



บทที่ 4

กฎหมายต่างประเทศที่กำหนดความรับผิด สำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ในขณะที่เทคโนโลยีทางด้านคอมพิวเตอร์มีความเจริญก้าวหน้ามากขึ้น การกระทำความผิดโดยอาศัยคอมพิวเตอร์ก็มีปริมาณเพิ่มมากขึ้นด้วย จากการศึกษา รวบรวมข้อมูล พบว่า มีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เพิ่มมากขึ้นและมีการพัฒนารูปแบบทุกปี ทั้งนี้ เนื่องจากการกระทำความผิดในรูปแบบดังกล่าวมีลักษณะพิเศษว่าการกระทำความผิดในรูปแบบธรรมดา กล่าวคือ เป็นการกระทำที่ไร้พรมแดน ผู้กระทำความผิดสามารถกระทำความผิดโดยจะอยู่ที่ใดในโลกก็ได้ การกระทำความผิดเกิดขึ้นได้อย่างรวดเร็ว ไม่ต้องลงทุนมาก แต่ได้รับผลตอบแทนสูง และที่สำคัญการกระทำความผิดเกี่ยวกับคอมพิวเตอร์สามารถสร้างความเสียหายให้กับสังคมได้อย่างมากมาย ด้วยเหตุผลที่กล่าวมาข้างต้น จึงทำให้ทั่วโลกพยายามหาทางรับมือกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยการบัญญัติกฎหมายที่มีความเป็นสากลและสอดคล้องกันกับประเทศอื่น ๆ จึงทำให้องค์กรระหว่างประเทศมีความพยายามร่วมกันที่จะสร้างบทบัญญัติที่เป็นมาตรฐาน เพื่อให้แต่ละประเทศมีแนวทางในการบัญญัติกฎหมายที่สอดคล้องไปในทางเดียวกัน

ในบทนี้ผู้เขียน ได้กล่าวถึงกฎหมายต่างประเทศที่กำหนดความรับผิดเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ทั้งนี้เพื่อเป็นข้อมูลในการนำไปใช้เป็นแนวทางแก้ไขปัญหา อุปสรรคที่เกิดขึ้นจากการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังที่ได้กล่าวมาแล้วในบทที่ 3 ทั้งนี้ เนื่องจากนานาอารยประเทศมีความเจริญก้าวหน้าทางเทคโนโลยีมาก่อนประเทศไทย เพราะหลายประเทศเป็นผู้คิดค้นเทคโนโลยีขึ้นเอง จึงต้องประสบกับปัญหาอาชญากรรมทางคอมพิวเตอร์มาก่อนประเทศไทย ดังนั้นการนำกฎหมายของนานาอารยประเทศมาศึกษา ก็จะทำให้พบแนวทางที่ต่างประเทศคิดค้นขึ้นมาเพื่อจัดการกับปัญหาดังกล่าวได้อย่างมีประสิทธิภาพที่สุด แต่ด้วยความที่แต่ละประเทศมีความแตกต่างกันทั้งทางด้านสังคม เศรษฐกิจ และวัฒนธรรม จึงทำให้ต้องศึกษากฎหมายของหลาย ๆ ประเทศ เพื่อหาแนวทางแก้ไขปัญหาคดีและเหมาะสมที่สุด แล้วนำมาปรับให้เข้ากับสภาพสังคมของประเทศไทย

สำหรับกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของต่างประเทศที่นำมาศึกษานี้จะแบ่งเป็น 2 กลุ่ม กล่าวคือ กลุ่มแรก เป็นกฎหมายที่มักถูกนำไปใช้เป็นต้นแบบในการร่าง

กฎหมายของอีกหลายๆ ประเทศ ส่วนกลุ่มที่สอง เป็นกฎหมายของประเทศที่มีสภาพเศรษฐกิจ สังคม วัฒนธรรม และระบบกฎหมายที่มีความคล้ายคลึงกับประเทศไทย

ในบทนี้ผู้เขียนมุ่งศึกษากฎหมายต่างประเทศเฉพาะในประเด็นที่ประเทศไทยกำลัง ประสบปัญหา ทั้งนี้เพื่อเป็นข้อมูลในการพิจารณาแนวทางในการขจัดปัญหาและข้อขัดข้องที่ เกิดขึ้นประเทศไทย โดยสามารถสรุปสาระสำคัญเป็นประเด็นต่าง ๆ ได้ดังต่อไปนี้

4.1 แนวทางของกฎหมายต่างประเทศในการกำหนดบทนิยามศัพท์

องค์ประกอบประการแรกที่สำคัญของการบัญญัติกฎหมาย คือ บทนิยามศัพท์ เนื่องจาก เป็นสิ่งที่ให้ความหมายของถ้อยคำที่ปรากฏอยู่ในตัวบทกฎหมายว่าหมายถึงความถึงสิ่งใดบ้าง ซึ่ง บางถ้อยคำเป็นองค์ประกอบที่สำคัญของฐานความผิดต่าง ๆ ซึ่งหากบทนิยามศัพท์มีความไม่ ชัดเจน ก็จะทำให้เกิดปัญหาในการตีความว่า การกระทำที่เกิดขึ้น เป็นความผิดตามที่กฎหมายได้กำหนด ไว้หรือไม่ ซึ่งในบางกรณีอาจไม่สามารถลงโทษผู้กระทำความผิดได้ เพราะมีความไม่ชัดเจน ส่งผลให้กฎหมายดังกล่าวไม่สามารถบังคับใช้ได้อย่างมีประสิทธิภาพ

บทบัญญัติในส่วนบทนิยามศัพท์ของกฎหมายต่างประเทศนั้นมีการกำหนดความหมายไว้ ค่อนข้างชัดเจน จึงมักไม่ค่อยเกิดปัญหาในการตีความ ซึ่งสามารถสรุปรายละเอียดได้ดังต่อไปนี้

(ก) คำว่า ระบบคอมพิวเตอร์

1. **สภายุโรป**¹⁶ ได้ให้ความหมายไว้ว่า หมายถึง อุปกรณ์หรือกลุ่มของอุปกรณ์ที่เชื่อมโยงระหว่างกัน หรือเกี่ยวข้องกันใด ๆ ซึ่งอุปกรณ์อันหนึ่งหรือหลายอันในกลุ่มนั้น เป็นไปตามโปรแกรม โดยทำหน้าที่ประมวลข้อมูลโดยอัตโนมัติ

2. **ประเทศฟิลิปปินส์**¹⁷ ได้ให้ความหมายไว้ว่า หมายถึงความรวมถึง อุปกรณ์ หรือชุดของ อุปกรณ์ ซึ่งโดยผ่านทางระบบอิเล็กทรอนิกส์ เครื่องมือทางอิเล็กทรอนิกส์ หรือเครื่องจักรกล หรือไม่ก็โดยผ่านทางอื่นใด สามารถรับ บันทึก เผยแพร่ จัดเก็บ ดำเนินการ ค้นหาและกู้เก็บกลับ คืนมา หรือสร้างฐานข้อมูล รูปแบบ หรือสัญลักษณ์ หรือสิ่งอื่นใด ซึ่งถูกเขียนขึ้นโดยอาศัย หลักเกณฑ์ทางคณิตศาสตร์และตรรกศาสตร์ หรือโดยการแสดงองค์ประกอบอย่างใดอย่างหนึ่ง หรือหลายองค์ประกอบเข้าด้วยกัน

¹⁶ Convention on Cybercrime, (ETS No.185). Articles 1 a.

¹⁷ Electronic Commerce Act, 2000, (Republic Act No. 8792). Articles 5.

3. **ประเทศรัฐอินเดีย**¹⁸ ได้ให้ความหมายไว้ว่า หมายถึง อุปกรณ์หรือส่วนประกอบของ อุปกรณ์ ซึ่งรวมถึงสิ่งที่ป้อนเข้าไป หรือผลการแสดงข้อมูลที่สนับสนุนการทำงานของอุปกรณ์นั้น แต่ไม่รวมถึงเครื่องคิดเลขซึ่งไม่สามารถตั้งชุดคำสั่ง และไม่สามารถใช้เชื่อมต่อกับอุปกรณ์ภายนอกอื่นซึ่งบรรจุชุดคำสั่งคอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ ฐานข้อมูลที่ป้อนเข้าหรือแสดงออกมาซึ่ง แสดงให้เห็นถึงตรรกศาสตร์ ผลรวมทางคณิตศาสตร์ ที่เก็บรักษาฐานข้อมูล และเครื่องมือ ติดต่อสื่อสารทางโทรคมนาคม และฟังก์ชันอื่น ๆ

4. **มลรัฐฟลอริดา**¹⁹ ได้ให้ความหมายไว้ว่า หมายถึง ชุดของอุปกรณ์ทางคอมพิวเตอร์ หรือกลุ่มของอุปกรณ์ที่เชื่อมโยงระหว่างกัน หรือเกี่ยวข้องกันใด ๆ ซึ่งอุปกรณ์อันหนึ่งหรือหลายอัน ในกลุ่มนั้น เป็นไปตามโปรแกรม โดยทำหน้าที่ประมวลข้อมูลโดยอัตโนมัติ

(ข) คำว่า ข้อมูลคอมพิวเตอร์

1. **สภายุโรป**²⁰ ได้ให้ความหมายไว้ว่า หมายถึง สิ่งใดที่ใช้เป็นตัวแสดงออกของข้อเท็จจริง ข้อมูล หรือความคิด ในรูปแบบที่เหมาะสมจะใช้ในการประมวลผลลงในระบบคอมพิวเตอร์ รวมถึงโปรแกรมที่เหมาะสมจะทำให้ระบบคอมพิวเตอร์ทำหน้าที่ได้

2. **ประเทศอินเดีย**²¹ ได้ให้ความหมายไว้ว่า หมายถึง การแสดงออกของข้อมูลข่าวสาร ความรู้ ข้อเท็จจริง หลักการ หรือโครงสร้าง ซึ่งกำลังมีการจัดเตรียมหรือที่มีการจัดเตรียมมาแล้ว อย่างเป็นระบบระเบียบ และเคยได้มีกระบวนการ กำลังมีกระบวนการ หรือจะมีกระบวนการ ประมวลผลในระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ และอาจอยู่ในรูปแบบอื่น ๆ หรือถูก เก็บรักษาไว้ภายในหน่วยความจำของเครื่องคอมพิวเตอร์

(ค) คำว่า ผู้ให้บริการ

1. **สภายุโรป**²² ได้ให้ความหมายไว้ว่า หมายถึง (1) หน่วยของรัฐ หรือของเอกชน ซึ่งจัด ให้ผู้ใช้บริการนั้น สามารถติดต่อสื่อสารโดยวิธีการของระบบคอมพิวเตอร์ และ (2) หน่วยอื่นใดซึ่ง ประมวลหรือเก็บรักษาข้อมูลคอมพิวเตอร์ในนามของการบริการทางการติดต่อสื่อสารหรือ ผู้ใช้บริการนั้น

¹⁸ The Information Technology Act, 2000, (Act No.21 of 2000). Section 2.

¹⁹ Penal Code. Title 13.

²⁰ Convention on Cybercrime, (ETS No.185). Articles 1 b.

²¹ The Information Technology Act, 2000, (Act No.21 of 2000). Section 2.

²² Convention on Cybercrime, (ETS No.185). Articles 1 c.

2. ประเทศฟิลิปปินส์²³ ได้ให้ความหมายไว้ว่า ผู้ให้บริการแก่ผู้อื่นในกรณี

1) บริการในการเข้าสู่อินเทอร์เน็ต หรือการเข้าสู่ระบบการเชื่อมโยงเครือข่าย หรือเป็นผู้อำนวยความสะดวกในการให้บริการดังกล่าว รวมถึง บุคคลผู้เสนอการส่งผ่านข้อมูล ช่องทางการติดต่อสื่อสาร หรือให้บริการในการติดต่อทางอินเทอร์เน็ต ดิจิตอล หรือวิธีการอื่นใด ระหว่างจุดที่กำหนดโดยผู้ใช้บริการ หรือข้อมูลทางอิเล็กทรอนิกส์ หรือการเลือกของผู้ใช้บริการ

2) การดำเนินการทางเทคนิคในทางจำเป็นเพื่อที่เอกสารอิเล็กทรอนิกส์ของผู้สร้างสรรค์จะได้รับการเก็บรักษา และสร้างช่องทางในการที่จะสามารถส่งต่อการเข้าถึงข้อมูลดังกล่าว ต่อบุคคลที่สาม ไม่ว่าจะเป็นผู้ที่ถูกกำหนดไว้หรือไม่ก็ตาม

3) ผู้ให้บริการไม่มีอำนาจในการเปลี่ยนแปลง หรือแก้ไขเนื้อหาของข้อมูลอิเล็กทรอนิกส์ หรือเอกสารอิเล็กทรอนิกส์ที่ตนได้รับ หรือกระทำการใด ๆ โดยแอบอ้างชื่อของผู้สร้างสรรค์ข้อมูล ผู้รับข้อมูล หรือ บุคคลที่สาม โดยไม่ได้รับอนุญาตเป็นกรณีพิเศษ และในกรณีที่เป็นผู้เก็บรักษาเอกสารอิเล็กทรอนิกส์ จะต้องมีการะหน้าที่ในการแสดงข้อมูลของการให้บริการตามคำร้องขอเป็นกรณีพิเศษ หรือโดยความจำเป็นอย่างยิ่ง

(ง) คำว่า คอมพิวเตอร์

1. ประเทศสิงคโปร์²⁴ ได้ให้ความหมายไว้ว่า หมายถึง อุปกรณ์อิเล็กทรอนิกส์ คลื่นแม่เหล็กไฟฟ้า เครื่องฉายแสงออปติก เคมีภัณฑ์อิเล็กทรอนิกส์ หรือ ชุดอุปกรณ์ประมวลผลข้อมูล หรือ ชุดอุปกรณ์ที่เกี่ยวข้องกับการติดต่อสื่อสาร การแสดงผลรวมของข้อมูลทางคณิตศาสตร์ หรือ ตรรกศาสตร์ หรืออุปกรณ์เก็บรักษาฐานข้อมูล และรวมถึงเครื่องอำนวยความสะดวกในการเก็บรักษาฐานข้อมูล หรือเครื่องอำนวยความสะดวกสื่อสารอันเกี่ยวข้องโดยตรง หรือ เครื่องอุปกรณ์แสดงผลของการติดต่อสื่อสารอย่างใดอย่างหนึ่ง หรือหลายอย่างรวมกัน แต่ไม่รวมถึง

(ก) ระบบเครื่องพิมพ์ดีดอัตโนมัติ หรือเครื่องควบคุมระบบการพิมพ์อัตโนมัติ

(ข) เครื่องคิดเลขขนาดพกพา

(ค) อุปกรณ์อื่นใดอันมีลักษณะคล้ายคลึงกัน ซึ่งไม่สามารถป้อนคำสั่งควบคุม หรือไม่สามารถบรรจุข้อมูล หรือเก็บรักษาฐานข้อมูลได้ หรือ

(ง) อุปกรณ์อื่นใดซึ่งรัฐมนตรีได้กำหนดไว้ในประกาศกระทรวง

²³ Electronic Commerce Act, 2000, (Republic Act No. 8792). Section 5.

²⁴ Computer Misuse Act, 1993, (Bill No.17/93). Section 2.

2. **ประเทศมาเลเซีย**²⁵ ได้ให้ความหมายไว้ว่า หมายถึง อุปกรณ์อิเล็กทรอนิกส์ คลื่นแม่เหล็กไฟฟ้า เครื่องฉายแสงออปติก เคมีภัณฑ์อิเล็กทรอนิกส์ หรือ ชุดอุปกรณ์ประมวลผลข้อมูล หรือ ชุดอุปกรณ์ที่เกี่ยวข้องกับการติดต่อสื่อสาร การแสดงผลรวมของข้อมูลทางคณิตศาสตร์ หรือ ตรรกศาสตร์ หรือ อุปกรณ์เก็บรักษาฐานข้อมูล และรวมถึงเครื่องอำนวยความสะดวกในการเก็บรักษาฐานข้อมูล หรือ เครื่องอำนวยความสะดวกสื่อสารอันเกี่ยวของโดยตรง หรือ เครื่องอุปกรณ์แสดงผลของการติดต่อสื่อสารอย่างใดอย่างหนึ่ง หรือหลายอย่างรวมกัน แต่ไม่รวมถึงระบบเครื่องพิมพ์ดีดอัตโนมัติ หรือ เครื่องควบคุมระบบการพิมพ์อัตโนมัติ หรือ เครื่องคิดเลขขนาดพกพา หรือ อุปกรณ์อื่นใดอันมีลักษณะคล้ายคลึงกัน ซึ่งไม่สามารถป้องกันคำสั่งควบคุม หรือ ไม่สามารถบรรจุข้อมูล หรือ เก็บรักษาฐานข้อมูลได้

3. **ประเทศอินเดีย**²⁶ ได้ให้ความหมายไว้ว่า หมายถึง เครื่องฉายแสงออปติก หรือ อุปกรณ์ประมวลผลข้อมูลความเร็วสูงอื่น ๆ หรือระบบซึ่งแสดงผลทางตรรกศาสตร์ ผลรวมทางคณิตศาสตร์ และฟังก์ชันความจำโดยการรวบรวมกันขึ้นโดยใช้อิเล็กทรอนิกส์ คลื่นแม่เหล็กไฟฟ้า หรืออุปกรณ์อื่น ๆ และรวมถึงข้อมูลที่มีการป้อนเข้า หรือผลแสดงข้อมูลรวม กระบวนการประมวลผลข้อมูล คอมพิวเตอร์ซอฟต์แวร์ หรืออุปกรณ์ช่วยในการติดต่อสื่อสารซึ่งเชื่อมต่อ หรือ เกี่ยวกับคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

(จ) คำว่า รหัสเฉพาะการเข้าถึง

1. **ประเทศญี่ปุ่น**²⁷ ได้ให้ความหมายไว้ว่า หมายถึง รหัสที่ได้มีการมอบให้แก่บุคคล (ซึ่งจากนี้ต่อไปจะเรียกว่า “ผู้ใช้ซึ่งได้รับอนุญาต” ซึ่งได้รับอนุญาตโดยผู้ควบคุมการเข้าถึงระบบให้สามารถเข้าใช้งานโดยเฉพาะสำหรับเครื่องคอมพิวเตอร์เฉพาะ หรือเข้าถึงระบบการควบคุม (ซึ่งจากนี้ต่อไปในวรรคนี้ ผู้ใช้ซึ่งได้รับอนุญาต และผู้ควบคุมการเข้าถึงระบบ ย่อมหมายถึง “ผู้ใช้ซึ่งได้รับอนุญาต หรืออื่น ๆ”) ซึ่งสามารถจำแนกผู้ใช้ซึ่งได้รับอนุญาตคนหนึ่งออกจากผู้ใช้ซึ่งได้รับอนุญาตคนอื่น ๆ และ

(1) องค์ประกอบของรหัสซึ่งผู้ควบคุมการเข้าถึงระบบดูแลอยู่นั้น ต้องมิให้บุคคลที่สามล่วงรู้

²⁵ Computer Crimes Act, 1997, (Law of Malaysia, Act 563). Section 2.

²⁶ The Information Technology Act, 2000, (Act No.21 of 2000). Section 2.

²⁷ Unauthorized Computer Access Law, 2000, (Law No.128). Articles 2(2).

(2) รหัสดังกล่าวอาจเป็นสิ่งใด ๆ ที่กำหนดโดยผู้ควบคุมการเข้าถึงระบบนั้น อาจใช้รูปภาพของร่างกาย ไม่ว่าจะทั้งหมด หรือบางส่วน ของผู้ใช้ซึ่งได้รับอนุญาต หรือเสียงของผู้ใช้ซึ่งได้รับอนุญาต

(3) รหัสดังกล่าวอาจเป็นสิ่งใด ๆ ที่กำหนดโดยผู้ควบคุมการเข้าถึงระบบนั้น อาจใช้ลายมือชื่อของผู้ใช้ซึ่งได้รับอนุญาตก็ได้

2. **ประเทศอินเดีย**²⁸ ได้ให้ความหมายไว้ว่า หมายถึง หมายถึง หมายถึง หมายถึง รายชื่อของชุดคำสั่ง คำสั่ง สำหรับคอมพิวเตอร์ รูปแบบและโครงสร้าง และบทสรุปของชุดคำสั่งสำหรับทรัพยากรคอมพิวเตอร์ ไม่ว่าจะอยู่ในรูปใด ๆ

(จ) คำว่า การเข้าถึง

1. **สภายุโรป**²⁹ ได้ให้ความหมายไว้ว่า หมายถึง การเข้าสู่ระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วน ไม่ว่าจะเป็นการเข้าสู่ส่วนอุปกรณ์ ข้อมูลคอมพิวเตอร์ที่ถูกจัดเก็บไว้ในระบบการทำงาน ของระบบคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ สารบบการทำงาน ของระบบคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลอื่นใดที่เกี่ยวข้อง ทั้งนี้ให้รวมถึงการเข้าสู่ระบบคอมพิวเตอร์อื่นที่ได้เชื่อมต่อเข้ากับเครือข่ายโทรคมนาคมสาธารณะหรือระบบคอมพิวเตอร์ในเครือข่ายเดียวกัน โดยไม่คำนึงว่าการเชื่อมต่องดกล่าวจะได้กระทำผ่านทางสายสัญญาณสื่อสารหรือไม่

2. **ประเทศออสเตรเลีย**³⁰ ได้ให้ความหมายไว้ว่า หมายถึง

(1) การแสดงผลข้อมูลคอมพิวเตอร์โดยระบบคอมพิวเตอร์ หรือข้อมูลอื่นใดจากระบบคอมพิวเตอร์ หรือ

(2) การทำซ้ำหรือโอนย้ายข้อมูลคอมพิวเตอร์ไปยังหน่วยความจำอื่นในระบบคอมพิวเตอร์นั้นเองหรืออุปกรณ์สำหรับบันทึกข้อมูลคอมพิวเตอร์อื่น หรือ

(3) กระทำการใด ๆ เพื่อให้ชุดคำสั่งปฏิบัติการ

3. **ประเทศนิวซีแลนด์**³¹ ได้ให้ความหมายไว้ว่า หมายถึง การสั่งการให้ระบบคอมพิวเตอร์ปฏิบัติการเพื่อให้สามารถบันทึกข้อมูลคอมพิวเตอร์ หรือ ได้รับข้อมูลคอมพิวเตอร์ดังกล่าวตลอดการกระทำการอื่นใดเพื่อหาประโยชน์จากระบบคอมพิวเตอร์นั้น

²⁸ The Information Technology Act, 2000, (Act No.21 of 2000). Section 2.

²⁹ Convention on Cybercrime, (ETS No.185). Articles 46.

³⁰ Cybercrime Act, 2001 . Article 476.1.

4. **ประเทศอินเดีย**³² ได้ให้ความหมายไว้ว่า หมายถึง การสั่งการให้คอมพิวเตอร์ปฏิบัติ การหรือดำเนินการอื่นเพื่อให้สามารถสื่อสารข้อมูลกับหน่วยประมวลผลหรือหน่วยบันทึกผลของ ระบบคอมพิวเตอร์ได้

5. **รัฐนิวยอร์ก**³³ ได้ให้ความหมายไว้ว่า หมายถึง การติดตั้งชุดคำสั่ง หรือการสั่งให้ชุด คำสั่งปฏิบัติการ การดักหรือการสื่อสารข้อมูลคอมพิวเตอร์การจับหรือค้นคืนข้อมูล คอมพิวเตอร์

6. **รัฐนอร์ท แคโรไลนา**³⁴ ได้ให้ความหมายไว้ว่า หมายถึง การสั่งการให้ระบบคอมพิวเตอร์ ปฏิบัติการ หรือสื่อสารกับระบบคอมพิวเตอร์ และหมายความรวมถึงการจับหรือค้นคืนข้อมูลคอมพิวเตอร์ ในระบบคอมพิวเตอร์หรือค้นคืนข้อมูลคอมพิวเตอร์จากระบบคอมพิวเตอร์ด้วยตลอดจนการใช้ ประโยชน์ใดๆ จากระบบคอมพิวเตอร์

(ข) คำว่า การดักข้อมูล

1. **ประเทศสิงคโปร์**³⁵ ได้ให้ความหมายของ การดักข้อมูลในส่วนที่เกี่ยวกับฟังก์ชัน หรือ ระบบคอมพิวเตอร์ ว่าหมายความรวมถึง การดักฟัง หรือบันทึกฟังก์ชันของระบบคอมพิวเตอร์ หรือการได้รับข้อมูลที่มีความสำคัญหรือความหมายหรือการยืนยันสถานะของข้อมูลนั้น

4.2 แนวทางของกฎหมายต่างประเทศในการกำหนดฐานความผิดและบทกำหนดโทษ

สิ่งสำคัญที่จะทำให้กฎหมายสามารถบังคับใช้ได้อย่างมีประสิทธิภาพ คือ การกำหนดฐาน ความผิดที่มีความชัดเจน ครอบคลุม ทั้งนี้เพื่อไม่ให้เกิดปัญหาในการตีความว่า การกระทำที่ เกิดขึ้นเป็นความผิดที่ต้องถูกดำเนินคดีตามกฎหมายหรือไม่

บทบัญญัติในส่วนฐานความผิดของกฎหมายต่างประเทศนั้นมีการกำหนดไว้ค่อนข้าง ชัดเจน จึงมักไม่ค่อยเกิดปัญหาในการตีความ ซึ่งสามารถสรุปรายละเอียดได้ดังต่อไปนี้

(ก) ความผิดฐานเข้าถึงโดยมิชอบด้วยกฎหมาย (illegal access)

1. **สภายุโรป**³⁶ ได้กำหนดไว้ว่า ประเทศภาคีแต่ละประเทศพึงจัดให้มีมาตรการทางนิติ บัญญัติและมาตรการอื่นที่จำเป็นเพื่อกำหนดให้เป็นความผิดทางอาญาภายใต้กฎหมายภายใน

³¹ Crimes Amendment Act 2003 , (July 7 th).No 39 Part 1 s 15.

³² The Information Technology Act, 2000, (Act No.21 of 2000). Section 2.

³³ Penal Code. Title 5.

³⁴ Penal Code. Title 3.

³⁵ Computer Misuse Act, 1993, (Bill No.17/93). Section 2.

ของประเทศนั้น ซึ่งการเข้าถึงระบบคอมพิวเตอร์ทั้งหมด หรือบางส่วน ซึ่งได้กระทำโดยเจตนา และโดยไม่มีสิทธินั้น ประเทศภาคีอาจกำหนดให้เป็นความผิดนี้เฉพาะกรณีเป็นการกระทำโดย ล้วงล้ามาตรการรักษาความปลอดภัย โดยมีเจตนาที่จะได้มาซึ่งข้อมูลคอมพิวเตอร์ หรือโดย มีเจตนาทุจริตประการอื่น หรือเฉพาะกรณีเป็นการกระทำเกี่ยวกับระบบคอมพิวเตอร์ที่เชื่อมโยงกับ ระบบคอมพิวเตอร์อื่นนั้นก็ได้

2. ประเทศญี่ปุ่น³⁷ ได้กำหนดไว้ว่า ห้ามมิให้บุคคลใดเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ตามที่บัญญัติไว้ในวรรคก่อนนั้น หมายความว่า การกระทำได้ดังต่อไปนี้

(1) การกระทำด้วยประการใด ๆ เพื่อการใช้งานโดยเฉพาะซึ่งได้ถูกกำหนดการ ควบคุมการเข้าถึงโดยระบบปฏิบัติการในเครื่องคอมพิวเตอร์เฉพาะซึ่งมีระบบควบคุมการเข้าถึง โดยการป้อนข้อมูลเข้าไปในเครื่องคอมพิวเตอร์เฉพาะ โดยผ่านทางระบบโทรคมนาคม โดยการรั่ว รหัสเฉพาะที่เป็นของบุคคลอื่นเพื่อการใช้งานระบบการควบคุม (แต่ทั้งนี้ไม่รวมถึงการกระทำของผู้ ควบคุมการเข้าถึงระบบซึ่งเพิ่มช่องทางการเข้าถึงระบบการควบคุม หรือการกระทำเพื่อตรวจสอบ รหัสเฉพาะของผู้ใช้ซึ่งได้รับอนุญาต)

(2) การกระทำด้วยประการใด ๆ เพื่อได้เข้าใช้งานโดยเฉพาะซึ่งได้ถูกกำหนดการ ควบคุมการเข้าถึงโดยระบบปฏิบัติการในเครื่องคอมพิวเตอร์เฉพาะซึ่งมีระบบควบคุมการเข้าถึง โดยการป้อนข้อมูลเข้าไปในเครื่องคอมพิวเตอร์เฉพาะ โดยผ่านทางระบบโทรคมนาคม โดยข้อมูล ข่าวสารใด ๆ (แต่ไม่รวมถึงรหัสเฉพาะ) หรือการให้คำสั่งใด ๆ อันสามารถหลีกเลี่ยงระบบการ ควบคุมในการใช้งานโดยเฉพาะนั้น (แต่ทั้งนี้ไม่รวมถึงการกระทำของผู้ควบคุมการเข้าถึงระบบซึ่ง เพิ่มช่องทางการเข้าถึงระบบการควบคุม หรือการกระทำเพื่อตรวจสอบของผู้ควบคุมการเข้าถึง ระบบ)

(3) การกระทำด้วยประการใด ๆ เพื่อได้เข้าใช้งานโดยเฉพาะซึ่งได้ถูกกำหนดการ ควบคุมการเข้าถึงโดยระบบปฏิบัติการในเครื่องคอมพิวเตอร์เฉพาะซึ่งมีระบบควบคุมการเข้าถึงที่ ได้ถูกติดตั้งเอาไว้ในเครื่องคอมพิวเตอร์เฉพาะเครื่องอื่น ซึ่งได้เชื่อมต่อผ่านทางโทรคมนาคมกับ เครื่องคอมพิวเตอร์เฉพาะเครื่องดังกล่าว โดยผ่านทาง การป้อนข้อมูลเข้าไป โดยผ่านทาง

³⁶ Convention on Cybercrime, (ETS No.185). Articles 2.

³⁷ Unauthorized Computer Access Law, 2000, (Law No.128). Articles 3.

โทรคมนาคม หรือข้อมูลข่าวสารใด ๆ หรือการให้คำสั่งใด ๆ อันสามารถหลีกเลี่ยงระบบการควบคุมในการใช้งานโดยเฉพาะนั้น

บุคคลใดกระทำความผิดตามที่กำหนดไว้ในบทบัญญัตินี้ จะต้องระวางโทษจำคุกไม่เกิน 1 ปี และปรับไม่เกิน 500,000 เยน

3. **ประเทศฟิลิปปินส์**³⁸ ได้กำหนดไว้ว่า การกระทำความผิดต่อไปนี้ยอมถูกลงโทษปรับ หรือจำคุก

ก) เข้าถึงข้อมูลอิเล็กทรอนิกส์ของผู้อื่นในระบบคอมพิวเตอร์ หรือฐานเก็บรักษาข้อมูล หรือข้อมูลและระบบการติดต่อสื่อสารโดยไม่ได้รับอนุญาต เพื่อการฉ้อฉล เปลี่ยนแปลง ขโมย หรือทำลายข้อมูลอิเล็กทรอนิกส์ หรือชุดอุปกรณ์ข้อมูลและระบบการติดต่อสื่อสาร โดยที่เจ้าของระบบคอมพิวเตอร์ หรือเจ้าของข้อมูลและระบบการติดต่อสื่อสารไม่ได้รับทราบหรือให้ความยินยอม รวมถึงการเผยแพร่ไวรัสคอมพิวเตอร์หรือสิ่งอื่นใดในทำนองเดียวกัน เพื่อการฉ้อฉล ทำลาย เปลี่ยนแปลง ขโมย หรือทำลายข้อมูลอิเล็กทรอนิกส์ หรือเอกสารอิเล็กทรอนิกส์ ผู้กระทำความผิดต้องระวางโทษปรับไม่น้อยกว่า 100,000 เปโซ และในกรณีที่ก่อให้เกิดความเสียหายอย่างร้ายแรง ผู้กระทำความผิดต้องระวางโทษจำคุกตั้งแต่ 6 เดือน ถึง 3 ปี

4. **ประเทศสิงคโปร์**³⁹ ได้กำหนดไว้ว่า

(1) ภายใต้บังคับบทบัญญัติแห่งวรรค (2) ผู้ใดเจตนากระทำให้ระบบคอมพิวเตอร์แสดงฟังก์ชันใด โดยประสงค์ที่จะเข้าถึงระบบ อันนำไปสู่ชุดคำสั่งหรือฐานข้อมูลที่เก็บรักษาไว้ในคอมพิวเตอร์โดยที่ตนไม่ได้รับมอบอำนาจให้กระทำได้ ย่อมเป็นความผิดในฐานความผิดนี้ และต้องระวางโทษปรับไม่เกิน 5,000 ดอลลาร์ หรือจำคุกไม่เกิน 2 ปี หรือทั้งจำทั้งปรับ แต่ในกรณีเป็นการกระทำความผิดซ้ำ หรือเป็นการกระทำความผิดต่อเนื่อง ผู้นั้นต้องระวางโทษปรับไม่เกิน 10,000 ดอลลาร์ หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ

(2) หากความเสียหายใด ๆ ที่เกิดขึ้น เป็นผลเนื่องมาจากการกระทำความผิดในบทบัญญัติความผิดฐานนี้ ผู้กระทำความผิดต้องระวางโทษปรับไม่เกินกว่า 50,000 ดอลลาร์ หรือจำคุกไม่เกิน 7 ปี หรือทั้งจำทั้งปรับ

³⁸ Electronic Commerce Act, 2000, (Republic Act No. 8792). Section 33.

³⁹ Computer Misuse Act, 1993, (Bill No.17/93). Section 3.

(3) เพื่อประโยชน์แห่งบทบัญญัติมาตรานี้ ไม่ว่าจะกระทำที่เป็นความผิดดังกล่าวนั้นจะได้กระทำต่อสิ่งเหล่านี้โดยตรงหรือไม่

(ก) ชุดคำสั่งหลัก หรือฐานข้อมูลหลัก

(ข) ชุดคำสั่ง หรือฐานข้อมูลใด ๆ ทุกประเภท หรือ

(ค) ชุดคำสั่ง หรือ ฐานข้อมูลที่เก็บรักษาไว้ในระบบคอมพิวเตอร์หลัก

นอกจากนี้ ยังได้มีการกำหนดฐานความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยมีเจตนาที่จะกระทำ หรือเตรียมกระทำ ความผิด ดังนี้

(1) ผู้ใดทำให้ระบบคอมพิวเตอร์แสดงฟังก์ชันใด ๆ โดยประสงค์ที่จะเข้าถึงระบบอันนำไปสู่ชุดคำสั่งหรือฐานข้อมูลที่เก็บรักษาไว้ในคอมพิวเตอร์ โดยมีเจตนาที่จะกระทำความผิดอย่างใดตามที่บัญญัติไว้ในมาตรานี้ ย่อมเป็นความผิดในฐานความผิดนี้

(2) บทบัญญัติมาตรานี้ รวมความถึงการกระทำใด ๆ อันเป็นผลให้เกิดการยกยอกทรัพย์ การปลอมแปลง การฉ้อฉล หรือการทำร้ายร่างกายผู้อื่น ผู้กระทำต้องระวางโทษ จำคุกไม่น้อยกว่า 2 ปี

(3) ผู้ใดถูกตัดสินว่ามีความผิดตามบทบัญญัติมาตรานี้ ต้องระวางโทษปรับไม่เกิน 50,000 ดอลลาร์ หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ

(4) เพื่อประโยชน์แห่งบทบัญญัติมาตรานี้ ไม่สำคัญว่า

(ก) การเข้าถึง ตามความในวรรค (1) นั้นจะเป็นการเข้าถึงโดยชอบหรือไม่

(ข) การกระทำความผิดตามบทบัญญัติมาตรานี้ จะได้กระทำลงในเวลาที่ระบบป้องกันการเข้าถึงนั้นยังคงทำงานอยู่หรือไม่ หรือไม่ว่าในเวลาใด ๆ

5. ประเทศมาเลเซีย⁴⁰ ได้กำหนดไว้ว่า

(1) บุคคลจะถูกตัดสินว่ามีความผิดในกรณีนี้

(ก) บุคคลนั้นกระทำให้ระบบคอมพิวเตอร์แสดงฟังก์ชันใด โดยประสงค์ที่จะเข้าถึงระบบ อันนำไปสู่ชุดคำสั่งหรือฐานข้อมูลที่เก็บรักษาไว้ในคอมพิวเตอร์

⁴⁰ Computer Crimes Act, 1997, (Law of Malaysia, Act 563). Section 3.

(ข) การเข้าถึงระบบซึ่งบุคคลนั้นเจตนากระทำ เป็นกรณีที่ตนไม่ได้รับมอบอำนาจให้กระทำได้

(ค) บุคคลนั้นรู้ในเวลาที่ดินกระทำว่า การกระทำดังกล่าวเป็นเหตุให้ระบบคอมพิวเตอร์แสดงฟังก์ชันนั้น

(2) ไม่ว่าการกระทำที่เป็นความผิดตามบทบัญญัติมาตรานี้ ดังกล่าวนั้นจะได้กระทำต่อสิ่งเหล่านี้โดยตรงหรือไม่

(ก) ชุดคำสั่งหลัก หรือฐานข้อมูลหลัก

(ข) ชุดคำสั่ง หรือฐานข้อมูลใด ๆ ทุกประเภท หรือ

(ค) ชุดคำสั่ง หรือ ฐานข้อมูลที่เก็บรักษาไว้ในระบบคอมพิวเตอร์หลัก

(3) บุคคลซึ่งถูกตัดสินว่ามีความผิดตามบทบัญญัติมาตรานี้ ต้องระวางโทษปรับไม่เกิน 50,000 ริงกิตหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ

6. ประเทศสหรัฐอเมริกา⁴¹ ได้กำหนดไว้ว่า

1. ผู้ใด โดยรู้ถึงคอมพิวเตอร์โดยปราศจากอำนาจ หรือเกินขอบเขตอำนาจ และด้วยวิธีดังกล่าว ได้ไปซึ่งข้อมูลที่รัฐบาลสหรัฐอเมริกา มีคำสั่งของฝ่ายบริหารหรือกฎหมายลายลักษณ์อักษรกำหนดให้มีการคุ้มครองเพื่อป้องกันการเปิดเผยข้อมูลนั้นโดยปราศจากอำนาจ เนื่องจากเหตุผลเกี่ยวกับความปลอดภัยของประเทศหรือเกี่ยวกับต่างประเทศ หรือเป็นข้อมูลใด ๆ ที่มีความลับตามความหมายในย่อหน้า ของมาตรา 11 แห่ง Atomic Energy Act of 1954 ซึ่งมีเหตุผลอันเชื่อได้ว่ามานั้นอาจถูกนำไปใช้เพื่อสร้างความเสียหายให้กับสหรัฐอเมริกา หรือเพื่อให้เกิดประโยชน์ต่อรัฐต่างชาติใดๆ บุคคลนั้นโดยเจตนาติดต่อสื่อสาร ส่ง รับส่ง ข้อมูลดังกล่าวไปให้แก่เจ้าหน้าที่ของรัฐผู้มีสิทธิที่จะรับข้อมูลนั้นได้

2. ผู้ใดเข้าถึงคอมพิวเตอร์ปราศจากอำนาจ หรือเกินขอบอำนาจการเข้าถึงโดยชอบโดยเจตนา และเพื่อให้ได้รับไปซึ่ง

(a) ข้อมูลซึ่งเก็บไว้ในบันทึกทางการเงิน หรือของผู้ออกบัตร ตามที่กำหนดไว้ในมาตรา 1602 (n) ของหมวด 15 หรือข้อมูลซึ่งเก็บไว้ในแฟ้มของข้อมูลของผู้บริโภค ซึ่งมีข้อความอย่างเดียวกันกับที่กำหนดไว้ใน Fair Credit Reporting Act (15 U.S.C. 1681 et seq)

⁴¹18 U.S.C. 1030 Fraud and related activity in connection with computer .

(b) ข้อมูลจากหน่วยงาน หรือสำนักงานใดๆ ของสหรัฐอเมริกา หรือ

(c) ข้อมูลจากคอมพิวเตอร์ที่ได้รับการคุ้มครอง ถ้าการกระทำนั้น เกี่ยวข้องกับการติดต่อสื่อสารระหว่างมลรัฐ หรือการติดต่อสื่อสารกับต่างประเทศ

3. ผู้ใดโดยเจตนาเข้าถึงคอมพิวเตอร์ของหน่วยงาน หรือสำนักงานของ สหรัฐอเมริกาโดยปราศจากอำนาจ ซึ่งคอมพิวเตอร์นั้นมีไว้เพื่อการใช้งานสำหรับรัฐบาล สหรัฐอเมริกาโดยเฉพาะ หรือกรณีที่คอมพิวเตอร์มิได้ถูกใช้สำหรับสหรัฐอเมริกาโดยเฉพาะ แต่ถูก ใช้โดย หรือสำหรับรัฐบาลสหรัฐอเมริกา และการกระทำดังกล่าวส่งผลกระทบต่อการใช้งานของ รัฐบาลสหรัฐอเมริกา หรือการใช้งานสำหรับรัฐบาลสหรัฐอเมริกา

4. ผู้ใดโดยรู้ และเจตนาที่จะฉ้อโกง เข้าถึงคอมพิวเตอร์ที่ได้รับการคุ้มครอง โดยปราศจากอำนาจหรือเกินขอบเขตอำนาจการเข้าถึงโดยมิชอบ และวิธีการดังกล่าวทำให้เกิด การฉ้อโกงโดยเจตนา และได้รับไปซึ่งสิ่งมีค่าใดๆ เว้นแต่วัตถุประสงค์ของการฉ้อโกงและสิ่งของที่ได้มา รวมเฉพาะการใช้ดังกล่าวนั้นไม่เกิน 5000 เหรียญสหรัฐในช่วงเวลาหนึ่งปี

5. (a) ผู้ใด โดยรู้ทำให้เกิดการส่งโปรแกรม ข้อมูล รหัส คำสั่ง และการกระทำ ดังกล่าวเจตนาทำให้เกิดความเสียหายต่อคอมพิวเตอร์ที่ได้รับการคุ้มครองโดยปราศจากอำนาจ

(b) เจตนาเข้าถึงคอมพิวเตอร์ที่ได้รับการคุ้มครองโดยปราศจากอำนาจ และ จากการกระทำดังกล่าวทำให้เกิดความเสียหายโดยประมาทโดยรู้ตัว (reckless) หรือ

(c) เจตนาเข้าถึงคอมพิวเตอร์ที่ได้รับการคุ้มครองปราศจากอำนาจ และจาก การกระทำดังกล่าว ทำให้เกิดความเสียหาย

6. ผู้ใด โดยรู้ และโดยเจตนาที่จะฉ้อโกงการพาณิชย์ (ตามที่กำหนดไว้ใน มาตรา 1029) ในรหัสผ่านใดๆ หรือข้อมูลที่มีลักษณะคล้ายคลึงกัน โดยการใช้คอมพิวเตอร์ซึ่ง อาจถูกเข้าถึงโดยปราศจากอำนาจถ้า

(a) การพาณิชย์นั้นส่งผลกระทบต่อการค้าพาณิชย์ระหว่างรัฐ หรือระหว่าง ประเทศ หรือ

(b) คอมพิวเตอร์ดังกล่าวถูกใช้โดยรัฐบาลของสหรัฐอเมริกา หรือถูกใช้สำหรับ รัฐบาลสหรัฐอเมริกา

7. ผู้ใดโดยเจตนาที่จะกรรโชกเอาเงิน หรือสิ่งมีค่าอื่นใดจากผู้อื่น ส่งการ ติดต่อดังกล่าวใดๆ ในการพาณิชย์ระหว่างมลรัฐหรือระหว่างประเทศที่มีลักษณะเป็นการข่มขู่ว่าจะ ก่อให้เกิดความเสียหายต่อคอมพิวเตอร์ที่ได้รับการคุ้มครอง

7. ประเทศอังกฤษ⁴² ได้กำหนดไว้ว่า

(1) บุคคลจะมีความผิด เมื่อ

(a) บุคคลได้กระทำการให้คอมพิวเตอร์แสดงผล หรือแสดงการทำงานใดๆ ด้วยเจตนาที่จะผ่านสิ่งป้องกันที่มีไว้เพื่อป้องกันการเข้าถึงระบบ และได้ทำการผ่านสิ่งป้องกันเช่นว่านั้น เข้าถึงโปรแกรมคอมพิวเตอร์ใดๆ หรือสารสนเทศที่เก็บไว้ในคอมพิวเตอร์ใดๆ

(b) การผ่านสิ่งป้องกันเข้าไปยังระบบนั้น เป็นการกระทำโดยปราศจากอำนาจ และ

(c) บุคคลนั้นได้รู้ขณะที่กระทำอยู่แล้วว่า การกระทำอันเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานนั้นปราศจากอำนาจ

(2) เจตนาของบุคคลที่ได้กระทำความผิดภายใต้มาตรานี้ ไม่จำเป็นต้องเป็นการกระทำที่เป็น

(a) โปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล

(b) โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือ

(c) โปรแกรมหรือข้อมูลที่ถูเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ

(3) บุคคลที่มีความผิดภายใต้บทบัญญัตินี้ จะต้องถูกพิจารณาคดีแบบรวดเร็วและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐาน หรือทั้งจำทั้งปรับ นอกจากนี้ยังมีการกำหนดความผิดฐานเข้าถึงโดยปราศจากอำนาจโดยมีเจตนาที่จะกระทำหรือเพื่อความสะดวกในการกระทำความผิดอื่นๆ (unauthorized Access with Intent to Commit of Further Offences) ไว้ว่า

(1) บุคคลจะมีความผิดภายใต้บทบัญญัตินี้ ถ้าหากว่าเขาได้กระทำความผิดตามมาตรา 1 ข้างต้น (ความผิดฐานเข้าถึงโดยปราศจากอำนาจ) โดยมีเจตนา

(a) กระทำความผิดในสิ่งที่มาตรานี้ใช้บังคับ หรือ

(b) ให้ความสะดวกในการกระทำความผิด (ไม่ว่าจะเป็นการกระทำความผิดของตนเอง หรือของบุคคลอื่น) และความผิดที่เขาเจตนากระทำหรือให้ความสะดวกดังจะกล่าวต่อไปในมาตรานี้ ให้ถือว่าเป็นผู้กระทำความผิดเช่นเดียวกับผู้กระทำความผิดที่ตนช่วยเหลือ

(2) มาตรานี้ใช้กับความผิด

(a) ใช้กับความผิดที่ถูกกำหนดไว้ในกฎหมาย หรือ

(b) ใช้กับบุคคลที่มีอายุ 21 ปี หรือ กว่านั้น

⁴² Computer misuse act 1990. Article 3.

(3) เพื่อวัตถุประสงค์ของมาตรานี้ ไม่ว่าจะการกระทำความผิดของผู้กระทำที่อยู่ระยะไกล (Remote) จะได้กระทำลงในโอกาสที่ปราศจากอำนาจเข้าสู่ระบบหรือไม่ หรือโดยการอาศัยโอกาสอื่นใดก็ตาม

(4) บุคคลอาจมีความผิดตามมาตรานี้ แม้จะปรากฏข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำที่อยู่ระยะไกลจะไม่ได้กระทำลงก็ตาม

(5) บุคคลผู้กระทำความผิดตามมาตรานี้ จะต้อง

(a) ถูกพิจารณาแบบบรรทัดและจะต้องถูกลงโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินชั้นสูงตามที่กฎหมายกำหนด หรือทั้งจำทั้งปรับ และ

(b) หากเป็นความผิดร้ายแรงจะถูกลงโทษจำคุกไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ

8. ประเทศฟินแลนด์⁴³ ได้กำหนดไว้ว่า ผู้ใดใช้รหัสที่ใช้ในการบ่งบอกบุคคลซึ่งไม่ใช่ของตนเองหรือฟังก์ชันที่ใช้ในการป้องกันโดยไม่มีเหตุอันจะอ้างได้ จะเข้าไปในระบบคอมพิวเตอร์ซึ่งเป็นที่จัดเก็บข้อมูล เก็บรักษา หรือถูกส่งโดยทางอิเล็กทรอนิกส์ หรือวิธีการทางเทคนิคอื่นๆ หรือในส่วนของระบบที่ได้รับการป้องกันไว้โดยเฉพาะ จะถูกลงโทษสำหรับการบุกรุกข้อมูลนั้นโดยการปรับหรือจำคุกไม่เกิน 1 ปี

9. ประเทศไอร์แลนด์⁴⁴ ได้กำหนดไว้ว่า

(1) ผู้ใดโดยปราศจากเหตุอันจะอ้างได้โดยชอบด้วยกฎหมายใช้คอมพิวเตอร์

(a) ภายในรัฐด้วยเจตนาที่จะเข้าสู่ข้อมูลที่ถูกเก็บไว้ไม่ว่าจะอยู่ภายในหรือภายนอกรัฐหรือ

(b) ภายนอกรัฐด้วยเจตนาที่จะเข้าสู่ข้อมูลที่ถูกเก็บไว้ภายในรัฐ ไม่ว่าจะได้เข้าสู่ข้อมูลหรือไม่ มีความผิดและอาจถูกลงโทษใช้ค่าปรับไม่เกิน 500 หรือจำคุกไม่เกิน 3 เดือน หรือทั้งจำทั้งปรับ

(2) ในอนุ (1) ใช้กับผู้ใดซึ่งมีเจตนาไม่ว่าเขามีเจตนาที่จะเข้าสู่ข้อมูลโดยเฉพาะหรือข้อมูลที่จัดแบ่งไว้หรือข้อมูลที่ถูกเก็บไว้โดยบุคคลใดโดยเฉพาะ

⁴³ Penal Code . chapter 38 section 8

⁴⁴ Criminal Damage Act , 1991. Section 5.

10. **ประเทศอิตาลี**⁴⁵ ได้กำหนดไว้ว่า บุคคลใดเข้าสู่สารสนเทศหรือระบบการสื่อสารซึ่งได้รับการป้องกันจากมาตรการรักษาความปลอดภัยโดยไม่มีอำนาจ อาจถูกตัดสินลงโทษจำคุกไม่เกิน 3 ปี

11. **ประเทศนอร์เวย์**⁴⁶ ได้กำหนดไว้ว่า ผู้ใดเปิดจดหมายหรือเอกสารที่ปิดผนึกหรือในลักษณะเดียวกัน เข้าสู่เนื้อหาของเอกสารนั้นหรือผู้ซึ่งเจาะเข้าไปในตู้เก็บสิ่งของ ต้องรับโทษปรับหรือโทษจำคุกไม่เกิน 6 เดือน

การลงโทษเช่นเดียวกันนี้ใช้บังคับต่อบุคคลผู้ซึ่งกระทำโดย “เจาะ” เครื่องมือป้องกันหรือกระทำในลักษณะเดียวกัน เข้าสู่ข้อมูลหรือโปรแกรมซึ่งเก็บไว้หรือถูกส่งโดยอิเล็กทรอนิกส์หรือโดยทางเทคนิคอื่นๆ

ถ้าความเสียหายเกิดจากการได้มาซึ่งข้อมูลหรือโดยใช้ความรู้เช่นนั้นหรือถ้าผู้กระทำลงมือกระทำเพราะมีจุดประสงค์จากบุคคลอื่น ต้องลงโทษโดยจำคุกไม่เกิน 2 ปี

ผู้ร่วมลงมือต้องรับผิดเช่นเดียวกัน

การฟ้องคดีโดยรัฐจะเกิดขึ้นเมื่อเกี่ยวกับส่วนได้เสียของรัฐ

12. **ประเทศสวิสเซอร์แลนด์**⁴⁷ ได้กำหนดไว้ว่า ผู้ใดโดยไม่ได้รับอนุญาตและมีเจตนาเข้าสู่ระบบประมวลผลซึ่งมีการป้องกันเป็นพิเศษจากการ “ เข้า ” โดยไม่ได้รับอนุญาตโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ อาจจะได้รับโทษจำคุกหรือปรับ

(ข) ความผิดฐานดัักข้อมูลคอมพิวเตอร์ (illegal interception)

1. **สภายุโรป**⁴⁸ ได้กำหนดไว้ว่า ประเทศภาคีแต่ละประเทศพึงจัดให้มีมาตรการทางนิติบัญญัติ หรือมาตรการอื่นที่จำเป็น เพื่อกำหนดให้เป็นความผิดทางอาญาภายใต้กฎหมายภายในของประเทศนั้น ซึ่งการดักการส่งข้อมูลคอมพิวเตอร์ ซึ่งส่งไป หรือส่งจาก หรือส่งภายในระบบคอมพิวเตอร์ที่มีไซ้ข้อมูลสาธารณะ โดยวิธีการทางเทคนิครวมถึงการแผ่รังสีทางแม่เหล็กไฟฟ้าจากระบบคอมพิวเตอร์ที่มีข้อมูลคอมพิวเตอร์เช่นว่านั้น ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น ประเทศภาคีอาจกำหนดให้เป็นความผิดนี้เฉพาะกรณีเป็นการกระทำโดยมีเจตนาทุจริต

⁴⁵ Penal Code . Article 615 ter.

⁴⁶ Penal Code . Section 145.

⁴⁷ Penal Code . Article 143 bis.

⁴⁸ Convention on Cybercrime, (ETS No.185). Articles 3.

หรือ เฉพาะกรณีเป็นการกระทำเกี่ยวกับระบบคอมพิวเตอร์ที่เชื่อมโยงกับระบบคอมพิวเตอร์อื่นนั้นก็ได้

2. ประเทศสิงคโปร์⁴⁹ ได้กำหนดไว้ว่า

(1) ภายใต้บังคับบทบัญญัติแห่งวรรค (2) ผู้ใดเจตนา

(ก) เข้าถึงระบบคอมพิวเตอร์โดยไม่มีอำนาจ เพื่อประสงค์ที่จะได้รับการให้บริการคอมพิวเตอร์ใด ๆ ไม่ว่าจะโดยทางตรงหรือทางอ้อม

(ข) ดัก หรือเป็นเหตุให้เกิดการดักการทำงานของฟังก์ชันของคอมพิวเตอร์โดยไม่มีอำนาจ ไม่ว่าจะทางตรงหรือทางอ้อม โดยวิธีการทางแม่เหล็กไฟฟ้า เครื่องเสียง เครื่องจักรกล หรืออุปกรณ์อื่นใด

(ค) ใช้ หรือเป็นเหตุให้มีการใช้ระบบคอมพิวเตอร์ หรืออุปกรณ์อื่นใด ไม่ว่าจะโดยทางตรงหรือทางอ้อม เพื่อกระทำความผิดตามที่บัญญัติไว้ในวรรค (ก) หรือ (ข) ย่อมเป็นความผิดในฐานความผิดนี้ และต้องระวางโทษปรับไม่เกิน 10,000 ดอลลาร์ หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ ในกรณีที่เป็นการกระทำความผิดซ้ำ หรือการกระทำความผิดต่อเนื่อง ผู้นั้นต้องระวางโทษปรับไม่เกิน 20,000 ดอลลาร์ หรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ

(2) หากความเสียหายใด ๆ ที่เกิดขึ้น เป็นผลเนื่องมาจากการกระทำความผิดในบทบัญญัติความผิดฐานนี้ ผู้กระทำต้องระวางโทษปรับไม่เกิน 50,000 ดอลลาร์ หรือจำคุกไม่เกิน 7 ปี หรือทั้งจำทั้งปรับ

(3) เพื่อประโยชน์แห่งบทบัญญัติมาตรานี้ ไม่ว่าจะการกระทำที่เป็นความผิดดังกล่าวนี้ จะได้กระทำต่อสิ่งเหล่านี้โดยตรงหรือไม่

(ก) ชุดคำสั่งหลัก หรือฐานข้อมูลหลัก

(ข) ชุดคำสั่ง หรือฐานข้อมูลใด ๆ ทุกประเภท หรือ

(ค) ชุดคำสั่ง หรือ ฐานข้อมูลที่เก็บรักษาไว้ในระบบคอมพิวเตอร์หลัก

(ค) ความผิดฐานรบกวนข้อมูลคอมพิวเตอร์ (data interference)

1. สภายุโรป⁵⁰ ได้กำหนดไว้ว่า

⁴⁹ Computer Misuse Act, 1993, (Bill No.17/93). Chapter 50A Section 6.

1. ประเทศภาคีแต่ละประเทศพึงจัดให้มีมาตรการทางนิติบัญญัติ หรือมาตรการอื่นที่จำเป็น เพื่อกำหนดให้เป็นความผิดอาญา ภายใต้กฎหมายของประเทศนั้น ซึ่งการทำให้เสียหาย การลบ การทำให้เสื่อมเสีย การแก้ไขตัดแปลง หรือการทำลายข้อมูลคอมพิวเตอร์ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น

2. ประเทศภาคี อาจสงวนสิทธิที่จะกำหนดให้การกระทำตามวรรค 1 เป็นความผิดเฉพาะกรณีที่เกิดจากการกระทำได้ก่อความเสียหายอย่างร้ายแรงนั้นก็ได้

2. ประเทศอังกฤษ⁵¹ ได้กำหนดไว้ว่า

(1) บุคคลจะมีความผิด ถ้า

(a) ผู้นั้นได้กระทำการใด ๆ ซึ่งก่อให้เกิดการแก้ไขเปลี่ยนแปลงในเนื้อหาของสาระของคอมพิวเตอร์ใดๆ และ

(b) ผู้ที่กระทำการเช่นว่านั้น จะต้องมีความเจตนาหรือจะต้องรู้ถึงการกระทำของตนในขณะทำการนั้น

(2) เพื่อวัตถุประสงค์ของอนุมาตรา (1) (b) ข้างต้น เจตนาจะต้องเป็นเจตนาที่ต้องการแก้ไขเปลี่ยนแปลงเนื้อหาของสาระของคอมพิวเตอร์ใดๆ โดยการกระทำ เช่น

(a) ทำให้เกิดความเสียหายต่อการทำงานของคอมพิวเตอร์

(b) ทำการกีดกั้น หรือขัดขวางการเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลในคอมพิวเตอร์ หรือ

(c) ทำให้เกิดความเสียหายต่อการทำงานของโปรแกรมคอมพิวเตอร์ หรือทำลายความเชื่อถือของข้อมูล

(3) เจตนาของการกระทำดังกล่าว ไม่จำเป็นต้องเป็นเจตนาที่กระทำโดยตรงต่อ

(a) คอมพิวเตอร์พิเศษเฉพาะเจาะจงใดๆ

(b) โปรแกรมหรือข้อมูลพิเศษเฉพาะเจาะจงใดๆ หรือโปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่งโดยเฉพาะ หรือ

(c) การแก้ไขเปลี่ยนแปลงพิเศษเฉพาะเจาะจงใดๆ หรือการแก้ไขเปลี่ยนแปลงชนิดใดชนิดหนึ่งโดยเฉพาะ

(4) เพื่อวัตถุประสงค์ของอนุมาตรา (1) (b) ข้างต้น ผู้กระทำต้องรู้ว่าการแก้ไขเปลี่ยนแปลงดังกล่าว เขาเจตนาที่กระทำโดยปราศจากอำนาจ

⁵⁰ Convention on Cybercrime, (ETS No.185). Articles 4.

⁵¹ Computer misuse act 1990. Article 3.

(5) มาตรานี้ไม่ถือวัตถุประสงค์เป็นสิ่งสำคัญ โดยไม่คำนึงว่าการแก้ไขเปลี่ยนแปลงโดยปราศจากอำนาจ หรือผลที่เจตนาที่จะให้เกิดขึ้นตามอนุมาตรา (2) ข้างต้น จะเป็นการเจตนาให้เกิดขึ้นเป็นการถาวรหรือเกิดขึ้นเพียงชั่วคราว

(6) การแก้ไขเปลี่ยนแปลงในเนื้อหาสาระของคอมพิวเตอร์ตามกฎหมายฉบับนี้ จะไม่ถือว่าเป็นการก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ใดๆ ตามกฎหมายอาญาเกี่ยวกับก่อให้เกิดความเสียหาย (The Criminal Damage Act 1971) เว้นแต่การกระทำนั้นมีผลทางกายภาพเท่านั้น

(7) บุคคลผู้กระทำความผิดตามมาตรานี้ จะต้อง

(a) ถูกพิจารณาแบบรวดรัดและจะต้องถูกลงโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินขั้นสูงตามที่กฎหมายกำหนด หรือทั้งจำทั้งปรับ และ

(b) หากเป็นความผิดร้ายแรงจะถูกลงโทษจำคุกไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ

3. **ประเทศอินเดีย**⁵² ได้กำหนดไว้ว่า ผู้ใดรู้ หรือจงใจปิดบังซ่อนเร้น ทำลาย หรือเปลี่ยนแปลง หรือจงใจ หรือรู้ถึงสาเหตุอื่นใดอันทำให้เกิดการปิดบังซ่อนเร้น ทำลาย หรือเปลี่ยนแปลง รหัสการเข้าถึงทรัพยากรคอมพิวเตอร์ซึ่งใช้สำหรับคอมพิวเตอร์ ชุดคำสั่ง ระบบคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ เมื่อรหัสการเข้าถึงทรัพยากรคอมพิวเตอร์นั้นได้ถูกเก็บหรือถูกป้องกันไว้โดยคำสั่งของกฎหมายในขณะเวลาที่ใช้บังคับอยู่ ผู้นั้นต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 200,000 รูปี หรือทั้งจำทั้งปรับ

4. **ประเทศฟิลิปปินส์**⁵³ ได้กำหนดไว้ว่า การกระทำความดังต่อไปนี้ยอมถูกลงโทษปรับ หรือจำคุก

ข) การละเมิดสิทธิโดยการทำซ้ำ ทำขึ้นใหม่ เผยแพร่ จำหน่าย นำเข้ามาในในประเทศ ใช้ ลบ ดัดแปลง ทำสำรอง ปรับปรุง เก็บรักษา รับข้อมูล ติดตั้งข้อมูล ติดต่อสื่อสาร กระทำด้วยประการใด ๆ เพื่อเผยแพร่สู่สาธารณชน หรือทำให้แพร่หลายซึ่งสิ่งอันได้รับการคุ้มครอง ลายมือชื่ออิเล็กทรอนิกส์ หรืองานอันมีลิขสิทธิ์ ซึ่งรวมถึงสื่อบันทึกเสียงที่ได้รับการคุ้มครองตามกฎหมาย หรือภาพถ่าย หรือวัตถุอันบรรจุข้อมูลที่ได้รับการคุ้มครอง โดยผ่านทางติดต่อสื่อสารผ่านเครือข่ายรูปแบบใด ๆ ไม่เพียงแต่อินเทอร์เน็ตเท่านั้น โดยมีเจตนา

⁵² The Information Technology Act, 2000, (Act No.21 of 2000). Section 65.

⁵³ Electronic Commerce Act, 2000, (Republic Act No. 8792). Section 33.

ละเมิดสิทธิในทรัพย์สินทางปัญญา ผู้กระทำต้องระวางโทษปรับไม่น้อยกว่า 100,000 เปโซ และในกรณีที่ก่อให้เกิดความเสียหายอย่างร้ายแรง ผู้กระทำต้องระวางโทษจำคุกตั้งแต่ 6 เดือน ถึง 3 ปี

ค) การกระทำอันเป็นการละเมิดต่อรัฐบัญญัติคุ้มครองผู้บริโภค หรือรัฐบัญญัติฉบับที่ 7394 หรือกฎหมายอื่นที่เกี่ยวข้อง ซึ่งได้กระทำการด้วยการใช้ข้อมูลอิเล็กทรอนิกส์ หรือเอกสารอิเล็กทรอนิกส์ ผู้กระทำต้องระวางโทษตามที่กำหนดไว้ในรัฐบัญญัติฉบับดังกล่าว

ง) การกระทำอันเป็นการละเมิดต่อบทบัญญัติแห่งกฎหมายนี้ในกรณีอื่น ๆ ผู้กระทำต้องระวางโทษปรับไม่เกิน 1,000,000 เปโซ หรือจำคุกไม่เกิน 6 ปี

5. ประเทศสิงคโปร์⁵⁴ ได้กำหนดไว้ว่า

(1) ภายใต้บังคับบทบัญญัติแห่งวรรค (2) ผู้ใดกระทำการอันตนรู้ว่าเป็นการเหตุให้เกิดการปรับเปลี่ยนส่วนประกอบใด ๆ ของคอมพิวเตอร์โดยไม่มีอำนาจที่จะกระทำได้ ย่อมเป็นความผิดในฐานความผิดนี้ และต้องระวางโทษปรับไม่เกิน 10,000 ดอลลาร์ หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ ในกรณีที่เป็นการกระทำความผิดซ้ำ หรือเป็นความผิดต่อเนื่อง ผู้นั้นต้องระวางโทษปรับไม่เกิน 20,000 ดอลลาร์ หรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ

(2) หากความเสียหายใด ๆ ที่เกิดขึ้น เป็นผลเนื่องมาจากการกระทำความผิดในบทบัญญัติความผิดฐานนี้ ผู้กระทำต้องระวางโทษปรับไม่เกิน 50,000 ดอลลาร์ หรือจำคุกไม่เกิน 7 ปี หรือทั้งจำทั้งปรับ

(3) เพื่อประโยชน์แห่งบทบัญญัติมาตรานี้ ไม่ว่าจะการกระทำที่เป็นความผิดดังกล่าวนี้จะได้กระทำได้ต่อสิ่งเหล่านี้โดยตรงหรือไม่

(ก) ชุดคำสั่งหลัก หรือฐานข้อมูลหลัก

(ข) ชุดคำสั่ง หรือฐานข้อมูลใด ๆ ทุกประเภท หรือ

(ค) ชุดคำสั่ง หรือ ฐานข้อมูลที่เก็บรักษาไว้ในระบบคอมพิวเตอร์หลัก

(4) เพื่อประโยชน์แห่งบทบัญญัติมาตรานี้ ไม่สำคัญว่าการปรับเปลี่ยนส่วนประกอบของคอมพิวเตอร์โดยไม่มีอำนาจนั้นจะมีผลเป็นการปรับเปลี่ยนอย่างถาวร หรือเพียงชั่วคราวก็ตาม

6. ประเทศมาเลเซีย⁵⁵ ได้กำหนดไว้ว่า

⁵⁴ Computer Misuse Act, 1993, (Bill No.17/93). Chapter 50A Section 5.

⁵⁵ Computer Crimes Act, 1997, (Law of Malaysia, Act 563). Section 5.

(1) บุคคลจะถูกตัดสินว่ามีความผิด ถ้ากระทำการอันตนรู้ว่าเป็นการเหตุให้เกิดการปรับเปลี่ยนส่วนประกอบใด ๆ ของคอมพิวเตอร์โดยไม่มีอำนาจที่จะกระทำได้

(2) เพื่อประโยชน์แห่งบทบัญญัติมาตรานี้ ไม่ว่าจะกระทำที่เป็นความผิดดังกล่าวนั้นจะได้กระทำต่อสิ่งเหล่านี้โดยตรงหรือไม่

(ก) ชุดคำสั่งหลัก หรือฐานข้อมูลหลัก

(ข) ชุดคำสั่ง หรือฐานข้อมูลใด ๆ ทุกประเภท หรือ

(ค) ชุดคำสั่ง หรือ ฐานข้อมูลที่เก็บรักษาไว้ในระบบคอมพิวเตอร์หลัก

(3) เพื่อประโยชน์แห่งบทบัญญัติมาตรานี้ ไม่สำคัญว่าการปรับเปลี่ยนส่วนประกอบของคอมพิวเตอร์โดยไม่มีอำนาจนั้นจะมีผลเป็นการปรับเปลี่ยนอย่างถาวร หรือเพียงชั่วคราวก็ตาม

(4) บุคคลซึ่งถูกตัดสินว่ามีความผิดตามบทบัญญัติมาตรานี้ ต้องระวางโทษปรับไม่เกิน 100,000 ริงกิตหรือจำคุกไม่เกิน 7 ปี หรือทั้งจำทั้งปรับ หรือต้องระวางโทษปรับไม่เกิน 150,000 ริงกิต หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ถ้าหากว่าการกระทำดังกล่าวเป็นเหตุให้เกิดการละเมิดตามที่บัญญัติไว้ในประมวลกฎหมายอาญา

6. ประเทศเยอรมัน⁵⁶ ได้กำหนดไว้ว่า

(1) ผู้ใดโดยมิชอบด้วยกฎหมาย ลบ ทำให้สิ้นไป ทำให้ไร้ประโยชน์ หรือแก้ไขเปลี่ยนแปลงข้อมูล ต้องระวางโทษจำคุกไม่เกิน 2 ปี หรือ ปรับ

(2) การพยายามกระทำความผิดต้องระวางโทษ

(ง) ความผิดฐานรบกวนระบบคอมพิวเตอร์ (system interference)

1. สภายุโรป⁵⁷ ได้กำหนดไว้ว่า ประเทศภาคีแต่ละประเทศ พึงจัดให้มีมาตรการทางนิติบัญญัติหรือมาตรการอื่นที่จำเป็น เพื่อกำหนดให้เป็นความผิดทางอาญาภายใต้กฎหมายภายในของประเทศนั้น ซึ่งการกีดขวางการทำงานของระบบคอมพิวเตอร์อย่างร้ายแรงโดยการใส่เข้า การส่งต่อ การทำให้เสียหาย การลบ การทำให้เสื่อมเสีย การแก้ไขดัดแปลง หรือการทำลายข้อมูลคอมพิวเตอร์ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น

⁵⁶ Criminal Code . Section 303a

⁵⁷ Convention on Cybercrime, (ETS No.185). Articles 5.

2. ประเทศอินเดีย⁵⁸ ได้กำหนดไว้ว่า

(1) ผู้ใดเจตนากระทำ หรือรู้ว่าจะตนได้ก่อให้เกิดการสูญเสียอย่างร้ายแรง หรือสร้างความเสียหายให้แก่สังคม หรือบุคคลหนึ่งบุคคลใด หรือลบ หรือเปลี่ยนแปลงข้อมูลข่าวสารที่อยู่ในทรัพยากรคอมพิวเตอร์ หรือทำให้คุณค่า หรือประสิทธิภาพลดน้อยลงไป หรือก่อให้เกิดผลเป็นการประทุษร้ายไม่ว่าด้วยวิธีใด ด้วยการเจาะระบบคอมพิวเตอร์

(2) ผู้ใดกระทำการเจาะระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 200,000 รูปี หรือทั้งจำทั้งปรับ

3. ประเทศฟิลิปปินส์⁵⁹ ได้กำหนดไว้ว่า การกระทำความดังต่อไปนี้ย่อมถูกลงโทษปรับ หรือจำคุก

ก) เข้าถึงข้อมูลอิเล็กทรอนิกส์ของผู้อื่นในระบบคอมพิวเตอร์ หรือฐานเก็บรักษาข้อมูล หรือข้อมูลและระบบการติดต่อสื่อสารโดยไม่ได้รับอนุญาต เพื่อการฉ้อฉล เปลี่ยนแปลง ขโมย หรือทำลายข้อมูลอิเล็กทรอนิกส์ หรือชุดอุปกรณ์ข้อมูลและระบบการติดต่อสื่อสาร โดยที่เจ้าของระบบคอมพิวเตอร์ หรือเจ้าของข้อมูลและระบบการติดต่อสื่อสารไม่ได้รับทราบหรือให้ความยินยอม รวมถึงการเผยแพร่ไวรัสคอมพิวเตอร์หรือสิ่งอื่นใดในทำนองเดียวกัน เพื่อการฉ้อฉล ทำลาย เปลี่ยนแปลง ขโมย หรือทำลายข้อมูลอิเล็กทรอนิกส์ หรือเอกสารอิเล็กทรอนิกส์ ผู้กระทำความดังระวางโทษปรับไม่น้อยกว่า 100,000 เปโซ และในกรณีที่ก่อให้เกิดความเสียหายอย่างร้ายแรง ผู้กระทำความดังระวางโทษจำคุกตั้งแต่ 6 เดือน ถึง 3 ปี

4. ประเทศสิงคโปร์⁶⁰ ได้กำหนดไว้ว่า

(1) ผู้ใดจงใจกระทำการโดยไม่มีอำนาจและไม่ได้รับอนุญาตโดยชอบด้วยกฎหมาย ในการ

(ก) สร้างความรำคาญ หรือหยุดยั้ง หรือขัดขวาง ต่อการใช้คอมพิวเตอร์โดยชอบด้วยกฎหมายของผู้อื่น

⁵⁸ The Information Technology Act, 2000, (Act No.21 of 2000). Section 66.

⁵⁹ Electronic Commerce Act, 2000, (Republic Act No. 8792). Section 33.

⁶⁰ Computer Misuse Act, 1993, (Bill No.17/93). Chapter 50A Section 7.

(ข) ทำให้ช้าลง หรือ หยุดยั้งการเข้าถึงระบบคอมพิวเตอร์ หรือทำให้เกิดความเสียหาย หรือทำให้ไร้ประโยชน์ หรือทำให้ประสิทธิภาพลดลง ซึ่งการทำงานของชุดคำสั่งหรือฐานข้อมูลที่เกิดขึ้นในคอมพิวเตอร์

ย่อมเป็นความผิดในฐานความผิดนี้ และต้องระวางโทษปรับไม่เกิน 10,000 ดอลลาร์ หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ ในกรณีที่เป็นการกระทำความผิดซ้ำ หรือการกระทำความผิดต่อเนื่อง ผู้นั้นต้องระวางโทษปรับไม่เกิน 20,000 ดอลลาร์ หรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ

(2) หากความเสียหายใด ๆ ที่เกิดขึ้น เป็นผลเนื่องมาจากการกระทำความผิดในบทบัญญัติความผิดฐานนี้ ผู้กระทำต้องระวางโทษปรับไม่เกิน 50,000 ดอลลาร์ หรือจำคุกไม่เกิน 7 ปี หรือทั้งจำทั้งปรับ

(จ) ความผิดฐานส่งข้อมูลคอมพิวเตอร์รบกวนการใช้งานคอมพิวเตอร์โดยปกติสุข

1. ประเทศสิงคโปร์⁶¹ ได้กำหนดไว้ว่า

(1) บุคคลใดส่ง หรือกระทำการใด ๆ ให้มีการส่ง หรือเป็นการส่งโดยไม่มีอำนาจซึ่งข้อความอิเล็กทรอนิกส์ทางการค้าที่ไม่ได้รับการร้องขอ เป็นจำนวนมาก บุคคลนั้นต้องชดเชยค่าเสียหายให้แก่ผู้ที่ได้รับผลกระทบ

2. ประเทศนิวซีแลนด์⁶² ได้กำหนดไว้ว่า ผู้ใด

(1) ส่งหรือ เชื่อมโยงการส่งมาจากมาจากประเทศนิวซีแลนด์ ซึ่งข้อความอิเล็กทรอนิกส์ทางการค้าที่ผู้รับไม่ได้ร้องขอ ผู้นั้นมีความผิด

(ฉ) ความผิดฐานใช้อุปกรณ์โดยมิชอบ (misuse of device)

1. สภายุโรป⁶³ ได้กำหนดไว้ว่า

1. ประเทศภาคีแต่ละประเทศ พึงจัดให้มีมาตรการทางนิติบัญญัติ หรือ มาตรการอื่นที่จำเป็น เพื่อกำหนดให้เป็นความผิดอาญาภายใต้กฎหมายภายในของประเทศนั้น ซึ่งการกระทำดังต่อไปนี้ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น

⁶¹ THE SPAM CONTROL ACT , 2007. section 8.

⁶² Unsolicited Electronic Message Act, 2007 . section 3.

⁶³ Convention on Cybercrime, (ETS No.185). Articles 6.

(ก) การผลิต การขาย การจัดให้มีเพื่อใช้ประโยชน์ การนำเข้า การจำหน่าย จ่ายแจก หรือการทำให้มีขึ้นซึ่ง

(1) อุปกรณ์ รวมถึงโปรแกรมคอมพิวเตอร์ ที่ถูกออกแบบ หรือดัดแปลง โดยมีวัตถุประสงค์หลักเพื่อใช้ในการกระทำความผิดใดประเภทดังกล่าวในข้อ 2 – 5 ข้างต้น

(2) รหัสผ่านคอมพิวเตอร์ รหัสการเข้าถึงคอมพิวเตอร์ หรือ ข้อมูลที่มีลักษณะทำนองเดียวกัน ซึ่งทำให้สามารถใช้ในการเข้าถึงระบบคอมพิวเตอร์ทั้งหมด หรือส่วนหนึ่ง ส่วนใด โดยมีเจตนาที่จะใช้เพื่อวัตถุประสงค์ในการกระทำความผิดใด ประเภทดังกล่าวในข้อ 2 – 5 และ

(ข) การครอบครองสิ่งซึ่งระบุใน ก (1) หรือ (2) ข้างต้น โดยมีเจตนาที่จะใช้เพื่อวัตถุประสงค์ในการกระทำความผิด ประเภทดังกล่าวในข้อ 2 – 5 ประเทศภาคีอาจกำหนดในกฎหมายว่า การครอบครองสิ่งดังกล่าวตั้งแต่จำนวนเท่าใดจึงจะถือว่าต้องรับผิดทางอาญา

2. ความในข้อนี้ไม่พึงถูกตีความในทางกำหนดความรับผิดทางอาญาลำหรับกรณี ที่การผลิต การขาย การจัดให้มีเพื่อใช้ประโยชน์ การนำเข้า การจำหน่ายจ่ายแจก หรือการทำให้มีขึ้น หรือการครอบครองตามวรรค 1 ของข้อนี้ ไม่ได้มีวัตถุประสงค์ในการกระทำความผิดใด ประเภทดังกล่าวในข้อ 2 – 5 ของอนุสัญญาฉบับนี้ เช่น มีวัตถุประสงค์เพื่อการทดสอบ หรือ คัดกรองระบบคอมพิวเตอร์ที่ได้รับอนุญาตโดยชอบนั้น

3. ประเทศภาคีแต่ละประเทศอาจสงวนสิทธิที่จะไม่นำความในวรรค 1 ของข้อนี้ มาใช้ภายใต้เงื่อนไขว่า การสงวนสิทธินั้นไม่ได้ระบุเกี่ยวกับการขาย การจำหน่ายจ่ายแจก หรือ การทำให้มีขึ้น ซึ่งสิ่งดังกล่าวในวรรค 1 (ก) (2) ของข้อนี้

2. ประเทศสิงคโปร์⁶⁴ ได้กำหนดไว้ว่า

(1) ผู้ใดจงใจเปิดเผยรหัสผ่าน รหัสการเข้าถึง หรือสิ่งอื่นใดในลักษณะทำนองเดียวกัน ที่ทำให้สามารถเข้าถึงชุดคำสั่งหรือฐานข้อมูลใด ๆ ที่เก็บรักษาไว้ในคอมพิวเตอร์ใด ๆ ของผู้อื่น โดยที่ตนไม่มีอำนาจที่จะกระทำได้ ผู้นั้นย่อมมีความผิดหากว่าตนได้กระทำไปโดย

(ก) เพื่อให้ตนได้รับผลประโยชน์โดยมิชอบด้วยกฎหมาย

(ข) เพื่อวัตถุประสงค์อันมิชอบด้วยกฎหมาย หรือ

⁶⁴ Computer Misuse Act, 1993, (Bill No.17/93). Chapter 50A Section 8.

(ค) รู้ว่าการกระทำดังกล่าวจะเป็นเหตุทำให้เกิดความเสียหายแก่บุคคลหนึ่งบุคคลใด

(2) ผู้ใดถูกตัดสินว่ามีความผิดตามบทบัญญัติแห่งวรรค (1) ต้องระวางโทษปรับไม่เกิน 10,000 ดอลลาร์ หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ ในกรณีที่เป็นการกระทำความผิดซ้ำหรือการกระทำความผิดต่อเนื่อง ผู้นั้นต้องระวางโทษปรับไม่เกิน 20,000 ดอลลาร์ หรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ

3. ประเทศมาเลเซีย⁶⁵ ได้กำหนดไว้ว่า

(1) บุคคลจะถูกตัดสินว่ามีความผิด ถ้ากระทำการเผยแพร่หมายเลข รหัส รหัสผ่าน หรือสิ่งอื่นใดในลักษณะทำนองเดียวกันที่ทำให้สามารถเข้าถึงระบบคอมพิวเตอร์ของผู้อื่น โดยที่ตนไม่มีอำนาจที่จะกระทำได้

(2) บุคคลซึ่งถูกตัดสินว่ามีความผิดตามบทบัญญัติมาตรานี้ ต้องระวางโทษปรับไม่เกิน 25,000 ริงกิตหรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ

4. ประเทศญี่ปุ่น⁶⁶ ได้กำหนดไว้ว่า ห้ามมิให้บุคคลใดมอบให้ซึ่งรหัสเฉพาะที่เกี่ยวกับการเข้าถึงระบบการควบคุมของผู้อื่น ให้แก่บุคคลอื่นใด นอกจากผู้ควบคุมการเข้าถึงระบบสำหรับการเข้าถึงระบบควบคุมนั้น หรือผู้ใช้ซึ่งได้รับอนุญาตให้ใช้รหัสเฉพาะนั้น โดยแสดงให้เห็นว่ารหัสเฉพาะนั้นได้มีเพื่อใช้กับเครื่องคอมพิวเตอร์เฉพาะและสำหรับการใช้งานโดยเฉพาะ ในประการที่บุคคลนั้นมีเหตุอันควรรู้ได้ ยกเว้นในกรณีที่การกระทำดังกล่าวเป็นการกระทำของผู้ควบคุมการเข้าถึงระบบ หรือเพื่อการตรวจสอบการเข้าถึงระบบของผู้ใช้ซึ่งได้รับอนุญาต

บุคคลใดกระทำความผิดตามที่บัญญัติไว้ ต้องระวางโทษปรับไม่เกิน 300,000 เยน (มาตรา 9)

(ข) ความผิดฐานปลอมแปลงเกี่ยวกับคอมพิวเตอร์ (computer-related forgery)

1. สภายุโรป⁶⁷ ได้กำหนดไว้ว่า ประเทศภาคีแต่ละประเทศ พึงจัดให้มีมาตรการทางนิติบัญญัติและมาตรการอื่นที่จำเป็น เพื่อกำหนดให้เป็นความผิดทางอาญาภายใต้กฎหมายภายในของประเทศนั้น ซึ่งการใส่เข้า การแก้ไขดัดแปลง การลบ หรือการทำลาย

⁶⁵ Computer Crimes Act, 1997, (Law of Malaysia, Act 563). Section 6.

⁶⁶ Penal Code. Article 4.

⁶⁷ Convention on Cybercrime, (ETS No.185). Articles 7.

ข้อมูลคอมพิวเตอร์ ซึ่งส่งผลให้ข้อมูลคลาดเคลื่อนโดยประสงค์ที่จะทำให้เห็นไปว่า หรือใช้ในทางกฎหมายในลักษณะเหมือนกับว่า ข้อมูลที่ถูกกระทำดังกล่าวแล้วนั้น เป็นข้อมูลที่ต้องการ ทั้งนี้โดยไม่คำนึงถึงว่าข้อมูลนั้น สามารถอ่านได้หรือเข้าใจได้โดยตรงหรือไม่ก็ตาม ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น ประเทศภาคีอาจกำหนดให้ต้องรับผิดชอบทางอาญาในการกระทำนี้ เฉพาะกรณีเป็นการกระทำโดยมีเจตนาที่จะฉ้อโกงหรือมีเจตนาทุจริตในลักษณะทำนองเดียวกัน

2. ประเทศเยอรมัน⁶⁸ ได้กำหนดไว้ว่า

(1) ผู้ใด เพื่อวัตถุประสงค์ในการหลอกลวงในทางกฎหมาย เก็บรักษา หรือปรับปรุงข้อมูลราชการ ด้วยการปลอมหรือแปลงเอกสารที่อาจเรียกกลับมา หรือใช้ประโยชน์ข้อมูลที่เกิดขึ้นรักษา หรือถูกปรับปรุง ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับ

(2) การพยายามกระทำความผิดต้องระวางโทษ

(ซ) บทเพิ่มโทษสำหรับความผิดที่กระทำต่อระบบคอมพิวเตอร์ที่ได้รับการป้องกันเป็นพิเศษ

1. ประเทศสิงคโปร์⁶⁹ ได้กำหนดไว้ว่า

(1) ในกรณีที่มีการเข้าถึงระบบคอมพิวเตอร์ที่ได้รับการป้องกันเป็นพิเศษ ในกรณีที่เป็นการกระทำความผิดตามที่บัญญัติไว้ในมาตรา 3 มาตรา 5 มาตรา 6 หรือ มาตรา 7 ผู้กระทำนั้นไม่ต้องรับโทษตามที่บัญญัติไว้ในมาตราเหล่านั้น หากแต่จะต้องระวางโทษปรับไม่เกิน 100,000 ดอลลาร์ หรือจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ

(2) เพื่อประโยชน์แห่งบทบัญญัติวรรค (1) ระบบคอมพิวเตอร์ที่ได้รับการป้องกันเป็นพิเศษ หากผู้กระทำความผิดดังกล่าว ได้รู้ หรือมีเหตุอันควรได้ว่าระบบคอมพิวเตอร์ หรือชุดคำสั่ง หรือฐานข้อมูลนั้น ได้ใช้โดยตรงในการติดต่อสื่อสารด้วยความจำเป็นอย่างยิ่งเพื่อ

(ก) ความมั่นคงแห่งรัฐ หรือการป้องกันทางทหาร หรือความสัมพันธ์ระหว่างประเทศของสาธารณรัฐสิงคโปร์

(ข) การเก็บรักษาข้อมูลหรือเอกลักษณ์บุคคลซึ่งเป็นพยานหลักฐานอันสำคัญที่เกี่ยวข้องกับการบังคับใช้กฎหมายอาญา

⁶⁸ Criminal Code . Section 269.

⁶⁹ Computer Misuse Act, 1993, (Bill No.17/93). Chapter 50A Section 9.

(ค) ระบบบริการสาธารณะ เกี่ยวกับระบบการติดต่อสื่อสารขั้นพื้นฐาน ระบบการเงิน การธนาคาร ระบบสาธารณูปโภค ระบบการขนส่งสาธารณะ หรือระบบบริการสาธารณะขั้นพื้นฐานอื่น ๆ หรือ

(ง) การรักษาความสงบเรียบร้อย รวมถึงระบบที่เกี่ยวข้องกับการป้องกันภัยพิบัติสาธารณะ เช่น กิจการตำรวจ ระบบการป้องกันภัยฝ่ายพลเรือน หรือระบบการให้บริการทางการแพทย์

(3) เพื่อประโยชน์ในการดำเนินกระบวนการพิจารณาภายใต้บทบัญญัติมาตรานี้ ให้สันนิษฐานไว้ก่อนว่าผู้ถูกฟ้องว่ากระทำความผิดตามมาตรา⁷⁰นี้รู้ถึงองค์ประกอบความผิดตามวรรค (2) และได้เข้าถึงระบบคอมพิวเตอร์ ชุดคำสั่ง หรือฐานข้อมูล หรือระบบอิเล็กทรอนิกส์ หรือสิ่งอื่นใดที่ต้องห้ามนั้นโดยไม่มีอำนาจ อันทำให้ผู้นั้นจะต้องถูกเพิ่มโทษตามบทบัญญัติมาตรานี้ จนกว่าข้อเท็จจริงจะปรากฏเป็นประการอื่น

(ณ) ความผิดฐานฉ้อโกงทางคอมพิวเตอร์

1. สภายุโรป⁷⁰ ได้กำหนดไว้ว่า ประเทศภาคีแต่ละประเทศ พึงจัดให้มีมาตรการทางนิติบัญญัติและมาตรการอื่นที่จำเป็น เพื่อกำหนดให้เป็นความผิดอาญาภายใต้กฎหมายภายในของประเทศนั้น ซึ่งการทำให้เกิดความสูญเสียในทรัพย์สินของบุคคลอื่นโดยวิธีการดังต่อไปนี้ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธิ

(ก) การใส่เข้า การแก้ไขดัดแปลง การลบ หรือการทำลายข้อมูลคอมพิวเตอร์

(ข) การแทรกแซงต่อการทำงานของระบบคอมพิวเตอร์

ทั้งนี้ โดยผู้กระทำมีเจตนาในทางฉ้อโกง หรือเจตนาทุจริตที่จะเอาไปเสีย ซึ่งประโยชน์ทางเศรษฐกิจ สำหรับตนเองหรือบุคคลอื่นโดยไม่มีสิทธินั้น

2. ประเทศสิงคโปร์⁷¹ ได้กำหนดไว้ว่า

(1) ผู้ใดทำให้ระบบคอมพิวเตอร์แสดงฟังก์ชันใด ๆ โดยประสงค์ที่จะเข้าถึงระบบ อันนำไปสู่ชุดคำสั่งหรือฐานข้อมูลที่เก็บรักษาไว้ในคอมพิวเตอร์ โดยมีเจตนาที่จะกระทำความผิดอย่างใดตามที่บัญญัติไว้ในมาตรานี้ ย่อมเป็นความผิดในฐานความผิดนี้

⁷⁰ Convention on Cybercrime, (ETS No.185). Articles 8.

⁷¹ Computer Misuse Act, 1993, (Bill No.17/93). Chapter 50A Section 4.

(2) บทบัญญัติมาตรานี้ รวมความถึงการกระทำใด ๆ อันเป็นผลให้เกิด การยกยอก ทรัพย์สิน การปลอมแปลง การฉ้อฉล หรือการทำร้ายร่างกายผู้อื่น ผู้กระทำต้องระวางโทษจำคุกไม่น้อยกว่า 2 ปี

(3) ผู้ใดถูกตัดสินว่ามีความผิดตามบทบัญญัติมาตรานี้ ต้องระวางโทษปรับไม่เกิน 50,000 ดอลลาร์ หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ

(4) เพื่อประโยชน์แห่งบทบัญญัติมาตรานี้ ไม่สำคัญว่า

(ก) การเข้าถึง ตามความในวรรค (1) นั้นจะเป็นการเข้าถึงโดยชอบหรือไม่

(ข) การกระทำความผิดตามบทบัญญัติมาตรานี้ จะได้กระทำลงในเวลาที่ระบบป้องกันการเข้าถึงนั้นยังคงทำงานอยู่หรือไม่ หรือไม่ว่าในเวลาใด ๆ

3. ประเทศเยอรมัน⁷² ได้กำหนดไว้ว่า

(1) ผู้ใดโดยเจตนาเพื่อให้ตนเอง หรือ บุคคลอื่นได้รับซึ่งประโยชน์ใดๆในทางทรัพย์สินที่มีขอบด้วยกฎหมาย ทำให้เกิดความเสียหายต่อทรัพย์สินของผู้อื่น โดยทำให้เกิดผลกระทบต่อ การประมวลผลข้อมูล โดยใช้โปรแกรมที่มีขอบ โดยการใส่ข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์ โดยการใส่ข้อมูลโดยปราศจากอำนาจ หรือโดยการแทรกแซงใดๆ โดยปราศจากอำนาจในการทำธุรกรรม บุคคลนั้นจะต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับ

(ญ) ความผิดเกี่ยวกับการฉ้อโกงในรูปแบบของ Phishing

1. มลรัฐแคลิฟลอเนีย⁷³ ได้กำหนดไว้ว่า บุคคลใด ส่งเว็บเพจอิเล็กทรอนิกส์ ข้อความอีเมล หรือกระทำการอื่นใดที่มีลักษณะคล้ายคลึงกัน โดยผ่านทางอินเทอร์เน็ตเพื่อชักจูง ร้องขอ หรือกระทำการใดอันเป็นการชักจูงใจให้บุคคลอีกคนหนึ่ง ให้ข้อมูลที่ระบุตัวบุคคลได้ โดยการใส่ข้อมูลเพื่อแสดงตนในธุรกิจที่ไม่มีอยู่จริง หรือถูกสร้างขึ้นโดยไม่มีอำนาจ

(ฎ) ความผิดฐานจารกรรมข้อมูลคอมพิวเตอร์

1. ประเทศเยอรมัน⁷⁴ ได้กำหนดไว้ว่า

(1) ผู้ใด โดยปราศจากอำนาจ ได้รับมาเพื่อตนเองหรือผู้อื่น ซึ่งข้อมูลที่มีได้มิไว้เพื่อผู้นั้น และเป็นข้อมูลที่ถูกเก็บไว้เป็นพิเศษ เพื่อป้องกันการเข้าถึงโดยปราศจาก ผู้นั้นจะต้องถูกจำคุกไม่เกิน 3 ปี หรือปรับ

⁷² Criminal Code . Section 269.

⁷³ Anti Phishing Act ,2005 Section 2.

⁷⁴ Criminal Code . Section 202a.

(2) ข้อมูลในความหมายของอนุมาตรา 1 หมายถึงแต่เฉพาะข้อมูลที่ถูกเก็บไว้ หรือถูกส่งทางอิเล็กทรอนิกส์ ทางแม่เหล็ก หรือทางอื่น ๆ ที่ไม่สามารถสังเกตได้ทางประสาทสัมผัสโดยตรง

(ฎ) ความผิดเกี่ยวกับการขโมยสิ่งแสดงตัวบุคคล

1. ประเทศออสเตรเลีย⁷⁵ ได้กำหนดไว้ว่า

(3) บุคคลเป็นผู้กระทำความผิด ถ้า

ก) บุคคลกระทำการโดยมีเจตนามิชอบ ก่อให้เกิดการสูญเสียไปยังอีกบุคคลหนึ่ง หรือ

ข) นิติบุคคลอื่น

ต้องระวางโทษ จำคุก 5 ปี.

2. ประเทศแคนาดา⁷⁶ ได้กำหนดไว้ว่า ทุกคนที่หลอกลวงสวมสิทธิ์เป็นบุคคลอื่น ไม่ว่าจะบุคคลที่ถูกสวมสิทธิ์นั้นจะมีชีวิตอยู่หรือตายแล้วก็ตาม

(ก) โดยเจตนาเพื่อที่จะได้รับผลประโยชน์ สำหรับตัวเองหรือบุคคลอื่น

(ข) โดยเจตนาที่จะได้รับทรัพย์สิน หรือผลประโยชน์ในทรัพย์สินใด ๆ หรือ

(ค) โดยมีเจตนาที่จะทำให้เกิดความเสียหายกับบุคคลที่ถูกผู้สวมสิทธิ์ หรือบุคคลอื่น ถือว่าบุคคลนั้นเป็นผู้กระทำความผิดกฎหมาย ระวางโทษจำคุกไม่เกิน 10 ปี

3. ประเทศฮ่องกง⁷⁷ ได้กำหนดไว้ว่า

(1) หากบุคคลใด โดยการหลอกลวง (ไม่ว่าจะเป็นการหลอกลวงเพียงอย่างเดียวหรือมีการชักจูงด้วย) โดยมีเจตนาหลอกลวงในการชักจูงบุคคลอื่น เพื่อกระทำการกระทำหรือละเว้นไม่กระทำใด ซึ่งก่อให้เกิดผลลัพธ์ดังนี้

(ก) ประโยชน์ใดๆ กับบุคคลอื่นนอกเหนือจากบุคคลฝ่ายที่สอง หรือ

(ข) ความเสียหายหรือความเสี่ยงที่จะได้รับความเสียหายกับบุคคลหนึ่งบุคคลใด นอกเหนือบุคคลฝ่ายแรก ซึ่งเป็นผู้กระทำความผิดในการหลอกลวง

ต้องระวางโทษจำคุก 14 ปี

⁷⁵ Criminal Code Amendment Act ,2000 .Section 135.1

⁷⁶ Criminal Code Of Canada.Section 403.

⁷⁷ Theft Ordinance, Section16a.

4. **ประเทศอินเดีย** ได้กำหนดไว้ว่า หากบุคคลใดๆ โดยไม่ได้รับอนุญาตของเจ้าของหรือบุคคลที่ครอบครองคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

(b) การดาวน์โฮลด์ สำเนา หรือดึงออกมาซึ่งข้อมูลใดๆ จากคอมพิวเตอร์ ฐานข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์รวมถึงข้อมูลที่ถูกจัดเก็บไว้ในที่เก็บข้อมูลใดๆ

บุคคลนั้นจะต้องรับผิดชอบต่อความเสียหายโดยการชดเชยค่าเสียหายให้แก่ผู้ได้รับผลกระทบไม่เกิน 100,000 รูปี

(ฐ) ความรับผิดกรณีเตรียมกระทำความผิด

1. ประเทศสิงคโปร์⁷⁸ ได้กำหนดไว้ว่า

(1) ผู้ใดทำให้ระบบคอมพิวเตอร์แสดงฟังก์ชันใด ๆ โดยประสงค์ที่จะเข้าถึงระบบ อันนำไปสู่ชุดคำสั่งหรือฐานข้อมูลที่ถูกรักษาไว้ในคอมพิวเตอร์ โดยมีเจตนาที่จะกระทำความผิดอย่างใดตามที่บัญญัติไว้ในมาตรานี้ ย่อมเป็นความผิดในฐานความผิดนี้

(2) บทบัญญัติมาตรานี้ รวมความถึงการกระทำใด ๆ อันเป็นผลให้เกิด การยกยอกทรัพย์ การปลอมแปลง การฉ้อฉล หรือการทำร้ายร่างกายผู้อื่น ผู้กระทำความผิดต้องระวางโทษ จำคุกไม่น้อยกว่า 2 ปี

(3) ผู้ใดถูกตัดสินว่ามีความผิดตามบทบัญญัติมาตรานี้ ต้องระวางโทษปรับไม่เกิน 50,000 ดอลลาร์ หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ

(4) เพื่อประโยชน์แห่งบทบัญญัติมาตรานี้ ไม่สำคัญว่า

(ก) การเข้าถึง ตามความในวรรค (1) นั้นจะเป็นการเข้าถึงโดยชอบหรือไม่

(ข) การกระทำความผิดตามบทบัญญัติมาตรานี้ จะได้กระทำลงในเวลาที่ระบบป้องกันการเข้าถึงนั้นยังคงทำงานอยู่หรือไม่ หรือไม่ว่าในเวลาใดๆ

2. ประเทศมาเลเซีย⁷⁹ ได้กำหนดไว้ว่า

(2) ผู้ใดกระทำการใด ๆ อันเป็นการเตรียม หรือจะกระทำต่อไปในอนาคตซึ่งการกระทำอันเป็นความผิดที่บัญญัติไว้ในพระราชบัญญัตินี้ ผู้นั้นต้องระวางโทษตามที่บัญญัติไว้ในมาตรานั้น ๆ

⁷⁸ Computer Misuse Act, 1993, (Bill No.17/93). Chapter 50A Section 4.

⁷⁹ Computer Crimes Act, 1997, (Law of Malaysia, Act 563). Section 7.