



## บทที่ ๔

### นโยบายทางอาญาสำหรับผู้เจาะระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต

ภายหลังจากการศึกษาพฤติกรรมของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตและเหตุผลในการบัญญัติให้การเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดอาญาแล้ว ก่อให้เกิดความสงสัยในประการต่อมาว่า อะไรเป็นสาเหตุหรือแรงจูงใจให้มีการเจาะระบบคอมพิวเตอร์ และเมื่อมีการเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตแล้วจะมีความรับผิดชอบตามประมวลกฎหมายอาญาหรือไม่ รวมถึงปัญหาว่าการลงโทษประเภทใดจึงจะเหมาะสมกับผู้กระทำความผิด ซึ่งวิธีการศึกษาคำตอบต่อปัญหาทั้งหลายเหล่านี้พร้อมทั้งวิธีการป้องกัน รวมเรียกว่าการศึกษานโยบายทางอาญา

นโยบายทางอาญา (Criminal policy) หมายถึงนโยบาย<sup>๑</sup>ทั้งหลายเกี่ยวกับการกำหนดความผิด กำหนดประเภทของโทษและกำหนดแบบวิธีในการลงโทษแต่ละประเภท เป็นนโยบายที่จะนำไปสู่การบัญญัติกฎหมายว่าด้วยความผิด ว่าด้วยประเภทของโทษ และว่าด้วยแบบวิธีในการลงโทษเพื่อสนองรับนโยบาย ซึ่งนอกจากอาศัยความรู้ทางนิติศาสตร์แล้ว หากแต่อาศัยความรู้ทางปกครองหรือรัฐศาสตร์ ทางสังคมวิทยา จิตวิทยา ทางเศรษฐศาสตร์ และหลักสิทธิมนุษยชนอีกด้วย<sup>๒</sup>

ดังนั้นผู้เขียนจึงนำวิธีการศึกษาดังกล่าวมาเป็นแนวทางในการศึกษาความรับผิดชอบทางอาญาของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งได้แก่การศึกษาถึงวิธีการดังต่อไปนี้ คือ

๑. วิธีการป้องกันมิให้เกิดอาชญากรรม (Criminal probhylaxy) โดยกำจัดมูลเหตุที่ศึกษามาจากอาชญาวิทยา
๒. วิธีการทางนิติบัญญัติ (Legislation) ได้แก่การศึกษาให้ทราบถึงกฎหมายที่ควรจะมีขึ้นอย่างไร จึงจะได้ผลในทางป้องกัน ปราบปรามการกระทำความผิด

---

<sup>๑</sup>นโยบาย คือ เป้าหมายหรือจุดประสงค์ที่จะปฏิบัติการสิ่งหนึ่งสิ่งใดให้สำเร็จภายในระยะเวลาที่กำหนดไว้

<sup>๒</sup>อมราวดี อังคสุวรรณ, "กฎหมายอาญาและอำนาจรัฐในการรักษาความสงบเรียบร้อยของสังคม," วารสารกฎหมาย ปีที่ ๑๒ ฉบับที่ ๒ (ตุลาคม ๒๕๓๑) : ๑๐๙-๑๑๗.

๓. วิธีการบังคับ (Sanction) คือจะดำเนินการลงโทษผู้กระทำผิดอย่างไร จึงจะได้ผลในทางป้องกันอาชญากรรม
๔. การประสานงานระหว่างสถาบันทั้งหลายที่มีส่วนในนโยบายทางความผิดอาญานี้ให้ดำเนินไปสู่จุดหมายอันเดียวกัน<sup>๑</sup>

## ๑ การป้องกันมิให้เกิดการกระทำความผิดโดยกำจัดมูลเหตุแห่งอาชญากรรม และปัจจัยสัมพันธ์หรือโน้มน้าวให้เกิดอาชญากรรม

สาเหตุแห่งการประกอบอาชญากรรมที่จะกล่าวถึงต่อไปนี้ ผู้เขียนขอถือว่าเป็นเพียงปัจจัยที่มีผลโน้มน้าวทำให้คนเอนเอียงไปในทางที่จะประกอบอาชญากรรมขึ้น (Factors related or favorable to Crime) โดยหลีกเลี่ยงในการที่จะถือว่าเป็นมูลเหตุหรือสาเหตุแห่งอาชญากรรม (Crime causation) เพราะเมื่อกล่าวถึงมูลเหตุแห่งอาชญากรรมคนทั่วไปมักจะเข้าใจกันในทำนองว่าเป็นสิ่งที่เป็นคำตอบเด็ดขาดเป็นอันสิ้นสุดแต่เพียงนั้น แต่หาได้เป็นเช่นนั้นไม่ นอกจากนั้นการค้นคว้าหาสาเหตุแห่งอาชญากรรมนั้น มีความยากลำบากและมีข้อจำกัดที่เป็นผลให้ไม่สามารถหาเหตุผลที่แท้จริงได้เพียงพอ ซึ่งข้อจำกัดดังกล่าวนี้ได้แก่

๑. ความโน้มเอียงในด้านของนักศึกษาทางอาชญาวิทยา และในด้านประชาชนทั่วไป ในการค้นหาเหตุผลเอาอย่างง่าย ๆ แล้วสรุปออกมาเป็นคำตอบว่าอาชญากรรมมีมูลเหตุมาจากสิ่งนั้นสิ่งนี้ ซึ่งคำตอบเช่นนี้จะได้คำตอบที่ผิดมากกว่าถูก
๒. ความเชื่อที่ว่าคนที่เป็นอาชญากรและคนที่ไม่ใช่อาชญากรมีความแตกต่างกันทั้งทางร่างกายและจิตใจ ซึ่งไม่เป็นความจริงเสมอไป
๓. ในการศึกษาค้นคว้าสามารถกระทำได้สองวิธี คือ การศึกษาเป็นบุคคลและศึกษาเป็นกลุ่ม แต่มีข้อจำกัด<sup>๒</sup>

<sup>๑</sup> จิตติ ดิงสภักดิ์, คำอธิบายประมวลกฎหมายอาญาภาค ๑ พิมพ์ครั้งที่ ๙ (กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, ๒๕๓๖), หน้า ๔.

<sup>๒</sup> ชาย เสวิกุล, คำสอนชั้นปริญญาตรี พ.ศ. ๒๕๐๙ อาชญาวิทยาและทัณฑวิทยา (กรุงเทพมหานคร: มปท.), หน้า ๕๔.

เช่นกรณีการศึกษาเป็นรายบุคคล ไม่แน่ว่าผู้ที่ศึกษาค้นคว้าจะได้ข้อเท็จจริงหรือข้อมูลสำคัญมาทั้งหมดซึ่งข้อที่ขาดไปอาจมีความสำคัญอย่างยิ่งต่อการที่ทำให้เขาเป็นอาชญากร หรือกรณีการแปลความหมายของปัจจัยต่างๆ ที่มีอิทธิพลต่อความประพฤติอาจผิดพลาดเพราะปัจจัยบางอย่างที่เห็นว่าเป็นสิ่งเล็กน้อยไม่สำคัญและถูกมองข้ามอาจเป็นสิ่งที่มียอิทธิพลเหนือบุคคล อีกทั้งยังขึ้นกับความรู้ความสามารถของผู้วิจัยเป็นใหญ่

กรณีการศึกษาเป็นกลุ่ม นอกจากข้อจำกัดในการศึกษาเป็นรายบุคคลที่อาจเกิดขึ้นกับการศึกษาเป็นรายกลุ่มแล้ว การศึกษาเป็นกลุ่มมีข้อมูลบางอย่างที่สำคัญและจำเป็นแต่ยากที่จะเก็บสถิติมาเปรียบเทียบได้ ดังเช่นกรณีการศึกษาสถิติระหว่างเด็กกระทำผิดในครอบครัวที่ยากจนและเด็กที่กระทำผิดในชนชั้นกลางหรือชนชั้นสูง การกระทำผิดในเด็กชนชั้นสูงจะได้รับการช่วยเหลือทางด้านคดี ซึ่งมีผลให้สถิติไม่สมบูรณ์ หรือกรณีข้อจำกัดในจำนวนของบุคคลที่ถูกนำมาศึกษา มักจะนำมาจากอาชญากรจำนวนน้อย เพราะหากจะหาส่วนเฉลี่ยจากคนจำนวนมากจะสิ้นเปลืองทั้งเวลา กำลังคนและเงินทองซึ่งผลที่ได้ก็ไม่แน่ว่าจะเป็นเครื่องชี้วัด

แต่อย่างไรก็ตามข้อจำกัดทั้งสี่ประการดังกล่าวไม่ใช่สาเหตุที่ทำให้การศึกษาถึงสาเหตุการกระทำของผู้เจาะระบบคอมพิวเตอร์ด้อยค่าลง เพราะการศึกษาสเหตุของการเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นเพียงการตั้งสมมุติฐาน ความสำคัญจึงไม่ได้อยู่ที่ว่าสมมุติฐานถูกหรือผิดแต่อยู่ที่ว่าได้มีการศึกษาหรือหาสมมุติฐานไว้หรือไม่

## ๑.๑ ทฤษฎีทางอาชญาวิทยา

อาชญาวิทยา<sup>\*</sup> (Criminology) เป็นวิชาที่ว่าด้วยสมมุติฐานแห่งอาชญากรรม อันมีสมมุติฐานทางตัวบุคคลผู้กระทำผิด<sup>๑</sup> (Criminal Biology) และสมมุติฐานทางสังคม (Criminal Sociology) ซึ่งมีวัตถุประสงค์เพื่อสอนให้รู้ถึงสาเหตุแห่งอาชญากรรม การป้องกัน แก้ไข และวิธีการปฏิบัติต่อผู้กระทำผิด หรืออาจกล่าวเพื่อความเข้าใจว่าเป็นวิชาที่หาคำตอบว่าเพราะเหตุใดบุคคลจึงกระทำความผิด และมีหนทางใดบ้างเพื่อป้องกันการกระทำความผิด นักอาชญาวิทยายพยายามหาทฤษฎี

<sup>\*</sup> จิตติ ดิงสภักดิ์. คำอธิบายประมวลกฎหมายอาญาภาค ๑, หน้า ๔.

<sup>๑</sup> สมมุติฐานทางตัวบุคคลผู้กระทำผิด หมายถึงแยกออกเป็นสองส่วนทางร่างกาย (Physical, criminal anthropology, criminal physiology) และทางจิตใจ (Mental, criminal psychology)

ที่จะสามารถอธิบายให้ได้ว่าเพราะเหตุใดบุคคลจึงกระทำผิด ซึ่งเมื่อพูดถึงทฤษฎี บุคคลทั่วไปอาจเห็นว่าทฤษฎีเป็นเพียงนามธรรมและไม่มีความสอดคล้องกับโลกของความเป็นจริง แต่ไม่ว่าจะมีผู้คิดเช่นนี้หรือไม่ก็ตาม ทุกคนก็ใช้ทฤษฎีอยู่ตลอดเวลา การสร้างสมมุติฐานและวางหลักเกณฑ์เกี่ยวกับสิ่งใดสิ่งหนึ่งที่บุคคลมีความสัมพันธ์ด้วย นั่นก็คือทฤษฎี

ทฤษฎีเป็นรูปทรงทางตรรกวิทยาที่อธิบายปรากฏการณ์ธรรมชาติ ทฤษฎีโดยตัวเองไม่สามารถสังเกตได้โดยตรง แต่สามารถได้รับการสนับสนุนหรือถูกปฏิเสธโดยการค้นพบจากการสังเกต ทฤษฎีและการวิจัยที่ได้จากการสังเกตได้เกี่ยวโยงกันจากสมมุติฐานซึ่งเป็นข้อความที่ทดสอบได้ ซึ่งนำมาจากทฤษฎี ในส่วนที่ทดสอบได้เป็นสิ่งสำคัญเพราะสมมุติฐานทางวิทยาศาสตร์ต้องสามารถที่จะถูกยอมรับหรือปฏิเสธ ทฤษฎีอาจเป็นเพียงสิ่งง่ายหรือซับซ้อน ขึ้นอยู่กับว่าความสัมพันธ์ที่ใช้ในการก่อทฤษฎีนั้นเป็นอย่างไร ทฤษฎีอาจเป็นสิ่งเปล็ดเปล็น ขึ้นกับว่าจะถูกนำไปใช้อย่างไร เช่นถ้าใช้เวลาในการซื้อสินค้าในห้างสรรพสินค้า ก็จะได้เห็นว่าทฤษฎีทำให้เปล็ดเปล็นได้อย่างไร ปัญหาที่แท้จริงจึงอยู่ที่ว่าเราต้องการทฤษฎีเพื่อที่จะทำหน้าที่ และเพื่อความเข้าใจที่ดีต่อโลกที่อยู่รอบๆตัวเรา ชีวิตคงจะไม่น่าสนุกถ้าไม่สามารถวางหลักหรือให้สมมุติฐานเกี่ยวกับบุคคลและสิ่งของ

พฤติกรรมมนุษย์เป็นสิ่งซึ่งซับซ้อนและเกือบจะเป็นนามธรรม ทฤษฎีเกี่ยวกับการกระทำผิดก็เช่นกัน ทฤษฎีส่วนใหญ่ที่มีขณะนี้เกิดจากการวิจัยในพฤติกรรมของผู้กระทำผิดทั้งจากอดีตและปัจจุบัน ซึ่งสะท้อนให้เห็นถึงการสังเกตที่เป็นระบบและเป็นการให้เหตุผลอย่างระมัดระวัง ทฤษฎีไม่เพียงแต่ทำให้เราเห็นโครงสร้างในการตีความหมายของรูปแบบที่เกิดจากการสังเกต แต่ยังช่วยเราในการตัดสินใจว่าเมื่อไหร่รูปแบบเหล่านี้มีความหมายที่ควรได้รับความสนใจและเมื่อใดที่ไม่มีความหมาย

ทฤษฎีทางอาชญาวิทยาสามารถจัดแบ่งประเภทออกได้เป็น ๓ กลุ่มด้วยกันคือ<sup>๗</sup>

<sup>๗</sup> เรียบเรียงจาก ประเทือง ธนียผล, อาชญาวิทยาและทัณฑวิทยา พิมพ์ครั้งที่ ๓ (กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยรามคำแหง, ๒๕๓๘), หน้า ๘๒-๑๐๘

### ๑.๑.๑ กลุ่มทฤษฎีที่กล่าวถึงสาเหตุอาชญากรรมทางชีววิทยา ประกอบด้วย

- ทฤษฎีอาชญากรโดยกำเนิดของลอมโบโซ ซึ่งโดยสรุปได้ความว่า การเป็นอาชญากรโดยกำเนิดก็คือการที่สภาพธรรมชาติได้กำหนดให้บุคคลนั้น มีนิสัยและจิตใจชอบทำร้ายและเบียดเบียนผู้อื่น มักต่อต้านสังคม ไม่สามารถปรับตัวให้เข้ากับระเบียบแบบแผนของสังคมอย่างคนปกติได้และพบว่าพวกที่มีพฤติกรรมต่อต้านสังคมหรือมีพฤติกรรมเบี่ยงเบนต่างๆ มักจะมีลักษณะรูปร่างหน้าตาที่แตกต่างจากคนปกติทั่วไปอย่างเด่นชัดมาตั้งแต่เกิดหรือมีความบกพร่องทางกายมาโดยกำเนิด

- ทฤษฎีของฮูตัน<sup>๕</sup> (Hooton's Theory) ผลสรุปจากการวิจัยพบว่า พฤติกรรมของอาชญากรเป็นผลโดยตรงมาจากความบกพร่องทางชีวกายภาพซึ่งได้รับการถ่ายทอดมาจากบรรพบุรุษ อาชญากรรมแต่ละประเภทแตกต่างกันในด้านสภาพของร่างกาย ตัวอย่างเช่น พวกผอมสูงมักประกอบอาชญากรรมประเภทปล้นทรัพย์และฆ่าคนตาย ทั้งยังได้ความว่าบุคคลที่มีเชื้อชาติต่างกัน จะประกอบอาชญากรรมในลักษณะที่ต่างกัน

- ทฤษฎีรูปร่าง เป็นทฤษฎีที่ให้ความสนใจต่อขนาดร่างกายว่ามีส่วนสัมพันธ์กับสภาพจิตใจ อารมณ์ และพฤติกรรมของบุคคล ในบรรดาผู้ที่มีขนาดร่างกายต่างกันมีความสัมพันธ์กับความแตกต่างในสาเหตุของพฤติกรรมเบี่ยงเบนและอาชญากรรม

- แนวคิดเรื่องกรรมพันธุ์ ซึ่งเป็นการศึกษาการถ่ายทอดลักษณะร่างกาย จิตใจและสัญชาตญาณทางสายโลหิตจากบรรพบุรุษสู่ลูกหลานซึ่งสรุปได้ว่าลักษณะด้อยของตระกูลที่มีสายโลหิตในทางเลว และลักษณะดีของตระกูลที่มีสายโลหิตในทางดี มีการถ่ายทอดสู่ลูกหลาน

- ทฤษฎีโครโมโซม (xyy Chromosome Theory) ได้ผลจากการวิจัยที่พบว่าคนที่มีโครโมโซมผิดปกติ เช่น xyy หรือxxyหรือ xxxหรือ xxyหรือ xyyyจะมีความผิดปกติทางร่างกายและจิตใจ รวมทั้งสติปัญญา ส่วนใหญ่จะเป็นคนเก็บความรู้สึก ไม่ค่อยชอบการคบค้าสมาคมกับใคร มีความรู้สึกโน้มเอียงไปในทางรักร่วมเพศ

<sup>๕</sup> เออร์เนส ฮูตัน (Ernest Hooton) ชาวอเมริกา นักมานุษยวิทยากายภาพแห่งมหาวิทยาลัยฮาวาร์ด

- ทฤษฎีต่อมไร้ท่อ ถือว่าความไม่สมดุลย์หรือความแปรปรวนผิดปกติในระบบต่างๆ ของต่อมไร้ท่อ อาจเป็นสาเหตุหนึ่งที่ทำให้บุคคลนั้นกระทำได้

### ๑.๑.๒ กลุ่มทฤษฎีที่กล่าวถึงสาเหตุอาชญากรรมทางจิตวิทยา ประกอบด้วย

- สาเหตุจากการผิดปกติของจิต โดยเห็นว่าความเจ็บป่วยทางจิตเป็นสาเหตุสำคัญประการหนึ่งที่จะทำให้เกิดอาชญากรรม เช่นพวกโรคจิต พวกจิตบกพร่อง พวกปัญญาอ่อน พวกคาบเส้นระหว่างจิตปกติกับจิตไม่ปกติ และพวกอารมณ์แปรปรวน

- ทฤษฎีจิตวิเคราะห์ (Psychoanalytic Theory) ผู้ก่อตั้งคือซิกมันด์ ฟรอยด์<sup>๔</sup> มีสาระสำคัญคือ เชื่อว่าโครงสร้างบุคลิกภาพที่อยู่ในจิตใต้สำนึกของบุคคลประกอบด้วย ๓ ส่วน คือ อิด อีตตา และอภีอิตตาหรือสติสัมปชัญญะ บุคคลกระทำได้เมื่อบุคคลมีแรงปรารถนาสูง เกิดแรงขับมากจนสติสัมปชัญญะและอิตตาไม่สามารถยับยั้งได้ เมื่อนั้นบุคคลก็จะทำอะไรต่างๆโดยไม่คำนึงถึงสิ่งใดๆ

- ทฤษฎีปมด้อย (Inferiority Complex) อธิบายสาเหตุของการก่ออาชญากรรมของบุคคลบางประเภทว่า อาชญากรจำนวนมากมักมีลักษณะดื้อรั้น ไม่ให้ความร่วมมือ และต่อต้านสังคม ทั้งนี้เพราะอาชญากรเหล่านั้นมักมีประสบการณ์ในทางลบตั้งแต่เยาว์วัย ทำให้เกิดปมด้อยขึ้นในตัวเอง จึงประกอบอาชญากรรมขึ้นเพื่อเรียกร้องความสนใจและคิดว่าเป็นวิธีเดียวที่จะแสดงออกแล้วทำให้สาธารณชนสนใจได้อย่างมาก ต้องการความสนใจจากผู้อื่นเพื่อชดเชย ทดแทนปมด้อยของตนเอง

- ทฤษฎีเชาว์ปัญญา เป็นทฤษฎีที่ได้จากการตั้งสมมุติฐานว่า อาชญากรน่าจะมีระดับสติปัญญาต่ำกว่าคนปกติทั่วไป จึงขาดสติขาดความรู้ลึกซึ้งผิดชอบ ทำให้ก่ออาชญากรรมขึ้น ซึ่งจากผลการศึกษา เจฟเฟอร์รี่ ให้ทัศนะว่า อาชญากรนั้นมีทั้งที่ฉลาดและโง่ เชาว์ปัญญาจึงมีลักษณะเป็นปัจจัยที่เร่งหรือถ่วงความสามารถในการประกอบอาชญากรรมแต่ละประเภท

<sup>๔</sup> Sigmund Freud (1856-1939) เป็นจิตแพทย์ชาวออสเตรเลียน เชื้อสายยิว

### ๑.๑.๓ กลุ่มทฤษฎีที่กล่าวถึงสาเหตุอาชญากรรมทางสังคมวิทยา ประกอบด้วย

- สาเหตุทางเศรษฐกิจ หรือระบบเศรษฐกิจเป็นตัวก่อให้เกิดบรรยากาศของกระบวนการผลักดันให้มีพฤติกรรมอาชญากร
- ทฤษฎีสภาพไร้บรรทัดฐาน (Anomie Theory) เป็นทฤษฎีที่มีรากฐานมาจากแนวความคิดที่ว่า อาชญากรรมเป็นปรากฏการณ์ปกติของสังคม เมื่อใดที่บรรทัดฐานของสังคมไม่สามารถควบคุมการกระทำของบุคคลในสังคม หรือไม่สามารถตอบสนองความต้องการทางสังคมของบุคคล ก็จะเป็นเหตุให้บุคคลล่องละเมิดฝ่าฝืนบรรทัดฐานทางสังคม นำไปสู่การกระทำผิด ผู้เสนอแนวความคิดนี้คือเดอริโคม<sup>๑๐</sup> และเรียกสภาพดังกล่าวว่า Anomie โดยเกิดจากการเปลี่ยนแปลงทางสภาพแวดล้อม เศรษฐกิจและเทคโนโลยีอย่างรวดเร็ว ทางแก้ไขคือต้องสร้างความเป็นธรรมในสังคม ให้สังคมส่วนรวมมีความสุข ซึ่งในภายหลังเมอร์ตัน<sup>๑๑</sup> ได้ขยายแนวคิดดังกล่าวเป็นแนวคิดใหม่โดยเสนอว่าทุกสังคมประกอบไปด้วย ๒ องค์ประกอบใหญ่คือ โครงสร้างทางวัฒนธรรม ซึ่งเป็นสิ่งกำหนดเป้าหมายและแบบบรรทัดฐานของแต่ละบุคคลและโครงสร้างทางสังคม ซึ่งเป็นสิ่งกำหนดวิธีการที่เหมาะสมอันชอบธรรมที่บุคคลจะใช้ไปสู่การบรรลุเป้าหมายที่ตนตั้งไว้ เมื่อใดก็ตามที่เป้าหมายและวิธีการขัดแย้งกัน และเมื่อไม่สามารถใช้วิธีการที่ชอบธรรมเพื่อบรรลุเป้าหมายได้ ก็จะเลิกให้ความชอบธรรมที่อยู่ในกรอบของบรรทัดฐานของสังคม โดยละเมิดฝ่าฝืนกฎหมายเพื่อให้ได้บรรลุเป้าหมายและผลประโยชน์แห่งตน
- กฎการเลียนแบบ (Law of Imitation) กฎนี้ตั้งขึ้นโดยทาร์ด<sup>๑๒</sup> โดยชี้ให้เห็นว่าอาชญากรก่ออาชญากรรมได้เพราะเคยรู้เคยเห็นมาก่อน นั่นคืออาชญากรรมเกิดจากการเลียนแบบ การเลียนแบบเกิดจากการติดต่อสัมพันธ์หรือพบเห็น เรียนรู้
- ทฤษฎีความสัมพันธ์แตกต่าง (Theory of Differential Association) ก่อตั้งโดยชัทเธอร์แลนด์<sup>๑๓</sup> ครั้งแรกในปี ๑๙๓๔ โดยมีความเห็นว่าอาชญากรรมเป็นผลของการคบค้าสมาคม

<sup>๑๐</sup> เดอริโคม (Emile Durkheim 1858-1917) ชาวฝรั่งเศส

<sup>๑๑</sup> Robert K. Merton, 1938 นักสังคมวิทยาชาวอเมริกัน

<sup>๑๒</sup> Gabriel Tarde นักอาชญาวิทยาผู้บุกเบิกแนวความคิดการเรียนรู้ทางสังคม

<sup>๑๓</sup> Edwin H. Sutherland

ระหว่างบุคคลหรือระหว่างกลุ่มบุคคลกับแบบอาชญากร ยิ่งมีการคบหาสมาคมดี สม่่าเสมอ และใกล้ชิดมากเท่าใด บุคคลนั้นยิ่งกลายเป็นอาชญากรเร็วขึ้น และมีขบวนการในการถ่ายทอดจากบุคคลหนึ่งไปสู่อีกบุคคลหนึ่ง ดังนี้คือ

๑. อาชญากรเกิดจากการเรียนรู้
๒. การเรียนรู้เกิดจากการคบหาสมาคมกับผู้อื่น
๓. การสัมพันธ์กันอย่างใกล้ชิดเป็นส่วนสำคัญของการเรียนรู้พฤติกรรมอาชญากรที่เกิดขึ้นภายในกลุ่ม
๔. การเรียนรู้พฤติกรรมอาชญากร รวมถึงวิธีการ เทคนิค แรงจูงใจ ทศนคติ การหาเหตุผลเข้าข้างตัวเอง
๕. ข้อกำหนดของกฎหมาย เป็นสิ่งที่ใช้ในการเรียนรู้แรงจูงใจและแรงผลักดันภายในของบุคคลที่จะประกอบอาชญากรรมนั้น โดยขึ้นอยู่กับว่าอาชญากรจะอยู่ในแวดวงสังคมที่เคารพกฎหมายหรือสังคมที่สมาชิกชอบละเมิดกฎหมาย และสังคมใดมีอิทธิพลต่อเขามากกว่ากัน
๖. บุคคลกระทำผิดเพราะมีแนวโน้มเอียงไปทางสังคมที่ชอบละเมิดฝ่าฝืนกฎระเบียบ ไม่เคารพกฎหมายมากกว่าสังคมที่เคารพกฎหมาย
๗. ความถี่ของการติดต่อสัมพันธ์หรือระยะเวลาในการติดต่อสัมพันธ์ ทำให้บุคคลนั้นได้รับการยอมรับและสนิทสนมจากกลุ่ม ยิ่งมีมากเท่าใดยิ่งทำให้เกิดการเรียนรู้มากและเลียนแบบเป็นไปได้ง่าย
๘. กระบวนการเรียนรู้เพื่อประกอบอาชญากรรม มีทั้งจากคำพูด การกระทำ การให้ข้อมูลต่างๆ
๙. ในขณะที่พฤติกรรมอาชญากร เป็นการแสดงออกถึงความต้องการและค่านิยมโดยทั่วไป ของแต่ละบุคคล แต่ความต้องการและค่านิยมเหล่านี้ก็ไม่อาจใช้อธิบายพฤติกรรมของอาชญากรได้

- ทฤษฎีความขัดแย้งทางวัฒนธรรม (Theory of Culture Conflict) อธิบายถึงความขัดแย้ง การปรับตัว เข้ากันไม่ได้ทางวัฒนธรรมของกลุ่มคนบางกลุ่ม ซึ่งอยู่ในสังคมใหญ่ที่มีต่อวัฒนธรรมมาตรฐานของสังคมนวม และนำไปสู่การเกิดอาชญากรรม พวกที่มีวัฒนธรรมต่ำกว่าไม่สามารถปรับตัวให้เข้ากับวัฒนธรรมที่สูงกว่าได้ จึงเกิดการขัดแย้งทางวัฒนธรรมทำให้กลุ่มชนที่มีวัฒนธรรมต่ำกว่านั้นมีพฤติกรรมฝ่าฝืนละเมิดกฎระเบียบและมาตรฐานของวัฒนธรรมที่สูงกว่า จนกลายเป็นการกระทำผิด



- ทฤษฎีวัฒนธรรมรอง (Sub-Culture Theory) เป็นแนวคิดของ อัลเบิร์ต โคเฮน ซึ่งอธิบายว่า วัฒนธรรมย่อยของบุคคลที่กระทำผิดนั้น เกิดขึ้นภายในวัฒนธรรมหลักของสังคม วัฒนธรรมย่อยหรือวัฒนธรรมรองเป็นสิ่งที่ตรงกันข้ามกับวัฒนธรรมหลัก ผู้กระทำผิดมักจะยึดถือวัฒนธรรมย่อยของตนเองเป็นสิ่งที่ถูกต้อง แม้ว่าวัฒนธรรมนั้นจะมีลักษณะมุ่งร้าย ผิดกฎหมาย และปฏิเสธวัฒนธรรมใหญ่

- ทฤษฎีวัฒนธรรมของชนชั้นต่ำ (Theory of Low Class Culture) ซึ่งอธิบายว่าในสังคมของคนชั้นต่ำหรือสลัมนั้น พวกเขาจะมั่วสุมกันเป็นแก๊งและมีพฤติกรรมเบี่ยงเบนอันขัดกับความสงบเรียบร้อยและศีลธรรมอันดี มีพฤติกรรมเป็นนักเลง อวดเบ่งทำโก้ ไม่มีงานเป็นหลักแหล่ง รับจ้างทำได้ทุกอย่าง ชอบทำอะไรแปลก ให้เป็นจุดสนใจแก่คนอื่น

- ทฤษฎีตราหน้า มีจุดกำเนิดจากผลงานเขียนของ แฟรงค์ แทนเนนบาม<sup>๑๔</sup> ซึ่งอธิบายว่าแม้อาชญากรรมจะเป็นสิ่งชั่วร้าย แต่ที่ร้ายยิ่งกว่าคือการที่สังคมพยายามผลักดันให้อาชญากรดล่ำ ลีกลงไปในทางที่ผิดเป็นภัยแก่สังคมมากยิ่งขึ้น โดยไม่ยอมเปิดโอกาสให้บุคคลที่ประพฤติผิดกลับตัวเป็นคนดี ทฤษฎีนี้ชี้ให้เห็นถึงปฏิกิริยาตอบโต้ของสังคมที่มีต่อบุคคลที่กระทำผิด ที่แสดงออกมาในแง่ลบ ได้แก่การรังเกียจ ถูกเหยียดหยาม ไม่ยอมรับ ซึ่งมีแต่จะเกิดผลร้ายที่ผลักผู้กระทำผิดให้ถดถอยยิ่งขึ้น แม้จะกลับตัวเป็นคนดีแล้ว สังคมก็ไม่ยอมรับ จึงไม่มีทางเลือก และเป็นสาเหตุหนึ่งที่ทำให้เกิดการกระทำผิดซ้ำซาก และทำให้ผู้กระทำผิดก่ออาชญากรรมรุนแรงขึ้นเรื่อยๆ ด้วย

นักอาชญาวิทยาสมัยใหม่หลายท่านเห็นด้วยว่า การศึกษาสาเหตุการกระทำผิดไม่สามารถให้ความสนใจหรือยึดถือทฤษฎีใดทฤษฎีหนึ่งโดยเฉพาะ ซึ่งผู้เขียนเห็นด้วยกับความเห็นดังกล่าวเพราะมนุษย์ประกอบไปด้วยองค์ประกอบหลายๆอย่างทั้งทางด้านกายภาพ ทางด้านจิตใจและรวมถึงสังคมที่อยู่อาศัย การที่อธิบายความเป็นมนุษย์จึงไม่สามารถที่นำความรู้หรือทฤษฎีด้านใดด้านหนึ่งมาใช้ โดยไม่พิจารณาถึงปัจจัยทางด้านอื่น<sup>๑๕</sup> เหตุที่นักอาชญาวิทยาเลือกที่จะ

<sup>๑๔</sup> Frank Tannenbaum, 1983

<sup>๑๕</sup> อาชญาวิทยาจึงเป็นการศึกษาแบบ สหวิชา (multidisciplinary) คือนำเอาวิธีการและข้อมูลความรู้จากสาขาวิชาต่างๆ ที่เกี่ยวข้องมาช่วยในการศึกษา

ศึกษาเฉพาะด้านอาจเป็นเพราะเห็นว่าด้านที่ทำการศึกษานั้นมีส่วนในการอธิบายการกระทำ ความผิดจึงศึกษาให้ลึกลงไปในแต่ละด้านเพื่อหาคำตอบที่ใกล้เคียงความเป็นจริงมากที่สุด แต่การศึกษาดังกล่าวก็ไม่มีนักอาชญาวิทยาท่านใดคิดว่าทฤษฎีของตนที่น่าเสนอนั้นสามารถอธิบายได้ ทุกเรื่องที่เกี่ยวข้องกับสาเหตุการกระทำ ความผิด

## ๑.๒ แรงจูงใจของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

ลารี โคเฮนและมาคัส เฟลสัน นักอาชญาวิทยาได้กล่าวไว้ว่า มีองค์ประกอบที่จำเป็นในการเกิดการกระทำ ความผิดอยู่ ๓ ประการคือ

๑. แรงจูงใจของผู้กระทำ (motivated offenders)
๒. มีเป้าหมายที่เหมาะสม (suitable targets)
๓. ไม่มีผู้ดูแลที่มีประสิทธิภาพ (the absence of capable guardians)

ถ้าองค์ประกอบใดในทั้งสามประการนี้ขาดหายไป ดูเหมือนว่าการกระทำ ความผิดจะไม่เกิดขึ้น แต่ถ้าองค์ประกอบทั้งสามนี้อยู่พร้อมกันก็จะมีโอกาสสูงที่จะเกิดการกระทำ ความผิด ดังนั้น หากเราสามารถลดองค์ประกอบทั้งสามประการได้ จึงเป็นไปได้ว่าจะมีส่วนที่จะทำให้การกระทำ นั้นลดลง โดยเฉพาะในเรื่องแรงจูงใจของผู้กระทำซึ่งเป็นสิ่งกำหนดการกระทำภายในของแต่ละบุคคล สำหรับแรงจูงใจของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตนั้นจำแนกได้เป็น ๕ ประเภท ได้แก่<sup>๑๖</sup>

### ๑.๒.๑ แรงจูงใจทางสังคม (Social Motivations)

ผู้เจาะระบบคอมพิวเตอร์ในกลุ่มนี้เป็นกลุ่มที่พบได้ทั่วไป กลุ่มนี้เจาะระบบคอมพิวเตอร์ เพื่อพยายามให้เป็นที่ยอมรับของเพื่อนในกลุ่ม ทำให้มีความรู้สึกว่าตนเองเหนือกว่าและมีอำนาจ

<sup>๑๖</sup> John Vranesevich, "How to become A hacker profiler," INTERNET

<http://www.antonline.com/specialReports/hacker-profiler-II> กลุ่มของแรงจูงใจที่น่าเสนอนี้ได้มาจากการศึกษาพฤติกรรมของแฮกเกอร์ในต่างประเทศ ซึ่งผู้เขียนเห็นว่าสามารถนำมาเป็นแนวทางในการศึกษาถึงแรงจูงใจของผู้เข้าสู่ระบบคอมพิวเตอร์โดยไม่มีอำนาจได้เช่นกัน

ควบคุมทุกอย่าง ผู้เจาะระบบคอมพิวเตอร์ในกลุ่มนี้ถ้าไม่ได้บุกรุกเข้าไปในระบบคอมพิวเตอร์ ก็จะออกไปกลางถนนแล้วขีดเขียนบนผนังกำแพงตึกที่สูงเท่าที่พวกเขาสามารถเอื้อมมือไปถึง

### ๑.๒.๒ แรงจูงใจทางเทคนิค (Technical Motivation)

กลุ่มนี้เป็นกลุ่ม ที่ผู้เจาะระบบคอมพิวเตอร์ในกลุ่มแรกมักอ้างว่าตนก็อยู่ในกลุ่มนี้เช่นกัน กลุ่มนี้เป็นกลุ่มที่เจาะระบบคอมพิวเตอร์เพื่อช่วยเหลือ ซึ่งในความคิดของเขาเพื่อเป็นการก้าวไปสู่การพัฒนาทางเทคโนโลยี การบุกรุกเข้าไปในระบบคอมพิวเตอร์ก็เพื่อที่จะแสดงให้เห็นถึงความอ่อนแอของระบบ จนกระทั่งนำไปสู่ความสามารถในการบังคับให้องค์กรต่างๆ เช่น องค์กรทางทหาร แก้ไขข้อบกพร่องของตนเอง

### ๑.๒.๓ แรงจูงใจทางการเมือง(Political Motivations)

กลุ่มนี้เป็นกลุ่มที่มีความเชื่อรุนแรงทางการเมือง หรือบุคคลที่กำลังเผชิญความยุ่งยากทางการเมือง เช่นประเทศจีน ผู้เจาะระบบคอมพิวเตอร์ในกลุ่มนี้จะบุกรุกเข้าสู่ระบบคอมพิวเตอร์ซึ่งโดยปกติจะเป็นระบบที่มีความสัมพันธ์กับการเคลื่อนไหวทางการเมืองที่พวกเขากำลังต่อต้านอยู่ เพื่อให้ความคิดเห็นทางการเมืองที่เขาได้แสดงออกมานั้นเป็นที่สนใจ

### ๑.๒.๔ แรงจูงใจทางการเงิน(Financial Motivations)

กลุ่มนี้มีไว้สำหรับบุคคลที่เจาะระบบคอมพิวเตอร์เพื่อผลประโยชน์ของตนเอง บุคคลที่อยู่ในกลุ่มนี้ดังเช่น การโจรกรรมข้อมูลของบริษัท สถาบันการเงิน และรวมถึงบุคคลที่ลักลอบพิมพ์ Software ออกจำหน่ายเพื่อผลกำไร ซึ่งกลุ่มนี้เป็นเพียงกลุ่มเดียวที่ไม่ต้องการให้คนอื่นรู้การกระทำของตน และพยายามอย่างมากที่จะซ่อนการกระทำของพวกเขาไว้

### ๑.๒.๕ แรงจูงใจทางรัฐบาล(Governmental Motivations)

กลุ่มนี้เป็นกลุ่มที่มีระดับสูงชันกว่าบุคคลในกลุ่มที่ ๓ กลุ่มนี้จะกระทำโดยรัฐบาลหนึ่ง กระทำต่อรัฐบาลหนึ่ง การกระทำที่เข้าอยู่ในกลุ่มนี้ดังเช่น การต่อสู้กันระหว่างข้อมูลข่าวสารและการโจรกรรมระดับรัฐบาล เป็นต้น

### ๑.๓ แรงจูงใจกับแนวโน้มการกระทำผิดและทฤษฎีทางอาชญาวิทยา

แรงจูงใจทั้ง ๕ ประการดังกล่าวเป็นเสมือนตัวแทนสิ่งทีผลักดันให้ผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ประพฤติตนหรือกระทำการใดๆ ไม่ว่าจะถูกต้องหรือไม่ ดังนั้น การพิจารณาว่าแรงจูงใจทั้ง ๕ ประการนี้มีโอกาสที่จะนำไปสู่การกระทำผิดหรือไม่อาจพิจารณาจากทฤษฎีทางอาชญาวิทยาดังต่อไปนี้ คือ

#### ๑.๓.๑ กรณีการกระทำของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตที่เกิดจากแรงจูงใจทางสังคม (Social Motivations)

การเจาะระบบคอมพิวเตอร์ที่เกิดจากแรงจูงใจทางสังคมเป็นการกระทำเพื่อให้เป็นที่ยอมรับของเพื่อนในกลุ่ม เพื่อที่จะทำให้ตนเองเหนือกว่าหรือมีอำนาจ หากพิจารณาตามทฤษฎีปมด้อย (Inferiority Complex) ที่กล่าวไว้ว่าปมด้อยที่มาจากประสบการณ์ในทางลบตั้งแต่วัยเยาว์ เป็นสาเหตุให้มีการกระทำความผิดเพื่อเรียกร้องความสนใจ โดยคิดว่าเป็นวิธีที่จะแสดงออกแล้วทำให้สาธารณชนสนใจ เพื่อชดเชยและทดแทนปมด้อยของตนเอง ทำให้เห็นได้ว่าแรงจูงใจทางสังคมนี้มีแนวโน้มที่จะนำไปสู่การกระทำผิดได้เช่นกัน ส่วนการกระทำผิดจะรุนแรงหรือไม่นั้น ขึ้นกับว่าผู้กระทำมีความต้องการที่จะชดเชยปมด้อยของตนในระดับใด

การป้องกันในกรณีนี้จึงอยู่ที่ว่าจะทำอย่างไรให้ผู้กระทำแสดงการเรียกร้องความสนใจ โดยที่ไม่อาศัยการเจาะระบบคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต เพื่อเป็นการสร้างปมเด่นให้ตนเอง ดังที่กล่าวไว้แล้วว่าปมด้อยเกิดจากประสบการณ์ด้านลบในวัยเยาว์ หากตอบอย่างตรงไปตรงมาแล้วการป้องกันก็คือให้งดเว้นการก่อให้เกิดประสบการณ์ทางด้านลบแก่เด็กในวัยเยาว์ ปัญหาที่ตามมาคือเป็นไปได้ที่จะห้ามมิให้เกิดประสบการณ์ด้านลบแก่เด็ก เพราะไม่อาจทราบได้ว่ากรกระทำใดของผู้ใหญ่ที่มีผลต่อความประพฤติของเด็กในอนาคต ในการตอบปัญหานี้ผู้เขียนเห็นว่าเมื่อต้นเหตุเกิดจากสภาพจิตใจของผู้กระทำที่เกิดจากการถูกปิดกั้น การป้องกันคือกระทำให้บุคคลนั้นมีสภาพจิตใจที่เข้มแข็งและยอมรับสภาพที่เกิดขึ้นกับตนเองได้ ซึ่งสถาบันที่มีส่วนสำคัญในการสร้างภูมิคุ้มกันดังกล่าวได้แก่สถาบันครอบครัว ซึ่งสามารถแนะนำอย่างมีเหตุผลได้ว่ากรกระทำใดเป็นที่ยอมรับของสังคมและการกระทำใดไม่เป็นที่ยอมรับ ซึ่งหากกระทำได้เช่นนี้แล้วน่าจะลดการเจาะระบบคอมพิวเตอร์ฯ ที่มีแรงจูงใจทางสังคมได้มากขึ้นอีกทั้งยังสามารถลดการกระทำผิดได้ในอนาคต

### ๑.๓.๒ กรณีการกระทำของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตที่เกิดจากแรงจูงใจทางเทคนิค (Technical Motivation)

เมื่อพิจารณาทฤษฎีทางอาชญวิทยาคือทฤษฎีวัฒนธรรมรอง (Sub-Culture Theory) ที่อธิบายว่าวัฒนธรรมย่อยของบุคคลที่กระทำผิดนั้น เกิดขึ้นภายในวัฒนธรรมของสังคม ผู้กระทำผิดมักจะยึดถือวัฒนธรรมย่อยของตนเองเป็นสิ่งที่ถูกต้อง ผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตที่มีแรงจูงใจทางเทคนิคนี้ เป็นเสมือนผู้ยึดถือวัฒนธรรมรองที่คิดว่า การที่ตนเจาะระบบคอมพิวเตอร์ของผู้อื่นแม้โดยไม่ได้รับอนุญาต แต่เพื่อช่วยเหลือแก้ไขข้อบกพร่องภายในระบบคอมพิวเตอร์ให้ผู้อื่น เป็นสิ่งที่ถูกต้อง ซึ่งนำไปสู่การกระทำผิดโดยไม่สนใจว่าจะเป็นการละเมิดสิทธิของผู้อื่นหรือไม่

การป้องกันไม่ให้เกิดแรงจูงใจดังกล่าวคือการแสดงให้เห็นให้ผู้กระทำผิดเห็นว่า แม้การกระทำของตนจะเป็นการช่วยเหลือผู้อื่น แต่อย่างไรเสียต้องพึงระลึกว่า การกระทำของตนต้องเป็นการกระทำที่มีวิถีทางโดยชอบธรรมที่จะนำไปสู่การช่วยเหลืออื่นๆ มิเช่นนั้นแล้วแม้จะเป็นการกระทำโดยมีเจตนาดีก็หาได้ชื่อว่าเป็นการกระทำที่ถูกต้องและไม่ต่างกับการกระทำผิดโดยทั่วไปอย่างใดเลย

### ๑.๓.๓ กรณีการกระทำของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตที่เกิดจากแรงจูงใจทางการเมือง (Political Motivations)

กลุ่มแรงจูงใจทางการเมืองนี้เป็นกลุ่มที่มีความเชื่อรุนแรงและขัดแย้งกับลักษณะและระบบการปกครองในปัจจุบัน ซึ่งทฤษฎีความขัดแย้งทางวัฒนธรรม (Theory of Culture Conflict) ชี้ให้เห็นว่าความขัดแย้งทางวัฒนธรรมเป็นสาเหตุนำไปสู่การเกิดอาชญากรรม เมื่อกลุ่มชนที่มีวัฒนธรรมที่ต่ำกว่า ไปอยู่ท่ามกลางสังคมใหญ่ ซึ่งมีวัฒนธรรมที่มาตรฐานสูงกว่า และไม่สามารถปรับตัวให้เข้ากับวัฒนธรรมที่สูงกว่าได้ จึงเกิดการขัดแย้งและละเมิดกฎระเบียบและมาตรฐานของวัฒนธรรมที่สูงกว่า ดังเช่นการเปลี่ยนแปลงระบบการปกครองในประเทศจีนมาเป็นระบบการปกครองแบบสังคมนิยมในปัจจุบัน ซึ่งทำให้กลุ่มชนที่มีความคิดทางเสรีนิยมไม่สามารถปรับตัวให้เข้ากับระบบการปกครองใหม่ได้ จึงเคลื่อนไหวก่อความไม่สงบและต่อต้านระบบการปกครอง ทำให้เห็นได้ว่าผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตที่มีแรงจูงใจเช่นนี้ มีแนวโน้มที่จะกระทำผิดโดยก่อให้เกิดความไม่สงบเรียบร้อยในสังคมโดยผ่านทางคอมพิวเตอร์ได้เช่นกัน

การป้องกันไม่ให้เกิดแรงจูงใจเช่นนี้จึงอยู่ที่ว่า ทำอย่างไรให้บุคคลเหล่านี้สามารถปรับตัวและยอมรับกับสภาพที่ตนเป็นอยู่ได้

### ๑.๓.๔ กรณีการกระทำของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตที่เกิดจากแรงจูงใจทางการเงิน (Financial Motivations)

กลุ่มนี้เป็นกลุ่มที่กระทำเพื่อประโยชน์ของตนเองด้วยเหตุผลทางเศรษฐกิจ ดังที่ วิลเลียม บองเช นักอาชญาวิทยาเห็นด้วยว่าระบบเศรษฐกิจเป็นตัวก่อให้เกิดบรรยากาศของกระบวนการผลักดันให้มีพฤติกรรมอาชญากร และพบว่าในสังคมที่มีการแข่งขันทางด้านเศรษฐกิจ ที่มุ่งหวังผลกำไรจนเกินควรและประกอบธุรกิจแบบเห็นแก่ประโยชน์ส่วนตน โดยขาดความรับผิดชอบต่อส่วนรวมแล้ว จะส่งผลให้สังคมเกิดความสับสน ชัดแย้ง และจากสถิติอาชญากรรมส่วนมากพบว่าผู้กระทำผิดส่วนใหญ่เป็นผู้มีฐานะยากจนและขาดเสถียรภาพในการประกอบอาชีพ แม้ว่าการค้นพบของ บองเช มีผู้โต้แย้งเนื่องจากมีผู้กระทำความผิดหลายประเภทที่ไม่ได้มีพื้นฐานมาจากปัญหาความยากจนเช่นอาชญากรรมคอเช็ตขาว (white-collar crime) แต่อย่างไรก็ตามก็ไม่สามารถปฏิเสธได้ว่าเหตุผลทางเศรษฐกิจมีส่วนเกี่ยวข้องกับสาเหตุการกระทำความผิดเช่นกัน

*การป้องกัน* ในกรณีนี้เป็นปัญหาในระดับรัฐในการดูแลความเป็นอยู่ของประชาชน ส่งเสริมให้บุคคลมีเสถียรภาพในการทำงานและสวัสดิการสังคม เพราะเมื่อทุกคนมีความเป็นอยู่ที่ดีขึ้นอย่างน้อยก็เป็นการลดจำนวนบุคคลที่คิดจะหันมากระทำความผิดได้เช่นกัน

### ๑.๓.๕ กรณีการกระทำของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตที่เกิดจากแรงจูงใจทางรัฐบาล (Governmental Motivations)

ผู้เจาะระบบคอมพิวเตอร์ที่มีแรงจูงใจเช่นนี้ จะแสดงออกซึ่งความขัดแย้งระหว่าง ๒ กลุ่ม ซึ่งเป็นระดับความขัดแย้งที่สูงกว่าในกลุ่มแรงจูงใจทางการเมือง ที่เป็นความขัดแย้งระหว่างบุคคลกับลักษณะการปกครอง ผู้เจาะระบบคอมพิวเตอร์ที่มีแรงจูงใจทางรัฐบาลนี้เป็นความขัดแย้งระหว่าง ๒ รัฐบาล ดังเช่นเป็นการขัดแย้งระหว่างรัฐต่อรัฐหรือระหว่างประเทศ ๒ ประเทศขัดแย้งกัน เมื่อศึกษาถึงทฤษฎีทางอาชญาวิทยาเพื่อที่จะนำมาอธิบายการกระทำที่เกิดจากแรงจูงใจทางรัฐบาล ว่ามีแนวโน้มที่จะนำไปสู่การกระทำความผิดหรือไม่ ทำให้สังเกตได้ประการหนึ่งว่า ทฤษฎีทางอาชญาวิทยาใดที่กล่าวถึงสาเหตุของการกระทำความผิด ว่ามีสาเหตุมาจากความขัดแย้งหรือความไม่ลงรอยในแนวความคิด สามารถนำมาประกอบการพิจารณาการกระทำของผู้เจาะระบบคอมพิวเตอร์ที่มีแรงจูงใจทางรัฐบาลได้ทั้งสิ้น ดังเช่น ทฤษฎีความขัดแย้งทางวัฒนธรรม และทฤษฎีวิวัฒธรรมรอง

ถ้าหากถือว่าโลกคือสังคมหนึ่ง ที่ภายในประกอบด้วยประเทศที่มีวัฒนธรรมแตกต่างกัน บางประเทศอาจมีวัฒนธรรมที่ไม่สามารถเข้ากันได้กับวัฒนธรรมของประเทศอื่นๆ หรือประเทศข้างเคียง หรือประเทศส่วนใหญ่มีวัฒนธรรมที่สูงกว่า วัฒนธรรมของประเทศใดที่ต่ำกว่าก็ไม่สามารถปรับตัวให้เข้ากับวัฒนธรรมของสังคมโลกได้ ดังเช่น ปัญหาการก่อการร้ายระหว่างประเทศ หรือด้วยวัฒนธรรมที่ต่างออกไปเนื่องจากอิทธิพลทางศาสนาหรือประวัติศาสตร์นั้น ได้ถูกยึดถือว่าเป็นวิถีทางที่ถูกต้องและถือว่าวัฒนธรรมของสังคมโลกหรือประเทศอื่นไม่ถูกต้องซึ่งขัดแย้งกับวัฒนธรรมส่วนใหญ่ดังเช่น ประเทศจีนและประเทศไต้หวัน ประเทศอินเดียและบังคลาเทศ หรือประเทศอิสราเอลและประเทศที่นับถือศาสนาอิสลาม เป็นต้น

สำหรับผู้เจาะระบบคอมพิวเตอร์นั้นไม่ใช่ประเทศและจะถือว่าเป็นตัวแทนของประเทศไม่ได้เช่นกัน ผู้เขียนเพียงต้องการแสดงให้เห็นระดับของความขัดแย้งว่ามีระดับที่ต่างจากแรงจูงใจทางการเมืองที่จำกัดอยู่ภายในประเทศ แต่การเปรียบเทียบนี้ก็ทำให้ทราบได้ประการหนึ่งว่า ผู้เจาะระบบคอมพิวเตอร์ที่มีแรงจูงใจทางรัฐบาลมีแนวโน้มที่ก่อให้เกิดการกระทำคามผิดได้ตามทฤษฎีทางอาชญาวิทยา

*การป้องกัน* นอกจากการกระทำให้ผู้กระทำมีความสามารถในการปรับตัวและยอมรับกับสภาพที่ตนเป็นอยู่เพื่อหลีกเลี่ยงปัญหาความขัดแย้ง ดังเช่นกรณีแรงจูงใจทางการเมืองแล้วยังต้องแสดงให้เห็นให้ผู้ที่มีแรงจูงใจทางรัฐบาลทราบว่าประเทศใดประเทศหนึ่งไม่สามารถจะอยู่ในสังคมโลกได้โดยไม่ติดต่อกับภายนอกและการก่อให้เกิดความไม่สงบเรียบร้อยในประเทศอื่นๆ หากไม่ทำให้เกิดความไม่สงบเรียบร้อยเพียงในประเทศนั้นๆ ไม่ แต่มีผลถึงประเทศข้างเคียงหรือประเทศอื่นๆ ทั่วทั้งโลกด้วยเช่นกัน

นอกจากทฤษฎีทางอาชญาวิทยาที่นำมาพิจารณาประกอบแรงจูงใจดังกล่าวแล้วยังมีทฤษฎีทางอาชญาวิทยาอีกสองทฤษฎีที่ผู้เขียนเห็นว่าน่าสนใจและสามารถอธิบายถึงแนวโน้มในการกระทำคามผิดของผู้มีแรงจูงใจทั้งห้าประการได้ คือ ทฤษฎีความสัมพันธ์แตกต่างและทฤษฎีสภาพไร้บรรทัดฐาน แต่อย่างไรก็ตามทั้งสองทฤษฎีนี้ผู้เขียนถือว่าเป็นการอธิบายแรงจูงใจที่เกิดจากแรงผลักดันภายนอกมากกว่าที่จะเป็นแรงจูงใจที่เกิดขึ้นจากความคิดภายในของผู้กระทำผิดเองดังเช่นแรงจูงใจทั้งห้าประการดังกล่าวข้างต้น

- ทฤษฎีความสัมพันธ์แตกต่างเป็นทฤษฎีที่มีความเห็นว่าอาชญากรรมเป็นผลของการคบค้าสมาคมระหว่างกลุ่มบุคคลกับแบบอาชญากร ยิ่งคบหาสมาคมสม่ำเสมอจะยิ่งทำให้บุคคลนั้น

เป็นอาชญากรเร็วขึ้น ซึ่งหากนำทฤษฎีนี้มาปรับกับผู้เจาะระบบคอมพิวเตอร์จะทำให้เห็นได้ว่า หากผู้เจาะระบบคอมพิวเตอร์ได้คบหาสมาคมกับบุคคลที่ประพฤตินั้นเป็นผู้เจาะระบบคอมพิวเตอร์ซึ่งเป็นแม่แบบในการกระทำความผิด ก็จะมีส่วนที่ทำให้บุคคลทั่วไปกระทำความผิดได้เร็วขึ้น

- ทฤษฎีสภาพไร้บรรทัดฐาน ซึ่งเป็นทฤษฎีที่มีแนวคิดว่าการกระทำความผิดเกิดขึ้นเมื่อบรรทัดฐานของสังคมไม่สามารถควบคุมการกระทำของบุคคลในสังคม หรือไม่สามารถตอบสนองความต้องการทางสังคมของบุคคล ทฤษฎีนี้อธิบายได้ดีในประเทศที่การเปลี่ยนแปลงทางสภาพแวดล้อม เศรษฐกิจและเทคโนโลยีอย่างรวดเร็ว รวมถึงประเทศไทยซึ่งยังไม่มีบรรทัดฐานหรือกฎหมายในการควบคุมการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ทำให้บุคคลเลือกกระทำความผิดเพราะไม่มีกรอบที่เป็นบรรทัดฐานให้สังคมดูแลหรือลงโทษผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์

เมื่อศึกษาคำอธิบายทางอาญาวิทยาประกอบกับแรงจูงใจทั้ง ๕ ประการแล้วจะเห็นได้ว่าแรงจูงใจทั้ง ๕ ประการมีแนวโน้มที่จะไปสู่การกระทำความผิดตามลักษณะทฤษฎีทางอาญาวิทยา และสำหรับนโยบายทางอาญาในข้อที่ว่าด้วยวิธีการป้องกันความผิดโดยจำกัดมูลเหตุแห่งอาชญากรรม ผู้เขียนสรุปได้เป็น ๓ ประการ ดังนี้คือ

๑. ให้ความสำคัญกับครอบครัวในการปลูกฝังความคิดที่ถูกต้อง เพื่อเป็นการป้องกันแรงจูงใจทางสังคม ทางเทคนิคและทางการเมือง
๒. ให้ความสำคัญต่อความเป็นอยู่หรือสวัสดิการของประชาชน เพื่อเป็นการป้องกันแรงจูงใจทางการเงิน
๓. ให้ความสำคัญกับความสัมพันธ์ระหว่างประเทศและวิถีทางการทูตเพื่อลดปัญหาความขัดแย้งระหว่างรัฐ เพื่อป้องกันแรงจูงใจทางรัฐบาล

โดยสรุป แม้การศึกษาจะทำให้ทราบถึงสาเหตุและการป้องกันการกระทำความผิดของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต แต่การศึกษาดังที่กล่าวมาอาศัยหลักการทางสังคมวิทยาและจิตวิทยาเข้ามาเกี่ยวข้องเป็นส่วนมาก คำแนะนำในการป้องกันการกระทำความผิดจึงเน้นหนักไปในด้านที่ต้องอาศัยความร่วมมือของสมาชิกในสังคม ดังนั้นสภาพบังคับจึงมีน้ำหนักน้อยและต้องกระทำร่วมกับมาตรการอื่น ดังเช่นการใช้มาตรการทางอาญาตามวิธีการทางนิติบัญญัติ ซึ่งจะได้ทำการศึกษาในลำดับต่อไป





## ๒. วิธีการทางนิติบัญญัติเพื่อจะได้ผลในทางป้องกันและปราบปรามการกระทำ ความผิด

การที่รัฐจะรักษาความสงบเรียบร้อยของสังคม รัฐต้องตั้งต้นจากนโยบายข้อแรกก่อนว่าจะถือเอาพฤติกรรมใดเป็นสิ่งไม่พึงปรารถนาอันควรกำหนดเอาว่าเป็น "อาชญากรรม"<sup>๓๓</sup> และถ้ารัฐต้องการให้บุคคลทั่วไปปฏิบัติตามมาตรฐานที่กำหนดไว้ บุคคลทั่วไปนั้นต้องทราบว่าจะอะไรคือมาตรฐาน ซึ่งเป็นแนวคิดที่มาตั้งแต่อดีต เรียกว่าหลัก Legality

### ๒.๑ หลัก Legality (The principle of Legality)

ความสำคัญของหลักนี้คือ รัฐไม่สามารถที่จะลงโทษประชาชนโดยปราศจากกฎหมายที่มีความชัดเจนเพียงพอที่จะเตือนประชาชนว่า รัฐจะลงโทษการกระทำใดๆได้ เมื่อมีบทบัญญัติว่าการกระทำนั้นเป็นความผิด

ซึ่งหลักการนี้ประกอบไปด้วย

๑. *Mullum crimen sine lege* คือ จะไม่เป็นความผิดโดยปราศจากกฎหมายที่บัญญัติไว้ว่าการกระทำใดเป็นความผิด

๒. *Void-for-vagueness* คือ ฝ่ายนิติบัญญัติจะต้องร่างกฎหมายที่ชัดเจนเพียงพอสำหรับประชาชนทั่วไปและเจ้าหน้าที่ผู้บังคับใช้กฎหมายเข้าใจได้

๓. *Ex post facto law* คือ กฎหมายไม่มีผลย้อนหลัง

๔. *Nulla poena sine lege* คือ จะไม่มีการลงโทษโดยปราศจากอำนาจที่ให้ไว้ในกฎหมาย<sup>๓๔</sup>

---

<sup>๓๓</sup> อาชญากรรม สามารถพิจารณาได้เป็นสองนัยคือ ประการแรก อาชญากรรมทางด้านกฎหมาย ซึ่งคือการกระทำอันเป็นการฝ่าฝืนหรือขัดกับกฎหมายที่วางไว้และผู้กระทำนั้นจะต้องได้รับโทษตามที่กำหนดไว้ในกฎหมาย ประการที่สองอาชญากรรมทางด้านสังคม โดยเพิ่งเล็งถึงความขัดแย้งระหว่างบุคคลกับสังคมเป็นหลัก การศึกษาในบทนี้เป็นการพิจารณาทางด้านสังคมเนื่องจาก เป็นการกำหนดนโยบายซึ่งยังไม่มีกรณีบัญญัติเป็นกฎหมาย

<sup>๓๔</sup> Joel Samaha, *criminal law* 4<sup>th</sup> edition (Minnesota: west publishing company, 1993), p. 43.

หลัก Legality นี้นำมาซึ่งปัญหาในการเอาผิดกับผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต กล่าวคือกฎหมายในประเทศไทยโดยเฉพาะกฎหมายอาญาไม่มีบทบัญญัติใดที่กล่าวถึงความรับผิดทางอาญาเกี่ยวกับคอมพิวเตอร์ ดังนั้นการศึกษาความรับผิดทางอาญาของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตโดยผ่านวิธีการทางนิติบัญญัตินี้จึงพบอุปสรรคซึ่งสามารถแสดงให้เห็นได้ดังต่อไปนี้ คือ

## ๒.๒ ปัญหาในการปรับใช้ประมวลกฎหมายอาญาในปัจจุบัน

สำหรับปัญหาการปรับใช้กฎหมายอาญาในปัจจุบันกับผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตนั้น ผู้เขียนขอแยกพิจารณาออกเป็น ๓ ขั้นตอน คือ

๑. ปัญหาการปรับบทกฎหมายกับกระทำต่อข้อมูลหรือระบบคอมพิวเตอร์ ภายหลังจากเจาะเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตได้แล้ว
๒. ปัญหาการปรับบทกฎหมายกับการกระทำก่อนหรือขณะเจาะระบบคอมพิวเตอร์
๓. ปัญหาการปรับบทกฎหมายกับการแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่มีอำนาจ

### ๒.๒.๑ กรณีการกระทำต่อข้อมูลและระบบคอมพิวเตอร์ที่เกิดขึ้นภายหลังจากเจาะเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตได้แล้ว

แม้ว่าระบบคอมพิวเตอร์จะหมายถึง องค์ประกอบทางคอมพิวเตอร์ที่ทำงานประสานกันในหลายส่วนดังที่ได้กล่าวไว้แล้ว แต่เป้าหมายของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตโดยแท้จริงแล้วอยู่ที่ส่วนข้อมูล (Data) และส่วนสารสนเทศ (Information) ซึ่งอยู่ภายในระบบคอมพิวเตอร์ เหตุนี้เมื่อผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเข้าไปในระบบคอมพิวเตอร์ได้แล้ว การกระทำใดๆที่เกิดขึ้นภายหลังจากนั้นจึงมีแนวโน้มที่จะเกี่ยวข้องกับข้อมูลและสารสนเทศในระบบคอมพิวเตอร์เป็นส่วนใหญ่ จนกระทั่งก่อให้เกิดกระแสในการตั้งคำถามที่ว่า หาก

เกิดมีการกระทำต่อข้อมูลดังกล่าวแล้ว กฎหมายที่มีอยู่ในปัจจุบันโดยเฉพาะประมวลกฎหมายอาญาจะเอาผิดกับผู้กระทำได้หรือไม่ ซึ่งเห็นได้จากในช่วงเวลาปลายศตวรรษที่ ๒๐ นี้ มีบทความทางวิชาการและการสัมมนา เพื่อหาแนวทางในการแก้ปัญหาย่างสม่ำเสมอ ซึ่งผู้เขียนขอสรุปปัญหาในส่วนการปรับใช้กฎหมายอาญากับการกระทำต่อข้อมูลภายในระบบคอมพิวเตอร์ดังนี้คือ

๑. การลักลอบเอาข้อมูลภายในระบบคอมพิวเตอร์ไปโดยไม่ได้รับอนุญาต มีการกระทำคือการ“เอาไป” มีกรรมของการกระทำคือ ข้อมูลภายในเครื่องคอมพิวเตอร์ แต่ไม่สามารถที่จะนำความผิดฐานลักทรัพย์มาปรับใช้กับการกระทำดังกล่าวได้เนื่องจากการ“เอาไป” ตามประมวลกฎหมายอาญามาตรา ๓๓๔<sup>๑๙</sup> นั้น ศาสตราจารย์จิตติ ดิงศภัทย์ได้อธิบายไว้ว่า “... เอาไปเป็นองค์ประกอบในส่วนการกระทำ หมายความว่าพหุทรัพย์เคลื่อนที่ไปจากการครอบครองของผู้อื่น จึงต้องมีการกระทำเป็นสองประการ คือแย่งการครอบครองประการหนึ่งและพาเคลื่อนที่ไปอีกประการหนึ่ง ...เพียงแต่แย่งการครอบครอง แต่ยังไม่ได้พหุทรัพย์เคลื่อนที่ไป ก็ยังไม่เป็นการลักทรัพย์สำเร็จ...”<sup>๒๐</sup> ซึ่งเมื่อพิจารณาข้อมูลภายในระบบคอมพิวเตอร์ แม้โดยทั่วไปจะเห็นว่ามี การเอาไปซึ่งข้อมูล แต่หาได้เป็นไปตามหลักเกณฑ์ในกฎหมายไม่ เพราะข้อมูลยังคงมีอยู่เช่นเดิม มิได้ถูก“เอาไป” ดังคำอธิบายดังกล่าว เพียงแต่เป็นการคัดลอกไปเท่านั้น ซึ่งกรณีนี้ไม่มีบทบัญญัติใดที่ห้ามการคัดลอกหรือการทำสำเนา จึงไม่ชัดเจนในการที่จะปรับใช้ความผิดฐานลักทรัพย์กับการเอาไปซึ่งข้อมูลภายในเครื่องคอมพิวเตอร์ นอกจากนี้ ปัญหาในเรื่องข้อมูลภายในเครื่องคอมพิวเตอร์ จะถือได้หรือไม่ว่าเป็นทรัพย์ตามความมุ่งหมายในกฎหมายอาญา ซึ่งยังเป็นปัญหาที่ยังถกเถียงกันอยู่

๒. เมื่อเข้าไปภายในระบบคอมพิวเตอร์แล้ว ได้ทำลายข้อมูลภายในเครื่องคอมพิวเตอร์ เช่นนี้จะถือได้หรือไม่ว่าเป็นการทำให้เสียหายตามประมวลกฎหมายอาญามาตรา ๓๕๘<sup>๒๐</sup> ซึ่งนอกจากปัญหาที่ว่าข้อมูลเป็นทรัพย์หรือทรัพย์สินดังกล่าวข้างต้นแล้ว การทำให้เสียหายหรือ

<sup>๑๙</sup> มาตรา ๓๓๔ ผู้ใดเอาทรัพย์ของผู้อื่น หรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วยไปโดยทุจริต ผู้นั้นกระทำความผิดฐานลักทรัพย์ ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินหกพันบาท

<sup>๒๐</sup> จิตติ ดิงศภัทย์,กฎหมายอาญา ภาค ๒ ตอน ๒ และภาค ๓ พิมพ์ครั้งที่ ๓ (กรุงเทพมหานคร: เนติบัณฑิตยสภา, ๒๕๓๒), หน้า ๒๔๙๕.

<sup>๒๑</sup> มาตรา ๓๕๘ ผู้ใดทำให้เสียหาย ทำลาย ทำให้เสื่อมค่าหรือทำให้ไร้ประโยชน์ซึ่งทรัพย์ของผู้อื่นหรือผู้อื่นเป็นเจ้าของรวมอยู่ด้วย ผู้นั้นกระทำความผิดฐานทำให้เสียหาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ

ทำลายซึ่งข้อมูลทางคอมพิวเตอร์นั้นสามารถกระทำได้โดยวิธีการทางเทคโนโลยี เช่นการใช้ชุดคำสั่งสั่งให้เครื่องคอมพิวเตอร์ลบชุดคำสั่งหรือข้อมูลที่มีอยู่ ซึ่งการทำให้เสียหายโดยใช้คำสั่งเช่นนี้ไม่สามารถชี้ชัดได้ว่าเป็นการทำให้เสียหายตามองค์ประกอบความผิดฐานทำให้เสียหายหรือไม่

๓. กรณีการเติมหรือตัดทอนข้อมูลซึ่งเป็นความผิดตามมาตรา ๒๖๔<sup>๒๒</sup> มีปัญหาในการปรับใช้กฎหมายคือ ตามประมวลกฎหมายอาญามาตรา ๑(๗) “เอกสาร” หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผังหรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพหรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น ซึ่งจะมีปัญหาว่าข้อมูลภายในระบบคอมพิวเตอร์นั้นทำให้ปรากฏความหมายโดยอาศัยรหัสซึ่งเป็นภาษาคอมพิวเตอร์ จะถือว่าเป็นเอกสารตามความหมายในประมวลกฎหมายอาญาหรือไม่ นอกจากนี้กรณีการแก้ไขตัดทอนข้อความหรือแก้ไขด้วยประการใดๆ ในเอกสารนั้นจะต้องมีเอกสารที่แท้จริงอยู่ แต่ด้วยลักษณะพิเศษของคอมพิวเตอร์ การแก้ไขที่กระทำต่อข้อมูลนั้นไม่ปรากฏร่องรอยการแก้ไข หรือตัดแปลง จึงเป็นการยากที่จะทราบว่าข้อมูลใดเป็นเอกสารที่แท้จริง

จากตัวอย่างปัญหาการปรับใช้กฎหมายอาญาดังกล่าว ผู้เขียนจึงเห็นว่าเมื่อกฎหมายอาญาที่ใช้บังคับอยู่ในปัจจุบันไม่สามารถรองรับการกระทำเกี่ยวกับคอมพิวเตอร์ได้ จึงเป็นการสมควรที่จะบัญญัติกฎหมายขึ้นใหม่เป็นพิเศษ และไม่ควรรสร้างความปลอดภัยต่อหลักเกณฑ์ทางกฎหมาย ดังเช่นปัญหาการลักกระแสไฟฟ้า ตามคำพิพากษาฎีกาที่ ๘๗๗/๒๕๐๑ (ประชุมใหญ่) ซึ่งผู้เขียนเห็นคล้อยตามกับเหตุผลดังที่ ดร.คณิต ณ นคร<sup>๒๓</sup> ได้กล่าวไว้ว่า

“...ไฟฟ้าเป็นพลังงานหาใช้ทรัพย์ไม่ สิทธิในไฟฟ้าจึงไม่ใช่กรรมสิทธิ์ ทั้งการที่จะแสดงอำนาจแท้จริงเหนือไฟฟ้าจะเป็นไปได้อย่างไร ผู้เขียนยังมองไม่เห็น ดังนั้นการลักเอากระแสไฟฟ้าไปจึงหาใช้การเอาไปตามความหมายของการลักทรัพย์ไม่ การลักกระแสไฟฟ้าจึงไม่เป็นความผิด

<sup>๒๒</sup> มาตรา ๒๖๔ ผู้ใดทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในเอกสารที่แท้จริง หรือประทับตราปลอม หรือลงลายมือชื่อปลอมในเอกสาร โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ถ้าได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง ผู้นั้นกระทำความผิดฐานปลอมเอกสาร ต้องระวางโทษ .....

<sup>๒๓</sup> คณิต ณ นคร . " คุณธรรมทางกฎหมายกับการใช้กฎหมายอาญา , "วารสารอัยการ ปีที่ ๓ , (มกราคม ๒๕๒๓) : ๕๕-๖๑.

ฐานลัทธิทฤษฎี และจากการพิจารณาในเรื่องคุณธรรมทางกฎหมาย<sup>๒๔</sup> นี้เองที่เป็นเหตุผลอันหนึ่งที่ว่าทำไมในเยอรมันจึงต้องบัญญัติเรื่องลัทธิกระแสไฟฟ้าขึ้นเป็นเอกเทศ”

เป็นที่ทราบแล้วว่า คำว่าทฤษฎีและทฤษฎีสินในกฎหมายอาญายังคงใช้ในความหมายที่สับสนกันอยู่ แต่แม้ว่าความสับสนดังกล่าวยังคงมีอยู่ การปรับข้อเท็จจริงที่เกิดขึ้นกับตัวบทกฎหมาย ก็ยังต้องการตัวบทกฎหมายที่มีความแน่นอน ดังคำกล่าวของ ศาสตราจารย์จิตติ ดิงส์คีย์ท์ที่ว่า “ตามปกติการใช้กฎหมายก็ต้องอาศัยความหมายที่ปรากฏในกฎหมายที่บัญญัติถึงถ้อยคำนั้นไว้โดยตรง แม้จะบัญญัติไว้ในกฎหมายอื่น เว้นแต่ตามบทบัญญัตินั้นๆ จะมีข้อความแสดงให้เห็นได้ว่ามิได้ประสงค์ให้มีความหมายดังที่บัญญัติไว้ในกฎหมายอื่นนั้น”<sup>๒๕</sup> ดังนั้นจึงมิใช่เพียงการอาศัยดุลพินิจของศาลในการกำหนดหลักเกณฑ์ของกฎหมายตามอำเภอใจ จนผิดไปจากเจตนารมณ์ดั้งเดิม เมื่อยังไม่มีข้อยุติว่าไฟฟ้าเป็นทฤษฎีตามความหมายในมาตรา ๓๓๔ หรือไม่ ฉะนั้นเหตุใดมาตรา ๓๓๔ จึงเป็นมาตราที่จะนำมาปรับใช้กับข้อเท็จจริงดังกล่าวได้

ดังนั้นเมื่อข้อมูลภายในคอมพิวเตอร์มีลักษณะพิเศษและเป็นสิ่งที่เกิดขึ้นใหม่ในขณะประมวลกฎหมายอาญามีได้มีเจตนารมณ์ที่จะกำหนดความหมายแต่ดั้งเดิม การบัญญัติกฎหมายขึ้นใหม่จึงเป็นหนทางหนึ่งในการแก้ปัญหาในเรื่องนำบทกฎหมายที่มีอยู่ไปใช้โดยผิดเจตนารมณ์ของกฎหมายในมาตรานั้น และจะทำให้ไม่มีการกล่าวอ้างว่าขณะที่มีการบัญญัติกฎหมายในเรื่องนั้นๆ เจตนารมณ์ของกฎหมายไม่สามารถทำนายได้ล่วงหน้าว่าในอนาคตจะมีการกระทำเช่นนี้เกิดขึ้น จึงเลือกที่จะนำกฎหมายอาญาที่มีอยู่มาใช้โดยขยายความให้ครอบคลุมพฤติกรรมใหม่ๆที่เกิดขึ้นในอนาคต ซึ่งเป็นสิ่งที่ผู้เขียนไม่เห็นด้วย

## ๒.๒.๒ กรณีการกระทำก่อนหรือขณะเจาะระบบคอมพิวเตอร์

การพิจารณาการกระทำก่อนหรือขณะเจาะระบบคอมพิวเตอร์นั้น ต้องทำความเข้าใจในเบื้องต้นก่อนว่า การเริ่มต้นของการกระทำที่จะเป็นความผิดย่อมต้องมีเหตุการณ์เป็นมาตามลำดับ โดยเริ่มจากความคิดทบทวนที่จะกระทำ (conception) ความตกลงใจ (resolution) การเตรียม

<sup>๒๔</sup> คุณธรรมทางกฎหมาย เป็นเรื่องทางความคิดที่กฎหมายประสงค์จะคุ้มครอง เป็นส่วนที่แฝงอยู่ในบทบัญญัติความผิดฐานต่างๆ และเป็นสภาพที่พึงปรารถนาที่กฎหมายต้องการประกันจากการล่วงละเมิด

<sup>๒๕</sup> จิตติ ดิงส์คีย์ท์. คำอธิบายประมวลกฎหมายอาญาภาค ๒ ตอนที่ ๒ และภาค ๓. พิมพ์ครั้งที่ ๒ (กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, ๒๕๑๔), หน้า ๒๒๕๗

(preparation) และการลงมือ (commencement)<sup>๒๖</sup> การกระทำ “ก่อน” เจาะระบบคอมพิวเตอร์นั้น เมื่อเทียบกับลำดับข้างต้นจะอยู่ในขั้นตอนการเตรียมที่จะกระทำความผิด สำหรับการกระทำ “ขณะ” เจาะระบบคอมพิวเตอร์เทียบได้กับการกระทำขั้นลงมือกระทำความผิด ซึ่งแยกพิจารณาได้ดังต่อไปนี้ คือ

#### การเตรียมกระทำความผิด (preparation)

การปรับบทกฎหมายในปัจจุบันกับการกระทำในขั้นตอนก่อนเจาะระบบคอมพิวเตอร์ ประสบปัญหาดังเช่นกรณีการกระทำต่อข้อมูลภายหลังจากเจาะเข้าไปในระบบคอมพิวเตอร์แล้ว เพราะไม่มีกฎหมายใดที่บัญญัติให้การเตรียมเพื่อเจาะระบบคอมพิวเตอร์เป็นความผิด แต่อย่างไรก็ตามหากตั้งคำถามต่อไปว่าถ้าการเจาะระบบคอมพิวเตอร์เป็นความผิด ควรจะมีบทบัญญัติว่าด้วยการเตรียมกระทำความผิดเพื่อลงโทษผู้เตรียมเจาะระบบคอมพิวเตอร์หรือไม่ ซึ่งก่อนที่จะตอบปัญหาดังกล่าวในเบื้องต้นต้องทราบว่าในประมวลกฎหมายอาญามีการกำหนดความผิดในชั้นเตรียมไว้เพียง ๒ กรณีคือ กรณีที่หนึ่ง เป็นการเตรียมกระทำความผิดที่ร้ายแรงพอที่จะถือเป็นความผิดเท่ากับความสำเร็จ ได้แก่มาตรา ๑๐๗-๑๑๐, ๑๑๔ และ ๑๒๔ กรณีที่ ๒ คือ กรณีที่เป็นการยากในการพิสูจน์ความผิดในชั้นพยายาม ดังเช่น ความผิดฐานเตรียมเพื่อวางเพลิงในมาตรา ๒๑๙<sup>๒๗</sup> ซึ่งศาสตราจารย์จิติ ติงสภักดิ์ ได้ให้คำอธิบายในมาตรา ๒๑๙ ดังนี้คือ “... มาตรานี้มีข้อความทำนองเดียวกับมาตรา ๑๘๗ วรรค ๓ แห่งกฎหมายลักษณะอาญาเดิมที่เพิ่มเติมขึ้นโดยพระราชบัญญัติแก้ไขเพิ่มเติมกฎหมายลักษณะอาญา พ.ศ. ๒๔๗๕ มาตรา ๕ เนื่องจากความยากในการพิสูจน์ความผิดฐานพยายามวางเพลิง ซึ่งมักจะยังไกลจากผล ไม่เข้าชั้นพยายาม จึงเอาผิดตั้งแต่ชั้นเตรียมเช่นเดียวกับชั้นพยายาม...”

ดังนั้นหากไม่ประสบปัญหาดัง ๒ กรณีดังกล่าวข้างต้นแล้ว ก็ไม่สมควรที่จะเอาผิดในชั้นเตรียมเพื่อเจาะระบบคอมพิวเตอร์ ซึ่งเพียงการเตรียมเพื่อเจาะระบบคอมพิวเตอร์นั้น เห็นได้ชัดว่าไม่ใช่กรณีร้ายแรงเหมือนกับ มาตรา ๑๐๗-๑๑๐<sup>๒๘</sup>, ๑๑๔<sup>๒๙</sup> และ ๑๒๔<sup>๓๐</sup> ส่วนว่ายากที่จะ

<sup>๒๖</sup> จิติ ติงสภักดิ์, คำอธิบายประมวลกฎหมายอาญามาตรา ๑, หน้า ๒๗๘.

<sup>๒๗</sup> ประมวลกฎหมายอาญามาตรา ๒๑๙ ผู้ใดเตรียมเพื่อกระทำความผิดดังกล่าวในมาตรา ๒๑๙ หรือมาตรา ๒๑๘ ต้องระวางโทษเช่นเดียวกับพยายามกระทำความผิดนั้นๆ

พิสูจน์ความผิดหรือไม่นั้น ผู้เขียนเห็นว่าคำอธิบายของศาสตราจารย์จิติ ดิงศภทิพย์ ในส่วนของ มาตรา ๒๑๙ ข้างต้นนั้น ต้องการที่จะแสดงให้เห็นว่าการกระทำบางการกระทำหากนำหลักทาง กฎหมายอาญามาปรับแล้ว การกระทำนั้นยังไม่ถึงขั้นที่จะถือว่าเป็นการลงมือกระทำความผิด เพราะยังไกลจากผล ดังนั้นเมื่อเป็นการยากที่จะพิสูจน์ว่าการกระทำดังกล่าวเป็นการลงมือกระทำ หรือยัง จึงบัญญัติกฎหมายลงไปเสียเลยว่าการกระทำขั้นเตรียมการก็เป็นความผิดแล้ว ดังเช่น การเอาเชื้อเพลิงมาวางไว้เพื่อเตรียมจุดไฟ การกระทำเช่นนี้ยังห่างไกลที่จะพิสูจน์ว่าเป็นการลงมือ กระทำหรือยัง แต่เมื่อรัฐเห็นว่าการกระทำดังกล่าวสมควรห้ามปราม แม้ยังอยู่ในขั้นเตรียมจึง บัญญัติการเตรียมเพื่อวางเพลิงเผาทรัพย์เป็นความผิด ซึ่งเมื่อนำมาเปรียบเทียบกับ การเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตความสำคัญจึงอยู่ที่ว่าเป็นการสมควรและจำเป็นต้องห้าม การเจาะระบบคอมพิวเตอร์ตั้งแต่ขั้นเตรียมการหรือไม่ ซึ่งในปัญหานี้ผู้เขียนเห็นว่าแม้การ เจาะระบบคอมพิวเตอร์จะมีความร้ายแรงในระดับหนึ่ง แต่คงไม่ถึงระดับเดียวกับมาตรา ๑๐๗- ๑๑๐, ๑๑๔ และ ๑๒๔ อีกทั้งการเตรียมอุปกรณ์ในการเจาะระบบคอมพิวเตอร์กับการเตรียมน้ำ มันเพื่อวางเพลิงเผาทรัพย์ การเตรียมเพื่อวางเพลิงแม้จะไกลกว่าการที่จะถือว่าเป็นการลงมือ กระทำ แต่ยังถือว่าใกล้ชิดกว่าการเตรียมอุปกรณ์เพื่อการเจาะระบบคอมพิวเตอร์ เพราะการเจาะ ระบบคอมพิวเตอร์ต้องอาศัยการเตรียมเครื่องมือ อาศัยความมานะอดทน เพื่อหารหัสผ่านซึ่งต่าง กับการวางเพลิงที่ต้องการเพียงไม้ขีดไฟที่หาได้ง่ายโดยทั่วไป จึงเป็นเหตุผลหนึ่งที่สนับสนุนให้ผู้ เขียนเห็นว่าไม่สมควรที่จะกำหนดให้การเตรียมเพื่อเจาะระบบคอมพิวเตอร์เป็นความผิด อีกทั้งนอกจากการพิจารณาทางทฤษฎี หากพิจารณาในเรื่องการรักษาความสงบเรียบร้อยของสังคม เปรียบเทียบระหว่างการเตรียมเพื่อวางเพลิงและการเตรียมเพื่อเจาะระบบคอมพิวเตอร์ เห็นได้ชัดว่าการเตรียมเพื่อวางเพลิงมีแนวโน้มที่จะขัดต่อความสงบเรียบร้อยของสังคมได้ชัด เจนกว่าการเตรียมการเพื่อเจาะระบบคอมพิวเตอร์

<sup>๒๘</sup> เป็นบทบัญญัติในหมวดที่ ๑ ความผิดต่อองค์พระมหากษัตริย์ พระราชินี รัชทายาท และผู้สำเร็จราชการ แทนพระองค์ ลักษณะ ๑ ว่าด้วยความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร

<sup>๒๙</sup> เป็นบทบัญญัติในหมวดที่ ๒ ความผิดต่อความมั่นคงของรัฐภายในราชอาณาจักร ในลักษณะ ๑ ว่า ด้วยความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร

<sup>๓๐</sup> เป็นบทบัญญัติในหมวดที่ ๓ ความผิดต่อความมั่นคงของรัฐภายนอกราชอาณาจักร ในลักษณะ ๑ ว่าด้วยความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร

## การกระทำอย่างไรเป็นการลงมือเจาะระบบคอมพิวเตอร์

การลงมือเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเทียบได้กับการกระทำ “ขณะ” เจาะระบบคอมพิวเตอร์ คือเริ่มจากการเจาะระบบคอมพิวเตอร์โดยใช้ความรู้หรือเครื่องมือต่างๆ ยกตัวอย่างเช่น นาย ก. มีความคิดที่จะเจาะระบบคอมพิวเตอร์ของธนาคาร ข. ขั้นตอนแรกคือ การเตรียมในการเจาะระบบคอมพิวเตอร์ซึ่งได้แก่การศึกษาระบบคอมพิวเตอร์ของธนาคาร ข. และหาเครื่องมือและอุปกรณ์ที่จะช่วยในการถอดรหัส ขั้นตอนที่สองเป็นการเริ่มเจาะระบบคอมพิวเตอร์ ซึ่งต้องไม่สับสนว่าการเปิดเครื่องคอมพิวเตอร์ การต่อโทรศัพท์หรือการเชื่อมต่อสำเร็จระหว่างเครื่องคอมพิวเตอร์ด้วยกันเป็นการลงมือเจาะระบบคอมพิวเตอร์แล้ว การเจาะระบบคอมพิวเตอร์เริ่มขึ้นเมื่อนาย ก. เข้าไปถึงเป้าหมายถึงระบบคอมพิวเตอร์ของธนาคาร ข. และเมื่อได้รับการร้องขอจากเครื่องคอมพิวเตอร์เพื่อให้แสดงสิทธิโดยชอบที่จะใช้ระบบคอมพิวเตอร์ การที่นาย ก. เริ่มกรอกข้อความ ตัวเลขหรือรหัสเพื่อแสดงตน นั่นคือการเริ่มลงมือกระทำการเจาะระบบคอมพิวเตอร์<sup>๓๐</sup>

ดังนั้นถ้าหากนาย ก. สามารถเจาะระบบคอมพิวเตอร์และเข้าไปได้ก็เป็น การลงมือสำเร็จ หากไม่สามารถเข้าไปได้จะเป็นการพยายามเจาะระบบคอมพิวเตอร์ ซึ่งสามารถแยกพิจารณาได้เป็น ๒ ประการ คือ ประการแรกเมื่อเจาะระบบคอมพิวเตอร์สำเร็จและประการที่สองการพยายามเจาะระบบคอมพิวเตอร์ (กระทำไม่สำเร็จ) สำหรับในประการแรกผู้เขียนจะนำไปกล่าวในตอนต่อไปคือในตอนที่ ๕ ในที่นี้จะกล่าวถึงเฉพาะในประการที่สองคือกระทำการเจาะระบบคอมพิวเตอร์ไม่สำเร็จ

## การพยายามเจาะระบบคอมพิวเตอร์

การพยายามกระทำความผิดตามประมวลกฎหมายอาญามาตรา ๘๐ ได้บัญญัติไว้ว่า “ผู้ใดลงมือกระทำความผิดแต่กระทำไปไม่ตลอด หรือกระทำไปตลอดแล้วแต่การกระทำนั้นไม่บรรลุผล ผู้นั้นพยายามกระทำความผิด.....” เมื่อทราบแล้วว่าการลงมือกระทำความผิดคือการเริ่มกรอกข้อความ รหัสหรือตัวเลขที่แสดงสิทธิอันเป็นเท็จ ดังนั้นถ้าระบบคอมพิวเตอร์ไม่อนุญาตให้นาย ก. เข้าไปในระบบคอมพิวเตอร์แสดงว่าเป็นการลงมือกระทำความผิดแต่กระทำไปไม่ตลอด ซึ่งตามหลักการในประมวลกฎหมายอาญาถือว่าการพยายามกระทำความผิดฐานเจาะระบบ

<sup>๓๐</sup> อ่านประกอบคดีระหว่างรัฐแคนซัสและแอนโทนี เอเลน หน้า ๑๐๗



คอมพิวเตอร์โดยไม่ได้รับอนุญาต ปัญหาที่ตามมาคือตามลักษณะของการกระทำความผิดฐานเจาะระบบคอมพิวเตอร์ควรลงโทษผู้กระทำฐานพยายามเจาะระบบคอมพิวเตอร์หรือไม่ แม้ว่าในปัจจุบันยังไม่มีบทความผิดว่าด้วยการเจาะระบบคอมพิวเตอร์ แต่การตอบปัญหาดังกล่าวอาจเป็นประโยชน์หากมีบทบัญญัติดังกล่าวในอนาคต

สำหรับปัญหานี้ผู้เขียนเห็นว่าแม้การเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตจะต้องอาศัยระยะเวลาและการเตรียมการเป็นอย่างดี ซึ่งแสดงให้เห็นถึงเจตนาร้ายในการบุกรุกระบบคอมพิวเตอร์ของผู้อื่น แต่การพยายามเจาะระบบคอมพิวเตอร์ยังห่างไกลจากความเสียหายที่จะเกิดขึ้นเพราะการที่จะก่อให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์ต้องสามารถติดต่อสื่อสารกับเครื่องคอมพิวเตอร์ที่เป็นเป้าหมายนั้นได้เสียก่อนมิฉะนั้นแล้วจะเป็นเสมือนยืนอยู่หน้าประตูบ้านแต่ยังไม่เริ่มจัดประตูบ้านแล้วจะก่อความเสียหายได้อย่างไร อีกทั้งการจะลงโทษผู้พยายามกระทำความผิดหรือไม่ ขึ้นอยู่กับนโยบายของรัฐในขณะนั้น สำหรับประเทศไทยนั้นในปัจจุบันเมื่อพิจารณาถึงความเชี่ยวชาญทางคอมพิวเตอร์และการส่งเสริมการพัฒนาทางเทคโนโลยี ผู้เขียนเห็นว่ายังไม่ควรลงโทษผู้พยายามเจาะระบบคอมพิวเตอร์ แต่อย่างไรก็ตามเมื่อประเทศไทยพัฒนาทางเทคโนโลยีและต้องการป้องกันการเจาะระบบคอมพิวเตอร์มากขึ้น เมื่อนั้นนโยบายของรัฐอาจเปลี่ยนแปลงไปและเน้นที่การลงโทษผู้พยายามเจาะระบบคอมพิวเตอร์ได้ในอนาคต

### ๒.๒.๓ กรณีการแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

ปัญหาในการปรับใช้บทกฎหมายกับการกระทำในการแรกเข้าสู่ระบบคอมพิวเตอร์นั้นยังไม่ได้รับความสนใจจากบุคคลทั่วไปมากนัก ทั้งที่การกระทำในส่วนนี้สามารถกำหนดเป็นความผิดและมีปัญหาในเรื่องการปรับใช้ตัวบทกฎหมายที่มีอยู่ในปัจจุบันเช่นเดียวกัน ซึ่งอาจจะเป็นเพราะมุ่งที่จะให้ความสนใจต่อข้อมูลและสารสนเทศซึ่งเป็นส่วนที่มีความสำคัญในระบบคอมพิวเตอร์มากกว่า ดังที่ได้กล่าวไว้ข้างต้น แต่โดยเหตุที่ผู้เขียนเห็นว่าปัญหาที่เกิดขึ้นภายหลังจากมีการเข้าไปในระบบคอมพิวเตอร์แล้ว ก่อให้เกิดการผลลัพธ์ตามมามากมาย เช่นกรณีความเสียหายจากการกระทำและกรณีไม่มีตัวบทกฎหมายที่จะปรับใช้กับการกระทำความผิด เหตุนี้เพื่อเป็นการตัดไฟเสียแต่ต้นลม ผู้เขียนจึงเห็นว่าควรกำหนดให้การแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดอาญา หรืออาจกล่าวได้ว่าเมื่อเข้าไปโดยไม่ได้รับอนุญาตก็ผิดแล้ว เพื่อเป็นการป้องกันความเสียหายในอนาคตและเป็นการข่มขู่ที่อยู่ระหว่างการตัดสินใจที่จะเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต จนกระทั่งเป็นที่มาของแนวคิดในการกำหนดให้การแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดอาญา ซึ่งจะขอนำมากล่าวในบทที่ ๕ ต่อไป



โดยสรุปแล้วเมื่อรัฐยังไม่มีความชัดเจนที่รองรับการกระทำของผู้เจาะระบบคอมพิวเตอร์โดยตรง นโยบายของรัฐจึงควรให้ความสนใจในการปรับปรุงบทบัญญัติกฎหมายที่มีอยู่ให้สอดคล้องกับวิวัฒนาการที่เกิดขึ้นใหม่ในอนาคต สำหรับการกระทำที่มีลักษณะพิเศษหากเลือกที่จะปรับปรุงกฎหมายที่มีอยู่อาจก่อให้เกิดความไม่ชัดเจนในหลักของกฎหมายอาญา ก็สมควรได้รับการบัญญัติขึ้นใหม่เพื่อเป็นประโยชน์ต่อประชาชนซึ่งจะทราบและเข้าใจโดยไม่เคลือบแคลงสงสัยได้ว่าการกระทำใดได้ถูกห้ามไว้ อีกทั้งเพื่อประสิทธิภาพและความชัดเจนของผู้บังคับใช้กฎหมาย

### ๓ วิธีการบังคับเพื่อจะได้ผลในทางป้องกันอาชญากรรม

วิธีการป้องกันทางนิติบัญญัติหรือการร่างกฎหมายนั้น มีข้อจำกัดที่ไม่สามารถแยกพิจารณาลักษณะของแต่ละบุคคลเพื่อนำมาใช้ในการบัญญัติกฎหมาย เพราะโดยหลักการของกฎหมายที่ดีต้องมีความชัดเจนแน่นอน และกำหนดได้ว่าการกระทำใดเป็นการกระทำที่ต้องห้าม ซึ่งจะแตกต่างจากวิธีการบังคับหรือการลงโทษ ที่เปิดโอกาสให้นำปัจจัยหรือสาเหตุการกระทำผิดของผู้กระทำความผิดแต่ละบุคคลมาใช้พิจารณาว่าสมควรลงโทษผู้กระทำความผิดแต่ละคนอย่างไร ดังเช่น เปรียบเทียบระหว่าง นาย ก.กระทำความผิดฐานลักทรัพย์ เพื่อช่วยเหลือพี่น้องที่ยากจน และนาย ข. ซึ่งกระทำความผิดฐานลักทรัพย์เพื่อความโก้หรูทางสังคม เช่นนี้ หากเป็นวิธีการทางนิติบัญญัติเพื่อป้องกันการลักทรัพย์ การกระทำของทั้งนาย ก.และนาย ข.ต้องถูกกำหนดเป็นความผิด แต่สำหรับการพิจารณาว่าการกระทำของ นาย ก.และนาย ข. สมควรลงโทษอย่างไรเพื่อเป็นการป้องกันมิให้กระทำความผิดอีกสามารถนำลักษณะเฉพาะของแต่ละบุคคลมาเป็นเหตุผลประกอบในการใช้ดุลยพินิจ เพื่อลงโทษผู้กระทำความผิดได้ต่างกัน

#### ๓.๑ วัตถุประสงค์ของการลงโทษ

ตามความคิดของคนทั่วไป การกระทำต่อผู้หนึ่งผู้ใดที่ทำให้ผู้นั้นได้รับความยากลำบากถือเป็นการลงโทษทั้งสิ้น แต่ตามความจริงแล้ว การทำให้ได้รับความยากลำบากจะเป็นการลงโทษหรือไม่ ต้องแล้วแต่วัตถุประสงค์ของการทำเช่นนั้น เช่น เด็กนักเรียนที่ถูกกักไว้ในห้องเรียนเพราะไม่ทำการบ้านอาจถือเป็นการลงโทษ แต่การที่เด็กถูกพ่อแม่บังคับให้ไปโรงเรียนไม่ใช่การลงโทษ<sup>๓๖</sup>

<sup>๓๖</sup> อุททิศ แสนโกศิก, กฎหมายอาญามาตรา ๑ (กรุงเทพมหานคร: ม.ป.ท., ๒๕๒๕), หน้า ๑๘.

การลงโทษนั้นคือ ผลที่ได้รับจากการกระทำที่ขัดกับกฎหมาย ข้อบังคับ หรือ ระเบียบต่างๆ เช่นเดียวกัน การลงโทษทางอาญาคือผลที่ได้รับจากการกระทำที่ขัดต่อกฎหมายอาญา ซึ่งมีลักษณะเฉพาะ ๕ ประการ ที่แตกต่างจากการลงโทษอื่นๆ คือ

๑. จะต้องเกี่ยวกับความเจ็บปวด หรือมีผลที่โดยปกติแล้วถือว่าได้รับความลำบาก
๒. จะต้องมิใช่ขึ้นสำหรับการกระทำที่ขัดกับกฎหมาย
๓. จะต้องมิใช่ขึ้นสำหรับผู้กระทำผิดสำหรับการกระทำของเขา
๔. จะต้องถูกจัดการโดยมนุษย์คนอื่นที่ไม่ใช่ผู้กระทำผิด
๕. จะต้องถูกตัดสินและจัดการโดยบทบัญญัติที่มีอำนาจโดยระบบกฎหมายที่ต่อต้านการกระทำผิด<sup>๓๓</sup>

บทบัญญัติในกฎหมายอาญา ได้บัญญัติถึงการลงโทษผู้กระทำการฝ่าฝืนโดยมีเหตุผลหรือวัตถุประสงค์ที่แตกต่างกัน ซึ่งวัตถุประสงค์ในการลงโทษที่แฝงอยู่ในแต่ละบทบัญญัตินั้นนักวิชาการได้เสนอเป็นทฤษฎีต่างๆโดยแยกพิจารณาได้เป็น ๕ ทฤษฎีด้วยกัน คือ

### ๓.๑.๑ ทฤษฎีการลงโทษเพื่อเป็นการแก้แค้น (Retribution)

ทฤษฎีการลงโทษเพื่อเป็นการแก้แค้นเป็นทฤษฎีที่แสดงให้เห็นวัตถุประสงค์ของการลงโทษอย่างตรงไปตรงมาที่สุด ซึ่งคือการแก้แค้นต่อผู้กระทำผิด โดยเป็นทางที่ทำให้กลุ่มสังคม,เหยื่อ หรือผู้ถูกกระทำได้รับความพอใจ และถือว่าเป็นความชอบธรรมที่จะลงโทษเนื่องจากผู้กระทำผิดสมควรที่จะได้รับผลเช่นนั้น ซึ่งก็ทำให้เห็นเหตุผลที่ในอดีต แม้การทำผิดเพียงเล็กน้อยก็สามารถถูกลงโทษอย่างรุนแรงได้เช่นกัน

การมุ่งให้ความสนใจ เพื่อที่จะเข้าใจทฤษฎีนี้ในฐานะเป็นปรัชญาการลงโทษ ทำให้ตระหนักถึงความจริงที่ว่า การแก้แค้นเป็นสิ่งที่ผู้กระทำผิดต้องรับผิดชอบในพฤติกรรมของตนเอง ขณะเดียวกันก็สนับสนุนมุมมองที่ว่าผู้ละเมิดกฎหมายมีอิสระในการตัดสินใจเลือกว่าจะกระทำ ความผิดหรือไม่

<sup>๓๓</sup>H.L.A.Hart,Punishment and Responsibility (New York:oxford 1986) อ้างถึงใน Frank Schmallegger ,Criminal Law today (USA:Prentice-Hall 1999), p. 528

### ๓.๑.๒ ทฤษฎีการลงโทษเพื่อเป็นการข่มขู่ (Deterrence)

ทฤษฎีการลงโทษเพื่อเป็นการข่มขู่คล้ายกับทฤษฎีการแก้แค้นในแง่ที่ขึ้นกับการกำหนดโทษเพียงแต่ต่างกันในเรื่องวัตถุประสงค์ ซึ่งภายใต้ปรัชญาของการข่มขู่ การลงโทษถูกมองในฐานะเป็นสิ่งสกัดกั้นที่มีอำนาจกำหนดความประพฤติให้อยู่ในกรอบ โดยแยกออกเป็น ๒ ประเภทคือ การข่มขู่ประเภทเจาะจง (Specific) และประเภททั่วไป (General)

*ประเภทเจาะจง* มีเจตนาที่จะขัดขวางผู้กระทำที่ถูกตัดสินลงโทษแล้วมิให้กลับมากระทำความผิดอีก เช่นผู้ถูกลงโทษอาจจะพบว่า การขาดเสรีภาพเป็นประสบการณ์ที่เจ็บปวดและเป็นผลให้เขาหลีกเลี่ยงจากการกระทำความผิดซ้ำอีกในอนาคต

*ประเภททั่วไป* ได้แก่การใช้การลงโทษเป็นตัวอย่างแก่บุคคลทั่วไปที่มีความคิดจะฝ่าฝืนกฎหมาย ดังเช่นผู้ต้องคดีลักทรัพย์ถูกตัดสินจำคุก จะเป็นตัวอย่างแก่ผู้ร่วมลงมือให้เห็นได้ว่า พวกเขาเหล่านั้นอาจตกอยู่ในสถานการณ์เช่นเดียวกันได้เมื่อเลือกที่จะกระทำความผิดเช่นเดียวกันนั้น

ตามทฤษฎีนี้มีผู้โต้แย้งว่า มีหลักฐานเพียงเล็กน้อยเท่านั้นที่แสดงว่าการลงโทษเป็นการป้องกันพฤติกรรมกระทำผิด ซึ่งผู้โต้แย้งเห็นว่าในความเป็นจริงแล้วมีผู้ทำผิดจำนวนมากที่กระทำผิดเป็นครั้งที่ ๒ แต่อย่างไรก็ตามการโต้แย้งเช่นนี้ก็ไม่ได้แสดงว่าทฤษฎีนี้ได้ผล เพราะเป็นการยากที่จะตรวจสอบว่าทฤษฎีการข่มขู่ใช้ได้ผลหรือไม่ หรืออาจจะกล่าวได้ว่าแม้ทฤษฎีการข่มขู่จะวัดความสำเร็จได้ยากแต่ก็ไม่ได้หมายความว่าใช้ไม่ได้ผลเสียเลย

ผู้ทำวิจัยหลายท่านพบว่าถ้าจะให้ทฤษฎีการข่มขู่ได้ผล การลงโทษต้องรวดเร็วและแน่นอน การผ่อนผันการลงโทษหรือการลังเลในการลงโทษ มีผลทำให้ประสิทธิภาพของความพยายามที่จะลดการกระทำผิดลดลง การลงโทษที่รุนแรงอาจจะสำคัญในฐานะเป็นการขัดขวาง แต่อาจจะมีผลกับการกระทำเล็กน้อยๆ มากกว่าการกระทำผิดที่ร้ายแรง ดังเช่นการลงโทษผู้กระทำผิดจรรยาซึ่งเป็นความผิดเล็กน้อยโดยใช้ความรุนแรง ในทางทฤษฎีอาจเป็นการป้องกันขัดขวางบุคคลที่มีแนวโน้มที่จะละเมิดข้อกำหนดจรรยาในอนาคตที่มีประสิทธิภาพ แต่ไม่แน่ว่าการลงโทษที่รุนแรงจะให้ได้ผลในการลดการฆาตกรรมซึ่งเป็นความผิดที่ร้ายแรง

### ๓.๑.๓ ทฤษฎีการลงโทษเพื่อเป็นการฟื้นฟูผู้กระทำความผิด (Rehabilitation)

จุดประสงค์ของทฤษฎีนี้คือการปฏิรูปผู้กระทำความผิดโดยการฟื้นฟูให้มีชีวิตที่สมบูรณ์ในสังคม หลักการฟื้นฟูผู้กระทำความผิดซึ่งมีความเกี่ยวข้องกับส่วนประกอบของการลงโทษ มักจะรวมถึงการฝึกงาน การฝึกความเชี่ยวชาญ การศึกษา การให้คำปรึกษาและการบำบัดทางจิต ปกติแล้วลักษณะของความผิดมีความสำคัญน้อยกว่าการฟื้นฟูผู้กระทำความผิด ยกเว้นแต่ลักษณะของความผิดนั้นแสดงให้เห็นว่าความผิดนั้นต้องการวิธีการเป็นพิเศษในการฟื้นฟู

### ๓.๑.๔ ทฤษฎีการลงโทษเพื่อชดเชยการกระทำ (Restoration)

ทฤษฎีการลงโทษเพื่อชดเชยการกระทำเป็นทฤษฎีที่เน้นทางด้านความรู้สึกและความเสียหายที่เป็นเงินของผู้เสียหาย โดยหาวิธีชดเชยผู้เสียหายให้อยู่ในสถานะเดิมก่อนที่จะตกอยู่ในฐานะผู้เสียหาย ทฤษฎีนี้มีจุดประสงค์โดยถือว่าผู้ได้รับความเสียหายและสังคมคือสิ่งเดียวกันเมื่อการกระทำของผู้กระทำความผิดต่อผู้เสียหายขณะเดียวกันก็มีผลต่อสังคมที่อยู่อาศัยด้วยเช่นกัน การลงโทษจึงได้แก่ การใช้ค่าปรับ การใช้คืน และการให้บริการแก่สังคม

### ๓.๑.๕ ทฤษฎีการลงโทษเพื่อตัดไม่ให้มีโอกาสกระทำความผิดอีก (Incapacitation)

ทฤษฎีนี้มีหลักการที่จะใช้ประโยชน์จากการกักขังหรือการตัดสินอื่นๆที่จะลดความสามารถของผู้ที่จะกระทำความผิดในอนาคต ปรัชญาของการตัดออกจากสังคมต้องการเพียงการจำกัดแต่ไม่เน้นที่การลงโทษ การจำกัดขอบเขต การใช้เครื่องมือทางอิเล็กทรอนิกส์ติดตาม อยู่ภายใต้ความหมายของการตัดออกจากสังคมทั้งสิ้น แต่อย่างไรก็ตามทฤษฎีนี้ได้รับอิทธิพลจากทฤษฎีแก้แค้นอยู่บ้าง ดังเช่นนอกจากการจำกัดขอบเขต แต่อาจจำกัดความสามารถผู้ต้องขังในการใช้เครื่องมือบางชนิด หรือลดความบันเทิงซึ่งรวมถึงการดูโทรทัศน์หรือรายการโทรทัศน์บางรายการ ซึ่งการผสมกันของทฤษฎีดังกล่าวนี้ อาจทำให้เห็นแนวโน้มของปรัชญาการตัดสินลงโทษในอนาคตที่ไม่จำกัดเพียงทฤษฎีใดทฤษฎีหนึ่งเท่านั้น

### ๓.๒ การลงโทษผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตที่คำนึงถึงความเหมาะสมแต่ละบุคคลตามลักษณะแรงจูงใจ

เมื่อนำทฤษฎีอาชญาวิทยาทางสังคมมาอธิบายการกระทำของผู้เจาะระบบคอมพิวเตอร์ การลงโทษจึงมุ่งเน้นในด้านการลงโทษที่ตอบสนองต่อสังคม ดังนั้นในการวิเคราะห์ว่าสมควรนำวัตถุประสงค์ของการลงโทษตามทฤษฎีใดมาปรับใช้ จึงไม่สามารถละเลยทฤษฎีการแก้แค้นทดแทน (Retribution) เพราะเกี่ยวข้องกับความรู้สึกต่อมหาชน อีกทั้งทฤษฎีการแก้แค้นทดแทนก็แทรกอยู่ในทุกบทบัญญัติที่ว่าด้วยการลงโทษ เพียงแตกต่างกันที่บทบัญญัติโดยยึดถือทฤษฎีการแก้แค้นมากกว่ากัน ดังนั้นการวิเคราะห์ในส่วนต่อไปผู้เขียนจึงไม่ขอกล่าวถึงทฤษฎีการแก้แค้นทดแทนสำหรับทฤษฎีอีก ๔ ทฤษฎีนั้นในขณะวิเคราะห์ ผู้เขียนก็ไม่สามารถพูดได้ว่าห้ามใช้ทฤษฎีใดเสียเลยเพราะทฤษฎีทั้งสี่ทฤษฎีควรนำมาใช้พร้อมกันทั้งหมด แต่หากกล่าวเช่นนี้อาจเป็นการกล่าวแบบกำปั้นทุบดินที่ไม่ได้แสดงให้เห็นประโยชน์ถึงการศึกษาได้เลย ดังนั้นผู้เขียนจึงขอพิจารณาในแต่ละทฤษฎีโดยเริ่มจากคำถามที่ว่า ทฤษฎีใดสมควรนำมาใช้มากที่สุดหรือน้อยที่สุดสำหรับผู้เจาะระบบคอมพิวเตอร์ที่มีแรงจูงใจต่างกันโดยเลือกที่จะจัดอันดับทฤษฎีที่น่าจะมีส่วนในการกำหนดบทลงโทษจากมากไปน้อย ดังนี้ คือ

#### ๓.๒.๑ การลงโทษกรณีผู้กระทำโดยมีแรงจูงใจเพื่อต้องการให้เป็นที่ยอมรับของสังคม

ในกรณีนี้ผู้เขียนขอจัดลำดับการนำทฤษฎีการลงโทษมาใช้ดังต่อไปนี้ คือ

๑. ทฤษฎีการลงโทษเพื่อเป็นการฟื้นฟูผู้กระทำผิด
๒. ทฤษฎีการลงโทษเพื่อเป็นการข่มขู่
๓. ทฤษฎีการลงโทษเพื่อตัดไม่ให้มีโอกาสกระทำความผิดอีก

#### เหตุผล

พื้นฐานของผู้กระทำความผิดเพื่อต้องการให้เป็นที่ยอมรับของสังคมจะต่างจากผู้กระทำความผิดในกรณีอื่นๆ สังเกตได้จากความต้องการของผู้กระทำเพื่อต้องการส่งเสริมตนเองให้โดดเด่นและได้รับการยอมรับจากสังคม ผลจากการกระทำดังกล่าวแม้จะกระทบบุคคลภายนอกไม่ว่าจะตั้งใจหรือไม่ก็ตาม แต่ก็มิได้มีความมุ่งหมายที่จะก่อให้เกิดความเดือดร้อนแก่ผู้อื่นโดยตรง ดังนั้นผู้เขียนจึงเห็นว่าในส่วนของ การลงโทษควรมีจุดประสงค์เพื่อให้ผู้กระทำสามารถพัฒนาความสามารถในการยับยั้งการกระทำผิดของตนเองมากกว่าการกำหนดบทลงโทษโดยรุนแรง เพื่อข่มขู่มิให้ผู้ใดคิดจะกระทำความผิดหรือผู้กระทำความผิดแล้ว กระทำความผิดอีก

ปัญหาที่ตามมาคือ โทษประเภทใดที่สมควรนำมาลงโทษแก่ผู้เจาะระบบคอมพิวเตอร์โดย  
ไม่ได้รับอนุญาต ซึ่งตามประมวลกฎหมายอาญามาตรา ๑๘ ได้แบ่งโทษออกได้เป็น ๕ ประเภท  
ด้วยกันคือ โทษประหารชีวิต จำคุก กักขัง ปรับ และริบทรัพย์สิน

## โทษ

โทษจำคุก เมื่อพิจารณาประกอบกับทฤษฎีการลงโทษเพื่อฟื้นฟูผู้กระทำผิดซึ่งมี  
จุดประสงค์ที่จะไม่ให้ผู้ที่กระทำความผิดหันกลับมากระทำผิดอีก คือนอกจากจะพยายามหาทาง  
ให้ผู้กระทำผิดมาแล้วเกิดความประสงค์ที่จะยับยั้งไม่ทำผิดซ้ำอีกแล้ว ยังต้องทำให้ผู้นั้นเกิดความ  
สามารถที่จะยับยั้งด้วยตนเองด้วย<sup>๑๔</sup> ถ้าเลือกใช้โทษจำคุกเพราะเหตุผลเพื่อต้องการยับยั้งไม่ให้ผู้  
เจาะระบบคอมพิวเตอร์กระทำความผิดซ้ำอีก ผู้เขียนเห็นว่านอกจากจะเป็นการผลักดันให้ผู้ทำผิด  
เข้าร่วมกลุ่มกันแล้ว การอยู่ร่วมกันอาจจะเป็นการถ่ายทอดความรู้ในทางที่ผิดให้แก่กัน ซึ่งจะไม่  
เป็นผลดีในการยับยั้งผู้กระทำความผิดไม่ให้เกิดกลับมากระทำผิดอีก อีกทั้งยังไม่เป็นการปลูกฝัง  
ให้ผู้กระทำผิดเกิดความสามารถที่จะยับยั้งการกระทำได้ด้วยตนเอง ดังนั้นโทษจำคุกจึงไม่เหมาะที่  
จะนำมาใช้ในการลงโทษผู้เจาะระบบคอมพิวเตอร์ที่มีแรงจูงใจทางสังคม

โทษกักขัง สำหรับโทษกักขังนั้น แม้จะเป็นหนึ่งในวิธีการที่หลีกเลี่ยงและผ่อนคลายเป็นให้  
ศาลลงโทษจำคุกโดยไม่จำเป็น และแม้สถานที่ยกขังจะมีไซเรออนจำ<sup>๑๕</sup> แต่อย่างไรก็ตามโทษกักขังก็  
เป็นการจำกัดเสรีภาพในร่างกายเช่นเดียวกับโทษจำคุก เพียงแต่เบากว่า ซึ่งผู้เขียนไม่เห็นด้วยที่จะ  
นำโทษกักขังนี้มาปรับใช้กับผู้เจาะระบบฯ ด้วยเหตุผลทางด้านพื้นฐานของการกระทำของผู้เจาะ  
ระบบคอมพิวเตอร์และความสามารถในการแก้ไขฟื้นฟูผู้กระทำผิด ดังเหตุผลที่ผู้เขียนได้กล่าวไว้ใน  
กรณีโทษจำคุก

โทษปรับและโทษริบทรัพย์สิน เป็นโทษที่ไม่เหมาะสมที่จะนำมาใช้ในการแก้ไขฟื้นฟูผู้เจาะ  
ระบบคอมพิวเตอร์ เพราะเป็นการเยียวยาแก้ไขที่ปลายเหตุและมีแนวโน้มที่จะไม่สามารถแก้ไข  
ความประพฤติของบุคคลได้ โดยเฉพาะโทษริบทรัพย์สิน เช่นคอมพิวเตอร์หรืออุปกรณ์ที่ช่วยในการ  
เจาะระบบคอมพิวเตอร์ เป็นการห้ามเพียงชั่วคราว เพราะเมื่อพ้นโทษแล้วไม่สามารถรับรองได้

<sup>๑๔</sup> อุททิศ แสนโกศิก, กฎหมายอาญามาตรา ๑๘, หน้า ๒๘๗.

<sup>๑๕</sup> ประมวลกฎหมายอาญา มาตรา ๒๔

แน่นอนว่าผู้เจาะระบบคอมพิวเตอร์จะไม่กลับไปใช้เครื่องมือดังกล่าวอีก ซึ่งเป็นการให้ความสนใจต่อวัตถุโดยละเอียดที่จะให้ความสำคัญต่อผู้กระทำผิด ซึ่งเป็นต้นเหตุของการกระทำ

แต่อย่างไรก็ตาม เมื่อพิจารณาโทษทั้งสี่ประการแล้ว แม้ว่าจะไม่สอดคล้องตามทฤษฎีการลงโทษเพื่อฟื้นฟูผู้กระทำผิดแต่โทษทั้งสี่ประการนี้ก็มีความสอดคล้องกับวัตถุประสงค์ในการลงโทษตามทฤษฎีการลงโทษในลำดับต่อมาคือทฤษฎีการลงโทษเพื่อเป็นการข่มขู่ และขณะเดียวกันก็เป็นการป้องกันการเจาะระบบคอมพิวเตอร์ได้ส่วนหนึ่ง

**การคุมประพฤติ** ผู้เขียนได้รับทราบข่าวทางหนังสือพิมพ์ กรณีนักกีฬาฟุตบอลทะเลาะวิวาทและทำร้ายร่างกายพนักงานในร้านอาหาร ศาลตัดสินให้ทำความดีทดแทนสังคม<sup>๓๖</sup> โดยให้สอนเยาวชนเล่นกีฬาฟุตบอลแทน ซึ่งผู้เขียนเห็นว่าน่าจะนำมาเป็นแบบอย่างในการลงโทษผู้กระทำความผิดทางคอมพิวเตอร์ โดยเฉพาะผู้เจาะระบบคอมพิวเตอร์ที่มีแรงจูงใจเพื่อให้ตนเป็นที่ยอมรับทางสังคม เนื่องจากการลงโทษที่สอดคล้องและปรองดองกับการจัดลำดับวัตถุประสงค์ของการลงโทษที่ผู้เขียนได้เสนอไว้ทั้งสามประการได้ อีกทั้ง

<sup>๓๖</sup> เป็นการกำหนดบทลงโทษโดยอาศัยอำนาจตามประมวลกฎหมายอาญา มาตรา ๕๖ ซึ่งบัญญัติได้ว่า ผู้กระทำความผิดซึ่งมีโทษจำคุก และในคดีนั้นศาลจะลงโทษจำคุกไม่เกินสองปี ถ้าไม่ปรากฏว่าผู้นั้นได้รับโทษจำคุกมาก่อน หรือปรากฏว่าได้รับโทษจำคุกมาก่อนแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษเมื่อศาลได้คำนึงถึงอายุ ประวัติ ความประพฤติ สติปัญญา การศึกษาอบรม สุขภาพ ภาวะแห่งจิต นิสัย อาชีพและสิ่งแวดล้อมของผู้นั้น หรือสภาพความผิด หรือเหตุอื่นอันควรปรานีแล้ว เห็นเป็นการสมควร ศาลจะพิพากษาว่าผู้นั้นมีความผิดแต่รอการกำหนดโทษไว้ หรือกำหนดโทษแต่รอการลงโทษไว้ แล้วปล่อยตัวไปเพื่อให้โอกาสผู้นั้นกลับตัวภายในระยะเวลาที่ศาลจะได้กำหนด แต่ต้องไม่เกินห้าปีนับแต่วันที่ศาลพิพากษา โดยจะกำหนดเงื่อนไขเพื่อคุมความประพฤติของผู้นั้นด้วยหรือไม่ก็ได้

เงื่อนไขเพื่อคุมความประพฤติของผู้กระทำความผิดนั้น ศาลอาจกำหนดข้อเดียวหรือหลายข้อ ดังต่อไปนี้

- (๑) ให้ไปรายงานตัวต่อเจ้าพนักงานที่ศาลระบุไว้เป็นครั้งคราว เพื่อเจ้าพนักงานจะได้สอบถาม แนะนำ ช่วยเหลือ หรือตักเตือนตามที่เห็นสมควรในเรื่องความประพฤติและการประกอบอาชีพหรือจัดให้กระทำกิจกรรมบริการสังคมหรือสาธารณประโยชน์ตามที่เจ้าพนักงานและผู้กระทำความผิดเห็นสมควร
- (๒) ให้ฝึกหัดหรือทำงานอาชีพอันเป็นกิจจะลักษณะ
- (๓) ให้ละเว้นการคบหาสมาคมหรือการประพฤติดังอันน่าไปสู่การกระทำความผิดในทำนองเดียวกันอีก
- (๔) ให้ไปรับการบำบัดรักษาการติดยาเสพติดให้โทษ ความบกพร่องทางร่างกายหรือจิตใจ หรือความเจ็บป่วยอย่างอื่น ณ สถานที่และตามระยะเวลาที่ศาลกำหนด
- (๕) เงื่อนไขอื่นๆ ตามที่ศาลเห็นสมควรกำหนดเพื่อแก้ไขฟื้นฟู หรือป้องกันมิให้ผู้กระทำความผิดกระทำหรือมีโอกาสกระทำความผิดขึ้นอีก .....



๑. การลงโทษดังกล่าวไม่เป็นการลงโทษที่รุนแรง แต่พยายามเน้นไม่ให้กระทำความผิดอีกโดยให้มีความสามารถที่จะยับยั้งตนเองไม่ให้กระทำความผิดซึ่งเป็นปัจจัยภายใน มากกว่าที่จะบังคับโดยปัจจัยภายนอกเพื่อบังคับไม่ให้ผู้กระทำ กระทำความผิดอีก

๒. การแสดงออกเพื่อให้เป็นที่ยอมรับของสังคมเป็นพื้นฐานอย่างหนึ่งของผู้เจาะระบบคอมพิวเตอร์ที่มีแรงจูงใจทางสังคม การให้ผู้เจาะระบบคอมพิวเตอร์ทำประโยชน์ต่อสังคมมีส่วนช่วยแก้ไขภาวะของบุคคลที่ขาดการยอมรับจากสังคมได้ และมีส่วนที่จะลดพฤติกรรมที่ต้องการเป็นที่ยอมรับโดยปกปิดและมีแนวโน้มในทางที่ผิด โดยสนับสนุนให้แสดงออกในทางที่ถูกโดยเปิดเผยแทน

๓. การให้ผู้เจาะระบบคอมพิวเตอร์ บริการสังคมในด้านคอมพิวเตอร์เป็นการอาศัยความรู้ทางคอมพิวเตอร์ของผู้เจาะระบบคอมพิวเตอร์มาทดแทนความเสียหายของสังคมโดยการให้ความรู้แก่เยาวชนไม่ได้ทำให้ผู้เจาะระบบคอมพิวเตอร์ถูกตัดขาดจากการใช้คอมพิวเตอร์ทั้งหมดซึ่งเป็นการแก้ปัญหาสาเหตุของการกระทำความผิดที่เกิดจากความกดดันในการพรางจากสิ่งที่ชอบ การให้ผู้เจาะระบบคอมพิวเตอร์สอนหรือถ่ายทอดความรู้ทางคอมพิวเตอร์แก่เยาวชนมีส่วนที่จะทำให้ผู้กระทำความผิดพัฒนาความคิดทางศีลธรรมได้ว่าการกระทำอย่างใดผิดและไม่ควรกระทำ โดยอาศัยเยาวชนเป็นสิ่งสะท้อนความคิดของผู้กระทำในทางที่ถูกต้อง

### ๓.๒.๒ การลงโทษกรณีผู้กระทำโดยมีแรงจูงใจทางเทคนิค

ในกรณีนี้ผู้เขียนขอจัดลำดับการนำทฤษฎีการลงโทษมาใช้ดังต่อไปนี้ คือ

๑. ทฤษฎีการลงโทษเพื่อเป็นการฟื้นฟูผู้กระทำผิด
๒. ทฤษฎีการลงโทษเพื่อเป็นการข่มขู่
๓. ทฤษฎีการลงโทษเพื่อตัดไม่ให้มีโอกาสกระทำความผิดอีก

#### เหตุผล

กลุ่มผู้เจาะระบบคอมพิวเตอร์กรณีแรงจูงใจทางเทคนิคนี้ คล้ายกับแรงจูงใจทางสังคม แต่กลุ่มแรงจูงใจนี้กระทำเพราะเห็นว่าการบุกรุกเข้าไปในระบบคอมพิวเตอร์โดยมีจุดประสงค์เพื่อตรวจสอบและแก้ไขข้อบกพร่องในระบบคอมพิวเตอร์ของผู้อื่นเป็นสิ่งถูกต้อง เพื่อความเข้าใจอาจเทียบได้กับจอมโจรโรบินฮูด ที่กระทำความผิดโดยการปล้นทรัพย์สินของผู้ที่มีฐานะร่ำรวย เพื่อนำมาแจกจ่ายแก่คนยากจน ส่วนโรบินฮูดในทางคอมพิวเตอร์บุกรุกเข้าไปในระบบของผู้อื่น เพื่อจะ

บอกแก่บุคคลทั่วไปว่าระบบคอมพิวเตอร์ที่ตนได้เข้าไปนั้นมีความบกพร่องอย่างไร ซึ่งการกระทำดังกล่าวนี้อาจกล่าวได้ว่าเป็นการกระทำที่มีเป้าหมายที่ถูกต้อง เพียงแต่วิธีการที่จะบรรลุเป้าหมายนั้นไม่ถูกต้อง

ดังนั้นโดยพื้นฐานทางจิตใจ ผู้กระทำจึงไม่ถึงขนาดที่เป็นอาชญากรโดยสันดาน การใช้การลงโทษที่มีวัตถุประสงค์ในการฟื้นฟูผู้กระทำผิด โดยการพัฒนาความสามารถของผู้กระทำในการยับยั้งที่จะกระทำความผิด จึงเป็นวิถีทางที่ผู้เขียนเลือกที่จะให้ความสำคัญเป็นลำดับแรก

## โทษ

ดังนั้นโทษที่จะลงแก่ผู้กระทำที่มีแรงจูงใจทางเทคนิคนี้ จึงควรมีลักษณะเป็นการกำหนดเงื่อนไขในการคุมประพฤติ ดังเช่นผู้ที่มีแรงจูงใจทางสังคม ซึ่งนอกจากการกำหนดให้ทำความดีทดแทนสังคมแล้ว อาจรวมถึงการกำหนดให้มีการให้คำปรึกษาและการบำบัดทางจิตได้ด้วย

### ๓.๒.๓ การลงโทษกรณีผู้กระทำโดยมีแรงจูงใจทางการเงิน การเมือง ทางรัฐบาล

ในกรณีนี้ผู้เขียนขอจัดลำดับการนำทฤษฎีมาใช้ดังต่อไปนี้ คือ

๑. ทฤษฎีการลงโทษเพื่อเป็นการข่มขู่
๒. ทฤษฎีการลงโทษเพื่อตัดไม่ให้มีโอกาสกระทำความผิดอีก
๓. ทฤษฎีการลงโทษเพื่อเป็นการฟื้นฟูผู้กระทำผิด

## เหตุผล

เหตุที่ผู้เขียนให้ความสำคัญกับทฤษฎีการข่มขู่ในกรณีนี้เนื่องจากว่า ผู้เจาะระบบคอมพิวเตอร์ที่มีแรงจูงใจทางการเงิน ทางการเมือง หรือทางรัฐบาล ก่อให้เกิดการกระทำที่มีผลกระทบและสามารถนำไปสู่ความเสียหายที่ร้ายแรงต่อความเป็นอยู่ของสมาชิกภายในสังคมได้ เหตุนี้การเน้นที่ทฤษฎีการฟื้นฟูผู้กระทำผิดอาจไม่ใช่หนทางที่รับประกันได้ว่าผู้กระทำความผิดจะไม่หันมากระทำความผิดอีก ดังนั้นเพื่อแสดงให้เห็นว่าสังคมเอาใจใส่กับการกระทำดังกล่าวและไม่ต้องให้การกระทำดังกล่าวเกิดขึ้นในอนาคตจึงสมควรที่จะกำหนดบทลงโทษที่มีวัตถุประสงค์เน้นหนักไปในด้านป้องกันและข่มขู่เพื่อไม่ให้มีการกระทำความผิด รวมถึงเพื่อตัดโอกาสไม่ให้กระทำความผิดได้อีก

## โทษ

หากกล่าวถึงโทษที่มีจุดประสงค์เพื่อเป็นการข่มขู่ผู้กระทำความผิด ขณะเดียวกันก็เป็นการตัดโอกาสไม่ให้มีการกระทำความผิดอีก คงจะเลยไม่ได้ที่จะกล่าวถึงโทษจำคุกและกักขัง โทษจำคุกและกักขังมีลักษณะเป็นการข่มขู่ เนื่องจากมีผลในการเป็นตัวอยางแก่บุคคลทั่วไปซึ่งมุ่งที่จะฝ่าฝืนกฎหมาย กล่าวคือหากเลือกที่จะกระทำความผิดตั้งเช่นผู้ต้องโทษแล้วอาจได้รับผลโดยการถูกจำกัดเสรีภาพเช่นเดียวกัน

วิธีการลงโทษที่ได้กล่าวมาแสดงให้เห็นว่าบทบัญญัติที่เกี่ยวกับผู้เจาะระบบคอมพิวเตอร์นั้น ต้องกำหนดโทษจำคุกไว้ด้วยซึ่งจะสอดคล้องกับทฤษฎีข่มขู่และทฤษฎีการลงโทษเพื่อตัดไม่ให้มีโอกาสกระทำความผิด ขณะเดียวกันก็สามารถให้ดุลยพินิจแก่ศาลในการใช้วิธีการคุมประพฤติเพื่อแก้ไขฟื้นฟูผู้กระทำความผิดตามประมวลกฎหมายอาญามาตรา ๕๖ ด้วย กล่าวคือกำหนดโทษจำคุกขั้นต่ำน้อยกว่าสองปีส่วนกำหนดโทษขั้นสูงแล้วแต่ความเหมาะสม ซึ่งในอนาคตอัตราโทษอาจต่ำกว่านี้ก็ได้หาก ผลประโยชน์ของสังคมสามารถปกป้องได้ด้วยวิธีอื่น เช่น เอกชนมีมาตรการรักษาความปลอดภัยที่ดีขึ้นกว่าเดิม

โดยสรุปแล้ว แม้ทฤษฎีการลงโทษทั้งห้าประการที่กล่าวมาถูกมองว่ามีลักษณะขัดแย้งกัน ในทางปฏิบัติ แต่โดยธรรมชาติของความพยายามในการแก้ไขผู้กระทำความผิดของสังคมแล้วคงไม่ยากนักที่จะประองตองทฤษฎีการลงโทษดังกล่าวเข้าด้วยกัน เพราะในที่สุดแล้วจุดมุ่งหมายไม่ได้อยู่ที่ว่าทฤษฎีใดใช้ได้ดีกว่าทฤษฎีใด แต่อยู่ที่จะรักษาความสงบสุขภายในสังคมที่ตนอาศัยอยู่ได้อย่างไร

#### ๔. การประสานงานระหว่างสถาบันที่มีส่วนในการป้องกันอาชญากรรม

องค์กรของรัฐหรือบุคลากรในกระบวนการยุติธรรม เป็นปัจจัยที่สำคัญยิ่งในการทำนายถึงความมีประสิทธิภาพของกฎหมายอาญาที่ประกาศใช้บังคับ ดังเช่น คำกล่าวที่ว่า “หากรัฐมุ่งแต่จะควบคุมความประพฤติของสมาชิกในสังคมโดยใช้กฎหมายอาญาเป็นเครื่องมือ โดยไม่พิจารณาถึงประสิทธิภาพและความสามารถของกลไกของรัฐที่จะใช้บังคับกฎหมายแล้ว กฎหมายจะไร้ความหมายขาดความศักดิ์สิทธิ์ และเป็นการเปิดโอกาสให้เจ้าพนักงานของรัฐที่ประพฤติมิชอบมีโอกาสแสวงหาประโยชน์เพื่อตนเองจากกฎหมายเหล่านี้ หรือหากมีการใช้บังคับกฎหมายซึ่งมิได้มีการใช้บังคับมาเป็นเวลานาน ผู้ถูกใช้บังคับก็จะเกิดปฏิกริยาเพราะถือว่าถูกเลือกปฏิบัติซึ่งจะทำให้ความ

สัมพันธ์ระหว่างผู้บังคับกฎหมายกับชุมชนเสียไป" <sup>๓๓</sup> .....ผู้บัญญัติกฎหมายควรจะคำนึงถึงองค์กรของรัฐ ซึ่งปฏิบัติหน้าที่ในการบังคับใช้กฎหมายให้มากเท่าๆกับการบัญญัติกฎหมาย มิใช่ปล่อยให้ เป็นหน้าที่ของฝ่ายบริหารหรือหน่วยงานในกระบวนการยุติธรรมรับผิดชอบกฎหมายซึ่งบัญญัติ โดยฝ่ายนิติบัญญัติแต่เพียงฝ่ายเดียว โดยไม่คำนึงถึงบุคลากร งบประมาณและ ทรัพยากรธรรมชาติ"<sup>๓๔</sup>

นักอาชญาวิทยาส่วนมากเชื่อว่า ความแน่นอนในการลงโทษ (Certainty of punishment) มีความสำคัญมากกว่าการลงโทษด้วยวิธีรุนแรงหรือการเพิ่มอัตราโทษสูงขึ้นโดยไม่คำนึงถึงปัจจัยอื่น ซึ่งความแน่นอนในการลงโทษนี้หมายถึงความสามารถของเจ้าหน้าที่ในกระบวนการยุติธรรม ในการสืบสวน สอบสวน จับกุม ฟ้องร้อง ให้ผู้กระทำผิดได้รับการลงโทษ ความแน่นอนที่ผู้กระทำ ความผิดจะได้รับโทษในอัตราส่วนที่สูงมีมากเท่าใดย่อมมีความสำคัญต่อผลของการป้องกันทั่วไป ในกฎหมายอาญามากเท่านั้น

อุปสรรคในการนำผู้กระทำความผิดทางคอมพิวเตอร์มาลงโทษนอกจากปัญหาเรื่องความ หลากหลายของสถานที่กระทำผิดยังรวมถึงการที่ผู้บังคับใช้กฎหมายส่วนใหญ่ขาดผู้ที่มีความ ชำนาญหรือเงินทุนที่จะจัดการกับปัญหาดังกล่าว ซึ่งหากเปรียบเทียบบุคลากรที่ดูแลทางด้าน อาชญากรรมคอมพิวเตอร์ ระหว่างไทยและต่างประเทศ ดังเช่น สหรัฐอเมริกาจะพบเห็นความสนใจต่อปัญหานี้ในระดับที่แตกต่างกันดังต่อไปนี้ คือ

#### ๔.๑ ประเทศไทย

สำนักงานตำรวจแห่งชาติ ได้มอบหมายให้ ศูนย์ข้อมูลสารสนเทศ เป็นผู้ดูแลการกระทำ อาชญากรรมทางคอมพิวเตอร์นี้ แต่เนื่องจากตามนโยบายของสำนักงานตำรวจแห่งชาติในขณะนี้ (พ.ศ. ๒๕๔๒) จะไม่มีการเพิ่มกำลังพลหรือหน่วยงานใหม่ในช่วยระยะเวลา ๓ ปีนี้ จึงยังไม่มี การ

<sup>๓๓</sup> เกียรติขจร วัจนะสวัสดิ์, คำอธิบายกฎหมายอาญา ภาค ๑ พิมพ์ครั้งที่ ๑ (กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, ๒๕๓๑), หน้า ๘.

<sup>๓๔</sup> ประธาน วัฒนวานิชย์, "แนวความคิดในการลงโทษ: การวิเคราะห์ร่างพระราชบัญญัติแก้ไขเพิ่มเติม ประมวลกฎหมายอาญา," วารสารนิติศาสตร์ ปีที่ ๑๒ ฉบับที่ ๒ (ธันวาคม ๒๕๒๔) : ๒๐

ตั้งหน่วยงานที่รับผิดชอบด้านนี้โดยเฉพาะ ขณะนี้จึงเป็นการเตรียมการไว้ล่วงหน้า เมื่อสิ้นสุดระยะเวลาตามนโยบายดังกล่าวแล้วก็จะสามารถทำการจัดตั้งได้ทันที<sup>๓๘</sup>

## ๔.๒ สหรัฐอเมริกา

ในสหรัฐอเมริกา มีหน่วยงานที่เห็นความสำคัญต่อการกระทำคามผิดเกี่ยวกับคอมพิวเตอร์หลายหน่วยงานด้วยกัน ทั้งที่เป็นหน่วยงานของรัฐ หรือของเอกชน ดังเช่น

### ๔.๒.๑ The U.S. Secret Service

The U.S. Secret Service ซึ่งเป็นที่รู้จักในหน้าที่คุ้มกันประธานาธิบดีและครอบครัว ก่อตั้งในปี ค.ศ. ๑๘๖๕ ในฐานะเป็นกรมคลัง (Treasury Department) ดูแลการปลอมแปลงเงินตราหรือเอกสาร ซึ่งปัจจุบันยังคงทำหน้าที่นี้ แต่ด้วยคำสั่งของรัฐสภาของสหรัฐอเมริกา (Congress) The Secret Service จึงทำหน้าที่ดูแลการกระทำคามผิดเกี่ยวกับคอมพิวเตอร์ด้วย

ในมาตรา ๑๒๐๙ ลักษณะ ๑๘ ของ U.S. code ได้บัญญัติให้ The Secret Service มีอำนาจเหนือการขโมยโดยใช้เครื่องมือในการเข้าสู่ระบบคอมพิวเตอร์ (access device fraud) ดังเช่น บัตร แผ่น รหัส เลขบัญชี หรือสิ่งอื่นๆที่แสดงถึงการเข้าสู่ระบบคอมพิวเตอร์ ที่สามารถใช้ได้ด้วยตัวมันเอง หรือโดยอาศัยการเชื่อมต่อกับเครื่องมือในการเข้าสู่ระบบคอมพิวเตอร์อื่นๆ เพื่อให้ได้มาซึ่งเงิน สินค้า บริการ หรือสิ่งมีค่าอื่นๆ หรือสามารถใช้ในการโอนเงิน ลักษณะ ๑๘ นี้ไม่ได้อ้างถึงการทำความผิดเกี่ยวกับคอมพิวเตอร์โดยเฉพาะ แต่มาตรา ๑๐๒๙ นี้ทำให้ The Secret Service มีหน้าที่ที่จะติดตามผู้ซึ่งใช้รหัสทางไกลที่ได้ขโมยมา ผู้ซึ่งเสนอขายเลขบัตรเครดิต หรือผู้ซึ่งให้รหัสผ่านแก่ผู้อื่นเพื่อให้ช่วยบุกรุกเข้าสู่ระบบคอมพิวเตอร์

แต่อย่างไรก็ตามหน้าที่ของ The Secret Service ก็มีข้อจำกัด คือ

ก. ข้อหานั้นต้องกระทัประหว่างรัฐหรือการพาณิชย์ระหว่างประเทศ เพื่อที่จะให้เป็นปัญหาของรัฐบาลกลางของสหรัฐอเมริกา (Federal jurisdiction)

<sup>๓๘</sup> "อาชญากรรมคอมพิวเตอร์ภัยคุกคามอี-คอมเมิร์ซ."วารสาร e-commerce (กรกฎาคม ๒๕๔๒):

ข. มาตรา ๑๐๒๙ กำหนดความสูญเสียขั้นต่ำไว้ ๑,๐๐๐ ดอลลาร์ ซึ่งทำให้เห็นได้ว่าไม่ใช่การกระทำผิดเกี่ยวกับคอมพิวเตอร์ทุกอย่างจะอยู่ในอำนาจของ The Secret Service

และในมาตราถัดไป มาตรา ๑๐๓๐(d) The Secret Service กระทำหน้าที่ของตนภายใต้การกำกับของเลขาธิการกรมคลังและอธิบดีกรมอัยการ ซึ่งอธิบดีกรมอัยการเป็นหัวหน้าของ FBI ซึ่งหมายความว่ามิใช่เขตอำนาจคาบเกี่ยวกันระหว่างสององค์กร

#### ๔.๒.๒ NCCS (The National Computer Crime Squad)

NCCS เป็นหน่วยงานพิเศษของ FBI ซึ่งรับผิดชอบการสืบสวนการละเมิดต่อ พระราชบัญญัติการขโมยและการกระทำผิดเกี่ยวกับคอมพิวเตอร์ปี ๑๙๘๖ พระราชบัญญัตินี้ได้บัญญัติถึงการบุกรุกทางคอมพิวเตอร์ระหว่างรัฐหรือระหว่างประเทศโดยเข้าไปในเครื่องคอมพิวเตอร์ของรัฐบาลกลางหรือมลรัฐ หรือการเข้าถึงคอมพิวเตอร์ซึ่งมีข้อมูลที่บันทึกไว้ทางการเงินหรือทางการแพทย์

นอกจากนี้ NCCS ยังสืบสวนการบุกรุกเข้าไปในบริษัทโทรศัพท์หรือเครือข่ายคอมพิวเตอร์ที่สำคัญเช่น อุตสาหกรรม จารกรรม ขั้วโรงงานอาคาร อาชญากรรมองค์กรและการละเมิดลิขสิทธิ์ซอฟต์แวร์<sup>๕๐</sup> รวมถึงการกระทำผิดอื่นซึ่งมีเครื่องคอมพิวเตอร์เป็นปัจจัยหลัก

#### ๔.๒.๓ The Infrastructure Protection Task Force (IPTF)

IPTF เป็นหน่วยงานหนึ่งของรัฐบาล เพื่อสืบสวนความเป็นไปได้ในการถูกโจมตีจากผู้ก่อการร้ายทางอิเล็กทรอนิกส์ ต่ออุตสาหกรรมและบริการที่สำคัญ มีหน้าที่ร่วมมือกับรัฐบาลและเอกชนพยายามที่จะป้องกันสาธารณูปโภคที่สำคัญของชาติ IPTF ประกอบด้วยสมาชิกจากหลายองค์กรของรัฐบาล เช่น FBI ,The Central Intelligence Agency, The National Security Agency, The national Communications System, The Departments of Defense, Energy, Justice, Commerce, Transportation, and Treasury

---

<sup>๕๐</sup> การละเมิดลิขสิทธิ์และการขโมยส่วนประกอบทางคอมพิวเตอร์นั้น มีการประมาณความสูญเสียประจำปี มากกว่า ยี่สิบสี่พันล้านเหรียญสหรัฐ ทั่วโลก

สาธารณูปโภคหลายชนิดที่ IPTF ดูแล ใช้เครื่องคอมพิวเตอร์ในการปฏิบัติงานทำให้ภาระหน้าที่ในการดูแลของ IPTF มีความสำคัญมากในการป้องกันผลกระทบต่อความเป็นอยู่ของประชาชน สาธารณูปโภคที่สำคัญนี้ หน่วยงานของรัฐคือ FBI ได้กำหนดไว้ ๘ ประการด้วยกันคือ

๑. การติดต่อสื่อสาร เช่นบริษัทโทรศัพท์ และเครือข่ายคอมพิวเตอร์
๒. ระบบไฟฟ้า เช่นบริษัทที่จัดการเกี่ยวพลังงาน
๓. การผลิต การเก็บรักษา การขนถ่ายก๊าซและน้ำมัน
๔. การเงินและธนาคาร
๕. ระบบขนส่ง เช่น เครื่องบิน รถไฟ และถนน
๖. ระบบจ่ายน้ำ
๗. บริการฉุกเฉิน เช่น ตำรวจ รถพยาบาล รถดับเพลิง หรือการช่วยเหลือบุคคลอื่นๆ
๘. การให้บริการของรัฐบาล

#### ๔.๒.๔ The Federal Computer Investigations Committee (FCIC)

FCIC ตั้งอย่างไม่เป็นทางการในปี ค.ศ. ๑๙๘๖ ซึ่งหน่วยงานนี้มีผู้ให้ความเห็นว่าเป็นหน่วยงานที่สำคัญและทรงอิทธิพลในยุคที่อเมริกาเต็มไปด้วยอาชญากรรมคอมพิวเตอร์ FCIC จะแปลกกว่าหน่วยงานของรัฐทั่วไป ตรงที่ FCIC ไม่มีสำนักงาน จดหมายร้องเรียนที่ส่งถึง FCIC จะถูกส่งต่อไปยังกองที่รับผิดชอบการฉ้อโกง (Fraud Division) ของ The Secret Service คณะทำงานของ FCIC จะประกอบด้วยผู้เชี่ยวชาญด้านการรักษาความปลอดภัยทางคอมพิวเตอร์จากหลายแห่งและหลายสาขา เช่น พนักงานของบริษัทโทรศัพท์ ตำรวจของรัฐหรือของท้องถิ่น นักสืบเอกชน เจ้าหน้าที่ของ The Secret Service เจ้าหน้าที่ FBI นักกฎหมาย โปรแกรมเมอร์ ทหาร โดยสมาชิกเหล่านี้จะไม่ทำงานเต็มเวลา แต่จะร่วมมือกันเป็นคราวๆไป เมื่อถึงเวลา และกลับไปทำงานตามปกติเมื่อยังไม่เป็นที่ต้องการ ซึ่งองค์กรที่ต่อสู้กับการทำความผิดเกี่ยวกับคอมพิวเตอร์ในอนาคตอาจถูกบังคับให้ทำงานในลักษณะนี้ก็เป็นได้ เมื่อพิจารณาถึงลักษณะการทำความผิดทางคอมพิวเตอร์ที่ต้องการความเชี่ยวชาญเฉพาะแต่ไม่ได้เกิดขึ้นบ่อยครั้ง

#### ๔.๒.๕ Computer Emergency Response Team (CERT)

CERT ก่อตั้งขึ้นในปี ค.ศ. ๑๙๘๘ โดยสถาบันวิศวกรรมทางซอฟต์แวร์ (the software engineering institute) ที่มหาวิทยาลัย Carnegie Mellon ใน Pittsburgh ทำหน้าที่หลักในการป้องกันการกระทำผิดจากผู้ใช้อินเทอร์เน็ต CERT รู้ว่าควรกระทำอย่างไรเมื่อพบการทำความผิด

ผิดหรือเมื่อเผชิญกับสถานการณ์ฉุกเฉิน ข้อมูลเกี่ยวกับการรักษาความปลอดภัยนอกจากหาได้ที่ CERT แล้วสามารถค้นได้จากเครือข่ายอินเทอร์เน็ตที่

[www.ovnet.com/~dckinder/frmain01.htm](http://www.ovnet.com/~dckinder/frmain01.htm)

หรือหาได้จากเครื่องช่วยในการค้นข้อมูล(search engine) อื่นๆ บนอินเทอร์เน็ต<sup>๙๙</sup>

โดยสรุปแล้ว ลักษณะพิเศษของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตคือ การมีความรู้ ความชำนาญ ประกอบกับความเร็วในการลงมือกระทำคามผิดที่มีหน่วยวัดเพียงแค่วินาทีหรือนาที ความมีประสิทธิภาพในการทำงานประสานกันขององค์กรหรือหน่วยงานที่เกี่ยวข้องจะเป็นเป้าหมายหรือจุดประสงค์ข้อหนึ่งในการป้องกันการกระทำคามผิด ซึ่งไม่เพียงมีผลเฉพาะผู้เจาะระบบคอมพิวเตอร์โดยไม่มีอำนาจเท่านั้น แต่รวมถึงอาชญากรรมคอมพิวเตอร์หรือการกระทำผิดเกี่ยวกับคอมพิวเตอร์อื่นๆด้วยเช่นกัน

เมื่อพิจารณาถึงหน่วยงานในกระบวนการยุติธรรมในประเทศไทย เห็นได้ว่ามีเพียงหน่วยงานเดียวซึ่งถือว่าเป็นด่านแรกในการสืบสวนสอบสวนการกระทำคามผิด คือตำรวจ ซึ่งผู้เขียนเห็นว่าลำพังการดูแลรักษาความสงบเรียบร้อยของสังคมโดยทั่วไป พนักงานตำรวจต้องรับภาระเป็นจำนวนมากอยู่แล้ว ดังนั้นการก่อตั้งหน่วยงานไม่ว่าจะเป็นในระดับองค์กรหรือในระดับแผนกขึ้นใหม่ เพื่อเป็นหน่วยงานที่ช่วยเสริมหรือร่วมลงมือในการสืบสวน และดูแลทางด้านเทคนิคเกี่ยวกับคอมพิวเตอร์ร่วมกับพนักงานตำรวจ อาจขจัดปัญหาในกรณีขาดความเชี่ยวชาญของพนักงานตำรวจได้ แต่อย่างไรก็ตามพนักงานตำรวจเป็นเพียงองค์ประกอบหนึ่งของกระบวนการยุติธรรม ซึ่งต้องอาศัยการทำงานประสานกันกับองค์กรที่เหลือคือ อัยการซึ่งมีหน้าที่ในการพิจารณาพยานหลักฐานว่าสมควรเสนอฟ้องต่อศาลหรือไม่ และศาลซึ่งเป็นผู้มีหน้าที่วินิจฉัยพยานหลักฐานที่น่าเสนอขึ้นมาเช่นกัน เพราะหากว่าองค์ประกอบทั้งสามองค์กรนี้้องค์กรใดไม่มีความเข้าใจหรือขาดความเชี่ยวชาญทางคอมพิวเตอร์โดยเฉพาะ ก็จะมีผลต่อความมีประสิทธิภาพในการนำตัวผู้กระทำผิดมาลงโทษและมีผลทำให้การป้องกันการกระทำคามผิดตามนโยบายทางอาญาไม่ประสบผลสำเร็จ

<sup>๙๙</sup> เรียบเรียงจาก Gina De Angelis, *Cyber Crimes* (Philadelphia:Chelsea House



กฎหมายโดยตัวของมันเองไม่มีผลบังคับ ต้องอาศัยคนดำเนินการให้เป็นไปตามกฎหมาย จึงเป็นการสมควรที่เราจะต้องเอาใจใส่ต่อบุคคลที่ประกอบเป็นกลไกของกฎหมายว่ามีความสามารถในการทำงานขนาดไหนและไม่มอบงานให้ทำมากกว่าความสามารถนั้น ...กฎหมายไม่ใช่เครื่องมือที่ใช้ทำอะไรได้ทุกอย่างดังประสงค์เสมอไป ฉะนั้นเมื่อจะออกกฎหมายอย่างไร เราจะต้องพิจารณาถึงความสามารถและความเหมาะสมในการใช้กฎหมายเป็นเครื่องมือนำมาซึ่งผลที่เราประสงค์ด้วย<sup>๙๖</sup>

จากการศึกษาความรับผิดชอบทางอาญาของผู้เจาะระบบคอมพิวเตอร์ตามนโยบายทางอาญา ทั้งสี่ประการสรุปได้ว่า ประมวลกฎหมายอาญาปัจจุบันไม่สามารถรองรับกับการกระทำของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ไม่ว่าจะอยู่ในขั้นตอนใดของการเจาะระบบคอมพิวเตอร์ อีกทั้งการปรับใช้มาตราที่ใกล้เคียงได้ก่อให้เกิดปัญหาความไม่สอดคล้องกับจุดประสงค์หรือองค์ประกอบในแต่ละมาตรา ซึ่งทำให้ปัญหาการกระทำผิดของผู้เจาะระบบคอมพิวเตอร์ไม่ได้รับการแก้ไข แต่อย่างไรก็ตามจากการศึกษาทำให้ทราบว่า การปฏิบัติต่อผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตต้องอาศัยความร่วมมือของคนในสังคมและหน่วยงานในกระบวนการยุติธรรมเพื่อประสิทธิภาพในการป้องกันและปราบปรามการเจาะระบบคอมพิวเตอร์

---

<sup>๙๖</sup> อุททิศ แสนโกติก,กฎหมายอาญาภาค ๑ ,หน้า ๑๒