บทที่ 5

มาตรการในการปราบปรามและการป้องกันการหลอกลวงทางอินเตอร์เน็ต

บทนี้จะศึกษาถึงมาตรการทางกฎหมายและมาตรการอื่น ๆ ที่เกี่ยวข้องในการป้องกันและปราบปรามการหลอกลวงทางอินเตอร์เน็ต ซึ่งจะเน้นศึกษาถึงมาตรการของประเทศสหรัฐอเมริกา เนื่องจากเป็นประเทศที่มีความเจริญก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์เป็นอย่างมาก ประกอบกับปัญหาอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ตกำลังทวีความรุนแรงมากในประเทศสหรัฐอเมริกา สำหรับประเทศไทยเริ่มได้รับผลกระทบจากการประกอบอาชญากรรมดังกล่าว จึงควรศึกษาหามาตรการเพื่อเป็นแนวทางในการกำหนดมาตรการทางกฎหมายและมาตรการอื่น ๆ เพื่อให้การป้องกันและปราบปรามการหลอกลวงทางอินเตอร์เน็ตของประเทศไทยเป็นไปอย่างมีประสิทธิภาพ โดยจะศึกษาร่างพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ พ.ศ. .... ของประเทศไทย (ขณะนี้อยู่ระหว่างขั้นตอนการยกร่างของคณะอนุกรรมการเพื่อขอความเห็นชอบจากคณะรัฐมนตรี) ว่าจะสามารถปราบปรามการหลอกลวงทางอินเตอร์เน็ตได้อย่างมีประสิทธิภาพหรือไม่ และควรจะมีทิศทางในการบัญญัติกฎหมายดังกล่าวอย่างไร นอกจากนั้นเนื่องจากการหลอกลวงทางอินเตอร์เน็ตเป็นการติดต่อสื่อสารและส่งผ่านข้อมูลผ่านระบบเครือข่ายอินเตอร์เน็ต ซึ่งมีความรวดเร็วและแพร่หลายไปทั่วโลก ประกอบกับไม่มีผู้ใดหรือองค์กรที่มีอำนาจหรือหน้าที่ในการควบคุมเครือข่ายการติดต่อสื่อสารผ่านระบบเครือข่ายอินเตอร์เน็ต ดังนั้นการกำหนดมาตรการในการปราบปรามอาชญากรรมดังกล่าวอย่างเดียวคงไม่สามารถทำให้อาชญากรรมดังกล่าวหมดสิ้นไป จำเป็นจะต้องศึกษาถึงมาตรการอื่น ๆ ในการป้องกันอาชญากรรมดังกล่าวประกอบด้วย

5.1 มาตรการในการปราบปรามอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ต

จากการศึกษากฎหมายของประเทศต่าง ๆ ที่มีการบัญญัติกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ขึ้นใช้บังคับนั้นพบว่ามีรูปแบบที่แตกต่างกันไป บางประเทศได้ทำการแก้ไขเพิ่มเติมในประมวลกฎหมายอาญา เช่น ประมวลกฎหมายอาญาของประเทศเยอรมัน กฎหมาย Federal ของสหรัฐอเมริกา (และในแต่ละมลรัฐได้ออกกฎหมายคอมพิวเตอร์มาใช้บังคับด้วย) และประมวลกฎหมายอาญาของประเทศญี่ปุ่น (Penal Code) ประเทศออสเตรเลีย

(Australian Crimes Act 1914) ประเทศแคนนาดา (The Canadian Criminal Code) แต่ในบางประเทศได้มีการตรากฎหมายเฉพาะขึ้นใช้บังคับ โดยอาจใช้ชื่อกฎหมายที่แตกต่างกันไป เช่น Computer Crime Act ของประเทศอังกฤษ Computer Misuse Act ของประเทศสิงคโปร์ Computer Crime Ordinance ของประเทศฮ่องกง Computer Crime Act ของประเทศมาเลเซีย เป็นต้น

นอกจากนี้องค์การระหว่างประเทศหลายองค์การได้ตระหนักถึงความร้ายแรงของปัญหาอาชญากรรมทางคอมพิวเตอร์ จึงพยายามกำหนดแนวทางให้กับประเทศภาคีสมาชิกนำมาตรการที่กำหนดไปปฏิบัติ เช่น คณะมนตรีแห่งยุโรป (Council of Europe) องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) สหประชาชาติ (United Nations) เป็นต้น ทั้งนี้ Council of Europe ยังได้ยกร่างอนุสัญญาเพื่อให้ประเทศภาคีสมาชิกบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์เป็นไปในแนวทางเดียวกันและใช้บังคับกับรูปแบบการกระทำความผิดทางอาญาที่เปลี่ยนไปมากที่สุด อนุสัญญาดังกล่าวคือ Convention on Cyber-Crime โดยมีเนื้อหาครอบคลุมการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ เช่น การฉ้อโกง (Computer-related Fraud) การปลอมเอกสาร (Computer-related Forgery) สื่อลามก (Offences related to child pornography) การคุ้มครองทรัพย์สินทางปัญญา (Offence related to infringements of copyright and related rights) เป็นต้น

5.1.1 มาตรการทางด้านกฎหมายสารบัญญัติ

5.1.1.1 กฎหมายเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตของประเทศสหรัฐอเมริกา

การกระทำความผิดอาญาที่มีเครื่องคอมพิวเตอร์เข้ามาเกี่ยวข้องนั้นเป็นปัญหาที่ทวีความรุนแรงเพิ่มมากขึ้น โดยเฉพาะในประเทศสหรัฐอเมริกาที่เป็นแหล่งกำเนิดของการใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายอินเตอร์เน็ต ดังจะเห็นได้จากเหตุผลในการประกาศใช้กฎหมายอาชญากรรมคอมพิวเตอร์ของมลรัฐฟลอริด้า ซึ่งประกาศว่า

รัฐสภาได้ค้นพบและขอประกาศว่า

(1) การกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์เป็นปัญหาที่กำลังก่อตัวเพิ่มขึ้นทั้งในภาครัฐและภาคเอกชน

(2) การกระทำความผิดอาญาเกี่ยวกับคอมพิวเตอร์ได้ก่อให้เกิดความสูญเสียที่มีมูลค่ามหาศาลต่อสาธารณชน ซึ่งความเสียหายในเหตุการณ์แต่ละครั้งของการกระทำความผิดมีแนวโน้มที่จะสูงมากกว่าความเสียหายที่เกี่ยวข้องกับเหตุการณ์ในแต่ละครั้งของอาชญากรรมโจรผู้ดีอื่น ๆ

(3) โอกาสที่จะเกิดอาชญากรรมดังกล่าวต่อสถาบันการเงิน โครงการต่าง ๆ ของรัฐบาล เอกสารของทางราชการ รัฐวิสาหกิจอื่น ๆ โดยผ่านทางการนำข้อมูลเท็จเข้าไปในระบบคอมพิวเตอร์ การใช้เครื่องอำนวยความสะดวกทางคอมพิวเตอร์โดยไม่มีอำนาจ การแก้ไขเปลี่ยนแปลง หรือทำลายข่าวสารหรือแฟ้มข้อมูลทางคอมพิวเตอร์ และการลักขโมยเอกสารทางการเงิน ข้อมูลและทรัพย์สินอื่น ๆ ที่สูงมาก

(4) ในขณะที่รูปแบบต่าง ๆ ของการกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์อาจถือได้ว่าเป็นเรื่องของความผิดอาญาที่ตั้งอยู่บนพื้นฐานของบทบัญญัติทางกฎหมายที่มีอยู่แล้วโดยทั่วไป แต่ก็นับว่าเป็นที่เรียกร้องและเป็นเรื่องที่เหมาะสมที่จะพิจารณาว่าควรที่จะมีกฎหมายใหม่มาผนวกหรือเสริมเพิ่มเติม เพื่อที่จะห้ามการใช้เครื่องคอมพิวเตอร์ในทางที่ผิดรูปแบบต่าง ๆ

ในประเทศสหรัฐอเมริกามีกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ทั้งระดับรัฐบาลกลาง (Federal Law) และระดับมลรัฐ ซึ่งผู้เขียนจะขอกล่าวถึงแต่กฎหมายระดับรัฐบาลกลางเท่านั้น สำหรับกฎหมายที่จะนำมาใช้บังคับกับการหลอกลวงทางอินเตอร์เน็ต คือ กฎหมายรัฐบาลกลางแห่งสหรัฐอเมริกาได้มีการแก้ไขเพิ่มเติมบรรพที่ 18 แห่งประมวลกฎหมายของสหรัฐอเมริกา (Title 18 of the United States Code) โดยกฎหมายการคุ้มครองระบบคอมพิวเตอร์ ค.ศ.1979 (Federal Computer System Protection Act of 1979) * ดังนี้

---

* ปรากฏตามภาคผนวก ข.

มาตรา 1028 การฉ้อฉลและการกระทำที่ผิดกฎหมายทางคอมพิวเตอร์

ก. ผู้ใดเข้าถึง ก่อให้เกิดการเข้าถึง หรือพยายามเข้าถึงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข่ายงานคอมพิวเตอร์ หรือส่วนหนึ่งส่วนใดของสิ่งดังกล่าว ซึ่งได้ปฏิบัติงานทั้งหมดหรือแต่บางส่วนให้แก่ธุรกิจการค้าระหว่างรัฐหรือเป็นของ หรืออยู่ภายใต้สัญญาของ หรือร่วมกับสถาบันทางการเงินใด ๆ หรือกระทรวง ทบวง กรม หรือตัวแทนใด ๆ ของรัฐบาลแห่งสหรัฐอเมริกา หรือสถาบันที่มีอยู่ใด ๆ ซึ่งดำเนินการในธุรกิจการค้าระหว่างรัฐ หรือมีผลกระทบต่อธุรกิจการค้าระหว่างรัฐ โดยรู้อยู่แล้วและโดยจงใจ ไม่ว่าทางตรง หรืออ้อม ด้วยความประสงค์แห่ง

(1) การคิดหรือการวางแผนการหรือกลอุบายใด ๆ เพื่อที่จะหลอกลวง หรือ

(2) การได้ไปซึ่งเงิน ทรัพย์สินหรือบริการ สำหรับตนเองหรือผู้อื่นโดยวิธีของการปลอมแปลงหรือการฉ้อโกง หรือการเป็นตัวแทน หรือการให้สัญญา

ต้องระวางโทษปรับไม่เกินสองเท่าครึ่งของความผิดฐานฉ้อโกงหรือลักทรัพย์ หรือจำคุกไม่เกินสิบห้าปี หรือทั้งจำทั้งปรับ

ข. ผู้ใดเข้าถึง แก้ไข เปลี่ยนแปลง ทำให้เสียหาย ทำลายหรือพยายามทำให้เสียหายหรือทำลายเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์ ดังที่ได้ระบุไว้ในอนุมาตรา ก. หรือคอมพิวเตอร์ซอฟท์แวร์ โปรแกรม หรือข้อมูลใด ๆ ที่ได้บรรจุอยู่ในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์ โดยเจตนาและโดยปราศจากอำนาจไม่ว่าทางตรงหรือทางอ้อม ต้องระวางโทษปรับไม่เกิน 50,000 เหรียญสหรัฐ หรือจำคุกไม่เกินสิบห้าปี หรือทั้งจำทั้งปรับ

ค. คำนิยาม

(1) "เข้าถึง" (Access) หมายถึง เข้าไปสู่ สั่ง สื่อสารกับ ใส่ข้อมูลเข้าไป เก็บไว้ ล้วงข้อมูลมาจาก หรืออีกนัยหนึ่งเอาประโยชน์ใด ๆ ของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์มาใช้

(2) "คอมพิวเตอร์" (Computer) หมายถึง เครื่องมือประดิษฐ์ทางอิเล็กทรอนิกส์ชนิดหนึ่ง ซึ่งปฏิบัติงานเกี่ยวกับทางตรรกวิทยา การคำนวณ และความจำ โดยอาศัยการยักย้ายถ่ายเทของแรงกระตุ้นทางอิเล็กทรอนิกส์หรือทางแม่เหล็ก และรวมถึงเครื่องมืออำนวยความสะดวกทั้งหลายเกี่ยวกับการนำข้อมูลเข้า การนำข้อมูลออก การประมวลผล การเก็บรักษา ข้อมูลซอฟท์แวร์หรือการสื่อสาร ซึ่งเชื่อมโยงกับ หรือเกี่ยวพันกับเครื่องมือประดิษฐ์ดังกล่าว ภายใต้ระบบหรือเครือข่ายงานอันหนึ่ง

(3) "ระบบคอมพิวเตอร์" (Computer System) หมายถึง ชุดอุปกรณ์ทางคอมพิวเตอร์ เครื่องมือประดิษฐ์ทั้งหลายและซอฟท์แวร์ที่เกี่ยวข้องสัมพันธ์กัน ทั้งที่ได้เชื่อมโยงกันหรือไม่ได้เชื่อมโยงกัน

(4) "ข่ายงานคอมพิวเตอร์" (Computer Network) หมายถึง การติดต่อเชื่อมโยงกันภายในของระบบการสื่อสารกับเครื่องคอมพิวเตอร์ โดยผ่านสถานีรับส่งทางไกลหลายแห่งหรือหน่วยงานอันซับซ้อนที่ประกอบด้วยเครื่องคอมพิวเตอร์ตั้งแต่สองเครื่องขึ้นไป ซึ่งเชื่อมโยงเข้าด้วยกัน

(5) "ทรัพย์สิน" (Property) รวมถึง เอกสารทางการเงิน ข่าวสาร ตลอดจนข้อมูลที่ได้ประมวลผล หรือได้ผลิตขึ้นด้วยวิธีการทางอิเล็กทรอนิกส์และคอมพิวเตอร์ซอฟท์แวร์กับโปรแกรมคอมพิวเตอร์ที่อยู่ในรูปแบบซึ่งทั้งมนุษย์และเครื่องจักรกลต่างก็สามารถที่จะอ่านเข้าใจได้ รวมทั้งวัตถุมีรูปร่างหรือไม่มีรูปร่างซึ่งอาจมีราคาได้อื่น ๆ

(6) "บริการ" (Service) รวมถึง เวลาของการทำงานของเครื่องคอมพิวเตอร์ การประมวลผลข้อมูลและงานเก็บรักษาข้อมูล

(7) "เอกสารทางการเงิน" (Financial Instrument) หมายถึง เช็ค ดร๊าฟท์ ธนาณัติ สมุดเงินฝากธนาคาร หนังสือเลตเตอร์ออฟเครดิต ตั๋วแลกเงิน บัตรเครดิต หรือพันธบัตรใด ๆ หรือเอกสารที่ใช้แทนการประมวลผลทางอิเล็กทรอนิกส์ใด ๆ

(8) "โปรแกรมคอมพิวเตอร์" (Computer Program) หมายถึง คำสั่งหรือรายการหรือชุดของคำสั่ง หรือรายการที่อยู่ในรูปแบบอันเป็นที่ยอมรับได้ของเครื่องคอมพิวเตอร์ (ใช้งานได้กับเครื่องคอมพิวเตอร์) ซึ่งทำให้หน่วยงานของระบบคอมพิวเตอร์ตามที่ได้ออกแบบขึ้นสามารถผลิตผลผลิตที่เหมาะสมออกมาได้

(9) "คอมพิวเตอร์ซอฟท์แวร์" (Computer Software) หมายถึงชุดของโปรแกรมคอมพิวเตอร์ ระเบียบการและเอกสารที่เกี่ยวข้องกับการทำงานของระบบคอมพิวเตอร์

ตามคำนิยามของคำว่า "การเข้าถึง" กำหนดไว้หลายวิธี ซึ่งพอจะสรุปได้ดังนี้[76]

เข้าไปสู่ (Approach) หมายถึง การกระทำที่เป็นการเข้า หรือเข้าไปสู่สิ่งที่ตนต้องการภายในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์

สั่ง (Instruct) หมายถึง การกระทำที่เป็นการสั่งให้เครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ ทำงานได้ตามความต้องการของตน

สื่อสารกับ (Communicate with) หมายถึง การกระทำที่เป็นการติดต่อกับเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ ด้วยวิธีการทางการสื่อสาร เช่น ผ่านสายโทรศัพท์ เป็นต้น เพื่อให้ได้ข้อมูลหรือประโยชน์อย่างอื่นตามความต้องการของตน

ใส่ข้อมูลเข้าไปเก็บไว้ (Store data in) หมายถึง การกระทำที่เป็นการนำข้อมูลใส่เข้าไปในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ เพื่อตนจะได้ประโยชน์จากการทำงานของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ในภายหลัง

---

[76] ภานุ รังสีสหัส, "การกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์," (วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2533), หน้า 53-54.

ล้วงข้อมูลจาก (Retire data from) หมายถึง การกระทำที่เป็นการเอาข้อมูลออกมาจากเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ เพื่อประโยชน์ของตน

เอาประโยชน์ใด ๆ มาใช้ (make use of any resources of) หมายถึง การกระทำใด ๆ ต่อเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ ที่เป็นไปเพื่อประโยชน์ของตน

เมื่อพิจารณาการเข้าถึงทางคอมพิวเตอร์จะก่อให้เกิดการกระทำที่มิชอบขึ้นได้ในรูปแบบต่าง ๆ กัน การกระทำที่มิชอบเหล่านี้มีลักษณะเช่นเดียวกับความผิดฐานลักทรัพย์ ความผิดฐานฉ้อโกง ความผิดฐานปลอมแปลงเอกสาร และความผิดฐานทำให้เสียทรัพย์ในกฎหมายอาญา แต่มีความแตกต่างในเรื่องขององค์ประกอบของความผิดบางประการ ซึ่งทำให้ไม่สามารถนำบทบัญญัติของกฎหมายในเรื่องความผิดฐานลักทรัพย์ ความผิดฐานฉ้อโกง ความผิดฐานปลอมเอกสารและความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญามาบังคับใช้กับการกระทำที่ก่อให้เกิดความเสียหายที่เกิดขึ้นได้

ตามกฎหมายการคุ้มครองระบบคอมพิวเตอร์ของรัฐบาลกลาง ค.ศ.1979 ซึ่งแก้ไขเพิ่มเติมประมวลกฎหมายของสหรัฐอเมริกา บรรพที่ 18 โดยเพิ่มเติม มาตรา 1028 ขึ้นนั้น ได้บัญญัติความผิดฐานเข้าถึงไว้ 2 อนุมาตราด้วยกัน คือ ในอนุมาตรา (ก) บัญญัติถึงการเข้าถึงก่อให้เกิดการเข้าถึงหรือพยายามเข้าถึงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข่ายงานคอมพิวเตอร์ หรือส่วนหนึ่งส่วนใดของสิ่งดังกล่าว ซึ่งได้ปฏิบัติงานให้แก่องค์กรที่สำคัญ ๆ ของรัฐ โดยมีเจตนาพิเศษในการหลอกลวงหรือได้ไปซึ่งเงิน ทรัพย์สิน หรือบริการ เป็นความผิดฐานหนึ่ง และในอนุมาตรา (ข) บัญญัติถึงการเข้าถึงตามอนุมาตรา (ก) และการเข้าถึงคอมพิวเตอร์ ซอฟท์แวร์ โปรแกรมคอมพิวเตอร์ หรือข้อมูลที่บรรจุอยู่ในเครื่องคอมพิวเตอร์ระบบ หรือข่ายงานคอมพิวเตอร์โดยปราศจากอำนาจเป็นความผิดอีกฐานหนึ่ง

การกำหนด "ความผิดฐานเข้าถึง" ตามมาตรา 1028 เป็นฐานความผิดชนิดหนึ่ง โดยกฎหมายบัญญัติเป็นพิเศษว่าเมื่อมีการเข้าถึงเกิดขึ้น ผู้กระทำจะต้องมีความผิดตามมาตรานี้ ซึ่งเป็นการบัญญัติขึ้นเพื่อแก้ไขปัญหาข้อขัดข้องของกฎหมายอาญาโดยเฉพาะความผิดฐานลักทรัพย์ เนื่องจากกฎหมายที่มีอยู่แล้วในเรื่องลักทรัพย์ได้ประสบปัญหาข้อขัดข้องในการนำมาบังคับใช้กับความผิดที่เกิดขึ้นกับเทคโนโลยีสมัยใหม่ โดยเหตุที่ความผิดฐานลักทรัพย์นั้น

ส่วนใหญ่จะเป็นเรื่องที่เกี่ยวกับทรัพย์ที่จับต้องได้และทรัพย์ที่จับต้องไม่ได้ในบางกรณี ประกอบกับองค์ประกอบอันเป็นสาระสำคัญของความผิดฐานลักทรัพย์กำหนดว่าต้องมีการ "เอาไป" จึงก่อให้เกิดปัญหาขึ้นในเมื่อการกระทำความผิดได้เข้าไปเกี่ยวข้องกับคอมพิวเตอร์ เพราะการ "เอาไป" ในกรณีนี้อาจจะมิได้จับต้องทรัพย์หรือพาทรัพย์ไปเลยก็ได้ แต่ในความเป็นจริงแล้วผู้กระทำความผิดได้ไปซึ่งข้อมูลแล้ว ในขณะที่ข้อมูลเดิมนั้นก็ยังอยู่เหมือนเดิม จึงเกิดปัญหาว่าการกระทำดังกล่าวเป็นการลักทรัพย์หรือไม่ ซึ่งแตกต่างจากการประกอบอาชญากรรมในรูปแบบเดิมที่จะต้องมีการ "เอาไป" เพื่อแก้ไขสภาพปัญหาดังกล่าวประเทศสหรัฐอเมริกาจึงได้บัญญัติกฎหมายอาญาในความผิดเกี่ยวกับคอมพิวเตอร์ในส่วนของความผิดดังกล่าวเป็น "ความผิดฐานเข้าถึง" (Access) ขึ้นต่างหากจากความผิดฐานลักทรัพย์ เพื่อที่จะสามารถนำมาใช้บังคับกับการกระทำที่ก่อให้เกิดความเสียหายอันมีลักษณะของการลักขโมยนี้โดยเฉพาะ

5.1.1.2 ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... ของประเทศไทย

จะเห็นได้ว่าวิวัฒนาการทางเทคโนโลยีสมัยใหม่มีผลกระทบต่อระบบเศรษฐกิจการเมืองและสังคมโลกอย่างทั่วถึง โดยเฉพาะอย่างยิ่งเครื่องคอมพิวเตอร์ได้เข้าไปมีส่วนเกี่ยวข้องกับชีวิตประจำวันของมนุษย์ ทำให้เกิดการกระทำความผิดเกี่ยวกับเครื่องคอมพิวเตอร์หรือที่เรียกกันว่า "อาชญากรรมทางคอมพิวเตอร์" เพิ่มมากขึ้นเรื่อย ๆ สำหรับประเทศไทยแม้ว่าจะได้มีการนำเครื่องคอมพิวเตอร์มาใช้ไม่ต่ำกว่า 30 ปีแล้ว แต่ปรากฏว่ายังขาดกฎหมายที่จะบังคับใช้กับอาชญากรรมดังกล่าวโดยเฉพาะ จะมีเพียงแต่ใช้กฎหมายอื่นที่มีข้อหาความผิดใกล้เคียงกันมาปรับใช้เท่านั้น ทำให้เกิดปัญหาในการบังคับใช้กฎหมายเนื่องจากองค์ประกอบความผิดไม่สมบูรณ์เพียงพอที่จะปราบปรามการกระทำความผิดในลักษณะนี้ได้ ในขณะที่ประเทศต่าง ๆ ได้มีการเคลื่อนไหวดำเนินการกำหนดกฎหมายเฉพาะเพื่อปราบปรามอาชญากรรมไปแล้วหลายประเทศ ซึ่งการบัญญัติกฎหมายในเรื่องนี้นับว่าเป็นเรื่องค่อนข้างละเอียด ผู้มีหน้าที่บัญญัติกฎหมายจะต้องมีความรู้ในเรื่องคอมพิวเตอร์เป็นอย่างดี หากบทบัญญัติกฎหมายกำหนดฐานความผิดไว้ไม่ครอบคลุมก็จะเกิดเป็นช่องว่างทำให้อาชญากรสามารถกระทำความผิดได้ แต่ถ้าบัญญัติไว้เคร่งครัดเกินไป ก็จะเป็นการขัดขวางความเจริญก้าวหน้าทางเทคโนโลยี นอกจากนี้บทกำหนดโทษก็เป็นส่วนสำคัญที่จะต้องพิจารณา เพราะอาชญากรรมทางคอมพิวเตอร์จะสร้างความเสียหายเป็นมูลค่ามหาศาล นอกจากความเสียหายที่สามารถคำนวณเป็นตัวเงินได้แล้ว ยังก่อให้เกิดความเสียหายบางประการที่ไม่อาจคำนวณเป็นตัวเงินได้ เช่น ทำให้ต่างประเทศเกิดความไม่เชื่อมั่นในการที่จะมาร่วมลงทุนในประเทศไทย เพราะเกรงว่า

อาจจะไม่ได้รับความคุ้มครอง เป็นต้น และยังก่อให้เกิดความเสียหายต่อความเจริญทางด้านเทคโนโลยีสารสนเทศ ความสงบสุขและความมั่นคงของประเทศอีกด้วย

ก. ความเป็นมาของร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ....

ด้วยบทบาทของเทคโนโลยีสารสนเทศที่มีต่อการดำเนินชีวิตเพิ่มขึ้นทุกขณะ จึงได้มีการจัดตั้งคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ซึ่งมีชื่อย่อว่า "กทสช." โดยจัดตั้งขึ้นตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศ พ.ศ. 2535 โดยมีวัตถุประสงค์เพื่อให้การดำเนินงานด้านการส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศเป็นไปอย่างต่อเนื่องและมีประสิทธิภาพ โดยให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติมีอำนาจและหน้าที่ในการเสนอแนะแผนการพัฒนาเทคโนโลยีสารสนเทศแห่งชาติต่อคณะรัฐมนตรี เพื่อพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศ สร้างบรรยากาศให้มีการนำเทคโนโลยีสารสนเทศเข้ามาใช้ในการดำเนินงานต่าง ๆ พัฒนาโครงสร้างพื้นฐานด้านโทรคมนาคม ปรับปรุงกฎหมาย ระเบียบข้อบังคับให้สอดคล้องกับการดำเนินธุรกิจสมัยใหม่โดยสื่ออิเล็กทรอนิกส์ ส่งเสริมการผลิต การบริการ การวิจัยและพัฒนาให้มีเทคโนโลยีด้านสารสนเทศขึ้นในประเทศไทย ตลอดจนส่งเสริมผู้ประกอบการขนาดกลางและขนาดเล็ก นอกจากนั้นยังให้มีอำนาจหน้าที่ในการส่งเสริมและสนับสนุนการผลิต การบริการและการใช้เทคโนโลยีสารสนเทศของประเทศ และเสนอแนะต่อคณะรัฐมนตรีเพื่อกำหนดมาตรการแก้ไขปัญหาและอุปสรรคในการพัฒนาเทคโนโลยีสารสนเทศ รวมทั้งให้มีอำนาจแต่งตั้งคณะอนุกรรมการใด ๆ ตามระเบียบสำนักนายกรัฐมนตรีตามความจำเป็นและเหมาะสมและปฏิบัติการอื่นใดตามที่คณะรัฐมนตรีมอบหมาย

เพื่อปฏิบัติตามอำนาจหน้าที่และภารกิจที่ได้รับมอบหมาย คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ จึงได้จัดทำนโยบายไอที 2000 ขึ้น โดยเสนอภารกิจหลักเบื้องต้นที่รัฐควรจะดำเนินการโดยเร่งรีบ 3 ประการ ได้แก่ การลงทุนในโครงสร้างพื้นฐานสารสนเทศแห่งชาติ การลงทุนในด้านพัฒนาคุณภาพของพลเมือง และการลงทุนในการบริหารและบริการภาครัฐที่ดี ทั้งนี้โดยมีกลยุทธ์ในการบรรลุเป้าหมายหลักแห่งภารกิจในประการสำคัญ ๆ ได้แก่ นโยบายด้านโครงสร้างพื้นฐานสารสนเทศ โดยเร่งพัฒนาและขยายระบบสื่อสารในชนบทไทย รวมทั้งทบทวนและปฏิรูปกฎหมายอื่น ๆ ที่เกี่ยวข้อง นโยบายการพัฒนาทรัพยากรมนุษย์ โดยการเร่งผลิตบุคลากรด้านเทคโนโลยีสารสนเทศอย่างจริงจังในทุกระดับ นโยบายพัฒนาระบบสารสนเทศภาครัฐ ปรับปรุงบทบาทของภาครัฐเพื่อบริการที่ดีขึ้นและเพื่อสร้างฐานอุตสาหกรรมสารสนเทศ

ที่แข็งแกร่ง โดยดำเนินโครงการระบบสารสนเทศภาครัฐให้ครอบคลุมทั่วประเทศ อย่างไรก็ดี เพื่อรองรับการเติบโตและการก้าวเข้าสู่สังคมสารสนเทศได้อย่างมั่นใจด้วยความระมัดระวังและปลอดภัย กฎหมายจึงเป็นมาตรการอันจำเป็นประการหนึ่งที่ใช้เป็นกรอบในการกำหนดกติกาของสังคม ดังนั้นทิศทางและกลยุทธ์เบื้องต้นประการหนึ่งที่จำเป็นต่อการบรรลุเป้าหมายของนโยบายไอที 2000 คือ การทบทวนและแก้ไขกฎหมายที่เกี่ยวข้องทั้งหมด รวมทั้งการยกร่างกฎหมายใหม่ที่จะส่งเสริมการพัฒนาและการใช้เทคโนโลยีสารสนเทศ โดยคณะรัฐมนตรีได้มีมติเมื่อวันที่ 28 กุมภาพันธ์ 2539 เห็นชอบกับนโยบายเทคโนโลยีสารสนเทศ (ไอที 2000) ตามที่กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อมเสนอ เพื่อพัฒนาสังคมและเสริมสร้างความแข็งแกร่งทางธุรกิจ อุตสาหกรรม และการค้าระหว่างประเทศ ในการก้าวเข้าสู่สังคมสารสนเทศซึ่งเป็นยุคเศรษฐกิจใหม่แห่งศตวรรษ ที่ 21 [77]

กฎหมายเทคโนโลยีสารสนเทศ (Information Technology Law) หรือมักเรียกกันว่า "กฎหมายไอที (IT Law)" ในเบื้องต้นที่จำเป็นต้องมีการตรากฎหมายขึ้นใช้บังคับมีทั้งสิ้น 6 ฉบับ ได้แก่ กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ กฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายลำดับรองของรัฐธรรมนูญ มาตรา 78 ว่าด้วยการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน ซึ่งมีสาระสำคัญสรุปได้ดังนี้

1. <u>พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์</u> กฎหมายฉบับนี้เป็นกฎหมายเสริมเข้ากับประมวลกฎหมายแพ่งและพาณิชย์และกฎหมายอื่น ๆ ซึ่งไม่จำเป็นที่จะต้องเข้าไปแก้กฎหมายเดิมให้ยุ่งยาก โดยผลของกฎหมายนี้ก็จะทำให้เกิดความน่าเชื่อถือในการทำธุรกรรมอิเล็กทรอนิกส์ เป็นการรองรับสถานะทางกฎหมายให้การรับส่งข้อมูลทางอิเล็กทรอนิกส์เป็นเสมือนการส่งเอกสารที่มีหลักฐานเป็นหนังสือ

---

[77] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, <u>โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 2)</u>, หน้า 13-17.

2. พระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ กฎหมายฉบับนี้เกิดขึ้นเพื่อที่จะรองรับความน่าเชื่อถือด้านเทคโนโลยีการลงลายมือชื่ออิเล็กทรอนิกส์ให้มีความน่าเชื่อถือเช่นเดียวกับการลงลายมือชื่อแบบธรรมดา ซึ่งได้วางหลักเกณฑ์และวิธีการที่เชื่อถือได้ในการสร้างลายมือชื่ออิเล็กทรอนิกส์ที่สามารระบุตัวบุคคลผู้ลงลายมือชื่อ และที่แสดงว่าบุคคลนั้นเห็นด้วยกับข้อมูลอิเล็กทรอนิกส์ที่มีการลงลายมือชื่อนี้ กฎหมายลายมือชื่ออิเล็กทรอนิกส์มีความซับซ้อนยุ่งยากมากและต้องมีมาตรฐานที่ทัดเทียมกับนานาประเทศ เพื่อให้มีความน่าเชื่อถือโดยจะต้องพิสูจน์ว่าข้อมูลนี้มีความครบถ้วนแท้จริงสามารถระบุตัวบุคคลได้จริงและมีวิธีการห้ามปฏิเสธความรับผิดชอบ

3. กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ กฎหมายฉบับนี้เพื่อเพิ่มความมั่นใจของผู้ประกอบการต่าง ๆ ที่ใช้พาณิชย์อิเล็กทรอนิกส์ เพราะการลักลอบเข้าสู่ระบบสามารถทำกันได้และยังไม่มีกฎหมายใด ๆ ระบุโทษเพื่อรองรับปัญหานี้ ซึ่งกฎหมายฉบับนี้มีความสลับซับซ้อนในการตรวจสอบ แต่ก็มีความเร่งด่วนที่จะอนุมัติใช้อย่างมาก

4. กฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ เป็นกฎหมายที่ร่างขึ้นเพื่อวางกฎเกณฑ์ในการทำธุรกรรมทางการเงินให้มีความสะดวกและปลอดภัยมากขึ้น บนพื้นฐานของการติดต่อกันผ่านทางเครือข่ายอิเล็กทรอนิกส์ อันจะส่งผลให้ผู้บริโภคได้รับความคุ้มครองมากขึ้น

5. กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ปัจจุบันการเก็บรวบรวมข้อมูลในเครื่องคอมพิวเตอร์และการนำไปเผยแพร่มีความสะดวกรวดเร็วและทำได้ง่ายมาก จึงมีกฎหมายออกมาเพื่อคุ้มครองสิทธิส่วนบุคคลป้องกันมิให้ผู้อื่นนำข้อมูลส่วนตัวไปใช้ในทางเสียหาย

6. กฎหมายลำดับรองของรัฐธรรมนูญ มาตรา 78 กฎหมายฉบับนี้เป็นกฎหมายที่จะลดช่องว่างระหว่างผู้ที่ด้อยโอกาสในการใช้เทคโนโลยีสารสนเทศกับผู้ที่มีโอกาสใช้เทคโนโลยีเพราะเกิดจากโครงสร้างพื้นฐานสารสนเทศการเข้าถึงข้อมูลข่าวสารอย่างไม่ทัดเทียมและไม่ทั่วถึงกัน ซึ่งอาจจะเกิดจากความเจริญไม่ทั่วถึงหรือประชาชนไม่สามารถที่จะรับข้อมูลข่าวสารผ่านทางอินเตอร์เน็ตได้ พระราชบัญญัติการประกอบการโทรคมนาคมมีการให้จัดสรรงบประมาณที่จำเป็นผ่านทางกองทุนมาสู่การตอบแทนสังคมเพื่อยกระดับสังคมให้สูงขึ้น หากไม่มีกฎหมายฉบับนี้ก็จะมีการเอารัดเอาเปรียบกันเป็นอย่างมาก ระหว่างผู้ประกอบการกับบุคคลทั่วไปที่มีโอกาสในการใช้เทคโนโลยีสารสนเทศได้ไม่ทัดเทียมกัน

ต่อมาเมื่อวันที่ 15 ธันวาคม 2541 คณะรัฐมนตรีได้เห็นชอบต่อการจัดทำโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศที่เสนอโดยกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม และเห็นชอบให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ (National Information Technology Committee) หรือที่เรียกโดยย่อว่า "คณะกรรมการไอทีแห่งชาติ หรือ กทสช. (NITC)" ทำหน้าที่เป็นศูนย์กลางและประสานงานระหว่างหน่วยงานต่าง ๆ ที่กำลังดำเนินการจัดทำกฎหมายเทคโนโลยีสารสนเทศและกฎหมายอื่น ๆ ที่เกี่ยวข้อง ทั้งนี้ คณะกรรมการไอทีแห่งชาติได้แต่งตั้งคณะอนุกรรมการเฉพาะกิจเพื่อยกร่างกฎหมายไอทีทั้ง 6 ฉบับ โดยมอบหมายให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center) หรือที่มักเรียกโดยย่อว่า "เนคเทค" (NECTEC) สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (National Science and Technology Development Agency) หรือที่เรียกโดยย่อว่า "สวทช." กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม ในฐานะสำนักงานเลขานุการคณะกรรมการไอทีแห่งชาติทำหน้าที่เป็นเลขานุการในการยกร่างกฎหมายไอทีทั้ง 6 ฉบับ เนคเทคจึงได้เริ่มต้นโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศขึ้นเพื่อปฏิบัติตามนโยบายที่ได้รับมอบหมายจากรัฐบาลและคณะกรรมการไอทีแห่งชาติในการยกร่างกฎหมายไอทีทั้ง 6 ฉบับ ซึ่งในปัจจุบันนี้ได้มีการประกาศใช้กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และกฎหมายว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ โดยรวมเป็นกฎหมายฉบับเดียวกัน ใช้ชื่อว่า "พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544" โดยได้ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 4 ธันวาคม 2544 และมีผลบังคับใช้เมื่อวันที่ 3 เมษายน 2545 สำหรับกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ยังอยู่ระหว่างยกร่างกฎหมายโดยคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ เพื่อขอความเห็นชอบต่อคณะรัฐมนตรี

ข. สาระสำคัญของร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ....

ร่างพระราชบัญญัติอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... * ฉบับนี้เป็นร่างฉบับล่าสุด (ฉบับผ่านการพิจารณาของคณะทำงานเพื่อพิจารณากฎหมายอาชญากรรมทางคอมพิวเตอร์) [78]

1. ชื่อร่างพระราชบัญญัติ

ในปัจจุบันอาชญากรรมมีหลายรูปแบบ โดยเฉพาะอาชญากรรมทางคอมพิวเตอร์เป็นอาชญากรรมรูปแบบใหม่ ร่างพระราชบัญญัติฉบับนี้จึงได้มีการกำหนดชื่อร่างพระราชบัญญัติไว้ให้มีความแตกต่างจากอาชญากรรมประเภทอื่นในกฎหมายอาญา เนื่องด้วยโครงสร้างการกระทำความผิดตลอดจนความเสียหายที่เกิดขึ้นมีความแตกต่างจากกฎหมายอาญาโดยทั่วไป แม้ว่าลักษณะของการกระทำความผิดจะคล้ายคลึงกันก็ตาม ดังนั้นเพื่อป้องกันความสับสนที่เกิดขึ้นและวัตถุประสงค์ของการตรากฎหมาย จึงเป็นที่มาของชื่อ "ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ...."

2. ระยะเวลาการบังคับใช้กฎหมาย

เนื่องจากร่างพระราชบัญญัติดังกล่าวได้กำหนดขึ้นเพื่อป้องกันการกระทำความผิดทางคอมพิวเตอร์และสร้างวินัยในการใช้ข้อมูลทางคอมพิวเตอร์ ร่างพระราชบัญญัติฉบับนี้จึงควรกำหนดให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป คือมีผลบังคับใช้ทันที

---

* รายละเอียดปรากฏในภาคผนวก ค.

[78] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม, ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... และร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... (กรุงเทพมหานคร : บริษัท โรงพิมพ์เดือนตุลา จำกัด, 2544), หน้า 146-149.

3. **บทนิยามที่สำคัญ**

เนื่องจากร่างพระราชบัญญัติฉบับนี้ยังมิได้กำหนดคำนิยามเอาไว้ อยู่ระหว่างขั้นตอนการพิจารณาของอนุคณะกรรมการว่าเหมาะสมจะบัญญัติไว้ในร่างพระราชบัญญัติหรือไม่ ผู้เขียนจึงได้นำเอาคำนิยามในร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... ฉบับก่อนหน้านี้ (ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... ฉบับยกร่างขึ้นโดยโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ เพื่อเผยแพร่ในงานสัมมนา "กฎหมายเทคโนโลยีสารสนเทศ" ระหว่างวันที่ 31 กรกฎาคม - 3 สิงหาคม 2544 [79] มาศึกษาไปพลางก่อน

ร่างพระราชบัญญัติฉบับนี้ได้กำหนดนิยามไว้หลายนิยาม โดยผู้เขียนจะขอกล่าวถึงบางคำนิยามที่เกี่ยวข้องเท่านั้น

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดโปรแกรมให้อุปกรณ์หนึ่งหรืออุปกรณ์ใดชุดหนึ่งทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูล" หมายความว่า สิ่งซึ่งสื่อความหมายหรือการแสดงข้อความหรือความคิดที่ตระเตรียมหรือได้ตระเตรียมไว้ในรูปแบบที่เหมาะสมสำหรับใช้กับคอมพิวเตอร์

"ข้อมูลอิเล็กทรอนิกส์" หมายความว่า ข้อมูลหรือข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผล ด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร รวมทั้งลายมือชื่ออิเล็กทรอนิกส์

---

[79] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม, ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... และร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (กรุงเทพมหานคร:หจก. จิรรัชการพิมพ์, 2544), หน้า 21-31.

4. ฐานความผิด

ปัญหาพื้นฐานของกฎหมายอาชญากรรมทางคอมพิวเตอร์นั้นล้วนแต่เกิดจากกฎหมายอาญาที่ใช้อยู่ในปัจจุบันนั้น มุ่งที่จะคุ้มครองทรัพย์ที่มีรูปร่าง (Corporeal Object) โดยมิได้มุ่งเน้นที่จะคุ้มครองข้อมูลข่าวสารซึ่งเป็นวัตถุที่ไม่มีรูปร่าง (Incorporeal Object) เช่น คลื่นแม่เหล็กไฟฟ้า (Electromagnetic Impulse) เป็นต้น และในยุคที่พัฒนาการทางเทคโนโลยีเจริญก้าวหน้าไปอย่างรวดเร็ว ทำให้เกิดรูปแบบของอาชญากรรมแบบใหม่ โดยเฉพาะอย่างยิ่งอาชญากรรมทางคอมพิวเตอร์ ซึ่งได้เปลี่ยนแปลงรูปแบบของการก่ออาชญากรรมไปจากเดิม ที่กฎหมายอาญามุ่งคุ้มครองทรัพย์ที่มีรูปร่างไปสู่การคุ้มครองทรัพย์ที่ไม่มีรูปร่าง ซึ่งอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ไม่ว่าจะเป็นการบุกรุกทางเครือข่าย การฉ้อโกง การปลอมแปลงข้อมูล หรือการทำลายระบบคอมพิวเตอร์ เป็นต้น โดยรูปแบบของการก่ออาชญากรรแบบใหม่นี้ก่อให้เกิดช่องว่างที่กฎหมายอาญาไม่สามารถครอบคลุมถึงการกระทำความผิดเหล่านี้ได้ และเนื่องจากการกระทำความผิดนั้นอาจซับซ้อนและยากต่อการตรวจสอบหรือทำการสืบพิสูจน์ แต่ในทางกลับกันการกระทำความผิดนั้นทำให้เกิดความเสียหายในทางเศรษฐกิจเป็นมูลค่ามหาศาล จนเป็นเหตุให้ต้องบัญญัติกฎหมายขึ้นมารองรับและคุ้มครองสังคมและเพื่อป้องกันมิให้เกิดการสูญหายหรือความเสียหายอันอาจเกิดขึ้นในอนาคต

ร่างพระราชบัญญัติฉบับนี้ได้กำหนดฐานความผิดไว้หลายฐานความผิดด้วยกัน เช่น การเข้าถึงข้อมูลโดยไม่มีอำนาจ (มาตรา 6) การดักข้อมูลคอมพิวเตอร์ (มาตรา 7) การรบกวนการทำงานของโปรแกรมคอมพิวเตอร์ (มาตรา 8) การผลิตหรือจำหน่ายเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่เกี่ยวข้องเพื่อใช้ในการกระทำความผิด (มาตรา 10) การเปลี่ยนแปลงการปลอมแปลงข้อมูล (มาตรา 11) การฉ้อโกงทางคอมพิวเตอร์ (มาตรา 12) การจารกรรมข้อมูลและการก่อวินาศกรรมทางคอมพิวเตอร์ (มาตรา 13) ซึ่งผู้เขียนจะขอกล่าวถึงเฉพาะฐานความผิดเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์ ซึ่งเป็นการกำหนดฐานความผิดเพื่อที่จะลงโทษผู้กระทำความผิดเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตโดยตรง

ความผิดฐานฉ้อโกงนี้บัญญัติอยู่ในหมวด 2 ความผิดเกี่ยวข้องกับคอมพิวเตอร์ (Computer related Crime) มาตรา 12 บัญญัติว่า "ผู้ใดกระทำการใด ๆ อันเป็นการรบกวนโปรแกรมคอมพิวเตอร์ หรือโดยใช้ข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์ หรือใช้ข้อมูลโดยไม่มีอำนาจโดยชอบ หรือทำการรบกวนทำธุรกรรมโดยไม่มีอำนาจ เพื่อให้ได้มาซึ่งประโยชน์ในลักษณะที่เป็นทรัพย์สินสำหรับตนหรือผู้อื่น ต้องระวางโทษ ..."

มาตรานี้บัญญัติขึ้นเพื่อกำหนดฐานความผิดและลงโทษสำหรับการกระทำโดยเจตนาทุจริตในการประมวลผลข้อมูลเพื่อโอนทรัพย์หรือได้ทรัพย์ของผู้อื่นมาเป็นของตนโดยฝ่าฝืนต่อบทบัญญัติแห่งกฎหมาย เช่น การสร้างโปรแกรม salami techniques เพื่อปัดเศษเงินในบัญชีของบุคคลอื่นมารวมเก็บไว้ในบัญชีของตนเอง หรือโปรแกรม logic bombs เพื่อเฝ้าติดตามความเคลื่อนไหวของระบบบัญชีและระบบเงินเดือนและทำการเปลี่ยนแปลงตัวเลขในระบบดังกล่าว เป็นต้น [80]

และยังมีบทบัญญัติกำหนดความผิดฐานเข้าถึงไว้ในหมวด 1 ความผิดเกี่ยวกับการรักษาความลับ และการทำงานของระบบข้อมูลและระบบคอมพิวเตอร์ มาตรา 6 บัญญัติว่า "ผู้ใดโดยไม่มีอำนาจโดยชอบ เข้าถึงเพื่อตนหรือผู้อื่นซึ่งข้อมูลมิได้มีไว้สำหรับตนเอง ที่เก็บหรือส่งโดยวิธีการทางอิเล็กทรอนิกส์และที่มีวิธีการป้องกันเฉพาะ ต้องระวางโทษ ..."

การกระทำความผิดฐานเข้าถึงโดยมิชอบหรือโดยไม่มีอำนาจหรือโดยฝ่าฝืนต่อบทบัญญัติแห่งกฎหมายนี้อาจเกิดขึ้นหลายวิธี เช่น การเจาะระบบ (Hacking or Cracking) หรือการบุกรุกทางคอมพิวเตอร์ (Computer Trespass) เพื่อทำลายระบบคอมพิวเตอร์หรือเปลี่ยนแปลงแก้ไขข้อมูล หรือเข้าถึงข้อมูลที่เก็บรักษาไว้เป็นความลับ เช่น รหัสผ่าน (Passwords) หรือความลับทางการค้า (Secret Trade) เป็นต้น และอาจเป็นที่มาของการกระทำความผิดฐานอื่นต่อไป เช่น การใช้คอมพิวเตอร์เพื่อฉ้อโกงหรือปลอมเอกสาร เป็นต้น อันอาจก่อให้เกิดความเสียหายต่อเนื่องเป็นมูลค่ามหาศาล

---

[80] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม, ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... และร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ...., หน้า111.

คำว่า "การเข้าถึง" (access) ในที่นี้ หมายความถึง การเข้าถึงทั้งในระดับกายภาพ เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์และผู้กระทำความผิดดำเนินการด้วยวิธีใดวิธีหนึ่ง เพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้ โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเอง และหมายรวมถึงการเข้าถึงระบบคอมพิวเตอร์ แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์ แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์ที่ตนต้องการได้

นอกจากนั้นความผิดฐานนี้อาจเป็นการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้นจึงอาจหมายถึงการเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์ ข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจร เป็นต้น และยังหมายรวมถึงการเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น ระบบเครือข่ายอินเตอร์เน็ต อันเป็นการเชื่อมโยงระหว่างเครือข่ายหลาย ๆ เครือข่ายเข้าด้วยกัน และยังหมายถึงการเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN (Local Area Network) อันเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ ๆ กันเข้าด้วยกัน

ประเด็นที่จำเป็นต้องพิจารณาเกี่ยวกับการกระทำความผิดฐานนี้ คือ เพียงแต่มีการเข้าถึงโดยไม่ได้รับอนุญาตจะถือว่าเป็นการก่ออาชญากรรมได้หรือไม่ หรือผู้กระทำต้องมีมูลเหตุจูงใจที่จะกระทำให้เกิดความเสียหายด้วย เช่น บุคคลซึ่งมิได้มีมูลเหตุจูงใจดังกล่าว แต่ต้องการทดลองวิชา จึงเข้าไปในระบบข้อมูลของบุคคลอื่นโดยมิได้มีมูลเหตุจูงใจที่จะก่อให้เกิดความเสียหาย กรณีดังกล่าวควรกำหนดให้ต้องรับผิดและมีบทลงโทษหรือไม่ หรือกรณีที่มีการเข้าถึงแม้โดยไม่มีมูลเหตุจูงใจที่จะก่อให้เกิดความเสียหาย เช่น การเข้าไปในระบบข้อมูลของโรงพยาบาลและทำให้เกิดการเปลี่ยนแปลงคำสั่งการรักษาพยาบาล การผ่าตัดหรือการจ่ายยาให้ผู้ป่วยผิดพลาดไปจากที่กำหนดไว้เดิม อันก่อให้เกิดความเสียหาย คือ อันตรายอย่างยิ่งต่อผู้ป่วย กรณีดังกล่าวนี้จะกำหนดขอบเขตในการพิจารณาว่าเป็นความผิดอย่างไร ซึ่งร่างพระราชบัญญัติฯ มาตรา 6 ได้กำหนดให้การเข้าถึงโดยมิชอบเป็นความผิด แม้ว่าผู้กระทำมิได้มีมูลเหตุจูงใจเพื่อก่อให้เกิดความเสียหายก็ตาม ทั้งนี้เพราะว่าการกระทำดังกล่าวนั้นสามารถก่อให้เกิดการกระทำฐานอื่นหรือฐานที่ใกล้เคียงค่อนข้างง่าย และอาจก่อให้เกิดความเสียหาย

ร้ายแรง รวมทั้งการพิสูจน์มูลเหตุจูงใจทำได้ค่อนข้างยาก ซึ่งเป็นการบัญญัติตรงกับความผิดตามมาตรา 1028 อนุมาตรา (ข) ที่บัญญัติให้การเข้าถึงโดยปราศจากอำนาจเป็นความผิด [81]

5. บทสันนิษฐาน

เพื่อความสอดคล้องกับยุคข้อมูลข่าวสารได้มีการกำหนดให้มีบทสันนิษฐานการกระทำความผิดทางคอมพิวเตอร์ไว้ ซึ่งได้กำหนดว่าบุคคลใดที่มีการครอบครองหรือควบคุมโปรแกรมคอมพิวเตอร์ หรือข้อมูลต่าง ๆ ไว้โดยไม่มีอำนาจ ให้ถือว่าผู้นั้นได้เข้าถึงโปรแกรมข้อมูล หรือข้อความนั้นแล้ว

6. ผู้รักษาการตามกฎหมาย

ร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัติฉบับนี้

7. ความจำเป็นในการตรากฎหมายอาชญากรรมทางคอมพิวเตอร์

เนื่องจากประเทศไทยกำลังก้าวเข้าสู่ยุคสังคมสารสนเทศ ความก้าวหน้าทางเทคโนโลยีได้เปลี่ยนวิถีชีวิตเดิม ๆ ของคนในสังคมไปเป็นอย่างมาก โดยเฉพาะอย่างยิ่งในการนำเอาเครื่องคอมพิวเตอร์มาใช้ในชีวิตประจำวัน ซึ่งหากมิได้นำไปใช้ในทางสร้างสรรค์แต่นำไปใช้ในทางมิชอบหรือทำลายก็จะสร้างความเดือดร้อนหรือไม่สงบสุขมาสู่ชุมชน รวมทั้งอาจจะส่งผลกระทบต่อความมั่นคงของรัฐได้ และเนื่องจากการประกอบอาชญากรรมคอมพิวเตอร์นั้นมีความแตกต่างไปจากการประกอบอาชญากรรมแบบเดิมมาก และกฎหมายที่มีอยู่เดิมไม่สามารถนำมาปรับใช้กับพฤติกรรมใหม่ ๆ ที่ก่อเกิดความเสียหายต่อสังคม จึงจำเป็นต้องตรากฎหมายดังกล่าวขึ้นใช้บังคับกับสังคม

---

[81] เรื่องเดียวกัน, หน้า 105-107.

8. ข้อสังเกตร่างพระราชบัญญัติอาชญากรรมทางคอมพิวเตอร์

ร่างพระราชบัญญัติฉบับนี้เป็นเพียงกฎหมายเบื้องต้นในการกำหนดความผิดเท่านั้น ซึ่งได้มีนักวิชาการหลายท่านได้เสนอให้มีการพิจารณาในเรื่องความผิดอันยอมความไว้ด้วย โดยเป็นการเปิดโอกาสให้กับผู้เสียหายสำหรับการกระทำความผิดที่เกิดขึ้น นอกจากนี้ในการรับฟังพยานเอกสารของศาลไทยตามประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 93 นี้ก็ได้กำหนดให้การรับฟังพยานเอกสารเพียงต้นฉบับเอกสารเท่านั้น ซึ่งพยานเอกสารหมายถึงข้อความใด ๆ ที่ศาลอาจตรวจดูได้จากหนังสือลายลักษณ์อักษรหรือรูป โดยประการที่ว่ารูปรอยนั้นได้เป็นเครื่องหมายแทนคำพูดในภาษาใดภาษาหนึ่ง ดังนั้นโปรแกรมหรือคำสั่งที่เข้าเครื่องคอมพิวเตอร์ เพื่อแสดงผลเป็นข้อมูลต่าง ๆ ออกมาเป็นภาษาหรือตัวเลขย่อมอยู่ในความหมายของพยานเอกสารด้วย ซึ่งในขณะนี้ได้มีข้อกำหนดของศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศกลางรวมทั้งศาลล้มละลายกลาง กำหนดให้รับฟังพยานหลักฐานที่อยู่ในรูปของสื่ออิเล็กทรอนิกส์แล้ว นอกจากนี้ปัจจุบันประมวลกฎหมายวิธีพิจารณาความแพ่งและประมวลกฎหมายวิธีพิจารณาความอาญาก็อยู่ในระหว่างการปรับแก้เพื่อให้สามารถรับฟังพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ได้เช่นกัน

5.1.2.3 วิเคราะห์ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... ของประเทศไทยกับการหลอกลวงทางอินเตอร์เน็ต

เมื่อพิจารณาร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... ว่าจะครอบคลุมถึงการประกอบอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ตทุกประเภทหรือไม่นั้น ผู้เขียนมีความเห็นว่าร่างพระราชบัญญัติดังกล่าวยังไม่ครอบคลุมถึงการหลอกลวงทางอินเตอร์เน็ต และยังมีปัญหาในการตีความอีกหลายประการ ซึ่งผู้เขียนขอสรุปปัญหาดังนี้

1. ตามพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ได้กำหนดให้ความผิดฐานฉ้อโกงประกอบด้วยการกระทำความผิดหลายประการ ดังนี้

1.1 กระทำการใดๆ อันเป็นการรบกวนโปรแกรมคอมพิวเตอร์

1.2 โดยใช้ข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์

1.3 ใช้ข้อมูลโดยไม่มีอำนาจโดยชอบ

1.4 ทำการรบกวนการทำธุรกรรมโดยไม่มีอำนาจ

การกระทำอันเป็นการรบกวนโปรแกรมคอมพิวเตอร์ หมายถึง การกระทำอันเป็นการรบกวนการกระทำโดยปกติของโปรแกรมคอมพิวเตอร์ เช่น การสร้างโปรแกรม salami techniques เพื่อปัดเศษเงินในบัญชีของบุคคลอื่นมารวมเก็บไว้ในบัญชีของตนเอง หรือโปรแกรม logic bombs เพื่อเฝ้าติดตามความเคลื่อนไหวของระบบบัญชีและระบบเงินเดือนและทำการเปลี่ยนแปลงตัวเลขในระบบดังกล่าว สำหรับการใช้ข้อมูลที่ไม่ถูกต้องและการใช้ข้อมูลโดยไม่มีอำนาจ เมื่อพิจารณาประกอบกับนิยามคำว่า "ข้อมูล" ซึ่งหมายถึงสิ่งซึ่งสื่อความหมายหรือการแสดงข้อความหรือความคิดที่ตระเตรียมหรือได้ตระเตรียมไว้ในรูปแบบที่เหมาะสมสำหรับใช้กับคอมพิวเตอร์ ผู้เขียนเห็นว่าหมายถึงข้อมูลที่บุคคลเตรียมไว้เพื่อนำไปใส่ในเครื่องคอมพิวเตอร์เท่านั้น ไม่หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ที่ได้ประมวลผลโดยเครื่องคอมพิวเตอร์แล้ว ซึ่งจะทำให้กฎหมายครอบคลุมถึงการกระทำความผิดแค่การใช้ข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์ หมายถึงการใช้ข้อมูลที่เป็นเท็จนั่นเอง และการกระทำที่บุคคลอื่นที่ไม่มีอำนาจจะใช้ข้อมูลนั้นนำข้อมูลดังกล่าวมาแสวงหาประโยชน์เท่านั้นเอง หาได้ครอบคลุมถึงการใช้ข้อมูลที่เครื่องคอมพิวเตอร์ได้ประมวลผลแล้วหรือข้อมูลอิเล็กทรอนิกส์ที่ไม่ถูกต้องไม่

เมื่อพิจารณาถึงการบังคับใช้ร่างพระราชบัญญัติดังกล่าวกับการหลอกลวงทางอินเตอร์เน็ตนั้น ผู้เขียนเห็นว่าน่าจะครอบคลุมถึงการกระทำการหลอกลวงในรูปแบบเดิม คือ การใช้ข้อมูลอันเป็นเท็จหรือปกปิดข้อความจริงอันควรบอกกล่าวให้แจ้ง เพื่อให้ได้ไปซึ่งทรัพย์สินเท่านั้น แต่ไม่หมายความรวมถึงการหลอกลวงที่ผู้กระทำความผิดใช้ข้อมูลอิเล็กทรอนิกส์ที่ไม่ถูกต้อง หรือไม่สมบูรณ์ หรือไม่มีอำนาจโดยชอบด้วยกฎหมาย เช่น กรณีการหลอกลวงเกี่ยวกับการประกอบธุรกิจที่บ้าน (Work at Home Scams) การหลอกลวงเกี่ยวกับการลงทุน (Investment Scams) การหลอกลวงเกี่ยวกับทุนการศึกษา (Scholarship Scams) โดยผู้หลอกลวงกระทำผ่านทางส่งจดหมายอิเล็กทรอนิกส์ (e-mail) กรณีนี้จะถือว่าผู้หลอกลวงกระทำความผิดหรือไม่ เนื่องจากกฎหมายบัญญัติว่า "ผู้ใดกระทำการใดๆ ... โดยใช้ข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์ ..." ในขณะที่สิ่งที่ผู้หลอกลวงได้ใช้คือข้อมูลอิเล็กทรอนิกส์ (ตามนิยามคำว่า "ข้อมูลอิเล็กทรอนิกส์ หมายความว่า ข้อมูลหรือข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น ... จดหมายอิเล็กทรอนิกส์ ...") หาใช่ข้อมูลที่ตระเตรียมไว้ในรูปแบบที่เหมาะสมกับคอมพิวเตอร์ (นิยามของคำว่า "ข้อมูล") แต่อย่างใดไม่ไม่ ซึ่งผู้เขียนเห็นว่าการบัญญัติความผิดฐานฉ้อโกง ตามมาตรา 12 นี้ไม่ครอบคลุมถึงการกระทำความผิดเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตทุกกรณี จึงควรมีการแก้ไขฐานความผิดให้หมายความรวมถึงการใช้ข้อมูลอิเล็กทรอนิกส์ที่ไม่ถูกต้องหรือไม่สมบูรณ์ด้วย

หรือกรณีการหลอกลวงเกี่ยวกับบัตรเครดิต (Credit Card Loss Protection) ผู้หลอกลวงนำเอารายละเอียดบัตรเครดิตที่ผู้ถูกหลอกลวงให้ไว้เพื่อยืนยันว่าตนเองมีอายุ 18 ปีบริบูรณ์ เพื่อเข้าดูเว็บไซต์ลามก (ไม่ได้ให้เพื่อชำระเป็นค่าสินค้าหรือบริการ) หรือการหลอกลวงเกี่ยวกับการซื้อสินค้าออนไลน์ (General Merchandise Sales) หรือการประมูลสินค้าออนไลน์ (Online Auctions) ซึ่งผู้ถูกหลอกลวงให้รายละเอียดบัตรเครดิตเพื่อเป็นการรับประกันว่าเมื่อได้รับสินค้าแล้วผู้ซื้อจะชำระราคาค่าสินค้าให้ และผู้หลอกลวงได้นำรายละเอียดบัตรเครดิตดังกล่าวไปใช้ชำระค่าสินค้าหรือบริการโดยไม่มีอำนาจ กรณีนี้ผู้กระทำจะมีความผิดหรือไม่ เนื่องจากกฎหมายกำหนดว่า " ผู้ใดกระทำการใด ๆ ... โดยใช้มูลโดยไม่มีอำนาจโดยชอบ ... " กรณีนี้ผู้กระทำความผิดใช้ข้อมูลอิเล็กทรอนิกส์ (เนื่องจากข้อมูลดังกล่าวได้ผ่านการรับ ส่ง ด้วยวิธีการทางอิเล็กทรอนิกส์แล้ว) โดยไม่มีอำนาจโดยชอบ หาใช่เป็นการใช้ข้อมูลโดยไม่มีอำนาจโดยชอบไม่ ซึ่งหากจะพิจารณาถึงความผิดฐานเข้าถึงตามมาตรา 6 ของร่างพระราชบัญญัติฯ แล้ว จะพบว่าการกระทำดังกล่าวก็ไม่เป็นความผิดตามมาตราดังกล่าวเช่นกัน เนื่องจากกฎหมายบัญญัติว่า "ผู้ใดไม่มีอำนาจโดยชอบเข้าถึงเพื่อตนหรือผู้อื่นซึ่งข้อมูล ซึ่งมิได้มีไว้สำหรับตนเองที่เก็บหรือส่งโดยวิธีการทางอิเล็กทรอนิกส์ และที่มีวิธีการป้องกันเฉพาะ" จะเห็นได้ว่าความผิดฐานเข้าถึงนี้จะต้องมีการเข้าถึงโดยไม่มีอำนาจโดยชอบเท่านั้น แต่การกระทำความผิดดังกล่าวข้างต้นนั้นเป็นการเข้าถึงโดยมีอำนาจ เนื่องจากผู้หลอกลวงมีสิทธิ์ที่จะเข้าถึงเพื่อทราบรายละเอียดของบัตรเครดิตดังกล่าว จึงไม่ใช่เป็นการเข้าถึงโดยไม่มีอำนาจอันจะเป็นความผิดฐานเข้าถึงได้ ดังนั้นร่างพระราชบัญญัติดังกล่าวจึงไม่ได้ครอบคลุมถึงการหลอกลวงที่ได้ไปซึ่งข้อมูลอิเล็กทรอนิกส์ อันทำให้เป็นช่องว่างของกฎหมายทำให้ผู้กระทำความผิดไม่ต้องรับโทษตามกฎหมาย

เมื่อเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกา จะพบว่าได้มีการกำหนดฐานความผิดไว้กว้างกว่ากฎหมายของประเทศไทย โดยรวมความผิดฐานฉ้อโกงให้อยู่ในความผิดฐานเข้าถึงด้วย คือ ตามมาตรา 1028 อนุมาตรา ก. กำหนดว่าไม่ว่าจะเป็นการเข้าถึงโดยมีอำนาจหรือไม่มีอำนาจก็ตาม เพื่อได้ไปซึ่งเงิน ทรัพย์สิน หรือบริการสำหรับตนเองหรือผู้อื่นโดยวิธีการปลอมแปลงหรือการฉ้อโกง ซึ่งได้มีนิยามคำว่า "ทรัพย์สิน" รวมถึงข้อมูลที่ได้ประมวลผลหรือได้ผลิตขึ้นด้วยวิธีการอิเล็กทรอนิกส์และคอมพิวเตอร์ซอฟท์แวร์กับโปรแกรมคอมพิวเตอร์ที่อยู่ในรูปแบบซึ่งทั้งมนุษย์และเครื่องจักรกลสามารถอ่านเข้าใจได้ จะเห็นว่า

กฎหมายของประเทศสหรัฐอเมริกาได้มีการกำหนดว่าทรัพย์สินให้หมายความรวมถึงข้อมูลที่เกิดจากการประมวลผลของเครื่องคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ด้วย ดังนั้นกรณีที่ผู้หลอกลวงได้ทำการหลอกลวงเพื่อให้ได้ไปซึ่งข้อมูลอิเล็กทรอนิกส์ จึงถือว่าเป็นการได้ไปซึ่งทรัพย์สินแล้ว ผู้กระทำความผิดจึงต้องรับโทษตามกฎหมาย

2. ร่างพระราชบัญญัติอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... ของประเทศไทย กำหนดให้วัตถุแห่งการกระทำความผิดฐานนี้คือ ประโยชน์ในลักษณะที่เป็นทรัพย์สิน คำว่า "ประโยชน์ในลักษณะที่เป็นทรัพย์สิน" เท่าที่ปรากฏในตัวบทกฎหมายจะพบในประมวลกฎหมายอาญา ความผิดฐานกรรโชกทรัพย์ตามมาตรา 337 ความผิดฐานรีดเอาทรัพย์ตามมาตรา 338 ความผิดฐานผู้จัดการทรัพย์สินทำผิดหน้าที่ตามมาตรา 353 เป็นต้น ซึ่งการที่บัญญัติวลีนี้แทนคำว่า "ทรัพย์สิน" ก็เพราะประมวลกฎหมายอาญาประสงค์จะให้มีความหมายกว้างกว่าคำว่าทรัพย์สิน ซึ่งคำว่า "ประโยชน์ในลักษณะที่เป็นทรัพย์สิน" มีความหมายสองประการ ประการแรกหมายถึงตัวทรัพย์สิน และประการที่สองหมายถึงประโยชน์อื่นใดที่ไม่ถึงกับเป็นตัวทรัพย์สินดังกล่าวแล้ว แต่เข้าลักษณะที่เป็นทรัพย์สินเพราะอาจคิดราคาได้

ผู้เขียนมีข้อสังเกตว่าประโยชน์ในลักษณะที่เป็นทรัพย์สิน หมายความแค่ไหน เพียงไรจะหมายความรวมถึงข้อมูลอิเล็กทรอนิกส์หรือไม่ เช่น กรณีที่ผู้หลอกลวงได้ไปเพียงข้อมูลบัตรเครดิตของบุคคลอื่น และยังไม่ได้นำไปซื้อสินค้าหรือชำระค่าบริการ ซึ่งเป็นข้อมูลอิเล็กทรอนิกส์เท่านั้น กรณีนี้จะถือว่าการกระทำความผิดสำเร็จ และผู้กระทำความผิดจะต้องรับโทษตามกฎหมายหรือไม่ หรือผู้กระทำความผิดจะต้องรับโทษเพียงแค่พยายามกระทำความผิดเท่านั้น เนื่องจากผลของการกระทำยังไม่เกิดขึ้น หรือจะหมายความรวมถึงการได้ไปซึ่งบริการหรือไม่ เช่น กรณีผู้หลอกลวงได้ไปซึ่งการใช้บริการอินเตอร์เน็ต อันเป็นการได้ไปซึ่งบริการเท่านั้น ผู้กระทำความผิดจะต้องรับโทษหรือไม่ เนื่องจากได้มีแนวคำพิพากษาฎีกาวางหลักไว้ว่า "ทรัพย์สิน" ไม่หมายความรวมถึงบริการ จึงต้องว่าวินิจฉัยว่าคำว่า "ประโยชน์ในลักษณะที่เป็นทรัพย์สิน" จะหมายความรวมถึงบริการหรือไม่

ผู้เขียนเห็นว่าเพื่อมิให้เกิดปัญหาในการตีความภายหลังเช่นที่เคยปรากฏมาแล้วอดีต เนื่องจากการตีความกฎหมายอาญาต้องตีความโดยเคร่งครัด กล่าวคือเมื่อกฎหมายบัญญัติชัดแจ้งว่าการกระทำหรือการไม่กระทำอย่างหนึ่งอย่างใดเป็นความผิดอาญาแล้ว ก็ถือเฉพาะกรณีนั้น ๆ เท่านั้นที่เป็นความผิด จะไปรวมถึงกรณีอื่น ๆ ด้วยไม่ได้ หลักการตีความโดยเคร่งครัดนี้ยังหมายความรวมถึงการตีความดังกล่าวจะนำเอาบทกฎหมายใกล้เคียงมาใช้เป็นผลร้ายมิได้

ซึ่งหมายความถึงไม่ตีความโดยการเทียบเคียง (Analogy) นำเอาบทกฎหมายใกล้เคียงมาปรับใช้เพื่อลงโทษจำเลย หากจะปล่อยให้ศาลต้องมาตีความกับคำว่า "ประโยชน์ในลักษณะที่เป็นทรัพย์สิน" ก็อาจจะเกิดปัญหาในการบังคับใช้กฎหมายดังกล่าวได้ในอนาคต จึงควรจะกำหนดวัตถุแห่งการกระทำความผิดให้ชัดเจนเช่นเดียวกับกฎหมายของประเทศสหรัฐอเมริกาที่กำหนดให้ผู้ใดเข้าถึงโดยไม่มีอำนาจ และได้ไปซึ่งเงิน ทรัพย์สิน หรือบริการ มีความผิด และกำหนดนิยามคำว่า "ทรัพย์สิน" ให้หมายความรวมถึงข้อมูลที่ได้ประมวลผลหรือได้ผลิตขึ้นด้วยวิธีการทางอิเล็กทรอนิกส์และคอมพิวเตอร์ซอฟท์แวร์กับโปรแกรมคอมพิวเตอร์ ที่อยู่ในรูปแบบซึ่งทั้งมนุษย์และเครื่องจักรกลต่างก็สามารถที่จะอ่านเข้าใจได้ รวมทั้งวัตถุมีรูปร่างหรือไม่มีรูปร่างซึ่งอาจมีราคาได้อื่นๆ ด้วย

จากปัญหาดังกล่าวข้างต้นผู้เขียนเห็นว่าร่างพระราชบัญญัติอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... มาตรา 12 ซึ่งกำหนดเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์นั้นไม่ครอบคลุมถึงการหลอกลวงทางอินเตอร์เน็ตทุกประเภทด้วยเหตุผลที่กล่าวไปแล้วข้างต้น จึงควรจะต้องมีการปรับปรุงแก้ไขกฎหมายดังกล่าวเพื่อให้การปราบปรามอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ตมีประสิทธิภาพมากยิ่งขึ้น โดยนำกฎหมายของประเทศสหรัฐอเมริกามาเป็นแบบอย่างในการกำหนดกฎหมายของประเทศไทย ในฐานะที่เป็นประเทศที่ประสบปัญหาและได้รับความเสียหายจากอาชญากรรมโดยเฉพาะการหลอกลวงทางอินเตอร์เน็ตมากที่สุดในโลก นอกจากนี้ผู้เขียนยังมีความคิดเห็นเสนอแนะเพิ่มเติมว่าควรบัญญัติให้การกระทำความผิดดังกล่าวเป็นความผิดอันยอมความไม่ได้ เนื่องจากการประกอบอาชญากรรมทางระบบเครือข่ายอินเตอร์เน็ตเป็นการประกอบอาชญากรรมที่เกิดขึ้นอย่างรวดเร็วและในวงกว้าง หากการสืบสวนสอบสวนผู้กระทำความผิดจะกระทำได้ต่อเมื่อมีผู้มาแจ้งความร้องทุกข์ อันเป็นองค์ประกอบในการดำเนินการสืบสวนสอบสวนของคดีอาชญากรรมอันยอมความได้แล้วนั้น อาจจะไม่ทันต่อการปราบปรามอาชญากรรมดังกล่าว ดังนั้นจึงเห็นควรกำหนดให้อาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ตเป็นความผิดอันยอมความไม่ได้ ซึ่งการดำเนินการสืบสวนสอบสวนของพนักงานสามารถกระทำได้เพียงแค่มีผู้มากล่าวโทษเท่านั้น ซึ่งจะส่งผลให้การดำเนินการปราบปรามอาชญากรรมดังกล่าวเป็นไปอย่างมีประสิทธิภาพมากยิ่งขึ้น

5.1.1.4 มาตรการการลงโทษจำเลยในความผิดเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ต

ก. โทษจำคุก

โทษจำคุกเป็นโทษที่จำกัดเสรีภาพในร่างกายของผู้ต้องโทษโดยควบคุมไว้ในเรือนจำ ซึ่งก่อให้เกิดผลที่สอดคล้องกับทฤษฎีการลงโทษโดยทดแทน และทฤษฎีอรรถประโยชน์ (Utilitarian Theories) กล่าวคือ โทษจำคุกถูกนำมาใช้เพื่อตอบแทนผู้กระทำผิดตามความร้ายแรงแห่งความผิด ซึ่งพิจารณาจากความน่าตำหนิทางศีลธรรมของผู้กระทำจึงสอดคล้องกับทฤษฎีทดแทน นอกจากนี้การลงโทษจำคุกยังมีผลทำให้ผู้กระทำความผิดหลาบจำ และเกรงกลัวไม่กล้ากระทำผิดอีก อันเป็นการป้องกันโดยเฉพาะ และมีผลเป็นการข่มขู่มิให้ผู้อื่นกระทำผิดอีกด้วย สิ่งที่เป็นเป้าหมายของการลงโทษจำคุกบุคคลที่อยู่ในเรือนจำโดยมุ่งหวังว่าเมื่อผู้ต้องหาออกไปจากเรือนจำจะสามารถประพฤติตนเป็นคนดี มีศีลธรรมและสามารถประกอบอาชีพในสังคมได้ และเป็นการตัดมิให้นักโทษกระทำผิดอาญาได้ชั่วขณะหนึ่ง ซึ่งผู้เขียนเห็นว่าเหตุที่โทษจำคุกเป็นวิธีที่สามารถบรรลุวัตถุประสงค์ของการลงโทษได้กว้างขวาง จึงควรกำหนดโทษจำคุกเป็นโทษหลักสำหรับลงโทษผู้กระทำความผิด โดยกำหนดให้มีโทษจำคุกสูงกว่าที่กำหนดไว้ในประมวลกฎหมายอาญา ฐานความผิดฉ้อโกงประชาชน กำหนดโทษจำคุกไว้สูงสุดเจ็ดปี เนื่องจากการหลอกลวงทางอินเตอร์สามารถกระทำได้โดยง่าย และเข้าถึงกลุ่มบุคคลได้มากกว่าการหลอกลวงด้วยสื่ออื่น ๆ ดังที่กฎหมายของประเทศของประเทศสหรัฐอเมริกากำหนดโทษจำคุกไว้สูงสุดสิบห้าปี

ข. โทษปรับ

เนื่องจากการประกอบอาชญากรรมคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ตเป็นอาชญากรรมที่มุ่งประสงค์ต่อทรัพย์สินของบุคคลอื่น ดังนั้นโทษทางอาญาที่เหมาะสมจะลงโทษกับผู้กระทำความผิดน่าจะเป็นโทษปรับ ซึ่งการจะลงโทษตามกฎหมายอาญาได้นั้นจะต้องเป็นไปตามที่กฎหมายอาญาได้กำหนดไว้ และศาลต้องพิพากษาว่าการกระทำของจำเลยเป็นความผิดด้วยตามหลักไม่มีโทษโดยไม่มีกฎหมาย ดังนั้น ผู้เขียนจึงมีความเห็นว่าควรจะกำหนดโทษปรับให้สูง โดยพิจารณาถึงสัดส่วนระหว่างความเสียหายกับโทษที่จำเลยจะได้รับ เพื่อให้สอดคล้องกับทฤษฎีการลงโทษแบบทดแทน ที่มุ่งจะลงโทษเพื่อข่มขู่หรือยับยั้งให้ผู้กระทำความผิดไม่กล้ากระทำความผิด เนื่องจากหากถูกจับได้ก็จะถูกปรับเป็นจำนวนเงินที่สูง ทำให้ผู้กระทำความผิดเกรงกลัวต่อการกระทำความผิดอันจะทำให้สมประสงค์ของทฤษฎีการลงโทษ

ต้นฉบับ หน้าขาดหาย

3. ประมวลกฎหมายอาญา มาตรา 33 ทรัพย์สินที่บุคคลได้ใช้หรือมีไว้เพื่อใช้ในการกระทำความผิด หรือได้มาจากการกระทำความผิด ซึ่งการริบทรัพย์สินประเภทนี้ศาลสามารถใช้ดุลพินิจว่าจะริบหรือไม่ก็ได้ แต่ถ้าทรัพย์สินนั้นเป็นของบุคคลอื่นซึ่งมิได้รู้เห็นเป็นใจในการกระทำความผิด ศาลจะสั่งริบทรัพย์นั้นไม่ได้

ตามหลักกฎหมายของประเทศสหรัฐอเมริกา การริบทรัพย์แบ่งออกเป็น 2 ประเภท คือ การริบทรัพย์ทางแพ่งและการริบทรัพย์ทางอาญา

1. การริบทรัพย์ทางแพ่งเป็นการดำเนินคดีที่เรียกว่า อินเร็ม (Inrem) เป็นกระบวนการพิจารณาคดีกับทรัพย์สินมากกว่าตัวบุคคล โดยมีพื้นฐานหลักกฎหมายว่าทรัพย์สินมีความผิดในฐานะที่ถูกใช้หรือได้มาจากการกระทำความผิด กล่าวอีกนัยหนึ่ง คือ จำเลยในกระบวนการพิจารณาแบบอินเร็มคือตัวทรัพย์นั่นเอง ซึ่งจะเป็นการพิจารณาแยกต่างหากเด็ดขาดจากการดำเนินคดีอาญากับผู้เป็นเจ้าของตัวทรัพย์นั้น

การริบทรัพย์ทางแพ่งมีรากฐานมาจากแนวความคิดกฎหมายคอมมอนลอว์ (Common Law) ที่ว่าตัวทรัพย์สินที่เกี่ยวกับการกระทำความผิดนั่นเองเป็นทรัพย์สินที่ผิดและต้องปรับให้แก่พระเจ้า ทรัพย์สินที่จะริบได้นั้นต้องเป็นทรัพย์สินผิดกฎหมายโดยไม่คำนึงว่าทรัพย์สินนั้นเป็นของผู้กระทำความผิดหรือของผู้อื่นที่เกี่ยวข้อง เนื่องจากทรัพย์สินนั้นเองเป็นสิ่งที่ผิดกฎหมาย การริบทรัพย์สินจึงมีผลให้ทรัพย์สินนั้นตกเป็นของแผ่นดินตั้งแต่กระทำความผิด การโอนต่อๆ มาจึงไม่มีผล ผู้รับโอนจะอ้างว่าตนได้รับมาโดยสุจริตไม่ได้ [83] นอกจากนี้เรื่องการรับฟังพยานหลักฐานถือหลักการชั่งน้ำหนักพยานหลักฐาน (Preponderance of the Evidence) ตามวิธีพิจารณาความแพ่งทั่วไป โดยไม่ต้องพิสูจน์พยานหลักฐานจนปราศจากข้อสงสัย (Beyond Resonable Doubt) เหมือนในคดีอาญา

---

[83] จักรรัตน์ ศรีโกมุท, "อาชญากรรมเศรษฐกิจ : ศึกษากรณีอุปสรรคในการบังคับใช้กฎหมาย," (วิทยานิพนธ์ปริญญามหาวิทยาลัย ภาควิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 25), หน้า 103.

2. การริบทรัพย์ทางอาญาจะเกิดขึ้นได้เมื่อมีคำพิพากษาลงโทษว่าจำเลยกระทำความผิด เป็นการดำเนินคดีแบบ "อิน เพอร์โซนัม" เป็นการดำเนินคดีเพื่อลงโทษตัวบุคคล ไม่ใช่ตัวทรัพย์ ซึ่งถือว่าเป็นโทษอย่างหนึ่งทางอาญา การที่รัฐจะริบทรัพย์สินได้จะต้องปรากฏว่ามีกฎหมายบัญญัติไว้เท่านั้น และหลักการรับฟังพยานหลักฐานจะต้องพิสูจน์พยานหลักฐานจนปราศจากข้อสงสัย

จะเห็นได้ว่าประเทศสหรัฐอเมริกาได้ใช้หลักการริบทรัพย์ทั้งทางแพ่งและทางอาญาผสมผสานกันในการแก้ไขปัญหาการป้องกันและปราบปรามทางอาชญากรรมคอมพิวเตอร์ ผู้เขียนจึงมีความคิดเห็นว่าการกระทำความผิดของอาชญากรในปัจจุบันส่วนใหญ่มุ่งให้ได้ผลตอบแทนในลักษณะที่เป็นเงิน หรือทรัพย์สิน โดยเฉพาะอาชญากรรมทางคอมพิวเตอร์ที่เกี่ยวกับการหลอกลวงทางอินเตอร์เน็ต ซึ่งสามารถอำนวยประโยชน์ให้ผู้กระทำความผิดได้รับผลตอบแทนเป็นมูลค่ามหาศาล อีกทั้งกระบวนการยุติธรรมในปัจจุบันไม่อาจประสบความสำเร็จในการบังคับใช้กฎหมายต่ออาชญากรรมในลักษณะเช่นว่านี้ ซึ่งผลประโยชน์ที่ได้จากการประกอบอาชญากรรมดังกล่าวจะถูกนำไปใช้ในการทำธุรกิจอาชญากรรม หรือถูกนำไปเป็นทุนในการประกอบธุรกิจต่างๆ หรืออาจจะถูกนำกลับมาใช้เป็นเงินทุนหมุนเวียนกลับมาใช้ในวงจรของการกระทำความผิดอีก ซึ่งก่อให้เกิดความเสียหายทางเศรษฐกิจและสังคมของประเทศเป็นอย่างมาก ดังนั้นเพื่อให้มาตรการกำหนดโทษแก่ผู้กระทำความผิดเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตในประเทศไทยเป็นไปอย่างมีประสิทธิภาพ ควรขยายขอบเขตของกฎหมายในเรื่องการริบทรัพย์ให้ใช้หลักการริบทรัพย์ทั้งทางแพ่งและทางอาญาด้วย จะทำให้ผู้ที่กระทำความผิดหรือจะกระทำความผิดเกรงกลัวที่จะกระทำความผิด เนื่องจากหากถูกจับกุมแล้วก็อาจจะต้องถูกริบทรัพย์สินทั้งหมดที่เกี่ยวเนื่องกับการกระทำความผิด อันเป็นการตัดแรงจูงใจในการกระทำความผิดลงได้ เป็นการตัดโอกาสไม่ให้ผู้กระทำความผิดได้รับประโยชน์ในทรัพย์สินที่ได้มาจากการกระทำความผิดและเป็นการป้องกันสังคมมิให้ผู้กระทำความผิดนำทรัพย์สินดังกล่าวไปใช้ในการกระทำความผิดอีก

นอกจากนั้นผู้เขียนเห็นว่ามาตรการในการป้องกันและปราบปรามการฟอกเงินเป็นอีกมาตรการหนึ่งทางกฎหมายที่สำคัญ โดยจะดำเนินคดีกับบุคคลที่โอน รับโอน หรือเปลี่ยนสภาพทรัพย์สินที่เกี่ยวกับการกระทำความผิด หรือกระทำด้วยประการใดๆ เพื่อปกปิด หรืออำพรางลักษณะที่แท้จริง การได้มา แหล่งที่ตั้ง การจำหน่าย การโอน การได้สิทธิใดๆ ซึ่งทรัพย์สินที่เกี่ยวกับการกระทำความผิดที่ถือว่าเป็นการฟอกเงิน และยังมีการนำมาตรการเกี่ยวกับการยึดทรัพย์สินทางแพ่งมาใช้ โดยกฎหมายได้ขยายหลักเกณฑ์การยึดทรัพย์สินให้มี

ขอบเขตกว้างขวางขึ้นกว่าการริบทรัพย์สินตามกฎหมายที่มีอยู่เดิม โดยให้สามารถยึดทรัพย์สินที่เกี่ยวกับการกระทำความผิดได้ทั้งหมด โดยไม่คำนึงว่าทรัพย์สินดังกล่าวจะมีการโอน แปรเปลี่ยน สภาพไปแล้วหลายครั้ง หรือตกไปเป็นกรรมสิทธิ์ของบุคคลอื่นแล้วก็ตาม ซึ่งเป็นมาตรการการยึดทรัพย์สินทางแพ่ง แต่เนื่องจากพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ไม่ได้กำหนดการประกอบอาชญากรรทางคอมพิวเตอร์เป็นหนึ่งในความผิดมูลฐาน ทำให้ไม่สามารถนำมาตรการยึดทรัพย์สินทางแพ่งตามพระราชบัญญัติดังกล่าวมาใช้บังคับกับอาชญากรรทางคอมพิวเตอร์ได้ ซึ่งมีประสิทธิภาพมากกว่ามาตรการริบทรัพย์ตามประมวลกฎหมายอาญา เนื่องจากการริบทรัพย์สินตามพระราชบัญญัตินี้ต้องการภาระพิสูจน์เพียงแค่ชั่งน้ำหนักพยานหลักฐาน ไม่ต้องถึงกับสิ้นสงสัยหรือให้ภาระการพิสูจน์ความบริสุทธิ์ของทรัพย์สินที่ต้องสงสัยตกอยู่แก่ผู้ต้องหาหรือจำเลยในชั้นตรวจสอบทรัพย์สินและชั้นศาล โดยพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ได้กำหนดแนวทางซึ่งเป็นข้อสันนิษฐานว่าหากผู้อ้างว่าเป็นเจ้าของหรือผู้รับโอนทรัพย์สินเป็นผู้ซึ่งเกี่ยวข้องหรือเคยเกี่ยวข้องสัมพันธ์กับผู้กระทำความผิดมูลฐานหรือความผิดฐานฟอกเงินมาก่อน ให้สันนิษฐานว่าบรรดาทรัพย์สินดังกล่าวเป็นทรัพย์สินที่เกี่ยวกับการกระทำผิดหรือได้รับมาโดยไม่สุจริต ซึ่งพนักงานอัยการเพียงนำสืบให้เข้าข้อสันนิษฐานว่าทรัพย์สินนั้นเป็นทรัพย์สินที่เกี่ยวกับการกระทำความผิด จากนั้นผู้อ้างว่าเป็นเจ้าของทรัพย์สินหรือผู้รับโอนหรือผู้รับประโยชน์จะต้องพิสูจน์หรือแสดงข้อเท็จจริงหักล้างข้อสันนิษฐานดังกล่าว ซึ่งถ้าศาลเชื่อหรือฟังขึ้นก็จะเป็นผลให้ศาลสั่งคืนทรัพย์สินนั้น แต่ถ้าศาลไม่เชื่อข้อเท็จจริงที่แสดงต่อศาล ศาลก็จะสั่งให้ทรัพย์สินตกเป็นของแผ่นดิน ซึ่งต่างกับการริบทรัพย์สินทางอาญา เพราะต้องมีการพิสูจน์ความผิดก่อนจึงบังคับโทษได้ ในคดีอาชญากรรมทางคอมพิวเตอร์หรือทางเครือข่ายอินเตอร์เน็ตเป็นการยากยิ่งที่จะพิสูจน์ความผิดอย่างแจ้งชัด ดังนั้นผู้เขียนจึงเห็นว่าการนำมาตรการการยึดทรัพย์สินทางแพ่งตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 51 มาใช้บังคับกับอาชญากรรมทางคอมพิวเตอร์หรือเครือข่ายอินเตอร์เน็ตจะทำให้การปราบปรามอาชญากรรมดังกล่าวมีประสิทธิภาพเพิ่มมากขึ้น

5.1.1.5 **มาตรการการใช้วิธีการเพื่อความปลอดภัย**

แนวความคิดพื้นฐานอันเป็นที่มาของวิธีการเพื่อความปลอดภัยนั้นเป็นความคิดในเรื่องการป้องกันการกระทำความผิดในสังคม เพราะสภาพบังคับทางอาญาว่าด้วยเรื่องโทษมุ่งหมายเพื่อปราบปรามการกระทำความผิด โดยมุ่งกระทำต่อบุคคลที่ฝ่าฝืนกฎหมายอาญา ซึ่งมาตรการดังกล่าวไม่เพียงพอต่อการป้องกันมิให้เกิดอาชญากรรมขึ้นในสังคม เพราะใน

บางกรณีการกระทำของบุคคลบางประเภทหรือพฤติการณ์บางลักษณะยังไม่อาจถือว่าเป็นความผิดตามกฎหมาย แต่ลักษณะของบุคคลเหล่านั้นหรือพฤติการณ์นั้นถึงขั้นที่อาจจะก่อให้เกิดอันตรายแก่สังคมแล้ว และถ้าปล่อยให้บุคคลนั้นอยู่ในสังคมหรือพฤติการณ์ดังกล่าวดำเนินต่อไปได้ก็จะนำมาซึ่งการกระทำความผิด ด้วยเหตุนี้รัฐจึงควรจะมีมาตรการควบคุมบุคคลบางประเภทหรือการกระทำที่น่าจะเป็นอันตรายแก่สังคมนั้นเพื่อป้องกันการกระทำความผิด มาตรการนี้เรียกว่าวิธีการเพื่อความปลอดภัย

วิธีการเพื่อความปลอดภัย หมายถึง มาตรการทางกฎหมายอาญาที่รัฐใช้กับบุคคลซึ่งมีสภาพหรือพฤติการณ์ที่เป็นอันตรายต่อสังคม เพื่อควบคุมมิให้ผู้นั้นกระทำผิดกฎหมายอาญา ทั้งนี้โดยมุ่งประสงค์เพื่อให้สังคมปลอดภัยจากการกระทำความผิด มาตรการดังกล่าวจึงอาจนำมาใช้แก่บุคคลหนึ่งบุคคลใด แม้ว่าบุคคลนั้นจะยังไม่ได้กระทำผิดหรือได้กระทำผิดแล้วแต่มีแนวโน้มที่จะกระทำผิดขึ้นในอนาคต [84]

เนื่องจากวิธีการเพื่อความปลอดภัยมีลักษณะเป็นการจำกัดตัดทอนสิทธิและเสรีภาพของบุคคล ดังนั้นหลักเกณฑ์การใช้บังคับวิธีการเพื่อความปลอดภัยมีอยู่ 2 ประการ คือ ต้องมีกฎหมายให้อำนาจ ศาลจึงจะใช้ได้ และกฎหมายที่ศาลจะนำมาใช้บังคับเกี่ยวกับวิธีการเพื่อความปลอดภัยนี้ได้แก่กฎหมายที่ใช้กันอยู่ในขณะที่ศาลพิพากษา ซึ่งวิธีการเพื่อความปลอดภัย ประมวลกฎหมายอาญา มาตรา 39 กำหนดวิธีการเพื่อความปลอดภัย ไว้ 5 ประเภท คือ กักกัน ห้ามเข้าเขตกำหนด เรียกประกันทัณฑ์บน คุมตัวไว้ในสถานพยาบาล ห้ามการประกอบอาชีพบางอย่าง

วิธีการเพื่อความปลอดภัยต่างกับโทษทางอาญา คือ โทษนั้นจะต้องเป็นไปตามกฎหมายที่ใช้อยู่ในขณะกระทำความผิด* เว้นแต่จะมีกฎหมายภายหลังกำหนดโทษเบากว่า ถ้าไม่มีกฎหมายในขณะกระทำความผิดกำหนดว่าการกระทำความผิดและกำหนดโทษไว้แล้ว ศาลจะลงโทษผู้กระทำไม่ได้เลย แต่วิธีการเพื่อความปลอดภัยนั้นแม้ขณะกระทำความผิดไม่มี

---

[84] ณรงค์ ใจหาญ, คำอธิบายกฎหมายอาญา ภาคหนึ่งว่าด้วยโทษและวิธีการเพื่อความปลอดภัย,หน้า 94.

* ประมวลกฎหมายอาญา มาตรา 2 บัญญัติว่า บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการอันกฎหมายที่ใช้ใน**ขณะกระทำ**นั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่ผู้กระทำความผิดนั้น ต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย

กฎหมายกำหนดวิธีการเพื่อความปลอดภัยไว้ แต่ถ้าในขณะพิพากษามีกฎหมายกำหนดให้ใช้บังคับวิธีการเพื่อความปลอดภัย ศาลก็จะใช้วิธีการเพื่อความปลอดภัยนั้นได้ * ทั้งนี้เพื่อจะให้สังคมปลอดภัยจากผู้กระทำความผิดในเวลาเร็วที่สุด นอกจากนี้ยังต่างกันที่วัตถุประสงค์ กล่าวคือโทษนั้นมีไว้เพื่อตอบแทนการกระทำความผิด แต่วิธีการเพื่อความปลอดภัยนั้นมุ่งหมายที่จะให้สังคมปลอดภัยจากผู้กระทำ ดังนั้นมาตรการที่นำมาใช้จึงไม่คำนึงว่าผู้นั้นจะมีความรับผิดทางอาญาดังเช่นการลงโทษ แต่พิจารณาเพียงว่าผู้นั้นมีพฤติการณ์ที่น่าจะเป็นอันตรายแก่สังคมก็ใช้วิธีการเพื่อความปลอดภัยได้ ทั้งนี้เพราะวิธีการเพื่อความปลอดภัยไม่ใช่โทษ เป็นแต่วิธีการป้องกันสังคมให้ปลอดภัยจากการที่บุคคลนั้นอาจกระทำความผิดในภายหน้า จึงควรให้สังคมได้รับความปลอดภัยจากผู้กระทำความผิดให้เร็วที่สุดเท่าที่จะเร็วได้

สำหรับการห้ามประกอบอาชีพบางอย่าง ตามประมวลกฎหมายอาญา มาตรา 50 บัญญัติว่าเมื่อศาลพิพากษาให้ลงโทษผู้ใด ถ้าศาลเห็นว่าผู้นั้นกระทำความผิดโดยอาศัยโอกาสจากการประกอบอาชีพหรือวิชาชีพ หรือเนื่องจากการประกอบอาชีพหรือวิชาชีพ และเห็นว่าหากผู้นั้นประกอบอาชีพหรือวิชาชีพนั้นต่อไปอาจจะกระทำความผิดเช่นนั้นขึ้นอีก ศาลจะสั่งไว้ในคำพิพากษาห้ามการประกอบอาชีพหรือวิชาชีพนั้นมีกำหนดเวลาไม่เกินห้าปีนับแต่วันพ้นโทษไปแล้วก็ได้ ซึ่งหากจะแยกองค์ประกอบที่ศาลจะสั่งห้ามประกอบอาชีพอันเป็นวิธีการเพื่อความปลอดภัยวิธีการหนึ่งมีดังนี้

1. ผู้ใดกระทำความผิดใด ๆ โดยอาศัยโอกาสหรือเนื่องจากการประกอบอาชีพหรือวิชาชีพของตน

คำว่า "อาชีพ" หมายถึง กิจการที่เป็นเครื่องยังชีพหรือเลี้ยงชีพเป็นปกติธุระและต้องอาศัยฝีมือและความชำนาญ ส่วนวิชาชีพเป็นกิจการที่เป็นเครื่องมือในการเลี้ยงชีพเป็นปกติ โดยอาศัยศิลปศาสตร์หรือความรู้และปัญญา เช่น นักกฎหมาย แพทย์ เป็นต้น [87]

---

* ประมวลกฎหมายอาญา มาตรา 12 บัญญัติว่า วิธีการเพื่อความปลอดภัยจะใช้บังคับแก่บุคคลใดได้ ก็ต่อเมื่อมีบทบัญญัติแห่งกฎหมายให้ใช้บังคับได้เท่านั้น และกฎหมายที่จะใช้บังคับนั้นให้ใช้กฎหมายใน**ขณะที่ศาลพิพากษา**

[87] วินัย ทองลงยา, กฎหมายอาญา เล่ม 1 (กรุงเทพมหานคร : โรงพิมพ์สำนักนายกรัฐมนตรี, 2514), หน้า 200.

2. ศาลได้พิพากษาให้ลงโทษผู้นั้นตามความผิดที่พิจารณาได้ ความผิดที่จะลงโทษนั้นอาจเป็นความผิดที่กระทำโดยเจตนา ประมาทหรือความผิดลหุโทษก็ได้ และโทษนั้นก็ไม่จำกัดว่าต้องเป็นโทษจำคุก อาจเป็นโทษปรับหรือกักขังก็ได้ ซึ่งการที่ศาลพิพากษาลงโทษนั้น ศาลต้องลงโทษจริงๆ มิใช่พิพากษาว่ามีความผิดแล้วรอการลงโทษหรือรอการกำหนดโทษ [88]

3. ศาลเห็นว่าถ้าให้ผู้นั้นประกอบอาชีพหรือวิชาชีพนั้นต่อไปอาจจะกระทำความผิดขึ้นอีก ซึ่งศาลอาจจะสั่งได้ 2 กรณี คือ สั่งห้ามประกอบอาชีพหรือวิชาชีพนั้น หรือสั่งห้ามประกอบอาชีพหรือวิชาชีพโดยมีกำหนดเวลาไม่เกิน 5 ปี นับแต่วันพ้นโทษ

ประโยชน์ที่จะได้รับจากการใช้วิธีการเพื่อความปลอดภัยประเภทห้ามประกอบอาชีพบางอย่างแก่ผู้กระทำความผิดภายหลังจากที่ได้รับโทษตามคำพิพากษาแล้ว คือ

ก. ตัดความสัมพันธ์หรืออิทธิพลทางธุรกิจ ซึ่งทำให้หวนกลับไปกระทำความผิดได้ยากขึ้น

ข. เป็นการข่มขู่ผู้ที่คิดจะกระทำความผิดประเภทนี้ ในแง่ที่ว่าอาจจะไม่สามารถประกอบอาชีพลักษณะนี้ได้ต่อไป

ค. คุ้มครองสังคมให้ได้รับความปลอดภัยอันเป็นวัตถุประสงค์ของการใช้วิธีการเพื่อความปลอดภัย

จะเห็นได้ว่าการปราบปรามความผิดเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตยังไม่มีประสิทธิภาพเพียงพอที่จะดำเนินการกับผู้กระทำความผิดได้อย่างแท้จริง เพื่อเป็นการตัดโอกาสมิให้มีการกระทำความผิดเช่นนี้ขึ้นมาอีก ผู้เขียนจึงเห็นควรใช้วิธีการเพื่อความปลอดภัยโดยห้ามการประกอบอาชีพดังที่ประมวลกฎหมายอาญากำหนดไว้ อย่างไรก็ตามวิธีการเพื่อความปลอดภัยตามประมวลกฎหมายอาญานั้นยังมีข้อจำกัดอยู่ คือจะนำมาใช้ได้ต่อเมื่อศาลมีคำพิพากษาให้ลงโทษแก่ผู้ใดแล้วเท่านั้น โดยที่หากไม่มีการลงโทษหรือมีการรอการลงโทษ หรือรอการกำหนดโทษ ศาลจะใช้วิธีการนี้ไม่ได้ ซึ่งจะขัดกับแนวความคิดของวิธีการ

---

[88] โกเมน ภัทรภิรมย์. คำอธิบายประมวลกฎหมายอาญาลักษณะวิธีการเพื่อความปลอดภัย, หน้า 79.

เพื่อความปลอดภัยที่มุ่งจะคุ้มครองลักษณะการกระทำที่อาจก่อให้เกิดภยันอันตรายต่อประชาชน ก่อนที่กระบวนการกฎหมายจะตัดสินว่าการกระทำเป็นความผิดด้วย เพราะฉะนั้นเป็นการที่กฎหมายไม่สามารถแก้ปัญหาได้ทันกับความเสียหายที่เกิดขึ้น จึงเป็นความจำเป็นที่จะต้องคำนึงถึงมาตรการคุ้มครองสังคมในเรื่องการกระทำที่เป็นอันตรายได้ก่อนที่ศาลจะพิพากษา ทั้งนี้เพื่อให้บทบัญญัติมาตรานี้สามารถนำไปใช้กับอาชญากรรมคอมพิวเตอร์ที่กระทำความผิด แต่กฎหมายไม่สามารถนำมาลงโทษได้ เพราะปัจจัยต่าง ๆ เช่น ความไม่รัดกุมของบทบัญญัติกฎหมาย

มาตรการดังกล่าวจะส่งผลให้เป็นการบรรลุผลในการปราบปรามอาชญากรรมทางคอมพิวเตอร์ได้อย่างแท้จริง เพราะเป็นการตัดการกระทำที่เป็นภยันอันตรายแก่สังคมให้พ้นจากสังคม และเป็นการตัดโอกาสผู้กระทำความผิดไม่ให้กระทำผิดได้อีก หากวิธีการเพื่อความปลอดภัยดังกล่าวสามารถนำมาใช้เป็นมาตรการควบคู่กับการลงโทษปรับ จะมีประสิทธิภาพยิ่งขึ้นในการยับยั้งความเสียหายและมิให้มีการกระทำผิดอีกทั้งในขั้นตอนก่อนมีการดำเนินคดีและหลังการพิจารณาแล้วก็ตาม ดังนั้นผู้เขียนเห็นว่าควรมีการปรับปรุงแก้ไขกฎหมายเกี่ยวกับวิธีการเพื่อความปลอดภัย โดยการให้ใช้วิธีการเพื่อความปลอดภัยครอบคลุมถึงกรณีที่การกระทำนั้นอยู่ระหว่างถูกฟ้อง หรือดำเนินคดีอยู่ก่อนที่ศาลจะพิพากษาด้วย เพื่อที่จะช่วยให้การบังคับใช้วิธีการเพื่อความปลอดภัยมีประสิทธิภาพมากยิ่งขึ้น ซึ่งจะส่งผลโดยตรงต่อการคุ้มครองสังคมคือเป็นการตัดสัมพันธ์ ทำให้ผู้กระทำความผิดหวนกลับไปกระทำความผิดใหม่ได้ยาก เป็นการข่มขู่อาชญากรรมทางคอมพิวเตอร์ในแง่ที่ว่าอาจจะไม่สามารถประกอบอาชีพหรือวิชาชีพได้ตลอดไป และยังเป็นการคุ้มครองสังคมให้ได้รับความปลอดภัยตามความมุ่งหมายของวิธีการเพื่อความปลอดภัย แม้จะไม่สามารถลงโทษได้ก็ตาม

5.1.2 มาตรการทางด้านกฎหมายวิธีสบัญญัติ

เนื่องจากร่างพระราชบัญญัติอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... ของประเทศไทยนั้น ได้บัญญัติแต่เฉพาะในส่วนการกระทำความผิดหรือกฎหมายสารบัญญัติเท่านั้น หาได้กำหนดถึงขั้นตอนการนำตัวผู้กระทำความผิดมาลงโทษตามกฎหมายไม่ ซึ่งผู้เขียนเห็นว่าเพื่อให้ร่างพระราชบัญญัติดังกล่าวมีความครบถ้วนทั้งกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติที่เกี่ยวข้องกับการปราบปรามอาชญากรรมทางคอมพิวเตอร์นั้น จึงเห็นควรกำหนดกฎหมายวิธีสบัญญัติไว้ในร่างพระราชบัญญัติดังกล่าวด้วย เช่นเดียวกับที่พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 ซึ่งเป็นกฎหมายที่บัญญัติทั้งในส่วนของกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติไว้ในกฎหมายฉบับเดียวกัน ทั้งนี้ ผู้เขียนยังเห็นว่า

การเพิ่มเติมกฎหมายวิธีสบัญญัติในร่างพระราชบัญญัติดังกล่าว จะเป็นการง่ายและสะดวกกว่าการแก้ไขประมวลกฎหมายวิธีพิจารณาความอาญาอีกด้วย โดยในส่วนของกฎหมายวิธีสบัญญัติที่ควรจะเพิ่มเติมในร่างพระราชบัญญัติดังกล่าว ผู้เขียนขอเสนอดังนี้

5.1.2.1 มาตรการผลักภาระการพิสูจน์ให้กับจำเลย

ประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศไทย มาตรา 227 บัญญัติว่า "ให้ศาลใช้ดุลพินิจวินิจฉัยชั่งน้ำหนักพยานหลักฐานทั้งปวง อย่าพิพากษาลงโทษจนกว่าจะแน่ใจว่ามีการกระทำความผิดจริงและจำเลยเป็นผู้กระทำความผิดนั้น เมื่อมีความสงสัยตามสมควรว่าจำเลยได้กระทำผิดหรือไม่ ให้ยกประโยชน์แห่งความสงสัยนั้นให้จำเลย" ประกอบกับประเทศไทยใช้ระบบการพิจารณาคดีแบบกล่าวหา ทำให้ผู้กล่าวหาจะต้องเป็นฝ่ายพิสูจน์ความผิดจนปราศจากข้อสงสัยว่าผู้ถูกกล่าวหากระทำความผิดจริงตามฟ้อง หากข้อเท็จจริงฟังไม่ได้ความว่าจำเลยกระทำความผิดหรือฟังไม่ชัดว่าจำเลยกระทำความผิด ศาลจะพิพากษาลงโทษจำเลยไม่ได้ ซึ่งหลักการที่เคร่งครัดในการพิสูจน์ความผิดของจำเลยดังกล่าวอาจเหมาะสมที่จะใช้บังคับกับคดีอาญาทั่วๆ ไป แต่สำหรับผู้กระทำความผิดอาชญากรรมทางคอมพิวเตอร์ซึ่งเป็นผู้มีความรู้ การศึกษา มีความเชี่ยวชาญชำนาญในการใช้เทคโนโลยี ทำให้ไม่ค่อยเหลือร่องรอยพยานหลักฐานของการกระทำความผิดไว้ให้พนักงานเจ้าหน้าที่นำไปพิสูจน์ความผิด หรือหากจะมีพยานหลักฐานต่างๆ ผู้กระทำความผิดก็จะเป็นผู้ครอบครองพยานหลักฐานดังกล่าวทั้งหมด ทำให้โจทก์ไม่สามารถนำพยานหลักฐานมายืนยันข้อเท็จจริงอันเป็นองค์ประกอบความผิดพิสูจน์ให้ศาลเห็นอย่างแน่ชัดว่าจำเลยกระทำความผิดจริง คงเป็นได้ยากลำบาก ดังนั้นหลักการรับฟังพยานหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์หรือทางเครือข่ายอินเตอร์เน็ตจึงควรจะต้องมีการกำหนดประเภทของข้อสันนิษฐานขึ้นในกฎหมาย โดยผลักภาระการพิสูจน์ให้จำเลย (Reverse Burden of Proof) แทนที่โจทก์จะต้องพิสูจน์ความจริงอย่างปราศจากข้อสงสัยก็นำสืบเพียงให้เห็นข้อเท็จจริงอันเป็นเงื่อนไขแห่งข้อสันนิษฐานตามกฎหมาย ต่อจากนั้นเป็นหน้าที่ของจำเลยต้องนำสืบหักล้างข้อสันนิษฐานนั้น โดยอาจนำสืบข้อเท็จจริงโต้แย้งข้อสันนิษฐานให้เห็นเป็นอย่างอื่น หากจำเลยไม่นำพยานหลักฐานมาสืบให้เห็นเป็นอย่างอื่นได้ศาลก็ต้องรับฟังข้อเท็จจริงตามข้อสันนิษฐานและตัดสินลงโทษจำเลยโดยผลของข้อสันนิษฐานตามกฎหมาย ทำให้สามารถนำตัวผู้กระทำความผิดมาลงโทษได้

5.1.2.2 มาตรการการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

เนื่องจากประมวลวิธีพิจารณาความอาญาของประเทศไทยยังไม่มีการกำหนดเกี่ยวกับการรับฟังและการนำสืบพยานหลักฐานอิเล็กทรอนิกส์ ทำให้เกิดปัญหาในกระบวนการพิจารณาคดีของศาลว่าจะสามารถรับฟังพยานหลักฐานอิเล็กทรอนิกส์ได้หรือไม่ ถ้ารับฟังได้จะรับฟังในฐานะพยานรูปแบบใด และจะมีวิธการนำสืบอย่างไร ซึ่งผู้เขียนเห็นว่าเพื่อมิให้เกิดปัญหาในทางปฏิบัติ ควรจะมีการกำหนดเกี่ยวกับการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ไว้โดยเฉพาะเช่นเดียวกับที่หลาย ๆ ประเทศได้มีการกำหนดไว้

ก. หลักเกณฑ์การรับฟังพยานหลักฐานของประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาถือหลักการรับฟังพยานหลักฐานตามหลักพยานหลักฐานที่ดีที่สุด (Best Evidence Rule) ได้ปรับปรุงแก้ไขกฎหมายลักษณะพยานเพื่อรับฟังข้อมูลที่บันทึกด้วยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์ไว้ในข้อ 1001 แห่ง Federal Rules of Evidence หรือ FRE ซึ่งบัญญัติว่า

(1) "ข้อเขียนหรือบันทึก" หมายถึง อักษร ข้อความ ตัวเลขหรือสิ่งเทียมเท่าอย่างอื่นซึ่งถูกทำขึ้นโดยการเขียน พิมพ์ดีด เครื่องพิมพ์ การถ่ายสำเนา การถ่ายรูป แรงกระตุ้นแม่เหล็ก ไฟฟ้า เครื่องจักรกลอิเล็กทรอนิกส์หรือการประมวลผลข้อมูล

(2) "ภาพถ่าย" รวมถึงภาพนิ่ง ฟิล์มเอกซเรย์ วิดิทัศน์และภาพยนตร์

(3) "ต้นฉบับของข้อเขียนหรือบันทึก" คือ ตัวข้อเขียนหรือบันทึกนั้นเองหรือคู่ฉบับใด ๆ ซึ่งผู้ทำหรือผู้ออกให้มีเจตนาจะให้มีผลเช่นเดียวกัน ต้นฉบับของรูปถ่ายรวมตลอดถึงฟิล์มหรือรูปที่อัดได้จากฟิล์มนั้น ถ้ามีข้อมูลถูกเก็บบันทึกไว้ในคอมพิวเตอร์หรือเครื่องอื่นซึ่งมีทำนองเดียวกัน เอกสารจากคอมพิวเตอร์หรือผลลัพธ์ที่สามารถอ่านได้ด้วยสายตาซึ่งแสดงไว้เพื่อให้ปรากฏรายละเอียดของข้อมูลที่ถูกต้องนับว่าเป็นต้นฉบับด้วย

(4) "ต้นฉบับ" หมายถึง คู่ฉบับที่ถูกผลิตขึ้นโดยให้มีผลเช่นเดียวกับต้นฉบับจากสิ่งพิมพ์ ภาพถ่าย (รวมตลอดถึงภาพอัด ภาพขยาย) หรือถูกผลิตขึ้นจากการประมวลผลซ้ำของเครื่องจักรกล หรือเครื่องบันทึกอิเล็กทรอนิกส์หรือกระบวนการผลิตทางเคมีหรือผลิตขึ้นโดยทางเทคนิคอย่างอื่น โดยให้มีผลที่ถูกต้องเช่นเดียวกับต้นฉบับ

จากบทบัญญัติ FRE ข้อ 1001(1) ยอมรับว่าข้อมูลจากเครื่องคอมพิวเตอร์ซึ่งถูกทำขึ้นจากเครื่องพิมพ์ แรงกระตุ้นแม่เหล็กไฟฟ้า เครื่องจักรกลอิเล็กทรอนิกส์หรือการประมวลผลข้อมูล เป็นข้อเขียน หรือบันทึก และบทบัญญัติ FRE ข้อ 1001(3) ถ้าข้อมูลที่ถูกเก็บบันทึกไว้ในเครื่องคอมพิวเตอร์ หรือเครื่องอื่นซึ่งมีทำนองเดียวกันแล้ว เอกสารจากคอมพิวเตอร์ (Printout) หรือผลลัพธ์ที่สามารถอ่านได้ด้วยสายตาอาจจะอยู่ในรูปแผ่นดิสก์ก็มีฐานะเป็นต้นฉบับ (Original) แต่ต้องเป็น Printout หรือแผ่นดิสก์ที่ได้จากเครื่องคอมพิวเตอร์โดยตรง ไม่ใช่สำเนาภาพถ่ายหรือแผ่นดิสก์ที่เกิดขึ้นจากการอัดสำเนา เท่ากับกฎหมายลักษณะพยานของสหรัฐอเมริกายอมรับการอ้างส่ง Printout เป็นพยานหลักฐานต่อศาลเพื่อพิสูจน์เนื้อหาของข้อมูลที่บันทึกไว้ [89] การบัญญัติยอมรับการอ้างส่ง Printout หรือแผ่นดิสก์ของกฎหมายลักษณะพยานดังกล่าวนั้นก็เพื่อให้สอดคล้องกับหลักพยานหลักฐานที่ดีที่สุด ซึ่งเป็นหลักกฎหมายคอมมอนลอว์ (Common Law) ที่เก่าแก่ที่ได้กำหนดหลักว่าบุคคลใดที่ประสงค์แสดงความเป็นจริงหรือความถูกต้องของข้อเขียนต้องนำต้นฉบับของข้อเขียนนั้นมาแสดงต่อศาล เพื่อให้ได้ข้อมูลที่ไว้ใจที่สุด นอกจากนั้นหลัก Best Evidence Rule บังคับให้ส่งต้นฉบับแล้ว ปัญหาที่ตามมาคือข้อมูลที่ได้จากสื่ออิเล็กทรอนิกส์หรือคอมพิวเตอร์ อะไรคือต้นฉบับ อะไรคือสำเนา เพราะการทำซ้ำสามารถกระทำได้ตลอดเวลาและไม่สามารถระบุได้ว่าอะไรคือต้นฉบับ ด้วยเหตุนี้ FRE ข้อ 1001 บัญญัติว่า printout หรือสิ่งอื่นที่อ่านได้ซึ่งสะท้อนให้เห็นถึงข้อมูลที่บันทึกไว้เป็นต้นฉบับเพื่อแก้ไขปัญหาที่เกิดขึ้น

---

[89] พรเพชร วิชิตชลชัย, คำอธิบายกฎหมายลักษณะพยาน (กรุงเทพมหานคร:บริษัทเกรนโกรว จำกัด, 2542), หน้า 91.

ข. หลักเกณฑ์การรับฟังพยานหลักฐานของประเทศอังกฤษ

เนื่องจากเป็นระบบกฎหมาย Common Law เช่นกัน จึงมีหลัก Best Evidence Rule เช่นเดียวกันกับประเทศสหรัฐอเมริกา โดยมีกฎหมายที่เกี่ยวข้องคือ Civil Evidence Act 1968 และ The Police and Criminal Evidence Act 1984 กำหนดว่าข้อมูลจากเครื่องคอมพิวเตอร์สามารถรับฟังเป็นพยานหลักฐานได้ แต่ต้องมีคุณสมบัติตามที่มาตรา 68 และมาตรา 69 บัญญัติไว้ คือ

บทบัญญัติมาตรา 69 ได้บัญญัติว่า ในกระบวนการพิจารณาคดีใด ๆ ข้อความในเอกสารที่ทำขึ้นโดยคอมพิวเตอร์จะไม่เป็นที่รับฟังในฐานะพยานหลักฐานตามข้อเท็จจริงที่ระบุไว้นั้น เว้นเสียแต่จะแสดงให้เห็นว่า

(1) ไม่มีเหตุผลอื่นอันควรเชื่อได้ว่าข้อความไม่ถูกต้อง อันเนื่องจากการใช้เครื่องคอมพิวเตอร์ไม่ถูกวิธี และ

(2) ตลอดระยะเวลาที่สำคัญนั้น เครื่องคอมพิวเตอร์ได้ปฏิบัติการอย่างถูกต้องและแม้หากมีกรณีการทำงานของเครื่องคอมพิวเตอร์ขัดข้อง ก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

และบทบัญญัติในมาตรา 68 ได้บัญญัติถึงมาตรา 69 คือในการพิจารณาคดีใด ๆ ถ้าต้องการให้ข้อความในเอกสารเป็นพยานหลักฐานในคดีตามมาตรา 69 จะต้องมีใบรับรองแสดงรายละเอียดพิสูจน์เอกสารที่บรรจุข้อความและอธิบายวิธีการที่ได้มา รายละเอียดโดยอธิบายให้เห็นว่าข้อมูลถูกทำขึ้นโดยเครื่องคอมพิวเตอร์ และได้ลงนามโดยบุคคลที่ดำรงตำแหน่งหน้าที่รับผิดชอบเกี่ยวข้องกับการใช้คอมพิวเตอร์

จากบทบัญญัติมาตรา 68 และมาตรา 69 แสดงให้เห็นว่ากฎหมายอังกฤษยอมรับว่าเอกสารหรือข้อมูลที่ได้จากเครื่องคอมพิวเตอร์ สามารถรับฟังเป็นพยานหลักฐานได้โดยไม่นำหลัก Best Evidence Rule มาใช้ แต่จะต้องมีการรับรองความถูกต้องแท้จริงของเอกสารหรือข้อมูลจากเครื่องคอมพิวเตอร์ โดยเพียงคำรับรองของผู้ที่เกี่ยวข้องนั้นจะต้องให้คำรับรองยืนยันความถูกต้องของระบบการทำงานของเครื่องคอมพิวเตอร์ไว้ด้วย [90]

---

[90] สุรพันธ์ มั่นคงดี, พยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์, หน้า 102-103.

จะเห็นได้ว่าการที่จะนำตัวผู้กระทำความผิดมาลงโทษในคดีเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตนั้น คงไม่สามารถหลีกเลี่ยงการนำข้อมูลจากสื่ออิเล็กทรอนิกส์มาใช้เป็นพยานหลักฐานในศาลได้ ซึ่งกฎหมายวิธีพิจารณาความอาญาของประเทศไทยมิได้มีการกำหนดเกี่ยวกับการรับฟังพยานหลักฐานที่เป็นสื่ออิเล็กทรอนิกส์ จึงทำให้เกิดปัญหาในเรื่องประเภทของพยาน การนำสืบพยาน ดังนั้นเพื่อแก้ไขปัญหาดังกล่าวให้หมดสิ้นไป ผู้เขียนเห็นว่าควรที่จะกำหนดให้มีบทบัญญัติรับรองการอ้างข้อมูลจากสื่ออิเล็กทรอนิกส์เป็นพยานหลักฐานในศาลได้ โดยบทบัญญัติดังกล่าวควรจะได้กำหนดถึงความหมายของพยานที่เป็นสื่ออิเล็กทรอนิกส์ วิธีการอ้างและวิธีการนำเสนอพยานหลักฐานอิเล็กทรอนิกส์เป็นพยานหลักฐานในศาล รวมถึงวิธีการนำสืบพยานหลักฐานเช่นว่านั้นด้วย ซึ่งในการแก้ไขกฎหมายนั้นผู้เขียนเห็นว่าน่าจะนำกฎหมายของประเทศสหรัฐอเมริกาหรือประเทศอังกฤษมาเป็นแม่แบบสำหรับการปรับปรุงแก้ไขกฎหมายลักษณะพยานของไทย เนื่องจากระบบวิธีพิจารณาความและกฎเกณฑ์ทางกฎหมายลักษณะพยานในหลายเรื่องของไทยได้รับอิทธิพลจากกฎหมายคอมมอนลอว์

นอกจากนั้นในประเด็นเรื่องความน่าเชื่อถือของพยานหลักฐานนั้น ในกฎหมายต่างประเทศได้มีการกำหนดวิธีการให้อำนาจเจ้าพนักงานยึดคอมพิวเตอร์ที่มีข้อมูลที่ใช้พิสูจน์ความผิดของผู้ถูกกล่าวหาไว้ โดยมีกระบวนการที่เข้ามาทำให้มีความมั่นใจต่อศาลว่าข้อมูลที่ยึดได้นั้นจะไม่มีการเปลี่ยนแปลงแก้ไขก่อนนำเสนอต่อศาล ดังนั้นพยานหลักฐานดังกล่าวจึงมีความน่าเชื่อถือว่าเป็นความจริง เมื่อนำเสนอต่อศาลจึงมีน้ำหนักและสามารถรับฟังได้ ฉะนั้นเพื่อแก้ไขปัญหาเหล่านี้จึงจำเป็นต้องมีการพัฒนากฎหมายเพื่อรองรับข้อมูลอิเล็กทรอนิกส์ที่อยู่ในระบบเครือข่ายอินเตอร์เน็ตหรือข้อมูลที่อยู่ในแผ่นดิสก์ เพื่อให้สามารถนำมาอ้างเป็นพยานหลักฐานในการพิสูจน์ความผิดของผู้ถูกกล่าวหาในกระบวนพิจารณาคดีทั้งในชั้นสืบสวนสอบสวนและในชั้นศาลได้

นอกจากนี้ในคดีอาญาการรับฟังพยานหลักฐานเพื่อพิสูจน์ความผิดของจำเลยเป็นสิ่งที่พึงต้องระวังเป็นอย่างมาก เพราะการจะรับฟังพยานหลักฐานเพื่อลงโทษจำเลยได้นั้นจะต้องพิสูจน์จนสิ้นสงสัย ดังนั้นในคดีอาชญากรรมทางคอมพิวเตอร์การนำสืบพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์จึงเป็นสิ่งที่ต้องให้ความสำคัญเป็นพิเศษ โดยเฉพาะเรื่องความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์เนื่องจากสามารถแก้ไขเปลี่ยนแปลงได้โดยง่ายและไม่ทิ้งร่องรอยไว้ให้ตรวจสอบได้ ทำให้ศาลอาจจะไม่เชื่อถือพยานหลักฐานดังกล่าว หรือไม่รับฟังพยานหลักฐานเพื่อลงโทษจำเลยได้ เพื่อมิให้เกิดปัญหาดังกล่าวจึงจำเป็นต้องใช้พยานชำนาญการพิเศษ หรือพยานผู้เชี่ยวชาญในคดีอาญา อธิบายเหตุผลประกอบการตรวจพิสูจน์หรือ

ให้ความเห็นซึ่งคนธรรมดาไม่มีความรู้ในวิทยาการแขนงนั้นได้เห็นคล้อยตามด้วย เช่น ผู้เชี่ยวชาญในสาขาวิทยาการคอมพิวเตอร์มาให้ความเห็นเกี่ยวกับระบบข้อมูลคอมพิวเตอร์ หรือพฤติกรรมการกระทำความผิดของอาชญากรรมคอมพิวเตอร์จะทำอย่างนั้นอย่างนี้กับข้อมูลคอมพิวเตอร์ด้วยวิธีใด อย่างใด เป็นต้น เพื่อให้ศาลเกิดความเชื่อมั่นในพยานหลักฐานดังกล่าว โดยรับฟังประกอบกับความเห็นของพยานผู้เชี่ยวชาญ อันจะทำให้พยานหลักฐานดังกล่าวมีน้ำหนักมากขึ้น

ดังนั้นความเห็นของพยานผู้เชี่ยวชาญจึงเป็นสิ่งที่สำคัญมากสำหรับการพิจารณาคดีอาชญากรรมทางคอมพิวเตอร์ เพราะในการพิสูจน์ข้อมูลอิเล็กทรอนิกส์ที่อยู่ในลักษณะเลขฐานสองในฮาร์ดดิสก์นั้น พนักงานสอบสวน อัยการ ศาล เมื่อตรวจดูฮาร์ดดิสก์แล้วมีข้อจำกัดว่าแปลข้อความหรือความหมายของข้อมูลที่เป็นสัญลักษณ์ทางคณิตศาสตร์นั้นไม่ได้ พยานผู้เชี่ยวชาญจึงมีบทบาทอย่างมากในการช่วยแปลข้อความหรือความหมายของข้อมูลที่อยู่ในรูปของตัวเลขนั้น นอกเหนือจากการช่วยวิเคราะห์ให้เห็นพฤติกรรมของอาชญากรคอมพิวเตอร์ แต่ประเทศไทยยังขาดบุคลากรที่มีคุณสมบัติเป็นพยานผู้เชี่ยวชาญที่มีความรู้ ความชำนาญและมีประสบการณ์ด้านการวิเคราะห์พิสูจน์ข้อมูลคอมพิวเตอร์อย่างแท้จริงเพียงพอ จึงอาจทำให้ความเชื่อถือของศาลที่มีต่อพยานผู้เชี่ยวชาญน้อยตามไปด้วย เพราะแม้พยานผู้เชี่ยวชาญที่มาเบิกความในศาลนั้น จะเบิกความในประเด็นซึ่งคนธรรมดาไม่มีความรู้ก็มิใช่ว่าศาลจะเชื่อถือพยานผู้เชี่ยวชาญทุกกรณีไป ศาลต้องพิจารณาถึงเหตุผลและน้ำหนักพยานหลักฐานอื่นประกอบด้วย และความรู้หรือความชำนาญของพยานผู้เชี่ยวชาญก็เป็นปัจจัยสำคัญอย่างยิ่งในการยอมรับของศาล หากพยานผู้เชี่ยวชาญไม่มีความรู้มากพอที่จะเชื่อถือขาดประสบการณ์น้ำหนักพยานก็น้อยได้เช่นเดียวกัน

5.1.3 มาตรการในการจัดตั้งหน่วยงานที่รับผิดชอบเกี่ยวกับการประกอบอาชญากรรมทางคอมพิวเตอร์โดยตรง

ประเทศสหรัฐอเมริกาได้ตระหนักถึงปัญหาอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ต เนื่องจากลักษณะพิเศษของระบบเครือข่ายอินเตอร์เน็ตที่เป็นเครือข่ายไร้พรมแดน การที่จะบังคับใช้กฎหมายเพื่อปราบปรามอาชญากรรมทางอินเตอร์เน็ตและองค์กรบังคับใช้กฎหมายจะต้องใช้ความร่วมมือและประสานงานกันอย่างใกล้ชิดใน

การปราบปรามการหลอกลวงทางอินเตอร์เน็ต กระทรวงยุติธรรมของประเทศสหรัฐอเมริกา (Department of Justice) จึงได้ดำเนินการสองขั้นตอนด้วยกันคือ [91]

1. การให้ความร่วมมือระหว่างองค์กรผู้บังคับใช้กฎหมายในการปราบปรามการหลอกลวงทางอินเตอร์เน็ต โดยเริ่มต้นความร่วมมือในในวันที่ 26 กุมภาพันธ์ ค.ศ.1999 ซึ่งเป็นความร่วมมือระหว่างหน่วยงานของชาติเพื่อประสานงาน และสืบสวนสอบสวนเพื่อปราบปรามการหลอกลวงทางอินเตอร์เน็ตโดยเฉพาะ ซึ่งมีวัตถุประสงค์หลัก 6 ประการ คือ

1.1 ศึกษาข้อมูลเกี่ยวกับลักษณะ วิธีการและขอบเขตของการหลอกลวงทางอินเตอร์เน็ต โดยเป็นความร่วมมือกับสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐในการศึกษาข้อมูลดังกล่าว รวมทั้งศึกษาถึงแนวโน้มของการแพร่หลายและผลกระทบจากการหลอกลวงทางอินเตอร์เน็ตที่จะเกิดขึ้นในอนาคตอีกด้วย

1.2 พัฒนาและให้คำแนะนำแก่อัยการและเจ้าพนักงานในการบังคับใช้กฎหมาย และบุคลากรของรัฐในการป้องกันและปราบปรามการหลอกลวงทางอินเตอร์เน็ต โดยจัดให้มีการฝึกอบรมให้ความรู้เฉพาะทางเกี่ยวกับระบบเครือข่ายอินเตอร์เน็ต โดยผ่านทาง National Advocacy Center (NAC) ที่จะจัดฝึกอบรมให้ความรู้ทั้งในระดับพื้นฐานและในระดับสูง นอกจากนี้ยังฝึกอบรมเรื่องดังกล่าวให้กับองค์กรผู้บังคับใช้กฎหมายในแต่ละมลรัฐเพื่อสามารถนำความรู้ไปป้องกันและปราบปรามอาชญากรรมในแต่ละมลรัฐได้อีกด้วย

1.3 สนับสนุนและพัฒนาในเรื่องการสืบสวนสอบสวน การวิเคราะห์ถึงการกระทำความผิด ตลอดจนการนำตัวผู้กระทำความผิดมาลงโทษ และก่อตั้งศูนย์ร้องเรียนเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ต

1.4 เสนอแนะและอำนวยความสะดวก การร่วมมือระหว่างระหว่างรัฐหน่วยงานบังคับใช้กฎหมายในระดับท้องถิ่นเกี่ยวกับการสืบสวนสอบสวนคดีอาชญากรรมดังกล่าว

1.5 สนับสนุนและให้แนะนำในการดำเนินคดีเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ต

---

[91] Internet Fraud [Online]. Available from: htpp://www.internetfraud .usdoj.gov /htm. [2002, June 20]

1.6 ริเริ่มให้มีการให้ความรู้แก่ประชาชนในการหลีกเลี่ยงการหลอกลวงทางอินเตอร์เน็ต รวมทั้งวิธีการทางเทคโนโลยีในการป้องกันการหลอกลวงทางอินเตอร์เน็ต และขยายมาตรการในการป้องกันและปราบปรามอาชญากรรมดังกล่าวทั้งหน่วยงานของรัฐและหน่วยงานของภาคเอกชน

2. ได้มีการจัดตั้งหน่วยรับร้องเรียนเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ต (Internet Fraud Complaint Center : IFCC) เป็นความร่วมมือกับ FBI และ National White Collar Crime Center เป็นหน่วยงานที่รับร้องเรียนเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตให้กับองค์กรบังคับใช้กฎหมายของรัฐบาลสหรัฐ และองค์กรบังคับใช้กฎหมายท้องถิ่น ซึ่งนอกจากหน่วยงานดังกล่าวแล้วยังมีอีกหลายหน่วยงานที่รับร้องเรียน โดยแบ่งแยกประเภทของการถูกหลอกลวงไว้ เช่น การหลอกลวงเกี่ยวกับสินค้าเกษตรแจ้งที่ Commodity Futures Trading Commission (CFTC) การหลอกลวงผู้บริโภคทั่วไปแจ้งที่ Federal Trade Commission (FTC) หรือการหลอกลวงเกี่ยวกับหลักทรัพย์แจ้งที่ SEC Enforcement Division Complaint Center

นอกจากนั้นยังมีการจัดตั้งหน่วยงานรับร้องเรียนเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตขององค์กรภาคเอกชนอีกด้วย เช่น The National Fraud Information Center (NFIC) ตั้งขึ้นเมื่อ ค.ศ.1992 เป็นการก่อตั้งโดยสมาคมผู้บริโภคแห่งชาติ (National Consumers League : NCL) ซึ่งเป็นหน่วยงานเก่าแก่ในการคุ้มครองผู้บริโภคของประเทศสหรัฐอเมริกา ทำงานในลักษณะองค์กรที่ไม่ค้ากำไร เพื่อปราบปรามการกระทำการหลอกลวงทุกประเภท นอกจากทางสามารถร้องเรียนการกระทำความผิดทางเว็บไซต์แล้ว ผู้ตกเป็นเหยื่อของอาชญากรรมดังกล่าวยังสามารถร้องเรียนผ่านทางสายด่วน (Hot Line) โดยไม่เสียค่าบริการอีกด้วย [92]

สำหรับประเทศไทยการรับแจ้งเว็บไซต์ผิดกฎหมาย สำนักงานตำรวจแห่งชาติได้มีการรับแจ้งเว็บไซต์ผิดกฎหมายแล้วที่ www.police.go.th ซึ่งเว็บไซต์ที่ได้รับแจ้งว่าผิดกฎหมายมากที่สุด ได้แก่เว็บไซต์ลามกอนาจาร 1,624 เว็บไซต์ คิดเป็นร้อยละ 38.62 % (ข้อมูล ณ วันที่ 27 เดือนธันวาคม 2545) และปัจจุบันมีเจ้าหน้าที่ในสำนักงานตำรวจแห่งชาติคอยติดตามดูเว็บไซต์ต่าง ๆ เช่น เว็บไซต์ลามก โดยค้นหาเว็บที่มีคำว่า nude xxx sex เป็นต้น เว็บไซต์ขาย

---

[92] About the National Fraud Information Center & Internet Fraud Watch [Online]. Available from:http://www.fraud.org/info/aboutnfic.htm. [2002, May 20]

ดูเว็บไซต์ต่าง ๆ เช่น เว็บไซต์ลามก โดยค้นหาเว็บที่มีคำว่า nude xxx sex เป็นต้น เว็บไซต์ขายสิ่งผิดกฎหมายอื่น เว็บไซต์ขายบริการทางการเพศ เว็บไซต์การพนัน เว็บไซต์ที่เป็นภยันอันตรายต่อความมั่นคงของชาติและสถาบัน ซึ่งผู้เขียนเห็นว่าควรจะมีการสนับสนุนให้เว็บไซต์ของกรมตำรวจเป็นเว็บไซต์หลักในการรับร้องเรียนเกี่ยวกับการประกอบอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ต

ดังที่ได้กล่าวมาแล้วว่าอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ตเป็นอาชญากรรมรูปแบบใหม่สำหรับประเทศไทย และผู้ประกอบอาชญากรรมดังกล่าวมีความรู้ความสามารถ ซึ่งการสืบสวนสอบสวนในคดีอาชญากรรมทางคอมพิวเตอร์ไม่ใช่เรื่องง่ายที่เจ้าหน้าที่คนหนึ่งคนใดจะสามารถกระทำได้เหมือนคดีอาชญากรรมธรรมดา แต่ต้องเป็นเจ้าหน้าที่ที่ต้องมีความรู้ความเข้าใจในระบบต่าง ๆ ของเครื่องคอมพิวเตอร์ เครื่องมือและอุปกรณ์ในการตรวจสถานที่เกิดเหตุย่อมมีความแตกต่างจากคดีอาชญากรรมทั่วไป จึงมีความจำเป็นจะต้องจัดตั้งหน่วยงานที่มีอำนาจหน้าที่โดยเฉพาะ มีองค์ประกอบของบุคคลที่มีความรู้ความชำนาญทั้งในด้านคอมพิวเตอร์ และการสืบสวนคดีอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยี ซึ่งในประเทศไทยยังไม่มีหน่วยงานเฉพาะ เจ้าหน้าที่ผู้ปฏิบัติขาดความรู้ความเข้าใจในด้านวิธีการตรวจค้นและยึดพยานหลักฐานที่เกี่ยวข้องกับคอมพิวเตอร์ ในขณะที่ประเทศสหรัฐอเมริกากำลังเผชิญหน้ากับปัญหาอาชญากรรมทางคอมพิวเตอร์มากที่สุด ได้มีการจัดตั้งหน่วยงานที่มีหน่วยงานภาครัฐและภาคเอกชน เช่น Computer Crimes Squad ซึ่งสังกัดอยู่ใน F.B.I. ทำหน้าที่ตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ ส่วนในภาคเอกชนก็จะอยู่ในรูปแบบของสมาคมหรือชมรมจัดตั้งหน่วยงานขึ้นมาศึกษาและติดตามอาชญากรรมคอมพิวเตอร์โดยเฉพาะเช่นเดียวกัน

สำหรับประเทศไทยเมื่อผู้ปฏิบัติไม่มีความรู้เกี่ยวกับเทคโนโลยีคอมพิวเตอร์แต่มีความจำเป็นที่จะต้องปฏิบัติงานในสิ่งที่ตนเองไม่รู้จักและยังไม่มีขั้นตอนที่ชัดเจนให้ถือปฏิบัติตาม ผู้ปฏิบัติก็ขาดความกล้าที่จะเข้าไปทำการสืบสวนสอบสวนในคดีหรือหากว่าผู้นั้นจะเข้าไปทำการสืบสวนสอบสวนด้วยความจำเป็นเพราะสถานการณ์บังคับ เขาผู้นั้นก็อาจกลายเป็นผู้ก่อให้เกิดความเสียหายต่อรูปคดีหรือเป็นผู้ทำลายหลักฐานสำคัญทางคดีเสียเอง เนื่องจากความรู้เท่าไม่ถึงการณ์ได้ ผู้ปฏิบัติจึงมีความจำเป็นที่จะต้องมีความรู้ความชำนาญและมีความสามารถเพียงพอในการที่จะกำหนดหลักฐานที่มีความจำเป็นในทางคดี ยึด เก็บรักษาและนำส่งพยานหลักฐานทางคดีได้อย่างถูกต้อง ดังนั้นจึงควรมีการดำเนินการพัฒนาความรู้แก่

ผู้ที่มีหน้าที่ในการปฏิบัติ โดยจัดอบรมความเข้าใจพื้นฐานของหลักการเบื้องต้นเพื่อให้สอบสวนดำเนินคดีในความผิดประเภทนี้ได้อย่างมีประสิทธิภาพ

ดังนั้นนอกจากแนวทางในการบัญญัติกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะแล้ว ผู้เขียนยังเห็นว่าการจะบังคับใช้กฎหมายที่มีอยู่ในการปราบปรามอาชญากรรมให้มีประสิทธิภาพได้นั้น จะต้องมีองค์กรบังคับใช้กฎหมายที่มีประสิทธิภาพเพียงพอด้วย โดยการจัดตั้งหน่วยงานเฉพาะขึ้นเพื่อปราบปรามการอาชญากรรมคอมพิวเตอร์ขึ้น ตัวบุคลากรที่เกี่ยวข้องในการบังคับใช้กฎหมายจึงควรจะมีความรู้ความชำนาญเฉพาะเรื่องดังกล่าวเป็นอย่างดี แต่ข้อเท็จจริงปรากฏว่าผู้ปฏิบัติงานในกระบวนการยุติธรรมของประเทศไทยยังขาดความรู้ในการติดตามการกระทำความผิดทางอินเตอร์เน็ต ทั้งในด้านกฎหมายและการปฏิบัติ ซึ่งในหลายประเทศมีหน่วยพิเศษที่มีทั้งผู้เชี่ยวชาญด้านอินเตอร์เน็ตและตำรวจที่ได้รับการฝึกมาทางด้านนี้และปฏิบัติงานมานาน รวมทั้งมีอัยการซึ่งเป็นผู้รู้กฎหมายและได้รับการฝึกด้านอินเตอร์เน็ต ดังนั้นสำหรับประเทศไทยในเบื้องต้นควรจะสรรหาและพัฒนาบุคลากรจากกลุ่มผู้มีประสบการณ์ด้านการสืบสวนคดีอาญาที่มีความรู้พื้นฐานทางคอมพิวเตอร์และอิเล็กทรอนิกส์และกลุ่มผู้มีวิชาชีพทางด้านคอมพิวเตอร์ เพื่อฝึกอบรมในด้านวิธีการตรวจและยึดพยานหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะ เพื่อเตรียมการที่จะจัดการกับอาชญากรรมทางคอมพิวเตอร์ในประเทศไทยต่อไป และมีการอบรมให้ความรู้แก่พนักงานสอบสวน พนักงานอัยการและศาล เกี่ยวกับเครื่องคอมพิวเตอร์ การทำงานของเครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ เพียงเพื่อจะได้เข้าใจถึงลักษณะของการประกอบอาชญากรรม รวมทั้งลักษณะของอาชญากรรมทางคอมพิวเตอร์ วิธีการกระทำความผิด เพื่อให้มีความรู้ความชำนาญในการปราบปรามอาชญากรรมดังกล่าว และควรมีการกำหนดแนวทางและกฎเกณฑ์ในการรวบรวมพยานหลักฐานและดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ เพื่อให้พนักงานสอบสวนและพนักงานอัยการทราบว่าพยานหลักฐานเช่นไรควรนำเข้าสู่กระบวนการพิจารณาคดีของศาลเพื่อให้ลงโทษผู้กระทำความผิดได้ และหน่วยงานนี้ควรสนับสนุนให้มีความร่วมมือกับองค์กรภายนอกทั้งด้านเอกชนด้วย รวมทั้งส่งเสริมความร่วมมือกับต่างประเทศทั้งโดยสนธิสัญญาเกี่ยวกับความร่วมมือระหว่างประเทศหรือโดยวิธีการอื่นในการสืบสวนสอบสวน ดำเนินคดีและการป้องปรามอาชญากรรมทางคอมพิวเตอร์

5.2 มาตรการในการป้องกันอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ต

ปัจจุบันการหลอกลวงได้มีพัฒนารูปแบบและวิธีการหลากหลายขึ้น ประกอบกับความก้าวหน้าทางเทคโนโลยีสารสนเทศ ผนวกกับการพัฒนาทางด้านคอมพิวเตอร์ และระบบเครือข่ายอินเตอร์เน็ต ทำให้การหลอกลวงทางอินเตอร์เน็ตสามารถแพร่หลายไปสู่สังคมของประเทศต่าง ๆ ทั่วโลกได้อย่างรวดเร็วจนยากที่จะควบคุมป้องกัน แม้หลายประเทศจะได้มีการบัญญัติกฎหมายขึ้นมาเพื่อปราบปรามการหลอกลวงทางอินเตอร์เน็ตก็ตาม แต่ก็ยังไม่สามารถที่จะนำกฎหมายดังกล่าวมาแก้ไขปัญหาการหลอกลวงทางอินเตอร์เน็ตได้อย่างมีประสิทธิภาพ เนื่องจากเป็นการแก้ไขปัญหาที่ปลายเหตุ เพื่อให้อาชญากรรมดังกล่าวหมดสิ้นไปควรจะต้องเป็นแก้ไขปัญหาที่ต้นเหตุ คือ มาตรการป้องกันไม่ให้เกิดการกระทำความผิดเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตเกิดขึ้น จากการศึกษามาตรการในการป้องกันการหลอกลวงทางอินเตอร์เน็ตในประเทศสหรัฐอเมริกาจะพบว่ามีหลายวิธี ซึ่งผู้เขียนพอจะสรุปมาตรการในการป้องกันอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ตได้ ดังนี้

5.2.1 มาตรการการให้ความรู้แก่ประชาชนโดยทั่วไป

เนื่องจากผู้กระทำความผิดเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตเป็นผู้มีความรู้ความสามารถ หรือที่เรารู้จักกันในนามของอาชญากรเชิ้ตขาว (White Collar Crime) ซึ่งก่อให้เกิดความเสียหายต่อระบบเศรษฐกิจของประเทศเป็นอย่างมาก หรือกล่าวอีกนัยหนึ่งคือการหลอกลวงทางอินเตอร์เน็ตถือเป็นอาชญากรรมทางเศรษฐกิจรูปแบบหนึ่ง ในขณะนี้เป็นที่ยอมรับกันในบรรดานานาประเทศว่านโยบายในการป้องกันอาชญากรรมทางเศรษฐกิจจะประสบความสำเร็จมากกว่าการปราบปราม ดังนั้นการดำเนินการกับการหลอกลวงทางอินเตอร์เน็ตก็เช่นกัน ซึ่งมาตรการสำคัญในการป้องกันการประกอบอาชญากรรมดังกล่าวคือการให้ความรู้แก่ประชาชนโดยทั่วไป

โดยปกติผู้ใช้อินเตอร์เน็ตจะพบการหลอกลวงทางอินเตอร์เน็ตมากมายไม่ว่าจะเป็นทางจดหมายอิเล็กทรอนิกส์ ทางกระดานข่าว ทางเว็บไซต์ ทางช่องสนทนา ซึ่งนับว่าเป็นสิ่งที่มิอาจหลีกเลี่ยงได้ ในขณะที่เราไม่สามารถหลีกเลี่ยงการหลอกลวงทางอินเตอร์เน็ตและไม่สามารถปราบปรามการกระทำความผิดดังกล่าวให้หมดสิ้นไปได้ จึงเห็นควรต้องแก้ปัญหาดังกล่าวด้วยการให้ความรู้แก่ประชาชนทั่วไปไม่ให้ตกเป็นเหยื่อของอาชญากรรมดังกล่าว

ประเทศสหรัฐอเมริกาได้มีความคิดริเริ่มที่จะให้ความรู้แก่ประชาชนที่ใช้บริการอินเตอร์เน็ตทั่วไปได้ตระหนักถึงประเภท วิธีการของอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ต รวมทั้งมีการให้คำแนะนำกับผู้ที่ตกเป็นเหยื่อของอาชญากรรมดังกล่าวแล้ว ซึ่งเป็นความร่วมมือกันระหว่างหน่วยงานของรัฐหลายหน่วยงาน เช่น สมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐ (FTC), FBI หรือกระทรวงยุติธรรมของประเทศสหรัฐอเมริกา (Department of Justice) ซึ่งวิธีการในการให้ความรู้แก่ประชาชนส่วนใหญ่จะใช้เป็นการให้ความรู้โดยผ่านทางระบบเครือข่ายอินเตอร์เน็ต เนื่องจากการประกอบอาชญากรรทางอินเตอร์เน็ตเป็นการประกอบอาชญากรรมที่รวดเร็วมาก จึงจำเป็นต้องใช้ระบบเครือข่ายอินเตอร์เน็ตเป็นเครื่องมือในการให้ความรู้เช่นกัน เพื่อให้การเผยแพร่ความรู้แก่ประชาชนทันกับการประกอบอาชญากรรมดังกล่าว ดังนี้

1. ทางเว็บไซต์ โดยสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐได้ดำเนินการเปิดเว็บไซต์ของสำนักงาน ตั้งแต่เดือนเมษายน ค.ศ.1995 คือ www.ftc.gov เพื่อให้ความรู้ความเข้าใจและตอบข้อซักถามจากประชาชนทั่วไป รวมทั้งการให้คำแนะนำแก่ผู้ที่ตกเป็นเหยื่อของอาชญากรรมดังกล่าวด้วย ซึ่งหลังจากเปิดเว็บไซต์ดังกล่าวได้มีประชาชนที่สนใจเข้ามาชมถึงวันละประมาณ 95,000 ครั้ง จนกระทั่งภายในเดือนเมษายน ค.ศ.1998 เพียงเดือนเดียวเท่านั้นได้มีผู้เข้าชมถึง 3 ล้านครั้ง จากผู้เข้าชมถึงหลายหมื่นคน [93] นอกจากนี้เว็บไซต์ดังกล่าวยังมีบริการค้นหาข้อมูล (Search Engine) เพื่อให้ผู้สนใจหาข้อมูลต่าง ๆ สามารถค้นหาข้อมูลได้ง่ายเพียงแค่ใส่คำสำคัญ (Key Word) เท่านั้น โดยเว็บไซต์ดังกล่าวจะประกอบด้วยข้อมูลต่าง ๆ เกี่ยวกับประเภท วิธีการการหลอกลวงทางอินเตอร์เน็ต คำพิพากษาของศาลกฎหมายที่มีผลบังคับใช้กับการหลอกลวง และมีการเตือนภัยแก่ผู้บริโภคให้ไม่ต้องยุ่งเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ต มีการให้สอบถามข้อมูลที่สงสัยได้ รวมทั้งมีการรับร้องเรียนเกี่ยวกับการการหลอกลวงอีกด้วยด้วย ทำให้ประชาชนทั่วไปหรือผู้ถูกหลอกลวงสามารถหาความรู้ ขอคำปรึกษา หรือร้องเรียนถึงการกระทำความผิดดังกล่าวได้ง่าย สะดวกผ่านทางอินเตอร์เน็ต โดยไม่ต้องเดินทางไปแจ้งที่สำนักงานโดยตรง นอกจากนี้เมื่อเว็บไซต์ดังกล่าวได้รับความนิยมเป็นอย่างมาก สมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐจึงได้มีแนวความคิดที่จะสร้างเว็บไซต์ใหม่ คือ www.consumer.gov ขึ้นใหม่อีกด้วย ซึ่งเว็บไซต์ใหม่นี้

---

[93] FTC, Prepared Statement of The Federal Trade Commission on "Consumer Protection in Cyberspace:Combating Fraud on the Internet" [Online]. Available from: http:// www.ftc.gov/ os/1998/9806/test.623.htm [2002, July 9]

เป็นความร่วมมือกันระหว่างหน่วยงานที่บังคับใช้กฎหมาย เช่น คณะกรรมการหลักทรัพย์และตลาดหลักทรัพย์ (Securities and Exchange Commission :SEC) คณะกรรมการอาหารและยา (Food and Drug Administration :FDA) เป็นต้น [94]

นอกจากเว็บไซต์ดังกล่าวแล้ว ยังมีเว็บไซต์ของหน่วยงานต่าง ๆ ในประเทศสหรัฐอเมริกาอีกมากที่เปิดเว็บไซต์ให้ความรู้กับประชาชนทั่วไป ซึ่งมีทั้งเว็บไซต์ของหน่วยงานรัฐบาล เช่น Computer Crime and Intellectual Property (Section ,Criminal Division ,US), Federal Bureau of Investigation, Securities and Exchange Commison, U.S.Customs Service, U.S. Postal Inspection Service, U.S.Secret Service หรือเว็บไซต์ของภาคเอกชนต่าง ๆ เช่น Better Business Bureau, Internet Fraud Council, Internet Fraud Watch, Internet ScamBusters, National Consumers League[95] เป็นต้น เพื่อให้ข้อมูลเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ต ซึ่งเป็นความร่วมมือระหว่างรัฐบาลและภาคเอกชนต่าง ๆ ในการให้ความร่วมมือเพื่อป้องกันอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ต ไม่ว่าจะเป็นประเภทของการหลอกลวง ลักษณะ และการให้ความคุ้มครองทางด้านกฎหมาย ตัวอย่างคดีที่เกิดขึ้น เป็นต้น เพื่อเป็นการให้ความรู้แก่ผู้บริโภคอันเป็นการป้องกันให้ผู้บริโภคห่างไกลจากการหลอกลวงทางอินเตอร์เน็ต ซึ่งแต่ละเว็บไซต์จะสามารถลิงค์ถึงกันได้

2. มีการสร้างเว็บไซต์ของปลอม (Teaser web site) มาตรการนี้เป็นความร่วมมือระหว่างหน่วยงานของรัฐและหน่วยงานเอกชนที่จะป้องกันประชาชนให้ปลอดภัยจากอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ต โดยการสร้างเว็บไซต์ที่เกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตรูปแบบต่าง ๆ ซึ่งเป็นเว็บไซต์ของปลอมขึ้นมา เช่น สร้างเว็บไซต์การหลอกลวงการประกอบธุรกิจ (Business Opportunity) ของปลอมขึ้นมา ซึ่งเว็บไซต์ดังกล่าวจะมีลักษณะเช่นเดียวกับเว็บไซต์ที่ประกอบอาชญากรรมหลอกลวงการประกอบธุรกิจทุกประการ เช่น มีการกล่าวอ้างว่าท่านสามารถเป็นเจ้าของกิจการได้ และมีการสัญญาว่าจะได้รับเงินก้อนโต

---

[94] FTC, Prepared Statement of The Federal Trade Commission on "Internet Fraud" [Online]. Available from:http://www.ftc.gov/os/2001/ 04/internetfraudstate.htm [2002, May 5]

[95] Internet Fraud [Online]. Available from: http://www.internetfraud.usdoj .gov / htm. [2002, July 9]

อย่างง่ายดาย จะบรรยายถึงการหลอกลวงต่าง ๆ เพื่อหลอกลวงผู้บริโภคมีการกล่าวอ้างถึงวิธีการประกอบธุรกิจต่าง ๆ หรือกล่าวอีกนัยหนึ่งก็คือเป็นการจำลองเว็บไซต์ที่กระทำการหลอกลวงทางอินเตอร์เน็ตนั่นเอง แต่เว็บไซต์ของปลอมนั้นเมื่อเข้าไปดูที่หน้าต่อ ๆ ไป จะพบว่ามีการเตือนประชาชนผู้เข้าเยี่ยมชมว่าหากหลงเชื่อเข้าไปร่วมประกอบธุรกิจกับเว็บไซต์ที่กระทำการเช่นนี้จะต้องสูญเสียเงินทั้งหมด และให้คำแนะนำวิธีการหลีกเลี่ยงการหลอกลวงดังกล่าว รวมทั้งมีการลิงค์เว็บไซต์ดังกล่าวกลับไปที่เว็บไซต์ของสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐ (FTC) อีกด้วยสำหรับบุคคลที่ต้องการค้นหาข้อมูล ในปัจจุบันนี้ได้มีเว็บไซต์เกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตปลอมที่สมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐ (FTC) ได้สร้างขึ้นมา 10 ประเภท เช่น การหลอกลวงเกี่ยวกับแชร์ลูกโซ่ (Pyramid scheme) การหลอกลวงเกี่ยวกับการให้ทุนการศึกษา (Scholarship Scams) การหลอกลวงเกี่ยวกับการท่องเที่ยว (Travel Fraud) การหลอกลวงเกี่ยวกับการประกอบธุรกิจ (Business Opportunities) เป็นต้น เพื่อเป็นแบบทดสอบให้กับประชาชนทั่วไป ซึ่งจะมีการส่งอีเมล์ไปยังบุคคลต่าง ๆ เพื่อให้เข้ามาเยี่ยมชมเว็บไซต์ดังกล่าว (เช่นเดียวกับ Spam mail ทั่วไป) และยังมีการนำไปลิงค์อยู่ในเว็บไซต์ที่เอาไว้ค้นหาข้อมูล (Search Engine) ที่เป็นที่ได้รับความนิยม เช่น www.yahoo.com[96] ซึ่งเป็นการเผยแพร่ให้ประชาชนเข้าเยี่ยมชมเว็บไซต์ดังกล่าวได้มากขึ้น

3. มีการจัดสัมมนาทางอินเตอร์เน็ต เป็นการนำเอาเทคโนโลยีสมัยใหม่มาใช้เป็นเครื่องมือในการป้องกันอาชญากรรม ซึ่งนับว่าเป็นมาตรการที่ได้ผลดีเพราะสามารถเข้าถึงประชนชนได้อย่างทั่วถึง โดยสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐ (FTC) ได้ร่วมมือกับ North American Securities Administrators Association จัดการสัมมนาทางอินเตอร์เน็ต (On-line forum) ขึ้นในเดือนเมษายน ค.ศ.1997 มีประชาชนเข้าร่วม 100 กว่าคน โดยมีการส่งคำถามถามถึงผู้เชี่ยวชาญเกี่ยวกับการหลอกลวงต่าง ๆ และได้รับทราบคำตอบจากผู้เชี่ยวชาญ และได้นำคำถามดังกล่าวไปไว้ในเว็บไซต์ของสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐ (FTC) ซึ่งทำให้ผู้ที่เข้าชมจะได้รับประโยชน์จากการอ่านคำถามต่าง ๆ โดยไม่ต้องเสียเวลาในการถามเอง

---

[96] FTC, "Consumer Protection in Cyberspace:Combating Fraud on the Internet" [Online]. Available from: http://www.ftc.gov/os/1998/9806/test.623.htm. [2002, May 20]

4. มีการจัดทำแผ่นพับเว็บไซต์หลอกลวง ซึ่งจะระบุรายชื่อเว็บไซต์ต่าง ๆ ที่กระทำการหลอกลวงทางอินเตอร์เน็ต นับตั้งแต่การหลอกลวงการประมูลสินค้าออนไลน์ การหลอกลวงให้ประกอบธุรกิจลูกโซ่ การหลอกลวงขายสินค้าทางอิเล็กทรอนิกส์ การหลอกลวงเกี่ยวกับบัตรเครดิต

5.2.2 มาตรการการให้ความร่วมมือในการป้องกันและปราบปรามการหลอกลวงทางอินเตอร์เน็ต

เนื่องจากกลุ่มอาชญากรอาศัยระบบเครือข่ายอินเตอร์เน็ตในการประกอบอาชญากรรม ทำให้สามารถเข้าถึงกลุ่มบุคคลได้เป็นจำนวนมาก หน่วยงานของรัฐต่างๆ ได้เล็งเห็นถึงข้อดีของระบบเครือข่ายอินเตอร์เน็ตดังกล่าว จึงได้มีแนวความคิดที่จะนำระบบเครือข่ายอินเตอร์เน็ตมาเป็นเครื่องมือในการป้องกันและปราบปรามอาชญากรรมดังกล่าวเช่นกัน ซึ่งวิธีการนี้จะเป็นจัดวันกวาดล้าง (Surf Day) ขึ้น เพื่อเป็นการค้นหาเว็บไซต์ที่กระทำการหลอกลวงทางอินเตอร์เน็ต เมื่อพบเว็บไซต์ที่กระทำการลักษณะหลอกลวงแล้วจะมีการดาว์นโหลด พิมพ์และส่งไปยังสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐ (FTC) ไว้เป็นหลักฐานและทำการส่งอีเมล์เตือนผู้กระทำความผิดดังกล่าวว่าการกระทำความผิดของเขาอาจเป็นการกระทำความที่ผิดกฎหมาย (FTC Acts) ซึ่งมีเว็บไซต์จำนวนมากที่ได้รับอีเมล์เตือนดังกล่าวแล้วได้หยุดการกระทำความผิด ซึ่งหากเว็บไซต์นั้นยังคงดำเนินการต่อไป ก็จะมีการฟ้องร้องเว็บไซต์ดังกล่าวทันที [97]

มาตรการนี้เกิดขึ้นครั้งแรกเมื่อเดือนธันวาคม ค.ศ. 1996 โดยมุ่งเน้นถึงการหลอกลวงประเภทแชร์ลูกโซ่ (Pyramid Schemes) จากการกวาดล้างการหลอกลวงดังกล่าวเพียงเวลาแค่สามชั่วโมง พบเว็บไซต์ที่กระทำการหลอกลวงลักษณะดังกล่าวมากกว่า 500 เว็บไซต์ รวมทั้งการหลอกลวงทางกระดานข่าวด้วย ซึ่งเจ้าหน้าที่ของสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติ (FTC) ได้ส่งอีเมล์เตือนไปยังผู้กระทำการดังกล่าวว่าเป็นการกระทำที่ฝ่าฝืนต่อบทบัญญัติกฎหมาย และหากสนใจจะสอบถามรายละเอียดเพิ่มเติมก็สามารถดูได้ที่เว็บไซต์ของสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติ (FTC) ได้อีกด้วย ซึ่งในปัจจุบันได้มีการกวาดล้างการหลอกลวงอีกหลายรูปแบบ เช่น การกวาดล้างการหลอกลวงเกี่ยวกับการให้ทุนการศึกษา เมื่อเดือนมิถุนายน 1997 ได้พบว่ามีเว็บไซต์ที่น่าสงสัยว่าจะกระทำการดังกล่าวอยู่ 28 เว็บไซต์ จึงได้มีการส่งอีเมล์เตือนไปว่า

---

[97] FTC, Surf Days:Detection and Deterrence [Online]. Available from: http://www. ftc.gov/reports/ fraud97/surfdays.htm [2002, May 20]

การกระทำการดังกล่าวจะถูกดำเนินคดีในชั้นศาล ทำให้มีเว็บไซต์จำนวน 6 เว็บไซต์ได้ทำการปิดตัวลงทันที หรือการกวาดล้างการหลอกลวงเกี่ยวกับการประกอบธุรกิจ เมื่อเดือนเมษายน 1997 พบว่ามีมากเป็นจำนวนหลายร้อยเว็บไซต์ ซึ่งภายหลังจากได้รับอีเมล์เตือนถึงการกระทำดังกล่าวพบว่าร้อยละ 23 ของเว็บไซต์ดังกล่าวได้หยุดกระทำการดังกล่าว ซึ่งมาตราดังกล่าวเป็นความร่วมมือระหว่างบาลกลางสหรัฐสี่หน่วยงาน ได้แก่ กระทรวงยุติธรรมของสหรัฐอเมริกา (Department of Justice) และองค์กรคุ้มครองผู้บริโภคจากประเทศต่าง ๆ 9 ประเทศ ได้แก่ ประเทศออสเตรเลีย ประเทศแคนนาดา ประเทศฟินแลนด์ ประเทศเยอรมัน ประเทศไอร์แลนด์ ประเทศนิวซีแลนด์ ประเทศนอร์เวย์ ประเทศอังกฤษ และประเทศสหรัฐอเมริกา และองค์กรคุ้มครองผู้บริโภคจากมลรัฐต่าง ๆ 23 มลรัฐในประเทศสหรัฐอเมริกา เช่น มลรัฐเนวาดา มลรัฐนิวเจอรซี่ มลรัฐแมรีแลนด์ มลรัฐแมสซาชูเซสส์ มลรัฐมิชิแกน เป็นต้น [98]

---

[98] FTC, Prepared Statement of The Federal Trade Commission on "INTERNET FRAUD" [Online]. Available from: http://www.ftc.gov/os/2001/04/internetfraudstate.htm [2002. May 20]