุ้มครองคนของรัฐนั้น ๆ ไม่ว่าจะอยู่ ณ ที่ใด แบ่งออกเป็น 2 กรณี

กรณีบังคับกับคนของรัฐนั้น กฎหมายอาญาของรัฐใดย่อมใช้บังคับกับบุคคลที่ถือสัญชาติของรัฐที่กระทำความผิดทั้งในและนอกอาณาเขตของรัฐนั้น ๆ ไม่ว่าผู้เสียหายจะเป็นคนสัญชาติใดก็ตาม กรณีนี้ถือสัญชาติของผู้กระทำความผิดเป็นสำคัญ

กรณีคุ้มครองคนของรัฐนั้น กฎหมายอาญาของรัฐใดย่อมใช้คุ้มครองบุคคลที่ถือสัญชาติของรัฐนั้นที่ได้รับความเสียหายจากการกระทำความผิด ไม่ว่าในหรือนอกอาณาเขตของรัฐนั้น ไม่ว่าผู้กระทำความผิดจะเป็นบุคคลสัญชาติใดก็ตา ม หลักนี้ถือสัญชาติของผู้เสียหายเป็นสำคัญ ผู้กระทำความผิดจะถูกดำเนินดคีโดยกฎห มายแห่งรัฐที่ผู้เสียหายมีสัญชาติ

การถือหลักดินแดนโดยเคร่งครัด จะเป็นอุปสรรคหรือเป็นข้อจำกัดต่อการลงโทษการกระทำที่เกิดขึ้นนอกราชอาณาจักร กฎหมายอาญาจึงบัญญัติรับรองหลักบุคคล เข้าไว้ด้วยเพื่อเสริมหลักดินแดน

(3) หลักความมั่นคงแห่งรัฐ (Protective Principle) ตามประมวลกฎหมายอาญามาตรา 7(1) และ(2) เป็นหลักที่ถือว่าทุกรัฐจำเป็นต้องใช้อำนาจลงโทษผู้ที่กระทำการกระทบกระเทือนต่อความมั่นคงของรัฐ แม้ว่าการกระทำความผิดจะเกิดนอกราชอาณาจัก ร หรือผู้กระทำความผิดจะเป็นบุคคลสัญชาติใดก็ตามศาลไทยก็ยังมีอำนาจในการพิจารณาพิพากษาคดี

---

[137] นรเทพ บุญเก็บ, “มาตรการทางกฎหมายเกี่ยวกับการพนันบนอินเตอร์เน็ต,” (วิทยานิพนธ์ปริญญามหาบัณฑิตคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย,2548),หน้า 110.

(4) หลักอำนาจลงโทษสากล (Universal Principle) ตามประมวลกฎหมายอาญา มาตรา 7 (3) ประเทศใดที่จับตัวผู้กระทำความผิดได้ เป็นผู้มีอำนาจพิจารณาลงโทษตามกฎหมายของประเทศนั้น โด ยไม่ต้องคำนึงถึงสัญชาติของผู้กระทำความผิดหรือผู้เสียหาย และไม่ต้องคำนึงถึงสถานที่ที่เกิดการกระทำความผิด ซึ่งจะพบว่ากรณีของศาลไทยมีเขตอำนาจเหนือในทางคดีอาญาเมื่อมีข้อเท็จจริงใดข้อเท็จจริงที่เข้าเงื่อนไขหรือองค์ประกอบทางกฎหมายดังกล่าว โดยเฉพาะเมื่อมีการกร ะทำความผิด ซึ่งมีการกระทำความผิดนอกราชอาณาจักรไทย แต่ผลเกิดขึ้นในราชอาณาจักรไทยไม่ว่าจะโดยประสงค์ต่อผลหรือเล็งเห็นผลก็ตาม ให้ถือว่าความผิดนั้นเป็นความผิดที่ได้กระทำในราชอาณาจักรไทย ศาลไทยมีเขตอำนาจเหนือในการพิจารณาคดีอาญานั้นโดยผลของมาตรา 5 แห่งประมวลกฎหมายอาญา

สำหรับกรณีการคุกคา มทางอินเตอร์เน็ตนั้น เมื่อพิจารณาลักษณะของการคุกคามจะต้องมีผู้คุกคาม เหยื่อ หากมีการคุกคามทางอินเตอร์เน็ตเกิดขึ้นในประเทศไทยการนำตัวผู้กระทำความผิดมาลงโทษนั้นย่อมไม่มีปัญหา ศาลย่อมมีอำนาจในการพิจารณาคดี สำหรับการคุกคามท างอินเตอร์เน็ตนั้นหากตัว ผู้กระทำความผิดหรือผู้คุกคามนั้นอยู่ต่างประเทศ ย่อมถือว่าการกระทำส่วนหนึ่งส่วนใดได้เกิดขึ้นในราชอาณาจักรเช่นเดียวกัน ทั้งนี้ตามที่ประมวลกฎหมายอาญามาตรา 5 ได้บัญญัติไว้ จากบทบัญญัติดังกล่าวศาลไทยจึงมีอำนาจในการพิจารณาการกระทำควา มผิดเกี่ยวกับการคุกคามทางอินเตอร์เน็ต แต่ปัญหาที่ตามมา คือ กรณีที่ผู้กระทำความผิดอยู่ต่างประเทศ การที่จะนำตัวผู้กระทำความผิดมาศาลเพื่อพิจารณาและพิพากษาลงโทษนั้นเป็นไปได้ยากเนื่องจากการกระทำความผิดบนโลกของอินเตอร์เน็ตนั้นการจับกุมตัวผู้กระทำความผิดนั้นเป็น ไปได้ยากหรือแทบจะเป็นไปไม่ได้ นอกจากนี้ยังมีความจำเป็นที่จะต้องอาศัยความร่วมมือจากต่างประเทศเป็นอย่างมาก

4.2.3 ปัญหาเกี่ยวกับการรับฟังพยานหลักฐาน

เมื่อได้ตัวผู้กระทำความผิดเข้าสู่การพิจารณาคดีแล้ว หลักการของประมวลกฎหมายวิธีพิจารณาความอาญาให้สันนิษฐานเอาไว้ก่อนว่าจำเลยนั้นเป็นผู้บริสุทธิ์

จากหลักการดังกล่าวจึงมีความจำเป็นที่จะต้องพิสูจน์การกระทำความผิดของจำเลยจนปราศจากข้อสงสัย แต่พยานหลักฐานที่ได้มาจากการกระทำความผิดบนอินเตอร์เน็ตนั้นมักจะอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ซึ่งพยานหลักฐานที่อยู่ในรู ปของข้อมูลอิเล็กทรอนิกส์นั้นสามารถแก้ไขเปลี่ยนแปลงได้ง่าย หากการเปลี่ยนแปลงแก้ไขนั้นทำโดยผู้ชำนาญแล้วจะไม่สามารถหาร่องรอยได้ การแก้ไขจึงไม่สามารถปรากฏต่อบุคคลทั่วไป

หรือปรากฏต่อศาลอย่างชัดเจน ซึ่งการค้นหาร่องรอยของการกระทำความผิดต่าง ๆ บนอินเตอร์เน็ตอาจต้องอาศัยความร่วมมือจากผู้เชี่ยวชาญหรือนักเทคนิคคอมพิวเตอร์

ในส่วนของพยานหลักฐานนั้นหากเป็นพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้นสามารถรับฟังเป็นพยานหลักฐานหลักฐานได้ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 การคุกคามทางอิเ ล็กทรอนิกส์หากเป็นการส่งข้อความที่มีลักษณะไม่ประสงค์ดี ทำให้ผู้รับข้อความนั้นรู้สึกหวาดกลัวถึงอันตรายต่อร่างกาย ชีวิตหรือ ทรัพย์สิน รวมถึงการได้รับรูปภาพลามกอนาจารต่าง ๆ หากมีการบันทึกไว้ในแผ่นดิสก์ หรือ CD แล้วย่อมสามารถนำมาใช้เป็นหลักฐานได้

4.2.4 ปัญหาเกี่ยวกับผู้กระทำความผิด

เนื่องจากระบบเครือข่ายอินเตอร์เน็ตที่สามารถสื่อสารโยงใยกันได้ทั่วโลก จึงทำให้การติดต่อสื่อสารระหว่างกันจึงเป็นไปได้โดยง่ายได้แม้จะอยู่กันคนละประเทศ ทั้งนี้ทำให้การกระทำความผิดก็สามารถกระทำได้โดยง่ายเช่นเดียวกัน ผู้กระทำควา มผิดอาจจะอยู่กันคนละประเทศกับผู้ที่เป็นเหยื่อ และด้วยคุณสมบัติพิเศษของอินเตอร์เน็ตที่ไม่จำเป็นต้องเปิดเผยตัวตนจึงทำให้การสืบหาตัวผู้กระทำความผิดบนโลกของอินเตอร์เน็ตนั้นเป็นไปได้ยาก ไม่สามารถระบุได้อย่างชัดเจนแน่นอนว่าผู้กระทำความผิดนั้นเป็นใครและอยู่ที่ ใด เพราะผู้กระทำความผิดนั้นสามารถกระทำความผิดได้ในทุกที่ที่มีระบบเครือข่ายของอินเตอร์เน็ตเป็น นอกจากนี้ผู้กระทำความผิดอาจจะใช้อินเตอร์เน็ตคาเฟ่กระทำการต่าง ๆ ที่ถือว่าเป็นการคุกคามเหยื่อ จึงทำให้การสืบหาตัวตนของผู้คุกคามนั้นมีความยากเพิ่มขึ้น นอ กจากนี้บางครั้งตัวผู้กระทำความผิดเองนั้นมีความสามารถในด้านคอมพิวเตอร์หรือระบบของอินเตอร์เน็ตอาจกระทำการต่าง ๆ ที่เป็นการลบข้อมูลหรือหลักฐานของการกระทำความผิดออกจึงทำให้เจ้าหน้าที่ไม่สามารถสืบหาร่องรองของการกระทำความผิดได้

ดังนั้นจึงมีความจำเป็นต้องอาศัยผู้ ที่มีความรู้ความเชี่ยวชาญเฉพาะด้านในการค้นหาหลักฐานในการกระทำความผิด สำหรับการกระทำความผิดที่อาศัยช่องว่างของกฎหมายโดยการใช้อินเตอร์เน็ตคาเฟ่นั้น ผู้ประกอบการอินเตอร์เน็ตคาเฟ่ควรจะบันทึกข้อมูลของผู้ใช้บริการอินเตอร์เน็ตทุกครั้ง เช่น การจดบันทึกหมายเลขประจำตัวของผู้เข้ามาใช้บริการ เพื่อเป็นการช่วยเหลือเจ้าหน้าที่ในการสืบหาตัวผู้กระทำความผิด

4.2.5 ปัญหาเกี่ยวกับบทกำหนดโทษ

การคุกคามทางอินเตอร์เน็ตสำหรับประเทศไทยนั้นยังไม่มีกฎหมายเกี่ยวกับการคุกคามออกมาเป็นกฎหมายเฉพาะเหมือนกับประเทศสหรัฐอเมริกาที่ถือ อว่าการรุกล้ำสิทธิส่วนตัวของบุคคลอื่นไม่ว่าโดยวิธีใดนั้นถือว่าเป็นความผิด ดังนั้นการคุกคามทางอินเตอร์เน็ตบางครั้งหากไม่เกิดความรุนแรงอาจจะเป็นเพียงแค่การสร้างความเดือดร้อนรำคาญให้กับผู้ถูกคุกคามเท่านั้น ซึ่งกฎหมายอาญาในมาตรา 392 เป็นบทลหุโทษซึ่งมีโทษจำคุกไม่เกินหนึ่งเดือน ปรับไม่เกินหนึ่งเดือน หรือทั้งจำทั้งปรับ หากพิจารณาเปรียบเทียบถึงลงโทษกับความเสียหายที่เกิดขึ้นแล้วนั้นจะเห็นได้ว่าบทลงโทษนั้นเป็นบทลงโทษเพียงสถานเบาเท่านั้นไม่สามารถทำให้ผู้กระทำความผิดเกิดความเกรงกลัวต่อกฎหมายได้ และเนื่องจากในสมัยก่อนนั้นการกระทำความผิดในลักษณะของการสร้างความเดือดร้อนรำคาญให้กับผู้อื่นนั้นยังไม่มีลักษณะเหมือนปัจจุบันที่ลักษณะของการกระทำความผิดนั้นพัฒนาไปตามความก้าวหน้าของเทคโนโลยีจึงทำให้บทลงโทษนั้นไม่สามารถยับยั้งผู้กระทำความผิดให้เกิดความเกรงกลัวได้ นอกจากนี้หา กผู้กระทำความผิดนั้นกระทำความผิดซ้ำอีกก็ไม่สามารถเพิ่มโทษได้เนื่องจากผู้กระทำความผิดเคยรับโทษในความผิดลหุโทษเท่านั้นจึงไม่สามารถเพิ่มโทษผู้กระทำความผิดในลักษณะเดิมได้อีก

สำหรับบทลงโทษในส่วนของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ .ศ. 2550 แม้จะมีบทลงโทษที่มากกว่าประมวลกฎหมายอาญาคือมีโทษจำคุกไม่เกินห้าปี ปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ แต่โทษตามพระราชบัญญัติฉบับดังกล่าวก็เป็นเพียงบทลงโทษที่จะนำมาลงโทษผู้กระทำความผิดได้แค่บางกรณีเท่านั้นไม่สามารถนำมาลงโทษผู้กระทำความผิดฐานคุกคามทางอินเตอร์เน็ตได้ทุกกรณี

4.3 มาตรการอื่น ๆ ในการแก้ไขปัญหาการคุกคามทางอินเตอร์เน็ต

4.3.1 มาตรการทางสังคม

สังคมในปัจจุบันกำลังเผชิญปัญหาของอาชญากรรมในรูปแบบต่าง ๆ โดยอาศัยช่องทางของระบบเครือข่ายอินเตอร์เน็ตในการกระทำความผิด และแนวโน้มของปัญหาอาชญากรรมในรูปแบบต่าง ๆ ที่พัฒนาตามความก้าวหน้าของเทคโนโลยีก็มีสัดส่วนที่เพิ่มมากขึ้น ส่งผลกระทบต่อสังคมส่วนรวม การคุกคามทางอินเตอร์เน็ตถือเป็นการรุกล้ำสิทธิส่วนของบุคคลประเภทหนึ่งเป็นการละเมิดสิทธิและเสรีภาพความเป็นส่วนตัวของบุคคลบนโลกของอินเตอร์เน็ต

ภาครัฐและภาคเอกช นควรร่วมมือกันในการสร้างความรู้ความเข้าใจ ตลอดจนถึงการอบรมให้ความรู้กับบุคคลทั่วไปไม่ว่าจะเป็นเด็ก เยาวชน กลุ่มคนทำงาน ฯ ให้มี

ความรู้ความเข้าใจและสร้างจิตสำนึกรวมถึงการสร้างวิสัยทัศน์ที่ดีในการใช้อินเตอร์เน็ตเป็นเครื่องมือสื่อสารชนิดหนึ่งที่มีประโยชน์แล ะมีโทษในขณะเดียวกัน หากใช้ในทางที่ผิดจะสร้างปัญหาให้กับสังคมส่วนรวมมากน้อยเพียงใดเพื่อเป็นการสร้างเกราะป้องกันก่อนที่จะมีการกระทำความผิด และสังคมส่วนรวมอาจมีความจำเป็นที่จะต้องมีกฎหมายสำหรับสังคมอิเล็กทรอนิกส์หรืออินเตอร์เน็ตเป็นการเฉพาะเพื่อการดูแล ป้อง กัน ควบคุมผู้ใช้อินเตอร์เน็ต รวมถึงการกำหนดแบบแผนในการใช้ระบบอินเตอร์เน็ตให้เป็นไปในทิศทางเดียวกัน หรือกำหนดบทลงโทษสำหรับผู้กระทำความผิดตลอดจนถึงวิธีการเยียวยาผู้กระทำความผิดก่อนที่จะมีการลงโทษ ซึ่งหากภาครัฐตระหนักถึงความสำคัญและได้รับความร่วมมือหรือ การสนับสนุนจากภาคเอกชนต่าง ๆ แล้วย่อมสามาร ถป้องกันหรือแก้ไขปัญหาการคุกคามทางอินเตอร์เน็ตได้อีกทางหนึ่ง

4.3.2 มาตรการในการพัฒนาผู้เชี่ยวชาญ

เมื่อสังคมมีการพัฒนาความเจริญก้าวหน้าทางเทคโนโลยี ระบบเครือข่ายคอมพิวเตอร์เข้ามามีบทบาทที่สำคัญในชีวิตประจำวัน ผู้ กระทำความผิดอาศัยระบบเครือข่ายคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด เนื่องจากระบบเครือข่ายอินเตอร์เน็ตมีลักษณะพิเศษที่ไร้พรมแดนสื่อสารได้สะดวกรวดเร็ว การคุกคามทางอินเตอร์เน็ตจึงเกิดขึ้นโดยอาศัยลักษณะพิเศษดังกล่าวในการกระทำความผิด สาเหตุที่ทำให้การกระทำความผิดโดยอาศัยคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ในการกระทำความผิดเนื่องจาก[138]

(1) บุคคลทั่วไปสามารถเข้าถึงเทคโนโลยีทางคอมพิวเตอร์ได้ง่ายขึ้น
(2) เทคโนโลยีทางคอมพิวเตอร์มีราคาต่ำลง
(3) มีบุคคลที่มีความรู้เกี่ยวกับเทคโนโลยีเกี่ยวกับคอมพิวเตอร์เพิ่มมากขึ้น
(4) สามารถค้นหาข้อมูลและรวบรวมข้อมูลได้อย่างกว้างขวาง
(5) แนวทางปฏิบัติและประเด็นทางกฎหมายยังมีช่องโหว่
(6) เทคโนโลยีมีสมรรถนะสูงขึ้นนำมาใช้ได้ง่ายขึ้น
(7) การใช้คอมพิวเตอร์ประกอบอาชญากรรมนั้นกระทำได้โดยง่าย การตรวจสอบและการจับกุมยาก

ในการดำเนินการสืบหาตัวผู้กระทำความผิด หรือการนำผู้กระทำความผิดมาลงโทษและการควบคุมมิให้ผู้กระทำความผิดนำเทคโนโลยีมาใช้ในการกระทำความผิดนั้นขึ้นอยู่กับหน่วยงานและเจ้าพนักงานที่ทำหน้าที่ในการบังคับใช้กฎหมายจึงมีจำเป็นต้องมี

[138] เรื่องเดียวกัน, หน้า 136.

การฝึกอบรมเจ้าหน้าที่ให้มีความเชี่ยวชาญ ตลอดจนการจัดตั้งหน่วยงานที่รับผิด ชอบคดีเกี่ยวกับเทคโนโลยีเป็นการเฉพาะรวมทั้งเป็นหน่วยงานในการดูแลตรวจตราเว็บไซต์ต่าง ๆ และเพื่อเป็นการสร้างองค์ความรู้ให้กับหน่วยงานและเจ้าหน้าที่ที่บังคับใช้กฎหมาย

4.3.2 มาตรการในการขอความร่วมมือระหว่างประเทศ

การคุกคามทางอินเตอร์เน็ตนั้นสามารถกระทำได้ข้ามประเทศ ตัวผู้กระทำความผิดกับเหยื่อนั้นอาจจะอยู่กันคนละประเทศกัน ผู้กระทำความผิดนั้นอาจจะอยู่นอกประเทศแต่ผลของการกระทำนั้นเกิดขึ้นในราชอาณาจักร ซึ่งศาลไทยย่อมมีอำนาจพิจารณาพิพากษาคดี

อย่างไรก็ตาม แม้ศาลไทยจะมีอำนาจในการพิจารณาพิพากษาคดีก็ตาม แต่ปัญหาที่ตามมาคื อ การนำตัวผู้กระทำความผิดมาดำเนินคดี หากผู้คุกคามนั้นอยู่นอกราชอาณาจักร ซึ่งการดำเนินการต้องเป็นไปตามหลักการส่งผู้ร้ายข้ามแดนและจะต้องกระทำโดยมีความตกลงระหว่างประเทศ หรือมีกฎหมายภายในบัญญัติไว้ และจะต้องดำเนินการตามขั้นตอนที่กฎหมายกำหนด หรือการดำเนินการข อความร่วมมือกับองค์กรตำรวจสากล (International Criminal Police Organization : Interpol) ซึ่งเป็นองค์กรความร่วมมือระหว่างประเทศในคดีอาญา โดยองค์การตำรวจสากลเป็นกลไกหรือตัวกลางในการปฏิบัติการเพื่อแลกเปลี่ยนข้อมูลข่าวสารในการกระทำความผิดและช่วยติดตามจับกุมผู้กระทำความผิดมาดำเนินคดีให้ได้อย่างมีประสิทธิภาพอีกทางหนึ่ง

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

ด้วยเทคโนโลยีด้านการสื่อสารและคอมพิวเตอร์มีการพัฒนาอย่างรวดเร็ว การสื่อสารทางระบบอินเตอร์เน็ตเป็นอีกทางหนึ่งที่ทำให้การสื่อสารนั้นปร าศจากพรหมแดน คนในสังคมต่าง ๆ สามารถติดต่อแลกเปลี่ยนข้อมูลและสื่อสารกันได้โดยไม่มีอุปสรรคไม่ว่าจะเป็นระยะทาง หรือวัฒนธรรมรวมถึงประเพณีทางสังคม ระบบอินเตอร์เน็ตนั้นทำให้เกิดการโต้ตอบระหว่างกันเสมือนการอยู่ต่อหน้ากันจริง เหตุนี้จึงมีการนำเอาระบบอินเตอร์เน็ตมาใช้ประโยชน์เพื่ออำนวยความสะดวกในการติดต่อสื่อสารต่าง ๆ เช่น การติดต่อธุรกิจ การเผยแพร่ข้อมูลข่าวสาร และการสันทนาการอื่น ๆ ส่งผลให้อินเตอร์เน็ตเข้ามามีอิทธิพลอย่างสูงในชีวิตประจำวันของคนในสังคม ในขณะที่อีกด้านหนึ่งของสังคมได้มีผู้ที่นำเอ าความก้าวหน้าทางเทคโนโลยีและความสลับซับซ้อนของเทคโนโลยีบนโลกอินเตอร์เน็ตมาเป็นเครื่องมือในการกระทำความผิดอีกทั้งหาประโยชน์จากผู้ที่ใช้อินเตอร์เน็ตที่ขาดความรู้ความเข้าใจในระบบอินเตอร์เน็ตนั้นกลายเป็นเหยื่อ และนำเอาความก้าวหน้าทางเทคโนโลยีนั้นไปใช้ในทางที่ ไม่เหมาะสม โดยอาศัยระบบเครือข่ายอินเตอร์เน็ตนั้นไปก่ออาชญากรรมทางคอมพิวเตอร์ (Computer Crime) ซึ่งอาชญากรรมดังกล่าวถือเป็นการกระทำความผิดในรูปแบบใหม่

การใช้อินเตอร์เน็ตเป็นเครื่องมือในการกระทำความผิดนั้นมีหลายรูปแบบด้วยกัน เช่น การเผยแพร่รูปลามกอนาจ าร การหลอกลวงบนอินเตอร์เน็ต การค้าประเวณีบนอินเตอร์เน็ต รวมถึงการใช้อินเตอร์เน็ตในการคุกคามบุคคลอื่น หรือการใช้อินเตอร์เน็ตเป็นเครื่องมือในการยุยงส่งเสริมบุคคลที่สามในการคุกคามบุคคลอื่น หรือการบิดเบือนข้อมูลหรือเผยแพร่ข้อมูลที่เป็นเท็จบนอินเตอร์เน็ตจนก่อให้เกิดการคุกคาม

จากการศึกษาทำให้ทราบว่าปัญหา Cyberstalking นั้นก่อให้เกิดปัญหาและผลกระทบต่อความสงบสุขของตัวผู้ถูกคุกคามหรือเหยื่อ ซึ่งบางครั้งเราอาจมองปัญหาดังกล่าวว่าเป็นเพียงการคุกคามที่ไม่ก่อให้เกิดอันตรายใดเท่ากับการคุกคามแบบธรรมดาทั่วไปซึ่งมีการกระทำทางกายภาพหรือมีความใกล้ชิดกับตัวเหยื่อหรือผู้ถูกคุกคามโดยตรงที่ก่อให้เกิดภยันตรายต่อร่างกายและจิตใจ รวมถึงขาดความสงบสุขและสวัสดิภาพในชีวิตและทรัพย์สิน แต่ในความเป็นจริงแล้วการคุกคามทางอินเตอร์เน็ตนั้นสามารถบิดเบือนข้อมูลรวมทั้งเผยแพร่หรือขยายข้อมูลออกไปสู่โลกแห่งความจริงได้มากมายและรวดเร็วกว่าการคุกคามแบบธรรมดา ดังนั้นเพื่อเป็นการป้องกันตัวเองจาก Cyberstalking หรือ

ป้องกันตนเองจากการตกเป็นเหยื่อ เราจึงควรศึกษาการใช้อินเตอร์เน็ตให้ถูกวิธีและรู้จักวิธีการป้องกันตนเองเมื่อใช้อินเตอร์เน็ต เช่น ไม่ควรใช้ชื่อจริงหรือชื่อเล่นของตนเองเป็นชื่อที่ปรากฏอยู่บนหน้าจอ หรือรหัสแสดงตนเอง ควรใช้ อีเมล์แอดเดรสที่ไม่สามารถระบุเพศได้ นอกจากนี้ผู้ที่ใช้อินเตอร์เน็ตทุกคนควรสร้างสามัญสำนึกในการใช้อินเตอร์เน็ตให้ถูกวิธี และควรให้ความสำคัญในการใช้อินเตอ ร์เน็ต ไม่ควรที่จะใช้ชื่อที่จะส่อให้เกิดการคุกคามเช่น sexygirl@domain.com เพราะอีเมล์ในลักษณะดังกล่าวทำให้เกิดความรู้สึกหรือเกิดความคิดในทางที่ไม่ดี การป้องกันตนเองจากการคุกคามทางอิเล็กทรอนิกส์นั้นควรเริ่มจากตนเองก่อนเป็นสำคัญ หากขาดความรับผิดชอบห รือสามัญสำนึกแล้วอาจจะเป็นการกระตุ้นหรือยุยงส่งเสริมให้เกิดการคุกคามโดยผู้ใช้อินเตอร์เน็ตนั้นไม่รู้ตัว

นอกจากการป้องกันการตกเป็นเหยื่อหรือถูกคุกคามโดยเริ่มต้นจากตนเองแล้ว สังคมโดยรวมควรตระหนักถึงปัญหา Cyberstalking ว่าเป็นปัญหาที่เพิ่มขึ้นจากการใช้ชีวิตประจำวัน ซึ่งปัญหาดังกล่าวนั้นสามารถนำไปสู่การคุกคามบนโลกแห่งความเป็นจริงได้ และยังสามารถทวีความรุนแรงจนกลายเป็นอาชญากรรมได้ ทั้งนี้รวมถึงผู้ให้บริการทางอินเตอร์เน็ตที่ควรจะกำหนดเงื่อนไขข้อตกลงการใช้บริการ อีเมล์ของตนเองว่าห้ามทำการคุกคามผ่านทางอินเตอร์ เน็ตหรือใช้อินเตอร์เน็ตเพื่อเป็นการยุยงส่งเสริมให้เกิดการคุกคาม เนื่องจากอินเตอร์เน็ตนั้นเป็นแหล่งข้อมูลที่ใคร ๆ ก็สามารถเข้าถึงได้อย่างไร้พรหมแดนและไม่มีขีดจำกัดและสามารถกระทำได้อย่างไม่จำกัดช่วงเวลา

การคุกคามทางอินเตอร์เน็ตนั้นไม่ว่าในรูปแบบใดก็ถือเป็ นการกระทำความผิดที่อาศัยเครือ ข่ายอินเตอร์เน็ตที่มีความสลับ ซับซ้อนทางด้านเทคโนโลยีเป็นช่องทางในการกระทำความผิด ทำการคุกคามต่อสิทธิส่วนบุคคล เสรีภาพในการติดต่อสื่อสาร ก่อให้เกิดการกลัวว่าจะเกิดภยันตรายต่อชีวิตและทรัพย์สิน รวมถึงการคุกคามนั้นอาจกระตุ้นให้มีการก่ออาชญากรรมที่รุนแรงในสังคม แต่เนื่องจากมาตรการทางกฎหมายและมาตรการทางสังคมที่มีอยู่นั้นยังไม่สามารถเข้าถึงรูปแบบของปัญหาการคุกคามได้ดีเพียงพอ และยังไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพเพียงพอ ทำให้รูปแบบและพฤติกรรมการคุกคามนั้นเปลี่ยนแปลงไปตลอดเวลาแล ะมาตรการทางกฎหมายก็ยังไม่สามารถลงโทษผู้กระทำความผิดได้อย่างจริงจังและครอบคลุม

จากการศึกษาบทบัญญัติของกฎหมายประเทศสหรัฐอเมริกาการคุกคามทางอินเตอร์เน็ตหรือ Cyberstalking นั้นเป็นบทบัญญัติกฎหมายที่ออกมาเพื่อรองรับการกระทำความผิดฐานคุกคามที่กระทำในรูปแบบที่แตกต่างไปจากเดิม คือการคุกคามที่เกิดขึ้นนี้จะเกิดในรูปแบบที่ผู้คุกคามนั้นไม่จำเป็นต้องมีการเผชิญหน้ากับเหยื่อ หรือเหยื่อนั้นไม่รู้ว่าผู้คุกคามคือใคร เนื่องจากลักษณะพิเศษของอินเตอร์เน็ตคือการไม่เปิดเผยชื่อ จึงทำให้ผู้ที่ต้องการก่ออาชญากรรมนั้นนำช่องว่ างดังกล่าวมาเป็นช่องทางในการก่ออาชญากรรม

นอกจากนี้พฤติกรรมการคุกคามนั้นอาจจะเป็นเพียงแค่การก่อให้เกิดความรำคาญ ความเดือดร้อน แต่ในประเทศสหรัฐอเมริกาเราจะพบว่าการคุกคามทางอินเตอร์เน็ตนั้นได้ขยายผลและทวีความรุนแรงถึงชีวิตและทรัพย์สินของเหยื่อ บาง ครั้งการคุกคามที่เกิดขึ้นกับเหยื่อนั้นบุคคลที่สามก็อาจจะเป็นเครื่องมือของการคุกคามได้เช่นเดียวกัน จึงทำให้บางมลรัฐนั้นได้ตระหนักถึงรูปแบบการคุกคามที่เปลี่ยนแปลงไป รวมถึงความรุนแรงเพิ่มขึ้นจนกลายเป็นอาชญกรรมในรูปแบบใหม่ จึงได้ออกกฎหมายการคุกคามทางอินเตอร์เน็ต Cyberstalking ออกมาเพื่อเป็นการป้องกัน ปราบปราม และลงโทษผู้กระทำความผิดในลักษณะดังกล่าวนี้ออกมา ซึ่งกฎหมายเกี่ยวกับการคุกคามทางอินเตอร์เน็ตนี้มีเพียง 6 มลรัฐเท่านั้นในประเทศสหรัฐอเมริกาคือ มลรัฐอิลลินอยส์ มลรัฐ หลุยส์เซียน่า มลรัฐมิสซิส ซิปปี้ มลรัฐโร้ดไอร์แลนด์ มลรัฐวอชิงตัน และ มลรัฐนอร์ทคาโรไลน่า เท่านั้นที่ออกบทบั ญญัติดังกล่าว มาใช้โดยตรง ส่วนมลรัฐที่เหลือนั้นคงใช้กฎหมายเกี่ยวกับการคุกคามมาใช้เทียบเคียงเพื่อลงโทษผู้กระทำ ความผิด โดยแต่ละรัฐนั้นได้บัญญัติกฎหมายที่แตกต่างกั น และแต่ละรัฐก็บัญญัติองค์ประกอบของการกระทำความผิดฐาน Cyberstalking ไม่แตกต่างกันเท่าใดนัก เช่ นมลรัฐมิสซิสซิปปี้ แต่โดยหลัก แล้วจะประกอบด้วย 1. มีการใช้หรือส่งการสื่อสารทางอิเล็กทรอนิกส์ 2. มีการข่มขู่ ข่มขวัญ หรือรังควน 3. มีเจตนาทำให้เหยื่อนั้ นเกิดความกลัวเกี่ยวกับความปลอดภัยในชีวิตและทรัพย์สิน หรือความกลัวว่าจะเกิดภยันตรายกับคนใกล้ชิดหรือคนในครอบครัวของเหยื่อ แต่ในส่วนของมลรัฐอิลลินอยส์นั้นจะแตกต่างจากมลรัฐอื่นที่มีการกำหนดว่าการกระทำนั้นจะต้องมีการกระทำอย่างน้อยสองคราวอย่างชัดเจน

นอกจาก นี้บทลงโทษของแต่ละมลรัฐที่บัญญัติเกี่ยวกับการกระทำความผิดฐานคุกคามทางอินเตอร์เน็ตนั้นก็บัญญัติเอาไว้แตกต่างกัน

ในบางมลรัฐเช่นอิลลินอยส์นั้นได้กำหนดบทลงโทษความผิดฐานคุกคามทางอินเตอร์เน็ตครั้งแรกไว้ว่าเป็นความผิดร้ายแรงระดับที่สี่ (Class 4 Felony) คือมีโทษปรับไม่เกิน 25,000 ดอลล่าร์ จำคุกตั้งแต่หนึ่งปีขึ้นไปแต่ไม่เกินสามปี หากมีการกระทำความผิดอีกครั้งที่สองหรือครั้งต่อ ๆ มาลงโทษในความผิดร้ายแรงระดับที่สาม (Class 3 Felony) ซึ่งโทษก็จะรุนแรงขึ้น ในมลรัฐโร้ดไอร์แลนด์บทลงโทษสำหรับการกระทำความผิดฐานคุกคามทางอินเตอร์เน็ต คือ ความผิดฐานเบาจำคุกไม่เกินหนึ่งปี ปรับไม่เกิน 500 ดอลล่าร์หรือทั้งจำทั้งปรับ หากเป็นการกระทำความผิดครั้งที่สองหรือครั้งต่อ ๆ มาจะถือว่าเป็นความผิดร้ายแรงจำคุกไม่เกินสองปีปรับไม่เกิน 6,000 ดอลล่าร์หรือทั้งจำทั้งปรับ เช่ นเดียวกับมลรัฐนอร์ทคาโรไลน่าซึ่งจัดให้เป็นความผิดฐานเบา ส่วนมลรัฐหลุย ส์เซียน่าหากการกระทำความผิดครั้งแรกลงโทษจำคุกไม่เกินหนึ่งปี ปรับไม่เกิน 2,000 ดอลล่าร์ หรือทั้งจำทั้งปรับ หากกระทำความผิดฐานคุกคามทางอินเตอร์ครั้งที่สอง

ซึ่งเคยกระทำมาแล้วภายใน ระยะเ วลาเจ็ดปีก่อนหน้าที่จะได้กระทำความผิดครั้งที่สองนี้ จะต้องถูกจำคุกอย่างต่ำ 180 วัน แต่สูงสุดจำคุกไม่เกินสามปี ปรับไม่เกิน 5,000 ดอลล่าร์ หรือทั้งจำทั้งปรับ หากการกระทำความผิดครั้งที่สามเกิดขึ้นภายในระยะเวลาเจ็ดปีก่อนหน้านี้เกี่ยวกับความผิดฐานคุกคามจะต้องถูกจำคุกไม่น้อยกว่าสองปี แต่สูงสุดจำคุกไม่เกินห้าปี ปรับไม่เกิน 5,000 ดอลล่าร์หรือทั้งจำทั้งปรับ ในมลรัฐวอชิงตันมีโทษจำคุกไม่เกินหนึ่งปี ปรับไม่เกิน 5,000 ดอลล่าร์ หากผู้กระทำความผิดฐานนี้เคยถูกตัดสินให้มีความผิดเกี่ยวกับการรังควานมาก่อน และกร ะทำต่อเหยื่อรายเดิมหรือบุคคลที่ศาลสั่งห้ามแล้วผู้กระทำความผิดจะต้องได้รับโทษหนักขึ้น ถือเป็นการกระทำความผิดร้ายแรงต้องโทษจำคุกห้าปีหรือปรับ 10,000 ดอลล่าร์หรือทั้งจำทั้งปรับรวมถึงการคุกคามและข่มขู่ว่าจะฆ่าก็รับโทษสถานเดียวกัน สำหรับมลรัฐมิสซิสซิปปี้บทลงโ ทษคือจำคุกไม่เกินสองปี ปรับไม่เกิน 5,000 ดอลล่าร์หรือทั้งจำทั้งปรับ หากการกระทำนั้นเป็นการฝ่าฝืนข้อห้ามตามที่กฎหมายกำหนดไว้ก็จะต้องได้รับโทษหนักขึ้น คือโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกิน 10,000 ดอลล่าร์ หรือ หรือทั้งจำทั้งปรับ

เมื่อพิจารณา พฤติกรรมการคุกคามทางอินเตอร์เน็ตในประเทศสหรัฐอเมริกาและบทลงโทษสำหรับความผิดฐานนี้แล้วจะพบว่าการบัญญัติกฎหมายเกี่ยวกับความผิดฐานคุกคามทางอินเตอร์เน็ตของ 6 มลรัฐดังกล่าวนั้นมีวัตถุประสงค์ไม่แตกต่างกันในการป้องกัน ปราบปราม และลงโทษผู้กระทำความผิด เพียงแต่บทลงโทษและอัตราโทษของแต่ละรัฐนั้นไม่เท่ากัน เช่น มลรัฐหลุยส์เซียน่าเองก็จะกำหนดระยะเวลาเอาไว้คือ 7 ปี หากมีการกระทำความผิดขึ้นอีกก็จะต้องได้รับโทษหนักขึ้น และบางมลรัฐถือว่าการกระทำความผิ ดครั้งแรกเป็นความผิดฐานเบา ซึ่งแต่ละมลรัฐเองนั้นกฎหมายที่มีอยู่ก็ ไม่ได้ครอบคลุมปัญหาที่เกิดขึ้นได้ทั้งหมด ซึ่งบางครั้งก็อาจจะต้องใช้กฎหมายที่มีอยู่ตีความให้ครอบคลุมกับปัญหาที่เกิดขึ้นหรือตีความเพื่อจะลงโทษผู้กระทำผิดหรือเยียวยาผู้ที่ตกเป็นเหยื่อ

สำหรับประเทศไทยนั้นพฤติกรรมที่เป็นลักษณะของการคุกคามทางอินเตอร์เน็ต นั้นอาจจะยังไม่เป็นที่เข้าใจกันเท่าใดนักว่ารูปแบบของการคุกคามทางอินเตอร์นั้นเป็นเช่นไรและอันตรายที่เกิดขึ้นนั้นจะก่อให้เกิดผลเสียหายได้อย่างไรกับผู้ที่ตกเป็นเหยื่อ นอกจากนั้นพฤติกรรมการคุกคามทางอินเตอร์เน็ตนั้นเกิดจากการกระทำหลายอย่าง มิได้เกิดจากการ กระทำเดียว และการกระทำนั้น ๆ โดยตัวของมันเองอาจจะไม่เป็นความผิด พฤติกรรมการคุกคามทางอินเตอร์เน็ตนั้นต้องไม่ใช่เกิดจากการกระทำครั้งเดียวแต่เกิดจากการกระทำซ้ำ ๆ ในช่วงระยะเวลาหนึ่ง นอกจากนี้ต้องมีการข่มขู่ข่มขวัญ หรือรังควาน

จนทำให้เหยื่อนั้นเกิดความก ลัวว่าจะเป็นอันตรายต่อร่างกายหรือชีวิตตลอดจนทรัพย์สินของตนเองหรือบุคคลในครอบครัว

กฎหมายอาญาของไทยที่พอจะนำมาปรับใช้ได้กับพฤติกรรมการคุกคามทางอินเตอร์เน็ตได้นั้นคือความผิดฐานหมิ่นประมาท ตามมาตรา 326 มาตรา 328 และมาตรา 392 ซึ่งเมื่อพิจารณาถึงอง ค์ประกอบภายนอกของการกระทำความผิดแล้ว ความผิดทั้งสองมาตราดังกล่าวนั้นไม่จำเป็นต้องมีการกระทำซ้ำ ๆ ภายในระยะเวลาหนึ่ง เหมือนกับบทบัญญัติของกฎหมายประเทศสหรัฐอมริกา นอกจากนั้นการลงโทษผู้กระทำความผิดจะกระทำได้ต่อเมื่อกฎหมายได้บัญญัติเอาไว้ว่าเป็นความผิดเท่านั้ น และการกระทำความผิดทั้งสองมาตราดังกล่าวนี้ไม่มีบทลงโทษที่รุนแรง และการกระทำความผิดทั้งสองฐานดังกล่าวก็ไม่มีฐานพยา ยามกระทำความผิด เนื่องจากความผิดตามมาตรา 392 เป็นความผิดลหุโทษ ซึ่งความผิดลหุโทษนั้นไม่สามารถลงโทษฐานพยา ยามกระทำความผิดเนื่องจากตามมาตรา 105 บัญญัติเอาไว้ว่า “ผู้ใดพยายามกระทำความผิดลหุโทษผู้นั้นไม่ต้องรับโทษ” จากบทบัญญัติดังกล่าวทำให้เกิดช่องว่างทางกฎหมายที่ไม่สามารถลงโทษผู้กระทำความผิดได้และบทลงโทษนี้เป็นเพียงแค่ลหุโทษซึ่งมีบทลงโทษสถานเบาเท่านั้น คือจำคุกไม่เกินหนึ่งเดือนปรับไม่เกินห นึ่งพันบาท ซึ่งศาลไทยมักจะลงโทษเพียงแค่ปรับเท่านั้นหากผู้กระทำความผิดไม่เคยกระทำความผิดมาก่อน และจากบทลงโทษที่ไม่รุนแรงเพียงพอนั้นทำให้ไม่สามารถหยุดยั้งพฤติกรรมของคุกคามทางอินเตอร์เน็ตได้ ซึ่งการคุกคามทางอินเตอร์เน็ตนั้นสร้างความเสียหายมากกว่ามาตรการท างกฎหมายที่ลงโทษเพียงแค่ลหุโทษ

เมื่อพิจารณารูปแบบการคุกคามทางอินเตอร์เน็ตที่ส่งผลกระทบอย่างรุนแรงและอาจจะก่อให้เกิดอันตรายแก่ร่างกายและทรัพย์สินแล้ว ทำให้ต้องพิจารณาว่ากฎหมายของไทยเพียงพอหรือไม่ที่จะนำมาปรับใช้กับพฤติกรรมการคุกคามทางอินเตอร์เน็ต บทลงโท ษที่เหมาะสมกับพฤติกรรมการกระทำผิดฐานคุกคามทางอินเตอร์เน็ตนั้นควรกำหนดบทลงโทษเท่าใดจึงจะเพียงพอและเหมาะสมเพื่อเป็นการยับยั้งพฤติกรรมของผู้กระทำความผิด นอกจากนี้การให้ความรู้ความเข้าใจในพฤติกรรมการคุกคามทางอินเตอร์เน็ตแก่หน่วยงานที่บังคับใช้กฎหมาย ได้แก่ตำรวจ พนักงานอัยการ ทนายความและผู้พิพากษาว่าการคุกคามทางอินเตอร์เน็ตนั้นมีลักษณะอย่างไร และการคุกคามนั้นสามารถกระทำได้ในรูปแบบใดบ้าง พฤติกรรมของผู้คุกคามนั้นเป็นอย่างไร อีกทั้งความเสียหายหรืออันตรายที่เกิดขึ้นกับเหยื่อนั้นมีความรุนแรงมากน้อยเพียงใด สร้างความเสียหายร้ายแรงต่อสังคมส่วนรวมมากน้อยเพียงใดและผู้บังคับใช้กฎหมายนั้นควรพิจารณาหามาตรการคุ้มครองหรือป้องกันผู้ที่ตกเป็นเหยื่ออย่างไร

5.2 ข้อเสนอแนะ

1. ควรจะมีการแก้ไขบทลงโทษที่บัญญัติอยู่ในมาตรา 392 ให้มีโทษเพิ่มขึ้น เนื่องจากพฤติกรรมการคุกค ามทางอินเตอร์เน็ตนั้นเป็นพฤติกรรมที่คุกคามความเป็นส่วนตัวของบุคคลอื่นไม่น้อยไปกว่าพฤติกรรมการคุกคามในรูปแบบทั่วไป และการคุกคามในลักษณะดังกล่าวนี้เป็นรูปแบบการคุกคามแนวใหม่ที่บางครั้งผู้เสียหายหรือเหยื่อนั้นไม่รู้ตัวผู้คุกคามว่าเป็นใคร ซึ่งมาตรา 392 นั้นลงโทษเพียงแค่จำคุกไม่เกินหนึ่งเดือนหรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ อัตราโทษดังกล่าวนั้นถือว่าเป็นอัตราโทษที่ต่ำมาก ไม่สามารถหยุดยั้งพฤติกรรม Cyberstalking ได้ และโดยทั่วไปแล้วในความผิดลหุโทษนั้นศาลมักจะลงโทษเพียงแค่ปรับเท่านั้น แต่ ถ้าหากนำอัตราโทษมาเปรียบเทียบกับความเสียหายที่อาจจะเกิดขึ้นกับเหยื่อแล้ว ความเสียหายที่เกิดขึ้นกับเหยื่ออาจจะรุนแรงจนก่อให้เกิดอันตรายต่อชีวิต โดยอัตราโทษนั้นน่าจะอยู่ในอัตราเดียวกับความผิดต่อเสรีภาพ มาตรา 309 คือจำคุกไม่เกินสามปี ปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ

2. การกระทำการคุกคามซึ่งถือว่าเป็นองค์ประกอบภายนอกไม่ควรระบุว่าเป็นการกระทำในลักษณะใด เนื่องจากการคุกคามนั้นประกอบด้วยหลายพฤติกรรมและพฤติกรรมบางอย่างนั้นกฎหมายไม่ถือว่าเป็นการกระทำความผิด หากแต่เมื่อรวมกันแล้วถือว่าเป็นการคุกคาม ดังนั้นจึงควรถือหลักสำคัญที่ว่ามีการกระทำซ้ำ ๆ ช่วงเวลาหนึ่ง

3. ควรมีบทบัญญัติความผิดฐาน Cyberstalking ขึ้นมาเป็นการเฉพาะ เนื่องจากมาตรา 392 นั้นยังไม่ครอบคลุมถึงพฤติกรรมของ Cyberstalking จึงควรเพิ่มความผิดฐาน Cyberstalking ให้สอดคล้องครอบคลุมถึงลักษณะและพฤติกรรมการ Cyberstalking ดังนี้

“ผู้ใดกระทำการอันเป็นการข่มขู่ คุกคาม รบกวน ทำให้ตื่นตกใจ ไม่ว่าโดยวิธีการใด ๆ ผ่านทางอินเตอร์เน็ตหรือเครือข่ายการสื่อสารอันมีลักษณะเดียวกัน โดยกระทำการนั้นอย่างซ้ำ ๆในช่วงระยะเวลาหนึ่ง และการกระ ทำดังกล่าวนั้นทำให้ผู้อื่นเกิดความกลัวว่าจะเกิดอันตรายต่อร่างกาย ชีวิต ทรัพย์สิน และความปลอดภัยของสมาชิกในครอบครัว ผู้นั้นต้องระวางโทษจำคุกไม่เกินสามปี ปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ”

4. ออกกฎหมายแก้ไขปัญหา Cyberstalking โดยเฉพาะ เนื่องจา กปัญหาของ Cyberstalking นั้นเกิดจากความสลับซับซ้อนทางเทคโนโลยีที่ก้าวไกล และไม่สามารถให้

คำจำกัดความของปัญหาดังกล่าว ทำให้ประเทศที่มีเทคโนโลยี ทันสมัยอย่างประเทศสหรัฐอเมริกา ก็ยังไม่สามารถแก้ไขปัญหาได้ทุกแง่มุม และก็ยังไม่สามารถให้คำจำกัดความที่มีลักษณะเป็นหนึ่งเดียวกันได้ อีกทั้งการออกกฎหมายของประเทศสหรัฐอเมริกาก็ยังไม่สามารถแก้ไขปัญหาได้ชัดเจนเพียงพอ ดังนั้นเราจึงควรศึกษาปัญหาดังกล่าวให้ละเอียดรอบคอบโดยศึกษาจากประเทศสหรัฐอเมริกาเป็นหลักและบัญญัติกฎหมายเฉพาะเรื่อง Cyberstalking ขึ้นมาต่างหากจากการแก้ไ ขหรือเพิ่มเติมฐานความผิดในประมวลกฎหมายอาญา เพื่อจะได้แก้ไขปัญหาดังกล่าวได้อย่างมีประสิทธิภาพ หากแต่การ ศึกษาและพิจารณาออกกฎหมายใหม่ของประเทศไทย นั้นใช้เวลา ในการศึกษาและพิจารณานานพอสมควร จึงอาจจะไม่ทันการณ์กับปัญหาที่เกิดขึ้น ดังนั้นวิธีการแก้ไขประมวลกฎหมายอาญาหรือเพิ่มเติมฐานความผิดอาจจะเป็นวิธีที่ดีกว่าในการรองรับปัญหาที่อาจจะเกิดขึ้นก่อนการออกกฎหมายเฉพาะเกี่ยวกับ Cyberstalking

5. องค์กรผู้บังคับใช้กฎหมาย เช่น ตำรวจ พนักงานอัยการ และผู้พิพากษา ในส่วนขององค์กรผู้บังคับใช้กฎหมายนั้นควรให้การอ บรมและให้ความรู้ความเข้าใจอย่างสม่ำเสมอเกี่ยวกับอินเตอร์เน็ตหรือเทคโนโลยีสารสนเทศ หรือสื่อต่าง ๆ เพิ่มมากขึ้นว่าการใช้อินเตอร์เน็ตเหรือการใช้เทคโนโลยีเป็นช่องทางในการก่ออาชญากรรมนั้นได้พัฒนาไปในรูปแบบใด ไม่ควรยึดลักษณะของพฤติกรรมหรือองค์ประกอบภายนอ กของการกระทำความผิดตามตัวบทกฎหมายที่มีอยู่มากเกินไป นอกจากนี้ควรให้ความรู้ความเข้าใจกับลักษณะของพฤติกรรม Cyberstalking และให้ความรู้ความเข้าใจถึงอันตรายที่อาจจะเกิดขึ้นจากพฤติกรรม Cyberstalking ว่าอันตรายที่เกิดขึ้นนั้นจะเป็นเช่นไร หากไม่มีการยับยั้งพฤติกรรม Cyberstalking เพื่อให้องค์กรผู้บังคับใช้กฎหมายตระหนักถึงอันตรายที่อาจจะเกิดขึ้น อีกทั้งควรให้ความรู้หรือแนวทางทางในการปรับใช้ตัวกฎหมายที่มีอยู่ให้ครอบคลุมกับพฤติกรรมการกระทำความผิดเปลี่ยนแปลงไป เพื่อที่จะสามารถนำตัวผู้กระทำความผิดมาลงโทษ และเป็นการยับยั้งพฤติกรรมการกระทำความผิดดังกล่าว

6. พฤติกรรมการคุกคามนั้นบางครั้งเกิดจากความไม่ปกติทางจิตของผู้คุกคาม บุคคลเหล่านี้อาจจะอยู่ในกลุ่มของบุคคลที่มีพฤติกรรมสร้างความเดือดร้อนรำคาญ หรือก่อให้เกิดความเสียหายกับบุคคลที่ตกเป็นเป้าหมายหรือเหยื่ อ โดยที่คนเหล่านี้นั้นไม่รู้ตัวหรือไม่สามารถควบคุมจิตใต้สำนึกของตนเองได้ จึงกระทำการใด ๆ ที่ถือว่าเป็นการคุกคาม ดังนั้นในกระบวนการยุติธรรมจึงสมควรให้มีการประเมินสุขภาพจิตของผู้กระทำผิดว่า บุคคลเหล่านี้กระทำความผิดเพราะมีปัญหาทางสุขภาพจิตหรือไม่ หรือกระทำความผิดเพราะมีเ จตนาที่จะคุกคามบุคคลอื่นจริง ก่อนที่ศาลจะได้ลงโทษ หากเป็นผู้ที่เป็นโรคจิต

จริง ๆ ก็เป็นการสมควรอย่างยิ่งที่ศาลควรจะกำหนดวิธีการบำบัดหรือเยียวยาผู้คุกคามที่เป็นโรคจิตมากกว่าจะใช้มาตรการลงโทษที่รุนแรง

7. หน่วยงานของภาครัฐและภาคเอกชน ควรจัดตั้งเว็บไซต์กลางขึ้นมาเพื่อสนับสนุนให้มีข้อมูลเกี่ยวกับ Cyberstalking โดยเฉพาะว่าจะทำอย่างไรหากตกเป็นเหยื่อหรืออย่างไรจึงถือว่าเป็น Cyberstalking หรืออาจมีฮอตไลน์สายด่วนให้คำปรึกษาหรือแนะนำแนวทางแก้ไขปัญหาต่างๆ เกี่ยวกับ Cyberstalking สำหรับผู้ที่ถูกคุกคาม เช่นในประเทศสหรัฐอเมริกานั้นมีองค์กรที่ไม่แสวงหากำไร คือ CyberAngles ที่คอยช่วยเหลือเหยื่อผู้ถูกคุกคามทางอินเตอร์เน็ตมีเว็บไซต์ให้บริการ www.cyberangles.org. หรือหน่วยงานหรือเว็บไซต์ต่าง ๆ มากมายที่คอยให้คำแนะนำหรือให้ความช่วยเหลือ อาทิเช่น GetNetWise (www.getnetwise.org) , IACIS (International Association of Computer Investigate : www.iacis.com) , National Center for victim of Crime (www.ncvc.org) , National Cybercrime Training Partnership (www.cybercrime.org) , Privacy Rights Clearinghouse (www.privacyrights.org) , Search Group, Inc. (www.search.org) และ WHOA (Working to Halt Online Abuse : www.haltabuse.org) บรรดาหน่วยงานเหล่านี้เป็นหน่วยงานที่ให้ความรู้ความเข้าใจเกี่ยวกับกฎหมาย เกี่ยวกับอาชญากรรมคอมพิวเตอร์ และเป็น เว็บไซต์ที่ให้ความรู้ในการป้องกันตนเองจากการถูกคุกคาม หรือให้ความรู้ว่าจะทำอย่างไรเมื่อตนเองถูกคุกคาม เป็นต้น

8. ผู้ให้บริการทางอินเตอร์เน็ต (Internet Service Provider : ISP) นั้น นอกจากจะมีเงื่อนไขสำหรับผู้ใช้บริการอินเตอร์ว่าจะไม่ใช้บริการเว็บไซ ต์ในการรบกวนคุกคามบุคคลอื่นแล้ว ผู้ให้บริการควรจะมีบริการสำหรับลูกค้าผู้ใช้อินเตอร์เน็ตในการแจ้งข่าวหรือแจ้งข้อมูลเกี่ยวกับ Cyberstalking เพื่อผู้ให้บริการจะได้ดำเนินการป้องกันอันตรายที่เกิดขึ้นหรือดำเนินการทางกฎหมายกับบรรดา Cyberstalker

9. บุคคลที่ใ ช้อินเตอร์เน็ตควรสร้างจิตสำนึกของตนเองก่อนเป็นอันดับแรกว่าอินเตอร์เน็ตนั้นมีประโยชน์และมีอันตรายไม่ยิ่งหย่อนกว่ากัน และไม่ควรอาศัยช่องว่างของอินเตอร์เน็ตนั้นกระทำผิดกฎหมาย และครอบครัวก็ควรจะหมั่นคอยดูแลสอดส่องพฤติกรรมการใช้อินเตอร์เน็ตของสมาชิกในครอบครัว ด้วยเช่นกันเพื่อป้องกันมิให้เกิดการก่ออาชญากรรม และผู้ใช้อินเตอร์เน็ตเองก็ควรจะแจ้งหน่วยงานที่มีหน้าที่ดูแลเมื่อตนเองถูกคุกคาม

10. ในกรณีที่ตนเองถูกคุกคามในลักษณะของการลงข้อความต่าง ๆ บนเว็บบอร์ดสาธารณะหรือได้รับ อีเมล์ ที่มีลักษณะข่มขู่คุกคามแล้วเหยื่ อควรจะบันทึกข้อมูลต่าง ๆ เหล่านั้นเอาไว้ในรูปลักษณะของเอกสาร หรือบันทึกข้อมูลต่าง ๆ เอาไว้ในแผ่นดิสก์เพื่อใช้เป็นหลักฐานในการดำเนินคดีกับผู้กระทำความผิด

11. ถ้าได้อีเมล์ที่มีข้อความในลักษณะคุกคามหรือรังควาน ให้เปลี่ยนอีเมล์แอดเดรสใหม่ เปลี่ยนรหัสผู้ใช้ และรหัสผ่านใหม่ทั้งหมด ปิด อีเมล์แอดเดรสเดิมทิ้ง และศึกษาวิธีการใช้โปรแกรมกรองจดหมาย หรือศึกษาวิธีการใช้โปรแกรมป้องกัน อีเมล์ที่ไม่ต้องการ เพื่อเป็นการป้องกันตนเองมิให้ถูกคุกคาม

บรรณานุกรม

ภาษาไทย

หนังสือ

จิตติ ติงศภัทิย์. (2545). กฎหมายอาญาภาค 2 ตอน 2และภาค 3 (พิมพ์ครั้งที่ 6). กรุงเทพมหานคร : ห้างหุ้นส่วนจิรรัชการพิมพ์.

ทวีเกียรติ มีนะกนิษฐ์. (2546). หลักกฎหมายอาญาภาคทั่วไป (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม). กรุงเทพมหานคร : สำนักพิมพ์วิญญูชน.

พจนานุกรมราชบัณฑิตยสถาน พ.ศ. 2542, (2546). กรุงเทพฯ : นานมีบุ๊คส์

หยุด แสงอุทัย. (2540). กฎหมายอาญาภาค 2-3 (พิพม์ครั้งที่ 8 แก้ไขเพิ่มเติม). กรุงเทพมหานคร : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

วารสาร

จอมพล พิทักษ์สันตโยธิน. (2548).การตามรังควานบนอินเตอร์เน็ต(Cyberstalking)กับความผิดทางอาญาในสหรัฐอเมริกาและสหราชอาณาจักร.วารสารวิชาการมนุษย์ศาสตร์และสังคมศาสตร์, 13,(19),51-65.

วิทยานิพนธ์

นรเทพ บุญเก็บ,(2548).มาตรการทางกฎหมายเกี่ยวกับการพนันบนอินเตอร์เน็ต. วิทยานิพนธ์ปริญญามหาบัณฑิตคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

วิจิตรา เลิศหิรัญกิจ,(2550).ความผิดฐานเฝ้าติดตามและข่มขู่ Stalking. วิทยานิพนธ์ปริญญามหาบัณฑิตคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

อินเตอร์เน็ต

วิจารณ์ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.....
http://gotoknow.org/blog/LA641/64031. ค้นเมื่อ 15 กันยายน 2550.

ภาษาอังกฤษ

Book

Bryan A. Garner. Black 's Law Dictionary (8th ed.).(2004) St. Paul:Minn West.

Articles

Naomi H. Goodno, Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws," The Berkeley Electronic Press , (2006) : 1- 62.

Internet

CyberAngels. Retrieved April 26, 2007, from http://www.cyberangels.org.

Emma Ogilvie.(2000). "Trends & Issues in crime and criminal justice". Australian Institue of Criminalogy.(September 2000),No.166. Retrived April 24, 2007, from http://www.aic.gov.au.

Mullen, P.,Pathe, M. ,Purcell R. ,and Stuart, G. (1999). "Study of Stalker". American Journal of Psychiatry. Vol. 156. Retrieved April 28, 2007, from http:// ajp.psychiatryonline.org/cgi/content/full.156/8/1244.

P. E. Mullen. "Type of Stalker and Stalking Patterns". Retrieved Febuary 8, 2007, from http://www.sexualharassmentsupport.org/TypesofStalker.html.

Rose Hunter.(2001).“Cyberstalking, Law and the Internet”. Retrieved April 22, 2007, from http//gsu.edu/lawand/papers/fa01/hunter/.

U.S. the Attorney General.(1999). “1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry, A Report from the Attorney General to the Vice President”. Retrived April 25, 2007, from http://www.usdj.gov/criminal/cybercrime/cyberstalking.htm.

“What is a Personal Order Protection Order?” Retrieved May 21, 2007, from http://msu.edu./safe/facts/ppo.html.

Wikipedia, the free encyclopedia “Cyberstalking” Retrieved Febuary 8, 2007, from http://enwikipedia.org/wiki/cyberstalking.

Wikipedia, the free encyclopedia “Stalking” Retrieved Febuary 8, 2007, from http://enwikipedia.org/wiki/stalking.

ภาคผนวก

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๕๐

เป็นปีที่ ๖๒ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบ

คอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑)(๒) (๓) หรือ (๔)

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิด ตาม

มาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือ บุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษจะต้องรับโทษภายในราชอาณาจักร

หมวด ๒
พนักงานเจ้าหน้าที่

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่

อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือ ผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา ๒๐ ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้อง พร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา ๒๑ ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครองหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวงทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจมีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับไม่เกินสองแสนบาทและปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๒๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือ

พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

ที่มา : ราชกิจจานุเบกษา
เล่มที่ ๑๒๔ ตอนที่ ๒๗ ก หน้า ๔ – ๑๓
ประกาศ ณ วันที่ ๑๘ มิถุนายน ๒๕๕๐

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

พ.ศ. .....

.....

.....

.....

....

....

โดยที่เป็นการสมควรให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัตินี้มีบทบัญญัติบางประการที่จำกัดสิทธิและเสรีภาพ ซึ่งมาตรา ๒๙ ประกอบ มาตรา ๓๑ มาตรา ๓๔ มาตรา ๓๕ และมาตรา ๕๘ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย ให้กระทำได้โดยบทบัญญัติของกฎหมาย

....

....

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า " พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ."

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยแปดสิบวันนับแต่วันที่ประกาศในราชกิจจานุเบกษา

มาตรา ๓ ในพระราชบัญญัตินี้

"ข้อมูลส่วนบุคคล" หมายความว่า สิ่งสื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูลหรือสิ่งอื่นใดๆ เกี่ยวกับตัวบุคคลธรรมดาอันมีผลให้สามารถกำหนดตัวบุคคลได้แน่นอนหรือที่อาจกำหนดตัวบุคคลนั้นได้ ไม่ว่าการสื่อสารความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ ที่อาจจัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ ทั้งนี้ หมายความรวมถึงข้อเท็จจริงหรือพฤติการณ์ของผู้ที่ถึงแก่กรรมด้วย

"การประมวลผล" หมายความว่า การดำเนินการใด ๆ เกี่ยวกับการเก็บรวบรวม การบันทึกการจัดหมวดหมู่ การเก็บรักษา การจัดลำดับตำแหน่ง การแก้ไข การเลือก การเรียก การเปรียบเทียบ การใช้ การเชื่อมต่อ การระงับ การเปิดเผยโดยเฉพาะเจาะจง การเปิดเผยทั่วไป การลบ หรือการทำลายซึ่งข้อมูลส่วนบุคคลไม่ว่าจะใช้วิธีการใดๆ และให้หมายความรวมถึงการส่ง หรือโอนข้อมูลส่วนบุคคล

"การเก็บรวบรวม" หมายความว่า การกระทำด้วยประการใดๆ เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล

“การเก็บรักษา” หมายความว่า การกรอกหรือป้อนข้อมูล การบันทึกหรือการเก็บข้อมูลบนสื่อที่ใช้ในการเก็บข้อมูลเพื่อให้สามารถประมวลผลหรือใช้ข้อมูลนั้นได้อีก

“การแก้ไข” หมายความว่า การแก้ไขเปลี่ยนแปลงเนื้อหาสาระของข้อมูลส่วนบุคคลที่เก็บรักษาไว้

“การโอน” หมายความว่า การเปิดเผยข้อมูลส่วนบุคคลที่เก็บรักษาไว้หรือได้จากการประมวลผลต่อบุคคลที่สามไม่ว่าโดยการส่งข้อมูลนั้นไปยังบุคคลที่สามหรือโดยการตรวจ การเรียกดูหรือคิดค้นข้อมูลนั้นโดยบุคคลที่สาม

“การลบ” หมายความว่า การลบข้อมูลส่วนบุคคลที่เก็บไว้ทิ้งไปจากสื่อที่บันทึกเก็บข้อมูลนั้น

“ผู้ประมวลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือองค์กรผู้ดำเนินการประมวลผลตามพระราชบัญญัตินี้

“เจ้าของข้อมูลส่วนบุคคล” ให้หมายความรวมถึง

(๑) ทายาทหรือคู่สมรสของบุคคลนั้นในกรณีที่เจ้าของข้อมูลถึงแก่ความตาย ทั้งนี้ตามลำดับก่อนหลังตามที่กำหนดในกฎกระทรวง

(๒) ผู้ซึ่งมีหน้าที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของบุคคลนั้นตามที่กำหนดในกฎกระทรวง

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“นายทะเบียน” หมายความว่า ผู้ซึ่งได้รับการแต่งตั้งหรือมอบหมายจากผู้ประมวลข้อมูลส่วนบุคคล เพื่อทำหน้าที่ควบคุมดูแลและรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคล

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ

“เลขาธิการ” หมายความว่า เลขาธิการของคณะกรรมการข้อมูลข่าวสารของราชการ

“พนักงานเจ้าหน้าที่” หมายความว่า เลขาธิการและข้าราชการในสังกัดสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการและการคุ้มครองข้อมูลส่วนบุคคล และให้หมายความรวมถึงข้าราชการหรือพนักงาน ซึ่งมาในส่วนราชการในสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการและการคุ้มครองข้อมูลส่วนบุคคล ซึ่งประธานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้แต่งตั้งให้ปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

มาตรา ๔ พระราชบัญญัตินี้ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลข้อมูลส่วนบุคคลทั้งที่เป็นบุคคล องค์กร หรือหน่วยงานของรัฐที่มีวัตถุประสงค์ในการดำเนินงานเชิงธุรกิจหรือการพาณิชย์ เว้นแต่มีบทบัญญัติแห่งกฎหมายในการประมวลผลข้อมูลส่วนบุคคลเรื่องหนึ่งเรื่องใดกำหนดไว้เป็นการเฉพาะให้เป็นไปตามบทบัญญัติแห่งกฎหมายนั้น การยกเว้นการบังคับใช้กับการประมวลผลข้อมูลส่วนบุคคลในลักษณะใดหรือกิจการประเภทใดให้ตราเป็นกฎกระทรวง

เพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่บทบัญญัติแห่งกฎหมายอื่นตามวรรคหนึ่งมิได้บัญญัติถึงการประมวลผลข้อมูลส่วนบุคคลเรื่องหนึ่งเรื่องใดไว้ ให้นำการประมวลผลข้อมูลส่วนบุคคลในเรื่องนั้นตามที่บัญญัติไว้ในพระราชบัญญัตินี้ไปใช้บังคับ

มาตรา ๕ ภายใต้บังคับ มาตรา ๔ พระราชบัญญัตินี้ไม่ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐที่อยู่ภายใต้บังคับตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

มาตรา ๖ ให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัตินี้ และมีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา ๗ ให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลคณะหนึ่ง ประกอบด้วย

(๑) นายกรัฐมนตรีหรือรัฐมนตรีซึ่งนายกรัฐมนตรีมอบหมายเป็นประธานกรรมการ

(๒) กรรมการโดยตำแหน่ง ประกอบด้วย ปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เลขาธิการคณะกรรมการกฤษฎีกา อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ

(๓) กรรมการซึ่งเป็นผู้แทนของหอการค้าไทย สมาคมธนาคารไทย คณะกรรมการสิทธิมนุษยชน คณะกรรมการคุ้มครองผู้บริโภค

(๔) กรรมการผู้ทรงคุณวุฒิซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญด้านกฎหมายและด้านการประมวลผลอิเล็กทรอนิกส์ จำนวนสี่คน

ให้เลขาธิการเป็นกรรมการและเลขานุการและเจ้าหน้าที่สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการและการคุ้มครองข้อมูลส่วนบุคคล จำนวนไม่เกิน ๒ คน เป็นผู้ช่วยเลขานุการ

การได้มาซึ่งกรรมการตาม (๔) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะรัฐมนตรีกำหนดและประกาศในราชกิจจานุเบกษา

มาตรา ๘ กรรมการผู้ทรงคุณวุฒิให้มีวาระการดำรงตำแหน่งคราวละสามปี ผู้พ้นจากตำแหน่งแล้วอาจได้รับการแต่งตั้งอีกได้ในกรณีที่กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งตามวาระ แต่ยังมิได้แต่งตั้งกรรมการใหม่ให้กรรมการซึ่งพ้นจากตำแหน่งนั้นปฏิบัติหน้าที่ต่อไปจนกว่าจะได้มีการแต่งตั้งกรรมการขึ้นใหม่

มาตรา ๙ นอกจากการพ้นตำแหน่งตามวาระ กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ลาออก

(๓) คณะรัฐมนตรีมีมติให้ออกเพราะบกพร่องต่อหน้าที่ มีความประพฤติเสื่อมเสียหรือหย่อนความสามารถ

(๔) เป็นบุคคลล้มละลาย

(๕) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๖) ได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

มาตรา ๑๐ ในกรณีที่กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนครบวาระและยังมิได้แต่งตั้งกรรมการขึ้นแทนตำแหน่งที่ว่าง ให้กรรมการที่เหลืออยู่ปฏิบัติหน้าที่ต่อไปได้

เมื่อกรรมการผู้ทรงคุณวุฒิว่างลงก่อนครบวาระให้ดำเนินการแต่งตั้งกรรมการภายในสามสิบวัน เว้นแต่วาระของกรรมการเหลือไม่ถึงหนึ่งร้อยแปดสิบวันจะไม่แต่งตั้งกรรมการก็ได้ ทั้งนี้ ให้กรรมการซึ่งได้รับแต่งตั้งมีวาระการดำรงตำแหน่งเท่ากับเวลาที่เหลืออยู่ของกรรมการที่ยังอยู่ในตำแหน่ง

มาตรา ๑๑ คณะกรรมการมีอำนาจและหน้าที่ ดังต่อไปนี้

(๑) กำหนดนโยบาย มาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

(๒) เสนอความเห็นต่อนายกรัฐมนตรีเพื่อออกกฎกระทรวงตามพระราชบัญญัตินี้

(๓) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใดๆ ในการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมในการพัฒนาเทคโนโลยีที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(๔) กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประมวลผล

(๕) กำหนดหลักเกณฑ์และเงื่อนไขในการได้รับเครื่องหมายรับรองการประมวลผล

(๖) ติดตาม ตรวจสอบและประเมินผลการดำเนินการของผู้ประมวลข้อมูลส่วนบุคคล

(๗) พิจารณาดำเนินการเกี่ยวกับเรื่องร้องเรียนตามพระราชบัญญัตินี้

(๘) ออกระเบียบ ข้อบังคับ ประกาศ คำสั่งหรือปฏิบัติการอื่นใดเพื่อให้เป็นไปตามวัตถุประสงค์ของพระราชบัญญัตินี้

(๙) แต่งตั้งคณะอนุกรรมการ เพื่อดำเนินการใดๆ ตามพระราชบัญญัตินี้ตามความจำเป็นและเหมาะสม

(๑๐) ปฏิบัติการอื่นตามที่บัญญัติไว้ในพระราชบัญญัตินี้หรือตามที่กฎหมายอื่น

กำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการหรือตามที่นายกรัฐมนตรีหรือคณะรัฐมนตรีมอบหมาย

(๑๑) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงแก้ไขกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องและเหมาะสม

(๑๒) จัดทำรายงานเกี่ยวกับการปฏิบัติการตามพระราชบัญญัตินี้เสนอต่อคณะรัฐมนตรีรัฐสภาหรือสาธารณชนเป็นครั้งคราวตามความเหมาะสมอย่างน้อยปีละหนึ่งครั้ง

ในการปฏิบัติหน้าที่ตามมาตรานี้ ให้สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการและการคุ้มครองข้อมูลส่วนบุคคลเป็นหน่วยงานฝ่ายเลขานุการของคณะกรรมการและปฏิบัติหน้าที่ตามที่คณะกรรมการมอบหมาย

มาตรา ๑๒ ในการประชุมคณะกรรมการ ถ้าประธานกรรมการไม่มาประชุมหรือไม่อยู่ในที่ประชุมให้กรรมการที่มาประชุมเลือกกรรมการคนหนึ่งเป็นประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากันให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

กรรมการผู้ใดมีส่วนได้เสียไม่ว่าโดยตรงหรือโดยอ้อมในเรื่องที่ที่ประชุมพิจารณา ให้แจ้งการมีส่วนได้เสียของตนให้คณะกรรมการทราบล่วงหน้าก่อนการประชุมและห้ามมิให้ผู้นั้นเข้าร่วมประชุมพิจารณาในเรื่องดังกล่าว

มาตรา ๑๓ ในการปฏิบัติหน้าที่ตามมาตรา ๑๑ คณะกรรมการหรือคณะอนุกรรมการอาจเชิญบุคคลใดมาให้ข้อเท็จจริง คำอธิบาย คำแนะนำ หรือความเห็น หรือให้บุคคลใดส่งเอกสารหรือหลักฐานที่เกี่ยวข้องหรือสิ่งใดมาเพื่อประกอบการพิจารณาได้ตามที่เห็นสมควร

มาตรา ๑๔ เมื่อมีเหตุอันควรสงสัยว่าการดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลซึ่งอาจก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือบุคคลที่เกี่ยวข้อง คณะกรรมการอาจสั่งให้ผู้ประมวลข้อมูลส่วนบุคคลดำเนินการพิสูจน์การดำเนินการดังกล่าวได้ ถ้าผู้ประมวลข้อมูลส่วนบุคคลไม่ดำเนินการพิสูจน์การดำเนินการนั้นหรือดำเนินการล่าช้า โดยไม่มีเหตุผลอันสมควรคณะกรรมการอาจจัดให้มีการพิสูจน์โดยผู้ประมวลข้อมูลส่วนบุคคลเป็นผู้เสียค่าใช้จ่ายก็ได้

ถ้าผลจากการพิสูจน์ปรากฏว่าการดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลของหน่วยงานหรือผู้ประมวลข้อมูลส่วนบุคคลอาจก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องหรือบุคคลอื่น และกรณีไม่อาจป้องกันความเสียหายที่จะเกิดจากการดำเนินการนั้นได้ตามที่กำหนดในกฎหมายนี้หรือกฎหมายอื่นให้คณะกรรมการมีอำนาจสั่งห้ามการดำเนินการนั้น และถ้าเห็นสมควรจะสั่งให้หน่วยงานหรือผู้ประมวลข้อมูลส่วนบุคคลทำลายหรือจะจัดให้มีการทำลายโดยหน่วยงานหรือผู้ประมวลข้อมูลส่วนบุคคลเป็นผู้เสียค่าใช้จ่ายก็ได้

ในกรณีจำเป็นเร่งด่วน ถ้าคณะกรรมการมีเหตุที่น่าเชื่อว่าการดำเนินใดๆ เกี่ยวกับข้อมูลส่วนบุคคลอาจก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้อง ให้คณะกรรมการมีอำนาจสั่งห้ามการดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลตามวรรคหนึ่งหรือวรรคสองได้ตามสมควร

การสั่งห้ามดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลตามวรรคสองและวรรคสาม ให้ประกาศในราชกิจจานุเบกษา

มาตรา ๑๕ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ คณะกรรมการต้องให้โอกาสแก่ผู้ถูกกล่าวหาหรือสงสัยว่ากระทำการอันเป็นการฝ่าฝืนบทบัญญัติแห่งพระราชบัญญัตินี้ได้ทราบข้อเท็จจริงอย่างเพียงพอ ชี้แจงเหตุผลหรือแสดงความคิดเห็นและมีโอกาสโต้แย้งและแสดงพยานหลักฐานของตนตามสมควร

ความในวรรคหนึ่งมิให้นำมาใช้บังคับในกรณีดังต่อไปนี้ เว้นแต่คณะกรรมการจะเห็นสมควรปฏิบัติเป็นอย่างอื่น

(๑) เมื่อมีความจำเป็นรีบด่วนหากปล่อยให้เนิ่นช้าไปจะก่อให้เกิดความเสียหายอย่างร้ายแรงแก่ผู้หนึ่งผู้ใดหรือจะกระทบต่อประโยชน์สาธารณะ

(๒) เมื่อจะมีผลทำให้ระยะเวลาที่กำหนดไว้ในกฎหมายหรือกฎต้องล่าช้าออกไป

(๓) เมื่อเป็นข้อเท็จจริงที่คู่กรณีนั้นเองได้ให้ไว้ในคำขอ คำให้การหรือคำแถลง

(๔) เมื่อโดยสภาพเห็นได้ชัดในตัวว่าการให้โอกาสดังกล่าวไม่อาจกระทำได้

(๕) กรณีอื่นตามที่คณะกรรมการประกาศกำหนด

การกำหนดหรือการออกคำสั่งในเรื่องใดตามพระราชบัญญัตินี้ให้คณะกรรมการคำนึงถึงความเสียหายที่อาจเกิดขึ้นแก่เจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้อง และในกรณีที่เห็นสมควรคณะกรรมการอาจกำหนดเงื่อนไขหรือวิธีการชั่วคราวในการบังคับให้เป็นไปตามคำสั่งก็ได้

หมวด ๒
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา ๑๖ ให้มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ โดยมีผู้อำนวนการสำนักงานเป็นผู้บังคับบัญชาและรับผิดชอบในการปฏิบัติราชการของสำนักงาน

มาตาม ๑๗ ให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีอำนาจหน้าที่ปฏิบัติงานเกี่ยวกับงานวิชาการและธุรการให้แก่คณะกรรมการตามพระราชบัญญัตินี้ รวมทั้งให้มีอำนาจหน้าที่ ดังต่อไปนี้

(๑) ประสานงานกับส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(๒) ให้คำปรึกษาแก่องค์กรภาครัฐและภาคเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

(๓) วางระเบียบรวมถึงการกำหนดหลักสูตรฝึกอบรมการปฏิบัติหน้าที่ของนายทะเบียน

(๔) จัดทำบัญชีรายชื่อผู้ประมวลผลข้อมูลส่วนบุคคล

(๕) ติดตามและประมวลผลในการปฏิบัติตามพระราชบัญญัตินี้

(๖) ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการมอบหมาย

หมวด ๓
การประมวลผลข้อมูลส่วนบุคคล

มาตรา ๑๘ การประมวลผลข้อมูลส่วนบุคคลจะกระทำมิได้ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลและเป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้หรือตามกฎหมายอื่นที่เกี่ยวข้อง

ในการประมวลผลข้อมูลส่วนบุคคลตามวรรคหนึ่ง ต้องเป็นไปเพื่อประโยชน์ในการดำเนินการตามวัตถุประสงค์ของกิจการของผู้นั้น

มาตรา ๑๙ ผู้ดำเนินการประมวลข้อมูลส่วนบุคคลต้องดำเนินการให้เป็นตามหลักเกณฑ์วิธีการและเงื่อนไขที่บัญญัติไว้ในพระราชบัญญัตินี้

เพื่อประโยชน์ในการให้ความคุ้มครองข้อมูลส่วนบุคคลและการประมวลผลตามพระราชบัญญัตินี้คณะกรรมการจะกำหนดประมวลจริยธรรมเกี่ยวกับการประมวล ผลก็ได้

มาตรา ๒๐ ให้ผู้ซึ่งต้องดำเนินการประมวลผลตามมาตรา ๑๙ จัดให้มีนายทะเบียนทำหน้าที่ควบคุมดูและรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคล

รายชื่อผู้ทำหน้าที่นายทะเบียนตามวรรคหนึ่ง ให้ผู้ประมวลข้อมูลส่วนบุคคลแจ้งให้คณะกรรมการทราบภายในเจ็ดวันนับแต่วันที่ได้แต่งตั้ง ในกรณีที่มิได้แจ่งตั้งบุคคลอื่นเป็นนายทะเบียนให้ถือว่าผู้นั้นเป็นนายทะเบียน ถ้าเป็นนิติบุคคลให้ถือว่าผู้จัดการหรือผู้แทนของนิติบุคคลนั้นเป็นนายทะเบียน

ผู้ซึ่งจะได้รับการแต่งตั้งเป็นนายทะเบียนตามวรรคหนึ่งต้องมีคุณสมบัติตามที่คณะกรรมการกำหนด

ส่วนที่ ๑
การเก็บรวบรวมข้อมูลส่วนบุคคล

.....

มาตรา ๒๑ การเก็บรวบรวมข้อมูลส่วนบุคคลต้องเป็นไปเพียงเท่าที่เกี่ยวข้องและจำเป็นแก่การดำเนินกิจการตามวัตถุประสงค์ของผู้ประมวลข้อมูลส่วนบุคคลเท่านั้น

ในการเก็บรวบรวมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ห้ามมิให้เก็บรวบรวมส่วนบุคคลที่เกี่ยวกับพฤติกรรมทางเพศ ประวัติอาชญากรรม ประวัติสุขภาพ หรือข้อมูลอื่นใดที่กระทบต่อความรู้สึกของผู้อื่นหรือประชาชนตามที่กำหนดในกฎกระทรวง เว้นแต่ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลหนึ่งบุคคลใด จากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรงโดยปราศจากความยินยอมของเจ้าของข้อมูลจะกระทำมิได้ เว้นแต่

(๑) การเก็บรวบรวมข้อมูลดังกล่าวเป็นสิ่งที่จำเป็นสำหรับการรักษาพยาบาลเจ้าของข้อมูลและเจ้าของข้อมูลไม่สามารถให้คำยินยอมได้

(๒) การเก็บรวบรวมข้อมูลดังกล่าวเป็นไปเพื่อการสืบสวน สอบสวนหรือเพื่อการตรวจสอบการกระทำหรือความประพฤติและมีเหตุผลที่น่าเชื่อถือได้ว่าการเก็บข้อมูลส่วนบุคคลโดยขอคำยินยอมจากเจ้าของข้อมูลก่อนจะมีผลกระทบต่อความมีอยู่หรือความถูกต้องของข้อมูล

(๓) การเก็บรวบรวมข้อมูลส่วนบุคคลซึ่งได้จากการดูสังเกตการณ์ การแสดงกีฬาหรือกิจกรรมอื่นที่คล้ายคลึงกัน เมื่อบุคคลที่ถูกเก็บรวบรวมข้อมูลนั้นได้ปรากฏตัวหรือเข้าร่วมกิจกรรมนั้นด้วยความสมัครใจและกิจกรรมนั้นเป็นกิจกรรมที่เปิดเผยต่อสาธารณะ

(๔) การเก็บรวบรวมนั้น เป็นสิ่งจำเป็นเพื่อใช้ประกอบการพิจารณาตัดสินความเหมาะสมของบุคคลในการที่ให้ได้รับรางวัลเกียรติยศ หรือผลประโยชน์ในลักษณะคล้ายคลึงกัน

(๕) การเก็บรวบรวมข้อมูลโดยหน่วยงานข้อมูลด้านเครดิต ซึ่งมีหน้าที่เก็บรวบรวมข้อมูลบุคคลเพื่อทำรายงานข้อมูลเครดิต และเจ้าของข้อมูลส่วนบุคคลได้ให้คำยินยอมไว้ในครั้งแรกที่มีการจัดเก็บข้อมูลว่าให้สามารถเก็บรวบรวมเปิดเผยเพื่อการจัดทำข้อมูลเครดิตนี้ได้

(๖) การเก็บรวบรวมซึ่งเป็นไปตามที่กฎหมายบัญญัติ

มาตรา ๒๒ ในการเก็บรวบรวมข้อมูลส่วนบุคคลให้นายทะเบียนแจ้งต่อเจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่จะดำเนินการถึงรายละเอียด ดังต่อไปนี้

(๑) ชื่อ สถานที่ทำการ และสถานภาพของผู้ประมวลข้อมูล

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูล

(๓) ประเภทของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมข้อมูล

(๔) วิธีการเก็บรวบรวมข้อมูลส่วนบุคคล

(๕) ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

(๖) เงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคล

(๗) รายละเอียดอื่นตามที่คณะกรรมการกำหนด

มาตรา ๒๓ เมื่อนายทะเบียนได้ดำเนินการเก็บรวบรวมข้อมูลข้อมูลส่วนบุคคลแล้ว ให้จัดทำรายการการจัดเก็บข้อมูส่วนบุคคลหรือระบบข้อมูลส่วนบุคคล ณ สถานที่ทำการเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้

มาตรา ๒๔ ความในส่วนนี้มิให้ใช้คับแก่กิจการตามกฎหมายว่าด้วยการพิมพ์ หรือกิจการอื่นตามที่กำหนดในกระทรวง

ส่วนที่ ๒
การใช้และการเปิดเผยข้อมูลส่วนบุคคล

.....

มาตรา ๒๕ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องใช้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูแลตามวัตถุประสงค์ของการรวบรวมเท่านั้น

การใช้ข้อมูลส่วนบุคคลนอกเหนือจากวัตถุประสงค์ของการเก็บรวบรวมให้ผู้ประมวลข้อมูลส่วนบุคคลแจ้งต่อเจ้าของข้อมูลส่วนบุคคลเป็นหนังสือโดยแสดงเหตุผลในการดำเนินการดังกล่าวและต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลด้วย

ในกรณีที่มีเหตุจำเป็นที่มีผลกระทบต่อชีวิต ร่างกายหรืออนามัยของบุคคล ซึ่งอาจดำเนินการตามวรรคสองได้ให้ผู้ประมวลข้อมูลส่วนบุคคลใช้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูและได้เท่าที่จำเป็นแห่งการนั้น โดยมิต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง ทั้งนี้ผู้ประมวลข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลนั้นทราบโดยเร็ว

มาตรา ๒๖ การเปิดเผยข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูและของตนต่อผู้อื่นโดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลส่วนบุคคลจะกระทำมิได้ เว้นแต่เป็นการเปิดเผยในกรณี ดังต่อไปนี้

(๑) เจ้าหน้าที่ของรัฐร้องขอเพื่อป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวนการสอบสวนหรือการฟ้องคดีไม่ว่าเป็นคดีประเภทใดก็ตาม

(๒) ศาลและเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐที่มีอำนาจตามกฎหมายที่จะขอข้อมูลส่วนบุคคลดังกล่าว

(๓) เพื่อป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(๔) หน่วยงานอื่นที่มีบทบัญญัติของกฎหมายให้อำนาจ

(๕) เพื่อประโยชน์ในการศึกษาวิจัยโดยไม่ระบุหรือมีส่วนใดที่ทำให้รู้ว่าเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับบุคคลใด

(๖) ปรากฏโดยชัดแจ้งว่า เพื่อประโยชน์ของเจ้าของข้อมูลและการขอความยินยอมไม่สามารถดำเนินการได้ในเวลาที่จำเป็นนั้น

(๗) เพื่อการรักษาพยาบาลเจ้าของข้อมูล และในขณะนั้น เจ้าของข้อมูลไม่อยู่ในสภาวะตามกฎหมายที่จะให้ความยินยอมได้

การเปิดเผยข้อมูลส่วนบุคคลตาม(๑)(๒)(๓)(๔)(๔)(๕)(๖) และ(๗) ให้ผู้ประมวลข้อมูลส่วนบุคคลต้องเปิดเผยเฉพาะที่เกี่ยวข้องกับเจ้าของข้อมูลนั้นโดยตรง และเท่าที่จำเป็นและเหมาะสมแก่การนั้น ทั้งนี้เมื่อเปิดเผยข้อมูลประการใดแล้วให้แจ้งให้เจ้าของข้อมูลทราบ

ผู้ซึ่งได้รับข้อมูลส่วนบุคคลจากการเปิดเผยข้อมูลตามวรรคหนึ่ง จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับเพื่อวัตถุประสงค์อย่างอื่นนอกเหนือจากที่ได้แจ้งความประสงค์ไว้

ส่วนที่ ๓
การเก็บรักษา การแก้ไขและการโอนข้อมูลส่วนบุคคล

.....

มาตรา ๒๗ ผู้ประมวลผลข้อมูลส่วนบุคคลจะเก็บรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลนั้นไว้ได้เท่าระยะเวลาที่กำหนดในมาตรา ๒๒ (๕) หรือเท่าที่จำเป็นตามวัตถุประสงค์ของการเก็บรวบรวมของผู้ประมวลผลข้อมูลส่วนบุคคลนั้น

เมื่อกำหนดระยะเวลาหรือหมดความจำเป็นในการเก็บรวบรวมข้อมูลส่วนบุคคลตามวรรคหนึ่งหรือเจ้าของข้อมูลเพิกถอนความยินยอม ให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลนั้นโดยเร็ว ในกรณีที่จำเป็นเพื่อประโยชน์ในกิจการของผู้ประมวลผลข้อมูลนั้นที่ต้องมีการรวบรวมข้อมูลส่วนบุคคลดังกล่าวไว้เพื่อเป็นสถิติหรือการศึกษาวิจัย ผู้ประมวลผลข้อมูลส่วนบุคคลอาจไม่ลบหรือทำลายข้อมูลส่วนนั้นได้แต่ต้องมีหนังสือแจ้งเจ้าของข้อมูลส่วนบุคคลนั้นเพื่อให้ความยินยอมเป็นหนังสือ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมแล้วให้ผู้ประมวลผลข้อมูลส่วนบุคคลนั้นมีหน้าที่และความรับผิดในข้อมูลส่วนบุคคลนั้นตามพระราชบัญญัตินี้

มาตรา ๒๘ ให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แก้ไขข้อมูลส่วนบุคคลที่อยู่ในความครอบครองให้ถูกต้อง สมบูรณ์และทันสมัย ตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอเป็นหนังสือ

ในการแก้ไขข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ประมวลผลข้อมูลส่วนบุคคลอาจขอให้เจ้าของข้อมูลส่วนบุคคลนั้นจัดส่งเอกสารหรือหลักฐานที่เกี่ยวข้องเพื่อประกอบการแก้ไขก็ได้

ในกรณีที่ข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้แก้ไข ซึ่งโดยการเก็บรวบรวมอาจไม่ดำเนินการแก้ไขได้โดยวิธีอื่นนอกจากการทำลายเพื่อเก็บรวบรวมใหม่ ให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการทำลายเพื่อเก็บรวบรวมข้อมูลดังกล่าวใหม่ตามที่ขอแก้ไขได้โดยแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบล่วงหน้าไม่น้อยกว่าเจ็ดวัน

มาตรา ๒๙ ผู้ประมวลผลข้อมูลส่วนบุคคลจะส่งหรือโอนข้อมูลส่วนบุคคลที่อยู่ในครอบครองหรือควบคุมดูแลให้กับผู้อื่นไม่ได้ เว้นแต่ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล หรือตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนด

ในกรณีที่มีความจำเป็นเร่งด่วนที่หากรอให้ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งแล้ว จะก่อให้เกิดความเสียหายแก่ส่วนรวมหรือชีวิต ร่างกาย หรืออนามัยของบุคคลให้ผู้ประมวลข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลนั้นได้ แต่ให้นายทะเบียนแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบโดยเร็ว ทั้งนี้ภายในไม่เกิน ๑๕ วัน นับแต่วันส่งหรือโอนข้อมูลแล้วแต่กรณี

มาตรา ๓๐ การส่งหรือโอนข้อมูลส่วนบุคคลออกไปนอกราชอาณาจักรโดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลส่วนบุคคลจะกระทำมิได้ เว้นแต่เป็นการกระทำตามบทบัญญัติแห่งกฎหมาย หรือเพื่อการดำเนินคดีนอกราชอาณาจักร หรือเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลนั้นและเมื่อมีการโอนแล้วให้ทำรายงานไว้ด้วย

การขอความยินยอมตามวรรคหนึ่ง ให้ผู้ประมวลข้อมูลส่วนบุคคลผู้โอนระบุชื่อและประเทศผู้รับโอนข้อมูล ข้อมูลส่วนบุคคลที่จะโอนและวัตถุประสงค์ของการโอนในหนังสือขอความยินยอมด้วย

มาตรา ๓๑ ห้ามมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศซึ่งมิได้มีบทบัญญัติในการให้ความคุ้มครองข้อมูลส่วนบุคคลหรือมีแต่บทบัญญัติของกฎหมายในประเทศนั้นมีมาตรฐานในการให้ความคุ้มครองข้อมูลส่วนบุคคลในสาระสำคัญต่ำกว่าบทบัญญัติแห่งพระราชบัญญัตินี้ เว้นแต่ในกรณีต่อไปนี้

(๑) ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูล

(๒) กรณีอื่นตามที่คณะกรรมการประกาศกำหนด

หมวด ๔
สิทธิของเจ้าของข้อมูลส่วนบุคคล

.....

มาตรา ๓๒ ภายใต้บังคับของกฎหมายเจ้าของข้อมูลส่วนบุคคลมีสิทธิดังต่อไปนี้

(๑) เข้าตรวจดูข้อมูลส่วนบุคคลที่เกี่ยวกับตน ขอสำเนาหรือขอสำเนารับรองถูกต้องข้อมูลส่วนบุคคลดังกล่าวได้

(๒) ขอให้แก้ไขหรือเปลี่ยนแปลงข้อมูลส่วนบุคคลที่เกี่ยวกับตนให้ถูกต้อง สมบูรณ์หรือทันสมัย

(๓) ขอให้ระงับการใช้หรือเปิดเผยกรณีที่ข้อมูลส่วนบุคคลที่เกี่ยวกับตนไม่ถูกต้องตามความเป็นจริง

(๔) ขอให้ลบหรือทำลายข้อมูลส่วนบุคคลส่วนที่พ้นระยะเวลาการเก็บรวบรวม

หรือไม่เกี่ยวข้องหรือเกินกว่าความเป็นจริงตามวัตถุประสงค์การเก็บรวบรวมข้อมูลส่วนบุคคลนั้น

มาตรา ๓๓ ในกรณีเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ คนไร้ความสามารถคนเสมือนไร้ความสามารถให้ผู้ใช้อำนาจปกครอง ผู้อนุบาล หรือผู้พิทักษ์แล้วแต่กรณีมีสิทธิดำเนินการตามบทบัญญัติแห่งพระราชบัญญัตินี้

มาตรา ๓๔ เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ ผู้ซึ่งได้รับข้อมูลส่วนบุคคลจากการเปิดเผยข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคลโดยมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลจะต้องเปิดเผยถึงการได้มาของข้อมูลให้เจ้าของข้อมูลทราบ หากไม่เปิดเผยผู้ซึ่งได้รับข้อมูลส่วนบุคคลมาโดยมิได้รับความยินยอมจะต้องรับผิดชอบชดใช้ค่าสินไหมทดแทนในความเสียหายที่เกิดขึ้นให้แก่เจ้าของข้อมูลส่วนบุคคล

กรณีที่ผู้ซึ่งได้รับข้อมูลส่วนบุคคลมาโดยมิได้รับความยินยอมไม่ยอมเปิดเผยถึงแหล่งที่มาของข้อมูลส่วนบุคคลตามวรรคหนึ่ง เจ้าของข้อมูลอาจร้องขอให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลพิจารณาให้ผู้ซึ่งได้รับข้อมูลส่วนบุคคลไว้โดยมิได้รับความยินยอมเปิดเผยถึงที่มาของแหล่งข้อมูลก็ได้

คำสั่งของคณะกรรมการตามวรรคก่อนไม่ตัดสิทธิเจ้าของข้อมูลส่วนบุคคลในอันที่จะเรียกร้องค่าสินไหมทดแทนจากผู้ซึ่งได้รับข้อมูลส่วนบุคคลมาโดยมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

หมวดที่ ๕
หน้าที่นายทะเบียน

.....

มาตรา ๓๕ นายทะเบียนมีหน้าที่ประมวลผลข้อมูลส่วนบุคคลให้ถูกต้อง ทันสมัย ครบถ้วนและรักษาความปลอดภัยของข้อมูลส่วนบุคคลไม่ให้สูญหาย ถูกแก้ไขเปลี่ยนแปลง เปิดเผยหรือกระทำการใด ๆ แก่ข้อมูลส่วนบุคคลให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือผู้ซึ่งเกี่ยวข้อง ทั้งนี้ตามหลักเกณฑ์ วิธีการและเงื่อนไขที่คณะกรรมการกำหนด

ในกรณีที่มีความจำเป็นเพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการอาจสั่งให้นายทะเบียนรายงานการประมวลผลเพิ่มเติมจากที่กำหนดในวรรคหนึ่งก็ได้

มาตรา ๓๖ ให้นายทะเบียนรายงานการประมวลผลต่อคณะกรรมการอย่างน้อยปีละหนึ่งครั้งทั้งนี้ตามหลักเกณฑ์ วิธีการที่กำหนดในกฎกระทรวง

หมวดที่ ๖
การร้องเรียน

.....

มาตรา ๓๗ เมื่อมีการร้องเรียนตามพระราชบัญญัตินี้ คณะกรรมการต้องดำเนินการให้แล้วเสร็จโดยเร็วและต้องเปิดโอกาสให้ผู้ร้องเรียน เจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องชี้แจงและแสดงพยานหลักฐานประกอบคำชี้แจงของตนได้ตามสมควร

เรื่องใดที่คณะกรรมการสั่งไม่รับไว้พิจารณาหรือให้ยุติเรื่องให้แจ้งแก่ผู้ร้องเรียนทราบพร้อมทั้งเหตุผลที่ไม่รับไว้พิจารณาให้ยุติเรื่อง

มาตรา ๓๘ ในกรณีที่นายทะเบียนไม่ปฏิบัติตามที่บัญญัติไว้ในพระราชบัญญัตินี้ หรือปฏิบัติการไม่เป็นไปตามที่บัญญัติไว้ในพระราชบัญญัตินี้ ให้เจ้าของข้อมูลส่วนบุคคลผู้ซึ่งได้รับความเสียหายมีสิทธิแจ้งเป็นหนังสือให้นายทะเบียนดำเนินการแก้ไขหรือดำเนินการให้ถูกต้องภายในสิบห้าวันนับแต่วันที่ได้รับแจ้ง

ถ้านายทะเบียนไม่ดำเนินการแก้ไขหรือดำเนินการให้ถูกต้องหรือไม่ดำเนินการภายในที่กำหนดนับแต่วันที่ได้รับแจ้ง ให้เจ้าของข้อมูลส่วนบุคคลหรือผู้ซึ่งได้รับความเสียหายนั้นมีสิทธิยื่นคำร้องเรียนต่อคณะกรรมการเพื่อขอให้สั่งให้นายทะเบียนดำเนินการได้

เมื่อได้รับคำร้องเรียนตามวรรคหนึ่ง ให้คณะกรรมการพิจารณาและมีคำสั่งให้แล้วเสร็จภายในสามสิบวันนับแต่วันที่ได้รับคำร้องเรียน

การยื่นและการพิจารณคำร้องเรียนให้เป็นไปตามระเบียบที่คณะกรรมการกำหนด

มาตรา ๓๙ ในกรณีที่นายทะเบียนไม่รายงานตามมาตรา ๓๖ และคณะกรรมการได้แจ้งเตือนแล้วหรือไม่ปฏิบัติตามคำสั่งของคณะกรรมการตามมาตรา ๑๔ หรือมาตรา ๓๘ วรรคสาม คณะกรรมการอาจสั่งให้ผู้ประมวลข้อมูลส่วนบุคคลนั้นเปลี่ยนนายทะเบียนได้

มาตรา ๔๐ ในกรณีที่ผู้ประมวลข้อมูลส่วนบุคคลไม่ดำเนินการตามบทบัญญัติแห่งพระราชบัญญัตินี้และก่อความเสียหายอย่างร้ายแรงแก่ส่วนรวมหรือต่อชีวิต ร่างกายและอนามัยของบุคคล หากผู้ประมวลผลข้อมูลส่วนบุคคลนั้นเป็นผู้ประกอบกิจการตามกฎหมายอื่นด้วยแล้ว คณะกรรมการอาจเสนอความเห็นต่อหน่วยงานที่มีอำนาจหน้าที่ในการควบคุมหรือกำกับดูแล การประกอบกิจการของผู้ประมวลข้อมูลส่วนบุคคล เพื่อให้มีคำสั่งให้หยุดประกอบกิจการ หรือพักใช้หรือเพิกถอนใบอนุญาตประกอบกิจการตามกฎหมายอื่นนั้นก็ได้ ทั้งนี้ตามความร้ายแรงและกรณี

หมวดที่ ๗
พนักงานเจ้าหน้าที่

.....

มาตรา ๔๑ ในการปฏิบัติการให้เป็นไปตามพระราชบัญญัตินี้ให้พนักงานเจ้าหน้าที่โดยความเห็นชอบของเลขาธิการมีอำนาจหน้าที่ ดังต่อไปนี้

(๑) เรียกให้บุคคลมาให้ถ้อยคำหรือส่งวัตถุ เอกสาร หรือพยานหลักฐานมาประกอบการพิจารณาเพื่อประโยชน์ในการปฏิบัติการให้เป็นไปตามพระราชบัญญัตินี้

(๒) เข้าไปในอาคารหรือสถานที่ที่เกี่ยวข้องกับการประมวลผลตามพระราชบัญญัตินี้ ในระหว่างเวลาทำการของผู้ดำเนินการประมวลผลนั้น เพื่อตรวจสอบว่ามีการกระทำอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้หรือไม่ รวมถึงดูเอกสารและหลักฐานอื่นที่เกี่ยวข้อง เพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคล

(๓) ตรวจสถานที่ที่เกี่ยวกับเรื่องที่มีการร้องเรียน โดยแจ้งให้เจ้าของข้อมูลหรือผู้ครอบครองสถานที่ทราบล่วงหน้าในเวลาอันควร

(๔) ยึดหรืออายัดทรัพย์สิน เอกสาร หรือสิ่งของที่เกี่ยวกับการกระทำความผิดเพื่อประโยชน์ในการดำเนินการตามพระราชบัญญัตินี้

(๕) ปฏิบัติการอื่นตามที่กำหนดไว้ในพระราชบัญญัตินี้ หรือตามที่กฎหมายอื่นกำหนดหรือตามที่คณะกรรมการร้องขอ

มาตรา ๔๒ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลอื่นซึ่งเกี่ยวข้อง

บัตรประจำตัวพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่กำหนดในกฎกระทรวง

มาตรา ๔๓ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ให้พนักงานเจ้าหน้าที่เป็นเจ้าพนักงานตามประมวลกฎหมายอาญา

หมวด ๘
มาตรการส่งเสริม

.....

มาตรา ๔๔ ผู้ประมวลข้อมูลส่วนบุคคลอาจขอรับการส่งเสริมและสนับสนุนจากสำนักงานในการให้ความช่วยเหลือ แนะนำและให้คำปรึกษาในการดำเนินการประมวลผลหรือการดำเนินการอื่นที่เกี่ยวข้อง รวมถึงการอบรมพัฒนาความรู้ความสามารถของบุคลการซึ่งปฏิบัติงานเกี่ยวกับการประมวลผลหรือการดำเนินงานอื่นที่เกี่ยวข้อง

มาตรา ๔๕ ในการพิจารณาคำขอรับการส่งเสริมและสนับสนุนตามมาตรา ๔๔ให้คณะกรรมการพิจารณาตามที่เห็นควร โดยคำนึงถึงความจำเป็นในการให้ความคุ้มครองข้อมูล

ส่วนบุคคลในเรื่องนั้น ทั้งนี้คณะกรรมการอาจขอความร่วมมือจากผู้ประมวลข้อมูลส่วนบุคคลอื่นหรือหน่วยงานของรัฐก็ได้

มาตรา ๔๖ ในแต่ละปีให้สำนักงานประเมินผลการประมวลผลของผู้ประมวลผลข้อมูลส่วนบุคคลหากผู้ประมวลข้อมูลส่วนบุคคลใดดำเนินการประมวลผลได้อย่างมีประสิทธิภาพและเป็นไปตามหลักเกณฑ์และมาตรฐานที่คณะกรรมการกำหนด ให้สำนักงานเสนอต่อคณะกรรมการเพื่อให้ได้รับเครื่องหมายรับรองมาตรฐานการประมวลผล

ลักษณะและรายละเอียดของเครื่องหมายรับรองมาตรฐานการประมวลผลให้เป็นไปตามที่คณะกรรมการกำหนด

หมวดที่ ๙
ความรับผิดทางแพ่ง

.....

มาตรา ๔๗ ผู้ประมวลข้อมูลส่วนบุคคล ผู้ครอบครองหรือควบคุมข้อมูลดูแลข้อมูลส่วนบุคคลใดกระทำการเกี่ยวกับข้อมูลส่วนบุคคลอันก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือแก่บุคคลที่เกี่ยวข้องต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้น ไม่ว่าจะเป็นการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตามเว้นแต่จะพิสูจน์ได้ว่าการกระทำนั้นเกิดจากเหตุสุดวิสัย เป็นการกระทำตามกฎหมายหรือตามคำสั่งของเจ้าหน้าที่ผู้ปฏิบัติตามอำนาจหน้าที่ตามกฎหมาย หรือเกิดเพราะการกระทำหรือละเว้นการกระทำของบุคคลที่เกี่ยวข้องหรือเจ้าของข้อมูลส่วนบุคคล

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายที่เจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นที่เกี่ยวข้องแล้วแต่กรณีได้ใช้จ่ายไปตามความจำเป็นเพื่อป้องกันความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นด้วย

หมวด ๑๐
บทกำหนดโทษ

.....

มาตรา ๔๘ ผู้ใดกระทำการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย หรือให้ผู้อื่นเสียหาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่งเป็นการเผยแพร่ข้อมูลส่วนบุคคลโดยเฉพาะเจาะจงหรือโดยเปิดเผยซึ่งข้อมูลส่วนบุคคลดังกล่าว ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๕๙ นายทะเบียนผู้ใดไม่ดำเนินการตามมาตรา ๒๓ ต้องระวางโทษปรับไม่เกินหนึ่งหมื่นบาท

มาตรา ๕๐ นายทะเบียนผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของคณะกรรมการตามมาตรา ๑๔ หรือมาตรา ๓๘ วรรคสอง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๕๑ ในกรณีผู้ที่ต้องรับโทษเป็นนิติบุคคลให้ผู้แทนนิติบุคคลต้องระวางโทษที่กำหนดสำหรับความผิดนั้น เว้นแต่จะพิสูจน์ได้ว่าตนไม่มีส่วนในการกระทำความผิดของนิติบุคคลนั้น

บทเฉพาะกาล

.....

มาตรา ๕๒ ให้ดำเนินการแต่งตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้บังคับใช้

มาตรา ๕๓ ในระหว่างที่ยังมิได้แต่งตั้งเลขาธิการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการให้ผู้ซึ่งดำรงตำแหน่งผู้อำนวยการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการในวันก่อนวันที่พระราชบัญญัตินี้มีผลใช้บังคับปฏิบัติหน้าที่เลขาธิการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการและตามพระราชบัญญัตินี้

.....

ประวัติผู้เขียน

ชื่อ – สกุล : นางสาวรักข์ษิตา โพธิ์พิทักษ์กุล

วัน เดือน ปีเกิด : 5 กันยายน 2517

วุฒิการศึกษา :

ปีการศึกษา 2539 นิติศาสตรบัณฑิต มหาวิทยาลัยธรรมศาสตร์

ประสบการณ์การทำงาน

ทนายความประจำบริษัทกรัณฑ์การกฎหมาย จำกัด