



บทที่ 4

ประเทศไทยกับการเข้าร่วมเป็นภาคีและผลกระทบในการเข้าเป็นภาคี อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

จากการที่ได้ทำการศึกษาวิเคราะห์ประเด็นต่างๆในบทบัญญัติของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 และรวมถึงปัญหาและอุปสรรคในการปฏิบัติตามพันธกรณีของประเทศที่เป็นภาคี ทำให้ทราบถึงมาตรการและหลักการต่างๆ ที่กำหนดไว้ในอนุสัญญาซึ่งมักจะเป็นการกำหนดให้ประเทศสมาชิกดำเนินการเกี่ยวกับมาตรการทางกฎหมาย โดยการกำหนดแนวทางในลักษณะกว้างๆ เพื่อให้การดำเนินการมีมาตรฐานใกล้เคียงกัน ซึ่งการบัญญัติเช่นนี้ทำให้เกิดความสอดคล้องกันของกฎหมายภายในของประเทศภาคีแต่ละประเทศที่มีความแตกต่างกันในด้านต่างๆ เช่น แนวคิดทางการเมือง ทางเศรษฐกิจ หรือแนวทางในการคุ้มครองสิทธิเสรีภาพ แต่ความแตกต่างดังกล่าวจะต้องไม่ก่อให้เกิดอุปสรรคที่จะปฏิบัติตามพันธกรณี และในการปฏิบัติตามพันธกรณีถึงแม้จะมีประเด็นขัดข้องในเรื่องของการคุ้มครองเกี่ยวกับสิทธิส่วนบุคคลและเสรีภาพในการแสดงออก ซึ่งเป็นหลักการสำคัญที่ต้องคำนึงถึงเป็นอย่างมาก มาตรฐานในการคุ้มครองสิทธิมนุษยชนระหว่างประเทศส่วนใหญ่ ต่างมุ่งเน้นการรักษาความเท่าเทียมกันและการคุ้มครองบุคคลพลเมืองจากการกระทำของรัฐบาล ซึ่งประเทศภาคีควรให้ความสำคัญกับประเด็นดังกล่าว

อย่างไรก็ตาม เนื่องจากอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 เป็นกฎหมายระหว่างประเทศ หากประเทศไทยจะทำการพิจารณาเพื่อเข้าเป็นภาคีอนุสัญญานี้จะต้องพิจารณาถึงความสัมพันธ์ระหว่างกฎหมายภายในและอนุสัญญาซึ่งในการพิจารณาความสัมพันธ์จะขึ้นอยู่กับแนวคิดหรือทฤษฎีที่ประเทศใช้ว่าจะนำกฎหมายระหว่างประเทศมาใช้ได้ในทันทีหรือไม่ มีแนวคิดหรือทฤษฎีในการอธิบายความสัมพันธ์ของกฎหมายระหว่างประเทศกับกฎหมายภายในในการกระทำให้กฎหมายระหว่างประเทศมีผลบังคับใช้ได้ภายในประเทศ ทฤษฎีที่ว่าได้แก่¹ ทฤษฎีเอกนิยม (Monism) และทฤษฎีทวินิยม (Dualism)

ทฤษฎีเอกนิยม (Monism) แนวความคิดของนักกฎหมายที่สนับสนุนทฤษฎีนี้ถือว่ากฎหมายภายในรัฐและระบบกฎหมายระหว่างประเทศเป็นกฎหมายระบบเดียวกันไม่ว่าจะเป็นกฎหมายที่ผูกพันรัฐหรือเป็นกฎหมายที่ผูกพันปัจเจกชน

¹ จมพต สายสุนทร, กฎหมายระหว่างประเทศ เล่ม 1, พิมพ์ครั้งที่ 6, (กรุงเทพฯ: วิญญูชน, 2549), หน้า 105-107.

ทฤษฎีทวินิยม (Dualism) แนวความคิดของนักกฎหมายที่สนับสนุนทฤษฎีนี้ถือว่ากฎหมายภายในรัฐเป็นระบบกฎหมายแยกต่างหากจากกฎหมายระหว่างประเทศ

ดังนั้น กระบวนการเข้าเป็นภาคีอนุสัญญาฉบับต่างๆของประเทศไทยจะต้องทำการพิจารณาความสัมพันธ์ระหว่างอนุสัญญาและกฎหมายภายในว่าเป็นความสัมพันธ์ตามทฤษฎีใด แม้ว่ารัฐธรรมนูญแห่งราชอาณาจักรไทยจะไม่ได้ระบุเอาไว้ว่าประเทศไทยยอมรับทฤษฎีใดเกี่ยวกับการนำกฎหมายระหว่างประเทศมาใช้ และในปี พ.ศ. 2550 ที่ประเทศไทยมีการแก้ไขรัฐธรรมนูญใหม่ ทำให้มีการเพิ่มเติมหลักการบางประการในการทำอนุสัญญา เมื่อทำการพิจารณาตามถ้อยคำในรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 190 ดังนี้

“พระมหากษัตริย์ทรงไว้ซึ่งพระราชอำนาจในการทำหนังสือสัญญาสันติภาพ สัญญาสงบศึก และสัญญาอื่น กับนานาประเทศหรือกับองค์การระหว่างประเทศ

หนังสือ สัญญาใดมีบทเปลี่ยนแปลงอาณาเขตไทย หรือเขตพื้นที่นอกอาณาเขตซึ่งประเทศไทยมีสิทธิอธิปไตย หรือมีเขตอำนาจตามหนังสือสัญญา หรือตามกฎหมายระหว่างประเทศ หรือจะต้องออกพระราชบัญญัติเพื่อให้การเป็นไปตามหนังสือสัญญา หรือมีผลกระทบต่อความมั่นคงทางเศรษฐกิจหรือสังคมของประเทศอย่างกว้างขวาง หรือมีผลผูกพันด้านการค้า การลงทุน หรืองบประมาณของประเทศอย่างมีนัยสำคัญ ต้องได้รับความเห็นชอบของรัฐสภา ในการนี้ รัฐสภาจะต้องพิจารณาให้แล้วเสร็จภายในหกสิบวันนับแต่วันที่ได้รับเรื่องดังกล่าว

ก่อนการดำเนินการเพื่อทำหนังสือสัญญากับนานาประเทศหรือองค์การระหว่างประเทศ ตามวรรคสอง คณะรัฐมนตรีต้องให้ข้อมูลและจัดให้มีการรับฟังความคิดเห็นของประชาชน และต้องชี้แจงต่อรัฐสภาเกี่ยวกับหนังสือสัญญานั้น ในการนี้ ให้คณะรัฐมนตรีเสนอรอบการเจรจาต่อรัฐสภาเพื่อขอความเห็นชอบด้วย

เมื่อลงนามในหนังสือสัญญาตามวรรคสองแล้ว ก่อนที่จะแสดงเจตนาให้มีผลผูกพัน คณะรัฐมนตรีต้องให้ประชาชนสามารถเข้าถึงรายละเอียดของหนังสือสัญญานั้น และในกรณีที่การปฏิบัติตามหนังสือสัญญาดังกล่าวก่อให้เกิดผลกระทบต่อประชาชนหรือผู้ประกอบการขนาดกลาง และขนาดย่อม คณะรัฐมนตรีต้องดำเนินการแก้ไขหรือเยียวยาผู้ได้รับผลกระทบนั้นอย่างรวดเร็ว เหมาะสม และเป็นธรรม

ให้กฎหมายว่าด้วยการกำหนดขั้นตอนและวิธีการจัดทำหนังสือสัญญาที่มีผลกระทบต่อความมั่นคงทางเศรษฐกิจหรือสังคมของประเทศอย่างกว้างขวาง หรือมีผลผูกพันด้านการค้า หรือการลงทุนอย่างมีนัยสำคัญ รวมทั้งการแก้ไขหรือเยียวยาผู้ได้รับผลกระทบจากการปฏิบัติตาม

หนังสือสัญญาดังกล่าวโดยคำนึงถึงความเป็นธรรมระหว่างผู้ที่ได้ประโยชน์กับผู้ที่ได้รับผลกระทบจากการปฏิบัติตามหนังสือสัญญานั้นและประชาชนทั่วไป

ในกรณีที่มีปัญหาตามวรรคสอง ให้เป็นอำนาจของศาลรัฐธรรมนูญที่จะวินิจฉัยชี้ขาด โดยให้นำบทบัญญัติตามมาตรา 154 (1) มาใช้บังคับกับการเสนอเรื่องต่อศาลรัฐธรรมนูญโดยอนุโลม"

จากบทบัญญัติดังกล่าวแสดงให้เห็นว่า ก่อนการทำอนุสัญญาตามวรรคสอง คณะรัฐมนตรีต้องให้ข้อมูลและจัดให้มีการรับฟังความคิดเห็นของประชาชน และต้องชี้แจงต่อรัฐสภา รวมถึงเสนอกรอบการเจรจาเพื่อขอความเห็นชอบด้วย ซึ่งในส่วนี้การกำหนดกติกาและกระบวนการเกี่ยวกับอนุสัญญาได้มีความชัดเจนและรัดกุมยิ่งขึ้น มีการเปิดโอกาสให้ประชาชนมีส่วนร่วมมากขึ้นถือเป็นผลดีแก่ประชาชนที่เกี่ยวข้อง เนื่องจากสามารถเสนอความเห็นให้แก่ภาครัฐได้ และหากภาครัฐได้รับทราบความคิดเห็นและได้รับทราบข้อเท็จจริงก็สามารถเข้าใจถึงปัญหา คัดเลือกกรันกรอง และสรุปประเด็นด้านบวกและด้านลบเพื่อนำไปกำหนดกรอบในการเจรจาเพื่อให้เกิดประโยชน์สูงสุดแก่ประเทศไทย ทั้งนี้ หากมีการให้สัตยาบันไปแล้วถ้าอนุสัญญาดังกล่าวส่งผลกระทบต่อประชาชน รัฐบาลจะต้องมีมาตรการเยียวยาออกมารองรับด้วย

ดังนั้น จึงสามารถสรุปได้ว่าประเทศไทยยอมรับทฤษฎีทวินิยมจากถ้อยคำดังกล่าว ทำให้การที่จะพิจารณาว่าควรลงนามเป็นภาคีอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 หรือไม่นั้น จะต้องพิจารณาก่อนว่ากฎหมายภายในที่มีอยู่สอดคล้องกับพันธกรณีตามบทบัญญัติของอนุสัญญาหรือไม่ เพราะหากพบว่ามีกฎหมายภายในของไทยรองรับสนธิสัญญาอยู่แล้ว ก็ไม่จำเป็นต้องมีการออกกฎหมายอนุวัติการ ศาลไทยสามารถที่จะนำอนุสัญญาเช่นว่านั้นมาใช้ในการวินิจฉัยบรรดคดีโดยอาศัยบทบัญญัติแห่งกฎหมายซึ่งรองรับอนุสัญญาเช่นว่านั้น² หรือหากพบว่าไม่มีกฎหมายที่รองรับหรือบทบัญญัติกฎหมายโดยทั่วไปของไทยไม่เพียงพอต่อการปฏิบัติตามพันธกรณีของอนุสัญญา ประเทศไทยจะได้ดำเนินมาตรการเตรียมความพร้อมทางด้านกฎหมายเพื่อรองรับพันธกรณีที่จะเกิดขึ้นต่อไปตามเหตุผลที่กล่าวมาข้างต้น

ด้วยเหตุนี้ผู้เขียนจึงศึกษาถึงมาตรการต่างๆ ที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ของประเทศไทยไม่ว่าจะเป็นมาตรการทางด้านนิติบัญญัติ มาตรการทางด้านบริหาร มาตรการทางด้านตุลาการ หน่วยงานและความพร้อมด้านอื่นๆ ที่เกี่ยวข้อง รวมถึงผลที่ประเทศไทยจะได้รับ

² เรื่องเดียวกัน, หน้า 151-152.

หากมีการลงนามเป็นภาคีในอนุสัญญาดังกล่าว ซึ่งก่อนที่จะกล่าวถึงเรื่องดังกล่าว ผู้เขียนจะกล่าวถึงสถานการณ์ปัญหาอาชญากรรมทางคอมพิวเตอร์ในประเทศไทยให้ทราบ

4.1 สถานการณ์เกี่ยวกับปัญหาอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ตในประเทศไทย

หลายปีที่ผ่านมาประเทศต่างๆ โดยเฉพาะประเทศที่พัฒนาแล้วได้ให้ความสำคัญกับการออกกฎหมายอาชญากรรมทางคอมพิวเตอร์เพื่อกำหนดสิทธิในการใช้และการเข้าถึงระบบคอมพิวเตอร์และอินเทอร์เน็ตรวมถึงตัวบทกฎหมายให้เป็นไปในทิศทางเดียวกัน เพื่อลดปัญหาการใช้คอมพิวเตอร์ไปในทางที่ผิด ประเทศไทยเองก็ได้ตระหนักถึงความสำคัญและไม่ละเลยในเรื่องการคุ้มครองประชาชนผู้ใช้บริการเกี่ยวกับคอมพิวเตอร์และอินเทอร์เน็ต เนื่องจากในปัจจุบันมีการใช้งานคอมพิวเตอร์มากขึ้น และอาจส่งผลให้เกิดการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ เห็นได้จากตัวอย่างของเหตุการณ์ที่เกิดขึ้นบ่อยในประเทศไทยไม่ว่าจะเป็น

กรณีการเผยแพร่สื่อลามกหรือภาพผู้อื่นโดยไม่ได้รับอนุญาต³ ปัญหาการเผยแพร่สื่อลามกอนาจารบนเครือข่ายอินเทอร์เน็ตเป็นปัญหาที่ประสบอยู่เป็นประจำ เว็บไซต์ที่เผยแพร่สื่อลามกเหล่านี้มีทั้งที่ตั้งอยู่ในประเทศและนอกประเทศ เมื่อเจ้าหน้าที่ได้รับแจ้งเบาะแสของเว็บไซต์ที่ไม่เหมาะสมเหล่านี้ หากตั้งอยู่ในประเทศไทยก็จะทำการตักเตือนและสั่งให้กำจัดเนื้อหาเหล่านั้น หากตั้งอยู่นอกประเทศก็จะประสานให้ผู้ให้บริการอินเทอร์เน็ตทำการปิดกั้น แต่อย่างไรก็ตามเว็บไซต์ประเภทนี้เกิดขึ้นใหม่อย่างต่อเนื่องจึงยากที่จะทำการปิดกั้นได้อย่างทั่วถึงในทางปฏิบัติ ในบางกรณีภาพลามกที่ถูกนำมาเผยแพร่เป็นภาพที่เกิดขึ้นจากการตัดต่อทำให้บุคคลในภาพได้รับความเสียหายอย่างมาก อีกทั้งภาพลามกจำนวนมากไม่น้อยได้มาจากการแอบถ่ายที่ใช้เทคโนโลยีสมัยใหม่เข้ามาอำนวยความสะดวก โดยเฉพาะกล้องดิจิทัลบนโทรศัพท์มือถือ หรือใช้กล้องประเภทแอบถ่ายทะเลื้อผ้าซึ่งผู้กระทำความผิดสามารถหลบซ่อนกล้องไว้ได้เพื่อแอบถ่ายภาพลามกต่างๆ ได้อย่างสะดวก นอกจากนี้บางเว็บไซต์ยังเผยแพร่ภาพบุคคลที่ได้จากร้านอัดรูปดิจิทัล เนื่องจากผู้ต้องการอัดรูปภาพจากกล้องดิจิทัลต้องนำรูปภาพบันทึกลงในอุปกรณ์คอมพิวเตอร์ของร้านอัดรูปเพื่อทำการอัดภาพ รูปภาพเหล่านี้จึงอาจถูกนำมาเผยแพร่บนอินเทอร์เน็ตได้ เช่น

³ การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร, รายงานของประเทศไทย: การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร ประเทศไทย "การฝึกกำลังและการโต้ตอบ : การดำเนินกลยุทธ์ร่วมกันในการป้องกันอาชญากรรมและความยุติธรรมทางอาญา", (กรุงเทพฯ : โรงพิมพ์ราชทัณฑ์ กรมราชทัณฑ์ กระทรวงยุติธรรม, 2548), หน้า 72.

คดีเสียใหญ่ตัดต่อภาพแฟนโพสต์เน็ต⁴ มีรายงานจากเว็บไซต์ posttoday.com ว่าตำรวจกองบังคับการปราบปรามการกระทำผิดต่อเด็กเยาวชนและสตรี เข้าจับกุมผู้ต้องหาชื่อนายสมพงษ์ จำปาทอง นักธุรกิจใหญ่ในจังหวัดปทุมธานี ในข้อหานำภาพถ่ายอดีตแฟนสาวไปตัดต่อให้เป็นภาพลามกอนาจารก่อนนำเข้าระบบอินเทอร์เน็ตภายในของธนาคารและชมรมซูบีบับังคับอดีตแฟนสาวว่า หากไม่ต้องการให้โพสต์ภาพเพิ่มเติมอีกต้องยอมกลับมาคืนดีด้วย นามสมพงษ์รับสารภาพว่าเพิ่งลงมือทำเป็นครั้งแรกโดยทำไปเพราะความรักไม่ต้องการเลิกกับผู้เสียหาย แต่หลังจากงอนข้อสารพัดรูปแบบแล้วไม่สำเร็จ จึงตัดสินใจนำภาพไปเผยแพร่เพื่อหวังชมชู้ เบื้องต้นตำรวจแจ้งข้อหานายสมพงษ์ว่า "นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกอนาจาร และข้อมูลนั้น ประชาชนทั่วไป อาจเข้าถึงได้และนำไปเผยแพร่หรือส่งต่อเพื่อแจกจ่ายหรือเพื่อการทำให้แพร่หลายซึ่งเป็นการฝ่าฝืนพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550"

คดีอดีตแฟนโพสต์ภาพโป๊ประจานหญิง⁵ มีรายงานจากเว็บไซต์ gotoknow.org ว่าศาลได้อ่านคำพิพากษาในคดีหมายเลขดำที่ อ.2097/2551 ที่พนักงานอัยการฝ่ายคดีอาญา 6 เป็นโจทก์ยื่นฟ้องนายพุทธพงศ์ ฉลาดธัญกิจ อายุ 34 ปี เป็นจำเลยในฐานความผิดตามมาตรา ๑๔ (๔) "ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ...(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้"

โจทก์ฟ้องว่าจำเลยได้ใส่ความผู้เสียหาย โดยการโฆษณาด้วยภาพจดหมายอิเล็กทรอนิกส์หรืออีเมลผ่านเข้าสู่ระบบคอมพิวเตอร์ เป็นภาพการมีเพศสัมพันธ์ระหว่างจำเลยกับผู้เสียหายจำนวน 2 ภาพ โดยประการที่น่าจะทำให้ผู้เสียหายเสื่อมเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง ต่อมาจำเลยนำภาพการมีเพศสัมพันธ์เข้าสู่ระบบคอมพิวเตอร์อีกหลายครั้ง ภายหลังผู้เสียหายได้เข้าแจ้งความกับพนักงานสอบสวนกองบังคับการปราบปรามการกระทำผิดต่อเด็กเยาวชนและสตรี และสามารถจับกุมจำเลย โดยขอให้ลงโทษตามประมวลกฎหมายอาญา มาตรา 326 และมาตรา 328 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ศาลพิเคราะห์แล้วเห็นว่าผู้เสียหายกับจำเลยเคยคบหากันเป็นคนรักกันมาก่อนเคยบันทึกภาพระหว่างการมีเพศสัมพันธ์กันไว้หลายครั้ง แต่เมื่อทั้งสองเลิกกันและฝ่ายชายเกิด

⁴ ศรีศักดิ์ จามรมาน, สมิติใหม่แห่งการเรียนรู้ เอกสารประกอบการอบรมสำหรับสมาชิก NTU หลักสูตร การบริหารจัดการ สมัยใหม่ เรื่อง ความผิดตามพ.ร.บ.คอมพิวเตอร์ ที่ทุกคนควรรู้อ, ธนาคารกรุงเทพ จำกัด มหาชน, 12 พฤศจิกายน 2552, หน้า 23.

⁵ เรื่องเดียวกัน, หน้า 23

ความหึงหวงจึงนำภาพที่เคยถ่ายไว้เผยแพร่ทางคอมพิวเตอร์ทั้งที่ในระหว่างจำเลยและผู้เสียหาย คบกันไม่เคยมีภาพดังกล่าวปรากฏมาก่อน ศาลรับฟังประกอบกับการถ่ายโอนข้อมูลภาพทั้งหมดที่ กระทำภายในคราวเดียวจากเครื่องคอมพิวเตอร์ของกลาง นอกจากนี้ พยานโจทก์ทุกปากไม่มี สาเหตุโกรธเคืองกับจำเลยมาก่อนไม่มีเหตุให้สงสัยว่าจะแก้มือเปิดความปรักปรำจำเลย เชื่อว่า ภาพในเว็บไซต์เป็นภาพเดียวกับที่อยู่ในเครื่องคอมพิวเตอร์ของจำเลย และถูกส่งมาจากเครื่อง คอมพิวเตอร์ดังกล่าว ในคดีแพ่งนั้นศาลเห็นสมควรกำหนดค่าสินไหมทดแทนให้แก่ผู้เสียหายด้วย และพิพากษาว่าจำเลยมีความผิดตามประมวลกฎหมายอาญา และพระราชบัญญัติว่าด้วย ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14 (4) และ (5)

คดีเจ้าของเว็บไซต์เผยแพร่คลิปครูสาว⁶ มีรายงานจากเว็บไซต์ kroobannok.com ว่ากอง บังคับการปราบปรามการกระทำผิดต่อเด็กเยาวชนและสตรี และเจ้าหน้าที่ตำรวจแถลงข่าวจับกุม นายชูศักดิ์ เสียงระฆัง อายุ 24 ปี เจ้าของเว็บไซต์ gooseed.com และเป็นผู้ต้องหาตาม หมายจับของศาลอาญา ในข้อหาเพื่อความประสงค์แห่งการค้า หรือโดยการค้า เพื่อการแจกจ่าย หรือแสดงอวดอ้างแก่ประชาชนให้แพร่หลายด้วยประการใดๆซึ่งสิ่งใดอันลามกและเป็นผู้ให้บริการ สนับสนุน หรือยินยอมให้มีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พร้อมของ กลางคอมพิวเตอร์ 1 เครื่อง และอุปกรณ์เชื่อมต่ออินเทอร์เน็ต ทั้งยังจับกุมนายจักรพงษ์ เกาะศิริ อายุ 33 ปี เป็นพนักงานระดับ 3 อบจ. กาญจนบุรี ซึ่งเป็นผู้ต้องหาตามหมายจับของศาลอาญา ในข้อหาเพื่อจะช่วยให้การทำให้แพร่หลาย หรือการค้าสิ่งของลามก โฆษณา หรือโฆษณาว่าสิ่งของ ดังกล่าวจะหาได้จากบุคคลใดหรือโดยวิธีใด และข้อหาสนับสนุนการเผยแพร่ซึ่งข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชน ทั่วไปอาจเข้าถึงได้

เจ้าหน้าที่ตำรวจเปิดเผยว่า สืบเนื่องจาก น.ส. เอ (นามสมมุติ) อายุ 27 ปี เข้าแจ้งความร้อง ทูลทุกข์ว่ามีบุคคลใช้ชื่อผู้ใช้ (User Name) ว่า "Jak696" นำคลิปขณะมีเพศสัมพันธ์กับแฟนหนุ่มมา เผยแพร่ลงบนเว็บไซต์ของนายชูศักดิ์ จึงรวบรวมหลักฐานขอออกหมายจับและจับกุมตัวผู้ต้องหา ทั้ง 2 ราย ด้านนายชูศักดิ์ เจ้าของเว็บไซต์ กล่าวว่า เว็บไซต์ดังกล่าวเปิดมาได้ประมาณ 5 ปีแล้ว ก่อนจะมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยเปิดให้ โพล์ติภาพหรือคลิปลักษณะลามกอนาจารจริง แต่พอมีกฎหมายออกมาก็ปรับเปลี่ยนให้เว็บไซต์ที่ มีรูปสาว ๆ น่ารัก เข้มขี้ แต่ไม่โป๊เปลือย หรือลามกอนาจารโดยให้เพื่อนๆที่เป็นสมาชิกช่วยกันดูแล หากพบว่ามีใครนำภาพหรือคลิปโป๊มาอัปโหลดลงบนเว็บไซต์ก็จะแจ้งมายังตนและจะลบออก

⁶ เรื่องเดียวกัน, หน้า 27

ส่วนคลิปที่นายจักรพงษ์นำมาโพสต์เป็นคลิปครูสาวจังหวัดนครสวรรค์ หลังจากอัปโหลดคลิปแล้วลงบนเว็บไซต์ได้เพียง 1 วัน ตนเองก็ลบคลิปออกทันทีที่ทราบเรื่องและติดต่อมาทาง ปตส. เมื่อประมาณ 6 เดือนที่ผ่านมา หลังทราบว่า ปตส. ส่งหมายเรียกมาถึงทาง E-mail ตน และนึกว่าไม่มี ความผิด เรื่องจะจบแต่กลับกลายเป็นว่ามาถูกตำรวจจับกุมตัวถึงบ้านพัก ทั้งนี้ นายจักรพงษ์ ยอมรับว่านำคลิปไปอัปโหลดลงบนเว็บไซต์ดังกล่าวของนายชูศักดิ์จริงหลังได้รับคลิปผ่านทาง E-mail ที่มีผู้ส่งต่อมาให้ โดยไม่ทราบว่าคลิปดังกล่าวเป็นคลิปของครูสาวจริงหรือไม่ และไม่ได้รู้จักกับตัวครูสาวในคลิปแต่อย่างใด ซึ่งที่มาของคลิปวิดีโอดังกล่าวนั้น เมื่อประมาณเดือนเมษายน พ.ศ. 2551 น.ส. เอ ซึ่งเป็นอาจารย์มหาวิทยาลัยแห่งหนึ่งได้แจ้งความดำเนินคดีแพนหนุ่มวัย 33 ปี ซึ่งเป็นอาจารย์วิทยาลัยเทคนิคแห่งหนึ่งว่านำคลิปลับเป็นภาพขณะมีเพศสัมพันธ์กันไปเผยแพร่ ตามเว็บไซต์หลังที่ทั้งคู่แยกทางกัน ต่อมา ปตส. จับกุมตัวแพนหนุ่มดำเนินคดี แต่ให้การปฏิเสธ โดยอ้างว่าไม่ทราบไปปรากฏตามเว็บไซต์ต่างๆ ได้อย่างไร

คดีนักศึกษามหาวิทยาลัยเอกชนชื่อดังเผยแพร่คลิปอนาจาร⁷ มีรายงานจากเว็บไซต์ ผู้จัดการว่า ปตส. จับกุมนางสาวแสงดาว (นามสมมติ) อายุ 20 ปี นักศึกษาชั้นปีที่ 3 คณะ บริหารคอมพิวเตอร์ มหาวิทยาลัยเอกชนชื่อดังแห่งหนึ่ง ซึ่งเป็นผู้โพสต์แพร่คลิปอนาจารนักเรียนหญิงสำเร็จความใคร่ด้วยปากให้เพื่อนชายบนรถเมล์ปรับอากาศ เบื้องต้นผู้ต้องหาให้การสารภาพ ว่ารับคลิปจากเพื่อนทาง E-mail ก่อนนำไปโพสต์ลงในเว็บไซต์ต่างๆ หลายแห่ง โดยอ้างว่า รู้เท่าไม่ถึงการณ์และไม่ทราบว่ากระทำดังกล่าวเป็นความผิด

กรณีเว็บไซต์ที่เผยแพร่ข้อมูลต่อต้านหรือดูหมิ่นสถาบันชาติ ศาสนา พระมหากษัตริย์ สถาบันชาติ ศาสนา พระมหากษัตริย์ เป็นสถาบันที่สังคมไทยให้ความเคารพเป็นอย่างมาก การลบหลู่ดูหมิ่นสถาบันเหล่านี้ถือว่าเป็นสิ่งที่ยอมรับไม่ได้ เว็บไซต์ที่ถูกใช้เป็นเครื่องมือในการปลุก ระดมเยาวชนหรือประชาชนทั่วไปให้ต่อต้านหรือดูหมิ่นสถาบันเหล่านี้จะถูกตักเตือน ปิดกั้น หรือ ดำเนินคดีทางอาญา แต่บางครั้งพบว่ากลุ่มที่เผยแพร่เหล่านี้เป็นกลุ่มคนภายนอกและจัดตั้ง เว็บไซต์ไว้นอกประเทศ บางครั้งทางรัฐจึงทำได้เพียงการปิดกั้นเนื้อหา แต่อย่างไรก็ตามเว็บไซต์ เหล่านี้ก็ยังสามารถเข้าถึงได้หากผู้ที่ต้องการเข้าถึงใช้งานระบบที่มีตัวแทนในต่างประเทศเพื่อเล็ด รอดการปิดกั้นของรัฐ ตัวอย่าง เช่น

⁷ เรื่องเดียวกัน, หน้า 31.

⁸ การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร, รายงานของประเทศไทย : การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร ประเทศไทย "การรณรงค์กำลังและการโต้ตอบ : การดำเนินกลยุทธ์ ร่วมกันในการป้องกันอาชญากรรมและความยุติธรรมทางอาญา", หน้า 72.

คดีหมิ่นพระบรมเดชานุภาพ⁹ กรณีนายสุวิชา ทำคือ อายุ 34 อาชีพวิศวกร ถูกตำรวจจับกุมตัวที่จังหวัดนครพนม พร้อมกับถูกบุกค้นบ้านในกรุงเทพมหานครที่มีเครื่องคอมพิวเตอร์ที่ใช้งานในวันที่ 14 มกราคม พ.ศ. 2552 โดยกรมสอบสวนพิเศษ ในข้อหาว่าด้วยการหมิ่นพระบรมเดชานุภาพ ระหว่างที่ถูกฝากขังนายสุวิชาได้ขอประกันตัวสองครั้ง แต่คำร้องถูกยกทั้งสองครั้ง จนกระทั่งเมื่อวันที่ 26 มีนาคม พ.ศ. 2552 อัยการได้ส่งฟ้องศาลกล่าวหาว่ากระทำความผิดโดยการโพสต์รูปและข้อความลงบนอินเทอร์เน็ต โดยใช้นามแฝง 2 ชื่อ ทั้งนี้ อัยการ ระบุว่าผู้ต้องหาซึ่งถูกอัยการสั่งฟ้องกระทำความผิดโดยร่วมกับพวกที่หลบหนี หมิ่นประมาท ดูหมิ่น หรือแสดงความอาฆาตมาดร้าย พระมหากษัตริย์ พระราชินี รัชทายาท นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จโดยประการที่น่าจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ และเป็นข้อมูลคอมพิวเตอร์อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร นำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏภาพของผู้อื่น และภาพนั้นเป็นภาพที่ตัดต่อ เต็ม หรือตัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดโดยประการที่น่า จะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย อัยการขอให้ลงโทษตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 มาตรา 8 และ 9 ประมวลกฎหมายอาญา มาตรา 33, 83, 91 และ 112 และพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 3, 14 และ 16 จำเลยให้การรับสารภาพต่อศาลว่าตนได้กระทำความผิดตามข้อกล่าวหา

คดีตำรวจรวบมือโพสต์ข่าวลือที่ไม่เป็นมงคล¹⁰ กรณีที่มีการโพสต์ข่าวลือที่ไม่เป็นมงคลจนส่งผลให้ตลาดหลักทรัพย์แห่งประเทศไทย ได้รับความเสียหายอย่างรุนแรง เมื่อเดือนพฤศจิกายน พ.ศ. 2552 ตำรวจได้ทำการจับกุมนางธีรนันท์ วิภูษนันท์ ที่ปรึกษาผู้ลงทุน อดีตผู้บริหารบริษัทหลักทรัพย์ต่างชาติแห่งหนึ่ง ที่ลงนามบินสุวรรณภูมิ ขณะเดินทางกลับจากกรุงเวียนนา ประเทศออสเตรีย ทั้งนี้ เจ้าหน้าที่ได้ทำการสอบปากคำนางธีรนันท์ ประมาณ 30 นาที ก่อนจะแจ้งข้อหา นำเข้าข้อมูลคอมพิวเตอร์อันเป็นเท็จที่น่าจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน ในขณะที่นางธีรนันท์ กล่าวเพียงสั้นๆ ด้วยสีหน้ายิ้มแย้ม ไม่ได้มีความวิตกกังวลว่า ตนได้แปลข้อความจากเว็บไซต์สำนักข่าวต่างประเทศ เนื่องจากวันดังกล่าวหุ้นตกลงอย่างมากประชาชนอยากรู้ว่าเกิดจากอะไร ไม่มีเจตนาเผยแพร่ข้อความเพื่อ

⁹ ศรีศักดิ์ จามรมาน, สมิติใหม่แห่งการเรียนรู้ เอกสารประกอบการอบรมสำหรับสมาชิก NTU หลักสูตร การบริหารจัดการสมัยใหม่ เรื่อง ความผิดตามพ.ร.บ.คอมพิวเตอร์ ที่ทุกคนควรรู้อ่าน, หน้า 17-18.

¹⁰ หนังสือพิมพ์โพสต์ทูเดย์ (2 พฤศจิกายน 2552) : หน้า 1.

ทำให้หุนตก ทั้งนี้ ตำรวจได้ทำการยึดคอมพิวเตอร์โน้ตบุ๊ก กล้องดิจิทัล โทรศัพท์มือถือของนางธีรพันธ์ไว้ตรวจสอบ รวมถึงฮาร์ดดิสก์ เครื่องคอมพิวเตอร์ที่อยู่ในบ้านนางธีรพันธ์

ก่อนที่จะทำการจับกุมนางธีรพันธ์นั้นเจ้าหน้าที่ได้ทำการจับกุมนายครา ปาจาจิริยะพงษ์ พนักงานบริษัทเคที ซีมิโก้ ได้ที่บริษัทแห่งหนึ่ง ย่านถนนสีลม และเข้าตรวจค้นบ้านพักนายครา พบหลักฐานการโพสต์ข้อความดังกล่าว และได้เข้าตรวจค้นห้องคำหลักทรัพย์ของ บล.เคที ซีมิโก้ สาขาอาคารสินธร และทำการยึดฮาร์ดดิสก์ 1 ตัว โดยได้รับการเปิดเผยว่าบริษัทได้ทำการปฏิเสธว่าการกระทำดังกล่าวบริษัทไม่มีส่วนเกี่ยวข้องเพราะไม่มีนโยบายเช่นนั้น เป็นการดำเนินการส่วนตัวของเจ้าหน้าที่การตลาด ทั้งนี้ กรมสอบสวนคดีพิเศษจะดำเนินคดีกับสำนักข่าวต่างประเทศชื่อดังทางเศรษฐกิจสาขาฮ่องกง ซึ่งนำข่าวไม่เป็นมงคลออกมาเผยแพร่ เพราะถือเป็นส่วนหนึ่งของการกระทำความผิด การดำเนินการดังกล่าวถือว่าเป็นเรื่องละเอียดอ่อน เพราะเป็นสำนักข่าวต่างประเทศ และเกรงว่าจะกระทบกับประเทศไทย จึงต้องมีการพิจารณาให้รอบคอบ และรัดกุม โดยเฉพาะข้อกฎหมายที่ใช้ในการดำเนินการ

กรณีการล่อลวงเด็กผ่าน Chat Room¹¹ ปัจจุบันเยาวชนจำนวนหนึ่งนิยมใช้งานอินเทอร์เน็ตและหาเพื่อนในห้องสนทนาต่างๆ บนเครือข่าย การมองไม่เห็นหน้าตากันสามารถทำให้เยาวชนเชื่อใจคู่สนทนาที่มีลีลาในการชักจูงใจสูงได้ง่าย บ่อยครั้งที่อาชญากรในคราบของคู่สนทนาชักจูงเยาวชนให้หลงผิด หรือหลอกลวงเพื่อลักพาหรือล่อลวงละเมิดทางเพศ นอกจากนี้ยังมีเยาวชนอีกจำนวนหนึ่งที่ใช้อินเทอร์เน็ตเป็นสื่อในการหาคู่หลับนอนหรือการค้าประเวณี ต้องการสร้างประสบการณ์ทางเพศให้กับเด็ก หรือแม้แต่ทำในเชิงการค้าด้วยการร่วมเพศกับเด็ก แล้วถ่ายทอดสดออกทางอินเทอร์เน็ต ตามความต้องการของลูกค้าที่อยากดู บางการกระทำอาชญากรทำให้เหยื่อไว้เนื้อเชื่อใจยอมให้เข้าใกล้ เมื่อรู้จักกันแล้วคนเหล่านี้จะพยายามบังคับหลอกล่อให้เด็กแสดงท่าทางยั่ววนทางเว็บแคม โดยคนเหล่านี้จะมีวิธีในการบังคับให้เด็กทำกิจกรรมทางเพศ (Internet Sexual Coercion) นอกจากนี้ยังมีการทำสื่อลามกเด็กโดยไม่ใช้เด็กเป็นบุคคลจริง แต่เปลี่ยนไปใช้ตัวการ์ตูน ตัวอย่าง เช่น

¹¹ การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร, รายงานของประเทศไทย : การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร ประเทศไทย "การหมิ่นก่อกวนและการโต้ตอบ : การดำเนินกลยุทธ์ร่วมกันในการป้องกันอาชญากรรมและความยุติธรรมทางอาญา" หน้า 72-73.

คดีวัยโจ๋ดูเว็บโป๊จากร้านเน็ตแล้วสำเร็จความใคร่¹² มีรายงานจากเว็บไซต์ hillght.kapook.com เจ้าหน้าที่ฝ่ายสืบสวนได้นำกำลังเข้าจับกุมนายชาญวิทย์ สังข์ทอง อายุ 35 ปี เจ้าของร้านบีบีเน็ต เป็นตึกแถวชั้นเดียวภายในร้านแบ่งซอยเป็นห้องเล็กๆ ทั้งหมด 20 ห้อง โดยปล่อยให้เด็กวัยรุ่นเข้าไปสำเร็จความใคร่ โดยมีบริการอินเทอร์เน็ตและภาพลามกอนาจารซึ่งจะคิดค่าบริการชั่วโมงละ 20 บาท เมื่อสอบสวนนายชาญวิทย์ซึ่งเป็นเจ้าของร้าน เบื้องต้นให้การรับสารภาพว่าได้ปล่อยให้เด็กเกิดเหตุการณ์ลักษณะดังกล่าวมาเป็นระยะเวลา 3 เดือน ซึ่งเป็นที่นิยมของลูกค้าวัยรุ่นที่เข้ามาใช้บริการจำนวนมาก โดยมีรายได้ 2,500 บาท ต่อวัน เจ้าหน้าที่จึงได้แจ้งข้อหาความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก่อนส่งผู้ต้องหาให้พนักงานสอบสวน สถานีตำรวจนครบาลวังทองหลาง เพื่อดำเนินคดีตามกฎหมายต่อไป

กรณีการแอบอ้างตัวบุคคล¹³ เนื่องจากการทำธุรกรรมหรือติดต่อสื่อสารกันทางเครือข่าย ไม่จำเป็นต้องมีการแสดงหน้าตาเพียงแต่มีการพิสูจน์บุคคลด้วยข้อมูลบางอย่าง เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ หมายเลขบัตรประชาชน หมายเลขบัตรเครดิต ตัวอย่างคดี เช่น

คดีชาวไต้หวันโกงบัตรเอทีเอ็มโดยอ้างว่าเป็นการคืนเงินภาษี ที่ศาลอาญา ถ.รัชดาภิเษก วันที่ 3 มี.ค. 52 พนักงานสอบสวน สน.ชนะสงคราม นำตัวนายเซิน เชิง ฮวน หรืออาหมิง อายุ 30 ปี นายเซิง ซี หมิง หรือ ป่านชาย อายุ 22 ปี ทั้งสองเป็นชาวไต้หวัน และนายสุรพงศ์ แซ่หู อายุ 32 ปี ชาว จ.เชียงใหม่ 3 ผู้ต้องหาคดีโกงบัตรอิเล็กทรอนิกส์ การรับคืนเงินภาษี มายื่นคำร้องฝากขัง เนื่องจากต้องสอบปากคำพยานอีก 4 ปาก รอผลการตรวจประวัติผู้ต้องหา รอผลรอยพิมพ์นิ้วมือ และอื่นๆ

สืบเนื่องจากนาย เจย์ ลี (MR. JAY LI) ตำรวจสากลไต้หวันประจำประเทศไทย (Interpol) ได้เดินทางเข้าพบ พ.ต.อ.สุพิศาล ภักดีดินถนาถ รอง ผบก.ป. พ.ต.ท.สุรพงษ์ ไทยประเสริฐ รอง ผบก.2 บก.ป. เพื่อประสานข้อมูลแก๊งค์ต้มตุ๋นชาวไต้หวันร่วมกับคนไทยใช้กลวิธีหลอกเหยื่อว่าเป็นเจ้าหน้าที่สรรพากรจะคืนเงินภาษีผ่านระบบเอทีเอ็มแต่กลับขโมยเงินในบัญชีไป ทั้งนี้ กอง

¹² ศรศักดิ์ จามรนาน, สถิติใหม่แห่งการเรียนรู้ เอกสารประกอบการอบรมสำหรับสมาชิก NTU หลักสูตร การบริหารจัดการสมัยใหม่ เรื่อง ความผิดตามพ.ร.บ.คอมพิวเตอร์ ที่ทุกคนควรทราบ, หน้า 30.

¹³ การประชุมสนประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร, รายงานของประเทศไทย : การประชุมสนประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร ประเทศไทย "การฉีกก้ำกั้วและการโต้ตอบ : การดำเนินกลยุทธ์ร่วมกันในการป้องกันอาชญากรรมและความยุติธรรมทางอาญา", หน้า 73.

ปราบปรามได้มีการประสานข้อมูลกับตำรวจสากลได้วันประจำประเทศไทยเพื่อให้ช่วยตรวจสอบประวัติแก๊งอาชญากรชาวไต้หวันกลุ่มนี้ว่าเครือข่ายหรือวิธีการกระทำผิดอย่างไรบ้าง รวมถึงเส้นทางของเงินที่มีการเข้าออกของแก๊งอาชญากรกลุ่มนี้

ข้อมูลที่มีการประสานกันนั้นส่วนใหญ่เป็นข้อมูลทางเทคนิค และเบาแสบต่างๆในการสืบสวนหาตัวคนร้ายชาวไต้หวันรายอื่นๆที่คาดว่าอาจยังหลบหนีอยู่ในประเทศไทย ส่วนความคืบหน้าในการสอบสวนรวบรวมหลักฐานในคดีนี้ นั้น ยังมีผู้เสียหายทยอยเดินทางมาให้ข้อมูลอย่างต่อเนื่อง ซึ่งในขณะนี้พนักงานสอบสวนได้ตรวจสอบหมายเลขบัญชีธนาคารต่างๆของกลุ่มผู้ต้องหาไปแล้วทั้งหมด 44 บัญชี ก่อนจะส่งต่อให้ ตำรวจท้องที่ที่ยึดหลักฐานมาได้เพื่อดำเนินการขออายัดเงินในบัญชีต่อไป

หากผู้เสียหายรายใดพบว่าได้ออนเงินจากบัญชีตัวเองไปยังบัญชีปลายทางของกลุ่มผู้ต้องหาภายใน 44 บัญชีนี้ ทางตำรวจก็จะทำการอายัดเงินในบัญชีนั้นๆเพื่อขอคืนให้กับผู้เสียหาย

สำหรับผู้ต้องหาทั้ง 4 รายที่ถูกจับกุมตัวได้นั้น ได้แยกส่งตัวไปดำเนินคดีที่ สน.ปทุมวัน และ สน.ชนะสงคราม โดยพนักงานสอบสวนแต่ละท้องที่ได้นำตัวไปขออำนาจศาลฝากขังที่ศาลอาญาแล้ว โดยมีการคัดค้านการให้ประกันตัว ส่วนความคืบหน้าในการติดตามตัวผู้ร่วมขบวนการล่าสุดทางตำรวจได้พบผู้ต้องหาเพิ่มเติมเป็นหญิงชาวไทยอายุประมาณ 50 ปี มีหน้าที่คอยกว้านซื้อสำเนาบัตรประชาชนของชาวบ้านในราคารายละ 500 บาท เพื่อนำสำเนาดังกล่าวไปใช้เปิดบัญชีให้กับกลุ่มผู้ต้องหาซึ่งทางกองปราบปรามกำลังรวบรวมพยานหลักฐานเพื่อขออนุมัติหมายจับ

ข้อมูลเพิ่มเติมจากผู้เสียหายที่ตกเป็นเหยื่อแก๊งประเภทนี้นั้นพบว่า มีหลากหลายอาชีพ ตั้งแต่พ่อค้า พนักงานบริษัท ครู อาจารย์ พนักงานบัญชี ข้าราชการ ส่วนความเสียหายที่เกิดขึ้นนั้นมีตั้งแต่หลักพันบาทไปจนถึงเกือบล้านบาท อย่างไรก็ตามจากข้อมูลจากผู้เสียหายนำเข้ามาให้พนักงานสอบสวนกองปราบปรามนั้นส่วนใหญ่พบว่าบัญชีปลายทางที่เงินผู้เสียหายถูกโอนเข้าไปนั้นไม่ตรงกับบัญชีของกลุ่มผู้ต้องหา ตำรวจจึงเชื่อว่าน่าจะเป็นฝีมือของคนร้ายคนละกลุ่มกันแต่น่าจะมีความเชื่อมโยงถึงกันเพราะมีพฤติการณ์กระทำผิดลักษณะเดียวกัน

กรณีการแพร่กระจายไวรัสคอมพิวเตอร์และโค้ดอันตรายต่างๆหรือสิ่งอื่นที่มีลักษณะคล้ายกัน¹⁴ สามารถสร้างความเสียหายให้กับระบบคอมพิวเตอร์และเครือข่ายได้มาก อาทิ การทำลายหรือเปลี่ยนแปลงข้อมูลต่างๆบนระบบ การทำให้ระบบมีการทำงานเปลี่ยนไปหรือทำให้

¹⁴ เรื่องเดียวกัน, หน้า 73.

ระบบหยุดทำงาน และสามารถแพร่กระจายด้วยตัวเองผ่านทางอินเทอร์เน็ตได้อย่างรวดเร็วโดยอาศัยช่องโหว่ของระบบปฏิบัติการ หรือซอฟต์แวร์ต่างๆบนระบบ หรืออาศัยความรู้เท่าไม่ถึงการณ์ กรณีของผู้ใช้คอมพิวเตอร์ในการเปิดไฟล์ที่ได้รับจากอินเทอร์เน็ตโดยไม่ทำการตรวจสอบให้แน่ใจก่อนว่าปราศจากโค้ดอันตรายเหล่านี้หรือไม่ ถึงแม้จะมีการป้องกันทางด้านเทคนิคด้วยรูปแบบใหม่

ความผิดอื่นๆ เช่น การพนันและการขายของผิดกฎหมายบนอินเทอร์เน็ต การเปลี่ยนหน้าเว็บไซต์ การดักฟังข้อมูลบนเครือข่ายคอมพิวเตอร์ไร้สาย การส่งข้อมูลอีเมลขู่เหตุการณ์ก่อการร้าย และ Spam Mail รวมถึงการบุกรุกโจมตีระบบและการทำให้ระบบไม่สามารถทำงานได้ตามปกติ และปัญหาเด็กติดเกมที่นับวันจะยิ่งทวีความรุนแรงขึ้นเรื่อยๆ ในอดีตผู้ตกเป็นเหยื่อของเกมส่วนใหญ่จะเป็นผู้เล่นที่ได้รับผลกระทบทั้งทางด้านร่างกายและจิตใจ ฟุ่มเฟือย เหม่อลอย การเรียนตกต่ำ มีเพศสัมพันธ์ก่อนวัยอันควร แสดงความก้าวร้าวหรือมีพฤติกรรมเลียนแบบโดยใช้ความรุนแรง เช่น กรณีเด็กนักเรียน ม.6 ฆ่าคนขับรถแท็กซี่ตาย โดยวางแผนมาอย่างดี และอ้างว่าเลียนแบบเกมออนไลน์ ผลกระทบอันเนื่องมาจากเด็กติดเกม เช่น

คดี ดร.ตุนแซร์โฆษณาเว็บไซต์ปลอม¹⁵ มีรายงานจากเว็บไซต์มติชน ว่าเจ้าหน้าที่ตำรวจได้จับกุมนายธรรวัฒน์ เพิ่มโคตรทรัพย์ อายุ 45 ปี ตามหมายจับศาลจังหวัดอุดรธานี ที่ จ 381/2552 ลงวันที่ 27 กรกฎาคม 2552 โดยกล่าวหาว่าร่วมกันกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน โดยจับกุมได้ที่ปั้มน้ำมันไฮเวย์ จังหวัดนครราชสีมา ควบคุมตัวส่งพนักงานสอบสวน ผู้ต้องหาขอให้การปฏิเสธ

คดีนี้ นางสาวสาวิณี พิมศิริ พร้อมพวก 30 คน เข้าแจ้งความต่อเจ้าหน้าที่ตำรวจ สถานีตำรวจภูธรเมืองอุดรธานี กล่าวหาว่าถูกนายธรรวัฒน์ ผู้จัดการบริษัทบลูโอเซียน จำกัด สำนักงานจังหวัดอุดรธานี โฆษณาว่าจบปริญญาตรีวิทยาศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ปริญญาโท และปริญญาเอก มหาวิทยาลัยปทุมธานี หลอกให้นำเงินมาลงทุนเพื่อจะได้ผลกำไรมากกว่าสถาบันการเงิน โดยใช้การขายพื้นที่โฆษณาในเว็บไซต์ webinvester.com และเว็บไซต์ moh-art.com บังหน้า ผู้เสียหายหลงเชื่อจึงนำเงินไปสมัครเป็นสมาชิกรายละ 10,700-214,000 บาท ซึ่งผู้ลงทุนขั้นต่ำ จะได้รับเงินปันผล 20,000 บาทต่อปี เมื่อลงทุนปีแรกก็ไม่มีปัญหา ได้เงินปันผลตรงตามที่นายธรรวัฒน์บอก แต่พอเข้าปีที่ 2 เริ่มมีปัญหาไม่ได้เงินปันผลตามที่ตกลงกันได้

¹⁵ ศรศักดิ์ จามรมาน, สมมติใหม่แห่งการเรียนรู้ เอกสารประกอบการอบรมสำหรับสมาชิก NTU หลักสูตร การบริหารจัดการ สมัยใหม่ เรื่อง ความผิดตามพ.ร.บ.คอมพิวเตอร์ ที่ทุกคนควรรู้, หน้า 26.

สุดท้ายนายธราวัฒน์ก็ปิดสำนักงานหลบหนี จึงมาแจ้งความต่อเจ้าหน้าที่ตำรวจเพื่อให้จับกุม คดีนี้ถือว่าผู้ต้องหามีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 9

จากตัวอย่างสถานการณ์และปัญหาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ดังกล่าวที่จะเห็นได้ว่า ประเทศไทยประสบกับปัญหาอาชญากรรมทางคอมพิวเตอร์อย่างมากและหากผู้กระทำความผิดหรือเว็บไซต์นั้นอยู่นอกประเทศ บางครั้งรัฐทำได้เพียงแค่การปิดกั้นเนื้อหา แต่อย่างไรก็ตามเว็บไซต์เหล่านี้ก็ยังสามารถเข้าถึงได้หากผู้ที่ต้องการเข้าถึงใช้งานระบบที่มีตัวแทนในต่างประเทศเพื่อเล็ดรอดการปิดกั้นของรัฐ การจัดการกับปัญหาดังกล่าวจำเป็นต้องอาศัยความร่วมมือจากหลายฝ่าย และรัฐได้ดำเนินการทางด้านต่างๆ เพื่อป้องกันและแก้ไขปัญหาดังกล่าวไม่ว่าจะเป็นมิติด้านการปฏิบัติ ทั้งทางด้านนิติบัญญัติ ด้านบริหาร ด้านตุลาการ และทางด้านอื่นๆ ซึ่งต้องพิจารณาว่ามาตรการต่างๆ เหล่านี้สอดคล้องกับบทบัญญัติตามที่อนุสัญญากำหนดหรือไม่อย่างไร

4.2 มิติด้านนิติบัญญัติ

ประเทศไทยได้มีการวางแผนและจัดเตรียมความพร้อมเพื่อป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ทั้งทางด้านการบัญญัติแก้ไขเพิ่มเติมกฎหมายและจัดตั้งหน่วยงานต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายของประเทศชาติ ทั้งนี้ การเตรียมการทางด้านนิติบัญญัติก่อนการพิจารณาลงนามเข้าเป็นภาคีเป็นสิ่งสำคัญ และโดยเฉพาะหากการปฏิบัติตามพันธกรณีของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 นั้นอาจส่งผลกระทบต่อสิทธิของประชาชน ชัดแย้งต่อความคุ้มครองตามรัฐธรรมนูญ เป็นต้น ดังนั้นควรมีการทบทวนว่ามีกฎหมายส่วนใดบ้างที่จะมีผลต่อการปฏิบัติตามพันธกรณีของอนุสัญญา

มาตรการที่สำคัญและจำเป็นต่อการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ ได้แก่ การบัญญัติกฎหมายที่เกี่ยวข้องให้ทันสมัยและสามารถนำมาบังคับใช้ในโลกยุคเทคโนโลยีล้ำ สมัยในปัจจุบันได้ ประเทศไทยได้มีการบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศขึ้นมาใหม่และแก้ไขกฎหมายอื่นๆ ที่เกี่ยวข้องเพื่อสามารถนำมาบังคับใช้ได้เหมาะสม ซึ่งประเทศไทยมีกฎหมายภายในที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์โดยตรง และกฎหมายอื่นที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ หลายฉบับด้วยกัน เริ่มต้นจากการจัดทำกฎหมายเกี่ยวกับเทคโนโลยีสารสนเทศ จำนวน 5 ฉบับหลักๆ ตามนโยบายเทคโนโลยีสารสนเทศแห่งชาติ (ไอที 2000) ซึ่งอยู่ภายใต้ความรับผิดชอบของโครงการพัฒนากฎหมายเทคโนโลยี

สารสนเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ได้แก่ กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับความคุ้มครองข้อมูลส่วนบุคคล กฎหมายเกี่ยวกับการพัฒนาโครงสร้างพื้นฐานสารสนเทศ กฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ และกฎหมายภายในอื่นๆ ที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์¹⁶ ดังนี้

4.2.1 กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

กฎหมายฉบับนี้ได้บัญญัติเกี่ยวกับการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ ที่ผู้เขียนให้ความสำคัญในการศึกษาวิจัย เนื่องจากสามารถนำไปเทียบเคียงกับบทบัญญัติในอนุสัญญาในส่วนของข้อกำหนดฐานความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ รวมถึงอำนาจหน้าที่ในการสืบสวนสอบสวนคดีที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ดังนั้นผู้เขียนจะนำสาระสำคัญของกฎหมายฉบับนี้มาวิเคราะห์ว่ามีความสอดคล้องกับอนุสัญญาเพียงใดหรือไม่

ก. ความเป็นมาของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

กฎหมายฉบับนี้เรียกว่า "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550" ได้บัญญัติขึ้นเพื่อป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่อาจก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน* โดยคำนึงถึงกรอบและแนวทางตามอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 และกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของหลายประเทศ เช่น สหรัฐอเมริกา สหราชอาณาจักร เยอรมัน โดยได้มีการศึกษาทบทวนร่างกฎหมายมากกว่าหนึ่งฉบับเป็นเวลา

¹⁶ การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร, รายงานของประเทศไทย : การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร ประเทศไทย "การฝึกกำลังและการโต้ตอบ : การดำเนินกลยุทธ์ร่วมกันในการป้องกันอาชญากรรมและความยุติธรรมทางอาญา" หน้า 62.

* หมายเหตุ - เหตุผลในการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

หลายครั้งด้วยกัน¹⁷ จนในที่สุดกฎหมายฉบับนี้ได้มีการประกาศในราชกิจจานุเบกษา และมีผลบังคับใช้ตั้งแต่วันที่ 18 กรกฎาคม พ.ศ. 2550

เนื่องจากกฎหมายฉบับนี้ใช้เวลาในการเตรียมการนาน มีการประชุมรับฟังความคิดเห็นต่างๆมากมายได้รับการตอบรับที่ดีในแง่ของความจำเป็นที่จะต้องมียกกฎหมาย เพราะคนส่วนใหญ่ได้ทราบถึงพฤติกรรมหลายอย่างของการใช้คอมพิวเตอร์ที่ไม่พึงประสงค์ และอาจก่อให้เกิดความสูญเสียรุนแรงต่อความมั่นคงของประเทศหรือเกิดความเสียหายต่อผู้ถูกระทำ และที่สำคัญที่สุดคือเหตุการณ์ที่มีการใช้ระบบคอมพิวเตอร์ในการเผยแพร่ข้อความอันเป็นการหมิ่นพระบรมเดชานุภาพ ซึ่งสามารถแพร่หลายได้อย่างรวดเร็วและทั่วไป โดยการกระทำดังกล่าวนั้นยังไม่มีกฎหมายรองรับที่เพียงพอ หรือในบางกรณีไม่มีกฎหมายมารองรับ ทำให้หลายกรณีที่เกิดขึ้นไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้ หลักการสำคัญที่ใช้ในการยกร่างกฎหมาย และการพิจารณาในทุกขั้นตอนคือ “หลักความเป็นกลางทางเทคโนโลยี” (Technology Neutral)¹⁸ ทั้งนี้เพื่อให้กฎหมายที่จัดทำขึ้นสามารถใช้บังคับได้กับเทคโนโลยีในหลากหลายรูปแบบ ไม่ได้อ้างอิงเฉพาะเทคโนโลยีประเภทใดประเภทหนึ่ง จึงถือว่ามีคามทันสมัยและสามารถปรับใช้กับเทคโนโลยีใหม่ เช่น การกระทำความผิดผ่านโทรศัพท์มือถือ หรืออุปกรณ์อื่นใดที่สามารถทำงานได้อย่างเครื่องคอมพิวเตอร์

ข. ขอบเขตและวัตถุประสงค์ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นี้ นอกจากจะมีบทกำหนดโทษความผิดทางอาญาซึ่งเป็นกฎหมายในสวนสารบัญญัติแล้ว ยังมีบทบัญญัติเกี่ยวกับวิธีการสืบสวนสอบสวนคดีโดยพนักงานเจ้าหน้าที่และการดำเนินคดีกับผู้กระทำความผิดซึ่งเป็นกฎหมายวิธีสบัญญัติเพื่อให้สามารถดำเนินการป้องกันและปราบปรามผู้กระทำความผิดตามวัตถุประสงค์ของพระราชบัญญัติ

ค. หลักการและสาระสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

¹⁷ การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร, รายงานของประเทศไทย : การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร ประเทศไทย “การรณรงค์กำลังและการโต้ตอบ : การดำเนินกลยุทธ์ร่วมกันในการป้องกันอาชญากรรมและความยุติธรรมทางอาญา”, หน้า 63.

¹⁸ เรื่องเดียวกัน, หน้า 63.

เดิมที่ยังไม่มีการกำหนดคำนิยามเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์อย่างเป็นทางการ โดยส่วนใหญ่เป็นการกำหนดคำนิยามโดยนักกฎหมาย นักวิทยาศาสตร์ และ นักคอมพิวเตอร์ศาสตร์ ซึ่งก็เป็นการกำหนดคำนิยามที่เป็นการทั่วไปตามลักษณะของการกระทำ ความผิด ดังนั้น เมื่อมีการบัญญัติกฎหมายดังกล่าวจึงได้มีการกำหนดคำนิยามความหมาย รวมถึงคำจำกัดความไว้ รวมถึงการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ว่าจะมีหลักเกณฑ์ในการ จัดเก็บอย่างไรบ้าง เพื่อให้สอดคล้องกับหลักการที่อนุสัญญาได้บัญญัติให้คำนี้ถึง เช่น หลักการ ค้ำครองสิทธิส่วนบุคคลและเสรีภาพขั้นพื้นฐานในการติดต่อสื่อสารผู้เขียนจะกล่าวในส่วนต่อไป รวมถึงประเด็นที่ประเทศไทยควรมีหลักการคุ้มครองข้อมูลส่วนบุคคลเช่นประเทศภาคีอื่น ของอนุสัญญาหรือไม่ ดังนี้

1. ความหมายและคำจำกัดความ

เมื่อพิจารณาความหมายและคำจำกัดความของระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ และผู้ให้บริการ ตามนิยามที่ระบุไว้ใน อนุสัญญาซึ่งผู้เขียนได้กล่าวถึงในบทที่ 2 แล้วนั้น จะเห็นได้ว่ากฎหมายของไทยคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ให้บทนิยามศัพท์ เกี่ยวกับระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ และผู้ให้บริการ ที่มีความหมายใกล้เคียงกับนิยามของอนุสัญญา ได้แก่

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อม การทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงาน ให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ (มาตรา 3) ทั้งนี้ ยังรวมถึง อุปกรณ์รอบข้างต่างๆ ในการนำเข้าข้อมูล แสดงผลข้อมูล และบันทึกข้อมูล ระบบคอมพิวเตอร์ จึงอาจเป็นเพียงเครื่องเดียว หรือหลายเครื่องที่มีลักษณะเชื่อมต่อกัน โดยอาจเชื่อมต่อผ่านระบบ เครือข่ายให้มีการทำงานโดยอัตโนมัติตามโปรแกรมที่ตั้งไว้ ดังนั้น เครื่องคอมพิวเตอร์ที่ชื่อมายัง ไม่ถือว่าเป็นระบบคอมพิวเตอร์ จนกว่าจะได้มีการทำงานผ่านระบบเครือข่ายหรือโดยคำสั่งหรือ ชุดคำสั่ง¹⁹

ข้อมูลคอมพิวเตอร์ หมายถึงข้อมูลทุกอย่างที่อยู่ในระบบคอมพิวเตอร์ ไม่ว่าจะเป็น ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบ

¹⁹ พรเพชร วิชิตชลชัย, โปบุลย์ อมรภิญโญเกียรติ และนิเวศน์ อากาศิน, เอกสารประกอบการบรรยายพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550, (ม.ป.ท. : ม.ป.ท.,2550), หน้า 4.

คอมพิวเตอร์อาจประมวลผลได้ (มาตรา 3) นอกจากนั้นยังให้รวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย*

ความจริงแล้วคำว่า ข้อมูลอิเล็กทรอนิกส์ ย่อมอยู่ในความหมายของ ข้อมูลคอมพิวเตอร์อยู่แล้ว แต่การที่กฎหมายกำหนดเช่นนี้อาจเพื่อให้มีความครอบคลุมถึงข้อมูลประเภทอื่นๆที่อาจสร้างด้วยวิธีการทางอิเล็กทรอนิกส์อื่นๆในอนาคต ที่ไม่ใช่คอมพิวเตอร์ก็อาจเป็นได้ ทั้งนี้ในกรณีของโทรเลข โทรพิมพ์ โทรสารดังกล่าวหากจะเป็นความผิดอาจต้องพิจารณาว่ามีความเชื่อมโยงกับระบบคอมพิวเตอร์หรือไม่ตามองค์ประกอบความผิดฐานนั้นๆ คำนิยามตามบทบัญญัติในส่วนนี้ ได้บัญญัตินิยามของคำว่าข้อมูลคอมพิวเตอร์ไว้แคบกว่าบทบัญญัติของอนุสัญญา เนื่องจากข้อมูลคอมพิวเตอร์ตามพระราชบัญญัตินี้ หมายถึงข้อมูลที่อยู่ในระบบคอมพิวเตอร์แล้วทุกอย่าง แต่ในส่วนของอนุสัญญานั้นสามารถรวมถึงสิ่งที่อยู่ภายนอกระบบคอมพิวเตอร์ ซึ่งเป็นสิ่งที่ใช้แสดงออกข้อเท็จจริง ข้อมูลหรือความคิด ในรูปแบบที่เหมาะสมจะใช้ในการประมวลผลลงในระบบคอมพิวเตอร์ เช่น ข้อมูลที่มีการเตรียมไว้ในกระดาษก่อนที่จะมีการบันทึกลงในระบบคอมพิวเตอร์เพื่อประมวลผล

ข้อมูลจราจรทางคอมพิวเตอร์ (มาตรา 3) หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงรายการให้เห็นถึงการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ แสดงถึงแหล่งกำเนิด เช่น หมายเลขของเครื่อง ทั้งเครื่องต้นทาง และปลายทาง เส้นทาง การติดต่อสื่อสาร วันเวลาของการส่งข้อมูล ปริมาณ ระยะเวลา ชนิดของการบริการ หรืออื่นๆที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ไม่ว่าจะ เป็นชื่อที่อยู่ของผู้ใช้บริการ กรณีที่เป็นบริการที่มีการลงทะเบียน ข้อมูลของผู้ให้บริการเอง ลักษณะของการให้บริการว่าผ่านระบบหรือเครือข่ายใด และข้อมูลทุกประเภทเกิดจากการสื่อสารผ่านระบบคอมพิวเตอร์ เนื่องจากข้อมูลดังกล่าวนี้มีความสำคัญ

ผู้ให้บริการ หมายถึง ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น (มาตรา 3) และกฎหมายยังได้กำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลคอมพิวเตอร์ที่ผู้ให้บริการได้ใช้ผ่านระบบคอมพิวเตอร์ของตน (มาตรา 25) ในพระราชบัญญัติฉบับนี้ได้กำหนดให้ผู้ให้บริการ

* พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, มาตรา 4 ... "ข้อมูลอิเล็กทรอนิกส์" หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร...

หน้าที่ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นไปในทิศทางเดียวกัน ทำให้หลายองค์กรทั้งภาครัฐและเอกชนต้องมีการปรับตัวครั้งใหญ่ โดยองค์กรแต่ละองค์กรมีลักษณะการใช้งานสารสนเทศแตกต่างกัน การเก็บรักษาข้อมูลจราจรที่มีลักษณะที่ถูกต้องเหมาะสมตามลักษณะการใช้งานระบบสารสนเทศ หรือระบบอินเทอร์เน็ตของแต่ละองค์กรที่มีความแตกต่างกันค่อนข้างมาก ไม่ว่าจะเป็นร้านอินเทอร์เน็ตคาเฟ่ที่มีอยู่อย่างมากมายในประเทศไทย อย่างไรก็ตามผู้เขียนเห็นว่าข้อควรพิจารณาประการหนึ่งสำหรับภาครัฐในการออกคำสั่งให้เก็บรักษาข้อมูลดังกล่าว เกี่ยวกับค่าใช้จ่ายในการเก็บข้อมูลที่เกิดขึ้นจากการเก็บรักษาข้อมูลซึ่งล้วนเป็นค่าใช้จ่ายของผู้ให้บริการทั้งสิ้น

ผู้ให้บริการ (มาตรา 3) ในส่วนนี้อนุสัญญาไม่ได้กล่าวถึง แต่ในพระราชบัญญัตินี้ ได้ให้คำนิยามหมายความถึงผู้ให้บริการของผู้ให้บริการทุกประเภทไม่ว่าจะเสียค่าใช้จ่ายหรือไม่ก็ตาม เช่น ผู้ให้บริการอินเทอร์เน็ตของ Hotmail หรือ Yahoo

พนักงานเจ้าหน้าที่ (มาตรา 3) หมายถึงผู้ที่มีอำนาจหน้าที่ในการสืบสวนสอบสวน การกระทำความผิดตามพระราชบัญญัตินี้ ซึ่งต้องเป็นผู้ที่มีความรู้และความเชี่ยวชาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด และต้องเป็นผู้ที่ถูกแต่งตั้งโดยรัฐมนตรี เนื่องจากพระราชบัญญัตินี้เป็นกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะ จึงได้บัญญัติให้มีพนักงานเจ้าหน้าที่ ที่ดำรงตำแหน่งในวาระคราวละ 4 ปี* เพื่อให้มีอำนาจหน้าที่ในการดำเนินการเกี่ยวกับการสืบสวนสอบสวนในเรื่องพยานหลักฐานจากระบบคอมพิวเตอร์เป็นสำคัญ อำนาจหน้าที่ที่เพิ่มเติมขึ้นนี้ผู้เขียนได้อธิบายไว้ในส่วนถัดไปเกี่ยวกับ คุณสมบัติเกี่ยวกับพนักงานเจ้าหน้าที่ซึ่งเป็นคุณสมบัติที่กฎหมายกำหนดไว้ค่อนข้างกว้างคือ เพียงแต่มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์ก็เพียงพอ

เนื่องจากการดำเนินการเกี่ยวกับมาตรการสืบสวนสอบสวนที่กำหนดไว้ในอนุสัญญาได้กำหนดให้มีหน่วยงานที่มีอำนาจหน้าที่โดยเฉพาะในการสืบสวนสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ วิธีการในการดำเนินการดังกล่าวจำเป็นต้องอาศัยความรู้ความสามารถในเรื่องของเทคโนโลยีและคอมพิวเตอร์ที่เพียงพอและสามารถดำเนินการอย่างรวดเร็วและมีประสิทธิภาพ และการกำหนดคุณสมบัติเบื้องต้นให้มีความรู้เกี่ยวกับสาขาวิชาที่มีความเกี่ยวข้องกับทั้งทางกฎหมายและคอมพิวเตอร์ถือได้ว่าเป็นการส่งเสริมและสนับสนุนให้มีการ

* ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2552, ข้อ 4

ดำเนินการและเป็นการสร้างความเชื่อมั่นว่าประเทศไทยจะสามารถดำเนินการเกี่ยวกับการสืบสวนสอบสวนและให้ความร่วมมือได้อย่างรวดเร็วและมีประสิทธิภาพ

รัฐมนตรี (มาตรา 3) หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้ ซึ่งได้แก่รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร มีอำนาจรักษาการและออกกฎกระทรวง (มาตรา 4) นอกจากนั้นยังมีอำนาจหน้าที่ในการให้ความเห็นชอบในการยื่นคำร้องต่อศาลเพื่อให้ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ (มาตรา 20) กำหนดเรื่องชุดคำสั่งไม่พึงประสงค์ (มาตรา 21) ประกาศหลักเกณฑ์เกี่ยวกับผู้ให้บริการที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (มาตรา 26) กำหนดคุณสมบัติของพนักงานเจ้าหน้าที่ (มาตรา 28) กำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ โดยร่วมกับนายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติ (มาตรา 29) และกำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่ (มาตรา 30)

2. มาตรการทางด้านสารบัญญัติ

เนื่องจากอนุสัญญาได้กำหนดให้ประเทศภาคีทำการกำหนดให้อาชญากรรมทางคอมพิวเตอร์เป็นความผิดทางอาญาตามกฎหมายภายในประเทศให้สอดคล้องกันเพื่อให้สามารถดำเนินคดีกับผู้กระทำความผิดได้อย่างมีประสิทธิภาพ ดังนั้น ผู้เขียนจึงได้ศึกษาและวิเคราะห์ถึงฐานความผิดในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มีการกำหนดฐานความผิดและบทลงโทษไว้ตั้งแต่มาตรา 5 ถึงมาตรา 16 โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มิได้ทำการแบ่งแยกเป้าหมายของการกระทำความผิดตามอนุสัญญาแต่ได้บัญญัติให้การกระทำที่เป็นความผิดทั้งหมดดังต่อไปนี้ เป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

1. การเข้าถึงโดยไม่ชอบ แบ่งออกเป็น 2 ฐานความผิด คือการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) และการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) หมายถึงลักษณะการกระทำความผิด ดังนี้

การเข้าถึง กฎหมายได้กำหนดองค์ประกอบความผิดตามเอกสารการชี้แจงของสำนักงานเลขาธิการคณะกรรมการคุ้มครองสิทธิเสรีภาพ ซึ่งใช้อธิบายประกอบเสนอร่างกฎหมายต่อคณะกรรมการวิสามัญพิจารณาร่างพระราชบัญญัตินี้ ให้ความหมายไว้ว่า การเข้าถึง ตรงกับภาษาอังกฤษว่า Access หมายถึง การเข้าถึงทั้งในระดับกายภาพ เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ และผู้กระทำความผิดดำเนินการ

ด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั่นเอง และหมายความรวมถึงการเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์ แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างไกลโดยระยะทางภูมิศาสตร์กับเครื่องคอมพิวเตอร์แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้

นอกจากนั้นยังหมายถึง การเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้นจึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่างๆของคอมพิวเตอร์ ข้อมูลที่ถูกบันทึกไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น

ส่วนวิธีการเข้าถึงนั้นรวมทุกวิธีการไม่ว่าจะเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตอันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆ เครือข่ายเข้าด้วยกัน และยังหมายความถึงการเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN อันเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆ เข้าด้วยกัน นอกจากนี้ยังหมายความรวมถึงการเข้าถึงโดยการติดต่อสื่อสารแบบไร้สายอีกด้วย

การเข้าถึงดังกล่าวต้องเป็นการกระทำโดยมิชอบ ซึ่งองค์ประกอบความผิดนี้มีใช้อยู่ในประมวลกฎหมายอาญาในเรื่องความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ความหมายที่เข้าใจกันคือการเข้าถึงที่ถือว่าเป็นความผิดฐานนี้ จะต้องเป็นการเข้าถึงโดยปราศจากสิทธิโดยชอบธรรมด้วย แต่หากว่าผู้ทำการเข้าถึงนั้นเป็นบุคคลที่มีสิทธิเข้าถึงไม่ว่าด้วยถือสิทธิตามกฎหมายหรือได้รับอนุญาตจากเจ้าของระบบ ตัวอย่างเช่น การเข้าถึงเพื่อดูแลระบบของผู้ดูแลเว็บไซต์ อย่างไรก็ตาม หากผู้ได้รับอนุญาตให้ทำการเข้าถึงนั้นได้เข้าถึงระบบหรือข้อมูลคอมพิวเตอร์เกินกว่าที่ตนได้รับอนุญาต ในกรณีนี้บุคคลดังกล่าวก็ย่อมต้องรับผิดชอบเช่นเดียวกัน ทั้งนี้ คำว่า โดยมิชอบจึงอาจเทียบเคียงได้กับคำว่า ปราศจากสิทธิโดยชอบธรรม หรือ ไม่มีอำนาจในการเข้าถึง

การเข้าถึงดังกล่าวต้องเป็นการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามคำนิยามศัพท์ในมาตรา 3 และผู้เขียนได้อธิบายไว้ข้างต้นแล้ว แต่ทั้งนี้ ตามเจตนารมณ์ของกฎหมาย ข้อมูลคอมพิวเตอร์ที่จะได้รับความคุ้มครองตามมาตรานี้ย่อมหมายถึงข้อมูลที่มีการเก็บหรือส่งด้วยวิธีการทางคอมพิวเตอร์หรือวิธีการทางอิเล็กทรอนิกส์ ดังนั้นจึงไม่น่าจะหมายความรวมถึงข้อมูลที่บรรจุไว้ในแผ่นซีดี หรือแผ่นดิสก์ อย่างไรก็ตามหากมีการนำแผ่นซีดี หรือแผ่นดิสก์ดังกล่าวมาเล่นผ่านระบบคอมพิวเตอร์ก็จะอยู่ในความหมายของข้อมูลคอมพิวเตอร์ตามกฎหมายนี้ทันที

ซึ่งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่มีการเข้าถึงนั้นต้องเป็นระบบที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะ ผู้เขียนเห็นว่าระบบคอมพิวเตอร์ใดเป็นระบบที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะอาจเป็นข้อเท็จจริงที่จะต้องนำสืบเป็นเรื่องๆไป เนื่องจากมีระบบคอมพิวเตอร์จำนวนมากที่เจ้าของไม่ได้วางแผนการที่บุคคลใดจะเข้าถึง

ถึงแม้การกระทำของผู้กระทำจะครบองค์ประกอบความผิดในส่วนที่เป็นการกระทำก็ยังคงต้องการองค์ประกอบทางจิตใจคือ ผู้กระทำต้องมีเจตนาตามประมวลกฎหมายอาญา มาตรา 59 ด้วย ทั้งนี้ การกระทำความผิดโดยฝ่าฝืนต่อบทบัญญัติแห่งมาตรานี้ อาจเกิดขึ้นหลายวิธี เช่น การเจาะระบบ หรือการบุกรุกทางคอมพิวเตอร์ ซึ่งการกระทำเช่นนี้เป็นการขัดขวางการใช้ระบบคอมพิวเตอร์โดยชอบของบุคคลอื่นอันอาจทำให้เกิดการเปลี่ยนแปลงแก้ไข หรือทำงานระบบคอมพิวเตอร์ได้โดยปกติความผิดฐานนี้จะเป็นที่มาของการกระทำความผิดฐานต่อไป เช่นการใช้คอมพิวเตอร์เพื่อประกอบอาชญากรรมอื่น หรือเพื่อกระทำความผิดฐานอื่นตามบทบัญญัติมาตราต่อไปในพระราชบัญญัติ

2. การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ (มาตรา 6) มีลักษณะการกระทำความผิด ดังนี้ การกระทำที่เป็นการล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ หมายความว่า ระบบคอมพิวเตอร์ดังกล่าวนั้นมีมาตรการป้องกันการเข้าถึง เช่น มีการลงทะเบียน หรือมีวิธีการอื่นใดที่จัดทำขึ้นเป็นการเฉพาะ ซึ่งการล่วงรู้ที่เป็นความผิดตามมาตรานี้จะต้องเป็นเรื่องที่ผู้กระทำล่วงรู้ ซึ่งการล่วงรู้นั้นจะได้มาโดยชอบหรือไม่ชอบก็ได้

เมื่อล่วงรู้มาตรการดังกล่าวแล้วหากมีการเปิดเผยโดยมิชอบ คือ เพียงแค่นำมาตรการนั้นมาเปิดเผยแก่ผู้หนึ่งผู้ใด หรือหลายคนก็เป็นความผิดแล้ว เมื่อเปิดเผยแล้วผู้หนึ่งผู้ใดนั้นจะทราบหรือนำไปใช้หรือไม่ ไม่สำคัญ ซึ่งการเปิดเผยดังกล่าวต้องพิจารณาด้วยว่าการเปิดเผยมาตรการนั้น น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือไม่ หากเป็นเรื่องที่ไม่น่าจะเกิดความเสียหายแก่ผู้ใดก็ไม่เป็นความผิด

ทั้งนี้ ผู้กระทำต้องมีเจตนาในการกระทำความผิด หากผู้กระทำความผิดไม่มีเจตนาย่อมไม่มีความผิด เช่น การกระทำดังกล่าวเกิดจากความประมาททำให้มีการเปิดเผยมาตรการการเข้าถึงย่อมไม่มีความผิด

3. การดักจับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 8) วัตถุประสงค์ของมาตรานี้เพื่อคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสารดังเช่นที่กำหนดในอนุสัญญา

ทำนองเดียวกับความคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสารรูปแบบที่ห้ามดักฟังหรือแอบบันทึกการสนทนาทางโทรศัพท์ มีลักษณะการกระทำความผิด ดังนี้

กระทำการด้วยประการใดด้วยวิธีทางอิเล็กทรอนิกส์เพื่อดักจับไว้ ตามคำอธิบายของเนคเทคประกอบการเสนอร่างกฎหมายได้ให้ความหมายของการดักจับข้อมูลตามมาตรานี้ หมายถึง การดักจับโดยวิธีทางเทคนิค เพื่อลักลอบดักฟัง ตรวจสอบ หรือติดตามเนื้อหาสาระของข่าวสาร สื่อสารกันระหว่างบุคคล หรือเป็นการกระทำเพื่อให้ได้มาซึ่งเนื้อหาข้อมูลโดยตรงหรือโดยการเข้าถึง และใช้ระบบคอมพิวเตอร์ หรือการทำให้ได้มาซึ่งเนื้อหาของข้อมูลโดยทางอ้อม ด้วยวิธีการแอบบันทึกข้อมูลที่สื่อสารถึงกันด้วยอุปกรณ์อิเล็กทรอนิกส์ โดยไม่คำนึงว่าอุปกรณ์อิเล็กทรอนิกส์ที่ใช้บันทึกข้อมูลดังกล่าวจะต้องเชื่อมต่อเข้ากับสายสัญญาณสำหรับส่งผ่านข้อมูลหรือไม่ เพราะบางทีกรณีอาจใช้อุปกรณ์เช่นว่านั้นเพื่อทำการบันทึกการสื่อสารข้อมูลที่ได้ส่งผ่านด้วยวิธีการแบบไร้สายก็ได้ เช่น การติดต่อผ่านโทรศัพท์เคลื่อนที่ การติดต่อสื่อสารโดยใช้เทคโนโลยีไร้สาย เป็นต้น ซึ่งนอกจากการใช้อุปกรณ์อิเล็กทรอนิกส์เพื่อบันทึกข้อมูลที่มีการส่งผ่านกันแล้ว ยังรวมถึงกรณีการใช้ซอฟต์แวร์ หรือรหัสผ่านต่างๆ เพื่อทำการแอบบันทึกข้อมูลที่ส่งผ่านกันด้วย²⁰

ข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ หมายถึง การดักจับข้อมูลคอมพิวเตอร์ของผู้อื่นนี้จะต้องเป็นข้อมูลที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะ หรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ ซึ่งการที่จะพิจารณาว่าข้อมูลคอมพิวเตอร์ดังกล่าวมีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้หรือไม่นั้น อาจต้องพิจารณาจากข้อเท็จจริงว่าลักษณะการส่งข้อมูลคอมพิวเตอร์ดังกล่าวนั้นผู้ส่งต้องการให้เป็นเรื่องเฉพาะตน ไม่ได้ต้องการให้เปิดเผยข้อมูลนั้นแก่บุคคลใด การพิจารณาว่าข้อมูลคอมพิวเตอร์ใดมีไว้เพื่อประโยชน์สาธารณะจึงต้องพิจารณาจากการที่ข้อมูลนั้นมีการเข้ารหัสการเข้าถึงข้อมูลนั้นหรือไม่

ดังนั้นจึงไม่ใช่เรื่องที่จะพิจารณาจากเนื้อหาของข้อมูลว่าเป็นความลับหรือไม่²¹ เช่น เนื้อหาข้อมูลอาจเป็นความลับทางการค้า แต่หากผู้ส่งใช้วิธีการส่งที่ไม่ได้มีมาตรการป้องกันการเข้าถึงข้อมูลนั้น ผู้ที่ดักจับย่อมไม่มีความผิด ทั้งนี้ ยังต้องคำนึงถึงข้อมูลส่วนบุคคลซึ่งผู้เขียนจะได้อธิบายต่อไป

²⁰ พรเพชร วิชิตชลชัย, คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, หน้า 13.

การดักจับข้อมูลดังกล่าวต้องเป็นการกระทำโดยมิชอบ กระทำไปโดยที่ไม่มีอำนาจกระทำ ดังนั้น ถ้าผู้กระทำมีอำนาจกระทำได้ไม่ว่าโดยกฎหมายหรือ โดยการอนุญาตของเจ้าของสิทธิ ผู้กระทำย่อมไม่มีความผิด และต้องมีเจตนาในการกระทำความผิด

4. การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์ โดยมิชอบ ความผิดตามมาตรา ๓๓ หมายถึงการกระทำที่เป็นการรบกวนข้อมูลคอมพิวเตอร์ของผู้อื่น โดยไม่ชอบ ซึ่งมีลักษณะการกระทำความผิด ดังนี้ ต้องมีกระทำการอันเป็นการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมโดยมิชอบ องค์ประกอบในข้อนี้ใช้ถ้อยคำซึ่งเป็นองค์ประกอบความผิดฐานทำให้เสียหายตามประมวลกฎหมายอาญา มาตรา ๓๕๘ คือคำว่า ทำให้เสียหาย และทำลาย แต่ในส่วนที่เกี่ยวกับการปลอมนั้น มาตรา ๓๓ ไม่ได้ยกองค์ประกอบของความผิดฐานปลอมเอกสารมา แต่เขียนองค์ประกอบให้ชัดเจนว่าเป็นการแก้ไข เปลี่ยนแปลง เพิ่มเติม ซึ่งเป็นคำสามัญที่เข้าใจได้แน่นอนว่าต้องคงองค์ประกอบความผิดในเรื่อง โดยมิชอบ ไว้เสมอ เพราะมีกรณีจำนวนมากที่ผู้กระทำมีอำนาจและสิทธิที่จะเข้าไปแก้ไขข้อมูลคอมพิวเตอร์ได้

การทำให้ข้อมูลคอมพิวเตอร์ของผู้อื่นเกิดความเสียหาย ความหมายของข้อมูลคอมพิวเตอร์ เป็นไปตามนิยามศัพท์ และจะเป็นความผิดตามมาตรา ๓๓ ต้องเป็นข้อมูลคอมพิวเตอร์ของผู้อื่น โดยต้องกระทำโดยเจตนา เนื่องจากกฎหมายมุ่งประสงค์ที่จะคุ้มครองความถูกต้องของข้อมูล ความถูกต้องแท้จริง และเสถียรภาพ หรือความพร้อมในการใช้งาน หรือการใช้ข้อมูลคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ที่บันทึกเก็บไว้บนสื่อคอมพิวเตอร์ ได้อย่างเป็นปกติ จึงเป็นการกำหนดขึ้นเพื่อให้ข้อมูลคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ได้รับความคุ้มครอง เช่นเดียวกับสิ่งของที่สามารถจับต้องได้

การกระทำความผิดดังกล่าวกระทำโดยบุคคลที่มีสิทธิโดยชอบก็ไม่ใช่ความผิด เช่น การเปลี่ยนแปลงข้อมูลจราจรทางคอมพิวเตอร์เพื่อประโยชน์ในการสื่อสารแบบไม่ระบุชื่อ การเปลี่ยนแปลงข้อมูลเพื่อการรักษาความลับและความปลอดภัยของการสื่อสาร การเข้ารหัสข้อมูล เป็นต้น

5. การกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ (มาตรา ๓๔) ความผิดตามมาตรา ๓๔ มีวัตถุประสงค์และองค์ประกอบความผิด คล้ายคลึงกับมาตรา ๓๓ เพียงแค่เปลี่ยนวัตถุที่ถูกกระทำจาก ข้อมูลคอมพิวเตอร์ เป็น ระบบคอมพิวเตอร์ ซึ่งมีลักษณะการกระทำความผิด ดังนี้ กระทำด้วยประการใดโดยมิชอบ จากนิยามที่มีการใช้ข้อความดังกล่าวนี้มีความหมายกว้างมาก แต่เนื่องจากกฎหมายฉบับนี้เป็นกฎหมายเฉพาะที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ดังนั้น ผู้เขียนจึงเห็นควรหมายถึงการกระทำที่

เป็นการเข้าไปทำกับระบบคอมพิวเตอร์ หรือจะหมายถึงการกระทำทางกายภาพอื่นๆ เช่น การระเบิด การวินาศกรรมเพื่อให้มีผลทำลายการทำงานของระบบคอมพิวเตอร์ด้วย เท่าที่มีการอภิปรายกันในที่ประชุมของคณะกรรมการเป็นไปในทิศทางเดียวกันที่จะขยายผลให้รวมถึง การกระทำทางกายภาพที่เข้าไปยุ่งเกี่ยวกับระบบคอมพิวเตอร์ด้วย หากการกระทำดังกล่าวผู้กระทำทำไปโดยมีอำนาจ หรือมีสิทธิโดยชอบธรรม ย่อมไม่เป็นความผิดตามมาตรา 11 เช่น การทดสอบ หรือรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์โดยบุคคลที่ได้รับมอบอำนาจจากผู้เป็นเจ้าของระบบคอมพิวเตอร์ หรือผู้ปฏิบัติการ หรือการปรับแก้ระบบปฏิบัติการของคอมพิวเตอร์ โดยผู้ปฏิบัติการก่อนทำการติดตั้งซอฟต์แวร์ใหม่ เช่น การติดตั้งซอฟต์แวร์เพื่อทำการเชื่อมต่อกับ อินเทอร์เน็ตซึ่งจะมีผลให้ระบบคอมพิวเตอร์ทำงานไม่เป็นปกติทั้งก่อนและหลังการติดตั้งโปรแกรม

การกระทำดังกล่าวต้องมีเจตนาเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติ ซึ่งอาจต้องพิจารณาจากข้อเท็จจริงที่ผู้กระทำได้กระทำไปตามหลัก กรรมเป็นเครื่องชี้เจตนา

กรณีที่มีการกระทำดังกล่าวต้องทำจนกระทั่งไม่สามารถทำงานได้ตามปกติ หมายถึง กระทำถึงขนาดที่ระบบคอมพิวเตอร์ทำงานได้ไม่สมบูรณ์ ดังนั้น แม้ว่าระบบคอมพิวเตอร์จะสามารถทำงานได้ แต่เป็นการทำงานที่ไม่สมบูรณ์ หรือผิดปกติไป ก็ย่อมต้องตกอยู่ภายใต้ความหมายขององค์ประกอบความผิดตามมาตรา 11

6. การส่งข้อมูลคอมพิวเตอร์รบกวนการใช้งานระบบคอมพิวเตอร์ของบุคคลอื่น โดยปกติสุข (มาตรา 11) ความผิดตามมาตรา 11 คณะกรรมการได้เพิ่มเติมขึ้นมาใหม่เป็นการบัญญัติเอาผิดแก่การกระทำที่ไม่ถึงกับทำให้ระบบคอมพิวเตอร์ของบุคคลอื่นไม่สามารถทำงานได้ตามปกติ แต่เป็นการกระทำที่ทำให้เกิดการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข เช่น การส่งจดหมายอิเล็กทรอนิกส์ มากจนล้นระบบคอมพิวเตอร์ทำให้เกิดความยุ่งยากในการใช้งานระบบคอมพิวเตอร์ หรือที่เรียกกันว่า Spam Mail ซึ่งลักษณะการกระทำผิดคดีนี้ ต้องมีการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ความจริงแล้ว จดหมายอิเล็กทรอนิกส์ ก็อยู่ในความหมายของข้อมูลอิเล็กทรอนิกส์ แต่ต้องการให้มีความชัดเจนขึ้น จึงได้เพิ่มเติมมาตรา 11

การส่งข้อมูลโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูล ซึ่งแหล่งที่มาของข้อมูลนั้นสามารถตรวจสอบได้จากข้อมูลจราจรทางคอมพิวเตอร์ ได้แก่ การปกปิด หรือปลอมแปลงหมายเลขประจำตัวเครื่อง และหมายถึงการกระทำที่ทำให้ไม่สามารถตรวจสอบ

แหล่งที่มาของการส่งข้อมูล และส่งผลให้ไม่อาจตรวจสอบได้ทางระบบข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น

การกระทำดังกล่าวต้องเป็นการรบกวนการใช้งานระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข องค์ประกอบของความผิดมาตรานี้คล้ายคลึงกับองค์ประกอบความผิดฐานบุกรุกมาตรา 362 ในประมวลกฎหมายอาญา ดังนั้น จึงน่าจะมีความรุนแรงของการรบกวนพอสมควร ซึ่งอาจต้องใช้มาตรฐานของวิญญูชนเป็นการวัดระดับของการพิจารณา

7. การจำหน่ายชุดคำสั่งที่จัดทำขึ้นเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด (มาตรา 13) ลักษณะการกระทำความผิดนี้ ได้แก่ มีการจำหน่ายหรือเผยแพร่ คำว่าจำหน่าย มีความหมายค่อนข้างชัดเจนอยู่แล้ว ส่วนคำว่า เผยแพร่ นั้นเป็นคำที่มีความหมายกว้าง ซึ่งน่าจะหมายความรวมถึง การโฆษณา จ่าย แจก

ทั้งนี้เป็นที่น่าสังเกตว่า การมีไว้เพื่อจำหน่าย ไม่เข้าองค์ประกอบความผิดฐานนี้ ซึ่งแตกต่างจากที่อนุสัญญากำหนด อาจเป็นเพราะลักษณะของสิ่งที่มีไว้ หรือชุดคำสั่งดังกล่าวยากต่อการพิสูจน์ว่ามีไว้โดยเจตนาที่ชอบ หรือไม่ชอบ หากจะพิจารณาด้วยปริมาณของการมีไว้แบบยาเสพติดก็ทำไม่ได้ เพราะชุดคำสั่งในลักษณะของโปรแกรมคอมพิวเตอร์ส่วนใหญ่เป็นข้อมูลดิจิทัล

การจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 และมาตรา 11 ซึ่งชุดคำสั่งอาจจะอยู่ในรูปแบบวัตถุ เช่น ดิสเกตต์ ไฟล์ดิจิทัล ก็ได้ ส่วนการใช้เป็นเครื่องมือในการกระทำความผิดนั้นเป็นความผิดตามมาตราใดมาตราหนึ่งก็ได้ เพราะถ้อยคำในกฎหมายใช้คำว่า หรือ การจำหน่ายหรือเผยแพร่ต้องมีผู้กระทำความผิดมีเจตนาในการกระทำความผิด หมายความว่า ผู้กระทำต้องรู้ข้อเท็จจริงด้วยว่าชุดคำสั่งนั้นได้จัดทำขึ้น โดยเฉพาะเพื่อเป็นเครื่องมือในการกระทำความผิด

8. การใช้คอมพิวเตอร์กระทำความผิดอื่น (มาตรา 14) ทั้งนี้ยังกำหนดให้การกระทำดังต่อไปนี้เป็นความผิดตามกฎหมายไม่ว่าจะเป็น

ก. การนำข้อมูลปลอม หรือข้อมูลคอมพิวเตอร์เข้าสู่ระบบคอมพิวเตอร์ ข้อมูลที่นำเข้าสู่ระบบและถือเป็นความผิดคือ การนำเข้าสู่ข้อมูลอันเป็นเท็จ หรือข้อมูลปลอมไม่ว่าจะเป็นการปลอมทั้งหมดหรือบางส่วนนั้น หากน่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน (มาตรา

14 (2) ซึ่งองค์ประกอบความผิดตามมาตรา 14 นี้ ได้แก่ การนำเข้าสู่ระบบคอมพิวเตอร์ การนำเข้าสู่ หมายถึงการนำข้อมูลคอมพิวเตอร์หรือโปรแกรมซอฟต์แวร์ต่างๆ เข้าสู่ระบบคอมพิวเตอร์

ข้อมูลคอมพิวเตอร์ดังกล่าวเป็นข้อมูลปลอมไม่ว่าทั้งหมด หรือบางส่วน หรือข้อมูลคอมพิวเตอร์ที่เป็นเท็จ หมายถึง ข้อมูลคอมพิวเตอร์ที่มีการเปลี่ยนแปลงแก้ไข ไม่ว่าจะเปลี่ยนแปลงแก้ไขนั้นจะทั้งหมด หรือเพียงบางส่วน ส่วนคำว่าข้อมูลคอมพิวเตอร์เป็นเท็จ นั้น น่าจะหมายถึงข้อมูลคอมพิวเตอร์ที่ไม่ใช่ของจริง เช่น ข้อมูลคอมพิวเตอร์ที่ระบุว่าเป็นเครื่องมือป้องกันไวรัสของบริษัทหนึ่ง แต่แท้จริงแล้วไม่ใช่ เป็นต้น

การกระทำได้ดังกล่าวน่าจะเกิดความเสียหายแก่บุคคลอื่นหรือประชาชน องค์ประกอบความผิดนี้มีใช้อยู่ในหลายฐานความผิดในประมวลกฎหมายอาญา ซึ่งเป็นเรื่องที่จะต้องพิจารณาจากลักษณะของการกระทำในเรื่องเจตนาด้วย

ข้อมูลที่กฎหมายกำหนดตามมาตรา 14 นี้ก็ประการหนึ่งคือ ข้อมูลอันเป็นเท็จ หรือข้อมูลปลอมไม่ว่าจะเป็นการปลอมทั้งหมดหรือบางส่วนนั้น หากน่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตระหนกแก่ประชาชน (มาตรา 14 (3)) โดยผู้กระทำความผิดนำเข้าข้อมูลอันเป็นเท็จสู่ระบบคอมพิวเตอร์ ซึ่งน่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

รวมถึง ข้อมูลคอมพิวเตอร์ใดๆที่เป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา (มาตรา 14 (3)) อาจพิจารณาได้จากลักษณะข้อมูลคอมพิวเตอร์ที่ใช้ในการกระทำความผิดว่ากระทบต่อความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา ซึ่งความผิดตามมาตรา 14 นี้เป็นการบัญญัติเพื่อที่จะเอาผิดเพิ่มเติมจากการกระทำซึ่งเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้าย โดยในการกระทำความผิดดังกล่าวได้ใช้วิธีการทางคอมพิวเตอร์นำข้อมูลคอมพิวเตอร์อันเป็นความผิดตามมาตรา 14 ดังกล่าวเข้าสู่ระบบคอมพิวเตอร์ ดังนั้น ผู้กระทำความผิดอาจต้องรับโทษตามประมวลกฎหมายอาญาตามบทบัญญัติที่กล่าวมาด้วย

การกระทำความผิดยังรวมถึงข้อมูลที่มีลักษณะลามกและข้อมูลดังกล่าว ประชาชนโดยทั่วไปอาจเข้าถึงได้(มาตรา 14 (4)) คือ ต้องเป็นข้อมูลคอมพิวเตอร์ที่มีลักษณะอันลามก คำว่า ลามก เป็นคำสามัญที่ไม่มีการนิยามศัพท์ แต่เป็นคำที่ใช้เป็นองค์ประกอบความผิดตามประมวลกฎหมายอาญา มาตรา 287 ซึ่งเป็นความผิดฐานเผยแพร่วัตถุลามก ดังนั้น

ข้อมูลคอมพิวเตอร์ใดจะเข้าองค์ประกอบความผิด ลามก หรือไม่นั้น จึงควรใช้มาตรฐานเดียวกับความผิดอาญา กรณีนี้มีการคุ้มครองแตกต่างจากที่กำหนดในอนุสัญญาที่มุ่งคุ้มครองเด็กและเยาวชนเป็นหลักแต่พระราชบัญญัตินี้กำหนดถึงข้อมูลที่มีลักษณะลามกทั้งหมดไม่ว่าจะเป็นเด็กหรือผู้ใหญ่

การเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ ตามมาตรา 14 (1) (2) (3) หรือ (4) กฎหมายได้บัญญัติให้เป็นความผิด ดังนี้

การเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ คำว่า เผยแพร่หรือส่งต่อ ต้องเป็นการเผยแพร่หรือส่งต่อในระบบคอมพิวเตอร์ ไม่น่าจะหมายความรวมถึงการส่งต่อทางกายภาพ เช่น การส่งดิสก์เกตต์ หรือทำการส่งพิมพ์ออก ซึ่งผู้กระทำรู้อยู่แล้วว่าข้อมูลคอมพิวเตอร์ที่ตนทำการเผยแพร่หรือส่งต่อนั้นเป็นข้อมูลซึ่งเป็นความผิดตามมาตรา 14 (1) (2) (3) หรือ (4) นั้น หมายความว่าผู้กระทำมีเจตนาในการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าว

9. การตกแต่งข้อมูลคอมพิวเตอร์ที่เป็นภาพของบุคคล ความผิดในมาตรานี้เป็นลักษณะของการหมิ่นประมาทด้วยการตกแต่งภาพของบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด หมายถึง การกระทำที่มีเจตนาเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปสามารถเข้าถึงได้ ถ้าเป็นระบบคอมพิวเตอร์ของตนเองก็ไม่เป็นความผิด

ข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของบุคคลอื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด หมายถึง การแสดงข้อมูลคอมพิวเตอร์นั้นออกเป็นภาพของบุคคล และภาพนั้นอาจเกิดจากการสร้างขึ้นใหม่ หรือเป็นภาพที่มีอยู่แต่ได้มีการตัดต่อ เติม หรือดัดแปลงซึ่งเป็นการทำด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด

คำว่า วิธีการอื่นใด เป็นการเขียนไว้เพื่อให้สามารถครอบคลุมการเปลี่ยนแปลงแก้ไขข้อมูลคอมพิวเตอร์ที่เป็นภาพบุคคลนั้นด้วยวิธีการอื่นใด ก็ได้ ซึ่งมีผลทำให้เกิดการเปลี่ยนแปลงต่อข้อมูลคอมพิวเตอร์ จึงไม่น่าจะหมายความรวมถึง การตัดต่อ เติม หรือดัดแปลงภาพบุคคลซึ่งเป็นภาพที่พิมพ์จากเครื่องคอมพิวเตอร์ การกระทำดังกล่าวอาจทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย องค์ประกอบในข้อนี้ใช้ข้อความในทำนองเดียวกับความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา มาตรา 326 เพียงแต่เพิ่มเติมคำว่า ได้รับความอับอาย เข้าไป ความหมายในมาตรานี้จึงกว้างกว่าที่กำหนดในประมวลกฎหมายอาญา

ข้อสังเกตตามมาตรานี้คือ ความผิดฐานนี้เป็นความผิดอันยอมความได้ ทั้งนี้เนื่องจากความเสียหายที่เกิดขึ้นนั้นเป็นความเสียหายเฉพาะบุคคล เมื่อเป็นความผิดยอมความได้ กฎหมายจึงต้องบัญญัติเกี่ยวกับผู้เสียหายไว้ในทำนองเดียวกับความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญาว่า ถ้าผู้เสียหายตายก่อนทำการร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

จากการกำหนดค่านियาม ความหมายและคำจำกัดความ ในส่วนนี้การกำหนดกรอบของการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศไทยมีความชัดเจน อาจเนื่องจากการที่ประเทศไทยเป็นประเทศที่ใช้กฎหมายลายลักษณ์อักษรจึงต้องมีการกำหนดกรอบกฎหมายไว้อย่างชัดเจน เพื่อไม่ให้เกิดอุปสรรคในการตีความ มีการกำหนดครอบคลุมทุกขั้นตอน และสามารถรองรับพันธกรณีที่อาจเกิดจากการเป็นภาคีอนุสัญญาได้ แม้จะมีการกำหนดฐานความผิดไว้มากกว่าอนุสัญญาซึ่งอาจเนื่องจากเหตุผลที่ผู้เขียนได้กล่าวไว้ข้างต้นแล้วว่าการบัญญัติกฎหมายดังกล่าวนี้ประเทศไทยเองใช้อนุสัญญารวมถึงกฎหมายจากหลายๆประเทศเพื่อเป็นแนวทาง

แต่อย่างไรก็ตามหากเมื่อทำการวิเคราะห์ฐานความผิดทั้งหมดที่กำหนดในพระราชบัญญัติแล้วพบว่าวัตถุประสงค์ในการปกป้องและคุ้มครองตามพระราชบัญญัติและตามอนุสัญญาล้วนเป็นสิ่งเดียวกันไม่ว่าจะเป็นการบัญญัติการกระทำความผิดที่กระทำต่อความลับ ความเที่ยงตรงและความมีอยู่ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ได้แก่ การเข้าถึงโดยมิชอบ การดักจับข้อมูลโดยมิชอบ การแทรกแซงต่อข้อมูล การแทรกแซงต่อระบบ การนำสิ่งที่ได้จากคอมพิวเตอร์ไปใช้ในทางมิชอบ ความผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่ การกระทำความผิดเกี่ยวกับการปลอมแปลงเกี่ยวกับคอมพิวเตอร์ ความผิดในการใช้คอมพิวเตอร์ในการฉ้อโกง ความผิดเกี่ยวกับเนื้อหา ได้แก่ การกระทำที่เป็นความผิดเกี่ยวกับสื่อลามกอนาจารที่บัญญัติครอบคลุมถึงกรณีที่เกี่ยวข้องกับเด็ก แต่มิได้มีการบัญญัติความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้อง

กฎหมายกำหนดให้ผู้ให้บริการและบุคคลทั่วไปต้องรับผิดชอบหากไม่ปฏิบัติตามหน้าที่ ซึ่งความรับผิดชอบของผู้ให้บริการ ความหมายของผู้ให้บริการผู้เขียนได้อธิบายไว้แล้วในส่วนตัวผ่านมา ซึ่งในส่วนนี้ผู้เขียนจะขอกล่าวถึงเฉพาะหน้าที่ของผู้ให้บริการ (26) กฎหมายได้กำหนดหน้าที่และความรับผิดชอบของผู้ให้บริการไว้ 2 ประการ คือ

1. เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ไว้ไม่น้อยกว่า 90 วันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่อาจขยายออกไปในกรณีที่พนักงานเจ้าหน้าที่สั่งให้เก็บรักษาข้อมูลไว้เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราว

2. เก็บรักษาข้อมูลผู้ให้บริการ หมายถึง การเก็บรักษาข้อมูลที่บ้านที่ถึงตัวตนของบุคคลในการเข้าใช้บริการทางเครือข่ายของผู้ให้บริการนับตั้งแต่เริ่มให้บริการและต้องเก็บรักษาไว้ไม่น้อยกว่า 90 วัน นับตั้งแต่การให้บริการสิ้นสุดลง ตัวอย่างของข้อมูลผู้ให้บริการ เช่น ชื่อ-สกุล รหัสเลขประจำตัว หรือรหัสผ่านใดๆ ความรับผิดชอบของผู้ให้บริการ ผู้ให้บริการมีความผิดหากไม่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลผู้ให้บริการตามที่กฎหมายกำหนด (มาตรา 26)

ส่วนความรับผิดชอบของบุคคลทั่วไปซึ่งไม่ได้เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แต่หากได้ไปล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลผู้ให้บริการที่พนักงานเจ้าหน้าที่ได้มาจากการใช้อำนาจในการสืบสวนสอบสวนตามกฎหมาย แล้วนำข้อมูลดังกล่าวไปเปิดเผยต่อผู้หนึ่งผู้ใดถือว่ามีความผิดตามมาตรา 24 และบุคคลทั่วไปที่ไม่ปฏิบัติตามคำสั่งพนักงานเจ้าหน้าที่มาตรา 18 หรือมาตรา 19 ก็เป็นความผิด

2. มาตรการทางด้านสับัญญัติ

ตามที่อนุสัญญาได้กำหนดให้ประเทศภาคีกำหนดหลักการเกี่ยวกับกฎหมายวิธีพิจารณาความอาญาในการเก็บรวบรวมพยานหลักฐานในการสืบสวนสอบสวนและการดำเนินคดีไม่ว่าจะเป็นวิธีการค้นหาข้อมูลอย่างรวดเร็ว การยึดและเก็บรักษาข้อมูล ที่ต้องมีการคำนึงถึงสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน เพื่อให้สอดคล้องกับหลักการดังกล่าวประเทศไทยได้มีการดำเนินการดังนี้

ก. มาตรการการสืบสวนสอบสวนและการดำเนินคดี

ความผิดตามพระราชบัญญัติฉบับนี้เป็นความผิดอาญา ดังนั้น การดำเนินคดีไม่ว่าจะเป็นเรื่องการจับกุม ค้น ชั่ง การสืบสวนสอบสวน ย่อมเป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอื่นที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยวิธีพิจารณาคดีในศาลแขวง กฎหมายว่าด้วยวิธีพิจารณาคดีเยาวชนและครอบครัว เป็นต้น อย่างไรก็ตามเพื่อให้การดำเนินคดีตามพระราชบัญญัตินี้มีประสิทธิภาพมากขึ้น จึงได้มีการบัญญัติหลักเกณฑ์พิเศษเพิ่มเติมขึ้นใหม่ 2 ประการ ดังนี้

1. การเพิ่มวิธีการพิเศษในการสืบสวนสอบสวน ซึ่งเป็นอำนาจเฉพาะในการสืบสวนสอบสวนเพื่อดำเนินคดีอาชญากรรมทางคอมพิวเตอร์และ

2. การเพิ่มให้มีพนักงานเจ้าหน้าที่ที่มีอำนาจในการสืบสวนสอบสวนความผิดดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ตามพระราชบัญญัติฉบับนี้ด้วย นอกเหนือจากเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญา

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 บัญญัติให้พนักงานเจ้าหน้าที่ที่มีอำนาจเพื่อประโยชน์ในการสืบสวนสอบสวนอย่างหนึ่งอย่างใดรวม 8 ประการ นอกเหนือจากอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งพนักงานเจ้าหน้าที่ย่อมมีอำนาจ เนื่องจากมาตรา 29 บัญญัติว่าในการปฏิบัติตามหน้าที่ตามพระราชบัญญัตินี้ให้อำนาจพนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญา มีอำนาจรับคำร้องทุกข์ หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้ มีข้อน่าสังเกตว่าพระราชบัญญัติฉบับนี้ ไม่ได้ตัดอำนาจของเจ้าพนักงานตามกฎหมายอื่น เช่น ประมวลกฎหมายวิธีพิจารณาความอาญา หรือตามกฎหมายอื่นที่มีการให้อำนาจในการทำงานเดียวกัน ซึ่งบทบัญญัติที่ให้อำนาจพนักงานเจ้าหน้าที่เป็นพิเศษ (มาตรา 18) ดังนี้

1. การใช้อำนาจของพนักงานเจ้าหน้าที่ซึ่งไม่ต้องขออนุญาตศาล เป็นอำนาจที่พนักงานเจ้าหน้าที่สามารถดำเนินการอย่างใดอย่างหนึ่ง โดยไม่จำเป็นต้องขออนุญาตศาล ทั้งนี้กฎหมายยังได้ควบคุมการใช้อำนาจโดยได้กำหนดให้พนักงานเจ้าหน้าที่จะใช้อำนาจได้ต่อเมื่อมีเหตุอันควรเชื่อได้ว่าการกระทำความผิดเกิดขึ้น และต้องใช้เฉพาะเท่าที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและ เพื่อหาตัวผู้กระทำความผิด โดยพนักงานเจ้าหน้าที่มีอำนาจดังนี้

อำนาจในการรวบรวมพยานหลักฐานโดยวิธีการเรียกให้บุคคลมาให้ถ้อยคำ หรือให้บุคคลชี้แจงเป็นหนังสือ หรือให้ส่งเอกสาร ข้อมูล หรือวัตถุอื่นใด อำนาจในข้อนี้เป็นอำนาจที่เจ้าพนักงานฝ่ายปกครองและตำรวจชั้นผู้ใหญ่มีตามประมวลกฎหมายวิธีพิจารณาความอาญา และคำว่า ข้อมูล ตามมาตรานี้ให้หมายความถึงข้อมูลทั่วไป เช่น ข้อมูลที่เก็บไว้ในดิสก์เกตต์หรือสื่อบันทึกข้อมูล แต่ไม่รวมถึง ข้อมูลคอมพิวเตอร์ ทั้งนี้ บุคคลที่ถูกเรียกตัวหากไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ ถือว่ามีความผิดตามพระราชบัญญัตินี้เช่นกัน

อำนาจในการเรียกข้อมูลจากรายการทางคอมพิวเตอร์ที่เกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์จากผู้ให้บริการแล้ว ก็ยังมีอำนาจเรียกจากบุคคลอื่นที่เกี่ยวข้องได้อีกด้วย ทั้งนี้ ผู้ให้บริการ หรือบุคคลที่ถูกเรียกขอข้อมูล หากไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ ถือว่ามีความผิดตามพระราชบัญญัตินี้เช่นกัน

อำนาจในการสั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่ เป็นอำนาจในการเรียกข้อมูลเกี่ยวกับผู้ใช้บริการจากผู้ให้บริการ ซึ่งข้อมูลเกี่ยวกับผู้ใช้บริการนี้เป็นข้อมูลที่ใช้บริการมีหน้าที่เก็บรักษา หรืออาจเป็นข้อมูลของผู้ใช้บริการที่ไม่ได้มีหน้าที่ต้องเก็บรักษาแต่อยู่ในความครอบครอง หรือควบคุมของผู้ให้บริการข้อมูลที่เกี่ยวข้องกับผู้ใช้บริการ เช่น ข้อมูลรหัสประจำตัวผู้ใช้บริการ ข้อมูลเกี่ยวกับบุคคลที่ใช้บริการซึ่งได้มีการลงทะเบียนไว้ เป็นต้น

2. การใช้อำนาจของพนักงานเจ้าหน้าที่ซึ่งต้องขออนุญาตศาล ซึ่งพระราชบัญญัติได้กำหนดให้การใช้อำนาจของพนักงานเจ้าหน้าที่ที่ต้องขออนุญาตศาลตามกฎหมายบัญญัติ ได้แก่

อำนาจในการทำสำเนาข้อมูลคอมพิวเตอร์หรือข้อมูลจากรายการทางคอมพิวเตอร์เมื่อไปกระทำจากระบบคอมพิวเตอร์ ถือว่าเป็นการล่วงล้ำเข้าไปในข้อมูลคอมพิวเตอร์ ซึ่งหากบุคคลทั่วไปกระทำย่อมเป็นความผิด ดังนั้น พนักงานเจ้าหน้าที่จะกระทำได้อีกต่อเมื่อได้รับอนุญาตจากศาลก่อน เนื่องจากเป็นการทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจากรายการทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ในกรณีจากระบบคอมพิวเตอร์นั้นยังมีได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

ข้อความที่ว่า ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมีได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่ หมายถึง ในกรณีที่หากพนักงานเจ้าหน้าที่ได้ยึดหรืออายัดระบบคอมพิวเตอร์นั้นมาแล้ว ดังนั้น เมื่อได้ยึดหรืออายัดระบบคอมพิวเตอร์มาแล้วย่อมใช้อำนาจทำสำเนาข้อมูลคอมพิวเตอร์ได้เลยโดยไม่ต้องขออนุญาตต่อศาลอีก ซึ่งการใช้อำนาจตามมาตรานี้หมายถึง การที่พนักงานเจ้าหน้าที่จะเข้าไปตรวจสอบข้อมูลในระบบคอมพิวเตอร์ หรือในข้อมูลคอมพิวเตอร์ใดๆ ก็ได้ ซึ่งได้แก่การเจาะระบบเพื่อให้ทราบถึงระบบคอมพิวเตอร์ หรือข้อมูลจากรายการทางคอมพิวเตอร์ ซึ่งปกติแล้ว

อำนาจในการสั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

อำนาจในการตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐาน หรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิด และสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

อำนาจในการถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

อำนาจในการยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและตัวผู้กระทำความผิด

การใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ที่ได้มีการกำหนดเพิ่มเติมนี้ยังเป็นประเด็นในเรื่องของการกระทำดังกล่าวถือเป็นการละเมิดสิทธิส่วนบุคคลหรือไม่นั้น พระราชบัญญัตินี้เป็นกฎหมายพิเศษ ทั้งนี้ สามารถเทียบเคียงได้ คำวินิจฉัยของคณะกรรมการกฤษฎีกาจากการพิจารณาข้อหาหรือของหน่วยงานของรัฐเกี่ยวกับอำนาจค้นเคหสถาน หรือยานพาหนะในส่วนที่เป็นรโหฐานโดยไม่ต้องมีหมายค้นของเจ้าพนักงานตามมาตรา 14 (1) และ (2) ของพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ.2519 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติป้องกันและปราบปรามยาเสพติด (ฉบับที่ 2) พ.ศ.2534 ว่าชัดรัฐธรรมนูญหรือไม่ ทั้งนี้ คณะกรรมการกฤษฎีกาได้เคยวินิจฉัยในกรณีดังกล่าวเอาไว้ว่า อำนาจค้นของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ.2519 นั้น เป็นอำนาจค้นตามกฎหมายพิเศษที่บัญญัติให้อำนาจแก่พนักงานเจ้าหน้าที่ไว้โดยเฉพาะให้กระทำการค้นในที่รโหฐานได้โดยไม่ต้องมีหมายค้นจึงไม่ขัดต่อรัฐธรรมนูญ

หรือกรณีอำนาจค้นในที่รโหฐานโดยไม่ต้องมีหมายค้นของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ ตามมาตรา 92 วรรคสอง แห่งประมวลกฎหมายวิธีพิจารณาความอาญา และอำนาจค้นโดยไม่มีหมายค้นในเคหสถาน สถานที่ใดๆหรือยานพาหนะใดๆ ในส่วนที่เป็นที่รโหฐานของเจ้าพนักงานตามมาตรา 14 (1) และ (2) ของพระราชบัญญัติป้องกันและปราบปราม

ยาเสพติดพ.ศ. 2519 นอกจากนั้น ยังมีคำพิพากษาที่ได้วินิจฉัยว่า บทบัญญัติเรื่องการค้นในที่
รโหฐานในกรณีมีเหตุจำเป็นเร่งด่วนนั้นให้ใช้บังคับได้ไม่ขัดต่อรัฐธรรมนูญ²²

ดังนั้น เมื่อพิจารณาเทียบเคียงอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการ
สืบสวนสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ดังกล่าวตามพระราชบัญญัตินี้ กับคำวินิจฉัย
ของคณะกรรมการกฤษฎีกาและคำพิพากษาศาลฎีกาข้างต้นแล้ว ผู้เขียนเห็นว่า การให้อำนาจเจ้า
พนักงานในกรณีดังกล่าวไม่ขัดต่อบทบัญญัติตามรัฐธรรมนูญแต่อย่างใด

พระราชบัญญัตินี้ได้ให้ความหมายและคุณสมบัติของพนักงานเจ้าหน้าที่ตามที่
ผู้เขียนได้อธิบายในข้างต้น (มาตรา 3) สถานะและอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ (มาตรา
29) พนักงานเจ้าหน้าที่มีอำนาจทุกอย่างตามที่พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตาม
ประมวลกฎหมายวิธีพิจารณาความอาญา มี แต่มีอำนาจสืบสวนสอบสวนเฉพาะความผิดตาม
พระราชบัญญัตินี้เท่านั้น ซึ่งอำนาจที่กำหนดไว้โดยเฉพาะตามพระราชบัญญัตินี้ คือ

1. อำนาจในการสืบสวนและสอบสวนเพื่อรวบรวมพยานหลักฐานเกี่ยวกับการ
กระทำความผิดและหาตัวผู้กระทำความผิด (มาตรา 18)
2. อำนาจในการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อดำเนินคดี ในกรณีที
กฎหมายกำหนดให้ต้องมีการขออนุญาตศาลก่อน ตามที่ผู้เขียนได้อธิบายไว้ข้างต้น
3. อำนาจในการยื่นคำร้อง (ซึ่งได้รับความเห็นชอบจากรัฐมนตรี) ต่อศาลที่มี
เขตอำนาจ เพื่อขอให้มีการสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจ
กระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อย
หรือศีลธรรมอันดีของประชาชน (มาตรา 20)
4. อำนาจในการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีการสั่งห้ามจำหน่าย
หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ (มาตรา 21)
5. อำนาจในการสั่งให้ผู้ให้บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เป็น
กรณีพิเศษเฉพาะราย คือเก็บไว้เกิน 90 วัน แต่ไม่เกิน 1 ปี (มาตรา 26)

²² การประชุมสนพระราชดำริว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร, รายงานของประเทศไทย : การประชุมสนพระราชดำริว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร ประเทศไทย "กรณีนี้กำลังและการโต้ตอบ : การดำเนินกลยุทธ์ร่วมกันในการป้องกันอาชญากรรมและความยุติธรรมทางอาญา". หน้า 21.

จะเห็นได้ว่าการกำหนดใช้อำนาจของพนักงานเจ้าหน้าที่จะสามารถทำได้ในกรณีที่ต้องเป็นการใช้อำนาจเพื่อประโยชน์ในการสืบสวนและสอบสวน หรือในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์เท่านั้น และต้องใช้เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด และเพื่อหาตัวผู้กระทำความผิดเท่านั้น ทั้งนี้หลักการดังกล่าวสามารถเป็นหลักประกันให้กับบุคคลทั่วไปว่าจะได้รับความคุ้มครองในเรื่องสิทธิส่วนบุคคล ทั้งนี้ อำนาจบางประการที่อาจกระทบกับสิทธิมนุษยชน กฎหมายก็ได้กำหนดให้มีขั้นตอนเพิ่มเติมโดยต้องผ่านการพิจารณาจากศาล คือหากจะดำเนินการตามหน้าที่ดังกล่าวได้ต้องขออนุญาตจากศาล มิเช่นนั้นจะถือว่าเจ้าหน้าที่ทำการบุกรุก หรือเข้าถึงข้อมูลคอมพิวเตอร์โดยมิได้รับอนุญาตและอาจถือได้ว่าเจ้าหน้าที่กระทำความผิดเสียเอง

ทั้งนี้ พระราชบัญญัติก็ได้กำหนดความรับผิดของพนักงานเจ้าหน้าที่ ไว้ดังนี้

1. ความรับผิดหากกระทำโดยเจตนา ตามที่ผู้เขียนได้กล่าวมาแล้วว่า ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่ได้มาจากการใช้อำนาจในการสืบสวนสอบสวน เป็นกรณีที่ต้องกระทำไปเพื่อประโยชน์ในการใช้เป็นหลักฐานในการสืบสวนสอบสวนความผิดตามพระราชบัญญัตินี้เท่านั้น หากนำไปเปิดเผยหรือส่งมอบแก่บุคคลทั่วไป ถือได้ว่ามีความผิดใช้อำนาจหน้าที่โดยมิชอบ ยกเว้น กรณีที่เปิดเผยหรือส่งมอบไปเพื่อดำเนินคดีกับผู้กระทำความผิดหรือดำเนินคดีกับพนักงานเจ้าหน้าที่หากมีการใช้อำนาจโดยมิชอบ อย่างไรก็ตามเพื่อเปิดช่องให้สามารถนำข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่ได้มาจากการใช้อำนาจในการสืบสวนสอบสวนไปใช้เพื่อประโยชน์อย่างอื่นได้ เช่น เพื่อใช้ในการดำเนินคดีอาญาอื่น หรือเพื่อใช้ในเรื่องความร่วมมือระหว่างประเทศตามสนธิสัญญาหรือข้อตกลงที่ประเทศไทยเป็นภาคี กฎหมายกำหนดให้จะต้องเป็นการกระทำตามคำสั่งศาลหรือได้รับอนุญาตจากศาล ส่วนในปัญหาว่าจะต้องขออนุญาตต่อศาลใด น่าจะหมายถึงศาลที่พนักงานเจ้าหน้าที่จะเปิดเผยหรือส่งมอบข้อมูลดังกล่าวอยู่ในเขตอำนาจ

2. ความรับผิดหากกระทำโดยประมาท ในมาตรานี้กล่าวถึงในกรณีที่พนักงานเจ้าหน้าที่ไม่ได้มีเจตนาแต่กระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่ได้มาจากการใช้อำนาจในการสืบสวน

จากการวิเคราะห์มาตรการที่เกี่ยวข้องกับการสืบสวนสอบสวนอาชญากรรมรูปแบบใหม่นี้ประเทศไทยก็ได้ดำเนินการเกี่ยวกับมาตรการที่จำเป็นในการสืบสวนสอบสวนเพื่อค้นหา

พยานหลักฐานในการดำเนินคดีและการบังคับใช้อำนาจตามกฎหมายเพื่อให้เกิดความรวดเร็วและมีประสิทธิภาพเพียงพอในการเก็บรักษาข้อมูลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ทั้งนี้การกำหนดมาตรการและการกำหนดให้มีเจ้าหน้าที่ที่มีหน้าที่ในการสืบสวนสอบสวนตามพระราชบัญญัตินี้จึงแสดงให้เห็นว่าประเทศไทยเองก็สามารถดำเนินในทิศทางเดียวกันกับอนุสัญญาในการรวบรวมหรือบันทึกเนื้อหาโดยไม่ก่อให้เกิดอุปสรรคในการบังคับใช้กฎหมาย

ข. เขตอำนาจในการดำเนินคดีเกี่ยวกับการกระทำความผิด

ลักษณะการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ส่วนใหญ่จะเกิดผลโดยไม่มีเขตแดน โดยเฉพาะที่เกี่ยวข้องกับการส่งข้อมูลคอมพิวเตอร์ ซึ่งไม่ว่าจะทำการส่งข้อมูลที่ใดในโลก ก็สามารถเปิดระบบคอมพิวเตอร์ดูได้ทั่วโลก จึงถือว่าเป็นอาชญากรรมที่ไร้พรมแดน ดังนั้น การพิจารณาความรับผิดและการรับโทษตามบททั่วไปของประมวลกฎหมายอาญาด้วย ดังนี้.

1. การกระทำส่วนหนึ่งส่วนใดในราชอาณาจักรหรือผลแห่งการกระทำเกิดขึ้นในราชอาณาจักร (ประมวลกฎหมายอาญา มาตรา 5) เนื่องจากการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นี้เป็นบทบัญญัติความผิดที่มีโทษทางอาญา ดังนั้นจึงต้องนำหลักกฎหมายความรับผิดในเรื่องหลักดินแดน ตามที่บัญญัติไว้ในประมวลกฎหมายอาญามาใช้ด้วย ซึ่งการกระทำความผิดเกี่ยวกับคอมพิวเตอร์โดยเฉพาะที่เกี่ยวข้องกับข้อมูลคอมพิวเตอร์ ไม่ว่าจะเป็นการเข้าถึง การแทรกแซง ทำลาย การนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ การเผยแพร่ นั้น ถึงแม้ว่าจะไม่ได้กระทำในประเทศไทย แต่ถ้าผลแห่งการกระทำเกิดขึ้น คือผู้รับข้อมูลสามารถเปิดรับข้อมูลคอมพิวเตอร์นั้นในประเทศไทยได้ ย่อมถือว่าผลแห่งการกระทำเกิดขึ้นในประเทศไทย และถือว่าความผิดนั้นได้กระทำในประเทศไทย
2. การกระทำของตัวการ ผู้สนับสนุน หรือผู้ใช้ให้กระทำความผิดที่ได้กระทำนอกราชอาณาจักร ในเรื่องนี้ต้องนำหลักเรื่องสถานที่ในการกระทำความผิดมาใช้ตามประมวลกฎหมายอาญา มาตรา 6 มาใช้บังคับด้วย เพราะหากเมื่อพิจารณาบทบัญญัติดังกล่าวแล้วจะเห็นได้ว่า ตัวการ ผู้สนับสนุน และผู้ใช้ให้กระทำความผิดตามพระราชบัญญัตินี้ หากได้กระทำสนับสนุน หรือชี้แนะนอกประเทศไทย ก็ถือว่าตัวการ ผู้สนับสนุน หรือผู้ใช้ให้กระทำความผิดนั้นได้กระทำความผิดในประเทศไทย
3. การกระทำความผิดนอกราชอาณาจักรที่ต้องรับโทษในราชอาณาจักร ดังที่ได้กล่าวมาแล้วว่าลักษณะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ส่วนใหญ่ไม่ว่าจะกระทำ ณ

สถานที่ใดในโลก อาจเกิดผลในประเทศไทยด้วย ดังนั้น การส่งข้อมูลคอมพิวเตอร์ที่เป็นความผิดถึงแม้จะกระทำที่ประเทศอื่นแต่ผลของข้อมูลที่เกิดขึ้นในประเทศไทย ให้ใช้หลักตามประมวลกฎหมายอาญา มาตรา 6 แต่ก็อาจมีความผิดบางลักษณะซึ่งเป็นการกระทำนอกราชอาณาจักร และผลที่เกิดขึ้นก็มีนอกราชอาณาจักรเท่านั้น เช่น การเข้าไปเจาะทำลายข้อมูลคอมพิวเตอร์ของสถานทูตไทยในต่างประเทศ กรณีเช่นนี้ถือว่าผู้เสียหายเป็นคนไทย ซึ่งหลักกฎหมายตามประมวลกฎหมายอาญา มาตรา 8 นั้น จะให้ผู้กระทำความผิดต้องรับโทษในราชอาณาจักรหากมีการร้องขอให้ลงโทษจากผู้เสียหายหรือรัฐบาลไทย

อย่างไรก็ตาม บทบัญญัติประมวลกฎหมายอาญา มาตรา 8 นี้ใช้บังคับเฉพาะความผิดที่กำหนดไว้ในมาตรา 8 เท่านั้น แต่ความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้อยู่ในบัญชีตามอนุมาตราต่างๆตามมาตรา 8 ดังนั้นจึงได้มีการบัญญัติไว้เพิ่มเติมหลักความรับผิดโดยนำหลักในเรื่องดังกล่าวมาบัญญัติไว้ในพระราชบัญญัติ ดังนี้

นอกจากนี้ พระราชบัญญัตินี้ยังได้กำหนดหลักเรื่องเขตอำนาจในการดำเนินคดีกรณีที่ต้องรับโทษภายในราชอาณาจักร

1. ผู้กระทำความผิดนั้นเป็นคนไทย แม้ได้กระทำความผิดนอกราชอาณาจักร และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นร้องขอให้มีการลงโทษ
2. ผู้กระทำความผิดนั้นเป็นคนไทย แม้ได้กระทำความผิดนอกราชอาณาจักร และผู้เสียหายร้องขอให้มีการลงโทษ
3. ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยเป็นผู้ได้รับความเสียหาย และรัฐบาลไทยได้ร้องขอให้มีการลงโทษ
4. ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และคนไทยเป็นผู้ได้รับความเสียหาย และผู้เสียหายได้ร้องขอให้มีการลงโทษ

สำหรับประเด็นในเรื่องเขตอำนาจศาลของประเทศไทยเป็นหลักเกณฑ์หนึ่งที่เกี่ยวข้องกับการให้ความร่วมมือระหว่างประเทศในการนำตัวผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์มาลงโทษ จึงต้องมีกำหนดไว้อย่างชัดเจนในหลักเรื่องเขตอำนาจในการดำเนินคดีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ซึ่งในอนุสัญญาเองก็ได้บัญญัติเกี่ยวกับการกำหนดเขตอำนาจศาลตามอนุสัญญามีได้ลงล้างเขตอำนาจศาลในการดำเนินคดีอาญาตามกฎหมาย

ภายในของประเทศภาคีนั้น และหากเกิดกรณีที่หลายประเทศมีการอ้างเขตอำนาจในการดำเนินคดีเหนือความผิดที่มีอยู่ ให้ประเทศภาคีทั้งหลายของอนุสัญญานั้นปรึกษาหารือกันตามสมควรเพื่อพิจารณาว่าเขตอำนาจการดำเนินคดีของประเทศใดมีความเหมาะสมที่สุดที่จะใช้เพื่อการฟ้องร้องดำเนินคดีอาญากับผู้กระทำความผิดนั้น และสามารถจัดอุปสรรคในการดำเนินคดีกับผู้กระทำความผิด จากเหตุผลดังกล่าวนี้แสดงให้เห็นว่าเขตอำนาจศาลตามกฎหมายภายในประเทศไทยก็ยังคงสามารถใช้บังคับได้ และหากเป็นภาคีอนุสัญญาประเทศไทยยังอาจจัดข้อขัดข้องในเรื่องเขตอำนาจศาลที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ที่มีลักษณะข้ามประเทศได้

3. มาตรการทางด้านความร่วมมือระหว่างประเทศ

ก. การส่งผู้ร้ายข้ามแดน

การส่งผู้ร้ายข้ามแดนเป็นความร่วมมือระหว่างประเทศในการนำตัวผู้กระทำความผิดมาลงโทษ วิธีการนำตัวจำเลยมาขึ้นศาลหรือขั้นตอนการดำเนินคดีในประเทศไทยนั้น ต้องเป็นไปตามพระราชบัญญัติการส่งผู้ร้ายข้ามแดน พ.ศ. 2472 ซึ่งในขณะนี้ประเทศไทยมีสนธิสัญญาส่งผู้ร้ายข้ามแดนกับต่างประเทศไทยจำนวน 10 ประเทศ คือ อังกฤษ สหรัฐอเมริกา จีน เกาหลีใต้ ลาว เบลเยียม อินโดนีเซีย ฟิลิปปินส์ กัมพูชา และบังกลาเทศ นอกจากนี้ยังมีอีก 4 ประเทศที่สืบสนธิสัญญาจากอังกฤษ คือ มาเลเซีย แคนาดา ออสเตรเลีย และฟิจิ หลักการที่สำคัญที่ระบุไว้ในกฎหมายดังกล่าวสามารถสรุปได้ดังนี้

ความผิดที่จะขอให้ส่งผู้ร้ายข้ามแดนได้นั้นต้องเป็นความผิดที่กฎหมายไทยกำหนดโทษจำคุกไว้ไม่ต่ำกว่า 1 ปี และต้องเป็นความผิดตามกฎหมายอาญาที่สามารถลงโทษได้ทั้งในประเทศที่ร้องขอและประเทศที่รับคำร้องขอด้วย

ความผิดที่จะขอให้ส่งผู้ร้ายข้ามแดนต้องไม่ใช่คดีที่ศาลประเทศผู้ร้องขอได้พิจารณาและพิพากษาให้ปล่อยหรือได้รับโทษในความผิดที่ร้องขอให้ส่งผู้ร้ายข้ามแดนแล้ว ซึ่งหลักการข้อนี้ต้องพิจารณาตามหลัก Double Jeopardy คือ ไม่พิพากษาลงโทษบุคคลคนเดียวกันในความผิดที่ได้กระทำในครั้งเดียวเป็นครั้งที่สอง

ความผิดดังกล่าวต้องมีโทษความผิดทางการเมือง หรือมีวัตถุประสงค์อื่นที่มีลักษณะทางการเมือง

ทั้งนี้ หลักการต่างๆ เกี่ยวกับการขอส่งผู้ร้ายข้ามแดนจะต้องดำเนินการตามพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ.2472 และต้องเป็นไปตามสัญญา อนุสัญญา สนธิสัญญา หรือความตกลงกับรัฐบาลต่างประเทศ การขอส่งผู้ร้ายข้ามแดนจากประเทศอื่นเพื่อกำหนดคดี ความผิดที่เกิดขึ้นในประเทศไทยนั้น ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 141 วรรคท้าย กำหนดให้เป็นหน้าที่ของพนักงานอัยการ ซึ่งเมื่อมีคำสั่งควรสั่งฟ้องผู้ต้องหาแล้ว ถ้าผู้ต้องหา อยู่ต่างประเทศ ก็ให้พนักงานอัยการจัดการขอให้ส่งตัวผู้ร้ายข้ามแดนมาดำเนินคดีภายในกำหนดอายุความ อัยการที่ทำหน้าที่ดังกล่าว เช่น อัยการฝ่ายต่างประเทศ และอัยการฝ่ายคดีพิเศษ

อย่างไรก็ดี การขอส่งตัวผู้ร้ายข้ามแดนมาทุกกรณี จะต้องดำเนินการโดยส่งผ่านวิธีทางการทูต กล่าวคือ ต้องมีคำร้องขอส่งผ่านกระทรวงการต่างประเทศของทั้งสองประเทศ ส่วนการพิจารณาว่าจะส่งบุคคลใดเป็นผู้ร้ายข้ามแดนหรือไม่ เป็นอำนาจของฝ่ายบริหารแต่ละประเทศที่จะพิจารณาจากหลักเกณฑ์ตามที่กำหนดในสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างประเทศไทยกับประเทศผู้รับคำร้องขอ หรือกฎหมายภายในของประเทศนั้นในกรณีที่ไม่ มีสนธิสัญญาระหว่างกัน

อย่างเช่น กรณีระหว่างประเทศไทยกับอังกฤษ ได้มีประกาศสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดนกันระหว่างกรุงสยามกับอังกฤษ ตั้งแต่ 4 มีนาคม รศ.130 (ค.ศ.1911 / พ.ศ.2454) โดยหลักใหญ่ของการขอส่งผู้ร้ายข้ามแดนต้องมีความผิดทางอาญาโดยอาจมีหมายจับหรือคำพิพากษาของศาลในคดีนั้นๆ ซ้ำยกเว้นประการหนึ่งตามหลักกฎหมายระหว่างประเทศว่าด้วยเรื่องการส่งผู้ร้ายข้ามแดน คือ อาจไม่ส่งบุคคลใดเป็นผู้ร้ายข้ามแดน หากมูลกรณีที่ร้องขอเป็นความผิดทางการเมือง หรือมีลักษณะในทางการเมือง

ทั้งนี้ ผู้เขียนจะขอยกตัวอย่างกรณีที่มีการส่งผู้ร้ายข้ามแดนของประเทศไทย กรณีการขอตัว นายปิ่น จักกะพาก อดีตผู้บริหารบริษัทเงินทุนเอกชนกิจ และนายราเกษ สักเสนา อดีตที่ปรึกษากรรมการผู้จัดการใหญ่ธนาคารกรุงเทพพาณิชย์การ²³ เป็นผู้ร้ายข้ามแดนกลับมาดำเนินคดีในประเทศไทย โดยคดีนายปิ่น ศาลสูงของอังกฤษมีคำพิพากษาไม่ส่งตัวเป็นผู้ร้ายข้ามแดน

ภายหลังคดีนายปิ่น จักกะพาก ลี้ลับลง สำนักงานอัยการสูงสุดได้จัดทำรายงานเสนอต่อคณะกรรมการการยุติธรรมและสิทธิมนุษยชน สภาผู้แทนราษฎร เมื่อเดือนกันยายน พ.ศ.2544 สรุปได้ว่า สาเหตุสำคัญที่ทำให้การขอตัวนายปิ่นไม่ประสบความสำเร็จ คือ

²³ The Nation, [Online], 2009, Available from: <http://www.suthichaiyoon.com/>. [2010, January 11]

ช่องโหว่ตามสนธิสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดนกันในระหว่างกรุงสยามกับอังกฤษ รศ.130 ที่ระบุหลักเกณฑ์เอาไว้ว่า การจะส่งผู้ร้ายข้ามแดนให้แก่กันได้ จะต้องมีการพยานหลักฐานเพียงพอที่จะลงโทษจำเลยได้ตามกฎหมายของประเทศอังกฤษ ถ้าหากความผิดนั้นได้กระทำความผิดในประเทศอังกฤษ ด้วยเหตุนี้ จึงทำให้ที่มทนายความและอัยการของอังกฤษต้องเปรียบเทียบการกระทำของนายปิ่น จักกะพาก ตามที่ถูกกล่าวหาในประเทศไทยว่า หากการกระทำเดียวกันนั้นได้กระทำความผิดในอังกฤษ นายปิ่น จักกะพาก จะมีความผิดตามกฎหมายอังกฤษในข้อหาใด กฎหมายฉบับไหน และความผิดนั้นยังจะต้องเป็นความผิดที่ได้ระบุไว้ในสนธิสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดนอีกด้วย

ในการวิเคราะห์ดังกล่าว ที่มทนายความและอัยการอังกฤษจะดูกฎหมายไทยเป็นเพียงข้อเท็จจริงประกอบเท่านั้น โดยจะไม่พิจารณาว่าการกระทำดังกล่าวผิดกฎหมายไทยหรือไม่ สำนักงานอัยการสูงสุดจึงเสนอให้มีการเจรจาแก้ไขปรับปรุงสนธิสัญญาส่งผู้ร้ายข้ามแดนที่ประเทศไทยทำไว้กับอังกฤษ และประเทศอื่นๆ ให้ทันสมัยมากขึ้น เพราะปัจจุบันมีความผิดอาญาใหม่ๆ ถูกกำหนดขึ้นเป็นจำนวนมาก เช่น ความผิดเกี่ยวกับยาเสพติด การฟอกเงิน ความผิดเกี่ยวกับการเงิน การธนาคาร หรือสถาบันการเงิน เป็นต้น ซึ่งตามสนธิสัญญามีได้ระบุไว้ให้ครอบคลุมโดยชัดแจ้ง ทำให้ตกเป็นดุลพินิจของประเทศนั้นๆ ว่า จะส่งผู้ต้องหาให้กับประเทศไทยหรือไม่ ซึ่งในกรณีของนายปิ่น จักกะพาก ก็ประสบปัญหาลักษณะนี้เช่นกัน

คดีชาวมาเลเซียจำเลยแก๊งโจรกรรมข้อมูลบัตรเครดิตรายใหญ่ เป็นผู้ร้ายข้ามแดนไปดำเนินคดีที่ประเทศสหรัฐอเมริกา ตามคำร้องขอหลังจากที่มีการโจรกรรมบัตรเครดิตรายใหญ่ในประเทศสหรัฐอเมริกา และเอเชียตะวันออกเฉียงใต้ สร้างความเสียหายกว่า 150 ล้านดอลลาร์สหรัฐ หรือประมาณกว่า 5,000 ล้านบาท

ศาลมีคำพิพากษาในคดีหมายเลขดำ อผ.5/2552 ที่พนักงานอัยการต่างประเทศเป็นโจทก์ยื่นคำร้องขอให้ศาลมีคำสั่งให้ นายเอฟเอ็นยู แอลเอ็นยู หรือ เดลปีเอโร หรือ กุ่ย ก๊อก เส็ง อายุ 44 ปี ชาวมาเลเซีย เป็นจำเลย ส่งตัวเป็นผู้ร้ายข้ามแดนไปดำเนินคดีที่ประเทศสหรัฐอเมริกา เมื่อจำเลยเป็นหนึ่งในแก๊งโจรกรรมข้อมูลบัตรเครดิตรายใหญ่ในสหรัฐอเมริกา และเอเชียตะวันออกเฉียงใต้ สร้างความเสียหายกว่า 150 ล้านดอลลาร์สหรัฐ หรือประมาณกว่า 5,000 ล้านบาท

โจทก์ฟ้องและนำสืบว่าจำเลยกระทำความผิดข้อหาร่วมกันสมคบกันไว้ในครอบครอง ซึ่งอุปกรณ์เข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และลักลอบค้าอุปกรณ์เข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เป็นความผิดที่มีโทษเทียบเท่ากฎหมายไทย ตามพระราชบัญญัติว่าด้วย

ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 7, 8, 9 และ 12 ประมวลกฎหมายอาญา มาตรา 83, 269/1, 269/3 และ 269/7 และ พระราชบัญญัติการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ. 2545 มาตรา 3, 9 และ 43 มีโทษจำคุกไม่น้อยกว่า 1 ปี และไม่เป็นความผิดทางการเมือง คดียังไม่ขาดอายุความ เนื่องจากเป็นคดีเร่งด่วน ตามข้อ 10 แห่งสนธิสัญญาส่งผู้ร้ายข้ามแดน ระหว่างราชอาณาจักรไทยและประเทศสหรัฐอเมริกา ขอให้ศาลมีคำสั่งส่งจำเลยเป็นผู้ร้ายข้ามแดน ศาลพิเคราะห์แล้วเห็นว่า มีปัญหาต้องวินิจฉัยว่า จำเลยเป็นบุคคลเดียวกันกับที่ประเทศ สหรัฐต้องการตัวหรือไม่ เห็นว่าหลังจากที่ศาลได้ออกหมายจับจำเลย ตามที่ร้องขอผ่านกระทรวง การต่างประเทศ โดยระบุรูปพรรณสัณฐาน และภาพถ่ายของหมายจับ ต่อมาเจ้าหน้าที่ตำรวจ สามารถจับกุมจำเลยได้ และจำเลยรับว่าเป็นบุคคลเดียวกันกับคนในภาพ เห็นว่าเจ้าหน้าที่ สืบสวนราชการลับของประเทศสหรัฐอเมริกา ได้ติดตามสืบสวนการโจรกรรมข้อมูลบัตรเครดิตที่ จำเลยกระทำความผิดตั้งแต่ปี พ.ศ. 2548 ก่อนจะให้สายลับติดต่อขอซื้อข้อมูลบัตรเครดิตจากจำเลยที่ กรุงเทพมหานคร เมื่อปี พ.ศ. 2552 และจากการตรวจสอบหนังสือเดินทางของจำเลย เลขที่ A10696072 ตรงกับชื่อของจำเลย เป็นบุคคลเดียวกับในภาพถ่าย แสดงว่า หน่วยราชการลับของ สหรัฐฯ ติดตามตัวจำเลยมาเป็นเวลานาน วางแผนกันเป็นขั้นตอน สอดคล้องกับคำให้การของ จำเลยที่ระบุว่าเป็นบุคคลเดียวกันตามหมายจับและภาพถ่าย

แม้ต่อมาจำเลยจะอ้างในชั้นศาลว่าไม่ใช่บุคคลคนเดียว และไม่เคยเดินทางไป ประเทศสหรัฐอเมริกา แต่เชื่อว่าจำเลยอาจจะเดินทางเข้าประเทศสหรัฐอเมริกาทางช่องทางอื่นได้ คำปฏิเสศของจำเลยเป็นเพียงคำกล่าวอ้างลอยๆ ไม่มีน้ำหนักหักล้างพยานหลักฐานโจทก์ ประกอบกับความผิดของจำเลยไม่ใช่ความผิดทางการเมือง และมีความผิดเทียบเท่ากับกฎหมาย ไทยหลายบท มีโทษจำคุกไม่ต่ำกว่า 1 ปี จึงรับฟังได้ว่าจำเลยเป็นบุคคลเดียวกับที่ทางการ ประเทศสหรัฐอเมริกาขอส่งตัวเป็นผู้ร้ายข้ามแดน จึงให้ขังจำเลยไว้มีกำหนด 30 วัน เมื่อครบ กำหนดจึงให้ส่งตัวจำเลยเป็นผู้ร้ายข้ามแดนให้ประเทศสหรัฐอเมริกาต่อไป ตามสนธิสัญญาส่ง ผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทย และประเทศสหรัฐอเมริกา

จากกรณีดังกล่าว จะเห็นได้ว่าหากเป็นประเทศที่มีสนธิสัญญาการส่งผู้ร้ายข้าม แคนระหว่างกันกับประเทศไทยการส่งผู้ร้ายข้ามแดนระหว่างกันก็อาจทำได้โดยง่าย แต่ทั้งนี้อาจมี อุปสรรคในการส่งผู้ร้ายข้ามแดนจากการกำหนดหลักความผิดอาญาของทั้งสองประเทศ ซึ่ง สามารถนำมาเทียบเคียงกับการกระทำความผิดอาญากรรมทางคอมพิวเตอร์ได้ว่าสนธิสัญญาว่า ด้วยการส่งผู้ร้ายข้ามแดนระหว่างประเทศไทยและประเทศภาคีอื่นๆ เป็นสนธิสัญญาที่มีการทำ ขึ้นมาช้านาน มิได้มีการผ่อนคลายหลักการความผิดอาญาของทั้งสองประเทศ เพื่อให้สามารถนำ ตัวผู้กระทำความผิดอาญากรรมทางคอมพิวเตอร์ซึ่งเป็นอาญากรรมรูปแบบใหม่ที่อาจไม่มีการ

กำหนดในสนธิสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดนระหว่างประเทศภาคีอนุสัญญา จากผลคดีที่เกิดขึ้นแสดงให้เห็นว่าการที่ประเทศไทยกำหนดหลักการเรื่องความผิดอาญาของทั้งสองประเทศไว้ อาจทำให้เป็นอุปสรรคเกี่ยวกับการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมทางคอมพิวเตอร์ได้ เนื่องจากความผิดอาชญากรรมทางคอมพิวเตอร์มิได้เป็นความผิดที่กำหนดให้มีการส่งผู้ร้ายข้ามแดน ซึ่งสนธิสัญญาหลายฉบับที่มีอยู่ก็ไม่เอื้ออำนวยสำหรับกรณีนี้ ดังนั้น แนวทางการแก้ไขปัญหาดังกล่าวอาจสามารถทำได้โดยการระงับอาชญากรรมทางคอมพิวเตอร์ไว้ในอนุสัญญา และมีการผ่อนคลายหลักการเรื่องความผิดอาญาของทั้งสองประเทศ อย่างไรก็ตามถึงแม้จะผ่อนคลายหลักการเรื่องความผิดอาญาของทั้งสองประเทศแล้วแต่ก็อาจเกิดข้อขัดข้องได้สำหรับกรณีที่มีสนธิสัญญาต่อกัน เพราะการพิจารณาในหลักการขึ้นอยู่กับดุลพินิจของประเทศผู้รับคำร้องขอ แต่หากประเทศไทยพิจารณาเข้าเป็นภาคีอนุสัญญา แม้หากไม่ได้มีการทำสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างกันแต่ต้องการให้มีการส่งผู้ร้ายข้ามแดน ประเทศไทยอาจใช้หลักการส่งผู้ร้ายข้ามแดนตามที่บัญญัติในอนุสัญญา ประเทศภาคีผู้รับคำร้องขออาจพิจารณาใช้สนธิสัญญาเป็นแนวทางของกฎหมายในการส่งผู้ร้ายข้ามแดนสำหรับกรณีความผิดทางอาญาที่มีโทษจำคุกในอัตราขั้นสูงที่มีกำหนดตั้งแต่หนึ่งปีขึ้นไป หรืออัตราโทษที่หนักกว่านั้น

ข. การช่วยเหลือซึ่งกันและกัน

จากที่มีการศึกษาแล้วว่าอาชญากรรมทางคอมพิวเตอร์อาจก่อให้เกิดอาชญากรรมที่มีลักษณะที่ผลของการกระทำความผิดเกิดขึ้นในเขตแดนมากกว่าหนึ่งประเทศ และผู้กระทำความผิด หรือผู้เสียหายอาจเป็นพลเมืองของหลายประเทศเข้ามาเกี่ยวข้อง ลักษณะการกระทำความผิดก็มีความซับซ้อน แนวทางปฏิบัติในการให้ความช่วยเหลือเพื่อให้สามารถนำตัวผู้กระทำความผิดมาลงโทษของประเทศไทยกำหนดไว้ในพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องคดีอาญา พ.ศ. 2535 ซึ่งสามารถสรุปได้ดังนี้

พระราชบัญญัตินี้ได้กำหนดนิยามของคำว่า ความช่วยเหลือ หมายความว่า ความช่วยเหลือในเรื่องที่เกี่ยวกับการสืบสวนสอบสวน การฟ้องร้องคดี ริบทรัพย์สิน และการดำเนินการอื่นๆ ที่เกี่ยวเนื่องกับคดีอาญา ซึ่งการร้องขอความช่วยเหลือสามารถทำได้ 2 วิธี กรณีที่มีสนธิสัญญาว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญากับประเทศไทย ให้ส่งคำร้องขอไปยังหน่วยงานผู้ประสานงานกลาง กรณีที่ไม่มีสนธิสัญญาอาจทำได้โดยวิธีทางการทูต

หลักเกณฑ์เกี่ยวกับให้ความช่วยเหลือทางอาญาต้องปรากฏว่าต้องมีสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันกับประเทศผู้ร้องขอ หรือหากไม่มีต้องปรากฏว่าจะสามารถให้ความช่วยเหลือในทำนองเดียวกันได้หากประเทศเป็นผู้ร้องขอ การกระทำความผิดที่เป็นมูลเหตุให้

มีการร้องต้องเป็นความผิดตามกฎหมายไทย เว้นแต่สนธิสัญญาจะกำหนดไว้เป็นอย่างอื่น ทั้งนี้ ประเทศไทยสามารถปฏิเสธการให้ความช่วยเหลือดังกล่าวได้ หากการให้ความช่วยเหลือดังกล่าว จะกระทบอธิปไตยความมั่นคง หรือสาธารณประโยชน์ที่สำคัญของประเทศไทย หรือเกี่ยวกับ ความผิดทางการเมืองและการทหาร ประเทศไทยเองอาจร้องขอความช่วยเหลือจากต่างประเทศ ได้ในทำนองเดียวกันกับการให้ความช่วยเหลือซึ่งกันและกัน โดยให้เสนอเรื่องต่อผู้ประสานงาน กลาง

กฎหมายกำหนดการให้ความช่วยเหลือซึ่งกันและกันจะต้องทำผ่านผู้ประสานงาน กลางคืออัยการสูงสุดโดยจะทำหน้าที่รับคำร้องขอจากต่างประเทศแล้วทำการพิจารณาเบื้องต้นว่า การร้องขอดังกล่าวเป็นไปตามที่กำหนดในหลักเกณฑ์หรือไม่ หากไม่เป็นไปตามหลักเกณฑ์ก็ จะแจ้งให้ประเทศผู้ร้องขอทราบ แต่หากเป็นไปตามหลักเกณฑ์ที่กำหนดในกฎหมายก็ต้องส่ง เรื่องให้เจ้าหน้าที่ผู้มีอำนาจดำเนินการ ซึ่งหมายถึงเจ้าหน้าที่ตามที่กฎหมายภายในได้กำหนด อำนาจหน้าที่ไว้ เพื่อดำเนินการสอบปากคำบุคคล การรวบรวมพยานหลักฐานในชั้นสืบสวน สอบสวน การจัดส่งเอกสาร การค้นและการยึดเอกสารหรือพยานวัตถุ การสืบหาตัวบุคคล เป็นต้น เมื่อเจ้าหน้าที่ผู้มีอำนาจดำเนินการเสร็จแล้วก็จะส่งเรื่องกลับมาให้ผู้ประสานงานเพื่อส่งให้ ประเทศผู้ร้องขอต่อไป

4.2.2. กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

การทำธุรกรรมทางอิเล็กทรอนิกส์นับเป็นอีกทางเลือกหนึ่งในการติดต่อสื่อสารยุค โลกาภิวัตน์โดยอาศัยพัฒนาการทางเทคโนโลยีซึ่งมีความสะดวก รวดเร็ว และมีประสิทธิภาพ เอื้ออำนวยในการติดต่อสื่อสารระหว่างกัน แต่เนื่องจากรูปแบบใหม่ในการทำธุรกรรมทาง อิเล็กทรอนิกส์แตกต่างไปจากเดิมโดยสิ้นเชิง ไม่ว่าจะเป็นการติดต่อสื่อสารกันบนเครือข่ายโดยใช้ วิธีการทางอิเล็กทรอนิกส์ การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ ไปรษณีย์อิเล็กทรอนิกส์ หรือ วิธีการทางอิเล็กทรอนิกส์อื่นๆ ล้วนแต่ทำอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ มิได้ทำลงบน กระดาษดังเช่นเดิมอีกต่อไป

การนำวิธีการดังกล่าวมาใช้จึงส่งผลให้ต้องมีการรับรองสถานะทางกฎหมายของข้อมูล อิเล็กทรอนิกส์ให้เสมือนกับหนังสือ หรือหลักฐานเป็นหนังสือรับรองวิธีการส่งและรับข้อมูล อิเล็กทรอนิกส์ และจากจำนวนมูลค่าการทำธุรกรรมทางอิเล็กทรอนิกส์ในประเทศไทยที่ได้ ขยายตัวเพิ่มมากขึ้นอย่างต่อเนื่อง ทั้งนี้จะเห็นได้จากจำนวนการใช้คอมพิวเตอร์และอินเทอร์เน็ตที่ เพิ่มสูงขึ้น ส่งผลให้การซื้อขายทางอินเทอร์เน็ตเพิ่มสูงขึ้นเช่นเดียวกัน อย่างไรก็ตาม การทำ ธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทยยังไม่ขยายตัวมากเท่าที่ควร อันเนื่องมาจากปัญหา

ค่าใช้จ่ายในการใช้เทคโนโลยีสารสนเทศพื้นฐานสำหรับภาคธุรกิจค่อนข้างสูง เช่น การเชื่อมต่ออินเทอร์เน็ต และเทคโนโลยีที่มีความซับซ้อน รวมไปถึงปัญหาเรื่องความมั่นคงปลอดภัยในการทำธุรกรรมออนไลน์ ส่งผลให้ผู้ใช้บริการขาดความเชื่อมั่น และกระทบถึงมูลค่าและปริมาณการทำธุรกรรมทางอิเล็กทรอนิกส์ขยายตัวได้ไม่มากนัก²⁴

ดังนั้น การพัฒนาโครงสร้างพื้นฐานทางกฎหมายเทคโนโลยีสารสนเทศ จึงเป็นปัจจัยในการธุรกรรมทางอิเล็กทรอนิกส์ และเพื่อการพัฒนาสังคมและเสริมสร้างความแข็งแกร่งทางธุรกิจอุตสาหกรรมการค้าระหว่างประเทศ เพื่อส่งเสริมการติดต่อสื่อสารโดยวิธีการทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ (Reliability) และก่อให้เกิดความเชื่อมั่น (Confidence) ซึ่งเชื่อต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ พร้อมทั้งก่อให้เกิดกฎหมาย ข้อบังคับ หรือระเบียบที่เป็นเอกภาพ (Uniformity of Law Rule and Regulations) ที่สอดคล้องกับมาตรฐานที่นานาประเทศยอมรับ²⁵ จึงจัดทำกฎหมายฉบับนี้

ก. หลักการทั่วไปของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.

2544

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้ยกร่างตามแนวทางกฎหมายแม่แบบว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ (Model Law on Electronic Commerce 1996) และกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ (Model Law on Electronic Signature 2001) ของคณะกรรมการการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติ (United Nation Commission on International Trade Law: UNCITRAL) อันเป็นกฎหมายที่หลายประเทศยอมรับและใช้เป็นแนวทางในการยกร่างกฎหมาย โดยมีหลักการพื้นฐานที่สำคัญ²⁶ ดังนี้

²⁴ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับ สำนักงานเลขาธิการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, การสัมมนา สรุปผลการดำเนินงานของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, (4 กันยายน 2549), หน้า 7-8.

²⁵ ชัยวัฒน์ วงศ์วัฒนสานต์, ทวีศักดิ์ กอนันตกุล และสุรางคนา แก้วจันทน์, คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, สำนักงานเลขาธิการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, หน้า 10-11.

²⁶ UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nation, p 17 อ้างถึงใน คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, สำนักงานเลขาธิการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, หน้า 11-12.

หลักความเท่าเทียมกัน (Functional Equivalent Approach) หมายถึง ความเท่าเทียมกันระหว่างการใช้เอกสารที่อยู่ในรูปของกระดาษ (Paper-Based Document) และการใช้ข้อมูลคอมพิวเตอร์ (Computer-Based Information) กล่าวคือ การติดต่อสื่อสารหรือการผูกนิติสัมพันธ์ผ่านสื่อที่อยู่ในรูปของกระดาษ หรือการทำธุรกรรมผ่านสื่ออิเล็กทรอนิกส์จะต้องมีผลทางกฎหมายที่เท่าเทียมกัน ตามวัตถุประสงค์ในการรับรองผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ เช่นเดียวกับการทำธุรกรรมโดยวิธีการแบบปกติทั่วไปและสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ให้เท่าเทียมและมีผลในทางกฎหมาย อันเป็นการรองรับนิติสัมพันธ์ในรูปแบบใหม่ที่จัดทำขึ้นในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ให้เทียบเท่ากับนิติสัมพันธ์ต่างๆ ในรูปแบบเดิม รวมถึงการรับรองการใช้ลายมืออิเล็กทรอนิกส์ด้วยกระบวนการใดๆ ทางเทคโนโลยีให้เสมอด้วยการลงลายมือชื่อธรรมดา และการรับฟังพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยพยานหลักฐานที่เป็นต้นฉบับโดยสอดคล้องกับหลัก "พยานหลักฐานที่ดีที่สุด" (best evidence rule)

หลักความเป็นกลางทางเทคโนโลยีรวมทั้งหลักความเป็นกลางของสื่อ (Technology Neutrality / Media Neutrality) หมายถึง ในการติดต่อสื่อสารจะต้องไม่มีการเลือกปฏิบัติเทคโนโลยีใดเทคโนโลยีหนึ่งโดยเฉพาะ ทั้งนี้กฎหมายฉบับนี้ได้เปิดกว้างเพื่อรองรับการติดต่อสื่อสารด้วยวิธีการทางอิเล็กทรอนิกส์ในทุกูปแบบไม่ว่าจะเป็น โทรศัพท์ โทรสาร ข้อมูลดิจิทัล หรือการติดต่อสื่อสารผ่านทางคอมพิวเตอร์ซึ่งกำหนดให้โปรแกรมทำงานโดยอัตโนมัติ ทั้งนี้การวางหลักการดังกล่าวนี้ก็เพื่อรองรับเทคโนโลยีที่มีอยู่ในปัจจุบันและที่จะมีการพัฒนาขึ้นในอนาคต²⁷

อย่างไรก็ตามขอบเขตของการใช้บังคับของกฎหมายฉบับนี้ ครอบคลุมให้รองรับทั้งการทำธุรกรรมด้วยวิธีการทางแฟงและพาณิชย์ด้วยวิธีการทางอิเล็กทรอนิกส์ และยังรองรับการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐเพื่อรองรับภารกิจในส่วนที่เป็นงานรัฐบาลอิเล็กทรอนิกส์ด้วย อันเนื่องมาจากขอบเขตของการใช้บังคับของกฎหมายฉบับนี้ประกอบกับรูปแบบการประกอบธุรกิจที่มีความซับซ้อน การให้บริการภาครัฐที่มีความจำเป็นต้องดำเนินการภายใต้มาตรฐานหรือแนวทางที่มั่นคงและปลอดภัย จำเป็นต้องมีการกำกับดูแลการให้บริการทั้งภาครัฐและภาคเอกชน รวมทั้งการผลักดันมาตรการต่างๆ ที่รองรับการแก้ไขปัญหาและอุปสรรคต่างๆ ที่เกิดขึ้น จึงได้มีการตั้ง

²⁷ UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nation, p 18 para.8 อ้างถึงใน คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, สำนักงานเลขาธิการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, หน้า 11-12.

คณะทำงานคณะหนึ่งเพื่อทำหน้าที่วางนโยบายเพื่อผลักดัน ส่งเสริม ติดตามดูแล ตลอดจนเสนอแนะแนวทางแก้ไขอุปสรรคและปัญหาที่เกี่ยวข้องกับการประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ทั้งภายในประเทศและระหว่างประเทศ เรียกว่า "คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์"*

ข. กรอบการดำเนินงานด้านกฎหมายของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์²⁸

กรอบการดำเนินงานในปี 2547 ดังนี้ การจัดทำร่างพระราชกฤษฎีกากำหนดขอบเขตหรือข้อยกเว้นในการใช้บังคับกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กำหนดมิให้รูปแบบธุรกรรมบางประเภทดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ การจัดทำพระราชกฤษฎีกาการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ การจัดทำร่างพระราชบัญญัติว่าด้วยการกำกับดูแลการให้บริการชำระเงินทางอิเล็กทรอนิกส์ และร่างพระราชกฤษฎีกาว่าด้วยการกำกับดูแลการให้บริการออกใบรับรองอิเล็กทรอนิกส์ และการผลักดันร่างกฎหมายเทคโนโลยีสารสนเทศอื่นๆ

กรอบการดำเนินงานในปี 2548 ดังนี้ การตราพระราชกฤษฎีกาการกำกับดูแลผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ การบูรณาการกฎหมายเทคโนโลยีสารสนเทศและการสื่อสาร การจัดตั้งสถาบันกฎหมาย ICT

กรอบการดำเนินงานในปี 2549 ดังนี้ การตรากฎหมายลำดับรองภายใต้กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (Subordinate Laws under ETA) การจัดตั้งสถาบันกฎหมายเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Law Institution) การพัฒนากฎหมายเทคโนโลยีสารสนเทศ (IT Laws Development) และการระงับข้อพิพาททางออนไลน์ (Online Disputes Resolution)

4.2.3. กฎหมายเกี่ยวกับความคุ้มครองข้อมูลส่วนบุคคล

กฎหมายฉบับนี้อยู่ในระหว่างการยกร่าง เป็นกฎหมายที่จัดทำขึ้นเพื่อก่อให้เกิดการรับรองสิทธิและให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจถูกประมวลผล เปิดเผยหรือเผยแพร่ถึง

* มาตรา 36 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

²⁸ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับ สำนักงานเลขาธิการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, *การสัมมนา สรุปผลการดำเนินงานของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์*, หน้า 21-24.

บุคคลจำนวนมากได้ในระยะเวลาอันรวดเร็วโดยอาศัยพัฒนาการทางเทคโนโลยี จนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ในทางมิชอบอันเป็นการละเมิดต่อเจ้าของข้อมูล รวมถึงการคุ้มครองควบคุมการถ่ายโอนข้อมูลไปต่างประเทศ ทั้งนี้โดยคำนึงถึงการรักษาคุณภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัว เสรีภาพในการติดต่อสื่อสาร และความมั่นคงของรัฐ

โดยเหตุที่บทบัญญัติของรัฐธรรมนูญแห่งราชอาณาจักรไทย ได้ให้ความคุ้มครองสิทธิของบุคคลใน ครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว การกล่าว หรือโฆษณาแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใด ไปยังสาธารณชน อันเป็นการ ละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียงหรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อ สาธารณชน จึงต้องมีการกำหนดกลไกใน การให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นสิ่งที่สามารถประมวลผลและเผยแพร่ถึงบุคคล จำนวนมากได้โดยง่าย สะดวก และรวดเร็ว โดยอาศัยเทคโนโลยีสารสนเทศ อันทันสมัย ทั้งนี้ โดยกำหนดให้มีคณะกรรมการข้อมูลส่วนบุคคล เพื่อวางนโยบาย และกำกับดูแลเกี่ยวกับ การให้ความคุ้มครอง ข้อมูลส่วนบุคคลจึงเป็นสิ่งจำเป็น

ความเป็นส่วนตัว เป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์ที่สังคมยุคใหม่เกือบทุกประเทศให้ความสำคัญอย่างมาก ดังจะเห็นได้จากการรับรองหลักการดังกล่าวไว้ในรัฐธรรมนูญ หรือแม้บางประเทศจะไม่ได้บัญญัติรับรองไว้โดยตรงในรัฐธรรมนูญ แต่ก็ได้ตราบทบัญญัติรับรองไว้ในกฎหมายเฉพาะ

4.2.4. กฎหมายเกี่ยวกับการพัฒนาโครงสร้างพื้นฐานสารสนเทศ

กฎหมายฉบับนี้เป็นกฎหมายเพื่อก่อให้เกิดการส่งเสริม สนับสนุน และการพัฒนาโครงสร้างพื้นฐานสารสนเทศ อันได้แก่ โครงข่ายโทรคมนาคมเทคโนโลยีสารสนเทศ ทรัพยากรมนุษย์ และโครงสร้างพื้นฐานสารสนเทศที่สำคัญอื่นๆ อันเป็นปัจจัยพื้นฐานสำคัญในการพัฒนาสังคมและชุมชนโดยอาศัยกลไกของรัฐ เพื่อสนับสนุนให้ท้องถิ่นมีศักยภาพในการปกครองตนเอง พัฒนาเศรษฐกิจภายในชุมชน และนำไปสู่สังคมแห่งปัญญาและการเรียนรู้

4.2.5. กฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์

กฎหมายฉบับนี้เป็นกฎหมายเพื่อกำหนดกลไกสำคัญทางกฎหมายในการรองรับระบบการโอนเงินทางอิเล็กทรอนิกส์ ทั้งที่เป็นการโอนเงินระหว่างสถาบันการเงิน และระบบการชำระเงินรูปแบบใหม่ๆ ในรูปอิเล็กทรอนิกส์ ก่อให้เกิดความเชื่อมั่นต่อระบบการทำธุรกรรมทางการเงิน และการทำธุรกรรมทางอิเล็กทรอนิกส์มากยิ่งขึ้น

4.2.6. กฎหมายภายในอื่น ๆ ที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์

ก. พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 เพื่อกำหนดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ โดยกำหนดฐานความผิดเกี่ยวกับการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ตลอดจนฐานความผิดเกี่ยวกับการใช้ มีไว้เพื่อใช้ นำเข้า หรือส่งออก การจำหน่ายบัตรอิเล็กทรอนิกส์ปลอมหรือแปลง และลงโทษบุคคลที่ทำการผลิต หรือมีเครื่องมือในการผลิตบัตรดังกล่าว

ปัจจุบันการใช้เอกสาร วัตถุอื่นใดหรือข้อมูล ที่จัดทำขึ้นในลักษณะอิเล็กทรอนิกส์ เช่น บัตรเครดิต บัตรเดบิต บัตรสมาร์ตการ์ด หรือบัตรอื่นใดในลักษณะคล้ายกัน โดยมีวัตถุประสงค์เพื่อประโยชน์ในการชำระค่าสินค้า ค่าบริการ หรือหนี้อื่น หรือเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อย่างหนึ่งอย่างใด กำลังเพิ่มปริมาณประเภทการใช้งานอย่างแพร่หลายและปรากฏว่าได้มีการกระทำความผิดเกี่ยวกับบัตรและลักลอบนำข้อมูลอิเล็กทรอนิกส์ของผู้อื่นมาใช้อันส่งผลกระทบต่อเศรษฐกิจในวงกว้าง รวมถึงการรับฝากเงินโดยวิธีออกบัตรเงินฝากโดยธนาคารพาณิชย์ ตามกฎหมายว่าด้วยการธนาคารพาณิชย์ รวมตลอดถึงบริษัทเงินทุนตามกฎหมายว่าด้วยการประกอบธุรกิจเงินทุน และธุรกิจฟองซิเอร์และบัตรเงินฝากดังกล่าวเป็นตราสารซึ่งเปลี่ยนมือได้ จึงได้กำหนดมาตรการป้องกันการปลอมตราสารดังกล่าวเพื่อคุ้มครองประโยชน์ส่วนรวม ซึ่งอาจเกิดความเสียหายจากการใช้บัตรเงินฝากปลอม

มาตรการควบคุมทางอาญาในการประกอบธุรกิจบัตรเครดิตตามกฎหมายไทย เริ่มต้นจากบันทึกสถิติการกระทำความผิดเกี่ยวกับบัตรเครดิตในประเทศไทยของสำนักงาน ตำรวจเศรษฐกิจ สำนักงานตำรวจแห่งชาติ²⁹ ที่ได้มีการบันทึกไว้ตั้งแต่ปี 2538 พบว่ามีคดีเกี่ยวกับบัตรเครดิตเกิดขึ้นเป็นจำนวนกว่า 53 คดี สามารถจับผู้ต้องหามาดำเนินคดีได้รวม 46 คดี และสามารถจับผู้กระทำความผิดได้ 67 คน คิดเป็นมูลค่าความเสียหายรวม 21,583,374.03 บาท และในปีต่อๆ มาการกระทำความผิดเกี่ยวกับบัตรเครดิตในประเทศไทยก็มีจำนวนคดีเพิ่มขึ้นอย่างต่อเนื่องจนถึงปี พ.ศ. 2541 มีจำนวนคดีที่เกี่ยวกับบัตรเครดิตเกิดขึ้นรวม 63 คดี คิดเป็นมูลค่าความเสียหายกว่า 13 ล้านบาท

หลังจากนั้นปรากฏว่าจำนวนคดีและมูลค่าความเสียหายจากการกระทำความผิดที่เกี่ยวกับบัตรเครดิตลดลง โดยสถิติในปี 2545 ได้ชี้ให้เห็นว่าคดีที่เกี่ยวกับการกระทำความผิดใน

²⁹ พันตำรวจโทสุรเชษฐ ชีรวินิจ, โกงสะบัด โกงสะบัด เรื่อง บัตรเครดิตและเส้นเหลี่ยมกลโกง[ออนไลน์]. แหล่งข้อมูล : <http://www.law2day.com/hotstories/www.bot.or.th> [2001, September 20]

เรื่องบัตรเครดิตลดลงเหลือ 20 คดี คิดเป็นจำนวนความเสียหายรวม 5,822,708 บาท จากสถิติดังกล่าวจะเห็นได้ว่าอาชญากรรมที่เกี่ยวกับบัตรเครดิตได้ลดลง

อย่างไรก็ตาม หน่วยงานต่างๆ แสดงถึงความกังวลเกี่ยวกับการกระทำความผิดที่เกี่ยวกับบัตรเครดิตและได้ให้การสนับสนุนในการเสนอร่างกฎหมายการประกอบธุรกิจบัตรเครดิต โดยมีความเห็นว่าหากมีการออกกฎหมายขึ้นมาบังคับใช้แก่การประกอบธุรกิจโดยเฉพาะจะทำให้การใช้บังคับกฎหมายมีความคล่องตัวสูง และนอกจากนี้ ประเทศไทยยังไม่มีกฎหมายที่ใช้บังคับเกี่ยวกับบัตรเครดิตโดยเฉพาะอันอาจเป็นช่องทางที่ทำให้มีการเคลื่อนย้ายองค์การอาชญากรรมจากต่างชาติเข้ามาประกอบการกระทำที่ผิดกฎหมายเรื่องบัตรเครดิตในประเทศไทย

การกระทำความผิดที่เกี่ยวกับบัตรเครดิต อาจกระทำได้หลายรูปแบบ³⁰ เช่น

1. การลักบัตรเครดิต เดิมการลักทรัพย์ของผู้อื่นเป็นการกระทำความผิดตามประมวลกฎหมายอาญา มาตรา 334

2. การยกยอกบัตรเครดิต การกระทำความผิดโดยการยกยอกบัตรเครดิตเป็นความผิดตามประมวลกฎหมายอาญา มาตรา 352 การยกยอกบัตรเครดิตเป็นเรื่องที่ค่อนข้างก่อให้เกิดปัญหากับธนาคารและเจ้าของบัตรเครดิต เป็นอย่างมาก เนื่องจากเจ้าของบัตรเครดิตไม่อาจทราบได้ว่าบัตรเครดิตถูกนำไปใช้ประโยชน์ ซึ่งอาจเกิดขึ้นจาก กรณีที่เจ้าของบัตรปล่อยให้บัตรอยู่ในความครอบครองของบุคคลอื่นโดยที่เจ้าของบัตรไม่ได้อนุญาตให้ใช้บัตรเครดิตนั้น และเมื่อเจ้าของบัตรได้รับบัตรกลับคืนไปอยู่ในความครอบครอง ผู้กระทำความผิดก็ได้นำ บัตรไปใช้ประโยชน์เสียแล้ว กว่าจะทราบว่ามีการนำบัตรเครดิตไปใช้ก็ต่อเมื่อได้รับแจ้งหนี้จากธนาคารให้ไปชำระเงินที่เกิดจากการใช้บัตรเครดิต ในกรณีเช่นนี้เจ้าของบัตรจึงไม่อาจแจ้งอายัดการใช้บัตรต่อธนาคารได้

3. การปลอมบัตรเครดิต การปลอมบัตรเครดิต คือ การทำเลียนแบบบัตรที่แท้จริงการปลอมบัตรเครดิตนี้สามารถเทียบได้กับการกระทำความผิดในฐานปลอมเอกสารสิทธิ ตามประมวลกฎหมายอาญา มาตรา 265 สำหรับการปลอมบัตรเครดิตสามารถทำได้หลายวิธี เช่น โดยวิธีนำข้อมูลที่แท้จริงของบัตรเครดิตมาพิมพ์ข้อมูลบนบัตรและบันทึกข้อมูล บัตรเครดิตลงในแถบแม่เหล็กบันทึกข้อมูลของบัตรโดยเครื่องมือที่เรียกว่า Embossing machine ดังกล่าว ผู้กระทำความผิดอาจนำเข้ามาจากต่างประเทศหรืออาจจะทำขึ้นเองก็ได้ ซึ่งข้อมูลที่จะถูกบันทึก

³⁰ เรื่องเดียวกัน

ลงในแถบแม่เหล็กนั้นจะประกอบไปด้วยหมายเลขบัญชีของผู้ถือบัตร หมายเลขบัตร วันหมดอายุบัตร และชุดตัวเลขที่ธนาคารซึ่งเป็นผู้ออกบัตรเครดิตได้เข้ารหัสไว้ ข้อมูลดังกล่าวข้างต้นนี้เป็นข้อมูลที่ใช้ในการทำรายการจากการซื้อสินค้าและบริการ นอกจากนี้ ข้อมูลดังกล่าวยังเป็นข้อมูลที่ใช้นืนยันว่าบัตรเครดิตดังกล่าวเป็นบัตรเครดิตที่แท้จริงซึ่งธนาคารเป็นผู้ออกให้ โดยข้อมูลของบัตรเครดิตเหล่านี้ผู้กระทำความผิดอาจได้มาจากสำเนาใบบันทึกการขาย เครื่องถือปียีแถบแม่เหล็ก (Skimmer) การหลอกลวงให้มีการบอกข้อมูลของบัตรเครดิต หรือการนำข้อมูลจากการสั่งซื้อสินค้าผ่านทางอินเทอร์เน็ต เป็นต้น หลังจากที่ได้ทำการพิมพ์และบันทึกข้อมูลลงในแถบแม่เหล็กของบัตรเครดิตแล้วผู้กระทำความผิดจะลงลายมือชื่อไว้หลังบัตรเครดิต และนำบัตรเครดิตไปใช้ในการซื้อสินค้าและบริการ ในส่วนของผู้ให้บริการรับชำระเงินด้วยบัตรเครดิตก็จะไม่สามารถทราบได้ว่าบัตรเครดิตนั้นเป็นบัตรเครดิตปลอมเนื่องจากมีลายมือชื่อที่ตรงกับในบัตรเครดิต ซึ่งในท้องตลาดมีการซื้อขายบัตรเครดิตปลอมประเภทนี้กันในราคาประมาณใบละ 1,000 - 5,000 บาท

กรณีการปลอมบัตรเช่นเดียวกับวิธีแรกแต่แตกต่างตรงบัตรที่ใช้ปลอมซึ่งเรียกว่าพลาสติกขาว พลาสติกขาวนี้มีลักษณะเป็นแผ่นพลาสติกสีขาวมีขนาดเท่ากับบัตรเครดิต ผู้ที่กระทำความผิด โดยใช้พลาสติกขาวจะต้องร่วมมือกับร้านค้าเนื่องจากพลาสติกขาวไม่มีลักษณะที่เหมือนกับบัตรเครดิตเลย เช่น ไม่มีตราของธนาคารหรือลวดลายที่บัตรเครดิตนั้นๆ จะต้องมี เมื่อได้มีการปลอมบัตรเครดิตแล้วก็จะมีการนำมาสอดผ่านเครื่องรับบัตร หลังจากนั้นร้านค้าจะนำใบบันทึกการขายไปเรียกเก็บเงินจากธนาคารต่อไป สำหรับการปลอมบัตรเครดิตนั้น อาจเกิดจากการผู้กระทำความผิดที่เป็นเจ้าของบัตรเครดิตเอง ร้านค้า หรืออาชญากรก็ได้ ในกรณีของเจ้าของบัตรเครดิตนั้นจะนำข้อมูลบัตรเครดิตไปขายให้แก่ร้านค้าที่ทุจริต หรืออาชญากรเพื่อให้มีการนำข้อมูลไปทำบัตรปลอม หลังจากนั้นจึงไปแจ้งธนาคารว่าบัตรเครดิตหายหรือถูกลักขโมย เป็นต้น ในส่วนของร้านค้าก็จะนำบัตรของลูกค้าไปสอดผ่านเครื่องถือปียีแถบแม่เหล็กหรือนำข้อมูลจากใบบันทึกการขายมาใช้ในการปลอมบัตรเครดิต และในกรณีของผู้กระทำความผิดที่เป็นอาชญากร จะทำการเข้าถึงข้อมูลบัตรเครดิตด้วยวิธีการต่างๆ ดังที่ได้กล่าวมาแล้วและนำข้อมูลนั้นมาทำบัตรปลอม สำหรับผู้กระทำความผิดซึ่งทำการปลอมบัตรเครดิตของผู้อื่นนั้นอาจจะร่วมกับร้านค้าที่ทุจริตเพื่อทำการใช้จ่ายผ่านบัตรก็ได้

4. การฉ้อโกงโดยการแสดงตนเป็นคนอื่น เป็นการกระทำความผิดเมื่อบัตรเครดิตเป็นเอกสารสิทธิซึ่งสามารถนำไปใช้ประโยชน์ในทางทรัพย์สินได้แล้ว การที่บุคคลที่ไม่มีอำนาจกล่าวคือไม่ได้รับอนุญาตจากเจ้าของบัตรเครดิตให้นำบัตรเครดิตไปใช้ อาจจะด้วย วิธีการขโมยหรือยกยอกบัตรเครดิตของผู้อื่น ผู้ที่นำไปใช้นั้นจะต้องแสดงตนเป็นคนอื่น และถ้าบัตรเครดิตนั้น

ได้ถูกทำปลอมขึ้นและผู้กระทำความผิดได้นำบัตรเครดิตปลอมมาใช้ ซึ่งในกรณีที่มีการเอาบัตรผู้อื่นไปใช้ ผู้เสียหายคือธนาคารไม่ใช่ผู้ถือบัตรที่ถูกปลอมลายมือชื่อ

5. การปลอมใบบันทึกการขายและนำใบบันทึกการขายปลอมไปใช้ การกระทำความผิดที่เกิดขึ้นนี้อาจเป็นกรณีที่เกิดจากการกระทำความผิดของร้านค้า ที่ทุจริต หรือพนักงานของร้านค้านั้นๆ กระทำการทุจริตโดยที่เจ้าของร้านค้าไม่มีส่วนรู้เห็นในการกระทำความผิด ซึ่งในการชำระค่าสินค้าและบริการผ่านเครื่องรับบัตรเครดิตมีระบบการทำงาน ดังนี้ เมื่อมีการซื้อสินค้าหรือบริการ เจ้าของร้านหรือพนักงานของร้านจะนำบัตรเครดิตของลูกค้าไปรูดผ่านเครื่องรับบัตรเครดิตหรือที่เรียกกันว่า EDC Terminal ซึ่งเป็นเครื่องมือที่ใช้สำหรับการทำรายการชำระค่าซื้อขายสินค้าหรือบริการ ซึ่งร้านค้าจะต้องขออนุมัติติดตั้งเครื่องรับบัตรเครดิตและต้องเปิดบัญชีกับธนาคาร ธนาคารจะทำการตรวจสอบความน่าเชื่อถือของร้านค้าก่อนที่จะอนุมัติให้ติดตั้งเครื่องรับบัตร เครดิต ซึ่งร้านค้าจะต้องมีคู่สายโทรศัพท์เพื่อใช้ในการติดต่อกับธนาคารผ่านระบบเครือข่าย โดยที่การทำรายการชำระค่าสินค้าและบริการนั้น เจ้าของร้านจะทำการรูดบัตรเครดิตของลูกค้าผ่านเครื่องรับบัตรเครดิตเพื่อชำระค่าสินค้าหรือบริการ หลังจากที่เครื่องทำการแล้ว จะส่งข้อมูลการทำรายการไปยังธนาคาร ธนาคารจะทำการตรวจสอบและเก็บข้อมูลพร้อมกับส่งข้อมูลกลับไปยังเครื่องรับบัตรเครดิต เมื่อเครื่องรับบัตรเครดิตได้รับข้อมูลแล้วก็จะทำการตรวจสอบข้อมูลและจัดเก็บรายการที่ธนาคารส่งกลับมาพร้อมกับพิมพ์ใบบันทึกการขายสินค้า เจ้าของร้านหรือพนักงานก็จะนำมาให้ลูกค้าตรวจสอบและลงชื่อรับรองค่าสินค้าหรือค่าใช้จ่ายบริการที่ชำระด้วยบัตรเครดิตผ่านเครื่องรับบัตรเครดิตดังกล่าว การกระทำความผิดที่เกิดจากการปลอมใบบันทึกการขายของร้านค้าที่ทุจริตหรือพนักงานที่ทุจริตอาจกระทำได้โดย การนำบัตรเครดิตของลูกค้ามารูดชำระค่าสินค้าและบริการมากกว่า 1 ครั้ง หลังจากนั้นจึงค่อยปลอมลายมือชื่อของลูกค้าในบันทึกการขายที่เหลือ การใช้บัตรเครดิตปลอมทำรายการโดยอาจเป็นกรณีที่เจ้าของร้านหรือพนักงาน ทุจริตแอบทำซ้ำ (copy) ข้อมูลบัตรเครดิตของลูกค้าโดยเครื่องก๊อปปี้แถบแม่เหล็ก (Skimmer) หรือการยอมให้อาชญากรรมมารูดบัตรเครดิตชำระค่าสินค้าหรือบริการในร้านและให้ผลตอบแทนเป็นเงินหรือสิ่งของที่มีราคาน้อย กว่าที่มีการชำระเงินผ่านบัตรเครดิต และการทำใบบันทึกการขายปลอมโดยไม่มีการทำรายการจริง

จากเหตุการณ์การกระทำความผิดที่เกิดขึ้น กลไกสำคัญที่จะทำให้การใช้บริการบัตรเครดิตเป็นสิ่งที่น่าเชื่อถือ นอกจากนี้ยังเป็นการคุ้มครองผู้ถือบัตร ร้านค้าและธนาคารมิให้ต้องตกเป็นเหยื่อจากการกระทำที่ไม่ชอบด้วยกฎหมาย ภายหลังจากที่สำนักงานคณะกรรมการกฤษฎีกาได้ศึกษากฎหมายและการบังคับใช้กฎหมายเกี่ยวกับการประกอบธุรกิจบัตรเครดิตของต่างประเทศแล้วพบว่า ไม่มีการออกกฎหมายเพื่อนำมาบังคับใช้กับกรณีของการประกอบธุรกิจบัตรเครดิต

โดยเฉพาะ หากแต่ได้มีการนำบทบัญญัติของกฎหมายที่เกี่ยวข้องในแต่ละเรื่องมาบังคับใช้กับกรณีของการประกอบธุรกิจบัตรเครดิต ซึ่งในเรื่องนี้คณะกรรมการพิจารณาปรับปรุงกฎหมายอาญา สำนักงานคณะกรรมการกฤษฎีกา ได้พิจารณากฎหมายที่เกี่ยวข้องและวิเคราะห์โครงสร้างของประมวลกฎหมายอาญาฉบับปัจจุบันแล้ว เห็นว่า การกำหนดมาตรการทางอาญาในเรื่องนี้จะต้องกำหนดให้ครอบคลุมลักษณะของการกระทำความผิดที่เกี่ยวข้องทุกประเภท โดยการแก้ไขเพิ่มเติมประมวลกฎหมายอาญา เพื่อให้ครอบคลุมการกระทำความผิดเกี่ยวกับบัตรเครดิตอิเล็กทรอนิกส์ประเภทต่างๆ ได้อย่างกว้างขวางไม่เฉพาะเพียงกรณีของบัตรเครดิตเท่านั้น จึงได้เสนอแก้ไขเพิ่มเติมประมวลกฎหมายอาญาโดยเพิ่มบทบัญญัติความผิดเกี่ยวกับบัตรเครดิตอิเล็กทรอนิกส์³¹ โดยมีสาระสำคัญดังจะได้พิจารณาไปตามลำดับ ดังนี้

1. การกำหนดนิยามของคำว่า "บัตรเครดิตอิเล็กทรอนิกส์" โดยกำหนดให้บัตรเครดิตอิเล็กทรอนิกส์เป็นเอกสารสิทธิประเภทหนึ่งที่อยู่ภายใต้การออกให้แก่ผู้มีสิทธิใช้ซึ่งจะระบุชื่อผู้มีสิทธิใช้ หรือไม่ก็ตาม โดยที่รูปร่างและลักษณะของบัตรเครดิตอิเล็กทรอนิกส์นั้นอาจจะไม่ได้อยู่แต่ในรูปสี่เหลี่ยมผืนผ้าเท่านั้น แต่อาจอยู่ในรูปเอกสารหรือวัตถุอื่นใด หรืออาจจะมีการเปลี่ยนแปลงออกไปที่อาจมีขึ้นต่อไปในอนาคตก็ได้ และกรรมวิธีในการทำบัตรเครดิตดังกล่าวอาจกระทำได้โดยการบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ เช่น ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็ก เพื่อให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่มองเห็นและมองไม่เห็นด้วยตาเปล่า ที่ใช้แสดงถึงความเป็นผู้มีสิทธิใช้บัตรเครดิตอิเล็กทรอนิกส์นั้น จึงกำหนดนิยามโดยมุ่งหมายให้ครอบคลุมถึงบัตรเครดิตอิเล็กทรอนิกส์ประเภทต่างๆ ทุกชนิด

นอกจากนี้ ยังได้นิยามบัตรเครดิตอิเล็กทรอนิกส์ให้หมายความรวมถึง ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยไม่มีการออกเอกสารหรือวัตถุอื่นใดให้ เช่น การออกรหัส หมายเลขบัญชี หรือหมายเลขชุดทางอิเล็กทรอนิกส์ ให้ผู้มีสิทธิใช้เพื่อให้ผู้มีสิทธิใช้ได้รับรหัส หมายเลขบัญชี หรือหมายเลขชุดทางอิเล็กทรอนิกส์ดังกล่าว ในการสั่งซื้อสินค้าหรือบริการทางอินเทอร์เน็ตโดยที่ผู้ออกข้อมูลทางอิเล็กทรอนิกส์ให้แก่ผู้มีสิทธิใช้ไม่ได้ออกเอกสาร หรือวัตถุอื่นใดให้ผู้มีสิทธิใช้ไว้สำหรับแสดงความเป็นเจ้าของสิทธิแต่อย่างใด เป็นต้น

³¹ พันตำรวจโทสุรเชษฐ ชีรวินิจ, เอกสารอ้างอิงคำชี้แจงประกอบร่างพระราชบัญญัติการประกอบธุรกิจบัตรเครดิต พ.ศ. ของกระทรวงการคลังกฎหมายบัตรเครดิต (Law On Credit[Online], แหล่งข้อมูล : <http://www.law2day.com/hotstories/www.speciacrime.go.th/cardmember.htm> [2001, September 20]

2. กำหนดให้การกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ซึ่งได้กระทำนอกราชอาณาจักรถ้าผู้กระทำความผิดเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายร้องขอให้ลงโทษ หรือผู้กระทำความผิดเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

3. กำหนดความผิดสำหรับการปลอมหรือแปลง หรือการทำหรือมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลของบัตรอิเล็กทรอนิกส์ ถ้าได้กระทำเพื่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชนเป็นความผิด โดยกำหนดให้การกระทำความผิดฐานทำหรือมีเครื่องมือหรือวัตถุสำหรับการให้ได้มาซึ่งข้อมูลของบัตรอิเล็กทรอนิกส์นั้น เช่น การใช้ อุปกรณ์หรือเครื่องมือสำหรับดูดข้อมูลในบัตรอิเล็กทรอนิกส์ (Skimmer) แล้วเก็บไว้ในหน่วยความจำของอุปกรณ์หรือเครื่องมือดังกล่าวเพื่อใช้ในการปลอมบัตรอิเล็กทรอนิกส์ต่อไป เป็นความผิด

4. กำหนดความผิดสำหรับการนำเข้าหรือส่งออกซึ่งบัตรอิเล็กทรอนิกส์ปลอมหรือแปลงหรือเครื่องมือสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลของบัตรอิเล็กทรอนิกส์เป็นความผิด

5. กำหนดความผิดสำหรับการใช้หรือจำหน่ายบัตรอิเล็กทรอนิกส์ที่ได้ทำปลอมหรือแปลงขึ้นตามมาตรา 269/1* หรือมีบัตรดังกล่าวเพื่อใช้หรือจำหน่ายเป็นความผิด ทั้งนี้ ถ้าผู้กระทำความผิดฐานใช้หรือจำหน่ายหรือมีไว้ในครอบครองเพื่อใช้หรือจำหน่ายบัตรดังกล่าวเป็นผู้กระทำความผิดปลอมหรือแปลงด้วย ให้ลงโทษผู้กระทำความผิดแต่เฉพาะความผิดฐานปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ตามมาตรา 269/4** เพียงกระทงเดียว

6. กำหนดความผิดสำหรับการใช้หรือมีไว้เพื่อใช้ซึ่งบัตรอิเล็กทรอนิกส์หรือข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชนเป็นความผิด ทั้งนี้ เพื่อให้ผู้ถือหรือครอบครองหรือเก็บได้ซึ่งบัตรอิเล็กทรอนิกส์หรือข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ และนำไปใช้โดยมิชอบเป็นความผิด

* ประมวลกฎหมายอาญา มาตรา 269/1 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ผู้ที่ทำบัตรอิเล็กทรอนิกส์ปลอมขึ้นทั้งฉบับหรือแม้แต่นบางส่วนใด เดิมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใด ในบัตรอิเล็กทรอนิกส์ที่แท้จริง โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน ถ้าได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นบัตรอิเล็กทรอนิกส์ที่แท้จริงหรือเพื่อใช้ประโยชน์อย่างหนึ่งอย่างใด ผู้นั้นกระทำความผิดฐานปลอมบัตรอิเล็กทรอนิกส์

** ประมวลกฎหมายอาญา มาตรา 269/4 ผู้ใดใช้หรือมีไว้เพื่อใช้ซึ่งบัตรอิเล็กทรอนิกส์ปลอมอันได้มาโดยรู้ว่าเป็นของที่ปลอมหรือแปลงขึ้น

7. กำหนดให้การกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ถ้าเป็นการกระทำที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้เพื่อประโยชน์ในการชำระค่าสินค้า หรือบริการ หรือหนี้อื่นแทน การชำระด้วยเงินสด หรือใช้เบิกถอนเงินสด ผู้กระทำต้องระวางโทษหนักกว่าที่บัญญัติไว้ในมาตรานั้นๆ ที่หนึ่ง อื่นๆ กรณีการกำหนดอัตราโทษสำหรับการกระทำความผิดในหมวดดังกล่าวได้พิจารณาเปรียบเทียบกับความผิดเกี่ยวกับเอกสารสิทธิโดยเห็นว่าการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ก็คือการกระทำความผิดเกี่ยวกับเอกสารสิทธินั่นเอง ทั้งนี้ เนื่องจากการใช้บัตรอิเล็กทรอนิกส์นั้นมีวัตถุประสงค์เพื่อใช้ประโยชน์ในการชำระค่าสินค้า ค่าบริการ หรือหนี้อื่นแทนการชำระด้วยเงินสด เป็นต้น จึงมีลักษณะเดียวกันกับเอกสารสิทธิที่เป็นเอกสารแห่งการก่อให้เกิดเปลี่ยนแปลง โอน สงวน หรือระงับซึ่งสิทธิ แต่อย่างไรก็ตาม เนื่องจากการกระทำผิดฐานดังกล่าวเป็นการกระทำที่มีผลกระทบต่อสภาพเศรษฐกิจและสังคมของประเทศและยังมีการกระทำอย่างแพร่หลาย จึงควรกำหนดอัตราโทษให้สูงขึ้น เพื่อความเหมาะสมในการป้องกันและปราบปรามความผิดร้ายแรง

ข. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

คณะกรรมการพิจารณาเรื่องการปิดกั้นการเข้าถึงข้อมูลข่าวสารในอินเทอร์เน็ตซึ่งมีอำนาจหน้าที่พิจารณาเรื่องการปิดกั้นการเข้าถึงข่าวสารในอินเทอร์เน็ต โดยทำการศึกษาข้อเท็จจริงและกำหนดหลักเกณฑ์หรือแนวทางปฏิบัติ เกี่ยวกับการเผยแพร่ข้อมูลข่าวสารและการเข้าถึงข้อมูลข่าวสารในอินเทอร์เน็ต ศึกษาถึงปัญหา สาเหตุของปัญหา ข้อเท็จจริง ผลกระทบ และแนวทางแก้ไข ในกรณีที่มีการปิดกั้นการเข้าถึงข้อมูลข่าวสารในอินเทอร์เน็ต มีอำนาจในการสอบสวนข้อเท็จจริง และเรียกให้บุคคลใด ให้ถ้อยคำหรือให้ส่งวัตถุ เอกสาร หรือพยานหลักฐานมาประกอบการพิจารณา มีอำนาจในการสอบสวนข้อเท็จจริง และเรียกให้บุคคลใด ให้ถ้อยคำหรือให้ส่งวัตถุ เอกสาร หรือพยานหลักฐานมาประกอบการพิจารณารายงานผลการดำเนินการให้คณะกรรมการข้อมูลข่าวสารของราชการทราบ

4.3 มิติด้านการบริหาร

ประเทศไทยมีการเตรียมความพร้อมด้านหน่วยงานและองค์การการจัดตั้งหน่วยงานกำกับดูแล รวมถึงการเตรียมการเกี่ยวกับความปลอดภัยระบบคอมพิวเตอร์และเครือข่าย ดังนี้

1. การก่อตั้งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

รัฐบาลไทยได้เล็งเห็นถึงความสำคัญในการพัฒนาด้านเทคโนโลยีสารสนเทศ (Information and Communication Technology : ICT) ของประเทศอย่างเป็นรูปธรรม ตาม

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย พ.ศ. 2545 – 2553 (ICT Master Plan 2002-2010) ซึ่งได้รับความเห็นชอบจากคณะรัฐมนตรี เมื่อวันที่ 25 กันยายน พ.ศ. 2545 ทางคณะรัฐมนตรีจึงได้เสนอให้มีการจัดตั้งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ตามพระราชบัญญัติการปฏิรูประบบราชการ ในเดือนตุลาคม พ.ศ. 2545 โดยมีภารกิจหลักในการกำหนดการบริหารจัดการกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศและการสื่อสารให้สอดคล้องกับนโยบายเทคโนโลยีสารสนเทศ พ.ศ. 2544-2553 (IT 2010) ของประเทศไทย และแผนแม่บทการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย พ.ศ. 2545-2549 รวมถึงการวิเคราะห์แนวทาง การวางแผนและประสานงานฐานะศูนย์กลางการประสานแผนปฏิบัติการทางด้านเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานภาครัฐและเอกชน ตลอดจนองค์การภายในและต่างประเทศ รวมถึงภารกิจในการสนองนโยบายภาครัฐในการนำเทคโนโลยีสารสนเทศและการสื่อสารมาพัฒนาในภาครัฐ ภาคการผลิต ภาคการพาณิชย์ ภาคการศึกษา และภาคสังคม³²

นโยบายส่วนหนึ่งที่สำคัญของกระทรวงคือ นโยบายด้านข้อมูล (Information) ซึ่งเป็นงานเชิงป้องกันโดยเน้นการสร้างระบบรักษาความปลอดภัยของคอมพิวเตอร์และเครือข่ายอย่างจริงจัง หน่วยงานกำกับดูแลจึงได้มีการจัดตั้งหน่วยงานกำกับดูแลขึ้นคือกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

2. ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (Thai Computer Emergency Response Team : ThaiCERT)

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย เป็นหน่วยงานด้านการรักษาความปลอดภัย ในสังกัดของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ซึ่งได้รับการจัดตั้งขึ้นเมื่อปี พ.ศ. 2543 โดยมีภารกิจในการบริหารตอบสนองเหตุการณ์ต่างๆ ที่อาจกระทบความมั่นคงของระบบคอมพิวเตอร์และเครือข่ายของประเทศไทย เพื่อรับมือกับปัญหาฉุกเฉินด้านความมั่นคงคอมพิวเตอร์ การเผยแพร่และการให้คำแนะนำในการปฏิบัติเพื่อความปลอดภัยคอมพิวเตอร์

3. สำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบและสำนักคดีเทคโนโลยีและสารสนเทศ

³² ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย พ.ศ. 2545-2549, (กรุงเทพฯ : สำนักงานเลขาธิการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, 2545), หน้า 32.

อาชญากรรมคอมพิวเตอร์อาจมีผลกระทบอย่างสำคัญต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน ความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของ ประเทศหรือที่มีลักษณะเป็นการกระทำความผิดข้ามชาติหรือเป็นการกระทำขององค์กรอาชญากรรมโดยมีขอบเขตความรับผิดชอบที่วราชอาณาจักร ทำให้กรมสอบสวนคดีพิเศษ ภายใต้กระทรวงยุติธรรม ได้เล็งเห็นความสำคัญและได้จัดตั้งสำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบและสำนักคดีเทคโนโลยีและสารสนเทศขึ้น เป็นหน่วยงานด้านการรักษาความปลอดภัย เพื่อป้องกันการเกิดขึ้นของคดีและลดความเสียหายที่เกิดขึ้นของคดีที่เกี่ยวข้องกับการกระทำความผิดโดยใช้คอมพิวเตอร์และเครือข่ายเป็นเครื่องมือในการดำเนินการ โดยใช้วิธีการติดตาม สอบสวน เผื่อระวัง ตรวจสอบการกระทำความผิด โดยมีการปฏิบัติงาน ดังนี้ ปฏิบัติงานด้านการป้องกันปราบปราม และสืบสวนผู้กระทำความผิดทางคดีเทคโนโลยีและสารสนเทศ ด้านการสอบสวนและดำเนินคดีกับผู้กระทำความผิดทางคดีเทคโนโลยีและสารสนเทศ ด้านวิเคราะห์และพิสูจน์ความผิดทางคดีเทคโนโลยีและสารสนเทศ ด้านการป้องกันปราบปราม สืบสวนและสอบสวนผู้กระทำความผิดในคดีอื่นตามที่ได้รับมอบหมาย และการดำเนินการวิเคราะห์ วิจัย วางแผนงาน บริหารจัดการและประสานงานเพื่อการป้องกันและปราบปราม การกระทำความผิดทางคดีเทคโนโลยีและสารสนเทศ การเก็บรักษาพยานหลักฐานและของกลางในคดี รวมถึงการปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

ทั้งนี้ อำนาจหน้าที่ของสำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ ดำเนินการเกี่ยวกับการเสนอแนะนโยบาย กำกับดูแล สนับสนุน ส่งเสริม วางแผนและติดตามประเมินผลการทำงานเทคโนโลยีสารสนเทศมาใช้พัฒนาระบบงานของกรมสอบสวนคดีพิเศษ ดำเนินการเกี่ยวกับการวางระบบหรือพัฒนาระบบงานคอมพิวเตอร์และการเขียนโปรแกรมคอมพิวเตอร์ของกรมสอบสวนคดีพิเศษ ดำเนินการเกี่ยวกับการพัฒนาระบบ รูปแบบและมาตรฐานการสำรวจ การจัดเก็บ การประมวลผลและการใช้ประโยชน์ข้อมูลของกรมสอบสวนคดีพิเศษ ดำเนินการติดตามข้อมูลทางด้านอิเล็กทรอนิกส์ คอมพิวเตอร์ และสื่อทางเทคโนโลยีสารสนเทศ ดำเนินการตรวจพิสูจน์ทางวิทยาศาสตร์เกี่ยวกับลายพิมพ์นิ้วมือ ร่องรอยทุจริตและตรวจสอบสถานที่เกิดเหตุ ตลอดจนการตรวจพิสูจน์ทางอิเล็กทรอนิกส์หรือการสื่อสารใด ๆ ดำเนินการสรรหาและจัดให้มีผู้เชี่ยวชาญผู้ชำนาญพิเศษในการตรวจพิสูจน์หลักฐานและการเงินการบัญชี ดำเนินการวิจัยและพัฒนาอุปกรณ์พิเศษสำหรับเจ้าหน้าที่ของกรมสอบสวนคดีพิเศษ และรวมถึงปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย และดำเนินการเกี่ยวกับงานประมวลผลข้อมูลและสถิติของกรมสอบสวนคดีพิเศษ

กรมสอบสวนคดีพิเศษยังได้มีการจัดตั้งสำนักกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ ซึ่งบางอำนาจหน้าที่สามารถสนับสนุนการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ได้ เช่น การติดต่อและประสานงานกับองค์กรและหน่วยงานต่างประเทศด้านความช่วยเหลือและร่วมมือในการป้องกัน และปราบปรามอาชญากรรมระหว่างประเทศ การส่งผู้ร้ายข้ามแดน การโอนตัวนักโทษ และการดำเนินคดี ที่เกี่ยวข้องกับชาวต่างประเทศ การติดต่อและประสานงานกับองค์กรและหน่วยงานต่างประเทศด้านความช่วยเหลือและร่วมมือในด้านการศึกษา ฝึกอบรม ตู๋งาน และวิจัย ณ ต่างประเทศ รวมทั้งปฏิบัติงานเป็นผู้ช่วยทูตด้านคดีพิเศษ การปฏิบัติงานด้านการป้องกัน ปราบปราม และสืบสวนผู้กระทำความผิดด้านอาชญากรรมระหว่างประเทศ การปฏิบัติงานด้านการสอบสวนและดำเนินคดีกับผู้กระทำความผิดด้านอาชญากรรมระหว่างประเทศ การปฏิบัติงานวิเคราะห์และพิสูจน์ความผิดทางคดีอาชญากรรมระหว่างประเทศ การดำเนินการเก็บรักษาพยานหลักฐานและของกลางในคดีและปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

4. ศูนย์อาชญากรรมทางเทคโนโลยี (Hi – Tech Crime Center)

สำนักงานตำรวจแห่งชาติได้ดำเนินการจัดตั้งศูนย์อาชญากรรมทางเทคโนโลยี ซึ่งมีภารกิจต่อต้านการก่อการร้ายและอาชญากรรมคอมพิวเตอร์ โดยเน้นการดูแลการใช้คอมพิวเตอร์เป็นเครื่องมือประกอบอาชญากรรมทุกรูปแบบ และป้องกันการถูกโจมตีระบบคอมพิวเตอร์ในกิจกรรมสาธารณะ นอกจากนี้ จะมีการเก็บรวบรวมพยานหลักฐานที่เกี่ยวข้องกับการประกอบอาชญากรรมโดยใช้คอมพิวเตอร์เป็นเครื่องมือตรวจสอบเว็บไซต์ของกลุ่มก่อการร้าย

จากการดำเนินการทางด้านบริหารนี้จะเห็นได้ว่าประเทศไทยเองมีการเตรียมความพร้อมเกี่ยวกับหน่วยงานที่ต้องทำหน้าที่ติดต่อประสานงาน และเก็บรักษาข้อมูลคอมพิวเตอร์ให้สอดคล้องกับบทบัญญัติในอนุสัญญา แม้ว่าหน่วยงานที่สามารถดำเนินการเกี่ยวกับการบังคับใช้กฎหมายเกี่ยวกับการส่งผู้ร้ายข้ามแดนหรือการช่วยเหลือซึ่งกันและกันจะยังคงเป็นหน่วยงานอัยการก็ตามที่ แต่จากวัตถุประสงค์ของหน่วยงานดังกล่าวข้างต้นนั้นก็เน้นที่การปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่น ซึ่งเพียงพอที่จะแสดงให้เห็นว่าประเทศไทยได้มีศูนย์ติดต่อประสานงานที่มีสมรรถภาพเพียงพอที่จะติดต่อสื่อสารกับศูนย์ติดต่อประสานงานกับอื่นโดยวิธีการที่รวดเร็ว แม้ว่าศูนย์ติดต่อประสานงานดังกล่าวไม่ได้เป็นส่วนหนึ่งของหน่วยงานที่ทำหน้าที่รับผิดชอบเกี่ยวกับการช่วยเหลือซึ่งกันและกันระหว่างประเทศและการส่งผู้ร้ายข้ามแดน ศูนย์ก็สามารถทำให้เกิดความแน่นอนว่าสามารถที่จะติดต่อประสานงานกับหน่วยงานดังกล่าวโดยวิธีการที่รวดเร็วทันทีได้ ซึ่งสอดคล้องกับบทบัญญัติในอนุสัญญา

4.4 มิติด้านตุลาการ

ในการเตรียมการทางด้านตุลาการไม่ปรากฏความเคลื่อนไหวบทบาททางด้านตุลาการมากนัก อย่างไรก็ตามพระราชบัญญัตินี้ได้กำหนดให้ศาลมีบทบาทในการบังคับใช้กฎหมายกับผู้กระทำความผิดเช่นความผิดอื่นๆ ซึ่งสำนักงานศาลยุติธรรมได้ให้ความสนใจและให้ความสำคัญกับการพัฒนาด้านเทคโนโลยีสารสนเทศเพื่อนำมาสนับสนุนการพิจารณาพิพากษาคดีของศาลยุติธรรมให้มีประสิทธิภาพมากยิ่งขึ้น โดยให้คณะผู้พิพากษาและเจ้าหน้าที่เข้าร่วมประชุมเจรจาระหว่างศาลยุติธรรมและกระทรวงกฎหมายของสิงคโปร์ในโครงการ Civil Service Exchange เพื่อความร่วมมือระหว่างประเทศเกี่ยวกับการแลกเปลี่ยนข้อมูลด้านระบบการไกล่เกลี่ยข้อพิพาทและการพัฒนาระบบเทคโนโลยีสารสนเทศของศาลทั้งสองประเทศ ดังนั้นหากแนวโน้มของผู้กระทำความผิดเพิ่มสูงขึ้น ตุลาการก็ควรจะมียุทธศาสตร์ที่ชัดเจนมากขึ้น

4.5 มิติด้านอื่นๆ

4.5.1 มิติด้านเทคโนโลยี

มาตรการทางด้านเทคโนโลยีเป็นการต่อต้านอาชญากรรมทางคอมพิวเตอร์โดยผู้ใช้งานคอมพิวเตอร์สามารถใช้หรือติดตั้งเทคโนโลยีต่างๆที่มีอยู่ในปัจจุบัน เช่น การติดตั้งระบบการตรวจจับการบุกรุก (Intrusion Detection) หรือการติดตั้งกำแพงไฟ (Firewall) เพื่อป้องกันหรือรักษาคอมพิวเตอร์ให้มีความปลอดภัย ซึ่งนอกเหนือจากการติดตั้งเทคโนโลยีแล้ว การตรวจสอบเพื่อประเมินความเสี่ยง เช่น การจัดทำมีระบบวิเคราะห์ความเสี่ยงและการให้การรับรอง (Analysis Risk and Security Certification) รวมทั้งวินัยของผู้ปฏิบัติงานก็เป็นสิ่งสำคัญที่ต้องได้รับการปฏิบัติอย่างเคร่งครัดและสม่ำเสมอ มิเช่นนั้นการติดตั้งเทคโนโลยีที่มีประสิทธิภาพเพื่อใช้ในการป้องกันปัญหาดังกล่าวก็ไม่ก่อให้เกิดประโยชน์แต่อย่างใด³³

การสร้างระบบป้องกันให้กับเครือข่ายคอมพิวเตอร์ เช่น เทคโนโลยีใหม่ในการรักษาความปลอดภัยโดยใช้การตรวจสอบประวัติ (Reputation Based Security Technology) ที่สามารถรับมือกับมัลแวร์ใหม่ๆ และภัยคุกคามที่รุนแรงในปัจจุบัน และยังมีระบบควบคุมอัจฉริยะที่รองรับการเข้าใช้ฐานข้อมูลอย่างมีประสิทธิภาพด้วย

4.5.2 มิติด้านสังคม

³³ [ออนไลน์], แหล่งข้อมูล: http://www.ictlaw.thaigov.net/cc/general_info.html (2010, January 11)

มาตรการทางสังคมในการแก้ปัญหาเฉพาะของประเทศไทย สืบเนื่องจากในปัจจุบัน ปรากฏข้อเท็จจริงพบว่าสังคมไทยกำลังเผชิญกับปัญหาการใช้อินเทอร์เน็ตไปในทางมิชอบ หรือ ฝ่าฝืนต่อบทบัญญัติของกฎหมายโดยการเผยแพร่เนื้อหาอันไม่เหมาะสม ไม่ว่าจะเป็นสื่อลามก อนาจาร ข้อความหมิ่นประมาท การชักจูง ล่อลวง หลอกลวงเด็กและเยาวชนไปในทางที่เสียหาย โดยการสร้างความสัมพันธ์ผ่านทางโปรแกรมคอมพิวเตอร์ เช่น ไฮไฟว์ หรือพฤติกรรมอื่นอันเป็น ภัยต่อสังคม โดยคาดการณ์ว่าการกระทำหรือพฤติกรรม ดังกล่าวมีสัดส่วนเพิ่มสูงขึ้นตามสถิติ เพิ่มขึ้นของผู้ใช้อินเทอร์เน็ตอันส่งผลกระทบต่อเด็กและเยาวชนไทย โดยปัญหาดังกล่าวอยู่ใน ความสนใจของสังคมไทยเป็นอย่างมาก ดังนั้น หน่วยงานทั้งภาครัฐและเอกชนจึงรณรงค์ในการ ป้องกันปัญหาดังกล่าวร่วมกันเพื่อดูแลและปกป้องเด็กและเยาวชนจากผลกระทบของ อาชญากรรมทางคอมพิวเตอร์ ดังต่อไปนี้³⁴

1. มาตรการเร่งด่วนของคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติคณะกรรมการ เทคโนโลยีสารสนเทศแห่งชาติ (กทสช.) เกี่ยวกับการป้องกันและปราบปรามการเผยแพร่เนื้อหาที่ไม่เหมาะสมทางอินเทอร์เน็ต โดยกำหนดให้หน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องประสานความร่วมมือตามลำดับ เริ่มตั้งแต่ การบันทึกข้อมูลเกี่ยวกับผู้ใช้อินเทอร์เน็ตเพื่อประโยชน์ในการ สืบสวนสอบสวน และรวบรวมพยานหลักฐาน การสกัดกั้นการเผยแพร่เนื้อหาอันไม่เหมาะสม รวมทั้งการรับแจ้งเหตุเมื่อมีกรณีดังกล่าวเกิดขึ้น เช่น การกำหนดให้การสื่อสารแห่งประเทศไทย และบริษัท ทศท. คอร์ปอเรชั่น จำกัด (มหาชน) (องค์การโทรศัพท์แห่งประเทศไทย) กำหนด เงื่อนไขให้ผู้ให้บริการอินเทอร์เน็ต (ISP) และผู้ให้บริการโทรศัพท์ทุกรายให้ความร่วมมือในการตั้ง นาฬิกาของอุปกรณ์สื่อสารและอุปกรณ์ให้บริการให้ตรงกัน เพื่อบันทึกข้อมูลการบันทึกการเข้า- ออกจากระบบ รวมทั้งการบันทึกและเก็บข้อมูลการใช้อินเทอร์เน็ตของผู้ใช้บริการ (Log File for User Access) พร้อมหมายเลขโทรศัพท์ต้นทาง (Caller ID) เป็นระยะเวลาอย่างน้อย 3 เดือน

การกำหนดให้ผู้ให้บริการทุกรายระงับการเผยแพร่เนื้อหาอันมีข้อความหรือภาพไม่ เหมาะสม และสกัดกั้นมิให้ผู้ใช้บริการเข้าถึงแหล่งข้อมูลดังกล่าวในกรณีที่แหล่งข้อมูลดังกล่าวมา จากแหล่งอื่น รวมถึงการกำหนดให้สำนักงานตำรวจแห่งชาติประสานงานกับหน่วยงานที่เกี่ยวข้อง ทั้งฝ่ายเทคนิคและฝ่ายกฎหมายในการจัดตั้งศูนย์รับแจ้งเหตุบนอินเทอร์เน็ต (Hot Line) เมื่อพบ เห็นการเผยแพร่เนื้อหาที่ไม่เหมาะสมทางอินเทอร์เน็ตทั้งทางโทรศัพท์และอีเมล (Internet-hotline@police.go.th) รวมทั้งสอดส่องดูแลการให้บริการของร้านบริการอินเทอร์เน็ตคาเฟ่ไป ในทางที่ไม่ชอบ

³⁴ เรื่องเดียวกัน

2. การดำเนินการจัดทำฐานข้อมูลรวบรวมเว็บไซต์หรือ พฤติกรรมการใช้อินเทอร์เน็ตในทางไม่เหมาะสม เพื่อประโยชน์ในการศึกษา ติดตาม และเฝ้าระวังพฤติกรรมในการใช้อินเทอร์เน็ตหรือการเผยแพร่เนื้อหาทางอินเทอร์เน็ตในทางไม่เหมาะสมในรูปแบบหลากหลายที่มีซับซ้อนมากขึ้นเรื่อยๆ และบางครั้งยากต่อการติดตาม เพื่อใช้ข้อมูลในการสนับสนุนให้แก่หน่วยงานที่เกี่ยวข้อง รวมทั้งเพื่อประโยชน์ในการรณรงค์ป้องกันเด็กและเยาวชนจากปัญหาดังกล่าวด้วย พบว่าแม้บางกรณีจำเป็นต้องใช้มาตรการในการปิดกั้นการเผยแพร่เนื้อหาของเว็บไซต์ดังกล่าว แต่ก็อาจนำไปสู่ปัญหาและอุปสรรคในการติดตามพฤติกรรมก่อกวนเนื้อหาซึ่งส่งผลกระทบต่อสังคม รวมทั้งการรวบรวมพยานหลักฐานเกี่ยวกับผู้กระทำความผิดได้เช่นกัน เพราะแม้ปิดกั้นการเผยแพร่ข้างต้นแต่ผู้เผยแพร่เนื้อหาดังกล่าวก็สามารถย้ายฐานข้อมูลของตนไปเผยแพร่โดยใช้ชื่อเว็บไซต์ใหม่หรือใช้ชื่ออื่นได้โดยง่าย สะดวก และรวดเร็วมาก และในกรณีที่มีการปิดกั้นมิให้มีการเผยแพร่เนื้อหาแม้จะทำให้ไม่สามารถเรียกดูเนื้อความดังกล่าวจากประเทศไทยได้ แต่หากการเผยแพร่เนื้อหาหรือการใช้อินเทอร์เน็ตในทางไม่ชอบเป็นการกระทำโดยคนไทย เด็ก หรือเยาวชนไทย เนื้อความดังกล่าวก็ยังคงเผยแพร่อยู่ต่อไปโดยสามารถเรียกดูได้โดยใช้อินเทอร์เน็ตในประเทศอื่นอยู่ต่อไป ดังนั้น บางครั้งการใช้มาตรการปิดกั้นโดยเคร่งครัดหรือมาตรการรุนแรงอื่นจึงอาจกลายเป็นมาตรการที่เสมือนหนึ่งรัฐกำลังทอดทิ้งกลุ่มคนไทย เด็กหรือเยาวชนดังกล่าว โดยยังไม่ได้ให้โอกาสอย่างเพียงพอแก่บุคคลซึ่งอาจกระทำการข้างต้นไปโดยรู้เท่าไม่ถึงการณ์เพื่อนำไปสู่การปรับเปลี่ยนพฤติกรรมหรือทัศนคติของบุคคลดังกล่าว อันจะสามารถช่วยลดปัญหาซึ่งส่งผลกระทบต่อสังคมในระยะยาวลงได้อย่างแท้จริงแต่อย่างใด ทั้งนี้ ข้อมูลดังกล่าวมิได้ทำการเผยแพร่ข้อมูลเพื่อป้องกันมิให้มีการนำข้อมูลเหล่านั้นไปใช้ในทางไม่เหมาะสมต่อไป

3. การจัดทำรายงานผลการสำรวจกลุ่มผู้ใช้อินเทอร์เน็ตในประเทศไทยประจำปี นับตั้งแต่ปี 2543 เรื่อยมา โดยเป็นการสำรวจการใช้แบบทั่วไปรวมถึงการเผยแพร่เนื้อหาอันไม่เหมาะสม

4. การรณรงค์การท่องอินเทอร์เน็ตอย่างปลอดภัยและได้ประโยชน์ด้วยการให้ความรู้แก่ผู้ใช้อินเทอร์เน็ตอย่างถูกต้อง การปลูกฝังคุณธรรม จรรยาบรรณ หรือจริยธรรมนับเป็นมาตรการที่ดีที่สุดในการปกป้องเด็ก เยาวชน และสังคมจากการใช้อินเทอร์เน็ตโดยไม่เหมาะสม หรือฝ่าฝืนต่อบรรทัดฐานและครรลองที่ติงามของสังคม หรือฝ่าฝืนต่อบทบัญญัติของกฎหมาย เช่น การจัดทำหนังสือท่องอินเทอร์เน็ตอย่างปลอดภัยและได้ประโยชน์ หนังสือคำอธิบายร่างกฎหมายอาญากรรมทางคอมพิวเตอร์ การจัดทำบัญญัติเกี่ยวกับศีลป้องกันตัวของเยาวชนในการใช้อินเทอร์เน็ตและแนวทางป้องกันปัญหาสำหรับผู้ปกครองการตอบข้อหารือและให้คำแนะนำแก่

ประชาชนทางโทรศัพท์ หนังสือทำอะไรได้บ้างกับปัญหาภาพลามกและการล่อลวงบน อินเทอร์เน็ต การเผยแพร่ข้อมูลอันเป็นประโยชน์ผ่านเว็บไซต์ <http://www.thaiparents.net>

5. การจัดทำโครงการ Training for the trainers สืบเนื่องจากการเตรียมความพร้อม ในการรับมือกับปัญหาการก่ออาชญากรรมทางคอมพิวเตอร์ หรือการเผยแพร่เนื้อหาอันไม่ เหมาะสม ซึ่งคุกคามความสงบสุขของสังคมไทย ทำให้มีความจำเป็นต้องเตรียม ความพร้อมของ บุคลากรโดยเฉพาะอย่างยิ่งในสาขานิติศาสตร์ให้เตรียมรับมือกับปัญหาดังกล่าว และเพื่อความ สัมฤทธิ์ผลในการบังคับใช้กฎหมาย การทำความเข้าใจวิทยาการทางคอมพิวเตอร์หรือเทคโนโลยี สารสนเทศ ประกอบกับกฎหมายที่ตราขึ้นรองรับปัญหาดังกล่าวจึงจำเป็นต้องอาศัยทั้งความรู้ ความเข้าใจทางเทคนิคและกฎหมายเฉพาะด้านประกอบกัน โครงการนี้จัดอบรมความรู้ทั้งด้าน เทคนิค นโยบาย และกฎหมายให้แก่กลุ่มบุคลากรจากองค์กรต่างๆ เช่น สำนักงานศาลยุติธรรม สำนักงานอัยการสูงสุด สภานายความ และหน่วยงานของรัฐที่เกี่ยวข้อง เพื่อตอบสนองความ ต้องการของสังคมในภาวะขาดแคลนขณะนี้

6. การรณรงค์และสำรวจเกี่ยวกับการเผยแพร่สื่อลามกอนาจารโดยหน่วยงานอื่น นอกจากการรณรงค์เพื่อให้มีการใช้ประโยชน์จากอินเทอร์เน็ตอย่างถูกต้องรวมทั้งการสำรวจการ เผยแพร่สื่ออันไม่เหมาะสมที่มีผลกระทบต่อเด็ก เยาวชน และสังคมโดยหน่วยงาน ชำต้นแล้ว คณะกรรมการกิจการเด็ก เยาวชน สตรี และผู้สูงอายุ ของสภาผู้แทนราษฎรและวุฒิสภา ก็ได้ ให้ความสนใจกับการแก้ปัญหาดังกล่าวในขณะนี้ และยังพบว่ายังมีหน่วยงานของรัฐและขององค์กร เอกชนอีกหลายหน่วยงานที่ให้ความสำคัญต่อการป้องกันและแก้ปัญหาข้างต้น เช่น การรับแจ้ง เว็บไซต์ผิดกฎหมายซึ่งดำเนินการโดยสำนักงานตำรวจแห่งชาติ ศูนย์รับแจ้งเหตุการณ์เผยแพร่สื่อ ลามกอนาจารและข้อมูลที่ไม่เหมาะสมผ่านเครือข่ายอินเทอร์เน็ต การจัดทำคู่มือ ECPAT : ปกป้องน้องน้อยจากภัยออนไลน์ และการสำรวจสถิติการเผยแพร่สื่อลามกอนาจารโดยองค์กรไม่ แสวงหากำไร ECPAT International

4.6 ปัญหาและอุปสรรคต่อความพยายามของประเทศไทยในการต่อสู้กับปัญหา อาชญากรรมคอมพิวเตอร์

เนื่องจากปัญหาการก่ออาชญากรรมทางคอมพิวเตอร์สามารถกระทำได้ที่ทุกแห่งที่ สามารถเข้าถึงเครือข่ายอินเทอร์เน็ตถือเป็นอาชญากรรมข้ามชาติที่ไร้พรมแดน ดังนั้นปัญหาการ สืบสวนจับกุม เช่น การระบุตัวผู้กระทำความผิด การดำเนินคดีกับอาชญากรประเภทนี้ ขอบเขต อำนาจศาล แต่ในทางกลับกันอาชญากรและกลุ่มอาชญากรข้ามชาติกลับมีข้อได้เปรียบหลายๆ ด้าน ซึ่งถือเป็นปัญหาของฝ่ายสืบสวนสอบสวนและติดตาม ตัวแปรต่างๆ ที่เป็นผลต่อการ

ติดตาม สอบสวน และการปฏิบัติงานสืบสวนสอบสวนคดีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ ประเทศไทยเองก็กระทบปัญหาต่างๆมากมายในการต่อสู้กับอาชญากรรมทางคอมพิวเตอร์ แม้ว่าจะได้มีการบัญญัติกฎหมายเพื่อใช้บังคับกับอาชญากรรมทางคอมพิวเตอร์แล้วก็ตาม ทั้งนี้ ไม่ว่าจะเป็ปัญหาความพร้อมทางเทคโนโลยี ความสามารถในการซ่อนตัวของอาชญากรใช้นามแฝงต่างๆ ของผู้กระทำความผิดทำให้ยากต่อการพิสูจน์ตัวตน รวมถึงความสามารถของผู้กระทำความผิดในการหลบหนีได้ง่ายและรวดเร็วก่อนการถูกติดตาม ความสามารถของผู้กระทำความผิดในการกำหนดและการเลือกเป้าหมายสามารถทำได้หลากหลายในโลก รวมทั้งสามารถเลือกเป้าหมายให้เกิดการแพร่กระจายความเสียหายและความสามารถในการดำเนินการโจมตี หรือก่ออาชญากรรมจากจุดใดบนโลกก็ได้ โดยใช้ทรัพยากร บุคลากร และเงินทุนในการดำเนินการน้อย ความยากลำบากในการสืบหาและติดตามสอบสวนหาแหล่งต้นตอหรือแหล่งที่อยู่ของอาชญากรหรือกลุ่มอาชญากรโดยเฉพาะเมื่อมีความสัมพันธ์โยงใยระหว่างประเทศ การใช้ระบบ Proxy เพื่อหลบหลีกการปิดกั้น ในกรณีเว็บไซต์ที่เผยแพร่เนื้อหาที่ผิดกฎหมายหรือไม่เหมาะสม และมีการปิดกั้นไม่ให้ผู้ใช้เครือข่ายในประเทศไทยเข้าถึงเว็บไซต์เหล่านั้น ซึ่งในทางปฏิบัติผู้ใช้อีกยังสามารถเข้าถึงเว็บไซต์ดังกล่าวได้โดยอาศัยระบบ Proxy สาธารณะที่ให้บริการอยู่นอกประเทศเพื่อให้รอดจากการถูกปิดกั้น³⁵ ทั้งนี้ เนื่องจากในแต่ละประเทศมีฐานะทางเศรษฐกิจไม่เท่าเทียมกันทำให้ส่งผลต่อการลงทุนทางด้านเทคโนโลยีแตกต่างกัน ดังนั้น การสืบสวนคดีประเภทอาชญากรรมคอมพิวเตอร์ระหว่างประเทศนั้นอาจต้องดำเนินการภายใต้ข้อจำกัดทางด้านทรัพยากรที่แตกต่างกัน

ปัญหาการประสานงานในระดับประเทศ³⁶ การขอความร่วมมือและประสานงานกับภาคธุรกิจและอุตสาหกรรมทางเทคโนโลยีเป็นไปด้วยความยากลำบาก เพราะภาคธุรกิจอาจไม่ให้ความสำคัญมากพอต่อการรักษาความมั่นคงปลอดภัย เนื่องจากการเพิ่มต้นทุนในการดำเนินการ ภาครัฐเองยังไม่มีแนวทางปฏิบัติที่ชัดเจนเป็นกรอบในการคำนึงถึงผลกระทบจากการดำเนินการทางกฎหมายที่จะส่งผลต่อการแข่งขันในภาคเอกชน การติดต่อประสานงานระหว่างหน่วยงานราชการด้วยกันยังยึดติดรูปแบบที่เป็นทางการและใช้เวลานาน ซึ่งการแลกเปลี่ยนข้อมูลข่าวสาร งานการข่าวมีความสำคัญมากในการป้องกันและปราบปรามอาชญากรรม เพราะ

³⁵ การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร, รายงานของประเทศไทย : การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11 วันที่ 18-25 เมษายน พ.ศ. 2548 กรุงเทพมหานคร ประเทศไทย "การฝึกกำลังและการโต้ตอบ : การดำเนินกลยุทธ์ร่วมกันในการป้องกันอาชญากรรมและความยุติธรรมทางอาญา, หน้า 72.

³⁶ เรื่องเดียวกัน, หน้า 78.

สามารถนำข้อมูลการข่าวมาวางแผนทำงาน และรับมือกับปัญหาได้อย่างมีประสิทธิภาพ และใช้การข่าวนั้นในการคาดการณ์ถึงปัญหา และภัยคุกคามที่จะเกิดขึ้นในอนาคต ทำให้สามารถเตรียมพร้อมรับมือกับปัญหานั้นได้เป็นอย่างดี สิ่งสำคัญคือการจัดเก็บข้อมูลด้านการข่าวต้องทำเป็นระบบฐานข้อมูล เพื่อให้สามารถนำข้อมูลนั้นมาใช้ในการวิเคราะห์เชื่อมโยง และต้องมีรูปแบบการจัดเก็บที่มีลักษณะเป็นสากล เพื่อให้สามารถแลกเปลี่ยนข้อมูลกับหน่วยงานอื่นๆ ได้ด้วย

ทั้งนี้ จะเห็นได้ว่าการสืบสวนและสอบสวนการดำเนินคดีที่เกี่ยวข้องกับคอมพิวเตอร์มี ปัญหาและอุปสรรคต่างๆ มากมาย การดำเนินการให้บรรลุผลสำเร็จจำเป็นต้องอาศัยการร่วมมือกันอย่างจริงจังทั้งในระดับภายในประเทศระหว่างหน่วยงานราชการด้วยกัน และระหว่างภาครัฐกับภาคเอกชน ตลอดจนในระดับระหว่างประเทศที่ครอบคลุมความร่วมมือระหว่างประเทศ ในทางอาญาแบบเดิมๆ อาจไม่เพียงพอและไม่ทันต่อสถานการณ์การกระทำความผิดที่ส่งผลในวงกว้างได้อย่างรวดเร็วและสามารถทำลาย แก้ไขพยานหลักฐานได้ในเวลารวดเร็ว เช่น การใช้อำนาจเจ้าพนักงานเจ้าหน้าที่โดยความเห็นชอบของรัฐมนตรียื่นคำร้องต่อศาลในกรณีที่ปิดกั้น ข้อมูลอันเป็นเท็จ แม้ว่าการที่กฎหมายกำหนดให้การใช้อำนาจหน้าที่ดังกล่าวจะต้องผ่านการ กลับกรองและกฎหมายยังมุ่งหวังปกป้องสิทธิเสรีภาพของผู้ใช้งานโดยการกลับกรองดังกล่าว ซึ่ง บางครั้งอาจไม่ทันเวลาเนื่องจากกระบวนการใช้เวลา 15 วัน กว่าที่จะถึง 15 วันความเสียหาย อาจเกิดขึ้นมากมายและแพร่ขยายอย่างรวดเร็ว ดังนั้น อาจจะต้องลดขั้นตอนลงเพื่อระงับความเสียหายจากข้อมูลนั้นๆ

ปัญหาเรื่องการเคารพสิทธิส่วนบุคคลหรือความเป็นส่วนตัวกับประสิทธิภาพในการปราบปรามอาชญากรรม³⁷ ซึ่งเป็นปัญหาที่ประสบอยู่ในหลายประเทศเนื่องจากยังมีการให้คำ นิยามและกำหนดขอบเขตของข้อมูลส่วนบุคคลแตกต่างกัน ยิ่งไปกว่านั้นในบางประเทศยังมี กฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่แตกต่างกัน จึงทำให้เจ้าหน้าที่ในระดับปฏิบัติการไม่มีความมั่นใจในการดำเนินงานข้อมูลดังกล่าวจะได้รับการจัดเก็บอย่างถูกต้องและรวดเร็วหรือไม่ จากปัญหาและอุปสรรคของประเทศภาคีสัญญาที่กล่าวมาในบทที่ 3 ถือว่าเป็นบทเรียนที่ สำคัญที่ประเทศไทยจำเป็นต้องนำมาพิจารณาในการประกอบการร่างพระราชบัญญัติว่าด้วยการ คัดกรองข้อมูลส่วนบุคคล เพื่อที่จะให้นานาประเทศยอมรับในตัวร่างพระราชบัญญัตินี้ดังกล่าว มิฉะนั้นหากมาตรฐานไม่เป็นที่ยอมรับ ก็อาจจะมีผลความจำเป็นที่จะต้องทำข้อตกลงระหว่าง ประเทศเพิ่มขึ้น และส่งผลกระทบต่อการทำธุรกิจระหว่างประเทศ คือนานาชาติไม่กล้าที่จะเข้ามา ลงทุนเมื่อการคุ้มครองข้อมูลส่วนบุคคลไม่มีประสิทธิภาพที่จะคุ้มครองข้อมูลส่วนบุคคลได้

³⁷ เรื่องเดียวกัน, หน้า 79.

ปัญหาเรื่องความเหลื่อมล้ำของกฎหมายภายในของแต่ละประเทศซึ่งอาจทำให้ไม่สามารถเอาผิดกับอาชญากรรมคอมพิวเตอร์ผ่านเครือข่ายข้ามประเทศได้³⁸ เช่น กรณีของการส่งผู้ร้ายข้ามแดน การให้ความร่วมมือระหว่างประเทศ การช่วยเหลือซึ่งกันและกัน และการกระทำความผิดบางประการ เช่น ประเทศไทยไม่อนุญาตให้เล่นการพนันต่างๆ แต่บางประเทศให้เล่นพนันผ่านเว็บไซต์ได้ รวมถึงความสามารถของผู้กระทำผิดในการจัดการตั้งหรือเผยแพร่เว็บไซต์ที่มีเนื้อหาไม่เหมาะสมหรือขัดต่อกฎหมายของประเทศหนึ่งบนดินแดนของประเทศที่สามได้ ปัญหาเรื่องการจับเก็บข้อมูลที่สำคัญต่างๆ ที่สามารถโยงไปถึงตัวผู้กระทำความผิด แต่บางประเทศและบางหน่วยงานยังไม่ให้ความสำคัญกับการเก็บข้อมูลดังกล่าวไว้เป็นหลักฐาน และหน่วยงานยังไม่ให้ความสำคัญในการตรวจสอบเนื้อหาที่อยู่บนเว็บไซต์ ทั้งนี้ ประเทศไทยยังขาดระบบรับรองความน่าเชื่อถือของพยานผู้เชี่ยวชาญเกี่ยวกับคอมพิวเตอร์ และหากต้องมีการติดต่อประสานงาน อาจทำให้เกิดปัญหาช่องว่างในการสื่อสารระหว่างเจ้าหน้าที่ด้านคอมพิวเตอร์ พนักงานสอบสวน พนักงานอัยการ ผู้พิพากษา และผู้ที่เกี่ยวข้องทางด้านกระบวนการทางกฎหมายทั้งหลาย โดยเฉพาะช่องว่างระหว่างระหว่างภาษากฎหมายและภาษาเทคนิคทางคอมพิวเตอร์

4.7 ผลกระทบหากประเทศไทยเข้าเป็นภาคีอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

เนื่องจากประเทศไทยเองก็ได้เล็งเห็นความจำเป็นในการใช้กฎหมายที่เป็นสากล ซึ่งจะช่วยให้เกิดการปรับปรุง และเอื้อประโยชน์ให้ประเทศไทยได้อย่างเต็มที่³⁹ จากการศึกษาและวิเคราะห์ถึงการเตรียมตัวของประเทศไทยในการรับมือกับอาชญากรรมทางคอมพิวเตอร์ทั้งในแง่กฎหมาย และนโยบายเพื่อใช้เป็นข้อมูลประกอบการพิจารณาว่าประเทศไทยควรจะพิจารณาเข้าร่วมเป็นภาคีของอนุสัญญานี้หรือไม่ และประเทศไทยควรจะเตรียมความพร้อมหรือปรับปรุงพัฒนาในด้านมาตรการเพื่อรองรับอย่างไรบ้าง จึงจะสามารถใช้ประโยชน์จากอนุสัญญานี้ได้อย่างเต็มที่ ผู้เขียนสามารถสรุปได้ดังนี้

1. ประเทศไทยกับประเด็นเรื่องการกำหนดมาตรการทางสารบัญญัติ

ในประเด็นเรื่องการกำหนดให้ความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์เป็นความผิดอาญาตามกฎหมายภายในประเทศเพื่อให้เกิดความสอดคล้องกัน ซึ่งประเทศไทยเองได้มีการกำหนดมาตรการดังกล่าวโดยบัญญัติเป็นกฎหมายที่มีการกำหนดกรอบความผิดเกี่ยวกับ

³⁸ เรื่องเดียวกัน, หน้า 79.

³⁹ เรื่องเดียวกัน, หน้า 80.

อาชญากรรมทางคอมพิวเตอร์ไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งการกำหนดกรอบของการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศไทยนี้มีความชัดเจนและครอบคลุมการกระทำความผิดทุกขั้นตอน แม้ว่า จะมีได้กำหนดฐานความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้องไว้ในพระราชบัญญัตินี้ แต่ก็ได้มีมาตรการในการป้องกันการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้องไว้ในกฎหมายภายในฉบับอื่น ทั้งนี้ ในเรื่องของการใช้หรือการแปลถ้อยคำตามกฎหมายที่เวลาบัญญัติกฎหมายหากจะบัญญัติเพื่อให้เป็นไปตามถ้อยคำตามภาษาต่างประเทศโดยเคร่งครัดเกินไปคงเป็นไปได้ยาก เพราะลักษณะและการใช้ถ้อยคำของภาษาแตกต่างกันบางภาษาบางถ้อยคำอาจครอบคลุมได้หลายสถานการณ์แต่อีกภาษาอาจแยกและใช้ถ้อยคำที่แตกต่างกันได้

ดังนั้น หากประเทศไทยจะทำการพิจารณาเป็นภาคีอนุสัญญา ประเทศไทยก็ไม่จำเป็นต้องออกกฎหมายอนุวัติการ เนื่องจากมีกฎหมายภายในที่สอดคล้องกับพันธกรณีของอนุสัญญาอยู่แล้ว และจากการวิเคราะห์เกี่ยวกับมาตรการทางสารบัญญัติประเทศที่ประเทศไทยได้ใช้แนวทางตามอนุสัญญานี้ส่งผลให้ประเทศไทยมีกฎหมายที่สอดคล้องกับบทบัญญัติในอนุสัญญาซึ่งถือเป็นผลดีกับประเทศไทยคือไม่ก่อให้เกิดอุปสรรคในการบังคับใช้กฎหมายต่อไป

ทั้งนี้ ในส่วนที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นสิ่งที่อนุสัญญาได้คำนึงถึง ซึ่งกฎหมายฉบับนี้อยู่ในระหว่างการยกร่าง ดังนั้น หากประเทศไทยจะทำการพิจารณาเป็นภาคีอนุสัญญา อาจต้องเร่งดำเนินการเกี่ยวกับมาตรการดังกล่าว เนื่องจากประเทศส่วนใหญ่มักไม่ต้องการส่งข้อมูลไปยังประเทศที่ไม่สามารถให้การคุ้มครองควบคุมการถ่ายโอนข้อมูลไปต่างประเทศอย่างเพียงพอว่าข้อมูลดังกล่าวจะไม่ถูกนำไปใช้ในทางที่ผิด

2. ประเทศไทยกับประเด็นเรื่องการกำหนดมาตรการทางวิธีสบัญญัติ

ประเทศไทยได้มีการดำเนินการต่างๆ ในการกำหนดมาตรการวิธีสบัญญัติอย่างเต็มที่ไม่ว่าจะเป็นวิธีการสืบสวนสอบสวนเฉพาะคดีอาชญากรรมทางคอมพิวเตอร์รวมถึงพนักงานเจ้าหน้าที่ที่ทำหน้าที่สืบสวนสอบสวนความผิดและการดำเนินคดีตามกฎหมายภายในตามที่อนุสัญญากำหนด รวมถึงหน่วยงานที่สามารถติดต่อประสานงานกับศูนย์ติดต่อประสานงานของประเทศภาคีอื่นโดยวิธีการที่รวดเร็วโดยไม่ก่อให้เกิดอุปสรรคต่อการปฏิบัติตามพันธกรณีอนุสัญญา ซึ่งแสดงให้เห็นว่าประเทศไทยมีการเตรียมความพร้อมเพื่อให้สามารถรองรับพันธกรณีที่อาจเกิดขึ้น และยังแสดงให้เห็นว่าประเทศไทยสามารถดำเนินการทางด้านมาตรการทางวิธีสบัญญัติต่างให้สอดคล้องตามที่กำหนดในอนุสัญญา เช่น การเข้าถึงข้อมูลคอมพิวเตอร์โดยกระทำข้ามพรมแดน การรวบรวมข้อมูลจรรยาจรทางคอมพิวเตอร์โดยทันที หลักการเปิดเผยข้อมูลทางคอมพิวเตอร์ที่เก็บ

รักษาไว้โดยทันที เป็นต้น ซึ่งถือเป็นผลดีต่อประเทศไทยหากจะมีการพิจารณาเข้าเป็นภาคี เนื่องจากหลักการดังกล่าวสามารถทำให้ดำเนินการเกี่ยวกับการกระทำคามผิดที่มีลักษณะข้ามประเทศได้อย่างรวดเร็วและมีประสิทธิภาพ

แต่ทั้งนี้ มาตรการวิธีสบัญญัติจะต้องคำนึงถึงหลักสิทธิมนุษยชนที่มุ่งคุ้มครองสิทธิส่วนบุคคลและเสรีภาพขั้นพื้นฐาน ดังนั้น หากประเทศไทยจะทำการพิจารณาเป็นภาคีอนุสัญญา ประเทศไทยเองยังมิได้มีการบัญญัติกฎหมายเป็นลายลักษณ์อักษรเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังเช่นประเทศภาคีที่ผู้เขียนยกตัวอย่างคือประเทศสหรัฐอเมริกา และประเทศฝรั่งเศส ซึ่งอาจทำให้เกิดความไม่มั่นใจข้อมูลนั้นอาจถูกใช้ในทางมิชอบอันเป็นการละเมิดต่อเจ้าของข้อมูล รวมถึงการคุ้มครองควบคุมกรณีที่มีการถ่ายโอนข้อมูลไปต่างประเทศ หากต้องปฏิบัติตามพันธกรณี ประเทศไทยจึงควรเร่งพิจารณาเกี่ยวกับหลักการดังกล่าวโดยเร็ว

3. ประเทศไทยกับประเด็นเรื่องการทำหนดมาตรการด้านความร่วมมือระหว่างประเทศ

ในการดำเนินการนำตัวผู้กระทำความผิดมาลงโทษ และการให้ความช่วยเหลือซึ่งกันและกันเป็นปัญหาที่มีความสำคัญ หากเป็นการกระทำคามผิดข้ามประเทศ เนื่องจากกรกระทำคามผิดในรูปแบบนี้มีเทคโนโลยีที่ทันสมัยเข้ามาเกี่ยวข้อง ทำให้ยากต่อการจับกุมและนำตัวผู้กระทำความผิดมาลงโทษ หากไม่ได้รับความร่วมมือระหว่างประเทศที่เกี่ยวข้องซึ่งในประเด็นนี้ อนุสัญญาได้เน้นย้ำถึงความสำคัญดังกล่าวโดยบัญญัติให้มีวิธีดำเนินการเกี่ยวกับการส่งตัวผู้กระทำความผิดมาลงโทษในฐานะผู้ร้ายข้ามแดนให้ประเทศภาคีสามารถปฏิบัติต่อกันได้รวดเร็วขึ้น โดยมีการผ่อนคลายหลักเรื่องความผิดอาญาของทั้งสองประเทศ ซึ่งทำให้สามารถดำเนินการได้อย่างมีประสิทธิภาพมากขึ้น ทั้งนี้ หลักการภายในของประเทศก็ยังมีได้มีการระบุให้ความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์เป็นความผิดที่สามารถส่งผู้ร้ายข้ามแดนได้ และรวมถึงการที่ประเทศไทยเองมีการกำหนดหลักการเรื่องความผิดอาญาของทั้ง 2 ประเทศ ไว้ในกฎหมายจึงเกิดอุปสรรคในการปฏิบัติตามที่ได้วิเคราะห์ไว้ ผู้เขียนเห็นว่าเป็นข้อจำกัดอย่างหนึ่งของอนุสัญญาที่สามารถใช้บังคับได้เฉพาะประเทศเท่านั้น

ดังนั้น หากประเทศจะต้องทำการพิจารณาเข้าเป็นภาคีอนุสัญญา ประเทศไทยจึงจะสามารถขจัดข้อขัดข้องดังกล่าวได้ และสามารถนำตัวผู้กระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มาลงโทษได้ เนื่องจากอนุสัญญาได้เน้นย้ำถึงความสำคัญดังกล่าวโดยบัญญัติให้มีวิธีดำเนินการเกี่ยวกับการส่งตัวผู้กระทำความผิดมาลงโทษในฐานะผู้ร้ายข้ามแดนให้ประเทศภาคีสามารถปฏิบัติต่อกันได้รวดเร็วขึ้น โดยมีการผ่อนคลายหลักเรื่องความผิดอาญาของทั้งสองประเทศ ซึ่งทำให้สามารถดำเนินการได้อย่างมีประสิทธิภาพมากขึ้น

และเพื่อให้เห็นภาพชัดเจนเกี่ยวกับการปฏิบัติตามพันธกรณีอนุสัญญาเกี่ยวกับมาตรการทางสารบัญญัติของอนุสัญญา ประเทศภาคีสมาชิกอนุสัญญาอย่างประเทศสหรัฐอเมริกา และประเทศฝรั่งเศส และประเภทความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ที่กำหนดไว้ในกฎหมายไทยผู้เขียนจึงสรุปไว้ตามตารางที่ 2 ดังนี้

ตารางที่ 2 แสดงประเภทความผิดของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ประเทศสหรัฐอเมริกา
ประเทศฝรั่งเศส และประเทศไทย

ประเภทความผิด	Convention on Cyber crime 2001	ประเทศสหรัฐอเมริกา	ประเทศฝรั่งเศส	ประเทศไทย	หมายเหตุ
การใช้คอมพิวเตอร์ในทางมิชอบ	การเข้าถึงโดยมิชอบ (Article 2)	การเข้าถึงคอมพิวเตอร์ทำให้ได้มาซึ่งข้อมูลความมั่นคงแห่งชาติ ความผิดนี้ได้ถูกกำหนดไว้ใน (Title 18 U.S.C. § 1030 (a)(2)) การเข้าถึงคอมพิวเตอร์ทำให้ได้มาซึ่งข้อมูลสถาบันการเงินหรือหน่วยงานของรัฐ (Title 18 U.S.C. § 1030 (a)(2)) การกระทำความผิดโดยการบุกรุกเข้าไปในระบบคอมพิวเตอร์ของรัฐบาล (Title 18 U.S.C. § 1030 (a)(3))	การเข้าถึงระบบประมวลผลข้อมูลอัตโนมัติโดยปราศจากอำนาจ (Article 323-1)	การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) และการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ (มาตรา 6)	

ประเภท ความผิด	Convention on Cyber crime 2001	ประเทศสหรัฐอเมริกา	ประเทศฝรั่งเศส	ประเทศไทย	หมาย เหตุ
(ต่อ)การใช้ คอมพิวเตอร์ ในทางมิชอบ		การเข้าถึงคอมพิวเตอร์เพื่อ การฉ้อโกงและได้มาซึ่งสิ่งมี ค่า (Title 18 U.S.C. § 1030 (a)(4))			
	การดักจับข้อมูล โดยมิชอบ (Article 3)		การดักจับข้อมูล (Article 226-15)	การดักจับ ข้อมูลคอมพิวเตอร์ของ ผู้อื่นโดยมิชอบ (มาตรา 8)	
	การแทรกแซง ต่อข้อมูล (Article 4) การแทรกแซง ต่อระบบ (Article 5)		การกระทำโดยการ ขัดขวางการทำงานของ ระบบหรือการรบกวน การทำงานของระบบ ประมวลผลข้อมูล อัตโนมัติ (Article 323- 2)	การกระทำเพื่อให้การ ทำงานของระบบ คอมพิวเตอร์ของผู้อื่น ไม่สามารถทำงานได้ ตามปกติ (มาตรา 10)	

ประเภท ความผิด	Convention on Cyber crime 2001	ประเทศสหรัฐอเมริกา	ประเทศฝรั่งเศส	ประเทศไทย	หมาย เหตุ
(ต่อ)การใช้ คอมพิวเตอร์ ในทางมิชอบ				การส่ง ข้อมูลคอมพิวเตอร์ รบกวนการทำงานของระบบ คอมพิวเตอร์ของบุคคล อื่นโดยปกติสุข (มาตรา 11)	
	การนำสิ่งที่ได้ จาก คอมพิวเตอร์ไป ใช้ในทางมิชอบ (Article 6)		การนำเข้า การ ครอบครอง การเสนอ ขายหรือการผลิตอุปกรณ์ ใดๆ โปรแกรม คอมพิวเตอร์ หรือข้อมูล ใดๆ ที่ออกแบบหรือ ดัดแปลงเพื่อใช้กระทำ ความผิด (Article 323- 3)	การจำหน่ายชุดคำสั่งที่ จัดทำขึ้นเพื่อนำไปใช้ เป็นเครื่องมือในการ กระทำความผิด (มาตรา 13)	

ประเภท ความผิด	Convention on Cyber crime 2001	ประเทศสหรัฐอเมริกา	ประเทศฝรั่งเศส	ประเทศไทย	หมาย เหตุ
การฉ้อโกงที่ เกี่ยวกับ อินเทอร์เน็ต	การกระทำ ความผิด เกี่ยวกับการ ปลอมแปลง เกี่ยวกับ คอมพิวเตอร์ (Article 7)		การกระทำความผิดโดย นำเข้า เผยแพร่ แก้ไข รับหรือส่งต่อข้อมูลใน ระบบการประมวลผล ข้อมูลอัตโนมัติ หรือการ ก่อให้เกิดการหลอกลวง และการเปลี่ยนแปลง ข้อมูลที่มีอยู่ในระบบการ ประมวลผลโดยอัตโนมัติ (Article 323-3)	การใช้คอมพิวเตอร์ กระทำความผิดอื่น (มาตรา 14)	
	การฉ้อโกงที่ เกี่ยวกับ คอมพิวเตอร์ (Article 8)	การฉ้อฉลและการกระทำที่ เกี่ยวกับบัตรเครดิต (Title 18 U.S.C. § 1029 (e)(1))	ความผิดเกี่ยวกับบัตร เครดิต (Article L 163-4)		

ประเภท ความผิด	Convention on Cyber crime 2001	ประเทศสหรัฐอเมริกา	ประเทศฝรั่งเศส	ประเทศไทย	หมายเหตุ
ความผิด เกี่ยวกับ เนื้อหา	การกระทำที่เป็น ความผิด เกี่ยวกับสื่อ ลามกอนาจาร เกี่ยวกับเด็ก (Article 9)	การควบคุมการเผยแพร่ภาพ หรือสื่อลามกทางเครือข่าย อินเทอร์เน็ต (Title 18 U.S.C. § 1466A)		การตกแต่ง ข้อมูลคอมพิวเตอร์ที่ เป็นภาพของบุคคล (มาตรา 16)	