บทที่ 5

วิเคราะห์การดำเนินคดีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

จากการศึกษาเกี่ยวกับคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต ประเภทและรูปแบบลักษณะของอาชญากรรมคอมพิวเตอร์และการกระทำความผิดบนอินเทอร์เน็ตรวมถึงความเสียหายที่เกิดขึ้น แนวคิดและหลักการที่เกี่ยวข้องกับการดำเนินคดี กฎหมายสารบัญญัติของไทยและต่างประเทศ กระบวนการและขั้นตอนการดำเนินคดี ปัญหาในการดำเนินคดี หน่วยงานที่เกี่ยวข้องรวมถึงการดำเนินคดีกับผู้กระทำความผิดทั้งในประเทศและต่างประเทศดังที่ปรากฏในวิทยานิพนธ์ฉบับนี้ทั้งหมด ผู้เขียนได้วิเคราะห์พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในประเด็นต่างๆ ดังต่อไปนี้

5.1 <u>การบังคับใช้กฎหมาย</u>

(1.) เนื่องด้วยอาชญากรรมคอมพิวเตอร์มีหลากหลายรูปแบบ อีกทั้งยังมีการพัฒนารูปแบบการกระทำความผิดใหม่ๆอย่างรวดเร็ว จึงเป็นการยากเกินกว่าจะบัญญัติฐานความผิดตามกฎหมายให้ครอบคลุมอาชญากรรมคอมพิวเตอร์ได้ทั้งหมด แต่การดำเนินคดีและมาตรการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จำกัดเฉพาะการสืบสวนและสอบสวนการกระทำความผิดตามพระราชบัญญัตินี้เท่านั้น จึงไม่เอื้อต่อการนำไปใช้กับการกระทำความผิดอาญาตามกฎหมายอื่นซึ่งได้กระทำโดยใช้ระบบคอมพิวเตอร์หรือจัดเก็บข้อมูลไว้ในระบบคอมพิวเตอร์ เช่น ความผิดตามประมวลกฎหมายอาญา หรือ ความผิดตามพระราชบัญญัติการพนัน ความผิดตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน ความผิดตามพระราชบัญญัติทรัพย์สินทางปัญญา ซึ่งผู้กระทำความผิดได้ใช้ระบบคอมพิวเตอร์หรือจัดเก็บข้อมูลไว้ในระบบคอมพิวเตอร์ ทั้งที่การกระทำความผิดต่างๆเหล่านี้ก่อให้เกิดความเสียหายต่อสังคมอย่างกว้างขวางและร้ายแรง

ในประเทศสหรัฐอเมริกาได้แก้ปัญหานี้โดยปรับปรุงวิธีการดำเนินคดีอาญาทั่วไปให้ทันสมัยอยู่เสมอ และให้สามารถใช้ได้ครอบคลุมถึงอาชญากรรมคอมพิวเตอร์ด้วย ส่วนสหภาพยุโรปได้บัญญัติให้The Council of Europe Convention on Cybercrime ใช้ได้กับความผิดอาญา

อื่นๆที่ถูกกระทำโดยผ่านทางระบบคอมพิวเตอร์หรือจัดเก็บพยานหลักฐานในรูปแบบอิเล็กทรอนิกส์ และในประเทศสิงคโปร์ได้กำหนดให้อำนาจเจ้าพนักงานเข้าถึงและถอดรหัสข้อมูลคอมพิวเตอร์ได้ทั้งความผิดตามComputer Misuse Actและความผิดอาญาทั่วไปหากคอมพิวเตอร์เหล่านั้นถูกใช้หรือสงสัยว่าถูกใช้เกี่ยวกับ Seizable offence (ความผิดที่กฎหมายประเทศสิงคโปร์กำหนดให้จับได้โดยไม่ต้องมีหมาย)

(1.1) ควรนำหลักการที่ให้การดำเนินคดีและมาตรการต่างๆ สำหรับอาชญากรรมคอมพิวเตอร์สามารถใช้ได้กับความผิดอาญาอื่นที่ได้กระทำโดยใช้ระบบคอมพิวเตอร์ หรือจัดเก็บข้อมูลไว้ในระบบคอมพิวเตอร์ด้วย โดยควรเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 3/1 ดังนี้

" มาตรา 3/1 พระราชบัญญัตินี้ ให้ใช้กับ

(1.) การกระทำความผิดทางอาญาใดๆ ที่ใช้ระบบคอมพิวเตอร์ หรือ

(2.) การรวบรวมข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ที่เป็นพยานหลักฐานหรืออาจใช้เป็นหลักฐานในการพิสูจน์กระทำความผิดอาญาใดๆ ที่จัดเก็บไว้ในระบบคอมพิวเตอร์"

(1.2) หรือควรเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ให้ครอบคลุมถึงการกระทำความผิดอาญาเฉพาะฐานความผิดที่มีโทษร้ายแรงหรือกระทบต่อความสงบเรียบร้อยของประชาชน โดยเพิ่มเติม มาตรา 3/1 ดังนี้

"มาตรา 3/1 พระราชบัญญัตินี้ ให้ใช้กับ

(1.) การกระทำความผิดอาญาใดๆที่มีโทษถึงขั้นประหารชีวิตหรือจำคุกตลอดชีวิต หรือ

(2.) ความผิดที่ระบุไว้ท้ายพระราชบัญญัติฉบับนี้"

(ความผิดที่ควรระบุไว้ท้ายพระราชบัญญัติ เช่น ความผิดตามประมวลกฎหมายอาญาฐานฉ้อโกงประชาชน ความผิดฐานก่อการร้าย หรือ ความผิดอาญาตามกฎหมายอื่น เช่น ความผิดตามพระราชบัญญัติการพนัน ความผิดตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน ความผิดตามพระราชบัญญัติทรัพย์สินทางปัญญา เป็นต้น)

(2.) เมื่อพิจารณากฎหมายที่เกี่ยวข้องกับการดำเนินคดีทั้งในประเทศและต่างประเทศพบว่า มีความยากลำบากในการพิจารณาว่าการกระทำใดอยู่ในขั้นตอนลงมือกระทำความผิดหรือขั้นตอนตระเตรียม ยกตัวอย่างเช่น เจ้าหน้าที่ตรวจสอบพบว่าผู้กระทำความผิดได้ทำการเจาะระบบเพื่อทำลายคอมพิวเตอร์ที่ควบคุมระบบการจ่ายไฟฟ้าของประเทศ แต่ระหว่างกระทำผิดบังเอิญได้ไปกระตุ้นระบบรักษาความปลอดภัยของคอมพิวเตอร์ให้ทำงานเสียก่อนจึงกระทำผิดไม่สำเร็จ ในกรณีนี้เป็นการยากที่จะระบุว่าขั้นตอนใดเป็นขั้นตอนสุดท้าย(Last act) ที่ใกล้ชิดผลอันจะถือว่าเป็นขั้นลงมือกระทำความผิด

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550ได้นำหลักทั่วไปตามประมวลกฎหมายอาญามาใช้ กล่าวคือ จะลงโทษผู้กระทำได้ต่อเมื่อการกระทำนั้นพ้นขั้นตระเตรียมเข้าสู่ขั้นลงมือกระทำความผิดแล้ว ซึ่งหากพิจารณาตามหลักเกณฑ์นี้อาจไม่สามารถลงโทษผู้กระทำความผิดตามตัวอย่างข้างต้นได้ ทั้งที่หากผู้กระทำได้กระทำความผิดไปจนสำเร็จย่อมส่งผลเสียหายร้ายแรงต่อประชาชนในวงกว้าง (เช่น การกระทำความผิดตามมาตรา 12(2) ซึ่งเป็นการกระทำต่อความมั่นคงปลอดภัยของชาติ และสาธารณูปโภคของรัฐ)

ในประเทศสิงคโปร์ได้ให้ความสำคัญกับการบัญญัติฐานความผิดที่มีโทษร้ายแรงซึ่งได้กระทำโดยใช้คอมพิวเตอร์ให้ต้องรับโทษเช่นเดียวกับการกระทำความผิดสำเร็จแม้อยู่ในขั้นตอนตระเตรียมการ(Article 125B(4)) เช่น หากเจ้าหน้าที่พบพยานหลักฐานโดยการถอดรหัสข้อมูลแสดงให้เห็นว่าผู้กระทำได้วางแผนตระเตรียมในการกระทำความผิดอุกฉกรรจ์(Specified serious offence) ผู้นั้นย่อมได้รับโทษเช่นเดียวกับการกระทำผิดสำเร็จ

ดังนั้น เพื่อให้การควบคุมอาชญากรรมคอมพิวเตอร์มีประสิทธิภาพยิ่งขึ้นจึงควรบัญญัติให้การตระเตรียมกระทำผิดบางฐานที่ร้ายแรงเป็นความผิดในตัวเอง โดยควรเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.255 มาตรา 12 วรรคสาม ดังนี้

"มาตรา 12 วรรคสาม ผู้ใดตระเตรียมการเพื่อกระทำความผิดตามมาตรา 12 (2) ต้องระวางโทษเช่นเดียวกับการพยายามกระทำความผิดฐานนั้น"

5.2 <u>การค้นโดยมีหมาย</u>

(1.) จากการศึกษาแนวคิดที่เกี่ยวข้องกับการดำเนินคดีพบว่า การดำเนินคดีจำเป็นต้องคำนึงถึงการใช้อำนาจของเจ้าหน้าที่รัฐอย่างมีประสิทธิภาพและคำนึงถึงการคุ้มครองสิทธิของประชาชนควบคู่กันไป แต่เมื่อพิจารณาตามพระราชบัญญัติว่าด้วยการกระทำความผิด

เกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 พบว่าการแต่งตั้งพนักงานพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ได้กำหนดคุณสมบัติพนักงานเจ้าหน้าที่ไว้ 2 ประเภท คือ 1. ผู้มีความรู้ความเชี่ยวชาญเกี่ยวกับคอมพิวเตอร์ 2. ผู้ไม่มีความรู้ความเชี่ยวชาญเกี่ยวกับคอมพิวเตอร์แต่มีคุณสมบัติอื่น เช่น มีความรู้ด้านกฎหมาย หรือเป็นผู้ใดก็ได้ที่รัฐมนตรีแต่งตั้ง (ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550ข้อ2และข้อ3) การกำหนดคุณสมบัติในลักษณะนี้อาจทำให้การดำเนินคดีไม่มีประสิทธิภาพหรืออาจล่วงละเมิดสิทธิผู้ต้องหาได้ กล่าวคือ ในกรณีที่พนักงานเจ้าหน้าที่ทำการค้นโดยลำพัง พนักงานเจ้าหน้าที่ที่ได้รับการแต่งตั้งโดยอาศัยคุณสมบัติอื่นอาจไม่มีความรู้ความและความชำนาญในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์อย่างแท้จริง หรือ หากเป็นพนักงานเจ้าหน้าที่ที่มีความเชี่ยวชาญทางคอมพิวเตอร์แต่ไม่มีความเข้าใจในด้านกฎหมายอย่างดีพอก็อาจกระทำการล่วงละเมิดสิทธิของผู้ต้องหาได้

ในประเทศสหรัฐอเมริกาได้กำหนดให้การค้นต้องดำเนินการเป็นกลุ่มคณะ ซึ่งในคณะจะต้องประกอบด้วยเจ้าหน้าที่ในคดี พนักงานอัยการและผู้ชำนาญทางเทคนิค โดยเจ้าหน้าที่จะเป็นผู้ประสานงานในขอหมายศาล พนักงานอัยการมีหน้าที่ตรวจสอบการค้นว่าชอบด้วยกฎหมายและชอบด้วยรัฐธรรมนูญหรือไม่ ส่วนผู้เชี่ยวชาญทางเทคนิคจะเป็นผู้วางแผนและรับผิดชอบด้านการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ โดยในการดำเนินการค้นทุกฝ่ายจะต้องให้ความร่วมมือซึ่งกันและกัน

ดังนั้น เพื่อให้การดำเนินคดีเป็นไปอย่างมีประสิทธิภาพและเพื่อคุ้มครองสิทธิของประชาชนควบคู่กันไป หน่วยงานที่รับผิดชอบคือกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงควรที่จะกำหนดระเบียบเกี่ยวกับการค้น โดยกำหนดให้การค้นจะต้องเป็นดำเนินการร่วมกันระหว่างผู้เชี่ยวชาญเกี่ยวกับคอมพิวเตอร์และผู้มีความรู้ด้านกฎหมาย

(2.) จากการศึกษาปัญหาในการยึดและค้นพบว่า ในกรณีที่ผู้กระทำความผิดจัดเก็บข้อมูลสำคัญไว้ยังสถานที่อื่น อาจสร้างปัญหาในการดำเนินการตามหมายค้น เช่น เมื่อเจ้าหน้าที่เข้าตรวจค้นสถานที่ที่ผู้กระทำความผิดอาศัยอยู่ กลับพบว่าผู้กระทำความผิดได้ส่งข้อมูลที่เป็นพยานหลักฐานไปจัดเก็บไว้ยังสถานที่อื่นที่ไกลออกไป และเมื่อพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และประมวลกฎหมายวิธีพิจารณาความอาญาจะเห็นได้ว่า ในกรณีนี้เจ้าหน้าที่ไม่สามารถทำการค้นยังสถานที่อื่นนอกเหนือจากที่ระบุไว้ใน

หมายค้นได้และหากเจ้าหน้าที่ต้องขอออกหมายค้นฉบับใหม่ก็อาจไม่ทันการณ์เพราะพยานหลักฐานอาจถูกทำลายเสียก่อน

ในประเทศสหรัฐอเมริกาแก้ปัญหานี้โดยอนุญาตให้เจ้าหน้าที่สามารถขอออกหมายค้นได้หลายฉบับ(Multiple warrants) หรืออนุญาตให้ค้นต่อเนื่องไปยังสถานที่อื่นได้หากพบว่ามีสถานที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานในหลายท้องที่ ส่วนสหภาพยุโรปมีบทบัญญัติให้เจ้าหน้าที่สามารถขยายผลการค้นเพื่อทำการค้นอีกสถานที่หนึ่งได้อย่างต่อเนื่อง (Article 9(2)) โดยไม่ต้องขอหมายฉบับใหม่

เพื่อเป็นการแก้ปัญหาในลักษณะนี้จึงควรศึกษาแนวทางการแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550และประมวลกฎหมายวิธีพิจารณาความอาญาเพื่อให้พนักงานเจ้าหน้าที่สามารถทำการค้นได้อย่างต่อเนื่อง เช่น กรณีที่ตรวจสอบข้อมูลคอมพิวเตอร์ที่พบในสถานที่ที่ทำการค้นตามหมายแล้วพบหลักฐานโดยชัดเจนว่าผู้เสียหายได้เก็บข้อมูลที่เป็นหลักฐานสำคัญไว้ ณ สถานที่อื่น พนักงานเจ้าหน้าที่มีอำนาจทำการค้นยังสถานที่อื่นที่ผู้กระทำความผิดจัดเก็บข้อมูลเหล่านั้นไว้โดยไม่ต้องขอหมายค้นฉบับใหม่ เพื่อความรวดเร็วและป้องกันการสูญหายหรือทำลายพยานหลักฐาน

(3.) ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550กำหนดให้การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18(4)-(8) ต้องขออนุญาตจากศาลก่อนดำเนินการ อาจทำให้เกิดปัญหาความล่าช้าในการรวบรวมพยานหลักฐานซึ่งขัดกับเจตนารมณ์ของกฎหมายที่ประสงค์ให้เจ้าหน้าที่ของรัฐสามารถรวบรวมพยานหลักฐานได้อย่างรวดเร็วเพื่อป้องกันการสูญหายหรือการทำลายพยานหลักฐาน

เมื่อพิจารณาประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 59 วรรคสามได้กำหนดให้เจ้าหน้าที่ตำรวจขอหมายได้โดยการใช้โทรศัพท์ โทรสาร สื่ออิเล็กทรอนิกส์หรือสื่อเทคโนโลยีสารสนเทศประเภทอื่นได้ในกรณีจำเป็นเร่งด่วน แต่หลักการนี้ใช้กับการขอหมายจับหรือหมายค้นเท่านั้น

ในประเด็นนี้จึงควรแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา19 โดยเพิ่มเติมหลักการเกี่ยวกับการขออนุญาตศาลในกรณีจำเป็นเร่งด่วน เช่น ในกรณีจำเป็นเร่งด่วน ให้พนักงานเจ้าหน้าที่สามารถขออนุญาตศาลผ่านทาง

โทรศัพท์ โทรสาร สื่ออิเล็กทรอนิกส์หรือสื่อเทคโนโลยีสารสนเทศประเภทอื่นได้ในกรณีที่มีเหตุจำเป็นเร่งด่วน เพื่อพนักงานเจ้าหน้าที่จะได้สามารถรวบรวมพยานหลักฐานได้อย่างรวดเร็ว เช่นเดียวกับประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 59 วรรคสาม ดังนี้

" มาตรา 19/1 ในกรณีจำเป็นเร่งด่วน ให้พนักงานเจ้าหน้าที่สามารถขออนุญาตศาลผ่านทางโทรศัพท์ โทรสาร สื่ออิเล็กทรอนิกส์หรือสื่อเทคโนโลยีสารสนเทศประเภทอื่นก็ได้ และเมื่อศาลมีคำสั่งอนุญาตแล้วให้ส่งสำเนาคำสั่งอนุญาตดังกล่าวให้กับพนักงานเจ้าหน้าที่ผู้ขออนุญาต ทั้งนี้ตามหลักเกณฑ์และวิธีการที่ประธานศาลฎีกากำหนด"

5.3 **<u>การค้นโดยไม่ต้องมีหมาย</u>**

ปัญหาสำคัญในการรวบรวมพยานหลักฐาน คือ พยานหลักฐานอิเล็กทรอนิกส์อาจถูกแก้ไข เปลี่ยนแปลงหรือสูญหายหรือโยกย้ายหรือถูกทำลายได้โดยง่าย ยกตัวอย่างเช่น เมื่อมีการกระทำความผิดหมิ่นประมาทบนอินเทอร์เน็ตผู้กระทำความผิดอาจเข้าไปแก้ไขข้อความหรือลบข้อความ หรือHard disk ที่บรรจุข้อมูลอาจถูกทำลาย แต่เมื่อพิจารณาตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 การเข้ายึดหรืออายัดหรือทำสำเนาข้อมูลของพนักงานเจ้าหน้าที่ ต้องดำเนินการขออนุญาตศาลก่อน(มาตรา19)และอาจจะต้องขอออกหมายจับและหมายค้นด้วย ทำให้การดำเนินคดีประสบปัญหาจากความเนิ่นช้า ซึ่งอาจทำให้สูญเสียพยานหลักฐานจนไม่สามารถดำเนินคดีกับผู้กระทำความผิดได้

ในประเทศสหรัฐอเมริกาถือว่าในคดีที่เกี่ยวกับคอมพิวเตอร์ถือเป็นสถานการณ์ฉุกเฉิน(Exigent Circumstances) ซึ่งเจ้าหน้าที่สามารถค้น ยึด และทำสำเนาข้อมูลได้ หากพบว่าพยานหลักฐานเหล่านั้นมีความเสี่ยงสูงและอยู่ในสภาพที่พร้อมจะถูกทำลาย (เช่น ผู้ต้องสงสัยทราบว่าเจ้าหน้าที่กำลังติดตามตัวอยู่ และผู้ต้องสงสัยเป็นผู้ครอบครองข้อมูลและอุปกรณ์คอมพิวเตอร์เหล่านั้น ในกรณีนี้ผู้ต้องสงสัยอาจทำลายหลักฐานได้โดยง่าย) ในประเทศสิงคโปร์ได้ให้อำนาจเจ้าหน้าที่เข้าถึงและถอดรหัสข้อมูลได้ทุกเวลา(May at any time) หากตรวจสอบพบการกระทำความผิดที่ใช้หรือสงสัยว่าได้ใช้คอมพิวเตอร์เกี่ยวกับ Seizable offence(Criminal Procedure Article 125Aและ125)และถือว่าการกระทำผิดตาม Computer Misuse Act สามารถจับกุมได้โดยไม่ต้องมีหมาย(Article 16) และในสหภาพยุโรปให้อำนาจเจ้าหน้าที่รวบรวมพยานหลักฐานได้เองโดยรวดเร็ว(Article 16,17) เช่นให้อำนาจเรียกข้อมูลจากผู้ครอบครองได้โดยไม่ต้องขอศาล

ฉะนั้น จึงควรจะศึกษาหาแนวทางให้อำนาจพนักงานเจ้าหน้าที่สามารถดำเนินการตามมาตรา 18(4)-(8) ได้โดยไม่ต้องขออนุญาตจากศาลก่อนในกรณีฉุกเฉิน และควรศึกษาหาแนวทางบัญญัติความผิดตามพระราชบัญญัติฉบับนี้ไว้ท้ายประมวลกฎหมายวิธีพิจารณาความอาญาเพื่อให้พนักงานเจ้าหน้าที่สามารถจับกุมได้ในกรณีพบการกระทำความผิดซึ่งหน้าและสามารถค้นได้โดยไม่ต้องมีหมาย ในกรณีที่มีสถานการณ์ฉุกเฉินดังที่ได้กล่าวมาข้างต้น

5.4 การยึดและอายัด

การรวบรวมพยานหลักฐานอิเล็กทรอนิกส์อาจเกิดข้อโต้แย้งเกี่ยวกับการจัดเก็บพยานหลักฐานได้เสมอ เช่น ข้อโต้แย้งว่าการจัดเก็บไม่ถูกต้อง ไม่เป็นไปตามหลักวิชาการ ข้อมูลถูกเพิ่มเติมเปลี่ยนแปลงแก้ไข อุปกรณ์ถูกสับเปลี่ยน อุปกรณ์ได้รับความกระทบกระเทือนหรือผ่านสนามแม่เหล็กจนข้อมูลเสียหาย แต่เมื่อพิจารณาตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550และประกาศที่เกี่ยวข้องพบว่ายังไม่มีการออกระเบียบเกี่ยวกับการยึดและอายัดระบบคอมพิวเตอร์ไว้

ดังนั้นกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารซึ่งเป็นหน่วยงานที่รับผิดชอบในเรื่องนี้ ควรออกระเบียบเกี่ยวกับการยึดและอายัดระบบคอมพิวเตอร์ให้ชัดเจนและรัดกุม โดยพิจารณาประเด็นสำคัญต่างๆ ดังนี้

- ควรกำหนดให้พนักงานเจ้าหน้าที่จัดทำบันทึกรายละเอียดเกี่ยวกับคอมพิวเตอร์ เช่น หมายเลขเครื่อง รุ่น ยี่ห้อ จดบันทึกหมายเลขHard diskหรือหมายเลขServer และหมายเลขอุปกรณ์ต่างๆ ให้ชัดเจนเพื่อป้องกันการถูกสับเปลี่ยนหรือสูญหาย

- ควรกำหนดให้พนักงานเจ้าหน้าที่ต้องบรรจุอุปกรณ์คอมพิวเตอร์ด้วยอุปกรณ์ที่ปลอดภัยมิดชิด และวิธีการที่เหมาะสมเพื่อป้องกันการถูกแก้ไขเพิ่มเติมข้อมูลหรือถูกสัญญาณแม่เหล็กรบกวนทำให้ข้อมูลเสียหาย

- ควรกำหนดให้การยึดและอายัดต้องทำต่อหน้าพยานผู้รู้เห็น โดยกำหนดให้พยานต้องลงลายมือชื่อไว้ด้วย

- ควรกำหนดความรับผิดในกรณีอุปกรณ์คอมพิวเตอร์ชำรุดหรือสูญหายในขณะอยู่ในความครอบครองของพนักงานเจ้าหน้าที่หรือเก็บรักษาโดยหน่วยงานรัฐ เช่น กำหนดให้ต้องชดใช้ค่าเสียหายตามสมควร

5.5 <u>การดำเนินการของพนักงานเจ้าหน้าที่</u>

เนื่องจากการดำเนินคดีอาจมีความจำเป็นต้องยึดหรืออายัดระบบคอมพิวเตอร์ทั้งระบบแทนการทำสำเนาข้อมูล เช่น กรณีที่ข้อมูลถูกเก็บไว้หลายส่วนอาจจำเป็นต้องยึดหรืออายัดระบบคอมพิวเตอร์ทั้งระบบ ซึ่งส่งผลต่อธุรกิจของผู้ให้บริการทำให้ไม่สามารถดำเนินกิจการต่อไปได้ หรือกระทบต่อการใช้งานตามปกติของผู้ใช้บริการรายอื่นหรืออาจล่วงรู้ความลับของผู้ใช้บริการรายอื่นที่มิได้รู้เห็นในการกระทำความผิด เมื่อพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550แล้ว พบว่าตัวบทกฎหมายเปิดช่องให้พนักงานเจ้าหน้าที่สามารถยึดหรืออายัดเครือข่ายคอมพิวเตอร์ได้ทั้งระบบ อาจเกิดปัญหาในกรณีที่พนักงานเจ้าหน้าที่ใช้ดุลยพินิจเกินสมควร

สหรัฐอเมริกาได้ป้องกันปัญหานี้ด้วยการบัญญัติกฎหมาย Electronic Communication Privacy Act (ECPA) ที่กำหนดให้เจ้าหน้าที่หลีกเลี่ยงที่จะยึดหรืออายัดคอมพิวเตอร์ทั้งระบบเว้นแต่ไม่มีทางเลือกอื่น(เช่น ผู้ให้บริการเป็นผู้กระทำความผิดเอง)และต้องหลีกเลี่ยงไม่เข้าไปค้นข้อมูลของผู้ใช้รายอื่นที่ไม่เกี่ยวข้องกับการกระทำความผิดและต้องรักษาข้อมูลที่ได้จากการตรวจสอบไว้เป็นความลับ ผลของการฝ่าฝืนอาจทำให้เจ้าหน้าที่ถูกเอกชนฟ้องร้องได้

ดังนั้น จึงควรกำหนดขอบเขตการใช้อำนาจของพนักงานเจ้าหน้าที่ไว้เพื่อมิให้พนักงานเจ้าหน้าที่ใช้อำนาจยึดหรืออายัดคอมพิวเตอร์ทั้งระบบโดยไม่มีเหตุผลสมควร โดยควรเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ดังนี้

" มาตรา19 วรรคเจ็ด การยึดหรืออายัดตามมาตรา 18(8) ในกรณีที่ระบบคอมพิวเตอร์นั้นเป็นเครือข่ายคอมพิวเตอร์พนักงานเจ้าหน้าที่จะต้องหลีกเลี่ยงที่จะยึดหรืออายัดเครือข่ายคอมพิวเตอร์ทั้งระบบ เว้นแต่ มีเหตุจำเป็นอย่างยิ่ง และต้องหลีกเลี่ยงในการตรวจสอบข้อมูลของผู้ใช้รายอื่นที่ไม่เกี่ยวข้องกับการกระทำความผิดและจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการอื่นไว้เป็นความลับ"

"มาตรา19 วรรคแปด การกระทำอันฝ่าฝืนมาตรา19วรรคเจ็ด ให้นำมาตรา22 มาตรา23และมาตรา24 มาใช้โดยอนุโลม"

5.6 การควบคุมทางอิเล็กทรอนิกส์ในเครือข่ายสื่อสาร

จากการศึกษาการดำเนินคดีและมาตรการของต่างประเทศพบว่า มีความจำเป็นที่จะต้องใช้มาตรการเฝ้าระวังหรือสอดแนมการกระทำความผิด โดยเจ้าหน้าที่จะใช้วิธีการติดตั้งเครื่องมือสอดแนมและเจ้าหน้าที่จะใช้ระยะเวลาพอสมควรในการบันทึกร่องรอยการกระทำความผิดเพื่อสืบหาตัวคนร้าย สำหรับประเทศไทย ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ไม่ได้กำหนดมาตรการต่างๆเหล่านั้นไว้ อาจทำให้การสืบทราบการกระทำความผิดและการระบุตัวผู้กระทำความผิดทำได้ยากลำบาก

ในประเทศสหรัฐอเมริกาได้ใช้มาตรการควบคุมตามบทบัญญัติPen/Trap statute และWiretap statute ส่วนสหภาพยุโรปได้ใช้มาตรการReal time collection of traffic data และมาตรการ Intercept of content data ซึ่งมาตรการทั้งหลายเหล่านี้ มีวัตถุประสงค์ในการรวบรวมข้อมูลประเภทเนื้อหา(Content)และข้อมูลที่มิใช่เนื้อหา(Non-content) เพื่อเป็นการเฝ้าระวังการกระทำความผิดและเพื่อให้การสืบสวนสอบสวนมีประสิทธิภาพ

การนำมาตรการเฝ้าระวังและสอดแนมมาใช้จะช่วยให้เจ้าหน้าที่สามารถระบุตัวผู้กระทำความผิดได้อย่างมีประสิทธิภาพ ในอนาคตจึงควรนำมาตรการเหล่านี้มาใช้โดยควรพิจารณาในประเด็นต่างๆ ดังนี้

(1.) ศึกษาถึงแนวทางการกำหนดให้หน่วยงานและพนักงานเจ้าหน้าที่มีอำนาจรวบรวมหรือทำการบันทึกข้อมูลจราจรทางคอมพิวเตอร์แบบ Real-time (Real time collection of traffic data) โดยรวบรวมข้อมูลจราจรทางคอมพิวเตอร์(Traffic data)และข้อมูลที่ไม่ใช่เนื้อหา (Non-Content) และอาจกำหนดผู้ให้บริการมีหน้าที่รวบรวมหรือทำบันทึกข้อมูลจราจรทางคอมพิวเตอร์แบบReal-timeหรือให้ความร่วมมือและช่วยเหลือเจ้าหน้าที่ในการดำเนินการข้างต้น

(2.) ศึกษาถึงแนวทางการกำหนดให้หน่วยงานและพนักงานเจ้าหน้าที่มีอำนาจดักการสื่อสารของเนื้อหาข้อมูล(Interception of content data) โดยดักข้อมูลในลักษณะเนื้อหา

(Content) และอาจกำหนดให้ผู้ให้บริการมีหน้าที่รวบรวมหรือทำบันทึกเกี่ยวกับข้อมูลเนื้อหา (Content data) ในแบบ Real-timeหรือให้ความร่วมมือและช่วยเหลือเจ้าหน้าที่ในการดำเนินการข้างต้น แต่การใช้อำนาจดักเนื้อหา(Content data) จำเป็นต้องคำนึงถึงหลักเกณฑ์ที่ป้องกันการใช้อำนาจโดยมิชอบด้วย เช่น

(2.1) ควรกำหนดให้พนักงานเจ้าหน้าที่ต้องขออนุญาตจากศาลก่อนดำเนินการดักเนื้อหาข้อมูล และจะต้องแสดงเหตุอันสมควรว่ามีความจำเป็นหรือเหตุขัดข้องที่ทำให้ไม่สามารถแสวงหาพยานหลักฐานด้วยวิธีการอื่นอย่างไร

(2.2) ควรกำหนดให้พนักงานเจ้าหน้าที่ต้องรักษาข้อมูลดังกล่าวเป็นความลับ โดยจะเปิดเผยหรือส่งมอบข้อมูลแก่บุคคลใดมิได้ เว้นแต่จะได้รับอนุญาตจากศาล

(3.) ควรกำหนดให้คำสั่งศาลจะต้องระบุรายละเอียดในคำสั่งชัดเจนว่าให้ระยะเวลาในการดำเนินการเท่าใด เริ่มต้นและสิ้นสุดเมื่อใด เมื่อได้รับอนุญาตจากศาลแล้วให้พนักงานเจ้าหน้าที่ส่งคำสั่งศาลนั้นแก่ผู้ให้บริการเพื่อดำเนินการตามคำสั่งศาลต่อไป

หากผู้ให้บริการไม่สามารถกระทำการตามคำสั่งศาลหรือไม่ยอมปฏิบัติตามคำสั่งให้อำนาจพนักเจ้าหน้าที่เป็นผู้ดำเนินการได้เอง โดยร้องขอต่อศาล ซึ่งเนื้อหาของคำร้องควรจะต้องระบุถึง

-ชื่อและตำแหน่งของเจ้าหน้าที่ซึ่งทำการติดตั้ง และเครื่องมือที่ใช้

- วัน และเวลาที่เครื่องมือนั้นได้มีการติดตั้ง และนำออก

- จำนวนและชนิดเครื่องมือทั้งหมดที่ติดตั้ง

- ข้อมูลที่ต้องการได้จากเครื่องมือนั้น

เมื่อดำเนินการดังกล่าวเสร็จสิ้นแล้ว จะต้องรายงานต่อศาลถึงข้อมูลที่ได้จากการดำเนินการ เพื่อให้ศาลตรวจสอบว่าได้ใช้อำนาจโดยมิชอบหรือฝ่าฝืนกฎหมายหรือไม่

ในกรณีที่ผู้ให้บริการให้ความช่วยเหลือพนักงานเจ้าหน้าที่หรือเป็นผู้ดำเนินการเอง อาจจะกำหนดให้ผู้บริการมีสิทธิได้รับค่าใช้จ่ายในการดำเนินการตามสมควร (Reasonable expenses) และควรจะต้องมีบทบัญญัติคุ้มครองผู้ให้บริการที่กระทำการโดยสุจริตตามคำสั่งศาล

(4.) ศึกษาถึงแนวทางการกำหนดความรับผิดของพนักงานเจ้าหน้าที่ทั้งทางอาญาและทางแพ่ง รวมทั้งผลต่อการรับฟังพยานหลักฐานที่ฝ่าฝืนกฎหมาย เช่น หากพนักงานเจ้าหน้าที่ไม่ดำเนินการตามขั้นตอนให้ถูกต้องหรือเปิดเผยข้อมูลที่ได้จากการดำเนินการ จะต้องรับผิดชอบต่อผู้ได้รับความเสียหายและให้ศาลปฏิเสธที่จะรับฟังพยานหลักฐานอันมิชอบเหล่านั้น เป็นต้น

5.7 <u>การป้องกันหรือการตอบโต้ภัยคุกคามต่อความมั่นคงของชาติ</u>

อาชญากรรมคอมพิวเตอร์สามารถสร้างความเสียหายต่อสังคม เศรษฐกิจ ความมั่นคงของชาติและสาธารณูปโภคของรัฐได้อย่างรุนแรงและรวดเร็ว ซึ่งอาจส่งผลผลกระทบต่อประชาชนจำนวนมาก เช่น ทำให้ระบบการเงิน การธนาคาร บริการสาธารณะ ขนส่งสาธารณะหรือโครงสร้างพื้นฐานสาธารณะสำคัญ ระบบคอมพิวเตอร์ของตำรวจ ทหาร หรือบริการทางการแพทย์ได้รับความเสียหาย จึงมีความจำเป็นที่จะต้องใช้มาตรการป้องกันก่อนความเสียหายเหล่านั้นจะเกิด(Preemptive) เมื่อพิจารณาตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 พบว่ายังไม่มีมาตรการในลักษณะดังกล่าว

ในประเทศสิงคโปร์ ได้กำหนดให้มีการใช้มาตรการป้องกันหรือการตอบโต้ภัยคุกคามต่อความมั่นคงของชาติไว้โดยให้อำนาจเจ้าหน้าที่และหน่วยงานที่เกี่ยวข้องในการใช้มาตรการป้องกันก่อนความเสียหายจะเกิด(Preemptive) ซึ่งได้ให้อำนาจเจ้าหน้าที่จัดการปัญหาได้อย่างรวดเร็วตามดุลยพินิจโดยไม่ต้องมีหมายศาล เช่น หากจับสัญญาณได้ว่ามีการจู่โจมระบบคอมพิวเตอร์ของสถานที่สำคัญ เช่น โรงงานผลิตไฟฟ้า ให้อำนาจเจ้าหน้าที่เข้าถึงและถอดรหัสหรือดำเนินการอื่นใดเท่าที่จำเป็นได้ทันที

จะเห็นได้ว่ามาตรการป้องกันหรือการตอบโต้ภัยคุกคามต่อความมั่นคงของชาติเป็นมาตรการที่มีประโยชน์มากในการคุ้มครองประชาชนและรัฐก่อนความเสียหายจะเกิดขึ้น จึงควรศึกษาหาแนวทางในการนำมาตรการดังกล่าวมาใช้ โดยพิจารณาในประเด็นต่างๆ ดังนี้

(1.) ศึกษาถึงความเป็นไปได้ในการใช้มาตรการป้องกันหรือการตอบโต้ภัยคุกคามต่อความมั่นคงของชาติ ก่อนที่ความเสียหายจะเกิดขึ้น เช่น กรณีที่เจ้าหน้าที่มีพยานหลักฐานอันควรเชื่อได้ว่าอาจมีการกระทำความผิด ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มาตรา 12 (2) หน่วยงานหรือเจ้าหน้าที่รัฐมีอำนาจป้องกันหรือตอบโต้การกระทำผิดนั้นได้อย่างรวดเร็ว เช่น ให้อำนาจพนักงานเจ้าหน้าที่สามารถดำเนินการใดๆเพื่อระงับ ทำลายหรือแก้ไขปัญหาได้ทันทีโดยไม่ต้องขออนุญาตจากศาล แต่มาตรการที่จะนำมาใช้จำเป็นต้องมีหลักเกณฑ์ควบคุมเป็นพิเศษเพื่อป้องกันการกระทบสิทธิเสรีภาพของประชาชน เช่น

- มาตรการดังกล่าวจะใช้ได้เพื่อวัตถุประสงค์ในการป้องกันความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะหรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ เท่านั้น

- พยานหลักฐานใดๆ ที่ได้รับจากการใช้มาตรการนี้ จะรับฟังเพื่อพิสูจน์ความผิดของบุคคลไม่ได้

- ผู้ให้ข้อมูลหรือเบาะแส กับเจ้าหน้าที่จะต้องถูกปกปิดข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่ หรือข้อมูลอื่นใดที่ทำให้ทราบตัวบุคคลนั้น

(2.) เจ้าหน้าที่ที่จะใช้อำนาจในลักษณะนี้ต้องเป็นผู้เชี่ยวชาญที่ได้รับการแต่งตั้งเป็นพิเศษ เช่นได้รับการแต่งตั้งจากรัฐมนตรี

5.8 . <u>การระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์</u>

(1.) จากการศึกษาพบว่า ประกาศคณะปฏิรูปการปกครองในระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข ที่5/2549 ได้ให้อำนาจกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร(ICT) อย่างกว้างขวางมาก ทำให้ICT มีอำนาจปิดกั้นการสื่อสารได้แทบทุกชนิด ส่งผลให้ICT ถูกใช้เป็นเครื่องมือของผู้มีอำนาจเพื่อใช้ปิดกั้นเว็บไซต์การเมือง ซึ่งการใช้อำนาจลักษณะนี้ย่อมกระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชนเกินสมควร นอกจากนี้ อำนาจดังกล่าวยังทับซ้อนกับการใช้อำนาจของศาลตามพระราชบัญญัติว่าด้วยการ

กระทำความผิดเกี่ยวกับคอมพิวเตอร์ มาตรา20 อีกด้วยดังนั้น จึงว่าสมควรพิจารณายกเลิกประกาศฉบับนี้

(2.) จากการศึกษาพบว่าการใช้อำนาจในการปิดกั้นเว็บไซต์ของICTไม่มีขั้นตอนและหลักเกณฑ์ที่แน่นอนและไม่มีขอบเขตการใช้อำนาจ เช่น ปัญหากรณีการปิดกั้นเว็บไซต์ Youtube.comทั้งเว็บไซต์ ทั้งที่มีข้อมูลที่เป็นปัญหาเพียงเล็กน้อย ทำให้ประชาชนไม่สามารถเข้าถึงข้อมูลอื่นๆที่เป็นประโยชน์ในเว็บไซต์ได้

ภาครัฐจึงควรศึกษาวิจัยหาแนวทางบัญญัติกฎหมายเฉพาะสำหรับการปิดกั้นเว็บไซต์ที่ไม่เหมาะสม โดยจะควรพิจารณาในประเด็นสำคัญต่างๆ ดังนี้

- ควรกำหนดขั้นตอนการปิดกั้นและขั้นตอนขอยกเลิกการปิดกั้นให้ชัดเจน

- ควรกำหนดมาตรฐานและรายละเอียดของข้อมูลที่ถือว่าไม่เหมาะสมให้ชัดเจน

- ควรปิดกั้นเฉพาะเนื้อหาส่วนที่เป็นปัญหา โดยจะต้องไม่กระทบต่อเนื้อหาส่วนอื่นๆที่ไม่เกี่ยวข้อง และหลีกเลี่ยงที่จะปิดกั้นเนื้อหาทั้งหมด เว้นแต่ มีเหตุผลอันจำเป็น

- ควรกำหนดให้เจ้าหน้าที่ทำการปิดกั้นได้อย่างต่อเนื่อง เช่น เมื่อเจ้าหน้าที่ทำการปิดกั้นเว็บไซต์ A1 ผู้กระทำความผิดได้หลีกเลี่ยงโดยเปลี่ยนชื่อเป็นเว็บไซต์ A2 ในกรณีนี้ควรให้อำนาจเจ้าหน้าที่ปิดกั้นเว็บไซต์ที่ตั้งชื่อใหม่โดยอาศัยคำสั่งฉบับเดิมได้ โดยไม่ต้องดำเนินการใหม่ทั้งหมด

- อาจกำหนดให้รัฐจ่ายค่าชดเชยหรือค่าเสียหายให้แก่ผู้ได้รับความเสียหายจากการปิดกั้นที่ไม่ถูกต้อง

(3.) นอกจากนี้จากการศึกษายังพบว่า การปิดกั้นเว็บไซต์อาจส่งผลกระทบต่อธุรกิจของเจ้าของเว็บไซต์เป็นอย่างมากเพราะไม่สามารถดำเนินธุรกิจได้ตามปกติ อีกทั้งการขอยกเลิกการปิดกั้นอาจใช้ระยะเวลายาวนาน จึงควรศึกษาหาแนวทางกำหนดให้ผู้ที่ได้รับความเสียหายจากการปิดกั้น เช่น เว็บมาสเตอร์ ผู้ให้บริการ สามารถร้องขอต่อศาลเพื่อขอคุ้มครองชั่วคราวเพื่อให้ยกเลิกมาตรการดังกล่าวเป็นการชั่วคราวได้ในระหว่างดำเนินคดีได้ ทั้งนี้ เพื่อ

บรรเทาความเสียหายที่ผู้เสียหายได้รับจากการดำเนินการที่อาจไม่ชอบด้วยกฎหมาย (เช่น เจ้าหน้าที่ปิดกั้นเว็บไซต์โดยอ้างว่าขัดมาตรา20 โดยไม่ร้องขอต่อศาล หรือปิดกั้นเว็บไซต์เพราะถูกแทรกแซงด้วยอำนาจทางการเมืองโดยมิได้ปฏิบัติตามขั้นตอนให้ถูกต้อง เป็นต้น) นอกจากนี้อาจจะกำหนดให้ศาลวางเงื่อนไขในการอนุญาตให้คุ้มครองชั่วคราวได้ตามสมควร เช่น อนุญาตให้เปิดเว็บไซต์ได้ตามปกติแต่ให้ปิดกั้นเนื้อส่วนที่เป็นปัญหาไว้เป็นการชั่วคราวจนกว่าจะมีคำสั่งศาลเป็นอย่างอื่น

4.)ปัญหาในการดำเนินคดีอาญาบางฐาน เช่น ความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญาที่กระทำบนอินเทอร์เน็ต ผู้เสียหายอาจได้รับความเสียหายอย่างต่อเนื่องตราบเท่าที่ถ้อยคำหมิ่นประมาทยังปรากฏอยู่บนอินเทอร์เน็ต และความเสียหายอาจขยายไปยังวงกว้าง เช่น มีการคัดลอกถ้อยคำหมิ่นประมาทไปโพสท์ยังเว็บไซต์อื่นหรือเผยแพร่ลิงค์ของเว็บไซต์ดังกล่าวหรือส่งผ่านทางอีเมล์ต่อไปเป็นทอดๆ และในกรณีนี้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร(ICT) ปฏิเสธที่จะดำเนินการปิดกั้นเว็บไซต์ให้ผู้เสียหายเพราะถือว่าเป็นความผิดที่กฎหมายไม่ได้ให้อำนาจในการปิดกั้นไว้

เพื่อหาแนวทางแก้ปัญหาในลักษณะดังกล่าวจึงควรศึกษาแนวการการแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550และประมวลกฎหมายวิธีพิจารณาความอาญาเพื่อให้ผู้เสียหายสามารถร้องขอต่อศาลในการขอคุ้มครองชั่วคราวได้ เช่น ในระหว่างการดำเนินคดีตามประมวลกฎหมายอาญาฐานหมิ่นประมาทที่เผยแพร่บนอินเทอร์เน็ต ควรให้ผู้เสียหายสามารถร้องขอต่อศาลให้ถอนข้อความหมิ่นประมาทออกจากเว็บไซต์ได้ เมื่อศาลมีคำสั่งอนุญาตแล้วหากผู้ดูแลเว็บไซต์มิได้ดำเนินการถอนข้อความดังกล่าวภายในเวลาอันสมควร อาจกำหนดให้ต้องรับผิดทางแพ่งหรือทางอาญา เป็นต้น

5.9 <u>การห้ามจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์</u>

เนื่องจากชุดคำสั่งไม่พึงประสงค์ (Malicious code) เช่น โปรแกรมประเภท ไวรัส (Virus), มัลแวร์ (malware), เวิร์ม (worm), สปายแวร์ (spyware) สามารถกระจายและสร้างความเสียหายได้อย่างรวดเร็วแต่เมื่อพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พบว่ามาตรการที่นำมาใช้ยังไม่มีประสิทธิภาพในการควบคุมการกระทำความผิดได้อย่างรวดเร็ว กล่าวคือ ไม่ได้ให้อำนาจพนักงานเจ้าหน้าที่ในการระงับ ทำลายหรือแก้ไข

ข้อมูลคอมพิวเตอร์ที่เป็นปัญหาได้อย่างฉับไว เพราะขั้นตอนและวิธีการตามมาตรา 21 เป็นมาตรการที่ล่าช้าซึ่งขัดต่อรูปแบบของการกระทำความผิดที่ต้องจัดการปัญหาอย่างรวดเร็ว อีกทั้งหากผู้กระทำผิดไม่ปฏิบัติตามมาตรการดังกล่าว ก็มีผลเพียงโทษปรับและปรับเป็นรายวันจนกว่าจะปฏิบัติให้ถูกต้อง ตามมาตรา 27 เท่านั้น ซึ่งเทียบไม่ได้กับความเสียหายที่อาจเกิดขึ้น ยกตัวอย่างเช่น กรณีการกระทำผิดตามมาตรา12(2) โดยผู้กระทำความผิดใช้วิธีการปล่อยไวรัสเข้าสู่คอมพิวเตอร์ที่ควบคุมระบบสาธารณูปโภคของรัฐ

ดังนั้น จึงควรแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 21 เพื่อให้อำนาจเจ้าหน้าที่มีอำนาจการระงับความเสียหายได้อย่างรวดเร็วยิ่งขึ้น เช่น เมื่อเจ้าของหรือผู้ครอบครองชุดคำสั่งไม่พึงประสงค์ไม่ปฏิบัติตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่มีอำนาจดำเนินการใดๆเพื่อระงับ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์ที่เป็นปัญหาได้อย่างรวดเร็ว

5.10 การแต่งตั้งพนักงานเจ้าหน้าที่

เมื่อพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ประกอบประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ข้อ2และข้อ3 พบว่ากฎหมายเปิดช่องให้แต่งตั้งผู้ไม่มีความรู้และความชำนาญทางคอมพิวเตอร์เป็นพนักงานเจ้าหน้าที่ได้ ซึ่งสันนิษฐานว่าสาเหตุที่ระบุเช่นนั้นอาจเป็นเพราะข้อจำกัดของภาครัฐในการผลิตบุคลากร

อย่างไรก็ดี ในอนาคตเมื่อภาครัฐมีความพร้อมทั้งทางด้านเทคโนโลยีและบุคคลากรควรกำหนดให้คุณสมบัติพนักงานเจ้าหน้าที่ให้เป็นผู้มีความรู้ความและความชำนาญเกี่ยวกับระบบคอมพิวเตอร์เท่านั้น เพราะการแต่งตั้งพนักงานเจ้าหน้าที่ไม่มีความรู้ความเข้าใจเฉพาะด้านอย่างแท้จริงย่อมไม่เอื้อต่อการสอบสวนอย่างมีประสิทธิภาพ เช่น กำหนดคุณสมบัติให้พนักงานเจ้าหน้าที่จะต้องผ่านหลักสูตรอบรมตามที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกำหนดไว้โดยเฉพาะ

5.11 ความร่วมมือระหว่างประเทศ

(1.) การดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ตที่อยู่ในต่างประเทศทำได้ยากลำบาก เพราะการแสวงหาพยานหลักฐานทำได้ยาก, ขาดความรู้ด้านกฎหมายของประเทศที่กระทำผิด, การระบุสถานที่(Locating)กระทำความผิดทำได้ยาก, ไม่ทราบว่าเจ้าหน้าที่หรือหน่วยงานใดเป็นผู้รับผิดชอบ เป็นต้น

ปัญหานี้ในต่างประเทศ เช่น ประเทศในกลุ่มG-8, สหภาพยุโรปและองค์กรระหว่างประเทศอื่นๆหรือประเทศสหรัฐอเมริกาได้ส่งเสริมให้มีการจัดตั้งศูนย์ 24/7 network เพื่อให้ความช่วยเหลือในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ระหว่างประเทศ อีกทั้งให้ความร่วมมือในการถ่ายทอดเทคนิค, ร่วมกันจัดฝึกอบรมเจ้าหน้าที่และจัดหาเครื่องมือที่ทันสมัย (กลุ่ม Apecที่ประเทศไทยเป็นสมาชิกก็ถือว่า การจัดตั้งศูนย์ 24/7 network เป็นเรื่องจำเป็นเร่งด่วนเช่นกัน)

ดังนั้น จึงมีความจำเป็นที่ภาครัฐจะต้องจัดให้มีศูนย์ความร่วมมือด้านการกระทำความผิดทางคอมพิวเตอร์ที่มีเจ้าหน้าที่ปฏิบัติหน้าที่ตลอด 24 ชั่วโมง สัปดาห์ละ 7 วัน (24/7 network) และพัฒนาเทคโนโลยีและบุคคลากรให้มีความพร้อม เพื่อให้ศูนย์ดังกล่าวสามารถทำหน้าที่ให้การช่วยเหลือในการดำเนินคดีให้มีประสิทธิภาพยิ่งขึ้น เช่น เมื่อพนักงานเจ้าหน้าที่มีปัญหาเกี่ยวกับข้อกฎหมายในขณะทำการค้นสามารถติดต่อทางศูนย์ฯเพื่อขอคำแนะนำได้อย่างรวดเร็ว หรือหากเจ้าหน้าที่มีความจำเป็นที่จะต้องขอความร่วมมือจากต่างประเทศเพื่อขอความช่วยเหลือด้านComputer Forensic ก็สามารถประสานงานผ่านทางศูนย์24/7 network ได้อย่างรวดเร็ว

(2.) นอกจากนี้ จากการศึกษายังพบว่าการดำเนินคดีระหว่างประเทศจะอาศัยความร่วมมือลักษณะถ้อยทีถ้อยอาศัยมากกว่าการขอความร่วมมือตามกฎหมาย เพราะมีความคล่องตัวและรวดเร็วกว่าการขอความร่วมมือตามกฎหมายที่ยุ่งยาก อาจไม่ทันท่วงทีในการดำเนินคดีกับผู้กระทำความผิด แต่เมื่อพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 พบว่าหากพนักงานเจ้าหน้าที่ไม่สามารถดำเนินการข้างต้นได้(ยกตัวอย่างเช่นส่งมอบข้อมูลให้เจ้าหน้าที่ของต่างประเทศ) เพราะอาจได้รับโทษทางอาญาตามมาตรา 22 (แม้มาตรา22วรรคสองจะเปิดช่องให้ดำเนินการเช่นนั้นได้ แต่ก็ต้องขออนุญาตจากศาลซึ่งใช้เวลานานและไม่เหมาะสมกับการดำเนินคดีกับอาชญากรรมคอมพิวเตอร์ที่ต้องการความรวดเร็ว)

ในสหภาพยุโรปหรือองค์กรความร่วมมือระหว่างประเทศอื่นๆ และสหรัฐอเมริกา ซึ่งปัจจุบันเข้าเป็นภาคีตาม The Council of Europe Convention on Cybercrimeแล้ว ได้มีแนวทางความร่วมมือไปในแนวทางเดียวกันคือส่งเสริมการให้ความร่วมมือลักษณะถ้อยทีถ้อยอาศัยอย่างไม่เป็นทางการ

ในประเด็นนี้ควรเพิ่มเติมบทบัญญัติที่สอดคล้องกับการประสานงานระหว่างประเทศอย่างไม่เป็นทางการ เช่น ให้อำนาจพนักงานเจ้าหน้าที่ส่งมอบข้อมูลคอมพิวเตอร์เพื่อให้เจ้าหน้าของต่างประเทศดำเนินการกระบวนการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensic) ได้สะดวก และไม่ถือเป็นความผิด โดยควรเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 22 วรรคสี่ ดังนี้

"มาตรา 22 วรรคสี่ เพื่อประโยชน์ในการสืบสวน สอบสวน ในกรณีพนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลตามวรรคหนึ่ง ให้แก่เจ้าหน้าที่ต่างประเทศเพื่อความช่วยเหลือระหว่างประเทศ ไม่ถือเป็นความผิดตามวรรคสาม ทั้งนี้ ตามวิธีการ หลักเกณฑ์ และหน่วยงานที่รัฐมนตรีประกาศในราชกิจจานุเบกษา"

5.12 ข้อสันนิษฐานเพื่อการดำเนินคดี

ปัญหาสำคัญในการดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ตคือการระบุตัวผู้กระทำความผิดทำได้ยากลำบาก เพราะแม้พนักงานเจ้าหน้าที่จะสืบทราบถึงเครื่องคอมพิวเตอร์ที่ใช้กระทำความผิดและระบุสถานที่กระทำความผิดได้ก็ตาม แต่ก็ไม่อาจระบุตัวผู้กระทำความผิดเพื่อออกหมายจับได้ เช่น สถานที่กระทำความผิดเป็นร้านอินเทอร์เน็ตคาเฟ่ที่มีผู้ใช้บริการมากมาย หรือเป็นบ้านที่มีผู้อยู่อาศัยหลายคนและมีการใช้คอมพิวเตอร์ร่วมกัน

ในประเทศสิงคโปร์แก้ไขปัญหานี้ด้วยการกำหนดบทสันนิษฐานตามกฎหมาย โดยถือว่าผู้เข้ารหัสผ่านยังคงเป็นผู้ครอบครองรหัสผ่านนั้นอยู่ หากเจ้าหน้าที่ทำการถอดรหัสแล้วพบว่าเขาเป็นผู้เข้ารหัสก่อนหน้านั้น และผลักภาระการพิสูจน์ไปให้ผู้ครอบครองรหัสผ่าน เพื่อพิสูจน์ว่าเขามิได้เป็นผู้กระทำความผิด(Article125 B(7))

จึงควรบัญญัติที่เป็นข้อสันนิษฐานตามกฎหมาย เพื่อให้พนักงานเจ้าหน้าที่สามารถระบุผู้กระทำความผิดในการดำเนินคดีได้ (แม้การบัญญัติกฎหมายลักษณะนี้ทำได้ยาก และอาจมีข้อโต้แย้งมากมาย เพราะการบัญญัติบทสันนิษฐานในคดีอาญาอาจขัดต่อหลักการดำเนินคดีอาญาที่กำหนดให้หน้าที่นำสืบตกอยู่แก่โจทก์)

อย่างไรก็ดี ในความเห็นส่วนตัวของผู้เขียนเห็นว่าควรเพิ่มเติมบทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 25/1 และ 25/2 ดังนี้

"มาตรา 25/1 เพื่อประโยชน์ในการดำเนินคดี หากการพนักงานเจ้าหน้าที่ถอดรหัสข้อมูลแล้วสามารถระบุได้ว่าบุคคลใดครอบครองรหัสข้อมูลที่ถอดรหัสนั้น ให้ถือว่าบุคคลนั้นครอบครองรหัสข้อมูลต่ออย่างเนื่องเว้นแต่จะพิสูจน์ได้ว่า

ก. เขามิได้ครอบครองรหัสข้อมูลในช่วงเวลาที่เกิดการกระทำผิด และ

ข. เขามิได้ครอบครองรหัสข้อมูลต่อเนื่องภายหลังระยะเวลาที่พนักงานเจ้าหน้าที่ระบุได้โดยการถอดรหัส"

"มาตรา 25/2 ความตาม มาตรา 25/1 ไม่ผูกพันศาลในชั้นพิจารณา "