บทที่ ๕

แนวทางในการกำหนดให้การแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดอาญา

ดังที่ได้กล่าวในบทที่ ๔ ถึงปัญหาการปรับใช้ประมวลกฎหมายอาญากับการกระทำความผิดของผู้เจาะระบบคอมพิวเตอร์ในขั้นตอนต่างๆ ซึ่งผู้เขียนได้ละประเด็นในเรื่องการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตไว้ว่า ถึงแม้จะไม่มีกฎหมายบัญญัติให้การแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดโดยเฉพาะ แต่ถ้าหากได้ทำการศึกษาต่อไปอาจจะเป็นทางเลือกหนึ่งที่สามารถนำมาเป็นแนวทางในการกำหนดลักษณะของบทกฎหมายเพื่อป้องกันการกระทำความผิดทางคอมพิวเตอร์ได้ในอนาคต ดังนั้นในลำดับต่อไปจึงเป็นการเสนอแนวทางในการกำหนดความรับผิดสำหรับการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

๑. เหตุผลในการใช้มาตรการทางอาญากับการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

เหตุผลที่นำมาตรการทางอาญามาใช้กับการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต เพราะเมื่อพิจารณาขั้นตอนการกระทำความผิดของผู้เจาะระบบคอมพิวเตอร์ กล่าวคือ

ขั้นตอนที่ ๑. การกระทำก่อนหรือขณะเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

ขั้นตอนที่ ๒. การกระทำที่เกิดขึ้นภายหลังจากการเจาะระบบคอมพิวเตอร์แล้วก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์

ขั้นตอนที่ ๓. การแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

จะเห็นได้ว่าในขั้นตอนแรกเป็นขั้นตอนที่ต้องอาศัยวิธีการ เครื่องมือและระยะเวลาในการเจาะผ่านระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์ให้ได้ก่อน ซึ่งการลองผิดลองถูกและยังไม่มีการเข้าไปในระบบคอมพิวเตอร์นี้ยังห่างไกลต่อความเสียหายที่จะเกิดขึ้น จึงเป็นการไม่สมควรที่จะนำมาตรการทางอาญามาใช้กับการกระทำขั้นตอนก่อนหรือขณะเจาะระบบคอมพิวเตอร์นี้

สำหรับในขั้นตอนที่ ๒ คือเมื่อเข้าไปในระบบคอมพิวเตอร์ได้แล้ว ทำให้เสียหายแก่ข้อมูลหรือระบบคอมพิวเตอร์ เป็นขั้นตอนที่ล่วงเลยการป้องกันไม่ให้เกิดความเสียหายแล้ว แต่เป็นขั้นตอนในการแก้ไขหรือเยียวยาผลที่เกิดจากการกระทำ เช่นเมื่อมีการลบข้อมูลทั้งหมดในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การนำมาตรการทางอาญามาใช้ก็เพื่อจุดประสงค์ที่จะลงโทษผู้

กระทำผิดและหาทางแก้ไขข้อมูลที่สูญหายไป ซึ่งจะต่างกับการกระทำความผิดในขั้นตอนที่สาม คือการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ที่ต้องการมาตรการทางอาญาเพื่อจุดประสงค์ในการป้องกันการกระทำความผิดที่จะเกิดขึ้นในอนาคต ไม่ใช่มีมาตรการทางอาญาไว้เพื่อลงโทษหรือแก้ไขเมื่อเกิดการกระทำความผิดขึ้น จึงเป็นเหตุผลที่ผู้เขียนเลือกที่จะใช้มาตรการทางอาญาในขั้นตอนการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดสำเร็จทางอาญา อีกทั้งการนำมาตรการทางอาญามาใช้กับขั้นตอนการแรกเข้าไปในระบบคอมพิวเตอร์นี้สามารถป้องกันมิให้เกิดความเสียหายต่อข้อมูลที่เกิดขึ้นในขั้นตอนที่ ๒ ได้อีกทางหนึ่ง

๒. ลักษณะของบทบัญญัติว่าด้วยการแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตควรมีลักษณะอย่างไร

ลักษณะบทบัญญัติของกฎหมายอาญาแบ่งออกได้เป็น ๓ ลักษณะคือ

๑. บัญญัติว่าการกระทำอย่างนั้นอย่างนี้**เป็นความผิด** เช่น บัญญัติว่าผู้ใดกระทำการลักทรัพย์มีความผิด

๒. บัญญัติ**บังคับให้กระทำการ**อย่างนั้นอย่างนี้ และบัญญัติต่อไปว่าถ้าผู้ใดไม่ทำตามมีความผิด เช่นบัญญัติว่า ผู้ชายไทยที่มีอายุ ๑๗ ปีบริบูรณ์ต้องไปขึ้นทะเบียนทหาร ถ้าฝ่าฝืนไม่กระทำตามมีความผิด

๓. บัญญัติ**ห้ามมิให้กระทำ**อย่างนั้นอย่างนี้ และบัญญัติต่อไปว่าถ้าฝ่าฝืนไม่ปฏิบัติตามมีความผิด[๕]

การบัญญัติให้การแรกเข้าสู่ระบบคอมพิวเตอร์เป็นความผิดสมควรจะมีรูปแบบเช่นใดนั้นสามารถพิจารณาได้จากหลักที่แฝงอยู่ในแนวความคิดดังกล่าว ซึ่งคือต้องการป้องกันการกระทำความผิดที่อาจจะเกิดขึ้นต่อไปในอนาคต แต่โดยที่แนวความคิดนี้เป็นแนวคิดใหม่และคนส่วนใหญ่ไม่ทราบว่าการกระทำเช่นนี้เป็นความผิด เหตุนี้บทบัญญัติจึงควรอยู่ในรูปแบบแรกคือการกำหนดว่าการกระทำอย่างไรเป็นความผิด เพราะจะเป็นการขัดเขินหากบัญญัติห้ามมิให้กระทำ แต่มิได้กล่าวว่าการกระทำดังกล่าวเป็นความผิด ซึ่งจะต่างกับความผิดที่เห็นได้ว่าเป็นความผิดอย่างชัดเจน ซึ่งจะบัญญัติห้ามมิให้กระทำได้เลยเช่น ความผิดฐานลักทรัพย์เป็นต้น

---

[๕] พระยาอรรถการีย์นิพนธ์, "ความรับผิดของบุคคลในทางอาญา," บทบัณฑิตย์ เล่มที่ ๒๖ ตอนที่ ๑-๒ (พฤษภาคม ๒๕๑๒): ๙๘.

การบัญญัติความรับผิดทางอาญาขึ้นใหม่นั้น สิ่งที่จะต้องนำมาพิจารณาคือ*โครงสร้างความรับผิดทางอาญา*ซึ่งมีส่วนสำคัญอย่างมากในการที่จะกำหนดองค์ประกอบของความผิดที่จะบัญญัติขึ้นใหม่

โครงสร้างของความผิดอาญา (Varbrechensaufbau)

การพิจารณาในเรื่องบทบัญญัติของกฎหมายอาญา จำเป็นที่ต้องทราบว่าโครงสร้างของกฎหมายอาญาเป็นเช่นไร เพื่อที่จะสามารถศึกษาองค์ประกอบของแต่ละมาตราที่ได้บัญญัติขึ้นหรือที่จะบัญญัติขึ้นในอนาคตได้อย่างชัดเจนยิ่งขึ้น[๖] ประเทศเยอรมันเป็นประเทศที่มีการศึกษาค้นคว้าและพัฒนากฎหมายมาเป็นเวลานาน อีกทั้งยังเป็นประเทศที่มีอิทธิพลต่อการพัฒนากฎหมายในเอเชียโดยเฉพาะประเทศไทย ซึ่งมีระบบกฎหมายเป็นระบบประมวลกฎหมาย (Codification) เช่นเดียวกัน การแยกพิจารณาโครงสร้างความผิดอาญา จึงแยกพิจารณาตามหลักการในกฎหมายเยอรมันอันเป็นที่ยอมรับในปัจจุบัน ๓ ประการ คือ

- ส่วนขององค์ประกอบ หรือการกระทำที่กฎหมายบัญญัติ
- ส่วนของความผิด
- ส่วนของความชั่ว

เมื่อมีการแยกโครงสร้างความผิดอาญาออกเป็น ๓ ส่วนดังกล่าวแล้ว การวินิจฉัยความรับผิดทางอาญาในปัจจุบันจึงเริ่มจากการพิจารณาว่าการกระทำนั้นครบองค์ประกอบที่กฎหมายบัญญัติไว้หรือไม่ เมื่อการกระทำนั้นเข้าองค์ประกอบที่กฎหมายบัญญัติแล้วจึงจะพิจารณาต่อไปว่า การกระทำนั้นผิดกฎหมายหรือไม่ และขั้นต่อไปก็พิจารณาว่าตัวผู้กระทำมีความชั่วหรือไม่ ข้อสาระสำคัญทั้งสามประการของความผิดอาญานี้เกี่ยวข้องกันอย่างเรียงลำดับ กล่าวคือหากการกระทำใดไม่เป็นการกระทำที่ครบองค์ประกอบแล้วกรณีก็ไม่ต้องพิจารณาต่อไปถึงข้อสาระสำคัญประการที่สองและสาม และในทำนองเดียวกันหากการกระทำใดเป็นการกระทำที่ครบองค์ประกอบ

---

[๖] นอกจากนี้การวินิจฉัยคดีตามโครงสร้างของความผิดอาญาจะทำให้การวินิจฉัยคดีเป็นไปด้วยเหตุด้วยผลและตรงกับความรู้สึกของประชาชนทั่วไป และเกิดความเสมอเหมือนกันในทุกคดีซึ่งเป็นหลักประกันว่าการใช้กฎหมายจะมีความแน่นอนและมั่นคง

แต่การกระทำนั้นไม่เป็นการกระทำที่เป็นความผิด กรณีก็ไม่ต้องพิจารณาต่อไปถึงเรื่องความชั่ว[๓]ซึ่งหากข้อเท็จจริงที่เกิดขึ้นครบองค์ประกอบในโครงสร้างทั้ง ๓ ประการแล้ว จึงจะทำให้การกระทำนั้นเป็นความผิดอาญาและต้องรับโทษสำหรับการกระทำนั้น

ในส่วนแรกคือส่วนขององค์ประกอบ พิจารณาจากตัวบทบัญญัติที่ไม่ใช่เป็นการกระทำโดยประมาทโดยทั่วไปแล้วมีอยู่ ๒ ประเภท คือ องค์ประกอบภายนอกและองค์ประกอบภายใน

<u>องค์ประกอบภายนอกจะกล่าวถึง</u>

- ผู้กระทำ ในส่วนที่เกี่ยวกับตัวผู้กระทำโดยทั่วไปกฎหมายใช้คำว่า " ผู้ใด" โดยปกติจะไม่จำกัดว่าผู้กระทำเป็นใคร เว้นแต่ในบางกรณีผู้กระทำต้องเป็นเจ้าพนักงาน ดังเช่น มาตรา ๑๔๗-๑๖๖
- การกระทำ เช่นการทำร้าย การเอาไป การเข้าไป โดยรวมถึงการงดเว้นการที่จักต้องกระทำตามประมวลกฎหมายอาญามาตรา ๕๙ วรรคท้าย
- ผลของการกระทำ ซึ่งความผิดอาญามีทั้งที่ต้องการผล เช่น ทรัพย์ถูกทำลายในกรณีความผิดฐานทำให้เสียทรัพย์ และความผิดที่ไม่ต้องการผล เช่นการแจ้งความเท็จ
- กรรมของการกระทำ เช่นทรัพย์ในความผิดเกี่ยวกับทรัพย์หรือมนุษย์ในความผิดต่อร่างกายหรือต่อชีวิต

<u>องค์ประกอบภายใน ได้แก่</u>

- เจตนา กล่าวคือผู้กระทำจะต้องรู้ถึงข้อเท็จจริงอันเป็นองค์ประกอบของความผิดและผู้กระทำต้องประสงค์ต่อผลหรือย่อมเล็งเห็นผลของการกระทำนั้น ฉะนั้นผู้ที่มีเจตนาฆ่าผู้อื่นตามมาตรา ๒๘๘ ผู้กระทำจะต้องรู้ว่าผู้ที่ตนจะฆ่านั้นเป็นมนุษย์และตนต้องการให้มนุษย์นั้นตาย
- มูลเหตุชักจูงใจ เช่นการลักทรัพย์ จะต้องกระทำด้วยมูลเหตุชักจูงใจโดยทุจริต หรือการฆ่าผู้อื่นโดยมีมูลเหตุชักจูงใจเพื่อปกปิดความผิดของตน
- องค์ประกอบภายในที่นอกเหนือจากเจตนาและมูลเหตุชักจูงใจ เช่นการไตร่ตรองไว้ก่อน ทรมาน หรือกระทำทารุณโหดร้าย[๔]

---

[๓] คณิต ณ นคร ,"โครงสร้างความรับผิดทางอาญาและข้อถกเถียงทางวิชาการเกี่ยวกับ mens rea , "<u>วารสารนิติศาสตร์</u> ปีที่ ๑๖ ฉบับที่ ๓ (กันยายน ๒๕๒๙): ๒๐๙

[๔] กมลชัย รัตนสกาววงศ์, สัมนากฎหมายอาญาชั้นปริญญาโท(กรุงเทพมหานคร:สำนักพิมพ์นิติธรรม,๒๕๓๘),หน้า ๒.

โดยสรุปแล้วการบัญญัติกฎหมายจึงต้องพิจารณาทั้งองค์ประกอบภายนอกและองค์ประกอบภายใน ดังนี้คือ

๑. องค์ประกอบภายนอก ต้องบัญญัติลักษณะการกระทำให้ชัดแจ้งว่าต้องมีการกระทำอย่างไร การกระทำนี้ต้องการผลหรือไม่ และกรรมของการกระทำคืออะไร

๒. องค์ประกอบภายใน พิจารณาว่าการกระทำดังที่กล่าวในองค์ประกอบภายนอกนั้นควรมีเจตนา หรือมีเหตุจูงใจในการกระทำหรือไม่ หรือสมควรจะบัญญัติให้เป็นความรับผิดเด็ดขาดแม้ไม่ต้องการเจตนา และสมควรกำหนดความรับผิดในกรณีการกระทำโดยประมาทร่วมด้วยหรือไม่

๓. องค์ประกอบความผิดฐานบุกรุกและการแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

แนวความคิดเกี่ยวกับการเข้าสู่สถานที่ใดๆ โดยไม่ได้รับอนุญาตไม่ว่าในโลกของอิเล็กทรอนิกส์และในโลกของชีวิตจริงที่คล้ายกันคือ เพื่อปกป้องสิทธิและแยกความเป็นส่วนตัวออกจากความเป็นสาธารณะ ดังเช่นในโลกของชีวิตจริงมีการกำหนดความรับผิดเกี่ยวกับการบุกรุกไว้ในประมวลกฎหมายอาญา แต่สำหรับโลกของอิเล็กทรอนิกส์แล้ว จะเกิดปัญหาว่าความรับผิดของผู้บุกรุกเป็นเช่นใด การพิจารณาองค์ประกอบของความรับผิดฐานบุกรุกอาจทำให้มองเห็นแนวทางในการบัญญัติกฎหมายในส่วนที่เกี่ยวกับอิเล็คทรอนิกส์ได้เช่นกัน

ประมวลกฎหมายอาญา มาตรา ๓๖๒ ได้บัญญัติไว้ว่า *ผู้ใดเข้าไปในอสังหาริมทรัพย์ของผู้อื่น เพื่อถือการครอบครองอสังหาริมทรัพย์นั้นทั้งหมดหรือแต่บางส่วน หรือเข้าไปกระทำการใดๆ อันเป็นการรบกวนการครอบครองอสังหาริมทรัพย์ของเขาโดยปกติสุข ต้องระวางโทษจำคุกไม่เกินหนึ่งปีหรือปรับไม่เกินสองพันบาท หรือทั้งจำทั้งปรับ*

มาตรา ๓๖๔ ได้บัญญัติไว้ว่า *ผู้ใดไม่มีเหตุอันสมควร เข้าไปหรือซ่อนตัวอยู่ในเคหสถาน อาคารเก็บรักษาทรัพย์หรือสำนักงานในความครอบครองของผู้อื่น หรือไม่ยอมออกไปจากสถานที่เช่นว่านั้นเมื่อผู้มีสิทธิที่จะห้ามมิให้เข้าไปได้ไล่ให้ออก ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองพันบาท หรือทั้งจำทั้งปรับ*

ในกรณีมาตรา ๓๖๒ สามารถแยกพิจารณาได้เป็นสองตอน คือ

ตอนแรก บุกรุกเพื่อถือการครอบครอง

มีองค์ประกอบภายนอก คือ

๑. เข้าไป

๒. ในอสังหาริมทรัพย์ของผู้อื่น

องค์ประกอบภายใน คือ

๑. เจตนาธรรมดา

๒. มูลเหตุชักจูงใจ เพื่อถือการครอบครองอสังหาริมทรัพย์นั้น ทั้งหมดหรือแต่บางส่วน

ตอนที่สอง บุกรุกเข้าไปกระทำการรบกวนการครอบครอง

มีองค์ประกอบภายนอกคือ

๑. เข้าไป

๒. กระทำการใดๆอันเป็นการรบกวนการครอบครองอสังหาริมทรัพย์ของเขาโดยปกติสุข

องค์ประกอบภายใน คือ

๑. เจตนาธรรมดา

ในกรณีมาตรา ๓๖๔ สามารถแยกพิจารณาออกได้เป็นสองตอนเช่นกัน คือ

ตอนแรก บุกรุกโดยเข้าไปหรือซ่อนตัวอยู่

มีองค์ประกอบภายนอก คือ

๑. เข้าไปหรือซ่อนตัวอยู่

๒. ในเคหสถาน อาคารเก็บรักษาทรัพย์ หรือสำนักงานในความครอบครองของผู้อื่น

๓. โดยไม่มีเหตุอันสมควร

องค์ประกอบภายใน คือ

๑.เจตนาธรรมดา

ตอนที่สอง บุกรุกโดยไม่ยอมออกจากสถานที่

มีองค์ประกอบภายนอกคือ

๑. ไม่ยอมออกไป

๒. จากเคหสถาน อาคารเก็บรักษาทรัพย์ หรือสำนักงานในความครอบครองของผู้อื่น

๓. เมื่อผู้มีสิทธิที่จะห้ามมิให้เข้าไปได้ไล่ให้ออก

๔. โดยไม่มีเหตุอันสมควร

องค์ประกอบภายใน คือ

๑. เจตนาธรรมดา

เมื่อพิจารณาองค์ประกอบในความผิดฐานบุกรุกในมาตรา ๓๖๒ และ ๓๖๔ จะเห็นได้ว่าความผิดฐานบุกรุกมีองค์ประกอบโดยรวม ๔ ประการคือ ๑. การเข้าไป ๒. สถานที่ ๓.โดยไม่มีเหตุอันควร และ๔. เจตนา เมื่อพิจารณาประกอบกับแนวความคิดในกรณีการแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ผู้เขียนจึงแยกองค์ประกอบของการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเทียบเคียงกับองค์ประกอบความผิดฐานบุกรุก ดังนี้ คือ

๓.๑ การเข้าไป (Entry)

ตามประมวลกฎหมายอาญา ความผิดฐานบุกรุกกำหนดให้การเข้าไปเป็นการเข้าไปทางกายภาพและเป็นความผิดแม้จะเป็นการเข้าไปเพียงบางส่วนของร่างกาย[๕] ซึ่งสามารถเข้าใจได้โดยง่าย ดังเช่นนาย ก.นั่งอยู่หน้าเครื่องคอมพิวเตอร์ภายในบ้าน จึงเป็นไปไม่ได้ที่นาย ก.จะสามารถเข้าไปจับต้องทรัพย์สินในบ้านของผู้อื่นด้วยตนเอง แต่ถ้าเป็นระบบคอมพิวเตอร์ ซึ่งด้วยวิธีการทางอิเล็คทรอนิกส์นาย ก. สามารถเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นได้แม้ไม่ได้ออกจากบ้านซึ่งสามารถกระทำได้ง่ายและไม่ต้องเตรียมอุปกรณ์ที่มีประสิทธิภาพอย่างมืออาชีพในการ บุกรุกเข้าไปมากนัก

---

[๕] จิตติ ติงสภัทิย์, คำอธิบายประมวลกฎหมายอาญาภาค ๒ ตอนที่ ๒ และ ภาค ๓ พิมพ์ครั้งที่ ๒ (กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, ๒๕๑๔),หน้า ๒๓๙๔

การบุกรุกตามประมวลกฎหมายอาญาต้องการการเข้าไปทางกายภาพโดยตรง ปัญหาคือแล้วการเข้าไปในระบบคอมพิวเตอร์นั้นอะไรที่เข้าไปเมื่อไม่ใช่ตัวบุคคล ซึ่งแม้ว่ายังไม่มีการตัดสินและอธิบายในเรื่องการเข้าไปในระบบคอมพิวเตอร์ของศาลไทย แต่ก็ปรากฏคำพิพากษาฎีกาที่มีการตัดสินในกรณีเกี่ยวกับเทคโนโลยีทางอิเล็คทรอนิกส์ ดังเช่น การลักกระแสไฟฟ้าและการลักลอบจูนโทรศัพท์มือถือ ซึ่งแสดงให้เห็นว่าศาลไทยยอมรับในเรื่องเทคโนโลยีและอิเล็คทรอนิคที่ไม่อาจจับต้องได้หรือเห็นด้วยตาเปล่า จึงเป็นไปได้ที่จะแสดงให้เห็นว่า " *สัญญาณทางอิเล็คทรอนิคส์ที่สร้างโดยจำเลยมีเหตุเพียงพอที่จะถือว่า สามารถที่จะจับต้องได้และสนับสนุนการกระทำลักษณะบุกรุกดังเช่นประมวลกฎหมายอาญาได้เช่นกัน*" โดยที่คงไม่มีผู้ใดตั้งคำถามว่าหากยอมรับสัญญาณทางอิเล็คทรอนิกส์แล้ว การแอบมองข้อมูลขณะที่ผู้อื่นกำลังทำงานหรือการหายใจรดเครื่องคอมพิวเตอร์ซึ่งเป็นการสัมผัสโดยโมเลกุลของอากาศจะเป็นความผิดหรือไม่ เพราะคงเป็นการเข้าใจผิดหากคิดว่ากฎหมายต้องตอบคำถามได้ว่า ทำไมจึงไม่เป็นความผิด กฎหมายเป็นเครื่องมือของรัฐในการรักษาความสงบเรียบร้อยของสังคม แต่รัฐไม่สามารถที่จะกำหนดพฤติกรรมทุกอย่างให้สมาชิกในรัฐนั้นทราบได้ว่าการกระทำอย่างใดประพฤติได้ การกระทำใดไม่สมควรประพฤติเพราะการกระทำบางอย่างบุคคลทั่วไปสามารถอาศัยเหตุผลของความเป็นมนุษย์พิจารณาได้ว่าถูกต้องหรือไม่ เว้นแต่การกระทำบางประการที่กฎหมายต้องการดูแลเป็นพิเศษจึงต้องบัญญัติไว้ให้ความชัดเจนโดยเฉพาะ ซึ่งหากนักกฎหมายต้องมาตอบคำถามที่ว่าทำไมการสัมผัสโดยโมเลกุลของอากาศไม่ถูกนำมาพิจารณาด้วยก็จะมีปัญหาอีกมากมายที่ต้องการค้นคว้าและเข้าใกล้อภิปรัชญาเข้าไปทุกที การให้การยอมรับว่ามีบางสิ่งอยู่จริงตามหลักทางวิทยาศาสตร์น่าจะเป็นการเพียงพอ เพราะมิเช่นนั้นแล้วคงไม่มีนักกฎหมายใดกล้าที่จะบัญญัติกฎหมายเพียงเพราะไม่สามารถตอบคำถามได้ว่าโมเลกุลเกิดมาได้อย่างไร ซึ่งออกจะเกินเลยไป

คำว่า "**เข้าไป**" ถ้าหากจะเปรียบเทียบกับคำในบทกฎหมายที่เกี่ยวกับความรับผิดทางคอมพิวเตอร์แล้ว สามารถเทียบได้กับคำว่า "Access" ซึ่งมีความหมายดังที่กล่าวไว้แล้วในบทที่ ๒[๖] Access เป็นคำที่มีความหมายเฉพาะและกว้างกว่าความเข้าใจทั่วไปต่อคำว่า "เข้าไป" และการที่ Access มีความหมายเฉพาะเช่นนี้ นำมาซึ่งปัญหาในการปรับใช้บทกฎหมายในสหรัฐอเมริกา ดังเช่นคดีระหว่างรัฐแคนซัสและแอนโทนี เอเล็น (State v. Allen) ซึ่งมีข้อเท็จจริงดังนี้ คือ

---

[๖] อ่านประกอบหน้า ๑๗

ในวันเสาร์ที่ ๓ มีนาคม ขณะอายุ ๑๘ ปี เอเล็นถูกจับกุมในมณฑลจอห์นสัน ฐานประกอบอาชญากรรมคอมพิวเตอร์ หลังจากเจาะเข้าไปในระบบคอมพิวเตอร์ของ SWBT (Southwestern Bell Telephone) ระหว่างวันที่ ๑๕ ธันวาคม ๑๙๙๕ ถึงวันที่ ๒๔ มกราคม ๑๙๙๖ แต่คดีถูกยกในชั้นไต่สวนมูลฟ้อง เอเล็นใช้โมเด็มในการโทรศัพท์ถึงระบบคอมพิวเตอร์ของ SWBT โดยได้หมายเลขมาจากการใช้เครื่องมือ war dialer ในการสุ่มหมายเลขโทรศัพท์ โดยอ้างว่ากระทำไปเพื่อจุดประสงค์ในการเรียนรู้และอยู่ในระบบคอมพิวเตอร์เพียงเพื่อที่จะสำรวจโดยทั่วๆไปเท่านั้น แต่เอเล็นก็ยอมรับว่าเขาไม่สนใจต่อป้ายคำเตือนของบริษัท SWBT และรู้ว่าเขาไม่ได้รับอนุญาตในการต่อโทรศัพท์เข้าระบบคอมพิวเตอร์

บริษัท SWBT มีอุปกรณ์หลายชนิดซึ่งเป็นสิ่งจำเป็นในการให้บริการแก่ลูกค้า ดังเช่น ระบบควบคุมสภาพทั่วไปคือ SLC-96 และระบบฐานข้อมูลคือ SMS-800 บริษัท SWBT จะให้หมายเลขโทรศัพท์สำหรับระบบ SLC-96และ SMS-800 ในกรณีที่จำเป็น การทำงานของระบบดังกล่าวจะเริ่มจากเมื่อโทรศัพท์ถึงระบบ SLC-96 คำว่า "รหัสผ่าน" จะปรากฏขึ้นเพื่อจะรับคำสั่งและผู้ใช้ถูกกำหนดให้ใส่รหัสผ่านเพื่อที่จะสามารถใช้ระบบได้ ส่วนระบบ SMS-800 ระบบจะปรากฏคำเตือนว่า การเข้าไปในระบบนั้นถูกสงวนไว้โดยเฉพาะและเป็นสมบัติของ SWBT เท่านั้น ผู้อำนวยการทั่วไปว่าด้วยการรักษาความปลอดภัย (Ronald Knisley) ให้การว่า เอเล็นเชื่อมต่อกับระบบ SMS-800 โดยกระทำทั้งหมด ๒๘ ครั้ง ซึ่งใช้เวลาน้อยกว่าหนึ่งนาที ขณะที่ เจมส์ โรบินสัน (James K. Robinson) ให้การว่าเอเล็นใช้เวลาหกนาทีสามสิบห้าวินาทีสำหรับการโทรศัพท์ติดต่อกับระบบ SMS-800 ซึ่งการเข้าระบบ SMS-800 โดยใช้คำสั่งพิเศษจะทำให้สามารถเข้าถึงระบบ PBX ที่อนุญาตให้สามารถโทรศัพท์ทางไกลโดยไม่จำกัดและไม่เสียค่าใช้จ่ายใดๆ ซึ่งการกระทำของเอเล็นนี้ทำให้ SWBT ใช้เงินกว่า ๔,๑๔๐ เหรียญสหรัฐในการสืบสวนที่มาของการติดต่อ ๑,๖๕๖ เหรียญสหรัฐสำหรับพัฒนาระบบรักษาความปลอดภัยและ ๑๘,๐๐เหรียญสหรัฐในการทำบัตรรักษาความปลอดภัยประจำตัว ซึ่งรวมทั้งหมด ๒๓,๗๙๖ เหรียญสหรัฐ

รัฐแคนซัสฟ้องเอเล็นภายใต้บทบัญญัติว่าด้วยอาชญากรรมคอมพิวเตอร์ ในตอนที่ ๒๑ มาตรา ๓๗๕๕(b)[๗] แต่อย่างไรก็ตามรัฐก็ไม่สามารถแสดงพยานหลักฐานได้ว่าเอเล็นได้เข้าไป แก้

---

[๗] Kansas Statutes Annotated Chapter 21 ,section 3755

(B) computer crime is: (1) Intentionally and without authorization gaining or attempting to gain access to and damaging, modifying, altering, destroying, copying, disclosing or taking possession of a computer, computer system, computer network or any other property;...

ไข เพิ่ม ใช้หรือขัดขวางระบบคอมพิวเตอร์ของSWBT และไม่มีพยานหลักฐานที่แสดงว่าเอเล็นพยายามที่จะใช้รหัสผ่านหรือเชื่อมต่อกับระบบคอมพิวเตอร์ ผู้จัดการฝ่ายรักษาความปลอดภัยของบริษัทและเจมส์ โรบินสัน กล่าวว่าโดยปกติคอมพิวเตอร์จะบันทึกข้อมูลเกี่ยวกับการใช้โทรศัพท์ แต่ปรากฏว่าระหว่างการใช้งานของเอเล็นไม่พบข้อมูลดังกล่าว แม้โรบินสันจะไม่มีหลักฐานใดๆ แต่เขาสงสัยว่าเอเล็นได้เข้าระบบคอมพิวเตอร์และแก้ไขการทำงานในส่วนที่เกี่ยวกับการบันทึกการใช้โทรศัพท์ ซึ่งเขาก็ไม่สามารถที่จะแสดงให้เห็นได้ว่ามีการทำลายระบบคอมพิวเตอร์ดังกล่าว

ระหว่างการไต่สวนมูลฟ้องรัฐแคนซัสยอมรับว่าเอเล็นไม่ได้ แก้ไข เปลี่ยนแปลง ทำลาย สำเนา เปิดเผย หรือเอาไปซึ่งสิ่งใดเลย แต่ก็โต้แย้งว่าการกระทำของเอเล็นทำให้บริษัทต้องทำการแก้ไขและเพิ่มมาตรการรักษาความปลอดภัย ซึ่งการกระทำดังกล่าวเป็นการ"เข้าใกล้" (approach) ตามความหมายของบทบัญญัติในตอนที่ ๒๑ มาตรา ๓๗๕๕(a)(1)[๕] และค่าใช้จ่ายในการปรับปรุงมาตรการรักษาความปลอดภัยเป็นความเสียหายตามองค์ประกอบของบทบัญญัติดังกล่าว

ศาลชั้นต้นพบว่าบทบัญญัติในตอนที่ ๒๑ มาตรา ๓๗๕๕ ไม่ชัดเจนและตัดสินว่าการกระทำของเอเล็นที่ใช้โทรศัพท์ในการเชื่อมต่อกับโมเด็มไม่เป็นการเพียงพอที่จะพิสูจน์ว่าได้มีการ "ได้เข้า" (gained access) ระบบคอมพิวเตอร์ของ SWBT ส่วนค่าใช้จ่ายที่เกิดขึ้นก็เป็นความสมัครใจของบริษัทเองแต่ไม่มีความเสียหายต่อระบบคอมพิวเตอร์หรือทรัพย์สินใดๆดังที่ให้คำนิยามไว้ในบทบัญญัตินั้น

รัฐแคนซัสอุทธรณ์โดยตรงต่อศาลฎีกาภายใต้ บทบัญญัติในตอนที่ ๒๒ มาตรา ๒๖๐๒ (b)(๒)

ศาลฎีกาตัดสินว่าการกระทำความผิดทางคอมพิวเตอร์จะไม่เกิดขึ้นหากผู้กระทำผิดไม่มีความสามารถในการ"ได้รับหรือใช้ประโยชน์"(obtain or make use of) จากเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ถูกบุกรุกนั้น ดังนั้นการกระทำผิดทางคอมพิวเตอร์จึงไม่รวมถึงการกระทำ

---

[๕] Kansas Statutes Annotated Chapter 21 ,section 3755

(a) As used in this section,the following words and phrases shall have the meanings respectively ascribed thereto:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources f a computer,computer system or computer network...

ที่แสดงให้เห็นเพียงการ"เข้าใกล้หรือพยายามที่จะเข้าใกล้" (approaching or attempting to approach) ระบบคอมพิวเตอร์

นอกจากนั้นบทบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ต้องการผู้กระทำผิดที่ก่อให้เกิดความเสียหายสำหรับคอมพิวเตอร์และซอฟท์แวร์ ต้องเป็นการเอาคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือซอฟท์แวร์ไป แต่ค่าใช้จ่ายในการสืบสวนหรือการปรับปรุงระบบรักษาความปลอดภัยไม่สามารถอ้างได้ว่าเป็นค่าเสียหาย ศาลฎีกาตัดสินว่าศาลชั้นต้นตัดสินถูกต้องในการยกฟ้องด้วยเหตุผลที่ขาดมูลเหตุที่แสดงให้เห็นว่าเอเล็นได้เข้าไปในคอมพิวเตอร์ หรือเอาไปซึ่งทรัพย์สินของบริษัทของ SWBT

จากคดีดังกล่าวทำให้เห็นได้ว่าศาลฎีกาแปลความหมายของมาตรา ๓๕๗๗ ให้มีความหมายว่ารัฐจะต้องพิสูจน์องค์ประกอบสามประการในการพิจารณาชั้นไต่สวนมูลฟ้องเพื่อที่จะตัดสินว่าเป็นการกระทำผิดเกี่ยวกับคอมพิวเตอร์อย่างร้ายแรง คือ จงใจและเข้าสู่ระบบโดยไม่ได้รับอนุญาต ,ทำลายข้อมูล และมีความเสียหาย ถ้าเอเล็นไม่ได้ใส่รหัสผ่านเขาก็ไม่สามารถติดต่อกับระบบคอมพิวเตอร์ได้ดังนั้นเขาจึงไม่สามารถที่จะเข้าสู่ระบบคอมพิวเตอร์ได้ดังที่บทกฎหมายต้องการ อีกทั้งรัฐไม่สามารถพิสูจน์ได้ว่าเอเล็นเข้าสู่ระบบคอมพิวเตอร์ของ SWBT ได้โดยแค่เพียงการหมุนหมายเลขโทรศัพท์ **เอเล็นจึงไม่สามารถเข้าระบบคอมพิวเตอร์ได้จนกว่าจะใส่รหัสผ่านที่ถูกต้องและเข้าไปในระบบ**

แต่รัฐแคนซัสโต้เถียงว่าศาลชั้นต้นไม่ได้ปรับใช้คำนิยามที่ถูกต้องของคำว่า"เข้าสู่" (access) ซึ่งข้อนี้ศาลฎีกาได้ให้เหตุผลว่า การโต้เถียงดังกล่าวเป็นความต้องการที่จะให้ศาลเห็นว่าคำว่า "การเข้าใกล้" (approach) เป็นความผิดและเพียงพอที่จะฟ้องสำหรับการเข้าสู่ระบบแล้ว ซึ่งในบทกฎหมายก็ไม่ได้กำหนดให้การ "กำลัง"เข้าสู่ (accessing)และการ"กำลัง"เข้าใกล้ (approaching) เป็นความผิดแต่จะมุ่งถึงการ กำลัง "ได้"(gaining) หรือกำลังพยายาม (attempting) ที่จะ"ได้"เข้าสู่ระบบคอมพิวเตอร์ เมื่อเทียบการกระทำของเอเล็นจะทำให้การหมุนโทรศัพท์ของเอเล็นและการมองดูป้ายคำเตือนเป็นเพียงการ"กำลัง"เข้าใกล้เท่านั้น การกระทำของเขาจะเป็นการได้หรือพยายามที่จะได้เข้าสู่ระบบคอมพิวเตอร์ เมื่อเขาลองใส่รหัสผ่านที่จะทำให้เขาสามารถใช้งานคอมพิวเตอร์และแก้ไขข้อมูลได้ ซึ่งหากศาลยอมรับคำนิยามตามความเห็นของรัฐที่ให้การเข้าสู่กับการเข้าใกล้เหมือนกัน ก็จะทำให้การพยายามได้เข้าใกล้เป็นความผิด (attempting to gain approach) และศาลก็เชื่ออีกว่า*ประชาชนจะไม่เข้าใจว่าการกระทำใดเป็นความผิด* เพราะคำว่า access ไม่ได้มีความหมายโดยทั่วไป จึงทำให้เห็นว่าคำว่า access ควรมีความหมายโดย

ปกติมากกว่าการแปลที่บิดเบือน ซึ่งหากดูความหมายตามพจนานุกรม access จะหมายถึง เสรีภาพหรือความสามารถในการได้หรือได้ใช้ (freedom or ability to obtain or make use)[๙]

การให้ความหมายของคำในกฎหมายที่จะกำหนดพฤติกรรมใดเป็นความผิดจึงมีสำคัญต่อการบังคับใช้กฎหมายต่อไปในอนาคต กรณีของเอเล็นนี้ทำให้เกิดผลในประการต่อมาคือ รัฐแคนซัสไม่พยายามที่จะฟ้องบุคคลใดที่พยามที่จะเข้าสู่ระบบคอมพิวเตอร์โดยไม่มีอำนาจ รวมถึงรัฐอื่นๆก็แทบจะไม่ได้ใช้การเข้าสู่ระบบคอมพิวเตอร์โดยไม่มีอำนาจเป็นสิ่งแรกที่จะใช้ในการควบคุมพฤติกรรมในการกระทำความผิดทางคอมพิวเตอร์

จากที่กล่าวมาจึงสรุปได้ว่า การ"เข้าไป"ในกรณีการแรกเข้าไปในระบบคอมพิวเตอร์ คือการเข้าไปของสัญญาณทางอิเล็กทรอนิกส์ ส่วนคำว่า **"การแรกเข้า"หมายถึง สถานะแรกเมื่อผ่านเข้าไปในระบบคอมพิวเตอร์สำเร็จ** ดังนั้นการแรกเข้าไปในระบบคอมพิวเตอร์จะเป็นความผิดสำเร็จจึงพิจารณาสถานะแรกเมื่อเข้าไปในระบบคอมพิวเตอร์ ซึ่งอาจเปรียบเทียบกับการเจาะระบบคอมพิวเตอร์ในบทที่ ๔ ว่าด้วยการลงมือกระทำความผิด[๑๐]

๓.๒ ทรัพย์สิน (Property)

ความผิดฐานบุกรุกตามประมวลกฎหมายอาญา เป็นการเข้าไปในอสังหาริมทรัพย์[๑๑]ซึ่งเป็นวัตถุแห่งการกระทำ เช่น เคหสถาน อาคารเก็บรักษาทรัพย์หรือสำนักงาน ขณะที่การเข้าไปในทางคอมพิวเตอร์นั้น เป็นการเข้าไปในระบบคอมพิวเตอร์ ซึ่งหมายถึงองค์ประกอบทางคอมพิวเตอร์ที่ทำงานประสานกัน โดยในแต่ละองค์ประกอบอาจแยกย่อยลงไปได้อีกหลายประการ ดังเช่น web pages หรือ e-mail account เป็นส่วนหนึ่งของซอฟท์แวร์ database เป็นส่วนหนึ่ง

---

[๙] Criminal law:computer Hackers must do more than dial phone numbers to be charged with computer crime in Kansas [State m. Allen,917 p.2D 848 (Kan. 1996)] INTERNET http://washburnlaw.edu/wlj/36-3/articles/loehtxt.htm (July 17,1997) :pp. 1-12

[๑๐] อ่านประกอบหน้า ๗๘

[๑๑] ประมวลกฎหมายแพ่งและพาณิชย์มาตรา ๑๓๙ อสังหาริมทรัพย์ หมายความว่า ที่ดินและทรัพย์อันติดอยู่กับที่ดินมีลักษณะเป็นการถาวรหรือประกอบเป็นอันเดียวกับที่ดินนั้น และหมายความรวมถึงทรัพยสิทธิอันเกี่ยวกับที่ดินหรือทรัพย์อันติดอยู่กับที่ดิน หรือประกอบเป็นอันเดียวกับที่ดินนั้นด้วย

ของ ข้อมูล เป็นต้น ซึ่งเป็นสังหาริมทรัพย์[๖๒] ในอดีตการ "เข้าไป" ในสังหาริมทรัพย์จะเข้าใจได้ยากกว่าการ "เข้าไป"ในอสังหาริมทรัพย์เพราะยกตัวอย่างได้ยาก แต่เมื่อปัจจุบันยอมรับว่ามีสัญญาณทางอิเล็กทรอนิกส์ที่ไม่สามารถเห็นได้ด้วยตาเปล่า การเข้าไปของสัญญาณอิเล็กทรอนิกส์ในเครื่องคอมพิวเตอร์ ซึ่งเป็นสังหาริมทรัพย์จึงเป็นที่เข้าใจได้ง่ายขึ้น ดังนั้นปัญหาในการศึกษาจึงไม่ใช่การหาคำตอบว่าระบบคอมพิวเตอร์เป็นอสังหาริมทรัพย์หรือสังหาริมทรัพย์และมีการเข้าไปได้หรือไม่ แต่ปัญหาจะอยู่ที่ว่าระบบคอมพิวเตอร์ตามแนวคิดในเรื่องการแรกเข้าสู่ระบบคอมพิวเตอร์นี้ต้องเป็นของผู้อื่นหรือไม่

ในประมวลกฎหมายอาญามาตรา ๓๖๒ บัญญัติว่า ผู้ใดเข้าไปในอสังหาริมทรัพย์ของ *"ผู้อื่น"* ขณะที่มาตรา ๓๖๔ บัญญัติว่า ผู้ใด...เข้าไป...ในเคหสถาน อาคารเก็บรักษาทรัพย์สินหรือสำนักงานใน *"ความครอบครองของผู้อื่น"*

หากเป็นกรณีตามมาตรา ๓๖๔ เป็นที่แน่ชัดว่าเจ้าของซึ่งไม่ได้ครอบครองอยู่โดยตรงก็อาจบุกรุกที่ๆ ผู้อื่นครอบครองอยู่ได้ เช่นเจ้าของให้ผู้อื่นเช่าอาคารเหล่านั้นไปครอบครอง[๖๓] ส่วนกรณีมาตรา ๓๖๒ ในตอนต้นที่ว่า "เข้าไปในอสังหาริมทรัพย์ของ*ผู้อื่น*เพื่อถือการครอบครองนั้น" มีความชัดเจนอยู่แล้วว่าเป็นอสังหาริมทรัพย์ของผู้อื่น เจ้าของจึงบุกรุกที่ดินของตนเองตามมาตรานี้ไม่ได้ แต่ในส่วนโรงเรือนนั้น ถ้าเป็นของผู้อื่น ไม่ใช่ของเจ้าของที่ดิน ก็ต้องถือว่าเป็นการเข้าไปในอสังหาริมทรัพย์ของผู้อื่น อาจเป็นบุกรุกได้ แต่เป็นปัญหาอยู่อีกคือข้อความต่อไปในมาตรานี้ที่ว่า "เข้าไปกระทำการใดๆ อันเป็นการรบกวนการครอบครองอสังหาริมทรัพย์ของเขาโดยปกติสุข" จะหมายความว่าต้องเป็นอสังหาริมทรัพย์ของ*ผู้อื่น*ดังความตอนต้น หรือหมายความว่ารบกวนการ*ครอบครองของผู้อื่น*แม้อสังหาริมทรัพย์จะเป็นของผู้กระทำก็ตาม ถ้าอ่านข้อความทั้งหมดในมาตรานี้ตามความเข้าใจในภาษาไทย ก็ควรจะเข้าใจว่าข้อความว่า "หรือเข้าไปกระทำการใดๆ" นั้น ได้ละไว้ไม่ยกข้อความในตอนแรกมากล่าวซ้ำอีก ถ้าอ่านเต็มความโดยไม่ละไว้ ก็ต้องอ่านว่า "เข้าไปกระทำการใดๆในอสังหาริมทรัพย์ของผู้อื่นอันเป็นการรบกวนการครอบครองอสังหาริมทรัพย์ของเขาโดยปกติสุข" ความผิดตามมาตรานี้เป็นความผิดต่อกรรมสิทธิ์ดังจะเห็นได้ชัดจากความตอนแรก ควรจะตีความให้กลมกลืนในทางเดียวกัน[๖๔]

---

[๖๒] ประมวลกฎหมายแพ่งและพาณิชย์มาตรา ๑๔๐ สังหาริมทรัพย์ หมายความว่า ทรัพย์สินอื่นนอกจากอสังหาริมทรัพย์ และหมายความรวมถึงสิทธิอันเกี่ยวกับทรัพย์สินนั้นด้วย

[๖๓] จิตติ ติงสภัทิย์, คำอธิบายประมวลกฎหมายอาญาภาค ๒ ตอนที่ ๒ และ ภาค ๓ , หน้า ๒๗๗๐.

[๖๔] เรื่องเดียวกัน, หน้า ๒๗๕๔.

เมื่อนำมาพิจารณากับบทบัญญัติตามแนวความคิดว่าด้วยการแรกเข้าระบบคอมพิวเตอร์ จะมีปัญหาว่าจะกำหนดบทบัญญัติในแบบที่ ๑ ว่า "ผู้ใดแรกเข้าไปในระบบคอมพิวเตอร์*ของผู้อื่น* โดยไม่ได้รับอนุญาต" หรือในแบบที่ ๒ ว่า "ผู้ใดแรกเข้าไปในระบบคอมพิวเตอร์ซึ่งอยู่ในความ*ครอบครองของผู้อื่น*โดยไม่ได้รับอนุญาต" เพราะจะมีผลต่อผู้กระทำที่เป็นเจ้าของระบบคอมพิวเตอร์ ดังเช่น หากกำหนดบทบัญญัติในแบบแรก ถ้านาย ก. เช่าระบบคอมพิวเตอร์ของนาย ข. หากนาย ข. เข้าไปในระบบคอมพิวเตอร์ของนาย ก. นาย ข. จะไม่มีความผิดเพราะระบบคอมพิวเตอร์นั้นไม่ใช่ของ"ผู้อื่น" แต่หากกำหนดบทบัญญัติในแบบที่สอง การกระทำของนาย ข. จะเป็นความผิดเพราะถือว่าระบบคอมพิวเตอร์นั้นอยู่ในความครอบครองของ นาย ก. ซึ่งจากผลที่ปรากฏ จะก่อให้เกิดผลที่ต่างกันซึ่งขึ้นกับว่าผู้ร่างกฎหมายต้องการผลเช่นใด แต่สำหรับผู้เขียนแล้วเห็นด้วยกับแบบที่สอง เพราะเมื่อจุดประสงค์ของการกำหนดให้การแรกเข้าไปในระบบคอมพิวเตอร์เป็นความผิด เพราะต้องการปกป้องระบบคอมพิวเตอร์จากความเสียหายและการถูกรุกรานจากผู้ไม่มีสิทธิในข้อมูล เมื่อขณะนั้นระบบคอมพิวเตอร์อยู่ในความครอบครองของใครการจัดการระบบคอมพิวเตอร์นั้น ก็สมควรที่จะเป็นสิทธิของผู้ครอบครองในการที่จะป้องกันและขับไล่บุคคลที่จะเข้ามาในระบบของเขาโดยไม่ได้รับอนุญาต

ดังที่กล่าวมาจึงสรุปได้ว่า การแรกเข้านั้นเป็นการเข้าไปในระบบคอมพิวเตอร์ซึ่งหมายถึงองค์ประกอบทางคอมพิวเตอร์ที่ทำงานประสานกันไม่จำกัดเพียงองค์ประกอบใดองค์ประกอบหนึ่ง และระบบคอมพิวเตอร์ดังกล่าวต้องเป็นของผู้อื่นหรืออยู่ในความครอบครองของผู้อื่น และจะไม่เป็นความผิดหากเป็นการเข้าไปในระบบคอมพิวเตอร์ของตนเองแม้จะเป็นการทำลายระบบรักษาความปลอดภัยก็ตาม

๓.๓ การได้รับอนุญาต (Permission)

สิ่งสำคัญประการหนึ่งตามแนวคิดในการกำหนดให้การแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดคือ การไม่ได้รับอนุญาตที่จะเข้าไปในระบบคอมพิวเตอร์ การไม่ได้รับอนุญาตในการเข้าระบบคอมพิวเตอร์นั้นอาจพิจารณาได้จากการไม่สามารถเข้าระบบคอมพิวเตอร์ได้โดยปกติ แต่จำต้องมีลักษณะพิเศษจึงจะสามารถเข้าระบบคอมพิวเตอร์ได้ เช่นต้องมีรหัสผ่านหรือเครื่องมือโดยเฉพาะจึงจะสามารถเข้าไปได้ ดังนั้นผู้ที่ได้รหัสผ่านมาแม้จะไม่ได้รับการอนุญาตโดยตรงก็ถือว่าได้รับอนุญาตให้เข้าระบบคอมพิวเตอร์ในฐานะผู้ได้รับอนุญาตโดย

ปริยายได้ เว้นแต่จะมีข้อกำหนดเงื่อนไขเพิ่มเติมว่ารหัสผ่านหรือเครื่องมือนั้นใช้ได้เฉพาะผู้ที่ได้ระบุไว้ซึ่งจะทำให้การครอบครองรหัสผ่านยังไม่ถือว่าได้รับอนุญาตให้เข้าไปในระบบคอมพิวเตอร์ แต่อย่างไรก็ตามแม้ว่าจะสามารถเข้าระบบคอมพิวเตอร์ได้โดยวิถีทางปกติเช่นสามารถเข้าไปในระบบคอมพิวเตอร์ได้โดยไม่ต้องการรหัสผ่านหรือเครื่องมือใดๆ ซึ่งหมายความว่าไม่มีการป้องกันระบบคอมพิวเตอร์ไว้จากผู้ไม่ได้รับอนุญาต แต่ถ้ามีข้อกำหนดไว้แสดงออกชัดว่าห้ามบุคคลภายนอกเข้าไปในระบบคอมพิวเตอร์เช่นนี้หากผู้ใดเข้าไปโดยรู้ว่าตนไม่ใช่ผู้ได้รับสิทธิตามข้อกำหนดแต่ยังฝ่าฝืนเข้าไปก็ถือว่าเป็นการเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเช่นกัน

ดังที่จะได้กล่าวต่อไปในหัวข้อที่ว่าด้วยเจตนา ความแตกต่างในกรณีเจตนาพิเศษระหว่างมาตรา ๓๖๒ กับแนวคิดในการกำหนดให้การแรกเข้าไปในระบบคอมพิวเตอร์เป็นความผิดอยู่ที่ว่าการเข้าไปในอสังหาริมทรัพย์ของผู้อื่นตามมาตรา ๓๖๒ ไม่มีองค์ประกอบในส่วนที่แสดงให้เห็นว่าต้องเป็นการกระทำโดยไม่ได้รับอนุญาต ทำให้ต้องบัญญัติเจตนาพิเศษเพิ่มเติมคือ "เพื่อถือการครอบครองอสังหาริมทรัพย์ทั้งหมดหรือบางส่วน" ซึ่งจะต่างกับบทบัญญัติตามแนวความคิดนี้ที่มีองค์ประกอบความผิดในส่วนวิธีการกระทำ คือ "โดยไม่ได้รับอนุญาต" ซึ่งแม้ "โดยไม่ได้รับอนุญาต" จะไม่ใช่ส่วนของเจตนาพิเศษ แต่เป็นองค์ประกอบความผิดซึ่งหากไม่มีการกระทำ "โดยไม่ได้รับอนุญาต" ก็จะไม่เป็นความผิด

คำว่า "โดยไม่ได้รับอนุญาต" นี้อาจเทียบได้กับกรณี "ไม่มีเหตุอันสมควร" ในมาตรา ๓๖๔ ซึ่งเป็นองค์ประกอบของความผิดเช่นกัน แต่ก็ไม่เหมือนกัน เนื่องจากการได้รับอนุญาตเป็นการมอบสิทธิให้ในการจัดการกับสิ่งหนึ่งสิ่งใดโดยชัดแจ้ง ขณะที่การ "ไม่มีเหตุสมควร" ต้องอาศัยการพิจารณาตามความคิดของคนทั่วไป ดังเช่นกรณีการเข้าไปโดยกิจธุระ เก็บเงินอันเป็นหนี้ค้างชำระไม่ถือว่าเป็นกรณี "ไม่มีเหตุสมควร" การอาศัยการพิจารณาของคนทั่วไปเช่นนี้ หากนำมาใช้กับระบบคอมพิวเตอร์ซึ่งเป็นกรณีทางอิเล็คทรอนิกส์ อาจก่อให้เกิดความสับสนได้ว่าอย่างไรจึงเป็นกรณี "ไม่มีเหตุสมควร" เพราะขาดหลักเกณฑ์แน่นอน ซึ่งเป็นเหตุผลหนึ่งที่ทำให้ผู้เขียนเลือกที่จะใช้คำว่า"ไม่ได้รับอนุญาต" แทนคำว่า "ไม่มีเหตุสมควร"

๓.๔ ความเสียหาย

ความเสียหายเป็นองค์ประกอบความผิดซึ่งพบในบทมาตราในประมวลกฎหมายอาญาเป็นส่วนมาก เพราะเป็นการแสดงถึงเหตุผลที่ต้องกำหนดให้การกระทำอย่างใดหย่างหนึ่งเป็นความผิด ในเบื้องต้นแนวคิดในการกำหนดให้การแรกเข้าไปในระบบคอมพิวเตอร์เป็นความผิดได้

รับการคัดค้าน เนื่องจากการเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นไม่ได้ก่อให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์หรือผู้ครอบครองระบบคอมพิวเตอร์นั้น นอกจากการทำลายสิ่งป้องกันหรือระบบรักษาความปลอดภัยซึ่งเห็นได้ชัดเท่านั้น แต่ผู้เขียนเห็นว่าข้อคัดค้านดังกล่าวได้มองข้ามความเสียหายประเภทอื่นซึ่งไม่จำกัดเพียงความเสียหายในทรัพย์สินเท่านั้น ซึ่งได้แก่ความเสียหายต่อสิทธิโดยชอบธรรมของผู้ครอบครองระบบคอมพิวเตอร์นั้นด้วย อันได้แก่สิทธิดังต่อไปนี้ คือ

๓.๔.๑ ความเสียหายต่อสิทธิความเป็นส่วนตัว (Right of Privacy)

ผลกระทบหรือความเสียหายต่อสิทธิความเป็นส่วนตัว (Right of Privacy)นี้ เป็นการตอบปัญหาที่โต้เถียงกันว่ากรณีที่ผู้เจาะระบบคอมพิวเตอร์เข้าไปในระบบคอมพิวเตอร์โดยไม่ได้ลงมือกระทำสิ่งใดๆ เพียงแต่ดูสิ่งต่างๆภายในระบบคอมพิวเตอร์ภายหลังจากเข้าไปในระบบคอมพิวเตอร์ได้แล้ว ก่อให้เกิดความเสียหายเช่นใด

ความคิดในเรื่องสิทธิส่วนตัว เป็นแนวความคิดแบบปัจเจกชนนิยาม (Individualism) ซึ่งบุคคลแต่ละคนมีความสำนึกว่าตนมีพลังความคิดที่สามารถจะกำหนดวิถีชีวิตของตนเองได้อย่างอิสระ ปัจเจกชนนิยมนี้ มีรากฐานจากความคิดของพวกสโตอิก (Stoic) ที่เชื่อว่ามนุษย์ในสภาวะธรรมชาติสมบูรณ์นั้น เป็นอุดมคติที่สูงส่งของชีวิต การที่มนุษย์จะบรรลุสภาวะดังกล่าวได้มนุษย์ต้องมีความเป็นตัวของตัวเอง และรู้จักดำรงชีวิตอย่างมีเหตุผล ความมีเหตุผลจะช่วยให้มนุษย์รู้จักแยกว่าสิ่งใดเป็นความดีหรือความชั่วได้ แก่นแท้ของความเป็นมนุษย์จึงอยู่ที่ความสามารถที่จะใช้เหตุผลซึ่งเป็นพรสวรรค์ที่ทำให้มนุษย์มีความแตกต่างจากสัตว์โลกอื่นๆ ดังนั้นปัจเจกชนจึงมีสิทธิตามธรรมชาติ(natural rights) ในฐานะที่เกิดมาเป็นมนุษย์ และสิทธิตามธรรมชาติของมนุษย์เป็นสิทธิที่ไม่อาจจำหน่ายจ่ายโอนหรือถูกยกเลิกเพิกถอนไม่ว่ากรณีใดๆทั้งสิ้น โดยนัยดังกล่าวนี้ สิทธิตามธรรมชาติของมนุษย์ในฐานะปัจเจกชน จึงเป็นหลักการสูงสุดทั้งในทางจริยธรรมและกฎหมาย

สิทธิส่วนตัวหมายถึง สิทธิประจำตัวของบุคคล อันประกอบด้วยเสรีภาพในร่างกาย การดำรงชีวิต มีความเป็นส่วนตัว ซึ่งได้รับความคุ้มครองจากกฎหมายมิให้ผู้อื่นมาล่วงเกิน

ความเป็นส่วนตัว คือ "สถานะที่บุคคลจะรอดพ้นจากการสังเกต การรู้เห็น การสืบความสับ การรบกวนต่างๆ และมีความสันโดษ ไม่ติดต่อสัมพันธ์กับสังคม" ขอบเขตที่บุคคลควรจะได้รับความเคารพและได้รับความคุ้มครองในสิทธิส่วนตัวคือ มีการดำรงชีวิตอย่างเป็นอิสระ มีการพัฒนาบุคลิกลักษณะตามที่ต้องการ มีสิทธิที่จะแสวงหาความสุขในชีวิตตามวิถีทางที่อาจเป็นไป

ได้และเป็นความพอใจของเขาตราบเท่าที่ความสนุกสนานนั้นไม่ล่วงเกินสิทธิของผู้อื่นหรือขัดต่อกฎหมายและความสงบเรียบร้อย สิทธิที่จะไม่ถูกรบกวนในเรื่องส่วนตัวนี้ จำเป็นต้องได้รับการคุ้มครองป้องกันโดยกฎหมายให้สมกับความความสำคัญของสิทธิ[๙๕]

ตัวอย่างการละเมิดสิทธิส่วนตัวทางคอมพิวเตอร์ ดังเช่น

- กรณีแองเจลา เวสต์วอเตอร์ สุภาพสตรีชาวอังกฤษถูกสะกดรอยโดยชายคนหนึ่งที่อยู่ไกลออกไปถึง ๕,๐๐๐ ไมล์ เวสต์วอเตอร์ ซึ่งแต่งงานและมีลูก ๒ คน ต้องตกอยู่ในสภาพหวาดผวาเมื่อพบว่าชื่อและรายละเอียดส่วนตัวของเธอไปปรากฏอยู่ในเวบไซต์ประเภทหาคู่และยังพบว่าเจ้าของเวบไซต์นั้นอยู่ห่างไกลถึงรัฐฟลอริด้า เจ้าของเวบไซต์ดังกล่าวได้ใช้เทคนิคพิเศษด้วยการนำเอารูปของเธอเฉพาะส่วนศีรษะ ไปตัดต่อกับภาพเปลือยของผู้หญิงคนอื่น พร้อมกับบอกรายละเอียดเกี่ยวกับตัวเธอทั้งหมด พร้อมทั้งที่อยู่ หมายเลขโทรศัพท์ ทั้งยังประกาศข้อความว่าเวสต์วอเตอร์เป็นคนรักของเขาที่หายตัวไปนานแล้ว และเขาต้องการทราบข่าวคราวและที่อยู่ของเธอ[๙๖] หรือ

- คดีฆาตกรรมหนึ่งในรัฐเท็กซัส ที่มีผู้แก้ไขข้อมูลเกี่ยวกับการรักษาผู้ป่วยจนเป็นเหตุให้ผู้ป่วยถึงแก่ความตาย

ดังนั้นจึงเห็นได้ว่าแม้การแรกเข้าไปในระบบคอมพิวเตอร์จะไม่ได้ก่อให้เกิดความเสียหายในทางกายภาพที่มองเห็นได้ชัดเจน แต่การเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาตเป็นการทำให้สถานะของบุคคลที่มีสิทธิที่จะอยู่อย่างสันโดษ รอดพ้นจาการสังเกตและการรบกวนจากบุคคลที่ไม่สิทธิ ถูกรบกวนและถือว่ากระทบต่อสิทธิส่วนตัวของผู้ครอบครองระบบคอมพิวเตอร์นั้น นอกจากนั้นยังเป็นการก่อให้เกิดความเสียหายในฐานะที่เพิ่มระดับของความหวาดระแวง ที่มีผลเป็นการลดคุณค่าของการใช้ชีวิตของผู้ใช้คอมพิวเตอร์อย่างปกติสุข เป็นความเสียหายที่กระทบต่อสมาชิกในสังคมที่รัฐจะต้องหามาตราเพื่อแก้ไขและป้องกันเพื่อมิให้สมาชิกในสังคมได้รับความเสียหาย

---

[๙๕] ชูชีพ ปิณฑะสิริ, " การละเมิดสิทธิส่วนตัว " (วิทยานิพนธ์ปริญญานิติศาสตร์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, ๒๕๒๕),หน้า ๓-๗

[๙๖] ปิยรมณ์ ทรัพย์สุวรรณ ,ภัยแฝงอินเทอร์เนตระวังถูกสะกดรอยข้ามทวีป."หนังสือพิมพ์กรุงเทพธุรกิจ (๑ กรกฎาคม ๒๕๔๒): ๓

๓.๔.๒ ผลกระทบหรือความเสียหายต่อสิทธิในทรัพย์สิน

สิทธิในทรัพย์สินเป็นสิทธิพื้นฐานของมนุษย์ในการหวงกันและติดตามเอาคืนซึ่งทรัพย์สินของตนจากผู้ไม่มีสิทธิ เช่นเดียวกับสิทธิในระบบคอมพิวเตอร์ซึ่งเป็นสิทธิในทรัพย์สิน ผู้มีสิทธิครอบครองหรือเจ้าของจึงมีสิทธิหวงกันและปลดเปลื้องการรบกวนจากผู้ไม่มีสิทธิในระบบคอมพิวเตอร์ดังนั้น ดังนั้นหากผู้ใดเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต แม้จะเป็นเพียงเข้าไปโดยยังไม่ได้กระทำการใดก็ถือว่าเป็นการรบกวนสิทธิในทรัพย์สินได้เช่นกัน ความเสียหายหรือผลกระทบต่อสิทธิในทรัพย์สินสามารถพิจารณาได้จากตัวอย่างดังต่อไปใน คือ

- เมื่อวันที่ ๑๙ พฤศจิกายน ๒๕๔๑ เจ้าหน้าที่ประจำศูนย์ข่าวสารสงครามกองทัพอากาศ (Air Force Information War fare Center (AFIWC)) ฐานทัพอากาศเคลลี่ รัฐเท็กซัส สหรัฐอเมริกา ตรวจพบว่ามีการลักลอบติดต่อกับคอมพิวเตอร์ฐานทัพอากาศบรู๊คส์ (Brook Air Force Base) รัฐเท็กซัส ผ่านเครือข่ายอินเตอร์เน็ตในประเทศไทยและเครื่องคอมพิวเตอร์ที่ใช้ในระหว่างโจรกรรมข้อมูลเป็นเครื่องคอมพิวเตอร์ที่ติดตั้งอยู่ในศูนย์คอมพิวเตอร์เอเชียนเกมส์ ครั้งที่ ๑๓ ที่จัดขึ้นในประเทศไทย ซึ่งเป็นศูนย์ที่ใช้เครื่องคอมพิวเตอร์ระบบประมวลผลข้อมูลขนาดใหญ่โดยเป็นระบบยูนิกซ์ (Unix System) ผู้เจาะระบบคอมพิวเตอร์ซึ่งใช้รหัสว่า hdyang เข้าถึงระบบแฟ้มข้อมูลของฐานทัพบรู๊คส์และเรียกข้อมูลในแฟ้มต่างๆได้สำเร็จ ทั้งๆที่การเข้าไปถึงแฟ้มข้อมูลลับของกองทัพสหรัฐเป็นเรื่องลับสุดยอดและต้องผ่านโปรแกรมระบบรักษาความปลอดภัย (Fire Wall) อีกชั้นหนึ่ง บุคคลที่จะเข้าไปได้ต้องเป็นบุคลากรของกองทัพอากาศสหรัฐที่ได้รับอนุญาตและมีรหัสผ่าน (Password) ผู้เจาะระบบคอมพิวเตอร์ดังกล่าวใช้รหัสไอดีลูป (ID Loop) ผ่านไอดียูสเซอร์ (ID User) ของมหาวิทยาลัยแห่งอียิปต์ ใช้พาสเวร์ดหรือรหัสผ่าน ของมหาวิทยาลัยแห่งอียิปต์และเจาะเข้าไปในระบบฐานข้อมูล โดยเข้าไปดูข้อมูลและลบข้อมูลบางไฟล์ออกไป ซึ่งเป็นผลให้กองทัพสหรัฐต้องใช้เวลานานนับเดือนที่จะปรับปรุงข้อมูล ให้กลับมีสภาพดังเดิม[๙๙] หรือ

- กรณีแฮกเกอร์เจาะเข้าใน web site ของหนังสือพิมพ์นิวยอร์กไทม์ ในเดือนกันยายน ๑๙๙๘ เนื่องจากเหตุผลเพียงเพราะรู้สึกเบื่อ จึงเข้าครอบงำ web site ดังกล่าวและแทนหน้าจอด้วยรูปลามกและรูปเปลือย

---

[๙๙] "คดีโจรไฮเทค" หนังสือพิมพ์มติชน (๔ กุมภาพันธ์ ๒๕๔๒): ๒

- ความเป็นไปได้ที่แสดงออกทางภาพยนตร์ ในปี ๑๙๘๓ เรื่อง Wargames ซึ่งนำแสดงถึงวัยรุ่นที่เริ่มต้นอาชีพแฮกเกอร์ด้วยการปรับเกรดของตนเองทางคอมพิวเตอร์ของโรงเรียนมัธยม และในระหว่างที่ล็อกออนเข้าไปที่คอมพิวเตอร์ของกระทรวงกลาโหมและติดตั้งโปรแกรมที่เรียกว่า Global Thermonuclear War ทำให้เขาสามารถควบคุมเหนือระบบนิวเคลียร์ของสหรัฐโดยสมบูรณ์ และเกือบทำให้ทั้งโลกถูกทำลายด้วยระเบิดนิวเคลียร์ ซึ่งเป็นแนวคิดที่ทำให้เห็นว่ามีความเป็นไปได้ที่แฮกเกอร์จะสามารถควบคุมระบบพื้นฐานของประชาชนได้ ดังเช่น ระบบทางการเงินและธนาคาร ระบบการขนส่งและการโดยสารทางอากาศ ระบบหน่วยงานของกองทัพ และแม้กระทั่งระบบการศึกษาของเยาวชนซึ่งเป็นอนาคตของประเทศ

ความเสียหายต่อสิทธิส่วนตัวและสิทธิในทรัพย์สินเป็นความเสียหายที่แฝงอยู่และเกิดขึ้นทุกครั้งเมื่อมีการแรกเข้าไปในระบบคอมพิวเตอร์ ดังนั้นการบัญญัติในเรื่องความเสียหายต่อการแรกเข้าไว้ในบทมาตราจึงไม่จำเป็น เพราะอย่างไรแล้วไม่ว่าจะมีการแรกเข้าไปในระบบคอมพิวเตอร์เมื่อใดก็จะก่อให้เกิดความเสียหายต่อสิทธิทั้งสองประการทุกครั้ง อีกทั้งเมื่อเปรียบเทียบกับความผิดฐานบุกรุก กฎหมายก็ไม่ได้กล่าวว่าต้องมีการทำให้ทรัพย์สินเสียหาย เพียงแต่ต้องปรากฏว่ามีการรบกวนการครอบครองหรือมีการเข้าไปโดยไม่มีเหตุอันควรก็เป็นความผิด แต่ใช่ว่าความผิดฐานบุกรุกไม่ต้องการความเสียหาย ความเสียหายในกรณีการบุกรุกคือการถูกละเมิดสิทธิในทรัพย์สิน เหตุการณ์ที่สนับสนุนความคิดของผู้เขียนว่าไม่ต้องกำหนดความเสียหายเป็นองค์ประกอบของความผิด สามารถดูได้จากกฎหมายของประเทศกรีซและประเทศไอร์แลนด์ที่จะได้กล่าวถึงในหัวข้อที่ ๕ ต่อไป

๓.๕ เจตนา (Intent)

ประมวลกฎหมายอาญามาตรา ๕๙ วรรคแรกได้บัญญัติไว้ว่า "บุคคลจะต้องรับผิดในทางอาญาก็ต่อเมื่อได้กระทำโดยเจตนา....." ซึ่งเห็นได้ว่าการกระทำความผิดอาญาโดยปกตินั้นจะต้องมีเจตนา ซึ่งการกระทำโดยเจตนาหมายถึง การกระทำโดยรู้สำนึกในการที่กระทำและในขณะเดียวกันผู้ประทำประสงค์ต่อผล หรือย่อมเล็งเห็นผลของการกระทำนั้น[๑๕]

---

[๑๕] ประมวลกฎหมายอาญามาตรา ๕๙ วรรคสอง

ในกรณีความผิดฐานบุกรุกตามประมวลกฎหมายอาญามาตรา ๓๖๒ และ ๓๖๔ ต้องการเจตนาธรรมดาในการ "เข้าไป" โดยไม่ต้องมีเจตนาทุจริตหรือมีเจตนาร้ายที่ประสงค์ในการก่อให้เกิดความเสียหาย แต่เป็นเพียงแค่เจตนาที่จะเข้าไปอยู่ในสถานที่ซึ่งการบุกรุกได้เกิดขึ้น สิ่งที่น่าสนใจในส่วนของเจตนาในมาตรา ๓๖๒ คือข้อความ "เพื่อถือการครอบครองอสังหาริมทรัพย์นั้นทั้งหมดหรือแต่บางส่วน หรือเข้าไปกระทำการใดๆ อันเป็นการรบกวนการครอบครองอสังหาริมทรัพย์" ซึ่งเป็นเจตนาพิเศษ[๙๙] ถ้าการเข้าไปไม่เป็นการรบกวนการครอบครองและไม่มีเจตนาครอบครองก็ไม่เป็นความผิด ปัญหาก็คือเมื่อนำมาปรับใช้กับการบุกรุกระบบคอมพิวเตอร์ สมควรที่จะมีองค์ประกอบในส่วนเจตนาพิเศษเช่นนี้บ้างหรือไม่

สำหรับปัญหานี้ ควรที่จะวิเคราะห์จุดประสงค์ของการกำหนดให้การแรกเข้าระบบคอมพิวเตอร์เป็นความผิด ซึ่งคือเพื่อต้องการป้องกันการกระทำใดๆ ที่จะเกิดขึ้นภายหลังจากการเข้าไปในระบบคอมพิวเตอร์ ซึ่งอาจก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์โดยรวม ประกอบกับข้อมูลทางอิเล็คทรอนิคเป็นกรณีละเอียดอ่อนที่ง่ายต่อการแก้ไขเปลี่ยนแปลง การกระทำเพียงแค่การ "เข้าไป" จึงมีเหตุสมควรที่จะบัญญัติเป็นความผิด โดยไม่จำต้องกำหนดเพิ่มในส่วนเจตนาพิเศษใดๆ สาเหตุที่มาตรา ๓๖๒ กำหนดเจตนาพิเศษไว้เนื่องจากหากไม่กำหนดเจตนาพิเศษไว้โดยกำหนดเพียงว่า " ผู้ใดเข้าไปในอสังหาริมทรัพย์ของผู้อื่นเป็นความผิด" จะทำให้ผู้ใดก็ตามที่เข้าไปในอสังหาริมทรัพย์ของผู้อื่นไม่ว่ากรณีใดๆเป็นความผิดไปหมด แต่อย่างไรก็ตามการเพียงแรกเข้าระบบคอมพิวเตอร์คงไม่ถึงขนาดเป็นความผิดเว้นแต่เป็นการกระทำโดยไม่ได้รับอนุญาต

ข้อยกเว้นกรณีที่บุคคลไม่จำต้องมีเจตนาก็ต้องรับผิดในทางอาญา

ความต้องการเจตนาของบุคคลในการพิจารณาถึงความรับผิด อาจเห็นได้ถึงข้อบกพร่องหรือช่องโหว่ที่อาจก่อให้บุคคลไม่ระมัดระวังและก่อให้เกิดความเสียหายให้แก่บุคคลอื่น เหตุนี้จึงมีข้อยกเว้นให้การกระทำบางอย่างที่บุคคลไม่จำต้องมีเจตนาก็ต้องรับผิดในทางอาญาเช่นกัน คือ

---

[๙๙] ในความผิดบางฐาน ลำพังเจตนาอย่างเดียว ไม่พอที่จะถือว่าผู้กระทำมีความผิดฐานนั้น แต่จะต้องได้ความว่าผู้นั้นกระทำโดยเหตุจูงใจอย่างใดอย่างหนึ่งตามที่กฎหมายกำหนดด้วย ซึ่งเราอาจเรียกกรณีดังกล่าวว่ามูลเหตุจูงใจหรือเจตนาพิเศษ

๑. *การกระทำโดยประมาท* ได้แก่การกระทำความผิดมิใช่โดยเจตนา แต่กระทำโดยปราศจากความระมัดระวัง ซึ่งบุคคลในภาวะเช่นนั้นจักต้องมีตามวิสัยและพฤติการณ์ และผู้กระทำอาจใช้ความระมัดระวังเช่นว่านั้นได้ แต่หาได้ใช้ให้เพียงพอไม่[๒๐]

๒. *กรณีที่กฎหมายบัญญัติไว้ชัดแจ้งว่าต้องรับผิดแม้ได้กระทำโดยไม่มีเจตนา* ซึ่งหมายถึงพระราชบัญญัติอื่นๆ ได้กำหนดความผิดและโทษไว้ เมื่อบัญญัติให้ต้องรับผิดไม่ว่าผู้กระทำจะมีเจตนาหรือไม่

๓. *ความผิดลหุโทษ* คือความผิดเล็กน้อย ตามประมวลกฎหมายอาญาหมายถึงความผิดที่มีโทษไม่เกินหนึ่งเดือนหรือปรับไม่เกินหนึ่งพันบาท ซึ่งในมาตรา ๑๐๔ บัญญัติว่า "การกระทำความผิดลหุโทษตามประมวลกฎหมายนี้ แม้กระทำโดยไม่มีเจตนาก็เป็นความผิด เว้นแต่ตามบทบัญญัติความผิดนั้นจะบัญญัติให้เห็นเป็นอย่างอื่น"

เจตนาบุกรุกในทางอิเล็กทรอนิกส์ เป็นปัญหาที่ถูกท้าทายอย่างมาก ดังเช่นหากพิจารณาในชีวิตจริงแล้ว เมื่อนาย ก. เดินหรือวิ่งเข้าไปในสถานที่ใดที่หนึ่งนาย ก.อาจจะไม่รู้ว่าอยู่ในสถานที่ที่เรียกว่าอะไร แต่นาย ก.จะต้องรู้ว่ากำลังยืนอยู่ที่ใด สนามหญ้า สะพานหรือคอนกรีตและเข้ามาได้อย่างไร นาย ก.ไม่สามารถเข้าไปอยู่ในสถานที่ที่ไม่มีเจตนาจะเข้าไปเว้นแต่ถูกบังคับ แต่ในทางอิเล็กทรอนิกส์ การเข้าสู่ระบบคอมพิวเตอร์ ณ สถานที่ใด อาจไม่จำเป็นว่าผู้นั้นต้องมีเจตนา เช่น การกดปุ่มโดยไม่ตั้งใจ หรือการเชื่อมต่อโดยอาศัย Hypertext โดยไม่เจตนา เหตุนี้จึงเป็นเหตุให้เกิดแง่คิดในการพิจารณาบทบัญญัติว่าด้วยการแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตว่า สมควรมีบทบัญญัติว่าด้วยการแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่เจตนาหรือไม่ และเมื่อพิจารณาในเรื่องเจตนาคงละเลยไม่ได้ที่จะกล่าวถึงการกระทำโดยไม่เจตนาหากมีขึ้น

จุดประสงค์ของการบัญญัติให้บุคคลต้องรับผิดแม้กระทำโดยไม่เจตนาเนื่องมาจากเพื่อแก้ไขข้อบกพร่องให้บุคคลใช้ความระมัดระวังมากขึ้น ดังนั้นผู้เขียนจึงเห็นด้วยกับการบัญญัติบทบัญญัติที่ว่าด้วยการกระทำโดยประมาทกับการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งเป็นความเห็นในแง่ทฤษฎี แต่หากพิจารณาถึงการนำมาใช้ในทางปฏิบัติอาจแยกพิจารณาได้เป็น ๒ กรณีคือ

---

[๒๐] ประมวลกฎหมายอาญามาตรา ๕๙ วรรคสาม

ก. <u>การบุกรุกโดยประมาทเข้าระบบคอมพิวเตอร์ที่มีการป้องกันหรือมีระบบรักษาความปลอดภัยโดยอนุญาตเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น</u> ซึ่งกรณีนี้หากพิจารณาความเป็นไปได้ที่จะเกิดกรณีการบุกรุกโดยประมาทเข้าไปในระบบโดยไม่ได้รับอนุญาตนั้นเป็นเรื่องยาก เพราะการเข้าสู่ระบบคอมพิวเตอร์ที่มีอุปสรรคปิดกั้นไว้ เป็นไปไม่ได้ที่ผู้บุกรุกจะไม่ทราบว่าตนกำลังทำลายสิ่งกีดขวางเพื่อเข้าระบบคอมพิวเตอร์นั้นๆ ซึ่งจะทำให้โอกาสที่จะเป็นการกระทำโดยขาดความระมัดระวังในการเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นไปได้ยากหรือแทบจะไม่มีโอกาสเลยในทางปฏิบัติ การเจาะระบบคอมพิวเตอร์ไม่ใช่เรื่องง่ายต้องอาศัยเวลาและมีขั้นตอนในการเตรียมพร้อม ดังนั้นจึงเป็นไปได้ยากที่จะอ้างว่าเจาะระบบคอมพิวเตอร์โดยที่ไม่ทราบว่าตนกำลังเจาะระบบคอมพิวเตอร์ ความยากลำบากของการเป็นผู้เจาะระบบคอมพิวเตอร์นั้นอาจพิจารณาได้จากคำแนะนำผู้ที่ต้องการเป็นผู้เจาะระบบคอมพิวเตอร์ ดังนี้คือ

๑. การเป็นแฮกเกอร์จะต้องทำการศึกษาอย่างต่อเนื่อง ไม่สามารถหยุดทำ ๓ เดือนแล้วกับมาทำใหม่ได้ เนื่องจากเวลาบนอินเทอร์เน็ตเดินเร็วมาก มีระบบยูนิกส์รุ่นใหม่ๆ มีบัก (bug)[๒๑] ใหม่ๆ และการแก้ปัญหาใหม่ๆ เกิดขึ้นตลอดเวลา

๒. แฮกเกอร์ต้องทำงานหนักมาก ใช้เวลาส่วนมากกับการอ่านหนังสือ เพื่อเรียนรู้ช่องโหว่ทั้งระบบยูนิกส์และระบบรักษาความปลอดภัยบนอินเทอร์เน็ต บางครั้งต้องเรียนรู้ความผิดพลาดเนื่องจากการใช้งานของแต่ละบุคคลด้วย

๓. พยายามรับข่าวสารและตัวอย่างไฟล์ที่ได้จากอินเทอร์เน็ตด้วยการท่องไปบนอินเทอร์เน็ต ใช้เครื่องมือในการค้นหา (Search engine) เพื่อค้นหาข่าวสารสำคัญๆ การติดต่อกับแฮกเกอร์คนอื่นเพื่อแลกเปลี่ยนข่าวสารและประสบการณ์ด้วยวิธีส่งจดหมายอิเล็กทรอนิกส์อ่าน Newsgroups[๒๒] และ mailing list[๒๓] เข้าไปใน Ftp site หรือใช้ IRC เป็นต้น อาจเริ่มจากการเข้าไปในเวปไซท์ (web sites) เช่น

<u>http://www.2600.com</u> ,

<u>http://www.geocities.com/CapeCanaveral/3498/</u>.

<u>http:///www.t-online.de/home/at1962/</u>

---

[๒๑] คือความผิดพลาดที่อยู่ในโปรแกรมคอมพิวเตอร์

[๒๒] คือกลุ่มสัมมนานับพันกลุ่มที่ครอบคลุมเรื่องสารพัดที่พึงมี นิวส์กรุ๊ปแต่ละกลุ่มจะคุยกันเป็นเรื่องๆไป เช่น นักร้อง กีฬา วิชาการหรือการเมือง

[๒๓] คือกลุ่มสัมมนาที่ใช้อีเมล์เพื่อสื่อสาร เมื่อส่งข้อความไปที่เมลิ่งลิสต์ สำเนาของข้อความจะถูกส่งไปที่ตู้รับจดหมายของแต่ละคนที่อยู่ในบัญชีรายชื่อ

๔. การศึกษาระบบของยูนิกส์อาจเริ่มจากการหาซื้อยูนิกส์ที่มีอยู่ในท้องตลาด เช่น Linux, FreeBSD, Solaris หรือ AT&T UNIX เป็นต้น

๕. การเรียนรู้ภาษา C, Perl และ Shell script นั้นบางครั้งจำเป็นมากและอาจจำเป็นต้องเรียนรู้พื้นฐานของข้อมูล (Database) ด้วย

๖. ใช้อินเทอร์เน็ต Account ที่ไม่ใช่ของตนเอง พยายามหาจากแฮกเกอร์ที่รู้จัก จำไว้ว่าไม่พยายามใช้ Account ของตนเองขณะทำการเจาะระบบ

๗. ควรอ่านข่าวสารเรื่อง "suid", "sniffer", "firewall", "rdist", "nis" และ"satan" ตลอดเวลา[๒๔]

ข. <u>การบุกรุกโดยประมาทเข้าระบบคอมพิวเตอร์ที่ไม่มีระบบรักษาความปลอดภัย</u> กรณีนี้เห็นได้ชัดเจนว่าแม้การเข้าไปในระบบคอมพิวเตอร์จะเป็นการกระทำโดยขาดความระมัดระวังแต่เป็นการเข้าไปในสถานที่ที่เปิดทิ้งไว้ ซึ่งถ้าหากไม่มีสิ่งที่แสดงการหวงกันโดยชัดแจ้งแล้ว จะคล้ายกับการเดินเข้าหรือออกสถานที่สาธารณะตามปกติ ซึ่งหากเป็นเช่นนี้แล้วก็ไม่สมควรที่กฎหมายจะบัญญัติให้การกระทำดังกล่าวเป็นความผิด เพราะเป็นกรณีเล็กน้อยและกระทำโดยไม่มีเจตนา อีกทั้งระบบคอมพิวเตอร์ส่วนใหญ่ก็ไม่ได้มีข้อบ่งชี้เพื่อแสดงว่าห้ามบุคคลผู้ไม่ได้รับอนุญาตเข้าไปในระบบคอมพิวเตอร์ ในกรณีที่ระบบคอมพิวเตอร์นั้นไม่มีกระบวนการรักษาความปลอดภัย เว้นแต่เมื่อเข้าไปในระบบคอมพิวเตอร์นั้นแล้วก่อให้เกิดความเสียหาย ซึ่งเป็นความรับผิดในกรณีภายหลังจากการเข้าระบบคอมพิวเตอร์แล้ว ต้องนำไปศึกษาเป็นกรณีต่างหาก ซึ่งนอกเหนือขอบเขตของการศึกษาตามแนวความคิดนี้

ดังนั้น แม้ในทางทฤษฎีการกำหนดให้การกระทำโดยประมาทในการแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดจะมีเหตุสมควร แต่เมื่อพิจารณาถึงความเป็นไปได้ในการใช้บทกฎหมายและความเป็นไปได้ในทางปฏิบัติแล้ว ทำให้เห็นถึงความไม่จำเป็นที่จะต้องบัญญัติถึงการกระทำโดยประมาทต่อการแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต เพราะการกระทำโดยประมาทจะนำไปใช้ในการพิจารณาผลของการกระทำว่า ก่อให้เกิดความเสียหายโดยประมาทหรือโดยเจตนามากกว่าที่จะนำไปใช้ในการพิจารณาในกรณีการแรกเข้าไปในระบบคอมพิวเตอร์ ซึ่งเห็นได้จากกฎหมายต่างประเทศในส่วนของประเทศสหรัฐอเมริกา

---

[๒๔] เศรษฐพล ลิ้นปราชญา, "Hacker แอบเข้าระบบได้อย่างไร," <u>วารสารอินเทอร์เน็ต-อินทราเน็ต</u> ปีที่ ๒ ฉบับที่ ๙ (ธันวาคม ๒๕๔๐) : ๒๕

โดยสรุป องค์ประกอบความผิดของการแรกเข้าไปในระบบคอมพิวเตอร์ ประกอบไปด้วย

๑. การ "เข้าไป" ซึ่งหมายความรวมถึง การเข้าไปโดยใช้สัญญาณทางอิเล็กทรอนิกส์ สำหรับการพิจารณาว่าเมื่อใดเป็นการ "แรกเข้า"ไปในระบบคอมพิวเตอร์จะพิจารณาจากสถานะแรกเมื่อเข้าสู่ระบบคอมพิวเตอร์ได้แล้ว

๒. ระบบคอมพิวเตอร์ หรือองค์ประกอบทางคอมพิวเตอร์ซึ่งทำงานประสานกัน ต้องเป็นระบบคอมพิวเตอร์ของผู้อื่นหรืออยู่ในความครอบครองผู้อื่น ไม่รวมถึงระบบคอมพิวเตอร์ของตนเอง

๓. "โดยไม่ได้รับอนุญาต" หมายถึงการเข้าไปในระบบคอมพิวเตอร์โดยไม่มีสิทธิโดยชอบหรือไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้มีสิทธิครอบครอง

๔. ต้องมีเจตนาในการ "เข้าไป" ในระบบคอมพิวเตอร์ และไม่สมควรลงโทษผู้เข้าสู่ระบบคอมพิวเตอร์โดยประมาท

๕. กฎหมายต่างประเทศ

ถึงแม้ว่าแนวคิดในการกำหนดให้การแรกเข้าระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดนั้น เป็นแนวความคิดที่ผู้เขียนเสนอขึ้นมา แต่อย่างไรก็ตามคงไม่อาจละเลยการศึกษากฎหมายว่าด้วยความรับผิดเกี่ยวกับคอมพิวเตอร์ในต่างประเทศ เพราะถ้าหากกล่าวถึงความก้าวหน้าทางเทคโนโลยีที่มีผลต่อรูปแบบการกระทำความผิดนี้ คงไม่ได้เริ่มเกิดขึ้นในประเทศไทยเป็นแน่ ดังนั้นเพื่อประโยชน์ในการศึกษาต่อไป ผู้เขียนจึงขอกล่าวถึงบทกฎหมายในต่างประเทศที่ผู้เขียนเห็นว่าสมควรที่จะทำการศึกษาไว้ เพื่อนำไปศึกษารูปแบบและพัฒนาแนวความคิดในการบัญญัติกฎหมายที่ประเทศไทยจะต้องมีต่อไปในอนาคต[๒๕] การนำเสนอบทบัญญัติของกฎหมายต่างประเทศในลำดับต่อไปนี้ จึงไม่สามารถเสนอในลักษณะการศึกษากฎหมายเปรียบเทียบระหว่างประเทศไทยและต่างประเทศเพราะประเทศไทยยังไม่มีกฎหมายที่ว่าด้วยอาชญากรรมคอมพิวเตอร์ แต่จะเป็นการมุ่งเสนอลักษณะหรือข้อสังเกตจากผู้เขียนหรือจากการศึกษา

---

[๒๕] ปัจจุบันมีกฎหมายที่เกี่ยวข้องกับธุรกรรมทางทางอิเล็กทรอนิกส์ที่อยู่ในขั้นตอนการร่าง ๖ ฉบับ คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายอาชญากรรมทางคอมพิวเตอร์ กฎหมายว่าด้วยการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยลายมืออิเล็กทรอนิกส์ กฎหมายว่าด้วยการโอนเงินทางอิเล็กทรอนิกส์ กฎหมายโทรคมนาคม

กฎหมายที่เกี่ยวข้องในต่างประเทศเท่าที่ผู้เขียนสามารถค้นคว้ามาได้และเห็นว่าน่าจะเป็นประโยชน์ในการร่างกฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์ต่อไป อย่างไรก็ตามผู้ร่างกฎหมายต้องตระหนักว่ากฎหมายเป็นสิ่งที่สอดคล้องกับลักษณะเฉพาะของประเทศนั้นๆ การศึกษากฎหมายของต่างประเทศมีประโยชน์ในแง่ที่จะทำให้เห็นว่ากฎหมายควรเอาใจใส่ดูแลในเรื่องใดบ้าง แต่ไม่ถึงกับมีความสำคัญในฐานะที่จะเป็นกฎหมายที่ถูกลอกเลียนมาใช้ทั้งหมด ดังนั้นสิ่งที่สำคัญคือทราบว่าแนวคิดมีอย่างไรแล้วนำแนวคิดนั้นมาเป็นจุดเริ่มในการที่จะนำมาปรับใช้ โดยมีสิ่งที่กำหนดขอบเขตคือการปกครอง วัฒนธรรมและศีลธรรมของประเทศนั้นๆ

๓.๑ ประเทศสหรัฐอเมริกา

COMPUTER FRAUD AND ABUSE ACT (CFAA)
TITLE 18 UNITED STATES CODE
section 1030

CFAA เป็นกฎหมายที่ว่าด้วยการต่อต้านการเจาะคอมพิวเตอร์ ซึ่งภายใต้บทบัญญัตินี้รัฐบาลสามารถลงโทษผู้ใช้คอมพิวเตอร์ที่เข้าระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตและก่อให้เกิดความเสียหาย

การร่างกฎหมายนี้ในปี ๑๙๘๔ สภาคองเกรสหวั่นวิตกว่ากฎหมายนี้จะถูกนำออกใช้อย่างฟุ่มเฟือยหรือเกินพอดี ดังนั้นกฎหมายฉบับนี้จึงกำหนดให้แต่ละข้อหาผู้กระทำจะต้อง "รู้" (knowingly)[๒๖] ว่าได้เข้าระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต หรือได้กระทำโดยได้รับอนุญาตแต่กระทำเกินขอบเขต และนอกจากนั้นยังกำหนดให้ครอบคลุมใน ๓ ขอบเขตแคบๆคือ ๑. การเข้า

---

[๒๖] ใน The Model penal code ได้กำหนดระดับของเจตนาออกเป็น ๔ ระดับคือ
purposely หรือ intention คือระดับที่ต้องการการกระทำของบุคคลพร้อมด้วยความรู้ตัวที่เกี่ยวข้องกับการกระทำนั้น หรือก่อให้เกิดผลเช่นนั้นหรืออาจกล่าวได้ว่าคือการที่บุคคลมีความประสงค์ที่จะบรรลุจุดมุ่งหมาย
Knowingly คือการที่ผู้กระทำรับรู้และเชื่อว่าการกระทำของเขาเกิดตามธรรมชาติหรือตามพฤติการณ์
Recklessly คือ การที่ผู้กระทำได้กระทำไปโดยเฉยเมยไม่นำพาต่อเหตุการณ์ที่เกิดขึ้น กล่าวคือได้กระทำโดยรู้สำนึกอยู่แล้วว่าเป็นการเสี่ยงที่จะเกิดภัย แต่ยังขืนทำลง
Negligently คือการกระทำที่สภาวะจิตใจไม่คิดไม่นึกถึงอันตรายที่จะเกิดจากการกระทำของตนโดยที่ผู้กระทำสามารถจะใช้ความระมัดระวังได้แต่ไม่ได้ใช้ เป็นเหตุให้เกิดผลขึ้น

สู่คอมพิวเตอร์เพื่อเอาข้อมูลการป้องกันประเทศหรือข้อมูลเกี่ยวกับความสัมพันธ์ระหว่างประเทศเพื่อที่จะก่อให้เกิดความเสียหายแก่ประเทศหรือเพื่อประโยชน์ของประเทศอื่น ๒. เข้าสู่คอมพิวเตอร์เพื่อที่จะเอาข้อมูลทางการเงินจากสถาบันการเงินหรือข้อมูลของผู้บริโภคจากรายงานขององค์กรผู้บริโภค ๓. แก้ไข ทำลาย หรือเปิดเผยข้อมูลถ้าการกระทำนั้นกระทบถึงการใช้คอมพิวเตอร์ของรัฐบาล

กฎหมาย CFAA ในปี ค.ศ. ๑๙๘๔ เป็นเพียงก้าวแรกในการควบคุมอาชญากรรมคอมพิวเตอร์และมีข้อบกพร่อง ๓ ประการคือ ๑. มีการกำหนดหลักเกณฑ์ในการที่จะ"เข้า"ตามกฎหมายสูงเกินไปกว่ากฎหมายอื่นๆที่ว่าด้วยการโจรกรรมซึ่งอาจทำให้บทกฎหมายนี้ไม่ได้ใช้เลย ๒. กฎหมายนี้ปกป้องในขอบเขตแคบๆทางการเงิน ๓. กฎหมายนี้ปกป้องแต่ปัจเจกชนแต่ไม่รวมถึงบริษัท ซึ่งข้อบกพร่องทั้งสามประการนี้เป็นสาเหตุของการแก้ไขกฎหมาย CFAAในระยะต่อมา

การแก้ไขในปี ค.ศ. ๑๙๘๖ มีการเพิ่มข้อกำหนดทางเจตนาในมาตรา (a)(2) และ(a)(3) จาก "รู้" (knowingly) เป็น intentionally นอกจากนั้นยังได้ขยายขอบเขตของกฎหมายออกไปอีก ๓ ข้อหาคือ อนุมาตรา (a)(4) ในข้อหาฉ้อโกงคอมพิวเตอร์ของรัฐบาล โดยมีเจตนาที่จะฉ้อโกง , เพิ่มอนุมาตรา (a)(5) ลงโทษการแก้ไข การทำลายข้อมูล หรือขัดขวางการใช้งาน และเพิ่มอนุมาตรา (a)(6) กำหนดความผิดกรณีค้าขายรหัสคอมพิวเตอร์ ซึ่งมีจุดประสงค์แก้ไขการซื้อขายรหัสผ่านทาง bulletin boards

ในอดีตกฎหมาย CFAA มีจุดประสงค์ที่จะใช้ในขอบเขตที่แคบ แต่ในภายหลังมีอัตราการกระทำผิดเกี่ยวกับคอมพิวเตอร์รุนแรงเพิ่มมากขึ้น ซึ่งทำให้มีการแก้ไขเพิ่มขึ้นอีกในปีต่อๆมา

ปี ค.ศ. ๑๙๘๘ แก้ไขเครื่องหมายวรรคตอนในอนุมาตรา (a)(2)[๒๗] เพื่อชี้แจงว่ากฎหมายครอบคลุมถึงสถาบันการเงินทุกแห่งไม่เฉพาะเพียงเกี่ยวข้องเฉพาะบัตรเครดิตเท่านั้น

---

[๒๗] a. whoever-

... (2) intentionally accesses a computer without authorization or exceeds authorized access,and thereby obtains information contained in a financial record of a financial institution,or of a card issuer as defined in section 1620(n) of title 15,or contained in a file of a consumer reporting agency on a consumer,as such terms are defined in the Fair Credit Reporting Act

ปี ค.ศ. ๑๙๘๙ มีการแก้ไขโดยแทนคำว่า"ธนาคาร"(bank) ด้วยคำว่า"สถาบัน" (institution) ในอนุมาตรา (e)(4)(a)[๒๘] และนำคำว่า "สถาบันที่บัญชีได้รับการรับรองจากบริษัทที่ให้การรับรองการออมและกู้ยืม" ออกไปซึ่งมีผลให้มาตรานี้ครอบคลุมถึงสถาบันการเงินอื่นๆ

ปี ค.ศ. ๑๙๙๐ แก้ไขโดยขยายขอบเขตของ อนุมาตรา (e)(4) ให้รวมถึงเงื่อนไข ๒ ประการในความหมายของ "สถาบันการเงิน Financial Institution"

ปี ค.ศ. ๑๙๙๔ แก้ไขโดยการบัญญัติ (a)(5)[๒๙] ขึ้นใหม่ โดยแบ่งออกเป็น อนุมาตรา a และ b โดยห้ามการทำลายระบบคอมพิวเตอร์หรือองค์ประกอบทางคอมพิวเตอร์ โดยปราศจากอำนาจและจะต้องก่อความเสียหายมากกว่า ๑,๐๐๐ เหรียญสหรัฐ ในช่วงเวลา ๑ ปี หรือ แก้ไขประวัติทางการแพทย์[๓๐]

สิ่งที่เรียนรู้ได้จากการแก้ไขกฎหมาย CAFF หลายครั้งที่ผ่านมา คือ

๑. กฎหมายที่บัญญัติขึ้นมาเพื่อรองรับสิ่งที่มีวิวัฒนาการอย่างรวดเร็วดังเช่น คอมพิวเตอร์ ยากที่จะหลีกเลี่ยงไม่ให้มีการแก้ไขเปลี่ยนแปลงเนื่องจากมีความเคลื่อนไหวเปลี่ยนแปลงไปตามการพัฒนาที่เพิ่มมากขึ้นในอนาคต

๒. การแก้ไขส่วนใหญ่เป็นการแก้ไขที่มีแนวโน้มขยายความหมายเพื่อให้สามารถรองรับการกระทำใหม่ๆที่เกิดขึ้น

---

[๒๘] e. As used in this section-...(4) the term "financial institution" means-

(a) an institution,with deposits insured by the Federal Deposit Insurance Corporation;...

[๒๙] a.whoever- ...(5) intentionally accesses a Federal interest computer without authorization,and by means of one or more instances of such conduct alters,damages,or destroys information in any such Federal interest computer ,or prevents authorized use of any such computer or information,and thereby-

(A) causes loss to one or more others of a value aggregating one thousand dollars or more during any one year period;or

(B) modifies or impairs,or potentially modifies or impairs,the medical examination,medical diagnosis,medical treatment,or medical care of one or more individuals; or...

[๓๐] เรียบเรียงจาก Robert Scalione ,"crime on the internet :can the law keep up with a new generation of cyberspace hacker?"

http //wings.buffalo.edu/law/complaw/complawpapers/scalion.html

๓. ผลลัพธ์ที่แสดงออกมาทางสังคม ความเสียหายหรือความรุนแรงเป็นสิ่งที่มีส่วนใช้ในการพิจารณาว่ากฎหมายนั้นๆ สมควรมีการแก้ไขหรือไม่

นอกจากการแก้ไขดังกล่าวแล้วนั้น ยังมีข้อสังเกตุในเรื่องซึ่งมีความสำคัญในแง่โครงสร้างของกฎหมายอาญาเช่นกันคือ ในเรื่องของเจตนา

สภาคองเกรส แก้ไข CFAA ในปี ค.ศ. ๑๙๘๖ เพิ่มข้อกำหนดว่าด้วยเจตนาจากปี ค.ศ. ๑๙๘๔ จากเดิม Knowingly เป็น intentionally ในหลายมาตราโดยมีจุดประสงค์เพื่อแยกความรับผิดระหว่างผู้ซึ่งเข้าระบบคอมพิวเตอร์โดยตั้งใจและไม่ได้ตั้งใจออกจากกัน แต่อย่างไรก็ตามการแก้ไขก็ก่อให้เกิดความไม่กระจ่างเช่นกัน คือ การใส่คำว่า intentional ในหน้าประโยคที่ว่าด้วยการเข้าระบบ (access) แต่ไม่ใส่ในประโยคที่ว่าด้วยความเสียหาย (damage) ซึ่งมีผลให้การตีความใช้เฉพาะในประโยคที่ว่าด้วยการเข้าระบบเท่านั้น ดังเช่นคดี *United States v. Morris* Robert Tappan Morris นักศึกษาปีหนึ่งของมหาวิทยาลัย Cornell ในหลักสูตร Ph.D.วิทยาศาสตร์คอมพิวเตอร์ ปล่อย worm[๓๑] เข้าไปในอินเทอร์เน็ตเพื่อพยายามที่จะสาธิตความอ่อนแอของระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ แม้เขาจะคิดว่า worm เป็นสิ่งดีแต่เขาคำนวณผิดพลาดในการจำลองตัวเอง ซึ่งเมื่อเขาเริ่มตระหนักถึงปัญหาดังกล่าวโดยพยายามที่จะหยุดการกระทำของ worm ก็ช้าเกินไปเสียแล้วและทำให้คอมพิวเตอร์ทั่วประเทศพังลง ศาลตัดสินว่า ในกฎหมายคำว่า intentionally ใช้กับประโยคที่ว่าด้วยการเข้าสู่ระบบคอมพิวเตอร์เท่านั้น ไม่ต้องการเจตนาร้ายต่อการทำลายระบบคอมพิวเตอร์ ดังนั้นภายใต้ CFAA ปี ๑๙๘๖ แม้ว่า morris ไม่มีเจตนาที่จะก่อให้เกิดความเสียหายหรือทำลายระบบคอมพิวเตอร์ แต่เขาก็ต้องเราผิดถ้าเขาจงใจ(intended)ในการเข้าระบบคอมพิวเตอร์

ในปี ค.ศ. ๑๙๙๔ สภาคองเกรสได้แยกความแตกต่างระดับของเจตนาในข้อหาที่มีโทษร้ายแรง(felony) และโทษเล็กน้อย (misdemeanors) โทษร้ายแรงต้องการ knowingly และ intentional ส่วนโทษเล็กน้อยต้องการเพียง reckless เท่านั้น แต่เนื่องจากยังคงมีข้อจำกัดอยู่ สภาคองเกรสจึงแก้ไขอีกครั้งในปี ค.ศ. ๑๙๙๖ โดยกำหนดเจตนาในระดับต่ำลงอีก

---

[๓๑] โปรแกรมคอมพิวเตอร์ที่สำเนาตัวเองเข้าไปในระบบคอมพิวเตอร์ที่ถูกเชื่อมต่อ และสามารถจะทำลายระบบหรือใช้ทรัพยากรได้อย่างสิ้นเปลือง

ในปี ค.ศ. ๑๙๙๖ CFAA ได้เปลี่ยนโครงสร้างอย่างมาก สภาคองเกรสได้แบ่งมาตรา 1030 (a)(5)[๓๒] ออกเป็น ๓ อนุมาตราประกอบด้วย ๒ ฐานความผิดรุนแรงและ ๑ ความผิดเล็กน้อยการแก้ไขดังกล่าวสะท้อนให้เห็นว่าสภาคองเกรสต้องการให้ CFAA ครอบคลุมการกระทำผิดกว้างขึ้นกว่าเดิม ในอนุมาตราแรก(A) ลงโทษผู้ที่ knowingly ส่งโปรแกรมที่เป็นอันตรายและมีเจตนาที่จะก่อให้เกิดความเสียหาย ซึ่งเป็นอนุมาตราเดียวที่ใช้กับผู้กระทำความผิดที่อยู่ภายในองค์กร ดังเช่นถ้านาย ก ไม่ทราบว่าอีเมล์มีไวรัสติดมา ดังนั้นนาย ก ก็ไม่มีเจตนาที่จะส่งไวรัสไปสู่คอมพิวเตอร์เครื่องอื่น มีเพียงเจตนาที่จะส่งอีเมล์เท่านั้น ทำให้การกระทำของนาย ก ไม่เข้าตามอนุมาตราแรก แต่ถ้านาย ก รู้ว่าการส่งอีเมลพร้อมไวรัสเป็นอันตราย และนาย ก รู้ว่ามีไวรัสติดอยู่ที่อีเมล์ ดังนั้นนาย ก จึงจะเข้าตามอนุมาตราแรกในส่วนที่ว่าด้วยการส่ง (transmission) แต่ถ้าจะเข้าตามอนุมาตรา (A) ทั้งหมดนาย ก ต้องมีความประสงค์ในการทำให้เกิดความเสียหาย (damage) ด้วย

ในอนุมาตรา (B)(C) แตกต่างจากอนุมาตราแรกใน ๒ ประการคือ ๑. ทั้งสองอนุมาตราต้องการเจตนาในระดับที่ต่ำกว่าและ ๒. นำไปใช้กับผู้ซึ่งมีความประสงค์จะเข้าระบบคอมพิวเตอร์ (intentionally access a computer system) และเป็นเหตุให้นำไปบังคับใช้กับบุคคลภายนอกเท่านั้น โดยในอนุมาตรา (B) นำไปใช้กับแฮกเกอร์ผู้ที่ก่อให้เกิดความเสียหายเนื่องจากความรู้สำนึกว่าเป็นการเสี่ยงภัย(recklessly) แต่ยังกระทำลง ขณะที่อนุมาตรา(C) ไม่จำต้องมีเจตนาในการก่อให้เกิดความเสียหาย

ทั้งสองอนุมาตรา(B)และ(C) บุคคลใดๆจะต้องมีความประสงค์ (intentionally)ที่จะส่งe-mail หรือเข้า website หรือเข้าสู่ระบบคอมพิวเตอร์ ดังเช่น สมมุติว่านาย ข. พึ่งจะเรียนรู้การใช้ e-

---

[๓๒] a.whoever-

(5) (A) *knowingly* causes the transmission of a program,information,code,or command,and as a result of such conduct,*intentionally* causes damage without authorization,to a protected computer;

(B) *intentionally* accesses a protected computer without authorization,and as a result of such conduct,*recklessly* caused damage;or

(C) *intentionally* accesses a protected computer without authorization,and as a result of such conduct,causes damage

mail และได้ส่งไปยังที่อยู่หนึ่ง สถานะทางจิตใจของนาย ข. เข้าข้อกำหนดในเรื่องเจตนาเข้าสู่ระบบคอมพิวเตอร์เพราะนาย ข. มีเจตนาที่จะเข้าไปยังที่อยู่นั้นผ่านทาง e-mail ซึ่งถ้ามีไวรัสติดมาและนาย ข. คิดว่าไวรัสนั้นไม่มีอันตรายนาย ข. จะเข้าหลักเกณฑ์ในอนุมาตรา (B) ถ้านาย ข. ไม่ทราบว่ามีไวรัสติดมานาย ข. จะเข้าหลักเกณฑ์ในอนุมาตรา (C) ซึ่งเป็นความผิดที่ไม่ต้องการเจตนา[๓๓]

ข้อวิจารณ์ต่อ The Computer Fraud and Abuse Act

๑. ในประวัติศาสตร์ของการบัญญัติกฎหมาย CFAA นโยบายในการที่ตัดผู้กระทำโดยบริสุทธิ์ออกมีบทบาทสำคัญในการกำหนดนโยบายเกี่ยวกับเจตนาในปี ค.ศ. ๑๙๘๖ นโยบายนี้ประกอบด้วยความคิดที่ว่าเราจะลงโทษผู้กระทำผิดเพราะสังคมเรียกร้องให้ตอบแทนต่อผู้กระทำผิด แต่ CFAA ในปี ค.ศ. ๑๙๙๖ ได้บัญญัติความผิดทั้งต่อแฮกเกอร์ที่มีเจตนาก่อให้เกิดความเสียหายหรือเป็นเพียงผู้ที่ก่อความเสียหายโดยอุบัติเหตุไว้เหมือนกัน นอกจากนั้นการลงโทษแฮกเกอร์ที่มีเจตนาที่จะกระทำผิดเช่นเดียวกันกับผู้ที่ไม่มีเจตนากระทำ แสดงให้เห็นว่าสภาคองเกรสมองข้ามจุดมุ่งหมายของหลักเกณฑ์การตอบแทนผู้กระทำผิด ที่ให้ความสำคัญต่อความสัมพันธ์ระหว่างความรุนแรงของการกระทำและการลงโทษ เพราะการกระทำโดยจงใจและโดยอุบัติเหตุมีเจตนาที่ต่างกัน ไม่สมควรที่จะได้รับการตอบแทนที่เหมือนกัน

๒. CFAA ไม่สนใจที่จะปกป้องผู้ใช้จากภายนอกระบบ(outsider)ที่บริสุทธิ์หรือไม่มีเจตนา ดังเห็นได้จากการที่ อนุมาตรา (B)และ(C) ซึ่งใช้บังคับกับผู้กระทำจากภายนอกระบบ กำหนดระดับของเจตนาไว้ในระดับต่ำทำให้แม้กระทำโดยไม่มีเจตนาในการก่อให้เกิดความเสียหายก็เป็นความผิดได้

๓. เนื่องจากรัฐบาลมีข้อจำกัดในเรื่องความสามารถในการสอดส่องทางอินเทอร์เน็ต มาตรการรักษาความปลอดภัยของเอกชนจึงน่าจะใช้ได้อย่างมีประสิทธิภาพในการป้องกันอาชญากรรมคอมพิวเตอร์ ซึ่งสภาคองเกรสก็ตระหนักว่าภาคเอกชนจะมีความปลอดภัยถ้าภาคเอกชนมีมาตรการป้องกันของตัวเองเช่นเดียวกัน แต่การที่จะกระทำให้ภาคเอกชนกล้าที่จะลงทุนหรือกำหนดนโยบายในการเพิ่มมาตรการรักษาความปลอดภัย อาจจะไม่ได้ผลถ้ารัฐบาลฟ้องผู้กระทำ

---

[๓๓] เรียบเรียงจาก Haeji Hong ."Hacking Through the Computer Fraud and Abuse Act," INTERNET (http://www.aw.ucla.edu/Students/StudentOrgs/BLT/html/i3-hh.html)

ผิดทางคอมพิวเตอร์ทุกคนโดยไม่สนใจว่าผู้กระทำมีเจตนาอย่างไร เพราะภาคเอกชนอาจจะสันนิษฐานเอาเองว่าการเพิ่มมาตรการรักษาความปลอดภัยดังกล่าวไม่มีความจำเป็น เนื่องจากถึงอย่างไรรัฐก็สามารถนำผู้กระทำความผิดมาลงโทษได้อยู่แล้ว แต่ก็อาจมีผู้โต้แย้งว่าสถานการณ์อาจจะไม่เป็นเช่นนี้ก็ได้ เพราะการที่มีกฎหมายของรัฐลงโทษต่อผู้กระทำผิดเช่นนี้ เป็นประโยชน์ต่อเอกชนในแง่ที่ทำให้เอกชนไม่จำต้องใช้มาตรการในการป้องกันทุกมาตรการ แต่อาจเลือกใช้เพียงบางมาตรการเท่านั้น

๓.๒ สาธารณรัฐประชาชนจีน

กฤษฎีกา อันดับที่ ๑๔๗ สภาแห่งรัฐ วันที่ ๑๘ กุมภาพันธ์ ๑๙๙๔
ข้อกำหนดของสาธารณรัฐประชาชนจีนว่าด้วยการการปกป้องความปลอดภัยของข้อมูลคอมพิวเตอร์
บทที่ ๔ - ความรับผิดทางกฎหมาย

มาตรา ๒๓ บุคคลทั่วไปหรือหน่วยงานใดจงใจใส่ไวรัสคอมพิวเตอร์หรือข้อมูลที่เป็นอันตรายต่อระบบคอมพิวเตอร์ จะได้รับการตักเตือนจากองค์กรรักษาความปลอดภัยของรัฐหรือลงโทษปรับสูงสุด ๕,๐๐๐ หยวนในกรณีเป็นบุคคลทั่วไปและ ๑๕,๐๐๐ หยวนในกรณีเป็นหน่วยงาน หรือในกรณีที่ขายผลิตภัณฑ์พิเศษที่เกี่ยวกับความปลอดภัยสำหรับระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต โดยรายได้จากการนั้นจะถูกริบและค่าปรับจะเพิ่มเป็น ๓ เท่าของรายได้ที่ผิดกฎหมายนั้น (ถ้าหากมี)[๓๔]

๓.๓ ประเทศฟินแลนด์

ประมวลกฎหมายอาญาลักษณะที่ ๓๘ มาตรา ๘
การบุกรุกข้อมูล

ผู้ใดใช้รหัสที่ใช้ในการบ่งบอกบุคคลซึ่งไม่ใช่ของตนเองหรือพังระบบที่ใช้ในการป้องกันโดยไม่มีเหตุอันจะอ้างได้ เจาะเข้าไปในระบบคอมพิวเตอร์ที่ซึ่งเป็นที่จัดการข้อมูล เก็บรักษา หรือถูกส่งโดยทางอิเล็คทรอนิกส์ หรือวิธีการทางเทคนิคอื่นๆหรือในส่วนของระบบที่ได้รับการป้องกันไว้โดยเฉพาะ จะถูกลงโทษสำหรับการบุกรุกข้อมูลนั้นโดยการปรับหรือจำคุกไม่เกิน ๑ ปี

---

[๓๔] Stein Schjlberg. "Penal legislation in 37 countries," INTERNET (http://www.mossbyrett.of.no/info/legal.html) , p. ๗.

สำหรับการบุกรุกข้อมูลนี้รวมถึงการลงโทษผู้ที่ไม่ได้เจาะระบบคอมพิวเตอร์หรือส่วนอื่นๆ แต่ใช้เครื่องมือพิเศษเพื่อที่จะเอาไปซึ่งสารสนเทศที่บรรจุอยู่ในระบบคอมพิวเตอร์นั้นๆโดยไม่มีเหตุอันจะอ้างได้

ความพยายามกระทำการดังกล่าวลงโทษได้

มาตรานี้จะนำไปใช้ในกรณีการกระทำนั้นไม่ถูกลงโทษในฐานะข้อหาร้ายแรงเท่านั้น[๓๕]

๓.๔ ประเทศกรีซ

ประมวลกฎหมายอาญามาตรา ๓๗๐ อนุมาตรา ๒

ผู้ใดเข้าสู่ข้อมูลที่ถูกบันทึกในคอมพิวเตอร์หรือในหน่วยความจำภายนอกของคอมพิวเตอร์ หรือถูกส่งผ่านระบบการสื่อสารข้อมูลจะถูกลงโทษไม่เกิน ๓ เดือนหรือถูกปรับไม่น้อยกว่าหนึ่งหมื่นแดรกมา(drachmas) ภายใต้เงื่อนไขที่การกระทำดังกล่าวกระทำโดยไม่มีสิทธิโดยเฉพาะการละเมิดต่อข้อห้ามหรือมาตรการรักษาความปลอดภัยของผู้ที่มีสิทธิตามกฎหมาย ถ้าการกระทำมีความเกี่ยวข้องกับความสัมพันธ์ระหว่างประเทศหรือความปลอดภัยของรัฐ เขาจะถูกลงโทษตามมาตรา ๑๔๘

ถ้าผู้กระทำผิดเป็นผู้อยู่ภายในการให้บริการของผู้มีสิทธิในข้อมูล การกระทำในวรรคก่อนหน้านี้จะถูกลงโทษเฉพาะเป็นการห้ามโดยชัดแจ้งโดยข้อกำหนดภายในหรือโดยการตัดสินใจที่เขียนเป็นลายลักษณ์อักษรหรือนายจ้างผู้มีอำนาจของเขา

มาตรานี้ลงโทษการเข้าสู่ข้อมูลซึ่งบันทึกหรือเก็บไว้ในระบบคอมพิวเตอร์หรือที่ถูกส่งผ่านการสื่อสารผ่านเครือข่ายโดยไม่ได้รับอนุญาต บทบัญญัตินี้ครอบคลุมการ "เพียง" เข้าสู่ระบบและไม่ต้องการสิ่งที่แสดงให้เห็นว่าผู้กระทำผิดก่อให้เกิดความเสียหายต่อสารสนเทศ

บทบัญญัตินี้ใช้กับข้อมูลทุกประเภทที่ถูกดำเนินการหรือเก็บไว้ในหรือนอกเครื่องมือที่ใช้เก็บข้อมูลนั้น และรวมถึงข้อมูลที่ถูกส่งสำหรับจุดประสงค์ในการดำเนินการในระยะไกล เข้าสู่คลังข้อมูล หรือการสื่อสารระหว่างระบบคอมพิวเตอร์

การเข้าสู่ (Access) หมายถึงความเป็นไปได้ที่จะอ่าน เอาไปหรือแก้ไขข้อมูล และการเข้าสู่นั้นต้องเป็นการกระทำที่เป็นปฏิปักษ์ต่อเจตนาของผู้มีสิทธิในข้อมูลซึ่งมีอำนาจสั่งการในการใช้ข้อมูลเป็นพิเศษ[๓๖]

---

[๓๕] Ibid., p. ๘.

[๓๖] Ibid., p. ๑๐.

๓.๕ ประเทศไอร์แลนด์

ประมวลกฎหมายอาญาว่าด้วยการทำลาย ค.ศ. ๑๙๙๑

มาตรา ๕

(๑) ผู้ใดโดยปราศจากเหตุอันจะอ้างได้โดยชอบด้วยกฎหมายใช้คอมพิวเตอร์

(a) ภายในรัฐด้วยเจตนาที่จะเข้าสู่ข้อมูลที่ถูกเก็บไว้ไม่ว่าจะอยู่ภายในหรือนอกรัฐ หรือ

(b) ภายนอกรัฐด้วยเจตนาที่จะเข้าสู่ข้อมูลที่ถูกเก็บไว้ภายในรัฐ ไม่ว่าจะได้เข้าสู่ข้อมูลหรือไม่ มีความผิดและอาจถูกลงโทษใช้ค่าปรับไม่เกิน ๕๐๐ หรือจำคุกไม่เกิน ๓ เดือน หรือทั้งจำทั้งปรับ

(๒) ในอนุ (๑) ใช้กับผู้ใดซึ่งมีเจตนาไม่ว่าเขามีเจตนาที่จะเข้าสู่ข้อมูลโดยเฉพาะหรือข้อมูลที่จัดแบ่งไว้หรือข้อมูลที่ถูกเก็บไว้โดยบุคคลใดโดยเฉพาะ

จุดประสงค์ของมาตรานี้คือทำให้การ "เจาะ" เป็นความผิดเพื่อป้องกันการจงใจเข้าสู่ข้อมูลโดยไม่ได้รับอนุญาตหรือพยายามที่จะเข้าสู่ข้อมูลนั้น ซึ่งมาตรานี้นำไปใช้ไม่เพียงแค่การเข้าสู่ระบบคอมพิวเตอร์จากช่องทางระยะไกลโดยบุคคลซึ่งไม่มีอำนาจเชื่อมต่อกับองค์กรนั้นแต่ยังนำไปใช้กับผู้กระทำภายใน เช่นลูกจ้างหรือเจ้าหน้าที่ ในกรณีที่การเข้าสู่ข้อมูลโดยไม่มีอำาจหรือแม้ว่ามีอำนาจกระทำได้แต่ใช้เกินขอบอำนาจ

มาตรา ๕ ใช้บังคับได้ทั้งเมื่อการเข้าสู่นั้นสำเร็จและการที่คอมพิวเตอร์ได้ถูกใช้งานโดยมีจุดประสงค์เพื่อจะเข้าสู่แต่การเข้าสู่นั้นยังไม่สำเร็จ และถือว่าเป็นความผิดแม้ว่าแฮกเกอร์เพียงแค่มองไปรอบๆระบบที่เขาได้เข้าไปเท่านั้น[๓๗]

๓.๖ ประเทศอิตาลี

ประมวลกฎหมายอาญามาตรา ๖๑๕ b: การเข้าสู่สารสนเทศหรือระบบการสื่อสารโดยไม่มีอำนาจ

บุคคลใดเข้าสู่สารสนเทศหรือระบบการสื่อสารซึ่งได้รับการป้องกันจากมาตรการรักษาความปลอดภัยโดยไม่มีอำนาจ อาจถูกตัดสินลงโทษจำคุกไม่เกิน ๓ ปี

---

[๓๗] Ibid., p. ๑๐.

แต่อย่างไรก็ตามจากประสบการณ์ทั่วไปแสดงให้เห็นว่าหลักเกณฑ์นี้ถูกนำไปใช้ในการกระทำประเภทอื่นๆด้วยเช่น ฉ้อโกง และดูเหมือนว่าจะไม่มีการลงโทษตามหลักเกณฑ์นี้ภายใต้กฎหมายอาญาของอิตาลี เว้นแต่การกระทำนั้นแสดงให้เห็นว่าเป็นความผิดทางอาญาก่อนดังเช่นกระทำความผิดฐานบุกรุกเข้าในอาคารเพื่อเข้าสู่ระบบคอมพิวเตอร์ [๓๘]

๓.๗ ประเทศนอร์เวย์

ประมวลกฎหมายอาญามาตรา ๑๔๕ อนุมาตรา ๒–๕

ผู้ใดใดเปิดจดหมายหรือเอกสารที่ปิดผนึกหรือในลักษณะเดียวกัน เข้าสู่เนื้อหาของเอกสารนั้นหรือผู้ซึ่งเจาะเข้าไปในตู้เก็บสิ่งของ ต้องรับโทษปรับหรือโทษจำคุกไม่เกิน ๖ เดือน

การลงโทษเช่นเดียวกันนี้ใช้บังคับต่อบุคคลผู้ซึ่งกระทำโดย "เจาะ" เครื่องมือป้องกันหรือกระทำในลักษณะเดียวกัน เข้าสู่ข้อมูลหรือโปรแกรมซึ่งเก็บไว้หรือถูกส่งโดยอิเล็กทรอนิกส์หรือโดยทางเทคนิคอื่นๆ

ถ้าความเสียหายเกิดจากการได้มาซึ่งข้อมูลหรือโดยใช้ความรู้เช่นนั้นหรือถ้าผู้กระทำลงมือกระทำเพราะมีจุดประสงค์จากบุคคลอื่น ต้องลงโทษโดยจำคุกไม่เกิน ๒ ปี

ผู้ร่วมลงมือต้องรับผิดเช่นเดียวกัน

การฟ้องคดีโดยรัฐจะเกิดขึ้นเมื่อเกี่ยวกับส่วนได้เสียของรัฐ[๓๙]

๓.๘ ประเทศสวิสเซอร์แลนด์

ประมวลกฎหมายอาญามาตรา ๑๔๓ ทวิ:เข้าสู่ระบบประมวลผลโดยไม่ได้รับอนุญาต

ผู้ใดโดยไม่ได้รับอนุญาตและมีเจตนา เข้าสู่ระบบประมวลผลซึ่งมีการป้องกันเป็นพิเศษจากการ "เข้า"โดยไม่ได้รับอนุญาต โดยใช้เครื่องมือทางอิเล็กทรอนิกส์ อาจจะได้รับโทษจำคุกหรือปรับ[๔๐]

---

[๓๘] Ibid., p. ๑๑.

[๓๙] Ibid., p. ๑๓.

[๔๐] Ibid., p. ๑๕.

วิเคราะห์กฎหมายต่างประเทศ

กฎหมายเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ทั้ง ๘ ประเทศมีแนวความคิดและองค์ประกอบของการกำหนดความรับผิดที่คล้ายคลึงกัน กล่าวคือ

ประการแรก มีแนวความคิดที่จะป้องกันการบุกรุกทางคอมพิวเตอร์เช่นเดียวกัน

ประการที่สอง องค์ประกอบของความผิด จะประกอบไปด้วย

๑. ต้องมีการกระทำคือการ "เข้าไป" แต่ความหมายในทางกฎหมายของการ"เข้าไป" นี้ขึ้นอยู่กับการให้คำนิยามในแต่ละประเทศว่าจะให้มีความหมายครอบคลุมถึงการกระทำใดได้บ้าง แต่โดยรวมแล้วต้องมีกิริยาในการ "เข้าไป" เพื่อกำหนดเป็นความผิด

๒. ระบุเป้าหมายของการกระทำคือ ระบบคอมพิวเตอร์ซึ่งสามารถแยกได้เป็น ข้อมูลเอกสารลับ หรือจดหมายอิเล็กทรอนิกส์ รวมถึงการระบุเป้าหมายโดยเจาะจง ดังเช่น การเข้าไปในระบบคอมพิวเตอร์ทางทหาร ทางการเงิน ทางการแพทย์

๓. มีการกำหนดคำว่า "ไม่มีเหตุอันจะอ้างได้โดยชอบ" หรือ "ไม่มีสิทธิ" หรือ "ปราศจากเหตุโดยชอบ" เพื่อแสดงให้เห็นว่าการ "เข้าไป" ที่จะเป็นความผิดได้ต้องเป็นการกระทำโดยไม่ชอบและไม่อาจจะอ้างความชอบธรรมในการเข้าไปได้

๔. ความเสียหายอาจไม่จำเป็นต้องปรากฏชัด ในบางประเทศไม่ต้องการความเสียหายจากการ "เข้าไป" เพียงแค่เข้าไปก็เป็นความผิด ดังเช่น ประเทศกรีซ ขณะที่บางประเทศต้องการระดับของความเสียหายในการพิจารณาความรับผิด เช่น ประเทศสหรัฐอเมริกา

กฎหมายของต่างประเทศดังที่ได้ยกตัวอย่างมานี้ สะท้อนในเห็นความสนใจต่อการกระทำความผิดทางคอมพิวเตอร์ในแต่ละประเทศ เมื่อหันกลับมามองประเทศไทยซึ่งพยายามผลักดันและส่งเสริมความก้าวหน้าทางเทคโนโลยีกลับไม่มีกฎหมายว่าด้วยความผิดทางคอมพิวเตอร์ในการสร้างความมั่นใจให้แก่ประชาชนโดยทั่วไปหรือหน่วยงานที่ใช้เครื่องคอมพิวเตอร์ในการทำธุรกรรม ที่จะได้รับการดูแลและเอาใจใส่หากได้รับความเสียหายจากผู้กระทำผิดทางคอมพิวเตอร์ แต่อย่างไรก็ตามการบัญญัติกฎหมายเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ในแต่ละประเทศมีปัจจัยในการรองรับการกระทำความผิดแตกต่างกัน เหตุผลที่ขณะนี้ประเทศไทยยังไม่มีกฎหมายดังกล่าวอาจจะเนื่องมาจากความไม่พร้อมของประชาชน กระบวนการยุติธรรม และรัฐบาลที่จะเข้าใจต่อปัญหาดังกล่าว แต่ในไม่ช้าด้วยปัจจัยของการติดต่อสารที่รวดเร็วระหว่างประเทศต่อประเทศในอนาคตประเทศไทยจำต้องมีกฎหมายว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์เช่นกัน