

บทที่ 3

ความผิดมูลฐานตามกฎหมายฟอกเงินและ ความผิดเกี่ยวกับคอมพิวเตอร์ ของต่างประเทศ

การกำหนดความผิดมูลฐานตามกฎหมายฟอกเงินและความผิดเกี่ยวกับคอมพิวเตอร์ของแต่ละประเทศจะมีวิธีการปฏิบัติที่แตกต่างกัน เนื่องมาจากความแตกต่างของระบบกฎหมาย ขนบธรรมเนียมประเพณี และแนวคิดทางสังคม ถึงแม้จะมีการบัญญัติกฎหมายที่แตกต่างกัน แต่ทุกประเทศก็บัญญัติกฎหมายโดยมีวัตถุประสงค์ที่จะคุ้มครองประโยชน์ส่วนรวม มุ่งป้องกันและปราบปรามอาชญากรรมให้หมดไปเพื่อความสงบสุขของสังคม

3.1 แนวความคิดในการกำหนดความผิดมูลฐานของต่างประเทศ

ในศตวรรษที่ 18¹ แนวความคิดในการลงโทษผู้กระทำความผิดเพื่อเป็นการแก้แค้นทดแทน (Retributive Justice) ด้วยวิธีการลงโทษที่โหดร้ายทารุณนั้น ได้เสื่อมลงไป ทั้งนี้ด้วยเหตุผลว่ากฎหมายอาญาต้องมีจุดประสงค์ที่จะก่อให้เกิดประโยชน์แก่ส่วนรวม (Public Interest)² โดยใช้ป้องกันและควบคุมสิ่งไม่พึงประสงค์ ซึ่งการลงโทษเพราะว่าเขาได้ฝ่าฝืนกฎหมายซึ่งคุ้มครองผลประโยชน์ของทุก ๆ คน กฎหมายจะได้รับการพิจารณาในฐานะที่เป็นสัญญาประชาคม อันเป็นภาวะที่ทุกคนรวมกันเป็นอันหนึ่งอันเดียวกัน และมากไปกว่านั้น กฎหมายเป็นเจตจำนงร่วมกันของสมาชิกในชุมชนการบังคับต่อบุคคลที่ละเมิดกฎหมายเพื่อคุ้มครองประโยชน์ส่วนรวม จึงเป็นสิ่งที่ยุติธรรม³

ซึ่งแนวคิดในการป้องกันและปราบปรามอาชญากรรมนั้นไม่ได้ยึดคิดในแนวคิดใดเป็นแนวคิดหลัก โดยมีสองแนวคิดที่สำคัญได้แก่

¹ Alan Noris, Crime. (1993). *Reason and History: A Critical Introduction to Criminal Law*. p. 19.

² Roger Brownsword. (1993). *Law and the Public Interest*. p. 30.

³ David B. Young. "Cesare Beccaria: Utilitarian or Retributivist ?," *Journal of Criminal Justice*, vol.11, p. 319.

1. แนวคิดทางอาญาพื้นฐานทางอาญาที่เน้นการป้องกันและปราบปรามอาชญากรรมเป็นหลัก หรือเน้นการควบคุม อาชญากรรม (Crime Control Model) การป้องกันอาชญากรรมที่เกิดขึ้น จึงเน้นความรวดเร็วและเฉียบขาดในการจัดการกับอาชญากรรม ทั้งนี้เพราะว่า การทำเจ้าหน้าที่ของรัฐไม่สามารถที่จะควบคุม หรือปราบปรามอาชญากรรมได้นั้น จะถูกเพ่งเล็งจากประชาชนว่าไม่อาจจะรักษาความสงบเรียบร้อยของสังคมได้⁴

2. แนวคิดพื้นฐานทางอาญาที่เน้นการคุ้มครองสิทธิเสรีภาพของบุคคลตามหลัก “นิติรัฐ” (The Rule of Law) โดยใช้รูปแบบกระบวนการที่เป็นไปตามกฎหมาย (The Due Process of Law) เป็นกระบวนการที่เน้นการคุ้มครองผู้บริสุทธิ์เป็นกันการดำเนินคดีที่ผิดพลาด ซึ่งบางครั้งอาจขัดแย้งกับเป้าหมายการลดจำนวนอาชญากรรมและการดำเนินคดีโดยรวดเร็ว

นักกฎหมายของสหรัฐอเมริกาได้นำ 2 ทฤษฎี มาประกอบแนวคิดเรื่องการฟอกเงินของสหรัฐอเมริกา คือทฤษฎีสมคบ (Conspiracy Theory) ทฤษฎีการช่วยเหลือและสนับสนุน (Aiding and Abetting Theory)⁵ โดยมีรายละเอียดดังนี้

1) ทฤษฎีสมคบ (Conspiracy Theory)

เป็นไปตามหลักกฎหมายความคิดพื้นฐานของการของการสมคบการทำความผิดอาญาที่ว่าสมาชิกในการสมคบจะต้องมีการรับผิดเช่นเดียวกับตัวการ ในการกระทำของผู้ที่ร่วมในการสมคบกัน Pinkerton Rule ได้วางหลักว่าผู้ร่วมสมคบจะต้องถือว่าร่วมกันทำความผิดสำหรับการกระทำของผู้ที่ร่วมสมคบกัน ความหมายคือ การให้ความช่วยเหลือในการสมคบการทำความผิด ซึ่งจะทำให้คณะบุคคลกลายเป็นกลุ่มบุคคลตามหลักตรรกวิทยาก็คือ เพื่อการก่อตั้งในการตกลงและการตกลงอนุมานได้นำไปสู่การสมคบกัน และการสมคบกันก่อให้เกิดความรับผิดชอบเช่นเดียวกับตัวการ

สำหรับแนวคิดเรื่องความผิดเกี่ยวกับการฟอกเงิน ยังมีแนวคิดเพิ่มเติมที่ว่า การกระทำ ความผิด เกิดขึ้นเมื่อบุคคลตั้งแต่สองคนขึ้นไปสมคบกันทำความผิดต่อรัฐ หรือนั่นคือต่อรัฐ โดยถือว่ารัฐเป็นผู้เสียหายและเพื่อพิสูจน์ความผิดต้องแสดงให้เห็นว่า

- 1) บุคคลตั้งแต่สองคนขึ้นไปสมคบกัน หรือตกลงทำความผิดต่อรัฐ หรือนั่นคือ
- 2) อย่างน้อยที่สุดผู้ที่ได้สมคบกันมีการกระทำที่แสดงออกเพื่อบรรลุวัตถุประสงค์ของการสมคบกัน

⁴ ประธาน วัฒนวานิชย์. (2520, กันยายน-พฤศจิกายน). “ระบบความยุติธรรม: แนวคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม” วารสารนิติศาสตร์, 9, น. 150.

⁵ วีระพงษ์ บุญโยภาส ข เล่มเดิม. น. 16.

การสมคบกัน เป็นการการตกลงที่จะกระทำการมิชอบด้วยกฎหมาย โดยมีการกระทำที่แสดงออกมากกว่าหนึ่งหรือสองประการ การตกลงที่จะกระทำความผิดอาญาและมีการก้าวหน้าไปสู่การบรรลุข้อตกลง จึงจะนำมาเป็นสิ่งที่ฟ้องคดีได้ ถ้าข้อหาการฟอกเงินยังไม่เป็นที่เพียงพอที่จะฟ้องร้องก็อาจร้องในข้อหาสมคบกันกระทำความผิดได้

2) ทฤษฎีการช่วยเหลือและสนับสนุน (Aiding and Abetting Theory)

ทฤษฎีการช่วยเหลือและสนับสนุนนำมาใช้ประกอบกับคดีฟอกเงิน เพราะจำเลยได้กระทำความผิดเกี่ยวกับการฟอกเงินอันเป็นการกระทำความผิดกฎหมายซึ่งมีที่มาจากการค้ายาเสพติด เป็นการกระทำเพื่อช่วยเหลือและสนับสนุนต่อองค์กรค้ายาเสพติด ซึ่งแพร่ขยายอิทธิพลและแผนขององค์กรต่อไป ในกรณีนี้หากโจทก์พิสูจน์ได้ว่าจำเลยให้บริการฟอกเงิน และจำเลยรู้ว่าเงินเหล่านี้ได้มาจากการค้ายาเสพติด ซึ่งจำเลยได้กระทำไปโดยมีเจตนาที่จะให้มีการจำหน่ายหรือครอบครองยาเสพติดต่อไป หรือกล่าวได้ว่าเป็นผู้สืบทอดอาชญากรรม

3.2 ความผิดมูลฐานตามกฎหมายต่างประเทศ

การกำหนดความผิดมูลฐานของประเทศต่าง ๆ นั้นมีที่มาแตกต่างกัน ซึ่งมักจะเป็นอาชญากรรมที่ได้รับผลตอบแทนเป็นเงินจำนวนมาก เช่น การค้ายาเสพติด การหลอกลวงภาษี การก่อการร้าย เป็นต้น และยังมีการนำเงินนอกระบบมาเข้าสู่ระบบเพื่อฟอกเงินให้ผู้อื่นเข้าใจว่าเป็นเงินที่ถูกกฎหมายเป็นจำนวนมาก จึงทำให้รัฐต้องออกบทบัญญัติกฎหมายเกี่ยวกับการฟอกเงินมาบังคับใช้เพื่อเป็นเครื่องมือในการตัดวงจรทางการเงินของอาชญากรรมต่าง ๆ ให้หมดสิ้นไป

3.2.1 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาถือเป็นต้นแบบของแนวคิดในเรื่องการให้มีกฎหมายที่เกี่ยวกับการฟอกเงินขึ้นในประเทศต่าง ๆ ทั่วโลก ซึ่งกฎหมายที่เกี่ยวข้องกับการฟอกเงินมีดังนี้⁶

1) Federal Crimes and Criminal Procedure

เป็นกฎหมายเบื้องต้นในการป้องกันและปราบปรามการฟอกเงิน มีสาระสำคัญได้แก่

1. การกระทำหรือพยายามกระทำการ สนับสนุนหรือช่วยเหลือในการกระทำความผิดเกี่ยวกับการเงิน ปกปิดซ่อนเร้นการกระทำความผิด หลีกเลี่ยงไม่รายงานการโอนเงิน ต้องระวางโทษปรับไม่เกิน 500,000 เหรียญสหรัฐ หรือสองเท่าของมูลค่าของทรัพย์สินที่เกี่ยวข้อง ขึ้นอยู่กับว่าจำนวนไหนจะมากกว่า หรือจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ

⁶ วีระพงษ์ บุญโยภาส ง (2544, กรกฎาคม). “กฎหมายป้องกันปราบปรามการฟอกเงิน: ศึกษากรณี “ความผิดมูลฐาน” ของประเทศสหรัฐอเมริกาและออสเตรเลีย.” *วารสารกฎหมาย*, 20(3), น. 68-77.

2. การกระทำหรือพยายามนำเข้าหรือนำออกไปซึ่งตราสารหรือเอกสารทางการเงิน (Monetary instrument) เช่น เงินตราของต่างประเทศ เช็คเดินทาง เช็คนาการ ตัวเงิน ตัวสัญญาใช้เงิน เป็นต้น มีโทษปรับไม่เกิน 500,000 เหรียญสหรัฐ หรือสองเท่าของมูลค่านั้น ขึ้นอยู่กับว่าจำนวนไหนจะสูงกว่ากัน หรือจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ

3. ผู้กระทำความผิดทั้ง 2 กรณีดังที่กล่าวมาในข้างต้นต้องรับผิดทางแพ่งไม่เกินมูลค่าของทรัพย์สินนั้นหรือไม่เกิน 10,000 เหรียญสหรัฐ

จากหลักสำคัญของกฎหมายดังกล่าวจะเห็นได้ว่า กฎหมายฉบับนี้เน้นลงโทษผู้ที่กระทำความผิดเกี่ยวกับการเงิน ตราสารหรือเอกสารทางการเงิน ไม่ได้มีการบัญญัติความผิดมูลฐานไว้

2) Bank Secrecy Act 1970 (BSA)

กฎหมายฉบับนี้เป็นกฎหมายเกี่ยวกับการรายงานเรื่องการหมุนเวียนของเงินตรา โดยมีวัตถุประสงค์เพื่อต้องการพิสูจน์ทราบแหล่งที่มาของเงิน ปริมาณเงิน และความเคลื่อนไหวของกระแสการเงินที่นำเข้าหรือออกนอกประเทศหรือที่ฝากไว้ในธนาคารหรือสถาบันการเงินเพื่อช่วยให้เจ้าหน้าที่ของรัฐสามารถตรวจสอบและสืบสวนผู้กระทำการฝ่าฝืนกฎหมายอาญาและกฎหมายเกี่ยวกับภาษีได้ โดยมีต้องอาศัยข้อมูลจากธนาคารต่างประเทศ ซึ่งบัญญัติไว้ใน บรรพ 31 ของกฎหมายแห่งสหรัฐอเมริกา โดยมีสาระสำคัญ ดังนี้

1. ให้สถาบันการเงินภายในประเทศรายงานการโอนเงิน การจ่ายเงิน และการรับเงิน ที่มีมูลค่าตั้งแต่ 10,000 เหรียญสหรัฐขึ้นไป

2. ให้ผู้ที่ได้รับมอบหมายให้นำเข้าหรือนำออกเงินมากกว่า 5,000 เหรียญสหรัฐ ต้องรายงานการกระทำดังกล่าว

หากสถาบันการเงินใดฝ่าฝืนบทบัญญัติดังกล่าว จะต้องรับโทษที่มีทั้งโทษปรับและโทษจำคุก

จากหลักสำคัญของกฎหมายดังกล่าวจะเห็นได้ว่ามีการบัญญัติความผิดมูลฐานเกี่ยวกับความลับของสถาบันการเงินไว้โดยเฉพาะ คุ้มครองและตรวจสอบการหมุนเวียนของเงิน เพื่อความสะดวกในการสืบสวนของเจ้าหน้าที่ในการปราบปรามอาชญากรรมทางเศรษฐกิจ

3) Money Laundering Control Act 1986 (MLCA)

เนื่องจากกฎหมายที่ยังมีช่องโหว่วันที่ 27 ตุลาคม ค.ศ. 1986 ได้มีการประกาศใช้กฎหมาย Anti-Drug of 1986 หรือเรียกว่า “กฎหมายการควบคุมการฟอกเงิน” (Money Laundering

Control Act of 1986 หรือ MLCA) ซึ่งบัญญัติไว้ในบรรพ 18 ของกฎหมายสหรัฐอเมริกา มาตรา 1956⁷ โดยมีการปรับปรุงแก้ไขให้ทันสมัยตลอดมา ซึ่งมีหลักสำคัญดังนี้

(1) ผู้ใดดำเนินการหรือพยายามที่จะทำธุรกรรมทางการเงินที่เกี่ยวข้องกับเงินที่ได้มาจากการกระทำผิดกฎหมาย (Unlawful Activity) โดยรู้ถึงที่มาของเงินในการดำเนินธุรกรรมดังกล่าว ไม่ว่าจะโดยเจตนาช่วยเหลือ หรือรู้ว่าธุรกรรมทั้งหมดหรือแต่บางส่วนมาจากการกระทำผิดกฎหมายนั้น เพื่อ

1. ปกปิดหรือลวง สภาพ ที่ตั้ง แหล่งที่มา ความเป็นเจ้าของ หรือการควบคุม รายได้ของการกระทำผิดกฎหมายนั้น

2. หลีกเลี่ยงการรายงานธุรกรรมทางการเงินที่กำหนดตามกฎหมายมลรัฐหรือกฎหมายของสหรัฐ

ต้องระวางโทษปรับไม่เกิน 500,000 เหรียญสหรัฐ หรือปรับเป็นจำนวนสองเท่าของมูลค่าทรัพย์สินที่เกี่ยวข้องกับธุรกรรม ขึ้นอยู่กับว่าจำนวนไหนจะสูงกว่ากัน จำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ

(2) ผู้ใด ทำการส่งหรือพยายามที่จะส่งตราสารทางการเงิน หรือเงินทุน จากสหรัฐ ออกไปยังนอกประเทศสหรัฐอเมริกา หรือนำเข้าตราสารหรือเงินทุนใด ๆ มายังสหรัฐ ไม่ว่าจะโดยเจตนาโดยเจตนาช่วยเหลือในการกระทำผิดกฎหมาย หรือรู้ว่าตราสารหรือเงินทุนดังกล่าวเกี่ยวข้องกับการกระทำผิดกฎหมาย และรู้ถึงการส่งหรือนำเข้าทั้งหมดหรือแต่บางส่วนนั้น เพื่อ

1. ปกปิดหรือลวง สภาพ ที่ตั้ง แหล่งที่มา ความเป็นเจ้าของ หรือการควบคุม รายได้ของการกระทำผิดกฎหมาย หรือ

2. หลีกเลี่ยงการรายงานการธุรกรรมนั้น ที่กำหนดไว้ในกฎหมายมลรัฐหรือกฎหมายของสหรัฐ

ต้องระวางโทษปรับไม่เกิน 50,000 เหรียญสหรัฐ หรือปรับเป็นจำนวนสองเท่าของมูลค่าตราสารทางการเงินหรือเงินทุนที่เกี่ยวข้องกับการทำความผิดนั้น ขึ้นอยู่กับว่าจำนวนไหนจะสูงกว่ากัน หรือจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ

(3) ผู้ใด กระทำหรือพยายามกระทำธุรกรรมตามข้อ (2) และ (3) ข้างต้น ต้องรับผิดทางแพ่งต่อสหรัฐเป็นจำนวนไม่เกินมูลค่าของทรัพย์สินที่เกี่ยวข้องกับธุรกรรมนั้น หรือเป็นเงินจำนวน 10,000 เหรียญสหรัฐ⁸

⁷ 18 U.S.C. § 1956 - Laundering of monetary instruments.

⁸ วีระพงษ์ บุญโยภาส ข เล่มเดิม. น. 72.

กฎหมายฉบับดังกล่าว ได้กำหนดนิยามของคำว่า “การกระทำผิดกฎหมาย” (Unlawful Activity) ซึ่งเป็นความผิดมูลฐาน โดยกำหนดไว้เพื่อให้ครอบคลุมการกระทำความผิดมากมายหลายฐาน และยังมีการกำหนดความผิดเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ให้เป็นความผิดมูลฐานตามมาตราดังกล่าวอีกด้วย⁹

จากหลักกฎหมายดังกล่าวข้างต้น จะเห็นได้ว่าประเทศสหรัฐอเมริกา มีการกำหนดความผิดมูลฐานไว้อย่างกว้าง ๆ และกำหนดไว้เป็นจำนวนมาก เพื่อให้ครอบคลุมการกระทำความผิดต่าง ๆ มากที่สุด โดยมีวัตถุประสงค์ในการป้องกันและปราบปรามอาชญากรรมทางเศรษฐกิจและการฟอกเงินได้อย่างมีประสิทธิภาพ

3.2.1 สหพันธ์สาธารณรัฐเยอรมนี

สหพันธ์สาธารณรัฐเยอรมนี เป็นประเทศที่ใช้กฎหมายระบบลายลักษณ์อักษร (Civil Law) โดยยึดตามประมวลกฎหมายในการตัดสินคดี ซึ่งกฎหมายเกี่ยวกับการฟอกเงินนั้น ได้มีการบัญญัติไว้ในประมวลกฎหมายอาญามาตรา 261 มีสาระสำคัญดังนี้

มาตรา 261 ความผิดฐานฟอกเงิน ; ปกปิด ทรัพย์สินที่ได้มาจากการทำผิดกฎหมาย¹⁰

(1) ผู้ใดซุกซ่อน ทรัพย์สินที่ได้มาจากการทำผิดกฎหมายที่ระบุไว้ในวรรค 2 ปกปิดแหล่งที่มา หรือ ซัดขวาง หรือ รบกวณการสืบสวนแหล่งที่มา การค้นหา การริบทรัพย์สิน การยึดทรัพย์สิน หรือการควบคุม ต้องระวางโทษจำคุกตั้งแต่ 3 เดือน ถึง 5 ปี

การกระทำตาม วรรค 1 คือ

1. การกระทำความผิดอาญาร้ายแรง

2. การกระทำความผิดตาม

a) มาตรา 332 (1) เกี่ยวโยงกับอนุมาตรา (3) มาตรา 334;

b) มาตรา 29 (1) วรรค 1 ข้อ 1 ตามกฎหมายยาเสพติด และมาตรา 19 (1) ข้อ 1 ตามกฎหมายควบคุมสารตั้งต้นยาเสพติด

3. การกระทำความผิดตามมาตรา 373 มาตรา 374 (2) ตามกฎหมายการเงิน ถ้าผู้กระทำความผิดกระทำเป็นอาชีพ มาตรา 12 (1) ตามกฎหมายเกี่ยวกับการดำเนินงานขององค์กรตลาดร่วม และกฎหมายระบบจ่ายเงินตรง

⁹ 18 U.S.C. § 1956 (c) (7) (D) the term “specified unlawful activity” means— an offense under... section 1030 (relating to computer fraud and abuse)...

¹⁰ Strafgesetzbuch (StGB) § 261 Geldwäsche; Verschleierung unrechtmäßig erlangter Vermögenswerte

4. การกระทำความผิดตาม

a) มาตรา 152a มาตรา 181a มาตรา 232 (1) และ (2) มาตรา 233 (1) และ (2) มาตรา 233a มาตรา 242 มาตรา 246 มาตรา 253 มาตรา 259 มาตรา 263 to 264 มาตรา 266 มาตรา 267 มาตรา 269 มาตรา 271 มาตรา 284 มาตรา 326 (1)(2) และ (4) มาตรา 328 (1)(2) และ (4) มาตรา 348;

b) มาตรา 96 ตามกฎหมายต่างด้าว มาตรา 84 ตามกฎหมายเกี่ยวกับการขอสิทธิ์ และ มาตรา 270 ตามกฎหมายการเงิน ที่กระทำเป็นอาชญากรรม หรือ กระทำโดยสมาชิกของกลุ่มอาชญากรที่กระทำเป็นปกติธุระดังกล่าว และ

5. การกระทำความผิด ตามมาตรา 89 มาตรา 129 และมาตรา 129a (3) และ (5) ที่เกี่ยวข้องกับ มาตรา 129b (1) ที่กระทำโดยองค์กรอาชญากรรม หรือ องค์กรก่อการร้าย (มาตรา 129 และ 129a ที่เกี่ยวข้องกับมาตรา 129b (1))

ข้อความตามวรรค 1 นำไปใช้บังคับกับกรณีหลบเลี่ยงภาษีที่กระทำไปเพื่อหากำไร หรือ โดยกลุ่มอาชญากรรม ตามมาตรา 370 ของกฎหมายการเงิน การใช้จ่ายเงินที่ได้มาจากการหลบเลี่ยงภาษี จากการได้คืนภาษีที่ผิดกฎหมาย และ ในกรณีตามวรรค 2 ข้อ 3 ให้นำวรรค 1 มาใช้บังคับกับทรัพย์สินที่เกี่ยวข้องกับการหลบเลี่ยงค่าธรรมเนียมเช่นกัน

(2) ผู้ใด

1. จัดหาทรัพย์สินตาม (1) เพื่อตนเองหรือผู้อื่น หรือ
2. เก็บทรัพย์สินตาม (1) ไว้ในครอบครอง หรือใช้เพื่อตนเองหรือผู้อื่น โดยรู้ถึงแหล่งที่มาในเวลาที่ได้ทรัพย์สินนั้นไว้ในครอบครอง ต้องถูกลงโทษเช่นเดียวกัน

(3) การพยายามกระทำความผิดก็ต้องได้รับโทษ

(4) ในกรณีที่กระทำความผิดร้ายแรง ต้องระวางโทษจำคุกตั้งแต่ หกเดือนถึงสิบปี การกระทำความผิดร้ายแรงดังกล่าวให้หมายถึง ผู้กระทำความผิดเป็นอาชญากรรม หรือกระทำโดยสมาชิกกลุ่มอาชญากร กระทำการฟอกเงินเป็นปกติธุระ

(5) ผู้ใด กระทำผิดตาม (1) และ (2) อย่างประมาทโดยตั้งใจ ได้มาซึ่งทรัพย์สินจากการกระทำความผิดกฎหมายตาม (1) ต้องระวางโทษจำคุกไม่เกิน 2 ปี หรือปรับ

(6) การกระทำตาม (2) ไม่ต้องรับโทษ ถ้าผู้อื่นได้ทรัพย์สินนั้นมาก่อนที่จะมีการกระทำความผิด

(7) ทรัพย์สินที่เกี่ยวข้องกับการกระทำความผิดจะต้องถูกยึดทรัพย์ ให้นำมาตรา 74a มาบังคับใช้ ในกรณีกระทำความผิดโดยสมาชิกกลุ่มองค์กรอาชญากรรมที่ฟอกเงินเพื่อหากำไรหรือกระทำเป็นอาชญากรรมให้นำมาตรา 73d มาบังคับใช้

(8) ทรัพย์สินที่ได้มาจากการกระทำความผิดตาม (1) ที่เกิดขึ้นนอกราชอาณาจักร ให้ถือเสมือนว่าเป็นทรัพย์สินตาม (1)(2) และ (5) ถ้าการกระทำนั้นเป็นการกระทำที่ผิดกฎหมายไทยตามกฎหมาย

(9) ผู้ใด

1. สมัครใจรายงานการกระทำความผิดกล่าวโดยสมัครใจต่อเจ้าหน้าที่ของรัฐผู้มีอำนาจ หรือ สมัครใจที่จะทำให้เกิดการรายงาน ถ้าการกระทำนั้นยังไม่ถูกตรวจพบมาก่อนทั้งหมดหรือ แต่บางส่วน และผู้กระทำความผิดทราบ หรือ ควรจะต้องนำมาพิจารณาประเมินผลตามข้อเท็จจริง

2. กรณีตาม (1) หรือ (2) ภายใต้บทบัญญัติในข้อ 1 เป็นเหตุให้ทรัพย์สินที่เกี่ยวข้อง กับอาชญากรรมถูกควบคุม ไม่ต้องรับโทษตาม (1) – (5)

ผู้ใดถูกลงโทษเนื่องจากการเข้าร่วมการกระทำความผิดกล่าว ไม่ต้องรับโทษตาม (1) – (5) อีก จากหลักกฎหมายในข้างต้นจะเห็นว่า มีการบัญญัติความผิดเกี่ยวกับการฟอกเงินไว้เป็น ความผิดมูลฐานโดยเฉพาะ และมีการบัญญัติไว้อย่างกว้างคือ “การกระทำความผิดอาญาร้ายแรง” (Verbrechen) ซึ่งประมวลกฎหมายอาญาเยอรมันได้ให้คำนิยามของคำว่า “การกระทำความผิดอาญา ร้ายแรง” (Verbrechen) ไว้ในมาตรา 12 หมายถึง การกระทำความผิดกฎหมายที่ต้องระวางโทษจำคุก ตั้งแต่ 1 ปีขึ้นไป¹¹ ดังนั้น จึงเห็นได้ว่าความผิดมูลฐานตามกฎหมายฟอกเงินกฎหมายเยอรมัน จึงครอบคลุมความผิดที่กว้างมาก

3.2.2 สาธารณรัฐจีน (ไต้หวัน)

ไต้หวันใช้กฎหมายระบบลายลักษณ์อักษร (Civil Law) เป็นศูนย์กลางทางการเงินของ ภูมิภาค มีภาคธุรกิจทางการเงินที่ทันสมัย เป็นที่ตั้งของเส้นทางการจัดส่งสินค้าระหว่างประเทศ เชี่ยวชาญในด้านเทคโนโลยีขั้นสูง และมีบทบาทเป็นศูนย์กลางของการค้าระหว่างประเทศ จึงทำให้ มีความเสี่ยงต่อการเกิดอาชญากรรมข้ามชาติ รวมทั้งการฟอกเงิน การค้ายาเสพติด การฉ้อโกงทาง โทรคมนาคม และการทุจริตทางการค้า

การฟอกเงินในไต้หวันมักจะเป็นการกระทำความผิดเกี่ยวกับการหลีกเลี่ยงภาษี การค้า ยาเสพติด การทุจริตของประชาชน และอาชญากรรมทางเศรษฐกิจ ร้านอัญมณีมีจำนวนมากขึ้นและ มักถูกใช้เป็นสถานที่โอนเงินใต้ดิน ผู้ค้าอัญมณีมักจะแปลงเงินที่ไม่ชอบด้วยกฎหมายเป็นโลหะที่มี ค่า เพชรพลอย และสกุลเงินต่างประเทศ โดยใช้วิธีการการจัดส่งข้ามประเทศ การกระทำเหล่านี้ ใช้วิธีที่ซับซ้อนจึงทำให้ยากต่อการตรวจพบและยับยั้งการฟอกเงิน ซึ่งกฎหมายเกี่ยวกับการฟอกเงิน

¹¹ § 12 Verbrechen und Vergehen

(1) Verbrechen sind rechtswidrige Taten, die im Mindestmaß mit Freiheitsstrafe von einem Jahr oder darüber bedroht sind.

ได้มีการบัญญัติแยกออกมาจากประมวลกฎหมายอาญาเป็นกฎหมายป้องกันและปราบปรามการฟอกเงิน (Money Laundering control act) เมื่อวันที่ 23 ตุลาคม 2539 และมีผลบังคับใช้เมื่อวันที่ 23 เมษายน 2540 โดยมีมาตราที่เกี่ยวข้อง ดังนี้

มาตรา 1 กฎหมายนี้ บัญญัติเพื่อควบคุมการฟอกเงินที่มีขอบด้วยกฎหมายและกวดล้างอาชญากรรมร้ายแรง

มาตรา 2 ตามกฎหมายนี้ อาชญากรรม “ฟอกเงิน” หมายถึง ผู้ใด..

1. โดยรู้ ปลอมแปลง หรือ ปกปิด ทรัพย์สิน หรือ ประโยชน์ในทางทรัพย์สิน ที่ได้มาจากการกระทำอาชญากรรมร้ายแรงที่กระทำด้วยตนเอง

2. โดยรู้ ปกปิด ได้รับ ขนส่ง เก็บรักษา ซื่อโดยจงใจ หรือทำหน้าที่เป็นนายหน้าจัดการทรัพย์สิน หรือประโยชน์ในทางทรัพย์สินที่ได้มาจากการกระทำความผิดร้ายแรงที่กระทำโดยผู้อื่น

มาตรา 3 ตามกฎหมายนี้ “อาชญากรรมร้ายแรง” หมายถึงความผิดดังนี้ :

1. การกระทำความผิดที่มีโทษจำคุกตั้งแต่ห้าปีขึ้นไป

2. ประมวลกฎหมายอาญา มาตรา 201 และ 201-1

3. ประมวลกฎหมายอาญา มาตรา 240 วรรคหนึ่ง มาตรา 241 วรรคสอง และ มาตรา 243 วรรคหนึ่ง

4. ประมวลกฎหมายอาญา มาตรา 296 วรรคหนึ่ง มาตรา 297 วรรคสอง มาตรา 298 วรรคสอง มาตรา 300 วรรคหนึ่ง

5. กฎหมายป้องกันการค้าประเวณีเด็กและเยาวชน มาตรา 23 วรรคสองถึงวรรคสี่ และ มาตรา 27 วรรคสอง

6. กฎหมายควบคุมอาวุธ เครื่องกระสุนและมีดอันตราย มาตรา 13 วรรคหนึ่งถึงสาม และ มาตรา 13 วรรคหนึ่งและสอง

7. กฎหมายป้องกันการลักลอบขนของเถื่อน มาตรา 2 วรรคหนึ่ง และ มาตรา 3 วรรคหนึ่ง

8. กฎหมายหลักทรัพย์และตลาดหลักทรัพย์ มาตรา 171 วรรค 1 อนุมาตรา 1 มาตรา 155 วรรคหนึ่งและสอง มาตรา 157-1 วรรคหนึ่ง มาตรา 171 วรรคหนึ่ง อนุมาตรา 2 และ 3 และ มาตรา 174 วรรคหนึ่ง อนุมาตรา 8

9. กฎหมายธนาคาร มาตรา 125-2 วรรคหนึ่ง นำไปใช้กับ มาตรา 125 วรรคหนึ่ง มาตรา 125-2 วรรคหนึ่ง และ มาตรา 125-2 วรรคสี่

10. กฎหมายล้มละลาย มาตรา 154 และ มาตรา 155

11. กฎหมายป้องกันและปราบปรามองค์กรอาชญากรรม มาตรา 3 วรรคหนึ่งและสอง มาตรา 4 และมาตรา 6

12. กฎหมายชนกิจการเกษตร มาตรา 39 วรรคหนึ่ง และมาตรา 40 วรรคหนึ่ง

13. กฎหมายบริหารจัดการตราสารทางการเงิน มาตรา 39 วรรคหนึ่ง และมาตรา 58-1 วรรคหนึ่ง

14. กฎหมายประกันภัย มาตรา 168-2 วรรคหนึ่ง

15. กฎหมายบริษัทธุรกิจทางการเงิน มาตรา 58 วรรคหนึ่ง และมาตรา 57-1 วรรคหนึ่ง

16. กฎหมายบริษัททรัสต์ มาตรา 48-1 วรรคหนึ่ง และมาตรา 48-2 วรรคหนึ่ง

17. กฎหมายสหกรณ์ทรัสต์ มาตรา 38-2 วรรคหนึ่ง และมาตรา 38-3 วรรคหนึ่ง

18. ความผิดตามที่บัญญัติในมาตรา 11 ของกฎหมายนี้

อาชญากรรมดังต่อไปนี้ถือว่าเป็น “อาชญากรรมร้ายแรง” ถ้าทรัพย์สิน หรือประโยชน์ในทางทรัพย์สินที่ได้มาจากการกระทำความผิด มีจำนวนมากกว่า 5 ล้านเหรียญ

1. ประมวลกฎหมายอาญา มาตรา 336 วรรคสอง และมาตรา 344

2. กฎหมายการจัดซื้อจัดจ้างของรัฐ มาตรา 87 วรรคหนึ่ง วรรคสองส่วนท้ายถึงวรรคหก มาตรา 88 มาตรา 89 มาตรา 90 วรรคหนึ่ง วรรคสองส่วนท้ายและวรรคสาม มาตรา 91 วรรคหนึ่ง วรรคสองตอนท้ายและวรรคสาม

มาตรา 4 ภายใต้กฎหมายนี้ “ทรัพย์สิน หรือประโยชน์ในทางทรัพย์สินที่ได้มาจากการกระทำความผิด” หมายถึง

1. ทรัพย์สิน หรือ ผลกำไร จากทรัพย์สินที่ได้รับมาโดยตรงจากการกระทำความผิด

2. ค่าตอบแทนจากการกระทำความผิด

3. ทรัพย์สิน หรือประโยชน์ในทางทรัพย์สิน ที่ได้รับมาจาก 2 อนุมาตราก่อนหน้านี้ อย่างไรก็ตาม กฎหมายนี้ไม่นำไปใช้กับบุคคลภายนอกที่ได้รับทรัพย์สินหรือผลประโยชน์ในทางทรัพย์สินด้วยความสุจริตภายใต้ที่ระบุไว้ใน 2 อนุมาตราข้างต้น

มาตรา 11 ผู้ใดเกี่ยวข้องกับการฟอกเงิน ตามมาตรา 2 วรรคหนึ่งอนุมาตรา 1 ต้องระวางโทษจำคุกไม่เกิน 5 ปี และอาจมีโทษปรับไม่เกิน 3 ล้านเหรียญ

ผู้ใดเกี่ยวข้องกับการฟอกเงิน ตามมาตรา 2 วรรคหนึ่งอนุมาตรา 2 ต้องระวางโทษจำคุกไม่เกิน 7 ปี และอาจมีโทษปรับไม่เกิน 5 ล้านเหรียญ

ผู้ใด รวบรวม จัดหาซึ่งทรัพย์สินหรือประโยชน์ในทางทรัพย์สินเพื่อตนเองหรือผู้อื่นในการกระทำความผิด

ดังต่อไปนี้ที่เป็นการทำให้สาธารณชนตกใจกลัว ข่มขู่รัฐบาล รัฐบาลต่างชาติ สถาบันหรือองค์การระหว่างประเทศ ต้องระวางโทษตั้งแต่ 1 ปี ถึง 7 ปี และอาจจะมีโทษปรับไม่เกิน 10 ล้านบาท

1. ประมวลกฎหมายอาญา มาตรา 173 วรรคหนึ่งถึงสาม โดยนำมาตรา 176 ไปบังคับใช้โดยอนุโลม มาตรา 178 วรรคหนึ่งและวรรคสาม มาตรา 183 วรรคหนึ่งและวรรคสี่ มาตรา 184 วรรคหนึ่ง วรรคสอง และวรรคห้า มาตรา 185 มาตรา 185-1 วรรคหนึ่งถึงวรรคห้า มาตรา 185-2 มาตรา 186-1 วรรคหนึ่ง วรรคสอง และวรรคสี่ มาตรา 187-2 มาตรา 187-3 มาตรา 188 มาตรา 190 วรรคหนึ่งวรรคสองและวรรคสี่ มาตรา 190-1 วรรคหนึ่งถึงวรรคสาม มาตรา 191-1 มาตรา 192 วรรคสอง มาตรา 271 วรรคหนึ่งและวรรคสอง มาตรา 278 มาตรา 302 มาตรา 247 วรรคหนึ่งถึงวรรคสาม มาตรา 248 มาตรา 348-1

2. กฎหมายควบคุมอาวุธปืน เครื่องกระสุนและมีด มาตรา 7

3. กฎหมายการบินพลเรือน มาตรา 100

ผู้แทนนิติบุคคล ตัวแทน พนักงาน หรือลูกจ้างอื่น ๆ ของนิติบุคคล หรือนุคคลธรรมดาได้กระทำการฟอกเงินไปในทางการที่จ้าง ตามที่กำหนดไว้ในสามวรรคก่อน ต้องระวางโทษตามความผิดนั้น ๆ นอกจากนี้ หากผู้ที่กระทำการแทนหรือทำงานให้กับตัวแทนหรือนุคคลธรรมดาได้กระทำความผิดตามสามวรรคก่อน ตัวแทนหรือนุคคลธรรมดานั้นต้องถูกปรับตามสามวรรคก่อนด้วย เว้นแต่ ตัวแทนหรือนุคคลธรรมดาได้กระทำการบางอย่างเพื่อป้องกันหรือหยุดยั้งการฟอกเงินนั้น

ถ้าบุคคลใดมอบตัวต่อพนักงานเจ้าหน้าที่ภายในหกเดือนหลังจากที่มีส่วนร่วมในการกระทำการผิดฟอกเงิน ตามสามวรรคก่อนนี้ จะได้รับการยกเว้นโทษ แต่ถ้าบุคคลนั้นมอบตัวช้ากว่า 6 เดือน หลังจากมีส่วนร่วมในการกระทำความผิดฟอกเงิน ตามสี่วรรคก่อนนี้ จะได้รับการลดโทษหรือยกเว้นโทษ หากบุคคลใดสารภาพขณะอยู่ระหว่างการควบคุมตัวโดยเจ้าหน้าที่เพื่อสอบปากคำ หรือระหว่างการพิจารณาว่าตนได้เข้าร่วมการกระทำความผิดฟอกเงิน ตามสี่วรรคก่อน จะได้รับการลดโทษ

ความผิดตามวรรคหนึ่ง ถึงวรรคสาม ให้บังคับใช้กับกระทำของพลเมืองประเทศได้วันที่เกิดขึ้นนอกราชอาณาจักรด้วย

มาตรา 12 ผู้ใดมีส่วนร่วมในการกระทำความผิดฟอกเงิน ตามมาตรา 2 วรรคหนึ่ง อนุมาตรา 2 เพื่อปกปิด ได้รับ ขนส่ง เก็บรักษา ซื่อโดยจงใจ หรือทำหน้าที่เป็นนายหน้าจัดการทรัพย์สิน หรือประโยชน์ในทางทรัพย์สินที่ได้มาจากการกระทำความผิด ที่กระทำโดยญาติพี่น้องโดยตรง คู่สมรส ญาติที่อาศัยอยู่ร่วมกัน หรือเจ้าของรวม จะได้รับการลดโทษจำคุกหรือโทษปรับ

3.3 ความผิดเกี่ยวกับคอมพิวเตอร์ตามกฎหมายต่างประเทศ

จากการศึกษาสถิติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในบทที่ 2 ทำให้เห็นว่าการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ก่อให้เกิดความเสียหายแก่เศรษฐกิจเป็นอย่างมาก หัวข้อนี้จึงศึกษาถึงกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศต่าง ๆ ดังนี้

3.3.1 สหรัฐอเมริกา

สหรัฐอเมริกานับว่าเป็นประเทศที่มีความเจริญก้าวหน้าทางเทคโนโลยีมากที่สุดแห่งหนึ่งของโลก ดังนั้นอาชญากรรมเกี่ยวกับเทคโนโลยีต่าง ๆ จึงเกิดขึ้นเป็นจำนวนมากเมื่อกฎหมายที่มีอยู่ไม่สามารถดำเนินคดีกับผู้กระทำผิดได้ ทำให้สหรัฐอเมริกาจำเป็นต้องมีการบัญญัติกฎหมายที่ดำเนินการทางกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ขึ้น กฎหมายสหรัฐอเมริกาที่ใช้ดำเนินคดีเกี่ยวกับอาชญากรรมคอมพิวเตอร์นั้นมีอยู่หลายฉบับ¹² เช่น

1. กฎหมายว่าด้วยการโกงและการกระทำที่เกี่ยวข้องกับเอกสารแสดงตัวตน การตรวจสอบคุณสมบัติ และข้อมูล¹³

2. กฎหมายว่าด้วยการโจรกรรมเอกลักษณ์ของบุคคลอย่างร้ายแรง¹⁴

3. กฎหมายว่าด้วยการโกงและการกระทำที่เกี่ยวข้องกับการเข้าถึงอุปกรณ์¹⁵

4. กฎหมายว่าด้วยการโกงและการกระทำความผิดเกี่ยวกับคอมพิวเตอร์¹⁶

5. กฎหมายว่าด้วยการโกงและการกระทำที่เกี่ยวข้องกับจดหมายอิเล็กทรอนิกส์¹⁷

6. กฎหมายว่าด้วยการโกงผ่านทางสายสัญญาณ วิทยุ และโทรทัศน์¹⁸

7. กฎหมายว่าด้วยการติดต่อสื่อสารผ่านสาย สถานี หรือระบบ¹⁹

8. กฎหมายว่าด้วยการนำเข้าหรือการขนส่งสื่อลามกอนาจาร²⁰

9. กฎหมายว่าด้วยการทำให้เข้าใจผิดเกี่ยวกับคำพูด หรือ ภาพดิจิทัลบนอินเทอร์เน็ต²¹

¹² CYBERCRIME LAWS OF THE UNITED STATES. Retrieved December 9, 2013, from www.oas.org

¹³ 18 U.S.C. § 1028 – Fraud and related activity in connection with identification documents, authentication features, and information.

¹⁴ 18 U.S.C. § 1028A – Aggravated identity theft.

¹⁵ 18 U.S.C. § 1029 – Fraud and related activity in connection with access devices.

¹⁶ 18 U.S.C. § 1030 – Fraud and related activity in connection with computers.

¹⁷ 18 U.S.C. § 1037 – Fraud and related activity in connection with electronic mail.

¹⁸ 18 U.S.C. § 1343 – Fraud by wire, radio, or television.

¹⁹ 18 U.S.C. § 1362 – Communications lines, stations, or systems.

²⁰ 18 U.S.C. § 1462 – Importation or transportation of obscene matters.

10. กฎหมายว่าด้วยสื่อสิ่งพิมพ์หรือการใช้การสื่อสารที่ไม่ได้รับอนุญาต²²

11. กฎหมายว่าด้วยการพนันบนอินเทอร์เน็ต ค.ศ. 2006²³

กฎหมายที่สำคัญที่เกี่ยวข้องกับความผิดเกี่ยวกับคอมพิวเตอร์ คือ The Computer Fraud and Abuse Act (CFAA) ถูกบัญญัติไว้ใน บรรพ 18 ของกฎหมายแห่งสหรัฐอเมริกา มาตรา 1030²⁴ โดยสภาองเกรสในปี ค.ศ. 1986 โดยมีการปรับปรุงแก้ไขให้ทันสมัยตลอดมา ซึ่งแต่เดิมกฎหมายฉบับนี้ไม่ได้มีจุดประสงค์มุ่งคุ้มครองคอมพิวเตอร์และระบบคอมพิวเตอร์ของประชาชนทั่วไป แต่มุ่งคุ้มครองคอมพิวเตอร์ของรัฐบาลหรือสถาบันการเงินเท่านั้น แต่ต่อมาได้มีการแก้ไขให้ครอบคลุมถึงคอมพิวเตอร์ของเอกชนด้วย และภายหลังเหตุการณ์ 11 กันยายน ค.ศ. 2001 ที่มีผู้ก่อการร้าย ก่อวินาศกรรมอาคารเวิลด์เทรด ในกรุงนิวยอร์ก และอาคารเพนตากอน ในกรุงวอชิงตัน ก็ได้ถูกแก้ไขโดยกฎหมายต่อต้านก่อการร้าย (Patriot Act)²⁵ ที่ให้อำนาจแก่เจ้าพนักงานในการตรวจสอบได้มากยิ่งขึ้นเพื่อเพิ่มประสิทธิภาพในการปราบปรามอาชญากรรม และถูกปรับปรุงแก้ไขโดย กฎหมายว่าด้วยการโจรกรรมเอกลักษณ์บุคคล ค.ศ. 2007 (Identity Theft Enforcement and Restitution Act) ให้ครอบคลุมการกระทำความผิดรวมถึงผู้สมรู้ร่วมคิดด้วย ซึ่งกฎหมายดังกล่าว มีสาระสำคัญดังนี้

1. ความผิดฐานเข้าถึงโดยไม่ปราศจากอำนาจและได้ไปซึ่งข้อมูลความมั่นคงของรัฐ มาตรา 1030 (a)(1)²⁶ บัญญัติไว้ว่า

²¹ 18 U.S.C. § 2252C – Misleading words or digital images on the Internet.

²² 47 U.S.C. § 605 – Unauthorized publication or use of communications.

²³ The Unlawful Internet Gambling Enforcement Act of 2006.

²⁴ 18 U.S.C. § 1030 – Fraud and related activity in connection with computers.

²⁵ Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

²⁶ (a) Whoever--(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to

(a) ผู้ใด

(1) โดยรู้ เข้าถึงคอมพิวเตอร์²⁷ โดยปราศจากอำนาจหรือเกินขอบอำนาจ²⁸ และด้วยวิธีการดังกล่าว ได้ไปซึ่งข้อมูลที่รัฐบาลสหรัฐอเมริกา มีคำสั่งของฝ่ายบริหารหรือกฎหมายลายลักษณ์อักษรกำหนดให้มีการคุ้มครองเพื่อป้องกันการเปิดเผยข้อมูลนั้น โดยปราศจากอำนาจเนื่องจากเหตุผลที่เกี่ยวกับความปลอดภัยของประเทศหรือเกี่ยวกับการต่างประเทศ หรือเป็นข้อมูลใด ๆ ที่มีความลับตามความหมายในย่อหน้า y ของมาตรา 11 แห่ง Atomic Energy Act of 1954 ซึ่งเป็นเหตุผลอันเชื่อได้ว่าข้อมูลที่ได้รับมานั้นอาจถูกนำไปใช้เพื่อสร้างความเสียหายให้กับสหรัฐอเมริกา หรือเพื่อให้เกิดประโยชน์ต่อรัฐอื่น โดยเจตนาติดต่อสื่อสาร ส่ง รับส่งข้อมูล หรือพยายามติดต่อสื่อสาร ส่ง รับส่งข้อมูล หรือถูกติดต่อสื่อสาร ถูกส่ง ถูกรับส่ง ข้อมูลดังกล่าวไปยังบุคคลใด ๆ ซึ่งไม่มีสิทธิได้รับข้อมูลนั้น หรือเจตนาเก็บข้อมูลนั้นไว้โดยไม่ยอมส่งข้อมูลดังกล่าวไปให้แก่เจ้าหน้าที่ของรัฐผู้มีสิทธิที่จะรับข้อมูลนั้น

receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it.

²⁷ คอมพิวเตอร์ (computer) มีนิยามไว้ใน CFAA มาตรา 1030 (e) (1) ว่า คอมพิวเตอร์หมายถึง เครื่องอิเล็กทรอนิกส์ แม่เหล็ก แสง หรือไฟฟ้าอิเล็กทรอนิกส์ หรือเครื่องที่มีกระบวนการคำนวณข้อมูลความเร็วสูง ที่แสดงถึงตรรกะ คณิตศาสตร์ หรือเก็บข้อมูล และรวมถึงเครื่องเก็บข้อมูลใด ๆ หรือเครื่องติดต่อสื่อสาร ที่สัมพันธ์โดยตรงหรือปฏิบัติการร่วมกันกับเครื่องมือเหล่านี้ แต่ไม่หมายความรวมถึง เครื่องพิมพ์ดีด หรือเครื่องเรียงพิมพ์ เครื่องคำนวณที่พกพา หรือเครื่องมืออื่นที่มีลักษณะเดียวกัน (the term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device).

²⁸ เกินขอบอำนาจ (Exceeds authorized access) มีนิยามไว้ใน CFAA มาตรา 1030 (e) (6) หมายถึง การเข้าสู่คอมพิวเตอร์โดยมีอำนาจและใช้การเข้าถึงนั้นเอาไป หรือเปลี่ยนแปลงข้อมูลในคอมพิวเตอร์นั้นซึ่งผู้เข้าถึงไม่มีสิทธิเอาไปหรือเปลี่ยนแปลง (the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter).

จะต้องถูกลงโทษตามอนุมาตรา (c) ของมาตรานี้

ตามบทบัญญัติดังกล่าว อาจกล่าวได้ว่าความผิดตาม CFAA มาตรา 1030 (a)(1) นั้น เป็นความผิดฐานเข้าถึงโดยปราศจากอำนาจและได้ไปซึ่งข้อมูลความมั่นคงของรัฐ สามารถแยกองค์ประกอบได้ ดังนี้²⁹

1. ผู้ใด โดยรู้ เข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจ
2. ได้ไปซึ่งข้อมูลรัฐบาลสหรัฐอเมริกา
3. มีเหตุผลอันเชื่อได้ว่าข้อมูลที่ได้รับมานั้นอาจถูกนำไปใช้เพื่อสร้างความเสียหายให้กับสหรัฐอเมริกา หรือเพื่อให้เกิดประโยชน์ต่อรัฐอื่น
4. โดยเจตนาติดต่อสื่อสาร ส่ง รับส่งข้อมูล (หรือพยายาม) หรือเจตนาเก็บข้อมูลนั้นไว้ โดยไม่ยอมส่งข้อมูลดังกล่าวไปให้แก่เจ้าหน้าที่ของรัฐผู้มีสิทธิที่จะรับข้อมูลนั้น ผู้กระทำความผิดตามมาตรานี้เป็นความผิดร้ายแรง โดยมีโทษปรับ หรือโทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(1)(A)³⁰ และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(1)(B)³¹

2. ความผิดฐานเข้าไปโดยปราศจากอำนาจและเอาไปซึ่งความลับ มาตรา 1030 (a)(2) บัญญัติไว้ว่า

(a) ผู้ใด

(2) โดยเจตนาเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจ และได้รับซึ่ง

(A) ข้อมูลทางการเงินของสถาบันการเงินหรือสถาบันที่ให้ผู้ยืมที่ถูกละเมิดไว้ใน มาตรา 1602 (n) ของหมวด 15 หรือข้อมูลซึ่งเก็บไว้ในแฟ้มข้อมูลของสำนักงานข้อมูลของ

²⁹ United States Department of Justice, Prosecuting Computer Crimes: Computer Fraud and Abuse Act [Online] Available from: www.cybercrime.gov [วันที่ 10 ธันวาคม 2556]

³⁰ The punishment for an offense under subsection (a) or (b) of this section is--(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph

³¹ The punishment for an offense under subsection (a) or (b) of this section is--(1) (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph

ผู้บริโภค ซึ่งมีข้อความอย่างเดียวกันกับที่กำหนดไว้ใน The Fair Credit Reporting Act (15 U.S.C.1681 et seq.);

(B) ข้อมูลจากหน่วยงานหรือตัวแทนใด ๆ ของสหรัฐอเมริกา หรือ

(C) ข้อมูลจากคอมพิวเตอร์ที่ถูกป้องกัน³²

จะต้องถูกลบโทษตามอนุมาตรา (c) ของมาตรานี้

ซึ่งความผิดฐานเข้าไปโดยปราศจากอำนาจและเอาไปซึ่งความลับ (มาตรา 1030 (a)(2)) อาจแยกองค์ประกอบได้ ดังนี้

1. โดยเจตนาเข้าถึงคอมพิวเตอร์

2. โดยปราศจากอำนาจหรือเกินขอบอำนาจ

3. ได้ไปซึ่งข้อมูลจาก

3.1 ข้อมูลทางการเงินจากสถาบันการเงินหรือสำนักงานข้อมูลของผู้บริโภค หรือ

3.2 ข้อมูลที่รัฐบาลหรือข้อมูลจากหน่วยงานหรือตัวแทนใด ๆ ของสหรัฐอเมริกา

หรือ

3.3 ข้อมูลจากคอมพิวเตอร์ที่ถูกป้องกัน

ผู้กระทำความผิดตามมาตรานี้เป็นความผิดไม่ร้ายแรง โดยมีโทษปรับ หรือโทษจำคุก ไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(2)(A)³³ ถ้าหากเพียงได้รับไปซึ่งข้อมูลที่มีค่าน้อยกว่า 5,000 เหรียญสหรัฐ เป็นความผิดไม่ร้ายแรงถ้าไม่กระทำความผิดอื่นอีก แต่การกระทำความผิดหรือพยายามกระทำความผิดตามมาตรานี้จะกลายเป็นความผิดร้ายแรง เมื่อ

(1) เป็นการกระทำเพื่อผลประโยชน์ทางการค้าหรือข้อมูลทางการเงินของสถาบันการเงินหรือสถาบันที่ใหู้ยืม

³² (a) Whoever--(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-- (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(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 (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer

³³ The punishment for an offense under subsection (a) or (b) of this section is-- (2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

(2) กระทำความผิดอาญาอื่นหรือละเมิดที่ฝ่าฝืนต่อรัฐธรรมนูญหรือกฎหมายมลรัฐ หรือ

(3) ได้ไปซึ่งข้อมูลที่มีค่ามากกว่า 5,000 เหรียญสหรัฐ

ในกรณีดังกล่าวก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(2)(B)³⁴

3. ความผิดฐานบุกรุกเข้าไปในคอมพิวเตอร์ของรัฐ มาตรา 1030 (a)(3) บัญญัติไว้ว่า

(a) ผู้ใด

(3) โดยเจตนาเข้าถึงคอมพิวเตอร์ที่ไม่ได้มีไว้เพื่อการสาธารณะของหน่วยงาน หรือตัวแทนของสหรัฐอเมริกาโดยปราศจากอำนาจ ซึ่งคอมพิวเตอร์ของหน่วยงานหรือตัวแทนนั้น มีไว้เพื่อการใช้งานสำหรับรัฐบาลสหรัฐอเมริกาโดยเฉพาะ หรือในกรณีที่คอมพิวเตอร์ไม่ได้ถูกใช้งานสำหรับรัฐบาลสหรัฐอเมริกาโดยเฉพาะแต่ถูกใช้งานโดยหรือสำหรับรัฐบาลสหรัฐอเมริกา และการกระทำความผิดดังกล่าวส่งผลกระทบต่อการใช้งานของรัฐบาลสหรัฐอเมริกาหรือการใช้งานสำหรับสหรัฐอเมริกา³⁵

จะต้องถูกลงโทษตามอนุมาตรา (c) ของมาตรานี้

ความผิดฐานบุกรุกเข้าไปในคอมพิวเตอร์ของรัฐ (มาตรา 1030 (a)(3)) อาจแยกองค์ประกอบได้ ดังนี้

³⁴ The punishment for an offense under subsection (a) or (b) of this section is--(2) (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$5,000.

³⁵ (a) Whoever--(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States.

1. เจตนาเข้าถึง
 2. โดยปราศจากอำนาจ
 3. คอมพิวเตอร์ที่ไม่ได้มีไว้เพื่อการสาธารณะของสหรัฐอเมริกาซึ่งใช้งานหรือถูกใช้งานโดยหรือสำหรับรัฐบาลสหรัฐอเมริกาโดยเฉพาะ
 4. ส่งผลกระทบต่อการใช้คอมพิวเตอร์ของสหรัฐอเมริกา
- ผู้กระทำความผิดตามมาตรา³⁶ นี้ มีโทษปรับ หรือโทษจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(2)(A)³⁶ และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(2)(C)³⁷
4. ความผิดฐานเข้าถึงคอมพิวเตอร์เพื่อฉ้อโกง ตามมาตรา 1030 (a)(4) บัญญัติไว้ว่า
 - (a) ผู้ใด
 - (4) โดยรู้และตั้งใจฉ้อโกง เข้าถึงคอมพิวเตอร์ที่มีการป้องกัน³⁸ โดยไม่มีอำนาจหรือเกินขอบอำนาจ และกระทำการต่อไปโดยตั้งใจฉ้อโกงและได้รับไปซึ่งสิ่งที่มีค่าใด ๆ เว้นแต่

³⁶ (c) The punishment for an offense under subsection (a) or (b) of this section is— (2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

³⁷ (c) The punishment for an offense under subsection (a) or (b) of this section is—(2)(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

³⁸ คอมพิวเตอร์ที่มีการป้องกัน (protected computer) มีนิยามไว้ใน CFAA มาตรา 1030 (e) (2) ว่า คอมพิวเตอร์ที่ (A) ใช้โดยเฉพาะในสถาบันการเงินหรือรัฐบาลของสหรัฐอเมริกา หรือในกรณีที่คอมพิวเตอร์ไม่ได้ใช้ในกรณีดังกล่าว ถูกใช้หรือสำหรับสถาบันการเงินหรือรัฐบาลของสหรัฐอเมริกา และมีผลเป็นความผิดในการใช้หรือสำหรับสถาบันการเงิน หรือรัฐบาลของสหรัฐอเมริกา (B) ซึ่งถูกใช้ในการค้าพาณิชย์หรือติดต่อสื่อสารระหว่างมลรัฐหรือ ระหว่างประเทศ รวมถึงคอมพิวเตอร์ที่ตั้งอยู่นอกประเทศสหรัฐอเมริกาซึ่งถูกใช้จัดการในการค้าพาณิชย์หรือติดต่อสื่อสารระหว่างมลรัฐหรือระหว่างประเทศของสหรัฐอเมริกา ((2) the term "protected computer" means a computer--(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or(B) which is used in interstate or foreign commerce or communication,

วัตถุของการฉ้อโกงและสิ่งของที่ได้มา รวมเฉพาะการใช้คอมพิวเตอร์และมูลค่าของการใช้ดังกล่าว นั้นไม่เกิน 5,000 เหรียญสหรัฐในช่วงเวลาหนึ่งปี³⁹

จะต้องถูกลงโทษตามอนุมาตรา (c) ของมาตรานี้

โดยความผิดฐานเข้าถึงคอมพิวเตอร์เพื่อฉ้อโกง (มาตรา 1030 (a)(4)) อาจแยกองค์ประกอบได้ ดังนี้

1. เข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจซึ่งคอมพิวเตอร์ที่มีการป้องกันโดยรู้
2. ตั้งใจที่จะฉ้อโกง
3. เข้าถึงต่อไปเพื่อตั้งใจจะฉ้อโกง
4. ได้รับบางสิ่งที่มีมูลค่า รวมถึงการใช้ ถ้ามีมูลค่าเกิน 5,000 เหรียญดอลลาร์สหรัฐ

ผู้กระทำความผิดตามมาตรานี้ มีโทษปรับ หรือโทษจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030(c)(3)(A)⁴⁰ และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(3)(B)⁴¹

5. ความผิดฐานส่งหรือเข้าถึงทำให้เกิดความเสียหาย ตามมาตรา 1030 (a)(5)(A), (B) และ (C) บัญญัติไว้ว่า⁴²

including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States).

³⁹ Whoever--(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period.

⁴⁰ (c)The punishment for an offense under subsection (a) or (b) of this section is— (3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

⁴¹ (c)The punishment for an offense under subsection (a) or (b) of this section is— (3)(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),3 or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

⁴² (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;

(a) ผู้ใด

(5) (A) โดยรู้ทำให้เกิดการส่งโปรแกรม ข้อมูล รหัส หรือคำสั่งและการกระทำดังกล่าวเจตนาทำให้เกิดความเสียหายต่อคอมพิวเตอร์ที่ได้รับการป้องกันโดยปราศจากอำนาจ

(B) เจตนาเข้าถึงคอมพิวเตอร์ที่ได้รับการป้องกันโดยปราศจากอำนาจ และจากการกระทำดังกล่าวทำให้เกิดความเสียหายโดยประมาทโดยรู้ตัว⁴³ (Reckless) หรือ

(C) เจตนาเข้าถึงคอมพิวเตอร์ที่ได้รับการป้องกันโดยปราศจากอำนาจ และจากการกระทำดังกล่าวทำให้เกิดความเสียหาย

มาตรา 1030(c)(4)(A) และ (B) ยังได้บัญญัติความคิดเพื่อลงโทษผู้กระทำความผิดหนักขึ้นไว้ว่าหากการกระทำความผิดตามข้อ (A)(B) ของ (a)(5) ทำให้เกิด (หรือในกรณีที่เป็นการพยายามกระทำความผิด ถ้าความผิดนั้นได้กระทำสำเร็จจนเป็นเหตุให้เกิด)

(I) ความเสียหายต่อบุคคลหนึ่งหรือมากกว่าในช่วงเวลาหนึ่งปี (และสำหรับจุดประสงค์ในการสอบสวน คำวินิจฉัย หรือ กระบวนการพิจารณาอื่นโดยรัฐ ทำให้เกิดความเสียหายที่เกี่ยวข้องกับการกระทำดังกล่าวสำหรับคอมพิวเตอร์ที่ถูกป้องกันหนึ่งเครื่องหรือมากกว่า) เป็นเงินรวมกันไม่น้อยกว่า 5,000 เหรียญสหรัฐ

(II) การแก้ไขเปลี่ยนแปลงหรือการทำให้เกิดความเสียหายต่อผลทดสอบทางการแพทย์ คำวินิจฉัยทางการแพทย์ การรักษาพยาบาลหรืออนามัยของบุคคลหนึ่ง หรือมากกว่า

(III) การทำให้ผู้ใดได้รับบาดเจ็บทางร่างกาย

(IV) การข่มขู่จะทำให้เกิดอันตรายต่อสุขภาพและอนามัยของสาธารณะ

(V) ความเสียหายซึ่งส่งผลกระทบต่อระบบคอมพิวเตอร์ซึ่งถูกใช้โดยหรือสำหรับหน่วยงานของรัฐในการบริหารงานยุติธรรมการทหาร หรือความมั่นคงของชาติ

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

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

⁴³ ประมาทโดยรู้ตัว (Recklessness) เป็นสถานะทางจิตอย่างหนึ่งที่ผู้กระทำไม่เพียงแต่ขาดความระมัดระวังเท่านั้น แต่ได้กระทำไปโดยเจตนาไม่นำพาต่อเหตุการณ์ที่จะเกิดขึ้นกล่าวคือได้กระทำโดยรู้สีกอยู่แล้วว่าเป็นการเสี่ยงที่จะเกิดภัย แต่ยังไม่คำนึงถึง บางครั้งจึงมีผู้เรียกลักษณะของสถานะแห่งจิตเช่นนี้ว่า ประมาทโดยจงใจ (advertent negligence) คือจงใจทำแต่ไม่แน่ใจว่าจะเกิดผล บางทีก็เรียกว่าเป็น willfull negligence ซึ่งเรื่องนี้ศาลเคยวินิจฉัยไว้ในคดี R.V.Bateman (1925) ว่า ประมาทประเภทนี้ต้องถึงขนาดที่ลูกขุนเห็นว่าจะเพียงพอให้ใช้ค่าเสียหายกันยังไม่พอ เพราะเป็นความไม่นำพาต่อความปลอดภัยของผู้อื่นอันควรต้องรับผิดชอบในทางอาญา.

(VI) ความเสียหายส่งผลกระทบต่อคอมพิวเตอร์ที่มีการป้องกัน สิบเครื่องหรือ มากกว่า ในช่วงเวลาหนึ่งปี⁴⁴

องค์ประกอบความผิดฐานเข้าถึงทำให้เกิดความเสียหาย ตามมาตรา 1030 (a)(5)(A) ดังนี้

1. ผู้ใด โดยรู้ทำให้เกิดการส่งโปรแกรม ข้อมูล รหัส หรือคำสั่งและการกระทำได้กล่าว เจตนา

2. ทำให้เกิดความเสียหายต่อคอมพิวเตอร์ที่ได้รับการป้องกันโดยปราศจากอำนาจ

ผู้กระทำความผิดตามมาตรา 1030 (a)(5)(A) มีโทษปรับ หรือโทษจำคุกไม่เกิน 1 ปี หรือ ทั้งจำทั้งปรับตามมาตรา 1030 (c)(4)(G)⁴⁵ หากไม่เคยกระทำความผิดตามมาตรา 1030 มาก่อน ถ้าการ กระทำมีผลตามข้อ (I)-(VI) ในย่อหน้า (A)(i) จะถูกลงโทษปรับและจำคุกไม่เกิน 10 ปี ตามมาตรา

⁴⁴ (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period.

⁴⁵ The punishment for an offense under subsection (a) or (b) of this section is— (4)(G) a fine under this title, imprisonment for not more than 1 year, or both, for— (i) any other offense under subsection (a)(5); or (ii) an attempt to commit an offense punishable under this subparagraph.

1030 (c)(4)(B)⁴⁶ และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือ โทษจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ ตาม มาตรา 1030 (c)(4)(C)⁴⁷

ความผิดตามมาตรา 1030 (a)(5)(A) นั้น ได้มีการบัญญัติครอบคลุมไปถึงการกระทำที่มีผลต่อชีวิตหรือร่างกายของผู้อื่นด้วย เพื่อให้ผู้กระทำความผิดต้องรับโทษหนักขึ้นด้วย หากการกระทำไม่ว่าจะอยู่ในชั้นพยายาม กระทำโดยมีเจตนา หรือประมาทโดยรู้ตัวก็ตาม เป็นเหตุให้มีผู้ได้รับบาดเจ็บสาหัส จะถูกลงโทษปรับและจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(4)(E)⁴⁸ และหากการกระทำนั้นเป็นเหตุให้ผู้อื่นถึงแก่ความตาย จะถูกลงโทษปรับจำคุกอย่างสูงถึงตลอดชีวิต หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(4)(F)⁴⁹

ความผิดฐานเข้าถึงทำให้เกิดความเสียหาย ตามมาตรา 1030 (a)(5)(B) และ มาตรา 1030 (a)(5)(C) นั้นองค์ประกอบคล้ายคลึงกัน ซึ่งทั้ง (B) และ (C) มีองค์ประกอบแตกต่างกันเพียงชั้นของเจตนา จึงสามารถแยกองค์ประกอบ โดยรวมได้ ดังนี้

1. เจตนาเข้าถึงคอมพิวเตอร์ที่ได้รับการป้องกันโดยปราศจากอำนาจ
2. ทำให้เกิดความเสียหาย (1030 (a)(5)(C)) หรือ ประมาทโดยรู้ตัวเป็นเหตุให้เกิดความเสียหาย (1030 (a)(5)(B))

⁴⁶ The punishment for an offense under subsection (a) or (b) of this section is— (4)(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of— (i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii) an attempt to commit an offense punishable under this subparagraph.

⁴⁷ The punishment for an offense under subsection (a) or (b) of this section is— (4)(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of— (i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph.

⁴⁸ The punishment for an offense under subsection (a) or (b) of this section is— (4)(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both.

⁴⁹ The punishment for an offense under subsection (a) or (b) of this section is— (4)(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both.

ผู้กระทำความผิดตามมาตรา 1030 (a)(5)(B) มีโทษปรับ หรือโทษจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับตามมาตรา 1030 (c)(4)(G) หากไม่เคยกระทำความผิดตามมาตรา 1030 มาก่อน ถ้าการกระทำมีผลตามข้อ (I)-(VI) ในย่อหน้า (A)(i) จะถูกลงโทษปรับและจำคุกไม่เกิน 5 ปี ตามมาตรา 1030 (c)(4)(A) และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ ตาม มาตรา 1030 (c)(4)(C)

ผู้กระทำความผิดตามมาตรา 1030 (a)(5)(C) มีโทษปรับ หรือโทษจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับตามมาตรา 1030 (c)(4)(G) และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ตาม มาตรา 1030 (c)(4)(D)⁵⁰

6. ความผิดฐานลักลอบค้ารหัสผ่าน ตามมาตรา 1030 (a)(6)⁵¹ บัญญัติไว้ว่า

(a) ผู้ใด

(6) โดยรู้ และตั้งใจถือโกง ลักลอบค้า (ตามที่ระบุไว้ในมาตรา 1029) รหัสผ่าน หรือข้อมูลที่คล้ายคลึงกัน ซึ่งใช้สำหรับการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ ถ้า

(A) การค้าดังกล่าวมีผลกระทบต่อการค้าระหว่างมลรัฐหรือ ระหว่างประเทศ หรือ

(B) ระบบคอมพิวเตอร์ดังกล่าวถูกใช้โดยหรือสำหรับรัฐบาลสหรัฐอเมริกา จะต้องถูกลงโทษตามอนุมาตรา (c) ของมาตรานี้

ความผิดฐานลักลอบค้ารหัสผ่าน (มาตรา 1030 (a)(6)) สามารถแยกองค์ประกอบได้ดังนี้

1. ขาดรหัสผ่าน หรือ ข้อมูลที่คล้ายคลึงกัน ที่ใช้สำหรับการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ

2. โดยรู้และตั้งใจที่จะถือโกง ลักลอบค้า

⁵⁰ The punishment for an offense under subsection (a) or (b) of this section is— (4)(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph.

⁵¹ (a) Whoever— (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States.

3. มีผลกระทบต่อการค้าระหว่างมลรัฐหรือระหว่างประเทศ หรือ ระบบคอมพิวเตอร์ดังกล่าวถูกใช้โดยหรือสำหรับรัฐบาลสหรัฐอเมริกา

ผู้กระทำความผิดตามมาตรา 1030 (c)(2)(A)⁵² และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(2)(C)⁵³

7. ความผิดฐานข่มขู่ต่อคอมพิวเตอร์ที่มีการป้องกัน ตามมาตรา 1030 (a)(7)⁵⁴ บัญญัติไว้ว่า

(a) ผู้ใด

(7) โดยตั้งใจ ข่มขู่ บุคคลใด ทรัพย์สินใด ๆ หรือ สิ่งอื่นใดที่มีมูลค่า ถ้ายทอดลงในการค้าระหว่างมลรัฐหรือระหว่างประเทศ การสื่อสารใด ๆ เพื่อ

(A) คุกคาม ทำให้เกิดอันตรายต่อคอมพิวเตอร์ที่มีการป้องกัน

(B) คุกคาม ให้ได้รับข้อมูลจากคอมพิวเตอร์ที่มีการป้องกัน โดยไม่มีอำนาจหรือเกินขอบอำนาจ หรือ ทำอันตรายต่อข้อมูลที่เป็นความลับที่ได้มาจากการเข้าถึงคอมพิวเตอร์ที่มีการป้องกันโดยไม่มีอำนาจหรือเกินขอบอำนาจ หรือ

⁵² The punishment for an offense under subsection (a) or (b) of this section is— (2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

⁵³ The punishment for an offense under subsection (a) or (b) of this section is— (2) (C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

⁵⁴ (a) Whoever— (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.

(C) เรียกหรือได้มาซึ่งเงินหรือทรัพย์สินอื่นใด จากการที่จะทำอันตรายต่อคอมพิวเตอร์ที่มีการป้องกัน หรือจากการขู่เช่นนั้น

จะต้องถูกลงโทษตามอนุมาตรา (c) ของมาตรานี้

ความผิดฐานข่มขู่ต่อคอมพิวเตอร์ที่มีการป้องกัน (มาตรา 1030 (a)(7)) สามารถแยกองค์ประกอบได้ดังนี้

1. เจตนาข่มขู่

2. ข่มขู่ต่อ บุคคลใด ทรัพย์สินใด ๆ หรือ สิ่งอื่นใดที่มีมูลค่า ถ่ายทอดลงในการค้าระหว่างมลรัฐหรือระหว่างประเทศ การสื่อสารใด ๆ เพื่อ

3. การข่มขู่กระทำเพื่อ

3.1 คุกคาม ทำให้เกิดอันตรายต่อคอมพิวเตอร์ที่มีการป้องกัน

3.2 คุกคาม ให้ได้รับข้อมูลจากคอมพิวเตอร์ที่มีการป้องกันโดยไม่มีอำนาจหรือเกินขอบอำนาจ หรือ ทำอันตรายต่อข้อมูลที่เป็นความลับที่ได้มาจากการเข้าถึงคอมพิวเตอร์ที่มีการป้องกันโดยไม่มีอำนาจหรือเกินขอบอำนาจ หรือ

3.3 เรียกหรือได้มาซึ่งเงินหรือทรัพย์สินอื่นใด จากการที่จะทำอันตรายต่อคอมพิวเตอร์ที่มีการป้องกัน หรือจากการขู่เช่นนั้น

ผู้กระทำความผิดตามมาตรานี้ มีโทษปรับหรือโทษจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(3)(A)⁵⁵ และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(3)(B)⁵⁶

3.3.2 สหพันธ์สาธารณรัฐเยอรมนี

สหพันธ์สาธารณรัฐเยอรมนีเป็นประเทศหนึ่งที่ทำให้ความสำคัญกับปัญหาการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งการกระทำความผิดดังกล่าว นับวันได้เพิ่มขึ้นอย่างต่อเนื่อง โดยเยอรมันได้รับมือกับอาชญากรรมทางคอมพิวเตอร์โดยการแก้ไขเพิ่มเติมประมวลกฎหมายอาญา

⁵⁵ The punishment for an offense under subsection (a) or (b) of this section is— (3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

⁵⁶ The punishment for an offense under subsection (a) or (b) of this section is— (3)(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),3 or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

(StGB) มีบทบัญญัติที่กำหนดฐานความผิดพิเศษเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ไว้ โดยเฉพาะ รวมทั้งบทบัญญัติที่สามารถนำมาปรับใช้กับการกระทำความผิดที่อาศัยคอมพิวเตอร์เป็นเครื่องมือ ดังนี้⁵⁷

มาตรา 202a การเข้าสู่ช่องทางการเข้าถึงข้อมูลโดยมิชอบ (Ausspähen von Daten)

(1) ผู้ใดกระทำการโดยไม่มีอำนาจ เพื่อเข้าสู่ช่องทางการเข้าถึงข้อมูล ที่มิได้มีไว้สำหรับตน และเป็นช่องทางที่มีมาตรการรักษาความปลอดภัยโดยเฉพาะ ด้วยการฝ่าฝืนระบบรักษาความปลอดภัยนั้น ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือมีโทษปรับ

(2) ข้อมูลตามบทบัญญัติในวรรคแรก หมายถึง ข้อมูลที่มีการบันทึก หรือส่งผ่านไว้กันโดยวิธีทางอิเล็กทรอนิกส์ ด้วยแม่เหล็กไฟฟ้าหรือวิธีใด ๆ ที่ไม่สามารถมองเห็นด้วยตาเปล่า

มาตรา 202b การดักข้อมูล (Abfangen von Daten)

ผู้ใดกระทำโดยไม่มีอำนาจ โดยอาศัยวิธีทางเทคนิค ดักจับข้อมูลที่ไม่ได้มีไว้เพื่อตน ซึ่งอยู่ในระหว่างการสื่อสารที่ไม่ได้เปิดเผยต่อสาธารณะ หรือดักข้อมูลที่บันทึกอยู่ในระบบประมวลผลข้อมูลโดยวิธีการแพร่ของรังสีแม่เหล็กไฟฟ้า ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับ ในกรณีที่การกระทำนี้ไม่ได้ถูกลงโทษหนักกว่าโดยบทบัญญัติอื่น

มาตรา 303a การแก้ไขเปลี่ยนแปลงข้อมูล (Datenveränderung)

(1) ผู้ใด โดยไม่ชอบด้วยกฎหมาย ลบ ปิดกั้นการทำงาน ทำให้ใช้ประโยชน์ไม่ได้ หรือแก้ไขเปลี่ยนแปลงข้อมูล (ตามกฎหมายที่บัญญัติไว้ในมาตรา 202a(2)) ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับ

(2) การพยายามกระทำความผิดตามมาตรา 303a ต้องได้รับโทษ

(3) การเตรียมการกระทำความผิดตาม (1) เป็นการกระทำความผิดตามมาตรา 202

มาตรา 303b การก่อวินาศกรรมคอมพิวเตอร์ (Computersabotage)

(1) ผู้ใดกระทำการรบกวนอย่างสำคัญ ต่อการประมวลผลข้อมูลที่มีความสำคัญต่อบุคคลอื่น โดยวิธีการ

1. แก้ไขเปลี่ยนแปลงข้อมูลตาม มาตรา 303a StGB

2. นำเข้าสู่ หรือส่งผ่านสู่ระบบซึ่งข้อมูล (ตามความหมายในมาตรา 202a(2) StGB) เพื่อให้เกิดความเสียหายใด ๆ ต่อบุคคลอื่น หรือ

⁵⁷ สาวตรี สุขตรี. (2556). “อาชญากรรมคอมพิวเตอร์/อินเทอร์เน็ต ตามกฎหมายอาญาเยอรมัน.” วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 42(3). น. 499-532.

3. ด้วยการทำลาย ทำให้เสียหาย ทำให้เสื่อมประโยชน์ โยกย้าย หรือแก้ไข เปลี่ยนแปลงระบบการประมวลผลข้อมูล หรือสิ่งซึ่งให้นำส่งข้อมูลนั้น

ต้องระวางโทษจำคุกไม่เกินสามปี หรือ มีโทษปรับ

(2) ถ้าเป็นการกระทำความผิดต่อการประมวลผลข้อมูลที่มีความสำคัญต่อองค์กรธุรกิจ บริษัทเอกชน หรือหน่วยงานของรัฐ ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือโทษปรับ

(3) การพยายามกระทำความผิดตามมาตรา 262 ต้องได้รับโทษ

(4) การกระทำความผิดระบบประมวลผลใน (2) จะต้องรับโทษหนักขึ้นอีก กล่าวคือ ระวางโทษจำคุกตั้งแต่ 6 เดือน แต่ไม่เกิน 10 ปี หากผู้กระทำ

1. ก่อให้เกิดความเสียหายต่อทรัพย์สินจำนวนมาก

2. กระทำเป็นอาชีพหรือเป็นสมาชิกขององค์กรที่ตั้งขึ้นเพื่อก่อวินาศกรรม คอมพิวเตอร์อย่างต่อเนื่อง

3. กระทบ หรือทำลายสาธารณูปโภคของประชาชน การบริการสาธารณะ และระบบรักษาความปลอดภัยของสหพันธรัฐเยอรมนี

(5) การเตรียมการกระทำความผิดตามมาตรา (1) เป็นการกระทำความผิดตามมาตรา 202c StGB

มาตรา 269 การปลอมแปลงข้อมูลซึ่งเป็นพยานหลักฐาน (Fälschung beweiserheblicher Daten)

ผู้ใดโดยฉ้อฉลต่อกฎหมาย ทำการบันทึก หรือแก้ไขเปลี่ยนแปลงข้อมูลที่เป็นพยานหลักฐาน เพื่อให้ผู้อื่นหลงเชื่อว่าเอกสารเท็จ หรือเอกสารปลอมนั้นมีอยู่ หรือเพื่อใช้ประโยชน์จากข้อมูลที่ได้บันทึก หรือเปลี่ยนแปลงนั้น ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับ

การพยายามกระทำความผิดตามมาตรา 269 ผู้กระทำอาจต้องรับโทษด้วย

มาตรา 263a การฉ้อโกงทางคอมพิวเตอร์ (Computerbetrug)

(1) ผู้ใดโดยเจตนา เพื่อให้ตนเองหรือผู้อื่นได้ประโยชน์ในทางทรัพย์สินโดยไม่ชอบด้วยกฎหมาย และทำให้ทรัพย์สินของผู้อื่นได้รับความเสียหาย ด้วยการกระทำที่แสดงจากการประมวลผลเป็นไปตามความต้องการของตน โดยใช้โปรแกรมที่มีการจัดการไม่ถูกต้อง โดยใช้ข้อมูลที่ไม่ถูกต้องหรือไม่ครบถ้วนสมบูรณ์ โดยใช้ข้อมูลโดยไม่มีอำนาจ หรือโดยประการอื่นใดโดยไม่ได้รับอนุญาต ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับ

(2) ให้นำมาตรา 263 วรรค 2 ถึง 7 มาใช้บังคับกับการกระทำความผิดตามวรรคแรก โดยอนุโลม

(3) ผู้ใดเตรียมการที่จะกระทำความผิดตาม (1) โดยการเขียนโปรแกรม คอมพิวเตอร์เพื่อจะกระทำความผิด หรือจัดหาโปรแกรมดังกล่าวเพื่อตนเองหรือผู้อื่น เสนอเพื่อที่จะ ขาย ครอบครอง หรือ จัดหาโปรแกรมเหล่านั้นให้ผู้อื่น ต้องระวางโทษไม่เกิน 3 ปี หรือปรับ

(4) กรณีตาม (3) ให้นำมาตรา 149(2) ถึง (3) มาบังคับใช้โดยอนุโลม

จากหลักกฎหมายข้างต้น เห็นว่าเยอรมันได้บัญญัติความผิดการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ไว้ในประมวลกฎหมายอาญา ซึ่งแตกต่างกับประเทศอื่น ๆ ที่มักจะบัญญัติความผิด เกี่ยวกับคอมพิวเตอร์แยกออกมาจากประมวลกฎหมายอาญาโดยการบัญญัติเป็นพระราชบัญญัติไว้ เป็นการเฉพาะ

3.3.3 สาธารณรัฐจีน (ไต้หวัน)

ไต้หวันเป็นศูนย์กลางทางการเงินของภูมิภาค มีภาคธุรกิจทางการเงินที่ทันสมัย เป็นที่ตั้งของเส้นทางการจัดส่งสินค้าระหว่างประเทศ เชี่ยวชาญในด้านเทคโนโลยีขั้นสูง จึงมีการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์เกิดขึ้นจำนวนมาก และนับวันการกระทำความผิดก็เพิ่มขึ้น อย่างต่อเนื่อง จึงให้ความสำคัญกับปัญหาการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มีการรับมือกับ อาชญากรรมทางคอมพิวเตอร์โดยการบัญญัติเพิ่มเติมไว้ในประมวลกฎหมายอาญา ดังนี้⁵⁸

มาตรา 358 ผู้ใดโดยไม่มีเหตุอันสมควร ใช้บัญชีผู้ใช้และรหัสผ่านของผู้อื่น ทำลายการ ป้องกันของคอมพิวเตอร์ หรือใช้ประโยชน์จากช่องโหว่ในระบบ เช่น การเข้าถึงระบบคอมพิวเตอร์ ของผู้อื่นหรืออุปกรณ์ที่เกี่ยวข้อง ต้องระวางโทษจำคุกไม่เกินสามปี และอาจมีโทษปรับไม่เกินหนึ่ง แสนหยวน⁵⁹

มาตรา 359 ผู้ใดไม่มีเหตุอันสมควร ได้รับ ลบ หรือเปลี่ยนแปลง บันทึกแม่เหล็กของ คอมพิวเตอร์ของผู้อื่นหรืออุปกรณ์ที่เกี่ยวข้อง และทำให้ประชาชนหรือผู้อื่นเสียหาย ต้องระวาง โทษจำคุกไม่เกินห้าปี และอาจมีโทษปรับไม่เกินสองแสนหยวน⁶⁰

⁵⁸ Criminal Code of the Republic of China: Chapter 36 Offenses Against the Computer Security.

⁵⁹ Article 358 A person who without reason by entering another's account code and password, breaking his computer protection, or taking advantage of the system loophole of such other accesses his computer or relating equipment shall be sentenced to imprisonment for not more than three years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than one hundred thousand yuan may be imposed.

⁶⁰ Article 359 A person without reason obtains, deletes or alters the magnetic record of another's computer or relating equipment and causes injury to the public or others shall be sentenced to imprisonment of

หรือวิธีการทางแม่เหล็กอื่น ๆ ต่อคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องของผู้อื่น และทำให้ประชาชนหรือผู้อื่นเสียหาย ต้องระวางโทษจำคุกไม่เกินสามปี และอาจำมีโทษปรับไม่เกินหนึ่งแสนหยวน⁶¹

มาตรา 361 ผู้ใดกระทำความผิดตามสามมาตราก่อน กับคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องของสาธารณะสถานต้องระวางโทษเพิ่มขึ้นอีกกึ่งหนึ่ง⁶²

มาตรา 362 ผู้ใดสร้างโปรแกรมคอมพิวเตอร์สำหรับตนเองหรือผู้อื่นเพื่อกระทำความผิดตามหมวดนี้และทำให้ประชาชนหรือผู้อื่นเสียหาย ต้องระวางโทษจำคุกไม่เกินห้าปี และอาจำมีโทษปรับไม่เกินสองแสนหยวน⁶³

มาตรา 363 ความผิดตามมาตรา 358-360 จะดำเนินคดีได้เมื่อมีการแจ้งความ⁶⁴

จากหลักกฎหมายในข้างต้น เห็นว่าได้หวั่นได้บัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์รวมไว้ในประมวลกฎหมายอาญาเช่นเดียวกับสหพันธ์สาธารณรัฐเยอรมนีโดยมีการบัญญัติไว้ครอบคลุมการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ทั่วไปแล้ว

no more than five years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than two hundred thousand yuan may be imposed.

⁶¹ Article 360 A person who without reason interferes, through the use of computer programs or other electromagnetic methods, with the computer or relating equipment of another person and causes injury to the public or another shall be sentenced to imprisonment for not more than three years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than one hundred thousand yuan may be imposed.

⁶² Article 361 A person who commits the offenses specified in the three preceding articles against the computers and relating equipment of a public office shall be punished by increasing the punishment up to one half.

⁶³ Article 362 A person who makes computer programs specifically for himself or another to commit the offenses specified in this Chapter and causes injury to the public or another shall be punished for imprisonment for not more than five years or short-term imprisonment; in lieu thereof, or in addition thereto, a fine of not more than two hundred thousand yuan may be imposed.

⁶⁴ Article 363 The prosecution of the offenses specified in articles, 358 through 360, may be instituted only upon complaint.