บทที่ 2
ประวัติความเป็นมา แนวคิด ทฤษฎี เกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และความรับผิดทางอาญาของผู้ให้บริการอินเทอร์เน็ต

การกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นได้เกิดมีขึ้นมาช้านานแล้ว แต่ด้วยเหตุที่แต่ก่อนนั้นยังไม่มีความรุนแรงและความแพร่หลายเท่าใดนัก จึงทำให้บุคคลโดยส่วนใหญ่ในสังคมโลกไม่ค่อยตระหนักถึงพิษภัยของการกระทำความผิดและความเสียหายดังกล่าว แต่เมื่อเวลาผ่านพ้นไปพัฒนาการต่าง ๆ อันเกี่ยวกับคอมพิวเตอร์เริ่มขยับขยายและพัฒนาสู่สากลสู่โลกโลกาภิวัฒน์มากขึ้น ส่งผลให้การกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นเริ่มทวีความรุนแรงมากยิ่งขึ้นตามลำดับ จากแต่ก่อนอาจถูกจำกัดแต่เฉพาะในวงการธุรกิจ การพาณิชย์ วงการที่มีแต่ผู้มีฐานะ มีความรู้ความสามารถ แต่ปัจจุบันด้วยพัฒนาการดังกล่าวทำให้บุคคลโดยทั่วไปก็สามารถเข้าถึงคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ได้โดยง่าย จึงเกิดเป็นการเรียนรู้ การปรับใช้ในชีวิตประจำวันและถึงขั้นพัฒนาไปจนถึงการหาช่องว่างของระบบต่าง ๆ เหล่านั้นเพื่อแสวงหาประโยชน์อันมิควรได้เพื่อตนเองหรือผู้อื่น หรือเพื่อความสนุกหรือคึกคะนองเป็นต้น ด้วยเหตุดังกล่าวจึงเป็นต้นเหตุแห่งการเกิดรูปแบบใหม่ของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อาทิเช่น การยักยอก ฉ้อโกง การเผยแพร่ภาพลามกอนาจาร การกล่าวถ้อยคำดูหมิ่นหรือหมิ่นประมาทผ่านเครือข่ายอินเทอร์เน็ต รวมไปจนถึงการขโมยข้อมูลส่วนบุคคลหรือข้อมูลของผู้อื่นในระบบคอมพิวเตอร์เป็นต้น

ด้วยเหตุนี้จึงมีความจำเป็นอย่างยิ่งที่จะต้องศึกษาถึงเหตุแห่งการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยเริ่มศึกษาตั้งแต่ประวัติความเป็นมา วิวัฒนาการของคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แนวคิดและทฤษฎีอันเกี่ยวกับการกระทำความผิด รวมไปจนถึงมาตรการอันเป็นการป้องกันการกระทำความผิดในปัจจุบัน ทั้งนี้เพื่อให้ทราบถึงรายละเอียดอย่างชัดเจน และนำมา-

ศึกษาวิเคราะห์ประกอบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ-คอมพิวเตอร์ พ.ศ. 2550 ดังนี้

1. ความหมายของอาชญากรรมคอมพิวเตอร์ และอาชญากรรมอินเทอร์เน็ต

ปัจจุบันคอมพิวเตอร์ถือเป็นเครื่องมืออิเล็กทรอนิกส์ประเภทหนึ่งที่เข้าไปมี-บทบาทในชีวิตมนุษย์และสามารถอำนวยความสะดวกสบายให้กับมนุษย์อย่างมากมายมหาศาล จากการใช้งานคอมพิวเตอร์เพียงหนึ่งเครื่องพัฒนามาเป็นการใช้งานคอมพิวเตอร์หลายเครื่องโดยผ่านทางระบบเครือข่ายคอมพิวเตอร์ และเกิดการพัฒนาการด้านเครือข่ายมาเป็นการติดต่อสื่อสารที่ไร้พรมแดน แต่ถึงแม้ว่าพัฒนาการทางเทคโนโลยี-สารสนเทศนั้นจะถูกนำมาประยุกต์ใช้และก่อให้เกิดประโยชน์มากมายก็ตาม หากซึ่งนำไปใช้ในทางที่ไม่ดีไม่ชอบแล้ว อาจก่อให้เกิดความเสียหายอย่างร้ายแรงทั้งทาง-เศรษฐกิจและสังคมได้ ซึ่งความเสียหายที่เกิดขึ้นนั้นก็เนื่องมาจากการก่อการกระทำ-ความผิดผ่านระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เครือข่ายอินเทอร์เน็ตนั่นเอง

1.1 ความหมายของอาชญากรรมคอมพิวเตอร์

คำว่า "อาชญากรรมคอมพิวเตอร์" (Computer Crime) ในภาษาอังกฤษมีคำศัพท์ที่ใช้เรียกคำนี้อยู่หลายคำ ได้แก่ Computer Crime, Computer Related Crime, Cyber Crime, E-Crime, Information Technology Crime, Online Crime, High Technology Crime, Computer Misuse และ Computer Abuse โดยคำต่าง ๆ เหล่านี้ล้วน-มีความหมายในทำนองเดียวกันและสามารถใช้แทนกันได้[1]

---

[1]องอาจ เทียนหิรัญ, "อาชญากรรมทางคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์, 2546), หน้า 11.

กรณีความหมายของ “อาชญากรรมคอมพิวเตอร์” นั้น ได้มีผู้รู้รวมถึงนักกฎหมายได้อธิบายความหมายไว้หลายท่าน อาทิเช่น

คู่มืออาชญากรรมคอมพิวเตอร์ของกระทรวงยุติธรรมประเทศสหรัฐอเมริกา ให้ความหมายไว้ว่า อาชญากรรมคอมพิวเตอร์คือ การกระทำผิดกฎหมายอาญาที่ต้องใช้ความรู้ทางเทคโนโลยีคอมพิวเตอร์ ในการก่ออาชญากรรม ในการสืบสวนจับกุม และการดำเนินคดีในชั้นสอบสวน และการพิจารณาคดีในชั้นศาล

อัยการผู้เชี่ยวชาญคดีอาชญากรรมคอมพิวเตอร์ ชื่อ Kenneth S. Rosenblatt ผู้แต่งหนังสือเรื่อง **High Technology Crime** อธิบายความหมายของอาชญากรรมคอมพิวเตอร์ไว้ว่า เป็นอาชญากรรมที่เกิดขึ้นใหม่อันเป็นผลสืบเนื่องมาจากการใช้คอมพิวเตอร์ในสังคมอย่างแพร่หลาย เช่น การบุกรุกเข้าไปในระบบเครือข่าย-คอมพิวเตอร์ของบริษัทธุรกิจที่เชื่อมโยงเครือข่ายโทรคมนาคม นอกจากนี้ยังหมายถึงอาชญากรรมดั้งเดิมที่แปรสภาพไปเนื่องจากความก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์ ซึ่งในการสืบสวนคดีประเภทนี้จำเป็นต้องมีความรู้เกี่ยวกับคอมพิวเตอร์ และคุ้นเคยกับอุตสาหกรรมเทคโนโลยีชั้นสูง เช่น การโจรกรรมอุปกรณ์คอมพิวเตอร์จากหุบเขาซิลิกอน รัฐแคลิฟอร์เนีย สหรัฐอเมริกา และย่านอุตสาหกรรมผลิตเครื่องอุปกรณ์ไฮเทคต่าง ๆ

Donn Parker ได้ให้คำนิยามไว้ในหนังสือ **Fighting Computer Crime** ว่าอาชญากรรมคอมพิวเตอร์คือ การกระทำผิดกฎหมายที่ใช้ความรู้ด้านคอมพิวเตอร์ (Knowledge of Computer) เป็นปัจจัยหลักสำคัญในการก่ออาชญากรรมนั้น ๆ[2]

ดร.ไพจิตร สวัสดิสาร ได้ให้ความหมายของอาชญากรรมคอมพิวเตอร์ไว้ในหนังสือเรื่อง **การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายที่เกี่ยวกับคอมพิวเตอร์** ดังนี้

---

[2]นัยน์รัตน์ งามแสง, “อาชญากรรมคอมพิวเตอร์: ศึกษาเฉพาะกรณีปัจจัยที่มีผลต่อการเกิดปัญหาอาชญากรรมบนอินเทอร์เน็ต,” (วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์, 2547), หน้า 24.

"อาชญากรรมคอมพิวเตอร์ คือ การใช้คอมพิวเตอร์เพื่ออำนวยความสะดวกหรือนำไปสู่การกระทำผิดทางอาญา"[3]

จากคำนิยามความหมายของอาชญากรรมคอมพิวเตอร์ ดังกล่าวข้างต้นนั้น ดังจะเห็นได้ว่า ผู้รู้ รวมถึงนักกฎหมายหลายท่านต่างได้ให้ความหมายที่มีความแตกต่างกันพอสมควร และแม้ในที่สุดแล้วจนถึงปัจจุบัน ก็จะยังไม่มีใครสามารถให้คำนิยามคำว่า "อาชญากรรมคอมพิวเตอร์" ได้อย่างชัดเจน และครอบคลุมก็ตาม แต่ที่สามารถเห็นประจักษ์อย่างชัดเจนก็คือพฤติกรรมที่เป็นการกระทำความผิดอันเกี่ยวกับ-คอมพิวเตอร์ ซึ่งอาชญากรรมคอมพิวเตอร์ อาจแบ่งประเภทของการกระทำความผิดตาม-กระบวนการ ขั้นตอนของการกระทำโดยอาจแบ่งออกได้เป็น 3 ประเภท ดังนี้

1) การก่ออาชญากรรมคอมพิวเตอร์ในขั้นของกระบวนการนำเข้า (Input Process) นั้น อาจทำได้โดยการ

(1) การสับเปลี่ยน Disk โดยหมายความรวมถึง Disk ทุกชนิด ไม่ว่าจะเป็น Hard Disk, Floppy Disk รวมทั้ง Disk ชนิดอื่น ๆ ด้วย ซึ่งถือเป็นการกระทำในทางกายภาพโดยการถอดออก ย้ายออก หรือการเคลื่อนที่เพื่อย้ายออก เป็นต้น

(2) การทำลายข้อมูล ไม่ว่าจะใน Hard Disk หรือสื่อบันทึกข้อมูลชนิดอื่นที่ใช้ร่วมกับคอมพิวเตอร์โดยไม่ชอบ

(3) การป้อนข้อมูลเท็จ ในกรณีที่เป็นผู้มีอำนาจหน้าที่อันอาจเข้าถึงเครื่อง-คอมพิวเตอร์นั้น ๆ ได้ หรือแม้แต่ผู้ที่ไม่มีอำนาจเข้าถึงก็ตาม แต่ได้กระทำการอันมิชอบในขณะที่ตนเองอาจเข้าถึงได้

(4) การลักข้อมูลข่าวสาร ไม่ว่าโดยการกระทำด้วยวิธีการอย่างใด ๆ ให้ได้ไป ซึ่งข้อมูลอันตนเองไม่มีอำนาจ หรือเข้าถึงโดยไม่ชอบ

(5) การลักใช้บริการหรือเข้าไปใช้โดยไม่มีอำนาจ อาจกระทำโดยการเจาะระบบเข้าไป หรือใช้วิธีการอย่างใด ๆ เพื่อให้ได้มา ซึ่งรหัสผ่านเพื่อให้ตนเองเข้าไปใช้บริการได้โดยไม่ต้องลงทะเบียนเสียค่าใช้จ่าย

---

[3]ไพจิตร สวัสดิสาร, **การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายเกี่ยวกับคอมพิวเตอร์** (กรุงเทพมหานคร: โรงพิมพ์ชวนพิมพ์, 2550), หน้า 135.

2) การก่ออาชญากรรมคอมพิวเตอร์ในส่วนกระบวนการ Data Processing นั้น อาจกระทำความผิดได้โดย

(1) การทำลายข้อมูล และระบบโดยใช้ไวรัส (Computer Sabotage)

(2) การทำลายข้อมูล และโปรแกรม (Damage to Data and Program)

(3) การเปลี่ยนแปลงข้อมูล และโปรแกรม (Alteration of Data and Program)

3) กระบวนการนำออก (Output Process) โดยอาจกระทำความผิดได้ดังนี้

(1) การขโมยขยะ (Swaging) หมายถึง ขยะหรือข้อมูลที่ไม่ใช้แล้ว แต่ยังไม่ได้ทำลายนั่นเอง การขโมยขยะถือเป็นความผิด ถ้าขยะที่ถูกขโมยไปนั้นอาจทำให้เจ้าของต้องเสียหายอย่างใด ๆ อีกทั้งเจ้าของอาจจะยังมิได้มีเจตนาสละการครอบครอง

(2) การขโมยข้อมูลที่ถูกปริ้นส์ออกมาเป็นเอกสาร[4]

แต่อย่างไรก็ตามการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ บางประเภทนั้นอาจจะไม่เรียกว่าเป็นการก่ออาชญากรรม ทั้งนี้เนื่องจากมีความแตกต่างกันทางด้านรูปแบบของการกระทำความผิด ความรุนแรงของการกระทำความผิด และความเสียหายที่เกิดมีขึ้น กล่าวคือ อาชญากรรมคอมพิวเตอร์เป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มีโทษทางอาญา และมีบทลงโทษทางอาญาที่กระทบต่อเนื้อตัว ร่างกาย สิทธิและเสรีภาพอย่างร้ายแรงมาก ประกอบกับความเสียหายที่เกิดขึ้นจากการก่ออาชญากรรมนั้น สามารถสร้างความความเสียหายที่มีมูลค่ามหาศาล เป็นการกระทำความผิดที่กระทบต่อระบบเศรษฐกิจ สังคมและความมั่นคงของบุคคล องค์กร ของรัฐหรือประเทศ ซึ่งความเสียหายที่เกิดมีขึ้นนั้นสามารถเทียบได้กับอาชญากรรมทางเศรษฐกิจ หรือ “White Collar Crimes” ซึ่งเป็นอาชญากรรมเชิ้ตขาว ที่ผู้กระทำความผิดไม่ใช่คนตัวใหญ่ใจเหี้ยม หน้าตาโหด หรือมีลักษณะโจรใจร้าย แต่กลับกลายเป็นกลุ่มคนที่หน้าที่การงานสูง แต่งตัวดี และมีความรู้ความสามารถ ดังตัวอย่างเช่น

---

[4]ถนอมนวล สีหะกุลัง, **กฎหมายเทคโนโลยีสารสนเทศ และการกระทำความผิดเกี่ยวกับคอมพิวเตอร์** [Online], available URL: www.kmitl.ac.th/agritech/nutthakorn /04093009_2204/isweb/Lesson%208.doc, 2552 (สิงหาคม, 31).

อาชญากรรมเศรษฐกิจ อาทิเช่น ความผิดเกี่ยวกับการปลอมแปลงเงินตรา การปั่นหุ้น และความผิดเกี่ยวกับภาษีอากร เป็นต้น

การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในบางลักษณะของการกระทำนั้น ยังไม่มีความร้ายแรงถึงขนาดที่จะเรียกว่าเป็นอาชญากรรมทางคอมพิวเตอร์ ทั้งนี้เพราะความเสียหายแห่งการกระทำความผิดที่เกิดมีขึ้นนั้นจะยังไม่ร้ายแรง หรือไม่รุนแรงเท่ากับการก่ออาชญากรรม ดังนั้นเมื่อพิจารณาแล้ว อาชญากรรมคอมพิวเตอร์ กับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงมีความแตกต่างกันในแง่ของเรื่องความเสียหายและความร้ายแรงหรือรุนแรงที่เกิดมีขึ้นนั่นเอง

1.2 ความหมายของอาชญากรรมอินเทอร์เน็ต

อินเทอร์เน็ต (Internet) มาจากคำว่า Interconnected Networks เป็นระบบการสื่อสารที่เกิดขึ้นจากเครือข่ายคอมพิวเตอร์ของรัฐบาลประเทศสหรัฐอเมริกา ที่เรียกว่า ARPANET ซึ่งเกิดขึ้นในปี ค.ศ. 1969 (ในปัจจุบันเลิกใช้แล้ว) โดยการที่รัฐบาล และมหาวิทยาลัยต่าง ๆ ในประเทศสหรัฐอเมริกาได้ใช้เครือข่ายประเภทนี้ เป็นเหตุทำให้เกิดการสร้างเครือข่ายคอมพิวเตอร์ประเภทอื่นขึ้นตามมา และมีการคิดค้นการเชื่อมต่อเครือข่ายเหล่านั้นเข้าด้วยกันโดยผ่านทางสายโทรศัพท์ในประเทศ และระหว่างประเทศ ต่อมาเครือข่ายต่าง ๆ เหล่านี้ได้รับการพัฒนา และขยายตัวเพิ่มมากขึ้นทั้งในแง่ของขนาดและความสลับซับซ้อน จนในที่สุดแล้วกลายมาเป็นเครือข่ายอินเทอร์เน็ต[5] ซึ่งเป็นโครงสร้างพื้นฐานทางข้อมูลข่าวสารอันประกอบขึ้นจากเครือข่ายคอมพิวเตอร์ที่มาเชื่อมต่อกันเป็นจำนวนมากจากทั่วโลก ถือเป็นเครือข่ายแห่งเครือข่าย โดยจะอาศัยภาษาคอมพิวเตอร์กลางร่วมกัน มีมาตรฐานกลางในการรับส่งข้อมูลร่วมกัน ทำให้-

---

[5]พรรณสุวัชร รติพงศ์สิทธิ์, "อาชญากรรมทางคอมพิวเตอร์: ศึกษาวิเคราะห์หลักเกณฑ์ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...." (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยรามคำแหง, 2550), หน้า 23.

คอมพิวเตอร์ต่าง ๆ ในเครือข่ายสามารถสื่อสารกันได้[6] ทำให้เกิดการแบ่งปันข้อมูลข่าวสารระหว่างกันได้อย่างรวดเร็ว และนับว่าเป็นระบบทางด่วนข้อมูลข่าวสารสารสนเทศที่มีประสิทธิภาพสูงที่สุดในโลก

การเชื่อมต่ออินเทอร์เน็ตเพื่อใช้งานนั้น สามารถกระทำได้โดยการเชื่อมต่อผ่านทางผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider--ISP) ซึ่งเป็นหน่วยงานที่ให้บริการเชื่อมต่อเครื่องคอมพิวเตอร์ส่วนบุคคล หรือเครือข่ายคอมพิวเตอร์ของหน่วยงานต่าง ๆ เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก โดย ISP จะอนุญาตให้เฉพาะผู้ที่สมัครเป็นสมาชิกของหน่วยงานของตนเองเท่านั้นสามารถนำระบบของตนเข้าไปเชื่อมต่อได้ กล่าวคือ ISP ก็เปรียบเสมือนช่องทางผ่านเข้าสู่ระบบอินเทอร์เน็ต ซึ่งหลังจากที่ได้เชื่อมต่อเข้ากับระบบอินเทอร์เน็ตแล้ว ผู้ใช้บริการก็สามารถเข้าไปยังส่วนใด ๆ ก็ได้ในระบบอินเทอร์เน็ต

การเชื่อมต่ออินเทอร์เน็ตผ่านทางผู้ให้บริการนั้นสามารถแบ่งลักษณะการเชื่อมต่อออกเป็น 2 ประเภทตามความต้องการใช้งานดังนี้

1) การเชื่อมต่อแบบองค์กร อาทิเช่น สถาบันการศึกษา หน่วยงานของรัฐหรือบริษัทเอกชน เป็นต้น กล่าวคือเป็นองค์กรที่มีการจัดตั้งระบบเครือข่ายใช้งานภายในองค์กรอยู่แล้ว โดยจะสามารถนำเครื่องแม่ข่ายขององค์กร (Server) เข้าเชื่อมต่อกับผู้ให้บริการเพื่อเชื่อมโยง เข้าสู่ระบบอินเทอร์เน็ตได้เลย

2) การเชื่อมต่อส่วนบุคคล โดยเป็นการเชื่อมต่อของบุคคลธรรมดาทั่วไปซึ่งสามารถขอเชื่อมต่อเข้าสู่ระบบอินเทอร์เน็ตได้โดยใช้เครื่องคอมพิวเตอร์ที่ใช้อยู่ อาจจะเป็นที่บ้านหรือที่ทำงาน โดยเชื่อมต่อผ่านทางสายโทรศัพท์ หรือผ่านอุปกรณ์ที่เรียกว่าโมเดม (Modem) ซึ่งค่าใช้จ่ายไม่สูงมากนัก การเชื่อมต่อประเภทนี้มักถูกเรียกว่าเป็นการเชื่อมต่อแบบ Dial-Up แต่การเชื่อมต่อจะสามารถใช้งานได้ผู้ใช้บริการจะต้องมีการสมัครเป็นสมาชิกของผู้ให้บริการประเภทนี้ก่อนเพื่อขอเชื่อมต่อ

---

[6]พิรงรอง รามสูตรณะนันทน์ และนิธิมา คณานิธินันท์, **รายงานวิจัยเรื่องการกำกับดูแลเนื้อหาอินเทอร์เน็ต** (กรุงเทพมหานคร: สำนักงานกองทุนสนับสนุนการวิจัย, 2547), หน้า 2.

ดังจะเห็นได้ว่า การเข้าใช้งานเครือข่ายอินเทอร์เน็ตนั้นสามารถเข้าใช้งานได้โดยง่าย ผ่านทางช่องทางของผู้ให้บริการต่าง ๆ ไม่ว่าจะเป็นผู้ให้บริการที่เป็นหน่วยงานของรัฐ หรือผู้ให้บริการเชิงพาณิชย์ ทำให้เกิดการใช้งานอินเทอร์เน็ตทั่วโลกเป็นจำนวนมาก โดยลักษณะของการใช้งานที่มีความแตกต่างกัน อาทิเช่น การติดต่อสื่อสาร การศึกษาเรียนรู้ การประกอบธุรกิจ ประกอบกิจการ เป็นต้น และด้วยภายใต้ของการใช้บริการผ่านเครือข่ายอินเทอร์เน็ตนี้เอง ทำให้เกิดมีผู้ไม่ประสงค์ดีที่อาศัยช่องทาง หรือช่องว่างของปัจจัยแวดล้อมของเครือข่ายอินเทอร์เน็ต ก่อเป็นการกระทำความผิดบนเครือข่ายอินเทอร์เน็ตขึ้น ซึ่งเรียกว่าเป็น “อาชญากรรมอินเทอร์เน็ต”

“อาชญากรรมอินเทอร์เน็ต” หรือ “อาชญากรรมไซเบอร์” นั้นเป็นอาชญากรรมคอมพิวเตอร์ประเภทหนึ่ง แต่มีความแตกต่างกันตรงที่ อาชญากรรมอินเทอร์เน็ตเป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือระบบคอมพิวเตอร์โดยอาศัยช่องทางการติดต่อสื่อสารผ่านการให้บริการเครือข่ายอินเทอร์เน็ต ด้วยเหตุนี้ทำให้การกระทำความผิดขยายเป็นวงกว้าง สะดวกรวดเร็ว การกระทำความผิดเป็นการกระทำที่มีความสลับซับซ้อนมากยิ่งขึ้น และที่สำคัญอย่างยิ่งคือ การสามารถติดตามหาตัวผู้กระทำความผิดได้อย่างยากลำบากมาก โดยแรกเริ่มนั้นได้เกิดมีขึ้น และเติบโตมาพร้อม ๆ กับการให้บริการพาณิชย์อิเล็กทรอนิกส์ ซึ่งเป็นการทำธุรกรรมทางเศรษฐกิจผ่านสื่ออิเล็กทรอนิกส์ เช่น การซื้อขายสินค้าและบริหาร การโฆษณาสินค้า การโอนเงินทางอิเล็กทรอนิกส์ ทั้งนี้ด้วยเหตุที่เป็นบริการที่มีจำนวนของผู้เข้าใช้บริการจำนวนมาก เพราะสะดวกสบาย ประหยัดเวลา และประหยัดค่าใช้จ่ายให้แก่ผู้ใช้บริการ เป็นต้น

นอกเสียจากการกระทำความผิดดังกล่าวแล้วจวบจนถึงปัจจุบัน การกระทำความผิดผ่านเครือข่ายอินเทอร์เน็ตนั้นไม่ได้จำกัดแต่เพียงเฉพาะพาณิชย์อิเล็กทรอนิกส์เท่านั้น แต่ได้มีการคิดค้น และเปลี่ยนแปลง ปรับปรุงรูปแบบ วิธีการในการก่อความผิดมากขึ้น อาทิเช่น การขโมยข้อมูลทางอินเทอร์เน็ต การเผยแพร่ภาพ เสียง อันมีลักษณะลามกอนาจาร การฟอกเงิน การขโมยรหัสบัตรเครดิต รวมไปจนถึงการกระทำความผิดบางประเภท ซึ่งแต่เดิมจะเป็นการกระทำความผิดแบบที่ใช้แรงทางกายภาพโดยทั่วไป เพียงแต่เปลี่ยนแปลงรูปแบบของการกระทำความผิด จากเดิมผู้กระทำความผิดจะใช้แรงทางกายภาพก่อความผิด เปลี่ยนมาเป็นอาศัยเครือข่ายอินเทอร์เน็ต และความรู้

ความสามารถทางอินเทอร์เน็ตก่อเป็นความผิดขึ้น เช่นความผิดฐานหมิ่นประมาท ความผิดฐานลักทรัพย์ เป็นต้น

2. รูปแบบของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จากที่ผู้ศึกษาได้อธิบายแล้วว่าการกระทำความผิดเกี่ยวกับคอมพิวเตอร์บางประเภทนั้นอาจไม่ได้หมายความรวมถึงเป็นการก่ออาชญากรรมคอมพิวเตอร์ด้วยเหตุที่การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในบางลักษณะยังไม่มีความร้ายแรงถึงขนาดที่จะเรียกว่าเป็นอาชญากรรมทางคอมพิวเตอร์ เพราะความเสียหายแห่งการกระทำความผิดที่เกิดมีขึ้นนั้นจะยังไม่มีความร้ายแรง หรือไม่รุนแรงเท่าเทียมกับการก่ออาชญากรรมนั้นเอง

การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบันนั้นจะยิ่งทวีความรุนแรงมากขึ้นเรื่อย ๆ อย่างต่อเนื่อง ประกอบกับทั้งเกิดมีผู้กระทำความผิดที่มีอายุยังน้อย และมีความรู้ความสามารถ ทั้งนี้อาจกระทำความผิดลงด้วยความรู้เท่าไม่ถึงการณ์ หรือด้วยความที่อยากลองวิชา แต่อย่างไรก็ตามเมื่อเกิดเป็นการกระทำความผิดแล้วนั้นผลเสียหายย่อมเกิดมีขึ้นตามมา เกิดมีผู้ได้รับความเสียหายจากการกระทำความผิดของบุคคลเหล่านั้นเป็นจำนวนมากเช่นกัน โดยรูปแบบของการกระทำความผิดที่มักเกิดมีขึ้นในปัจจุบันนั้นได้แก่

2.1 การกระทำความผิดฐานหมิ่นประมาท

การกระทำความผิดฐานหมิ่นประมาทนั้น เป็นการกระทำโดยการใส่ความผู้อื่นไม่ว่าจะด้วยวิธีการใด ๆ อาทิเช่น การพูด การเขียน การพิมพ์ข้อความ หรือการแสดงกริยาต่าง ๆ โดยการใส่ความดังกล่าวนั้น ต้องเป็นใส่ความผู้อื่นและการกระทำดังกล่าวทำให้บุคคลที่สามรับทราบ ซึ่งเป็นเหตุทำให้ผู้ถูกใส่ความนั้น ได้รับความเสียหาย ความอับอาย โดยในอดีตนั้นการกระทำความผิดประเภทนี้สามารถกระทำได้หลายช่องทาง อาทิเช่น การหมิ่นประมาททางจดหมายส่งทางไปรษณีย์ การหมิ่นประมาทโดยกล่าว หรือไขข่าวแพร่หลายต่อบุคคลอื่น เป็นต้น ซึ่งการกระทำความผิด

ดังกล่าวแม้จะสามารถกระทำได้หลายช่องทาง แต่อย่างไรก็ตามผู้กระทำความผิดนั้นก็จะไม่สามารถปิดบังตัวตนของตนเองได้ หรืออาจจะสามารถกระทำได้ แต่เป็นการยากมาก เป็นเหตุทำให้ผู้เสียหายสามารถทราบถึงผู้กระทำความผิดได้โดยง่ายดาย

แต่ปัจจุบันเนื่องจากการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ตนั้น ผู้ใช้บริการสามารถปิดบังตัวตนที่แท้จริงได้ ซึ่งเป็นเหตุทำให้ผู้ใช้บริการอินเทอร์เน็ตสามารถต่อด่าทอ กล่าวหากัน รวมไปจนถึงกระทั่งการนำภาพ หรือเรื่องส่วนตัวของบุคคลอื่นมาเผยแพร่ การกระทำดังกล่าวเป็นเหตุนำมาซึ่งความเสียหายต่อชื่อเสียงเกียรติยศ โดยไม่ต้องเกรงว่าตนจะถูกจับได้ เป็นเหตุให้มีสถิติการนำคดีหมิ่นประมาทนี้ขึ้นสู่การพิจารณาในชั้นศาลเป็นจำนวนมากกว่าในอดีต ทั้งนี้ไม่ว่าโจทก์จะรู้ถึงตัวผู้กระทำความผิดหรือไม่ก็ตาม และนอกจากนั้นแล้วปัจจุบันยังปรากฏข้อเท็จจริงว่าคดีหมิ่นประมาทจำนวนไม่น้อยถูกใช้เป็นเครื่องมือทางการเมืองของนักการเมืองโดยมีการฟ้องร้องซึ่งกันและกัน หรือมีการฟ้องร้องสื่อมวลชน ไม่ว่าจะเป็นการฟ้องเป็นคดีอาญา หรือฟ้องเป็นคดีแพ่งเพื่อเรียกร้องค่าสินไหมทดแทนจำนวนมหาศาล เป็นต้น

2.2 การกระทำความผิดฐานฉ้อโกง

การฉ้อโกงเป็นการกระทำโดยทุจริตใช้เล่ห์เหลี่ยมหลอกลวงผู้อื่น ด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริง โดยมุ่งหวังเพื่อให้ตนเองได้รับผลประโยชน์อย่างใดอย่างหนึ่งจากการหลอกลวงนั้น ๆ โดยการหลอกลวงเช่นว่านี้เป็นการกระทำผ่านช่องทางการให้บริการเครือข่ายอินเทอร์เน็ต อาทิเช่น

1) การประมูลสินค้าทางอินเทอร์เน็ต

เป็นวิธีการซื้อขายสินค้าที่ได้รับความนิยมมาก และเป็นช่องทางการติดต่อซื้อขายสินค้าที่สะดวกและรวดเร็ว โดยมีวิธีการคือผู้ซื้อที่สนใจจะเข้าร่วมการประมูลมักต้องลงทะเบียนเป็นสมาชิกของเว็บไซต์นั้น ๆ ซึ่งโดยทั่วไปจะไม่เสียค่าใช้จ่ายใด ๆ หลังจากนั้นจะได้รับหมายเลขสมาชิก และรหัสผ่าน ผู้ซื้อจะต้องเสนอราคาซื้อแข่งขันกับผู้ซื้อรายอื่น เมื่อเสร็จสิ้นการประมูลถือว่ามีการทำสัญญาซื้อขายระหว่างผู้ประมูลและผู้เสนอขาย โดยจะมีการส่งข้อความทางอีเมล แจ้งให้ผู้ซื้อ และผู้ขายทราบผลการ-ประมูล และแจ้งรายละเอียดที่จะติดต่อกันได้ เพื่อให้ทั้งฝ่ายผู้ซื้อ และผู้ขายติดต่อกัน

ในเรื่องการชำระเงินและการส่งมอบสินค้า วิธีการหลอกลวงจะมีหลายรูปแบบ เช่น ผู้ขายไม่ส่งมอบสินค้าที่ผู้ซื้อประมูลได้ เพราะไม่มีสินค้าอยู่จริง หรือการหลอกลวงโดยการปั่นราคาซื้อขาย โดยผู้ขายหรือบุคคลที่เกี่ยวข้องกับผู้ขายจะเข้าเสนอราคาเพื่อประมูลสินค้าของตน เพื่อให้สินค้ามีราคาสูงขึ้น ทำให้ผู้ซื้อต้องซื้อสินค้าในราคาที่สูงเกินจริง เป็นต้น

2) การหลอกลวงโดยใช้การตลาดหรือการขายตรง

การหลอกลวงในลักษณะนี้จะเป็นการกระทำโดยมีการชักชวนให้บุคคลทั่วไปเข้าร่วมเป็นสมาชิกในเครือข่ายธุรกิจ โดยการกล่าวอ้างว่าผู้ขายจะได้รับสิทธิในการจำหน่ายสินค้าหลายชนิด และได้รับผลประโยชน์จากการขายสินค้าหรือชักชวนบุคคลอื่นเข้ามาเป็นตัวแทนขายตรงเป็นทอด ๆ ทำให้ผู้ที่ได้รับประโยชน์จริงมีจำนวนน้อยราย การหลอกลวงดังกล่าวทำให้ผู้ที่เข้าร่วมเครือข่ายจะต้องชำระค่าสมาชิกจำนวนหนึ่ง แต่จะไม่มีรายได้ประจำแต่อย่างใด รายได้ของผู้ที่เข้าร่วมเครือข่ายจึงไม่แน่นอน และมักจะไม่ได้รับผลประโยชน์ตามที่ผู้หลอกลวงกล่าวอ้าง เพราะไม่สามารถขายสินค้าได้ตามเป้าหมายนั่นเอง

2.3 การกระทำความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร

การกระทำความผิดประเภทนี้ มีลักษณะของการกระทำความผิดเช่นเดียวกับประมวลกฎหมายอาญา แต่มีความแตกต่างกันตรงที่รูปแบบ และช่องทางในการกระทำความผิดที่เป็นการกระทำความผิดโดยอาศัยช่องทางการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ตนั้นเอง การกระทำความผิดประเภทนี้ อาทิเช่น การที่มีการเผยแพร่คลิปบทความ วีดิทัศน์ อันปรากฏเป็นข้อความที่หมิ่นประมาท ดูหมิ่นต่อพระมหากษัตริย์ พระราชินี รัชทายาท หรือผู้สำเร็จราชการแทนพระองค์ การหมิ่นสถาบันฯ การก่อการร้ายล้มล้างหรือเปลี่ยนแปลงรัฐธรรมนูญ อำนาจนิติบัญญัติ อำนาจบริหาร รวมไปจนถึงอำนาจตุลาการ ซึ่งโดยส่วนใหญ่แล้วผู้กระทำความผิดจะใช้ช่องทางของการให้บริการบทเครือข่ายอินเทอร์เน็ตแบบสังคมออนไลน์ (Social Network) แบบกระดานสนทนาออนไลน์ในเว็บบอร์ด อาทิเช่น Facebook หรือ Twitter เป็นต้น

2.4 การกระทำความผิดเกี่ยวกับการล่อลวงทางอินเทอร์เน็ต

ปัญหาการล่อลวง หรือหลอกลวงผ่านทางอินเทอร์เน็ตนั้น เป็นผลพวงมาจากการเกิดมีขึ้นของสังคมออนไลน์ประเภทเว็บบล็อก ไดอารี่ออนไลน์ เว็บไซต์หาคู่ เว็บไซต์ที่ให้บริการห้องสนทนา หรือโปรแกรมสนทนา โดยผู้ใช้บริการทั้งสองฝ่ายจะมีการพูดคุยสนทนากันผ่านระบบเครือข่ายอินเทอร์เน็ต การให้บริการประเภทดังกล่าวนี้ หากนำมาใช้ไม่ถูกต้องแล้วก็จะเกิดเป็นโทษมหันต์ต่อผู้ใช้เป็นอย่างมาก โดยเฉพาะกับเด็กหรือเยาวชนซึ่งก็ถือเป็นการเปิดกว้างให้กับเหล่าอาชญากรสามารถกระทำการล่วงละเมิดทางเพศต่อเด็กและเยาวชนอย่างง่ายดาย โดยอาชญากรกลุ่มนี้จะอาศัยความอยากรู้ ความอยากได้ซึ่งทรัพย์สิน เงินทอง ความเหงา และแรงกระตุ้นทางเพศเป็นอาวุธในการล่อลวงเหยื่อให้ไปติดกับ จนกระทั่งทำให้เกิดความรู้สึกอยากพบอยากเจอกับเพื่อนใหม่ การนัดหมายเจอกันตามสถานที่ต่าง ๆ และตามมาด้วยการลงเอยจากการกระทำในสิ่งที่ไม่ถูกไม่ควร ไม่ว่าจะเป็นการกระทำอนาจาร การกระทำชำเรา และอาจถูกล่อลวงจากคู่สนทนาเพื่อพาไปข่มขืน หรือขืนใจ และท้ายที่สุดแล้วผู้เสียหายที่ตกเป็นเหยื่อเหล่านั้นก็จะไม่กล้าที่จะดำเนินคดีเอาผิดกับอาชญากรดังกล่าว เพราะด้วยความที่เป็นเด็กหรือเยาวชน และเกรงว่าจะเกิดเป็นความอับอาย ทำให้อาชญากรนั้นยังคงลอยนวล และก่อให้เกิดเป็นการกระทำความผิดซ้ำขึ้นในสังคมได้ ด้วยวิธีการและรูปแบบของการกระทำความผิดแบบเดิม

3. ประเภทของผู้ให้บริการ การติดต่อสื่อสาร ผ่านเครือข่ายอินเทอร์เน็ต

เมื่อเกิดการพัฒนาทางด้านเทคโนโลยีสารสนเทศมากขึ้น การพัฒนาทางด้านการติดต่อสื่อสารก็เพิ่มมากขึ้นเช่นกัน เกิดเป็นการแข่งขันกันทางการค้า การประกอบ-ธุรกิจ เป็นเหตุทำให้ผู้ให้บริการในการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ตนั้นมีจำนวน เพิ่มมากขึ้น และมีการให้บริการที่มีความแตกต่าง มีความหลากหลายกัน ทั้งนี้ขึ้นอยู่กับ รูปแบบ ประเภทและวัตถุประสงค์ของการให้บริการนั้น ๆ ซึ่งเริ่มตั้งแต่ผู้ให้บริการอินเทอร์เน็ต ที่ให้บริการให้เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนบุคคล

(กรณีบุคคลธรรมดา) หรือเครือข่ายคอมพิวเตอร์ (กรณีองค์กร หรือหน่วยงาน) เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก เรื่อยไปจนถึงผู้ให้บริการการเข้าใช้หรือเข้าถึงอินเทอร์เน็ตผ่านซอฟต์แวร์ หรือผ่านแอพพลิเคชั่น ต่าง ๆ ด้วย

3.1 ผู้ประกอบกิจการโทรคมนาคม

ผู้ให้บริการประเภทนี้ เป็นผู้ให้บริการอันดับแรกในการเชื่อมต่อเข้าใช้บริการเครือข่ายอินเทอร์เน็ตโดยจะหมายถึงผู้ให้บริการโครงข่ายโทรคมนาคม หรือสัญญาณ-โทรคมนาคม คือผู้ให้บริการคู่สายโทรศัพท์ และวงจรเช่าที่ใช้สื่อสารในเครือข่าย โดยปกติแล้วการบริการหลัก ๆ ของผู้ให้บริการกลุ่มนี้ คงมีเพียงการให้บริการจัดหาคู่สายโทรศัพท์สำหรับการเชื่อมต่อเครือข่ายอินเทอร์เน็ตแบบธรรมดา หรือบริการวงจรเช่า ให้กับผู้ใช้บริการที่ติดตั้ง Host อินเทอร์เน็ตเป็นของตนเองเท่านั้น หาได้มีบริการเสริมอื่นใดไม่ ซึ่งได้แก่

1) ผู้ให้บริการโทรศัพท์พื้นฐาน (Fixed Line Service Provider) คือ ผู้ให้บริการโครงข่ายโทรศัพท์ประเภทพื้นฐานโดยทั่วไป มีทั้งเป็นแบบมีสายสัญญาณและแบบไร้สาย สำหรับบริการโทรศัพท์บ้านก็มีโครงข่ายโทรศัพท์พื้นฐานซึ่งจะมีผู้ให้บริการอย่างเช่น บริษัท ทีโอที จำกัด (มหาชน) บริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัท ทีทีแอนด์ที จำกัด (มหาชน) เป็นต้น การนี้ผู้ให้บริการโทรศัพท์พื้นฐานประเภทดังกล่าวจะสามารถเปิดให้บริการโครงข่ายได้ จะต้องได้รับใบอนุญาตจากสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการ-โทรคมนาคมแห่งชาติ (กสทช.) ซึ่งเป็นหน่วยงานในการกำกับดูแลผู้ที่จะประกอบ-กิจการโทรคมนาคม ต้องกระทำการขอรับใบอนุญาตการให้บริการดังกล่าวก่อนการให้บริการ

2) ผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile Service Provider) เป็นการติดต่อสื่อสารผ่านมือถือ หรือโทรศัพท์เคลื่อนที่ ก็มีโครงข่ายที่ให้บริการทางด้านโทรศัพท์เคลื่อนที่เช่น GSM, GPRS, EDGE, HSPA, CDMA 2000 EVDO ของผู้ให้บริการเช่น AIS, CAT TELECOM, DTAC, HUTCH, THAI MOBILE, TRUE MOVE เป็นต้น โดยที่ผ่านมาโครงข่ายประเภทต่าง ๆ เหล่านี้จะมีโครงสร้างแบบแนวตั้ง

คือแต่ละโครงข่ายจะมีทั้งโครงสร้าง และบริการแยกออกจากกันเป็นเอกเทศ ดังนั้น บริการต่าง ๆ บนแต่ละโครงข่ายจึงไม่สามารถใช้ร่วมกันได้ ผลที่ตามมาสำหรับผู้ใช้บริการก็คือ ผู้ใช้บริการต้องสมัครใช้บริการสำหรับการใช้บริการโครงข่ายแต่ละ-ประเภทแยกกันไป จึงทำให้คนคนเดียว ต้องมีทั้งเบอร์โทรศัพท์บ้าน เบอร์มือถือ ชื่อผู้ใช้สำหรับต่อเข้าอินเทอร์เน็ต อีกทั้งบริการเสริมก็ต้องสมัครแยกกันโดยสิ้นเชิง ผู้ให้บริการประเภทนี้ก็ต้องได้รับใบอนุญาตจาก สำนักงานคณะกรรมการกิจการกระจายเสียง-กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) เช่นกัน

3.2 ผู้ให้บริการให้เช่าพื้นที่เพื่อเปิดให้บริการเว็บไซต์

ผู้ให้บริการประเภทนี้เป็นกลุ่มผู้ให้บริการที่ได้รับอนุญาตจากรัฐให้สามารถติดตั้งเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ (Computer Server) ประเภทต่าง ๆ เป็นของตนเองได้ ทั้งนี้เพื่อไว้เปิดบริการให้แก่ บุคคลหรือนิติบุคคลใดที่ประสงค์เผยแพร่ข้อมูลข่าวสาร หรือให้บริการเว็บไซต์ในเครือข่ายอินเทอร์เน็ตได้เช่าพื้นที่ในคอมพิวเตอร์เซิร์ฟเวอร์ของผู้ให้บริการประเภทนี้ อาทิเช่น การที่ผู้ให้บริการ ให้บุคคลหรือนิติบุคคลเช่าพื้นที่บนเครือข่ายอินเทอร์เน็ตในการนำเว็บไซต์ของตนมาฝาก เพื่อให้เว็บไซต์ที่นำมาฝากนั้นสามารถออนไลน์บนเครือข่ายอินเทอร์เน็ตได้ เป็นการให้บริการแบบเบ็ดเสร็จ โดยเพียงแต่บุคคลผู้ประสงค์ใช้บริการดังกล่าวจะต้องทำการจดทะเบียน โดเมนเนม (Domain Name) และดำเนินการยื่นคำขอต่อผู้ให้บริการขอเช่า Web Hosting โดยชื่อ Domain Name นั้นจะต้องไม่มีการซ้ำกัน ซึ่งการให้บริการประเภทนี้นอกจากจะเป็นการให้บริการ Host และให้บริการเช่าพื้นที่ในเซิร์ฟเวอร์ของตนแล้ว ยังมีการให้บริการทางด้านอื่น ๆ ตามมาอีกด้วย อาทิเช่น การให้บริการทางด้าน Web Hosting ร่วมกับ Web Design หรือร่วมกับ Web Applications รวมถึงการให้บริการจดทะเบียน Domain Name Registration และอาจพ่วงมาด้วยการเป็นที่ปรึกษาทางด้าน It Consultant อีกด้วย ซึ่งก็ขึ้นอยู่กับการให้บริการของแต่ละผู้ประกอบการ ถือเป็นการให้บริการ ณ ที่เดียว ที่มีความคุ้มค่าและครบวงจรมาก

3.3 ผู้ให้บริการเข้าใช้คอมพิวเตอร์เพื่อเชื่อมต่ออินเทอร์เน็ต

ผู้ให้บริการประเภทนี้เป็นผู้ให้บริการเพื่อเข้าถึง หรือเข้าใช้การใช้งานอินเทอร์เน็ต โดยมากผู้ให้บริการประเภทนี้จะจดทะเบียนประกอบการ หรือประกอบกิจการ และจะมีสถานะเป็นนิติบุคคล โดยบางประเภทอาจจดทะเบียนประกอบการประเภทอื่น แต่มีการให้บริการการเข้าใช้งานอินเทอร์เน็ตด้วย แต่บางประเภทอาจเปิดให้บริการร้านอินเทอร์เน็ตโดยตรงได้ อาทิเช่น ผู้ประกอบการห้องเช่า โรงแรม ร้านอาหารและเครื่องดื่ม ร้านอินเทอร์เน็ตคาเฟ่ ร้านเกมส์ออนไลน์ รวมไปถึงผู้ให้บริการที่มีลักษณะเป็นองค์กร หน่วยงานราชการ บริษัทต่าง ๆ หรือแม้แต่สถาบันการศึกษา เป็นต้น

3.4 ผู้ให้บริการเว็บไซต์

ผู้ให้บริการเว็บไซต์ หรือผู้ให้บริการ WWW (World Wide Web) หรือเอกสารบนเว็บไซต์ โดยชื่อของ WWW เราจะเรียกว่าเป็นชื่อของ URL (The Uniform Resource Locators)[7] ของเว็บไซต์ โดยการให้บริการก็จะ ขึ้นอยู่กับผู้ให้บริการแต่ละประเภทว่ามีความประสงค์ให้การเปิดให้บริการทางด้านใด อาทิเช่น ทางด้านธุรกิจ-การค้า ไปรษณีย์อิเล็กทรอนิกส์ บริการโอนย้ายไฟล์ข้อมูล การสนทนา การสนทนาออนไลน์ การให้บริการทางด้านกระดานข้าวสารต่าง ๆ การให้บริการอินเทอร์เน็ตฟอรัม เว็บฟอรัม เมสเซจบอร์ด หรือบูลิตินบอร์ด เป็นต้น ซึ่งผู้ให้บริการเว็บไซต์นี้อาจเป็นผู้ให้บริการที่ให้บริการในการเข้าใช้เครือข่ายอินเทอร์เน็ต ประกอบกับการจัดทำเว็บไซต์ของตนเองเพื่อให้บริการเว็บไซต์ของตนเองได้ อาทิเช่น สถานศึกษาต่าง ๆ ที่เปิดบริการให้นิสิต นักศึกษาเข้าใช้บริการเครือข่ายอินเทอร์เน็ต และสถานศึกษานั้นยังมีการให้บริการเว็บไซต์ซึ่งเป็นของสถานศึกษาเอง กรณีดังกล่าวในเว็บไซต์ของสถานศึกษา

---

[7]URL ย่อมาจากคำว่า Uniform Resource Locator หมายถึงที่อยู่ประกอบด้วย

1. ชื่อโปรโตคอลที่ใช้ (Http ซึ่งย่อมาจาก HyperText Transfer Protocol)
2. ชื่อเครื่องคอมพิวเตอร์ และชื่อเครือข่ายย่อย (www/urlbookmarks)
3. ประเภทของเว็บไซต์ เช่น .com.

ก็จะมีการให้บริการเว็บบอร์ด หรือกระดานแนะแนวเพื่อให้นิสิต นักศึกษาได้เข้ามาสนทนาแลกเปลี่ยนความรู้ซึ่งกันและกันก็อาจเป็นได้ หรือในเว็บไซต์ของเนติบัณฑิตไทย มีการให้บริการเว็บไซต์ มีการให้บริการกระดานสนทนา ซึ่งกระดานสนทนานี้เราเรียกว่า Web Board และเว็บไซต์ของพันธุ์ทิพย์ที่เป็นเว็บไซต์ที่ให้บริการทางด้านเว็บบอร์ดในการสนทนาแลกเปลี่ยนความรู้ทางด้านต่าง ๆ โดยเฉพาะ โดยในเว็บไซต์พันธุ์ทิพย์นี้จะแบ่งเป็นห้องสนทนาออกเป็นหลาย ๆ ห้อง ซึ่งแต่ละห้องนั้นจะกำหนดหัวข้อในการสนทนาต่างกัน แต่บางห้องสนทนาก็เปิดให้บริการไว้ให้บุคคลเข้ามาสนทนาเพื่อแลกเปลี่ยนประสบการณ์ความรู้ทางด้านต่าง ๆ เป็นต้น

4. มาตรการป้องกันการกระทำความผิดและการรักษาความปลอดภัยของผู้ให้บริการ

สืบเนื่องจากมาตรการในการป้องกันและปราบปรามการกระทำความผิดบางประเภทจำเป็นต้องอาศัยความร่วมมือจากผู้ให้บริการ ดังนั้นแนวคิดในการกำหนดให้ผู้ให้บริการเข้ามามีส่วนร่วมในการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้น จึงเป็นวิธีการที่สังคมตระหนักถึงความจำเป็นยิ่งขึ้น ทั้งนี้เนื่องมาจากผู้ให้บริการนั้นถือเป็นบุคคลกลุ่มแรก ๆ ที่เข้าถึง รับรู้ และรับทราบถึงการกระทำความผิดผ่านระบบคอมพิวเตอร์ภายใต้การให้บริการของตนเอง อีกทั้งยังมีความสามารถที่จะกระทำการระงับ ยับยั้งต่อการกระทำความผิดที่อาจเกิดมีขึ้นได้ แต่ก็ต้องเป็นการกระทำที่บทบัญญัติของกฎหมายบัญญัติให้อำนาจไว้โดยชัดแจ้ง แต่อย่างไรก็ดี การสร้างมาตรการป้องกันการกระทำความผิดนั้น เป็นถือเป็นมาตรการหนึ่งที่ผู้ให้บริการสามารถกระทำได้ภายใต้การให้บริการของตนเอง โดยอาจกำหนดเป็นมาตรการหรือข้อกำหนดในการเข้าใช้บริการเครือข่ายอินเทอร์เน็ตแก่ผู้ใช้บริการ ดังนี้

4.1 การสร้างเครือข่ายส่วนตัวของผู้ให้บริการ

เครือข่ายส่วนตัว หรือเครือข่ายส่วนตัวเสมือน (Virtual Private Network) คือเครือข่ายที่มีการติดต่อ เชื่อมโยงโดยอาศัยเส้นทางจากเครือข่ายสาธารณะในการ-

เชื่อมต่อกัน แต่เครือข่ายชนิดนี้จะเชื่อมต่อกันได้ภายในองค์กรเดียวกันเท่านั้น การส่งข้อมูลที่เป็นเครือข่ายส่วนตัว (Private Network) จะมีการเข้ารหัสแพ็กเก็ตก่อนการส่งเพื่อสร้างความปลอดภัยให้กับข้อมูล และส่งข้อมูลไปตามเส้นทางที่สร้างขึ้นเสมือนอุโมงค์ที่อยู่ภายในเครือข่ายสาธารณะ (Public Network) หรือเครือข่ายอินเทอร์เน็ต เครือข่ายส่วนตัวเสมือน สามารถเชื่อมต่อเครือข่ายจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งได้ โดย VPN จะช่วยให้สามารถส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ โดยผ่านระบบอินเทอร์เน็ตทำให้ได้รับความสะดวก และรวดเร็วในการส่งข้อมูลในแต่ละครั้ง

เครือข่ายส่วนตัวถือเป็นระบบเครือข่ายที่จัดตั้งขึ้นไว้สำหรับหน่วยงานหรือองค์กรที่เป็นเจ้าของ และมีการใช้ทรัพยากรร่วมกัน ซึ่งทรัพยากรและการสื่อสารต่าง ๆ ที่มีอยู่ในเครือข่ายนั้นจะมีไว้เฉพาะบุคคลในองค์กรเท่านั้นที่มีสิทธิเข้ามาใช้บริการ ซึ่งบุคคลภายนอกเครือข่ายไม่สามารถเข้ามาร่วมใช้งานบนเครือข่ายขององค์กรได้ ถึงแม้จะมีการเชื่อมโยงกันระหว่างสาขาองค์กร หรือในเครือข่ายสาธารณะก็ตาม

ลักษณะการทำงานนั้น เป็นเครือข่ายที่มีเส้นทางการทำงานอยู่ในเครือข่าย-สาธารณะ ดังนั้นเรื่องความปลอดภัยของข้อมูลในเครือข่ายส่วนตัวจึงเป็นเรื่องที่ต้องคำนึงถึงเป็นอย่างมาก เครือข่ายส่วนตัวเสมือน จะมีการส่งข้อมูลในรูปแบบแพ็กเก็ตออกมาที่เครือข่ายอินเทอร์เน็ต โดยมีการเข้ารหัสข้อมูล (Data Encryption) ก่อนการส่งข้อมูลเพื่อสร้างความปลอดภัยให้กับข้อมูล และส่งข้อมูลผ่านอุโมงค์ ซึ่งจะถูกสร้างขึ้นจากจุดต้นทางไปยังปลายทางระหว่างผู้ให้บริการ VPN กับผู้ใช้บริการ การเข้ารหัสข้อมูลนี้เองเป็นการไม่อนุญาตให้บุคคลอื่นที่ไม่เกี่ยวข้องกับข้อมูลสามารถอ่านข้อมูลได้จนสามารถที่จะส่งไปถึงปลายทาง และมีเพียงผู้รับปลายทางเท่านั้นที่สามารถถอดรหัสข้อมูล และนำข้อมูลไปใช้ได้[8]

การรักษาความปลอดภัย (Security Service) ของ VPN นั้นมีหลายรูปแบบด้วยกัน โดยในส่วนนี้จะทำให้การทำงานของระบบ VPN นั้นมีความเป็นส่วนตัวมากขึ้น ได้แก่

---

[8]วิกิพีเดีย สารานุกรมเสรี, **เครือข่ายส่วนตัวเสมือน** [Online], available URL: http://th.wikipedia.org/wiki/เครือข่ายส่วนตัวเสมือน, 2552 (พฤศจิกายน, 28).

1) Authentication เป็นรูปแบบของระบบความปลอดภัยที่เป็นการยืนยันผู้ใช้งาน หรือยืนยันข้อมูลที่มีการรับส่งว่ามาจากด้านที่ได้รับอนุญาตอย่างแท้จริง เช่น ต้องให้ผู้ใช้งานจำเป็นต้องใส่ชื่อ และรหัสผ่านก่อนการใช้งานต่อไป

2) Confidentiality (Encryption) เป็นการเข้ารหัสข้อมูลก่อนการทำการส่งไปบนระบบอินเทอร์เน็ต และเมื่อข้อมูลถึงปลายทาง อุปกรณ์ปลายทางจะทำการถอดรหัสข้อมูลให้เป็นเหมือนเดิมเพื่อนำมาใช้งานต่อไป โดยวิธีการนี้เป็นการป้องกันข้อมูลจากการถูกโจรกรรมจากพวกแฮ็กเกอร์

3) Access Control (Firewall) ระบบ Firewall จะเป็นระบบรักษาความปลอดภัยที่มีหน้าที่ป้องกันมิให้ผู้ที่มิได้รับอนุญาตเข้ามาใช้งานในระบบเครือข่าย โดยระบบ Firewall มีให้เลือกด้วยกันหลายประเภท โดยสามารถแบ่งได้ 3 รูปแบบดังต่อไปนี้[9]

(1) Packet filtering Firewall

(2) Applications Gateway Firewall

(3) Stateful Inspection Firewall

4.2 การจัดให้มีการพิสูจน์ตัวตนของผู้ใช้งาน

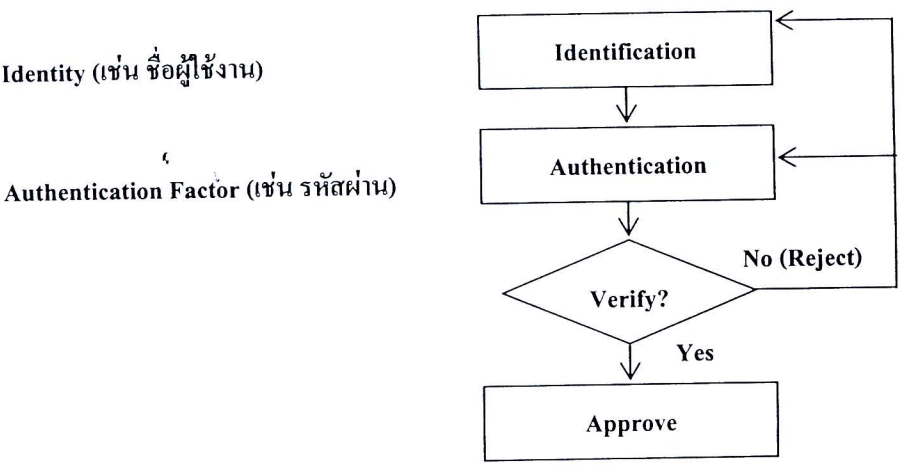
การจัดให้มีการพิสูจน์ทราบตัวตนของผู้ใช้งานและกำหนดเงื่อนไขแห่งการใช้งาน เป็นวิธีการหนึ่งที่ผู้ให้บริการสามารถนำมาใช้งานในระบบคอมพิวเตอร์ของตนเองได้ ทั้งนี้เพื่อเป็นการยืนยันตัวตนของผู้ใช้งานในการเข้าใช้ ซึ่งรูปแบบดังกล่าวนี้ยังเป็นการเอื้อประโยชน์แก่พนักงานเจ้าหน้าที่ในการตรวจสอบ หรือการพิสูจน์ตัวตนของผู้กระทำความผิด คือขั้นตอนการยืนยันความถูกต้องของหลักฐานที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

---

[9]อนวัช กาทอง, **ทำความรู้จัก VPN (Virtual Private Network)** [Online], available URL: http://www.lib.ubu.ac.th/weblib2009/wp-content/uploads/2009/11/ssl_vpn_ubu.pdf, 2552 (กันยายน, 1).

1) การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (User Name)

2) การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง



ภาพที่ 1 แผนผังแสดงกระบวนการการพิสูจน์ตัวตน

จากแผนผังแสดงกระบวนการพิสูจน์ตัวตน นั้นดังจะเห็นได้ว่าในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบ และในขั้นตอนต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้วถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูกปฏิเสธจากระบบ

การนี้หลักฐานที่ผู้ใช้นำมากล่าวอ้างที่เกี่ยวกับเรื่องของความปลอดภัยนั้นสามารถจำแนกได้ 2 ชนิด

1) Actual Identity คือหลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร

2) Electronic Identity คือหลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้ แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากกว่า 1 หลักฐาน อาทิเช่น บัญชีชื่อผู้ใช้ เป็นต้น

รูปแบบของการพิสูจน์ตัวตน (Authentication Mechanisms) เพื่อทำให้ทราบตัวตนของผู้ใช้งานนั้น สามารถแบ่งออกได้เป็น 3 ประเภทคือ

1) สิ่งที่คุณมี (Possession Factor) เช่น กุญแจหรือเครดิตการ์ด

2) สิ่งที่คุณรู้ (Knowledge Factor) เช่น รหัสผ่าน (Passwords) หรือการใช้ชุดตัวเลขหรือตัวอักษรที่กำหนดขึ้นเป็นรหัสลับเฉพาะส่วนบุคคล (PIN Code) เป็นต้น

3) สิ่งที่คุณเป็น (Biometric Factor) เช่น ลายนิ้วมือรูปแบบเรตินา (Retinal Patterns) หรือใช้รูปแบบเสียง (Voice Patterns) เป็นต้น

รูปแบบการพิสูจน์ตัวตนนั้นจะขึ้นอยู่กับระบบ และวิธีการที่ผู้ใช้นำมาใช้โดยการนำมาใช้ลักษณะอย่างใดอย่างหนึ่ง (Single Factor Authentication) นั้นจะมีข้อจำกัดในการใช้ อย่างเช่น สิ่งที่คุณมี (Possession Factor) นั้นอาจจะสูญหายหรือถูกขโมยได้ สิ่งที่คุณรู้ (Knowledge Factor) อาจจะถูกดักฟัง หรือขโมยจากเครื่องคอมพิวเตอร์ สิ่งที่คุณเป็น (Biometric Factor)

ซึ่งรูปแบบดังกล่าวนั้นจัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูง แต่อย่างไรก็ตามการที่จะใช้เทคโนโลยีนี้ได้นั้นจำเป็นต้องมีการลงทุนที่สูงเช่นกัน จากการดังกล่าวจึงได้มีการนำแต่ละคุณลักษณะมาใช้ร่วมกัน ตัวอย่างเช่น ใช้สิ่งที่คุณมีกับสิ่งที่คุณรู้มาใช้ร่วมกัน เช่น การใช้ลายมือชื่อร่วมกับการใช้บัตรเครดิตหรือการใช้รหัสผ่านร่วมกับการใช้บัตร ATM เป็นต้น ซึ่งการนำแต่ละลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกันมากกว่า 1 ลักษณะ จะช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของข้อมูลมากยิ่งขึ้น ดังตัวอย่างรูปแบบของการพิสูจน์ทราบตัวตนผู้ใช้งานดังตัวอย่างต่อไปนี้

1) การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords) ซึ่งเป็นวิธีการที่ใช้มานาน และนิยมใช้กันแพร่หลายแต่ว่าในปัจจุบันนี้ การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่ง่ายเกินไป และวิทยาการความรู้ที่ก้าวหน้า อาจทำให้รหัสผ่านถูกขโมยระหว่างการสื่อสารผ่านเครือข่ายได้

2) การพิสูจน์ตัวตนโดยใช้ PIN Code (Authentication by PIN) ที่ถือเป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN Code ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เช่นบัตร ATM และเครดิตการ์ดต่าง ๆ ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น เนื่องจาก PIN Code จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่น ฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับ และผู้ส่งเท่านั้น

3) การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric Traits) ซึ่งเป็นลักษณะเฉพาะ และลอกเลียนแบบกันไม่ได้ การนำมาใช้ในการพิสูจน์ตัวตนจะเพิ่มความน่าเชื่อถือได้มากขึ้น เช่น การใช้ลายนิ้วมือ เสียง ม่านตา เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความ-ปลอดภัยก่อนเข้าสู่ระบบ เช่นการใช้ควบคู่กับการใช้รหัสผ่าน

4) การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password--OTP) รูปแบบนี้ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำ ๆ กัน OTP จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะรหัสผ่านจะถูกเปลี่ยนทุกครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบการทำงานของ OTP คือเมื่อผู้ใช้ต้องการจะเข้าใช้ระบบ ผู้ใช้จะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่ง Challenge String[10] กลับมาให้ผู้ใช้ จากนั้นผู้ใช้จะนำ Challenge String และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้าฟังก์ชันแฮช[11] แล้วออกมาเป็นค่า Response ผู้ใช้ก็จะส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์จะทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบกับค่าที่เซิร์ฟเวอร์เองคำนวณได้ โดยเซิร์ฟเวอร์ก็ใช้วิธีการคำนวณเดียวกันกับผู้ใช้ เมื่อได้ค่าที่ตรงกัน

---

[10]Challenge String หมายถึง ตัวอักขระหลาย ๆ ตัวที่เมื่อนำมาต่อกันแล้วสื่อความหมายบางอย่างและสามารถนำไปเก็บในหน่วยความจำของเครื่องคอมพิวเตอร์หรือสื่อ (Media) ชนิดต่าง ๆ ได้.

[11]ฟังก์ชันแฮช (Hash Function) คือ วิธีการอย่างหนึ่งซึ่งทำให้ข้อมูลส่วนหนึ่งหรือทั้งหมด ให้กลายเป็นจำนวนเล็ก ๆ ซึ่งเปรียบได้ว่าเป็น “ลายนิ้วมือ” ของข้อมูล.

4.3 การรักษาความปลอดภัยของที่อยู่ของข้อมูลในอินเทอร์เน็ต

การป้องกันไม่ให้ผู้ใช้อินเทอร์เน็ตในองค์กรเข้าเว็บไซต์ที่ไม่เหมาะสมกำลังได้รับความนิยมเพิ่มขึ้นในหลาย ๆ องค์กร เทคโนโลยี URL[12] Filtering มีหน้าที่ในการปิดกั้นเว็บไซต์ที่ไม่ปลอดภัยและไม่เหมาะสม โดยมีการกำหนดประเภทของเว็บไซต์ต่าง ๆ ออกเป็นหลายประเภท เช่น เว็บไซต์ภาพโป๊ เว็บไซต์สปายแวร์ เว็บไซต์การพนัน หรือไม่ว่าจะเป็นเว็บไซต์ที่เกี่ยวกับการดาว์โหลดหนัง เพลง เป็นต้น และนอกจากนั้นเทคโนโลยี URL Filtering ยังมีประโยชน์ในการเตือน หรือตรวจสอบผู้ใช้งานอินเทอร์เน็ตที่ไม่ประพฤติปฏิบัติตามนโยบายด้านความปลอดภัย และกฎระเบียบขององค์กรอีกด้วย โดยสามารถออกรายงานสรุปการใช้งานอินเทอร์เน็ตของผู้ใช้อินเทอร์เน็ตในองค์กรซึ่งผู้ตรวจสอบสามารถตามร่องรอยในการเข้าเว็บไซต์ต่าง ๆ ของผู้ใช้งานอินเทอร์เน็ตในองค์กรได้อย่างง่ายดาย

เทคโนโลยี URL Filtering นั้นผู้ให้บริการสามารถติดตั้งเพื่อนำไปใช้ในการรักษาความปลอดภัยระบบคอมพิวเตอร์ที่อยู่ในความดูแลของตนเองได้หลายรูปแบบ อาทิเช่น แบบที่เป็นซอฟแวร์ติดตั้งที่ Server ซึ่งเป็นวิธีการรักษาความปลอดภัยที่ง่ายต่อการเลือกใช้งาน ทั้งผู้ใช้ และผู้ให้บริการ เพียงแต่ติดตั้งระบบซอฟต์แวร์ ในระบบ-คอมพิวเตอร์ที่อยู่ในความดูแลของตนเอง ระบบซอฟต์แวร์ดังกล่าวก็จะปฏิบัติการตรวจสอบ และรักษาความปลอดภัยโดยอัตโนมัติ ทั้งนี้ก็ขึ้นอยู่กับความสามารถ และประสิทธิภาพในการทำงานของซอฟต์แวร์นั้น ๆ ซอฟต์แวร์ในการรักษาความปลอดภัยดังกล่าว อาทิเช่น ซอฟต์แวร์ SCM (Security Content Manager) เป็นซอฟต์แวร์ที่เป็นหนึ่งในตระกูลของระบบการรักษาความปลอดภัย eTrust ซึ่งมีชื่อเสียงอย่างมากในด้านระบบรักษาความปลอดภัยซึ่งได้รับรางวัลโซลูชั่นความปลอดภัยยอดเยี่ยม (Best Security Solution) ในพิธีมอบรางวัลผลิตภัณฑ์สำหรับโอเพ่นซอร์สยอดเยี่ยม (Open Source Product Excellence Awards) ในงานนิทรรศการและการประชุม Linux World ที่มหานครนิวยอร์ก

---

[12]URL ย่อมาจาก Uniform Resource Locator หมายถึงที่อยู่ (Address) ของข้อมูลต่าง ๆ ในอินเทอร์เน็ต.

ดังจะเห็นได้ว่าการรักษาความปลอดภัยแบบ URL Filtering กรณีซอฟต์แวร์ SCM นั้น SCM สามารถกลั่นกรองเนื้อหาที่อยู่ในเว็บหรืออีเมล และสามารถกลั่นกรอง URL ของเนื้อหาที่ไม่เหมาะสมได้เช่นเดียวกัน ซอฟต์แวร์ดังกล่าวจะช่วยลดภาระให้แก่ผู้ดูแลระบบโดยผู้ดูแลระบบไม่มีความจำเป็นต้องคอยนั่งกำหนดประเภทของ URL ด้วยตัวเอง เนื่องมาจาก SCM ได้แยก URL ออกเป็นประเภทไว้เพื่อการตรวจสอบแล้ว อาทิเช่น Sex, Drugs, Sport, Games และ MP3 เป็นต้น ทั้งนี้เพื่อให้ผู้ดูแลระบบสามารถนำไปใช้ในการกำหนด Policy ตามที่ต้องการได้ทันที[13]

4.4 การรักษาความปลอดภัยของเนื้อหา หรือข้อมูลในอินเทอร์เน็ต

Content Filtering เป็นการรักษาความความปลอดภัยของระบบคอมพิวเตอร์แบบการกลั่นกรองเนื้อหา หรือข้อมูล ที่ผู้ใช้บริการเข้าใช้บริการระบบคอมพิวเตอร์ ซึ่งเป็นเนื้อหาหรือข้อมูลที่อยู่ภายในเว็บ ไฟล์ และอีเมลซึ่งผ่านเข้า-ออก ในระบบคอมพิวเตอร์ซึ่งอยู่ในการให้บริการของผู้ให้บริการ โดยการควบคุมในส่วนดังกล่าวนั้นอาจเป็นการควบคุมดูแลโดยผู้ดูแลระบบ (Webmaster) ซึ่งสามารถกลั่นกรองเนื้อหาที่ไม่เหมาะสมในแต่ละประเภทได้ตามต้องการ อาทิเช่น Keyword, Subject, Body, Attachment, File Name, File Extension, File Size เป็นต้น

5. ความรับผิดทางอาญาของนิติบุคคล

5.1 แนวคิดความรับผิดทางอาญาของนิติบุคคล

เป็นที่ทราบกันดีในปัจจุบันว่าการประกอบธุรกิจหรือกิจการโดยส่วนใหญ่นั้นจะเป็นการกระทำในรูปแบบสถานะของนิติบุคคล ซึ่งอาจหมายรวมไปถึงผู้ให้บริการอินเทอร์เน็ตด้วย ทั้งนี้เพื่อให้ง่ายต่อการประกอบกิจการ เพื่อความมั่นคงทางเศรษฐกิจ

---

[13]ชิดชนก อุทัยกร, **SCM ระบบการรักษาความปลอดภัยของเกตเวย์** [Online], available URL: http://www.nectec.or.th/images/pdf/techtrends/62/scm.pdf, 2552 (สิงหาคม, 3).

และรวมไปจนถึงเพื่อเป็นการสร้างความเชื่อมั่นให้แก่บุคคลภายนอกผู้ใช้บริการ และผู้ลงทุนเป็นต้น แต่ถึงอย่างไรก็ตามนิติบุคคลนั้นก็เป็นแต่เพียงบุคคลสมมติขึ้นตามกฎหมายเท่านั้นไม่มีตัวตน ดังนั้นการได้มาซึ่งความมั่นคงทางเศรษฐกิจและความเชื่อมั่นทางสังคมนั้น ย่อมต้องอาศัยบุคคลผู้ที่มีหน้าที่ในการขับเคลื่อนการดำเนินงานของนิติบุคคลนั้น ๆ ซึ่งก็ได้แก่บุคคลผู้อยู่เบื้องหลังการดำเนินงานของนิติบุคคลอย่างเช่น กรรมการผู้จัดการ ผู้จัดการต่าง ๆ นั่นเอง ทั้งนี้หมายรวมไปจนถึงการที่การกระทำความผิดใดเกิดขึ้นโดยผู้กระทำความผิดมีสถานะเป็นนิติบุคคล และในความรับผิดทางอาญาด้วย

กรณีความรับผิดทางอาญาที่กระทำลงโดยนิติบุคคลนั้น นิติบุคคลก็จะต้องถูกบังคับลงโทษตามกฎหมายเช่นกัน แต่เนื่องด้วยกฎหมายอาญามีการระบุโทษทางอาญาอยู่เพียง 5 สถานเท่านั้นซึ่งสามารถแบ่งการบังคับลงโทษได้ออกเป็น 3 ประเภท คือ

1) การบังคับลงโทษเอาแก่เนื้อตัว ร่างกายของผู้กระทำความผิด คืออัตราโทษประหารชีวิต โทษจำคุก และโทษกักขัง

2) การบังคับลงโทษเอาแก่ทรัพย์สินของผู้กระทำความผิดได้แก่ โทษปรับ และโทษริบทรัพย์สิน

3) การบังคับลงโทษเอาแก่เนื้อตัวร่างกาย และทรัพย์สินของผู้กระทำความผิด

การบังคับลงโทษดังกล่าว หากนำมาใช้บังคับเพื่อลงโทษผู้กระทำผิดที่มีสถานะเป็นนิติบุคคลแล้ว ดังจะเห็นได้ว่าโดยสภาพของนิติบุคคลนั้นจะสามารถนำมาใช้บังคับได้เพียงบางประเภทของโทษเท่านั้น คือโทษปรับ และริบเอาแก่ทรัพย์สินของสภาพนิติบุคคลเพียงเท่านั้น และเมื่อพิจารณาอัตราโทษปรับตามประมวลกฎหมายอาญาหรือกฎหมายพิเศษอื่นใดกับสถานะทางเศรษฐกิจ สังคมของนิติบุคคลแล้ว อัตราโทษปรับ และริบทรัพย์สินนั้นยังคงถือว่าเป็นอัตราโทษเพียงน้อยนิด และจะยังคงไม่สามารถที่จะแก้ไขปัญหาอันเกิดจากการกระทำความผิดของนิติบุคคลได้เท่าที่ควร เพราะนิติบุคคลส่วนใหญ่ มีกำลังทรัพย์หรือทุนทรัพย์ค่อนข้างมาก ประกอบกับเป็นแต่เพียงการบังคับลงโทษเอาแต่สถานะภายนอกของนิติบุคคล แต่บุคคลผู้ซึ่งขับเคลื่อนการดำเนินงานของนิติบุคคลก็ยังคงไม่เกิดความเข็ดหลาบ และยังคงลอยนวล และยังคงขับเคลื่อนนิติบุคคลนั้น ๆ ต่อไปได้

บุคคลผู้ซึ่งขับเคลื่อนการดำเนินงานของนิติบุคคล คือ บุคคลผู้เป็นกรรมการ-ผู้จัดการ ผู้จัดการของนิติบุคคลนั้น ๆ หรือที่เรียกโดยรวมว่า "ผู้แทน" เนื่องจากนิติบุคคลเป็นบุคคลโดยกฎหมายกำหนดขึ้น ไม่สามารถกระทำการได้ด้วยตนเองอย่างบุคคลธรรมดา นิติบุคคลจึงต้องมีกรรมการซึ่งเป็น "ผู้แทน" หรือผู้บริหารนิติบุคคลขึ้นมากระทำการแทน โดยสิทธิ หน้าที่ ความรับผิดของนิติบุคคลและผู้ถือหุ้นซึ่งเป็นผู้แทนนั้นจะแยกต่างหากจากกัน ทั้งนี้เพื่อช่วยปกป้องผู้ถือหุ้นมิให้ต้องรับผิดเป็นการส่วนตัวในกรณีที่นิติบุคคลนั้น ๆ กระทำความผิด ซึ่งเป็นไปตามประมวลกฎหมายแพ่งและ-พาณิชย์ที่บัญญัติให้ผู้ถือหุ้นแต่ละคนจะมีส่วนร่วมรับผิดเพียงเท่าจำนวนที่ตนลงทุนเท่านั้น และเมื่อเป็นเช่นนี้อาจถือเป็นช่องทางให้เกิดมีบุคคลผู้ก่อตั้งนิติบุคคลขึ้นมาเพื่อบังหน้าหาผลประโยชน์ส่วนตน หรือหลีกเลี่ยงความรับผิดตามกฎหมายได้

กรณีขอบเขตความรับผิดทางอาญาของนิติบุคคลนั้นสามารถอธิบายกรอบของความรับผิดเป็น 3 ประเภท คือ[14]

1) เมื่อมีกฎหมายบัญญัติโดยตรงให้นิติบุคคลใดต้องรับผิดทางอาญา นิติบุคคลนั้นก็ย่อมจะต้องรับผิดตามที่กฎหมายนั้นบัญญัติไว้ อาทิเช่น พระราชบัญญัติ-กำหนดความผิดเกี่ยวกับห้างหุ้นส่วนจดทะเบียน ห้างหุ้นส่วนจำกัด บริษัทจำกัด-สมาคม และมูลนิธิ พ.ศ. 2499

2) เมื่อมีกฎหมายบัญญัติให้นิติบุคคลใดต้องรับผิดในการกระทำของผู้อื่น ซึ่งนิติบุคคลจะต้องรับผิดชอบ

3) หากไม่มีกฎหมายบัญญัติโดยตรงให้นิติบุคคลต้องรับผิด หรือต้องรับผิดในการกระทำของผู้อื่นดังกล่าวข้างต้นแล้ว นิติบุคคลจะรับผิดทางอาญาก็ต่อเมื่อความผิดทางอาญานั้นได้กระทำไปในการดำเนินงานตามวัตถุประสงค์ของนิติบุคคลนั้น และนิติบุคคลได้รับประโยชน์จากการกระทำนั้นแล้ว ทั้งนี้จะเห็นได้จากคำพิพากษาฎีกาที่ 1669/2506 และ 584/2508 ซึ่งวินิจฉัยว่า บริษัทนิติบุคคลแม้ไม่สามารถกระทำการทุกอย่างได้เช่นบุคคลธรรมดาก็ตาม แต่ถ้าการกระทำนั้นเป็นไปตามความประสงค์

---

[14] บัญญัติ สุชีวะ, **ความรับผิดทางอาญาของนิติบุคคล** [Online], available URL: http://www.pattanakit.net/images/1186982866/articlehaya5.pdf, 2552 (สิงหาคม, 3).

ซึ่งได้จดทะเบียนไว้ และได้รับประโยชน์อันเกิดจากการกระทำนั้นแล้วก็ย่อมมีเจตนาในการรับผิดทางอาญาได้ คำพิพากษาฎีกาที่ 59/2507 นิติบุคคลย่อมแสดงความประสงค์จากทางผู้แทนเมื่อผู้แทนออกเช็คโดยเจตนาจะมิให้มีการใช้เงินตามเช็ค นิติบุคคลนั้นต้องรับผิดร่วมกับผู้แทนของนิติบุคคลด้วย คำพิพากษาฎีกาที่ 1620/2508 พบอาหาร-กระป๋องไม่บริสุทธิ์ ฝ่าฝืนพระราชบัญญัติควบคุมคุณภาพอาหาร พ.ศ. 2484 ในร้านของบริษัทจำกัด บริษัทจำกัดต้องมีความผิด คำพิพากษาฎีกาที่ 637/2509 บริษัทจำกัดที่ตั้งขึ้นเพื่อดำเนินการอันเป็นกุศล หรือสงเคราะห์ผู้ถือหุ้นอันมีลักษณะคล้ายคลึงกับการประกันชีวิตตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 861 และ 889 จะต้องได้รับ-อนุญาต มิฉะนั้นมีความผิดตามพระราชบัญญัติควบคุมกิจการค้าขายอันกระทบถึงความปลอดภัย และผาสุกแห่งสาธารณชน พ.ศ. 2471 มาตรา 7 และ 8 แต่ถ้าการกระทำ-ความผิดนั้น มิได้กระทำไปในกิจการที่อยู่ในขอบวัตถุที่ประสงค์ของนิติบุคคลแล้ว แม้ผู้แทนของนิติบุคคลกระทำไป ก็หาทำให้นิติบุคคลนั้นต้องรับผิดด้วยไม่ ผู้แทนของนิติบุคคลเท่านั้นต้องรับผิดทางอาญาเป็นส่วนตัว ทั้งนี้ดังที่วินิจฉัยไว้ในคำพิพากษาฎีกาที่ 1050/2504 ว่า เมื่อบริษัทจำกัดไม่มีวัตถุประสงค์ในการรับประกันภัย แต่ผู้จัดการไปกระทำกิจการคล้ายการรับประกันภัย อันเป็นความผิดต่อพระราชบัญญัติควบคุม-กิจการค้าขายอันกระทบถึงความปลอดภัยและผาสุกแห่งสาธารณชน พ.ศ. 2471 บริษัท-จำกัด ไม่มีความผิด เพราะเป็นการนอกวัตถุที่ประสงค์แต่ผู้จัดการที่กระทำมีความผิด

แต่อย่างไรก็ตามนอกจากกรอบความรับผิดทางอาญาของนิติบุคคลดังกล่าวแล้ว นิติบุคคลอาจจะรับผิดทางอาญาได้อันเป็นผลมาจากการกระทำของผู้แทนของนิติบุคคลนั้นเอง ดังนี้

1) ตามข้อเท็จจริงเมื่อนิติบุคคลแสดงเจตนาเองไม่ได้ จึงต้องถือเอาเจตนาของผู้แทนนิติบุคคลที่แสดงออกตามอำนาจ และหน้าที่ ที่มีอยู่ตามวัตถุประสงค์ของนิติบุคคลนั้น เมื่อเป็นเช่นนี้การแสดงเจตนาของผู้แทนนิติบุคคลดังว่านั้นก็ย่อมต้องมีผลผูกพันนิติบุคคล และต้องถือว่าเป็นการแสดงเจตนาของนิติบุคคลนั้นเองด้วย ดังนั้นแล้วหากการแสดงเจตนาอันใดของผู้แทนนิติบุคคลที่มีอยู่ตามวัตถุประสงค์ของนิติบุคคลนั้นมีลักษณะเป็นความผิด ฉะนั้นจึงต้องถือว่านิติบุคคลนั้นกระทำความผิด และต้องได้รับโทษทางอาญาเท่าที่ลักษณะแห่งโทษเปิดช่องให้ลงแก่นิติบุคคลได้

2) กรณีที่ผู้แทนนิติบุคคลกระทำการใดโดยไม่เจตนา หรือกระทำการใดโดยประมาทอันเป็นเหตุให้เกิดความเสียหายขึ้นผู้แทนนิติบุคคลย่อมต้องรับผิดเป็นการส่วนตัว แต่หากการกระทำนั้นเป็นการกระทำตามอำนาจหน้าที่ภายในขอบวัตถุประสงค์ของนิติบุคคล และนิติบุคคลได้รับประโยชน์จากการกระทำดังกล่าว นิติบุคคลก็ย่อมต้องรับผิดสำหรับการกระทำของผู้แทนนิติบุคคลนั้นด้วย

5.2 ความรับผิดทางอาญาของนิติบุคคลตามกฎหมายของต่างประเทศ

5.2.1 ประเทศฝรั่งเศส

ประเทศฝรั่งเศสเป็นประเทศที่ใช้ระบบกฎหมายแบบลายลักษณ์อักษรเหมือนกับประเทศไทย ในการบังคับใช้กฎหมายเพื่อลงโทษแก่นิติบุคคลนั้น ศาลจะไม่พิพากษาลงโทษนิติบุคคล เว้นเสียแต่ว่ามีบทบัญญัติของกฎหมายบัญญัติไว้โดยชัดแจ้งให้ต้องรับผิดหรือโดยปริยายเท่านั้น โดยความรับผิดทางอาญาของนิติบุคคลเป็นไปตามประมวลกฎหมายอาญาของประเทศฝรั่งเศส โดยได้บัญญัติไว้ว่า "นิติบุคคลอื่นยกเว้นรัฐพึงรับผิดทางอาญาสำหรับความผิดที่กระทำขึ้นโดยนิติบุคคลนั้นเองหรือโดยตัวแทนของนิติบุคคลเพื่อประโยชน์ของนิติบุคคลนั้น ทั้งนี้ตามกรณีที่กฎหมายบัญญัติ" ดังนั้นในความรับผิดทางอาญาของนิติบุคคลจึงอยู่ภายใต้หลักการ 2 ประการ คือ

1) หลักว่าด้วยความผิดเฉพาะกรณี กล่าวคือ นิติบุคคลจะรับผิดเฉพาะกรณีที่มีบทบัญญัติของกฎหมายกำหนดความรับผิดในเรื่องนั้นไว้โดยเฉพาะ

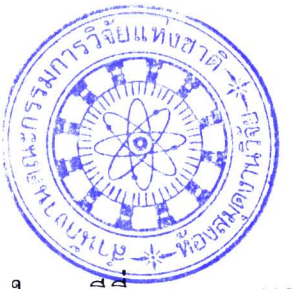
2) หลักการว่าด้วยความเกี่ยวพันระหว่างการกระทำความผิด และตัวของนิติบุคคลนั้น ๆ กล่าวคือ ความผิดนั้นกระทำขึ้นโดยนิติบุคคลหรือตัวแทนของนิติบุคคล หรือความผิดนั้นกระทำขึ้นเพื่อประโยชน์ของนิติบุคคลนั้นเอง

แต่ถึงอย่างไรก็ตามนิติบุคคลนั้นก็ต้องรับผิดในกรณีที่เป็นความผิดที่เกิดจากการละเว้นไม่กระทำการด้วย โดยผลแห่งความรับผิดของนิติบุคคลนั้นกฎหมายได้บัญญัติอัตราโทษไว้เป็นโทษปรับ โดยพิจารณาเทียบเคียงกับอัตราโทษปรับที่บังคับใช้กับนิติบุคคล กล่าวคือ นิติบุคคลต้องระวางโทษปรับไม่เกินห้าเท่าของอัตราที่กฎหมายกำหนดไว้สำหรับการกระทำความผิดของบุคคลธรรมดา นอกจากนี้หากนิติบุคคลนั้นเคยต้องคำพิพากษาถึงที่สุดให้ชำระค่าปรับมาแล้วแต่ได้กระทำความผิด

ที่มีอัตราโทษเดียวกันซ้ำอีก อัตราโทษปรับสูงสุดที่ศาลสามารถกำหนดให้นิติบุคคลชำระได้ คือไม่เกินสิบเท่าของอัตราโทษปรับที่กำหนดไว้สำหรับการกระทำความผิดเดียวกันโดยบุคคลธรรมดา ตามอัตราโทษขึ้นสูงดังกล่าวนั้นมิใช่ว่านิติบุคคลจะต้องได้รับโทษในอัตราขึ้นสูงเสมอไป แต่ได้บัญญัติยกเว้นไว้ให้ศาลพิจารณากรณีที่ศาลอาจพิพากษาให้จ่ายค่าปรับที่ต่ำกว่าอัตราโทษที่กฎหมายกำหนดไว้ก็ได้

โดยนอกเสียจากอัตราโทษปรับแล้วประมวลกฎหมายอาญาของประเทศฝรั่งเศสยังได้บัญญัติอัตราโทษอื่น ๆ อีก อาทิเช่น การสั่งยกเลิกกิจการ การสั่ง-ห้ามประกอบกิจการบางอย่าง การให้นิติบุคคลอยู่ภายใต้การควบคุมดูแลโดยเจ้าหน้าที่ของศาล การสั่งปิดกิจการ การเพิกถอนสิทธิในการยื่นประมูลโครงการจัดซื้อจัดจ้างของรัฐ การห้ามมิให้ระดมทุนจากสาธารณชน การห้ามมิให้ออกเช็ค การริบทรัพย์ที่ใช้ในการกระทำความผิดหรือที่ได้มาจากการกระทำความผิด และการปิดประกาศคำพิพากษาหรือการเผยแพร่คำพิพากษาผ่านสื่อสิ่งพิมพ์หรือสื่อโทรทัศน์ อัตราโทษอื่น ๆ เหล่านี้ดังจะเห็นได้ว่าล้วนแล้วแต่เป็นอัตราโทษที่ไม่เพียงแต่กระทบต่อสถานะภาพทางการเงินของนิติบุคคลแต่เพียงอย่างเดียว แต่ยังได้กระทบต่อความเป็นอยู่และชื่อเสียงของนิติบุคคลนั้น ๆ อีกด้วย

นอกเสียจากอัตราโทษที่บังคับเอาแต่สภาพของนิติบุคคลแล้วนั้น กฎหมายยังได้กำหนดอัตราโทษแก่ผู้บริหารของนิติบุคคลนั้นด้วย กล่าวคือความรับผิดของนิติบุคคลไม่มีผลลบล้างความรับผิดของบุคคลธรรมดาผู้กระทำความผิดหรือผู้มีส่วนร่วมในการกระทำความผิด โดยในความรับผิดข้อนี้มีความคิดเห็นของนักกฎหมายประเทศฝรั่งเศส 2 ฝ่ายด้วยกัน คือ ฝ่ายที่เห็นด้วยกับฝ่ายที่ไม่เห็นด้วย โดยฝ่ายที่เห็นด้วยนั้นมองว่าควรให้อิสระแก่ศาลในการพิจารณาข้อเท็จจริง และพิพากษาลงโทษทั้งนิติบุคคลและผู้บริหาร ทั้งนี้เพื่อป้องกันมิให้ผู้บริหารปัดภาระความ-รับผิด หรือปล่อยปละละเลยในการปฏิบัติหน้าที่ของตน ดังนั้นการที่นิติบุคคลต้องรับผิดจึงมิได้เป็นเหตุที่จะทำให้ผู้บริหารพ้นผิดได้ และฝ่ายที่สองมีความเห็นว่าผู้บริหารไม่ต้องร่วมรับผิด เนื่องจากเจตนารมณ์ในการกำหนดความรับผิดของนิติบุคคลนั้นเพื่อจำกัดความรับผิดของบุคคลธรรมดา กล่าวคือ บุคคลธรรมดาจะรับผิดเมื่อการกระทำความผิด



นั้นเป็นไปเพื่อประโยชน์ส่วนบุคคลของตนเท่านั้น ส่วนในกรณีที่บุคคลธรรมดากระทำความผิดเพื่อประโยชน์ของนิติบุคคล ความผิดนั้นก็พึงตกอยู่กับนิติบุคคลเพียงฝ่ายเดียว

โดยสรุปคือ กรณีที่มีบทบัญญัติของกฎหมายกำหนดความรับผิดทั้งของบุคคลธรรมดาและนิติบุคคลไว้สำหรับการกระทำความผิดตามกฎหมายนั้น หลักความรับผิดนั้นจะเป็นการเปิดโอกาสให้ศาลพิจารณาว่าจะเอาผิดกับนิติบุคคลเท่านั้นหรือจะให้ผู้บริหารร่วมรับผิดด้วย ทั้งนี้ผู้บริหารไม่ต้องรับผิดสำหรับความผิดพลาดในการกระทำเพื่อนิติบุคคลเฉพาะในกรณีที่มีบทบัญญัติของกฎหมายกำหนดไว้อย่างชัดแจ้งว่าผู้บริหารไม่ต้องรับผิดหรือในกรณีที่มีเหตุตามกฎหมายให้พ้นผิดเท่านั้น[15]

5.2.2 ประเทศสหรัฐอเมริกา[16]

ตามกฎหมายของประเทศสหรัฐอเมริกานั้น นิติบุคคลอาจต้องรับผิดทางอาญาได้ใน 2 กรณี คือ ความรับผิดตามหลัก Respondent Superior และความรับผิดตาม Model Penal Code ดังนี้

1) หลัก Respondent Superior มีสาระสำคัญว่าตัวการต้องรับผิดในการกระทำความผิดของตัวแทนซึ่งอยู่ในความควบคุมดูแลของตน และได้กระทำการไปภายในขอบเขตแห่งงานที่จ้างด้วย โดยความรับผิดทางอาญาของนิติบุคคล อันเนื่องมาจากการกระทำความผิดของลูกจ้างเกิดขึ้นจากแนวความคิดที่ว่า เมื่อนิติบุคคลมีความบกพร่องในการบริหารงานหรือในการสอดส่งดูแลการทำงานของลูกจ้างของตนแล้ว บริษัทก็ต้องรับผิดที่เกิดจากการกระทำของลูกจ้างด้วย

---

[15]ศุภวัฒน์ สิงห์สุวงษ์, **ระบบความรับผิดทางอาญาของนิติบุคคลและผู้แทนนิติบุคคลตามกฎหมายฝรั่งเศส** [Online], available URL: http://www.lawreform.go.th/lawreform/index.php?option=com_content&task=view&id=52&Itemid=12, 2554 (มีนาคม, 27).

[16]วรรณี ปิยะอารีธรรม, "ความรับผิดทางอาญาของนิติบุคคล: ศึกษาเฉพาะกรณีความรับผิดตามประมวลกฎหมายอาญา," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์, 2549), หน้า 75-77.

2) หลัก Model Penal Code มีรายละเอียดอันเกี่ยวกับความรับผิดของ-นิติบุคคล ดังนี้คือ

(1) นิติบุคคลจะต้องรับผิดในกรณีต่าง ๆ ดังนี้

ก. กรณีที่ความผิดนั้นเป็นความผิดเกี่ยวกับการละเมิดกฎเกณฑ์ ซึ่งได้แก่ความผิดเกี่ยวกับความปลอดภัยของสาธารณะหรือเป็นความผิดตามกฎหมายอื่น ซึ่งได้กำหนดความรับผิดของนิติบุคคล และเป็นการกระทำโดยตัวแทนของบริษัทซึ่ง กระทำในนามของบริษัทและอยู่ในของเขตของงานที่จ้าง หรือ

ข. กรณีที่ความผิดนั้นเป็นการงดเว้นการปฏิบัติหน้าที่อย่างใด อย่างหนึ่งตามที่กฎหมายกำหนดให้นิติบุคคลมีหน้าที่ต้องปฏิบัติ

(2) เมื่อความผิดนั้นเป็นความผิดเด็ดขาด นิติบุคคลก็ต้องรับผิด เว้นแต่กฎหมายจะได้บัญญัติเป็นอย่างอื่น

นอกจากการลงโทษดังกล่าวแล้ว ตามประเทศสหรัฐอเมริกายังมีการ-ลงโทษนิติบุคคลที่กระทำความผิดไว้หลายรูปแบบ กล่าวคือ

1) โทษปรับ โดยเป็นการคำนึงถึงฐานะทางการเงิน และขนาดของ ผู้กระทำความผิด

2) การคุมประพฤติ เช่นการให้นิติบุคคลทำงานด้านบริหารสังคมหรือ ช่วยเหลือสังคม

3) โทษริบทรัพย์ เป็นการริทรัพย์ที่ได้มาจากการกระทำความผิด ทั้งหมด รวมไปจนถึงประโยชน์ต่างๆ ที่งอกเงยขึ้นมาภายหลังด้วย และรวมไปจนถึง ทรัพย์ของบุคคลภายนอกที่นำมาใช้ในการกระทำความผิดด้วย

4) การแจ้งผู้เสียหายเพื่อลดความน่าเชื่อถือของนิติบุคคล

5) การชดใช้ความเสียหาย

6. แนวคิดและทฤษฎีที่เกี่ยวข้อง

6.1 แนวคิดการกำหนดความรับผิดทางอาญาของผู้ให้บริการอินเทอร์เน็ต[17]

เนื่องจากสภาพปัญหาในด้านต่าง ๆ ที่ทำให้การระบุตัวผู้กระทำความผิดโดยอาศัยเครือข่ายอินเทอร์เน็ตนั้นกระทำได้โดยยาก ประกอบกับการพิสูจน์ความผิดตั้งแต่ในขั้นตอนของการรวบรวมพยานหลักฐาน การรับฟังพยานหลักฐาน และการนำตัวผู้นั้นมาลงโทษยังมีอุปสรรคที่ไม่สามารถหาข้อยุติที่เหมาะสมได้ แม้จะสามารถระบุได้ว่าใครเป็นผู้กระทำแล้วก็ตาม ดังนั้นจึงมีผู้เสนอแนวความเห็นให้รัฐหันไปพิจารณาถึงความรับผิดชอบของผู้ให้บริการอินเทอร์เน็ตบ้าง ประกอบกับที่หลายฝ่ายเริ่มตระหนักว่าในสภาวการณ์เช่นนี้กฎหมายเพียงอย่างเดียวไม่สามารถแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นบนเครือข่ายอินเทอร์เน็ตได้อย่างมีประสิทธิภาพ หากแต่บริษัทผู้ให้บริการอินเทอร์เน็ตซึ่งเป็นผู้ควบคุมดูแลสังคมประเภทนี้โดยตรง ควรต้องมีจิตสำนึก และคิดค้นรูปแบบของเทคโนโลยี เพื่อกลั่นกรองเนื้อหาเหล่านั้นก่อนที่จะถูกส่งผ่านลงไปยังเครือข่ายอินเทอร์เน็ต

จากการดังกล่าว แนวคิดเรื่องการเพิ่มภาระหน้าที่และความรับผิดชอบให้กับผู้ให้บริการอินเทอร์เน็ตจึงเริ่มเกิดขึ้นในหลาย ๆ ประเทศ ซึ่งในที่นี้ก็รวมถึงประเทศไทยด้วย อย่างไรก็ตามแนวคิดดังกล่าวข้างต้นนี้ยังมีข้อโต้แย้งที่ไม่สามารถหาข้อสรุปที่ชัดเจนได้ โดยเหตุผลของแต่ละฝ่ายนั้นแบ่งออกเป็น ความคิดเห็นของฝ่ายที่เห็นด้วยกับฝ่ายที่ไม่เห็นด้วยกับการกำหนดภาระหน้าที่ และความรับผิดของผู้ให้บริการเป็นดังนี้

1) ฝ่ายที่เห็นควรกำหนดภาระหน้าที่และความรับผิดให้แก่ผู้ให้บริการ

แนวความคิดของฝ่ายนี้ก็คือ รัฐควรพิจารณากำหนดภาระหน้าที่ ที่ชัดเจนให้กับผู้ให้บริการอินเทอร์เน็ต เช่น หน้าที่ต้องตรวจสอบ กลั่นกรองเนื้อหาข้อมูลต่าง ๆ

---

[17]สาวตรี สุขศรี, "ภาระหน้าที่ และความรับผิดทางอาญาของผู้ให้บริการอินเทอร์เน็ต: ศึกษาเฉพาะกรณีการเผยแพร่ภาพลามกอนาจาร และการหมิ่นประมาทบนเครือข่ายอินเทอร์เน็ต," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์, 2547), หน้า 58-60.

ในเครือข่ายที่ให้บริการของตนอยู่เสมอเมื่อพบว่ามีการกระทำความผิด หรือหากพบว่ามีข้อมูลที่ไม่เหมาะสมเกิดขึ้นในบริการ ก็ต้องดำเนินการอย่างใดอย่างหนึ่งเพื่อที่จะระงับยับยั้ง หรือป้องกันความเสียหายไม่ว่าด้วยการแจ้งแก่เจ้าหน้าที่ให้ทราบโดยด่วน ลบข้อมูลนั้นออก หรืออย่างน้อยต้องสร้างระบบเซ็นเซอร์ทันที นอกจากนี้อาจกำหนดภาระหน้าที่ให้กับผู้ให้บริการต้องให้ความช่วยเหลือแก่เจ้าหน้าที่ในการสืบหาผู้กระทำความผิดด้วยการเปิดเผยข้อมูลที่เป็นประโยชน์ต่าง ๆ ในการสืบสวน สอบสวน ซึ่งในการกำหนดภาระหน้าที่และความรับผิดชอบนี้จะใช้วิธีการแก้ไขเพิ่มเติมกฎหมายสารบัญญัติ วิธีสบัญญัติที่มีอยู่ หรือจะบัญญัติกฎหมายขึ้นมาสำหรับการสืบสวนคดีประเภทนี้โดยเฉพาะก็ได้ อย่างไรก็ตามสำหรับภาระหน้าที่ ที่ต้องให้ข้อมูลกับเจ้าหน้าที่นั้นคงเป็นเรื่องที่ต้องพิจารณาควบคู่ไปกับกฎหมายฉบับอื่น ๆ ที่เกี่ยวข้องด้วยว่าสามารถทำได้โดยชอบหรือไม่ เช่น กฎหมายรัฐธรรมนูญ หรือพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลข่าวสารส่วนบุคคล

สำหรับในแง่ของความรับผิดเมื่อไม่ปฏิบัติหน้าที่ และสภาพบังคับหรือโทษนั้น ฝ่ายดังกล่าวมีความเห็นว่าควรให้มีการกำหนดด้วย ทั้งนี้เพื่อให้การป้องกันและปราบปรามเป็นไปอย่างมีประสิทธิภาพ ดังนั้นหากผู้ให้บริการปล่อยปละละเลยไม่ตรวจสอบพื้นที่ให้บริการของตนแล้วเกิดการกระทำความผิดขึ้น ก็อาจต้องรับผิดเพราะงดเว้นการกระทำเพื่อป้องกันผล หรือหากเป็นกรณีตรวจพบแล้ว แต่ไม่ดำเนินการอย่างหนึ่งอย่างใดที่เหมาะสม ก็อาจถือเป็นผู้ช่วยผู้สนับสนุน ซึ่งต้องรับผิดตามกฎหมายอาญา ส่วนกรณีที่ไม่ให้ความร่วมมือกับเจ้าหน้าที่ของรัฐในการให้ข้อมูลที่เป็นประโยชน์ก็อาจต้องรับผิดฐานขัดคำสั่งเจ้าพนักงานได้

2) ฝ่ายที่ไม่เห็นควรกำหนดภาระหน้าที่และความรับผิดให้แก่ผู้ให้บริการ

ความคิดเห็นของฝ่ายที่ไม่เห็นด้วยนั้นมีความเห็นว่า แม้ในทางเทคนิคแล้วผู้ให้บริการอาจสามารถป้องกันหรือกลั่นกรองข้อมูลที่ไม่เหมาะสมไม่ให้เกิดขึ้นบนเครือข่ายอินเทอร์เน็ตได้ แต่การดำเนินการต่าง ๆ ในลักษณะดังกล่าวนั้นกลับดูไม่เหมาะสมนักที่จะทำเช่นนั้น จนในที่สุดแล้วอาจทำให้ไม่มีผู้ใดเข้ามาประกอบการเป็นผู้ให้บริการอินเทอร์เน็ตอีกต่อไป เพราะนอกจากอาจต้องขาดทุนเพราะเสียค่าใช้จ่ายในการตรวจสอบข้อมูลแล้ว ยังอาจต้องรับผิดชอบในความผิดซึ่งตนไม่ได้ก่อขึ้นอีกด้วย

ย่อมเป็นผลเสียต่อการพัฒนาเทคโนโลยีประเภทนี้ ทั้งที่ในความเป็นจริงแล้วอินเทอร์เน็ตเป็นสื่อที่มีประโยชน์มากกว่าโทษ

อย่างไรก็ตามความคิดของฝ่ายนี้ยังคงมีความเห็นที่สอดคล้องกับฝ่ายแรกว่า หากมีผู้แจ้งถึงการกระทำความผิดไปยังผู้ให้บริการได้ทราบ หรือผู้ให้บริการบังเอิญตรวจพบข้อมูลที่เป็นความผิดเกิดขึ้นในพื้นที่การให้บริการของตน ผู้ให้บริการควรต้องดำเนินการอย่างใดอย่างหนึ่งเพื่อเซ็นเซอร์ หรือป้องกันการเข้าถึงข้อมูล หรือลบข้อมูลนั้นออกจากแม่ข่ายของตน รวมทั้งอาจแจ้งการกระทำความผิดเหล่านั้นแก่เจ้าหน้าที่ของรัฐเพื่อดำเนินการตามกฎหมายต่อผู้กระทำความผิดต่อไป

6.2 แนวคิดในการลงโทษผู้กระทำความผิด[18]

เนื่องจากวัตถุประสงค์หลักของกฎหมายอาญาเพื่อให้คนในสังคมอยู่ร่วมกันอย่างสันติสุข และมีความปลอดภัยในชีวิต และทรัพย์สิน รอดพ้นจากอาชญากรรมทั้งปวง หากฝ่าฝืนจะได้รับการลงโทษสำหรับความผิดนั้น ๆ ทั้งนี้ หากพิจารณาตามวัตถุประสงค์ในการลงโทษสามารถแบ่งออกได้ 4 ประเภท ดังนี้

1) การแก้แค้น หรือการตอบแทนความผิด (Retributive Justification) เพื่อให้ผู้กระทำความผิดสมควรได้รับโทษ เพราะเขาได้กระทำผิดและต้องรับผิดชอบในการกระทำของตนเอง ซึ่งโทษที่ได้รับต้องเหมาะสมกับความผิด ซึ่งโทษจะมากหรือน้อยย่อมขึ้นอยู่กับผลร้ายของการกระทำ เจตนา แรงจูงใจ พฤติการณ์แวดล้อม เหตุเพิ่มโทษ ลดโทษ และเหตุบรรเทาโทษ

2) การยับยั้งหรือข่มขู่ (Utilitarian or Deductive Justification) เพื่อให้การลงโทษมีส่วนในการลดจำนวนอาชญากรรมลงได้ ซึ่งการลงโทษรุนแรงจะเป็นการยับยั้งการกระทำความผิดหรือมีผลป้องกันอาชญากรรม เพราะมีส่วนในการยับยั้งผู้กระทำความผิดไม่ให้มีการกระทำผิดอีก และการลงโทษยังมีผลยับยั้งผู้ซึ่งกำลังจะกระทำ

---

[18]สุพล บริสุทธิ์, "การกำหนดความผิดทางอาญา: ศึกษาเฉพาะกรณีความผิดเกี่ยวกับการค้าประเวณี," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยธุรกิจบัณฑิตย์, 2550), หน้า 25-26.

ความผิดหรือผู้ที่จะเลียนแบบ และมีส่วนในการแก้ไขฟื้นฟูผู้กระทำความผิด ทำให้ประชาชนได้ตระหนักถึงการกระทำความผิด และมีความระมัดระวังไม่กระทำความผิด ทำให้ปัญหาอาชญากรรมลดลง นอกจากนั้นผลของการลงโทษยังช่วยคุ้มครองสังคม หรือช่วยมิให้บุคคลตกเป็นเหยื่อของอาชญากรรม เนื่องจากมีการแยกผู้กระทำความผิดออกไปจากสังคมแล้ว

3) การประณามหรือการไม่ยอมรับการกระทำความผิด (Expressive or Denunciatory Justification) ทั้งนี้เพื่อให้การลงโทษแก่ผู้กระทำความผิดเป็นการไม่ยอมรับการกระทำนั้น ๆ โดยการลงโทษเพียงอย่างเดียวไม่เพียงพอกับความผิดที่ได้กระทำลงไป คนในสังคมต้องประณามการกระทำนั้นด้วย การประณามผู้กระทำความผิดจะทำให้สังคมเกิดความเป็นปึกแผ่นได้

4) การแก้ไขฟื้นฟู (Reformation and Rehabilitation) เพื่อให้การลงโทษต่อผู้กระทำความผิดเป็นแก้ไขฟื้นฟูและบำบัดรักษา ทั้งทางร่างกาย จิตใจ หรือรวมทั้งการปรับปรุงเปลี่ยนแปลงบุคลิกภาพ เพื่อส่งเสริมให้ผู้ต้องโทษเป็นพลเมืองที่เคารพกฎหมายเมื่อพ้นโทษหรือมีทัศนคติที่ดีต่อสังคม

ดังนั้นหากพิจารณาแนวคิดในการลงโทษแล้วจะเห็นว่า การลงโทษไม่ได้มีวัตถุประสงค์เพื่อแก้แค้นทดแทนผู้กระทำความผิดแต่เพียงอย่างเดียว แต่มีวัตถุประสงค์อื่น ๆ ด้วยเช่นการคุ้มครองผู้กระทำความผิดและผู้ต้องสงสัยว่าการกระทำความผิดมิให้ถูกแก้แค้นจากผู้เสียหาย การยับยั้งการกระทำความผิดที่กฎหมายห้ามหรือยับยั้งผู้กระทำความผิด การลงโทษเพื่อให้ผู้กระทำความผิดรู้สำนึกผิด และผู้เสียหายได้รับการเยียวยาด้วย และการลงโทษต้องสามารถชี้นำให้เห็นว่าสังคมรังเกียจการกระทำความผิดนั้น ๆ นอกจากนั้นการลงโทษผู้กระทำผิดได้ส่งผลกระทบต่อการป้องกันมิให้อาชญากรรมเพิ่มขึ้นได้ ตลอดจนการลงโทษบางประเภทเป็นการตัดโอกาสที่บุคคลนั้นไม่ให้กระทำความผิดอีก เช่น โทษประหารชีวิตและจำคุกตลอดชีวิต หรือการลงโทษบางประเภทมีระบบการควบคุม และสอดส่อง เช่น การคุมความประพฤติ การกักขัง มีการฝึกอบรมควบคู่กับการใช้วิธีการลงโทษเพื่อให้เกิดการเรียนรู้ และเปลี่ยนแปลงพฤติกรรมให้เคารพกฎหมาย ผลการแก้ไขฟื้นฟูทำให้ผู้กระทำความผิดได้เปลี่ยนพฤติกรรม รู้สึกอับอาย เสียใจ สำนึกผิด และการลงโทษ เป็นการยืนยันความถูกต้อง หรือการคุ้มครอง

บรรทัดฐานทางสังคม การสร้างนิสัยในการเคารพกฎหมาย รวมทั้งเป็นการประณามการกระทำความผิดนั้นด้วย

6.3 ทฤษฎีการลงโทษเพื่อเป็นการข่มขู่หรือป้องกันอาชญากรรม

การลงโทษเพื่อเป็นการข่มขู่หรือป้องกันอาชญากรรมนั้นมีขึ้นในศตวรรษที่ 18 ตามแนวความคิดของสำนักคลาสสิก (Classical School) โดย Cesare Beccaria ได้กล่าวว่าเจตนาของการลงโทษไม่ควรจะเป็นการทรมานผู้กระทำความผิดหรือชดเชยความผิด แต่ควรป้องกันบุคคลอื่นมิให้กระทำความผิดเช่นเดียวกัน และการลงโทษที่ยุติธรรมควรจะมีอัตราของความรุนแรงพอเพียงที่จะยับยั้งคนอื่น

ผู้สนับสนุนทฤษฎีการลงโทษเพื่อเป็นการข่มขู่หรือป้องกันอาชญากรรมให้เหตุผลว่า การลงโทษมีผลเป็นการข่มขู่ และป้องกันไม่ให้มีการกระทำความผิดได้ดังนี้คือ

1) การลงโทษทำให้ผลร้ายที่เกิดจากการกระทำความผิดมีมากกว่าความหวังที่จะได้รับผลดีจากการกระทำนั้น ๆ ฉะนั้นคนจึงไม่กล้ากระทำความผิด

2) เมื่อคนเราไม่ต้องการที่จะได้รับการตำหนิและการดูหมิ่นจากเพื่อนมนุษย์ด้วยกัน อันจะเป็นผลเนื่องมาจากการถูกลงโทษ ใครต้องโทษเพราะได้กระทำความผิดจึงเป็นที่น่าตำหนิ และถูกดูหมิ่น เหยียดหยาม ดังนั้นคนจึงไม่อยากกระทำความผิด

3) ความประพฤติส่วนใหญ่ของมนุษย์ไม่ได้สืบเนื่องมาจากการคิดพิเคราะห์โดยตนเองว่าสิ่งใดถูก สิ่งใดผิด แต่มีสาเหตุมาจากนิสัยที่จะกระทำตามความคิดซึ่งเป็นที่ยอมรับกันในเรื่องความประพฤติอันชอบด้วยศีลธรรม ในมุมมองนี้การลงโทษไม่ได้เป็นเหตุบังคับกระทำตามความคิดดังกล่าว แต่การลงโทษเป็นเหตุหนึ่งซึ่งก่อให้เกิดความคิดว่าการกระทำอย่าใดถูกหรือผิด

ด้วยบทบัญญัติความรับผิดทางอาญาปัจจุบันนั้นมีลักษณะเป็นการข่มขู่มากกว่าความมุ่งหมายประการอื่น แต่การดังกล่าวก็มีผู้ตำหนิว่าไม่ได้ผลดีจริงซ้ำยังอาจทำให้เกิดผลร้ายอีกเสียด้วย เหตุผลของฝ่ายที่ไม่เห็นด้วยกับทฤษฎีข่มขู่ มีดังนี้

1) วัตถุประสงค์ของการลงโทษตามทฤษฎีข่มขู่ก็เพื่อลดจำนวนการกระทำผิดที่จะเกิดขึ้นต่อไป ทั้งจากผู้ที่ถูกลงโทษเองและจากผู้อื่นที่ได้รู้เห็นการลงโทษ แต่การ-

ลงโทษเพื่อข่มขู่ไม่ให้ผู้ถูกลงโทษไปกระทำความผิดซ้ำขึ้นอีกอาจไม่มีผลเป็นการข่มขู่ไม่ให้บุคคลอื่นกระทำผิดขึ้น และในทางกลับกันการลงโทษเพื่อการข่มขู่ไม่ให้บุคคลทั่วไปกระทำผิดขึ้นอาจไม่มีผลเป็นการข่มขู่ไม่ให้ผู้ถูกลงโทษไปกระทำผิดซ้ำขึ้นอีก

2) ทฤษฎีการลงโทษเพื่อเป็นการข่มขู่หรือป้องกันอาชญากรรมไม่สามารถแสดงให้เห็นอย่างชัดเจนว่าเมื่อมีการลงโทษโดยการข่มขู่หรือป้องกันอาชญากรรมแล้วจะสามารถทำให้อาชญากรรมลดลง เพราะผู้กระทำผิดที่ถูกลงโทษแล้วมีเป็นจำนวนไม่น้อยที่กลับกระทำความผิดซ้ำอีก เนื่องจากสาเหตุที่มาจากปัจจัยหลายประการ เช่น ปัจจัยทางเศรษฐกิจ สังคม และการเมือง

3) ตามทฤษฎีข่มขู่ถือว่าการลงโทษมีผลเป็นการข่มขู่ไม่ให้บุคคลกระทำผิด ฉะนั้นกฎหมายจึงควรกำหนดโทษในทางที่เป็นผลร้ายให้สูงกว่าผลดีที่ผู้กระทำผิดจะได้รับเพื่อคนจะได้ไม่กล้ากระทำผิดนั้น ฝ่ายที่ไม่เห็นด้วยกับทฤษฎีข่มขู่นี้ เห็นว่าทฤษฎีข่มขู่มองปัญหาในที่ง่ายเกินกว่าความเป็นจริง เนื่องจากในขณะที่คนตกลงใจกระทำผิด ไม่ได้คิดแต่ทางได้ ทางเสียเกี่ยวกับโทษ และผลที่จะได้รับจากการกระทำความผิดเท่านั้น แต่จะคำนึงถึงเหตุอื่น ๆ ด้วย และในบางกรณีอาจจะไม่ได้คำนึงถึงโทษที่จะได้รับจากการกระทำความผิดด้วยซ้ำ ฉะนั้นการลงโทษจึงไม่มีผลเป็นการข่มขู่ไม่ให้คนกระทำผิดเสมอไป

4) การลงโทษเพื่อข่มขู่ไม่มีผลในอันที่จะป้องกันให้ผู้ที่เคยกระทำผิดและต้องรับโทษมาแล้วกระทำผิดซ้ำขึ้นอีก เพราะวัตถุประสงค์ของการลงโทษมิได้คำนึงถึงการปรับปรุงตัวบุคคลผู้กระทำผิด นอกจากนี้ การลงโทษโดยการข่มขู่ยังอาจทำให้เกิดการถ่ายทอดความชั่วร้ายจากนักโทษที่กระทำความผิดเป็นสันดานไปยังนักโทษที่กระทำความผิดโดยไม่มีลักษณะเป็นคนชั่วร้าย[19]

จากทฤษฎีดังกล่าวนั้นหากซึ่งนำมาพิจารณาเปรียบกับการกำหนดความรับผิดเกี่ยวกับกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้วจะเห็นว่าอัตราโทษที่จะลงกับผู้กระทำความผิดตามกฎหมายนั้น มีอัตราโทษที่หนักและรุนแรงกว่าโทษที่บัญญัติไว้-

---

[19]อรรถสิทธิ์ กันมล, "ปัญหาการนำโทษทางปกครองมาใช้ควบคู่กับโทษทางอาญา," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์, 2549), หน้า 9-10.

ในประมวลกฎหมายอาญา กรณีนี้พิจารณาเปรียบเทียบกับเจตนาของผู้กระทำความผิด และความเสียหายที่เกิดขึ้น ซึ่งมีองค์ประกอบความผิดที่คล้ายคลึงกับการกำหนดฐานความผิดตามประมวลกฎหมายอาญา ที่เป็นเช่นนี้เนื่องมาจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้น เป็นการกระทำความผิดที่ส่งผลให้เกิดความเสียหายขึ้นในวงกว้าง และบางฐานความผิด ความเสียหายที่เกิดขึ้นอาจจะกระทบถึงความมั่นคงแห่งรัฐ กระทบต่อเศรษฐกิจ และสังคมของประเทศไปพร้อม ๆ กัน ซึ่งถือเป็นความเสียหายที่ใหญ่หลวงนัก เมื่อเป็นเช่นนี้กฎหมายที่เกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จึงต้องบัญญัติอัตราโทษและลงโทษผู้กระทำความผิดให้หนักยิ่งกว่าความรับผิดตามประมวลกฎหมายอาญาโดยทั่วไป ทั้งนี้ก็เพื่อที่จะให้อัตราโทษที่บัญญัติไว้ในกฎหมาย เป็นอัตราโทษที่มีความรุนแรงอย่างเพียงพอ และเหมาะสมกับการกระทำความผิดและความเสียหายที่เกิดขึ้น โดยมุ่งหวังเป็นอย่างยิ่งในการที่จะยับยั้ง ป้องกันและปราบปรามการกระทำความผิด เพื่อให้ผู้ที่มีเจตนาที่จะกระทำความผิดเกิดความหวาดกลัวในการกระทำความผิด และเกิดความเข็ดหลาบหากซึ่งถูกลงโทษตามกฎหมาย

6.4 ทฤษฎีเกี่ยวกับการป้องกัน[20]

"การป้องกันอาชญากรรม" นั้นมีผู้ให้ความหมายไว้มากมายหลากหลายด้วยกัน ดังนั้นจะเห็นได้จากคำจำกัดความของคำว่าการป้องกันอาชญากรรมในตำราอาชญาวิทยา ที่เกี่ยวข้องกับการป้องกันอาชญากรรมโดยตรงหลายเล่ม เช่น Sutherland and Cressey ได้ให้ความหมายของการป้องกันอาชญากรรมว่า "ความพยายามที่จะสกัดกั้นล่วงหน้ามิให้อาชญากรรมเกิดขึ้น" ในขณะที่การปฏิรูปแก้ไขหมายถึงการลดการกระทำผิดซ้ำ

---

[20]ทวีเกียรติ มีนะกนิษฐ และคณะ, **การศึกษากฎหมายรวบรวมความต้องการเบื้องต้นของหน่วยงานในประเทศไทยในกรณีจะต้องปฏิบัติตามพันธกรณีตามอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านการทุจริต ค.ศ. 2003** [Online], available URL: lhttp://www.oja.go.th/doc/Lists/doc1/Attachments/437/003%20Chapter%202%20pp10-44%20%20.pdf, 2552 (กันยายน, 28).

ส่วน Reckles ให้ความหมายของการป้องกันอาชญากรรมว่าเป็นความพยายามที่จะสกัดกั้นล่วงหน้ามิให้อาชญากรรมเกิดขึ้นในขณะที่การแก้ไขนั้นหมายถึงการลดการกระทำผิดซ้ำสอง

ส่วน Hubert Johnson มองว่าการป้องกันอาชญากรรมจะต้องครอบคลุมถึงการป้องกันการกระทำผิดซ้ำด้วย โดยเป็นความพยายามที่จะทำให้ปัญหาที่ยังไม่เกิดมิให้เกิดขึ้น

หากพิจารณาถึงความหมายของการป้องกันอาชญากรรม จากนักอาชญากรรมวิทยาดังกล่าวแล้ว จะเห็นได้ว่า Sutherland and Cressey ได้ให้ความหมายของการป้องกันในความหมายอย่างแคบโดยให้หมายถึง "ความพยายามที่จะสกัดกั้นล่วงหน้ามิให้อาชญากรรมเกิดขึ้น" เท่านั้น ส่วนการป้องกันการกระทำผิดซ้ำนั้นไม่ถือว่าเป็นการป้องกันอาชญากรรม แต่เป็นการแก้ปัญหาอาชญากรรมซึ่งแนวความคิดดังกล่าวสอดคล้องกับ Reckles ที่ถือว่า "การป้องกันอาชญากรรมเป็นการกระทำเพื่อหยุดยั้งการเกิดอาชญากรรม" ในขณะที่ Hubert Johnson มองการป้องกันอาชญากรรมในความหมายอย่างกว้าง ซึ่งหมายถึงการกระทำใด ๆ ที่เป็นการลดหรือยับยั้งอาชญากรรมมิให้เกิดหรือเกิดขึ้นซ้ำหรือการแก้ไขผู้กระทำผิดให้กลับตัวไม่กระทำผิดซ้ำด้วย

ดังนั้น จึงเห็นได้ว่า คำว่า "การป้องกันอาชญากรรม" เป็นคำที่มีความหมายทั้งแคบและกว้างซึ่งถือว่า การป้องกันอาชญากรรมหมายถึง กิจกรรมต่าง ๆ ที่ดำเนินการก่อนที่อาชญากรรมที่เกิดขึ้นเพื่อลดหรือขจัดการเกิดอาชญากรรม กิจกรรมดังกล่าวรวมถึงกิจกรรมที่ทำไม่ให้เกิดตัวอาชญากรและลดโอกาสในการเกิดอาชญากรรม ซึ่งรวมถึงกิจกรรมการแก้ไขอาชญากรและกิจกรรมในการปราบปรามอาชญากรรมด้วย หรืออีกนัยหนึ่งเป็นการให้ความหมายของการป้องกันอาชญากรรมในความหมายอันกว้างนั่นเองและโดยนัยนี้ความหมายของการป้องกันอาชญากรรมจึงไม่แตกต่างจากการควบคุมอาชญากรรม

6.5 ทฤษฎีกลไกแห่งการควบคุม[21]

การที่กฎหมายบัญญัติอำนาจหน้าที่ให้กระทำการแล้ว แต่ตนเองกลับยึดเอาอำนาจและหน้าที่ ที่ตนเองมีอยู่กระทำการโดยมิชอบ เช่นนี้ถือเป็นการกระทำความผิด ดังเช่นทฤษฎีกลไกการควบคุม (Containment Theory) ของ Walter C. Reckless นักอาชญาวิทยาชาวอเมริกัน ได้อธิบายและแยกระบบการควบคุมพฤติกรรมของคนที่เกี่ยวข้องกับการกระทำความผิดออกเป็น 2 ระบบ คือ

1) เกิดจากระบบการควบคุมภายใน ซึ่งเป็นระบบที่เกิดขึ้น และอยู่ภายใต้ตัวบุคคลหรืออาจเรียกว่าองค์ประกอบของความเป็นตัวตน (Self Components) เช่นการควบคุมตนเอง ความเข้มแข็งของจิตสำนึก ความรับผิดชอบ เป็นต้น ซึ่งสิ่งเหล่านี้สามารถบ่มขึ้น และสะสมไว้เป็นทุนของแต่ละบุคคล

2) ระบบการควบคุมภายนอก ซึ่งเป็นระบบที่อยู่ภายนอกตัวบุคคลที่เกี่ยวข้องกับสภาพแวดล้อมที่อยู่รอบ ๆ ตัวบุคคล ได้แก่ กฎเกณฑ์ ระเบียบ จารีตประเพณี มีความอ่อนแอ จึงทำให้เกิดการกระทำความผิดขึ้น

ดังจะเห็นได้ว่าในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรืออาชญากรรมคอมพิวเตอร์นั้น โดยส่วนใหญ่ที่เกิดมีขึ้นก็เพราะส่วนหนึ่งเกิดจากระบบการควบคุมภายนอก ซึ่งก็ได้แก่ บทบัญญัติของกฎหมายช่องว่างหรือมีข้อบกพร่องนั่นเอง กรณีในส่วนของการกระทำความผิดของผู้ให้บริการนั้น นอกเสียจากช่องว่างหรือข้อบกพร่องของกฎหมายแล้ว ยังรวมไปถึงการที่ผู้ให้บริการนั้นอาจอาศัยอำนาจหน้าที่ตามกฎหมายที่ตนเองมีอยู่ ที่เอื้ออำนวยต่อการกระทำผิดก่อเป็นความผิดขึ้นได้

---

[21]วิตถวัลย์ สุนทรขจิต, "ชุมชนกับการป้องกันและแก้ไขปัญหายาเสพติด," **วารสารสำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด** 1, 20 (มีนาคม-สิงหาคม 2547): 73.