บทที่ 3

การดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ตในประเทศไท

3.1 หน่วยงานและเจ้าหน้าที่ที่เกี่ยวข้องกับการดำเนินคดี

ในการดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ตมีหน่วยงานและเจ้าหน้าที่ที่เกี่ยวข้องดังนี้

1.หน่วยงานที่เกี่ยวข้องกับการดำเนินคดี

ก.) หน่วยงานที่รับผิดชอบในการดำเนินคดี

- สำนักงานตำรวจแห่งชาติ

ในปี พ.ศ. 2541ได้มีพระบรมราชโองการโปรดเกล้าฯ ให้ตราพระราชบัญญัติโอนกรมตำรวจที่สังกัดกระทรวงมหาดไทย ไปจัดตั้งเป็น สำนักงานตำรวจแห่งชาติขึ้นตรงต่อนายกรัฐมนตรี ซึ่งเป็นหน่วยงานสำคัญที่ดูแลกิจการเกี่ยวกับตำรวจในประเทศไทย[110] ดังนั้น สำนักงานตำรวจแห่งชาติจึงเป็นหน่วยงานหลักที่เกี่ยวข้องกับการสืบสวน สอบสวน และการดำเนินคดีโดยตรง

ข.) หน่วยงานที่เกี่ยวกับการรับแจ้งการกระทำความผิด

- ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center : NECTEC หรือเนคเทค)

จัดตั้งขึ้นโดยมติคณะรัฐมนตรี เมื่อวันที่ 16 กันยายน พ.ศ. 2529 โดยในระยะเริ่มต้นมีสถานะเป็นโครงการภายใต้ศูนย์ถ่ายทอดเทคโนโลยี สำนักงานปลัดกระทรวงวิทยาศาสตร์ เทคโนโลยีและการพลังงาน (ชื่อในขณะนั้น) ต่อมาในวันที่ 30 ธันวาคม 2534

---

[110] http://www.royalthaipolice.go.th

เนคเทคได้เปลี่ยนแปลง สถานะเป็นศูนย์แห่งชาติเฉพาะทาง และเปลี่ยนการจัดรูปแบบองค์กรใหม่ตามพระราชบัญญัติพัฒนาวิทยาศาสตร์และ เทคโนโลยี พ.ศ. 2534[2]

- ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT)

ก่อตั้งขึ้นในปีพ.ศ.2543 โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ(Nectec) มีหน้าที่หลักในการตอบโต้และจัดการกับเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางคอมพิวเตอร์บนอินเทอร์เน็ต และรับแจ้งเหตุเกี่ยวกับเหตุการณ์ที่ละเมิดความปลอดภัยคอมพิวเตอร์บนอินเทอร์เน็ต[3]

นอกจากนี้ยังมีหน่วยงานอื่นๆ เช่น กระทรวงวัฒนธรรม ,คณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.), ผู้ให้บริการอินเทอร์เน็ต(ISP), สำนักข่าวกรองแห่งชาติ หากหน่วยงานเหล่านี้ได้รับการแจ้งการกระทำความผิดก็อาจดำเนินการประสานงานกับหน่วยงานและเจ้าหน้าที่ที่เกี่ยวข้องได้

ค.) หน่วยงานที่เกี่ยวข้องกับการรวบรวมและตรวจพิสูจน์พยานหลักฐาน

- ศูนย์ตรวจสอบและวิเคราะห์การกระทำผิดทางเทคโนโลยี(ศตท.)

เดิมใช้ชื่อว่า ศูนย์อาชญากรรมทางเทคโนโลยี เป็นหน่วยงานพิเศษตั้งขึ้นตามคำสั่ง ตร.ที่ 225/2547 ลงวันที่ 2 เม.ย. 2547เพื่อรองรับอาชญากรรมที่เกี่ยวข้องกับการกระทำผิดทางเทคโนโลยี ใช้ชื่อภาษาอังกฤษว่าHigh-Tech Crime Center ต่อมาได้มีพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ พ.ศ.2548 จึงได้จัดตั้งศูนย์ตรวจสอบและวิเคราะห์การกระทำผิดทางเทคโนโลยี (ศตท.) ขึ้นเมื่อ 30 มิ.ย. 2548[4]

---

[2] http://www.nectec.or.th

[3] http://www.thaicert.nectec.or.th/about/ThaiCERT.pdf

[4] http://htcc.ict.police.go.th

- กองบังคับการปราบปรามอาชญากรรมทางเศรษฐกิจและเทคโนโลยี(ปศท.)

จัดตั้งขึ้นเมื่อวันที่ 30 มิถุนายน 2548 ตามพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ พุทธศักราช 2548 และกฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการที่เรียกชื่ออย่างอื่นในสำนักงานตำรวจแห่งชาติ พ.ศ. 2548 ให้เลิกส่วนราชการเดิมคือ กองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ แล้วจัดตั้งหน่วยงาน ปศท.ขึ้น[5]

- กรมสอบสวนคดีพิเศษ (DSI)

จัดตั้งขึ้นเมื่อวันที่ 3 ตุลาคม พ.ศ. 2545 ตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ.2545 ใช้ชื่อภาษาอังกฤษว่า Department of Special Investigation มีชื่อย่อว่า DSI ซึ่งมีบุคลากรที่มีความรู้ความชำนาญในด้านต่างๆ[6]

ง.) หน่วยงานที่ดำเนินการปิดกั้นเว็บไซต์ที่ไม่เหมาะสม

- กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร(ICT)

จัดตั้งขึ้นเมื่อวันที่ 3 ตุลาคม พ.ศ. 2545 ตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. 2545 มีอำนาจหน้าที่เกี่ยวกับการวางแผนส่งเสริม พัฒนา และดำเนินกิจกรรมเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสาร การอุตุนิยมวิทยา และการสถิติ และราชการอื่นตามที่มีกฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร[7]

ก่อนที่จะมีการบังคับใช้พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 การสืบสวนสอบสวนและการประสานงานระหว่างหน่วยงานต่างๆ จะเป็นลักษณะการขอความร่วมมือระหว่างหน่วยงานโดยไม่มีกฎหมายหรือระเบียบปฏิบัติ[8] ต่อมาภายหลังจากประกาศใช้พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

---

[5] http://www.ecotecpolice.com

[6] http://www.dsi.go.th

[7] http://www.mict.go.th

[8] http://wiki.nectec.or.th/nectecpedia/images/a/a8/20070509_cc_act_df_approved_print.pdf.

เพื่อให้การดำเนินการตามพระราชบัญญัติฉบับนี้เป็นไปอย่างมีประสิทธิภาพ จึงมีการเตรียมความพร้อมในการจัดทำบันทึกความร่วมมือหรือความตกลงกันเพื่อให้การประสานงานเป็นไปอย่างราบรื่น ตามรายงานการเตรียมความพร้อมในการบังคับใช้กฎหมาย[9]

2.เจ้าหน้าที่ที่เกี่ยวข้อง

เจ้าหน้าที่ที่เกี่ยวข้องกับการดำเนินคดีเกี่ยวกับคอมพิวเตอร์ ได้แก่

1.พนักงานสอบสวนทั่วไป

2.พนักงานสอบสวนคดีพิเศษ

3.พนักงานเจ้าหน้าที่

เดิมก่อนที่จะบังคับใช้พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 อำนาจในการสอบสวนย่อมเป็นอำนาจของพนักงานสอบสวนทั่วไปและพนักงานสอบสวนคดีพิเศษในกรณีที่เป็นการสอบสวนคดีพิเศษ[10] และเมื่อกฎหมายฉบับนี้มีผลบังคับใช้ได้เพิ่มเติมให้มี "พนักงานเจ้าหน้าที่" จึงขอกล่าวถึงพนักงานเจ้าหน้าที่เป็นการเฉพาะ ดังนี้

---

[9] ใจความสำคัญ ดังนี้ "...ในการแต่งตั้งพนักงานเจ้าหน้าที่หรือประสานการทำงานเพื่อปฏิบัติตามพระราชบัญญัติฉบับนี้นั้น อาจมีความเกี่ยวข้องกับหลายหน่วยงานและการแต่งตั้งพนักงานเจ้าหน้าที่ก็อาจแต่งตั้งบุคคลที่มีความรู้ความสามารถในหน่วยงานต่างๆที่เกี่ยวข้อง เช่น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงวิทยาศาสตร์และเทคโนโลยีโดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ กระทรวงยุติธรรมโดยกรมสอบสวนคดีพิเศษสำนักงานตำรวจแห่งชาติ สำนักงานข่าวกรองแห่งชาติ หรือ กองบัญชาการทหารสูงสุด เป็นต้น ซึ่งจำเป็นต้องทำความร่วมมือในทางปฏิบัติ เพื่อให้การบังคับใช้พระราชบัญญัตินั้นมีประสิทธิภาพสูงสุด จึงจำเป็นอย่างยิ่งที่ต้องเตรียมจัดทำการบันทึกความร่วมมือหรือความตกลงระหว่างกันเพื่อให้การประสานการทำงานนั้นเป็นไปอย่างราบรื่น ในภาวะที่ประเทศไทยยังขาดแคลนองค์ความรู้ในการรับมือกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และยังมีข้อจำกัดผู้เชี่ยวชาญที่จะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ นอกเหนือจากการกำหนดระเบียบร่วมกันระหว่างนายกรัฐมนตรีซึ่งอยู่ในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติกับรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศแห่งชาติ ที่ต้องจัดทำขึ้นภายใต้มาตรา 29" (http://wiki.nectec.or.th/nectecpedia/ images /a/a8/20070509 c c a c t d f ap proved print.pdf.)

[10] "พระราชบัญญัติสอบสวนคดีพิเศษ มาตรา 21"

พนักงานเจ้าหน้าที่ (Competent Official) หมายถึง ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550[11] และเป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลวิธีพิจารณาความอาญา มีอำนาจสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้ รวมถึงมีอำนาจในการรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจสืบสวนสอบสวนตามพระราชบัญญัตินี้อีกด้วย[12]

<u>คุณสมบัติของพนักงานเจ้าหน้าที่</u>

ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ฯ ได้กำหนดคุณสมบัติของพนักงานเจ้าหน้าที่ไว้ ดังนี้

(1) มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์

(2) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์ วิทยาศาสตร์วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์หรือรัฐประศาสนศาสตร์

(3) ผ่านการอบรมทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) สืบสวน สอบสวน และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) ตามภาคผนวกท้ายประกาศนี้ และ

(4) มีคุณสมบัติอื่นอย่างหนึ่งอย่างใด ดังต่อไปนี้

ก. รับราชการหรือเคยรับราชการไม่น้อยกว่าสองปีในตำแหน่งเจ้าหน้าที่ตรวจพิสูจน์พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์หรือพยานหลักฐานอิเล็กทรอนิกส์

---

[11] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 3 ประกอบประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ฯ ข้อ 1

[12] มาตรา 29

ข. สำเร็จการศึกษาตามข้อ (2) ในระดับปริญญาตรี และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสี่ปี

ค. สำเร็จการศึกษาตามข้อ (2) ในระดับปริญญาโท หรือสอบไล่ได้เป็นเนติบัณฑิต ตามหลักสูตรของสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสามปี

ง. สำเร็จการศึกษาตามข้อ (2) ในระดับปริญญาเอก หรือมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงาน ตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสองปี

จ. เป็นบุคคลที่ทำงานเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือมีประสบการณ์ในการดำเนินคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ไม่น้อยกว่าสองปี

และในกรณีจำเป็น รัฐมนตรีอาจยกเว้นคุณสมบัติข้างต้นไม่ว่าทั้งหมดหรือบางส่วนสำหรับการบรรจุและแต่งตั้งบุคคลใดเป็นการเฉพาะก็ได้[13]

<u>อำนาจของพนักงานเจ้าหน้าที่</u>

กฎหมายได้ให้อำนาจพนักงานเจ้าหน้าที่เพิ่มเติมจากอำนาจตามกฎหมายวิธีพิจารณาความอาญา 8 ประการ ตามมาตรา 18 ได้แก่

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องเพื่อให้ถ้อยคำ

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์ (Traffic data) จากผู้ให้บริการ

---

[13] ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ฯ ข้อ 3

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ (Computer data) ข้อมูลจราจรทางคอมพิวเตอร์(Traffic data)

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ (Computer data) ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic data) หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์

(7) ถอดรหัสลับ (Decrypt) ของข้อมูลคอมพิวเตอร์

(8) ยึดหรืออายัดระบบคอมพิวเตอร์

ตามพระราชบัญญัตินี้พนักงานเจ้าหน้าที่ยังมีบทบาทในการใช้อำนาจอื่นตามพระราชบัญญัตินี้ ได้แก่ การร้องขอต่อศาลให้ระงับการเผยแพร่ซึ่งข้อมูลคอมพิวเตอร์ (Blocking)[14], การร้องขอต่อศาลให้ห้ามจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์[15], อำนาจใน

---

[14] "มาตรา 20 ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลาย ซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้..."

[15] มาตรา 21 "ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้..."

การสั่งให้ผู้บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีเฉพาะราย[16]และเพื่อให้การสอบสวนเป็นไปอย่างมีประสิทธิภาพ กฎหมายจึงบัญญัติเกี่ยวกับการประสานงานในเรื่องการจับ การควบคุม ค้น การสืบสวนและสอบสวนระหว่างพนักงานเจ้าหน้าที่กับพนักงานสอบสวนผู้รับผิดชอบ[17]

นอกจากนี้พระราชบัญญัติฉบับนี้ยังวางเงื่อนไขการใช้อำนาจของพนักงานเจ้าหน้าที่ไว้ ได้แก่ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ให้แก่บุคคลใดหรือต้องรับผิดแม้เป็นการกระทำให้พยานหลักฐานรั่วไหลโดยประมาทและเอาผิดกับผู้ล่วงรู้ข้อมูลเหล่านั้นด้วย (มาตรา 22, 23และ 24) ทั้งนี้เพื่อมิให้เจ้าพนักงานใช้อำนาจหน้าที่โดยมิชอบซึ่งอาจกระทบต่อสิทธิของประชาชนทั่วไป

3.2 กระบวนการและขั้นตอนการดำเนินคดี

ก.การเริ่มการสอบสวน

กระบวนการเริ่มการสอบสวนการกระทำความผิดบนอินเทอร์เน็ตย่อมเป็นไปตามวิธีพิจารณาความอาญาเช่นเดียวกับการดำเนินคดีอาญาทั่วไป เช่น สามารถร้องทุกข์ยังสถานีตำรวจหรือแจ้งการกระทำผิดต่อหน่วยงานต่างๆที่เกี่ยวข้องเพื่อประสานงานกับเจ้าหน้าที่ตำรวจเพื่อดำเนินการทางคดีต่อไป เช่น การแจ้งการกระทำความผิดไปยังศูนย์รับแจ้งเหตุ เช่น ThaiCERT, Nectec, เว็บไซต์ของกรมสอบสวนคดีพิเศษ(www.dsi.go.th), เว็บไซต์ของสำนักงานตำรวจแห่งชาติ(www.royalthaipolice.go.th, www.sb.police.go.th) หรือ แจ้งเหตุด้วยวิธีการอื่นๆ[18]

---

[16] มาตรา 26 "ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้..."

[17] มาตรา 29 "...ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป..."

[18] เช่น Email: sb@police.go.th, ไปรษณีย์ : ตู้ ปณ. 999 รองเมืองกรุงเทพ,โทรศัพท์: ศูนย์เอกภพ : 0-2241-5990/ 0-2243-3107

ข.การรวบรวมพยานหลักฐาน

การดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือกระทำความผิดบนอินเทอร์เน็ต มีความจำเป็นต้องนำกระบวนการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์หรือนิติคอมพิวเตอร์ (Computer Forensic) มาใช้ ในการค้นหาและรวบรวมพยานหลักฐาน ซึ่งกระบวนการนี้เป็นกระบวนการสำคัญที่ทำให้การรวบรวมพยานหลักฐานสำหรับการกระทำผิดลักษณะนี้แตกต่างจากการรวบรวมพยานหลักฐานทั่วไป จึงขอกล่าวถึงกระบวนการComputer Forensic ไว้เป็นการเฉพาะ ดังนี้

สถาบันความปลอดภัยทางอิเล็กทรอนิกส์(Cyber security Institute) ได้ให้ความหมายของ Computer Forensic ไว้ดังนี้[19] *"เป็นการเก็บรักษาไว้ การขันสูตร การดึงหรือถอนพยานหลักฐานที่พบออกมา การอธิบายผล และการจัดทำเอกสารของพยานหลักฐานทางคอมพิวเตอร์ รวมถึงกฎเกณฑ์พยานหลักฐาน กระบวนการทางกฎหมาย ความน่าเชื่อถือของพยานหลักฐาน การรายงานข้อเท็จจริงของข้อมูลที่พบ และการเตรียมการเกี่ยวกับความเห็นของผู้เชี่ยวชาญ"* ดังนั้น สิ่งที่เกี่ยวข้องกับการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์มี ดังนี้[20]

1.การเก็บรักษาไว้ - เมื่อมีการวิเคราะห์ การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์จะต้องทำทุกอย่างที่เป็นไปได้ในการเก็บรักษาสื่อและข้อมูลต้นฉบับ โดยปกติแล้วจะเกี่ยวกับรูปจำลองทางการตรวจพิสูจน์หลักฐาน(Forensic image) หรือสำเนาของสื่อต้นฉบับและทำการวิเคราะห์จากทั้งสำเนาและต้นฉบับ

2.การขันสูตร - ในขั้นต้น เป็นการตรวจพิสูจน์สิ่งที่ใช้ในการบรรจุหลักฐานที่เกี่ยวกับคอมพิวเตอร์ เช่น อุปกรณ์เก็บข้อมูล(Hard drive) ฟลอปปี้ดิสก์และไฟล์ คอมพิวเตอร์หรืออุปกรณ์เก็บข้อมูล(Hard drive) เองไม่ใช่หลักฐาน ขั้นตอนต่อไปคือ การวิเคราะห์เป็นการตรวจพิสูจน์ข้อมูลที่เกี่ยวข้องกับสถานการณ์ที่มีอยู่ ค้นหาคำสำคัญ และตรวจดูไฟล์ต่างๆ

---

[19] ไพจิตร สวัสดิสาร, "การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์หรือนิติคอมพิวเตอร์(Computer Forensic)", ดุลพาห ปีที่53(มกราคม-เมษายน 2549), หน้า 63.

[20] เรื่องเดียวกัน, หน้า 63-65.

3.การดึงหรือถอนหลักฐานที่พบออกมา - หลักฐานที่พบต้องดึงออกมาจากสื่อนั้นและเก็บไว้ในสื่ออื่นรวมถึงพิมพ์ออกมาเป็นกระดาษ

4.การอธิบายผล - มีเครื่องมือหรือโปรแกรมที่เรียกว่า Graphical user Interface (GUI) ซึ่งเป็นวิธีการใช้งานของผู้ใช้คอมพิวเตอร์ที่เลือกแฟ้ม โปรแกรม หรือคำสั่งโดยชี้ไปยังรูปภาพแทนสิ่งเหล่านั้นบนจอภาพแทนการป้อนคำสั่งยาวๆ ความสามารถค้นหาหลักฐานเป็นสิ่งหนึ่งที่สำคัญแต่ความสามารถในการอธิบายได้อย่างถูกต้องเป็นอีกอย่างหนึ่งที่สำคัญเช่นกัน ตัวอย่างเช่น ผู้เชี่ยวชาญฝ่ายอัยการในคดีหนึ่งได้ใช้GUI ที่ใช้สำหรับหากิจกรรมของโปรแกรมการค้นหาข้อมูลในอินเทอร์เน็ต(Internet search engine) พบว่า มีการค้นหานับเป็นร้อยๆครั้ง ซึ่งคาดว่ากระทำโดยจำเลยและจำเลยมีเจตนาเข้าไปในข้อมูลเฉพาะประเภท การค้นหาจึงแสดงถึงเจตนาได้ แต่ผู้เชี่ยวชาญฝ่ายจำเลยตรวจสอบพยานหลักฐานเดียวกันพบว่าการค้นหาแต่ละครั้งเป็นการเรื่องการเชื่อมต่อกับเอกสารอื่นหรือHyperlink และไม่ใช่เป็นการค้นหาเลย การเชื่อมต่อกับเอกสารอื่นเป็นการการกดปุ่มคลิกฐานข้อมูลที่ถูกค้น เพื่อดึงข้อมูลที่เกี่ยวเนื่องกับการเชื่อมโยงนั้น วิธีการในการเชื่อมต่อคือ การที่GUI เข้าไปในช่องทาง ซึ่งเป็นขณะเดียวกับการเชื่อมต่อเหล่านั้นทำงานซึ่งคล้ายกับเว็บเพจที่สามารถพบได้ และเป็นเครื่องชี้ให้เห็นว่าเป็นกิจกรรมของโปรแกรมการค้นหาหรือSearch engine ผู้เชี่ยวชาญฝ่ายอัยการทึกทักเอาเองว่า เครื่องมืออัตโนมัติจะเกี่ยวข้องกับตัวแปรทุกตัวและสามารถแสดงการค้นที่แท้จริงได้ จึงเป็นการเข้าใจที่ผิด ผู้เชี่ยวชาญจึงขาดทักษะทางเทคนิคในการอธิบายผลที่แท้จริงและทำตัวพึ่งกับเครื่องมืออัตโนมัติเพียงอย่างเดียว ในคดีนี้ปรากฏต่อไปว่าผู้เชี่ยวชาญฝ่ายจำเลยพบอีเมล์จำนวนมากในขณะที่อัยการหาไม่พบ โดยทั้งผู้เชี่ยวชาญฝ่ายจำเลยและผู้เชี่ยวชาญฝ่ายอัยการใช่เครื่องมือในการวิเคราะห์ที่เหมือนกัน แต่ความแตกต่างเกิดจากประสบการณ์และระดับการศึกษาของผู้เชี่ยวชาญ ไม่ใช่เครื่องมือที่ใช้

5.การจัดทำเอกสาร - เอกสารควรเก็บไว้ตั้งแต่เริ่มต้นจนจบเป็นส่วนหนึ่งของเส้นทางการเก็บรักษาหรือChain of custody และเป็นสิ่งที่ต้องนำส่งศาลในที่สุด

6.กฎเกณฑ์พยานหลักฐาน - จะเกี่ยวกับเรื่องการเบิกความของผู้เชี่ยวชาญ การรับฟังพยานหลักฐาน ความเชื่อมั่น และความเกี่ยวข้องกับคดี นอกจากนั้นในบางประเทศ เช่น สหรัฐอเมริกา อาจมีการรับฟังพยานหลักฐานทางวิทยาศาสตร์ที่ต้องผ่านการทดสอบหรือหลักเกณฑ์ที่ได้วางหลักในคดีบรรทัดฐานมาก่อน เช่น Frye test และ Daubert test

7. กระบวนการทางกฎหมาย - เกี่ยวกับการออกหมายค้น การให้การเป็นพยาน การพิจารณาคดี การสอบสวน และการเปิดเผยเรื่องราวสาระ เป็นต้น

8. ความน่าเชื่อถือของพยานหลักฐาน - เป็นเรื่องการควบคุมทุกอย่างเกี่ยวกับคดีและสถานการณ์ เป็นเรื่องเส้นทางการเก็บรักษาหรือ Chain of custodyและความแน่ใจว่าสื่อต้นฉบับไม่ถูกเปลี่ยนแปลง

9. การรายงานข้อเท็จจริงของข้อมูลที่พบ - ซึ่งควรจะสามารถในการกระทำซ้ำผลที่ได้ด้วย

10.การเตรียมการเกี่ยวกับความเห็นของผู้เชี่ยวชาญ - อาจต้องมีการเบิกความในสิ่งที่พบและความเห็นต่างๆในศาลหรือที่อื่น

พ.ต.อ.ญาณพล ยั่งยืน ผู้บังคับการสำนักคดีเทคโนโลยีสารสนเทศ กรมสอบสวนคดีพิเศษ (DSI) กระทรวงยุติธรรม ได้ให้ความหมายของ Computer forensic ไว้ดังนี้ "...Computer forensic คือการแสวงหา ได้มา สงวน เก็บรักษา อนุรักษ์ให้คงอยู่ วิเคราะห์ หรือการรื้อฟื้นข้อมูลหรือดึงกลับมาอย่างมีมาตรฐาน เพื่อจะชี้ให้เห็นว่าบุคคลใดเป็นผู้กระทำความผิดในการดำเนินการของสำนักงานตำรวจแห่งชาติในหลายคดี พยานหลักฐานที่ได้จากกระบวนการรวบรวมพยานหลักฐานนั้นจะมีแหล่งที่มาสำคัญ 3 แหล่ง คือ

(1) ที่เครื่องมือหรืออุปกรณ์ของผู้กระทำความผิด

(2) ที่เครื่องมือหรืออุปกรณ์ของเป้าหมายหรือผู้ถูกกระทำ

(3) ที่เครื่องมือหรืออุปกรณ์ระหว่างกลาง

เครื่องมือหรืออุปกรณ์ของผู้กระทำผิดนั้น จะมีข้อมูลที่สำคัญอยู่ 2 ประเภท คือ (1) ข้อมูลที่ระเหยได้ (Volatile data) เมื่อปิดเครื่องคอมพิวเตอร์ลง และ (2) File หรือข้อมูลที่ถูกลบ ซึ่งการค้นหาข้อมูลทั้งสองประเภทนี้จะต้องกระทำโดยวิธีการทาง Computer forensic..."[21]

---

[21] ญาณพล ยั่งยืน, "บันทึกการประชุมเรื่องการรวบรวมพยานหลักฐานและการรับฟังพยานหลักฐานทางคอมพิวเตอร์," โรงแรมมิราเคิลแกรนด์ ถนนวิภาวดีรังสิต กรุงเทพมหานคร 11 กุมภาพันธ์ 2547

ค.การใช้มาตรการบังคับ

ก่อนที่จะมีบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 การใช้มาตรการบังคับย่อมเป็นไปตามกระบวนการดำเนินคดีอาญาตามปกติ และเมื่อพระราชบัญญัติฉบับนี้บังคับใช้ได้ให้อำนาจพนักงานเจ้าหน้าที่เพิ่มเติมจากประมวลกฎหมายวิธีพิจารณาความอาญา 8 ประการ ซึ่งอาจแบ่งแยกการใช้อำนาจดังกล่าวออกเป็น 2 กรณี คือ

ก.) การใช้อำนาจซึ่งไม่ต้องขออนุญาตศาล ตามมาตรา18 (1) - (3) ได้แก่

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์ (Traffic data) จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่ ได้แก่ ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic data) หรือข้อมูลเกี่ยวกับการระบุตัวผู้ใช้บริการ เช่น (User Id) ข้อมูลการลงทะเบียน (Register) เป็นต้น

ข.) การใช้อำนาจซึ่งต้องขออนุญาตศาล ตามมาตรา18 (4)-(8) ตามวิธีการที่กำหนดไว้ตามมาตรา19[22] เพื่อให้ศาลตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่ก่อน ได้แก่

(1) ทำสำเนาข้อมูลคอมพิวเตอร์ (Computer data) ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic data) จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงาน

---

[22] มาตรา19 " การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ(8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าดำเนินการตามคำร้อง ..."

เจ้าหน้าที่ การดำเนินการตามมาตรานี้หมายถึงการค้นในสถานที่นั้น (On-site) หากเป็นการยึดและค้นนอกสถานที่นั้น (Off-site) เจ้าหน้าที่จะต้องดำเนินการตามมาตรา18(8)

2) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(3) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ (Computer data) ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic data) หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(4) ถอดรหัสลับ (Decrypt) ของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(5) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

<u>ง.การใช้มาตรการพิเศษ</u>

พระราชบัญญัติฉบับนี้ได้กำหนดให้มีการใช้มาตรการพิเศษซึ่งแตกต่างจากการดำเนินคดีกับความผิดทั่วไป ดังนี้

<u>1.การปิดกั้น (Block) เว็บไซต์</u> การกระทำความผิดที่มีลักษณะเข้าข่ายเป็นความผิดที่กระทบต่อความมั่นคงแห่งราชอาณาจักรหรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พระราชบัญญัตินี้ให้อำนาจศาลปิดกั้นเว็บไซต์นั้นได้

<u>2.การห้ามจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์</u> ในกรณีพนักงานเจ้าหน้าที่พบคำสั่งไม่พึงประสงค์ (Malicious code) เช่น ไวรัส (Virus), มัลแวร์ (malware), เวิร์ม

(worm), สปายแวร์(spyware) ให้พนักงานเจ้าหน้าที่มีอำนาจร้องขอต่อศาลเพื่อระงับการกระทำดังกล่าวต่อไปได้ ตามวิธีการในมาตรา 21 เว้นแต่ ชุดคำสั่งเหล่านั้นเป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าว เช่น โปรแกรม Anti-virus

3.การให้ผู้ให้บริการมีหน้าที่ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือTraffic data หรือข้อมูลที่ทำให้สามารถระบุตัวผู้ใช้บริการ เช่น (User Id) ข้อมูลการลงทะเบียน (Register) เป็นหลักฐานสำคัญในการแกะรอยการกระทำความผิดได้ จึงกำหนดให้ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลดังกล่าวไว้ ภายในระยะเวลาที่กำหนดไว้ในมาตรา 26 ประกอบหลักเกณฑ์การเก็บข้อมูลตามประกาศฯ เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ

นอกจากที่ได้กล่าวมาแล้ว พระราชบัญญัติฉบับนี้ยังวางหลักการให้รับฟังข้อมูลข้อมูลคอมพิวเตอร์หรือข้อมูลจราจรทางคอมพิวเตอร์เป็นพยานหลักฐานได้ แต่ต้องมิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น ตามมาตรา 25

3.3 ปัญหาในการดำเนินคดี

3.3.1 ปัญหาในการเริ่มต้นคดีอาญา

ปัญหาเกี่ยวกับการร้องทุกข์ กล่าวโทษ

การกล่าวหาว่าได้มีการกระทำความผิดทางอาญา ไม่ว่าจะเป็นการร้องทุกข์หรือการกล่าวโทษย่อมมีความสำคัญอย่างยิ่งในการเริ่มต้นคดีอาญา อย่างไรก็ดีอาจเกิดปัญหาซึ่งทำให้ไม่สามารถดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ตได้

ก) ความกลัวของผู้เสียหายในการร้องทุกข์

ผู้เสียหายในการกระทำความผิดบนอินเทอร์เน็ต อาจเป็นได้ทั้งบุคคลธรรมดาและนิติบุคคล อาจเป็นผู้เสียหายทั้งทางตรงหรือทางอ้อม โดยผู้เสียหายที่เป็นบุคคลธรรมดาอาจตกเป็นเหยื่อของการกระทำความผิดประเภท Cyber-stalking หรือTheft of cybercash ส่วน

ผู้เสียหายที่เป็นนิติบุคคลอาจตกเป็นเหยื่อของการกระทำผิดประเภท Cyber-piracyหรือ Cyber-spying/terrorism อย่างไรก็ดีผู้เสียหายกลับไม่ได้แจ้งความเกี่ยวกับการกระทำความผิดนั้นเพราะความรู้สึกอึดอัดใจที่จะยอมรับว่าตนเองตกเป็นเหยื่อของอาชญากรรม ความรู้สึกเกรงกลัวที่จะได้รับการดูหมิ่นเกลียดชังจากบุคคลภายนอก ความรู้สึกเสื่อมเสียในทางสังคมหรือศีลธรรม หรือกลัวว่าจะมีผลกระทบต่อธุรกิจของตน รวมทั้งอาจเกิดจากความไม่มั่นใจในกฎหมายที่จะเข้ามารองรับในคดีต่างๆเหล่านั้น

ศาสตราจารย์วีระพงษ์ บุญโญภาส ได้กล่าวถึงปัญหานี้ไว้ว่า *"...เหยื่อของอาชญากรรมนั้นยังไม่กล้าที่จะแจ้งความในอาชญากรรมดังกล่าว ทั้งนี้เพราะกลัวต่อการที่จะตกเป็นเป้าสายตาและถูกวิพากษ์วิจารณ์จากสาธารณชน ตลอดจนการเกรงที่จะต้องเปิดเผยถึงความไม่แน่นอนของระบบคอมพิวเตอร์ของตน อันเป็นจุดที่ซ่อนอยู่ในอาชญากรรมคอมพิวเตอร์..."*[23]

ในกรณีที่ผู้เสียหายเป็นนิติบุคคล ผู้เสียหายอาจไม่กล้าที่จะแจ้งความร้องทุกข์เนื่องจากเกรงว่าจะมีผลเสียต่อธุรกิจของตนและมีผลกระทบต่อส่วนแบ่งทางการตลาด เพราะเป็นการแสดงให้คนทั่วไปเห็นว่ากิจการของตนไม่มีระบบรักษาความปลอดภัยข้อมูลที่เพียงพอ ผู้เสียหายจึงเลือกที่จะฟ้องร้องเรียกค่าเสียหายในทางแพ่งมากกว่าที่จะเลือกดำเนินคดีทางอาญาเนื่องจากมีภาระการพิสูจน์ที่น้อยกว่า หรือผู้เสียหายมีความรู้สึกว่าสามารถควบคุมกระบวนการพิจารณาในคดีแพ่งได้มากกว่า หรือผู้เสียหายเห็นว่าสามารถเรียกร้องค่าเสียหายจากบริษัทประกันภัยได้อยู่แล้ว หรืออาจผลักภาระค่าใช้จ่ายที่เกิดจากความเสียหายไปให้ผู้บริโภคได้[24]

ข) <u>การตกเป็นเหยื่อของการกระทำผิดโดยไม่รู้ตัวหรือความเชื่อมั่นว่าตนเองไม่ได้ตกเป็นเหยื่อ</u>

บางกรณีผู้เสียหายอาจไม่รู้ตัวว่าตนเองตกเป็นเหยื่อของการกระทำความผิดแล้วหรือเชื่อมั่นว่าตนเองไม่ได้ตกเป็นเหยื่อของการกระทำผิด เช่น ในกรณีความผิดเกี่ยวกับการเผยแพร่ภาพลามกอนาจารบนอินเทอร์เน็ต(Internet pornography)[25] ที่ผู้เสียหายถูกแอบถ่ายโดย

---

[23] วีระพงษ์ บุญโญภาส, <u>อาชญากรรมทางเศรษฐกิจ</u>,(กรุงเทพฯ: นิติธรรม, 2540), หน้า159.

[24] David S. Wall, <u>Cybercrimes and the internet</u>,(London : Routledge, 2001), p.8.

[25] Ibid., p.8.

ที่ตนเองไม่รู้ตัวจึงมิได้ดำเนินการทางกฎหมาย หรือกรณีที่ดาราถูกนำภาพของตนไปตัดต่อ โดยนำหน้าของดาราผู้นั้นไปรวมกับสรีระของผู้อื่นทำให้ภาพที่ปรากฏออกมาเป็นภาพโป๊เปลือย ซึ่งภาพดังกล่าวเป็นภาพไม่จริงที่ถูกตกแต่งหรือทำขึ้นโดยเทคนิคการตัดต่อภาพ ซึ่งอาจถือได้ว่าดาราผู้นั้นตกเป็นผู้เสียหายจากภาพที่ตัดต่อแล้ว แต่ด้วยความเข้าใจส่วนตัวของดาราผู้นั้นเองที่คิดว่าเมื่อตนเองไม่ได้ถ่ายภาพเช่นนั้นจริง จึงไม่ใช่เรื่องน่าอับอายหรือทำให้ตนเสียหายจนต้องออกมาเรียกร้องสิทธิของตน[26]

ค) <u>อำนาจในการร้องทุกข์ของผู้เสียหาย</u>

ในการกระทำความผิดบนอินเทอร์เน็ตบางฐานความผิดเป็นความผิดต่อส่วนตัว จึงจำเป็นต้องพิจารณาเรื่องอำนาจร้องทุกข์ แต่การพิจารณาเรื่องอำนาจร้องทุกข์และการกำหนดตัวผู้เสียหายอาจมีความยุ่งยากซับซ้อน เช่น กรณีที่ผู้เสียหายเป็นคนไทย มีเซิฟเวอร์อยู่ในต่างประเทศมีการถูกโจมตีต่างๆจากผู้กระทำความผิดบนอินเทอร์เน็ตโดยกระทำต่อเซิฟเวอร์ดังกล่าว จะถือเป็นผู้เสียหายตามกฎหมายไทยหรือไม่ เพราะคดีประเภทนี้ผู้เสียหายคนไทยไม่อาจร้องทุกข์ต่อFBI หรือตำรวจต่างประเทศได้ เพราะกฎหมายของต่างประเทศไม่เปิดช่องไว้ ในกรณีเช่นนี้จะสามารถร้องทุกข์ต่อเจ้าหน้าที่ของไทยได้หรือไม่[27]

นอกจากนี้ยังต้องพิจารณาว่าผู้ร้องทุกข์เป็นผู้เสียหายหรือไม่ ในกรณีนี้ผู้เขียนเห็นว่าจะต้องนำหลักการเรื่องผู้เสียหายโดยนิตินัยมาใช้กับการดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ตด้วย ดังนั้น หากผู้ร้องทุกข์ไม่ใช่ผู้เสียหายโดยนิตินัยก็อาจทำให้การดำเนินคดีเสียไป เช่น ผู้เสียหายที่นำรูปหรือภาพเคลื่อนไหวลามกอนาจารของตนเองเผยแพร่บนอินเทอร์เน็ตเพราะความอยากดังหรือเจ้าของเว็บไซต์ที่ยินยอมให้ผู้อื่นเจาะระบบของตนเพื่อต้องการทดสอบระบบป้องกันหรือเจ้าของเซิฟเวอร์ยินยอมให้ผู้อื่นเผยแพร่โปรแกรมอันตราย เช่น แจกจ่ายไวรัสบนเซิฟเวอร์ของตน ในกรณีต่างๆเหล่านี้น่าจะถือได้ว่าผู้ได้รับความเสียหายเหล่านั้นไม่ใช่ผู้เสียหายโดยนิตินัย

---

[26] สุรวุทธ กิจกุศลและปิยวัฒน์ สุรัติเจริญสุข, "หมิ่นประมาทบนอินเทอร์เน็ตจัดการอย่างไรจึงจะเหมาะสม",<u>วารสารข่าวกฎหมายใหม่</u> ,ปีที่ 2 ฉบับที่ 33: 31.

[27] ญาณพล ยั่งยืน, "บันทึกการประชุมคณะกรรมการกฤษฎีกา(คณะพิเศษ) เรื่องร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ... ครั้งที่1/2547" 16 มกราคม 2547

ง.) อำนาจในการรับคำร้องทุกข์

ในคดีอาญาความผิดต่อส่วนตัว อาจเกิดปัญหาในการพิจารณาเกี่ยวกับอำนาจรับคำร้องทุกข์ เช่น การแจ้งการกระทำความผิดต่อศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ศูนย์ฯ ThaiCERT) [28] เจ้าหน้าที่ที่รับแจ้งการกระทำผิดอาจไม่ใช่เจ้าพนักงานผู้มีอำนาจรับคำร้องทุกข์[29] จึงไม่สามารถดำเนินคดีกับผู้ต้องหาได้

จ) ปัญหาเกี่ยวกับการพิจารณาท้องที่ที่ความผิดเกิด

การพิจารณาว่าการกระทำผิดเกิดที่ใดเป็นปัญหาเกี่ยวกับอำนาจสอบสวนและอำนาจของพนักงานสอบสวนผู้รับผิดชอบโดยตรง เพราะท้องที่ที่ความผิดเกิดอาจมีได้มากกว่าสองแห่งขึ้นไปทำให้เกิดปัญหาในการพิจารณาอำนาจสอบสวน เช่น ความผิดฐานเข้าถึงคอมพิวเตอร์โดยมิชอบ(Illegal access) อาจถือว่าความผิดความผิดเกิดขึ้นในท้องที่ที่คอมพิวเตอร์นั้นตั้งอยู่(เทียบกับความผิดฐานบุกรุก ที่สถานที่ความผิดเกิดคือสถานที่ที่ถูกบุกรุก) แต่ในบางครั้งคอมพิวเตอร์หรือเซิฟเวอร์อาจไม่ได้ตั้งอยู่ในท้องที่ที่ผู้เสียหายร้องทุกข์ หรืออาจตั้งอยู่ยังต่างประเทศ ทำให้อาจเกิดปัญหาเกี่ยวกับอำนาจสอบสวนและอำนาจพนักงานสอบสวนผู้รับผิดชอบได้[30]

3.3.2 ปัญหาในการรวบรวมพยานหลักฐาน

ก) การรวบรวมพยานหลักฐานทำได้ยาก

สำหรับการรวบรวมพยานหลักฐานในการกระทำผิดอาญานั้น พนักงานสอบสวนมีอำนาจรวบรวมพยานหลักฐานทุกชนิดเท่าที่สามารถจะทำได้ ซึ่งหากเป็นการกระทำผิดอาญาทั่วไปก็อาจหาพยานหลักฐานได้ไม่ยากลำบากนัก เพราะพยานหลักฐานที่เกี่ยวข้องกับการกระทำ

---

[28] http://www.thaicert.nectec.or.th (ศูนย์ฯ (ThaiCERT) นั้นถือว่าเป็น CSIRT คือ กลุ่มหรือคณะบุคคลที่ ทำการ, ประสานงาน, และสนับสนุน การตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์และเครือข่าย (เหตุการณ์ฯ) ที่เกิดขึ้นภายใน Sites ของผู้ใช้บริการของ CSIRT นั้น ทั้งนี้มิได้หมายความว่า CSIRT จะต้องเป็นตำรวจหรือองค์กรผู้รักษากฎหมาย)

[29] ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 124 เจ้าพนักงานผู้มีอำนาจรับคำร้องทุกข์ได้แก่พนักงานฝ่ายปกครองหรือตำรวจ

[30] ญาณพล ยั่งยืน, นำเสนอในการประชุมคณะกรรมาธิการวิสามัญ 29 พฤศจิกายน 2549, http://wiki.nectec .or.th /nectecpedia/index.php

ความผิดอาจพบในที่เกิดเหตุ และเป็นพยานหลักฐานที่สามารถจับต้องได้ แต่พยานหลักฐานในคดีความผิดเกี่ยวกับคอมพิวเตอร์ไม่ใช่พยานหลักฐานทางกายภาพ โดยลักษณะเป็นเพียงคลื่นกระแสไฟฟ้าและรหัสโปรแกรมเท่านั้น หรือในบางกรณีข้อมูลซึ่งจะใช้เป็นพยานหลักฐานจัดเก็บหรือเชื่อมโยงกับเครือข่ายในต่างประเทศ ทำให้มีการรวบรวมพยานหลักฐานมีความยากยิ่งขึ้น

ในประเด็นนี้ พ.ต.อ.ญาณพล ยั่งยืน ได้ให้ความเห็นว่า *"...ควรกำหนดให้เจ้าหน้าที่มีอำนาจในการทำสำเนา (cloning) และให้ถือว่าสำเนามีสถานะเทียบเท่ากับของกลาง เพราะบางครั้งไม่สามารถนำ Hard disk หรือ Server ที่เป็นของกลางจริงๆ มาได้ เพราะยังคงต้องให้บริการอยู่ตลอดเวลา แต่การทำสำเนานั้นจะต้องเป็นการทำตามหลักวิชาที่กำหนด..."*[31]

ปัจจุบัน แนวทางการรวบรวมพยานหลักฐานของหลายประเทศทั่วโลก รวมถึงประเทศไทยได้ใช้กระบวนการ Computer Forensic ซึ่งเป็นการพิสูจน์หลักฐานในหน่วยความจำหรืออุปกรณ์เก็บข้อมูลที่เครื่องคอมพิวเตอร์ในการรวมรวมพยานหลักฐานและระบุตัวผู้กระทำผิด

ข) <u>*พยานหลักฐานสามารถแก้ไข เปลี่ยนแปลง สูญหายหรือถูกทำลายได้โดยง่าย*</u>

พยานหลักฐานอิเล็กทรอนิกส์อาจถูกแก้ไข เปลี่ยนแปลงหรือสูญหายหรือถูกทำลายได้โดยง่าย ตัวอย่างเช่น ในกรณีการหมิ่นประมาทด้วยข้อความที่ปรากฏบนเว็บไซต์ ข้อความดังกล่าวสามารถถูกลบทิ้งได้โดยง่าย โดยเจ้าของเว็บไซต์ที่มีรหัสผ่าน(Password) เข้าไปแก้ไขข้อมูล ตัวอย่างเช่น นาย ก. นำข้อมูลอันเป็นการหมิ่นประมาท นาย ข. ไปลงในเว็บไซต์ของตน ซึ่งมีผู้เข้าชมมากมาย หาก นาย ข.มาพบและดำเนินคดีทั้งทางแพ่งและอาญากับนาย ก.ฐานหมิ่นประมาท นาย ก.ทราบเรื่องจึงดำเนินการลบข้อความดังกล่าวทิ้งไป เช่นนี้ข้อความอันเป็นการหมิ่นประมาทก็ไม่มีอยู่ให้นาย ข.นำมาเป็นพยานหลักฐานในชั้นศาล ปัญหาต่อมาก็คือศาลจะรับฟังสำเนาจากTemporary files จากเครื่องคอมพิวเตอร์ของนาย ข.หรือสำเนาที่โจทก์บันทึกไว้ได้หรือไม่ เพียงใด[32]

---

[31] ญาณพล ยั่งยืน, "สรุปสาระสำคัญจากการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... ครั้งที่ 11/ 2550"

[32] ปกป้อง ศรีสนิท, "หมิ่นประมาททางอินเทอร์เน็ต",<u>บทบัณฑิตย์</u> เล่ม56, ตอน4 (ธันวาคม 2543): 44.

ในระหว่างการเคลื่อนย้ายข้อมูลที่ถูกบันทึกอยู่ในสื่อบันทึกข้อมูลถาวรของเครื่อง (Hard Disk) นั้น หากระหว่างการเคลื่อนย้ายได้รับความกระทบกระเทือนหรือเกิดการกระแทก หรือเคลื่อนย้ายผ่านจุดที่เป็นสนามแม่เหล็ก ข้อมูลที่บันทึกใน Hard Disk ดังกล่าวก็อาจสูญหายได้[33] หรือถ้าเจ้าหน้าที่ใช้วิธีเก็บพยานหลักฐานเช่นเดียวกับอาชญากรรมธรรมดา โดยมองข้ามไม่ได้ให้ความสนใจที่จะเก็บบันทึกข้อมูลที่ปรากฏอยู่บนจอหรือในหน่วยความจำของคอมพิวเตอร์ ซึ่งเป็นข้อมูลที่อยู่อินเทอร์เน็ต(URL) บนข้อมูลที่เกี่ยวกับเครื่องคอมพิวเตอร์หลัก(Host) และเครือข่ายwww ในช่วงเวลาที่ผู้ต้องหากระทำความผิดและร่องรอยเส้นทางการส่งผ่านข้อมูล(Audit Trail)ไว้เป็นหลักฐาน ก็จะขาดความสมบูรณ์ในการรวบรวมพยานหลักฐานที่สำคัญเพื่อประกอบคดี เพราะเครื่องมือในการกระทำความผิดในที่เกิดเหตุที่เจ้าพนักงานจะได้มามีเพียงเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบการทำงานของเครื่องเท่านั้น[34]

แนวทางที่ให้ศาลเชื่อถือพยานหลักฐานนั้น จะตั้งจัดเก็บพยานหลักฐานด้วยกระบวนการที่รัดกุม ชัดเจน และมีประสิทธิภาพ นับตั้งแต่กระบวนการตรวจยึดเครื่องมืออุปกรณ์ทางคอมพิวเตอร์หรืออิเล็กทรอนิกส์ต้องมีการห่อหุ้มอย่างมิดชิด เพื่อป้องกันมิให้มีการแก้ไขเพิ่มเติมข้อมูล ในขั้นตอนของการเก็บรักษานั้นต้องมิให้มีสัญญาณหรือคลื่นอิเล็กทรอนิกส์เข้ารบกวนหรือทำให้ข้อมูลเสียหาย ในขั้นตอนของการตรวจสอบนั้น จะต้องมีระเบียบวิธีการที่รัดกุม มีการบันทึกและยืนยันโดยพยานผู้รู้เห็น ผู้ร่วมดำเนินการ และประการสำคัญคือต้องไม่ทำการตรวจสอบโดยตรงจากเครื่องของกลาง (ทำการตรวจสอบโดยวิธีการทำสำเนาข้อมูล) ทั้งนี้เพื่อสร้างความเชื่อถือต่อพยานหลักฐาน[35]

ค) <u>เจ้าพนักงานขาดความเชี่ยวชาญในการจัดเก็บพยานหลักฐาน</u>

ในการจัดเก็บพยานหลักฐานบางประเภทที่ต้องใช้ความเชี่ยวชาญเฉพาะ อาจเกิดข้อโต้แย้งเกี่ยวกับการจัดเก็บพยานหลักฐานได้ เช่น ข้อโต้แย้งว่าการจัดเก็บพยานหลักฐานไม่ถูกต้อง ไม่เป็นไปตามหลักวิชาการ จำนวนหรือปริมาณพยานหลักฐานไม่ถูกต้องตามความเป็น

---

[33] http://www.lawyerthai.com/articles/it/index.php

[34] อณิญพิไล เงินวิจิตร, "ปัญหาการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์", วิทยานิพนธ์ (น.ม. จุฬาลงกรณ์มหาวิทยาลัย, 2544)

[35] ญาณพล ยั่งยืน, "บันทึกการประชุมเรื่องการรวบรวมพยานหลักฐานและการรับฟังพยานหลักฐานทางคอมพิวเตอร์," โรงแรมมิราเคิลแกรนด์ ถนนวิภาวดีรังสิต กรุงเทพมหานคร 11 กุมภาพันธ์ 2547

จริง ฯลฯ อาจส่งผลต่อคดีตามมา เช่น อัยการสั่งไม่ฟ้อง หรือเป็นปัญหาความน่าเชื่อถือของพยานหลักฐานในการพิจารณาในชั้นศาลได้

ดังนั้น ในการรวบรวมพยานหลักฐานจากการกระทำความผิดบนอินเทอร์เน็ต ที่พนักงานสอบสวนไม่สามารถจัดเก็บพยานหลักฐานได้เอง อาจจัดให้ผู้ชำนาญการ ผู้เชี่ยวชาญหรือผู้มีความสามารถในกรณีนั้นๆเป็นผู้จัดเก็บตามหลักการและควรกระทำต่อหน้าผู้ต้องหาเพื่อป้องกันการโต้แย้งในภายหลัง[36]

ง) <u>การแสวงหาพยานหลักฐานโดยมิชอบ</u>

ในปัจจุบันมีการหากินรูปแบบใหม่ โดยกลุ่มคนทั้งที่เกี่ยวข้องกับเจ้าของลิขสิทธิ์ (โดยมากเป็นลิขสิทธิ์โปรแกรมที่ขายไม่ออก) รวมกลุ่มกันเป็นขบวนการและรับมอบอำนาจหรือซื้อลิขสิทธิ์จากเจ้าของลิขสิทธิ์แล้วร่วมมือกับเจ้าหน้าที่ตำรวจ โดยมีวิธีการคือเข้าไปดาวน์โหลด (Download) โปรแกรมหรือเพลงที่มีลิขสิทธิ์ มาใส่ไว้ในเครื่องคอมพิวเตอร์ จากนั้นจะกลับเข้ามาตรวจค้นพร้อมเจ้าหน้าที่ตำรวจและข่มขู่จะให้เจ้าหน้าที่ตำรวจจับไปดำเนินคดีหากไม่ยอมจ่ายเงินให้ และเมื่อได้เงินแล้วก็นำเงินที่ได้มาแบ่งกับเจ้าหน้าที่ตำรวจ ซึ่งกรณีดังกล่าวเจ้าหน้าที่ตำรวจไม่มีอำนาจค้นและไม่มีอำนาจจับ เพราะไม่มีหมายค้น และในกรณีข้างต้นไม่ใช่ความผิดซึ่งหน้าเพราะเจ้าหน้าที่ไม่ได้เห็นเหตุการณ์ในขณะกระทำความผิดด้วยตนเอง[37]

---

[36] เทียบเคียงกับ คู่มือพนักงานสอบสวน ประมวลข้อหารือ กฎหมายและระเบียบ หน้า 300 รวบรวมโดย ยงยุทธ เตียวตระกูล (บันทึกข้อความ สำนักงานตำรวจแห่งชาติ ที่0004.6/ 2806 วันที่ 20 มีนาคม พ.ศ. 2546 เรื่องกำชับแนวทางการจัดเก็บตัวอย่างของกลางที่ถูกกล่าวหาว่ากระทำผิด "... เมื่อมีการจับกุมสิ่งผิดกฎหมายใดๆ เช่นน้ำมัน สารเคมี หรือก๊าซต่างๆซึ่งจะต้องมีการจัดเก็บตัวอย่างเพื่อตรวจพิสูจน์ ให้ดำเนินการจัดเก็บให้ถูกต้องตามวิธีการต่อหน้าผู้ต้องหาโดยมีพยานร่วมอยู่ด้วย และหากกรณีใดที่เจ้าพนักงานไม่สามารถจัดเก็บเองได้จะต้องจัดให้ผู้ชำนาญการ ผู้เชี่ยวชาญ หรือผู้มีความรู้ความสามารถในกรณีนั้นๆ เป็นผู้จัดเก็บตามหลักการและจะต้องกระทำต่อหน้าผู้ต้องหาเพื่อป้องกันการโต้แย้งในภายหลัง...")

[37] "บันทึกการประชุมคณะกรรมการกฤษฎีกา(คณะพิเศษ) เรื่องร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ... ครั้งที่1/2547" 16 มกราคม 2547 หน้า 9-10.

จ) ปัญหาในการยึดและค้น[38]

การออกหมายในคดีคอมพิวเตอร์มีขั้นตอนที่ยุ่งยากกว่าปกติ เพราะจะมีปัญหาว่าการออกหมายยึด หมายค้น จะต้องสามารถระบุให้ชัดเจนว่าสิ่งที่ต้องการจะค้นหรือยึดคืออะไร อยู่ที่ไหน และมีสิ่งใดบ้าง ซึ่งการกระทำผิดประเภทนี้ระบุรายละเอียดข้างต้นได้ยาก

ในกรณีที่ สิ่งที่จะต้องยึดมาจากเครือข่ายระบบคอมพิวเตอร์ของผู้อื่น และมีอยู่มากมายในหลายแห่ง จะต้องยึดเครือข่ายทั้งระบบเพื่อให้ได้ทุกสิ่งที่ต้องการหรือจำเป็นในการดำเนินคดี และการรวบรวมข้อมูลเหล่านั้นโดยทำสำเนาทางคอมพิวเตอร์ ก็อาจจะมีปัญหาในแง่ของวิธีการรับฟังพยานหลักฐานอยู่ด้วยว่าศาลจะยอมรับพยานหลักฐานที่เป็นสำเนาหรือไม่ และหากมีความจำเป็นที่จะต้องยึดระบบคอมพิวเตอร์ทั้งระบบเพื่อให้ได้ข้อมูลทุกสิ่งที่ต้องการมาดำเนินคดี อาจจะทำให้ธุรกิจนั้นประสบปัญหาไม่สามารถดำเนินกิจการต่อไปได้ เพราะธุรกิจเหล่านั้นต้องพึ่งพาระบบคอมพิวเตอร์ในการดำเนินงาน

นอกจากนั้นในการค้นตามหมายค้นที่ได้ระบุชัดเจนว่าสิ่งที่ต้องการค้นพบเพื่อนำมาดำเนินคดีคืออะไร หากเข้าไปค้นในระบบเครือข่ายของคอมพิวเตอร์แล้วพบข้อมูลอื่นซึ่งเป็นการกระทำความผิดอาญาฐานอื่นซึ่งไม่เกี่ยวกับความผิดที่มีการออกหมายค้น อาจเกิดปัญหาว่าจะดำเนินการกับสิ่งที่พบในขณะนั้นได้หรือไม่ เพราะเป็นการดำเนินการเกินกว่าที่กำหนดในหมายค้น

การค้นข้อมูลผ่านเครือข่ายอินเทอร์เน็ตอาจเกี่ยวพันไปถึงต่างประเทศทำให้เกิดปัญหาตามมา เช่น เมื่อพบข้อมูลจากต่างประเทศ จะสามารถโอนหรือคัดลอกข้อมูลมาได้หรือไม่ หรือต้องแจ้งต่างประเทศก่อน และประเทศดังกล่าวจะยินยอมหรือไม่ และในทางกลับกันหากต่างประเทศจะดำเนินการเช่นนี้กับไทย ประเทศไทยจะประสานงานได้มากน้อยเพียงใด

---

[38] สถาบันกฎหมายอาญา, "กฎหมายอาชญากรรมทางคอมพิวเตอร์ : แนวทางในการแก้ไขปัญหาอาชญากรรมยุคไอที,"รายงานการสัมมนาทางวิชาการ โครงการเวทีความคิดเพื่อการพัฒนากระบวนการยุติธรรมไทย, หน้า 15.

3.3.3 ปัญหาในการคุ้มครองผู้เสียหายชั่วคราวระหว่างการดำเนินคดี

ในการดำเนินคดีอาญาบางฐาน เช่น ความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญาที่กระทำบนอินเทอร์เน็ต ผู้เสียหายอาจได้รับความเสียหายอย่างต่อเนื่องตราบเท่าที่ถ้อยคำหมิ่นประมาทยังปรากฏอยู่บนอินเทอร์เน็ต และความเสียหายอาจขยายไปยังวงกว้าง เช่น มีการคัดลอกถ้อยคำหมิ่นประมาทไปโพสท์ยังเว็บไซต์อื่นหรือเผยแพร่ลิงค์ของเว็บไซต์ดังกล่าวหรือส่งผ่านทางอีเมล์ต่อไปเป็นทอดๆ และในกรณีนี้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ปฏิเสธที่จะดำเนินการปิดกั้นเว็บไซต์ให้ผู้เสียหายเพราะถือว่าเป็นความผิดส่วนตัวที่ผู้เสียหายต้องไปดำเนินการแจ้งความร้องทุกข์เอง[39]

ในการดำเนินคดีอาญาจึงควรกำหนดให้ผู้เสียหายร้องขอให้เจ้าของเว็บไซต์หรือผู้ควบคุมดูแล ถอนหรือนำข้อความที่หมิ่นประมาทออกในระหว่างดำเนินการทางคดีและอาจกำหนดให้ผู้ให้บริการต้องรับผิดชอบหากไม่ดำเนินการภายในเวลาอันสมควร

3.3.4 ปัญหาในการกำหนดตัวผู้ต้องหา และ/หรือ ผู้กระทำความผิด

ปัญหาสำคัญในการสืบสวนสอบสวนการกระทำความผิดบนอินเทอร์เน็ตคือการระบุตัวผู้กระทำความผิด เพราะการกระทำความผิดในลักษณะนี้แตกต่างจากการกระทำผิดอาญาทั่วไปที่อาจตรวจสอบพยานหลักฐานที่พบในที่เกิดเหตุได้ แต่การกระทำความผิดบนอินเทอร์เน็ตผู้กระทำผิดไม่ต้องมาในที่เกิดเหตุ การดำเนินคดีโดยอาศัยประจักษ์พยานเพื่อพิสูจน์ความผิดของจำเลยจึงไม่อาจกระทำได้หรือกระทำได้ด้วยความยากลำบาก[40] ดังนั้น การระบุตัวผู้กระทำความผิดจึงจำเป็นต้องใช้เทคนิคและขั้นตอนที่ซับซ้อนมากกว่าการสืบสวนสอบสวนคดีทั่วไป

กรณีการหมิ่นประมาทโดยใช้วิธีการส่งอีเมล์ ผู้ส่งสามารถปกปิดชื่อที่แท้จริงของผู้ส่งได้ โดยใช้ชื่อปลอมหรือไม่ระบุชื่อในการสมัครสมาชิก ซึ่งเรียกอีเมล์ดังกล่าวว่า "Anonymous E-mail"[41] หากผู้เสียหายต้องการดำเนินคดีกับผู้ส่งอีเมล์ย่อมเป็นการยากที่เจ้าหน้าที่ตำรวจจะสืบ

---

[39] หนังสือพิมพ์ผู้จัดการ, (11 มกราคม 2551)

[40] ญาณพล ยั่งยืน, "อาชญากรรมทางคอมพิวเตอร์ Computer – Related Crimes",การประชุมคณะกรรมาธิการวิสามัญ 29 พฤศจิกายน 2549, http://wiki.nectec.or.th/nectecpedia/index.php

[41] ปกป้อง ศรีสนิท, "หมิ่นประมาททางอินเทอร์เน็ต",บทบัณฑิตย์ หน้า29-46.

หาตัวผู้ส่งAnonymous E-mailได้ และหากผู้กระทำความผิดได้ส่งอีเมล์นั้นจากสถานที่ให้บริการอินเทอร์เน็ตสาธารณะเช่น โรงเรียน มหาวิทยาลัย ร้านที่ให้บริการอินเทอร์เน็ต(Internet café) การระบุตัวผู้กระทำความผิดย่อมเป็นการยากยิ่งขึ้น เพราะแม้การตรวจสอบหมายเลขไอพีจะระบุได้ว่าการกระทำความผิดเกิดขึ้น ณ สถานที่ใด ผู้กระทำความผิดกระทำความผิดใช้คอมพิวเตอร์เครื่องใดในการกระทำความผิด แต่ก็เป็นการยากที่จะหาพยานหลักฐานมายืนยันพิสูจน์ว่าผู้ต้องหาได้กระทำความผิดจริง ดังนั้น ในบางประเทศ อาทิ ฟิลิปปินส์ ได้พยายามที่จะแก้ปัญหานี้โดยการบัญญัติกฎหมายเพื่อบังคับให้ผู้ใช้งานให้ข้อมูลเกี่ยวกับตนเองก่อนเข้าใช้บริการ[42]

ข้อยุ่งยากอีกประการหนึ่งคือ ผู้กระทำความผิดมักจะไม่กระทำความผิดจากเครื่องตนเองโดยตรง แต่จะเชื่อมต่อไปยังเครื่องคอมพิวเตอร์อื่นเสียก่อนสัก 2-3 ที่เพื่อให้เจ้าของระบบตรวจหาตัวผู้กระทำความผิดไม่ได้ ตัวอย่างเช่น มหาวิทยาลัย A ตรวจสอบพบว่ามีผู้กระทำความผิดกำลังhackระบบ และทราบว่าผู้กระทำความผิดใช้ Log in มาจากมหาวิทยาลัย B เมื่อดำเนินการตรวจสอบที่มาของ Log in ดังกล่าวกับมหาวิทยาลัยB อาจพบว่าเป็น Log in ที่มาจากบริษัท Z และหากตรวจสอบกับบริษัท Z อาจพบว่าบุคคลนั้นไม่ใช่พนักงานของบริษัทแต่เป็น Log in มาจากต่างประเทศ ซึ่งความจริงแล้วผู้กระทำความผิดอยู่ที่กรุงเทพ แต่เชื่อมต่อไปยังเครื่องคอมพิวเตอร์อื่นหลายๆแห่ง ทำให้ไม่สามารถตรวจสอบหาแหล่งที่มาของการกระทำผิดได้ หรือแม้ตรวจสอบหาเครื่องคอมพิวเตอร์ที่ใช้กระทำความผิดพบก็ไม่สามารถตามหาตัวผู้กระทำได้

3.3.5 ปัญหาในการดำเนินการของหน่วยงานและเจ้าหน้าที่ที่เกี่ยวข้อง

ก) <u>ปัญหาด้านกฎหมายสารบัญญัติ</u>

ในขณะที่ยังไม่มีกฎหมายที่เหมาะสมที่จะนำมาปรับใช้กับการกระทำความผิดบนอินเทอร์เน็ตได้ทุกกรณี เช่นกฎหมายอาญาไม่คุ้มครองข้อมูลที่เป็นวัตถุไม่มีรูปร่าง (Intangible Object) จึงไม่สามารถนำฐานความผิดเกี่ยวกับทรัพย์มาปรับใช้ได้ หรือ ไม่สามารถสามารถนำฐานความผิดเกี่ยวกับเอกสาร มาใช้กับการปลอมแปลงข้อมูลในระบบคอมพิวเตอร์ได้ หรือ ในปัจจุบันไม่มีกฎหมายบัญญัติให้การขโมยโดเมนเนม(Domain name)เป็นความผิดจึงทำให้ผู้กระทำความผิดรอดพ้นจากการดำเนินคดี เนื่องจากไม่มีกฎหมายบัญญัติไว้ว่าการกระทำนั้นๆ

---

[42] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ,ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์ ," หน้า 84.

เป็นความผิด และไม่สามารถตีความขยายฐานความผิดตามประมวลกฎหมายอาญาได้ เพราะขัดกับหลักการ "กฎหมายอาญาต้องตีความโดยเคร่งครัด"

ข) ขาดแคลนบุคคลากรที่มีความรู้ความสามารถ

พ.ต.ต.ดร.กฤษณะ พัฒนเจริญ สารวัตรประจำสำนักงานผู้บัญชาการตำรวจแห่งชาติ ทำหน้าที่หัวหน้าฝ่ายอำนวยการ สถาบันฝึกอบรมระหว่างประเทศว่าด้วยการดำเนินการให้เป็นไปตามกฎหมาย ได้เปิดเผยว่า การพัฒนาบุคลากรให้มีความรู้เป็นสิ่งจำเป็น เพราะปัจจุบันมีตำรวจไม่ถึง 50 คน ที่มีความรู้ด้านอาชญากรรมทางอินเทอร์เน็ตโดยตรง[43]และในปัจจุบันภายหลังบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ผู้เขียนตรวจสอบพบว่ามีพนักงานเจ้าหน้าที่ที่แต่งตั้งตามกฎหมายนี้เพียง 35 คนเท่านั้น[44]

ปัญหานี้สำนักงานตำรวจแห่งชาติได้ดำเนินการแก้ไข โดยได้มีการพัฒนาบุคลากรอย่างต่อเนื่อง เช่น มีการจัดการอบรมเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมบนอินเทอร์เน็ต ได้ส่งเจ้าหน้าที่ตำรวจไปอบรมยังต่างประเทศ และ นำเจ้าหน้าที่จากต่างประเทศเข้ามาฝึกอบรมให้แก่เจ้าหน้าที่ในประเทศไทย เช่น มีการฝึกอบรมโดยความร่วมมือจากภาคเอกชนอย่างบริษัทไมโครซอฟ นอกจากนี้ยังมีการส่งเสริมและสนับสนุนให้เจ้าหน้าที่ตำรวจทุกสถานีตำรวจมีความสามารถในการใช้อินเทอร์เน็ตและใช้คอมพิวเตอร์ในการติดต่อกับหน่วยงานต่างๆของสำนักงานตำรวจแห่งชาติอีกด้วย[45] ไม่เพียงเฉพาะเจ้าหน้าที่ตำรวจเท่านั้นทุกหน่วยงานที่เกี่ยวข้องต้องพัฒนาความรู้ด้านนี้ให้มากขึ้น ไม่ว่าจะเป็นพนักงานอัยการหรือศาล มีความ

---

[43] หนังสือพิมพ์มติชน(30 กันยายน 2549): 17.

[44] "ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องแต่งตั้งพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่1 และฉบับที่ 2 "

[45] รายงานงานวิจัยประจำปี 2547 กองวิจัยและพัฒนาโครงการประเมินผลการปฏิบัติงานหัวหน้าสถานีตำรวจ และสำรวจความพึงพอใจของประชาชนในสถานีตำรวจที่ได้รับการกำหนดตำแหน่งหัวหน้าสถานีเป็นผู้กำกับการ มีใจความสำคัญว่า "...ด้านการปฏิบัติงาน1.ควรให้ทุกสถานีตำรวจมีการใช้อินเทอร์เน็ตเพื่อให้มีโลกทัศน์กว้างขึ้น สามารถทำงานโดยใช้อินเทอร์เน็ตให้การประสานงานกับหน่วยงานอื่น ๆ โดยเฉพาะการประสานด้านข้อมูลทางอาชญากรรมทั้งในส่วนของภูธรภาค ภูธรจังหวัด และแต่ละสถานีเพื่อเป็นการกำหนดขั้นตอนและเวลาในการทำงาน2. ในด้านของข้อมูลสารสนเทศ ควรมีการจัดเก็บเอกสารอย่างเป็นระบบโดยใช้คอมพิวเตอร์และสามารถเชื่อมโยงกับหน่วยงานกลางของสำนักงานตำรวจแห่งชาติด้วย..."

คาดหมายว่าหากมีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ศาลอาจยังไม่พร้อมกับการพิจารณาพิพากษาคดีดังกล่าว[46]

ค) ขาดแคลนบันทึกทางด้านสถิติ

อุปสรรคสำคัญประการหนึ่งในการศึกษาเกี่ยวกับการกระทำความผิดเพื่อหามาตรการป้องกันและปราบปรามการกระทำผิดบนอินเทอร์เน็ต คือ การขาดแคลนบันทึกทางด้านสถิติ (Lack of statistics)[47] โดยเฉพาะการบันทึกทางสถิติจากเจ้าหน้าที่ภาครัฐ บันทึกทางสถิติส่วนใหญ่จึงบันทึกทางสถิติที่จัดทำโดยองค์กรภาคเอกชนที่ประกอบธุรกิจเกี่ยวกับระบบรักษาความปลอดภัยอาชญากรรมคอมพิวเตอร์ จึงขาดความน่าเชื่อถือ

การขาดแคลนบันทึกทางสถิตินี้ไม่ใช่เพียงขาดแคลนเฉพาะบันทึกทางสถิติเกี่ยวกับแนวคิดของอาชญากรรมอย่างมีมาตรฐาน (Standardized conceptualization of crimes) แต่รวมถึงการขาดแคลนการจัดทำบันทึกที่มีระเบียบแบบแผน (Systematic reporting) หรือการบันทึกตามหลักเกณฑ์ทางวิชาการ (Recording methodologies) และถึงแม้จะมีบันทึกทางสถิติอย่างมีมาตรฐานหรือเป็นระเบียบแบบแผนก็ตาม แต่ก็ยังมีข้อโต้แย้งเกี่ยวกับความไม่ชัดเจนของข้อมูลที่ได้บันทึกไว้[48]

ทั้งนี้ ในประเทศไทยบันทึกทางสถิติที่เกี่ยวข้องกับการกระทำความผิดบนอินเทอร์เน็ตที่จัดทำขึ้นโดยหน่วยงานของรัฐ ไม่สามารถชี้วัดจำนวนการกระทำความผิดที่แท้จริงได้ โดยผู้เขียนศึกษาพบว่ารายงานปัญหาที่พบจากการใช้งานอินเทอร์เน็ตที่จัดทำโดยภาครัฐ[49] ไม่ได้เก็บบันทึกสถิติการกระทำความผิดจากข้อมูลการรายงานการกระทำผิดจริงโดยตรง แต่เป็นการประเมินผลจากการตอบแบบสอบถามจากกลุ่มตัวอย่าง 20,067 คน[50] ซึ่งจะเห็นได้ว่ารายงานทาง

---

[46] สราวุธ เบญจกุล, "ร่วมวิพากษ์ร่าง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...." การเสวนารับฟังความคิดเห็นจัดโดยสมาคมผู้ดูแลเว็บไทย วันที่ 21 ธันวาคม 2549.

[47] David S. Wall, Cybercrimes and the internet,(London : Routledge , 2001) p.7

[48] Ibid., p.18

[49] ฝ่ายพัฒนานโยบายและกฎหมาย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ [Nectec],"รายงานผลการสำรวจกลุ่มผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2548"

[50] เรื่องเดียวกัน, หน้า 79-89.

สถิติดังกล่าวไม่สามารถชี้วัดสถิติของการกระทำความผิดที่แท้จริงได้ เพราะไม่ได้บันทึกผลจากฐานข้อมูลการกระทำผิดจริงที่มีความน่าเชื่อถือ หรือรวบรวมจากหน่วยงานที่เกี่ยวข้องโดยตรง

ง) <u>การจัดทำประวัติของผู้กระทำผิด</u>

ประวัติของผู้กระทำความผิด (Offender profiles) มีความสำคัญต่อการควบคุมอาชญากรรม กล่าวคือ สามารถช่วยให้คาดหมายการก่ออาชญากรรมได้ ซึ่งสามารถนำมาใช้ประโยชน์ในการวางมาตรการป้องกันและปราบปรามการกระทำความผิดบนอินเทอร์เน็ต โดยการจัดกลุ่มผู้กระทำความผิด เช่น กลุ่มวัยทำงาน กลุ่มนักเรียนนักศึกษา ฯลฯ แล้วนำมาวิเคราะห์รูปแบบและลักษณะของการกระทำความผิด มูลเหตุจูงใจในการกระทำความผิด รวมถึงเป้าหมายของการกระทำความผิด ซึ่งนำไปสู่การวางมาตรการควบคุมการกระทำผิด เช่น การบัญญัติกฎหมายที่กำหนดบทลงโทษอย่างเหมาะสม แต่ในปัจจุบันไม่มีการจัดทำประวัติผู้กระทำความผิดที่มีรายละเอียดเพียงพอ โดยเฉพาะในประเทศไทย ขณะที่ยังไม่มีกฎหมายบัญญัติฐานความผิดที่กระทำบนอินเทอร์เน็ต การเขียนบันทึกประจำวันของเจ้าหน้าที่ตำรวจไม่ได้ระบุว่าเป็นการกระทำผิดบนอินเทอร์เน็ต แต่จะบันทึกตามฐานความผิดของกฎหมายอาญาเท่าที่สามารถเอาผิดกับผู้กระทำความผิดได้ เช่น การลงบันทึกประจำวันระบุว่ามีการกระทำผิดฐานฉ้อโกง หมิ่นประมาท จึงไม่สามารถนำข้อมูลดังกล่าวไปใช้ในการวิเคราะห์การกระทำความผิดบนอินเทอร์เน็ตได้[51]

จ) <u>ปัญหาอันเกิดจากสภาพไร้พรมแดนของอาชญากรรม[52]</u>

อาชญากรรมคอมพิวเตอร์มีลักษณะไร้พรมแดน เพราะโดยลักษณะของเครือข่ายอินเทอร์เน็ตมีลักษณะครอบคลุมไปทั่วโลกอย่างไร้พรมแดน ไม่ถูกจำกัดไว้ด้วยเขตแดนทางภูมิศาสตร์ของแต่ละรัฐ การกระทำความผิดบนอินเทอร์เน็ตจึงยากที่จะควบคุมด้วยกฎหมายของรัฐใดรัฐหนึ่ง เพราะการกระทำความผิดอาจเกี่ยวพันกันได้หลายประเทศ ผู้กระทำความผิด ผู้เสียหาย สถานที่เกิดการกระทำความผิด และสถานที่เกิดผลแห่งการกระทำ ไม่จำต้องอยู่ใน

---

[51] สัมภาษณ์ นิเวศน์ อาภาวศิน รองผกก.อก ศตท, 16 สิงหาคม 2549.

[52] สถาบันกฎหมายอาญา, "กฎหมายอาชญากรรมทางคอมพิวเตอร์ : แนวทางในการแก้ไขปัญหาอาชญากรรมยุคไอที," <u>รายงานการสัมมนาทางวิชาการ โครงการเวทีความคิดเพื่อการพัฒนากระบวนการยุติธรรมไทย</u>, หน้า 14.

ประเทศเดียวกัน จึงเกิดปัญหาว่าจะดำเนินคดีกับผู้กระทำความผิดอย่างไร ในปัญหานี้อาจแบ่งแยกได้เป็น 3 ประเด็นปัญหาใหญ่ ๆ คือ

1.) ปัญหาเรื่องเขตอำนาจศาล

โดยทั่วไปแล้ว แต่ละประเทศมีอำนาจอธิปไตยเป็นของตนเอง แต่ละรัฐจึงมีอำนาจที่จะออกกฎหมายเพื่อใช้บังคับในรัฐของตน มีอำนาจในการบริหารและวางมาตรการในการควบคุมความสงบเรียบร้อยในรัฐของตนได้ แต่ก็มีข้อจำกัดในเรื่องขอบเขตของการใช้กฎหมายอาญา เพราะกระทำความผิดบนอินเทอร์เน็ตนี้มีลักษณะไร้พรมแดนขยายเครือข่ายไปได้ทั่วโลก ซึ่งทำให้เกิดปัญหาทางกฎหมายในการพิจารณาว่าหากความผิดเกี่ยวพันระหว่างสองประเทศขึ้นไป ประเทศใดจะมีเขตอำนาจในการพิจารณาดำเนินคดีเกี่ยวกับเรื่องนั้น เช่น มีผู้ใช้คอมพิวเตอร์และระบบเครือข่ายที่ต่างประเทศสื่อสารเข้ามาถึงระบบเครือข่ายคอมพิวเตอร์ในไทย แล้วเข้ามาทำลายหรือขโมยข้อมูลทางคอมพิวเตอร์ในประเทศไทย จะเกิดปัญหาว่าประเทศใดมีเขตอำนาจศาลหรือเขตอำนาจในการดำเนินคดีนี้ จำเป็นต้องพิจารณาว่าความผิดเกิดขึ้นในเขตอำนาจของศาลใด

ในประเด็นดังกล่าวอาจจำเป็นต้องพิจารณาว่าการกระทำผิดสำเร็จแล้วหรือไม่ การกระทำผิดสำเร็จที่ใด เนื่องจากต้องนำมาใช้ในการวินิจฉัยเรื่องเขตอำนาจศาลด้วย เช่น ความผิดฐานหมิ่นประมาท ความผิดที่ต้องการผลของการกระทำในระดับหนึ่ง กล่าวคือ ต้องให้บุคคลที่สามรับทราบข้อความหมิ่นประมาทก่อน จึงจะถือว่าเป็นความผิดสำเร็จ ถ้าบุคคลที่สามไม่ทราบข้อความเลยก็เป็นเพียงการพยายามกระทำความผิด[53] ตัวอย่างเช่น นาย ก. ส่งอีเมล์ที่มีข้อความหมิ่นประมาทนาย ข. ไปให้นาย ค.อ่าน หากนาย ค.ยังไม่เปิดอ่าน การกระทำผิดก็ยังไม่บรรลุผลเพราะยังไม่มีบุคคลที่สามทราบข้อความนั้น การกระทำของนาย ก.จึงเป็นเพียงความผิดฐานพยายามหมิ่นประมาท แต่ถ้านาย ค. อ่านข้อความดังกล่าวแล้วถือว่าการกระทำของนาย ก. เป็นความผิดสำเร็จในฐานหมิ่นประมาท ปัญหาที่ตามมาก็คือ หากนาย ค .อยู่ที่ต่างประเทศ ศาลไทยจะมีอำนาจในการพิจารณาคดีกับนาย ข.ฐานหมิ่นประมาทในกรณีความผิดสำเร็จหรือไม่

ในประเด็นปัญหานี้มี พ.ต.อ.ญาณพล ยั่งยืน *"...ควรกำหนดให้ผู้มีสัญชาติไทยซึ่งกระทำความผิดเรื่องอาชญากรรมทางคอมพิวเตอร์ไม่ว่ากระทำความที่ใดบนโลกนี้ให้ถือว่าความผิดเกิดขึ้นในประเทศไทย เหมือนกับประเทศสหรัฐอเมริกาได้ออกกฎหมาย Patiot Act ไม่ว่าคนสัญชาติอเมริกันจะกระทำผิดที่ไหนก็ตาม ไม่การกระทำความผิดในสหรัฐเองหรือ*

---

[53] ปกป้อง ศรีสนิท, "หมิ่นประมาททางอินเทอร์เน็ต",บทบัณฑิตย์, หน้า 37.

ประเทศอื่น ถือเป็นความผิดในเขตอำนาจของสหรัฐ รวมทั้งกฎหมายประเทศเยอรมันก็กำหนดไว้ในลักษณะนี้เหมือนกัน..."[54] ซึ่งต่อมาแนวคิดนี้ได้ถูกนำไปใช้ประกอบการร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา17

2) ปัญหาความร่วมมือระหว่างประเทศในการดำเนินคดี

ปัญหานี้สืบเนื่องจากปัญหาเขตอำนาจศาล หากมีความจำเป็นต้องสืบสวน สอบสวน และดำเนินคดีในประเทศใดประเทศหนึ่ง จะขอความร่วมมือในทางคดีกับประเทศที่เกี่ยวข้องได้หรือไม่ และในขอบเขตมากน้อยเพียงใด ตามปกติแล้วประเทศที่มีสนธิสัญญาระหว่างกันก็สามารถขอความร่วมมือในการช่วยเหลือทางด้านคดีได้ ซึ่งในประเทศไทยมีพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535 แต่พระราชบัญญัติดังกล่าวมีเงื่อนไข และหลักเกณฑ์ที่ซับซ้อน อีกทั้งใช้เวลาประสานงานยาวนานในการดำเนินการยาวนาน ทำให้ไม่เหมาะสมกับการดำเนินคดีกับอาชญากรรมคอมพิวเตอร์ ซึ่งจะต้องอาศัยความรวดเร็วในการจัดการกับปัญหา เพราะพยานหลักฐานต่างๆอาจสูญหาย ถูกทำลาย แก้ไข เปลี่ยนแปลงส่งผลให้ไม่อาจลงโทษผู้กระทำความผิดได้

แนวทางการแก้ไขปัญหาดังกล่าวเจ้าหน้าที่ที่เกี่ยวข้องในแต่ละประเทศจะอาศัยความร่วมมือลักษณะถ้อยทีถ้อยอาศัยกันเป็นเครือข่ายประสานงาน มากกว่าการขอความร่วมมือตามสนธิสัญญาระหว่างประเทศ เพราะมีความคล่องตัวและรวดเร็วมากกว่า เช่น กรณีที่มีการกระทำความผิดในประเทศไทย และตรวจสอบได้ว่า IP ผู้กระทำความผิดอยู่ที่ประเทศสเปน การจะสืบทราบว่าผู้ใดเป็นผู้กระทำผิดย่อมเป็นเรื่องยาก เพราะไม่ทราบว่าจะขอความร่วมมือจากหน่วยงานใด เจ้าหน้าที่ใดเป็นผู้รับผิดชอบ จะขอความร่วมมือจากเว็บมาสเตอร์ของสเปนได้อย่างไร และต้องใช้ระยะเวลายาวนานเพียงใดกว่าจะสืบสวนไปถึงตัวผู้กระทำความผิด หรือ ในกรณีที่เจ้าหน้าที่ตำรวจของไทยได้รับแจ้งจากเจ้าหน้าที่ตำรวจฮ่องกงว่า มีการตั้งเซิฟเวอร์ของธนาคารฮ่องกงเถื่อนในประเทศไทย โดยเปิดเว็บไซต์หลอกลวงให้ผู้ที่มาติดต่อใช้บริการกับธนาคารเถื่อนดังกล่าว เจ้าหน้าที่ตำรวจของไทยก็อาจให้ความช่วยเหลือด้วยการลบเว็บไซต์ดังกล่าวได้

---

[54] ญาณพล ยั่งยืน, "บันทึกการประชุมคณะกรรมการกฤษฎีกา(คณะพิเศษ) เรื่องร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ... ครั้งที่1/2547" 16 มกราคม 2547

ทันที[55] จากตัวอย่างที่ได้ยกมาทั้ง 2 กรณี จะเห็นได้ว่าหาต้องดำเนินการตามขั้นตอนการขอความร่วมมือทางกฎหมายอาจไม่ทันท่วงทีในการดำเนินคดีกับผู้กระทำความผิด การอาศัยความร่วมมือลักษณะถ้อยทีถ้อยอาศัยกันเป็นเครือข่ายประสานงานจึงมีความฉับไวและคล่องตัวมากกว่า

ทั้งนี้ ในบางประเทศได้มีการจัดตั้งศูนย์บริการในเรื่องที่เกี่ยวกับการช่วยเหลือกันทางคดีระหว่างประเทศ โดยจัดบุคลากรพร้อมที่จะตอบสนองการร้องขอตลอด 24 ชั่วโมง (24/7 network) เพื่อให้สามารถสื่อสารต่อกันได้อย่างฉับไวตลอดเวลา[56]

3) ปัญหาความแตกต่างของกฎหมายในแต่ละประเทศ

กฎหมายในแต่ละประเทศมีความแตกต่างกัน เนื่องมาจากมาตรฐานทางวัฒนธรรมและ ศีลธรรมของแต่ละประเทศแตกต่างกัน โดยเฉพาะกฎหมายที่ควบคุมการกระทำที่ผิดศีลธรรมแท้ๆ (Moral Offence) เช่น ร่วมเพศวิตถาร รักร่วมเพศ โสเภณี การทำชู้ การเผยแพร่ภาพลามกอนาจาร การครอบครองภาพลามกอนาจารเด็ก การพนัน เป็นต้น ในบางประเทศบัญญัติให้การกระทำต่างๆเหล่านี้เป็นความผิดทางอาญา แต่อีกประเทศหนึ่งการกระทำเช่นเดียวกันกลับไม่ได้ถือเป็นความผิดทางอาญา ในกรณีนี้หากประเทศที่กำหนดเป็นความผิดต้องการดำเนินคดีความผิดนั้นกับบุคคลที่อยู่ในประเทศอื่นที่มิได้กำหนดเป็นความผิด ย่อมเกิดปัญหาในการขอความร่วมมือระหว่างประเทศทางอาญา หรือการขอให้ส่งผู้ร้ายข้ามแดนจากประเทศที่มิได้กำหนดความผิดไว้

สำหรับการดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ตอาจเกิดปัญหาในกรณีที่กฎหมายแต่ละประเทศกำหนดความผิดไว้แตกต่างกัน เช่น ในหลายประเทศไม่มีฐานความผิดเกี่ยวกับภาพลามกอนาจารเด็ก หรือ ไม่ถือว่าการละเมิดลิขสิทธิ์เป็นการกระทำผิดทางอาญา เป็นต้น

---

[55] "ญาณพล ยั่งยืน : กับงานสอบสวนคดีพิเศษบนโลกอาชญากรรมออนไลน์" บทสัมภาษณ์นักวิชาการ http://www.Thaicleannet.com .

[56] สถาบันกฎหมายอาญา, "กฎหมายอาชญากรรมทางคอมพิวเตอร์ : แนวทางในการแก้ไขปัญหาอาชญากรรมยุคไอที,"รายงานการสัมมนาทางวิชาการ โครงการเวทีความคิดเพื่อการพัฒนากระบวนการยุติธรรมไทย, หน้า 14.

ฉ) ปัญหาในการปิดกั้นเว็บไซต์ที่ไม่เหมาะสม

มาตรการการปิดกั้นเว็บไซต์ที่ไม่เหมาะสม เพื่อควบคุมการกระทำความผิดอาญาบนอินเทอร์เน็ตนั้น มีปัญหาในการดำเนินการในทางปฏิบัติมากมาย อันได้แก่

1. ปัญหาผู้กระทำความผิดย้ายที่อยู่หรือสถานที่กระทำความผิดบนพื้นที่อินเทอร์เน็ต

กล่าวคือ ทำให้ยากที่จะปิดกั้นเว็บไซต์ที่ไม่เหมาะสมได้ทั้งหมด เพราะเมื่อได้ทำการปิดกั้นเว็บไซต์ดังกล่าวแล้ว ผู้กระทำความผิดอาจเปลี่ยนชื่อเว็บไซต์ใหม่ทำให้ไม่สามารถติดตามไปปิดกั้นได้ เช่น เว็บไซต์ที่กระทำความผิดชื่อว่า XYZ เมื่อถูกปิดกั้นแล้ว ก็จะเปลี่ยนชื่อเป็น XYZ 1 เมื่อทำการปิดกั้นอีก ก็จะเปลี่ยนชื่อเป็น XYZ 2,3,4...ไปเรื่อยๆ[57] หรือเปลี่ยนเป็นชื่ออื่นเพื่อไม่ให้เจ้าหน้าที่ตรวจสอบได้โดยง่าย สร้างความยากลำบากให้กับเจ้าหน้าที่ที่เกี่ยวข้อง

2. ปัญหาเกี่ยวกับกฎหมายที่ให้อำนาจเจ้าหน้าที่ที่เกี่ยวข้อง

ในขณะที่การปิดกั้นเว็บไซต์ไม่มีกฎหมายใดกำหนดไว้โดยเฉพาะการปิดกั้นเว็บไซต์จึงเป็นการขอความร่วมมือระหว่างหน่วยงาน ในประเด็นนี้คณะกรรมการกฤษฎีกาได้มีคำวินิจฉัยที่น่าสนใจไว้ดังนี้

"...เมื่อไม่มีกฎหมายใดให้อำนาจไว้ เจ้าพนักงานตำรวจจึงไม่อาจสั่งปิดเว็บไซต์นั้นเองหรือขอให้ศาลสั่งปิดได้ อนึ่ง แม้เจ้าพนักงานตำรวจไม่อาจสั่งปิดเว็บไซต์ดังกล่าวได้ แต่อาจแจ้งให้คณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.) ในฐานะผู้ควบคุมและผู้อนุญาตในการประกอบกิจการโทรคมนาคมดำเนินการเพิกถอนใบอนุญาตการให้บริการอินเทอร์เน็ตได้ตามมาตรา 15 แห่งพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 ประกอบกับข้อ 13และข้อ 15 แห่งประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์และวิธีการขอรับใบอนุญาตการให้บริการอินเทอร์เน็ต ลงวันที่ 20 มิถุนายน 2548 ที่กำหนดให้คณะกรรมการกิจการโทรคมนาคมแห่งชาติมีอำนาจระงับ ยกเลิก หรือเพิกถอนใบอนุญาตการให้บริการ

---

[57] ญาณพล ยั่งยืน, "บันทึกการประชุมคณะกรรมการกฤษฎีกา(คณะพิเศษ) เรื่องร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ... ครั้งที่1/2547", หน้า 7.

อินเทอร์เน็ตได้ในกรณีมีความจำเป็นต้องปกป้องความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือในกรณีที่ผู้รับใบอนุญาตละเลยมาตรการเพื่อสังคมที่จะต้องพึงระมัดระวังมิให้ผู้ใช้บริการนำเครือข่ายอินเทอร์เน็ตไปใช้โดยมิชอบ หรือเผยแพร่ข้อมูลอันอาจทำลายความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน..."[58]

จากคำวินิจฉัยดังกล่าว จึงควรมีกฎหมายกำหนดหน่วยงานหรือเจ้าหน้าที่เป็นผู้มีอำนาจดำเนินการปิดกั้นเว็บไซต์ไว้เป็นการเฉพาะ[59] เพื่อป้องกันการโต้แย้งว่าเจ้าพนักงานหรือหน่วยงานนั้นๆมีอำนาจถูกต้องตามกฎหมายหรือไม่ และควรกำหนดหน้าที่ของผู้ให้บริการให้ชัดเจน และครอบคลุมถึงการเผยแพร่เนื้อหาที่ไม่เหมาะสมอื่นๆ(เช่น การแสดงลามกอนาจารผ่าน Camforg ที่ปัจจุบันกฎหมายยังไม่ครอบคลุมถึง[60])

นอกจากนี้การใช้อำนาจปิดกั้นเว็บไซต์เจ้าหน้าที่อาจใช้ดุลยพินิจโดยไม่มีหลักเกณฑ์ เช่น การปิดกั้นเว็บไซต์ Youtube.com ทั้งเว็บไซต์ ทั้งที่มีคลิปวีดิโอที่เป็นปัญหาเพียงไม่กี่ไฟล์เท่านั้น ตามเนื้อความในข่าว ดังนี้

รัฐมนตรีกระทรวง ICT ด.ร. สิทธิชัย โภไคยอุดม ให้สัมภาษณ์รอยเตอร์ *"...ยอมรับว่าสั่งบล็อค YouTube ทั้งเว็บไซต์ หลังได้พยายามขอความร่วมมือกูเกิลหลายครั้งในสัปดาห์ที่แล้ว ให้นำคลิปตัดต่อหมิ่นพระบรมฉายาลักษณ์ออกไม่เป็นผลสำเร็จ ICT จะเลิกบล็อค YouTube ก็ต่อเมื่อ YouTube นำเอาคลิปนั้นออกไปแล้ว..."*[61]

---

[58] "บันทึกสำนักงานคณะกรรมการกฤษฎีกาเรื่อง อำนาจของเจ้าพนักงานตำรวจในการปิดกั้นเว็บไซต์ที่ไม่เหมาะสม ทางอินเทอร์เน็ต และของพนักงานสอบสวนตามมาตรา 132 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา เรื่องเสร็จที่ 343/2549"

[59] "สรุปสาระสำคัญการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ครั้งที่ 13/2550"

[60] ญาณพล ยั่งยืน, "จ่อจับโชว์สยิว ในแคมฟรอก", หนังสือพิมพ์ไทยรัฐ, (20 ธันวาคม 2549)

[61] http://www.reuters.com/article/companyNewsAndPR/ idUSN0432594820070404?page Number=1

3. ปัญหามาตรฐานและหลักเกณฑ์จำแนกเพื่อการปิดกั้นเว็บไซต์ที่ไม่เหมาะสม

การปิดกั้นเว็บไซต์ที่ไม่เหมาะสม ในปัจจุบันไม่มีกฎหมายกำหนดมาตรฐานการปิดกั้น การใช้ดุลยพินิจในการพิจารณาความเหมาะสมเป็นอำนาจของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร(ICT) ทำให้การปิดกั้นเว็บไซต์อาจกระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชนและกระทบสิทธิเสรีภาพอื่นๆอีกหลายประการ เนื่องจากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมีอำนาจที่มากเกินไป อาจตกเป็นเครื่องมือของผู้มีอำนาจทางการเมืองได้ เช่นในปัจจุบันกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้รับอำนาจโดยอาศัยคำสั่งประกาศคณะปฏิรูปการปกครอง ฯ ดังนี้ [62]

"...ตามที่ คณะปฏิรูปการปกครองในระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข ได้ทำการยึดการปกครองแล้ว นั้น จึงให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการยับยั้ง สกัดกั้น และทำลาย การเผยแพร่ข้อมูลข่าวสารในระบบสารสนเทศ ผ่านระบบการสื่อสารทั้งปวงที่มีบทความ ข้อความ คำพูด หรืออื่นใด อันจะส่งผลกระทบต่อคณะปฏิรูปการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข ตามที่ คณะปฏิรูปการปกครองในระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข ได้ประกาศในเบื้องต้นแล้ว..."

ด้วยผลของคำสั่งฉบับดังกล่าวส่งผลให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารปิดกั้นเว็บไซต์ต่างๆมากมายโดยไม่มีการเปิดเผยว่าใช้หลักเกณฑ์ใดในการพิจารณา ทำให้ประชาชนถูกลิดรอนสิทธิเสรีภาพในการแสดงออกและสิทธิในการรับทราบข้อมูลข่าวสาร จึงควรมีการกำหนดมาตรฐานการปิดกั้น และมีขั้นตอนที่โปร่งใส มิให้มาตรการนี้ตกเป็นเครื่องมือทางการเมืองหรือการเลือกปฏิบัติ

นายปรเมศวร์ มินศิริ นายกสมาคมผู้ดูแลเว็บไทย กล่าวในการสัมมนาว่า *"...ในฐานะคนทำเว็บไซต์และนายกสมาคมฯ รู้สึกว่า รัฐบาลนี้ ตั้งอยู่บนความหวาดกลัว โดยรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร หรือ ไอซีที เคยติดต่อเจ้าของ*

---

[62] "ประกาศคณะปฏิรูปการปกครองในระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข ที่5/2549"

เว็บไซต์ให้โทรศัพท์ไปหาหรือโทรศัพท์ไปถามเจ้าของเว็บไซต์บางแห่งว่า ทำไมจึงมีข้อมูล หรือข้อความไม่เหมาะสมในเว็บไซต์ หรือ บนเว็บบอร์ด และกำชับให้ลบข้อความเหล่านั้น

สิ่งที่เกิดขึ้นแสดงว่า รัฐบาลเกรงกลัวว่า การแสดงความคิดเห็นผ่านเว็บไซต์จะมีผลกระทบต่อรัฐบาล แต่มาตรการปิดกั้น หรือ สั่งให้ผู้ให้บริการอินเทอร์เน็ตบล็อกไม่ใช่ทางเลือกที่ดี เพราะส่วนใหญ่เป็นเว็บไซต์ทางการเมือง ดังนั้น บางครั้งเว็บไซต์ใหญ่ๆ และผู้ให้บริการอินเทอร์เน็ต หรือ ไอเอสพี บางรายจึงขอให้กระทรวงไอซีทีทำหนังสือแจ้งมาเป็นลายลักษณ์อักษร แต่ก็ไม่เคยเห็น... ในสมัยรัฐบาลที่แล้ว ได้มีการตั้งหน่วยงานชื่อไซเบอร์อินสเปกเตอร์ขึ้นมาทำหน้าที่บล็อกและปิดเว็บไซต์ โดยมีสารวัตอินเทอร์เน็ตเป็นผู้รับผิดชอบ ทั้งๆ ที่กฎหมายรองรับไม่มี นอกจากนั้น ยังรู้สึกว่า การบล็อกเว็บไซต์ต่างๆ จะเป็นการบล็อกตามใบสั่งของผู้มีอำนาจ เพราะตนเองเคยแจ้งให้บล็อกเว็บไซต์ที่ไม่เหมาะสมมากๆ ตามช่องทางที่มีการวางกลไกไว้ แต่ก็ไม่มีการดำเนินการ"[63]

พ.ต.อ.ญาณพล ยั่งยืน ได้เสนอความเห็นในเรื่องการปิดกั้นเว็บไซต์ว่า *"ควรกำหนดมาตรฐานในการผิดกั้นเว็บไซต์ควรแยกออกเป็น 2 ประเภทคือ 1. เว็บไซต์ที่กระทำความผิดอย่างแน่นอน เช่น เว็บไซต์ที่เกี่ยวข้องกับการพนัน ภาพลามกอนาจารเด็ก สามารถดำเนินการปิดกั้นได้ทันทีโดยไม่ต้องร้องขอต่อศาล และ 2. เว็บไซต์ที่เกี่ยวข้องกับความมั่นคง ควรให้ศาลเป็นผู้พิจารณาวินิจฉัย เพราะการจะพิจารณาว่าเว็บไซต์ดังกล่าวกระทบต่อความมั่นคงหรือไม่เป็นเรื่องสลับซับซ้อน ผู้มีอำนาจในประเทศอาจเข้าแทรกแซงการปิดกั้นเว็บไซต์โดยอ้างของมั่นคงของประเทศได้ จึงควรให้ศาลพิจารณาว่าความมั่นคงนั้นเป็นความมั่นคงของรัฐ(ประเทศ) หรือความมั่นคงของรัฐบาล(ผู้มีอำนาจ) เพราะการใช้อำนาจดังกล่าวย่อมกระทำต่อสิทธิเสรีภาพของประชาชน"*[64] ซึ่งต่อมาแนวคิดนี้ได้ถูกนำไปใช้ประกอบการร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มาตรา20

---

[63] "ชี้ 'ไอซีที' ไล่บล็อกเว็บไซต์ภาพประ เทศไม่สวย แนะอาศัยอำนาจศาล"หนังสือพิมพ์ไทยรัฐ, (6 เมษายน 2550)

[64] ญาณพล ยั่งยืน , "ร่วมวิพากษ์ร่าง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...." การเสวนารับฟังความคิดเห็นจัดโดยสมาคมผู้ดูแลเว็บไทย วันที่ 21 ธันวาคม 2549.

4. ปัญหาการให้ความร่วมมือของผู้เกี่ยวข้อง

ในบางกรณีเจ้าหน้าที่ไม่อาจดำเนินคดีได้โดยสะดวก เพราะผู้ที่เกี่ยวข้อง เช่น ผู้ให้บริการหรือผู้ครอบครองข้อมูล ไม่ให้ความร่วมมือในการให้ข้อมูลของผู้เผยแพร่ภาพลามกอนาจารหรือ ข้อมูลการจัดให้มีการเล่นการพนันบนอินเทอร์เน็ตให้แก่เจ้าหน้าที่ตำรวจ โดยอ้างว่าพนักงานสอบสวนไม่มีอำนาจในการเรียกพยานหลักฐานดังกล่าว ดังเช่นที่ปรากฏตามหนังสือของสำนักงานตำรวจแห่งชาติ ถึงสำนักงานคณะกรรมการกฤษฎีกา ดังนี้[65]

"...1. กรณีที่เจ้าพนักงานตำรวจแจ้งผู้ให้บริการอินเทอร์เน็ตให้ทำการปิดกั้นเว็บไซต์ที่มีการเผยแพร่ภาพลามกอนาจารหรือการกระทำผิดกฎหมายอย่างอื่น แต่ผู้ให้บริการอินเทอร์เน็ตไม่ทำการปิดกั้นเว็บไซต์ดังกล่าว จะถือว่าผู้ให้บริการมีส่วนร่วมในการกระทำผิดในเรื่องนั้นหรือไม่ และการสั่งปิดเว็บไซต์จะต้องมีหมายศาลตามที่บริษัท เอเชีย อินโฟเน็ต จำกัด ร้องขอหรือไม่ ประการใด

2. กรณีพนักงานสอบสวนออกหมายเรียกเอกสารหรือพยานบุคคลที่เกี่ยวข้องตามมาตรา 132 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา นั้น พนักงานสอบสวนจะมีอำนาจเข้าถึงข้อมูลโทรคมนาคมได้หรือไม่ เพียงใด กรณีบริษัทผู้ครอบครองข้อมูลไม่ยินยอมโดยอ้างว่าพนักงานสอบสวนทั่วไปไม่ควรมีอำนาจมากกว่าหน่วยงานพิเศษ เช่น กรมสอบสวนคดีพิเศษซึ่งต้องอาศัยคำสั่งศาลเพื่อเข้าถึงข้อมูลโทรคมนาคม โดยต้องยื่นคำร้องฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญา เพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูล จึงขอหารือว่าอำนาจของพนักงานสอบสวนตามมาตรา 132 แห่งประมวลกฎหมายวิธีพิจารณาความอาญานั้น สามารถเข้าถึงข้อมูลทางโทรคมนาคมและอินเทอร์เน็ต โดยไม่ต้องมีคำสั่งจากศาลเช่นเดียวกับพนักงานสอบสวนคดีพิเศษของกรมสอบสวนคดีพิเศษได้หรือไม่ หรือจะต้องร้องขอต่อศาลเพื่อมีคำสั่งอนุญาตเสียก่อน.."

คณะกรรมการกฤษฎีกา(คณะที่ 11) ได้พิจารณาหนังสือของสำนักงานตำรวจแห่งชาติดังกล่าวแล้ว เห็นว่า มีปัญหาข้อกฎหมาย 3 ประเด็นและได้ให้ความเห็นในแต่ละประเด็น ดังนี้

---

[65] "หนังสือของสำนักงานตำรวจแห่งชาติ ที่ ตช 0031.212/2408 ลงวันที่ 10 เมษายน 2549"

"...ประเด็นที่1 ในกรณีที่เจ้าพนักงานตำรวจแจ้งไปยังผู้ให้บริการอินเทอร์เน็ตเพื่อให้ปิดกั้นเว็บไซต์ที่มีการเผยแพร่ภาพลามกอนาจารหรือมีการกระทำผิดกฎหมายอย่างอื่น แต่ผู้ให้บริการอินเทอร์เน็ตไม่ปิดกั้นเว็บไซต์ดังกล่าว จะถือว่าผู้ให้บริการอินเทอร์เน็ตมีส่วนร่วมในการกระทำความผิดในเรื่องนั้นหรือไม่ อย่างไร นั้น เห็นว่า ในกรณีที่ผู้ใช้บริการอินเทอร์เน็ตเปิดเว็บไซต์เพื่อเผยแพร่ภาพลามกอนาจาร เพื่อให้มีการเล่นพนันโดยไม่ได้รับอนุญาต หรือเพื่อกระทำความผิดอื่น ถ้าการกระทำดังกล่าวเข้าองค์ประกอบความผิดอาญาอย่างใดอย่างหนึ่ง เมื่อเจ้าพนักงานตำรวจได้แจ้งให้ผู้ให้บริการอินเทอร์เน็ตทราบเพื่อทำการปิดกั้นเว็บไซต์ดังกล่าวแล้ว แต่ผู้ให้บริการอินเทอร์เน็ตไม่ปฏิบัติตามที่เจ้าพนักงานตำรวจแจ้งก็อาจเป็นการเปิดโอกาสให้ผู้ใช้บริการอินเทอร์เน็ตกระทำความผิด ข้างต้นโดยใช้บริการของผู้ให้บริการอินเทอร์เน็ตกระทำความผิดนั้น ซึ่งอาจถือได้ว่าผู้ให้บริการอินเทอร์เน็ตให้ความช่วยเหลือหรือให้ความสะดวกแก่ผู้ใช้บริการอินเทอร์เน็ตในการกระทำความผิด อันเข้าข่ายเป็นผู้สนับสนุนให้มีการกระทำความผิดเกิดขึ้นตามมาตรา 86 [66] แห่งประมวลกฎหมายอาญา

ประเด็นที่2 ในกรณีที่เจ้าพนักงานตำรวจสั่งปิดเว็บไซต์ที่มีการเผยแพร่ภาพลามกอนาจารหรือมีการกระทำผิดกฎหมายอย่างอื่น จะต้องมีหมายศาลหรือไม่ อย่างไร นั้น เห็นว่า การสั่งปิดเว็บไซต์ที่มีการเผยแพร่ภาพลามกอนาจารหรือมีการกระทำผิดกฎหมายอย่างอื่นเป็นการกระทำที่กระทบกระเทือนต่อสิทธิเสรีภาพของบุคคล ต้องมีกฎหมายบัญญัติไว้อย่างชัดแจ้งเจ้าหน้าที่ของรัฐจึงจะมีอำนาจกระทำได้ ดังเช่นมาตรา 9[67] แห่งพระราชบัญญัติการพิมพ์พุทธศักราช 2484 ที่ให้อำนาจแก่เจ้าพนักงานการพิมพ์ที่จะมีคำสั่งเป็นหนังสือแก่ผู้หนึ่งผู้ใดโดยเฉพาะหรือมีคำสั่งทั่วไปโดยประกาศในราชกิจจานุเบกษาหรือหนังสือพิมพ์รายวันห้ามการขายหรือจ่ายแจกสิ่งพิมพ์นั้น ทั้งจะให้ยึดสิ่งพิมพ์และแม่พิมพ์นั้นด้วยก็ได้ เมื่อปรากฏว่าได้มีการโฆษณาหรือเตรียมการโฆษณาสิ่งพิมพ์ใดๆ ซึ่งเจ้าพนักงานการพิมพ์เห็นว่าอาจจะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน อย่างไรก็ตาม จากการตรวจสอบกฎหมายต่างๆ ไม่

---

[66] มาตรา 86 "ผู้ใดกระทำด้วยประการใดๆ อันเป็นการช่วยเหลือหรือให้ความสะดวกในการที่ผู้อื่นกระทำความผิดก่อนหรือขณะกระทำความผิด แม้ผู้กระทำความผิดจะมิได้รู้ถึงการช่วยเหลือหรือให้ความสะดวกนั้นก็ตาม ผู้นั้นเป็นผู้สนับสนุนการกระทำความผิด ..."

[67] มาตรา 9 "เมื่อปรากฏว่าได้มีการโฆษณาหรือเตรียมการโฆษณาสิ่งพิมพ์ใดๆ ซึ่งเจ้าพนักงานการพิมพ์เห็นว่าอาจจะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน เจ้าพนักงานการพิมพ์อาจมีคำสั่งเป็นหนังสือแก่ผู้หนึ่งผู้ใดโดยเฉพาะหรือมีคำสั่งทั่วไปโดยประกาศในราชกิจจานุเบกษาหรือหนังสือพิมพ์รายวันห้ามการขายหรือจ่ายแจกสิ่งพิมพ์นั้น ทั้งจะให้ยึดสิ่งพิมพ์และแม่พิมพ์นั้นด้วยก็ได้..."

พบว่ามีกฎหมายใดให้อำนาจแก่เจ้าพนักงานตำรวจที่จะสั่งปิดเว็บไซต์ที่มีการเผยแพร่ภาพลามกอนาจารหรือมีการกระทำผิดกฎหมายอย่างอื่น ดังนั้น เมื่อไม่มีกฎหมายใดให้อำนาจไว้ เจ้าพนักงานตำรวจจึงไม่อาจสั่งปิดเว็บไซต์นั้นเองหรือขอให้ศาลสั่งปิดได้

อนึ่ง แม้เจ้าพนักงานตำรวจไม่อาจสั่งปิดเว็บไซต์ดังกล่าวได้ แต่อาจแจ้งให้คณะกรรมการกิจการโทรคมนาคมแห่งชาติในฐานะผู้ควบคุมและผู้อนุญาตในการประกอบกิจการโทรคมนาคมดำเนินการเพิกถอนใบอนุญาตการให้บริการอินเทอร์เน็ตได้ตามมาตรา 15[68] แห่งพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 ประกอบกับข้อ 13[69] และข้อ 15[70] แห่งประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์และวิธีการขอรับใบอนุญาตการให้บริการอินเทอร์เน็ต ลงวันที่ 20 มิถุนายน 2548 ที่กำหนดให้คณะกรรมการกิจการโทรคมนาคมแห่งชาติมีอำนาจระงับ ยกเลิก หรือเพิกถอนใบอนุญาตการให้บริการอินเทอร์เน็ตได้ในกรณีมีความจำเป็นต้องปกป้องความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือในกรณีที่ผู้รับใบอนุญาตละเลยมาตรการเพื่อสังคมที่จะต้องพึงระมัดระวังมิให้ผู้ใช้บริการนำเครือข่ายอินเทอร์เน็ตไปใช้โดยมิชอบ หรือเผยแพร่ข้อมูลอันอาจทำลายความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

---

[68] มาตรา 15 "ในการประกอบกิจการโทรคมนาคม ผู้รับใบอนุญาตต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในกฎหมายว่าด้วยองค์กรจัดสรรคลื่นความถี่และกำกับกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม และตามเงื่อนไขที่คณะกรรมการกำหนด..."

[69] ข้อ 13 "การระงับ ยกเลิก หรือเพิกถอนใบอนุญาตการให้บริการอินเทอร์เน็ตคณะกรรมการอาจพิจารณาระงับ ยกเลิก หรือเพิกถอนใบอนุญาตการให้บริการอินเทอร์เน็ตได้ในกรณีดังต่อไปนี้ ...

13.3 กรณีที่มีความจำเป็นเพื่อประโยชน์ในการรักษาความมั่นคงของรัฐ รักษาผลประโยชน์ส่วนรวม หรือมีความจำเป็นที่ต้องปกป้องความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน

13.4 กรณีผู้รับใบอนุญาตทำผิดเงื่อนไขในใบอนุญาตไม่ว่าส่วนหนึ่งส่วนใดหรือทั้งหมด และไม่ทำการแก้ไขให้ถูกต้องภายในสามสิบวัน นับจากได้รับหนังสือแจ้งจากสำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ..."

[70] ข้อ 15 "มาตรการเพื่อสังคม ผู้รับใบอนุญาตการให้บริการอินเทอร์เน็ตพึงระมัดระวังมิให้ผู้ใช้บริการนำเครือข่ายอินเทอร์เน็ตไปใช้โดยมิชอบ หรือเผยแพร่ซึ่งข้อมูลอันอาจทำลายความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน..."

ประเด็นที่3 ในกรณีที่พนักงานสอบสวนใช้อำนาจตามมาตรา132 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ออกหมายเรียกเอกสารหรือพยานบุคคลที่เกี่ยวข้องเพื่อให้เข้าถึงข้อมูลทางโทรคมนาคมหรือข้อมูลทางอินเทอร์เน็ตนั้น พนักงานสอบสวนจะต้องมีหมายศาลหรือจะต้องร้องขอต่อศาลเพื่อมีคำสั่งอนุญาตก่อนดังเช่นพนักงานสอบสวนคดีพิเศษของกรมสอบสวนคดีพิเศษหรือไม่ อย่างไร นั้น ปรากฏจากคำชี้แจงของผู้แทนสำนักงานตำรวจแห่งชาติว่า ตามที่สำนักงานตำรวจแห่งชาติหารือมานี้เป็นเรื่องที่สำนักงานตำรวจแห่งชาติต้องการทราบข้อมูลจากบริษัทเอเชีย อินโฟเน็ต จำกัด เกี่ยวกับชื่อ ที่อยู่และหมายเลขโทรศัพท์ที่ใช้เชื่อมต่ออินเทอร์เน็ต ตลอดจนรายละเอียดการเชื่อมต่อที่ระบุระยะเวลา login และ logout ของผู้ใช้บริการอินเทอร์เน็ตซึ่งเปิดเว็บไซต์ที่เผยแพร่ภาพลามกอนาจารหรือมีการกระทำผิดกฎหมายอื่น เพื่อที่จะรู้ตัวผู้กระทำความผิดเท่านั้น มิได้ต้องการทราบรายละเอียดในข้อมูลส่วนบุคคลดังเช่นกรณีของการสอบสวนคดีพิเศษแต่อย่างใด คณะกรรมการกฤษฎีกา(คณะที่ 11)พิจารณาแล้วเห็นว่า ข้อมูลดังกล่าวมิใช่ข้อความในสิ่งสื่อสารที่บุคคลติดต่อกันซึ่งต้องห้ามตามมาตรา 37 วรรคสอง[71] ของรัฐธรรมนูญแห่งราชอาณาจักรไทย หรือเป็นข้อมูลข่าวสารอันเป็นรายละเอียดที่ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดตามที่พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 กำหนดไว้[72] ดังนั้น ถ้าปรากฏว่าข้อมูลที่พนักงานสอบสวนต้องการทราบปรากฏอยู่ในเอกสาร ก็อาจออกหมายเรียกบุคคลซึ่งครอบครองเอกสารให้จัดส่งเอกสารนั้นมาให้..."(ปัจจุบันเมื่อประกาศใช้พระราชบัญญัติว่าด้วยการการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550แล้ว ผู้เขียนเห็นว่าน่าจะไม่มีข้อโต้แย้งในลักษณะนี้)

---

[71] มาตรา 37 "การตรวจ การกัก หรือการเปิดเผยสิ่งสื่อสารที่บุคคลมีติดต่อถึงกัน รวมทั้งการกระทำด้วยประการอื่นใดเพื่อให้ล่วงรู้ถึงข้อความในสิ่งสื่อสารทั้งหลายที่บุคคลมีติดต่อถึงกัน จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อรักษาความมั่นคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน"

[72] มาตรา 25 "ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ พนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้..."

5. ปัญหาความพร้อมของภาครัฐในการบังคับใช้มาตรการกำกับดูแล

ด้วยข้อจำกัดต่างๆไม่ว่าจะเป็นด้านงบประมาณ กำลังคน และความรู้ความสามารถทางเทคโนโลยีของบุคคลากรและองค์กร เป็นปัญหาที่ทำให้การแก้ไขปัญหาต่างๆเกี่ยวกับการดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ตเป็นไปได้ยาก แม้ว่าจะมีการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550แล้ว ก็ไม่อาจแน่ใจได้ว่าจะสามารถควบคุมการกระทำความผิดบนอินเทอร์เน็ตได้

การมุ่งควบคุมสังคมโดยบัญญัติกฎหมายเป็นเครื่องมือโดยไม่พิจารณาถึงประสิทธิภาพและความสามารถของกลไกของรัฐที่จะใช้บังคับกฎหมายอาญาแล้วอาจเกิดภาวะกฎหมายอาญาเฟ้อ (Over criminalization) โดยประชาชนในรัฐอาจมองว่ากฎหมายไร้ความหมาย ไม่มีความศักดิ์สิทธิ์ และเป็นการเปิดโอกาสให้เจ้าพนักงานของรัฐประพฤติมิชอบมีโอกาสแสวงหาประโยชน์เพื่อตนเองจากกฎหมายได้ หรือ หากมีการบังคับใช้กฎหมายซึ่งมิได้มีการบังคับใช้เป็นเวลานาน ผู้ถูกใช้กฎหมายจะเกิดปฏิกิริยาเพราะถือว่าถูกเลือกปฏิบัติ ซึ่งจะทำให้ความสัมพันธ์ระหว่างผู้ใช้บังคับกฎหมายและชุมชนเสื่อมเสียไป[73]

---

[73] เกียรติขจร วัจนะสวัสดิ์, คำอธิบายกฎหมายอาญา ภาค1,พิมพ์ครั้งที่ 4(กรุงเทพ: หจก.จิรรัชการพิมพ์,2549), หน้า 7.