# มาตรการทางกฎหมายของ สปป.ลาว ในการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์

# LEGAL MEASURES OF LAO PDR FOR THE PROTECTION RELATED TO COMPUTER CRIME

เกมอุรา ไชยวงศ์

นิติศาสตรมหาบัณฑิต

สำนักวิชานิติศาสตร์
มหาวิทยาลัยแม่ฟ้าหลวง
2558

# มาตรการทางกฎหมายของ สปป.ลาว ในการคุ้มครอง และป้องกันอาชญากรรมทางคอมพิวเตอร์

# LEGAL MEASURES OF LAO PDR FOR THE PROTECTION RELATED TO COMPUTER CRIME

เกมอุรา ไชยวงศ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

สำนักวิชานิติศาสตร์
มหาวิทยาลัยแม่ฟ้าหลวง
2558

# มาตรการทางกฎหมายของ สปป.ลาว ในการคุ้มครอง และป้องกันอาชญากรรมทางคอมพิวเตอร์

# LEGAL MEASURES OF LAO PDR FOR THE PROTECTION RELATED TO COMPUTER CRIME

เกมอุรา ไชยวงศ์

วิทยานิพนธ์นี้ได้รับการพิจารณาอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
2558

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(ศาสตราจารย์ วีระพงษ์ บุญโญภาส)

.....อาจารย์ที่ปรึกษา
(ดร. ชูเกียรติ น้อยฉิม)

.....กรรมการ
(ดร. ณัฐกร วิทิตานนท์)

.....กรรมการภายนอกมหาวิทยาลัย
(ดร. อรดา เทพยายน)

# กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลงได้อย่างสมบูรณ์โดยได้รับความกรุณาและช่วยเหลือจาก อาจารย์ ดร. ชูเกียรติ น้อยฉิม ที่ได้เสียสละเวลาอันมีค่าในการรับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ พร้อมทั้งรับฟังและแนะนำข้อคิดเห็นต่าง ๆ ในทางวิชาการให้แก่ผู้เขียนเป็นอย่างดี ทั้งยังได้ตรวจทานแก้ไขเนื้อหาในวิทยานิพนธ์ตั้งแต่ต้นจนสำเร็จ ซึ่งผู้เขียนขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณ ศาสตราจารย์ วีระพงษ์ บุญโญภาส ดร. ณัฐกร วิทิตานนท์ และดร. อรดา เทพยายน เป็นอย่างสูง ที่เสียสละเวลาอันมีค่าให้เกียรติเป็นประธานและคณะกรรมการสอบวิทยานิพนธ์ ตลอดจนให้คำแนะนำต่าง ๆ ที่เป็นประโยชน์เพื่อให้วิทยานิพนธ์ฉบับนี้มีความสมบูรณ์มากยิ่งขึ้น

ขอขอบคุณ ว่าที่ร้อยตรี สมพร รุจิกิตติอังศุธร และอาจารย์ วรณัฐ บุญเจริญ มิตรที่ได้ให้คำแนะนำข้อมูลทางด้านวิชาการ ตรวจทานเนื้อหา และภาษาในเบื้องต้น และขอขอบคุณเจ้าหน้าที่ประจำสำนักวิชานิติศาสตร์ สำนักงานบัณฑิตศึกษา และส่วนอื่น ๆ ของมหาวิทยาลัยแม่ฟ้าหลวง ที่ได้อำนวยความสะดวกในการจัดทำวิทยานิพนธ์เล่มนี้ ขอบคุณเจ้าหน้าที่กระทรวงยุติธรรม กระทรวงไปรษณีย์ โทรคมนาคมและการสื่อสาร ศาลประชาชน อัยการประชาชนแห่ง สปป.ลาว และขอบคุณสำนักงานความร่วมมือเพื่อการพัฒนาระหว่างประเทศ กระทรวงการต่างประเทศ ที่ให้ความช่วยเหลือเอื้อเฟื้อข้อมูลต่าง ๆ ขอบพระคุณผู้เขียนวรรณกรรมทุกเรื่อง และงานเขียนทุกชิ้นที่ผู้เขียนได้นำมาอ้างอิงในการศึกษาค้นคว้าเพื่อจัดทำวิทยานิพนธ์ในครั้งนี้ให้สำเร็จลุล่วงไปด้วยดี

ขอขอบคุณครอบครัว เพื่อน ๆ ที่ได้คอยให้กำลังใจอันยิ่งใหญ่และคอยให้ความช่วยเหลือด้านต่าง ๆ ด้วยดีตลอดมา และขอบพระคุณครู อาจารย์ที่คอยประสิทธิ์ประสาทวิชาความรู้และปลูกฝังคุณธรรมความดีงามให้แก่ผู้เขียนด้วยดีเสมอมา ท้ายที่สุดนี้ ถ้าวิทยานิพนธ์ฉบับนี้มีประโยชน์แก่ผู้ที่สนใจประการใด ผู้เขียนขอมอบความรู้และคุณงามความดีนี้แก่มหาวิทยาลัยแม่ฟ้าหลวง บิดา มารดาและครูบาอาจารย์ทั้งหลาย แต่ถ้าวิทยานิพนธ์ฉบับนี้มีข้อบกพร่องตรงส่วนใด ผู้เขียนขอน้อมรับความบกพร่องนั้นไว้แต่เพียงผู้เดียวและต้องขออภัยมา ณ ที่นี้ด้วย

เกมอุรา ไชยวงศ์

**ชื่อเรื่องวิทยานิพนธ์** มาตรการทางกฎหมายของ สปป.ลาว ในการคุ้มครอง และป้องกันอาชญากรรมทางคอมพิวเตอร์

**ชื่อผู้เขียน** เกมอุรา ไชยวงศ์

**หลักสูตร** นิติศาสตรมหาบัณฑิต

**อาจารย์ที่ปรึกษา** ดร. ชูเกียรติ น้อยฉิม

## บทคัดย่อ

วิทยานิพนธ์ฉบับนี้มุ่งศึกษามาตรการทางกฎหมายในการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์ใน สปป.ลาว โดยศึกษาเปรียบเทียบกับอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ของสหภาพยุโรป พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2007 ของประเทศสิงคโปร์ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทย เพื่อปรับปรุงแก้ไขกฎหมายในการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์ใน สปป.ลาว ให้มีความชัดเจนยิ่งขึ้น

จากการศึกษาพบว่า ลักษณะการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์มีลักษณะแตกต่างไปจากลักษณะของการกระทำผิดอาญาทั่วไป ซึ่งก่อให้เกิดปัญหาแก่การปรับใช้กฎหมายของ สปป.ลาว ที่มีอยู่ปัจจุบันเพื่อนำตัวผู้กระทำความผิดมาลงโทษ เนื่องจากการกระทำของอาชญากรรมทางคอมพิวเตอร์ เป็นการกระทำต่อระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ เช่น การรบกวนข้อมูลคอมพิวเตอร์ การเข้าถึงข้อมูลคอมพิวเตอร์ การดักจับข้อมูลคอมพิวเตอร์ เป็นต้น ซึ่งเป็นการกระทำที่ไม่สามารถมองเห็นและจับต้องได้ ด้วยเหตุนี้กฎหมายของ สปป.ลาว ที่มีอยู่ในปัจจุบันจึงไม่สามารถปรับใช้ให้เกิดประสิทธิภาพสูงสุดในการดำเนินคดีต่อผู้กระทำความผิดทางคอมพิวเตอร์

ดังนั้น จึงเห็นควรที่ สปป.ลาว จะมีการออกมาตรการทางกฎหมายเพื่อมารองรับในกรณีความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ด้วยการกำหนดฐานความผิด ลักษณะของ

การกระทำผิด บทลงโทษสำหรับการก่ออาชญากรรมทางคอมพิวเตอร์ที่เป็นการเฉพาะ และให้พนักงานเจ้าหน้าที่มีอำนาจในการสืบสวนสอบสวนคดีเกี่ยวกับการกระทำผิดทางคอมพิวเตอร์ด้วย ซึ่งเป็นกฎหมายที่มีความเหมาะสมและสามารถนำมาบังคับใช้เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในการนำผู้กระทำผิดมาลงโทษให้ได้อย่างมีประสิทธิภาพ

**คำสำคัญ**: มาตรการทางกฎหมาย/การคุ้มครอง/อาชญากรรมทางคอมพิวเตอร์/สปป.ลาว

| | |
|---|---|
| **Thesis Title** | Legal Measures of Lao PDR for the Protection Related to Computer Crime |
| **Author** | Gemoula Sayavong |
| **Degree** | Master of Law |
| **Advisor** | Chukeat Niochim, Ph. D. |

# ABSTRACT

This thesis aims to study legal measures to protect and prevent cybercrime in Lao PDR, comparing with the 2001 Convention on Cybercrime in the EU, Computer misuse and cybersecurity Act 2007 of Singapore and the Computer Crime Act B.E. 2550 of Thailand. The comparative cases are employed in order to find out an approach for amendment of the law on the protection and prevention of computer crime in Lao PDR.

The research findings show that the nature of offense of computer crime is different from general characteristics of criminal offenses, because the act of crime such as distraction of computer system, access and trapping computer data are usually invisible and intangible. The key problem of consequently is the implementing Lao PDR laws relating to computer crime in order to bring the offenders in court in Lao PDR. For this reason, the current computer crime law in Lao PDR has not been able to achieve maximum efficiency in the prosecution of computer offenders.

Therefore the study proposes that Lao PDR shall issue legal measures to cope with computer crime offenses by specifically defining the criminal court of computer crime, the nature of the offense of misconduct and its penalties as well as empowering the related law enforcement

officers to investigate the cases in an attempt to effectively impose the law against the cybercrime.

**Keywords**: Legal Measures/Protection/Computer Crime/Lao PDR.

# สารบัญ

# สารบัญ (ต่อ)

# สารบัญตาราง

**ตาราง** **หน้า**

# บทที่ 1

# บทนำ

## 1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันพัฒนาการทางด้านเทคโนโลยีการสื่อสารและระบบคอมพิวเตอร์มีความเจริญก้าวหน้าอย่างไม่หยุดยั้ง จากการพัฒนาดังกล่าวได้นำโลกเข้าสู่ยุคโลกาภิวัฒน์ (Globalization) ที่เป็นสังคมแห่งข้อมูลข่าวสารและการติดต่อสื่อสารอย่างไร้ขีดจำกัดทางพรมแดน โดยเฉพาะอย่างยิ่งการสื่อสารผ่านระบบอินเทอร์เน็ตที่ถือว่าเป็นการสื่อสารวิธีหนึ่ง ที่เป็นผลมาจากความก้าวหน้าทางด้านเทคโนโลยีการสื่อสาร โดยส่งผลให้คนทั้งหลายในสังคมสามารถเข้าถึงการติดต่อแลกเปลี่ยนข้อมูลข่าวสารได้โดยง่ายและรวดเร็ว ยิ่งไปกว่านั้นบุคคลธรรมดาหรือองค์กรต่าง ๆ ก็สามารถเข้าถึงแหล่งข้อมูลได้ไม่ว่าจะเป็นทางด้านธุรกิจการค้าหรือด้านสันทนาการ รวมทั้งในด้านอื่น ๆ ได้อย่างสะดวกมากขึ้น แต่ในขณะเดียวกันในสังคมก็มีหลายเหตุการณ์ที่เกิดขึ้นจากการนำใช้เทคโนโลยีข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์มาใช้ในด้านที่ไม่เหมาะสม ก่อให้เกิดความเสียหายต่อบุคคลอื่น รวมทั้งส่งผลกระทบต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ โดยการอาศัยช่องว่างแห่งกฎหมายและระบบเครือข่ายอินเทอร์เน็ตที่มีความสลับซับซ้อนทางด้านเทคโนโลยีเป็นช่องทางในการก่ออาชญากรรมขึ้น ซึ่งอาชญากรรมที่เกิดขึ้นนี้เรียกว่า “อาชญากรรมคอมพิวเตอร์ (Computer Crime)”

เนื่องจากการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์เป็นอาชญากรรมที่ต้องอาศัยระบบคอมพิวเตอร์และอินเทอร์เน็ตที่มีลักษณะเป็นเครือข่ายการสื่อสารเชื่อมโยงเข้าด้วยกัน และมีความละเอียดซับซ้อนของความก้าวหน้าทางเทคโนโลยีเป็นอย่างยิ่ง ซึ่งอาจจะนำไปใช้ในการเข้าไปล่วงรู้ความลับทางการค้า การปลอมแปลงเอกสารทางอิเล็กทรอนิกส์ การเข้าถึงข้อมูลของผู้อื่นโดยที่ผู้กระทำไม่ได้รับอนุญาต การลักลอบแก้ไขภาพของผู้อื่นให้เป็นไปในทางลามกอนาจาร การเผยแพร่ภาพลามกอนาจาร การเล่นพนัน รวมทั้งการทำข้อความอื่นใดอันเป็นการหมิ่นประมาท

บุคคลอื่น เป็นต้น ซึ่งอาชญากรรมคอมพิวเตอร์นั้นได้สร้างความเสียหายต่อความมั่นคงของชาติ เศรษฐกิจ สังคมและความสงบเรียบร้อยโดยรวมเป็นอย่างมาก[1]

ดังนั้น จากปัญหาการใช้คอมพิวเตอร์เป็นเครื่องมือที่ทันสมัยเพื่อก่ออาชญากรรมทางคอมพิวเตอร์นี้ เป็นการกระทำความผิดที่ยากต่อการจับคุม และหาผู้กระทำผิดมาลงโทษรวมทั้งอาจจะเป็นการกระทำความผิดในลักษณะที่เรียกว่าเป็นอาชญากรรมข้ามชาติได้ และด้วยเหตุผลนี้เอง องค์กรระดับนานาชาติจึงได้เล็งเห็นความสำคัญของปัญหาที่เกิด จึงได้มีการร่วมมือกันในระดับระหว่างประเทศเพื่อจัดการกับปัญหาอาชญากรรมคอมพิวเตอร์ โดยองค์การสหประชาชาติ (United Nation: UN) ได้จัดทำคู่มือเกี่ยวกับการป้องกันและควบคุมอาชญากรรมคอมพิวเตอร์ (UN Manual on the Prevention and Control of Computer-related Crime) สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ก็ได้จัดทำกฎข้อบังคับว่าด้วยโทรคมนาคมระหว่างประเทศ (International Telecommunication Regulation: ITR) ขึ้น และสหภาพยุโรป (European union: EU) ได้จัดทำอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime) เป็นต้น

สำหรับในภูมิภาคเอเชียตะวันออกเฉียงใต้นั้น ประเทศสิงคโปร์ และประเทศไทย เป็นสองในห้าของสมาชิกผู้ก่อตั้งและเป็นจุดกำเนิดของอาเซียน[2] และเป็นประเทศที่ได้เล็งเห็นถึงความสำคัญของการนำเทคโนโลยีสารสนเทศมาใช้งาน โดยประเทศสิงคโปร์มีการขยายตัวทางด้านเศรษฐกิจ และระบบเทคโนโลยีสารสนเทศ ซึ่งได้มีการปรับปรุงแก้ไขกฎหมายให้ทันกับพัฒนาการของเทคโนโลยีที่ทันสมัย นอกจากนี้ประเทศไทยก็เป็นประเทศเพื่อนบ้านอีกประเทศหนึ่งที่มีความใกล้เคียงทางด้านภาษาและจารีตประเพณีคล้ายคลึงกับ สปป.ลาว และเห็นถึงความสำคัญทางด้านพัฒนาการในการใช้งานของระบบคอมพิวเตอร์ที่ทันสมัย โดยทั้งสองประเทศได้มีพัฒนาการทางกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ จึงได้ศึกษาเปรียบเทียบกับสองประเทศดังกล่าว

ด้วยเหตุนี้ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้ตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานของผู้อื่นผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไขทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบหรือใช้คอมพิวเตอร์เพื่อเผยแพร่ข้อมูลอันเป็นเท็จหรือมีลักษณะลามกอนาจาร ย่อมก่อให้เกิดความเสียหายต่อบุคคล เศรษฐกิจ สังคม และความมั่นคงของชาติ ด้วยเหตุนี้ประเทศสิงคโปร์จึงได้ตราและประกาศใช้พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทาง

---

[1] วีระพงษ์ บุญโญภาส, *อาชญากรรมทางเศรษฐกิจ*, (กรุงเทพฯ: นิติธรรม, 2549), 118.

[2] กรมอาเซียน กระทรวงการต่างประเทศ, *Asean mini book*, (กรุงเทพฯ: กรมฯ, ม.ป.ป.), 4.

คอมพิวเตอร์ ค.ศ. 2007 (Computer Misuse and Cybersecurity Act 2007) และประเทศไทยได้ตราและประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ในขณะเดียวกันประเทศสาธารณรัฐประชาธิปไตยประชาชนลาว[3] ซึ่งเป็นประเทศที่กำลังพัฒนาที่อยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ที่มีอัตราการเจริญเติบโตมากขึ้นไม่ว่าจะเป็นทางด้านเศรษฐกิจและสังคม ซึ่งการเจริญเติบโตในด้านเศรษฐกิจและสังคมที่เพิ่มมากขึ้นย่อมทำให้การใช้ข้อมูลข่าวสารและอินเทอร์เน็ตเข้ามาเกี่ยวข้องกับการดำเนินชีวิตประจำวันเพิ่มมากขึ้นตามไปด้วย ในทำนองเดียวกันการบริหารกิจกรรมทางธุรกิจการค้าของภาคเอกชน และการบริหารงานประเทศของภาครัฐ ก็ได้นำเอาความก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์ที่ทันสมัยมาปรับใช้ด้วยเช่นกัน โดยเฉพาะอย่างยิ่งอินเทอร์เน็ตได้เข้ามามีบทบาทในการเสริมสร้างการให้บริการส่งข้อมูลสารสนเทศการติดต่อสื่อสารกันได้อย่างสะดวก รวดเร็ว และขยายตัวอย่างต่อเนื่องตามลำดับ ซึ่งเห็นได้จากสถิติการเข้าใช้อินเทอร์เน็ตของ สปป.ลาว ในปี ค.ศ. 2009 มีเพียง 3% ซึ่งแตกต่างกับในปัจจุบัน (ค.ศ. 2011) ที่มีการเข้าใช้อินเทอร์เน็ตเพิ่มขึ้นเป็น 10%[4] อย่างไรก็ตาม เมื่อสังคมในปัจจุบันต้องมีการพึ่งพาอาศัยระบบเทคโนโลยีคอมพิวเตอร์ในการดำรงชีวิตประจำวัน และการทำงานมากยิ่งขึ้นเท่าไร โอกาสในการก่อให้เกิดการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ก็มีมากขึ้นเท่านั้น ถึงแม้ว่า สปป.ลาว ในระยะที่ผ่านมาจะมี (1) กฎหมายอาญา ค.ศ. 2005 (2) กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2012 และ (3) กฎหมายอื่น ๆ อีกหลายฉบับที่ใช้เป็นเครื่องมือในการดำเนินคดี แต่เนื่องจากอาชญากรรมคอมพิวเตอร์นั้นมีความแตกต่างจากอาชญากรรมทั่วไปในสังคม ซึ่งมีลักษณะของการกระทำความผิดบางประเภทได้เปลี่ยนไปจากรูปแบบเดิม ซึ่งได้ก่อให้เกิดลักษณะของความผิดรูปแบบใหม่ ซึ่งกฎหมายที่มีอยู่เดิมไม่สามารถนำมาปรับใช้ให้ครอบคลุมการกระทำความผิดในลักษณะนี้ได้ เช่น วัตถุแห่งการกระทำความผิดส่วนใหญ่เป็นข้อมูลข่าวสารในรูปแบบคลื่นแม่เหล็กไฟฟ้า ซึ่งเป็นสิ่งที่ไม่สามารถจับต้องได้ จึงทำให้กฎหมายต่าง ๆ ที่บังคับใช้อยู่ในปัจจุบันไม่สามารถลงโทษผู้กระทำผิดได้ และการปฏิบัติหน้าที่ของเจ้าพนักงานก็ไม่อาจกระทำได้อย่างมีประสิทธิภาพ หากไม่มีกฎหมายที่ให้อำนาจรัฐหรือเจ้าหน้าที่ของรัฐก็ไม่อาจกระทำการใด ๆ อันเป็นการกระทำที่กระทบต่อสิทธิเสรีภาพของประชาชนได้ ดังนั้นกฎหมายที่มีอยู่เดิมจึงไม่สามารถนำมาปรับใช้เพื่อลงโทษผู้ก่ออาชญากรรมคอมพิวเตอร์ให้ได้โทษเท่าที่ควร ด้วยเหตุผลที่กล่าวมาข้างต้นนี้ สามารถพิจารณาได้ว่าการกระทำความผิดเกี่ยวกับ

---

[3] สาธารณรัฐประชาธิปไตยประชาชนลาว (The Lao People's Democratic Republic: Lao PDR) ต่อไปในวิทยานิพนธ์นี้จะเรียกว่า "สปป.ลาว " และสปป.ลาว ใช้ปีศักราชที่เรียกว่า "คริสต์ศักราช (ค.ศ.)".

[4] กระทรวงไปรษณีย์ โทรคมนาคมและการสื่อสาร, *บทเสนอเกี่ยวกับการร่างกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์*, (นครหลวงเวียงจันทน์: กระทรวงฯ, 2014), 1.

คอมพิวเตอร์ภายใต้ระบบกฎหมายของ สปป.ลาว ในปัจจุบันยังไม่เพียงพอต่อการรับมือกับการกระทำผิดทางด้านอาชญากรรมคอมพิวเตอร์ จึงเห็นควรที่จะทำการศึกษาวิจัยเกี่ยวกับมาตรการทางกฎหมายของ สปป.ลาว ในการคุ้มครองและควบคุมการกระทำความผิดทางคอมพิวเตอร์

## 1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อศึกษาความเป็นมา และความหมายของอาชญากรรมทางคอมพิวเตอร์

1.2.2 เพื่อศึกษาแนวคิด ทฤษฎีทางกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

1.2.3 เพื่อศึกษามาตรการทางกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในระหว่างประเทศ และต่างประเทศ รวมทั้งประเทศไทย

1.2.4 เพื่อศึกษาวิเคราะห์ปัญหา และหามาตรการทางกฎหมายที่เหมาะสม เพื่อนำมาปรับปรุงมาตรการทางกฎหมายเกี่ยวกับการกระทำผิดทางคอมพิวเตอร์ใน สปป.ลาว

## 1.3 สมมติฐานของการวิจัย

ในปัจจุบันนี้ สปป.ลาว ขาดมาตรการทางกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ที่จะนำมาปรับใช้กับปัญหาของการกระทำผิดทางคอมพิวเตอร์ เพื่อให้เกิดประสิทธิภาพสูงสุด ด้วยเหตุนี้จึงควรทำการศึกษาเพื่อหาแนวทางหรือมาตรการทางกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ เพื่อนำมาใช้คุ้มครองและป้องกันปัญหาอาชญากรรมทางคอมพิวเตอร์ใน สปป.ลาว ให้มีประสิทธิภาพมากยิ่งขึ้นในอนาคต

## 1.4 ขอบเขตของการวิจัย

การศึกษาวิจัยนี้จะศึกษาเกี่ยวกับหลักทฤษฎีทางกฎหมาย หลักเกณฑ์ระหว่างประเทศ และมาตรการทางกฎหมายอื่น ๆ ที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ รวมถึงศึกษาระบบและมาตรการทางกฎหมายของประเทศสิงคโปร์และประเทศไทยที่ใช้เพื่อคุ้มครองและป้องกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อเป็นแนวทางเสนอแนะให้มีการพัฒนาและปรับปรุงมาตรการทางกฎหมายเกี่ยวกับการกระทำผิดทางคอมพิวเตอร์ใน สปป.ลาวให้มีความเหมาะสมต่อการควบคุมการก่ออาชญากรรมทางคอมพิวเตอร์ใน สปป.ลาว

## 1.5 วิธีดำเนินการวิจัย

วิทยานิพนธ์ฉบับนี้เป็นการศึกษาค้นคว้าวิจัยเอกสาร (Documentary Research) โดยการศึกษาวิจัยหลักทฤษฎีทางกฎหมาย เอกสารทางวิชาการ เช่น บทบัญญัติกฎหมาย หนังสือ บทความทางวิชาการ วารสาร วิทยานิพนธ์ สารนิพนธ์ ข้อมูลอิเล็กทรอนิกส์ และรวบรวมข้อมูลจากเอกสารต่าง ๆ ทั้งภาษาไทย ภาษาลาว และภาษาต่างประเทศ เพื่อเป็นข้อมูลทางวิชาการในการดำเนินการศึกษาวิจัย

## 1.6 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1.6.1 ทำให้ทราบถึงความเป็นมา และความหมายของอาชญากรรมทางคอมพิวเตอร์

1.6.2 ทำให้ทราบถึงแนวคิด ทฤษฎีทางกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

1.6.3 ทำให้ทราบถึงมาตรการทางกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในระหว่างประเทศ และต่างประเทศ รวมทั้งประเทศไทย

1.6.4 ได้มาซึ่งมาตรการทางกฎหมายที่เหมาะสม เพื่อนำมาปรับปรุงมาตรการทางกฎหมายเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ใน สปป.ลาว

# บทที่ 2

# วิวัฒนาการ แนวความคิด และทฤษฎีที่เกี่ยวข้องกับ อาชญากรรมทางคอมพิวเตอร์

เนื่องจากอาชญากรรมทางคอมพิวเตอร์เป็นอาชญากรรมที่อาศัยความสลับซับซ้อนของระบบคอมพิวเตอร์ การเข้าถึงที่ง่ายขึ้นของระบบเครือข่ายการสื่อสาร และการใช้ความรู้ความสามารถพิเศษที่ใช้อุปกรณ์หรือเทคโนโลยีชั้นสูงในการประกอบอาชญากรรม ซึ่งจะเพิ่มขึ้นพร้อม ๆ กับพัฒนาการทางเทคโนโลยีสารสนเทศที่มีการขยายตัวอย่างไม่หยุดยั้ง ทำให้ต้องมีการตรากฎหมายต่าง ๆ ขึ้นเพื่อบังคับใช้และควบคุมการใช้งานเทคโนโลยีสารสนเทศให้เป็นไปด้วยความเรียบร้อย เพื่อมิให้มีการนำเทคโนโลยีไปใช้ในการกระทำผิด อันส่งผลกระทบต่อส่วนรวม ซึ่งในบทนี้จะได้กล่าวถึง วิวัฒนาการเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ลักษณะของอาชญากรรมทางคอมพิวเตอร์ แนวความคิดเกี่ยวกับกฎหมายบนอินเทอร์เน็ต รูปแบบของการกระทำผิดบนอินเทอร์เน็ต ทฤษฎีที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ และความสำคัญของการมีกฎหมายป้องกันอาชญากรรมทางคอมพิวเตอร์ โดยสามารถสรุปได้ดังนี้

## 2.1 วิวัฒนาการของอาชญากรรมทางคอมพิวเตอร์

โดยธรรมชาติแล้วอาชญากรรมเป็นปรากฏการณ์ที่เกิดขึ้นในทุกสังคม ไม่มีสังคมใดที่ปลอดภัยจากปัญหาอาชญากรรมและการกระทำความผิดที่แท้จริง กล่าวคืออาชญากรรมเป็นปรากฏการณ์ธรรมดาของทุกสังคม แต่อาจมีรูปแบบเปลี่ยนแปลงไปตามพัฒนาการความก้าวหน้าของสังคมนั้น ๆ ในสังคมยุคแรกมีรูปแบบความสัมพันธ์ของสมาชิกในสังคมไม่ซับซ้อน ทำให้รูปแบบของอาชญากรรมมักเป็นรูปแบบที่รุนแรง และเกี่ยวข้องกับปัจจัยพื้นฐานของชีวิต เช่น การกระทำต่อร่างกาย ทรัพย์สิน และชีวิต การบังคับใช้กฎหมายก็กระทำได้ไม่ยาก แต่เมื่อสังคมมีการพัฒนาอย่างต่อเนื่อง ทำให้รูปแบบของอาชญากรรมเกิดขึ้นอย่างหลากหลาย มีความซับซ้อนมากยิ่งขึ้น มีการใช้

เทคโนโลยีในรูปแบบต่าง ๆ เข้ามาผสมผสานกับการกระทำความผิด[5] จึงทำให้ต้องมีการพัฒนากฎหมาย ให้ครอบคลุมถึงการกระทำผิดในรูปแบบใหม่ ๆ โดยเฉพาะการใช้เทคโนโลยีในการก่ออาชญากรรม เป็นต้น

นับตั้งแต่ทศวรรษที่ 60 (ช่วงปี ค.ศ. 1960-1970) นับเป็นช่วงเวลาแรก ๆ ที่เริ่มมีความพยายามในการชี้ให้เห็นถึงภยันตรายจากการกระทำความผิดทางคอมพิวเตอร์ ทั้งนี้ในสมัยนั้นหลายประเทศในแถบตะวันตกใช้คอมพิวเตอร์เป็นอุปกรณ์ในการเก็บบันทึก ถ่ายทอดและเชื่อมโยงฐานข้อมูลส่วนบุคคลของประชาชนในรัฐด้วยกัน และด้วยเหตุที่มีการนำข้อมูลต่าง ๆ ไปรวบรวมไว้ภายใต้การจัดการของรัฐนี้เอง นักวิชาการจำนวนหนึ่งจึงเริ่มมีการอภิปรายถกเถียงถึงประเด็นปัญหาที่ประชาชนอาจถูกตรวจสอบเฝ้ามองหรือควบคุมจากรัฐได้ โดยได้รับอิทธิพลมาจากหนังสือของ Georgo Orwell ชื่อ “1984 (Nineteen Eighty Four)” อันเป็นหนังสือด้านการเมืองการปกครอง แต่มีเนื้อหาส่วนหนึ่งที่ได้กล่าวถึงพัฒนาการทางด้านเทคโนโลยีข้อมูลข่าวสารที่มีผลประโยชน์ต่อระบบการจัดการระบบข้อมูลการทำงานของมนุษย์ ในขนาดเดียวกันก็สะท้อนถึงรัฐที่เริ่มล้ำเส้นและเกินขอบเขตความเป็นส่วนตัวของประชาชน ด้วยเหตุที่ในยุคสมัยนั้นคุณประโยชน์หลัก ๆ ของเครื่องคอมพิวเตอร์ยังจำกัดอยู่เพียงแค่การเก็บบันทึกประมวลผลหรือเชื่อมต่อข้อมูลต่าง ๆ ของประชาชนในประเทศเท่านั้น ความเข้าใจที่มีต่อการกระทำความผิดโดยมีคอมพิวเตอร์เข้าไปเกี่ยวข้องในยุคสมัยแรก ๆ จึงยังไม่ได้มีความหมายทำนองเดียวกับ “อาชญากรรมคอมพิวเตอร์” ที่เราเข้าใจกันในปัจจุบัน แต่หมายถึงการกระทำความผิดใด ๆ ที่เป็นอันตรายต่อข้อมูลข่าวสาร และระดับความลับหรือความเป็นส่วนตัวที่มนุษย์แต่ละคนอาจไม่ได้เปิดเผยให้ผู้อื่นรับรู้[6]

### 2.1.1 ความหมายของอาชญากรรมทางคอมพิวเตอร์

อาชญากรรมทางคอมพิวเตอร์ (Computer Crime) ยังไม่มีข้อยุติในทางสากลว่ามีนิยามหรือความหมายที่ชัดเจนอย่างไร เนื่องจากนักวิชาการยังมีความเห็นที่ไม่ตรงกัน แม้แต่ชื่อที่ใช้เรียกก็ยังมีความแตกต่างกัน เช่น Cyber Crime, Computer Related Crime, Computer Misuse, Computer Abuse, Information Technology Crime มีผู้ให้คำนิยามเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ซึ่งมีความหมายอย่างกว้างว่า “อาชญากรรมทางคอมพิวเตอร์ หมายถึง การกระทำที่ผิดกฎหมายใด ๆ ซึ่งความรู้ในเทคโนโลยีทางคอมพิวเตอร์มีความสำคัญต่อผลสำเร็จของการกระทำหรือการดำเนินคดี

---

[5] วีระพงษ์ บุญโญภาส, *อาชญากรรมทางเศรษฐกิจ*, 3.

[6] สาวิตรี สุขศรี, *ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์*, (9 พฤศจิกายน 2552), สืบค้นเมื่อ 1 พฤศจิกายน 2557, จาก https://facthai.wordpress.com/2009/11/09/ประวัติศาสตร์-อาชญากรรม/

และเป็นการกระทำความผิดทางอาญาซึ่งก่อการคุกคามต่อผู้ใช้คอมพิวเตอร์มากกว่าผู้ที่มิได้ใช้คอมพิวเตอร์ ประกอบไปด้วยการกระทำความผิด 2 ชนิด[7] คือ

1. การใช้คอมพิวเตอร์เพื่อกระทำความผิดฐานฉ้อโกง ลักทรัพย์ และยักยอกโดยมีเจตนาที่จะได้ไปซึ่งประโยชน์อันเกี่ยวกับเงิน การค้า ทรัพย์สินหรือบริการ และ

2. การกระทำความผิดต่อตัวเครื่องคอมพิวเตอร์เอง เช่น การลักขโมยเครื่องคอมพิวเตอร์ หรือซอฟท์แวร์ การทำลายหรือแก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์หรือสิ่งที่บรรจุอยู่ภายในเครื่องคอมพิวเตอร์

Donn B. Parker ชาวสหรัฐอเมริกา ผู้ริเริ่ม และได้รับการย่อมรับว่าเป็นบิดาแห่งความรู้ในเรื่องอาชญากรรมทางคอมพิวเตอร์ ซึ่งเขาได้เป็นส่วนหนึ่งของการวิจัยในช่วงต้นทศวรรษที่ 70 โดยดำรงตำแหน่ง Senior Computer Security Consultant ณ SRI International (Stanford Research Institute) และเป็นผู้ประพันธ์หลักในคู่มือการออกกฎหมายอาชญากรรมคอมพิวเตอร์ในสหรัฐอเมริกา (Computer Crime-Criminal Justice Resource Manual) ในปี ค.ศ. 1979 โดยคู่มือดังกล่าวได้เปรียบเสมือนสารานุกรมสำหรับแนวทางการออกกฎหมายอาชญากรรมคอมพิวเตอร์ ซึ่งในคู่มือดังกล่าวได้ให้ความหมายของอาชญากรรมคอมพิวเตอร์ในแบบกว้างไว้ว่า “การกระทำที่ผิดกฎหมายใด ๆ ซึ่งความรู้ทางวิทยาการคอมพิวเตอร์นั้นมีความสำคัญต่อการปฏิบัติการให้สำเร็จลุล่วง”[8]

The Organization for Economic Co-operation and Development: OECD ได้รวบรวมนิยามเพื่อเป็นฐานในการศึกษาไว้ว่า “อาชญากรรมที่เกี่ยวกับคอมพิวเตอร์นั้นพิจารณาเป็นพฤติกรรมอันมิชอบด้วยกฎหมาย ขัดต่อศีลธรรมจรรยาหรือไม่ได้รับอนุญาตที่เกี่ยวข้องกับการประมวลผลอัตโนมัติหรือการส่งข้อมูล”[9]

---

[7] ฉัทปณัย รัตนาพันธ์, *อาชญากรรมทางคอมพิวเตอร์: ศึกษาการกำหนดฐานความผิดและการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์*, สารนิพนธ์นิติศาสตรมหาบัณฑิต, (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2547), 4.

[8] “any illegal act for which knowledge of computer technology is essential for its successful prosecution”, SRI international, *The criminal justice resource manual on computer crime*, (Menlo Park, CA: SRI international, 1979).

[9] “Computer-related crime is considered as the offences enumerated and defined in the proposed guidelines or recommendation for national legislators”, Organization for Co-operation Development, *Computer related criminality: Analysis of legal politics in the OECD area*, (Paris: OECD, 1986).

The Council of Europe Recommendation of 1989 ได้นำวิธีเข้าถึงที่สามารถนำไปใช้ได้จริง อาชญากรรมทางคอมพิวเตอร์ถูกอธิบายว่า เป็นการกระทำผิดที่ชี้วัด และนิยามโดยแนวทางที่ถูกเสนอหรือคำแนะนำสำหรับผู้ร่างกฎหมายในแต่ละประเทศ[10]

Mr. Kenneth S. Rosendlatt อัยการผู้เชี่ยวชาญคดีอาญากรรมทางคอมพิวเตอร์ ซึ่งเป็นผู้เขียนหนังสือเรื่อง High Technology Crime ได้อธิบายความหมายของอาชญากรรมทางคอมพิวเตอร์ไว้ว่า เป็นอาชญากรรมที่เกิดขึ้นใหม่อันเป็นผลสืบเนื่องมาจากการใช้คอมพิวเตอร์อย่างแพร่หลาย เช่น การล่วงล้ำเข้าไปในระบบเครือข่ายคอมพิวเตอร์ของบริษัทธุรกิจที่เชื่อมโยงผ่านเครือข่ายโทรคมนาคม นอกจากนี้ยังหมายถึง อาชญากรรมแบบเดิมที่แปรสภาพไปเนื่องจากความก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์ ซึ่งในการสืบสวนคดีประเภทนี้ต้องมีความรู้เกี่ยวกับคอมพิวเตอร์ และคุ้นเคยกับอุตสาหกรรมเทคโนโลยีชั้นสูง[11]

ในปี ค.ศ. 2001 คณะกรรมาธิการสหภาพยุโรป (Commission of the European Union) ได้ให้คำนิยามว่า “อาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ที่ถูกระบุไว้ในความหมายที่กว้างคือ อาชญากรรมใด ๆ ซึ่งเกี่ยวข้องกับการใช้เทคโนโลยีข้อมูลข่าวสาร (Information Technology: IT) ไม่ทางใดก็ทางหนึ่ง”[12] และยังให้เห็นความแตกต่างระหว่างอาชญากรรมทั่วไปที่ใช้คอมพิวเตอร์ในการช่วยการกระทำการและอาชญากรรมทางคอมพิวเตอร์

อนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ (Convention on Cybercrime) ที่เกิดจากประเทศต่าง ๆ ในกลุ่มสหภาพยุโรป ซึ่งได้กำหนดมาตรการต่าง ๆ ไว้อย่างมากมายและได้ให้คำนิยามเกี่ยวกับอาชญากรรมคอมพิวเตอร์ไว้ใน มาตรา 2-10 อันเป็นกฎหมายลักษณะอาญา ใน 4 หมวดหมู่ ได้แก่ (1) ความผิดต่อความลับ ความสมบูรณ์ และการมีอยู่ของข้อมูลและระบบ (2) ความผิด

---

[10] “…the offences enumerated and defined in the proposed guidelines or recommendation for national legislators…”, Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on September 13 1989 and Report by the European Committee on Crime Problems: Computer-related crime.

[11] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, *โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ*, (กรุงเทพฯ: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, 2543), 29.

[12] The Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, “Computer-related crime is addressed in the broadest sense as: any crime that in some way or other involves the use of information technology”, The Communication from the Commission to the Council, the European Parliament, *The economic and social committee and the committee of the regions,* (2001, 26 January), Retrieved October 17, 2013, from http://eur-lex.europa.eu/legal-content/.EN/ALL/;ELX_SESSIONID=GwZLJy5TV3NhBcLyRM882MNrT022QNfGD15kddlNskcvqkPkC7PJ!-7040371?uri=CELEX:52000DC0890

เกี่ยวกับคอมพิวเตอร์ (3) ความผิดเกี่ยวกับเนื้อหา (4) ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิ์ที่เกี่ยวข้อง[13] โดยเป็นรายการของมาตรฐานขั้นต่ำที่ไม่แยกส่วนซึ่งขยายรวมไปถึงกฎหมายภายในประเทศสมาชิก

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติของประเทศไทย ได้อธิบายความหมายของอาชญากรรมทางคอมพิวเตอร์คือ การกระทำใด ๆ ที่เกี่ยวข้องกับการใช้คอมพิวเตอร์อันทำให้บุคคลอื่นได้รับความเสียหาย หรือผู้กระทำได้รับผลประโยชน์ตอบแทน หรือการกระทำผิดกฎหมายใด ๆ ซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือ และในการสืบสวนสอบสวนของเจ้าหน้าที่เพื่อนำผู้กระทำผิดมาดำเนินคดีต้องใช้ความรู้ทางเทคโนโลยี[14]

โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ ได้รวมคำนิยามของคำว่า “อาชญากรรมทางคอมพิวเตอร์” นั้นมีหลายแนวทาง ซึ่งโดยส่วนมากมักจะไม่ให้คำนิยามไว้อย่างชัดเจน อย่างไรก็ดีสามารถแบ่งคำนิยามได้ดังต่อไปนี้[15]

1. คำนิยามในความหมายแคบ อาชญากรรมทางคอมพิวเตอร์ จะมีความหมายเฉพาะความผิดที่เกิดขึ้นกับข้อมูลภายในคอมพิวเตอร์เท่านั้น

2. คำนิยามที่ใช้ความรู้ทางคอมพิวเตอร์เป็นเกณฑ์ จะเป็นการนิยามให้ครอบคลุมเฉพาะความผิดที่เกิดขึ้นไม่ว่าจะในเครื่องคอมพิวเตอร์หรือที่เกี่ยวกับเครื่องคอมพิวเตอร์ และความผิดดังกล่าวผู้กระทำความผิดจะต้องใช้ความรู้ความสามารถทางคอมพิวเตอร์เป็นพิเศษ

3. คำนิยามในความหมายอย่างกว้าง คือการนิยามให้ครอบคลุมถึงการกระทำความผิดทุกอย่างที่มีคอมพิวเตอร์เป็นส่วนประกอบ

ไพจิตร สวัสดิสาร ได้ให้ความหมายว่า อาชญากรรมคอมพิวเตอร์ คือ การใช้คอมพิวเตอร์เพื่ออำนวยความสะดวกหรือนำไปสู่การกระทำผิดทางอาญา[16]

---

[13] Convention on Cybercrime, Chapter 1-4, (1) Offences against the confidentiality, integrity and availability of computer data and systems; (2) computer-related offences, (3) content-related offences; (4) offences related to infringements of copyright and related rights.

[14] ฝ่ายศึกษาวิจัยประเด็นด้านจริยธรรม กฎหมาย และผลกระทบทางสังคมของเทคโนโลยีสารสนเทศ, *กฎหมายเทคโนโลยีสารสนเทศ IT Laws*, (ปทุมธานี: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2552), 68.

[15] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, *ประเทศไทยกับการพัฒนากฎหมายเทคโนโลยีสารสนเทศ*, (กรุงเทพฯ: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, 2542), 24.

[16] ไพจิตร สวัสดิสาร, *การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายที่เกี่ยวกับคอมพิวเตอร์*, (กรุงเทพฯ: ชวนพิมพ์, 2550), 135.

ดังนั้น จากคำนิยามและความหมายในข้างต้นอาจกล่าวได้ว่า “อาชญากรรมทางคอมพิวเตอร์” หมายถึงการกระทำใด ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ไม่ว่าในทางใดทางหนึ่งที่ผิดกฎหมาย โดยใช้ความรู้ความสามารถพิเศษทางอิเล็กทรอนิกส์เพื่อโจมตีระบบคอมพิวเตอร์และข้อมูลที่อยู่ในระบบดังกล่าว

**2.1.2 ลักษณะของอาชญากรรมทางคอมพิวเตอร์**

โดยธรรมชาติของอาชญากรรมทางคอมพิวเตอร์ มักมีลักษณะและพฤติกรรมที่ไม่รุนแรง ไม่ใช้อาวุธ ไม่ใช้กำลังทำร้าย ไม่ใช้วิธีเผชิญหน้าเหมือนความผิดฐานปล้นฆ่า ส่วนใหญ่แล้วจะเกิดขึ้นมาจากการนำคอมพิวเตอร์เข้ามามีส่วนเกี่ยวข้องกับการกระทำความผิด ซึ่งจากลักษณะพิเศษของอาชญากรรมทางคอมพิวเตอร์ที่แตกต่างไปจากอาชญากรรมทั่วไปสามารถเปรียบเทียบลักษณะที่แตกต่างกันได้ดังนี้[17]

[17] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, *ประเทศไทยกับการพัฒนากฎหมายเทคโนโลยีสารสนเทศ*, 26

**ตารางที่ 2.1** เปรียบเทียบลักษณะแห่งการกระทำความผิด

| อาชญากรรมทั่วไป | อาชญากรรมทางคอมพิวเตอร์ |
|---|---|
| 1. วัตถุแห่งการกระทำความผิดส่วนใหญ่เป็นทรัพย์ที่จับต้องได้ (Tangible Object) เช่น รถยนต์ ของมีค่าหรือเงินทอง เป็นต้น | 1. วัตถุแห่งการกระทำความผิดส่วนใหญ่เป็นข้อมูลข่าวสารในรูปแบบคลื่นแม่เหล็กไฟฟ้า (Electronic Impulse) ซึ่งเป็นสิ่งที่ไม่สามารถจับต้องได้ (Intangible Object) เช่น ข้อมูลทางการค้าของบริษัท ฐานข้อมูลลูกค้าของบริษัท หรือค่าเงินในบัญชีของธนาคาร เป็นต้น |
| 2. วิธีการกระทำความผิดเป็นการกระทำความผิดทางกายภาพ เช่น การทำลายทรัพย์สินของผู้อื่น (ความผิดฐานทำให้เสียทรัพย์) หรือการเข้าไปในแดนกรรมสิทธิ์ (ความผิดฐานบุกรุก) เป็นต้น | 2. วิธีการกระทำความผิดเป็นการกระทำความผิดรูปแบบใหม่ที่อาจไม่ต้องมีการกระทำทางกายภาพ เช่น การเข้าไปในระบบคอมพิวเตอร์ที่อยู่ในบ้านเรือนของผู้อื่นโดยไม่ได้รับอนุญาต (Unauthorized Access) ซึ่งผู้กระทำความผิดไม่จำเป็นที่จะต้องเข้าไปทางกายภาพแต่ประการใด เพียงแต่นั่งอยู่ที่บ้านของผู้กระทำความผิดก็สามารถกระทำความผิดได้ และนอกจากไม่ต้องอาศัยการกระทำทางกายภาพแล้ว การกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์ ยังมีวิธีของการกระทำความผิดที่แปลกใหม่และซับซ้อน ดังจะเห็นได้จากการเจาะระบบ (Hacking)[18] ไวรัสคอมพิวเตอร์ (Virus Computer)[19] ม้าโทจัน (Trojan Horse)[20] เป็นต้น |

[18] การโจรกรรมข้อมูล (Hacking) เป็นการกระทำของ Hacker โดยมีเจตนาที่จะลอกเลียนหรือเปลี่ยนแปลงข้อมูลต้นฉบับ การ Hacking จะไม่มีการสร้างความเสียหายกับข้อมูลตัวหลัก เพียงแต่ต้องการเปลี่ยนแปลงข้อมูลนั้นให้แสดงผลตามใจตนเท่านั้น, ดู English Daily, *Hacking: ศัพท์ภาษาอังกฤษว่าด้วยการโจรกรรมข้อมูล*, (2013, 19 ตุลาคม), สืบค้นเมื่อ 1 พฤศจิกายน 2557, จาก http://www.dailyenglish.in.th/hacking-vocabularies/

[19] ไวรัสคอมพิวเตอร์ (Virus Computer) เป็นโปรแกรมที่ได้รับการออกแบบมาเพื่อให้ก่อกวนทำลายระบบคอมพิวเตอร์ ไวรัสจะเข้าไปในระบบได้โดยผ่านทางแผ่นบันทึกที่มีเชื้อไวรัสอยู่หรือโดยทางแฟ้มที่เราคัดลอกมาจากคอมพิวเตอร์เครื่องอื่นโดยการใช้โมเด็ม ไวรัสจะติดเชื้ออยู่ในแฟ้มและนำชุดโปรแกรมออกมาทำลายระบบ เช่น โดยการลบกวนข้อมูลในแฟ้ม จัดรูปแบบซ้ำในจานบันทึกซึ่งทำให้ข้อมูลที่บันทึกอยู่หายไป หรือทำลายระบบแฟ้มที่คอมพิวเตอร์จำเป็นต้องใช้ในการดำเนินงาน, กิดานันท์ มลิทอง, *อธิบายศัพท์คอมพิวเตอร์ อินเทอร์เนต มัลติมีเดีย*, (กรุงเทพฯ, จุฬาลงกรณ์มหาวิทยาลัย, 2539

[20] ม้าโทรจัน (Trojan Horse) เป็นโปรแกรมที่ปรากฏให้เห็นในการทำงานที่เป็นประโยชน์แต่ได้ซ่อนรหัสคำสั่งที่จะทำความเสียหายให้แก่ระบบที่กำลังดำเนินงานนั้นได้ ม้าโทรจันนี้จะไม่เหมือนไวรัสเนื่องจากไม่สามารถติดลงไปในแผนบันทึกอื่นได้ ในขณะที่ไวรัสจะติดไปกับแผ่นบันทึกและแพร่เข้าไปในคอมพิวเตอร์เครื่องอื่น ๆ, กิดานันท์ มลิทอง, *อธิบายศัพท์คอมพิวเตอร์ อินเทอร์เนต มัลติมีเดีย*, 441.

**ตารางที่ 2.1** (ต่อ)

| อาชญากรรมทั่วไป | อาชญากรรมทางคอมพิวเตอร์ |
|---|---|
| 3. ระยะเวลาในการกระทำความผิด เนื่องจากการกระทำความผิดรูปแบบเดิมเป็นการกระทำความผิดทางกายภาพ ดังนั้นจึงต้องใช้ระยะเวลาในการกระทำความผิด ซึ่งอาจเป็น นาที ชั่วโมง วัน สัปดาห์ เดือน หรืออาจเป็นปีก็ได้ | 3. ระยะเวลาในการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์เป็นการใช้เทคโนโลยีชั้นสูงทางคอมพิวเตอร์ ซึ่งมีความรวดเร็วมาก ดังนั้นระยะเวลาในการกระทำความผิดจึงต้องคำนวณเป็นวินาที (Seconds) หรืออาจเป็นเสี้ยววินาที (Milliseconds, Microseconds) |
| 4. ขอบเขตในการกระทำความผิดโดยส่วนใหญ่เป็นการกระทำความผิดภายในอาณาเขตและดินแดนเพราะเหตุจำกัดทางกายภาพ | 4. ขอบเขตในการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์เป็นการกระทำความผิดที่ใช้การผสมผสานระหว่างเทคโนโลยีคอมพิวเตอร์กับเทคโนโลยีโทรคมนาคมอินเทอร์เน็ตที่มีเครือข่ายเชื่อมโยงทั่วโลก ดังนั้นจึงสามารถกระทำความผิดระหว่างประเทศได้และไม่มีขอบเขต |
| 5. ลักทรัพย์: ผู้กระทำต้องพรากเอาทรัพย์ของผู้อื่นไป | 5. ลักทรัพย์: ผู้กระทำสามารถทำซ้ำข้อมูลสารสนเทศไปโดยไม่ต้องเคลื่อนย้ายหรือพรากเอาทรัพย์ของผู้อื่นไป และข้อมูลสารสนเทศก็ไม่ใช่วัตถุที่จับต้องได้ |
| 6. บุกรุก: ผู้กระทำผิดจะต้องมีการเข้าไปในอสังหาริมทรัพย์ของผู้อื่น | 6. บุกรุก: ผู้กระทำความผิดสามารถเข้าดู แก้ไขเปลี่ยนแปลงหรือทำซ้ำซึ่งข้อมูลสารสนเทศที่เก็บไว้ในคอมพิวเตอร์ที่ตั้งอยู่ในอาคารสำนักงานของผู้อื่นได้โดยผู้กระทำความผิดไม่ต้องเข้าไปทางกายภาพในอาคารของผู้เสียหายนั้น |

อย่างไรก็ตามอาชญากรรมทางคอมพิวเตอร์ในขณะนี้ยังไม่มีคำนิยามของคำว่า “อาชญากรรมทางคอมพิวเตอร์” ที่เป็นสากล แต่เพื่อให้เข้าใจในเรื่องของอาชญากรรมทางคอมพิวเตอร์ โดยเฉพาะอย่างยิ่ง เรื่องการกระทำความผิดต่อคอมพิวเตอร์ ที่เข้าไปเกี่ยวข้องกับการกระทำความผิดแบ่งออกเป็น 3 ลักษณะดังต่อไปนี้[21]

1. คอมพิวเตอร์ในฐานะที่เป็นวัตถุแห่งการกระทำความผิด (Computer as the target of the crime) ในกรณีนี้คือ การกระทำความผิดในรูปแบบต่าง ๆ ต่อข้อมูลคอมพิวเตอร์ ระบบ

[21] องอาจ เทียนหิรัญ, *อาชญากรรมทางคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์*, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2546), 14-15.

คอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ เช่น การเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยปราศจากอำนาจ การดักข้อมูลคอมพิวเตอร์ การจารกรรมข้อมูลคอมพิวเตอร์ การทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ เป็นต้น

2. คอมพิวเตอร์ในฐานะที่เป็นเครื่องมือที่ใช้ในการกระทำความผิด (Computer as a tool in the commission of a crime) การกระทำในกรณีนี้คือการกระทำความผิดในลักษณะที่หนึ่ง แต่ผู้กระทำได้ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด เพื่อให้สามารถกระทำความผิดได้โดยสะดวก หรือมีประสิทธิภาพมากยิ่งขึ้น (If a computer is a tool of the crime, the computer is used to commit and old crime in a high-tech way) เช่น การเผยแพร่ภาพลามกอนาจาร การพนันที่ผิดกฎหมาย การละเมิดลิขสิทธิ์ การฟอกเงิน เป็นต้น

3. คอมพิวเตอร์ในฐานะที่มีส่วนเกี่ยวข้องกับการกระทำความผิด (Computer as incidental to crime) การกระทำในกรณีนี้ คอมพิวเตอร์จะมีส่วนเกี่ยวข้องกับการกระทำความผิดไม่ว่าทางใดทางหนึ่ง โดยการใช้คอมพิวเตอร์จะทำให้การกระทำผิดเป็นไปด้วยความสะดวกและมีประสิทธิภาพยิ่งขึ้น อย่างไรก็ดี บทบาทของคอมพิวเตอร์นั้นไม่มีความสำคัญถึงขนาดที่ถ้าไม่มีคอมพิวเตอร์แล้วความผิดจะไม่สามารถเกิดขึ้นได้เลย กล่าวอีกนัยหนึ่งคือ แม้จะไม่มีการใช้คอมพิวเตอร์ การกระทำความผิดนั้นก็ยังคงสามารถเกิดขึ้นได้อยู่ดี เช่น การใช้คอมพิวเตอร์เก็บข้อมูลเกี่ยวกับลูกค้ายาเสพติด ลูกค้าที่เล่นการพนัน เป็นต้น

**2.1.3 รูปแบบของการกระทำความผิดบนอินเทอร์เน็ต**

อาชญากรรมที่กระทำผ่านเครือข่ายอินเทอร์เน็ตหรือการกระทำต่อเครื่องหรือระบบคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ตนั้น ถือได้ว่าเป็นอาชญากรรมทางคอมพิวเตอร์เช่นกัน เนื่องจากเครือข่ายอินเทอร์เน็ตเป็นส่วนหนึ่งของระบบคอมพิวเตอร์ ที่ทำให้คอมพิวเตอร์จำนวนมากสามารถเชื่อมโยงกันได้ทั่วโลก ซึ่งในขนาดนี้พบว่าเครือข่ายอินเทอร์เน็ตนั้นเป็นเครือข่ายที่ใหญ่ที่สุดในโลก และมีการเชื่อมต่อกันตลอดเพื่อเก็บรวบรวมข้อมูลหรือใช้ข้อมูล อาชญากรรมที่เกิดขึ้นโดยผ่านอินเทอร์เน็ตจึงอาจจะเป็นอาชญากรรมที่มีมากที่สุดในส่วนของอาชญากรรมคอมพิวเตอร์ด้วยกัน[22]

---

[22] พรรณสุวัชร รติพงศ์สิทธิ์, *อาชญากรรมทางคอมพิวเตอร์: ศึกษาวิเคราะห์หลักเกณฑ์ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...*, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, (กรุงเทพฯ: มหาวิทยาลัยรามคำแหง, 2550), 26.

การกระทำความผิดบนเครือข่ายหรือข้อมูลที่อยู่ในระบบดังกล่าว ซึ่งเป็นวิธีการที่ใช้ในการประกอบอาชญากรรมทางคอมพิวเตอร์ โดยทั่วไปแล้วสามารถจำแนกรูปแบบได้ดังนี้[23]

1. การสกัดหรือคัดเอาข้อมูลมาใช้ประโยชน์โดยมิชอบ (Illegal interception of information) เป็นการเข้าแทรกแซงข้อมูล และนำข้อมูลของผู้อื่นมาเป็นประโยชน์ต่อตนโดยมิชอบด้วยกฎหมาย เช่น การผ่านระบบรักษาความปลอดภัยบนอินเทอร์เน็ตเข้าไปเจาะล้วงความลับเกี่ยวกับรหัส หมายเลขบัตรเครดิต เพื่อนำมาเป็นประโยชน์ในการก่ออาชญากรรมต่อไปหรือการล้วงความลับทางการค้าซึ่งสามารถทำได้โดยผ่านทางอินเทอร์เน็ต อาจเป็นลักษณะของการดักฟังข้อมูลเพื่อนำมาเป็นประโยชน์กับกิจการของตัวเอง[24] เป็นต้น

2. การฉ้อโกงการโอนเงินทางอิเล็กทรอนิกส์ (Electronic funds transfer crime) การโอนเงินแบบนี้ใช้โอกาสเมื่อสามารถเข้าไปในเครือข่ายคอมพิวเตอร์ของธนาคารได้แล้ว จะใช้เทคโนโลยีทางคอมพิวเตอร์ไปเปลี่ยนแปลง คัดแปลงข้อมูลหรือป้อนทรัพย์สินหรือเงินจากบัญชีหนึ่งไปยังอีกบัญชีหนึ่งได้ โดยที่ไม่ได้มีการเปลี่ยนค่าทรัพย์สินกันจริง แต่ผลคือสามารถได้ทรัพย์สินนั้นมาด้วยการกระทำผ่านคอมพิวเตอร์บนอินเทอร์เน็ต

3. การลักลอบหรือขโมยการใช้บริการสารสนเทศ (Theft of information service) อาชญากรรมที่เป็นการขโมยข้อมูล ซึ่งหมายรวมถึงการขโมยข้อมูลจาก Internet Service Provider: ISP[25] หรือผู้ที่มีเว็บไซต์ในอินเทอร์เน็ต รวมไปถึงขโมยข้อมูลเพื่อใช้ประโยชน์ในการลักลอบใช้บริการ เช่น การขโมยข้อมูลเกี่ยวกับศูนย์โทรศัพท์ เพื่อแอบใช้บริการฟรี เป็นต้น

4. การละเมิดทรัพย์สินทางปัญญา เช่น การทำซ้ำโปรแกรมคอมพิวเตอร์ การละเมิดลิขสิทธิ์อื่น ๆ การปลอมแปลงรูป เสียง หรือการปลอมแปลงสื่อทางคอมพิวเตอร์ที่เรียกว่ามัลติมีเดีย (Multimedia)

5. การหลอกลวงขายสินค้าและการลงทุนผ่านเครือข่ายอินเทอร์เน็ต (Telemarketing fraud) การค้าขายหรือการชวนลงทุนโดยหลอกลวง อาชญากรใช้เครือข่ายอินเทอร์เน็ตเป็นสื่อในการปลอมประกาศโฆษณาโดยไม่ได้ให้บริการจริง ในประเทศสหรัฐอเมริกาอุตสาหกรรมใหญ่ ๆ

---

[23] วัลลิกา อุ่นศรี (เนติบันลือฤทธิ์), *ปัญหาการรวบรวมและพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีอาญา*, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2544), 44-46.

[24] Grabosky, P. N. & Smith, R. G., *Crime in the digital age*, (Australia: Transaction Publishers, 1998), 16.

[25] Internet Service Provider: ISP เป็นหน่วยงานที่ให้บริการเชื่อมต่อเข้ากับเครือข่ายอินเทอร์เน็ต หรือพูดอีกนัยหนึ่งคือ ทำหน้าที่เสมือนเป็นประตูเปิดการเชื่อมต่อให้บุคคลหรือองค์กรสามารถใช้งานอินเทอร์เน็ตได้, ดู สถาบันการพลศึกษา วิทยาเขตสุพรรณบุรี, *เทคโนโลยีสารสนเทศเพื่อการเรียนรู้ บทที่ 6 อินเตอร์เน็ต:ISP คืออะไร*, สืบค้นเมื่อ 3 ธันวาคม 2558, จาก http://www.ipesp.ac.th/learning/071001/chapter6/UN6_2.html

ได้รับผลกระทบในกิจการการค้า เพราะภัยจากพวกนี้มากในเครือข่าย (Bulletin boards) มีผู้ถูกหลอกหลายราย และพวกนี้สามารถทำเงินได้ดี การหลอกลวงแบบนี้ในอนาคตจะมีพัฒนาการอย่างต่อเนื่อง และเป็นโอกาสใหม่ของคนร้าย มากยิ่งขึ้น

6. การเผยแพร่สิ่งผิดกฎหมาย เช่น ภาพลามก และวิธีการทำระเบิดทางอินเทอร์เน็ต (Pornography and other offensive content) การใช้คอมพิวเตอร์และการสื่อสารผ่านทางคอมพิวเตอร์ซึ่งมีเครือข่ายทั่วโลกเผยแพร่ภาพลามกอนาจาร รวมถึงข้อมูลที่ไม่สมควร ซึ่งการจะเป็นภาพลามกอนาจารที่ไม่สมควรนั้น อาจจะมีปัญหาคุณค่าวัฒนธรรมของแต่ละสังคมว่าจะรับได้หรือไม่ รวมทั้งการใช้คอมพิวเตอร์บอกกล่าวข้อมูลที่ไม่สมควรจะเผยแพร่ เช่น วิธีการการก่ออาชญากรรมหรือสูตรในการผลิตระเบิด เป็นต้น

7. การทำลายและการก่อการร้ายทางอิเล็กทรอนิกส์ (Electronic vandalism and terrorism) พวกอันธพาลทางคอมพิวเตอร์หรือพวกก่อการร้ายจะเข้าไปในเครือข่ายคอมพิวเตอร์แล้วทำลายข้อมูลหรือตัดต่อ ดัดแปลงภาพ หรือทำสิ่งที่ไม่สมควรต่าง ๆ นานา เพื่อรบกวนผู้อื่นรวมถึงผู้ใช้อินเทอร์เน็ตเผยแพร่ข้อมูลข่มขู่ผู้อื่น ที่น่ากลัวที่สุดคือพวกที่ใช้เครื่องมือการสื่อสารผ่านคอมพิวเตอร์เข้าไปแทรกแซงทำลายระบบเครือข่ายของระบบสาธารณูปโภค ไม่ว่าจะเป็นเรื่องการจ่ายน้ำ จ่ายไฟฟ้าหรือการจราจร พวกนี้สามารถเข้าไปแทรกแซงในระบบที่ใช้คอมพิวเตอร์เหล่านี้ให้ขัดข้องได้

8. การฟอกเงินทางอิเล็กทรอนิกส์ (Electronic money laundering) เป็นการใช้อุปกรณ์ทางคอมพิวเตอร์และการสื่อสารเป็นเครื่องมือทำให้ผู้กระทำผิดกลบเกลื่อนอำพรางตัวตนของผู้กระทำผิดได้ง่ายขึ้น ยิ่งปัจจุบันการพาณิชย์ทางอิเล็กทรอนิกส์เจริญมากขึ้นไม่ว่าจะในยุโรปหรือในเอเชีย ทำให้เป็นการง่ายที่จะใช้การพาณิชย์ทางอิเล็กทรอนิกส์กลบเกลื่อนว่าทรัพย์สินที่ได้มาไม่ใช่มาจากการกระทำความผิดแต่เป็นสิ่งที่ได้ตอบแทนจากธุรกิจโอนเข้าบัญชีของผู้กระทำผิด

9. การใช้อินเทอร์เน็ตในการอำนวยความสะดวกแก่การประกอบอาชญากรรมดั้งเดิมหรืออาชญากรรมที่นำเอาการสื่อสารผ่านทางคอมพิวเตอร์มาขยายความสามารถในการกระทำของตน (Communications in Furtherance of Criminal Conspiracies) คือการที่อาชญากรรมนำเอาการสื่อสารผ่านทางคอมพิวเตอร์มาขยายความสามารถในการกระทำความผิดของตนที่ทำผิดทั่วไป เช่น ค้ายาเสพติด โดยใช้สื่ออิเล็กทรอนิกส์ปกปิด กลบเกลื่อนการทำงานของตนไม่ให้ผู้อื่นล่วงรู้ตั้งรหัสสื่อสารขึ้นมาเฉพาะในหมู่อาชญากรรมด้วยกัน ซึ่งความทันสมัยนี้ทำให้การกระทำทำไปได้อย่างรวดเร็ว โอกาสหลีกเลี่ยงการถูกจับกุมจึงสูง

นอกจากนี้อาชญากรรมทางอินเทอร์เน็ตที่พบมากอีกอย่างหนึ่งก็คือ สแปมเมล์ (Spam Mail) ซึ่งได้สร้างปัญหาให้แก่เจ้าของระบบคอมพิวเตอร์ที่มาในรูปแบบไปรษณีย์อิเล็กทรอนิกส์

หรือการส่งอีเมล์จำนวนมาก ๆ ในครั้งหนึ่งหรือทยอยส่งแต่ส่งจำนวนมากฉบับที่ผู้ส่งได้ส่งไปยังผู้รับ และมิได้รับความยินยอมจากผู้รับ ซึ่งมีวัตถุประสงค์ใหญ่ ๆ 3 ประการ ได้แก่[26]

1. การแสวงหาผลประโยชน์ในเชิงพาณิชย์ เนื่องจากผู้ประกอบการเห็นประโยชน์ของการส่งไปรษณีย์อิเล็กทรอนิกส์ให้แก่ผู้รับได้โดยสะดวก เสียค่าใช้จ่ายน้อย และสามารถเข้าถึงผู้รับได้ในวงกว้าง จึงได้ใช้ไปรษณีย์อิเล็กทรอนิกส์เพื่อการโฆษณาขายสินค้าหรือบริการที่มิชอบด้วยกฎหมาย เช่น การขายสินค้าหรือโฆษณาขายบริการทางเพศ การพนันออนไลน์ เป็นต้น

2. การเผยแพร่สื่อลามก ผู้ส่งจะส่งภาพหรือเนื้อหาลามกอนาจารให้แก่ผู้ใช้อินเทอร์เน็ต แต่ผู้ส่งมิได้แสวงหาผลประโยชน์ในเชิงพาณิชย์

3. การเผยแพร่ลัทธิความเชื่อ ผู้ส่งจะใช้ไปรษณีย์อิเล็กทรอนิกส์เป็นสื่อเพื่อแสดง และเผยแพร่แนวความคิดของตนให้แก่ผู้ใช้อินเทอร์เน็ต เพื่อชักจูงให้ผู้รับอีเมล์เข้าร่วมเป็นสมาชิกกับกลุ่มของตนหรือเพื่อรวบรวมบุคคลเพื่อก่อตั้งลัทธิทางความเชื่อขึ้นใหม่

**2.1.4 ผลของอาชญากรรมทางคอมพิวเตอร์**

เนื่องจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์นั้น โดยอาศัยเทคโนโลยีสารสนเทศนับวันยิ่งเพิ่มมากขึ้นอย่างรวดเร็ว และหลายรูปแบบ ซึ่งไม่สามารถตรวจพบหรือติดตามผู้กระทำความผิดได้อย่างง่ายจึงส่งผลกระทบต่อความเสียหายของสังคม นอกจากนี้อาชญากรรมทางคอมพิวเตอร์ยังส่งผลกระทบต่อความมั่นคง เศรษฐกิจ สังคมอันเนื่องมาจากการกระทำเพื่อผลประโยชน์แก่ตน การอยากทดลองความรู้ เป็นต้น

2.1.4.1 ความเสียหายที่เกิดขึ้นจากอาชญากรรมทางคอมพิวเตอร์นั้นไม่ใช่มีผลกระทบเพียงแต่ความมั่นคงของบุคคลใดบุคคลหนึ่งเท่านั้น แต่ยังมีผลกระทบต่อความมั่นคง ทั้งภายในและภายนอกประเทศโดยเฉพาะในส่วนที่เกี่ยวกับข่าวกรองหรือการจารกรรมข้อมูลต่าง ๆ ที่เกี่ยวกับความมั่นคงของปะเทศ

2.1.4.2 อาชญากรรมทางคอมพิวเตอร์อาจทำให้การดำเนินงานของธนาคารเกิดชะงักหรือข้อมูลทางการค้าของบริษัทเปลี่ยนแปลงไป สืบเนื่องจากการจารกรรมข้อมูล การหลอกหลวงทางอินเทอร์เน็ต เพื่อปลอมแปลงหรือปิดบังตัวตนในการละเมิดลิขสิทธิ์ การจารกรรมทรัพย์สินทางปัญญา การเลี่ยงภาษี การฟอกเงินอิเล็กทรอนิกส์ ซึ่งส่งผลกระทบต่อความเชื่อมั่น ความน่าเชื่อถือ และชื่อเสี่ยงทางด้านเศรษฐกิจ

---

[26] กรุง เหลืองมโนธรรม, *การศึกษาประเด็นทางกฎหมายเกี่ยวกับการจัดการความไม่มั่นคงของระบบคอมพิวเตอร์ในสังคมไทย: ศึกษาเฉพาะภัยไวรัสคอมพิวเตอร์แฮกเกอร์และสแปมเมล์*, สารนิพนธ์นิติศาสตรมหาบัณฑิต, (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2548), 23-24.

2.1.4.3 การกระทำผิดเกี่ยวกับคอมพิวเตอร์โดยเฉพาะที่เกี่ยวข้องกับการนำเข้าข้อมูลคอมพิวเตอร์ที่เป็นเท็จ การเผยแพร่ภาพลามกอนาจาร การตัดต่อหรือปลอมแปลงข้อมูลคอมพิวเตอร์ ซึ่งก่อให้เกิดความตื่นตระหนกกับประชาชนและสังคม ย่อมส่งผลให้ภาพพจน์ของประเทศถูกมองในแง่ลบ

## 2.2 แนวความคิดเกี่ยวกับกฎหมายบนอินเทอร์เน็ต

### 2.2.1 แนวความคิดที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์

หลังจากปี ค.ศ. 1969 ที่เทคโนโลยีอินเทอร์เน็ตเกิดขึ้นครั้งแรกและได้รับการพัฒนาเรื่อยมาจนอินเทอร์เน็ตได้กลายเป็นส่วนสำคัญในการทำงานในหน่วยงานของรัฐ และผู้ประกอบธุรกิจทั้งหลาย ในขนาดที่เทคโนโลยีชนิดนี้ได้สร้างความสะดวก และความเป็นอิสระในการแลกเปลี่ยนข้อมูลข่าวสารระหว่างผู้ประกอบธุรกิจทั้งหลาย โดยไม่จำเป็นต้องเดินทางไปพบกันโดยตรง แต่อีกด้านหนึ่งก็เป็นประโยชน์ต่อผู้กระทำความผิดที่ต้องการจารกรรมหรือลักลอบทำซ้ำข้อมูลเหล่านั้นไปใช้ประโยชน์ทางธุรกิจของตนหรือสร้างความเสียหายทางด้านการเงินต่อธุรกิจของผู้อื่น[27]

เนื่องจากการกระทำความผิดอันมีคอมพิวเตอร์เข้าไปเกี่ยวข้องนี้ได้เคยถูกขึ้นบัญชีให้อยู่ในกลุ่มของอาชญากรรมทางเศรษฐกิจหรือที่รู้จักกันในนาม อาชญากรรมคอเชิ้ตขาวหรืออาชญากรรมปกขาว “White Collar Crime” ซึ่งความหมายของอาชญากรรมทางเศรษฐกิจค่อนข้างกว้างครอบคลุมความผิดหลายอย่าง เป็นการกระทำที่สร้างความเสียหายทั้งแก่เศรษฐกิจของปัจเจกชน และประเทศชาติ มีลักษณะของการทำลายความเชื่อถือ ความมั่นคงทางเศรษฐกิจ เช่น ความผิดเกี่ยวกับการปลอมแปลงเงินตรา การปั่นหุ้น ความผิดเกี่ยวกับภาษีอากร ธุรกิจต่าง ๆ สถาบันการเงินเกี่ยวกับการค้าหรือธุรกิจเงินนอกระบบ เป็นต้น[28] นอกจากนี้อาชญากรรมทางเศรษฐกิจยังจัดอยู่ในประเภทอาชญากรรมอาชีพที่ใช้เทคนิคชั้นสูงผสมผสานกับผู้ที่มีความรู้มีประสบการณ์ มีความเชี่ยวชาญในอาชีพเพื่อกระทำความผิด และเป็นสิ่งที่กำหนดภาพพจน์ขึ้นใหม่ว่า อาชญากรรมนั้นไม่จำเป็นจะต้องเกิดขึ้นโดยบุคคลที่ยากจนในทางเศรษฐกิจและสังคมเสมอไป บุคคลที่อยู่ในฐานะเศรษฐกิจที่ดีก็สามารถก่ออาชญากรรมขึ้นได้[29]

---

[27] พรรณสุวัชร รติพงศ์สิทธิ์, *อาชญากรรมทางคอมพิวเตอร์: ศึกษาวิเคราะห์หลักเกณฑ์ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ....*, 11.

[28] สาวิตรี สุขศรี, *ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์*.

[29] ชัชวาลย์ สุขสมจิตร์, *อาชญากรรมทางเศรษฐกิจกับการบังคับใช้กฎหมาย*, , (กรุงเทพฯ: วิทยาลัยการยุติธรรม, ม.ป.ป.), 31.

จากเดิมที่ “อาชญากรรมคอมพิวเตอร์” ไม่ได้มีเครื่องมือพิเศษเพื่อเพิ่มศักยภาพในการกระทำความผิดและมักเป็นแค่เพียงการปลอมแปลงหรือการกระทำต่อเอกสารบัญชีการเงินการธนาคารและเอกสารอื่น ๆ เท่านั้น กลายเป็นอาชญากรรมเศรษฐกิจรูปแบบใหม่ ที่มีเทคโนโลยีคอมพิวเตอร์ และเครือข่ายอินเทอร์เน็ตเข้ามาเกี่ยวข้องจนสามารถขยายขอบเขตไปสู่ความเสียหายต่อเศรษฐกิจในด้านอื่น ๆ ด้วย ในยุคปัจจุบันจึงได้มีการจำแนกอาชญากรรมคอมพิวเตอร์ออกเป็นสองกลุ่มใหญ่ คือ กลุ่มความผิดที่ผู้กระทำอาศัยคอมพิวเตอร์เป็น “เครื่องมือ” และกลุ่มความผิดที่ระบบคอมพิวเตอร์ และข้อมูลที่อยู่ในคอมพิวเตอร์เป็น “เป้าหมาย” ของผู้กระทำผิด[30]

นับตั้งแต่นั้นเรื่อยมาจนถึงปัจจุบันจะเห็นได้ว่าความผิดสำคัญ ๆ ที่เกิดขึ้นบ่อยครั้งและได้รับความสนใจจากนักกฎหมายและนักวิชาการด้านอื่น ๆ ด้วย ได้แก่ การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ (Computer manipulation)[31] การก่อวินาศกรรมคอมพิวเตอร์ (Computer sabotage)[32] หรือการกรรโชกรีดไถทางคอมพิวเตอร์ การเข้าไปในระบบโดยปราศจากอำนาจ

---

[30] พรรณสุวัชร รติพงศ์สิทธิ์, *อาชญากรรมทางคอมพิวเตอร์: ศึกษาวิเคราะห์หลักเกณฑ์ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.* ...., 12.

[31] การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ (Computer manipulation) ตั้งเดิมเป็นการกระทำความผิดโดยเป้าหมายหลักของผู้กระทำความผิดยังคงอยู่ที่บัญชีด้านการเงินการธนาคารของบริษัท และผู้ประกอบธุรกิจต่าง ๆ อาทิ การกระทำความผิดด้วยการเปลี่ยนแปลงหรือการบิดเบือนข้อมูลการชำระเงิน การเปลี่ยนแปลงรายรับ-รายจ่าย การเปลี่ยนแปลงงบดุลบัญชี การเปลี่ยนแปลงรายการหรือสถานภาพการเงินของธนาคาร รวมทั้งการเปลี่ยนแปลงระบบบัญชีเงินสะสมต่าง ๆ และในระยะต่อมาขอบเขตการกระทำความผิด Computer manipulation ก็ได้รับการพัฒนาให้กว้างขวางยิ่งขึ้นอีก เช่น การกระทำความผิดต่อเครื่องเบิกเงินอัตโนมัติ หรือตู้เอทีเอ็ม (Automatic Teller Machine: ATM) รวมทั้งบัตรชำระเงิน หรือบัตรเครดิตประเภทต่าง ๆ และบริการโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต, สาวิตรี สุขศรี, *ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์*.

[32] การก่อวินาศกรรมอินเทอร์เน็ต (Computer sabotage) เป็นการกระทำความผิดด้วยวิธีปล่อยโปรแกรมไวรัส (Virus) หรือวอร์ม (Worm) ทำลายระบบหรือข้อมูลคอมพิวเตอร์ การกระทำความผิดในลักษณะนี้เริ่มขยายตัวมากขึ้นภายหลังจากระบบเครือข่ายคอมพิวเตอร์ได้รับการพัฒนา ทั้งนี้เพราะผู้กระทำความผิด เขียนโปรแกรมทำลายแค่เพียงครั้งเดียวแต่สามารถส่งต่อ เผยแพร่สร้างความเสียหายให้เหยื่อได้จำนวนมาก นอกจากโปรแกรมไวรัสและวอร์มแล้ว ปัจจุบันโปรแกรมทำลายอื่น ๆ ยังได้รับการพัฒนาออกมาอีกจำนวนมาก อาทิ Trojan Horse, Logic-Bomb หรือ Time-Bomb เป็นต้น , สาวิตรี สุขศรี, *ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์*.

(Computer hacking)[33] และการละเมิดลิขสิทธิ์ซอร์ฟแวร์ การลักลอบขโมยผลิตภัณฑ์ที่มีลิขสิทธิ์ รวมทั้งการเผยแพร่ข้อมูลที่ไม่ชอบด้วยกฎหมายในแง่มุมต่าง ๆ อาทิ ภาพลามกอนาจารเด็ก การพนัน การจำหน่ายอาวุธ หรือเผยแพร่ข้อมูลที่มีเนื้อหาแอบแฝงแนวคิดก้าวร้าวรุนแรง หรือแนวคิดในการดูหมิ่นชนชาติ การเลือกปฏิบัติ และการหมิ่นประมาท ผ่านสื่อบริการทั้งหลายบนเครือข่ายอินเทอร์เน็ต ซึ่งทำให้กฎหมายเก่าที่มีอยู่ไม่อาจใช้บังคับได้ครอบคลุมอีกต่อไป ปัญหาประเภทความแตกต่างระหว่างคำนิยามของเอกสารกับฐานความผิด การบุกรุกทางกายภาพกับการเจาะระบบคอมพิวเตอร์ ไปจนถึงการลักทรัพย์ที่มีรูปร่างกับการจารกรรม ทำซ้ำข้อมูลคอมพิวเตอร์ จึงกลายเป็นโจทย์ข้อใหญ่ที่หลายประเทศต้องขบคิด เพื่อแก้ไขปรับปรุงกฎหมายของตนให้สอดคล้อง[34]

**2.2.2 แนวความคิดในการควบคุมการกระทำความผิดบนอินเทอร์เน็ต**

การเติบโตอย่างรวดเร็วของอินเทอร์เน็ตในช่วงทศวรรษที่ผ่านมา จากในระยะเริ่มต้นซึ่งการใช้อินเทอร์เน็ตจำกัดอยู่ในกลุ่มนักวิจัยและนักวิชาการ ต่อมาได้ขยายการใช้งานไปสู่รัฐบาล ภาคธุรกิจ และประชาชนทั่วไป ในปัจจุบันนั้นได้ส่งผลให้อินเทอร์เน็ตกลายเป็นเครื่องมือที่ทรงประสิทธิภาพที่สามารถใช้สืบค้นข้อมูล ติดต่อสื่อสาร ประกอบพาณิชย์อิเล็กทรอนิกส์และธุรกรรมต่าง ๆ ตลอดจนเป็นแหล่งรวบรวมความบันเทิงที่หลากหลายที่สามารถเข้าถึงได้อย่างสะดวก และรวดเร็วจากทั่วทุกมุมโลก[35]

อย่างไรก็ตามนอกเหนือจากประโยชน์ของอินเทอร์เน็ตดังกล่าวในการเติบโตอย่างรวดเร็วของอินเทอร์เน็ตยังนำมาซึ่งปัญหาต่าง ๆ โดยทั่วไปปัญหาที่เกิดขึ้นทางอินเทอร์เน็ตปรากฏได้หลายรูปแบบแตกต่างกันไป ซึ่งเกิดขึ้นตามลักษณะของการใช้งานอินเทอร์เน็ต เนื่องจากพัฒนาการทางเทคโนโลยีที่ทันสมัยได้แผ่ขยายเข้าไปยังทุกภาคส่วนของสังคม และถูกนำไปใช้อย่างแพร่หลายใน

---

[33] การเจาะระบบหรือเข้าถึงระบบของผู้อื่นโดยปราศจากอำนาจ (Computer hacking) เป็นการกระทำเพื่อฝ่าระบบรักษาความปลอดภัยของผู้อื่น ในระยะแรก ๆ ผู้กระทำผิดส่วนใหญ่ไม่ได้มีเป้าหมายในการกระทำความผิดอย่างอื่น อาทิ เปลี่ยนแปลงข้อมูลเพื่อหลอกลวง ทำลายระบบ หรือจารกรรมข้อมูล แต่ผู้กระทำต้องการเพียงทดลองหรือทดสอบความสามารถของตน แต่เมื่อเทคโนโลยีด้านนี้ยังได้รับการพัฒนาต่อ รูปแบบการกระทำความผิดก็ย่อมมีการพัฒนาและขยายตัวไปด้วย การเจาะระบบก็เช่นเดียวกัน ปัจจุบันไม่มีแต่ระบบคอมพิวเตอร์เท่านั้นที่เป็นเป้าหมายของการกระทำความผิด ระบบให้บริการอื่น ๆ โดยเฉพาะอย่างยิ่งบริการโทรศัพท์ทางอินเทอร์เน็ต โทรศัพท์ทางไกล บริการจดหมายเสียงได้กลายเป็นเป้าหมายใหญ่ของนักเจาะระบบ และการเข้าถึงต่าง ๆ ดังกล่าวย่อมมิใช่เพียงแค่การทำลายระบบป้องกันหรือรักษาความปลอดภัยอย่างเดียวแบบเดิม แต่ผู้กระทำยังมีเป้าหมายเพื่อลักลอบใช้บริการเหล่านั้นโดยไม่ต้องเสียเงินอีกด้วย, สาวิตรี สุขศรี, *ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์*.

[34] สาวิตรี สุขศรี, *ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์*.

[35] Internet Governance, *โครงการศึกษาวิจัยการอภิบาลกิจการเกี่ยวกับอินเตอร์เน็ต (Internet Governance)*, สืบค้นเมื่อ 30 พฤศจิกายน 2557, จาก http://www.nectec.or.th/pld/igovernance/index.htm

ระดับโลก ก่อให้เกิดปัญหาใหม่ ๆ ที่สืบเนื่องจากอินเทอร์เน็ต ทำให้แนวคิดในการจัดระเบียบอินเทอร์เน็ต และสร้างความร่วมมือในการแก้ไขปัญหาที่เกิดขึ้นบนอินเทอร์เน็ตกลายเป็นประเด็นที่ได้รับความสนใจในระดับโลก จนเมื่อ พ.ศ. 2545 ที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติ (United Nations General Assembly) ได้ลงนามรับรองเพื่อเสนอให้มีการจัดประชุมระดับโลกเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารก่อนจะนำมาสู่การเกิดขึ้นของการประชุมสุดยอดโลกว่าด้วยสังคมสารสนเทศ (World Summit on Information Society: WSIS)[36] ครั้งที่ 1 ณ กรุงเจนีวา ประเทศสวิสเซอร์แลนด์ (At Geneva, Switzerland) ในเดือนธันวาคม พ.ศ. 2546 ภายใต้หัวข้อ “การกำกับดูแลอินเทอร์เน็ต (Internet Governance)”

เนื่องจากที่ประชุมสุดยอดโลกว่าด้วยสังคมสารสนเทศ ครั้งที่ 1 ขาดการนิยามขอบเขตของปัญหาที่ชัดเจน และมุมมองที่แตกต่างกันของรัฐบาลประเทศต่าง ๆ ต่อรูปแบบที่เหมาะสมในการบริหารจัดการอินเทอร์เน็ต จึงไม่สามารถหาข้อมติสำหรับประเด็นดังกล่าวได้ และมีมติให้จัดตั้งคณะทำงานเรื่องการกำกับดูแลอินเทอร์เน็ต (Working Group on Internet Governance: WGIG) ขึ้นเพื่อศึกษาประเด็นเรื่องการกำกับดูแลอินเทอร์เน็ตเพื่อนำมาพิจารณาต่อไปในการประชุมใหญ่ ครั้งที่ 2 ณ กรุงตูนิส ประเทศตูนิเซีย (At Tunis, Tunisia) ในเดือนพฤศจิกายน พ.ศ. 2548[37] และมีมติให้มีการก่อตั้งการประชุมร่วมเรื่องการอภิบาลอินเทอร์เน็ต (Internet Governance Forum: IGF) โดยมีวัตถุประสงค์ในการเป็นพื้นที่ให้กับผู้มีส่วนได้เสีย (Stakeholder) เข้ามาพูดคุยแลกเปลี่ยนความคิดเห็นเกี่ยวกับนโยบาย และการจัดการกำกับดูแลอินเทอร์เน็ต

ผลลัพธ์ของกระบวนการกำกับดูแลอินเทอร์เน็ตของคณะทำงานเรื่องการกำกับดูแลอินเทอร์เน็ต เป็นกระบวนการสหวิทยาการ (Multidisciplinary approach) ซึ่งกล่าวถึงหลักการกำกับดูแลอินเทอร์เน็ตในหลายมิติทั้งทางเทคนิค นโยบาย เศรษฐกิจ สถาบัน และกฎหมาย และแม้ประเด็นทางกฎหมายจะมิใช่ประเด็นแรกของการพิจารณาในการกำกับดูแลอินเทอร์เน็ตของคณะทำงานเรื่องการกำกับดูแลอินเทอร์เน็ต แต่ประเด็นในทางกฎหมายก็ได้ย่อมรับว่าเป็นส่วนหนึ่งของการกำกับดูแลอินเทอร์เน็ต ซึ่งได้อภิปรายในข้อกฎหมายเกี่ยวกับการกำกับดูแลอินเทอร์เน็ตและรายงานต่อที่ประชุมสุดยอดโลกว่าด้วยข้อมูลข่าวสารใน 2 กรณี ดังนี้

2.2.2.1 ประเด็นกฎหมายเกี่ยวกับอินเทอร์เน็ต ได้แก่ การละเมิดทรัพย์สินทางปัญญาบนเครือข่ายอินเทอร์เน็ต อาชญากรรมทางคอมพิวเตอร์ การคุ้มครองข้อมูลส่วนบุคคลบนเครือข่าย

---

[36] Thainetizen Network, *(สรุปสั้น ๆ) การมีส่วนร่วมในการจัดทำนโยบายอินเทอร์เน็ต:กระบวนการระดับภูมิภาคและระดับสากล#tcr2012*, (9 พฤศจิกายน 2555), สืบค้นเมื่อ 30 พฤศจิกายน 2557, จาก http://thainetizen.org/2012/09/internet-policy-making/

[37] Internet Governance, *โครงการศึกษาวิจัยการอภิบาลกิจการเกี่ยวกับอินเตอร์เน็ต (Internet Governance)*.

อินเทอร์เน็ต สิทธิส่วนบุคคลบนเครือข่ายอินเทอร์เน็ต รวมทั้งสิทธิของผู้บริโภคบนเครือข่ายอินเทอร์เน็ต เป็นต้น

2.2.2.2 กลไกทางกฎหมายสำหรับการกำกับดูแลอินเทอร์เน็ต ได้แก่ กฎเกณฑ์การควบคุมตนเองของกิจการบนเครือข่ายอินเทอร์เน็ต (Self-Regulation) อนุสัญญาระหว่างประเทศและเขตอำนาจศาล

อย่างไรก็ตามพัฒนาการทางด้านอินเทอร์เน็ตนับวันยิ่งมีความก้าวหน้าอย่างไม่หยุดยั้ง และภัยคุกคามนับวันก็ยิ่งเพิ่มมากขึ้นเช่นกัน การเพิ่มความร่วมมือกับผู้มีส่วนร่วม ไม่ว่าจะเกี่ยวข้องกับอินเทอร์เน็ตโดยตรงหรือไม่ก็ตาม ควรจะให้ความสนใจ และตื่นตัวเกี่ยวกับการกำกับดูแลอินเทอร์เน็ตให้มากขึ้น เนื่องจากอินเทอร์เน็ตได้เข้าสู่ชีวิตประจำวันของคนจำนวนมาก และเป็นปัจจัยสำคัญในการเข้าถึงข้อมูลข่าวสาร การพัฒนาทางเศรษฐกิจ และทางการเมือง

## 2.3 ทฤษฎีที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์

ปัญหาที่เกิดขึ้นในสังคมแต่ละสังคมย่อมมีความแตกต่างกันออกไป เช่นเดียวกันกับวิธีการควบคุมพฤติกรรมของสมาชิกในสังคมหนึ่ง ย่อมแตกต่างกันออกไปจากอีกสังคมหนึ่ง ทั้งในด้านวิธีการ และวัตถุประสงค์ด้วย วิธีการควบคุมพฤติกรรมของสมาชิกในสังคมนั้นมีอยู่มากมายหลายวิธีด้วยกัน แต่วิธีการควบคุมวิธีการหนึ่งที่นิยมใช้กันอยู่แพร่หลายในปัจจุบันคือวิธีการควบคุมโดยกฎหมายอาญา อาจจะกล่าวในที่นี้ได้ว่าทุก ๆ ประเทศย่อมมีกฎหมายอาญาใช้อยู่เป็นของตนเอง[38] ซึ่งถือว่าเป็นกฎหมายที่นานาประเทศใช้ควบคุมอาชญากรรมหลากหลายประเภท เช่นเดียวกับอาชญากรรมทางคอมพิวเตอร์ ซึ่งเป็นอาชญากรรมอีกประเภทหนึ่งที่สามารถสร้างความเสียหายแก่เศรษฐกิจ สังคม และประเทศชาติ และนานาประเทศให้ความสำคัญในการบัญญัติให้เป็นความผิดในทางอาญา

ด้วยเหตุนี้กฎหมายที่มีโทษทางอาญานั้นควรจะมีขอบเขตกว้างขวางเพียงใด หรือจำกัดแค่ไหนเพียงไรเกี่ยวกับการกำหนดฐานความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์นั้น เกี่ยวข้องกับแนวคิดทฤษฎีต่าง ๆ เช่น ทฤษฎีอาญา ทฤษฎีเกี่ยวกับการลงโทษ เป็นต้น ซึ่งการศึกษาทฤษฎีทางกฎหมายดังกล่าวจะช่วยให้สามารถวิเคราะห์ การกระทำใดควรเป็นความผิดอาญาหรือไม่ มาตรการที่เป็นอยู่เหมาะสมหรือไม่ที่จะนำมาใช้ ในส่วนนี้จึงเป็นการศึกษาถึงทฤษฎีทางกฎหมายที่เกี่ยวข้องกับการกำหนดฐานความผิดและการกำหนดบทลงโทษเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ดังนี้

---

[38] อภิรัตน์ เพ็ชรศิริ, *ทฤษฎีอาญา*, (กรุงเทพฯ: วิญญชน, 2548), 50.

**2.3.1 ทฤษฎีกฎหมายอาญา**

เนื่องจากกฎหมายอาญาเป็นกฎหมายที่ว่าด้วยความผิด และโทษ ในส่วนที่กล่าวถึงความผิดหมายถึง การที่กฎหมายบัญญัติห้ามไว้ไม่ให้กระทำการอย่างใดอย่างหนึ่ง นอกจากนี้กฎหมายอาญายังบัญญัติให้บุคคลต้องกระทำการอย่างใดอย่างหนึ่ง ถ้าไม่กระทำตามที่กฎหมายกำหนดในกรณีนั้น ๆ ย่อมจะมีความผิดเช่นกัน และในส่วนที่กล่าวถึงโทษนั้น เป็นสภาพบังคับของกฎหมายอาญา เพราะหากกฎหมายบัญญัติแต่การกระทำที่เป็นความผิดโดยไม่ได้กำหนดสภาพบังคับอันเป็นบทลงโทษไว้ กฎหมายย่อมไม่มีความหมายอย่างใด[39]

การกระทำเป็นจุดเริ่มต้นในการพิจารณาความผิดของบุคคล หากไม่มีการกระทำของบุคคลเลย ก็คงเป็นเพียงเหตุการณ์ซึ่งไม่ใช่เรื่องของกฎหมายที่จะไปจัดการหรือยุ่งเกี่ยวได้ อย่างไรก็ตามหลักที่ต้องมีการกระทำในความหมายของกฎหมายก็เพราะ[40]

1. กฎหมายไม่ต้องการลงโทษความคิด (Punishment of thought) หากแต่ประสงค์จะป้องกัน ยับยั้งผลร้ายอันอาจเกิดขึ้นแก่สังคมส่วนร่วม แต่ผลร้ายดังกล่าวไม่อาจเกิดขึ้นได้โดยลำพังความคิด ซึ่งเป็นเพียงจินตนาการของบุคคล ไม่กระทบกระเทือนความสงบสุขของส่วนร่วม ตราบที่ยังไม่มีการกระทำปรากฏให้เห็น

2. ปัญหาในเรื่องสภาพจิตในขณะกระทำความผิดนั้นยังไม่อาจพิสูจน์ให้เห็นแจ้งชัดเพื่อนำบุคคลมาลงโทษได้ ในบางกรณีแม้ว่าจะมีการกระทำแต่หากมิได้เกิดขึ้นโดยสมัครใจแล้วผลที่เกิดจากการนั้นก็ไม่อาจใช้ลงโทษได้

3. ยังไม่มีวิธีพิจารณาความใด ๆ ในโลกที่จะหยั่งทราบถึงจิตใจของผู้กระทำว่ามีเจตนาอย่างไรแน่ นอกเสียจากว่าผู้กระทำจะแสดงออกมาภายนอก กฎหมายไม่อาจลงโทษสิ่งที่ไม่แน่ชัดได้ การลงโทษได้นั้นจะต้องไม่เพียงแต่การคาดว่ามีอยู่ หากจะต้องสามารถนำมาพิสูจน์ให้ปรากฏได้

ดังนั้น ในการบัญญัติกฎหมายอาญาที่มีความผิดและโทษนั้น ซึ่งเป็นเรื่องเกี่ยวกับชีวิตร่างกาย สิทธิเสรีภาพ และทรัพย์สินของประชาชนนั้น มีหลักเกณฑ์สำคัญ ดังนี้

2.3.1.1 หลักไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย

หลักสำคัญที่ทำให้กฎหมายอาญามีลักษณะแตกต่างจากกฎหมายแพ่งหรือกฎหมายอื่น ๆ อีกประการหนึ่งที่จะคุ้มครองสิทธิเสรีภาพของประชาชนก็คือ หลักไม่มีความผิดและไม่มีโทษได้โดยไม่มีกฎหมาย ซึ่งมาจากภาษิตที่ว่า “*Nullum crimen, nulla poena, sine lege*” หรือเรียกย่อ ๆ ว่า “หลักไม่มีโทษโดยไม่มีกฎหมาย *Nulla poena, sine lege* (no punishment without law)” หลักที่ว่านี้

---

[39] แสวง บุญเฉลิมวิภาส, *หลักกฎหมายอาญา*, พิมพ์ครั้งที่ 3, (กรุงเทพฯ: วิญญูชน, 2544), 13.

[40] ทวิเกียรติ มีนะกนิษฐ, *มุมมองใหม่ในกฎหมายอาญา*, (กรุงเทพฯ: วิญญูชน, 2552), 39.

มีรากฐานกำเนิดมาจากยุคฟื้นฟูศิลปวิทยาการ คือราวศตวรรษที่ 18 อันเป็นช่วงเวลาที่รัฐต่าง ๆ ในยุโรปได้พัฒนาสู่รัฐสมัยใหม่ (modern state) แล้ว และหลักไม่มีโทษโดยไม่มีกฎหมายก็เป็นลักษณะสำคัญประการหนึ่งของกฎหมายสมัยใหม่ (modern law) ซึ่งนักคิด และนักนิติศาสตร์ในยุโรปได้พัฒนาคำสอนทางกฎหมายขึ้นมาเพื่อรับรองศักดิ์ศรีของความเป็นมนุษย์โดยถือว่า "รัฐ" หรือ "ผู้มีอำนาจ" จะจับกุมลงโทษประชาชนโดยอ้างว่าเขาเหล่านั้นทำผิดอย่างลอย ๆ โดยปราศจากข้อจำกัดไม่ได้ ถือว่าประชาชนจะต้องรับโทษก็แต่เฉพาะกรณีที่ตนได้กระทำอันกฎหมายกำหนดว่าเป็นความผิด และกำหนดโทษไว้โดยชัดแจ้งเท่านั้น จึงเท่ากับเป็นการป้องกันมิให้เจ้าหน้าที่ของรัฐใช้อำนาจจนเกินขอบเขต ซึ่งถือได้ว่าเป็นความสำเร็จที่น่าสังเกตประการหนึ่งของกฎหมายสมัยใหม่เกี่ยวกับความผิดทางกฎหมายอาญา[41]

ลักษณะการใช้บังคับกฎหมายอาญานั้น มีหลักการสำคัญที่ว่า "จะไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย *nullum crimen, nulla poena sine lege*"[42] กล่าวคือ ตามกฎหมายอาญาไม่ว่าจะเป็นประมวลกฎหมายอาญา หรือพระราชบัญญัติอื่นที่กำหนดถึงความผิดอาญาและโทษอาญา การกระทำจะเป็นความผิดต่อเมื่อมีกฎหมายที่บัญญัติในขณะกระทำว่าเป็นความผิด คือ ไม่มีผลย้อนหลังไปลงโทษบุคคลให้หนักขึ้นเป็นอันขาด แต่อาจย้อนหลังไปบัญญัติว่าการกระทำนั้น ๆ ไม่เป็นความผิด หรือเป็นความผิดแต่ยกโทษให้ หรือให้ลงโทษบุคคลน้อยกว่าที่กำหนดไว้ในกฎหมายที่ใช้อยู่ในขณะทำความผิดได้ เพราะเป็นคุณแก่ผู้กระทำผิด "จะไม่มีโทษโดยไม่มีกฎหมาย" กล่าวคือ บุคคลจะต้องรับโทษต่อเมื่อมีกฎหมายที่ใช้อยู่ในขณะกระทำบัญญัติให้ต้องรับโทษนั้น ๆ เช่น การกระทำความผิดที่มีแต่โทษปรับ ศาลก็ได้แต่ลงโทษปรับ ศาลจะลงโทษจำคุกซึ่งไม่ใช่โทษที่กฎหมายบัญญัติไว้ไม่ได้[43] เป็นต้น และถ้อยคำในกฎหมายอาญาจะต้องบัญญัติให้ชัดเจนแน่นอน ปราศจากความคลุมเครือ การที่จำต้องเรียกร้องให้บัญญัติกฎหมายอาญาให้ชัดเจนแน่นอนนี้ก็เพราะว่า การลงโทษทางอาญาเป็นมาตรการที่รุนแรงที่สุดของรัฐที่ใช้กับประชาชนในรัฐ ฉะนั้นรัฐจึงต้องบัญญัติกฎหมายอาญาให้ชัดเจนแน่นอนที่สุดเท่าที่สามารถจะทำได้ ในการบัญญัติกฎหมายอาญาจะต้องหลีกเลี่ยงการใช้ถ้อยคำกำกวมไม่แน่นอน ทั้งนี้เพื่อเป็นหลักประกันว่ากฎหมายที่

---

[41] แสวง บุญเฉลิมวิภาส, *หลักกฎหมายอาญา*, 17-18.

[42] เกียรติขจร วัจนะสวัสดิ์, *คำอธิบายกฎหมายอาญาภาค 1*, พิมพ์ครั้งที่ 7, (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2544), 16-21; บุญเพราะ แสงเทียน, *กฎหมายอาญา 1 (ภาคบทบัญญัติทั่วไป) แนวประยุกต์*, (กรุงเทพฯ: วิทยพัฒน์, 2545), 18.

[43] หยุด แสงอุทัย, *ความรู้เบื้องต้นเกี่ยวกับกฎหมายทั่วไป*, พิมพ์ครั้งที่ 15, (กรุงเทพฯ, มหาวิทยาลัยธรรมศาสตร์, 2545), 200; คณิต ณ นคร, *กฎหมายอาญา ภาคทั่วไป*, (กรุงเทพฯ, วิญญชน, 2543), 36.

บัญญัตินั้นตรงกับเจตจำนงของฝ่ายนิติบัญญัติอย่างแท้จริง และทั้งจะเป็นเครื่องป้องกันมิให้ศาลใช้กฎหมายตามใจชอบหรือตามความรู้สึกของตน[44]

2.3.1.2 การตีความกฎหมายอาญา

การตีความกฎหมาย คือ การค้นหาความหมายของกฎหมายที่มีถ้อยคำไม่ชัดเจนแน่นอน คือ กำกวมหรือมีความหมายได้หลายทาง เพื่อหยั่งทราบว่าถ้อยคำของบทบัญญัติของกฎหมายว่ามีความหมายอย่างไร[45] เหตุที่ต้องตีความกฎหมายก็เพราะว่า ฝ่ายนิติบัญญัติไม่สามารถรู้เหตุการณ์ล่วงหน้าที่เกิดขึ้นในภายหน้าได้ทุกกรณี จึงไม่สามารถบัญญัติกฎหมายให้ครอบคลุมทุกกรณี นอกจากนั้นฝ่ายนิติบัญญัติอาจมีความผิดพลาดในเรื่องการตรากฎหมายขึ้นใช้บังคับได้ เช่น บัญญัติกฎหมายไว้เคลือบคลุมหรือขัดแย้งกันเอง เช่นนี้ ในการใช้กฎหมายจึงต้องมีการตีความกฎหมาย

การตีความกฎหมายต้องพิเคราะห์ตัวอักษรให้ได้ความหมายของตัวอักษร และการจะรู้ความหมายของตัวอักษรได้ต้องพิเคราะห์เหตุผลหรือความมุ่งหมายของกฎหมายประกอบด้วย การตีความกฎหมายจึงต้องพิจารณาประกอบกันไป 2 ด้าน คือ (1) พิเคราะห์ตัวอักษร (2) พิเคราะห์ความมุ่งหมายของกฎหมาย (เจตนารมณ์ของกฎหมาย) จากที่กล่าวข้างต้นจึงมิได้หมายความว่าต้องพิจารณาตัวอักษรก่อน ถ้าไม่ชัดจึงดูความมุ่งหมายหากแต่ต้องตีความทั้งตัวอักษรและความมุ่งหมายไปด้วยกัน[46] และการตีความกฎหมายย่อมมีหลักเกณฑ์แตกต่างกันไปตามลักษณะของกฎหมาย ในที่นี้ขอแยกพิจารณาเป็น 2 ลักษณะคือ (1) การตีความกฎหมายทั่วไป และ (2) การตีความกฎหมายพิเศษ กฎหมายพิเศษ ในที่นี้ หมายถึง กฎหมายที่มีโทษอาญา ซึ่งโดยหลักได้แก่ ประมวลกฎหมายอาญา นอกจากนี้ยังรวมถึงกฎหมายอื่น ๆ ที่มีโทษทางอาญาด้วย

เหตุที่การตีความกฎหมายอาญามีลักษณะต่างไปจากการตีความกฎหมายทั่วไป ก็เพราะกฎหมายอาญามีวัตถุประสงค์ในการลงโทษบุคคล ซึ่งการลงโทษนั้นกระทบสิทธิของประชาชน จึงต้องใช้กฎหมายอาญาด้วยความระมัดระวัง กฎหมายอาญามีหลักเกณฑ์ในการตีความดังต่อไปนี้

1. กฎหมายอาญาต้องตีความอย่างเคร่งคัด ประมวลกฎหมายอาญา มาตรา 2 บัญญัติไว้ความตอนหนึ่งว่า “บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อ....” ซึ่งแสดงให้เห็นว่ากฎหมายอาญาต้องตีความโดยเคร่งคัดตามตัวอักษร กล่าวอีกนัยหนึ่งก็คือ ตัวบทกฎหมายบัญญัติไว้

---

[44] คณิต ณ นคร, *กฎหมายอาญา ภาคทั่วไป*, 50.

[45] หยุด แสงอุทัย, *ความรู้เบื้องต้นเกี่ยวกับกฎหมายทั่วไป*, แก้ไขปรับปรุงโดย สมยศ เชื้อไทย, พิมพ์ครั้งที่ 19, (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2556), 118.

[46] มานิตย์ จุมปา (บรรณาธิการ), *ความรู้พื้นฐานเกี่ยวกับกฎหมาย*, พิมพ์ครั้งที่ 8, (กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย, 2551), 100-111.

เช่นใดก็ต้องตีความเช่นนั้น นอกจากนั้นจะนำหลักการตีความในกฎหมายแพ่งและพาณิชย์มาใช้ในกฎหมายอาญาก็ไม่ได้

2. กฎหมายอาญาจะตีความให้เป็นการลงโทษหรือเพิ่มโทษผู้กระทำให้หนักขึ้นไม่ได้ กล่าวคือ การตีความกฎหมายอาญาที่ห้ามตีความให้เป็นโทษหรือเพิ่มโทษ

3. กฎหมายอาญาในกรณีเป็นที่สงสัยต้องตีความให้เป็นผลดีแก่ผู้ต้องหา ในกรณีที่บทบัญญัติที่มีโทษอาญาอาจตีความได้หลายนัย ศาลจะต้องตีความตามนัยที่เป็นผลดีแก่จำเลย

จะเห็นได้ว่ากฎหมายอาญาเป็นกฎหมายที่บัญญัติว่าการกระทำหรืองดเว้นการกระทำใดเป็นความผิดและกำหนดโทษไว้ ด้วยเหตุนี้ ในการบัญญัติกฎหมายต้องบัญญัติให้ชัดเจนแน่นอนที่สุดเท่าที่สามารถจะทำได้ หลีกเลี่ยงการใช้ถ้อยคำกำกวมไม่แน่นอนปราศจากความคลุมเครือ เนื่องจากว่า การลงโทษทางอาญาเป็นมาตรการที่รุนแรงที่สุดของรัฐที่ใช้กับประชาชน ฉะนั้นรัฐจึงต้องบัญญัติกฎหมายอาญาให้ชัดเจนแน่นอน นอกจากนี้ในการบังคับใช้กฎหมายอาญาต้องตีความโดยเคร่งครัด กล่าวคือต้องตีความเฉพาะการกระทำหรืองดเว้นเท่าที่ระบุไว้ในกฎหมายเท่านั้น จึงเป็นความผิด ศาลจะตีความกฎหมายอาญาในทางขยายความไปเอาผิดกับการกระทำซึ่งไม่เป็นความผิดมาลงโทษไม่ได้ หรือจะตีความย้อนหลังไปลงโทษการกระทำซึ่งขณะกระทำไม่เป็นความผิดไม่ได้เช่นเดียวกัน ขณะเดียวกันศาลจะตีความไปเพิ่มโทษผู้กระทำความผิดให้รับโทษหนักขึ้นก็ไม่ได้ด้วย

**2.3.2 ทฤษฎีการลงโทษทางอาญา**

ปรัชญาของกฎหมายอาญาที่มุ่งจะคุ้มครองป้องกันส่วนได้เสียต่าง ๆ ของสังคมให้พ้นจากการประทุษร้ายโดยถือเกณฑ์ความประพฤติในระดับหนึ่ง จึงเป็นมูลฐานของความผิดในกฎหมายอาญา เช่น การคุ้มครองความมั่นคงของรัฐ การคุ้มครองกระบวนการยุติธรรม เป็นต้น อย่างไรก็ตาม (โทษ) นับแต่โบราณกาลมาแล้วที่สังคมมนุษย์โดยทั่วไปตระหนักว่ากฎหมายอาญาเป็นสิ่งจำเป็นยิ่งต่อความสงบเรียบร้อยของสังคม มาตรการที่กฎหมายอาญานำมาใช้เพื่อคุ้มครองส่วนได้เสียของสังคม และชักนำให้สมาชิกของสังคมหันมาประพฤติในแนวทางที่ถูกที่ควรคือ การลงโทษซึ่งหมายถึง การที่รัฐทำให้ผู้กระทำความผิดต้องได้รับผลร้าย เพราะเหตุที่ผู้นั้นฝ่าฝืนกฎหมาย ทั้งนี้โดยมีเจตนาให้ผู้ที่ได้รับรู้ถึงว่าสิ่งนั้นเป็นผลเสีย โทษจึงเป็นลักษณะสำคัญประการหนึ่งของกฎหมายอาญา และทฤษฎีกฎหมายอาญา ในเรื่องโทษแบ่งได้เป็นทฤษฎีใหญ่ ๆ 3 ทฤษฎี[47] คือ ทฤษฎีเงื่อนไข ทฤษฎีเด็ดขาด และทฤษฎีสัมพันธ์

---

[47] มหาวิทยาลัยสุโขทัยธรรมาธิราช, *เอกสารการสอนชุดวิชา กฎหมายอาญา 1: ภาคบทบัญญัติทั่วไป หน่วยที่ 1-7*, (นนทบุรี: มหาวิทยาลัยฯ, 2548), 21-23.

1. ทฤษฎีเงื่อนไข ทฤษฎีนี้ไม่ได้พิจารณาในแง่การกระทำความผิด แต่พิจารณาในแง่ที่ควรลงโทษอย่างไรจึงจะเกิดประโยชน์ทั้งแก่ตัวผู้กระทำความผิดเองและแก่สังคมส่วนรวม การลงโทษจะต้องคำนึงถึงตัวผู้กระทำความผิดและสภาพแวดล้อมอื่นด้วย และโทษนั้นควรจะมีผลทำให้ผู้กระทำความผิดเกิดความหวาดกลัว ทำให้ผู้กระทำความผิดกลับตัวเป็นคนดี หรือทำให้สังคมปลอดภัยจากการกระทำความผิด ทฤษฎีเงื่อนไขจึงมีลักษณะมองไปในอนาคต เพื่อป้องกันมิให้มีการกระทำความผิดเกิดขึ้นอีก อาจจะโดยการข่มขู่ไม่ให้คนทั่วไปกระทำความผิดหรือแก้ไขผู้กระทำความผิดให้เป็นคนดี

2. ทฤษฎีเด็ดขาด ถือว่าการลงโทษเป็นสิ่งที่มีอยู่โดยธรรมชาติในความผิดทุกความผิด คือ เป็นผลที่หลีกเลี่ยงไม่ได้ของความผิดนั่นเอง ฉะนั้นผู้ใดกระทำความผิดจะต้องถูกลงโทษ

3. ทฤษฎีสัมพันธ์ (Relative theory) ไม่ใช่เฉพาะเรื่องจุดประสงค์ของการลงโทษเท่านั้น แต่ใช้ในเรื่องอื่น ๆ ด้วย ทฤษฎีนี้ถือว่าทุกสิ่งทุกอย่างในโลกนี้ไม่เด็ดขาด ทฤษฎีนี้ย่อมถูกต้องต่อเมื่อคำนึงถึงกาลเทศะและพฤติการณ์แวดล้อมต่าง ๆ ในส่วนที่เกี่ยวแก่จุดประสงค์ของการลงโทษ ทฤษฎีสัมผัสไม่ได้พิจารณาในแง่การกระทำความผิด แต่ได้พิจารณาในแง่ที่ว่าควรจะลงโทษอย่างใดจึงเกิดประโยชน์และด้วยเหตุนั้นการลงโทษจึงต้องคำนึงถึงตัวผู้กระทำความผิดกับเพื่อนมนุษย์อื่น ๆ โทษนั้นควรจะมีผลเป็นการกระทำให้ผู้กระทำความผิดหวาดกลัว ทำให้ผู้กระทำความผิดกลับตัวเป็นคนดี หรือทำให้สังคมปลอดภัยจากการกระทำความผิด ทั้งนี้เพื่อเป็นการป้องกันขัดขวางมิให้มีการกระทำความผิดเกิดขึ้นอีก[48]

นอกจากนี้ในการกำหนดโทษที่จะลงต่อผู้ที่ได้กระทำผิดกฎหมายแล้ว การลงโทษผู้กระทำความผิดนั้นมีอยู่ด้วยกันหลายวิธีและมีการพัฒนารูปแบบของการลงโทษตามยุคสมัย[49] โดยวัตถุประสงค์ของการลงโทษมีหลายประการด้วยกัน คือ

2.3.2.1 เพื่อเป็นการแก้แค้นทดแทน เป็นหลักการลงโทษที่เก่าแก่ที่สุด ทั้งนี้เป็นไปตามแนวความคิดที่ว่า ผู้ใดกระทำผิดการใดย่อมได้รับผลตอบแทนการกระทำนั้น การลงโทษเพื่อเป็นการแก้แค้นทดแทนนั้นจะได้ผลต่อเมื่อได้กระทำโดยรวดเร็วและรุนแรง มิฉะนั้นแล้วประชาชนก็อาจขาดความเชื่อมั่นในกระบวนการยุติธรรมของบ้านเมือง และอาจหาทางแก้แค้นผู้กระทำผิดด้วยตนเองก็ได้

---

[48] หยุด แสงอุทัย, *กฎหมายอาญา ภาค 1*, พิมพ์ครั้งที่ 18, (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2544), 249-251.

[49] สำนักกฎหมายนิติศาสตร์ขาดรัก, *กฎหมายอาญา: วัตถุประสงค์ของการลงโทษ*, (1 มิถุนายน 2557), สืบค้นเมื่อ 6 มิถุนายน 2558, จาก http://chalermwutsa.blogspot.com/2014/06/blog-post.html

2.3.2.2 เพื่อเป็นการข่มขู่ตัวผู้กระทำความผิดนั้นเองให้เกิดความเข็ดหลาบ ไม่กล้ากระทำความผิดซ้ำขึ้นอีก และเพื่อเป็นตัวอย่างให้คนทั่วไปเห็นว่าเมื่อกระทำผิดแล้วจะต้องได้รับโทษเพื่อคนทั่วไปที่ได้ทราบจะได้เกรงกลัว ไม่กล้ากระทำผิดขึ้น

2.3.2.3 เพื่อเป็นการคุ้มครองสังคมให้พ้นจากภยันตรายในระหว่างที่ผู้กระทำถูกตัดขาดจากสังคมไป โดยการลงโทษประหารชีวิต จำคุกตลอดชีวิต หรือจำคุกมีกำหนดเวลา เป็นการคุ้มครองมิให้ผู้กระทำผิดกลับมาทำร้ายหรือเป็นภยันตรายต่อสังคมอีกต่อไปหรือชั่วระยะเวลาหนึ่ง

2.3.2.4 เพื่อเป็นการปรับปรุงแก้ไขตัวผู้กระทำความผิดให้กลับตัวเป็นพลเมืองดีเพราะผู้ที่ถูกจำคุกส่วนมากจะต้องถูกปล่อยตัวกลับมาสู่สังคมอีกในวันใดวันหนึ่ง

จากทฤษฎีดังกล่าวจะเห็นได้ว่าการลงโทษทางอาญาเป็นสภาพบังคับหลักทางอาญาที่ใช้กับการกระทำที่เป็นความผิดทางอาญา ซึ่งการลงโทษเป็นการดำเนินให้เป็นไปตามกฎหมาย เป็นการรักษากฎระเบียบ แบบแผนของสังคม และเป็นการป้องกันให้สังคมปลอดภัย รวมทั้งเป็นการป้องกันอาชญากรรมมิให้เกิดขึ้น

## 2.4 ความสำคัญของการมีกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

เหตุผลและความจำเป็นในการบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์ เนื่องจากอาชญากรรมทางคอมพิวเตอร์นั้นมีลักษณะแตกต่างจากอาชญากรรมในรูปแบบดั้งเดิม เช่น การปล้น ฆ่า ลักทรัพย์ ชิงทรัพย์ ข่มขืน ซึ่งสาเหตุส่วนใหญ่ตามทฤษฎีอาชญาวิทยาแบบดั้งเดิม เชื่อว่า เกิดจากความยากจน การขาดการศึกษา มีสภาพความเป็นอยู่ทางสังคมและเศรษฐกิจไม่ดี[50] แต่อาชญากรรมทางคอมพิวเตอร์นั้น ผู้กระทำความผิดส่วนใหญ่จะต้องเป็นผู้มีความรู้ ความชำนาญ มีการศึกษาที่ดี และนอกจากนี้ความเสียหายที่เกิดจากอาชญากรรมทางคอมพิวเตอร์นั้นจะเกิดในลักษณะเป็นวงกว้าง เนื่องจากระบบคอมพิวเตอร์นั้นมีการเชื่อมต่อกันไปทั่วโลก การกระทำความผิดจึงสามารถเกิดกับผู้เสียหายครั้งละเป็นจำนวนมาก มูลค่าของความเสียหายก็จะเกิดขึ้นมากตามไปด้วย

อย่างไรก็ตาม ความเสียหายที่เกิดขึ้นจากอาชญากรรมทางคอมพิวเตอร์นั้น อาจก่อให้เกิดความเสียหายให้แก่บุคคลหนึ่งหรือส่งผลกระทบแก่ความมั่นคงของชาติ และความสงบเรียบร้อยของสังคม ซึ่งการกระทำดังกล่าวมีการเปลี่ยนแปลงไปจากการกระทำความผิดรูปแบบเดิม ด้วยเหตุนั้นเพื่อให้มีประสิทธิภาพในการใช้คอมพิวเตอร์ และอินเทอร์เน็ตดังกล่าว จึงจำเป็นที่จะต้องวาง

---

[50] อัจฉรียา ชูตินันทน์, *อาชญาวิทยาและทัณฑวิทยา*, พิมพ์ครั้งที่ 2, (กรุงเทพฯ: วิญญูชน, 2557), 78.

หลักเกณฑ์หรือพิจารณาเกี่ยวกับมาตรการที่สามารถควบคุมอาชญากรรมทางคอมพิวเตอร์ เพื่อให้เกิดวินัยในการใช้คอมพิวเตอร์ของคนในสังคม

จากการที่สังคมโลกในปัจจุบันได้มีการพัฒนาไปในทุก ๆ ด้านโดยเฉพาะเทคโนโลยีการสื่อสารต่าง ๆ ทำให้มนุษย์มีความสะดวกสบายมากยิ่งขึ้นกว่าในอดีต แต่การพัฒนาเทคโนโลยีอย่างไม่หยุดยั้งเพื่อแสดงให้เห็นถึงความก้าวหน้า ขนาดเดียวกันการกระทำความผิดก็พัฒนาขึ้นเพื่อให้ได้มาซึ่งสิ่งที่ตนเองต้องการอย่างผิดกฎหมาย ทำให้กฎหมายที่มีและบังคับใช้ในปัจจุบันก้าวไม่ทันการกระทำผิดดังกล่าว และจากการศึกษายังพบอีกว่าลักษณะของการกระทำผิดในปัจจุบันมีการใช้เทคโนโลยีสารสนเทศในรูปแบบอินเทอร์เน็ตเข้ามามีส่วนร่วมด้วยในการกระทำผิด ซึ่งมีลักษณะแตกต่างจากอดีต การที่การกระทำผิดต้องมีการกระทำทางกายภาพ มีการเคลื่อนไหวร่างกายเพื่อให้ได้มาซึ่งทรัพย์สิ่งของต่าง ๆ โดยการนำทรัพย์สิ่งของนั้นเคลื่อนที่ไปด้วย แต่การกระทำผิดโดยใช้คอมพิวเตอร์และอินเทอร์เน็ตมิได้มีลักษณะเช่นนั้น ประกอบกับทฤษฎีอาญาวิทยาแบบดั้งเดิมเชื่อว่าสาเหตุของการกระทำผิดเกิดจากความยากจน การขาดการศึกษาอบรม มีสภาพความเป็นอยู่ทางเศรษฐกิจที่ไม่ดี เป็นต้น ทำให้บุคคลที่มีลักษณะเช่นนั้นประกอบอาชญากรรมขึ้นโดยง่าย แต่ในทางตรงกันข้ามการก่ออาชญากรรมโดยมีคอมพิวเตอร์และอินเทอร์เน็ตเป็นสื่อกลางในการกระทำความผิดนี้ เรียกว่า “อาชญากรรมทางคอมพิวเตอร์” เกิดขึ้นจากบุคคลที่มีความรู้ความสามารถเป็นอย่างดีเกี่ยวกับคอมพิวเตอร์และการใช้งานทางอินเทอร์เน็ต ซึ่งบุคคลผู้กระทำความผิดทางคอมพิวเตอร์นี้มักจะมีฐานะทางเศรษฐกิจดีและมีการศึกษาสูง และมีหน้าที่การงานอย่างมั่นคง จึงมักเรียกกันในทางอาชญาวิทยาใหม่ว่า “อาชญากรรมคอเชิ๊ตขาวหรืออาชญากรรมปกขาว” ซึ่งผลของการกระทำผิดทางคอมพิวเตอร์นี้มักมีความรุนแรง และกระทบต่อสังคมส่วนรวมทั้งภายในและภายนอกประเทศ ทั้งยังส่งผลในแง่ลบต่อความเชื่อมันของประเทศอีกด้วย

ด้วยเหตุนี้ นานาชาติจึงได้เห็นถึงความสำคัญของการร่วมมือกันป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ เป็นเหตุให้สหประชาชาติได้จัดการประชุมเกี่ยวกับเรื่องอาชญากรรมทางคอมพิวเตอร์ขึ้นและมีการตั้งคณะทำงานเรื่องการกำกับดูแลอินเทอร์เน็ต เพื่อให้การใช้งานทางอินเทอร์เน็ตของประเทศภาคีทั้งหลายเป็นไปด้วยความเรียบร้อย อย่างไรก็ตามประเด็นของข้อกฎหมายเกี่ยวกับการป้องกันและปราบปรามนั้นก็ได้รับการเอาใจใส่อย่างจริงจัง แต่ก็ยังมีความไม่ชัดเจนนัก กระนั้นสหประชาชาติก็มิได้ลดละแต่อย่างใด โดยได้มีการจัดการประชุมขึ้นเป็นครั้งคราว และได้มีการจัดทำ “คู่มือการป้องกันและควบคุมอาชญากรรมทางคอมพิวเตอร์ (UN Manual on the Prevention and Control of Computer-related Crime)” ขึ้น เพื่อให้เป็นแนวปฏิบัติแก่ทั้งคณะทำงานและประเทศภาคีสมาชิกในอันที่จะตรากฎหมายขึ้นภายในประเทศตน

ดังนั้น จะเห็นได้ว่าความเสียหายหรือผลกระทบของอาชญากรรมทางคอมพิวเตอร์ทำให้หน่วยงานระหว่างประเทศและประเทศต่าง ๆ มีการตรากฎหมายข้อบังคับใช้ภายในเพื่อป้องกันและปราบปรามอาชญากรรมดังกล่าวมิให้ขยายวงกว้างยิ่งขึ้น โดยในบทต่อไปจะได้กล่าวถึงบทบัญญัติทางกฎหมายและหลักเกณฑ์เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ระดับระหว่างประเทศและระดับภูมิภาคระหว่างประเทศ (กฎหมายของสหภาพยุโรป) และระดับประเทศ (กฎหมายของประเทศสิงคโปร์ และประเทศไทย) ต่อไป

# บทที่ 3

# บทบัญญัติทางกฎหมาย และหลักเกณฑ์เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ระดับระหว่างประเทศ ประเทศสิงคโปร์ และประเทศไทย

อาชญากรรมทางคอมพิวเตอร์เป็นปัญหาหนึ่งที่ทั้งองค์กรระหว่างประเทศ และประเทศต่าง ๆ ให้ความสำคัญ มีการร่วมมือกันในการป้องกันและปราบปรามอย่างจริงจัง โดยมีการตรากฎหมายขึ้นบังคับใช้ เพื่อเป็นเครื่องมือช่วยลดปัญหาอาชญากรรมดังกล่าวลง และควบคุมการใช้เทคโนโลยีการสื่อสารผ่านอินเทอร์เน็ตให้อยู่ในความเรียบร้อยมิให้ใช้เทคโนโลยีดังกล่าวไปในทางที่มิชอบอันก่อให้เกิดผลกระทบต่อส่วนร่วมและสร้างความเสียหายให้แก่ประเทศชาติ ซึ่งต่อไปในบทนี้จะได้กล่าวถึงหลักเกณฑ์สากลที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ บทบัญญัติทางกฎหมายและหลักเกณฑ์เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศสิงคโปร์และประเทศไทย โดยมีรายละเอียดดังนี้

## 3.1 หลักเกณฑ์สากลที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

สืบเนื่องจากสถานการณ์ของโลกมีการเปลี่ยนแปลงอย่างรวดเร็ว การพัฒนาด้านเทคโนโลยีส่งผลกระทบต่อระบบเศรษฐกิจ สังคม การเมือง วัฒนธรรม สิ่งแวดล้อม ไปตลอดถึงการก่ออาชญากรรม ซึ่งพัฒนาจากการใช้ความรุนแรงทางด้านกายภาพ มาเป็นการใช้เทคโนโลยีคุณภาพสูงในการก่ออาชญากรรมทางคอมพิวเตอร์ ซึ่งอาศัยช่องว่างของกฎหมายเพื่อปิดบังความผิดของตน เกิดอาชญากรรมที่ก่อให้เกิดความเสียหายทางเศรษฐกิจที่มีมูลค่ามหาศาล ส่งผลกระทบต่อประชาชนเป็นจำนวนมาก มีอิทธิพล และเครือข่ายองค์กรโยงใยทั้งภายในและภายนอกประเทศ ดังนั้น หน่วยงานต่าง ๆ จึงได้เล็งเห็นความสำคัญของปัญหาดังกล่าวดังต่อไปนี้

### 3.1.1 องค์การสหประชาชาติ (United Nations: UN)

องค์การสหประชาชาติได้เล็งเห็นถึงปัญหาทางด้านเทคนิค และการบังคับใช้กฎหมายอาชญากรรมที่เกี่ยวข้องกับการใช้คอมพิวเตอร์โดยมิชอบมาเป็นระยะเวลาอย่างน้อย 4 ครั้งการ

ประชุม ด้วยเหตุนี้จึงได้เริ่มพัฒนากรอบนโยบายด้านอาชญากรรมทางคอมพิวเตอร์ ซึ่งในการประชุมสหประชาชาติครั้งที่ 8 ว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อผู้กระทำผิด (8th United Nation Congress on the Prevention Of Crime and Treatment of Offenders) ที่จัดขึ้น ณ กรุงฮาวานา ประเทศคิวบา (Havana, Cuba) ระหว่างวันที่ 27 สิงหาคม ถึง 7 กันยายน พ.ศ. 2533 สมัชชาสหประชาชาติ (United Nation General Assembly) ได้กำหนดมาตรการเกี่ยวกับอาชญากรรมคอมพิวเตอร์ และรับเอาข้อมติในเรื่องแนวทางการออกกฎหมายเพื่อรับมือกับอาชญากรรมทางคอมพิวเตอร์บนพื้นฐานของมติการประชุมที่ 45/121 โดยหนึ่งในหลายเรื่องที่ข้อมติได้กล่าวถึงข้อเสนอแนะของการประชุมสหประชาชาติครั้งที่ 8 ว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อผู้กระทำผิด ซึ่งในมติของที่ประชุมเรียงร้องให้นานาประเทศเพิ่มความพยายามในการต่อสู้กับอาชญากรรมทางคอมพิวเตอร์ให้มีประสิทธิภาพมากขึ้น ซึ่งนับเป็นการกล่าวถึงเรื่องอาชญากรรมทางคอมพิวเตอร์เป็นครั้งแรกในมติของสหประชาชาติ ก่อนอินเทอร์เน็ตจะเปิดให้เอกชนได้ใช้งานเสียอีก[51]

ด้วยเหตุนี้สหประชาชาติได้นำแนวคิดดังกล่าวมาจัดทำ “คู่มือการป้องกันและควบคุมอาชญากรรมทางคอมพิวเตอร์ (UN Manual on the Prevention and Control of Computer-related Crime)” ออกเผยแพร่ในปี พ.ศ. 2537[52] ซึ่งมีเนื้อหาเกี่ยวกับแนวทางการบัญญัติถึงฐานความผิด และกฎหมายวิธีพิจารณาความ การป้องกันอาชญากรรมผ่านการรักษาความปลอดภัยของข้อมูลที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ รวมไปถึงกลไกความร่วมมือระหว่างประเทศในการนิยามรูปแบบของอาชญากรรมทางคอมพิวเตอร์ เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การสำเนาโปรแกรมคอมพิวเตอร์ การฉ้อโกง การปลอมแปลง และการก่อวินาศกรรมคอมพิวเตอร์ เป็นต้น

ในวันที่ 4 ธันวาคม พ.ศ. 2543 ได้มีการประชุมทั่วไปขององค์การสหประชาชาติ ในหัวข้อ “การรับมือกับการใช้เทคโนโลยี ข้อมูลข่าวสารในทางที่ผิดของอาชญากร”[53] และได้มีมติเลขที่ 55/63 ซึ่งมีเนื้อหาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์หลายประการ ดังนี้

1. รัฐควรสร้างกฎหมายและวิธีดำเนินการเพื่อทำลายแหล่งหลบภัยของผู้ซึ่งกระทำผิดโดยอาศัยเทคโนโลยีข้อมูลข่าวสารเป็นเครื่องมือ

---

[51] Lennon, L. Y.-c., *Cybercrime in the greater China region: Regulatory responses and crime prevention across the Taiwan strait*, (United Kingdom: Edward Elgar publishing, 2012), 90.

[52] United Nations, International review of criminal policy, *The United Nations manual on computer-related crime*, *43-44*(1994), Retrieved February 23, 2014, from http://www.uncjin.org/Documents/EighthCongress.html.

[53] “Combating the criminal misuse of information technology”, UN General Assembly (4 December 2000) Resolution 55/63.

2. ระบบยุติธรรมควรมีมาตรการคุ้มครองความลับ ความสมบูรณ์ และสภาพพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์ จากการเข้ามาสร้างความเสียหายโดยไม่ได้รับอนุญาต และรับรองว่าการกระทำผิดของอาชญากรต้องได้รับการลงโทษ

ต่อมาการประชุมทั่วไปของสหประชาชาติ ในวันที่ 19 ธันวาคม พ.ศ. 2544 ได้มีมติเลขที่ 56/121 ซึ่งมีเนื้อหาชักชวนให้ประเทศสมาชิกออกกฎหมาย นโยบายหรือแนวทางปฏิบัติระดับชาติในการรับการใช้ข้อมูลข่าวสารเพื่อกระทำความผิดของอาชญากร นำเอาข้อมูลต่าง ๆ ที่เกิดจากการประชุมของคณะกรรมการป้องกันอาชญากรรมและกระบวนการทางอาญามาพิจารณาประกอบการออกกฎหมาย นโยบายหรือแนวทางปฏิบัติ[54]

**3.1.2 สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunications Union: ITU)**

ITU ก่อตั้งเมื่อปี ค.ศ.1865 ที่กรุงปารีส ประเทศฝรั่งเศส (Paris, France) โดยในครั้งแรกใช้ชื่อว่า “สหภาพโทรเลขระหว่างประเทศ (International Telegraph Union)” และต่อมาเมื่อปี ค.ศ. 1934 ได้เปลี่ยนชื่อเป็น “สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunications Union)” เป็นองค์กรชำนาญพิเศษ (Specialized Agencies) ที่อยู่ภายใต้การกำกับของสหประชาชาติ เมื่อปี ค.ศ. 1947[55] ปัจจุบันขอบเขตการทำงานของ ITU ขยายจากโทรเลขและโทรศัพท์ มาเป็นการสื่อสารผ่านดาวเทียม มือถือ อินเทอร์เน็ต การสื่อสารในช่วงภัยพิบัติ การใช้งานเทคโนโลยีสารสนเทศ และยังมีบทบาทมากที่สุดในการทำงานเกี่ยวกับการสร้างมาตรฐานกลางของระบบการรักษาความปลอดภัยไซเบอร์ของโลก รวมถึงการออกกฎหมายอาชญากรรมทางอินเทอร์เน็ตด้วย

นอกจากนั้น ITU ยังมีเป้าหมายในการสร้างมาตรฐานกลางของกรอบความร่วมมือระหว่างประเทศในการรักษาความปลอดภัยไซเบอร์ และเพื่อที่จะบรรลุถึงความเข้าใจร่วมกันในปัญหาภัยคุกคามทางอินเทอร์เน็ตของนานาประเทศในทุกระดับของการพัฒนาเศรษฐกิจ ซึ่งรวมไปถึงการ

---

[54] “…invites Member States, when developing national laws, policy and practices, to combat the criminal misuse of information technologies, to take into account, *inter alia*, the work and achievements of the Commission on Crime Prevention and Criminal Justice.”, UN General Assembly (19 December 2001) Resolution 56/121.

[55] สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ, *ความรู้ทั่วไปเกี่ยวกับการกำกับดูแลกิจการโทรคมนาคมและการออกใบอนุญาตประกอบกิจการโทรคมนาคม*, (กรุงเทพฯ: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, 2552).

พัฒนา และนำไปปฏิบัติโดยแนวทางการแก้ไขปัญหาที่มุ่งเน้นไปยังการระบุปัญหาอาชญากรรมทางคอมพิวเตอร์ และความปลอดภัยไซเบอร์ในฐานะที่เป็นภัยคุกคามของโลก[56]

ในการประชุมผู้บริหารระดับโลกว่าด้วยการโทรเลขและโทรศัพท์ พ.ศ. 2531 (1988 World Administrative Telegraph and Telephone Conference: WATTC-88) ณ กรุงเมลเบิร์น ประเทศออสเตรเลีย (Melbourne, Australia) ได้มีการอนุมัติกฎข้อบังคับว่าด้วยโทรคมนาคมระหว่างประเทศ (International Telecommunication Regulations: ITRs) ซึ่งมีเนื้อหาครอบคลุมเรื่องหลักการทั่วไป และคำนิยามของกิจการโทรคมนาคมระหว่างประเทศ และกำหนดเงื่อนไข แนวทางการบังคับใช้ ข้อห้าม ฯลฯ[57] เช่น กำหนดมาตรฐานของคุณภาพในการบริการในระดับสากล ความพอเพียงของการให้บริการ จัดสรรเส้นทางของสัญญาณระหว่างประเทศ และยังกำหนดมาตรฐานในการลำดับความสำคัญในด้านความปลอดภัย กำหนดแนวทางในการหลีกเลี่ยงอันตรายต่อระบบเครือข่าย และการบริการต่าง ๆ เป็นต้น

เนื่องจากพัฒนาการทางเทคโนโลยีได้มีการเปลี่ยนแปลงไปอย่างรวดเร็ว ทำให้กฎข้อบังคับว่าด้วยโทรคมนาคมระหว่างประเทศมีเนื้อหาไม่ทันสมัย เมื่อเทียบกับการขยายตัวของเทคโนโลยีด้านโทรคมนาคม ดังนั้นในการประชุมสากลอย่างเป็นทางการว่าด้วยการโทรคมนาคมระหว่างประเทศในปี ค.ศ. 2012 (พ.ศ. 2555) (2012 World Conference on International Telecommunication: WCIT-12) ณ กรุงดูไบ ประเทศสหรัฐอาหรับเอมิเรตส์ (Dubai, United Arab Emirates) ระหว่างวันที่ 3-14 ธันวาคม พ.ศ. 2555 มีเป้าหมายที่จะเปิดโอกาสให้ประเทศสมาชิก[58] ได้เข้าร่วมแสดงความคิดเห็น เพื่อปรับปรุงแก้ไขข้อตกลง ITRs[59] หรือร่างกฎข้อบังคับว่าด้วยโทรคมนาคมระหว่างประเทศฉบับใหม่ (Draft of the Future ITR) ที่ได้เพิ่มเติมประเด็นสำคัญที่เกี่ยวข้องกับอินเทอร์เน็ต เช่น กำหนดให้ผู้ผลิตเนื้อหาต้องจ่ายค่าตอบแทนให้แก่ผู้ให้บริการอินเทอร์เน็ต กำหนดนิยามศัพท์ที่เกี่ยวข้องกับอินเทอร์เน็ตเข้าไปในข้อบังคับ และกำหนดให้กฎข้อบังคับว่าด้วยโทรคมนาคมระหว่างประเทศมีสภาพบังคับ ประเทศสมาชิกทุกประเทศจะต้องทำตามโดยไม่อาจตั้งข้อสงวนในข้อที่ไม่ต้องการผูกพันได้ เป็นต้น

---

[56] วรณัฐ บุญเจริญ, *มาตรการทางกฎหมายของอาเซียนเพื่อการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์*, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, (เชียงราย: มหาวิทยาลัยแม่ฟ้าหลวง, 2557), 50-51.

[57] Blohnone, *รู้จัก ITU สหภาพโทรคมนาคมนานาชาติ ผู้กำหนดมาตรฐานโทรคมนาคมโลก*, (22 พฤศจิกายน 2555), สืบค้นเมื่อ 8 ตุลาคม 2557, จาก http://www.blognone.com/node/38344

[58] ปัจจุบัน ITU มีสมาชิกทั้งสิ้น 193 ประเทศ, ดู International Telecommunication Union, *ITU Member states*, Retrieved May 7, 2015, from http://www.itu.int/online/mm/scripts/mm.list?_search=ITUstates&_languageid=1

[59] Ibid.

ประเด็นที่สำคัญที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ ได้มีการเสนอให้เพิ่มมาตรา 5A และมาตรา 5B ลงใน ITRs เพื่อเป็นการเสริมสร้างความมั่นคงทางด้านโทรคมนาคมและด้านเทคโนโลยีสารสนเทศ โดยได้มีการรวบรวมเรื่องที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ (Cyber Crime) สแปม (Spam) การกักเก็บข้อมูล (Data Retention) ความมั่นคงไซเบอร์ (Cyber Security) การคุ้มครองข้อมูล (Data Protection) ข้อมูลและการรักษาความปลอดภัยระบบเครือข่าย (Information and Network Security) การสงวนรักษาข้อมูล (Data Preservation) ความเป็นส่วนตัวและข้อมูล (Privacy and Data) การฉ้อโกง (Fraud) และการคุ้มครองข้อมูลส่วนบุคคล (Protection of Personal Information)[60] ซึ่งที่ประชุมมีข้อสรุป จากข้อเสนอแนะทั้งหมดมีเนื้อหาดังนี้

"มาตรา 5A การรักษาความปลอดภัยและความแข็งแกร่งของระบบเครือข่าย

ประเทศสมาชิกต้องพยายามทั้งโดยส่วนตนและส่วนรวม ในการคงไว้ซึ่งการรักษาความปลอดภัย และความแข็งแกร่งของเครือข่ายโทรคมนาคมระหว่างประเทศ เพื่อให้บรรลุถึงการใช้งานอย่างมีประสิทธิภาพ และหลีกเลี่ยงอันตรายทางเทคนิค เช่นเดียวกับการพัฒนาบริการทางโทรคมนาคมระหว่างประเทศที่นำเสนออย่างสอดคล้องกันแก่สาธารณะ"[61]

"มาตรา 5B กลุ่มก้อนการสื่อสารทางอิเล็กทรอนิกส์ที่ไม่ได้ถูกร้องขอ

ประเทศสมาชิกต้องมีความอุตสาหะที่จะใช้มาตรการที่จำเป็นในการป้องกันการถ่ายทอดของกลุ่มก้อนการสื่อสารทางอิเล็กทรอนิกส์ที่ไม่ได้ถูกร้องขอ และลดผลกระทบของกลุ่มก้อนดังกล่าวบนบริการโทรคมนาคมระหว่างประเทศให้เหลือน้อยที่สุด โดยให้ประเทศสมาชิกร่วมมือสนับสนุนด้วย"[62]

---

[60] International Telecommunication Union, *Draft of the future ITRs*, (2012), Retrieved September 5, 2014, from http://www.itu.int/en/wcit-12/Documents/draft-future-itrs-public.pdf, Article 5A and 5B

[61] Ibid, Article 5A Security and robustness of networks.

Article 41B Member States shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public.

[62] Article 5B Unsolicited bulk electronic communications

Article 41C Member States should endeavour to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication serv ices.

Member States are encouraged to cooperate in that sense.

International Telecommunication Union, *Final ACTS of the world conference on international telecommunications*, (Dubai: ITU, 2012), Retrieved April 19, 2014, from http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

**3.1.3 สหภาพยุโรป (European Union: EU)**

ในปี ค.ศ. 1985 คณะมนตรีแห่งยุโรป (Council of Europe) ได้มีการจัดตั้งกรรมาธิการผู้เชี่ยวชาญด้านอาชญากรรมทางคอมพิวเตอร์ขึ้น เพื่อกำหนดแนวทางในการบัญญัติกฎหมายให้ครอบคลุมถึงลักษณะการกระทำที่สมควรบัญญัติเป็นความผิด โดยมีอย่างน้อย 8 ฐานความผิดอันได้แก่ (1) การปลอมแปลงทางคอมพิวเตอร์ (2) การเข้าถึงโดยมิชอบ (3) การฉ้อโกงทางคอมพิวเตอร์ (4) การดักข้อมูลโดยมิชอบ (5) การรบกวนการทำงานของระบบโทรคมนาคม (6) การทำลายข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ (7) การรบกวนการทำงานของคอมพิวเตอร์หรือระบบโทรคมนาคม และ(8) การทำซ้ำลายพิมพ์วงจรโดยมิชอบ และยังมีความผิดอื่นที่กำหนดให้เป็นทางเลือกที่จะบัญญัติเป็นกฎหมายภายในอีก 4 ฐานความผิด ได้แก่ (1) การจารกรรมทางคอมพิวเตอร์ (2) การใช้โปรแกรมคอมพิวเตอร์ที่ได้รับการคุ้มครองโดยมิชอบ (3) การใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยมิชอบ และ(4) การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์[63]

คณะมนตรีได้จัดทำอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ซึ่งนับว่าเป็นอนุสัญญาฉบับแรกที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ โดยอนุสัญญานี้มีวัตถุประสงค์ที่สำคัญ 3 ประการดังนี้

1. เพื่อให้กฎหมายสารบัญญัติภายในประเทศต่าง ๆ ที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มีความสอดคล้อง และเป็นไปในทิศทางเดียวกัน

2. เพื่อให้กฎหมายวิธีพิจารณาความอาญาตามกฎหมายภายในให้อำนาจเท่าที่จำเป็นเพื่อประโยชน์ในการสืบสวนสอบสวนและฟ้องร้องการกระทำความผิดที่ได้กระทำโดยระบบคอมพิวเตอร์ ตลอดจนการรวบรวมพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

3. เพื่อเร่งให้เกิดความร่วมมือระหว่างประเทศที่รวดเร็ว และบรรลุเป้าหมายของอนุสัญญา

ต่อมาในปี ค.ศ. 2001 คณะกรรมาธิการยุโรป (European Commission) ได้เสนอ ข้อเสนอ “Network and Information Security: Proposal for a European Policy Approach” โดยมีวัตถุประสงค์เพื่อชี้ให้เห็นถึงการคุกคามความมั่นคงและความปลอดภัยของระบบคอมพิวเตอร์ด้วยวิธีการต่าง ๆ และข้อเสนอแนะในการกำหนดนโยบายด้านการรักษาความมั่นคง อาทิ มาตรการทางสังคม กฎหมาย และมาตรการทางเทคนิคอันรวมถึงมาตรฐานในการรักษาความมั่นคงต่าง ๆ

---

[63] ฉัทปณัย รัตนพันธ์, *อาชญากรรมทางคอมพิวเตอร์: ศึกษาการกำหนดฐานความผิดและการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์*, 10.

ในด้านมาตรการทางกฎหมายโดยเฉพาะนั้น คณะกรรมาธิการยุโรปได้ยื่นข้อเสนอที่เรียกว่า Council Framework Decision on attacks against information systems ต่อคณะมนตรีแห่งยุโรปในปี ค.ศ. 2002 โดยมีวัตถุประสงค์เพื่อนำเสนอรูปแบบการก่ออาชญากรรมทางคอมพิวเตอร์รูปแบบใหม่ ๆ และข้อเสนอในการบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์ภายในกลุ่มประเทศสมาชิก[64] เพื่อให้มีความสอดคล้องกันทั้งกฎหมายสารบัญญัติ และกฎหมายวิธีสบัญญัติ โดยมีเนื้อหาในส่วนของข้อเสนอที่ได้มาจากการศึกษาเปรียบเทียบ Convention on Cybercrime ของสภายุโรป อาทิ การกำหนดความผิดฐานการเข้าถึงระบบสารสนเทศโดยมิชอบ (Illegal access to Information Systems) ความผิดฐานรบกวนระบบสารสนเทศโดยมิชอบ (Illegal interference with Information Systems) เป็นต้น ทั้งนี้ประเทศสมาชิกจะต้องปฏิบัติให้เป็นไปตามข้อเสนอภายในวันที่ 31 ธันวาคม ค.ศ. 2003

อนุสัญญาอาชญากรรมคอมพิวเตอร์ ค.ศ. 2001 ได้เปิดให้ลงนามในการประชุม ณ กรุงบูดาเปส ประเทศฮังการี ในวันที่ 23 พฤศจิกายน ค.ศ. 2001 และมีผลบังคับใช้ในวันที่ 1 กรกฎาคม ค.ศ. 2004 โดยที่ประเทศสมาชิกสหภาพยุโรปรวมถึงประเทศอื่น ๆ ที่ลงนามในอนุสัญญาดังกล่าวได้ตระหนักถึงความจำเป็นเร่งด่วนในการป้องกันสังคมจากอาชญากรรมทางคอมพิวเตอร์ ซึ่งอนุสัญญาดังกล่าวนับเป็นเหตุการณ์สำคัญในประวัติศาสตร์ของการต่อสู้กับอาชญากรรมทางคอมพิวเตอร์ และอาจเรียกได้ว่าเป็นแม่แบบในการออกกฎหมายภายในสำหรับประเทศต่าง ๆ ทั่วโลก อีกทั้งยังเป็นแนวปฏิบัติ และเป็นการประสานความร่วมมือกับกลุ่มประเทศอื่น ๆ ที่ได้ร่วมลงนามในอนุสัญญาด้วย ซึ่งอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ใช้ภาษาที่เป็นกลางทางเทคโนโลยี เพื่อให้นำมาประยุกต์ใช้ได้ทั้งกับเทคโนโลยีที่มีอยู่ในปัจจุบันและต่อไปในอนาคต

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ประกอบด้วยบทบัญญัติทั้งหมด 4 บท ได้แก่ บทที่ 1 นิยามและคำจำกัดความ บทที่ 2 มาตรการการบังคับใช้ในระดับประเทศ บทที่ 3 ความร่วมมือระหว่างประเทศ และบทที่ 4 บทบัญญัติสุดท้ายเกี่ยวกับวิธีการต่าง ๆ เช่น การลงนามและมีผลใช้บังคับ การแก้ไขข้อพิพาท การเพิกถอน ฯลฯ เป็นต้น และในส่วนของความผิดที่กระทำต่อความลับ ความเที่ยงตรง และความมีอยู่ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ได้มีการกำหนดรูปแบบของการกระทำดังต่อไปนี้

3.1.3.1 การเข้าถึงโดยมิชอบด้วยกฎหมาย เป็นการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือบางส่วน ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น ประเทศภาคีอาจกำหนดให้เป็นความผิด

---

[64] ปัจจุบัน EU มีสมาชิกทั้งสิ้น 28 ประเทศ, ดู European Union, *EU member countries*, Retrieved June 7, 2015, from http://europa.eu/about-eu/countries/member-countries/

เฉพาะกรณีเป็นการกระทำโดยล่วงล้ำมาตรการรักษาความปลอดภัยโดยมีเจตนาที่จะได้มาซึ่งข้อมูลคอมพิวเตอร์หรือโดยมีเจตนาทุจริตประการอื่นหรือเฉพาะกรณีเป็นการกระทำเกี่ยวกับระบบคอมพิวเตอร์ที่เชื่อมโยงกับระบบคอมพิวเตอร์อื่นนั้นก็ได้[65]

3.1.3.2 การดักโดยมิชอบด้วยกฎหมาย เป็นการดักการส่งข้อมูลคอมพิวเตอร์ ซึ่งส่งไปหรือส่งจากหรือส่งภายในระบบคอมพิวเตอร์ที่มิใช่ข้อมูลสาธารณะ โดยวิธีการทางเทคนิครวมถึงการแผ่รังสีทางแม่เหล็กไฟฟ้าจากระบบคอมพิวเตอร์ที่มีข้อมูลคอมพิวเตอร์เช่นว่านั้น ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น ประเทศภาคีอาจกำหนดให้เป็นความผิดนี้เฉพาะกรณีเป็นการกระทำโดยมีเจตนาทุจริตหรือเฉพาะกรณีเป็นการกระทำเกี่ยวกับระบบคอมพิวเตอร์ที่เชื่อมโยงกับระบบคอมพิวเตอร์อื่นนั้นก็ได้[66]

3.1.3.3 การแทรกแซงต่อข้อมูล[67]

1. ประเทศภาคีแต่ละประเทศพึงจัดให้มีมาตรการทางนิติบัญญัติหรือมาตรการอื่นที่จำเป็น เพื่อกำหนดให้เป็นความผิดทางอาญาภายใต้กฎหมายภายในของประเทศนั้น ซึ่งการทำให้เสียหาย การลบ การทำให้เสื่อมเสีย การแก้ไขดัดแปลง หรือการทำลายข้อมูลคอมพิวเตอร์ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น

2. ประเทศภาคีอาจสงวนสิทธิที่จะกำหนดให้การกระทำตามวรรคหนึ่งเป็นความผิดเฉพาะกรณีที่ผลของการกระทำได้ก่อความเสียหายอย่างร้ายแรงนั้นก็ได้

---

[65] Convention on Cybercrime 2001, Article 2 Illegal access "…when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

[66] Ibid, Article 3 Illegal interception "…when committed intentionally, the interception without right, mad by technical means, of non-public transmission of computer data to, from or within a computer system, including electromagnetic emissions a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

[67] Ibid, Article 4 Data interference "…when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm."

3.1.3.4 การแทรกแซงต่อระบบ เป็นการกีดขวางการทำงานของระบบคอมพิวเตอร์อย่างร้ายแรงโดยการใส่เข้า การส่งต่อ การทำให้เสียหาย การลบ การทำให้เสื่อมเสีย การแก้ไขดัดแปลง หรือการทำลายข้อมูลคอมพิวเตอร์ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น[68]

3.1.3.5 การใช้อุปกรณ์โดยมิชอบ เป็นการกระทำดังต่อไปนี้ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น เช่น การผลิต การขาย การจัดให้มีเพื่อใช้ประโยชน์ การนำเข้า การจำหน่ายจ่ายแจกหรือการทำให้มีขึ้นซึ่ง (1) อุปกรณ์ รวมถึงโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบหรือดัดแปลงโดยมีวัตถุประสงค์หลักเพื่อใช้ในการกระทำความผิดใดประเภทดังกล่าวในข้อ 3.1.3.1-3.1.3.4 ข้างต้น และ (2) รหัสผ่านคอมพิวเตอร์ รหัสการเข้าถึงคอมพิวเตอร์ หรือข้อมูลที่มีลักษณะทำนองเดียวกัน ซึ่งทำให้สามารถใช้ในการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือส่วนหนึ่งส่วนใดโดยมีเจตนาที่จะใช้เพื่อวัตถุประสงค์ในการกระทำความผิดใดประเภทดังกล่าวในข้อ 3.1.3.1-3.1.3.4 ความในข้อนี้ไม่พึงถูกตีความในทางกำหนดความรับผิดทางอาญาสำหรับกรณีที่การผลิต การขาย การจัดให้มีเพื่อใช้ประโยชน์ การนำเข้า การจำน่ายจ่ายแจกหรือการทำให้มีขึ้นหรือการครอบครองดังกล่าวไว้ข้างต้นของข้อนี้ และไม่ได้มีวัตถุประสงค์ในการกระทำความผิดใดประเภทใดในข้อ 2-5 ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 นี้ เช่น มีวัตถุประสงค์เพื่อการทดสอบหรือคุ้มครองระบบคอมพิวเตอร์ที่ได้รับอนุญาตโดยชอบนั้น[69]

3.1.3.6 การปลอมแปลงเกี่ยวกับคอมพิวเตอร์เป็นการใส่เข้า การแก้ไขดัดแปลง การลบ หรือการทำลายข้อมูลคอมพิวเตอร์ ซึ่งส่งผลให้ข้อมูลคลาดเคลื่อนโดยประสงค์ที่จะทำให้เป็นไปว่าหรือใช้ในทางกฎหมายในลักษณะเหมือนกับว่า ข้อมูลที่ถูกกระทำดังกล่าวแล้วนั้นเป็นข้อมูลที่ถูกต้อง ทั้งนี้โดยไม่คำนึงถึงว่าข้อมูลนั้นสามารถอ่านได้หรือเข้าใจได้โดยตรงหรือไม่ก็ตาม ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น ประเทศภาคีอาจกำหนดให้ต้องรับผิดทางอาญาในการ

---

[68] Convention on Cybercrime 2001, Article 5 System interference "…when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."

[69] Ibid, Article 6 Misuse of devices "…when committed intentionally and without right: The production, sale, procurement for use, import, distribution or otherwise making available of (A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2-5. A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Article 2-5; and The possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Article 2-5. A Party may require by law that a number of such items be possessed before criminal liability attaches."

กระทำนี้เฉพาะกรณีเป็นการกระทำโดยมีเจตนาที่จะฉ้อโกงหรือมีเจตนาทุจริตในลักษณะทำนองเดียวกันก็ได้[70]

3.1.3.7 การฉ้อโกงที่เกี่ยวข้องกับคอมพิวเตอร์เป็นการทำให้เกิดความสูญเสียในทรัพย์สินของบุคคลอื่นโดยวิธีการดังต่อไปนี้ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธิ (ก) การใส่เข้า การแก้ไขดัดแปลง การลบ หรือการทำลายข้อมูลคอมพิวเตอร์ และ (ข) การแทรกแซงต่อการทำงานของระบบคอมพิวเตอร์ ทั้งนี้โดยผู้กระทำมีเจตนาในทางฉ้อโกงหรือเจตนาทุจริตที่จะเอาไปเสียซึ่งประโยชน์ทางเศรษฐกิจ สำหรับตนเองหรือบุคคลอื่นโดยไม่มีสิทธินั้น[71]

3.1.3.8 ความผิดเกี่ยวกับสื่อลามกอนาจารเด็ก ซึ่งเป็นการกระทำโดยเจตนาหรือโดยไม่มีสิทธินั้น เช่น การผลิตสื่อลามกอนาจารเกี่ยวกับเด็ก เพื่อวัตถุประสงค์ในการเผยแพร่ผ่านทางระบบคอมพิวเตอร์ การเสนอหรือการทำให้มีขึ้น ซึ่งสื่อลามกอนาจารเกี่ยวกับเด็ก การเผยแพร่หรือการส่งต่อซึ่งสื่อลามกอนาจารเกี่ยวกับเด็กผ่านทางระบบคอมพิวเตอร์ การจัดหาซึ่งสื่อลามกอนาจารเกี่ยวกับเด็กสำหรับตนเองหรือบุคคลอื่นผ่านทางระบบคอมพิวเตอร์ และการครอบครองสื่อลามกอนาจารเกี่ยวกับเด็กในระบบคอมพิวเตอร์หรือในสื่อกลางสำหรับบรรจุข้อมูลคอมพิวเตอร์นั้น[72]

ในเรื่องของสิทธิเสรีภาพนั้นอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ได้ให้ความสำคัญกับการเคารพสิทธิขั้นพื้นฐานของมนุษย์ รวมถึงความเท่าเทียมกันในการใช้สิทธิต่าง ๆ เพื่อดำเนินคดีตามกฎหมาย ดังที่ได้ระบุไว้ในอนุสัญญาแห่งสภาแห่งยุโรปว่าด้วยการปกป้องสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน ค.ศ. 1950 (The 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms) และกติการะหว่างประเทศว่าด้วยสิทธิ

---

[70] Convention on Cybercrime 2001, Article 7 Computer-related forgery "…when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches."

[71] Ibid, Article 8 Computer-related fraud "…when committed intentionally and without right, the causing of a loss of property to another by: Any input, alteration, deletion or suppression of computer data and Any interference with the functioning of a computer system. With fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another."

[72] Ibid, Article 9 Offences related to child pornography "…when committed intentionally and without right, the following conduct: Producing child pornography for the purpose of its distribution though a computer system; Offering or making available child pornography though a computer system; Distributing or transmitting child pornography though a computer system; Procuring child pornography though a computer system for oneself or for another and Possessing child pornography in a computer system or on a computer-data storage medium."

พลเมืองและสิทธิทางการเมือง ค.ศ. 1966 (The 1966 United Nation International Covenant on Civil and Political Rights) รวมถึงอนุสัญญาระดับนานาชาติอื่น ๆ ที่ว่าด้วยสิทธิมนุษยชน ซึ่งรับรองถึงสิทธิในการแสดงความคิดเห็นได้อย่างเสรีเช่นเดียวกับเสรีภาพในการแสดงออกในการค้นหา รับส่ง หรือนำเสนอข้อมูลหรือความคิดเห็นใด ๆ โดยไม่มีข้อจำกัด และสิทธิว่าด้วยการเคารพความเป็นส่วนตัว อีกทั้งยังตระหนักถึงการคุ้มครองข้อมูลส่วนบุคคล ดังที่ได้ระบุไว้ในอนุสัญญาสภาแห่งยุโรป ค.ศ. 1981ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในการนำข้อมูลส่วนบุคคลไปใช้โดยอัตโนมัติ (The 1981 Council of Europe Convention for the Protection of Individual with regard to Automatic Processing of Personal Data)

ในส่วนการใช้อำนาจของรัฐนั้น อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ได้ให้ความสำคัญของหลักการขั้นพื้นฐานของการใช้สิทธิเสรีภาพ โดยหลักเกณฑ์ดังกล่าวถูกระบุไว้ในมาตรา 15[73] แห่งอนุสัญญาดังกล่าว ในการใช้อำนาจของพนักงานเจ้าหน้าที่ผู้เกี่ยวข้องย่อมถูกจำกัดขอบเขต รวมถึงระยะเวลาเงื่อนไขและเหตุผลในการใช้อำนาจ อีกทั้งกระบวนการใช้อำนาจนั้นจะต้องถูกตรวจสอบและควบคุมโดยศาลหรือองค์กรอิสระ อันเนื่องมาจากการใช้อำนาจของพนักงานเจ้าหน้าที่นั้นอาจกระทบต่อสิทธิเสรีภาพขั้นพื้นฐานของประชาชน โดยรัฐต้องคำนึงถึงผลกระทบจากการใช้อำนาจและกระบวนการต่าง ๆ ที่กระทบต่อสิทธิรวมถึงความรับผิดชอบและผลประโยชน์อันชอบธรรมของประชาชนด้วย ซึ่งอำนาจของรัฐและพนักงานเจ้าหน้าที่ได้กำหนดไว้ ดังนี้

---

[73] Convention on Cybercrime 2001, Article 15 Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to condition and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on City and Political rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.

To the extent that it is consistent with the public interest, in particular the sound administration of justice, a Party shall consider the impact of the powers and procedures in this Section upon the rights, responsibilities and legitimate interests of third parties.

การคุ้มครองข้อมูลคอมพิวเตอร์ที่ถูกจัดเก็บไว้ (Expedited preservation of stored computer data) อยู่ในมาตรา 16[74] โดยบุคคลผู้ที่รักษาข้อมูลคอมพิวเตอร์ที่ถูกจัดเก็บไว้ในการครอบครองและควบคุมซึ่งข้อมูลนั้น (ผู้ให้บริการ) จะต้องทำการจัดเก็บข้อมูลคอมพิวเตอร์รวมถึงข้อมูลจราจรทางคอมพิวเตอร์เป็นระยะเวลาเท่าที่จำเป็น เพื่อให้หน่วยงานที่มีอำนาจสามารถตรวจสอบหาข้อเท็จจริงได้ และสามารถขยายระยะเวลาได้อีกในกรณีที่ครบกำหนดแล้ว และประเทศในสนธิสัญญาพึงบังคับใช้กฎหมายและมาตรการอื่น ๆ เท่าที่จำเป็น เพื่อบังคับให้ผู้ควบคุมดูแล หรือผู้ที่มีหน้าที่รักษาข้อมูลคอมพิวเตอร์ให้ปฏิบัติตามขั้นตอนต่าง ๆ นั้นไว้เป็นความลับ เป็นระยะเวลาหนึ่งตามกฎหมายภายในได้กำหนดไว้

สำหรับการคุ้มครองอย่างเร่งด่วนรวมถึงการเปิดเผยข้อมูลจราจรทางคอมพิวเตอร์บางส่วน (Expedited preservation and partial disclosure of traffic data) ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลจราจรทางคอมพิวเตอร์นั้น บุคคลผู้คุ้มครองดูแลต้องรับรองว่ามีการคุ้มครองข้อมูลจราจรทางคอมพิวเตอร์ โดยไม่คำนึงถึงว่าจะมีผู้บริการรายเดียวหรือมากกว่าเกี่ยวข้องในการส่งสัญญาณหรือการสื่อสารนั้น และยังต้องยืนยันว่ามีการเปิดเผยข้อเท็จจริงอย่างเร่งด่วน ต่อหน่วยงานหรือพนักงานเจ้าหน้าที่ที่ได้รับมอบหมายให้มีอำนาจควบคุมหรือไม่ เพื่อให้ทราบถึงชื่อผู้ให้บริการและเส้นทางของการส่งสัญญาณการสื่อสาร

คำสั่งให้ส่งข้อมูล (Production Order) ได้แก่ การออกหมายเรียกให้บุคคลผู้ครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ ซึ่งได้มีการจัดเก็บไว้ในระบบคอมพิวเตอร์ หรือสื่ออื่น ๆ ที่บันทึกข้อมูลคอมพิวเตอร์ ส่งมอบให้ซึ่งข้อมูลดังกล่าว โดยบุคคลผู้ที่รักษาข้อมูลคอมพิวเตอร์ที่ถูกจัดเก็บไว้ในการครอบครองหรือควบคุมของบุคคลนั้น (ผู้ให้บริการ)

---

[74] Ibid, Article 16 Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the computer authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

Each Party shall adopt such legislative or other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

ผู้ให้บริการซึ่งให้บริการภายในอาณาเขตของประเทศสนธิสัญญา ส่งข้อมูลสมาชิกที่เกี่ยวข้องกับการบริการดังกล่าวที่ผู้ให้บริการมีในครอบครองหรือควบคุมข้อมูลของสมาชิก เช่น ข้อมูลส่วนตัวที่ระบุถึงตัวตนของสมาชิก (ชื่อ ที่อยู่ เบอร์โทรศัพท์ ข้อมูลการแจ้งและการชำระเงินตามสัญญาหรือข้อตกลงในการใช้บริการ) สถานที่ที่ได้มีการติดตั้งอุปกรณ์การสื่อสาร เป็นต้น

การตรวจค้นและยึดข้อมูลคอมพิวเตอร์ที่ได้จัดเก็บไว้ (Search and seizure of stored computer data) ปรากฏอยู่ในมาตรา 19[75] ที่ให้อำนาจการตรวจค้นข้อมูลคอมพิวเตอร์แก่หน่วยงานที่มีอำนาจในการตรวจค้นหรือเข้าถึงระบบทั้งหมดหรือบางส่วนของระบบและข้อมูลคอมพิวเตอร์ที่ได้จัดเก็บไว้ และสื่อบันทึกข้อมูลคอมพิวเตอร์ที่ข้อมูลคอมพิวเตอร์นั้นได้ถูกจัดเก็บไว้ภายในสื่อบันทึก

อำนาจในการยึดหรืออายัดข้อมูลคอมพิวเตอร์ที่ถูกจัดเก็บไว้ในระบบหรือบางส่วนของระบบ หรือชื่อบันทึกข้อมูลคอมพิวเตอร์นั้น มีอำนาจทำสำเนาหรือเก็บสำเนาข้อมูลคอมพิวเตอร์และรักษาความสมบูรณ์ของข้อมูลคอมพิวเตอร์ที่ได้ถูกจัดเก็บเอาไว้ รวมถึงการกำจัดหรือเคลื่อนย้ายข้อมูลคอมพิวเตอร์ที่ทำให้ไม่สามารถเข้าถึงระบบคอมพิวเตอร์นั้น ๆ ได้

---

[75] Convention on Cybercrime 2001, Article 19 Search and seizure of stored computer data "…empower its computer authorities to search or similarly access:

a. A computer system or part of it and computer data stored therein; and

Computer-data storage medium in which computer data may be stored in its territory.,

… ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1 (a), and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.

… empower its computer authorities to seize or similarly secure computer data accessed according to paragraph 1 or 2. These measures shall include the power to:

a. Seize or similarly secure a computer system or part of it or a computer-data storage medium;

b. Make and retain a copy of those computer data;

c. Maintain the integrity of the relevant stored computer data; and

Render inaccessible or remove those computer data in the accessed computer system.

… empower its computer authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2

การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ (Real-time collection of traffic data) มีหลักอยู่ในมาตรา 20[76] ซึ่งให้อำนาจแก่หน่วยงานที่เกี่ยวข้องในการรวบรวมหรือบันทึกด้วยวิธีการทางเทคนิค และบังคับให้ผู้ให้บริการดำเนินการทางเทคนิคที่มีอยู่ในการรวบรวมหรือบันทึก ด้วยวิธีการทางเทคนิค และให้ความร่วมมือ ช่วยเหลือหน่วยงานที่มีอำนาจควบคุม ในการรวบรวมการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ตามเวลาที่เกิดขึ้นจริง การสื่อสารที่เกี่ยวข้องภายในอาณาบริเวณของประเทศภาคีอนุสัญญาฯ ซึ่งมีการส่งผ่านระบบคอมพิวเตอร์

ผู้ให้บริการต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ รวมถึงข้อมูลอื่น ๆ ที่เกี่ยวข้องเป็นความลับด้วย การลักลอบดักจับข้อมูลที่เป็นเนื้อหา (Interception of content data) มีหลักอยู่ในมาตรา 21 โดยหน่วยงานที่เกี่ยวข้องมีอำนาจเช่นเดียวกับมาตรา 20

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ของสหภาพยุโรปนับเป็นอนุสัญญาระหว่างประเทศที่มีผลผูกพันฉบับเดียวที่มีอยู่เกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ และเป็นแนวทางในการสร้างมาตรการ รวมทั้งประสานความร่วมมือระหว่างประเทศเพื่อรับมืออาชญากรรมทางคอมพิวเตอร์ โดยคำนึงถึงปัจจัยด้านเสรีภาพและสิทธิมนุษยชน ซึ่งในกระบวนการกำหนดนโยบาย บางครั้งรัฐได้ละเลย หรือจงใจละทิ้งหรือจำกัดทางเลือกของนโยบาย

---

[76] Convention on Cybercrime 2001, Article 20 Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its computer authorities to:

a. Collect or recode through application of technical means on the territory of that Party, and

b. Compel a service provider, within its existing technical capability, to

i. Collect or record through application of technical means on the territory of that Party, or on the territory of that Party, or

ii. Co-operate and assist the competent authorities in the collection or recording of, traffic data and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communication in its territory transmitted by means, in real-time, associated with specified communication in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1(a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communication in its territory through application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this article.

ที่เสริมสร้างให้อินเทอร์เน็ตพัฒนาขึ้นซึ่งเป็นพื้นฐานที่สำคัญสำหรับกิจกรรมทางเศรษฐกิจ การมีส่วนร่วมในนโยบายประชาธิปไตยและการพัฒนามวลมนุษยชาติ

ในปัจจุบันนานาประเทศกำลังแสวงหาข้อกำหนดใหม่ ๆ สำหรับการให้บริการอินเทอร์เน็ตและสื่อที่เกี่ยวข้อง เพื่อคัดกรองและสกัดกั้นเนื้อหาที่ไม่พึงประสงค์ ด้วยมาตรการควบคุมเครือข่ายและการเฝ้าระวังเพื่อบังคับใช้กฎระเบียบกับผู้ใช้งาน ซึ่งผลที่ได้ทำให้เกิดความยุ่งยากและขัดขวางการไหลเวียนของข้อมูลทั่วโลกจากการแข่งขันเรื่องอำนาจการควบคุม และการขัดกันของกฎหมายซึ่งคุกคามเสรีภาพอันเป็นคุณสมบัติเด่นที่ทำให้อินเทอร์เน็ตเป็นอย่างที่เป็นอยู่ทุกวันนี้ ดังนั้นการพัฒนากฎหมายและมาตรการความร่วมมือต่าง ๆ ร่วมกันในระดับโลกจึงเป็นสิ่งสำคัญที่จะทำให้กฎหมายทันสมัย ก่อให้เกิดความชอบธรรมและเป็นประโยชน์มากกว่าผลร้ายที่จะเกิดตามมา และที่สำคัญคือสามารถปราบปรามอาชญากรรมทางคอมพิวเตอร์ได้อย่างมีประสิทธิภาพสูงสุด

อย่างไรก็ดีอนุสัญญานั้นเป็นข้อตกลงที่มีผลผูกพันชัดเจน ซึ่งผู้ลงนามเป็นภาคีสมาชิกอาจต้องรับผิดภายใต้กฎหมายระหว่างประเทศในกรณีผิดข้อตกลง ดังนั้นบางกรณีการทำบันทึกความเข้าใจ (Memorandum of Understanding: MoU) จะเป็นข้อตกลงที่ยืดหยุ่นมากกว่า ซึ่งบันทึกความเข้าใจมักชี้วัดแนวทางการกระทำระหว่างพหุภาคี และมักถูกใช้ในกรณีที่แต่ละฝ่ายไม่ต้องการมีข้อผูกมัดทางกฎหมายหรืออยู่ในสถานการณ์ที่ไม่สามารถออกข้อตกลงที่บังคับใช้ตามกฎหมายได้ แม้ว่าบันทึกความเข้าใจจะไม่ผูกพันตามกฎหมายระหว่างประเทศแต่ก็จะถูกบันทึกไว้ในฐานข้อมูลสนธิสัญญาของสหประชาชาติ

นอกจากนี้แล้วสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (Association of Southeast Asian Nations: ASEAN) เป็นองค์กรระดับภูมิภาคที่ให้ความสำคัญกับปัญหาการก่ออาชญากรรมทางคอมพิวเตอร์ ซึ่งอาเซียนมีความพยายามที่จะสร้างกลไกเพื่อจัดการปัญหาอาชญากรรมทางคอมพิวเตอร์ทั้งภายในและภายนอกภูมิภาคโดยอาศัยแม่แบบจากหลักเกณฑ์สากลต่าง ๆ และนำมาปรับใช้ให้เหมาะสมกับภูมิภาคโดยผ่านการประชุมต่าง ๆ หลายครั้ง ซึ่งอาเซียนได้กำหนดเป้าหมายการพัฒนาโครงสร้างพื้นฐานทางเทคโนโลยีการสื่อสารและสารสนเทศและความปลอดภัยไซเบอร์ลงไปในแผนงานมากมาย เช่น ASEAN ICT Master plan 2015 และ Master plan on ASEAN connectivity ฯลฯ โดยอาเซียนได้มีการจัดตั้งหน่วยงานเพื่อต่อต้านการโจมตีไซเบอร์และประสานงานระหว่างประเทศสมาชิกด้วยกันตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์ (CERTs) และมีการจัดตั้งคณะทำงานเพื่อศึกษาหาแนวทางการสร้างมาตรการร่วมกันของประเทศสมาชิกอาเซียน นอกจากนี้ ประเทศสมาชิกอาเซียนเองก็มีความตระหนักถึงภัยไซเบอร์ที่มีการขยายตัวอย่างรวดเร็วอันเนื่องมาจากพัฒนาการของเทคโนโลยีที่ก้าวหน้าขึ้นเรื่อย ๆ ในปัจจุบัน ประเทศสมาชิกของ

อาเซียนเกือบทุกประเทศ[77] ได้พยายามออกกฎหมายเพื่อรับมือกับภัยจากอาชญากรรมทางคอมพิวเตอร์โดยมีกฎเกณฑ์ที่ครอบคลุมความผิดทั้งในด้านบุกรุก การควบคุมเนื้อหาออนไลน์ และการคุ้มครองข้อมูลส่วนบุคคล เพื่อเสริมสร้างศักยภาพและความปลอดภัยไซเบอร์ของภูมิภาคให้ได้มาตรฐานสากลและเท่าทันอาชญากรรมทางคอมพิวเตอร์ที่หลากหลายและซับซ้อนมากยิ่งขึ้น[78]

## 3.2 บทบัญญัติทางกฎหมาย และหลักเกณฑ์เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในระดับประเทศ

### 3.2.1 ประเทศสิงคโปร์

ประเทศสิงคโปร์ เป็นสาธารณรัฐ รัฐเดี่ยว ระบบการเมืองการปกครองเป็นประชาธิปไตยแบบรัฐสภา โดยรัฐสภาเป็นแบบสภาเดียวทำหน้าที่นิติบัญญัติ ฝ่ายบริหารคือรัฐบาล ประกอบด้วยนายกรัฐมนตรีและคณะรัฐมนตรี ประธานาธิบดี ทำหน้าที่เป็นประมุขของสาธารณรัฐทำหน้าที่ด้านพิธีการ และฝ่ายตุลาการซึ่งประกอบด้วยศาลสูงสุดและบรรดาศาลชั้นต้นในระดับต่าง ๆ นั้น ก็จะทำหน้าที่ด้านการใช้อำนาจอธิปไตยในส่วนของการตีความตัวบทกฎหมายต่าง ในรูปของการพิจารณาพิพากษาคดีความต่าง ๆ[79]

สำหรับประเทศสิงคโปร์ได้มีการบัญญัติกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ชื่อว่า “พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 1993” (Computer Misuse Act 1993) และได้มีการปรับปรุงแก้ไขเพิ่มเติมเมื่อปี ค.ศ. 2007 พร้อมทั้งเปลี่ยนชื่อเป็น “พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทางคอมพิวเตอร์ ค.ศ. 2007 (Computer Misuse and Cybersecurity Act 2007) ซึ่งเป็นกฎหมายที่ออกมาเพื่อคุ้มครองเกี่ยวกับการกระทำใดที่เกี่ยวข้องกับคอมพิวเตอร์ โปรแกรม และข้อมูลที่อยู่ในประเทศสิงคโปร์ เพื่อรองรับรูปแบบการ

---

[77] อาเซียนมีสมาชิกทั้งหมด 10 ประเทศ ได้แก่ มาเลเซีย สิงคโปร์ อินโดนีเซีย ฟิลิปปินส์ บรูไน กัมพูชา เวียดนาม ลาว และพม่า ซึ่งประเทศสมาชิกอาเซียนได้ตระหนักถึงความสำคัญของปัญหาอาชญากรรมทางคอมพิวเตอร์ โดยได้ให้ความสำคัญกับการบัญญัติกฎหมายเพื่อรับมือกับอาชญากรรมทางคอมพิวเตอร์ ถึง 8 ใน 10 ประเทศ ซึ่ง สปป.ลาว เป็นประเทศหนึ่งที่ยังไม่มีกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์.

[78] วรณัฐ บุญเจริญ, *มาตรการทางกฎหมายของอาเซียนเพื่อการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์*, 142.

[79] มหาวิทยาลัยสุโขทัยธรรมาธิราช, *เอกสารการสอนชุดวิชา การเมืองการปกครองของประเทศในเอเชีย หน่วยที่ 8-15*, (นนทบุรี: มหาวิทยาลัยฯ, 2548), 13-29-13-33.

กระทำผิดรูปแบบใหม่ของอาชญากรรมทางคอมพิวเตอร์ และได้มีการบัญญัติเกี่ยวกับฐานความผิดตามมาตราต่าง ๆ และการให้อำนาจแก่พนักงานเจ้าหน้าที่ ดังนี้

3.2.1.1 หลักเกณฑ์และมาตรการทางกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

ประเทศสิงคโปร์มีความตั้งใจในการปรับปรุงกฎหมายให้ได้มาตรฐานโลกอยู่เสมอ เพื่อรองรับรูปแบบใหม่ ๆ ของการกระทำความผิดทางคอมพิวเตอร์ ซึ่งได้มีการบัญญัติถึงลักษณะของการกระทำความผิด และมาตรการในการลงโทษอาชญากรรมทางคอมพิวเตอร์ ดังนี้

1. การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งบุคคลใดก็ตามที่เจตนาใช้คอมพิวเตอร์เพื่อวัตถุประสงค์ในการเข้าถึง โดยไม่ได้รับอนุญาต ซึ่งข้อมูลคอมพิวเตอร์หรือโปรแกรมที่อยู่ในคอมพิวเตอร์ใด ๆ ที่มีการป้องกันการเข้าถึงโดยเฉพาะถือว่ามีความผิด ถึงแม้ว่าการกระทำดังกล่าวจะเป็นการกระทำเพื่อการเข้าถึงคอมพิวเตอร์และระบบคอมพิวเตอร์ สำหรับวัตถุประสงค์ของส่วนนี้ให้ถือว่ามาตราต่าง ๆ นั้นไม่ได้มุ่งถึงโปรแกรมหรือข้อมูลใดโดยเฉพาะโปรแกรมหรือข้อมูลชนิดใด ๆ หรือโปรแกรมหรือข้อมูลในคอมพิวเตอร์เครื่องใด ๆ โดยเฉพาะ[80]

2. การเข้าถึงด้วยเจตนาในการกระทำความผิดหรือพยายามกระทำความผิดตามมาตรา 4 บุคคลใดก็ตามที่ใช้คอมพิวเตอร์ในการเข้าถึงข้อมูลหรือโปรแกรมที่อยู่ในคอมพิวเตอร์ใด ๆ โดยเจตนาที่จะกระทำความผิดหรือพยายามกระทำความผิดก็ถือเป็นความผิด ซึ่งการกระทำผิดนี้ให้บังคับใช้กับความผิดเกี่ยวกับทรัพย์สิน การฉ้อโกง หรือกระทำให้เกิดความเสียหายต่อร่างกาย

---

[80] Unauthorised Access to Computer Material 3, "(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at.,

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer."

โดยอนุโลม ซึ่งการกระทำนี้จะกระทำในขณะที่มีการเชื่อมต่อกับระบบรักษาความปลอดภัยหรือไม่ก็ตาม โดยไม่คำนึงว่าจะได้รับอนุญาตหรือไม่ก็ตาม[81] (เน้นเจตนาการกระทำผิดเป็นสำคัญ)

3. การดัดแปลงแก้ไขข้อมูลคอมพิวเตอร์ ซึ่งบุคคลใดกระทำการใด ๆ โดยมิชอบซึ่งรู้ว่าจะทำให้เกิดการดัดแปลงแก้ไขเนื้อหาใด ๆ ของคอมพิวเตอร์ เป็นการกระทำผิด อย่างไรก็ตามการดัดแปลงแก้ไขข้อมูลคอมพิวเตอร์ในกรณีที่จำเป็นแก่การใช้ เช่น ผู้ใช้สามารถดัดแปลงโปรแกรมคอมพิวเตอร์เท่าที่จำเป็น แต่ในกรณีนี้การดัดแปลงที่ก่อให้เกิดความเสียหายไม่ว่าจะเป็นการดัดแปลงเป็นการถาวรหรือเป็นการชั่วคราวก็ถือว่าเป็นการกระทำผิด[82]

4. การใช้หรือดักจับข้อมูลบริการคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งบุคคลใด ๆ ได้ทำการเข้าถึงคอมพิวเตอร์ใด ๆ โดยไม่ได้รับอนุญาตเพื่อรับบริการของคอมพิวเตอร์ ไม่ว่าโดยตรงหรือโดยอ้อม และได้กระทำการดักจับหรือทำให้ถูกดักจับโดยไม่ได้รับอนุญาตไม่ว่า

---

[81] Access with intent to commit or facilitate commission of offence 4, (1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.

(2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

(3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(4) For the purposes of this section, it is immaterial whether.,

(a) the access referred to in subsection (1) is authorised or unauthorised;

(b) the offence to which this section applies is committed at the same time when the access is secured or at any other time."

[82] Unauthorised modification of computer material 5, (1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at.,

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary."

ทางตรงหรือทางอ้อม ซึ่งการทำงานของคอมพิวเตอร์ ไม่ว่าโดยวิธีการใดก็ตาม โดยเจตนาในการใช้หรือทำให้เกิดการใช้ไม่ว่าโดยทางตรงหรือทางอ้อมซึ่งคอมพิวเตอร์หรืออุปกรณ์ใด ๆ และการกระทำดังกล่าวได้ก่อให้เกิดความเสียหาย สำหรับวัตถุประสงค์ของส่วนนี้ไม่ได้มุ่งถึงโปรแกรมหรือข้อมูลใด ๆ เป็นการเฉพาะ[83]

5. การเข้าขัดขวางการใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งบุคคลใดเจตนาและปราศจากอำนาจหรือข้ออ้างใด ๆ ตามกฎหมายเพื่อเข้ารบกวนหรือขัดขวางการใช้งานโดยถูกกฎหมายซึ่งคอมพิวเตอร์ หรือไม่ยอมให้เข้าถึงหรือทำให้ประสิทธิภาพในการทำงานลดลงซึ่ง

---

[83] Unauthorised use or interception of computer service 6. “(1) Subject to subsection (2), any person who knowingly.

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at.,

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.”

โปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์ ผู้นั้นมีความผิดและต้องได้รับโทษ หรือถ้าความเสียหายที่เกิดขึ้นเป็นผลมาจากการเข้าขัดขวางการใช้งานคอมพิวเตอร์ก็จะได้รับโทษเพิ่มมากยิ่งขึ้น[84]

6. การเปิดเผยรหัสเชื่อมต่อโดยไม่ได้รับอนุญาต ซึ่งบุคคลใดเจตนาและไม่ได้รับอนุญาตในการเปิดเผยรหัสเชื่อมต่อ รหัสผ่านหรือวิธีการอื่นใดก็ตามในการเข้าถึงโปรแกรมหรือข้อมูลที่เก็บไว้ในคอมพิวเตอร์ใด ๆ ให้ถือว่าเป็นการกระทำผิด หากผู้นั้นกระทำไปเพื่อผลประโยชน์โดยมิชอบ เพื่อวัตถุประสงค์ที่ผิดกฎหมายหรือรู้ว่าจะทำให้เกิดความเสียหายต่อบุคคลใดก็ตาม[85]

7. การสนับสนุนการกระทำความผิดและการพยายามกระทำความผิด ซึ่งบุคคลใดสนับสนุนหรือผู้ใดพยายามกระทำความผิดถือว่าเป็นการตระเตรียมที่จะกระทำความผิดต่อไปในภายหน้าภายใต้พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทาง

---

[84] Unauthorised obstruction of use of computer 7, "(1) Any person who, knowingly and without authority or lawful excuse.,

(a) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both."

[85] Unauthorised disclosure of access code. 8, "(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so.,

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

(2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both."

คอมพิวเตอร์ ค.ศ. 2007 ฉบับนี้ให้ถือว่ากระทำความผิดในความผิดนั้นและรับผิดตามที่ความผิดนั้นได้กำหนดไว้ สำหรับการกระทำผิดภายใต้มาตรานี้ไม่คำนึงถึงว่าการกระทำผิดจะเกิดขึ้นที่ใด[86]

จากลักษณะของการกระทำความผิดดังกล่าว จะเห็นได้ว่าพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทางคอมพิวเตอร์ ค.ศ. 2007 มีการบัญญัติตามแนวทางของอนุสัญญาระหว่างประเทศ และกฎหมายของประเทศในภูมิภาคยุโรป

3.2.1.2 อำนาจของพนักงานเจ้าหน้าที่

นอกจากรูปแบบต่าง ๆ ของการกระทำผิดแล้วในรัฐบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทางคอมพิวเตอร์ ค.ศ. 2007 ยังได้ให้อำนาจแก่เจ้าพนักงานในการดำเนินการสืบสวนโดยไม่มีสิ่งใดในกฎหมายฉบับนี้จะห้ามไม่ให้เจ้าหน้าที่ตำรวจ คือบุคคลที่ได้รับมอบอำนาจตามมาตรา 39 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ค.ศ. 2010 (The Criminal Procedure Code 2010) หรือเจ้าหน้าที่ผู้บังคับใช้กฎหมายใดที่ได้กระทำการตามกฎหมายในการสืบสวนตามอำนาจที่กฎหมายบัญญัติไว้[87]

ในมาตรา 39 แห่งประมวลกฎหมายวิธีพิจารณาความอาญาได้ให้อำนาจแก่เจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจตามกฎหมายสืบสวนคดีความการกระทำผิดที่สามารถจับกุมได้ และสามารถกระทำการสืบสวนสอบสวนได้เมื่อใดก็ได้ การเข้าถึง ตรวจสอบการทำงานของคอมพิวเตอร์ซึ่งเจ้าหน้าที่นั้นมีเหตุให้สงสัยว่าได้ถูกใช้ในการกระทำผิด การใช้หรือทำให้เกิดการใช้ซึ่งคอมพิวเตอร์เพื่อค้นข้อมูลหรือมีอยู่ในคอมพิวเตอร์นั้น เจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจตามกฎหมายอาจขอความช่วยเหลือจากบุคคลใดที่เจ้าหน้าที่สงสัยว่าจะใช้คอมพิวเตอร์ในการกระทำผิดหรือเคยใช้กระทำผิด หรือบุคคลใดก็ตามที่รับผิดชอบที่เกี่ยวข้องกับการทำงานของคอมพิวเตอร์ดังกล่าว บุคคลใดที่ขัดขวางการปฏิบัติหน้าที่ตามกฎหมายของเจ้าหน้าที่ตำรวจหรือ

---

[86] Abetments and attempts punishable as offences. 10. “(1) Any person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

(2) For an offence to be committed under this section, it is immaterial where the act in question took place.”

[87] Saving for investigations by police and law enforcement officers. 14, “Nothing in this Act shall prohibit a police officer, an authorised person within the meaning of section 39 of the Criminal Procedure Code 2010 or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to the powers conferred on him under any written law.”

บุคคลที่ได้รับมอบอำนาจหรือบุคคลซึ่งไม่สามารถกระทำตามความต้องการของเจ้าหน้าที่ตำรวจหรือผู้ได้รับมอบอำนาจให้ถือว่ากระทำความผิด[88]

จะเห็นได้ว่าสิงคโปร์ก็ได้ให้ความสำคัญในการออกกฎหมายเพื่อมาคุ้มครองและปราบปรามเกี่ยวกับอาชญากรรมคอมพิวเตอร์ เพื่อให้มีประสิทธิภาพในการควบคุมลักษณะของการกระทำความผิดรูปแบบใหม่ของการใช้เทคโนโลยีสารสนเทศมาใช้ในการกระทำความผิด ด้วยพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทางคอมพิวเตอร์

### 3.2.2 ประเทศไทย

ในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีการกระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะลามกอนาจาร ย่อมก่อให้เกิด

---

[88] Criminal Procedure Code, Chapter 68, Power to access computer 39, "(1) A police officer or an authorised person, investigating an arrestable offence, may at any time.,

(a) access, inspect and check the operation of a computer that he has reasonable cause to suspect is or has been used in connection with the arrestable offence; or

(b) use or cause to be used any such computer to search any data contained in or available to such computer.

(2) The police officer or authorised person may also require any assistance he needs to gain such access from.,

(a) any person whom he reasonably suspects of using the computer in connection with the arrestable offence or of having used it in this way; or

(b) any person having charge of, or otherwise concerned with the operation of, such computer.

(3) Any person who obstructs the lawful exercise by a police officer or an authorised person of the powers under subsection (1), or who fails to comply with any requirement of the police officer or authorised person under subsection (2), shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 6 months or to both.

(4) An offence under subsection (3) shall be an arrestable offence.

(5) A person who had acted in good faith under subsection (1) or in compliance with a requirement under subsection (2) shall not be liable in any criminal or civil proceedings for any loss or damage resulting from the act.

(6) In this section and section 40, "authorised person" means a person authorised in writing by the Commissioner of Police for the purposes of this section or section 40 or both."

ความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อปกป้องและปราบปรามการกระทำดังกล่าว[89] จึงได้มีการตราและประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งเป็นกฎหมายที่ออกมาเพื่อคุ้มครองผู้ที่ได้รับความเสียหายที่เกิดจากผู้ที่ใช้คอมพิวเตอร์เพื่อก่อความผิดและสร้างความเสียหายรวมทั้งเพื่อเป็นการกำหนด “ฐานความผิด” หรือลักษณะในการกระทำความผิด การกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งการกำหนดหน้าที่ของผู้ให้บริการต่าง ๆ ให้เกิดความชัดเจน เนื่องจากการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์มีลักษณะพิเศษ

ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นี้มีมาตราต่าง ๆ รวมทั้งสิ้น 30 มาตรา แบ่งออกเป็นสองหมวด ได้แก่ หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งเป็นบทบัญญัติที่เกี่ยวกับการกำหนดฐานความผิดและบทลงโทษผู้กระทำความผิดทั้งในส่วนของการใช้คอมพิวเตอร์เพื่อกระทำความผิดและการกระทำความผิดต่อคอมพิวเตอร์ หมวด 2 พนักงานเจ้าหน้าที่ มีการกำหนดเกี่ยวกับอำนาจของพนักงานเจ้าหน้าที่ และยังมีการกำหนดเกี่ยวกับการตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่ รวมทั้งมีการกำหนดหน้าที่ของผู้ให้บริการที่ต้องเก็บรักษาข้อมูลคอมพิวเตอร์และต้องให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการส่งมอบข้อมูลจราจรทางคอมพิวเตอร์แก่พนักงานเจ้าหน้าที่

3.2.2.1 หลักเกณฑ์และมาตรการทางกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บัญญัติเกี่ยวกับการกระทำความผิดมีทั้งสิ้น 13 มาตรา ตั้งแต่มาตรา 5 ถึงมาตรา 17 สำหรับการกระทำความผิดตั้งแต่มาตรา 5 ถึงมาตรา 13 นั้นเป็นการกระทำที่กระทบต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ และมาตรา 14 ถึงมาตรา 16 เป็นการกระทำผิดอันเกิดจากการเผยแพร่เนื้อหา ซึ่งฐานความผิดตามมาตราต่าง ๆ มีดังนี้[90]

1. การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ มาตรา 5 บัญญัติว่า “ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือนหรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ” ซึ่งเป็นการเข้าถึงในระดับกายภาพในกรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ และหมายความรวมถึงการเข้าระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วน

---

[89] หมายเหตุท้ายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550.

[90] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, (ม.ป.ท.: ม.ป.พ., ม.ป.ป.).

กล่าวคือระบบคอมพิวเตอร์ใดเป็นระบบที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะเป็นข้อเท็จจริงที่จะต้องนำสืบเป็นเรื่อง ๆ ไป ส่วนเหตุผลที่บัญญัติองค์ประกอบความผิดนี้ก็เพราะมีระบบคอมพิวเตอร์จำนวนมากที่เจ้าของไม่ได้หวงแหนการที่บุคคลใดจะเข้าถึง และการกระทำความผิดโดยฝ่าฝืนต่อบทบัญญัติแห่งมาตรานี้อาจเกิดขึ้นหลายวิธี เช่น การเจาะระบบ (Hacking or Cracking) หรือการบุกรุกทางคอมพิวเตอร์ (Computer Trespass)

2. การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะโดยมิชอบ มาตรา 6 บัญญัติว่า “ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ” การล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะกล่าวคือระบบคอมพิวเตอร์นั้นมีมาตรการเข้าถึง เช่น มีการลงทะเบียน Username และ Password หรือมีวิธีการอื่นใดที่จัดขึ้นเป็นการเฉพาะ การที่จะเป็นความผิดตามมาตรานี้ต้องเป็นเรื่องที่ผู้กระทำล่วงรู้ ซึ่งการล่วงรู้นั้นจะได้มาโดยชอบหรือไม่ชอบไม่สำคัญหากแต่นำมาตรการนี้เปิดเผยแก่ผู้หนึ่งผู้ใดหรือหลายคนและการเปิดเผยนั้นอยู่ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นแล้ว

3. การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ มาตรา 7 บัญญัติว่า “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ”

องค์ประกอบความผิดตามมาตรา 7 ตรงกับองค์ประกอบความผิดตามมาตรา 5 เพียงแต่เปลี่ยนจาก “ระบบคอมพิวเตอร์” เป็น “ข้อมูลคอมพิวเตอร์” กล่าวคือความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ ซึ่งหมายถึงข้อมูลนั้นเป็นการเก็บหรือส่งด้วยวิธีการทางคอมพิวเตอร์หรือวิธีการทางอิเล็กทรอนิกส์ ดังนั้นจึงไม่น่าจะหมายความรวมถึงข้อมูลที่บรรจุไว้ในแผ่นซีดี หรือแผ่นดิสเกตต์ อย่างไรก็ตามเมื่อใดที่มีการนำซีดีหรือแผ่นดิสเกตต์นั้นเล่นผ่านระบบคอมพิวเตอร์ก็จะอยู่ในความหมายของข้อมูลคอมพิวเตอร์ทันที

4. การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ มาตรา 8 บัญญัติว่า “ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

ซึ่งการดักรับข้อมูลในมาตรานี้หมายถึง การดักรับโดยวิธีการทางเทคนิค (Technical Means) เพื่อลักลอบดักฟัง (Listen) ตรวจสอบ (Monitoring) หรือติดตามเนื้อหาสาระ

ของข่าวสาร (Surveillance) ที่สื่อสารถึงกันระหว่างบุคคล[91] หรือเป็นการกระทำเพื่อให้ได้มาซึ่งเนื้อหาของข้อมูลโดยตรงหรือโดยการเข้าถึงและใช้ระบบคอมพิวเตอร์ หรือการทำให้ได้มาซึ่งเนื้อหาของข้อมูลโดยทางอ้อมด้วยการแอบบันทึกข้อมูลสื่อสารถึงกันด้วยอุปกรณ์อิเล็กทรอนิกส์

5. การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ มาตรา 9 บัญญัติว่า "ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ"

ความผิดตามมาตรา 9 มุ่งคุ้มครองความถูกต้องของข้อมูล (Integrity) ความถูกต้องแท้จริง (Authentication) และเสถียรภาพหรือความพร้อมในการใช้งานหรือการใช้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่บันทึกเก็บไว้บนสื่อคอมพิวเตอร์ได้อย่างเป็นปกติ เป็นการกำหนดขึ้นเพื่อให้ข้อมูลคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ได้รับความคุ้มครองเพื่อป้องกันการกระทำความผิด เช่น การป้อนโปรแกรมที่มีไวรัสทำลายข้อมูลหรือโปรแกรมคอมพิวเตอร์ หรือการป้อน Trojan Horse เข้าไปในระบบเพื่อขโมยรหัสผ่านของผู้ใช้คอมพิวเตอร์สำหรับเพื่อเข้าไปลบ เปลี่ยนแปลงแก้ไขข้อมูลหรือกระทำการใด ๆ อันเป็นการรบกวนข้อมูล

6. การกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานตามปกติได้ มาตรา 10 บัญญัติว่า "ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ" วัตถุประสงค์และองค์ประกอบความผิดคล้ายคลึงกับมาตรา 9 เพียงแต่เปลี่ยนวัตถุแห่งการถูกกระทำจาก "ข้อมูลคอมพิวเตอร์" เป็น "ระบบคอมพิวเตอร์[92]"

7. ส่งข้อมูลคอมพิวเตอร์รบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข มาตรา 11 บัญญัติว่า "ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท"

---

[91] Lawyerthai.com, *กฎหมายอาญากรรมทางคอมพิวเตอร์ตอน 4: กำหนดฐานความผิด และบทกำหนดโทษ*, สืบค้นเมื่อ 19 มีนาคม 2558, จาก http://www.lawyerthai.com/articles/it/031.php

[92] การเข้าไปทำกับระบบคอมพิวเตอร์หรือการกระทำทางกายภาพอื่น ๆ ที่เข้าไปยุ่งเกี่ยวกับระบบคอมพิวเตอร์และมุ่งถึงเจตนาพิเศษของผู้กระทำเป็นสำคัญ จึงต้องพิจารณาจากข้อเท็จจริงที่ผู้กระทำได้กระทำไปเพื่อค้นหาเจตนาพิเศษดังกล่าว เช่น การป้อนโปรแกรมที่ทำให้ระบบคอมพิวเตอร์ปฏิเสธการทำงาน (Denial of Service) หรือทำให้ระบบคอมพิวเตอร์ทำงานได้ช้าลงโดยการป้อนไวรัสคอมพิวเตอร์เพื่อให้เกิดผลชะลอการทำงานของระบบ เป็นต้น.

ความผิดฐานส่งข้อมูลคอมพิวเตอร์รบกวนบุคคลอื่นนี้ ได้มีการบัญญัติเพิ่มขึ้นในชั้นการพิจารณาของสภานิติบัญญัติแห่งชาติ โดยมีเจตนารมณ์ที่จะกำหนดความผิดของบุคคลที่ส่งสแปมเมล์ (Spam mail) โดยที่ในปัจจุบันการกระทำดังกล่าวได้ก่อให้เกิดความเสียหายแก่ผู้ใช้อินเทอร์เน็ตเป็นอย่างยิ่ง เพราะสร้างความเดือดร้อนรำคาญและความเสียหายทางเศรษฐกิจแก่ผู้ใช้ระบบคอมพิวเตอร์[93]

สำหรับความผิดตามมาตรานี้ คือเป็นบทบัญญัติที่มีโทษปรับสถานเดียวและไม่มีโทษจำคุก จึงถือว่าเป็นโทษที่ค่อนข้างเบา ในประเด็นที่เทียบเคียงกับความผิดฐานบุกรุกซึ่งเป็นความผิดอันยอมความได้ แต่เนื่องจากการส่งอีเมล์สแปม “Email Spam” นี้มักจะไม่ทำกับผู้เสียหายคนเดียว แต่มักจะทำในวงกว้าง หากกำหนดให้เป็นความผิดอันยอมความได้จะมีปัญหาเกี่ยวกับการร้องทุกข์เพื่อดำเนินคดีซึ่งมีผู้เสียหายจำนวนมาก จึงไม่ได้กำหนดให้เป็นความผิดอันยอมความได้

8. บทลงโทษที่หนักขึ้นสำหรับการกระทำที่ก่อให้เกิดความเสียหายแก่ประชาชนหรือการรักษาความมั่นคงของประเทศ ฯลฯ มาตรา 12 บัญญัติว่า “ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10

(1) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปีและปรับไม่เกินสองแสนบาท

(2) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะหรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

---

[93] มานิตย์ จุมปา, *คำอธิบายกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์*, พิมพ์ครั้งที่ 2, (กรุงเทพฯ: วิญญูชน, 2554), 83.

ถ้าการกระทำความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี"[94]

เป็นการพิจารณาผลที่ก่อให้เกิดความเสียหายนั้นต้องเกิดขึ้นอย่างแน่แท้ เพียงแต่ว่าถึงแม้จะยังไม่เกิดแต่แน่นอนว่าหากจะเกิดขึ้นในภายหน้าก็ถือว่าเข้าองค์ประกอบความผิด มาตรา 12(2) พิจารณาจากลักษณะของการกระทำที่ไปกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่กฎหมายมุ่งให้ความคุ้มครองเป็นพิเศษ เช่น ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือการบริการสาธารณะ และข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ส่วนความในวรรคท้ายของมาตรา 12 เป็นบทฉกรรจ์สำหรับการลงโทษที่หนักขึ้นของผู้กระทำความผิดตามมาตรา 12(2) ที่เป็นเหตุให้ผู้อื่นถึงแก่ความตาย คือต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

9. การจำหน่ายชุดคำสั่งที่จัดทำขึ้นเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด มาตรา 13 บัญญัติว่า "ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ"การจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด อาทิ โปรแกรมเจาะระบบ (Auto-rooters), โปรแกรมดักข้อมูลผ่านปุ่มคีย์บอร์ด (Keyloggers), โปรแกรม Macro Viruses, โปรแกรมส่งสแปมเมล์ (Spammer) เป็นต้น[95]

10. การใช้ระบบคอมพิวเตอร์ทำความผิดอื่น มาตรา 14 บัญญัติว่า "ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ

---

[94] มีข้อสังเกตว่า เหตุฉกรรจ์ตามมาตรา 12 วรรคท้าย ที่เป็นเหตุให้ผู้อื่นถึงแก่ความตายนั้น หากเป็นกรณีที่ผู้กระทำมีเจตนาฆ่า ผู้กระทำต้องมีความผิดตามประมวลกฎหมายอาญา มาตรา 288 หรือมาตรา 289 แล้วแต่กรณี ซึ่งมีอัตราโทษจำคุกสูงสุด คือประหารชีวิต หากเป็นกรณีที่ผู้กระทำได้กระทำไปโดยประมาทก็ต้องถือว่าเป็นกรรมเดียวผิดกฎหมายหลายบทต้องปรับบทความผิดตามประมวลกฎหมายอาญา มาตรา 291 ด้วย แต่เนื่องจากโทษตามมาตรา 12 แห่งพระราชบัญญัตินี้หนักกว่าโทษตามประมวลกฎหมายอาญา มาตรา 291 ที่กำหนดไว้จำคุกไม่เกินสิบปี จึงต้องใช้บทลงโทษตามมาตรา 12 วรรคท้าย ซึ่งหนักกว่า ทั้งนี้เป็นไปตามประมวลกฎหมายอาญา มาตรา 90 หรือแม้แต่การกระทำให้ผู้อื่นถึงแก่ความตายโดยไม่เจตนาตามประมวลกฎหมายอาญา มาตรา 290 ก็มีอัตราโทษ คือจำคุกตั้งแต่สามปีถึงสิบห้าปี ซึ่งเป็นอัตราโทษที่เบากว่ามาตรา 12 วรรคท้าย.

[95] ณัฐกร วิทิตานนท์, กฎหมายคอมพิวเตอร์ในประเทศไทย: พัฒนาการ ฐานความผิด และปัญหาการใช้บังคับ, ใน *Rapee, School of law, Mae Fah Luang University*, (กรุงเทพฯ: วิญญชน, 2557), 91-99.

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่คอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)"

ตามองค์ประกอบความผิดในฐานการนำข้อมูลคอมพิวเตอร์หรือโปรแกรมซอฟต์แวร์ต่าง ๆ เข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ที่มีการเปลี่ยนแปลงแก้ไข ไม่ว่าการเปลี่ยนแปลงแก้ไขนั้นจะทั้งหมดหรือแต่เพียงบางส่วนหรือข้อมูลคอมพิวเตอร์ที่ไม่ใช่ของจริงและผู้กระทำต้องมีเจตนานำเข้าสู่ระบบคอมพิวเตอร์ ในขณะเดียวกันผู้กระทำต้องรู้ถึงข้อเท็จจริงในองค์ประกอบความผิดว่าเป็นข้อมูลคอมพิวเตอร์ปลอมหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จและต้องรู้ว่าการกระทำดังกล่าวเป็นการกระทำที่น่าจะเกิดความเสียหายแก่ผู้อื่นและความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

11. ผู้ให้บริการจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิด มาตรา 15 บัญญัติว่า "ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14" ผู้ให้บริการ[96] แก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ตหรือผู้ใดก็ตามหากมีการกระทำอันเป็นการสนับสนุนหรือยินยอมให้มีการกระทำความผิด และต้องเป็นเรื่องที่ผู้ให้บริการรู้ว่ามีการกระทำความผิดตามมาตรา 14 กระทำความผิดในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

12. ตกแต่งข้อมูลคอมพิวเตอร์ที่เป็นภาพของบุคคล มาตรา 16 บัญญัติว่า "ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทาง

---

[96] "ผู้ให้บริการ" หมายถึง (1) ผู้ให้บริการแก่บุคคลอื่น ในการเข้าสู่อินเทอร์เน็ตหรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น (2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น.

อิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาทหรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย”

ฐานความผิดนี้เป็นลักษณะของการดูหมิ่นหรือหมิ่นประมาทด้วยการตกแต่งภาพของบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด มีองค์ประกอบความผิด ดังนี้ ผู้กระทำได้มีการกระทำอันเป็นการนำข้อมูลคอมพิวเตอร์เข้าสู่ระบบคอมพิวเตอร์ และระบบคอมพิวเตอร์นั้นเป็นระบบที่ประชาชนทั่วไปอาจเข้าถึงได้ถ้าเป็นระบบคอมพิวเตอร์ของตนเองก็ไม่เป็นความผิด และองค์ประกอบความผิดข้อนี้ต้องเป็นข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น หมายถึงการแสดงข้อมูลคอมพิวเตอร์ออกเป็นภาพของบุคคล และภาพนั้นอาจเกิดจากการสร้างขึ้นใหม่ หรือเป็นภาพที่มีอยู่แต่ได้มีการตัดต่อ เติมหรือดัดแปลงซึ่งเป็นการทำด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด

ข้อสังเกตประการต่อไปสำหรับความผิดตามมาตรา 16 ก็คือความผิดตามมาตรานี้เป็นความผิดอันยอมความได้ และเป็นความผิดมาตราเดียวที่บัญญัติให้เป็นความผิดอันยอมความได้ ทั้งนี้เนื่องจากเห็นได้ชัดเจนว่าความเสียหายที่เกิดขึ้นนั้นเป็นความเสียหายเฉพาะบุคคล

ดังที่กล่าวมาแล้วข้างต้น การกระทำความผิดตามมาตรา 5 ถึงมาตรา 8 นั้นเป็นการกล่าวถึงการกระทำโดยมิชอบ ซึ่งหมายความถึง การบุกรุก และการล่วงรู้มาตรการป้องกัน ก็คือ การแอบรู้มาตรการป้องกันระบบคอมพิวเตอร์ ส่วนการกระทำผิดตามมาตรา 9 และมาตรา 10 ซึ่งจะเป็นความผิดในการรบกวนหรือทำลายระบบและข้อมูลคอมพิวเตอร์ มาตรา 11 นั้นก็คือการส่งจดหมายอีเล็กทรอนิกส์ หรืออีเมล์เพื่อรบกวนการใช้งานระบบคอมพิวเตอร์ และมาตรา 14 มาตรา 15 สำหรับเป็นกรณีการกระทำความผิดโดยการโพส (Post) ข้อมูลเท็จในเว็บบอร์ด (Webboard) หรือข้อมูลที่ไม่มีความจริงและยังรวมทั้งการฟอร์เวิร์ด (Forward) อีเมล์หรือการส่งต่ออีเมล์ มาจากเพื่อนหรือคนรู้จักหรือเป็นอีเมล์สแปม นอกจากนี้แล้วยังมีการกระทำความผิดตามมาตรา 16 ที่เน้นในรูปภาพ การสร้าง ตัดต่อ แต่งเติมหรือดัดแปลง

3.2.2.2 อำนาจของพนักงานเจ้าหน้าที่

ในส่วนของอำนาจพนักงานเจ้าหน้าที่นั้น ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายที่กำหนดโทษความผิดทางอาญา ซึ่งในการดำเนินคดีไม่ว่าในเรื่องการค้น การสืบสวนสอบสวน การจับกุม กักขังย่อมเป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอื่นที่เกี่ยวข้อง อย่างไรก็ตามเพื่อให้การดำเนินคดีตามพระราชบัญญัตินี้มีประสิทธิภาพจึงได้มีหลักการพิเศษเพิ่มขึ้น 2 ประการ ดังนี้[97]

1. การเพิ่มวิธีการพิเศษในการสืบสวนและสอบสวน และ

2. การเพิ่มให้ “พนักงานเจ้าหน้าที่” เข้ามามีอำนาจในการสืบสวนสอบสวนความผิดตามพระราชบัญญัติฉบับนี้ด้วยนอกเหนือจากเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญา

การสืบสวนสอบสวนเป็นจุดเริ่มต้นที่สำคัญของการดำเนินคดีอาญา เพราะการสืบสวนสอบสวนมีผลกระทบโดยตรงต่อการสร้างหรือทำลายกระบวนการยุติธรรม (Due Process of Law) สุดแต่ว่าการสืบสวนสอบสวนได้ดำเนินไปโดยถูกต้องสมบูรณ์และชอบธรรมเพียงใด ถ้าการสืบสวนสอบสวนกระทำไปโดยไม่มีประสิทธิภาพ ขาดหลักการและเหตุผลแล้ว ผลการดำเนินการของเจ้าหน้าที่กระบวนการยุติธรรมในชั้นพนักงานอัยการและศาลก็จะดำเนินการให้เกิดความเที่ยงธรรมได้โดยยาก เพราะการพิจารณาคดีของศาลต้องอาศัยพยานหลักฐาน หากพยานหลักฐานไม่ชัดแจ้งศาลอาจยกประโยชน์แห่งความสงสัยให้จำเลยและพิจารณาพิพากษายกฟ้องของโจทก์ปล่อยตัวจำเลยพ้นข้อหาไป ทั้งที่ข้อเท็จจริงจำเลยเป็นผู้กระทำผิด[98]

ประมวลกฎหมายวิธีพิจารณาความอาญาไม่ได้บัญญัติว่าจะต้องมีวิธีการสืบสวนอย่างไร บัญญัติแต่เพียงว่า “การแสวงหา...” ซึ่งหมายถึง การกระทำเพื่อที่จะได้พบในสิ่งที่ต้องการพบ เพื่อที่จะได้ทราบในสิ่งที่ต้องการทราบ การแสวงหาอาจกระทำได้ทั้งโดยทางลับและโดยทางเปิดเผย อย่างไรก็ตาม การแสวงหาหลักฐานในการสืบสวนอาจแบ่งออกเป็น 2 กรณีคือ (1) การแสวงหาโดยไม่เป็นการละเมิดสิทธิเสรีภาพของผู้อื่น ซึ่งสามารถกระทำได้โดยไม่มีขีดจำกัด และ (2) การแสวงหาที่เป็นการกระทำอันละเมิดสิทธิเสรีภาพของผู้อื่น ซึ่งมีลักษณะเป็นการใช้อำนาจรัฐแทนในฐานะที่เป็นเจ้าพนักงาน เช่น การตรวจค้น ซึ่งโดยหลักผู้สืบสวนไม่มีอำนาจกระทำได้

---

[97] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*.

[98] ธาริต เพ็งดิษฐ์, แนวทางการสืบสวนสอบสวนคดีพิเศษ, ใน *เอกสารประกอบการบรรยาย หลักสูตรการบริหารงานยุติธรรมระดับกลาง รุ่นที่ 2 (ยธก. 2)*, (กรุงเทพฯ: สถาบันพัฒนาข้าราชการฝ่ายอัยการ, ม.ป.ป.).

จะกระทำได้ต่อเมื่อมีกฎหมายบัญญัติให้อำนาจกระทำและจะต้องกระทำไปตามเงื่อนไขที่กฎหมายกำหนดไว้เท่านั้น[99]

การใช้อำนาจของพนักงานเจ้าหน้าที่ในการสืบสวนสอบสวนนั้นได้กำหนดให้การใช้อำนาจในบางมาตราที่ไม่ก่อให้เกิดผลกระทบต่อสิทธิความเป็นส่วนตัว หรืออาจกระทบต่อการประกอบการของผู้ให้บริการไม่มากเกินไป และใช้เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด กล่าวคือ การใช้อำนาจของพนักงานเจ้าหน้าที่ซึ่งไม่ต้องขออนุญาตศาล นอกจากนี้ในการใช้อำนาจที่อาจเสี่ยงต่อการละเมิดสิทธิขั้นพื้นฐานความเป็นส่วนตัวของประชาชนหรืออาจกระทบการประกอบการขององค์กรธุรกิจในการใช้อำนาจของพนักงานเจ้าหน้าที่ซึ่งต้องขออนุญาตจากศาล[100]

---

[99] ธาริต เพ็งดิษฐ์, แนวทางการสืบสวนสอบสวนคดีพิเศษ.

[100] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, มาตรา 18 บัญญัติว่า “ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวน ในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างใดอย่างหนึ่งต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นพยานหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บรักษาตามมาตรา 26 หรือที่อยู่ในความครอบครอง หรือควบคุมของผู้ให้บริการแก่พนักงานเจ้าหน้าที่

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อว่าได้มีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดหรือเพื่อสอบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับข้อมูลคอมพิวเตอร์ของบุคคลใดหรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับหรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้”.

ปัจจุบันการกระทำที่เข้าข่ายว่าเป็นความผิดตามพระราชบัญญัตินี้ ที่อาจกระทบต่อความมั่นคง หรือขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน โดยกระทบต่อความรู้สึกของคนในสังคมเป็นอย่างมากและในการจัดการกับปัญหาดังกล่าวจะต้องกระทำด้วยความรวดเร็ว แต่การระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์หรือการบล็อก (Block) เว็บไซต์ไม่ให้ระบบคอมพิวเตอร์เผยแพร่ข้อมูลคอมพิวเตอร์ที่เป็นความผิดดังกล่าวในระบบคอมพิวเตอร์อีกต่อไปนั้นอาจส่งผลกระทบต่อธุรกิจของผู้ให้บริการ จึงอาจทำให้เกิดเหตุการณ์ฟ้องร้องพนักงานเจ้าหน้าที่กลับได้ ด้วยเหตุนั้น พระราชบัญญัติดังกล่าวจึงกำหนดให้รัฐมนตรีผู้รักษาการมีบทบาทในการกลั่นกรองดุลพินิจของพนักงานเจ้าหน้าที่ก่อนที่จะดำเนินการยื่นขอการบล็อกเว็บไซต์จากศาล[101]

นอกจากนั้นพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ยังได้ให้อำนาจแก่พนักงานเจ้าหน้าที่ในการห้ามจำหน่ายชุดคำสั่งไม่พึงประสงค์หรือเผยแพร่โปรแกรมชั่วร้ายทั้งหลายที่สร้างขึ้นมาเพื่อก่อกวน ทำลายระบบคอมพิวเตอร์ และกระทำความผิดตามพระราชบัญญัติดังกล่าว ในรูปแบบต่าง ๆ อาทิ ไวรัส (Virus) สปายแวร์ (Spyware)[102] เป็นต้น นอกจากจะห้ามการจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์แล้วพนักงานเจ้าหน้าที่ยังสามารถ

---

[101] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, มาตรา 20 บัญญัติว่า "ในกรณีที่มีการกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสอง ลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้".

[102] สปายแวร์ คือ ประเภทโปรแกรมคอมพิวเตอร์ที่บันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์ และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูล สถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม ซึ่งส่วนใหญ่แล้วบันทึกเว็บไซต์ที่ผู้ใช้เข้าถึง และส่งไปยังบริษัทโฆษณาต่าง ๆ บางโปรแกรมอาจบันทึกว่าผู้ใช้พิมพ์อะไรบ้าง เพื่อพยายามค้นหารหัสผ่าน หรือเลขหมายบัตรเครดิต.

กำหนดเงื่อนไขในการใช้ การครอบครอง และการเผยแพร่โปรแกรมข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วยนั้นด้วยการระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้[103]

สรุปได้ว่า องค์การสหประชาชาติอันเป็นองค์กรระหว่างประเทศระดับโลกได้เห็นถึงความสำคัญของการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์จึงได้มีการจัดทำคู่มือเกี่ยวกับการป้องกันและควบคุมอาชญากรรมคอมพิวเตอร์ (UN Manual on the Prevention and Control of Computer-related Crime) เพื่อให้เป็นแนวปฏิบัติแก่คณะทำงานและเป็นต้นแบบในการร่างกฎหมายกฎหมายเกี่ยวกับมาตรการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ของประเทศภาคีสมาชิกอีกด้วย ในขณะที่สหภาพโทรคมระหว่างประเทศ เป็นองค์กรระหว่างประเทศที่ทำหน้าที่เกี่ยวกับการดูแลควบคุมการสื่อสารและเทคโนโลยีการสื่อสารของประเทศภาคีสมาชิกให้อยู่ในความเรียบร้อย ก็ได้มีการออกกฎข้อบังคับว่าด้วยโทรคมนาคมระหว่างประเทศ (International Telecommunication Regulation: ITR) เพื่อป้องกันมิให้มีการนำเทคโนโลยีไปใช้ในทางที่ผิด อันจะสร้างความเสียหายให้แก่สังคมและประเทศชาติได้ นอกจากนี้องค์กรระดับภูมิภาคอย่างสหภาพยุโรป ได้มีการร่วมมือกันจัดทำอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime) เพื่อต้องการและปราบปรามอาชญากรรมทางคอมพิวเตอร์ให้หมดไป ตลอดทั้งเพื่อให้ประเทศภาคีสมาชิกได้ใช้เป็นแนวทางในการตรากฎหมายภายในให้เป็นไปในทิดทางเดียวกัน

ประเทศสิงคโปร์และประเทศไทย ต่างก็เห็นถึงความสำคัญและผลกระทบของการนำเทคโนโลยีการสื่อสารไปใช้ในทางที่ผิด อันส่งผลเสียหายต่อเศรษฐกิจ และประเทศชาติ จึงได้มีการตรากฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ขึ้นโดยมีการประยุกต์จากกฎหมายหรือหลักเกณฑ์ระหว่างประเทศต่าง ๆ ที่เกี่ยวข้อง เพื่อให้กฎหมายมีความสมบูรณ์มากที่สุด เพื่อให้สามารถบังคับใช้อย่างเหมาะสมและเป็นธรรม ด้วยเหตุนี้จึงได้ทำการศึกษาเปรียบเทียบเพื่อนำรายละเอียดของกฎหมายประเทศสิงคโปร์และไทยไปวิเคราะห์และสรุปเป็นข้อเสนอแนะให้มีการแก้ไขปรับปรุงมาตรการทางกฎหมายที่เกี่ยวการกระทำผิดทาง

---

[103] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, มาตรา 21 บัญญัติว่า "ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่ง หมายถึง ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา".

คอมพิวเตอร์ของ สปป.ลาว และส่งเสริมให้เห็นถึงความสำคัญและผลกระทบของอาชญากรรมทางคอมพิวเตอร์ พร้อมทั้งผลักดันให้มาตรการทางกฎหมายดังกล่าวได้มีการบังคับใช้เป็นกฎหมายอย่างสมบูรณ์โดยเร็ว ซึ่งในบทต่อไปจะได้วิเคราะห์ร่างกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางคอมพิวเตอร์ ค.ศ. ... และผลกระทบของอาชญากรรมทางคอมพิวเตอร์ใน สปป.ลาว ต่อไป

**ตารางที่ 3.1** เปรียบเทียบมาตรการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์

| | สหภาพยุโรป | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 1. กฎหมายที่เกี่ยวข้อง | อนุสัญญาของสหภาพยุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 | พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทางคอมพิวเตอร์ ค.ศ. 2007 | พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 | |
| 2. ฐานความผิด | มีลักษณะของการกระทำต่อความลับ ความเที่ยงตรง และความมีอยู่ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ | การกระทำผิดใด ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ โปรแกรม และข้อมูลคอมพิวเตอร์ | การกระทำที่กระทบต่อการรักษาความลับ ความสมบูรณ์และถูกต้อง และความพร้อมใช้งานของระบบคอมพิวเตอร์ | แต่ละประเทศได้มีการกำหนดถึงลักษณะของการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์ที่แตกต่างกันไป แต่สิ่งสำคัญคือ ต้องเป็นการกระทำผิดที่มีหรือใช้คอมพิวเตอร์ หรือที่กระทำต่อคอมพิวเตอร์ โปรแกรม และหรือระบบคอมพิวเตอร์ |
| 2.1 การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต | การเข้าถึงโดยมิชอบด้วยกฎหมายเป็นการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือบางส่วน ซึ่งได้กระทำโดยเจตนา และโดยไม่มีสิทธิ ประเทศภาคีอาจกำหนดให้เป็นความผิดเฉพาะกรณีเป็นการกระทำโดยล่วงล้ำมาตรการรักษา- | การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งบุคคลใดก็ตามที่เจตนาใช้คอมพิวเตอร์เพื่อวัตถุประสงค์ในการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งข้อมูลคอมพิวเตอร์หรือโปรแกรมที่อยู่ในคอมพิวเตอร์ใด ๆ ที่มีการป้องกันการเข้าถึง- | ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน (มาตรา 5)<br>ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และ- | สหภาพยุโรป มีการบัญญัติกฎหมายไว้ในลักษณะกว้าง เพื่อให้ประเทศภาคีสมาชิกนำไปอนุวัติการเป็นกฎหมายภายในและต้องมีความสอดคล้องกับอนุสัญญาดังกล่าวด้วย ซึ่งประเทศสิงคโปร์ และประเทศ- |

**ตารางที่ 3.1** (ต่อ)

| | สหภาพยุโรป | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 2.1 (ต่อ) | ความปลอดภัยโดยมีเจตนาที่จะได้มาซึ่งข้อมูลคอมพิวเตอร์หรือโดยมีเจตนาทุจริตประการอื่นหรือเฉพาะกรณีเป็นการกระทำเกี่ยวกับระบบคอมพิวเตอร์ที่เชื่อมโยงกับระบบคอมพิวเตอร์อื่นนั้นก็ได้ (มาตรา 2) | โดยเฉพาะ ถือว่ามีความผิด ถึงแม้ว่าการกระทำดังกล่าวจะเป็นการกระทำเพื่อการเข้าถึงคอมพิวเตอร์และระบบคอมพิวเตอร์ สำหรับวัตถุประสงค์ของส่วนนี้ ให้ถือว่าไม่ได้มุ่งถึงโปรแกรมหรือข้อมูลใดโดยเฉพาะโปรแกรมหรือข้อมูลชนิดใด ๆ หรือโปรแกรมหรือข้อมูลในคอมพิวเตอร์เครื่องใด ๆ โดยเฉพาะและในกรณีมีการกระทำผิดซ้ำจะได้รับโทษเพิ่มขึ้น (มาตรา 3) | มาตาการนั้นมิได้มีไว้สำหรับตน (มาตรา 7) | ไทย ต่างก็ได้มีการบัญญัติครอบคลุมเรื่องของการเข้าถึงระบบและข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาตด้วย แต่ประเทศสิงคโปร์มีความพิเศษกว่า คือมีการบัญญัติเพิ่มโทษด้วยในกรณีที่ได้มีการกระทำความผิดซ้ำ |
| 2.2 การดักรับข้อมูลโดยไม่ได้รับอนุญาต | การดักโดยมิชอบด้วยกฎหมายเป็นการดักการส่งข้อมูลคอมพิวเตอร์ซึ่งส่งไปหรือส่งจากหรือส่งภายในระบบคอมพิวเตอร์ที่มิใช่ข้อมูลสาธารณะ โดยวิธีการทางเทคนิค รวมถึงการแผ่รังสีทางแม่เหล็กไฟฟ้าจากระบบคอมพิวเตอร์ที่มีข้อมูล- | การใช้หรือดักจับข้อมูลบริการคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งบุคคลใด ๆ ได้ทำการเข้าถึงคอมพิวเตอร์ใด ๆ โดยไม่ได้รับอนุญาตเพื่อรับบริการของคอมพิวเตอร์ ไม่ว่าโดยตรงหรือโดยอ้อม และได้กระทำการดักจับหรือทำ- | ผู้ใดกระทำด้วยประการใด โดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้- | ประเทศสิงคโปร์ บัญญัติถึงการดักจับข้อมูลบริการเพื่อเข้ารับบริการของคอมพิวเตอร์โดยไม่ได้รับอนุญาต ไม่ว่าจะเป็นทางตรงหรือทางอ้อมโดยเจตนาในการใช้หรือการทำให้เกิดการใช้ ไม่ว่าทางตรงหรือทางอ้อม ซึ่งประเทศ- |

**ตารางที่ 3.1** (ต่อ)

| | สหภาพยุโรป | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 2.2 (ต่อ) | คอมพิวเตอร์เช่นว่านั้น ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธิ ประเทศภาคีอาจกำหนดให้เป็นความผิดนี้เฉพาะกรณีเป็นการกระทำโดยมีเจตนาทุจริตหรือเฉพาะกรณีเป็นการกระทำเกี่ยวกับระบบคอมพิวเตอร์ที่เชื่อมโยงกับระบบคอมพิวเตอร์อื่นนั้นก็ได้ (มาตรา 3) | ให้ถูกดักจับโดยไม่ได้รับอนุญาต ไม่ว่าทางตรงหรือทางอ้อม ซึ่งการทำงานของคอมพิวเตอร์ ไม่ว่าโดยวิธีการใดก็ตาม โดยเจตนาในการใช้หรือทำให้เกิดการใช้ ไม่ว่าโดยทางตรงหรือทางอ้อมซึ่งคอมพิวเตอร์หรืออุปกรณ์ใด ๆ และการกระทำดังกล่าวได้ก่อให้เกิดความเสียหายสำหรับวัตถุประสงค์ของส่วนนี้ไม่ได้มุ่งถึงโปรแกรมหรือข้อมูลใด ๆ เป็นการเฉพาะ (มาตรา 6) | ประโยชน์ได้ (มาตรา 8) | ไทยมิได้มีการบัญญัติในลักษณะดังกล่าว มีเพียงการดักจับข้อมูลทางอิเล็กทรอนิกส์ จะเห็นได้ว่าประเทศไทยบัญญัติกฎหมายได้กว้างกว่า หมายความว่า การดักจับนั้นอยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ที่ข้อมูลมิได้มีไว้เพื่อประโยชน์สาธารณะ |
| 2.3 การรบกวนข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต | การแทรกแซงต่อข้อมูล<br>1. ประเทศภาคีแต่ละประเทศพึงจัดให้มีมาตรการทางนิติบัญญัติหรือมาตรการอื่นที่จำเป็น เพื่อกำหนดให้เป็นความผิดทางอาญาภายใต้กฎหมายภายในของประเทศนั้น ซึ่งการทำให้เสียหาย การลบ การทำให้- | การดัดแปลงแก้ไขข้อมูลคอมพิวเตอร์ ซึ่งบุคคลใดกระทำการใด ๆ โดยมิชอบ ซึ่งรู้ว่าจะทำให้เกิดการดัดแปลง แก้ไขเนื้อหาใด ๆ ของคอมพิวเตอร์ เป็นการกระทำผิด อย่างไรก็ตามการดัดแปลงแก้ไขข้อมูลคอมพิวเตอร์ในกรณีที่- | ผู้ใดทำให้เสียหาย ทำลาย แก้ไขเปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 9) | ประเทศสิงคโปร์ มีการบัญญัติลักษณะของการกระทำไว้ คือ (1) เพิ่มมาตรการลงโทษในกรณีกระทำผิดซ้ำ (2) การดัดแปลงแก้ไขเป็นการถาวรหรือชั่วคราวก็ถือว่าเป็นการกระทำผิด<br>ส่วนของประเทศไทย มิได้มี- |

**ตารางที่ 3.1** (ต่อ)

| | สหภาพยุโรป | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 2.3 (ต่อ) | เสื่อมเสีย การแก้ไขดัดแปลง หรือการทำลายข้อมูลคอมพิวเตอร์ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น<br>2. ประเทศภาคีอาจสงวนสิทธิที่จะกำหนดให้การกระทำตามวรรคหนึ่งเป็นความผิดเฉพาะกรณีที่ผลของการกระทำได้ก่อความเสียหายอย่างร้ายแรงนั้นก็ได้ (มาตรา 4) | จำเป็นแก่การใช้ เช่น ผู้ใช้สามารถดัดแปลงโปรแกรมคอมพิวเตอร์เท่าที่จำเป็น และหากมีการกระทำผิดซ้ำต้องได้รับโทษเพิ่มขึ้น แต่ในกรณีนี้การดัดแปลงที่ก่อให้เกิดความเสียหายไม่ว่าจะเป็นการดัดแปลงเป็นการถาวรหรือเป็นการชั่วคราวก็ถือว่าเป็นการกระทำผิด (มาตรา 5) | | การบัญญัติถึงการกระทำผิดซ้ำที่จะต้องถูกลงโทษหลักขึ้น และมิได้จำกัดว่าการแก้ไขข้อมูลนั้นจะเป็นข้อมูลอันจำเป็นแก่การใช้หรือไม่ หมายความว่าหากทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลใด ๆ ย่อมมีความผิด |
| 2.4 การรบกวนระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต | การแทรกแซงต่อระบบ เป็นการกีดขวางการทำงานของระบบคอมพิวเตอร์อย่างร้ายแรง โดยการใส่เข้า การส่งต่อ การทำให้เสียหาย การลบ การทำให้เสื่อมเสีย การแก้ไขดัดแปลง หรือการทำลายข้อมูลคอมพิวเตอร์ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธิ (มาตรา 5) | การเข้าขัดขวางการใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งบุคคลใดเจตนาและปราศจากอำนาจหรือข้ออ้างใด ๆ ตามกฎหมาย เพื่อเข้ารบกวนหรือขัดขวางการใช้งานโดยถูกกฎหมายซึ่งคอมพิวเตอร์หรือไม่ยอมให้เข้าถึงหรือทำให้ประสิทธิภาพในการทำงานลดลงซึ่งโปรแกรมหรือข้อมูลที่ถูกเก็บไว้ใน- | ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ (มาตรา 10)<br>ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว- | ประเทศสิงคโปร์มีการบัญญัติกฎหมายโดยรวมการกระทำผิดดังกล่าวไว้ในมาตราเดียวกัน แต่ประเทศไทยมีการแยกบัญญัติไว้โดยมิได้ระบุเฉพาะเจาะจงเกี่ยวกับการขัดขวางการใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือรบกวนหรือขัดขวางการใช้งานของระบบคอมพิวเตอร์ จะเห็น |

**ตารางที่ 3.1** (ต่อ)

| | สหภาพยุโรป | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 2.4 (ต่อ) | การปลอมแปลงเกี่ยวกับคอมพิวเตอร์เป็นการใส่เข้า การแก้ไขดัดแปลง การลบ หรือการทำลายข้อมูลคอมพิวเตอร์ ซึ่งส่งผลให้ข้อมูลคลาดเคลื่อนโดยประสงค์ที่จะทำให้เป็นไปหรือใช้ในทางกฎหมายในลักษณะเหมือนกับว่าข้อมูลที่ถูกกระทำดังกล่าวแล้วนั้นเป็นข้อมูลที่ถูกต้อง ทั้งนี้โดยไม่คำนึงถึงว่าข้อมูลนั้นสามารถอ่านได้หรือเข้าใจได้โดยตรงหรือไม่ก็ตาม ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธินั้น ประเทศภาคีอาจกำหนดให้ต้องรับผิดทางอาญาในการกระทำนี้ เฉพาะกรณีเป็นการกระทำโดยมีเจตนาที่จะฉ้อโกงหรือมีเจตนาทุจริตในลักษณะทำนองเดียวกันก็ได้ | คอมพิวเตอร์ ผู้นั้นมีความผิดและต้องได้รับโทษ หรือถ้าความเสียหายที่เกิดขึ้นเป็นผลมาจากการเข้าขัดขวางการใช้งานคอมพิวเตอร์ก็จะได้รับโทษเพิ่มมากยิ่งขึ้น (มาตรา 7) | อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข (มาตรา 11)<br>ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตาการนั้นมิได้มีไว้สำหรับตน (มาตรา 7) | ได้ว่าประเทศไทย บัญญัติกฎหมายที่มีลักษณะให้ความหมายหรือการตีความได้กว้างกว่ากฎหมายของประเทศสิงคโปร์ |

**ตารางที่ 3.1** (ต่อ)

| | สหภาพยุโรป | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 2.5 การใช้อุปกรณ์โดยมิชอบและการจำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อใช้ในการกระทำความผิด | การใช้อุปกรณ์โดยมิชอบเป็นการกระทำดังต่อไปนี้ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธิ เช่น การผลิต การขาย การจัดให้มีเพื่อใช้ประโยชน์ การนำเข้า การจำหน่ายจ่ายแจกหรือการทำให้มีขึ้นซึ่ง (1) อุปกรณ์ รวมถึงโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบหรือดัดแปลงโดยมีวัตถุประสงค์หลักเพื่อใช้ในการกระทำความผิดใด ๆ ในประเภทดังกล่าว และ (2) รหัสผ่านคอมพิวเตอร์ รหัสการเข้าถึงคอมพิวเตอร์ หรือข้อมูลที่มีลักษณะทำนองเดียวกัน ซึ่งทำให้สามารถใช้ในการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือส่วนหนึ่งส่วนใด โดยมีเจตนาที่จะใช้เพื่อวัตถุประสงค์ในการกระทำความผิด ความในข้อนี้ไม่พึง- | ไม่มีการบัญญัติเกี่ยวกับฐานความผิดนี้ | ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด (มาตรา 13) | สหภาพยุโรปมีการบัญญัติแยกเป็น 2 กรณีคือ (1) การผลิตอุปกรณ์และโปรแกรมที่ใช้ในการกระทำความผิด และ (2) การล่วงรู้มาตรการเข้าถึงข้อมูล<br>ส่วนประเทศไทยได้มีการบัญญัติแยกประเด็นของการใช้อุปกรณ์ และโปรแกรมในการกระทำความผิด และการล่วงรู้มาตรการเข้าถึงข้อมูลไว้คนละมาตราเพื่อให้สะดวกต่อการบังคับใช้ |

**ตารางที่ 3.1** (ต่อ)

| | สหภาพยุโรป | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 2.5 (ต่อ) | ถูกตีความในทางกำหนดความรับผิดทางอาญาสำหรับกรณีที่การผลิต การขาย การจัดให้มีเพื่อใช้ประโยชน์ การนำเข้า การจำน่ายจ่ายแจกหรือการทำให้มีขึ้นหรือการครอบครองดังกล่าวไว้ข้างต้นของข้อนี้ และไม่ได้มีวัตถุประสงค์ในการกระทำความผิดใดประเภทใดในข้อ 2-5 ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 นี้ เช่น มีวัตถุประสงค์เพื่อการทดสอบหรือคุ้มครองระบบคอมพิวเตอร์ที่ได้รับอนุญาตโดยชอบนั้น (มาตรา 6) | | | |
| 2.6 การล่วงรู้มาตรการป้องกันการเข้าถึง และนำไปเผยแพร่ | | การเปิดเผยรหัสเชื่อมต่อโดยไม่ได้รับอนุญาต ซึ่งบุคคลใดเจตนาและไม่ได้รับอนุญาตในการเปิดเผยรหัสเชื่อมต่อ รหัสผ่านหรือวิธีการอื่นใดก็ตามในการเข้าถึงโปรแกรมหรือ- | ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่- | ประเทศไทยต้องมีการเปิดเผยการเข้าถึงมาตรการป้องกันโดยมิชอบ โดยมิได้นำเรื่องเจตนาหรือไม่เจตนาเข้ามาบัญญัติไว้ด้วย แต่ประเทศสิงคโปร์มีการ- |

**ตารางที่ 3.1** (ต่อ)

| | สหภาพยุโรป | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 2.6 (ต่อ) | | ข้อมูลที่เก็บไว้ในคอมพิวเตอร์ใด ๆ ให้ถือว่าเป็นการกระทำผิด หากผู้นั้นกระทำไปเพื่อผลประโยชน์โดยมิชอบ เพื่อวัตถุประสงค์ที่ผิดกฎหมายหรือรู้ว่าจะทำให้เกิดความเสียหายต่อบุคคลใดก็ตาม (มาตรา 8) | ผู้อื่น (มาตรา 6) | นำเรื่องเจตนามาบัญญัติไว้กล่าวคือถึงแม้ไม่มีเจตนากเปิดเผยก็มีความผิด |
| 2.7 การฉ้อโกง | การฉ้อโกงที่เกี่ยวข้องกับคอมพิวเตอร์ เป็นการทำให้เกิดความสูญเสียในทรัพย์สินของบุคคลอื่นโดยวิธีการดังต่อไปนี้ ซึ่งได้กระทำโดยเจตนาและโดยไม่มีสิทธิ (ก) การใส่เข้า การแก้ไขดัดแปลง การลบหรือการทำลายข้อมูลคอมพิวเตอร์ และ (ข) การแทรกแซงต่อการทำงานของระบบคอมพิวเตอร์ ทั้งนี้โดยผู้กระทำมีเจตนาในทางฉ้อโกงหรือเจตนาทุจริตที่จะเอาไปเสีย ซึ่งประโยชน์ทางเศรษฐกิจ สำหรับ- | การเข้าถึงด้วยเจตนาในการกระทำความผิดหรือพยายามกระทำความผิด บุคคลใดก็ตามที่ใช้คอมพิวเตอร์ในการเข้าถึงข้อมูลหรือโปรแกรมที่อยู่ในคอมพิวเตอร์ใด ๆ โดยเจตนาที่จะกระทำความผิดหรือพยายามกระทำความผิดก็ถือเป็นความผิด ซึ่งการกระทำผิดนี้ให้บังคับใช้กับความผิดเกี่ยวกับทรัพย์สิน การฉ้อโกง หรือกระทำให้เกิดความเสียหายต่อร่างกายโดยอนุโลม ซึ่งการกระทำนี้จะกระทำในขณะที่มีการ | ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 9) | ความผิดฐานฉ้อโกงนี้ ประเทศไทยมิได้มีการบัญญัติเป็นความผิดไว้โดยตรง กล่าวคือมีเพียงการบัญญัติถึงการแก้ไขเปลี่ยนแปลง ทำลาย ฯลฯ ต่อข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาตตามที่กฎหมายบัญญัติไว้เท่านั้นเป็นความผิด ส่วนสหภาพยุโรป และประเทศสิงคโปร์มีการบัญญัติไว้ชัดเจนกว่าถึงการฉ้อโกงหรือเอาไปเสียซึ่งประโยชน์ทางเศรษฐกิจสำหรับ- |

**ตารางที่ 3.1** (ต่อ)

| | สหภาพยุโรป | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 2.7 (ต่อ) | ตนเองหรือบุคคลอื่นโดยไม่มีสิทธิ | เชื่อมต่อกับระบบรักษาความปลอดภัยหรือไม่ก็ตาม โดยไม่คำนึงว่าจะได้รับอนุญาตหรือไม่ก็ตาม (มาตรา 4) | | ตนเองหรือบุคคลอื่นโดยไม่มีสิทธิ |
| 3. การให้อำนาจพนักงานเจ้าหน้าที่ | ประเทศภาคีแต่ละประเทศพึงจัดให้มีมาตรการทางนิติบัญญัติและมาตรการอื่นที่จำเป็น เพื่อกำหนดอำนาจหน้าที่และวิธีพิจารณาความตามความในตอนนี้ เพื่อวัตถุประสงค์ในการสอบสวนหรือดำเนินคดีอาญาในเรื่องอาชญากรรมทางคอมพิวเตอร์ | ได้มีการบัญญัติให้การดำเนินการสืบสวนสอบสวนของเจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจให้ดำเนินการสืบสวนตามมาตรา 39 แห่งกฎหมายวิธีพิจารณาความอาญา ค.ศ. 2010 | เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใดดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด | เพื่อให้การดำเนินการสืบสวนสอบสวนหาการกระทำผิด และผู้กระทำความผิดได้อย่างรวดเร็ว จึงได้มีการให้อำนาจแก่พนักงานเจ้าหน้าที่ |

**ตารางที่ 3.1** (ต่อ)

| | สหภาพยุโรป | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 3.1 ตรวจสอบระบบคอมพิวเตอร์ที่ต้องสงสัยว่ามีการนำมาใช้กระทำความผิด | ให้หน่วยงานที่มีอำนาจหน้าที่ที่เกี่ยวข้องของประเทศนั้นสามารถออกคำสั่งเรียกหรือรับเอาด้วยวิธีการอื่น ซึ่งการเก็บรักษาที่รวดเร็วของข้อมูลคอมพิวเตอร์ที่เฉพาะเจาะจง รวมถึงข้อมูลจราจรทางคอมพิวเตอร์ซึ่งถูกเก็บไว้โดยวิธีการของระบบคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งเมื่อมีเหตุอันควรเชื่อว่าข้อมูลคอมพิวเตอร์นั้นมีความเสี่ยงโดยเฉพาะที่จะสูญหายหรือจะถูกแก้ไข ดัดแปลง | เจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจตามกฎหมายสืบสวนคดีความการกระทำผิดที่สามารถจับคุมได้ สามารถเข้าถึงตรวจสอบการทำงานของคอมพิวเตอร์ซึ่งเจ้าหน้าที่นั้นมีเหตุให้สงสัยว่าได้ถูกใช้ในการกระทำผิด | มีหนังสือสอบถามหรือเรียกตัวบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจง เป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้ | ประเทศสิงคโปร์ได้มีการให้อำนาจเจ้าหน้าที่ในการจับกุมได้ |
| 3.2 อำนาจในการค้นหรือเข้ายึด | ให้อำนาจแก่หน่วยงานที่มีอำนาจหน้าที่ที่เกี่ยวข้องนั้นในการค้นหรือวิธีอื่นในลักษณะทำนองเดียวกันเพื่อเข้าถึงระบบคอมพิวเตอร์หรือบางส่วนของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ในระบบคอมพิวเตอร์นั้น และสื่อกลาง- | เจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจตามกฎหมายสืบสวนคดีความการกระทำผิดสามารถกระทำการใช้หรือทำให้เกิดการใช้ซึ่งคอมพิวเตอร์เพื่อค้นข้อมูลหรือที่มีอยู่ในคอมพิวเตอร์นั้น | ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหา- | สหภาพยุโรปได้ให้อำนาจในการเข้าถึงไม่ว่าทั้งหมดหรือบางส่วนของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ |

**ตารางที่ 3.1** (ต่อ)

| | สหภาพยุโรป | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 3.2 (ต่อ) | ที่ใช้เก็บข้อมูลคอมพิวเตอร์ในกรณีที่ข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้นั้นอาจอยู่ในอาณาเขตของประเทศนั้น | | ตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้ | |
| 3.3 การเรียกข้อมูลจราจรทางคอมพิวเตอร์ | ให้ผู้ให้บริการซึ่งให้บริการอยู่ในอาณาเขตของประเทศภาคีส่งข้อมูลของผู้สมัครเป็นสมาชิกซึ่งเป็นผู้รับบริการนั้น อันเป็นข้อมูลที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการนั้นไปให้ | เจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจตามกฎหมายอาจขอความช่วยเหลือจาก<br>ก. บุคคลใดที่เจ้าหน้าที่สงสัยว่าจะใช้คอมพิวเตอร์ในการกระทำผิดหรือเคยใช้กระทำผิด หรือ<br>ข. บุคคลใดก็ตามที่รับผิดชอบหรือเกี่ยวข้องกับการทำงานของคอมพิวเตอร์ดังกล่าว | เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง | ประเทศไทย ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง |

# บทที่ 4

# วิเคราะห์สภาพปัญหาและเปรียบเทียมมาตรการทางกฎหมายในปัจจุบันเกี่ยวกับการควบคุมอาชญากรรมทางคอมพิวเตอร์ใน สปป.ลาว

ความก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์และระบบคอมพิวเตอร์ที่ทันสมัย ได้ก่อให้เกิดประโยชน์อย่างมากมายต่อการพัฒนาทางด้านเศรษฐกิจ และสังคม แต่หากมีการนำเทคโนโลยีคอมพิวเตอร์ไปใช้ในทางที่ไม่เหมาะสม อาจก่อให้เกิดความเสียหายได้เช่นเดียวกัน ซึ่งการกระทำดังกล่าวนี้ถือว่าเป็นการใช้คอมพิวเตอร์เป็นเครื่องมือในการก่ออาชญากรรม จากการศึกษาปัญหาอาชญากรรมทางคอมพิวเตอร์ พบว่าปัญหาดังกล่าวเกิดขึ้นจากปัจจัยการขยายตัวของเส้นทางข้อมูลข่าวสารหรืออินเทอร์เน็ตที่เกิดขึ้นอย่างรวดเร็ว อินเทอร์เน็ตและเทคโนโลยีการติดต่อสื่อสารได้เข้ามามีบทบาทสำคัญต่อชีวิตประจำวันในทุกสังคมทั่วโลก ซึ่งช่วยอำนวยความสะดวกในการติดต่อสื่อสาร ส่งเสริมการพาณิชย์ พัฒนาการศึกษา และการรักษาสุขภาพ แต่เนื่องจากลักษณะของเทคโนโลยีที่มีความสลับซับซ้อน และมีลักษณะพิเศษคือการไม่เปิดเผย ทำให้ง่ายต่อการหลอกลวงและ/หรือฉ้อโกง การเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะลามกอนาจาร และปัญหาดังกล่าวได้ขยายวงกว้างมากขึ้นจนกลายเป็นปัญหาอาชญากรรมทางคอมพิวเตอร์

หากพิจารณาจากสถิติการใช้อุปกรณ์อิเล็กทรอนิกส์ และอินเทอร์เน็ตที่ผ่านการใช้บริการของเครือข่ายโทรคมนาคมที่ดำเนินการใน สปป.ลาว ระหว่างปี ค.ศ. 2009 ถึงปี ค.ศ. 2014 ตามตารางที่ 4.1 เห็นได้ว่าจำนวนผู้ลงทะเบียนใช้อินเทอร์เน็ตโดยเฉลี่ยมีอัตราเพิ่มขึ้น ซึ่งมีอัตราเสี่ยงในการเกิดปัญหาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์มากขึ้นเช่นกันโดยมีตัวเลขในการขยายตัวการใช้อินเทอร์เน็ตดังนี้

**ตารางที่ 4.1** สถิติการใช้บริการเครือข่ายโทรคมนาคม ตั้งแต่ พ.ศ. 2009 ถึง พ.ศ. 2014

| ลำดับ | บริษัท | ประเภท | ข้อมูลการใช้ | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 2552 | 2553 | 2554 | 2555 | 2556 | 2557 |
| 1 | VimpelCom Lao (Beeline) | โทรศัพท์ตั้งโต๊ะ | N/A | N/A | N/A | N/A | 3,339 | 3,251 |
| | | โทรศัพท์มือถือ | 239,753 | 292,659 | 414,973 | 317,648 | 325,340 | 316,911 |
| | | ผู้ลงทะเบียนใช้อินเทอร์เน็ต | 542 | 479 | 451 | 530 | 1,032 | 1,265 |
| 2 | Lao Telecom Co (LTC) | โทรศัพท์ตั้งโต๊ะ | 31,890 | 32,697 | 42,146 | 121,014 | 160,335 | 188,780 |
| | | โทรศัพท์มือถือ | 1,265,740 | 1,569,316 | 1,214,654 | 1,214,438 | 1,291,284 | 1,374,200 |
| | | ผู้ลงทะเบียนใช้อินเทอร์เน็ต | 4,702 | 9,203 | 14,953 | 56,970 | 76,696 | 82,037 |
| 3 | Enterprise of Telecom Lao (ETL) | โทรศัพท์ตั้งโต๊ะ | 17,993 | 17,719 | 18,340 | 18,027 | 40,507 | 40,304 |
| | | โทรศัพท์มือถือ | 956,799 | 1,262,872 | 1,138,495 | 471,583 | 788,934 | 864,878 |
| | | ผู้ลงทะเบียนใช้อินเทอร์เน็ต | 1,295 | 3,336 | 5,673 | 5,854 | 6,246 | 6,949 |
| 4 | Star Telecom Lao (Unitel) | โทรศัพท์ตั้งโต๊ะ | 3,112 | 3,258 | 3,324 | 3,342 | 477,463 | 469,377 |
| | | โทรศัพท์มือถือ | 726,102 | 2,613,703 | 1,796,676 | 1,496,322 | 2,075,837 | 1,817,087 |
| | | ผู้ลงทะเบียนใช้อินเทอร์เน็ต | N/A | 4,033 | 3,459 | 33,283 | 55,137 | 24,887 |

## 4.1 สภาพปัญหา และผลกระทบที่เกี่ยวกับการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์ใน สปป.ลาว

จากที่ได้กล่าวมาแล้วในบทที่ 2 เกี่ยวกับลักษณะของอาชญากรรมทางคอมพิวเตอร์จะเห็นได้ว่าในปัจจุบันเทคโนโลยีเป็นสิ่งที่มนุษย์พยายามพัฒนาอย่างไม่หยุดยั้ง เพื่อช่วยอำนวยความสะดวกให้แก่การใช้งานอย่างมากมาย ในการรับรู้ข้อมูลข่าวสาร การใช้งานระบบคอมพิวเตอร์และอินเทอร์เน็ตในชีวิตประจำวัน นับวันยิ่งเพิ่มมากขึ้น การจัดตั้งองค์กรและพัฒนาเศรษฐกิจ-สังคมทุกระดับ ทั้งภาครัฐ และเอกชน ต่างมีการใช้คอมพิวเตอร์และอินเทอร์เน็ตอย่างกว้างขวาง เพื่อตอบสนองการบริโภคของประชาชน ที่ต้องการความสะดวก รวดเร็ว และการบริการหลายรูปแบบ มีทั้งระบบอินเทอร์เน็ตใช้สาย (Land) และระบบอินเทอร์เน็ตไร้สาย (Wireless) ผ่านระบบโทรศัพท์เคลื่อนที่และระบบคอมพิวเตอร์อื่น ๆ แต่ในทางกลับกันในสังคมก็มีหลายปรากฏการณ์ที่ใช้เทคโนโลยีข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์ในทางที่ไม่ถูกต้อง เช่น การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นเพื่อขโมย ปลอมแปลง และทำลายข้อมูลคอมพิวเตอร์ การดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น การปล่อยไวรัสเพื่อรบกวนระบบปฏิบัติการของระบบคอมพิวเตอร์ การเผยแพร่ข้อมูลทางระบบคอมพิวเตอร์ และทางสื่อสังคมออนไลน์อื่น ๆ ที่สร้างความเสียหายให้แก่ภาครัฐ บุคคล นิติบุคคล องค์กร รวมทั้งสังคมและประเทศชาติ จึงนับว่าเป็นการกระทำผิดของอาชญากรทางคอมพิวเตอร์ที่ส่งผลเสียหายดังกล่าวได้

ความเจริญก้าวหน้า และการพัฒนาเทคโนโลยีสื่อสารโทรคมนาคมสมัยใหม่ที่นำเอาเทคโนโลยีระบบคอมพิวเตอร์ผนวกเข้ากับระบบสื่อสารโทรคมนาคม ประกอบกับการพัฒนาของเทคโนโลยีด้านโครงข่ายการสื่อสารข้อมูลความเร็วสูง เช่น โครงข่ายทางด่วนข้อมูล โครงข่ายอินเทอร์เน็ต ที่ใช้ข่ายระบบเชื่อมโยงผ่านสายเคเบิลใยแก้วนำแสง และระบบสื่อสารผ่านดาวเทียมที่ทันสมัย ทำให้สามารถรับส่งข่าวสารจำนวนมหาศาลในรูปของเสียง ข้อมูล ภาพนิ่งและภาพเคลื่อนไหว ให้สามารถรองรับบริการหลาย ๆ บริการได้พร้อมกัน ซึ่งในการบริการดังกล่าวอาจแฝงด้วยรูปแบบของการกระทำผิดอื่น ๆ ตามมาด้วยเช่นกัน เช่น

กรณีการตัดต่อรูปภาพเครื่องบินโดยสารแบบเอทีอาร์ 72 ของสายการบินลาวแอร์ไลน์ (Lao Airlines) เที่ยวบินที่ QV 301 ที่ตกกลางลำน้ำโขงในวันที่ 16 ตุลาคม ค.ศ. 2013 ซึ่งเครื่องบินดังกล่าวได้เดินทางออกจากสนามบินนานาชาติวัดไต นครหลวงเวียงจันทน์ สปป.ลาว ในเวลา 14.45 น. มุ่งหน้าสู่สนามบินเมืองปากเซ แขวงจำปาสัก ทางตอนใต้ของ สปป.ลาว เหตุการณ์ครั้งนี้เครื่องบินลำดังกล่าวได้ตกลงกลางลำน้ำโขงและปีกอีกข้างหนึ่งของเครื่องบินจมอยู่ใต้ลำน้ำโขง ทำให้นักบินและลูกเรือทั้งหมดเสียชีวิต ขณะเดียวกันก็มีคนกลุ่มหนึ่งตัดต่อรูปภาพเครื่องบินที่

ตกในต่างประเทศแล้วเขียนคำบรรยายว่าเป็นรูปเครื่องบินที่ตกในวันที่ 16 ตุลาคม ค.ศ. 2013 แล้วนำไปโพสลงทางเฟซบุ๊ค (Face book) และมีการแชร์ต่ออย่างรวดเร็วว่าเครื่องบินดังกล่าวมีการลอยตัวอยู่เหนือลำน้ำโขง ไม่ได้มีการจมลงในใต้ลำน้ำโขงแต่อย่างใด จากเหตุการณ์ดังกล่าวทำให้สังคมมีความเข้าใจผิดคาดเคลื่อนไปจากความเป็นจริง และทำให้สังคมโจมตีการปฏิบัติหน้าที่ของเจ้าพนักงานที่ทำการกู้ซากเครื่องบินขึ้นจากลำน้ำโขงว่านักบินและลูกเรือทั้งหมดไม่ควรจบชีวิตลง ถ้าหากพนักงานเจ้าหน้าที่ทำการกู้เอาทุกคนในเครื่องบินออกมาได้โดยเร็ว ทั้งที่ความเป็นจริงแล้วปีกด้านหนึ่งของเครื่องบินนั้นจมอยู่ใต้แม่น้ำโขงและแทบไม่มีความเป็นไปได้เลยที่ทุกคนในเครื่องบินจะมีโอกาสรอดชีวิตจากเหตุการณ์ดังกล่าว

อีกกรณี คือ ในต้นเดือนมิถุนายน ค.ศ. 2014 มีธนาคารแห่งหนึ่งใน สปป.ลาว (ไม่สารถเปิดเผยชื่อได้) ถูกกลุ่มคนไม่หวังดีใช้ระบบคอมพิวเตอร์ส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ไปยังลูกค้าของธนาคาร เพื่อหวังหลอกลวงเอาข้อมูลบัญชีของลูกค้า ซึ่งเนื้อหาของจดหมายแอบอ้างว่าส่งในนามของธนาคาร และมีการตรวจพบว่ามีการเคลื่อนไหวที่ผิดปกติในบัญชีของลูกค้า พร้อมกับแนะนำให้ลูกค้าปฏิบัติตามคำแนะนำหรือปิดบัญชีออนไลน์ เพื่อเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการเคลื่อนไหวบัญชีที่ผิดปกตินั้น ให้ลูกค้ายืนยันความถูกต้องอย่างละเอียดของข้อมูลเกี่ยวกับบัญชีของลูกค้าภายใน 24 ชั่วโมง และเพื่อหลีกเลี่ยงการเกิดข้อผิดพลาดระหว่างการปรับปรุงระบบความปลอดภัยให้ลูกค้าเชื่อมต่อไปยัง Link พร้อมทั้งกรอกข้อมูลทางบัญชีของลูกค้า ซึ่ง Link ดังกล่าวเป็นเว็บไซต์ปลอม กล่าวคือเว็บไซต์ดังกล่าวได้จัดทำขึ้นมาคล้ายคลึงกับเว็บไซต์ของธนาคาร แต่จะปรับเปลี่ยนบางตัวอักษร จากเหตุการณ์ดังกล่าวทำให้ลูกค้าบางรายหลงเชื่อ และเข้าใจผิดว่าทางธนาคารเป็นผู้ส่งมาจึงได้กรอกข้อมูลไป อย่างเช่นกรณีของผู้ใช้รายหนึ่งที่โพสลงในสื่อสังคมออนไลน์ ในวันที่ 14 สิงหาคม ค.ศ. 2014 ที่ถูกเจาะข้อมูลในบัญชี (Hack) ทำให้เงินในบัญชีหายไปจำนวน 99.99 USD จึงได้โพสลงในสื่อสังคมออนไลน์เพื่อเป็นการแจ้งเตือนเพื่อน ๆ เกี่ยวกับเหตุการณ์ที่เกิดขึ้น จึงได้ติดต่อไปยังธนาคาร และธนาคารได้ให้ความร่วมมือโดยการอธิบายให้เข้าใจว่าธนาคารไม่มีนโยบายแจ้งให้ลูกค้ายืนยันรายระเอียดข้อมูลทางบัญชีผ่านทางเว็บไซต์หรืออินเทอร์เน็ตแต่อย่างใด นอกจากนั้นธนาคารยังได้ให้ความร่วมมือในการติดตามนำเงินที่สูญหายไปคืนกลับมา อย่างไรก็ตามหน่วยงานที่เกี่ยวข้องก็คือ ศูนย์อินเทอร์เน็ตแห่งชาติ[104] ก็ได้ออกแถลงการณ์เพื่อให้ความรู้แก่สังคมเกี่ยวกับประเด็นดังกล่าวว่า ในกรณีที่ธนาคารพบเจอนั้นเป็นกรณีที่ทางด้านวิชาการเรียกว่า Phishing Site เป็นการหลอกล่อให้เหยื่อเปิดเผยข้อมูลส่วนตัว เช่น

---

[104] ศูนย์สกัดกั้นและแก้ไขเหตุฉุกเฉินทางคอมพิวเตอร์, *แจ้งเตือนภัยทางอินเทอร์เน็ต*, สืบค้นเมื่อ 23 พฤศจิกายน2558, จาก https://www.laocert.gov.la/News-Categories

ชื่อผู้ใช้ รหัสผ่านหรือข้อมูลส่วนบุคคลอื่น ๆ รหัสบัตรเครดิต ข้อมูลบัญชีธนาคาร เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือนำไปสร้างความเสียหายในด้านอื่น ๆ เป็นต้น ด้านการเงินด้วยรูปแบบของอีเมล (Email) Popup SMS และเว็บไซต์ (website) ต่าง ๆ[105] ซึ่งถือว่าเป็นภัยคุกคามที่สร้างความเสียหายได้อย่างมากมาย แต่สามารถระวังและป้องกันได้ถ้าหากผู้ที่ใช้งานบนอินเทอร์เน็ตมีการพิจารณาอย่างถ้วนถี่ในการใช้งานอินเทอร์เน็ต

กรณีสร้างความหวาดกลัวและตื่นตระหนกให้แก่สังคม โดยการอาศัยเหตุการณ์ขโมยเด็กที่เกิดขึ้นจริงในวันที่ 13 พฤษภาคม ค.ศ. 2014 ณ บ้านคอนลาด อำเภอเมือง จังหวัดสารวัน ที่มีการขโมยเด็กไปจากระหว่างทางกลับบ้านจากโรงเรียน แต่พอไปถึงระยะหนึ่งของเส้นทางก็ได้มีการปล่อยตัวเด็กกลับไปหาครอบครัว แต่ต่อมามีกลุ่มคนที่ไม่หวังดีสร้างข้อมูลบิดเบือนจากความเป็นจริง โดยมีการเขียนลงในสื่อสังคมออนไลน์ว่า สังคมลาวขาดความสงบสุขเพราะมีกลุ่มคนขโมยเด็กไปฆ่าและตัดต่อรูปภาพเกี่ยวกับการชำแหละอวัยวะส่วนต่าง ๆ ของเด็กโพสลงในเฟสบุ๊กและแชร์ต่อกันไป[106] ทำให้ข่าวดังกล่าวขยายออกไปอย่างรวดเร็ว ส่งผลให้สังคมแตกตื่นและหวาดกลัว บางครอบครัวไม่ยอมให้ลูกหลานไปโรงเรียนเพราะกลัวแก๊งขโมยเด็ก จากสถานการณ์ดังกล่าวทำให้บางท้องถิ่นขาดความสงบอย่างมาก

กรณีที่มีแหล่งข่าวจากหนังสือพิมพ์ต่างประเทศ ซึ่งมีการพาดพิงถึงกลุ่มบริษัท ดาวเรือง ผ่านสื่อออนไลน์โดยพาดหัวข้อข่าวว่า กัมพูชา ยึดกัญชา 1,5 ตัน และระบุเนื้อหาสั้น ๆ โดยอ้างว่าตำรวจประเทศกัมพูชาได้ทำการตรวจพบกัญชาจำนวน 1,5 ตันที่บรรจุในถุงกาแฟดาว[107] มาจาก สปป.ลาว ไปยังประเทศที่สาม ซึ่งต่อมาก็มีการนำไปพูดถึงและขยายเป็นวงกว้างในสื่อสังคมออนไลน์ ต่อกับประเด็นดังกล่าวจึงทำให้กลุ่มบริษัท ดาวเรือง ซึ่งทำธุรกิจหลักในการส่งออกกาแฟทั้งภายในและต่างประเทศได้รับผลกระทบทางด้านธุรกิจค่อนข้างมาก เช่น ขาดความเชื่อมั่นจากผู้บริโภค ขาดความน่าเชื่อถือในธุรกิจกาแฟ เป็นต้น นอกจากนี้ ยังมีเว็บไซต์หนึ่งที่ได้อ้างถึงกลุ่มบริษัท ดาวเรือง ว่าได้มีการลงทุนก่อสร้างร้านค้าปลอดภาษี (duty free) อยู่ที่นครหลวงเวียงจันทน์ (ด่านมิตรภาพไทย-ลาว แห่งที่ 1) ในวงเงิน 10,000 ล้านบาท หรือเท่ากับ 295 ล้านดอลลาร์สหรัฐ เกี่ยวกับข่าวดังกล่าวนั้นไม่มี

---

[105] ศูนย์อินเทอร์เน็ตแห่งชาติ, เรื่องปัญหาจดหมายเอเล็กทรอนิกส์ (E-mail), *หนังสือ*, เลขที่ 646/สอช, (17 มิถุนายน 2014).

[106] ข่าวลือ ฆ่าเด็กน้อยเอาอวัยวะ, *หนังสือพิมพ์เวียงจันทน์ใหม่*, (5 มิถุนายน 2014), สืบค้นเมื่อ 23 พฤศจิกายน 2558, จาก http://www.vientianemai.net/teen/khao/1/11950

[107] กาแฟดาว เป็นชื่อการค้ากาแฟของกลุ่มบริษัท ดาวเรือง ใน สปป.ลาว.

มูลความจริง โดยกลุ่มบริษัท ดาวเรือง ไม่ได้มีโครงการดังกล่าวเสนอต่อรัฐบาล สปป.ลาว[108] ดังนั้น แหล่งข่าวดังกล่าวจึงเป็นเพียงการใช้สื่อผ่านสังคมออนไลน์ เป็นแหล่งข่าวที่มุ่งหวังทำลายชื่อเสียงและความเชื่อมั่นในการดำเนินธุรกิจของกลุ่มบริษัท ดาวเรือง เท่านั้น

นอกจากนี้ยังมีกรณีการสร้างเพจปลอมในเฟซบุ๊ค ขายสินค้าราคาถูก โดยการล่อลวงเหยื่อให้เข้าใจผิดและหลงเชื่อโอนเงินค่ามัดจำการสั่งซื้อสินค้าก่อนล่วงหน้า หลังจากที่เหยื่อหลงเชื่อโอนเงินไปให้เสร็จแล้วเจ้าของเพจปลอมก็จะบล๊อกเฟซเหยื่อ บางครั้งก็มีการสร้างเพจใหม่ขึ้นแล้วใช้ชื่อรูปภาพและข้อมูลของเหยื่อเพื่อไปหลอกลวงคนคนอื่น ๆ ต่อไป

จากเหตุการณ์ต่าง ๆ ดังกล่าว จะเห็นได้ว่ามีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำผิด และมีระบบอินเทอร์เน็ตเป็นตัวอย่างในการเผยแพร่ข้อมูลข่าวสารต่าง ๆ ให้สังคมได้รับรู้อย่างรวดเร็ว ไม่ว่าข่าวสารดังกล่าวจะเป็นข่าวดีหรือข่าวที่มุ่งหวังทำลายความสงบสุขของสังคมหรือผู้หนึ่งผู้ใดก็ตาม ก็ล้วนแต่เป็นการกระทำผิดผ่านระบบคอมพิวเตอร์เช่นกัน

ซึ่งเป็นปัญหาการก่ออาชญากรรมทางคอมพิวเตอร์ และสามารถแบ่งผลกระทบของการกระทำผิดด้านอาชญากรรมทางคอมพิวเตอร์ได้ 3 ด้าน ดังนี้

1. ผลกระทบต่อความมั่นคง
2. ผลกระทบทางด้านเศรษฐกิจ
3. ผลกระทบทางด้านสังคม

ดังนั้น ในหัวข้อนี้จะได้วิเคราะห์ถึงปัญหาของการกระทำผิดทางคอมพิวเตอร์ที่ก่อให้เกิดความเสียหาย โดยสรุปได้ดังนี้

**4.1.1 ผลกระทบต่อความมั่นคง**

ปัจจุบัน สปป.ลาว ได้มีการพัฒนา และได้มีการใช้เครื่องมือที่ทันสมัยในการบริหารจัดการสาธารณูปโภคของประเทศเป็นจำนวนมาก ไม่ว่าจะเป็นระบบไฟจราจร ระบบไฟฟ้าภาคครัวเรือนและธุรกิจ เป็นต้น ซึ่งสถานการณ์ปัญหาและภัยคุกคามความมั่นคงของประเทศ เป็นลักษณะผสมผสานระหว่างปัญหาและภัยคุกคามความมั่นคงรูปแบบเก่ากับปัญหาและภัยคุกคามความมั่นคงรูปแบบใหม่ที่ใช้เทคโนโลยีคอมพิวเตอร์ที่มีความสลับซับซ้อน และมีความหลากหลายเพิ่มขึ้นเป็นลำดับ รวมทั้งการเปลี่ยนแปลงอย่างต่อเนื่อง ซึ่งส่งผลกระทบต่อความมั่นคงของประชาชนและของประเทศโดยรวม ในระยะที่ผ่านมาเป็นการดำเนินงานแก้ไขปัญหาและภัยความมั่นคงรูปแบบเก่าที่เป็นเรื่องของการทหาร ขณะที่ปัญหาความมั่นคงรูปแบบใหม่ที่เป็นเรื่องความมั่นคงด้านการบริหาร

---

[108] ดาวเรืองยืนยันไม่มีส่วนเกี่ยวข้องกับการขนส่งสิ่งผิดกฎหมาย, *หนังสือพิมพ์เวียงจันทน์ใหม่*, (15 กันยายน 2015), สืบค้นเมื่อ 22 พฤศจิกายน 2558, จาก http://www.vientianemai.net/teen/khao/1/14787 ดาวเรือง

จัดการเกี่ยวกับบริการสาธารณะทั้งหลาย เช่น ระบบไฟฟ้า ระบบน้ำประปา ระบบขนส่ง เป็นต้น ซึ่งก่อผลกระทบต่อการเสริมสร้างความมั่นคงของประเทศ โดยการกระทำผิดที่ส่งผลกระทบด้านความมั่นคงสรุปได้ ดังนี้

4.1.1.1 การเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์เพื่อการสอดแนมหรือการล่วงรู้ข้อมูลทางการทหาร ความลับทางราชการ ข้อมูลเกี่ยวกับการจ่ายกระแสไฟฟ้าน้ำประปา ซึ่งเป็นการเข้าไปในระบบคอมพิวเตอร์ที่มีมาตรการป้องกันไว้โดยเฉพาะ เพื่อดำเนินการอย่างใด ๆ อันก่อให้เกิดความเสียหายต่อการบริการดังกล่าว

4.1.1.2 การแอบดักรับข้อมูล เป็นการดักรับข้อมูลทางคอมพิวเตอร์ เป็นการใช้วิธีการทางอิเล็กทรอนิกส์เพื่อกระทำการให้ได้มาซึ่งเนื้อหาของข้อมูล ด้วยการแอบบันทึกข้อมูลสื่อสารถึงกันซึ่งเป็นข้อมูลที่ไม่ได้มีไว้เพื่อประโยชน์สาธารณะ เช่น ความลับทางราชการ เป็นต้น

4.1.1.3 การตั้งเวลาให้โปรแกรมทำลายข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อรบกวนการทำงานของระบบสาธารณูปโภค โดยการทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิมหรือหยุดทำงาน (Denial of Service) อันส่งผลกระทบต่อความมั่นคงของรัฐในการจัดการระบบบริการสาธารณะทั้งหลายได้

ความเสียหายที่เกิดขึ้นจากอาชญากรรมทางคอมพิวเตอร์นั้นคงจะมิใช้มีผลกระทบเพียงแต่ความมั่นคงของบุคคลใดบุคคลหนึ่งเท่านั้น แต่ยังมีผลกระทบไปถึงเรื่องความมั่นคงของประเทศชาติเป็นการส่วนรวม ทั้งความมั่นคงภายในประเทศและระหว่างประเทศ โดยเฉพาะในส่วนที่เกี่ยวข้องกับข่าวกรองหรือการจารกรรมข้อมูลต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงของประเทศ ซึ่งในปัจจุบันได้มีการเปลี่ยนแปลงรูปแบบจากเดิม เช่น ความมั่นคงของรัฐนั้นมิใช่จะอยู่ในวงทหารเพียงเท่านั้น บุคคลธรรมดาก็สามารถป้องกันหรือทำลายความมั่นคงของประเทศได้ การป้องกันประเทศอาจไม่ได้อยู่ในพรมแดนอีกต่อไป แต่อยู่ที่ทำอย่างไรจึงจะไม่ให้มีการคุกคามหรือทำลายโครงสร้างพื้นฐานสารสนเทศด้านการบริการสาธารณะที่รัฐบาลเป็นผู้ดูแล และการทำจารกรรมในสมัยใหม่นี้มักจะใช้วิธีการทางเทคโนโลยีที่มีความสลับซับซ้อนทางด้านเทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์ เข้ามาเป็นเครื่องมือช่วยในการกระทำเพื่อให้ได้ข้อมูลข่าวสารที่รวดเร็ว และสืบสวนหาผู้กระทำความผิดได้ยากขึ้น

โครงสร้างพื้นฐานด้านสารสนเทศ ความผิดต่าง ๆ ล้วนแต่สามารถเกิดขึ้นได้ตลอด เช่น การจารกรรม การก่อการร้าย การค้ายาเสพติด การแบ่งแยกดินแดน การโจมตีระบบสาธารณูปโภคพื้นฐานของประเทศที่มีระบบคอมพิวเตอร์ควบคุม เช่น ระบบจราจรหรือระบบไฟฟ้า เป็นต้น ฉะนั้น รัฐจึงต้องจัดให้มีมาตรการป้องกันอย่างเข็มงวด เพื่อป้องกันมิให้เกิดการกระทำผิดอีก

ดังนั้น จากการกระทำของอาชญากรรมทางคอมพิวเตอร์ในการเข้าไปรบกวนระบบคอมพิวเตอร์ การดักรับข้อมูล และล่วงรู้ความลับ เป็นต้น ซึ่งเป็นการกระทำผิดทางคอมพิวเตอร์เพื่อสร้างความเสียหายให้แก่ระบบโครงสร้างพื้นฐานของประเทศ ซึ่งจะเห็นได้ว่า ความสัมพันธ์ระหว่างอาชญากรรมทางคอมพิวเตอร์ ความมั่นคงของประเทศ และโครงสร้างพื้นฐานสารสนเทศของชาติ เป็นเรื่องที่ไม่สามารถแยกจากกันได้อย่างเด็ดขาด การโจมตีโครงสร้างพื้นฐานสารสนเทศสามารถทำได้ด้วยความเร็วของการเคลื่อนที่เกือบเท่าความเร็วแสงเหนือกว่าการเคลื่อนทัพทางบกหรือทางอากาศ[109] หลายเท่านัก ด้วยเหตุนี้ภาครัฐจึงต้องจัดการควบคุมปัญหาอาชญากรรมทางคอมพิวเตอร์เพื่อไม่ต้องการให้ประเทศชาติเกิดความวุ่นวาย และความเสียหายจากการใช้เทคโนโลยีคอมพิวเตอร์และสารสนเทศดังกล่าว

**4.1.2 ผลกระทบทางด้านเศรษฐกิจ**

เทคโนโลยีทางคอมพิวเตอร์ได้กลายเป็นส่วนสำคัญที่ใช้เป็นเครื่องมือในการพัฒนาองค์กรโดยการใช้คอมพิวเตอร์ และระบบคอมพิวเตอร์มาใช้เป็นกลไกในการขับเคลื่อนพัฒนากิจการ และเป็นกลไกสำคัญของการประกอบกิจการการค้า การลงทุน ซึ่งความก้าวหน้าทางเทคโนโลยีสารสนเทศนี้ และความสำคัญของการประกอบธุรกิจที่มีคอมพิวเตอร์เป็นเครื่องมือสำคัญในการดำเนินการ ทำให้อาชญากรที่ประสงค์ร้ายใช้เทคโนโลยีคอมพิวเตอร์ไปในทางที่มิชอบที่ส่งผลเสียหรือส่งผลกระทบต่อเศรษฐกิจโดยภาพรวมได้ ซึ่งการกระทำที่ส่งผลกระทบต่อเศรษฐกิจสามารถสรุปได้ ดังนี้

4.1.2.1 การล่วงรู้ข้อมูลความลับทางการค้าหรือทำให้ข้อมูลที่จัดเก็บอยู่ในฐานข้อมูลถูกดัดแปลงแก้ไขหรือกระทำการอย่างใดอย่างหนึ่ง อันส่งผลกระทบต่อข้อมูลทางธุรกิจ เช่น การเข้าถึงข้อมูลส่วนตัวของลูกค้า เช่น ข้อมูลบัตรเครดิต หมายเลขบัญชีธนาคาร เป็นต้น

4.1.2.2 การทำให้ระบบคอมพิวเตอร์ระงับ ชะลอหรือทำงานช้าลง เช่น การป้อนโปรแกรมที่ทำให้ระบบคอมพิวเตอร์ปฏิเสธการทำงานหรือทำให้ระบบคอมพิวเตอร์ทำงานช้าลงโดยการป้อนไวรัสคอมพิวเตอร์เพื่อให้เกิดผลชะลอการทำงานของระบบ หรือทำให้ระบบการทำงานขององค์กรธุรกิจหยุดการทำงานลง

4.1.2.3 การแอบดักรับข้อมูลทางคอมพิวเตอร์ที่อยู่ในระหว่างการส่ง เช่น ข้อมูลติดต่อทางจดหมายอิเล็กทรอนิกส์ คำสั่งซื้อขายออนไลน์ เป็นต้น

---

[109] Sasiwimontan, *หน่วยที่ 10 กฎหมายและความปลอดภัยบนอินเตอร์เน็ต*, (24 พฤศจิกายน 2554), สืบค้นเมื่อ 5 มีนาคม 2558, จาก http://sasiwimontan.blogspot.com/2011/11/10.html

เนื่องจากข้อมูลสารสนเทศบางครั้งมีคุณค่ามหาศาลสำหรับผู้ที่ได้รับข้อมูลข่าวสารนั้นก่อนคนอื่น โดยเฉพาะอย่างยิ่งในธุรกิจประเภทเดียวกันที่มีการแข่งขันสูง หากมีบุคคลอื่นได้ลงทุนลงแรงแสวงหาข้อมูลข่าวสารนั้นมา แต่มีบุคคลอื่นลักลอบเอาข้อมูลนั้นไปใช้ประโยชน์ทำให้กระทบต่อผลประโยชน์และเกิดความไม่เป็นธรรมต่อผู้แสวงหาข้อมูลคนแรก ด้วยเหตุนี้ในหลายประเทศได้พัฒนากฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อให้ความเป็นธรรมแก่ผู้ลงทุนและแสวงหาข้อมูลข่าวสาร เช่น กฎหมายลิขสิทธิ์ กฎหมายสิทธิบัตร กฎหมายความลับทางการค้า และกฎหมายเกี่ยวกับการถ่ายทอดเทคโนโลยี เป็นต้น

เมื่อความก้าวหน้าทางด้านเทคโนโลยีคอมพิวเตอร์ได้เข้ามามีบทบาทในการดำเนินการทางด้านธุรกิจของ สปป.ลาว เพิ่มมากขึ้น ภัยที่ตามมาก็คือการก่ออาชญากรรมทางคอมพิวเตอร์อาจมีการขยายตัวตามการเจริญเติบโตนั้น และส่งผลกระทบในการดำเนินธุรกิจ กล่าวคือการใช้คอมพิวเตอร์และระบบคอมพิวเตอร์ที่ทันสมัยช่วยในการติดต่อสื่อสาร การส่งข้อมูล การเก็บรักษาข้อมูลทางการค้า และอื่น ๆ เนื่องจากการค้าการลงทุนในปัจจุบันต้องอาศัยโทรคมนาคมและเทคโนโลยีสารสนเทศเป็นองค์ประกอบสำคัญสำหรับการประกอบธุรกิจและธุรกรรมต่าง ๆ แต่ลักษณะของความสลับซับซ้อนของระบบคอมพิวเตอร์ และช่องว่างทางกฎหมายทำให้อาชญากรสามารถล่วงรู้หรือจารกรรมข้อมูลก่อให้เกิดผลเสียหายในทางการค้าได้

ในด้านเศรษฐกิจนั้นปริมารการใช้เทคโนโลยีคอมพิวเตอร์ในการทำธุรกิจการค้า การลงทุน การติดต่อสื่อสาร และอื่น ๆ เป็นสิ่งที่มีการใช้งานอย่างแพร่หลาย เมื่อมีการล่วงรู้ความลับทางการค้า หรือการเข้าไปเพื่อกระทำการอย่างใดอย่างหนึ่งที่ส่งผลให้ระบบคอมพิวเตอร์ทำงานในการประมวลผลผิดพลาดไป บิดเบือนไม่ตรงกับความเป็นจริงหรือการกระทำเกี่ยวกับตัวเลขบัญชีในธนาคาร ซึ่งทำให้ธุรกิจเสียหายหรืออาจเกิดการกำหนดนโยบายทางด้านเศรษฐกิจที่ผิดพลาดได้ จึงอาจกล่าวได้ว่าการใช้คอมพิวเตอร์ และเทคโนโลยีสารสนเทศที่มิชอบ ย่อมทำให้เศรษฐกิจโดยภาพรวมของประเทศเสียหายได้

โดยสรุปแล้วการกระทำของอาชญากรรมทางคอมพิวเตอร์เป็นอาชญากรรมที่สร้างความเสียหายอย่างกว้างขวาง โดยเฉพาะการเข้าถึงข้อมูล การทำให้ระบบคอมพิวเตอร์ทำงานไม่ปกติที่อาจก่อให้เกิดความเสียหายที่เป็นตัวเงินที่วัดผลเสียหายได้ และความเสียหายที่ไม่สามารถวัดผลเป็นตัวเงินได้ ซึ่งมีมูลค่ามหาศาล และมีผู้เสียหายจำนวนมาก ทำให้ระบบเศรษฐกิจต้องสั่นคลอนได้ เช่น ธุรกิจธนาคารที่มีการยักยอกตัวเลขในบัญชี การกระทำให้ระบบคอมพิวเตอร์ของบริษัทถูกชะลอ เป็นต้น ปัจจุบัน สปป.ลาว ขาดบทบัญญัติกฎหมายในส่วนที่เกี่ยวข้องกับการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การจารกรรมข้อมูล เป็นต้น กล่าวคือการกระทำดังกล่าวอาจสร้างความหายนะต่อธุรกิจและหน่วยงานต่าง ๆ ที่ใช้เทคโนโลยีคอมพิวเตอร์ ซึ่งอาจส่งผลต่อนักลงทุนที่จะเข้ามาลงทุน

ใน สปป.ลาว เกิดความไม่มั่นใจในมาตรการทางกฎหมายในการป้องกันอาชญากรรมทางคอมพิวเตอร์หรืออาจกังวลต่อผลร้ายที่เกิดจากการกระทำของอาชญากรรมทางคอมพิวเตอร์อันเนื่องมาจาก สปป.ลาว ยังมีช่องว่างของกฎหมายที่ใช้บังคับกับอาชญากรรมทางคอมพิวเตอร์รูปแบบต่าง ๆ และกฎหมายที่มีอยู่ในปัจจุบันก็มีเพียงบทบัญญัติอย่างกว้าง จึงไม่เพียงพอที่จะนำมาใช้บังคับ และลงโทษผู้กระทำผิดได้อย่างจริงจัง

**4.1.3 ผลกระทบทางสังคม**

ในยุคของสังคมข้อมูลข่าวสาร (Information Society) ที่ทันสมัย และการติดต่อสื่อสารที่มีความรวดเร็วในการเผยแพร่ข่าวสาร นอกจากจะมาในรูปแบบของการโฆษณาทางโทรทัศน์ และวิทยุแล้วการกระจ่ายข้อมูลข่าวสาร (Data Broadcast) ทางคอมพิวเตอร์นับวันจะมีความสำคัญมากขึ้น ซึ่งเนื้อหาของข่าวสารบางประเภทจะมีลักษณะโน้มน้าวจิตใจของผู้เสพข่าวสารให้หลงเชื่อตามข้อมูลที่ถูกกระจายออกสู่ผู้เสพข่าวสาร ข้อมูลดังกล่าวอาจถูกจัดทำขึ้นเพื่อผลประโยชน์ในกิจการหรือธุรกิจของผู้ที่จัดส่งข้อมูล ข้อมูลบางประเภทซึ่งเป็นสิ่งที่ยอมรับได้ในประเทศหนึ่งอาจเป็นสิ่งที่ทำลายวัฒนธรรม สังคม ความเชื่อถือในอีกประเทศหนึ่ง ข้อมูลบางประเภทก็จะเป็นในลักษณะเผยแพร่ลัทธิความเชื่อถือ เป็นต้น เช่นนี้สังคมจึงมีลักษณะอันหลากหลายที่อยู่ท่ามกลางเทคโนโลยีสารสนเทศต่าง ๆ ที่ทำให้เกิดความเคลื่อนไหวได้อย่างง่ายดาย และหากมีการใช้เทคโนโลยีคอมพิวเตอร์ในทางที่ไม่ชอบย่อมเป็นการส่งเสริม และเกื้อหนุนให้เกิดความสับสนวุ่นวายมากยิ่งขึ้น อันส่งผลกระทบต่อวิถีการดำรงชีวิตของประชาชนได้ นอกจากการใช้เครื่องมือที่ทันสมัยอันก่อให้เกิดประโยชน์สูงสุดแล้วยังมีผลกระทบที่ตามมากับกลุ่มคนที่ไม่หวังดี ซึ่งได้กระทำการอันเป็นการรบกวนการใช้งานหรือก่อให้เกิดผลเสียหายแก่การใช้งานเทคโนโลยี ในการประกอบการธุรกิจหรือการล่อลวงประชาชนให้หลงเชื่อเกี่ยวกับข้อมูล ถูกกระทำการอันเป็นการล่วงสิทธิและเสรีภาพของประชาชนในการใช้งานเครื่องมือและระบบคอมพิวเตอร์ของตน ดังนี้

4.1.3.1 การเผยแพร่เนื้อหาที่มีการชวนเชื่อทางศาสนา ค่านิยม แนวคิด และการหมิ่นประมาท

4.1.3.2 การแก้ข้อมูลข่าวสารเผยแพร่ข้อมูลข่าวสารที่ไม่ชอบด้วยกฎหมายในแง่มุมต่าง ๆ เช่น การเผยแพร่ภาพลามกอนาจารเด็ก การพนันออนไลน์ การเผยแพร่ข้อมูลที่มีเนื้อหาแอบแฝงแนวคิกก้าวร้าว รุนแรงหรือแนวคิดในการดูหมิ่นเชื้อชาติ โดยอาศัยบริการทางด่วนข้อมูลหรืออินเทอร์เน็ต

4.1.3.3 การเข้าถึงข้อมูลส่วนตัวโดยไม่ได้รับอนุญาตเพื่อทำการแก้ไข เปลี่ยนแปลงก่อให้เกิดความเสียหาย และติดต่อสื่อสารกันในระบบปิดบังตัวตนหรือหลอกให้หลงเชื่อ เกิดการล่อลวงออกไปเพื่อประสงค์ร้ายทางเพศ เป็นต้น

นอกจากความเสียหายที่เกิดขึ้นในกรณีเกิดการเข้าใจผิดหรือการกลั่นแกล้งจากผู้ไม่หวังดี โดยมีการเข้าไปเจาะระบบข้อมูลของผู้อื่นแล้วนำไปเผยแพร่หรือตัดต่อดัดแปลงข้อมูล รูปภาพหรือสถานการณ์ต่าง ๆ ของผู้อื่นให้ไปในทิศทางที่ไม่เหมาะสม รวมทั้งอาจก่อให้เกิดความเสียหายแก่การดำเนินธุรกิจ ทำให้เสียชื่อเสียงทางธุรกิจ และอาจทำให้เข้าใจผิดต่อจารีตประเพณีอันดีงามของประชาชนด้วย

ทั้งนี้ สามารถสรุปได้ว่า จากการกระทำความผิดทางคอมพิวเตอร์ที่ส่งผลกระทบไม่ว่าทางตรงหรือทางอ้อมต่อประชาชนนั้น ทำให้ประชาชนและสังคมกำลังเผชิญกับปัญหาการใช้เทคโนโลยีที่ทันสมัยไปในทางไม่ชอบ โดยการเผยแพร่เนื้อหาอันไม่เหมาะสม ไม่ว่าจะเป็นสื่อลามกอนาจาร ข้อความหมิ่นประมาท การชักจูงล่อลวง หลอกลวงเด็ก และเยาวชนไปในทางที่เสียหายหรือพฤติกรรมอื่นอันเป็นภัยต่อสังคมที่เกิดจากงานใช้งานระบบคอมพิวเตอร์ไปในทางที่ไม่ชอบธรรม ซึ่งทำให้ประชาชนหลงเชื่อข้อมูลที่มีการดัดแปลงแก้ไข ก่อให้เกิดความเสียหายในการเข้าใจผิดหรือถูกกลั่นแกล้งโดยผู้ไม่หวังดีที่กระทำต่อบุคคลอื่นได้รับความเสียหายและเสื่อมเสียชื่อเสียงหรือต้องการทำให้การดำเนินธุรกิจของประชาชนล่าช้า และอาจทำให้การติดต่อสื่อสารหรือการทำธุรกิจของประชาชนได้รับความเสียหายจากการกระทำดังกล่าว

## 4.2 มาตรการทางกฎหมายในการจัดการปัญหาอาชญากรรมทางคอมพิวเตอร์ในปัจจุบันของ สปป.ลาว

ปัญหาข้อกฎหมายในปัจจุบันเกี่ยวกับการกำหนดรูปแบบของการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์ใน สปป.ลาว ยังไม่มีการกำหนดที่ชัดเจน ตามหลักของกฎหมายอาญาที่ระบุว่า “ไม่มีความผิด ไม่มีโทษโดยไม่มีกฎหมาย (*Nullum crime, nulla poena sine lege*)” บุคคลจะรับผิดทางอาญาได้ก็ต่อเมื่อได้กระทำการอันกฎหมายที่ใช้ในขณะกระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่ผู้กระทำความผิดนั้นต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย[110] แต่ในปัจจุบันสังคมได้มีการพึ่งพาอาศัยเทคโนโลยีคอมพิวเตอร์ที่ทันสมัยในการติดต่อสื่อสาร และการทำงานมากยิ่งขึ้น ซึ่งข้อมูลข่าวสารและระบบคอมพิวเตอร์นั้นเป็นวัตถุที่ไม่มีรูปร่าง ด้วยเหตุนั้นการก่ออาชญากรรมทางคอมพิวเตอร์นั้นเป็นสิ่งที่เกี่ยวข้องกับการก่ออาชญากรรมที่มุ่งกระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่เป็นคลื่นแม่เหล็กไฟฟ้าเป็นสิ่งที่ไม่สามารถจับต้องได้ และมองไม่เห็น แต่ในขณะเดียวกันบทบัญญัติกฎหมายอาญา

---

[110] บุญเพราะ แสงเทียน, *กฎหมายอาญา 1 (ภาคบทบัญญัติทั่วไป) แนวประยุกต์*, 18.

ในปัจจุบันมุ่งคุ้มครองวัตถุแห่งการกระทำความผิดส่วนใหญ่เป็นสิ่งที่สามารถจับต้องได้ และสามารถมองเห็นได้ เช่น การบุกรุก ขโมยทรัพย์สินและทำร้ายร่างกาย แต่เนื่องจากลักษณะที่ไม่มีตัวตนของการกระทำความผิดทางคอมพิวเตอร์ กฎหมายที่มีอยู่ในปัจจุบันจึงไม่สามารถนำมาปรับใช้ให้คลอบคลุมถึงการกระทำความผิดรูปแบบใหม่ และนำตัวผู้กระทำความผิดมารับโทษให้เกิดความยุติธรรมได้ เนื่องจากรูปแบบของการกระทำผิดต่างจากรูปแบบเดิม ดังนั้น หลักเกณฑ์ และมาตรการทางกฎหมายในการจัดการปัญหาอาชญากรรมทางคอมพิวเตอร์ในปัจจุบันของ สปป.ลาว ยังมีปัญหา และความไม่ชัดเจนโดยแยกพิจารณาได้ ดังนี้

**4.2.1 กฎหมายอาญา ค.ศ. 2005**

ปัจจุบัน สปป.ลาว ได้บังคับใช้กฎหมายอาญา ค.ศ. 2005 ซึ่งเป็นกฎหมายสำคัญฉบับหนึ่งที่รัฐใช้ปกป้องคุ้มครองสิทธิของประชาชนจากการกระทำความผิด และใช้ในการนำตัวผู้กระทำความผิดมาลงโทษ ซึ่งทุกการกระทำหรือการละเว้นการกระทำที่เป็นอันตรายต่อระบบการเมือง เศรษฐกิจ หรือสังคมของ สปป.ลาว ต่อกรรมสิทธิ์ของรัฐ ของส่วนร่วม และของบุคคล ชีวิต สุขภาพ เกียรติศักดิ์ศรี สิทธิ เสรีภาพของพลเมือง ความสงบของชาติหรือความเป็นระเบียบเรียบร้อยของสังคม ที่บัญญัติไว้ในกฎหมายอาญาหรือกฎหมายอื่นของ สปป.ลาว ที่กำหนดโทษทางอาญาจะถือว่าเป็นการกระทำผิดทางอาญา[111] นอกจากนี้ในมาตรา 2 ของกฎหมายฉบับนี้ได้มีการบัญญัติว่า “บุคคลใดจะมีความรับผิดชอบทางอาญา และจะถูกลงโทษทางอาญาได้ก็ต่อเมื่อบุคคลผู้นั้นหากมีการกระทำโดยเจตนาหรือด้วยความประมาทที่เป็นอันตรายต่อสังคม ซึ่งได้กำหนดไว้ในกฎหมายอาญาหรือกฎหมายอื่นของ สปป.ลาว ที่ได้กำหนดโทษทางอาญา และในเมื่อมีคำตัดสินของศาลเท่านั้น” จะเห็นได้ว่าในกฎหมายดังกล่าวได้มีการบัญญัติรองรับลักษณะการบังคับใช้กฎหมายอาญาให้สอดคล้องกับหลักการสำคัญที่ว่า “ไม่มีความผิด ไม่มีโทษโดยไม่มีกฎหมาย” ดังนั้นผู้กระทำความผิดจะต้องถูกลงโทษตามที่กฎหมายกำหนดไว้

ในกรณีที่จะสามารถนำตัวผู้กระทำความผิดมาลงโทษได้นั้น ผู้กระทำความผิดต้องมีการกระทำที่ครบองค์ประกอบของการกระทำความผิดทางอาญาตามกฎหมายอาญา ค.ศ. 2005 ของ

---

[111] กฎหมายอาญา ค.ศ. 2005, มาตรา 6 วรรคหนึ่ง.

สปป.ลาว ที่กำหนดไว้[112] ซึ่งองค์ประกอบของการกระทำความผิดทางอาญาประกอบด้วย องค์ประกอบด้านวัตถุกรรม องค์ประกอบด้านภาวะวิสัย (พฤติกรรมภายนอก) องค์ประกอบด้าน อัตวิสัย (เจตนา) และองค์ประกอบด้านเจ้ากรรม(ผู้กระทำความผิด) ซึ่งการกระทำความผิดรูปแบบใหม่ของอาชญากรรมทางคอมพิวเตอร์นั้น หากนำกฎหมายอาญาในปัจจุบันมาปรับใช้จะเกิดปัญหาในการตีความว่าการกระทำดังกล่าวจะเป็นความผิดหรือไม่ และหากมีการปรับใช้อาจขัดต่อหลักการตีความโดยเคร่งครัดของกฎหมายอาญา กล่าวคือ กฎหมายอาญาต้องตีความโดยเคร่งครัดตามตัวอักษร กล่าวอีกนัยหนึ่งก็คือ ตัวบทกฎหมายบัญญัติไว้เช่นใดก็ต้องตีความเช่นนั้น นอกจากนั้นจะนำหลักการตีความในกฎหมายแพ่งและพาณิชย์มาใช้ในกฎหมายอาญาก็ไม่ได้[113]

4.2.1.1 การเข้าถึงระบบคอมพิวเตอร์โดยมิได้รับอนุญาต หากการกระทำในการเข้าถึงระบบคอมพิวเตอร์ของบุคคลอื่นที่ไม่ใช่เจ้าของ และไม่ได้รับอนุญาตในการเข้าถึง ได้มีการเข้าไปทางกายภาพในสถานที่ตั้งของระบบคอมพิวเตอร์นั้นจริง โดยการเข้าไปในสถานที่ตั้งของคอมพิวเตอร์เป้าหมาย เพื่อสืบค้นข้อมูล เจาะข้อมูลของเครื่องคอมพิวเตอร์อื่นภายในองค์กรนั้น การกระทำดังกล่าวย่อมเป็นความผิดฐานบุกรุก ตามมาตรา 103[114] และมาตรา 104 วรรคสอง[115] แห่งกฎหมายอาญา ค.ศ. 2005 หากการกระทำความผิดทางอาญามีลักษณะครบองค์ประกอบของความผิดประเภทนั้น ผู้กระทำความผิดก็ต้องรับผิดตามฐานความผิดนั้น ๆ

อย่างไรก็ตาม ในการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตนี้ มิได้เกิดขึ้นเฉพาะความผิดทางกายภาพเพียงอย่างเดียว เพราะการเข้าถึงดังกล่าวผู้กระทำสามารถใช้เครือข่าย

---

[112] กฎหมายอาญา ค.ศ. 2005, มาตรา 7 บัญญัติว่า “องค์ประกอบด้านวัตถุกรรมของการกระทำความผิดหมายถึง ความเกี่ยวพันธ์ด้านสังคมที่รัฐคุ้มครองโดยกฎหมายอาญา และได้รับผลกระทบจากการกระทำความผิด

องค์ประกอบด้านภาวะวิสัยของการกระทำความผิด หมายถึง บรรดาเครื่องหมายภายนอกของพฤติกรรมที่ได้จัดตั้งและได้รับความเสียหายต่อความเกี่ยวพันธ์ด้านสังคมที่ถูกคุ้มครอง โดยกฎหมายอาญารวมทั้งวันเวลา สถานที่ พาหนะ อุปกรณ์ สภาพ และวิธีประกอบการกระทำผิดดังกล่าว

องค์ประกอบด้านอัตวิสัยของการกระทำความผิด หมายถึง บรรดาเครื่องหมายต่าง ๆ ทางด้านทัศนะแนวคิดของบุคคลผู้กระทำความผิดต่อการกระทำผิดของตนที่แสดงออกภายนอกต่อการกระทำความผิดโดยผ่านพฤติกรรม

องค์ประกอบด้านเจ้ากรรมของการกระทำความผิด หมายถึง ผู้กระทำความผิดซึ่งต้องเป็นบุคคลที่มีสติสัมปชัญญะ ไม่เป็นคนวิกลจริตหรือเสมือนไร้ความสามารถ และมีอายุสิบห้าปีขึ้นไป”.

[113] มานิตย์ จุมปา (บรรณาธิการ), *ความรู้พื้นฐานเกี่ยวกับกฎหมาย*, 108.

[114] กฎหมายอาญา ค.ศ. 2005, มาตรา 103 บัญญัติว่า “บุคคลใดล่วงเข้าเคหสถานผู้อื่นโดยไม่ถูกต้องตามกฎหมาย ด้วยการใช้ความรุนแรง การข่มขู่ การใช้เอกสารปลอม การปลอมแปลงเป็นเจ้าหน้าที่ หรือด้วยวิธีการอื่น ๆ ...”.

[115] เรื่องเดียวกัน, มาตรา 104 วรรคสอง บัญญัติว่า “บุคคลใดหากได้ลักเปิดจดหมาย โทรเลข หรือเอกสารอื่น ๆ หรือลักฟังโทรศัพท์ของผู้อื่น ซึ่งเป็นการก่อความเสียหายแก่ผู้อื่นนั้น...”.

คอมพิวเตอร์เป็นช่องทางในการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นได้ ไม่ว่าจะเป็น “การเจาะระบบคอมพิวเตอร์ (Hacking or Craking)” หรือ “การบุกรุกทางคอมพิวเตอร์ (Computer Trespass)” จึงทำให้เกิดปัญหาในการปรับใช้กฎหมายอาญา ค.ศ. 2005 เกี่ยวกับความผิดฐานบุกรุกต่อการกระทำดังกล่าว เนื่องจากการเข้าไปในเคหสถานตามความหมายของความผิดฐานบุกรุก ต้องเป็นการพาตัวผู้กระทำล่วงล้ำเข้าไปในอสังหาริมทรัพย์ของผู้อื่นทางกายภาพ ทั้งการเข้าไปทางพื้นดิน ใต้ดินหรือทางอากาศ แต่การบุกรุกทางคอมพิวเตอร์ผู้กระทำยังอยู่ ณ สถานที่ตั้งของคอมพิวเตอร์ที่ใช้ในการเจาะข้อมูล มิได้มีการพาตัวเองเข้าไปสู่สถานที่ตั้งของระบบคอมพิวเตอร์เป้าหมายแต่อย่างใด

4.2.1.2 การขโมยข้อมูลคอมพิวเตอร์ เป็นการกระทำของผู้ที่ไม่ได้รับอนุญาตได้เข้าไปล่วงรู้เอาข้อมูลของผู้อื่นที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์หรือดักจับข้อมูลขณะส่งผ่านระบบ หรือถ่ายโอนผ่านระบบเครือข่ายคอมพิวเตอร์ ซึ่งโดยส่วนใหญ่จะเป็นข้อมูลส่วนบุคคล ข้อมูลทางเศรษฐกิจหรือความลับทางการค้า ในกรณีความผิดฐานลักทรัพย์นั้น หากผู้กระทำได้เอาไปซึ่งเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ต่าง ๆ คงจะไม่เกิดปัญหาในการปรับใช้กฎหมายอาญา[116] แต่การกระทำดังกล่าวสิ่งที่ได้ไปคือข้อมูลที่อยู่ในรูปของดิจิตอลเป็นคลื่นแม่เหล็กไฟฟ้าที่ไม่ปรากฏรูปร่างหรือสภาพทางกายภาพอย่างชัดเจน ไม่สามารถสัมผัสจับต้องได้ นอกจากนี้ความผิดฐานลักทรัพย์ต้องมีการเอาไปจากการครอบครอง กล่าวคือ ขณะเอาไปต้องมีผู้อื่นครอบครองทรัพย์นั้นอยู่ และมีการแย่งไปจากการครอบครองนั้น[117] แต่ในกรณีการเอาไปซึ่งข้อมูลคอมพิวเตอร์นี้ เห็นได้ว่ามิได้มีการเอาไปในลักษณะของการแย่งการครอบครองหรือตัดกรรมสิทธิ์ในข้อมูลนั้นจากเจ้าของข้อมูล เพราะข้อมูลยังอยู่ในความครอบครองของเจ้าของข้อมูลนั้น ผู้กระทำเพียงได้เห็นข้อมูลที่ปรากฏอยู่ในเครื่องคอมพิวเตอร์ หรือได้ดักจับไว้หรือได้ทำสำเนาไปเท่านั้น ด้วยเหตุนี้เมื่อพิจารณาจากเหตุผลข้างต้นจะเห็นได้ว่าไม่สามารถนำความผิดฐานลักทรัพย์ตามกฎหมายอาญา ค.ศ. 2005 มาปรับใช้กับการกระทำดังกล่าวได้

4.2.1.3 การแก้ไข เปลี่ยนแปลง ทำลายข้อมูล และรบกวนการทำงานของระบบคอมพิวเตอร์ หากมีบุคคลได้สร้างความเสียหายต่อเครื่องคอมพิวเตอร์ โครงข่ายคอมพิวเตอร์ หรือข้อมูลที่ได้จากการประมวลผลของคอมพิวเตอร์ เช่น เอกสารต่าง ๆ การกระทำดังกล่าวย่อมเป็นความผิดฐานทำให้เสียทรัพย์ แต่ความเป็นจริงแล้วความเสียหายที่เกิดกับข้อมูลและโปรแกรมคอมพิวเตอร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ โดยมิได้สร้างความเสียหายหรือส่งผลกระทบต่อระบบ

---

[116] กฎหมายอาญา ค.ศ. 2005, มาตรา 119 ว่าด้วยการขโมย การชิงทรัพย์ของพลเมือง “บุคคลใดหากได้เอาทรัพย์ของผู้อื่นโดยลับหลัง...”.

[117] ทวีเกียรติ มีนะกนิษฐ, *ประมวลกฎหมายอาญา ฉบับอ้างอิง*, พิมพ์ครั้งที่ 29, (กรุงเทพฯ: วิญญชน, 2555), 509.

ฮาร์ดแวร์ แม้การกระทำดังกล่าวมิได้สร้างความเสียหายต่อคอมพิวเตอร์ฮาร์ดแวร์ แต่การทำลายข้อมูลและโปรแกรมต่าง ๆ ภายในเครื่อง จะถือเป็นการทำให้คอมพิวเตอร์ฮาร์ดแวร์ไร้ประโยชน์หรือไม่ เนื่องจากการทำงานของเครื่องคอมพิวเตอร์จะประกอบด้วยองค์ประกอบที่สำคัญอยู่ 3 ส่วน คือ ฮาร์ดแวร์ (Hardware) ซอฟท์แวร์ (Software)[118] และข้อมูล หากขาดส่วนใดส่วนหนึ่งการทำงานของเครื่องย่อมไม่สามารถปฏิบัติการได้อย่างปกติ หรือไม่สามารถทำงานได้เลย การทำลายข้อมูลหรือซอฟท์แวร์จะทำให้คอมพิวเตอร์ฮาร์ดแวร์เปรียบเสมือนเศษเหล็กชิ้นหนึ่ง เจ้าของคอมพิวเตอร์จะไม่สามารถใช้เครื่องคอมพิวเตอร์ฮาร์ดแวร์นั้นได้จนกว่าจะได้มีการติดตั้งซอฟท์แวร์และข้อมูลเข้าไปใหม่ ดังนั้น การสร้างความเสียหายต่อข้อมูลหรือซอฟท์แวร์คอมพิวเตอร์ที่อยู่ในเครื่อง จึงไม่สามารถตีความได้ว่าเป็นการทำให้คอมพิวเตอร์ฮาร์ดแวร์ไร้ประโยชน์อันเป็นความผิดฐานทำให้เสียทรัพย์[119]

ความผิดฐานปลอมแปลงเอกสาร การกระทำจะมีการเข้าไปแก้ไข เปลี่ยนแปลง เพิ่มเติม และตัดทอนข้อมูลคอมพิวเตอร์ที่เก็บอยู่ในเครื่องคอมพิวเตอร์ ปัญหาในการปรับใช้กฎหมายอาญา[120] ก็คือ ข้อมูลเป็นเอกสารตามนัยแห่งกฎหมายหรือไม่ เนื่องจากเอกสารจะต้องมีสิ่งรองรับ แต่ข้อมูลคอมพิวเตอร์ขาดวัตถุรองรับ เพราะเมื่อเปิดเครื่องข้อมูลจะหายไป แม้จะมีการบันทึกไว้ในฮาร์ดดิสก์ (Harddisk) แต่ก็ไม่สามารถมองเห็นได้ด้วยตาเปล่าต้องอาศัยอุปกรณ์อื่นช่วยจึงจะสามารถอ่านข้อความได้ ประกอบกับการปรากฏของเอกสารจะต้องเกิดจากการกระทำของบุคคลหากปรากฏขึ้นเองจะไม่เป็นเอกสาร ดังนั้น ข้อมูลที่คอมพิวเตอร์ทำให้ปรากฏขึ้นโดยอัตโนมัติจะมิใช่เอกสารตามกฎหมาย ส่วนข้อมูลที่บุคคลเป็นผู้ทำให้ปรากฏขึ้น บุคคลจะเป็นเพียงตัวเชื่อมในการสั่งให้คอมพิวเตอร์ทำการประมวลผลข้อมูล แล้วคอมพิวเตอร์ ซอฟท์แวร์ และฮาร์ดแวร์ จะปฏิบัติการเพื่อถอดข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องให้สามารถสื่อความหมาย และแสดงข้อมูลให้ปรากฏ จึงถือมิได้ว่าบุคคลเป็นผู้ทำให้ปรากฏขึ้น ดังนั้น เมื่อข้อมูลมิใช่เอกสาร การแก้ไข เปลี่ยนแปลง ตัดทอน เพิ่มหรือทำข้อมูลคอมพิวเตอร์ขึ้นมาใหม่จึงไม่เป็นความผิดฐานปลอมเอกสาร

---

[118] ฮาร์ดแวร์ (Hardware) เป็นความรู้ที่ประกอบอยู่ในสิ่งที่มีรูปร่าง เช่น ในเอกสารข้อมูล เครื่องจักร อุปกรณ์ ผัง หรือแผนแบบต่าง ๆ ส่วน ซอฟท์แวร์ (Software) หมายถึง ความรู้ที่ไม่สามารถแสดงออกเป็นรูปธรรมได้ เช่น ความรู้ที่ประกอบอยู่กับองค์กรหรือบุคลากร ในลักษณะของความเชี่ยวชาญ ประสบการณ์หรือระบบการบริหาร, ดู TDRI, *The barrier to and strategies for technology acquisition*, (Bangkok: Thailand Development Research Institute, 1991), 2.

[119] สำนักบริหารกลาง, *รวมสาระน่ารู้เกี่ยวกับกฎหมายไอที*, (กรุงเทพฯ: สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, ม.ป.ป.), 2-6.

[120] กฎหมายอาญา ค.ศ. 2005, มาตรา 161 ว่าด้วยการปลอมแปลงเอกสารหรือการใช้เอกสารปลอม “บุคคลใดหากได้ปลอมแปลงเอกสาร ลายเซ็น ตราประทับ ได้ตัดหรือเพิ่มข้อความใดข้อความหนึ่งในเอกสาร...”.

จากการศึกษาพบว่าการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์นั้น เป็นสิ่งที่ผู้กระทำเพียงป้อนคำสั่งเข้าไปในระบบคอมพิวเตอร์ก็จะทำงานได้เองโดยผู้กระทำผิดมิได้มีการแสดงออกซึ่งกายภาพดังที่ได้กล่าวแล้ว และหากนำกฎหมายอาญา ค.ศ. 2005 ที่มีอยู่มาปรับใช้ในการลงโทษ อาจไม่รองรับถึงลักษณะของการกระทำผิดทางคอมพิวเตอร์ ที่ผู้กระทำใช้ความสลับซับซ้อนของเทคโนโลยีคอมพิวเตอร์ในการกระทำความผิดและมีความแตกต่างจากการกระทำผิดทั่วไป และยากที่จะมองเห็น จึงไม่เข้าองค์ประกอบของความผิดทางอาญาทั่วไป

**4.2.2 กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2012**

เทคโนโลยีด้านการสื่อสารโทรคมนาคมได้เจริญก้าวหน้าไปอย่างรวดเร็ว การทำธุรกรรมทางอิเล็กทรอนิกส์นับเป็นอีกทางเลือกหนึ่งในการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลทางการค้า การลงทุน แต่เนื่องจากรูปแบบใหม่ในการทำธุรกรรมทางอิเล็กทรอนิกส์ ได้ใช้เครื่องคอมพิวเตอร์ และระบบคอมพิวเตอร์เข้าดำเนินการ ไม่ว่าจะเป็นการติดต่อสื่อสารกันบนเครือข่ายโดยใช้วิธีการทางอิเล็กทรอนิกส์ การแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ ไปรษณีย์อิเล็กทรอนิกส์หรือวิธีการทางอิเล็กทรอนิกส์อื่น ๆ ล้วนแต่ทำในรูปแบบของข้อมูลอิเล็กทรอนิกส์ มิได้ทำบนกระดาษดังเช่นเดิม

อย่างไรก็ตามหากมีการกระทำในรูปแบบของการส่งจดหมายอิเล็กทรอนิกส์ที่ผู้ส่งได้ส่งไปยังผู้รับอย่างต่อเนื่อง โดยส่งจำนวนครั้งละมาก ๆ และมิได้รับความยินยอมจากผู้รับ โดยการส่งจดหมายอิเล็กทรอนิกส์นั้นอาจมีวัตถุประสงค์เชิงพาณิชย์หรือไม่ก็ได้ ซึ่งในปัจจุบัน สปป.ลาว มีกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2012 ที่มีวัตถุประสงค์ในการกำหนดหลักการระเบียบการ และมาตรการเกี่ยวกับการสร้าง การใช้ การรับรู้ การคุ้มครอง และการตรวจตราธุรกรรมทางอิเล็กทรอนิกส์ เพื่อทำให้มีความเชื่อถือ และมีความมั่นใจต่อธุรกรรมทางอิเล็กทรอนิกส์ เพื่อปกป้องสิทธิ และผลประโยชน์โดยชอบธรรมของผู้ทำการค้าทางอิเล็กทรอนิกส์ และรับประกันการใช้ การส่งเสริมธุรกรรมทางอิเล็กทรอนิกส์ แต่ข้อห้ามในกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2012 ได้มีการห้ามมิให้สนองข้อมูลที่ไม่ถูกต้องหรือข้อมูลส่วนตัว

ต่อผู้ใช้บริการ ปลอมแปลงเอกสารหรือใช้ข้อมูลเฉพาะของผู้อื่นโดยไม่ได้รับอนุญาต[121] ซึ่งกฎหมายฉบับนี้ยังไม่ครอบคลุมถึงรูปแบบของการส่งจดหมายอิเล็กทรอนิกส์ ที่เป็นการส่งจดหมายต่อ ๆ กันมาที่มีวัตถุประสงค์แตกต่างกัน และจดหมายอิเล็กทรอนิกส์ในจำนวนมาก ๆ อาจก่อให้เกิดปัญหามากมายในขณะนี้ก็คือจดหมายที่มีการโฆษณาสินค้าและบริการที่ไม่ชอบด้วยกฎหมาย มีเนื้อหาที่ขัดต่อศีลธรรมอันดี และมีข้อความที่มีลักษณะหลอกลวง ย่อมส่งผลกระทบต่อเศรษฐกิจและสังคมใน สปป.ลาว อย่างมาก

นอกจากนั้น หากมีผู้ไม่หวังดีเข้าไปในระบบเพื่อดัดแปลงแก้ไขข้อมูลบางส่วนเกี่ยวกับการให้บริการทางด้านการเงินบางประเภท เช่น Electronic Data Interchange และ Electronic Fund Transfer เป็นต้น ซึ่งเกี่ยวข้องกับการรับรองลายมือชื่อที่ส่งผ่านเครือข่ายคอมพิวเตอร์ยังประสบปัญหาอยู่ ทำให้การพัฒนากิจการดังกล่าวไม่สามารถดำเนินการไปได้ดีเท่าที่ควร

ดังนั้น จากการศึกษากฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2012 พบว่า การปรับใช้กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ของ สปป.ลาว ในปัจจุบันไม่ครอบคลุมพฤติกรรมดังกล่าว และไม่สามารถนำตัวผู้กระทำการผิดมาลงโทษได้ อันเนื่องจากการกระทำดังกล่าวเป็นการกระทำต่อข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งมิใช่บุคคลเป็นผู้กระทำการส่งมอบทรัพย์สินหรือประโยชน์อื่นใดแก่ตนเองหรือผู้อื่น อันไม่มีบุคคลเข้ามาเกี่ยวข้องแต่อย่างใด เช่น การแก้ไขการเปลี่ยนแปลงจำนวนเงินในบัญชีธนาคาร หรือการโอนเงินจากบัญชีอื่นเข้าบัญชีของตน ด้วยเหตุนี้ เมื่อมีการดัดแปลงแก้ไขข้อมูลธุรกรรมทางอิเล็กทรอนิกส์ จึงส่งผลให้อีกฝ่ายเข้าใจผิดเกี่ยวกับสัญญาดังกล่าวได้ เช่นนี้ จึงทำให้กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2012 ยังไม่สามารถนำมาบังคับใช้ได้อย่างมีประสิทธิภาพต่อการก่ออาชญากรรมทางคอมพิวเตอร์

---

[121] กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2012, มาตรา 68 ว่าด้วยข้อห้ามสำหรับบุคคล นิติบุคคล และองค์กรอื่น.

"(1) ปลอมแปลงเอกสาร ลายเซ็นหรือหนังสือยืนยันทางอิเล็กทรอนิกส์หรือใช้ลายเซ็นดิจิตอลที่มีการป้องกันอันเป็นเท็จ

(2) สนับสนุนข้อมูลที่ไม่ถูกต้อง และลายเซ็นอิเล็กทรอนิกส์ปลอม

(3) เข้าถึง สำเนา ปรับปรุงหรือครอบครองระบบลายเซ็นอิเล็กทรอนิกส์ของผู้อื่นโดยไม่ได้รับอนุญาต

(4) ใช้ข้อมูลเฉพาะของผู้อื่นโดยไม่ได้รับอนุญาต

(5) แอบอ้างตนเองเป็นตัวแทน ในการเสนอหยุด ยกเลิกหรือรับรองลายเซ็นดิจิตอลที่มีการป้องกัน

(6) เผยแพร่หนังสือยืนยันดิจิตอลที่มีการป้องกันอันเป็นเท็จ ไม่ถูกต้อง ถูกยกเลิกหรือถูกหยุดใช้งานให้ผู้อื่นเอาไปใช้

(7) สนับสนุนข้อความที่เป็นข้อมูล และสิ่งบันทึกทางอิเล็กทรอนิกส์ ซึ่งส่งผลกระทบถึงความมั่นคงของชาติ ความสงบและความเป็นระเบียบเรียบร้อยของสังคม และ

(8) มีพฤติกรรมอื่นที่เป็นการละเมิดระเบียบกฎหมาย".

**4.2.3 ดำรัฐว่าด้วยการคุ้มครองข้อมูลข่าวสารผ่านอินเทอร์เน็ต ค.ศ. 2014**

จากความนิยมใช้บริการอินเทอร์เน็ตที่มีปริมาณเพิ่มมากขึ้นใน สปป.ลาว ทำให้ต้องมีการควบคุมการเผยแพร่ข้อมูลข่าวสารผ่านอินเทอร์เน็ต รัฐบาลแห่ง สปป.ลาว จึงได้มีมติเห็นชอบออกดำรัฐว่าด้วยการคุ้มครองข้อมูลข่าวสารผ่านอินเทอร์เน็ต ฉบับเลขที่ 327/รบ ลงวันที่ 16 กันยายน ค.ศ. 2014 ซึ่งดำรัฐดังกล่าวได้กำหนดหลักการ ระเบียบการ และมาตรการในการคุ้มครองข้อมูลข่าวสารผ่านอินเทอร์เน็ต เพื่อรับประกันความมั่นคงของชาติ ความสงบเรียบร้อยของสังคม โดยมีเป้าหมายเพื่อปกป้องคุ้มครองผลประโยชน์อันชอบธรรมของผู้ให้บริการ ผู้ใช้บริการ และสังคม ในมาตรา 16 ของดำรัฐฉบับนี้ได้กำหนดข้อห้ามสำหรับผู้ใช้บริการอินเทอร์เน็ต ในการนำเสนอ ส่ง ส่งต่อ ข้อมูลข่าวสาร ที่มีเนื้อหาตามที่ได้กำหนดไว้ในมาตรา 10 ดังนี้

4.2.3.1 โกหก หลอกลวงประชาชนที่อยู่ภายในประเทศและต่างประเทศให้หลงเชื่อเพื่อต่อต้านต่อพรรคประชาชนปฏิวัติลาว รัฐบาลแห่ง สปป.ลาว หรือทำลายสันติภาพ ความเป็นเอกราชอธิปไตย ความเป็นเอกภาพ และความเป็นวัฒนาถาวรของ สปป.ลาว

4.2.3.2 ยุยง และส่งเสริมการก่อการร้าย การฆาตกรรม และทำให้สังคมปั่นป่วน

4.2.3.3 โฆษณา บิดเบือนและปล่อยข่าวอกุศล เพื่อสร้างความแบ่งแยกระหว่างชนเผ่าและระหว่างชาติ

4.2.3.4 เผยแพร่รูปภาพลามก รูปภาพตัดต่อ และรูปภาพอื่น ๆ ที่กฎหมาย สปป.ลาว ต้องห้ามหรือส่งผลกระทบต่อจารีตประเพณีอันดีงามของชาติ และส่งผลกระทบต่อทรัพย์สินทางปัญญาของผู้อื่น และซื้อขายบริการทางเพศ

4.2.3.5 เผยแพร่ความลับของชาติ ทางการทหารหรือความลับด้านอื่น ๆ ที่กำหนดไว้อยู่ในกฎหมายของ สปป.ลาว

4.2.3.6 เผยแพร่ข้อมูลข่าวสารที่ไม่ถูกต้อง และบิดเบือนความจริง เพื่อจุดประสงค์สร้างความเสื่อมเสียต่อเกียรติศักดิ์ศรีหรือสิทธิส่วนบุคคลของผู้อื่น สถาบันหรือองค์กรอื่น

4.2.3.7 ใช้ชื่อของบุคคลหรือองค์กร รูปภาพ เสียง วิดีโอ ลายเซ็น รหัสต่าง ๆ บัตรเครดิต หรือเอกสารส่วนบุคคลอื่น เพื่อผลประโยชน์หรือเพื่อจุดประสงค์อื่น โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของ

ดังกล่าวมาจะเห็นได้ว่าดำรัฐฉบับนี้ ยังมิได้มีการกำหนดอย่างชัดเจนเกี่ยวกับรูปแบบของการกระทำผิด และยังไม่ได้มีการบัญญัติมาตรการในการลงโทษเกี่ยวกับการกระทำในรูปแบบตามต่าง ๆ ของข้อห้ามตามดำรัฐฉบับนี้ ซึ่งการที่จะนำผู้กระทำความผิดมาลงโทษได้นั้น ในลักษณะของกฎหมายอาญาแล้วหมายถึงกฎหมายที่ว่าด้วยความผิด และโทษ ในส่วนที่กล่าวถึงความผิดหมายถึงการที่กฎหมายบัญญัติห้ามไว้ไม่ให้กระทำการอย่างใดอย่างหนึ่ง นอกจากนี้กฎหมายอาญายังบัญญัติ

ให้บุคคลต้องกระทำการอย่างใดอย่างหนึ่ง ถ้าไม่กระทำตามที่กฎหมายกำหนดในกรณีนั้น ๆ ย่อมจะมีความผิดเช่นกัน และในส่วนที่กล่าวถึงโทษนั้น เป็นสภาพบังคับของกฎหมายอาญา เพราะหากกฎหมายบัญญัติแต่การกระทำที่เป็นความผิดโดยไม่ได้กำหนดสภาพบังคันอันเป็นบทลงโทษไว้กฎหมายย่อมไม่มีความหมายอย่างใด[122] นอกจากนี้การที่จะเอาตัวผู้กระทำความผิดมาลงโทษนั้นเกี่ยวกับรูปแบบของการกระทำความผิดทางคอมพิวเตอร์ เช่น การนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการตัดต่อ เติมหรือดัดแปลงด้วยวิธีทางอิเล็กทรอนิกส์หรือวิธีอื่นใด ซึ่งการกระทำดังกล่าวส่งผลกระทบต่อบุคคลทั่วไป ไม่ว่าในทางสังคม ความมั่นคง เศรษฐกิจหรือความรู้สึก เช่น การเข้าถึงระบบคอมพิวเตอร์ การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้น การเข้าถึงข้อมูลคอมพิวเตอร์ การดักรับข้อมูลคอมพิวเตอร์ การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์ โดยมิชอบ เป็นต้น ล้วนแต่สร้างความเสียหายให้เกิดขึ้นกับสังคมทั้งสิ้น

จากรูปแบบของการกระทำอาชญากรรมทางคอมพิวเตอร์ จะเห็นได้ว่าผู้กระทำเป็นผู้มีความชำนาญทางด้านคอมพิวเตอร์และโครงข่าย ด้วยการเข้าไปอยู่ในระบบโครงข่ายของผู้อื่นและดำเนินการให้เกิดผลเสียหายต่อบุคคลอื่น ๆ ที่ใช้โครงข่ายดังกล่าวทั้งในด้านการผลิต (Manufacturing) และการควบคุมดูแล (Monitoring) ซึ่งดำรัฐฉบับนี้ของ สปป.ลาว ยังขาดมาตรการลงโทษผู้กระทำการดังกล่าว

จากการศึกษาจะเห็นได้ว่าดำรัฐฉบับนี้ในปัจจุบันนั้นไม่สามารถนำมาใช้บังคับกับบริการต่าง ๆ ที่รวมเอาเทคโนโลยีด้านโทรคมนาคมและด้านคอมพิวเตอร์ในลักษณะผสมผสานกันอย่างกลมกลืนจนไม่สามารถแยกจากกันอย่างชัดเจน และไม่สามารถใช้ดำเนินการกับผู้ใช้บริการที่สามารถเข้าถึง (Access Number) ของผู้ใช้รายอื่น ๆ และการดักรับข้อมูลของผู้ใช้บริการรายอื่น ทั้งนี้เพราะข้อมูลที่ดักรับไปเป็นข้อมูลที่จับต้องมิได้ กล่าวคือ ฐานข้อมูล และเมื่อถูกดักรับไปแล้วข้อมูลดังกล่าวก็ยังคงอยู่กับผู้ใช้บริการเดิมมิได้หายไปไหน การจะตีความเอาผิดผู้กระทำตามดำรัฐว่าด้วยการคุ้มครองข้อมูลข่าวสารผ่านอินเทอร์เน็ต ค.ศ. 2014 ก็ยังมีความไม่ชัดเจน เพราะฐานข้อมูลมิได้จัดอยู่ในข่ายลิขสิทธิ์ (Copy Right) สิทธิบัตร (Patent) หรือเครื่องหมายการค้า (Trade Mark) แต่ฐานข้อมูลเป็นความลับทางการค้า (Trade Secret) ซึ่งมุ่งคุ้มครองความลับทางการค้าเป็นการเฉพาะได้กล่าวถึงวิธีการได้ไปซึ่งความลับทางการค้าแต่อย่างใด

---

[122] แสวง บุญเฉลิมวิภาส, *หลักกฎหมายอาญา*, 13.

ดังนั้นจึงจำเป็นที่จะต้องมีการบัญญัติกฎหมายให้มีความเฉพาะเจาะจง เพื่อให้สามารถบังคับใช้กับการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ และสามารถรักษาผลประโยชน์ของประเทศชาติและบุคคลได้

**4.2.4 ร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ...**

ปัจจุบัน สปป.ลาว ได้มีการเชื่อมโยงระบบโทรคมนาคม และอินเทอร์เน็ตกับสากล และภูมิภาคต่าง ๆ ในทั่วโลก ไม่ว่าจะเป็นภาครัฐ และเอกชนต่างก็ได้มีการใช้เทคโนโลยีทางด้านคอมพิวเตอร์เข้ามามีบทบาทสำคัญในการพัฒนาองค์กร จากการใช้งานดังกล่าวอาจมีผู้กระทำการอย่างใดอย่างหนึ่งที่เป็นการส่งผลกระทบให้แก่การใช้งานเทคโนโลยีทางคอมพิวเตอร์ได้ ด้วยเหตุนี้รัฐบาลของ สปป.ลาว จึงเห็นถึงความสำคัญดังกล่าว ได้มีการร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... โดยผ่านการรับรองในวันที่ 7 กรกฎาคม ค.ศ. 2015[123] จากกองประชุมสมัยสามัญ ครั้งที่ 9 ของสภาแห่งชาติ ชุดที่ 7 ของ สปป.ลาว ซึ่งในร่างกฎหมายดังกล่าวได้มีวัตถุประสงค์ในการกำหนดหลักการ ระเบียบการ และมาตรการเกี่ยวกับการคุ้มครอง การติดตามตรวจตราเกี่ยวกับการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์เพื่อทำให้งานดังกล่าวมีประสิทธิผลเพิ่มมากขึ้นในการต้าน สกัดกั้น จำกัด และกำจัดอาชญากรรมปกป้องระบบฐานข้อมูล ระบบเซิฟเวอร์ (Server System) ข้อมูลทางระบบคอมพิวเตอร์ และเป็นหลักประกันความมั่นคงของชาติ ความสงบ และความเป็นระเบียบเรียบร้อยของสังคม สามารถเชื่อมโยงกับภูมิภาค และสากล เป็นส่วนหนึ่งในการปกปักษ์รักษา และพัฒนาเศรษฐกิจ-สังคมให้เจริญก้าวหน้า[124]

จากการที่ สปป.ลาว ได้มีการร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ทำให้ สปป.ลาว ได้มีมาตรการทางกฎหมายในการดำเนินคดีต่อผู้กระทำผิดทางระบบคอมพิวเตอร์ ซึ่งในมาตรา 8 ของกฎหมายฉบับนี้ได้มีการกำหนดลักษณะของพฤติกรรมที่เป็นอาชญากรรมทางระบบคอมพิวเตอร์ ประกอบด้วยดังนี้:

1. การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์
2. การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต
3. การตัดต่อเนื้อหา รูปภาพโดยไม่ได้รับอนุญาต

---

[123] มติตกลงของสภาแห่งชาติ แห่ง สปป.ลาว ว่าด้วยการรับรองกฎหมาย 3 ฉบับ ฉบับเลขที่ 09/สภช. ลงวันที่ 7 กรกฎาคม 2015.

[124] ร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ..., มาตรา 1 วัตถุประสงค์.

4. การดักรับเอาข้อมูลในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

5. การสร้างความเสียหายผ่านสื่อออนไลน์

6. การเผยแพร่สิ่งลามกผ่านระบบคอมพิวเตอร์

7. การรบกวนระบบคอมพิวเตอร์

8. การปลอมแปลงข้อมูลคอมพิวเตอร์

9. การทำลายข้อมูลคอมพิวเตอร์

10. การดำเนินกิจการเกี่ยวกับเครื่องมืออาชญากรรมทางระบบคอมพิวเตอร์และ

11. การใช้ระบบคอมพิวเตอร์ในการก่อการร้าย และการเล่นการพนันที่ต้องห้ามผ่านระบบคอมพิวเตอร์

ซึ่งเป็นการกำหนดลักษณะความผิดของการกระทำทางระบบคอมพิวเตอร์ แต่อย่างไรก็ตามในกฎหมายดังกล่าวยังไม่ครอบคลุมลักษณะของการกระทำของอาชญากรรมทางคอมพิวเตอร์บางกรณีที่อาจสร้างความเสียหายอย่างมากมายได้ เช่น การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต ที่เป็นการกระทำใด ๆ โดยการใช้เทคโนโลยีทางคอมพิวเตอร์เพื่อเข้าถึงแฟ้มข้อมูล (File) ที่เป็นความลับโดยไม่ได้รับอนุญาต เป็นต้น

นอกจากนี้ มาตรา 59 ของร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ได้มีการกำหนดเกี่ยวกับมาตรการในการลงโทษเกี่ยวกับการกระทำความผิดทางระบบคอมพิวเตอร์ไว้ ซึ่งเป็นมาตรการต่อผู้ละเมิด “บุคคล นิติบุคคล หรือองค์กร ที่ละเมิดกฎหมายฉบับนี้ เช่น ข้อห้าม[125] จะถูกศึกษาอบรม กล่าวเตือน ลงวินัย ปรับ ใช้ค่าเสียหายหรือลงโทษทางอาญา แล้วแต่กรณีเบาหรือหนักตามที่ได้กำหนดไว้ในกฎหมายและระเบียบการ” ซึ่งในการกำหนดมาตรการดังกล่าวเป็นลักษณะของการปฏิบัติต่อบุคคล นิติบุคคลหรือองค์กร ที่ละเมิดกฎหมาย แต่ในขณะเดียวกันในการกำหนดมาตรการต่อผู้ละเมิดนั้น อาจเป็นการเปิดโอกาสให้ผู้กระทำความผิดไม่ได้รับโทษ เช่น มาตรา 60 ของร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... นี้ได้มีการบัญญัติมาตรการในการศึกษาอบรม “บุคคล นิติบุคคลหรือองค์กรที่ละเมิดกฎหมายฉบับนี้ ซึ่งเป็นการละเมิดครั้งแรก และก่อความเสียหาย

---

[125] ร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ..., มาตรา 41 ข้อห้าม “ห้ามบุคคล นิติบุคคลหรือองค์กรมีพฤติกรรม ดังนี้

1. มีพฤติกรรมที่ได้กำหนดไว้ในมาตรา ของกฎหมายฉบับนี้

2. ทำลายหรือสร้างความเสียหายให้แก่อุปกรณ์อิเล็กทรอนิกส์ คอมพิวเตอร์ และสิ่งอำนวยความสะดวกต่าง ๆ ในการแลกเปลี่ยนข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์

3. มีพฤติกรรมอื่นที่เป็นการละเมิดระเบียบกฎหมาย และระเบียบการ”.

ไม่มาก จะถูกศึกษาอบรมและกล่าวเตือน” จะเห็นได้ว่ามาตรการดังกล่าวยังไม่มีความชัดเจนเกี่ยวกับมาตรการลงโทษต่อผู้กระทำความผิดในรูปแบบต่าง ๆ กล่าวคือ บุคคลจะต้องรับโทษต่อเมื่อมีกฎหมายที่ใช้อยู่ในขณะกระทำบัญญัติให้ต้องรับโทษนั้น ๆ เช่น การกระทำความผิดที่มีแต่โทษปรับ ศาลก็ได้แต่ลงโทษปรับ ศาลจะลงโทษจำคุกซึ่งไม่ใช่โทษที่กฎหมายบัญญัติไว้ไม่ได้

นอกจากนี้มาตรา 44 ของร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ของ สปป.ลาว ยังได้มีการกำหนดเกี่ยวกับการสืบสวน-สอบสวนคดีทางระบบคอมพิวเตอร์ไว้ ซึ่งสาเหตุที่ทำให้ต้องมีการสืบสวน-สอบสวนคดีทางระบบคอมพิวเตอร์มีดังต่อไปนี้:

1. มีการแจ้งความ การรายงาน การร้องฟ้องของบุคคล นิติบุคคล หรือองค์กรเกี่ยวกับพฤติกรรมที่เป็นอาชญากรรมทางระบบคอมพิวเตอร์
2. มีการเข้ามอบตัวของผู้กระทำผิด และ
3. พบร่องรอย ข้อมูล หลักฐานของพฤติกรรมตามที่ได้กำหนดไว้ใน มาตรา 8 ของกฎหมายฉบับนี้

และมาตรา 45 ได้กำหนดขั้นตอนของการสืบสวน-สอบสวนคดีทางระบบคอมพิวเตอร์ให้ปฏิบัติ ดังนี้:

1. การแจ้งความ การรายงานหรือการร้องฟ้อง
2. การเปิดการสืบสวน-สอบสวน
3. การดำเนินการสืบสวน-สอบสวน และ
4. การสรุปการสืบสวน-สอบสวนและการประกอบสำนวนคดี

ซึ่งจะเห็นได้ว่าในร่างกฎหมายดังกล่าวไม่ได้มีการบัญญัติเกี่ยวกับอำนาจของพนักงานเจ้าหน้าที่สืบสวน-สอบสวนไว้เป็นการเฉพาะ

ดังนั้น จากการที่ สปป.ลาว ได้มีการตรากฎหมายออกมาบังคับใช้เกี่ยวกับการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... นี้ จะเห็นได้ว่าในการกำหนดฐานความผิดนั้นได้มีการจัดแบ่งพฤติกรรมของลักษณะของการกระทำที่เป็นอาชญากรรมทางคอมพิวเตอร์ไว้ และได้มีการกำหนดมาตรการลงโทษในบางกรณีที่เป็นการกระทำครั้งแรก และสร้างความเสียหายไม่มากให้สามารถยอมความกันได้ ทั้งนี้ จะเห็นว่าการกระทำความผิดทางคอมพิวเตอร์นี้ ยากที่จะประเมินค่าความเสียหายที่เกิดขึ้นนั้นได้อย่างทันท่วงที แต่เนื่องจากผลของการกระทำผิดหรือการก่อให้เกิดความเสียหายขึ้นนั้น อาจไม่เพียงแค่กระทบต่อบุคคลใดบุคคลหนึ่งเท่านั้น แต่อาจกระทบต่อสังคมหรือก่อให้เกิดความเสียหายทางเศรษฐกิจในวงกว้าง นอกจากนี้ ร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ยังกำหนดเกี่ยวกับการสืบสวน-สอบสวนของ

พนักงานเจ้าหน้าที่ให้เป็นไปตามกระบวนการทางอาญาทั่วไป ซึ่งการหาตัวผู้กระทำความผิดก็อาจทำไม่ได้ง่ายนัก และในบางครั้งก็อาจไม่รู้ว่าใครเป็นผู้เสียหาย อย่างไรก็ตาม เพื่อป้องกันไม่ให้อำนาจของพนักงานเจ้าหน้าที่เกิดผลกระทบกับผู้ให้บริการหรือสิทธิของประชาชนทั่วไปมากเกินไป ผู้เขียนเห็นว่าควรมีการกำหนดเงื่อนไขการใช้อำนาจไว้อย่างชัดเจนในกฎหมายด้วย เช่น การให้พนักงานเจ้าหน้าที่สามารถส่งหนังสือสอบถาม หรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดนั้นมาชี้แจ้งได้ การเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการ และการสั่งให้ส่งมอบข้อมูลของผู้ใช้บริการที่ผู้ให้บริการต้องจัดเก็บ เป็นต้น

## 4.3 สภาพปัญหาเกี่ยวกับการขาดมาตรการทางกฎหมายด้านอาชญากรรมทางคอมพิวเตอร์ของ สปป.ลาว

สืบเนื่องจากอาชญากรรมทางคอมพิวเตอร์รูปแบบใหม่นี้มีลักษณะการกระทำที่หลากหลายที่กฎหมายและหลักเกณฑ์ทั้งหลายที่มีอยู่ใน สปป.ลาว ยังมีช่องว่างในการกระทำทางคอมพิวเตอร์ที่มีความเป็นเทคนิค มีความสลับซับซ้อนกว่าการกระทำผิดทางอาญาทั่วไป จึงทำให้กฎหมายที่มีอยู่ดังที่ได้กล่าวมาในข้อ 4.2 ไม่สามารถบังคับใช้เพื่อลงโทษผู้กระทำผิดในบางกรณีนี้ได้ เนื่องจากลักษณะการใช้บังคับกฎหมายอาญามีหลักการสำคัญที่ว่า “ไม่มีความผิด ไม่มีโทษ ถ้าไม่มีกฎหมาย” (*Nullum crimen, nulla poena, sine lege*) หลักการนี้เป็นหลักเกณฑ์สากลเป็นที่ยอมรับกันโดยทั่วไปในนานาอารยประเทศ[126] สำหรับ สปป.ลาว หลักการดังกล่าวได้รับการรับรองโดยบัญญัติไว้ในมาตรา 2 ของกฎหมายอาญา ค.ศ. 2005 “บุคคลใดจะมีความรับผิดทางอาญาและจะถูกลงโทษทางอาญาได้ก็ต่อเมื่อบุคคลนั้นได้กระทำความผิดโดยเจตนา และโดยประมาทที่เป็นภยันตรายต่อสังคม ซึ่งได้บัญญัติไว้ในกฎหมายอาญาหรือกฎหมายฉบับอื่นของ สปป.ลาว ที่ได้กำหนดโทษทางอาญาและต้องมีคำพิพากษาของศาลเท่านั้น” ด้วยเหตุนั้น การกระทำของอาชญากรรมที่เกิดขึ้นจากการใช้งานเทคโนโลยีคอมพิวเตอร์ที่กระทำผิดต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ซึ่งการกระทำของอาชญากรรมทางคอมพิวเตอร์บางประเภทยังขาดกฎหมายรองรับถึงการกระทำ ดังนี้

1. การเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบเครือข่ายโดยไม่ได้รับอนุญาต ซึ่งการกระทำความผิดส่วนใหญ่จะเป็นการเข้าถึงระบบเครือข่ายหรือข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาตเข้าไปถึงฐานข้อมูลดังกล่าว สาเหตุที่ผู้บุกรุกสามารถเจาะระบบรักษาความปลอดภัยเข้าไป

---

[126] วิกรณ์ รักษ์ปวงชน, หน่วยที่ 3 การใช้บังคับกฎหมายอาญา, ใน *เอกสารการสอนชุดวิชา กฎหมายอาญา 1: ภาคบทบัญญัติทั่วไป หน่วยที่ 1-7*, (นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2548), 99.

ได้ก็เนื่องจากซอฟแวร์มีช่องโหว่ ผลก็คือ ผู้บุกรุกสามารถเข้ามาครอบครองการทำงานของเครื่องคอมพิวเตอร์ได้ จากนั้นก็ขึ้นอยู่กับผู้บุกรุกว่าจะกระทำการอันใดในระบบคอมพิวเตอร์

แม้ว่าการเจาะระบบคอมพิวเตอร์จะเป็นการบุกรุกประเภทหนึ่ง แต่ก็ไม่สามารถนำกฎหมายอาญา ค.ศ. 2005 มาปรับใช้ได้ เนื่องจากการบุกรุกผ่านทางระบบเครือข่าย โดยที่ผู้บุกรุกสามารถเจาะระบบคอมพิวเตอร์จากที่ใดก็ได้ ตราบเท่าที่มีระบบเครือข่ายเชื่อมโยงเข้าหากันได้ดังที่ได้อธิบายไว้แล้วในข้อ 4.2.1.1

2. การรบกวนการทำงานของระบบคอมพิวเตอร์ จากการโจมตีด้วย DDoS (Distributed Denial of Service) ซึ่งเป็นการโจมตีเครื่องคอมพิวเตอร์เป้าหมายด้วยการยิง Packet จำนวนมากจากคอมพิวเตอร์หลาย ๆ เครื่องโดยมีเครื่องคอมพิวเตอร์ในการควบคุมการโจมตีหนึ่งเครื่อง ส่งผลให้ระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตที่ตกเป็นเป้าหมายต้องหยุดชะงักการทำงานในทันที

3. การดักจับข้อมูลผ่านทางเครือข่ายคอมพิวเตอร์โดยไม่มีสิทธิ ซึ่งเป็นอีกวิธีการหนึ่งที่ผู้ก่ออาชญากรรมนิยมใช้ เพื่อดักจับรหัสผ่านของผู้ใช้งานและรหัสผ่านของโปรแกรมและอุปกรณ์ควบคุมเครือข่ายต่าง ๆ

อย่างไรก็ตามจากรูปแบบการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์ในปัจจุบัน ซึ่งได้เปลี่ยนแปลงไปอย่างรวดเร็ว จนทำให้กฎหมายที่มีอยู่ในปัจจุบันไม่เพียงพอที่จะนำมาปรับใช้เพื่อดำเนินคดีหาตัวผู้กระทำการดังกล่าวมาลงโทษได้ ประกอบกับอำนาจของพนักงานเจ้าหน้าที่ก็มีอย่างจำกัด จึงทำให้ไม่สามารถลงโทษผู้กระทำผิดอาชญากรรมทางคอมพิวเตอร์ได้อย่างทันท่วงที

**4.3.1 ปัญหาเกี่ยวกับการกำหนดฐานการกระทำความผิด**

ปัจจุบันเป็นที่ทราบกันโดยทั่วไปว่า เทคโนโลยีสารสนเทศได้กลายเป็นปัจจัยพื้นฐานที่สำคัญอย่างยิ่งต่อการพัฒนาเศรษฐกิจและสังคมของ สปป.ลาว ได้เข้าไปผูกพันกับกระแสการเปลี่ยนแปลงของเศรษฐกิจโลกมากยิ่งขึ้นอย่างหลีกเลี่ยงไม่ได้ จากความทันสมัยของระบบสารสนเทศส่งผลให้เกิดการบริการใหม่ ๆ ผ่านทางระบบคอมพิวเตอร์ เช่น บริการมัลติมีเดีย (Multimedia Service) บริการ Integrated Services Digital Network เป็นต้น ที่ได้รวมข้อมูล ภาพและเสียงไว้ในบริการเดียวกันทำให้อำนวยความสะดวก รวดเร็ว และน่าเชื่อถือแก่ผู้ใช้บริการให้สามารถนำไปใช้ประโยชน์ในด้านการทำงานและความบันเทิงในชีวิตประจำวันได้อย่างสะดวกสบาย

นอกจากนี้ปรากฏการณ์ทางด้านเทคโนโลยีสารสนเทศในปัจจุบัน เช่น การลักลอบนำข้อมูลสารสนเทศของผู้อื่นที่เก็บไว้ในคอมพิวเตอร์ไปใช้ประโยชน์ก่อนผู้เป็นเจ้าของที่แท้จริง หรือการที่บุคคลอื่นสามารถเข้าถึงคอมพิวเตอร์ และแก้ไขเปลี่ยนแปลงสารสนเทศที่เก็บในคอมพิวเตอร์

ย่อมส่งผลกระทบและทำให้ผู้เป็นเจ้าของเสียหาย[127] อย่างไรก็ตามในการกำหนดลักษณะความผิดและโทษเกี่ยวกับการกระทำอาชญากรรมทางคอมพิวเตอร์นั้น ต้องบัญญัติไว้เป็นลายลักษณ์ษรอย่างชัดแจ้ง โดยบัญญัติความผิดและโทษไว้ในขณะกระทำ และบทบัญญัตินั้นต้องชัดเจนปราศจากการคลุมเครือ[128] ด้วยเหตุที่ว่ามีจุดมุ่งหมายในการควบคุมหรือกำหนดความประพฤติของบุคคลในสังคม ซึ่งมีผลกระทบต่อสิทธิเสรีภาพ ชีวิต ร่างกาย และทรัพย์สินของประชาชน ในการกำหนดพฤติกรรมของบุคคลใดบุคคลหนึ่งเป็นพฤติกรรมที่เป็นความผิดและได้รับโทษ สาเหตุที่จะต้องบัญญัติกฎหมายอาญาไว้เนื่องจากการที่จะถือว่าการกระทำใดหรือการละเว้นการกระทำใดเป็นความผิดและประสงค์จะมิให้ประชาชนฝ่าฝืนก็ควรที่จะบัญญัติไว้อย่างชัดแจ้ง พร้อมทั้งกำหนดโทษทางอาญาไว้ด้วย หากประชาชนทราบแล้วยังฝ่าฝืนก็ให้ลงโทษผู้ฝ่าฝืนได้ หลักเกณฑ์นี้เป็นที่ยอมรับกันในนานาอารยประเทศจนกลายเป็นสุภาษิตกฎหมาย “ไม่มีความผิด ไม่มีโทษ ถ้าไม่มีกฎหมายบัญญัติไว้”[129] จากหลักเกณฑ์ของการบัญญัติกฎหมาย เมื่อนำรูปแบบการกระทำดังกล่าวมาปรับใช้กับฐานความผิดในลักษณะต่าง ๆ เข้ากับกฎหมายที่มีอยู่ในปัจจุบันจะเห็นได้ ดังนี้

4.3.1.1 การจารกรรมข้อมูลของบริษัท ข้อมูลของบุคคลต่าง ๆ ซึ่งเป็นการใช้เทคโนโลยีคอมพิวเตอร์เข้าถึงข้อมูลรหัสหรือจารกรรมข้อมูลของผู้ใช้บริการรายอื่นไป ซึ่งมาตรา 67 ของกฎหมายอาญา ค.ศ. 2005 การจารกรรม “บุคคลใดบุคคลหนึ่งได้เข้ารวมกลุ่มโดยมีอาวุธเพื่อโจมตี ทำลายโรงจักร โรงงาน สำนักงาน องค์การจัดตั้งทางสังคม หรือจับหรือฆ่าพนักงานประชาชน หรือปล้นเอาทรัพย์สมบัติของรัฐ ของส่วนรวม ของบุคคล เพื่อทำลายพื้นฐานความเป็นระเบียบเรียบร้อยของสังคม...” จากบทบัญญัติดังกล่าวจะเห็นได้ว่ามิได้ครอบคลุมถึงลักษณะของการกระทำความผิดในกรณีการจารกรรมข้อมูล เนื่องจากทรัพย์สินที่ถูกจารกรรมไปนั้นฐานข้อมูลที่เป็นทรัพย์สินนั้นจับต้องไม่ได้ เมื่อจารกรรมไปแล้วทรัพย์สินดังกล่าวก็ยังคงอยู่กับผู้ใช้บริการเดิมไม่ได้หายไป จึงทำให้กฎหมายอาญา ค.ศ. 2005 ไม่สามารถนำมาปรับใช้ได้ นอกจากกฎหมายอาญาแล้วร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... นั้นเกี่ยวกับการกระทำนี้ก็ยังไม่บัญญัติครอบครุมถึง

4.3.1.2 การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งเป็นการเข้าถึงในระดับกายภาพ ซึ่งผู้กระทำความผิดได้ใช้วิธีการใดวิธีการหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถเข้าถึง

---

[127] กองกรรมาธิการ สำนักงานเลขาธิการวุฒิสภา, *รายงานของคณะกรรมาธิการ การวิทยาศาสตร์ เทคโนโลยีและพลังงาน วุฒิสภา, พิจารณาศึกษาเรื่อง เทคโนโลยีสารสนเทศกับกฎหมายโทรคมนาคมในยุคโลกาภิวัตน์*, (กรุงเทพฯ: สำนักงานเลขาธิการวุฒิสภา, 2539), 74-76.

[128] วิกรณ์ รักษ์ปวงชน, หน่วยที่ 3 การใช้บังคับกฎหมายอาญา, 103.

[129] บุญเพราะ แสงเทียน, *กฎหมายอาญา 1 (ภาคบทบัญญัติทั่วไป) แนวประยุกต์*, 17-18.

ข้อมูลคอมพิวเตอร์ของผู้อื่นได้ มาตรา 104 ของกฎหมายอาญา ค.ศ. 2005 การล่วงละเมิดความลับส่วนตัว วรรคสอง “บุคคลใดหากได้ลักเปิดจดหมาย โทรเลข หรือเอกสารอื่น ๆ หรือลักฟังโทรศัพท์ของผู้อื่น ซึ่งเป็นการก่อความเสียหายแก่ผู้อื่น...” เมื่อนำตัวบทดังกล่าวมาประกอบกับการกระทำการเข้าถึงข้อมูลทางคอมพิวเตอร์แล้ว จะเห็นได้ว่าข้อมูลนั้นเป็นการเก็บหรือการส่งด้วยวิธีการทางคอมพิวเตอร์หรือวิธีทางอิเล็กทรอนิกส์ ซึ่งลักษณะข้อมูลดังกล่าวอาจเป็นรูปภาพ ภาพเคลื่อนไหว และเสียง เมื่อพิจารณาจากตัวบทแล้วจึงไม่เป็นความผิดตามมาตรานี้

4.3.1.3 การรบกวนข้อมูลคอมพิวเตอร์เพื่อนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าเกิดความเสียหายแก่ผู้อื่นหรือประชาชน เช่น การปลอมแปลงหน้าเว็บไซต์ให้ผู้ใช้เข้าใจผิดเพื่อขโมยข้อมูลของผู้ใช้ ซึ่งความผิดฐานปลอมแปลงเอกสาร ในมาตรา 161 ของกฎหมายอาญา ค.ศ. 2005 นั้น การปลอมแปลงเอกสารหรือการใช้เอกสารปลอม “บุคคลผู้ใดหากได้ปลอมแปลงเอกสาร ลายเซ็น ตราประทับ ได้ตัดหรือเพิ่มข้อความใดข้อความหนึ่งในเอกสาร ...” วรรคสาม “ในกรณีที่การปลอมแปลงเอกสารหรือการใช้เอกสารปลอมส่งผลเสียหายอย่างมากมาย...” ซึ่งเอกสารนั้นเป็นสิ่งที่มีรูปร่าง เพียงแต่แก้ไขข้อมูลในคอมพิวเตอร์จึงไม่สามารถตีความขยายรวมถึงว่าเป็นการปลอมแปลงเอกสาร เพราะข้อมูลคอมพิวเตอร์เป็นสิ่งที่ไม่มีรูปร่าง

จากการศึกษาพบว่า สปป.ลาว ขาดมาตรการกฎหมายรองรับกับรูปแบบของการกระทำอาชญากรรมทางคอมพิวเตอร์ จึงสามารถกล่าวได้ว่ากฎหมายที่ใช้บังคับอยู่ในปัจจุบันไม่สามารถนำมาใช้บังคับกับสภาพการณ์และแนวปฏิบัติในสังคมยุคข้อมูลข่าวสารได้อย่างถูกต้องและยุติธรรม

**4.3.2 ปัญหาเกี่ยวกับมาตรการในการลงโทษ**

เนื่องจาการลงโทษในทางอาญานั้นมีผลกระทบต่อชีวิต ร่างกาย สิทธิเสรีภาพ และทรัพย์สินของประชาชน เมื่อมีการกระทำความผิดเกิดขึ้นในสังคม ซึ่งเป็นการกระทำที่ส่งผลกระทบต่อความสงบสุขและความปลอดภัยของประชาชนในสังคม รัฐในฐานะเป็นผู้ปกครองจำเป็นจะต้องเข้าไปจัดการกับการกระทำความผิดดังกล่าว โดยอาศัยกฎหมายอาญาที่กำหนดให้การกระทำใดการกระทำหนึ่งมีความผิดและกำหนดโทษที่จะลงต่อผู้ที่ได้กระทำผิดกฎหมาย การลงโทษผู้กระทำความผิดนั้นมีอยู่ด้วยกันหลายวิธีและมีการพัฒนารูปแบบของการลงโทษตามยุคสมัย[130] โดยวัตถุประสงค์ของการลงโทษมีหลายประการด้วยกัน คือ

4.3.2.1 เพื่อเป็นการแก้แค้นทดแทน เป็นหลักการลงโทษที่เก่าแก่ที่สุด ทั้งนี้เป็นไปตามแนวความคิดที่ว่า ผู้ใดกระทำผิดการใดย่อมได้รับผลตอบแทนการกระทำนั้น การลงโทษเพื่อ

---

[130] สำนักกฎหมายนิติศาสตร์ขาดรัก, *กฎหมายอาญา: วัตถุประสงค์ของการลงโทษ*.

เป็นการแก้แค้นทดแทนนั้นจะได้ผลต่อเมื่อได้กระทำโดยรวดเร็วและรุนแรง มิฉะนั้นแล้วประชาชนก็อาจขาดความเชื่อมั่นในกระบวนการยุติธรรมของบ้านเมือง และอาจหาทางแก้แค้นผู้กระทำผิดด้วยตนเองก็ได้

4.3.2.2 เพื่อเป็นการข่มขู่ตัวผู้กระทำความผิดนั้นเองให้เกิดความเข็ดหลาบ ไม่กล้ากระทำความผิดซ้ำขึ้นอีก และเพื่อเป็นตัวอย่างให้คนทั่วไปเห็นว่าเมื่อกระทำผิดแล้วจะต้องได้รับโทษเพื่อคนทั่วไปที่ได้ทราบจะได้เกรงกลัว ไม่กล้ากระทำผิดขึ้น

4.3.2.3 เพื่อเป็นการคุ้มครองสังคมให้พ้นจากภยันตรายในระหว่างที่ผู้กระทำถูกตัดขาดจากสังคมไป โดยการลงโทษประหารชีวิต จำคุกตลอดชีวิต หรือจำคุกมีกำหนดเวลา เป็นการคุ้มครองมิให้ผู้กระทำผิดกลับมาทำร้ายหรือเป็นภยันตรายต่อสังคมอีกต่อไปหรือชั่วระยะเวลาหนึ่ง

4.3.2.4 เพื่อเป็นการปรับปรุงแก้ไขตัวผู้กระทำความผิดให้กลับตัวเป็นพลเมืองดีเพราะผู้ที่ถูกจำคุกส่วนมากจะต้องถูกปล่อยตัวกลับมาสู่สังคมอีกในวันใดวันหนึ่ง

ถ้าพิจารณาการลงโทษในแง่ของการปรับปรุงแก้ไขตัวผู้กระทำผิดแต่อย่างเดียว หรือในแง่ของการคุ้มครองสังคมให้ปลอดภัย ผลก็คือ เมื่อใดที่ผู้นั้นกลับตัวเป็นคนดีก็จะต้องปล่อยเขาให้พ้นโทษทันทีเพราะไม่มีเหตุใด ๆ ที่จะควบคุมตัวต่อไปอีกแล้ว แต่การปล่อยตัวดังกล่าวเป็นการขัดต่อทฤษฎีข่มขู่บุคคลอื่นและทฤษฎีแก้แค้นทดแทน เพราะหากกระทำความผิดร้ายแรงแต่เผอิญผู้กระทำความผิดกลับตัวเป็นคนดีอย่างแน่นอนแล้วจำต้องปล่อยก่อนกำหนดมาก ผลของการข่มขู่ก็ไม่มี การแก้แค้นทดแทนก็ไม่มี ด้วยเหตุนี้ การลงโทษจึงจะมุ่งเพื่อวัตถุประสงค์ประการหนึ่งประการใดแต่เพียงอย่างเดียวโดยไม่คำนึงถึงประการอื่น ๆ ไม่ได้ การลงโทษจะต้องมีความมุ่งหมายหลาย ๆ ประการประกอบกัน จะพิจารณาแง่หนึ่งแง่ใดโดยไม่คำนึงถึงจุดประสงค์อื่น ๆ ด้วยไม่ได้[131]

ด้วยเหตุนี้ ในมาตรา 27 แห่งกฎหมายอาญา ค.ศ. 2005 ของ สปป.ลาว ได้มีการบัญญัติเกี่ยวกับวัตถุประสงค์ของการลงโทษไว้ เพื่อกำหนดมาตรการในการลงโทษ กล่าวคือ “การลงโทษไม่เพียงแต่จะมีจุดประสงค์ลงโทษผู้กระทำผิดเท่านั้น แต่หากยังมีจุดประสงค์เพื่อปรับปรุงแก้ไขและศึกษาอบรมผู้ถูกลงโทษให้มีจิตใจบริสุทธิ์ต่อการออกแรงงาน ให้ปฏิบัติตามกฎหมายอย่างถูกต้อง และเคร่งครัด ให้เคารพระเบียบการดำรงชีวิตของสังคมพร้อมทั้งเป็นการป้องกันไม่ให้การกระทำผิดใหม่เกิดขึ้นสำหรับผู้ถูกลงโทษ และสำหรับบุคคลอื่นอีกด้วย การลงโทษไม่มีวัตถุประสงค์จะก่อความทุกข์ทรมานแก่ร่างกายหรือเหยียบย่ำเกียรติศักดิ์ศรีของมนุษย์” ตามหลักของกฎหมายอาญาแล้วไม่มีกฎหมายไม่มีความผิดไม่มีโทษ แต่ตามมาตรา 27 นี้หมายถึง การที่รัฐ

---

[131] เกียรติขจร วัจนะสวัสดิ์, *คำอธิบายกฎหมายอาญา ภาค 1 บทบัญญัติทั่วไป*, พิมพ์ครั้งที่ 10, (กรุงเทพฯ: พลสยาม, 2551), 846-848.

ทำให้ผู้กระทำความผิดต้องได้รับผลร้าย เพราะเหตุที่ผู้นั้นฝ่าฝืนกฎหมายทั้งนี้โดยมีเจตนาให้ผู้ที่ได้รับรู้ถึงว่าสิ่งนั้นเป็นผลเสีย โทษจึงเป็นลักษณะสำคัญประการหนึ่งของกฎหมายอาญา การกำหนดบทลงโทษต่ออาชญากรรมที่เกิดขึ้นจากการกระทำด้วยเทคโนโลยีคอมพิวเตอร์ ต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ซึ่งการกระทำความผิดของอาชญากรเป็นการกระทำความผิดรูปแบบใหม่ที่อาศัยความสลับซับซ้อนของระบบคอมพิวเตอร์ มักมีลักษณะ และพฤติกรรมที่ไม่รุนแรง ไม่ใช้อาวุธ ไม่ใช้กำลังทำร้าย ไม่ใช้วิธีเผชิญหน้าเหมือนความผิดฐานลักทรัพย์ ส่วนใหญ่จะเกิดขึ้นจากการนำคอมพิวเตอร์เข้ามาเกี่ยวข้องกับการกระทำความผิด

สืบเนื่องจากลักษณะของฐานการกระทำความผิดทางคอมพิวเตอร์ได้มีรูปแบบของการกระทำผิดแตกต่างจากการกระทำผิดทางอาญาทั่วไปใน สปป.ลาว จึงได้มีการรับรองกฎหมายว่าด้วยการต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์เพื่อรองรับรูปแบบของการกระทำความผิดดังกล่าว แต่เนื่องจากกฎหมายดังกล่าวได้มีการกำหนดมาตรการต่อผู้ละเมิดกฎหมายฉบับนี้จะถูกศึกษาอบรม กล่าวเตือน ลงวินัย ปรับ ใช้แทนค่าเสียหายหรือถูกลงโทษทางอาญา ซึ่งในการลงโทษนั้นให้ปฏิบัติตามแต่ละฐานความผิดที่ได้กำหนดไว้ในกฎหมายฉบับนี้ ในขณะเดียวกันลักษณะของการกระทำความผิดบางฐานยังไม่ได้มีการกำหนดไว้อย่างชัดเจน นอกจากนี้ในการบัญญัติเกี่ยวกับมาตรการลงโทษนั้นต้องชัดเจน กล่าวคือ บุคคลจะต้องรับโทษต่อเมื่อมีกฎหมายที่ใช้อยู่ในขณะกระทำบัญญัติให้ต้องรับโทษนั้น ๆ[132] จะเห็นได้ว่าหลัก “จะไม่มีความผิด ไม่มีโทษโดยไม่มีกฎหมาย” มีวัตถุประสงค์เพื่อป้องกันการใช้อำนาจตามอำเภอใจของผู้มีอำนาจของรัฐ ซึ่งหลักนี้เป็นหลักที่ว่าจะลงโทษบุคคลใดในทางอาญาได้นั้นก็ต่อเมื่อกฎหมายบัญญัติว่าการกระทำเช่นว่านั้นเป็นความผิดและกำหนดโทษด้วย แต่อย่างไรก็ตามกฎหมายที่มีอยู่ในปัจจุบันของ สปป.ลาว ยังได้เปิดโอกาสให้เจ้าหน้าที่ใช้ดุลพินิจในการลงโทษ เช่น การศึกษาอบรม การกล่าวเตือน ซึ่งมิได้กำหนดให้เป็นการแจ้งชัดว่าการกระทำความผิดทางคอมพิวเตอร์รูปแบบใดจะใช้มาตรการใดต่อผู้กระทำ จึงส่งผลให้การกำหนดโทษต่อผู้กระทำความผิดทางคอมพิวเตอร์กับลักษณะของฐานความผิดในการกระทำของอาชญากรรมยังไม่ครอบคลุม และไม่สอดคล้องกัน ทำให้ผู้กระทำความผิดมิได้รับการลงโทษจากการกระทำความผิดดังกล่าวเท่าที่ควร

### 4.3.3 ปัญหาเกี่ยวกับอำนาจของพนักงานเจ้าหน้าที่

การกระทำความผิดต่อข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ โดยการใช้เทคโนโลยีคอมพิวเตอร์ไปกระทำความผิด หากมีการกระทำความผิดเกิดขึ้นแล้วจะสามารถติดตามหาตัวผู้กระทำความผิดมาได้อย่างไรนั้นเนื่องจากปัจจุบันระบบคอมพิวเตอร์มีการเชื่อมโยงถึงกันเป็น

---

[132] หยุด แสงอุทัย, *ความรู้เบื้องต้นเกี่ยวกับกฎหมายทั่วไป*, 200.

เครือข่ายที่มีความสลับซับซ้อน จึงเป็นอุปสรรคสำคัญในการประติดประต่อข้อมูลจากพยานหลักฐานเพื่อไล่ล่าหาตัวผู้กระทำความผิดมาลงโทษ

ด้วยเหตุที่การกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีความยากต่อการตรวจพบ และยากต่อการพิสูจน์เพื่อนำตัวผู้กระทำความผิดมาลงโทษ อีกทั้งโดยลักษณะของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เองมีการกระทำได้อย่างรวดเร็วและอาจส่งผลกระทบให้เกิดความเสียหายในวงกว้าง[133] ด้วยเหตุนี้จึงจำเป็นต้องมีการบัญญัติอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ไว้เป็นกรณีพิเศษเพื่อให้สามารถรวบรวมพยานหลักฐานได้ทันการกับลักษณะของการกระทำความผิด

นอกจากนี้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการสืบสวน-สอบสวนหาตัวผู้กระทำความผิดมาลงโทษเป็นไปด้วยความยากลำบาก เพราะต้องใช้ข้อมูลทางอิเล็กทรอนิกส์ซึ่งสูญหายและถูกทำลายได้โดยง่าย เป็นเครื่องช่วยในการค้นหาแหล่งที่มาและตัวผู้กระทำความผิด และในบางครั้งการสืบสวน-สอบสวนจำต้องกระทำโดยทันทีเมื่อพบการกระทำความผิด เพราะหากเนิ่นช้าผู้กระทำความผิดสามารถลบร่องรอยในการเข้าสู่ระบบทำให้ไม่สามารถหาตัวผู้กระทำความผิดได้

การกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นเรื่องใหม่ในสังคมลาว ฉะนั้นเมื่อเกิดการกระทำความผิดขึ้นผู้ได้รับผลเสียหายจึงประสบกับปัญหาว่าจะต้องร้องทุกข์กล่าวโทษต่อหน่วยงานใดของรัฐ ซึ่งเป็นเรื่องที่สร้างความสับสนให้แก่ผู้ประสบปัญหาดังกล่าว ประกอบกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นเรื่องที่ต้องการความรวดเร็วในการเข้าจัดการ หากรอให้มีการดำเนินการร้องทุกข์ต่อพนักงานสอบสวนเช่นเดียวกับการดำเนินคดีอาญาโดยทั่วไปแล้ว ย่อมไม่สามารถยับยั้งความเสียหายที่เกิดขึ้นได้ทันท่วงที

ใน สปป.ลาว ได้มีการกำหนดเกี่ยวกับการเริ่มต้นการดำเนินคดีอาญา โดยเริ่มจากการสืบสวน-สอบสวน[134] ซึ่งเป็นขั้นตอนที่อยู่ในความรับผิดชอบขององค์การสืบสวน-สอบสวนของตำรวจ[135] ที่เป็นขั้นตอนในการแสวงหาพยานหลักฐานที่กระทำผิดและหาตัวผู้กระทำความผิดมาลงโทษ ด้วยเหตุนี้มาตรา 54 ของกฎหมายว่าด้วยการดำเนินคดีอาญา ค.ศ. 2012 ได้ให้สิทธิและกำหนดหน้าที่ของเจ้าพนักงานสืบสวน-สอบสวน “รับและบันทึกแจ้งความ การรายงานหรือการร้องทุกข์เกี่ยวกับการกระทำความผิดทางอาญา เสนอออกหมายเรียก ออกคำสั่งพาตัว คำสั่งกักตัว

---

[133] มานิตย์ จุมปา, *คำอธิบายกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์*, 123.

[134] กฎหมายว่าด้วยการดำเนินคดีอาญา ค.ศ. 2012, มาตรา 45 องค์การดำเนินคดีอาญาประกอบด้วยองค์การสืบสวน-สอบสวน องค์การอัยการ และศาล.

[135] องค์การสืบสวน-สอบสวน ตามกฎหมายว่าด้วยการดำเนินคดีอาญา ค.ศ. 2012 มาตรา 46 มีดังนี้ องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ เจ้าหน้าที่ทหาร เจ้าหน้าที่ภาษี เจ้าหน้าที่ป่าไม้ เจ้าหน้าที่ด้านการฉ้อราษฎร์บังหลวง เจ้าหน้าที่จากหน่วยงานอื่น ๆ ตามที่ได้กำหนดไว้ในกฎหมาย.

คำสั่งควบคุมตัวอยู่กับที่ คำสั่งยึดหรืออายัดทรัพย์ คำสั่งปล่อยตัวผู้ที่ถูกสงสัยที่ถูกกักตัว หาตัวผู้กระทำความผิด..." การจะดำเนินการสืบสวน-สอบสวนในทางอาญาได้จะเริ่มจากมีคำแจ้งความของผู้เสียหาย มีการเข้ามอบตัวของผู้กระทำความผิด และพบเห็นรองรอยของการกระทำความผิด แต่ในการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์ก็เป็นการกระทำผิดทางอาญาประเภทหนึ่งเช่นกัน แต่เนื่องจากการกระทำผิดนั้นเป็นความผิดที่พิเศษมีลักษณะซับซ้อน แล้วในกฎหมายอาญาก็ไม่ได้มีการบัญญัติครอบคลุมถึง เมื่อกฎหมายอาญาไม่ได้มีการบัญญัติครอบคลุมถึงแล้ว เจ้าพนักงานตามกฎหมายว่าด้วยการดำเนินคดีอาญา ค.ศ. 2012 ก็จะไม่มีอำนาจในการสอบสวนคดีความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

นอกจากนี้ กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2012 มีวัตถุประสงค์ในการควบคุมการดำเนินธุรกรรมทางอิเล็กทรอนิกส์เป็นส่วนใหญ่ ไม่ได้มุ่งที่จะลงโทษการกระทำความผิดทางอาชญากรรมทางคอมพิวเตอร์โดยตรง ซึ่งในการบังคับใช้กฎหมายได้ให้อำนาจแก่รัฐบาลเป็นผู้บังคับใช้กฎหมายงานธุรกรรมทางอิเล็กทรอนิกส์อย่างรวมศูนย์ และเป็นเอกภาพ โดยมอบให้กระทรวงวิทยาศาสตร์และเทคโนโลยี เป็นผู้คุ้มครองดูแลโดยตรง โดยมีสิทธิและหน้าที่ในการกำหนดนโยบายศึกษาค้นคว้า ปรับปรุงกฎหมาย โฆษณาเผยแพร่ พิจารณาเกี่ยวกับมาตรฐานและวิธีการเพื่อป้องกันและแก้ไขปัญหาที่อาจเกิดขึ้นในการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ อย่างไรก็ตามในกฎหมายฉบับนี้ยังไม่ได้มีการบัญญัติเกี่ยวกับการให้พนักงานเจ้าหน้าที่มีสิทธิในการดำเนินการสืบสวน-สอบสวนหาตัวผู้กระทำความผิดได้

ต่อมา ได้มีการออกดำรัฐว่าด้วยการคุ้มครองข้อมูลข่าวสารผ่านอินเทอร์เน็ต ค.ศ. 2015 ให้มีหน่วยงานในการคุ้มครองข้อมูลข่าวสารผ่านอินเทอร์เน็ต แต่ในดำรัฐฉบับนี้ไม่ได้บัญญัติเกี่ยวกับการให้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ไว้อย่างชัดเจน[136] จึงทำให้พนักงานเจ้าหน้าที่ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ ประกอบกับทั้งในการปฏิบัติหน้าที่ของเจ้าหน้าที่สอบสวนต้องปฏิบัติตามกฎหมายว่าด้วยการดำเนินคดีอาญา ค.ศ. 2005 เช่น การออกหมายค้น หมายจับ หมายขัง เป็นต้น ที่จะต้องมีการประสานงานกับอัยการ แต่จะเห็นได้ว่ามีกระบวนการและขั้นตอนที่มากเกินไปก่อให้เกิดความล่าช้าในการหาตัวผู้กระทำความผิดทางคอมพิวเตอร์ได้

---

[136] ดำรัฐว่าด้วยการคุ้มครองข้อมูลข่าวสารผ่านอินเทอร์เน็ต, มาตรา 20 ความรับผิดชอบของแขนงการป้องกันความสงบ (เจ้าหน้าที่ตำรวจ) "1) รับแจ้งความจากบุคคล นิติบุคคล และองค์กรในกรณีมีการกระทำผิดที่เกี่ยวพันธ์ถึงความมั่นคงของชาติ และความเป็นระเบียบเรียบร้อยของสังคม 2) รวยรวม ตรวจตรา และค้นคว้าวิจัยข้อมูลข่าวสารผ่านอินเทอร์เน็ต ที่มีลักษณะคุกคามถึงความมั่นคงของชาติ ความลับของชาติ และความสงบสุขของสังคม และ 3) สืบสวน-สอบสวน และดำเนินคดีต่อผู้กระทำผิด".

นอกจากนั้น ยังมีร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ซึ่งมีวัตถุประสงค์ในการกำหนดหลักการ และมาตรการเกี่ยวกับการคุ้มครอง ติดตามตรวจตรางานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ และได้มีการกำหนดฐานความผิด มาตรการในการลงโทษต่อผู้ที่ละเมิดกฎหมายดังกล่าว และได้มีการกำหนดหน่วยงานที่รับผิดชอบเกี่ยวกับงานต้านและสกัดกั้นอาชญากรรมทางคอมพิวเตอร์ และการดำเนินการสืบสวน-สอบสวนคดีทางระบบคอมพิวเตอร์ แต่มิได้มีการกำหนดเกี่ยวกับการให้อำนาจหน้าที่แก่พนักงานเจ้าหน้าที่ไว้เป็นการเฉพาะ กล่าวคือให้ปฏิบัติตามกฎหมายว่าด้วยการดำเนินคดีอาญาทั่วไป

จากการศึกษาพบว่าการดำเนินกระบวนการยุติธรรมที่เกี่ยวข้องกับการสืบสวน-สอบสวน การกระทำความผิดทางคอมพิวเตอร์ใน สปป.ลาว ในปัจจุบันจะเห็นได้ว่ามีขั้นตอนในการดำเนินงานของเจ้าหน้าที่ตำรวจบางกรณีต้องรายงานเป็นหนังสือเสนอต่อหน่วยงานที่มีความเชี่ยวชาญคือศูนย์อินเทอร์เน็ตแห่งชาติ กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสารเพื่อสนองข้อมูลเกี่ยวกับการกระทำผิดของอาชญากรได้ จึงจะสามารถดำเนินการสืบสวน-สอบสวนหาข้อมูลหลักฐานได้ อันเป็นการใช้ระยะเวลาในการดำเนินการสอบสวนที่นานไม่ทันต่อรูปแบบของการกระทำความผิดและไม่สามารถนำผู้กระทำผิดมาลงโทษได้อย่างทันท่วงที

## 4.4 ศึกษาเปรียบเทียบมาตรการทางกฎหมายที่เหมาะสมเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของ สปป.ลาว ในอนาคต

ในการนำหลักเกณฑ์ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มาใช้ในกฎหมายของ สปป.ลาว เพื่อต้องการสร้างหลักคุ้มครองให้แก่ผู้ใช้งานคอมพิวเตอร์ในการทำกิจกรรมต่าง ๆ และเพื่อกำหนดฐานความผิดเกี่ยวกับการกระทำอาชญากรรมทางคอมพิวเตอร์ ให้มีความชัดเจน และเป็นสากลสอดคล้องกับยุคสมัยมากยิ่งขึ้น

ในปัจจุบัน สปป.ลาว ได้เกิดปัญหาเกี่ยวกับการใช้ระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด เช่น ในกรณีที่มีการเข้าถึงข้อมูลคอมพิวเตอร์ การดักรับข้อมูลคอมพิวเตอร์ การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ เป็นต้น ด้วยเหตุนี้ในกองประชุมสมัยสามัญครั้งที่ 9 ของสภาแห่งชาติ ชุดที่ 7 จึงได้มีมติฉบับเลขที่ 09/สภช. ลงวันที่ 21 กรกฎาคม ค.ศ. 2015 ของสภาแห่งชาติ แห่ง สปป.ลาว ว่าด้วยการรับรองกฎหมาย 3 ฉบับ ซึ่งหนึ่งในนั้นมีกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ เพื่อใช้เป็นเครื่องมือในการลงโทษต่อผู้กระทำการใด ๆ ต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ และอีกประการหนึ่งก็เพื่อสร้างมาตรการแนวทางปฏิบัติให้แก่ผู้ใช้งานเครื่องคอมพิวเตอร์ให้อยู่ในกฎกติกา

การใช้งาน เพื่อคุ้มครองสิทธิส่วนบุคคล แต่ในกฎหมายดังกล่าวยังไม่มีการกำหนดถึงการกระทำในลักษณะใดบ้างที่จะเป็นความผิด เพื่อเป็นบรรทัดฐานในการปฏิบัติหน้าที่ของเจ้าพนักงานต่อผู้กระทำความผิดทางคอมพิวเตอร์ ดังนี้

1. การกำหนดฐานความผิดต่าง ๆ ในการกระทำต่อข้อมูลคอมพิวเตอร์ให้ครอบคลุมถึงลักษณะของการกระทำของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

2. การกำหนดโทษแต่ละฐานความผิดที่ชัดเจน

3. การบัญญัติให้อำนาจแก่พนักงานเจ้าหน้าที่ ผู้ที่มีความชำนาญ เพื่อปฏิบัติหน้าที่ให้มีประสิทธิภาพ

ดังนั้น ถ้าหาก สปป.ลาว ได้นำเอาหลักเกณฑ์หรือมาตรการเกี่ยวกับการกระทำความผิดด้านคอมพิวเตอร์ของต่างประเทศมาบัญญัติไว้ดังที่จะได้กล่าวต่อไปนี้ ผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ก็จะได้รับโทษตามความเหมาะสมของการกระทำความผิด เพราะมีกฎหมายบัญญัติให้การกระทำดังกล่าวเป็นความผิด

**4.4.1 ฐานความผิด**

จากการใช้เทคโนโลยีทางคอมพิวเตอร์ที่ทันสมัยในการกระทำการอย่างใดอย่างหนึ่งซึ่งก่อให้เกิดความเสียหายแก่ความมั่นคงปลอดภัยของระบบสารสนเทศ ย่อมถือเป็นการกระทำผิดอาชญากรรมทางคอมพิวเตอร์ อันมีผลกระทบต่อความมั่นคง เศรษฐกิจ และสังคม ซึ่งปัญหาอาชญากรรมทางคอมพิวเตอร์นี้ ใน สปป.ลาว ได้ตระหนักถึงผลกระทบดังกล่าวจึงได้มีการจัดทำกฎหมายขึ้นเพื่อป้องกันและปราบปรามผู้ก่ออาชญากรรม คือ “ร่างกฎหมายว่าด้วยการกระทำผิดทางระบบคอมพิวเตอร์ ค.ศ. ...” ต่อมาได้มีการปรับเปลี่ยนชื่อเป็น “กฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ...” โดยกฎหมายดังกล่าวนี้ ในปัจจุบันได้มีมติรับรองจากสภาแห่งชาติแห่ง สปป.ลาว แล้วเมื่อวันที่ 21 กรกฎาคม ค.ศ. 2015[137] แต่ยังอยู่ในขั้นตอนของการเรียบเรียง แต่ยังไม่มีผลบังคับใช้จนกระทั่งมีรัฐบัญญัติของประธานประเทศประกาศใช้และลงตีพิมพ์จดหมายเหตุทางราชการ

อย่างไรก็ตาม เพื่อให้กฎหมายอาชญากรรมทางคอมพิวเตอร์ที่จะเกิดมีขึ้นใน สปป.ลาว มีความสมบูรณ์ และสามารถบังคับใช้ได้อย่างมีประสิทธิภาพ ผู้เขียนจึงได้ศึกษาวิเคราะห์ถึงฐานความผิดต่าง ๆ ที่สำคัญ ดังนี้

---

[137] มติกลงของสภาแห่งชาติแห่ง สปป. ลาว ว่าด้วยการรับรองกฎหมาย 3 ฉบับ, ฉบับเลขที่ 09/สภช, ลงวันที่ 7 กรกฎาคม ค.ศ. 2015.

1. สปป.ลาว

ตามมาตรา 8 ของร่างกฎหมายว่าด้วยการกระทำผิดทางระบบคอมพิวเตอร์ ค.ศ. ... ได้มีการกำหนดฐานการกระทำความผิดอาชญากรรมคอมพิวเตอร์ ดังนี้

1) การเข้าถึงระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต
2) การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์
3) การดักสกัดเอาข้อมูลคอมพิวเตอร์ โดยไม่ได้รับอนุญาต
4) การทำลายข้อมูลในระบบคอมพิวเตอร์
5) การรบกวนระบบคอมพิวเตอร์
6) การปลอมแปลงข้อมูลทางระบบคอมพิวเตอร์
7) การผลิตเครื่องมือกระทำผิดทางระบบคอมพิวเตอร์
8) การเผยแพร่สื่อลามก
9) การตัดต่อรูปภาพ ภาพเคลื่อนไหวและเสียง
10) การกระทำผิดเกี่ยวกับสื่อสังคมออนไลน์

และตามมาตรา 8 ของกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ได้มีการกำหนดฐานการกระทำความผิดอาชญากรรมทางระบบคอมพิวเตอร์แก้ไขเพิ่มเติมดังนี้

1) การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์
2) การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต
3) การตัดต่อเนื้อหา รูปภาพ ภาพเคลื่อนไหวและเสียงโดยไม่ได้รับอนุญาต
4) การดักรับข้อมูลในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต
5) การสร้างความเสียหายผ่านสื่อออนไลน์
6) การเผยแพร่สิ่งลามกผ่านระบบคอมพิวเตอร์
7) การรบกวนระบบคอมพิวเตอร์
8) การปลอมแปลงข้อมูลคอมพิวเตอร์
9) การทำลายข้อมูลคอมพิวเตอร์
10) การดำเนินกิจการเกี่ยวกับเครื่องมืออาชญากรรมทางระบบคอมพิวเตอร์
11) การใช้ระบบคอมพิวเตอร์ในการก่อการร้าย
12) การเล่นการพนันที่ต้องห้ามผ่านระบบคอมพิวเตอร์

2. ประเทศสิงคโปร์

ประเทศสิงคโปร์เป็นประเทศหนึ่งที่ได้มีการตรากฎหมายขึ้นบังคับใช้ เพื่อป้องกันและปราบปรามผู้ก่ออาชญากรรมทางคอมพิวเตอร์ โดยกฎหมายที่ตราขึ้นนี้ชื่อว่า “พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทางคอมพิวเตอร์ ค.ศ. 2007[138]” ซึ่งพระราชบัญญัติดังกล่าวได้มีการกำหนดฐานความผิดไว้ในกรณีต่าง ๆ ดังนี้

1) การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต (มาตรา 3)

2) การเข้าถึงด้วยเจตนาในการกระทำความผิดหรือพยายามกระทำความผิด (มาตรา 4)

3) การดัดแปลงแก้ไขข้อมูลคอมพิวเตอร์ (มาตรา 5)

4) การใช้หรือดักจับข้อมูลบริการคอมพิวเตอร์โดยไม่ได้รับอนุญาต (มาตรา 6)

5) การเข้าขัดขวางการใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต (มาตรา 7)

6) การเปิดเผยรหัสเชื่อมต่อโดยไม่ได้รับอนุญาต (มาตรา 8)

7) การสนับสนุนการกระทำความผิดและพยายามกระทำความผิด (มาตรา 10)

3. ประเทศไทย

ประเทศไทยได้มีการประกาศใช้พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. 2550 เพื่อป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ในประเทศ ซึ่งพระราชบัญญัติดังกล่าวได้บัญญัติฐานความผิดไว้ ดังนี้

1) การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5)

2) การล่วงรู้มาตรการป้องกันการเข้าถึง และนำไปเปิดเผยโดยมิชอบ (มาตรา 6)

3) การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7)

4) การดักข้อมูลระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 8)

5) การรบกวนข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 9)

6) การรบกวนระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 10)

7) การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูล การจำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด (มาตรา 11)

8) การจำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด (มาตรา 13)

9) การปลอมแปลงข้อมูลคอมพิวเตอร์หรือเผยแพร่เนื้อหาที่ไม่เหมาะสม (มาตรา 14)

---

[138] Computer Misuse and Cybersecurity Act 2007, Part 2 Offences.

ในการกำหนดฐานความผิดจะเห็นได้ว่าฐานการกระทำความผิดตามร่างกฎหมายว่าด้วยการกระทำความผิดทางระบบคอมพิวเตอร์ ค.ศ. ... หรือกฎหมายว่าด้วยการต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ของ สปป.ลาว ยังมีความไม่ครอบคลุม และในบางลักษณะของการกระทำก็มิได้มีการบัญญัติไว้ ในขณะที่ฐานความผิดตามกฎหมายของประเทศสิงคโปร์ และไทยมีความชัดเจนครอบคลุมกว่า ส่วนหนึ่งเนื่องจากประเทศสิงคโปร์ และไทยตรากฎหมายขึ้นบังคับเป็นเวลาพอสมควรแล้ว และได้มีการศึกษากฎหมายต่างประเทศและระหว่างประเทศที่เกี่ยวข้องในเชิงเปรียบเทียบเพื่อเป็นแนวทาง ทำให้กฎหมายมีความทันสมัยและชัดเจนที่จะบังคับใช้ได้อย่างมีประสิทธิภาพ ด้วยเหตุนี้ผู้เขียนจึงได้ทำการวิเคราะห์ฐานความผิดของทั้ง 3 ประเทศ เฉพาะในฐานความผิดที่ร่างกฎหมายของ สปป.ลาว ยังไม่ครอบคลุม และไม่มีบัญญัติไว้ ดังนี้

4.4.1.1 ฐานความผิดเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์

1. สปป.ลาว

ตามร่างกฎหมายว่าด้วยการกระทำผิดทางระบบคอมพิวเตอร์ ค.ศ. ... หรือร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ยังไม่ได้บัญญัติถึงรูปแบบของการกระทำความผิดเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต ซึ่งการกระทำดังกล่าวเป็นการเข้าถึงข้อมูลคอมพิวเตอร์ที่มีการป้องกันมิให้บุคคลอื่นใช้ ที่ผู้กระทำความผิดดำเนินการด้วยวิธีการใดวิธีการหนึ่งเพื่อล่วงรู้ข้อมูลที่ตนเองต้องการ กล่าวคือ การเข้าไปถึงข้อมูลอย่างใดอย่างหนึ่งที่อยู่ในระบบคอมพิวเตอร์ รวมทั้งชุดคำสั่งด้วยหากอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้

2. ประเทศสิงคโปร์

ตามมาตรา 3 ของพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทางคอมพิวเตอร์ ค.ศ. 2007 การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งบุคคลใดก็ตามที่เจตนาใช้คอมพิวเตอร์เพื่อวัตถุประสงค์ในการเข้าถึง โดยไม่ได้รับอนุญาต ซึ่งข้อมูลคอมพิวเตอร์หรือโปรแกรมที่อยู่ในคอมพิวเตอร์ใด ๆ ที่มีการป้องกันการเข้าถึงโดยเฉพาะถือว่ามีความผิด[139] ถึงแม้ว่าการกระทำดังกล่าวจะเป็นการกระทำเพื่อการเข้าถึงคอมพิวเตอร์และระบบคอมพิวเตอร์ สำหรับวัตถุประสงค์ของส่วนนี้ ให้ถือว่ามาตราต่าง ๆ นั้นไม่ได้มุ่งถึงโปรแกรมหรือข้อมูลใดโดยเฉพาะ โปรแกรมหรือข้อมูลชนิดใด ๆ หรือโปรแกรมหรือข้อมูลในคอมพิวเตอร์เครื่อง

---

[139] Computer Misuse and Cybersecurity Act 2007, nauthorised Access to Computer Material 3. "(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer…".

ใด ๆ โดยเฉพาะ ซึ่งวัตถุประสงค์มุ่งการคุ้มครองข้อมูลทางคอมพิวเตอร์เพื่อไม่ให้มีการกระทำอย่างใดอย่างหนึ่งต่อข้อมูลดังกล่าว

3. ประเทศไทย

การกำหนดเกี่ยวกับฐานความผิดการเข้าถึงข้อมูลทางคอมพิวเตอร์ในมาตรา 7 ของพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ได้มีการบัญญัติการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน...” ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ ซึ่งหมายถึงข้อมูลนั้นเป็นการเก็บหรือส่งด้วยวิธีการทางคอมพิวเตอร์หรือวิธีการทางอิเล็กทรอนิกส์[140] ซึ่งไม่ได้หมายความถึงระบบคอมพิวเตอร์ เพราะระบบคอมพิวเตอร์ไม่สามารถเก็บหรือส่งได้

ผู้เขียนเห็นว่าการกระทำของบุคคลใดบุคคลหนึ่งในการเข้าถึงข้อมูลคอมพิวเตอร์ อาจก่อให้เกิดผลเสียหายแก่เจ้าของข้อมูลได้ ซึ่งการเข้าถึงดังกล่าวที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูล หากเพียงเพื่อเข้าไปล่วงรู้ความลับบางอย่างของข้อมูลคอมพิวเตอร์ที่อยู่ในระบบคอมพิวเตอร์ของผู้อื่นนั้น ก็ถือว่ามีความผิดแล้ว เช่น การเข้าไปล่วงรู้ความลับของคู่แข่งทางด้านการค้าการลงทุน หรือเข้าไปถึงข้อมูลการเก็บรักษาผู้ป่วยหรือเข้าถึงความลับของทางราชการย่อมส่งผลกระทบต่อการรักษาความมั่นคงของชาติได้

4.4.1.2 ฐานความผิดเกี่ยวกับการรบกวนข้อมูลคอมพิวเตอร์

1. สปป.ลาว

ตามมาตรา 12 ของร่างกฎหมายว่าด้วยการกระทำผิดทางระบบคอมพิวเตอร์ ค.ศ. ... ได้กำหนดการทำลายข้อมูลในระบบคอมพิวเตอร์ “การทำลายข้อมูลในระบบคอมพิวเตอร์ หมายถึง การลบ การดัดแปลงข้อมูลคอมพิวเตอร์ การทำให้ข้อมูลเสียหายและการเปลี่ยนแปลงข้อมูล เพื่อสร้างความเสียหายให้แก่ระบบคอมพิวเตอร์” และตามมาตรา 17 ของร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... การทำลายข้อมูลคอมพิวเตอร์ “การทำลายข้อมูลคอมพิวเตอร์ หมายถึง การลบ การดัดแปลงแก้ไข และการปลอมแปลงข้อมูลคอมพิวเตอร์หรือข้อมูลในระบบคอมพิวเตอร์ เพื่อทำให้ข้อมูลหรือระบบคอมพิวเตอร์นั้นเสียหาย” จากรูปแบบของความหมายการกระทำดังกล่าวจะเห็นได้ว่าการกระทำต่อข้อมูลคอมพิวเตอร์ ซึ่งอาจส่งผลให้เกิดความเสียหายแก่เจ้าของข้อมูลดังกล่าวได้ โดยในมาตรานี้

---

[140] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ พ.ศ. 2550.*

ไม่ได้ระบุว่าสร้างความเสียหายให้แก่ข้อมูลคอมพิวเตอร์หรือข้อมูลในระบบคอมพิวเตอร์ของผู้อื่น ซึ่งหากผู้เป็นเจ้าของข้อมูลเองได้มีการกระทำให้ข้อมูลของตนเกิดความเสียหาย ในมาตรานี้อาจสามารถตีความขยายความถึงได้ เช่น การลบข้อมูลหรือการดัดแปลงข้อมูลที่ก่อให้เกิดความเสียหายแก่ข้อมูลของตนเอง เป็นต้น

2. ประเทศสิงคโปร์

มาตรา 5 พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทางคอมพิวเตอร์ ค.ศ. 2007 ได้กำหนดว่า การดัดแปลงแก้ไขข้อมูลคอมพิวเตอร์ ซึ่งบุคคลใดกระทำการใด ๆ โดยมิชอบ ซึ่งรู้ว่าจะทำให้เกิดการดัดแปลงแก้ไขเนื้อหาใด ๆ ของคอมพิวเตอร์ เป็นการกระทำผิด[141] อย่างไรก็ตาม การดัดแปลงแก้ไขข้อมูลคอมพิวเตอร์ในกรณีที่จำเป็นแก่การใช้ เช่น ผู้ใช้สามารถดัดแปลงโปรแกรมคอมพิวเตอร์เท่าที่จำเป็น แต่ในกรณีนี้การดัดแปลงที่ก่อให้เกิดความเสียหายไม่ว่าจะเป็นการดัดแปลงเป็นการถาวรหรือเป็นการชั่วคราวก็ถือว่าเป็นการกระทำผิด

3. ประเทศไทย

การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบตามมาตรา 9 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้บัญญัติว่า “ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ...” ซึ่งความผิดตามมาตรา 9 นี้มุ่งคุ้มครองความถูกต้องของข้อมูล (Integrity) ความถูกต้องแท้จริง (Authentication) และเสถียรภาพหรือความพร้อมในการใช้งานหรือการใช้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่บันทึกเก็บไว้บนสื่อคอมพิวเตอร์ได้อย่างเป็นปกติ เป็นการกำหนดขึ้นเพื่อให้ข้อมูลคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ได้รับความคุ้มครองเพื่อป้องกันการกระทำความผิด เช่น การป้อนโปรแกรมที่มีไวรัสทำลายข้อมูลหรือโปรแกรมคอมพิวเตอร์ หรือการป้อน Trojan Horse เข้าไปในระบบเพื่อขโมยรหัสผ่านของผู้ใช้คอมพิวเตอร์สำหรับเพื่อเข้าไปลบ เปลี่ยนแปลงแก้ไขข้อมูลหรือกระทำการใด ๆ อันเป็นการรบกวนข้อมูล

ผู้เขียนเห็นว่าการรบกวนข้อมูลคอมพิวเตอร์นั้นเป็นการกระทำของบุคคลอื่นที่การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาตเพื่อการแก้ไข เปลี่ยนแปลง เพิ่มเติม ซึ่งข้อมูลคอมพิวเตอร์ที่ทำให้ข้อมูลคอมพิวเตอร์นั้นเสียหายหรือเปลี่ยนแปลงไปจากรูปแบบเดิมของข้อมูลที่เป็นของผู้อื่น ไม่ได้หมายรวมถึงการกระทำต่อข้อมูลของตนเอง ตามหลักการของการ

---

[141] Computer Misuse and Cybersecurity Act 2007, Unauthorised modification of computer material 5, “(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer …”.

บัญญัติกฎหมายอาญาแล้ว ต้องมีการบัญญัติไว้อย่างชัดเจนถึงรูปแบบของการกระทำนั้นเป็นการกระทำผิดหรือไม่

4.4.1.3 ฐานความผิดเกี่ยวกับการรบกวนระบบคอมพิวเตอร์

1. สปป.ลาว

มาตรา 13 ของร่างกฎหมายว่าด้วยการกระทำผิดทางระบบคอมพิวเตอร์ ค.ศ. ... ได้กำหนดเกี่ยวกับการรบกวนระบบคอมพิวเตอร์ ไว้ดังนี้ “การรบกวนระบบคอมพิวเตอร์ หมายถึง การกระทำ ดังต่อไปนี้

1) การขัดขวาง ซึ่งทำให้ระบบคอมพิวเตอร์อย่างใดอย่างหนึ่ง ไม่ปฏิบัติการปฏิบัติการช้าลง หรือไม่สามารถปฏิบัติการได้อย่างเป็นปกติ

2) การส่งข้อมูลระบบคอมพิวเตอร์ หรือจดหมายทางอิเล็กทรอนิกส์ โดยมีการปกปิดที่อยู่หรือแหล่งที่มาของการส่งข้อมูลดังกล่าว เพื่อรบกวนการปฏิบัติการของระบบคอมพิวเตอร์”

สำหรับมาตรา 15 ร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... “การรบกวนระบบคอมพิวเตอร์ หมายถึง การกระทำ ดังต่อไปนี้

1) การสร้าง และใช้โปรแกรมคอมพิวเตอร์ ไวรัสหรือเครื่องมืออื่น เพื่อขัดขวางหรือทำลายการปฏิบัติงานของระบบคอมพิวเตอร์

2) การส่งข้อมูลระบบคอมพิวเตอร์หรือจดหมายทางอิเล็กทรอนิกส์ โดยมีการปกปิดที่อยู่หรือแหล่งที่มาของผู้ส่ง เพื่อรบกวนหรือทำลายการปฏิบัติงานของระบบคอมพิวเตอร์”

เกี่ยวกับการรบกวนคอมพิวเตอร์ในการเข้าไปขัดขวางการใช้งานของระบบคอมพิวเตอร์นั้นเป็นการกระทำของบุคคลใดบุคคลคนหนึ่งที่กระทำอย่างใดอย่างหนึ่งเพื่อให้ระบบคอมพิวเตอร์นั้นทำงานไม่เป็นปกติหรือทำงานช้าลง และจากการกระทำความผิดในอนุมาตรา 2 จะเห็นได้ว่ามีเพียงการส่งข้อมูลคอมพิวเตอร์ที่มีการปกปิดที่อยู่หรือแหล่งที่มา อาจไม่หมายความรวมถึงการส่งข้อมูลคอมพิวเตอร์ที่มีการปลอมแปลงแหล่งที่อยู่ด้วย ซึ่งในการกระทำดังกล่าวอาจไม่ส่งผลกระทบให้ระบบคอมพิวเตอร์ แต่เป็นการส่งผลกระทบถึงผู้ใช้งานระบบคอมพิวเตอร์โดยปกติสุข

2. ประเทศสิงคโปร์

มาตรา 7 พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทางคอมพิวเตอร์ ค.ศ. 2007 การเข้าขัดขวางการใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งบุคคลใดเจตนาและปราศจากอำนาจหรือข้ออ้างใด ๆ ตามกฎหมายเพื่อเข้ารบกวนหรือขัดขวางการใช้งานคอมพิวเตอร์โดยถูกกฎหมาย หรือไม่ยอมให้เข้าถึงหรือทำให้ประสิทธิภาพในการทำงานลดลงซึ่ง

โปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์ ผู้นั้นมีความผิดและต้องได้รับโทษ[142] หรือถ้าความเสียหายที่เกิดขึ้นเป็นผลมาจากการเข้าขัดขวางการใช้งานคอมพิวเตอร์ก็จะได้รับโทษเพิ่มมากยิ่งขึ้น

3. ประเทศไทย

การกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานตามปกติได้ มาตรา 10 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้บัญญัติว่า “ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้...” วัตถุประสงค์ของมาตรานี้มีองค์ประกอบความผิดคือ การเข้าไปทำกับระบบคอมพิวเตอร์หรือการกระทำทางกายภาพอื่น ๆ ที่เข้าไปยุ่งเกี่ยวกับระบบคอมพิวเตอร์และมุ่งถึงเจตนาพิเศษของผู้กระทำเป็นสำคัญ จึงต้องพิจารณาจากข้อเท็จจริงที่ผู้กระทำได้กระทำไปเพื่อค้นหาเจตนาพิเศษดังกล่าว เช่น การป้อนโปรแกรมที่ทำให้ระบบคอมพิวเตอร์ปฏิเสธการทำงาน (Denial of Service) หรือทำให้ระบบคอมพิวเตอร์ทำงานได้ช้าลงโดยการป้อนไวรัสคอมพิวเตอร์เพื่อให้เกิดผลชะลอการทำงานของระบบ เป็นต้น

นอกจากนี้ การส่งข้อมูลคอมพิวเตอร์รบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุขนั้น มาตรา 11 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้บัญญัติว่า “ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข...” เป็นการบัญญัติเอาผิดแก่การกระทำที่ไม่ถึงกับทำให้ระบบคอมพิวเตอร์ของบุคคลอื่นไม่สามารถทำงานตามปกติได้ แต่เป็นการทำให้เกิดการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข เช่น ส่งอีเมล์ (E-mail) มากจนล้นระบบคอมพิวเตอร์ของบุคคลอื่นจนทำให้เกิดความยุ่งยากในการใช้งานระบบคอมพิวเตอร์ของเขา ภาษาอังกฤษเรียกว่า “อีเมล์สแปม (Email Spam)”

ผู้เขียนเห็นว่าการรบกวนระบบคอมพิวเตอร์ด้วยวิธีการอย่างใดอย่างหนึ่งนั้น ก็เพื่อทำให้ระบบคอมพิวเตอร์ถูกระงับ ขัดขวาง ชะลอ ซึ่งเป็นการกระทำของผู้ที่ไม่มีอำนาจในการกระทำดังกล่าว หรือผู้ใดกระทำด้วยประการใดโดยมิชอบเพื่อให้การทำงานของระบบคอมพิวเตอร์ของ

---

[142] Computer Misuse and Cybersecurity Act 2007, Unauthorised obstruction of use of computer 7. “(1) Any person who, knowingly and without authority or lawful excuse.,

(a) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer…”.

ผู้อื่นไม่สามารถใช้การได้อย่างสะดวก นอกจากนี้การส่งข้อมูลคอมพิวเตอร์ หรือจดหมายทางอิเล็กทรอนิกส์ เป็นการกระทำโดยการซ่อนหรือปลอมชื่ออีเมล์ เพื่อส่งจดหมายอิเล็กทรอนิกส์ หรืออีเมล์ไปให้แก่บุคคลอื่นโดยที่ผู้รับนั้นไม่ต้องการ และส่งผลกระทบถึงการใช้งานระบบคอมพิวเตอร์ของบุคคลอื่น

**4.4.2 มาตรการในการลงโทษ**

มาตรการในการลงโทษนั้น มีวัตถุประสงค์เพื่อให้ผู้กระทำความผิดได้รับผลตอบแทนของการกระทำดังกล่าว หรือเพื่อทำให้ผู้กระทำนั้นเกิดความเข็ดหลาบ ไม่กล้ากระทำความผิดซ้ำอีก เพื่อให้ทุกคนเกรงกลัวไม่กล้ากระทำความผิด หรือเพื่อไม่ให้ผู้กระทำความผิดกลับมากระทำความผิดอีก ซึ่งมาตรการลงโทษในกรณีของอาชญากรรมทางคอมพิวเตอร์สรุปได้ ดังนี้

4.4.2.1 สปป.ลาว

ตามมาตรา 58 ของร่างกฎหมายว่าด้วยการกระทำผิดทางระบบคอมพิวเตอร์ ค.ศ. ... ได้มีการกำหนดมาตรการในการลงโทษผู้กระทำความผิดทางระบบคอมพิวเตอร์ไว้ มาตรการต่อผู้ละเมิด “บุคคล นิติบุคคล หรือองค์กรใด ๆ ที่ละเมิดต่อกฎหมายฉบับนี้ จะถูกกล่าวเตือน ศึกษาอบรม ลงวินัย ปรับ ใช้ค่าเสียหายทางแพ่ง หรือถูกลงโทษทางอาญา ตามแต่กรณีเบาหรือหนัก ตามที่ได้กำหนดไว้ในระเบียบกฎหมาย” นอกจากนี้ตามมาตรา 59 ของกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ได้กำหนดมาตรการในการลงโทษไว้ มาตรการต่อผู้ละเมิด “บุคคล นิติบุคคลหรือองค์กร ที่ละเมิดกฎหมายฉบับนี้ เช่น ข้อห้าม จะถูกศึกษาอบรม กล่าวเตือน ลงวินัย ปรับ ใช้ค่าเสียหายทางแพ่งหรือถูกลงโทษทางอาญา แล้วแต่กรณีเบาหรือหนักตามที่ได้กำหนดไว้ในกฎหมายและระเบียบการ”

สำหรับกรณีผู้กระทำความผิดที่ได้กระทำผิดกฎหมายฉบับนี้ (ร่างกฎหมายว่าด้วยการกระทำผิดทางระบบคอมพิวเตอร์ ค.ศ. ...) ที่ก่อให้เกิดความเสียหายต่ำกว่า 10 ล้านกีบ จะถูกกล่าวเตือนศึกษาอบรม นอกจากนี้บุคคลหรือองค์กรที่ละเมิดกฎหมายฉบับนี้ ซึ่งได้ก่อความเสียหายแก่ผู้อื่น จะต้องใช้ค่าเสียหายที่ตนได้กระทำ และในมาตรการทางอาญาบุคคลใดที่ละเมิดกฎหมายฉบับนี้ ซึ่งเป็นการกระทำผิดทางอาญา จะถูกลงโทษตามกฎหมายอาญา ตามแต่ละกรณีเบาหรือหนัก รวมทั้งจ่ายค่าปรับที่ตนได้กระทำขึ้น แต่ร่างกฎหมายฉบับนี้ก็มิได้บัญญัติว่าเป็นมาตรการใดในกฎหมายอาญา ค.ศ. 2005 อย่างไรก็ตาม ดังที่ได้กล่าวแล้วว่ากฎหมายอาญา ค.ศ. 2005 ไม่อาจนำมาปรับใช้ได้จึงทำให้อาชญากรไม่ได้รับการลงโทษ

กรณีผู้กระทำการละเมิดต่อกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ซึ่งเป็นการละเมิดครั้งแรก และสร้างความเสียหายไม่มาก จะถูกศึกษาอบรมและกล่าวเตือน นอกจากนี้ยังมีมาตรการทางวินัยต่อเจ้าหน้าที่ และพนักงานที่เกี่ยวข้อง ที่ได้ละเมิด

กฎหมายฉบับนี้ ซึ่งไม่เป็นการกระทำผิดทางอาญา จะถูกลงวินัยตามแต่ละกรณี นอกจากนี้ ยังมีมาตรการทางอาญาต่อบุคคลที่ได้กระทำผิดในสถานที่ได้กำหนดในมาตรา 8 เกี่ยวกับพฤติกรรมที่เป็นอาชญากรรมทางคอมพิวเตอร์ (ฐานความผิด) ซึ่งมาตรการในการลงโทษทางอาญาต่อผู้กระทำความผิดทางระบบคอมพิวเตอร์ ขั้นต่ำสุดของโทษจำคุกตั้งแต่หนึ่งเดือน และสูงสุดห้าปี และปรับตั้งแต่ 10 ล้านกีบถึง 400 ล้านกีบตามแต่ละกรณี

4.4.2.2 ประเทศสิงคโปร์

สำหรับมาตรการลงโทษผู้กระทำความผิดทางคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทางคอมพิวเตอร์ ค.ศ. 2007 ได้มีการบัญญัติเกี่ยวกับมาตรการในการลงโทษเกี่ยวกับลักษณะของการกระทำผิดเป็นไปในการลงโทษทางอาญาแก่ผู้กระทำความผิด เพื่อก่อให้เกิดความตระหนักในการกระทำความผิด ซึ่งเป็นมาตรการลงโทษที่มีโทษขั้นต่ำคือจำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 5 พันดอลลาร์สิงคโปร์ และโทษจำคุกสูงสุด 20 ปี และโทษปรับสูงสุด 100,000 ดอลลาร์สิงคโปร์[143] เช่น การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต บุคคลใดก็ตามที่เจตนาใช้คอมพิวเตอร์เพื่อวัตถุประสงค์ในการเข้าถึง โดยไม่ได้รับอนุญาต ซึ่งข้อมูลคอมพิวเตอร์หรือโปรแกรมที่อยู่ในคอมพิวเตอร์ใด ๆ ที่มีการป้องกันการเข้าถึงโดยเฉพาะ ถือว่ามีความผิด ต้องระวางโทษปรับไม่เกิน 5 พันดอลลาร์สิงคโปร์หรือจำคุกไม่เกิน 2 ปี หรือทั้งจำทั้งปรับ[144] และในกรณีกระทำผิดซ้ำ ปรับไม่เกิน 1 หมื่นดอลลาร์สิงคโปร์หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ ถ้าความเสียหายเกิดขึ้นจากการกระทำดังกล่าว ผู้ต้องหาต้องมีความรับผิดในค่าปรับไม่เกิน 5 หมื่นดอลลาร์สิงคโปร์ หรือจำคุกไม่เกิน 7 ปี หรือทั้งจำทั้งปรับ

4.4.2.3 ประเทศไทย

พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ได้มีการกำหนดมาตรการลงโทษเป็นแต่ละกรณีกระทำความผิด ซึ่งเป็นมาตรการลงโทษทางอาญาที่มีโทษขั้นต่ำคือจำคุกไม่เกิน 6 เดือนหรือปรับไม่เกิน 10,000 บาท และโทษจำคุกสูงสุด 20 ปี และโทษปรับสูงสุด

---

[143] Computer Misuse and Cybersecurity Act 2007, Enhanced punishment for offences involving protected computers 9, "(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6, or 7, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable to a fine not exceeding $100,000 or to imprisonment for a tern not exceeding 20 years or to both. …".

[144] Ibid, Unauthorised Access to Computer Material 3. "(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both …".

300,000 บาท[145] เกี่ยวกับมาตรการลงโทษที่มุ่งเน้นการลงโทษทางอาญาแก่ผู้กระทำความผิดทางคอมพิวเตอร์ เพื่อทำให้เกิดความตะหนักในการใช้งานไปในทางที่ชอบด้วยกฎหมาย เช่น ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 1 หมื่นบาท หรือทั้งจำทั้งปรับ[146]

โดยสรุปจากการศึกษามาตรการในการลงโทษต่อผู้กระทำความผิดเกี่ยวกับความผิดทางคอมพิวเตอร์ ผู้เขียนเห็นว่า ในการกำหนดมาตรการในการลงโทษนั้นควรจะเป็นมาตรการในทางอาญา ซึ่งการกระทำของอาชญากรรมทางคอมพิวเตอร์เป็นผู้ที่มีความรู้ทางคอมพิวเตอร์ และในการกระทำดังกล่าวอาจประเมินค่าความเสียหายได้ยาก ถ้าเปิดโอกาสให้มีการใช้มาตรการในการศึกษาอบรมหรือกล่าวเตือนในกรณีมีการกระทำความผิดครั้งแรก และก่อความเสียหายไม่มาก อาจทำให้อาชญากรไม่เกรงกลัวต่อกฎหมาย นอกจากนั้น เพื่อเป็นการป้องกันการไม่ให้บุคคลใดบุคคลหนึ่งกระทำการเพื่อไปกระทบต่อสิทธิเสรีภาพของผู้อื่นในการใช้งานคอมพิวเตอร์และระบบคอมพิวเตอร์ ที่เป็นส่วนสำคัญในการประกอบกิจการและการดำรงชีวิตของมวลมนุษย์ หากมีการกระทำการใด ๆ โดยมิชอบแล้ว อาจส่งผลกระทบให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ และความสงบเรียบร้อยของสังคมได้

**4.4.3 อำนาจหน้าที่ของพนักงานเจ้าหน้าที่**

ตามหลักความชอบด้วยกฎหมายแล้ว องค์กรหรือพนักงานเจ้าหน้าที่จะกระทำการอย่างใดอย่างหนึ่งได้นั้นจะต้องมีกฎหมายบัญญัติให้อำนาจไว้ให้กระทำการดังกล่าว โดยเฉพาะการกระทำที่มีผลกระทบกระเทือนต่อสิทธิเสรีภาพของบุคคล เช่น การจับกุม การกักขัง เป็นต้น ซึ่งการทำงานของเจ้าหน้าที่ในการจัดการหรือดำเนินคดีกับเรื่องราวที่มีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือใช้คอมพิวเตอร์กระทำความผิดไม่อาจกระทำได้อย่างมีประสิทธิภาพ ทั้งนี้เพราะภายใต้หลักการของนิติรัฐที่มีหลักการสำคัญว่า เจ้าหน้าที่ของรัฐจะกระทำการใดอันเป็นการกระทบกระเทือน

---

[145] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, มาตรา 12 "... (2) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือต่อระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่ 3 ปีถึง 15 ปี และปรับตั้งแต่ 60,000 หมื่นบาทถึง 300,000 บาท ถ้าการกระทำความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ 10 ปีถึง 20 ปี".

[146] เรื่องเดียวกัน, มาตรา 5.

ต่อสิทธิเสรีภาพของประชาชนจะต้องมีกฎหมายให้อำนาจหน้าที่เจ้าหน้าที่รัฐ หากไม่มีกฎหมายให้อำนาจรัฐ เจ้าหน้าที่รัฐก็จะกระทำการใดอันเป็นการกระทบต่อสิทธิเสรีภาพของประชาชนไม่ได้[147]

ในขณะที่เทคโนโลยีมีการพัฒนาแต่กฎหมายยังไม่อาจตราขึ้นเพื่อควบคุมการใช้เทคโนโลยีได้อย่างมีประสิทธิภาพ ด้วยเหตุนี้เพื่อให้การสืบสวนสอบสวนทำได้อย่างเต็มที่ เช่น อำนาจในการตรวจสอบระบบคอมพิวเตอร์ที่ต้องสงสัยว่ามีการนำมาใช้กระทำความผิด อำนาจในการค้นหรือเข้ายึด การเรียกข้อมูลจราจรทางคอมพิวเตอร์ หรือการถอดรหัสลับของข้อมูลคอมพิวเตอร์ เป็นต้น จึงต้องมีกฎหมายบัญญัติให้อำนาจไว้โดยเฉพาะเช่นกันจึงจะดำเนินการได้

4.4.3.1 สปป.ลาว

ตามมาตรา 19 ของร่างกฎหมายว่าด้วยการกระทำผิดทางระบบคอมพิวเตอร์ ค.ศ. ... เกี่ยวกับอำนาจของพนักงานเจ้าหน้านั้นได้กำหนดขั้นตอนในการแจ้งเหตุฉุกเฉินที่เกิดขึ้นกับระบบคอมพิวเตอร์ของตนต่อกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร (Ministry of Post and Telecommunication) เพื่อค้นคว้าให้คำแนะนำวิธีการแก้ไขทางด้านเทคนิค เพื่อยับยั้งการสูญเสียข้อมูล การรบกวนข้อมูล การยุติการทำงานของระบบ การสกัดกั้นการกระจายไวรัสคอมพิวเตอร์ และการเข้าทำลายระบบคอมพิวเตอร์ด้วยการยื่นคำร้องตามแบบฟอร์มหรือโทรศัพท์ แฟกส์ และจดหมายอิเล็กทรอนิกส์ ภายหลังที่ได้รับแจ้งเหตุแล้ว กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร จะดำเนินการค้นคว้าพิจารณาคำร้องและแจ้งตอบ พร้อมทั้งแนะนำวิธีการแก้ไข ภายในกำหนดเวลาไม่เกิน 10 วันทำงานราชการ ในกรณีจำเป็นกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร ต้องดำเนินการแก้ไขทางเทคนิควิชาการช่วยผู้แจ้งเหตุฉุกเฉินตามการเสนอของผู้เสียหาย

และ ตามมาตรา 24 ของร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ได้มีการกำหนดเกี่ยวกับขั้นตอนในการแจ้งเหตุฉุกเฉินที่เกิดขึ้นกับระบบคอมพิวเตอร์ของตนต่อแขนงการไปรษณีย์ โทรคมนาคม และการสื่อสาร ซึ่งสามารถดำเนินด้วยวิธีการ เขียนคำร้องตามแบบฟอร์ม โทรศัพท์สายด่วนหรือแฟกซ์ จดหมายอิเล็กทรอนิกส์ หรือวิธีอื่น ภายหลังที่ได้รับแจ้งเหตุฉุกเฉินแล้ว กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสารต้องค้นคว้าพิจารณาคำร้อง และแจ้งตอบพร้อมทั้งแนะนำวิธีการแก้ไขภายในกำหนดเวลา 5 วันทำงานราชการ ในกรณีจำเป็น และเร่งด่วน กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสารต้องดำเนินการแก้ไขทางเทคนิควิชาการ ตามคำร้องของผู้เกี่ยวข้องอย่างทันการ นอกจากนั้นในกฎหมายดังกล่าวได้มีการกำหนดการดำเนินคดีการกระทำความผิดทางระบบคอมพิวเตอร์นั้นต้องมีขั้นตอนในการดำเนินคดี คือ การแจ้งความ และการพิจารณาการแจ้งความ ซึ่งในการพิจารณาการแจ้งความ

---

[147] มานิตย์ จุมปา, *คำอธิบายกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์*, 18.

นั้นก็ได้มีการกำหนดระยะเวลาในการพิจารณาด้วยการกำหนดขอบเขตคือ มีการแจ้งความ การรายงานหรือร้องฟ้องเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ต่อองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชน ซึ่งองค์การดังกล่าวต้องพิจารณาการแจ้งความดังกล่าวไม่เกิน 5 วันทำงานราชการ ในกรณีมีความยุ่งยากให้ขยายระยะเวลาดังกล่าว ไม่ให้เกิน 10 วันทำงานราชการ แต่ในการกำหนดระยะเวลาดังกล่าวที่เป็นการวางข้อบังคับเกี่ยวกับการกำหนดระยะเวลาของการพิจารณาคำร้อง เพื่อดำเนินการเริ่มการสืบสวน-สอบสวนการกระทำผิดทางระบบคอมพิวเตอร์ย่อมทำให้เกิดข้อดีและข้อเสียบ้างบางประการ ดังนี้

ข้อดี

1. เป็นการกำหนดวันเวลาที่แน่นอนเกี่ยวกับการตอบรับคำร้องของผู้เสียหาย และแจ้งผลให้ผู้เสียหายทราบได้ทราบ

2. เป็นกรอบระยะเวลาในการปฏิบัติงานของพนักงานเจ้าหน้าที่ที่แน่นอน

3. ทำให้ผู้เสียหายได้ทราบระยะเวลาการดำเนินการสันหาข้อมูลอันเป็นกระบวนการพิจารณาที่มีความแน่นอน

ข้อเสีย

1. การกำหนดระยะเวลาของการพิจารณาคำร้องของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชน ที่ใช้เวลาไม่เกิน 5 วันทำงานราชการ ในกรณีมีความยุ่งยากสับสนการกำหนดเวลาดังกล่าวต้องไม่ให้เกิน 10 วันทำงานราชการนั้น เห็นได้ว่ามีขั้นตอนเนินนาน ซึ่งเมื่อเทียบกับการกระทำความผิดทางระบบคอมพิวเตอร์นั้นใช้เวลาไม่มากนะ

2. เป็นการใช้เวลาพอสมควรก่อนที่จะได้ดำเนินการสืบสวน-สอบสวนเพื่อหาพยานหลักฐานของการกระทำผิดดังกล่าว

3. ทำให้ผู้กระทำความผิดอาจทำลายข้อมูลหลักฐานทางคอมพิวเตอร์ได้

4. ส่วนใหญ่ผู้กระทำความผิดเป็นผู้ที่มีความรู้ความเชี่ยวชาญทางด้านเทคโนโลยีคอมพิวเตอร์ที่สามารถทำลายหลักฐานหรือปรับเปลี่ยนข้อมูลได้อย่างรวดเร็ว

นอกจากนี้ ในการค้นหาพยานหลักฐานเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ การสืบสวน-สอบสวน การสั่งฟ้อง การดำเนินคดี และการปฏิบัติตามคำตัดสินของศาล ซึ่งในการดำเนินการสืบสวน-สอบสวนให้ปฏิบัติตามกฎหมายว่าด้วยการดำเนินคดีอาญา ค.ศ. 2012 และในกรณีเร่งด่วนถ้าหากมีข้อมูลที่สามารถยืนยันได้ว่ากำลังมีการตระเตรียมหรือการดำเนินการการกระทำผิดทางระบบคอมพิวเตอร์ องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ องค์การอัยการต้องออกคำสั่งให้เก็บรักษา และป้องกันข้อมูลทางคอมพิวเตอร์ หรือข้อมูลเกี่ยวกับการจราจรข้อมูล

ไว้[148] แต่อย่างไรก็ตามในกฎหมายดังกล่าวไม่ได้มีการบัญญัติให้สิทธิอำนาจหน้าที่แก่พนักงานเจ้าหน้าที่ที่จะกระทำการอย่างใดอย่างหนึ่งไว้เป็นการเฉพาะ เช่น การเรียกเก็บข้อมูลจราจรทางคอมพิวเตอร์ สั่งให้ผู้บริการส่งมอบข้อมูล เป็นต้น กล่าวคือให้ดำเนินการตามกระบวนการวิธีพิจารณาความอาญาทั่วไป และในการดำเนินการสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชนต้องประสานสมทบกับแขนงไปรษณีย์ โทรคมนาคม และการสื่อสาร และภาคส่วนที่เกี่ยวข้องเพื่อดำเนินการค้นหาข้อมูลหลักฐาน และที่มาของอาชญากรรมทางคอมพิวเตอร์เพื่อเป็นหลักฐานให้แก่การสืบสวน-สอบสวน การดำเนินการสืบสวน-สอบสวนคดีทางระบบคอมพิวเตอร์ ต้องใช้วิธีการสืบสวน-สอบสวน มาตรการสกัดกั้น และกำหนดเวลาในการสืบสวน-สอบสวนตามที่ได้กำหนดไว้ในกฎหมายว่าด้วยการดำเนินคดีอาญา ค.ศ. 2012 ซึ่งในกฎหมายดังกล่าวไม่ได้มีการบัญญัติเกี่ยวกับการดำเนินคดีต่อผู้กระทำความผิดทางระบบคอมพิวเตอร์ กล่าวคือให้ปฏิบัติตามคดีอาญาทั่วไป[149]

โดยสรุปจากการศึกษาวิจัย พบว่าร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ยังไม่ได้มีการกำหนดให้อำนาจแก่พนักงานเจ้าหน้าไว้อย่างชัดเจนเกี่ยวกับการบังคับใช้กับการกระทำความผิดทางคอมพิวเตอร์ไว้เป็นการเฉพาะ กล่าวคือให้ปฏิบัติตามกฎหมายว่าด้วยการดำเนินคดีอาญา ค.ศ. 2012 อันเป็นวิธีพิจารณาความอาญาทั่วไป ซึ่งในกฎหมายการดำเนินคดีอาญาก็มีได้บัญญัติเกี่ยวกับการให้อำนาจหน้าที่แก่เจ้าพนักงานในกรณีมีการกระทำความผิดทางคอมพิวเตอร์ไว้เช่นกัน ดังนี้ผู้เขียนเห็นว่าควรมีการกำหนดให้อำนาจแก่พนักงานเจ้าหน้าที่ไว้อย่างชัดเจน เพื่อให้พนักงานเจ้าหน้าที่สามารถดำเนินการสืบสวน-สอบสวนได้โดยเฉพาะทันท้วงที่ต่อการกระทำผิด

4.4.3.2 ประเทศสิงคโปร์

ตามมาตรา 14 ของพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความมั่นคงทางคอมพิวเตอร์ ค.ศ. 2007 ได้ให้อำนาจแก่เจ้าพนักงานตำรวจเป็นผู้สืบสวนสอบสวนการกระทำผิด[150] ซึ่งมีความสอดคล้องกับมาตรา 39 ของประมวลกฎหมายวิธีพิจารณาความอาญา ค.ศ. 2010 (The Criminal Procedure Code 2010) ที่ได้ให้อำนาจแก่เจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับ

---

[148] ร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ..., มาตรา 47.

[149] เรื่องเดียวกัน, มาตรา 48.

[150] Computer Misuse and Cybersecurity Act 2007, Saving for investigations by police and law enforcement officers 14, “Nothing in this Act shall prohibit a police officer, an authorised person within the meaning of section 39 of the Criminal Procedure Code 2010 or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to the powers conferred on him under any written law.”

มอบอำนาจตามกฎหมายสืบสวนคดีความการกระทำผิดที่สามารถจับคุมได้ และสามารถกระทำการสืบสวนสอบสวนเมื่อใดก็ได้ การเข้าถึง ตรวจสอบการทำงานของคอมพิวเตอร์ซึ่งเจ้าหน้าที่นั้นมีเหตุให้สงสัยว่าได้ถูกใช้ในการกระทำผิด การใช้หรือทำให้เกิดการใช้ซึ่งคอมพิวเตอร์เพื่อค้นข้อมูลหรือมีอยู่ในคอมพิวเตอร์นั้น เจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจตามกฎหมายอาจขอความช่วยเหลือจากบุคคลใดที่เจ้าหน้าที่สงสัยว่าจะใช้คอมพิวเตอร์ในการกระทำผิดหรือเคยใช้กระทำผิด หรือบุคคลใดก็ตามที่รับผิดชอบเกี่ยวข้องกับการทำงานของคอมพิวเตอร์ดังกล่าว บุคคลใดที่ขัดขวางการปฏิบัติหน้าที่ตามกฎหมายของเจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจถือว่ากระทำความผิด

จากการศึกษาพบว่าในการให้อำนาจแก่พนักงานเจ้าหน้าที่เกี่ยวกับการดำเนินการสืบสวนสอบสวนหาตัวผู้กระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์นั้น ประเทศสิงคโปร์ได้มีการบัญญัติให้อำนาจแก่เจ้าพนักงานไว้เป็นการเฉพาะในประมวลกฎหมายวิธีพิจารณาความอาญาที่จะดำเนินการอย่างใดอย่างหนึ่งตามที่กฎหมายกำหนดให้อำนาจต่อผู้กระทำความผิดได้

4.4.3.3 ประเทศไทย

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายที่กำหนดความผิดทางอาญา ซึ่งในการดำเนินคดีไม่ว่าในเรื่องการค้น การสืบสวนสอบสวน การจับกุม กักขังย่อมเป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญา

การใช้อำนาจของพนักงานเจ้าหน้าที่[151] ในการสืบสวนสอบสวนเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในมาตรา 18 ของกฎหมายฉบับนี้ “ภายใต้บังคับมาตรา 19[152] เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

1. มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

---

[151] พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 “พนักงานเจ้าหน้าที่ หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้”.

[152] เรื่องเดียวกัน, มาตรา 19 บัญญัติว่า “การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินตามคำร้อง ...”.

2. เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

3. สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

4. ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

5. สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวให้แก่เจ้าพนักงาน

6. ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

7. ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

8. ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้”

ซึ่งในการกำหนดให้การใช้อำนาจในบางมาตราที่ไม่ก่อให้เกิดผลกระทบต่อสิทธิความเป็นส่วนตัว หรืออาจกระทบต่อการประกอบการของผู้ให้บริการไม่มากเกินไป และใช้เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด ซึ่งพนักงานเจ้าหน้าที่สามารถดำเนินการได้เองโดยไม่ต้องขออนุญาตศาลตามความในข้อ 1-3 นอกจากนี้ ในการใช้อำนาจที่อาจเสี่ยงต่อการละเมิดสิทธิขั้นพื้นฐานความเป็นส่วนตัวของประชาชนหรืออาจกระทบต่อการประกอบการขององค์กรธุรกิจ ในการใช้อำนาจของพนักงานเจ้าหน้าที่ซึ่งต้องขออนุญาตจากศาลตามความในข้อ 4-8

ปัจจุบันการกระทำที่เข้าข่ายว่าเป็นความผิดตามพระราชบัญญัตินี้ ที่อาจกระทบต่อความมั่นคง หรือขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน โดยกระทบต่อความรู้สึกของคนในสังคมเป็นอย่างมากและในการจัดการกับปัญหาดังกล่าวจะต้องกระทำด้วยความรวดเร็ว แต่การระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์หรือการบล็อก (Block) เว็บไซต์ไม่ให้ระบบคอมพิวเตอร์เผยแพร่ข้อมูลคอมพิวเตอร์ที่เป็นความผิดดังกล่าวในระบบ

คอมพิวเตอร์อีกต่อไปนั้นอาจส่งผลกระทบต่อธุรกิจของผู้ให้บริการ จึงอาจทำให้เกิดเหตุการณ์ฟ้องร้องพนักงานเจ้าหน้าที่กลับได้ ด้วยเหตุนี้ พระราชบัญญัติดังกล่าวจึงกำหนดให้รัฐมนตรีผู้รักษาการมีบทบาทในการกลั่นกรองดุลพินิจของพนักงานเจ้าหน้าที่ก่อนที่จะดำเนินการยื่นขอการบล็อกเว็บไซต์จากศาล

นอกจากนั้น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ยังได้ให้อำนาจแก่พนักงานเจ้าหน้าที่ในการห้ามจำหน่ายชุดคำสั่งไม่พึงประสงค์หรือเผยแพร่โปรแกรมชั่วร้ายทั้งหลายที่สร้างขึ้นมาเพื่อก่อกวน ทำลายระบบคอมพิวเตอร์ และกระทำความผิดตามพระราชบัญญัติดังกล่าว ในรูปแบบต่าง ๆ อาทิ ไวรัส (Virus) สปายแวร์ (Spyware) เป็นต้น นอกจากจะห้ามการจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์แล้วพนักงานเจ้าหน้าที่ยังสามารถกำหนดเงื่อนไขในการใช้ การครอบครอง และการเผยแพร่โปรแกรมข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วยนั้นด้วยการระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้

ทั้งนี้ จากการศึกษาปัญหาดังกล่าวจะเห็นได้ว่าในการบัญญัติกฎหมายเกี่ยวกับขั้นตอนของการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในร่างกฎหมายว่าด้วยการกระทำผิดทางระบบคอมพิวเตอร์ ค.ศ. ... ร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ...ของ สปป.ลาว ไม่ได้มีการบัญญัติเกี่ยวกับการให้สิทธิอำนาจแก่พนักงานเจ้าหน้าที่ไว้เป็นการเฉพาะ นอกจากนั้นยังมีขั้นตอน และกระบวนการในการสืบสวน-สอบสวนหาตัวผู้กระทำความผิดนั้นผ่านหลายขั้นตอน ซึ่งการกระทำของอาชญากรรมทางคอมพิวเตอร์เป็นการกระทำที่อาศัยความสลับซับซ้อนของเครื่องคอมพิวเตอร์และระบบคอมพิวเตอร์ ที่สามารถจะทำลายพยานหลักฐานในไม่กี่วินาที หากกระบวนการดังกล่าวมีกระบวนการและขั้นตอนในการสืบหาพยานหลักฐานต้องอาศัยผู้ที่มีความรู้ความเชี่ยวชาญเกี่ยวกับคอมพิวเตอร์ แต่การค้นหาหลักฐานมีหลายขั้นตอนในการดำเนินงาน กล่าวคือ องค์กรสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ องค์การอัยการ ต้องประสานงานกับกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร และภาคส่วนต่าง ๆ ที่เกี่ยวข้องเพื่อดำเนินการค้นหาข้อมูลหลักฐาน และแหล่งที่มาของการกระทำความผิดทางระบบคอมพิวเตอร์ เพื่อนำผู้กระทำความผิดมาฟ้องลงโทษตามกฎหมายต่อไป ด้วยเหตุนี้เห็นควรให้มีการบัญญัติกฎหมายเกี่ยวกับการให้อำนาจหน้าที่แก่พนักงานเจ้าหน้าที่ไว้เป็นการเฉพาะ

**ตารางที่ 4.2** เปรียบเทียบมาตรการในการคุ้มครองและป้องกันอาชญากรรมคอมพิวเตอร์

| | สปป.ลาว | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 1. กฎหมายที่เกี่ยวข้อง | ร่างกฎหมายว่าด้วยการกระทำผิดทางระบบคอมพิวเตอร์ ค.ศ. … | พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2007 | พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 | |
| 2. ฐานความผิด<br>2.1 การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต | ยังไม่ได้บัญญัติถึงรูปแบบของการกระทำความผิดเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต | การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งบุคคลใดก็ตามที่เจตนาใช้คอมพิวเตอร์เพื่อวัตถุประสงค์ในการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งข้อมูลคอมพิวเตอร์หรือโปรแกรมที่อยู่ในคอมพิวเตอร์ใด ๆ ที่มีการป้องกันการเข้าถึงโดยเฉพาะ ถือว่ามีความผิด ถึงแม้ว่าการกระทำดังกล่าวจะเป็นการกระทำเพื่อการเข้าถึงคอมพิวเตอร์และระบบคอมพิวเตอร์ สำหรับวัตถุประสงค์ของส่วนนี้ ให้ถือว่าไม่ได้มุ่งถึงโปรแกรมหรือข้อมูลใดโดยเฉพาะ โปรแกรมหรือข้อมูลชนิดใด ๆ หรือโปรแกรมหรือข้อมูลในคอมพิวเตอร์- | ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน (มาตรา 5)<br>ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตาการนั้นมิได้มีไว้สำหรับตน (มาตรา 7) | สปป.ลาว ยังไม่มีบัญญัติครอบคลุมถึงการเข้าถึงข้อมูลทางคอมพิวเตอร์โดยไม่ได้รับอนุญาต |

**ตารางที่ 4.2** (ต่อ)

| | สปป.ลาว | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 2.1 (ต่อ) | | เครื่องใด ๆ โดยเฉพาะและในกรณีมีการกระทำผิดซ้ำจะได้รับโทษเพิ่มขึ้น (มาตรา 3) | | |
| 2.2 การรบกวนข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต | ได้กำหนดในมาตรา 12 การทำลายข้อมูลในระบบคอมพิวเตอร์ “การทำลายข้อมูลในระบบคอมพิวเตอร์ หมายถึง การลบ การดัดแปลงข้อมูลคอมพิวเตอร์ การทำให้ข้อมูลเสียหายและการเปลี่ยนแปลงข้อมูล เพื่อสร้างความเสียหายให้แก่ระบบคอมพิวเตอร์” | การดัดแปลงแก้ไขข้อมูลคอมพิวเตอร์ ซึ่งบุคคลใดกระทำการใด ๆโดยมิชอบ ซึ่งรู้ว่าจะทำให้เกิดการดัดแปลงแก้ไขเนื้อหาใด ๆ ของคอมพิวเตอร์ เป็นการกระทำผิด อย่างไรก็ตามการดัดแปลงแก้ไขข้อมูลคอมพิวเตอร์ในกรณีที่จำเป็นแก่การใช้ เช่น ผู้ใช้สามารถดัดแปลงโปรแกรมคอมพิวเตอร์เท่าที่จำเป็น แต่ในกรณีนี้การดัดแปลงที่ก่อให้เกิดความเสียหายไม่ว่าจะเป็นการดัดแปลงเป็นการถาวรหรือเป็นการชั่วคราวก็ถือว่าเป็นการกระทำผิด (มาตรา 6) | ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 9) | สปป.ลาว การรบกวนต่อข้อมูลคอมพิวเตอร์ สร้างความเสียหายให้ระบบคอมพิวเตอร์<br>ประเทศสิงคโปร์ ดัดแปลงข้อมูล รวมถึงดัดแปลงโปรแกรมก็มีความผิดแล้ว<br>ประเทศไทย การรบกวนไม่ว่าทั้งหมดหรือบางส่วนก็มีความผิดแล้ว |

**ตารางที่ 4.2** (ต่อ)

| | สปป.ลาว | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 2.3 การรบ-กวนระบบคอม-พิวเตอร์โดยไม่ได้รับอนุญาต | การรบกวนระบบคอมพิวเตอร์ “การรบกวนระบบคอมพิวเตอร์ หมายถึง การกระทำ ดังนี้<br>1. การขัดขวาง ซึ่งทำให้ระบบคอมพิวเตอร์อย่างใดอย่างหนึ่ง ไม่สามารถปฏิบัติการ ปฏิบัติการช้าลง หรือไม่สามารถปฏิบัติการได้อย่างเป็นปกติ<br>2. การส่งข้อมูลระบบคอมพิวเตอร์หรือจดหมายทางอิเล็กทรอนิกส์ โดยมีการปกปิดที่อยู่หรือแหล่งที่มาของการส่งข้อมูลดังกล่าว เพื่อรบกวนการปฏิบัติการของระบบคอมพิวเตอร์” | การเข้าขัดขวางการใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งบุคคลใดเจตนาและปราศจากอำนาจหรือข้ออ้างใด ๆ ตามกฎหมาย เพื่อเข้ารบกวนหรือขัดขวางการใช้งานโดยถูกกฎหมายซึ่งคอมพิวเตอร์ หรือไม่ยอมให้เข้าถึงหรือทำให้ประสิทธิภาพในการทำงานลดลงซึ่งโปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์ ผู้นั้นมีความผิดและต้องได้รับโทษ หรือถ้าความเสียหายที่เกิดขึ้นเป็นผลมาจากการเข้าขัดขวางการใช้งานคอมพิวเตอร์ก็จะได้รับโทษเพิ่มมากยิ่งขึ้น (มาตรา 7) | ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ (มาตรา 10) | สปป.ลาว การรบกวนระบบคอมพิวเตอร์ หมายความรวมถึงการส่งจดหมายอิเล็กทรอนิกส์ที่มีการปกปิดที่อยู่หรือแหล่งที่มาของการส่ง เพื่อรบกวนการปฏิบัติการของระบบคอมพิวเตอร์ ประเทศสิงคโปร์ บุคคลใดเจตนาและปราศจากอำนาจหรือข้ออ้างใด ๆ รบกวนหรือขัดขวางการทำงานของโปรแกรมหรือข้อมูล<br>ประเทศไทย ได้มีการบัญญัติถึงการกระทำอย่างใดอย่างหนึ่งโดยมิชอบให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นทำงานไม่ปกติ |
| 3. มาตรการลงโทษ | การกำหนดมาตรการลงโทษผู้กระทำความผิดทางระบบคอมพิวเตอร์คือ บุคคล นิติบุคคล - | การกำหนดมาตรการลงโทษเกี่ยวกับลักษณะของการกระทำผิดของอาชญากรรมทางคอมพิวเตอร์- | การกำหนดมาตรการลงโทษเป็นแต่ละกรณีกระทำความผิด ซึ่งเป็นมาตรการลงโทษทางอาญาที่มีโทษ- | สปป.ลาว ได้กำหนดมาตรการต่อผู้กระทำผิด คือ กล่าวเตือน ศึกษาอบรมลงวินัย ปรับ ชดใช้ - |

**ตารางที่ 4.2** (ต่อ)

| | สปป.ลาว | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 3. (ต่อ) | หรือองค์กร ที่กระทำการละเมิดต่อกฎหมายฉบับนี้ จะถูกกล่าวเตือน ศึกษาอบรม ลงวินัย ปรับ ใช้ค่าเสียหายทางแพ่ง หรือถูกลงโทษทางอาญา ตามแต่กรณีเบาหรือหนัก ตามที่ได้กำหนดไว้ในระเบียบกฎหมาย<br>ในกรณีผู้กระทำความผิดที่ได้กระทำผิดกฎหมายฉบับนี้ที่ก่อให้เกิดความเสียหายต่ำกว่า 10 ล้านกีบ จะถูกตักเตือนศึกษาอบรม นอกจากนี้ บุคคลหรือองค์กรที่ละเมิดกฎหมายฉบับนี้ ซึ่งได้ก่อความเสียหายแก่ผู้อื่น จะต้องใช้ค่าเสียหายที่ตนได้กระทำ และในมาตรการทางอาญาบุคคลใดที่ละเมิดกฎหมายฉบับนี้ ซึ่งเป็นการกระทำผิดทางอาญา จะถูกลงโทษตามกฎหมายอาญา รวมทั้งจ่ายค่าปรับที่ตนได้กระทำขึ้น | เป็นไปในการลงโทษทางอาญาแก่ผู้กระทำความผิด เพื่อก่อให้เกิดความตระหนักในการกระทำความผิด ซึ่งเป็นมาตรการลงโทษนั้นมีโทษขั้นต่ำคือจำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 5 พันดอลลาร์สิงคโปร์ และโทษจำคุกสูงสุด 20 ปี และโทษปรับสูงสุด 100,000 ดอลลาร์สิงคโปร์ | ขั้นต่ำคือจำคุกไม่เกิน 6 เดือนหรือปรับไม่เกิน 10,000 บาท และโทษจำคุกสูงสุด 20 ปี และโทษปรับสูงสุด 300,000 บาท เกี่ยวกับมาตรการลงโทษมุ่งเน้นการลงโทษทางอาญาแก่ผู้กระทำความผิดทางคอมพิวเตอร์ เพื่อทำให้เกิดความตะหนักในการใช้งานไปในทางที่ชอบด้วยกฎหมาย | ค่าเสียหาย ถูกลงโทษทางอาญาในการกระทำความผิดของบุคคลใดบุคคลหนึ่งที่ก่อให้เกิดความเสียหายที่มีมูลค่าต่ำกว่า 10 ล้านกีบจะถูกตักเตือนศึกษาอบรม ส่วนประเทศสิงคโปร์และไทยใช้มาตรการลงโทษทางอาญาและแพ่งควบคู่กันไป |

**ตารางที่ 4.2** (ต่อ)

| | สปป.ลาว | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 4. การให้อำนาจพนักงานเจ้าหน้าที่ | การกระทำความผิดทางระบบคอมพิวเตอร์ อยู่ในการควบคุมดูแลของรัฐบาล โดยมอบให้องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ และกระทรวงไปรษณีย์โทรคมนาคม และการสื่อสาร เป็นผู้รับผิดชอบโดยตรง และประสานความร่วมมือกับกระทรวงหรือองค์กรอื่น และองค์การปกครองส่วนท้องถิ่นที่เกี่ยวข้อง ตามภาระบทบาทของตน | ได้มีการบัญญัติให้การดำเนินการสืบสวนสอบสวนเป็นของเจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจให้ดำเนินการสืบสวนตามมาตรา 39 แห่งกฎหมายวิธีพิจารณาความอาญา ค.ศ. 2010 | เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใดดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด | |
| 4.1 ตรวจสอบระบบคอมพิวเตอร์ที่ต้องสงสัยว่ามีการนำมาใช้กระทำความผิด | องค์การสืบสวน-สอบสวน เจ้าหน้าที่ตำรวจตรวจสอบข้อมูลที่สงสัยหรือเสนอให้ภาคส่วนที่เกี่ยวข้องตรวจสอบข้อมูลที่สงสัยที่จะสร้างความเสียหายให้แก่บุคคล นิติ-บุคคล องค์กร สังคม และความมั่นคงของชาติ | เจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจตามกฎหมายสืบสวนคดีความการกระทำผิดที่สามารถจับกุมได้ สามารถเข้าถึงตรวจสอบการทำงานของคอมพิวเตอร์ซึ่งเจ้าหน้าที่นั้นมีเหตุให้สงสัยว่าได้ถูกใช้ในการกระทำผิด | มีหนังสือสอบถามหรือเรียกตัวบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือหรือส่งเอกสาร ข้อมูลหรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้ | สปป.ลาว มีเหตุสงสัยที่จะสร้างความเสียหายก็มีการตรวจสอบแล้ว |

**ตารางที่ 4.2** (ต่อ)

| | สปป.ลาว | ประเทศสิงคโปร์ | ประเทศไทย | หมายเหตุ |
|---|---|---|---|---|
| 4.2 อำนาจในการค้นหรือเข้ายึด | ใช้มาตรการทางกฎหมายในการจับตัว กักตัว ปล่อยตัว กักขัง ตรวจค้น และรายงานเป็นลายลักษณ์อักษรให้องค์การอัยการประชาชนทราบ | เจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจตามกฎหมายสืบสวนคดีความการกระทำผิดสามารถกระทำการใช้หรือทำให้เกิดการใช้ซึ่งคอมพิวเตอร์เพื่อค้นข้อมูลหรือที่มีอยู่ในคอมพิวเตอร์นั้น | ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้ | สปป.ลาว ใช้มาตรการทางกฎหมายเช่นเดียวกับการปฏิบัติกับการกระทำผิดทางอาญาทั่วไป |
| 4.3 การเรียกข้อมูลจราจรทางคอมพิวเตอร์ | ไม่ได้มีการบัญญัติไว้ | เจ้าหน้าที่ตำรวจหรือบุคคลที่ได้รับมอบอำนาจตามกฎหมายอาจขอความช่วยเหลือจาก (1) บุคคลใดที่เจ้าหน้าที่สงสัยว่าจะใช้คอมพิวเตอร์ในการกระทำผิดหรือเคยใช้กระทำผิด หรือ (2) บุคคลที่รับผิดชอบ หรือเกี่ยวข้องกับตาม (1) ดังกล่าว | เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง | สปป.ลาว ยังไม่มีการบัญญัติไว้ |

# บทที่ 5

# บทสรุป และข้อเสนอแนะ

เทคโนโลยีคอมพิวเตอร์ถือเป็นบทบาทสำคัญในการพัฒนาเศรษฐกิจ และการดำรงชีวิตของมนุษย์ และเป็นส่วนหนึ่งในการขยายตัวของสังคมด้านการติดต่อสื่อสารซึ่งกันและกันอย่างไร้ขีดจำกัดทางพรมแดน อีกทั้งเทคโนโลยีคอมพิวเตอร์ได้มีการเจริญเติบโตและเป็นฐานสำคัญในการพัฒนาเศรษฐกิจในทุก ๆ ด้าน โดยเฉพาะอย่างยิ่งการใช้เทคโนโลยีที่ทันสมัยในการเก็บข้อมูล การส่งข้อมูล และการประเมินผล เป็นต้น หากมีการกระทำใด ๆ อันก่อให้เกิดผลกระทบต่อระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ที่ทำให้เกิดความเสียหายต่อบุคคลอื่น รวมทั้งส่งผลกระทบต่อเศรษฐกิจ สังคม และความมั่นคงชองชาติ ซึ่งในบทนี้จะได้กล่าวสรุปเนื้อหาพร้อมทั้งเสนอแนะแนวทางที่เหมาะสม โดยมีรายละเอียด ดังนี้

## 5.1 บทสรุป

พัฒนาการทางด้านเทคโนโลยีคอมพิวเตอร์ที่มีการเจริญเติบโตอย่างไม่หยุดยั้ง ไร้ขีดจำกัด และก่อให้เกิดประโยชน์อย่างมากมายไม่ว่าจะเป็นด้านเศรษฐกิจ สังคม และการบริการระบบสาธารณูปโภค อย่างไรก็ตามหากมีผู้กระทำการอย่างใดอย่างหนึ่งในการใช้งานคอมพิวเตอร์ไปในทางที่ไม่ชอบ โดยการอาศัยความสลับซับซ้อนทางด้านเทคโนโลยีคอมพิวเตอร์ ประกอบกับกฎหมายที่มีอยู่ปัจจุบันยังไม่รองรับรูปแบบของการกระทำด้านอาชญากรรมทางคอมพิวเตอร์ อาจส่งผลกระทบให้การประกอบกิจการต่าง ๆ ที่ใช้เทคโนโลยีคอมพิวเตอร์ได้รับผลเสียหาย

จากการศึกษากฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศสิงคโปร์ ไทย และสหภาพยุโรป เห็นว่า กฎหมายที่มีอยู่ในปัจจุบันของ สปป.ลาว ยังไม่ครอบคลุมถึงรูปแบบการกระทำผิดของอาชญากรรมทางคอมพิวเตอร์ กล่าวคือ การกระทำต่อข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ที่มีลักษณะของการกระทำที่ไม่มีรูปร่างและไม่สามารถมองเห็น และรูปแบบของการกระทำผิดเปลี่ยนแปลงไปจากลักษณะของการกระทำผิดทางอาญาทั่วไป ที่กฎหมายอาญา ค.ศ. 2005 ที่ใช้บังคับในปัจจุบันมุ่งคุ้มครองวัตถุแห่งการกระทำผิดส่วนใหญ่เป็นสิ่งที่สามารถจับต้องได้

และสามารถมองเห็น แต่อย่างไรก็ตามหากการสืบสวนสอบสวนหากผู้กระทำความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ได้แล้ว จะปรับใช้รูปแบบของการกระทำดังกล่าวเข้ากับกฎหมายอาญา ค.ศ. 2005 อาจพบปัญหาในการตีความของการกระทำนั้นเข้าองค์ประกอบของการกระทำผิดฐานใด เช่น การเข้าถึงข้อมูลที่มีระบบป้องกันเฉพาะโดยไม่ได้รับอนุญาต การดักรับข้อมูลคอมพิวเตอร์ที่อยู่ในระหว่างการส่ง เป็นต้น ที่เป็นการใช้เทคโนโลยีคอมพิวเตอร์ในการกระทำผิดดังกล่าว แต่กฎหมายอาญา ค.ศ. 2005 ซึ่งเป็นกฎหมายหลักของประเทศในการดำเนินคดีเอาตัวผู้กระทำผิดมาลงโทษ ไม่สามารถรองรับรูปแบบของการกระทำผิดของอาญากรรมทางคอมพิวเตอร์ ด้วยเหตุนี้จึงทำให้การดำเนินคดีต่อผู้กระทำผิดไม่ได้รับโทษเท่าที่ควร ฉะนั้น หากมีผู้ใช้ความสลับซับซ้อนของระบบคอมพิวเตอร์เพื่อกระทำต่อระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ ซึ่งส่งผลกระทบต่อความมั่นคงของรัฐ เศรษฐกิจ และสังคมหรือแม้แต่บุคคล ผู้กระทำผิดนั้นก็จะมิได้รับการลงโทษเนื่องจากกฎหมายมิได้บัญญัติเป็นความผิดไว้

นอกจากการศึกษาวิจัยปัญหาและอุปสรรคเกี่ยวกับกฎหมายอาญา ค.ศ. 2005 แล้วผู้วิจัยยังศึกษาเกี่ยวกับกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2012 และดำรัฐว่าด้วยการคุ้มครองข้อมูลข่าวสารผ่านทางอินเทอร์เน็ต ค.ศ. 2014 ของ สปป.ลาว และลักษณะของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พบว่าปัญหาเกี่ยวกับการกระทำผิดของอาชญากรรมทางคอมพิวเตอร์ ไม่ว่าจะเป็นรูปแบบของการกระทำความผิดที่แตกต่างจากการกระทำความผิดรูปแบบเดิมที่กฎหมายมุ่งคุ้มครองในปัจจุบัน ลักษณะของฐานความผิดที่มีความสลับซับซ้อนยากต่อการมองเห็น และโทษที่จะปรับใช้ในกรณีการกระทำความผิดดังกล่าว หากมีการกำหนดฐานความผิดดังกล่าวไม่ชัดเจนอาจก่อให้เกิดปัญหาในการลงโทษได้ แต่อย่างไรก็ตามอาชญากรรมทางคอมพิวเตอร์ก็เป็นปัญหาใหม่ในสังคมลาว เนื่องจากการกระทำดังกล่าวเป็นการกระทำที่ทำให้ผู้คนเห็นหรือสัมผัสได้ยาก กล่าวคือเป็นการกระทำของผู้ที่ใช้งานทางด้านเทคโนโลยีคอมพิวเตอร์เพื่อกระทำการอย่างใดอย่างหนึ่งต่อข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ ที่อาจส่งผลกระทบต่อผู้ที่ใช้งานเทคโนโลยีสารสนเทศเท่านั้น

จากรูปแบบของการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์ ซึ่งอาจก่อให้เกิดผลกระทบต่อเศรษฐกิจ สังคม และความมั่นคงของประเทศ กล่าวคือ อาชญากรรมทางคอมพิวเตอร์เป็นการกระทำที่ใช้ลักษณะความสลับซับซ้อนของคอมพิวเตอร์ในการล่วงรู้ข้อมูลความลับ กระทำการดัดแปลงแก้ไขข้อมูล ดักรับข้อมูล และการกระทำการใด ๆ ต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งในปัจจุบัน สปป.ลาว มีมาตรการทางกฎหมายและมาตรการลงโทษเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์แต่ยังมีความไม่ชัดเจนและไม่เหมาะสม เมื่อเกิดปัญหากรณีมีการกระทำต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่สร้างความเสียหายและส่งผลกระทบให้แก่

การใช้งานคอมพิวเตอร์ การจะนำผู้กระทำผิดดังกล่าวมาลงโทษก็เป็นปัญหาในข้อกฎหมาย ซึ่งหลักกฎหมายอาญาระบุว่าไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย อาชญากรรมทางคอมพิวเตอร์ยังอยู่ในระยะเริ่มแรก แต่ก็มีแนวโน้มว่าจะมีการขยายตัวอย่างรวดเร็ว จึงควรที่จะศึกษาและเตรียมตัวรับมือกับปัญหาให้ทันกับสถานการณ์โดยเฉพาะอย่างยิ่งการศึกษาถึงกฎหมายที่มีในปัจจุบันว่าจะสามารถลงโทษผู้กระทำความผิดได้เพียงใด เมื่อพิจารณาถึงบทบาทและความสำคัญของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ในยุคที่สังคมมีการใช้สิ่งดังกล่าวในเกือบทุกกิจกรรมของมนุษย์แล้ว ก็สมควรอย่างยิ่งที่กฎหมายจะต้องให้ความคุ้มครองการใช้งานทางเทคโนโลยีคอมพิวเตอร์ให้เกิดประโยชน์สูงสุด เนื่องจากปรากฏการณ์ทางด้านเทคโนโลยีสารสนเทศในปัจจุบัน เช่น การลักลอบนำข้อมูลสารสนเทศของผู้อื่นที่เก็บไว้ในคอมพิวเตอร์ไปใช้ประโยชน์ก่อนผู้เป็นเจ้าของที่แท้จริง หรือการที่บุคคลอื่นสามารถเข้าถึงระบบคอมพิวเตอร์ และแก้ไขเปลี่ยนแปลงข้อมูลที่เก็บไว้ในคอมพิวเตอร์ ย่อมส่งผลกระทบและทำให้ผู้เป็นเจ้าของเสียหาย ซึ่งปัจจุบัน สปป.ลาว มีกฎหมายที่กำหนดรูปแบบฐานความผิดดังกล่าวแต่ยังไม่ครอบคลุมการกระทำผิดบางประการที่จะสามารถนำผู้กระทำผิดมาฟ้องลงโทษได้

นอกจากนั้นการกระทำของอาชญากรรมทางคอมพิวเตอร์เป็นการะกระทำที่ทำได้ในระยะเวลาสั้น ๆ และการทำลายหลักฐานก็ทำได้อย่างรวดเร็วโดยอาจส่งผลเสียหายในวงกว้าง แต่เนื่องจากการให้สิทธิอำนาจเจ้าหน้าที่ในการสืบสวนสอบสอบสวนใน สปป.ลาว นั้น ยังมีขั้นตอนและกระบวนการที่มีขั้นตอนของการดำเนินการที่ใช้เวลาพอสมควร กล่าวคือ ต้องมีการยื่นคำร้องหรือแจ้งความแล้วเจ้าพนักงานสืบสวนสอบสวนจะดำเนินการพิจารณาคำร้องดังกล่าวภายในกำหนดอย่างมากไม่เกิน 7 วัน ซึ่งอำนาจหน้าที่ในการสืบสวนสอบสวนหาตัวผู้กระทำความผิดมาลงโทษเป็นไปด้วยความยากลำบาก และยังได้มีการประสานสมทบกับหน่วยงานที่เกี่ยวข้อทางด้านการใช้เทคโนโลยีคอมพิวเตอร์และอินเทอร์เน็ต แต่การกระทำผิดของอาชญากรรมทางคอมพิวเตอร์เป็นการกระทำที่เกี่ยวกับการใช้เทคโนโลยีคอมพิวเตอร์ที่ทันสมัยซึ่งสูญหายและทำลายได้โดยง่าย

เพื่อป้องกันและปราบปรามการกระทำความผิดต่อคอมพิวเตอร์ ควรจะต้องอาศัยมาตรการทางกฎหมาย นอกจากจะต้องมีการแก้ไขปรับปรุงกฎหมายสารบัญญัติ เพื่อกำหนดฐานความผิดให้ครอบคลุมถึงการกระทำความผิดรูปแบบใหม่ที่อยู่นอกขอบเขตของกฎหมายที่ใช้บังคับอยู่ปัจจุบันแล้ว ยังต้องปรับปรุงกฎหมายวิธีสบัญญัติเพื่อให้สามารถดำเนินคดีกับผู้กระทำความผิดได้อย่างมีประสิทธิภาพและเป็นธรรมด้วย แต่เนื่องจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มีลักษณะของการกระทำผิดที่ไม่มีรูปร่าง

## 5.2 ข้อเสนอแนะ

จากการศึกษาวิจัยสามารถเสนอแนะได้ดังนี้

เสนอให้ สปป.ลาว มีการบัญญัติกฎหมายเพื่อให้ครอบคลุมถึงการกระทำของอาชญากรรมทางคอมพิวเตอร์โดยนำหลักทฤษฎีเกี่ยวกับการบัญญัติกฎหมายอาญา กล่าวคือ ในการกำหนดการกระทำใดการกระทำหนึ่งเป็นความผิด และมีโทษนั้นต้องบัญญัติให้ชัดแจ้งกับรูปแบบของการกระทำและโทษที่จะลงต่อผู้กระทำความผิดในฐานนั้น ๆ ซึ่งกฎหมายจะต้องให้ความคุ้มครองความลับ ความครบถ้วน และความสามารถในการใช้ประโยชน์ได้ซึ่งเป็นคุณลักษณะของสิ่งเหล่านี้ให้ครบถ้วน รวมทั้งการให้ความคุ้มครองสิทธิในทรัพย์สินของเจ้าของทรัพย์สินจากการกระทำความผิดของอาชญากรรมทางคอมพิวเตอร์ด้วยโดยมีการกำหนดรูปแบบต่าง ๆ ให้ชัดเจนว่าเป็นการกระทำความผิดดังนั้นผู้เขียนเห็นว่าควรมีการตรากฎหมายเฉพาะเพื่อเป็นการไม่กระทบต่อลักษณะขององค์ประกอบความผิดทางอาญาที่มีอยู่เดิม

ปัจจุบัน สปป.ลาว ได้มีการจัดทำร่างกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับระบบคอมพิวเตอร์ ค.ศ. ... ต่อมาได้มีการปรับปรุงเนื้อหา และเปลี่ยนชื่อร่างกฎหมายดังกล่าวเป็น “ร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ...” ซึ่งได้ผ่านการรับรองจากกองประชุมสมัยสามัญ ครั้งที่ 9 ของสภาแห่งชาติ ชุดที่ 7 ของ สปป.ลาว ซึ่งกฎหมายดังกล่าวจะมาปรับใช้รองรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แต่เนื้อหากฎหมายบางมาตรายังไม่ครอบคลุมถึงลักษณะของการกระทำบางอย่างของอาชญากรรมทางคอมพิวเตอร์ โดยผู้เขียนสามารถเสนอแนะได้ดังนี้

5.2.1 เพิ่มเติมการเข้าถึงข้อมูลทางคอมพิวเตอร์ของผู้อื่นที่มีมาตรการป้องกันเฉพาะโดยไม่ได้รับอนุญาต เนื่องจากความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต ข้อมูลนั้นต้องเป็นข้อมูลที่มีการเก็บหรือส่งด้วยวิธีการทางอิเล็กทรอนิกส์ ซึ่งไม่ได้หมายความรวมถึงระบบคอมพิวเตอร์ เพราะระบบคอมพิวเตอร์ไม่สามารถเก็บหรือส่งได้ ถึงแม้จะมีการบัญญัติเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดแล้ว ซึ่งโดยทั่วไปจะมีการเข้าถึงระบบคอมพิวเตอร์ก่อน แต่บางครั้งการกระทำดังกล่าวอาจไม่จำเป็นต้องมีการกระทำความผิดฐานเข้าถึงระบบคอมพิวเตอร์ เพราะหากมีการกระทำที่เข้าถึงข้อมูลของผู้อื่นแล้ว ถึงแม้ว่าการกระทำจะไม่ได้มีการดัดแปลงแก้ไข แต่อาจก่อให้เกิดผลเสียหายแก่ผู้เป็นเจ้าของได้ ด้วยเหตุนี้เห็นควรที่จะบัญญัติถึงการเข้าไปโดยไม่ได้รับอนุญาตก็เป็นความผิดแล้ว

5.2.2 ควรปรับปรุงมาตรา 12 แห่งร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... เกี่ยวกับการกำหนดฐานความผิดเกี่ยวกับการดักรับข้อมูลในระบบ

คอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งเป็นการดักรับข้อมูลที่อยู่ในระหว่างการรับหรือส่งผ่านระบบคอมพิวเตอร์ ด้วยการใช้เครื่องมือทางอิเล็กทรอนิกส์ ซึ่งผู้เขียนเห็นควรให้มีการบัญญัติเพิ่มเติมเกี่ยวกับข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ เนื่องจากข้อมูลคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะนั้นมิได้มีการเข้ารหัสการเข้าถึงข้อมูลคอมพิวเตอร์ที่มีการส่ง แต่ในทางกลับกันข้อมูลที่มีการเข้ารหัสผ่านก็ย่อมแสดงให้เห็นว่ามิได้มีไว้เพื่อประโยชน์สาธารณะ กล่าวคือเมื่อผู้ส่งข้อมูลดังกล่าวผ่านระบบคอมพิวเตอร์ที่ไม่มีมาตรการป้องกันการเข้าถึงข้อมูล ผู้กระทำการดักรับข้อมูลนั้นก็ไม่มีความผิด

5.2.3 ควรปรับปรุงมาตรา 15 (2) แห่งร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... เกี่ยวกับการรบกวนระบบคอมพิวเตอร์ “การส่งข้อมูลคอมพิวเตอร์หรือจดหมายทางอิเล็กทรอนิกส์ โดยมีการปกปิดที่อยู่หรือแหล่งที่มาของผู้ส่งเพื่อรบกวนและ/หรือทำลายการปฏิบัติงานของระบบคอมพิวเตอร์” เห็นควรมีการบัญญัติเพิ่มเติมเกี่ยวกับการปลอมแปลงแหล่งที่อยู่ของผู้ส่งด้วย กล่าวคือ ผู้ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์นั้นไม่ได้มีการปกปิดที่อยู่หรือแหล่งที่มาแต่มีการปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว ซึ่งการปลอมแปลงแหล่งที่มาของจดหมายส่อให้เห็นถึงเจตนาอันไม่สุจริตในการส่งข้อมูลนั้น

5.2.4 ในการกำหนดฐานความผิดนั้น ผู้เขียนเห็นควรให้มีการบัญญัติให้ชัดเจนเกี่ยวกับผู้ใดกระทำโดยมิชอบ ซึ่งทำให้ผู้อื่นได้รับความเสียหาย เช่น มาตรา 17 ของร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... “การทำลายข้อมูลคอมพิวเตอร์หมายถึง การลบ การดัดแปลง และ/หรือการปลอมแปลงข้อมูลคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์เพื่อทำให้ข้อมูลหรือระบบคอมพิวเตอร์นั้นเสียหาย” จะเห็นได้ว่าบทบัญญัติดังกล่าวยังไม่ชัดเจนเกี่ยวกับผู้กระทำความผิด และผู้ถูกเสียหาย ด้วยเหตุนี้ผู้เขียนเห็นควรให้มีการบัญญัติดังเช่นมาตรา 9 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 “ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ” ซึ่งในมาตราดังกล่าวได้มีการบัญญัติถึงผู้กระทำ และผู้ถูกกระทำไว้ด้วย

5.2.5 เกี่ยวกับมาตรการในการลงโทษในร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ได้มีการบัญญัติเกี่ยวกับการลงโทษผู้กระทำความผิดคือ บุคคล นิติบุคคล หรือองค์กร ที่กระทำการละเมิดต่อกฎหมาย ด้วยวิธีการกล่าวเตือน ศึกษาอบรมลงวินัย ปรับ ชดใช้ค่าเสียหายทางแพ่ง หรือถูกลงโทษทางอาญา ตามแต่กรณีของการกระทำ ซึ่งการกระทำความผิดของอาชญากรรมคอมพิวเตอร์นั้นเป็นการกระทำที่บางกรณีไม่อาจสามารถประเมินค่าเป็นตัวเงินได้อย่างชัดเจน จึงเห็นควรให้ยกเลิกมาตรการในการกล่าวเตือน เนื่องจากการกระทำ

ผิดทางคอมพิวเตอร์มีลักษณะของการกระทำผิดที่จะส่งผลกระทบต่อเศรษฐกิจ สังคม และประเทศโดยภาพรวมของประเทศในระยะยาวได้ ดั่งนั้น จึงควรกำหนดมาตรการลงโทษทางอาญาที่มีความชัดเจนจะส่งผลดีกว่า

5.2.6 การให้อำนาจหน้าที่แก่พนักงานเจ้าหน้าที่ในการหาตัวผู้กระทำความผิดมาลงโทษนั้น ในร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ค.ศ. ... ได้มีการกำหนดขั้นตอนในกรณีเกิดเหตุฉุกเฉินเกี่ยวกับระบบคอมพิวเตอร์ของตนต่อกระทรวงไปรษณีย์โทรคมนาคม และการสื่อสาร เพื่อค้นคว้าแนะนำวิธีการแก้ไขทางด้านเทคนิค แต่การดำเนินคดีต่อผู้กระทำความผิดทางระบบคอมพิวเตอร์นั้น ต้องมีขั้นตอนในการดำเนินคดีทางระบบคอมพิวเตอร์กล่าวคือ มีการแจ้งความ และพิจารณาการแจ้งความ การค้นหาหลักฐานเกี่ยวกับการกระทำความผิดทางระบบคอมพิวเตอร์ การสืบสวน-สอบสวนคดี การสั่งฟ้อง การดำเนินคดี และการบังคับคดี ซึ่งจะเห็นว่ากว่าจะได้ทำการสืบสวน-สอบสวนหาตัวผู้กระทำความผิดดังกล่าวมีหลายขั้นตอน ซึ่งลักษณะของการกระทำผิดทางคอมพิวเตอร์เป็นการกระทำที่ใช้เทคโนโลยีทางคอมพิวเตอร์ที่ง่ายต่อการทำลายหลักฐานและใช้เวลาไม่นาน นอกจากนั้นการทำงานของพนักงานเจ้าหน้าที่ในการจัดการหรือดำเนินคดีกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือใช้คอมพิวเตอร์กระทำความผิด ซึ่งพนักงานเจ้าหน้าที่จะกระทำการใดอันเป็นการกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนจะต้องมีกฎหมายให้อำนาจหน้าที่แก่พนักงานเจ้าหน้าที่ ด้วยเหตุนี้ผู้เขียนเห็นว่าควรมีการบัญญัติการให้อำนาจหน้าที่เป็นการเฉพาะแก่พนักงานเจ้าหน้าที่ที่จะดำเนินอย่างใดอย่างหนึ่งได้ในการส่งให้หรือมีหนังสือสอบถาม เรียกดูข้อมูลคอมพิวเตอร์ และกำหนดรายละเอียดเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้ชัดเจน ฉะนั้นในการพัฒนากฎหมายอาชญากรรมทางคอมพิวเตอร์ขึ้นบังคับใช้ต้องพิจารณาในเรื่องที่เกี่ยวกับการใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเพื่อหาตัวผู้กระทำความผิดนั้น ต้องอาศัยพนักงานสืบสวนสอบสวนหรือบุคคลที่เกี่ยวข้องในกระบวนการยุติธรรมที่มีความรู้ความเชี่ยวชาญทางคอมพิวเตอร์เพื่อที่จะติดตามลักษณะของการกระทำและหาผู้กระทำความผิดอย่างถูกต้อง และต้องอาศัยความเด็ดขาดและรวดเร็ว เพื่อให้ทันต่อการก่ออาชญากรรมทางคอมพิวเตอร์ที่มีความรวดเร็วดังกล่าว อันจะสามารถสืบสวนหาตัวผู้กระทำความผิดหรืออาชญากรรมมาลงโทษได้อย่างทันท่วงที

# รายการอ้างอิง

# รายการอ้างอิง


กรมอาเซียน กระทรวงการต่างประเทศ. (ม.ป.ป.). *Asean mini book*. กรุงเทพฯ: กรมฯ.

กระทรวงไปรษณีย์ โทรคมนาคมและการสื่อสาร. (2014). *บทเสนอเกี่ยวกับการร่างกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์*. นครหลวงเวียงจันทน์: กระทรวงฯ.

กรุง เหลืองมโนธรรม. (2548). *การศึกษาประเด็นทางกำหมายเกี่ยวกับการจัดการความไม่มั่นคงของระบบคอมพิวเตอร์ในสังคมไทย: ศึกษาเฉพาะภัยไวรัสคอมพิวเตอร์แฮกเกอร์และสแปมเมล์*. สารนิพนธ์นิติศาสตรมหาบัณฑิต. มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

กองกรรมาธิการ สำนักงานเลขาธิการวุฒิสภา. (2539). *รายงานของคณะกรรมาธิการ การวิทยาศาสตร์ เทคโนโลยีและพลังงาน วุฒิสภา, พิจารณาศึกษาเรื่อง เทคโนโลยีสารสนเทศกับกฎหมายโทรคมนาคมในยุคโลกาภิวัตน์*. กรุงเทพฯ: สำนักงานเลขาธิการวุฒิสภา.

กิดานันท์ มลิทอง. (2539). *อธิบายศัพท์คอมพิวเตอร์ อินเทอร์เนต มัลติมีเดีย*. กรุงเทพฯ, จุฬาลงกรณ์มหาวิทยาลัย.

เกียรติขจร วัจนะสวัสดิ์. (2544). *คำอธิบายกฎหมายอาญาภาค 1* (พิมพ์ครั้งที่ 7). กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์.

เกียรติขจร วัจนะสวัสดิ์. (2551). *คำอธิบายกฎหมายอาญา ภาค 1 บทบัญญัติทั่วไป* (พิมพ์ครั้งที่ 10). กรุงเทพฯ: พลสยาม.

ข่าวลือ ฆ่าเด็กน้อยเอาอวัยวะ. (2014, 5 มิถุนายน). *หนังสือพิมพ์เวียงจันทน์ใหม่*. สืบค้นเมื่อ 23 พฤศจิกายน 2558, จาก http://www.vientianemai.net/teen/khao/1/11950

คณิต ณ นคร. (2543). *กฎหมายอาญา ภาคทั่วไป*. กรุงเทพฯ, วิญญูชน.

ฉัทปณัย รัตนพันธ์. (2547). *อาชญากรรมทางคอมพิวเตอร์: ศึกษาการกำหนดฐานความผิดและการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์*. สารนิพนธ์นิติศาสตรมหาบัณฑิต. มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

ชัชวาลย์ สุขสมจิตร์. (ม.ป.ป.). *อาชญากรรมทางเศรษฐกิจกับการบังคับใช้กฎหมาย*. กรุงเทพฯ: วิทยาลัยการยุติธรรม.

ณัฐกร วิทิตานนท์. (2557). กฎหมายคอมพิวเตอร์ในประเทศไทย: พัฒนาการ ฐานความผิด และปัญหาการใช้บังคับ. ใน *Rapee, School of law, Mae Fah Luang University*. กรุงเทพฯ: วิญญูชน.

ดาวเรืองยืนยันไม่มีส่วนเกี่ยวข้องกับการขนส่งสิ่งผิดกฎหมาย. (2015, 15 กันยายน). *หนังสือพิมพ์เวียงจันทน์ใหม่*. สืบค้นเมื่อ 22 พฤศจิกายน 2558, จาก http://www.vientianemai.net/teen/khao/1/14787 ดาวเรือง

ทวิเกียรติ มีนะกนิษฐ. (2552). *มุมมองใหม่ในกฎหมายอาญา*. กรุงเทพฯ: วิญญูชน.

ทวีเกียรติ มีนะกนิษฐ. (2555). *ประมวลกฎหมายอาญา ฉบับอ้างอิง* (พิมพ์ครั้งที่ 29). กรุงเทพฯ: วิญญูชน.

ธาริต เพ็งดิษฐ์. (ม.ป.ป.). แนวทางการสืบสวนสอบสวนคดีพิเศษ, ใน *เอกสารประกอบการบรรยายหลักสูตรการบริหารงานยุติธรรมระดับกลาง รุ่นที่ 2 (ยธก. 2)*. กรุงเทพฯ: สถาบันพัฒนาข้าราชการฝ่ายอัยการ.

บุญเพราะ แสงเทียน. (2545). *กฎหมายอาญา 1 (ภาคบทบัญญัติทั่วไป) แนวประยุกต์*. กรุงเทพฯ: วิทยพัฒน์.

ฝ่ายศึกษาวิจัยประเด็นด้านจริยธรรม กฎหมาย และผลกระทบทางสังคมของเทคโนโลยีสารสนเทศ. (2552). *กฎหมายเทคโนโลยีสารสนเทศ IT Laws*. ปทุมธานี: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

พรเพชร วิชิตชลชัย. (ม.ป.ป.). *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*. ม.ป.ท.: ม.ป.พ.

พรรณสุวัชร รติพงค์สิทธิ์. (2550). *อาชญากรรมทางคอมพิวเตอร์: ศึกษาวิเคราะห์หลักเกณฑ์ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ....* วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยรามคำแหง, กรุงเทพฯ.

ไพจิตร สวัสดิสาร. (2550). *การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายที่เกี่ยวกับคอมพิวเตอร์*. กรุงเทพฯ: ชวนพิมพ์.

มหาวิทยาลัยสุโขทัยธรรมาธิราช. (2548). *เอกสารการสอนชุดวิชา กฎหมายอาญา 1: ภาคบทบัญญัติทั่วไป หน่วยที่ 1-7*. นนทบุรี: มหาวิทยาลัยฯ.

มหาวิทยาลัยสุโขทัยธรรมาธิราช. (2548). *เอกสารการสอนชุดวิชา การเมืองการปกครองของประเทศในเอเชีย หน่วยที่ 8-15*. นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมาธิราช.

มานิตย์ จุมปา (บรรณาธิการ). (2551). *ความรู้พื้นฐานเกี่ยวกับกฎหมาย* (พิมพ์ครั้งที่ 8). กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย.

มานิตย์ จุมปา. (2554). *คำอธิบายกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์* (พิมพ์ครั้งที่ 2). กรุงเทพฯ: วิญญูชน.

วรณัฐ บุญเจริญ. (2557). *มาตาการทางกฎหมายของอาเซียนเพื่อการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์*. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต. มหาวิทยาลัยแม่ฟ้าหลวง, เชียงราย.

วัลลิกา อุ่นศรี (เนติบัณลือฤทธิ์). (2544). *ปัญหาการรวบรวมและพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีอาญา*. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต. มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

วิกรณ์ รักษ์ปวงชน. (2548). หน่วยที่ 3 การใช้บังคับกฎหมายอาญา, ใน *เอกสารการสอนชุดวิชา กฎหมายอาญา 1: ภาคบทบัญญัติทั่วไป หน่วยที่ 1-7*. นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมาธิราช.

วีระพงษ์ บุญโญภาส. (2549). *อาชญากรรมทางเศรษฐกิจ*. กรุงเทพฯ: นิติธรรม.

ศูนย์สกัดกั้นและแก้ไขเหตุฉุกเฉินทางคอมพิวเตอร์. (ม.ป.ป.). *แจ้งเตือนภัยทางอินเทอร์เน็ต*. สืบค้นเมื่อ 23 พฤศจิกายน2558, จาก https://www.laocert.gov.la/News-Categories

ศูนย์อินเทอร์เน็ตแห่งชาติ. (2017, 17 มิถุนายน). เรื่องปัญหาจดหมายเอเล็กทรอนิกส์ (E-mail), *หนังสือ*. เลขที่ 646/สอช.

สถาบันการพลศึกษา วิทยาเขตสุพรรณบุรี. (ม.ป.ป.). *เทคโนโลยีสารสนเทศเพื่อการเรียนรู้ บทที่ 6 อินเตอร์เน็ต:ISP คืออะไร*. สืบค้นเมื่อ 3 ธันวาคม 2558, จาก http://www.ipesp.ac.th/learning/071001/chapter6/UN6_2.html

สาวตรี สุขศรี. (2552, 9 พฤศจิกายน). *ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์*. สืบค้นเมื่อ 1 พฤศจิกายน 2557, จาก https://facthai.wordpress.com/2009/11/09/ประวัติศาสตร์-อาชญากรรม/

สำนักกฎหมายนิติศาสตร์ขาดรัก. (2557, 1 มิถุนายน). *กฎหมายอาญา: วัตถุประสงค์ของการลงโทษ*. สืบค้นเมื่อ 6 มิถุนายน 2558, จาก http://chalermwutsa.blogspot.com/2014/06/blog-post.html

สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ. (2552). *ความรู้ทั่วไปเกี่ยวกับการกำกับดูแลกิจการโทรคมนาคมและการออกใบอนุญาตประกอบกิจการโทรคมนาคม*. กรุงเทพฯ: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ.

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ. (2542). *ประเทศไทยกับการพัฒนากฎหมายเทคโนโลยีสารสนเทศ*. กรุงเทพฯ: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ.

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ. (2543). *โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ*. กรุงเทพฯ: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ.

สำนักบริหารกลาง. (ม.ป.ป.). *รวมสาระน่ารู้เกี่ยวกับกฎหมายไอที*. กรุงเทพฯ: สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร.

แสวง บุญเฉลิมวิภาส. (2544). *หลักกฎหมายอาญา* (พิมพ์ครั้งที่ 3). กรุงเทพฯ: วิญญชน.

หยุด แสงอุทัย. (2544). *กฎหมายอาญา ภาค 1* (พิมพ์ครั้งที่ 18). กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์.

หยุด แสงอุทัย. (2545). *ความรู้เบื้องต้นเกี่ยวกับกฎหมายทั่วไป* (พิมพ์ครั้งที่ 15). กรุงเทพฯ, มหาวิทยาลัยธรรมศาสตร์.

หยุด แสงอุทัย. (2556). *ความรู้เบื้องต้นเกี่ยวกับกฎหมายทั่วไป* (แก้ไขปรับปรุงโดย สมยศ เชื้อไทย, พิมพ์ครั้งที่ 19), กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์.

องอาจ เทียนหิรัญ. (2546). *อาชญากรรมทางคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์*. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต. มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ:

อภิรัตน์ เพ็ชรศิริ. (2548). *ทฤษฎีอาญา*. กรุงเทพฯ: วิญญชน.

อัจฉรียา ชูตินันทน์. (2557). *อาชญาวิทยาและทัณฑวิทยา* (พิมพ์ครั้งที่ 2). กรุงเทพฯ: วิญญชน.

Blohnone. (2555, 22 พฤศจิกายน). *รู้จัก ITU สหภาพโทรคมนาคมนานาชาติ ผู้กำหนดมาตรฐานโทรคมนาคมโลก*. สืบค้นเมื่อ 8 ตุลาคม 2557, จาก http://www.blognone.com/node/38344

English Daily. (2013, 19 ตุลาคม). *Hacking: ศัพท์ภาษาอังกฤษว่าด้วยการโจรกรรมข้อมูล*. สืบค้นเมื่อ 1 พฤศจิกายน 2557, จาก http://www.dailyenglish.in.th/hacking-vocabularies/

European Union. (n.d.). *EU member countries*. Retrieved June 7, 2015, from http://europa.eu/about-eu/countries/member-countries/

Grabosky, P. N. & Smith, R. G. (1998). *Crime in the digital age*. Australia: Transaction Publishers.

International Telecommunication Union. (2012). *Draft of the future ITRs*. Retrieved September 5, 2014, from http://www.itu.int/en/wcit-12/Documents/draft-future-itrs-public.pdf

International Telecommunication Union. (2012). *Final ACTS of the world conference on international telecommunications*. Dubai: ITU. Retrieved April 19, 2014, from http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

International Telecommunication Union. (n.d.). *ITU Member states*. Retrieved May 7, 2015, from http://www.itu.int/online/mm/scripts/mm.list?_search=ITUstates&_languageid=1

Internet Governance. (ม.ป.ป.). *โครงการศึกษาวิจัยการอภิบาลกิจการเกี่ยวกับอินเตอร์เน็ต (Internet Governance)*. สืบค้นเมื่อ 30 พฤศจิกายน 2557, จาก http://www.nectec.or.th/pld/igovernance/index.htm

Lawyerthai.com. (ม.ป.ป.). *กฎหมายอาญากรรมทางคอมพิวเตอร์ตอน 4: กำหนดฐานความผิด และบทกำหนดโทษ*. สืบค้นเมื่อ 19 มีนาคม 2558, จาก http://www.lawyerthai.com/articles/it/031.php

Lennon, L. Y.-c. (2012). *Cybercrime in the greater China region: Regulatory responses and crime prevention across the Taiwan strait*. United Kingdom: Edward Elgar publishing.

Organization for Co-operation Development. (1986). *Computer related criminality: Analysis of legal politics in the OECD area*. Paris: OECD.

Sasiwimontan. (2554, 24 พฤศจิกายน). *หน่วยที่ 10 กฎหมายและความปลอดภัยบนอินเตอร์เน็ต*. สืบค้นเมื่อ 5 มีนาคม 2558, จาก http://sasiwimontan.blogspot.com/2011/11/10.html

SRI international. (1979). *The criminal justice resource manual on computer crime*. Menlo Park, CA: SRI international.

TDRI. (1991). *The barrier to and strategies for technology acquisition*. Bangkok: Thailand Development Research Institute.

Thainetizen Network. (2555, 9 พฤศจิกายน). *(สรุปสั้น ๆ) การมีส่วนร่วมในการจัดทำนโยบายอินเทอร์เน็ต:กระบวนการระดับภูมิภาคและระดับสากล#tcr2012*. สืบค้นเมื่อ 30 พฤศจิกายน 2557, จาก http://thainetizen.org/2012/09/internet-policy-making/

The Communication from the Commission to the Council, the European Parliament. (2001, 26 January). *The economic and social committee and the committee of the regions*. Retrieved October 17, 2013, from http://eur-lex.europa.eu/legal-content/.EN/ALL/;ELX_SESSIONID=GwZLJy5TV3NhBcLyRM882MNrT022QNfGD15kddlNskcvqkPkC7PJ!-7040371?uri=CELEX:52000DC0890

United Nations, International review of criminal policy. (1994). *The United Nations manual on computer-related crime*, *43-44*. Retrieved February 23, 2014, from http://www.uncjin.org/Documents/EighthCongress.html.

# ภาคผนวก

# ภาคผนวก ก

# ร่างกฎหมายว่าด้วยการกระทำความผิดทางระบบคอมพิวเตอร์

สาธารณรัฐ ประชาธิปไตย ประชาชนลาว

สันติภาพ เอกราช ประชาธิปไตย เอกภาพ วัฒนาถาวร

สภาแห่งชาติ เลขที่.../สภช

นครหลวงเวียงจันทน์, วันที่.../…./…

## ร่างกฎหมาย
## ว่าด้วยการกระทำความผิดทางระบบคอมพิวเตอร์

## ภาคที่ I
## บทบัญญัติทั่วไป

**มาตรา 1 วัตถุประสงค์**

กฎหมายฉบับนี้กำหนดหลักการ ระเบียบการ และมาตรการเกี่ยวกับการคุ้มครอง และการตรวจสอบการดำเนินคดีต่อผู้กระทำผิดทางคอมพิวเตอร์ เพื่อให้มีความถูกต้อง ยุติธรรม และสอดคล้องกับระเบียบกฎหมายของ สปป.ลาว ระเบียบการสากล สัญญา และสนธิสัญญาที่ สปป.ลาว เป็นภาคี เพื่อต้านและสกัดกั้นการกระทำผิดทางระบบคอมพิวเตอร์ ปกป้องข้อมูลข่าวสารทางระบบคอมพิวเตอร์ของรัฐ บุคคล นิติบุคคล และองค์กร รับประกันความปลอดภัยด้านข้อมูลข่าวสารทางระบบคอมพิวเตอร์ เป็นส่วนหนึ่งในการพัฒนาเศรษฐกิจ-สังคมของชาติ ทำให้ประเทศชาติมีความมั่นคง สังคมมีความสงบ มีความเป็นระเบียบเรียบร้อย และยุติธรรม

**มาตรา 2 การกระทำผิดทางระบบคอมพิวเตอร์**

การกระทำผิดทางระบบคอมพิวเตอร์ หมายถึง การเข้าถึงระบบคอมพิวเตอร์ การดักสกัดเอาข้อมูล การเผยแพร่ข้อมูลทางระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต การรบกวนระบบปฏิบัติการของระบบคอมพิวเตอร์ การทำลายข้อมูล การปลอมแปลงข้อมูล การกระทำผิดทางสื่อสังคมออนไลน์ และการกระทำอื่น ๆ ทางระบบคอมพิวเตอร์ ที่สร้างความเสียหายให้แก่รัฐ บุคคล นิติบุคคล และองค์กร

**มาตรา 3 การอธิบายคำศัพท์**

คำศัพท์ที่ใช้ในกฎหมายฉบับนี้มีความหมาย ดังนี้

1. **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์อิเล็กทรอนิกส์หรือชุดอุปกรณ์ของคอมพิวเตอร์ ที่เชื่อมโยงระบบการปฏิบัติการเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่น ๆ เพื่อให้อุปกรณ์อิเล็กทรอนิกส์หรือชุดอุปกรณ์ของคอมพิวเตอร์ ทำหน้าที่ประมวลผลข้อมูลแบบอัตโนมัติในคอมพิวเตอร์หนึ่งเครื่อง และหลายเครื่องที่เชื่อมต่อหากันผ่านเครือข่ายคอมพิวเตอร์ และเครือข่ายอินเทอร์เน็ต

2. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่น ๆ ในรูปแบบที่สามารถประมวลผล และทำให้ระบบคอมพิวเตอร์ทำงานได้

3. **ข้อมูลจราจรทางคอมพิวเตอร์** หมายถึง ข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการสื่อสารผ่านระบบคอมพิวเตอร์ ซึ่งถูกสร้างขึ้นโดยระบบคอมพิวเตอร์ ที่เป็นส่วนหนึ่งในการเชื่อมโยงของการสื่อสาร ที่บ่งบอกให้รู้ถึงแหล่งที่มา ต้นทาง ปลายทาง เส้นทาง วันเวลา ขนาด ระยะเวลาของการสื่อสาร ชนิดของการบริการและอื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

4. **ผู้ให้บริการ** หมายถึง

(ก) ผู้ให้บริการด้านการสื่อสารข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์แก่ผู้ใช้บริการโดยได้รับอนุญาตจากองค์การที่มีอำนาจเกี่ยวข้อง

(ข) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ ให้แก่บุคคล นิติบุคคล และองค์กร

5. **การประมวลข้อมูลแบบอัตโนมัติ** หมายถึง กระบวนการ ซึ่งข้อมูลในระบบคอมพิวเตอร์ได้รับการประมวลผลโดยโปรแกรมคอมพิวเตอร์

6. **โปรแกรมคอมพิวเตอร์** หมายถึง บรรดาคำสั่งที่ระบบคอมพิวเตอร์สามารถปฏิบัติได้เพื่อทำให้เกิดผลได้รับตามที่ได้กำหนดไว้

7. **ข้อมูลผู้ใช้บริการ** หมายถึง ข้อมูลใด ๆ ที่สามารถให้รู้ถึงประเภทของการติดต่อสื่อสาร ประเภทของการบริการ ที่อยู่ทางไปรษณีย์ ที่อยู่ภูมิลำเนา หมายเลขอินเทอร์เน็ต เบอร์โทรศัพท์ หรือ

เบอร์อื่น ๆ ที่ใช้เข้าระบบ และการใช้จ่ายสำหรับการบริการที่เกี่ยวข้องพร้อมทั้งข้อมูลอื่น ๆ ที่สามารถนำไปสู่การรู้บุคคลผู้ใช้บริการ

8. **มาตรการป้องกันเฉพาะ** หมายถึง การใช้กระบวนการเฉพาะเครื่องมือหรือโปรแกรมคอมพิวเตอร์พิเศษ เพื่อควบคุมหรือห้ามในการเข้าระบบคอมพิวเตอร์ของผู้ใช้บริการแต่ละประเภท

9. **สิ่งลามก** หมายถึง ข้อมูลต่าง ๆ ที่มีเนื้อหาเกี่ยวกับเด็ก วัยรุ่น และผู้ใหญ่รวมทั้งรูปภาพ ภาพเคลื่อนไหว เสียง และวิดีโอ (รวมทั้งการ์ตูน) ที่แสดงออกอย่างจะแจ้งเกี่ยวกับพฤติพรรมทางเพศ

10. **สื่อสังคมออนไลน์** หมายถึง สื่อหรือช่องทางการติดต่อสื่อสาร โดยผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งเป็นสื่อข่าวสารที่บุคคลทั่วไปสามารถนำเสนอ และเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะ โดยการใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารประเภทต่างๆ

**มาตรา 4 นโยบายของรัฐเกี่ยวกับการดำเนินคดีการกระทำความผิดทางระบบคอมพิวเตอร์**

รัฐสร้างเงื่อนไขและอำนวยความสะดวกให้แก่การดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์ ด้วยการวางระเบียบกฎหมาย สนองงบประมาน บุคลากร พาหนะ อุปกรณ์ และสร้างโครงสร้างพื้นฐาน เพื่อทำให้การดำเนินคดีมีความรวดเร็ว โปร่งใส ถูกต้องตามระเบียบกฎหมาย รับประกันความยุติธรรม และความปลอดภัยของข้อมูลข่าวสารทางระบบคอมพิวเตอร์

รัฐส่งเสริมการใช้คอมพิวเตอร์ ให้มีความปลอดภัย สะดวกรวดเร็ว และยุติธรรม พร้อมทั้งปกป้องสิทธิผลประโยชน์อันชอบธรรมของผู้ให้บริการ ผู้ใช้บริการระบบคอมพิวเตอร์ ตามระเบียบกฎหมาย

รัฐส่งเสริมทุกภาคส่วนเข้าร่วมงานต้าน และสกัดกั้นการกระทำผิดทางระบบคอมพิวเตอร์ด้วยการโฆษณาเผยแพร่ จัดฝึกอบรม จัดกิจกรรม และการแจ้งเตือนให้แก่ผู้ใช้บริการ

**มาตรา 5 หลักการเกี่ยวกับการดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์**

ในการดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์ ให้ปฏิบัติตามหลักการ ดังนี้

1. รับประกันการต้าน และสกัดกั้นการกระทำผิดทางระบบคอมพิวเตอร์ให้สอดคล้องกับแนวทางนโยบาย แผนยุทธศาสตร์ แผนพัฒนาเศรษฐกิจ-สังคมของชาติ

2. รับประกันให้มีความปลอดภัย สะดวกรวดเร็ว และยุติธรรม

3. รับประกันความลับของชาติ ความลับทางราชการ ของบุคคล นิติบุคคล และองค์กร

4. ปกป้องสิทธิ และผลประโยชน์อันชอบธรรมของผู้ให้บริการ และผู้ใช้บริการระบบคอมพิวเตอร์ตามระเบียบกฎหมาย

5. รับประกันความสงบ ความมั่นคงของชาติ ความเป็นระเบียบเรียบร้อยของสังคม และจารีตประเพณีอันดีงามของชาติ

6. รับประกันการปฏิบัติสนธิสัญญา และสัญญาสากลที่ สปป.ลาว เป็นภาคี

**มาตรา 6 ขอบเขตการใช้กฎหมาย**

กฎหมายฉบับนี้ ใช้สำหรับบุคคล นิติบุคคล และองค์กร รวมทั้งพลเมืองลาว คนต่างด้าว คนไม่มีสัญชาติ และคนต่างประเทศ ที่ดำรงชีวิต อาศัยและที่ใช้ระบบคอมพิวเตอร์อยู่ สปป.ลาว

**มาตรา 7 การประสานงานร่วมมือสากล**

รัฐเปิดกว้าง และส่งเสริมการประสานงานร่วมมือกับต่างประเทศ ภูมิภาค และสากล เกี่ยวกับการคุ้มครองงานกระทำผิดทางระบบคอมพิวเตอร์ ด้วยการแลกเปลี่ยนบทเรียน ข้อมูล ข่าวสาร การยกระดับวิชาเฉพาะ ความรู้ และความสามารถของบุคลากร การร่วมมือในการสนองข้อมูล การพิสูจน์ข้อมูล และการยืนยันข้อมูล โดยสอดคล้องกับระเบียบกฎหมายของ สปป.ลาว สัญญา และสนธิสัญญาสากลที่ สปป.ลาว เป็นภาคี

## ภาคที่ 2
## ประเภทการกระทำความผิดทางระบบคอมพิวเตอร์

**มาตรา 8 ประเภทการกระทำความผิดทางคอมพิวเตอร์**

ประเภทการกระทำความผิดทางคอมพิวเตอร์มี ดังนี้

1. การเข้าถึงระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต
2. การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์
3. การดักสกัดเอาข้อมูลคอมพิวเตอร์ โดยไม่ได้รับอนุญาต
4. การทำลายข้อมูลในระบบคอมพิวเตอร์
5. การรบกวนระบบคอมพิวเตอร์
6. การปลอมแปลงข้อมูลทางระบบคอมพิวเตอร์
7. การผลิตเครื่องมือกระทำผิดทางคอมพิวเตอร์
8. การเผยแพร่สิ่งลามก
9. การตัดต่อรูป ภาพเคลื่อนไหวและเสียง
10. การกระทำผิดเกี่ยวกับสื่อสังคมออนไลน์

**มาตรา 9 การเข้าถึงระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต**

การเข้าถึงระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต หมายถึง การใช้อุปกรณ์อีเล็กทรอนิกส์เข้าถึงระบบคอมพิวเตอร์ ที่มีมาตรการป้องกันเฉพาะ เพื่อเข้าไปขโมยข้อมูลทางด้านการค้า ข้อมูลด้านการเงิน และความลับของบุคคล นิติบุคคล องค์กร และข้อมูลอื่น ๆ โดยไม่ได้รับอนุญาต

**มาตรา 10 การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์**

การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ หมายถึง การเอามาตรการป้องกันเฉพาะที่บุคคลอื่นสร้างขึ้นไปเปิดเผย โดยไม่ได้รับอนุญาต ซึ่งสร้างความเสียหายให้แก่บุคคล นิติบุคคล และองค์กร

**มาตรา 11 การดักสกัดเอาข้อมูลในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต**

การดักสกัดเอาข้อมูลในระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต หมายถึง การใช้เครื่องมือทางด้านอิเล็กทรอนิกส์ เพื่อดักสกัดเอาข้อมูลที่กำลังรับหรือส่งผ่านระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์นั้น ไม่ได้มีไว้เพื่อสาธารณะหรือบุคคลทั่วไปใช้บริการ

**มาตรา 12 การทำลายข้อมูลในระบบคอมพิวเตอร์**

การทำลายข้อมูลในระบบคอมพิวเตอร์ หมายถึง การลบ การแก้ไขข้อมูลคอมพิวเตอร์ การทำให้ข้อมูลเสียหาย และการเปลี่ยนแปลงข้อมูล เพื่อสร้างความเสียหายให้แก่ระบบคอมพิวเตอร์

**มาตรา 13 การรบกวนระบบคอมพิวเตอร์**

การรบกวนระบบคอมพิวเตอร์ หมายถึง การกระทำ ดังนี้

1. การขัดขวาง ซึ่งทำให้ระบบคอมพิวเตอร์อย่างใดอย่างหนึ่ง ไม่ปฏิบัติการ ปฏิบัติการชักช้าหรือไม่สามารถปฏิบัติการได้อย่างปกติ

2. การส่งข้อมูลระบบคอมพิวเตอร์ หรือจดหมายทางอิเล็กทรอนิกส์ โดยมีการปกปิดที่อยู่หรือแหล่งที่มาของการส่งข้อมูลดังกล่าว เพื่อรบกวนการปฏิบัติการของระบบคอมพิวเตอร์

**มาตรา 14 การปลอมแปลงข้อมูลทางระบบคอมพิวเตอร์**

การปลอมแปลงข้อมูลทางระบบคอมพิวเตอร์ หมายถึง การใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อปลอมแปลงข้อมูลทางระบบคอมพิวเตอร์อย่างใดอย่างหนึ่งด้วยการกระทำ ดังนี้

1. การป้อนข้อมูล การเปลี่ยนแปลงข้อมูลหรือการลบข้อมูลในระบบคอมพิวเตอร์ ที่ส่งผลให้ข้อมูลทางระบบคอมพิวเตอร์อย่างใดอย่างหนึ่งเปลี่ยนแปลงจากข้อมูลเดิมโดยเจตนา

2. การใช้อุปกรคอมพิวเตอร์เพื่อปลอมแปลงข้อมูลธุรกรรมทางการเงิน การค้า ความรับของบุคคล นิติบุคคล องค์กร และข้อมูลอื่น ๆ โดยไม่ได้รับอนุญาต

3. การหลอกลวงให้ผู้ใช้ระบบคอมพิวเตอร์หรืออินเทอร์เน็ตป้อนข้อมูลบัญชีเงินฝาก รหัสบัตรเคดิส รหัสใช้อินเทอร์เน็ต และข้อมูลอื่น ๆ เพื่อสร้างความเสียหายให้แก่บุคคล นิติบุคคล และองค์กร

**มาตรา 15 การผลิตเครื่องมือกระทำผิดทางระบบคอมพิวเตอร์**

การผลิตเครื่องมือกระทำผิดทางระบบคอมพิวเตอร์ หมายถึง การผลิต มีไว้ครอบครอง ซื้อขาย จำหน่าย โฆษณา เผยแพร่หรือแนะนำอุปกรณ์อิเล็กทรอนิกส์ ได้แก่ โปรแกรมคอมพิวเตอร์

ชุดคำสั่ง รหัส หรือออกแบบข้อมูลคอมพิวเตอร์เพื่อขโมยข้อมูลในระบบคอมพิวเตอร์หรือเพื่อจุดประสงค์อื่นที่เป็นการกระทำผิดทางระบบคอมพิวเตอร์

**มาตรา 16 การเผยแพร่สิ่งลามก**

การเผยแพร่สิ่งลามก หมายถึง การเผยแพร่ การแจกยาย การส่งต่อ การแนะนำ รูปภาพ ภาพเคลื่อนไหว เสียง และวิดีโอ ที่มีเนื้อหาแสดงออกอย่างชัดเจนเกี่ยวกับพฤติกรรมทางเพศผ่านทางระบบคอมพิวเตอร์

**มาตรา 17 การตัดต่อรูป ภาพเคลื่อนไหว เสียง และวิดีโอ**

การตัดต่อรูป ภาพเคลื่อนไหว เสียง และวิดีโอ หมายถึง การสร้างขึ้นใหม่ เพิ่มเติมหรือการดัดแปลงจากต้นฉบับด้วยวิธีการทางอิเล็กทรอนิกส์หรือด้วยวิธีการอื่น เพื่อเผยแพร่ผ่านระบบคอมพิวเตอร์ ซึ่งสร้างความเสียหายให้แก่รัฐ บุคคล นิติบุคคล และองค์กร

**มาตรา 18 การกระทำผิดทางสื่อสังคมออนไลน์**

การกระทำผิดทางสื่อสังคมออนไลน์ หมายถึง การเขียน การพูดหรือด้วยรูปการอื่นผ่านทางสื่อสังคมออนไลน์ ซึ่งสร้างความเสียหายให้แก่รัฐ บุคคล นิติบุคคล และองค์กร

## ภาคที่ 3
## การแก้ไขเหตุการณ์ฉุกเฉินทางระบบคอมพิวเตอร์

**มาตรา 19 การแจ้งเหตุฉุกเฉิน**

บุคคล นิติบุกคน และองค์กรทั้งภายในและต่างประเทศ สามารถแจ้งเหตุฉุกเฉินที่เกิดขึ้นกับระบบคอมพิวเตอร์ของตนต่อกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร เพื่อค้นคว้าให้คำแนะนำ วิธีการแก้ไขทางด้านเทคนิค เพื่อลดการสูญเสียข้อมูล การรบกวนข้อมูล การยุติการทำงานของระบบคอมพิวเตอร์ การสกัดกั้นการกระจายไวรัสคอมพิวเตอร์ และการเข้าทำรายระบบคอมพิวเตอร์

การแจ้งเหตุฉุกเฉินสามารถแจ้งด้วยวิธีการ ดังนี้

1. คำร้องตามแบบฟอร์ม
2. โทรศัพท์ แฟกซ์
3. จดหมายอิเล็กทรอนิกส์

**มาตรา 20 การแนะนำวิธีการแก้ไข**

ภายหลังที่ได้รับแจ้งเหตุแล้วกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร ต้องค้นคว้าพิจารณาคำร้องและแจ้งตอบ พร้อมทั้งแนะนำวิธีการแก้ไข ภายในกำหนดเวลาไม่เกิน 10 วันราชการ

ในกรณีจำเป็นกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร ต้องดำเนินการแก้ไขทางเทคนิควิชาการช่วยผู้แจ้งเหตุฉุกเฉิน ตามการเสนอของผู้เสียหาย

## ภาคที่ 4
## การดำเนินคดีต่อการกระทำผิดทางระบบคอมพิวเตอร์

**มาตรา 21 ความจำเป็นต้องดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์**

การดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์ มีความจำเป็นในกานป้องกัน และสกัดกั้นการกระทำผิดทางระบบคอมพิวเตอร์ การรักษาข้อมูลข่าวสารทางระบบคอมพิวเตอร์ของรัฐ บุคคล นิติบุคคล และองค์กร ให้มีความปลอดภัย รวมทั้งรักษาสิทธิและผลประโยชน์อันชอบทำของผู้ให้บริการและผู้ใช้บริการระบบคอมพิวเตอร์ ตามระเบียบกฎหมาย เพื่อทำให้การใช้ระบบคอมพิวเตอร์มีความปลอดภัย สะดวกรวดเร็ว และยุติธรรม

**มาตรา 22 องค์การดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์**

องค์การดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์ ประกอบด้วย

- องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ
- องค์การอัยการประชาชน
- ศาลประชาชน

**มาตรา 23 ขั้นตอนการดำเนินคดีทางระบบคอมพิวเตอร์**

ในการดำเนินคดีทางระบบคอมพิวเตอร์ให้ปฏิบัติ ดังนี้

- การแจ้งความ และการพิจารณาการแจ้งความ
- การค้นหาหลักฐานเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์
- การสืบสวน-สอบสวนคดีการกระทำความผิดทางคอมพิวเตอร์
- การสั่งฟ้องคดีการกระทำผิดทางระบบคอมพิวเตอร์
- การดำเนินคดี
- การปฏิบัติคำตัดสินของศาล

**มาตรา 24 การแจ้งความ**

การแจ้งความเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ สามารถแจ้งปากเปล่าหรือทำเป็นลายลักษณ์อักษร และยื่นหรือแจ้งต่อองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชน ซึ่งต้องรับและพิจารณาตามที่ได้กำหนดไว้ในกฎหมายฉบับนี้ และกฎหมายว่าด้วยการดำเนินคดีอาญา

**มาตรา 25 การพิจารณาแจ้งความ**

องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ องค์การอัยการประชาชน ต้องพิจารณาการแจ้งความไม่ให้เกิน 7 วันราชการ นับตั้งแต่วันที่ได้รับการแจ้งความเป็นต้นไป ในกรณีมีความยุ่งยาก สับสน การกำหนดเวลาดังกล่าวไม่ให้เกิน 10 วันราชการ

**มาตรา 26 การค้นหาหลักฐานเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์**

องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ องค์การอัยการประชาชน ต้องประสารสมทบกับกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร และภาคส่วนที่เกี่ยวข้อง เพื่อดำเนินการค้นหาข้อมูลหลักฐาน และแหล่งที่มาของการกระทำผิดทางระบบคอมพิวเตอร์ เพื่อเป็นหลักฐานให้แก่การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ

**มาตรา 27 คำสั่งเปิดการสืบสวน-สอบสวน**

ในกรณีที่มีข้อมูลรัดกุมเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ หัวหน้าองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ หัวหน้าองค์การอัยการประชาชน ต้องออกคำสั่งเปิดการสืบสวน-สอบสวน ในขอบเขตสิทธิและหน้าที่ของตน ตามที่ได้กำหนดไว้ในกฎหมายว่าด้วยการดำเนินคดีอาญา

ในกรณีเร่งด่วนถ้ามีข้อมูลที่สามารถยื่นยันได้ว่า กำลังมีการตระเตรียมหรือการดำเนินการกระทำความผิดทางระบบคอมพิวเตอร์ องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ องค์การอัยการประชาชนต้องออกคำสั่งให้เก็บรักษา และป้องกันข้อมูลทางคอมพิวเตอร์หรือข้อมูลเกี่ยวกับการจราจรข้อมูลทางคอมพิวเตอร์ไว้

ผู้ให้บริการหรือภาคส่วนที่คุ้มครองข้อมูล มีหน้าที่ในการเก็บรักษา และปกป้องข้อมูลดังกล่าวไว้อย่างเร่งด่วน จนกว่าจะสิ้นสุดการดำเนินคดี เพื่อรับประกันความปลอดภัยของข้อมูล

**มาตรา 28 การสั่งฟ้องคดีการกระทำความผิดทางระบบคอมพิวเตอร์**

เมื่อมีเงื่อนไขครบถ้วนตามที่ได้กำหนดไว้ในกฎหมายฉบับนี้ และกฎหมายว่าด้วยการดำเนินคดีอาญา หัวหน้าองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือพนักงานอัยการประชาชนต้องส่งสำนวนคดีพร้อมทั้งของกลางให้องค์การอัยการประชาชนตามที่ได้กำหนดไว้ในกฎหมายว่าด้วยการดำเนินคดีอาญา

สำหรับการดำเนินคดี และการตัดสินของศาลประชาชน ต้องให้ปฏิบัติตามกฎหมายว่าด้วยการดำเนินคดีอาญา และกฎหมายอื่นที่เกี่ยวข้อง

## ภาคที่ 5
## การสกัดกั้น และการต้าน

**มาตรา 29 การเฝ้าละวังเหตุฉุกเฉิน**

กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร สนองอุปกรณ์ เทคนิค พาหนะ และบุคลากรเข้าในโครงสร้างการจัดตั้งของศูนย์สกัดกั้น และการแก้ไขเหตุฉุกเฉินแห่งชาติ เพื่อเฝ้าระวังติดตาม ตรวจสอบ แนะนำ แจ้งเตือน และโต้ตอบเหตุการณ์ฉุกเฉินทางระบบคอมพิวเตอร์

**มาตรา 30 การส่งเสริมการใช้ระเบียบกฎหมาย**

องค์การสืบสวน-สอบสวนเจ้าหน้าที่ตำรวจ ประสานสมทบกับกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร เป็นผู้จัดตั้งเผยแพร่ระเบียบกฎหมาย มาตรการเฉพาะในการรักษาความปลอดภัยของระบบคอมพิวเตอร์

**มาตรา 31 การสร้างกิจกรรมป้องกันข้อมูล**

เพื่อรับประกันความปลอดภัยของระบบคอมพิวเตอร์ และการป้องกันข้อมูลคอมพิวเตอร์ นิติบุคคล องค์กร และผู้ให้บริการ ต้องสร้างกิจกรรมในการป้องกันการจารกรรมข้อมูลทางคอมพิวเตอร์เป็นแต่ละระยะ เพื่อให้รู้เทคนิค และวิธีป้องกันข้อมูล

**มาตรา 32 การจัดตั้งโฆษณาเผยแพร่**

กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร เป็นผู้สร้างหนังสือคู่มือ แผนภาพติดผะหนัง(สติ๊กเกอร์) แผ่นโฆษณาเกี่ยวกับการรู้ทัน ละมัดละวัง และป้องกันภัยทางระบบคอมพิวเตอร์ พร้อมทั้งโฆษณาเผยแพร่ ในขอบเขตทั่วประเทศ เพื่อสกัดกั้น และต้านการจารกรรมข้อมูลทางระบบคอมพิวเตอร์ และป้องกันความเสี่ยงของผู้ใช้ระบบคอมพิวเตอร์

**มาตรา 33 การเก็บสถิติ**

องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ และกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร ต้องเก็บสถิติ และสร้างฐานข้อมูล เพื่อเก็บสถิติเกี่ยวกับจำนวนตัวเลขของผู้กระทำผิดทางระบบคอมพิวเตอร์ พร้อมทั้งศึกษาค้นคว้า เป็นแต่ละระยะเพื่อหาเงื่อนไขและสาเหตุที่ก่อให้เกิดการจารกรรมทางระบบคอมพิวเตอร์

**มาตรา 34 การฝึกอบรม**

องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ และกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร ต้องจัดฝึกอบรมให้ความรู้เกี่ยวกับการสืบสวน-สอบสวน งานสกัดกั้น และต้านการจารกรรมทางระบบคอมพิวเตอร์

**มาตรา 35 การแจ้งเตือน**

ผู้ให้บริการระบบคอมพิวเตอร์ต้องแจ้งเตือน และกำหนดเงื่อนไขในการเข้าถึงระบบคอมพิวเตอร์ เพื่อจำกัดหรือห้ามผู้ใช้บริการบางประเภทในการเข้าถึงระบบคอมพิวเตอร์

## ภาคที่ 6
## การร่วมมือสากล

**มาตรา 36 การร่วมมือภายใน**

องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ องค์การอัยการประชาชน มีหน้าที่ประสานสมทบกับกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร เพื่อเก็บข้อมูลหลักฐานที่เกี่ยวข้องกับการกระทำผิดทางระบบคอมพิวเตอร์

ผู้ให้บริการ บุคคล นิติบุคคล และองค์กร มีหน้าที่ให้การร่วมมือ และสนองข้อมูลให้แก่องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ องค์การอัยการประชาชน กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร และองค์การอื่นที่เกี่ยวข้อง

**มาตรา 37 การร่วมมือสากล**

องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ องค์การอัยการประชาชน มีหน้าที่ประสานงานกับองค์การของต่างประเทศ ที่มีภาระบทบาทคล้ายคลึงกันเกี่ยวกับการดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์ โดยสอดคล้องกับระเบียบกฎหมายที่เกี่ยวข้องของ สปป.ลาว สนธิสัญญา และสัญญาสากลที่ สปป.ลาว เป็นภาคี

กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร มีหน้าที่ประสารงาน และร่วมมือกับหน่วยงานป้องกัน และสกัดกั้นเหตุการณ์ฉุกเฉินทางระบบคอมพิวเตอร์ของต่างประเทศ โดยสอดคล้องกับระเบียบกฎหมายของ สปป.ลาว สนธิสัญญา และสัญญาสากลที่ สปป.ลาว เป็นภาคี

# ภาคที่ 7
# ข้อห้าม

**มาตรา 38 ข้อห้ามทั่วไป**

ห้ามบุคคล นิติบุคคล หรือองค์กรมีพฤติกรรม ดังนี้

1. มีการกระทำดังที่ได้กำหนดไว้ในภาคที่ 2 ของกฎหมายฉบับนี้

2. ทำลายหรือสร้างความเสียหายให้แก่อุปกรณ์อิเล็กทรอนิกส์ คอมพิวเตอร์ และสิ่งอำนวยความสะดวกต่าง ๆ ในการแลกเปลี่ยนข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์

3. มีพฤติกรรมอื่น ที่เป็นการละเมิดระเบียบกฎหมาย

**มาตรา 39 ข้อห้ามสำหรับพนักงาน**

ห้ามพนักงานที่มีหน้าที่คุ้มครองข้อมูลข่าวสารมีพฤติกรรม ดังนี้

1. เปิดเผยข้อมูลลับของรัฐ ความลับทางราชการ ของบุคคล นิติบุคคลหรือองค์กร ผ่านทางระบบคอมพิวเตอร์

2. หน่วงเหนี่ยว และปลอมแปลงเอกสารเกี่ยวกับการงาน การกระทำผิดทางคอมพิวเตอร์

3. ใช้หน้าที่ตำแหน่งเพื่อผลประโยชน์ส่วนตัว ครอบครัว และพวกพ้อง

4. ละเลยหน้าที่ความรับผิดชอบที่องค์กรมอบหมายให้

5. มีพฤติกรรมอื่น ที่เป็นการละเมิดระเบียบกฎหมาย

**มาตรา 40 ข้อห้ามสำรับผู้ให้บริการ**

ห้ามผู้ให้บริการระบบคอมพิวเตอร์ มีพฤติกรรม ดังนี้

1. เก็บรักษาข้อมูลจราจรทางระบบคอมพิวเตอร์ ต่ำกว่า 90 วันในสภาพเชื่อมโยง และ 365 วันในสภาพไม่เชื่อมโยง

2. ลบข้อมูลจราจรทางคอมพิวเตอร์ และข้อมูลผู้ใช้บริการก่อนกำหนดเวลาที่ระบุไว้ในข้อ 1 ของมาตรานี้

3. มีพฤติกรรมอื่นที่เป็นการละเมิดระเบียบกฎหมาย

**มาตรา 41 ข้อห้ามสำรับผู้ใช้บริการ**

ห้ามผู้ใช้บริการระบบคอมพิวเตอร์ มีพฤติกรรม ดังนี้

1. มีการกระทำตามที่ได้กำหนดไว้ใน ภาคที่ 2 ของกฎหมายฉบับนี้

2. มีพฤติกรรมอื่น ที่เป็นการละเมิดระเบียบกฎหมาย

# ภาคที่ 8
# การแก้ไขข้อขัดแย้ง

**มาตรา 42 รูปการแก้ไขข้อขัดแย้ง**

การแก้ไขข้อขัดแย้งเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ สามารถดำเนินด้วยรูปการอย่างใดอย่างหนึ่ง ดังนี้

1. การประนีประนอมโดยคู่กรณี
2. การแก้ไขทางด้านบริหาร
3. การแก้ไขโดยองค์การแก้ไขข้อขัดแย้งทางด้านเศรษฐกิจ
4. การฟ้องร้องต่อศาลประชาชน
5. การแก้ไขข้อขัดแย้งที่มีลักษณะสากล

**มาตรา 43 การประนีประนอมโดยคู่กรณี**

ในกรณีมีข้อขัดแย้งเกี่ยวกับการกระทำความผิดทางระบบคอมพิวเตอร์ ที่ไม่ใช้การละเมิดกฎหมายอาญา คู่กรณีสามารถปรึกษาหารือ และประนีประนอมด้วยกัน

**มาตรา 44 การแก้ไขทางด้านบริหาร**

ในกรณีมีข้อขัดแย้งเกี่ยวกับการกระทำความผิดทางระบบคอมพิวเตอร์ คู่กรณีมีสิทธิเสนอองค์การดำเนินคดีการกระทำความผิดทางระบบคอมพิวเตอร์ พิจารณาแก้ไขตามระเบียบกฎหมาย

**มาตรา 45 การแก้ไขโดยองค์การแก้ไขข้อขัดแย้งทางด้านเศรษฐกิจ**

ในกรณีเกิดข้อขัดแย้งทางด้านเศรษฐกิจ เนื่องจากการกระทำผิดทางระบบคอมพิวเตอร์ตามที่ได้กำหนดไว้ในภาคที่ 2 ของกฎหมายฉบับนี้ คู่กรณีมีสิทธิร้องขอให้องค์การแก้ไขข้อขัดแย้งทางด้านเศรษฐกิจ พิจารณาแก้ไขตามระเบียบกฎหมาย

**มาตรา 46 การฟ้องร้องต่อศาลประชาชน**

ในกรณีเกิดข้อขัดแย้งเนื่องจากการกระทำความผิดทางระบบคอมพิวเตอร์ ตามที่ได้กำหนดไว้ในภาคที่ 2 ของกฎหมายฉบับนี้ คู่กรณีมีสิทธิฟ้องร้องต่อศาลประชาชน พิจารณาแก้ไขตามระเบียบกฎหมาย

**มาตรา 47 การแก้ไขข้อขัดแย้งที่มีลักษณะสากล**

การกระทำผิดทางคอมพิวเตอร์ ที่มีลักษณะสากล ให้ปฏิบัติตามระเบียบกฎหมาย ที่เกี่ยวข้องของ สปป.ลาว สนธิสัญญา และสัญญาสากลเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ที่ สปป.ลาว เป็นภาคี

# ภาคที่ 9
# การคุ้มครองและการตรวจตรา

## หมวดที่ 1
## การคุ้มครอง

**มาตรา 48 องค์การคุ้มครอง**

การกระทำความผิดทางระบบคอมพิวเตอร์ อยู่ในการควบคุมดูแลของรัฐบาลอย่างรวมศูนย์เป็นเอกภาพในขอบเขตทั่วประเทศ โดยมอบให้องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจและกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร เป็นเจ้าการคุ้มครองโดยตรง และประสานสมทบกับกระทรวงหรือองค์กรอื่น และองค์การปกครองส่วนท้องถิ่นที่เกี่ยวข้อง ตามภาระบทบาทของตน

องค์การที่คุ้มครองเกี่ยวกับการกระทำความผิดทางระบบคอมพิวเตอร์ ประกอบด้วย

1. องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ
2. กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร
3. แผนกไปรษณีย์ โทรคมนาคม และการสื่อสาร แขวง (จังหวัด) นครหลวงเวียงจันทน์
4. ห้องการไปรษณีย์ โทรคมนาคม และการสื่อสารเมือง (อำเภอ) เทศบาล

**มาตรา 49 สิทธิและหน้าที่ขององค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ**

ในการดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์ องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจมีสิทธิ และหน้าที่ ดังนี้

1. รับ และบันทึกการแจ้งความเกี่ยวกับการกระทำผิด
2. รายงานอย่างทันท้วงที่ให้อัยการประชาชนทราบเกี่ยวกับการกระทำผิด
3. ออกคำสั่งเปิดการสืบสวน-สอบสวน และส่งสำเนาคำสั่งนั้นรายงานให้อัยการประชาชนทราบในทันใด
4. ดำเนินการสืบสวน-สอบสวน
5. ใช้มาตรการทางด้านกฎหมายในการจับตัว กักตัว ปล่อยตัว กักขัง ตรวจค้น และรายงานเป็นลายลักษณ์อักษรให้อัยการประชาชนทราบ
6. ขออุทธรณ์คำสั่งของอัยการประชาชนต่ออัยการประชาชนชั้นที่เหนือกว่า

7. ประสานสมทบกับกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร และแขนงการอื่นที่เกี่ยวข้อง เพื่อเก็บข้อมูลหลักฐานที่เกี่ยวข้องกับการกระทำผิดทางคอมพิวเตอร์

8. ประสานงานกับองค์การของต่างประเทศ และสากล ที่มีภาระบทบาทคล้ายคลึงกัน เกี่ยวกับการดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์โดยสอดคล้องกับระเบียบกฎหมาย สนธิสัญญา และสัญญาสากล

9. สรุปการสืบสวน-สอบสวน และประกอบสำนวนคดีส่งให้อัยการประชาชน

10. เสนอให้ภาคส่วนที่เกี่ยวข้องปิดเว็บไซต์ และข้อมูลจราจรทางคอมพิวเตอร์ ที่สร้างความเสียหายต่อบุคคล นิติบุคคล องค์กร สังคม และความมั่นคงของชาติ

11. ตรวจตราข้อมูลที่สงสัยหรือเสนอให้ภาคส่วนที่เกี่ยวข้องตรวจตราข้อมูลที่สงสัยที่จะสร้างความเสียหายให้บุคคล นิติบุคคล องค์กร สังคม และความมั่นคงของชาติ

12. ปฏิบัติสิทธิ และหน้าที่อื่นตามที่ได้กำหนดไว้ในระเบียบกฎหมาย

**มาตรา 50 สิทธิ และหน้าที่ของกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร**

ในการเข้าร่วมการดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์ กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร มีสิทธิ และหน้าที่ ดังนี้

1. ค้นคว้า สร้าง ปรับปรุงกฎหมาย ระเบียบการ และนิติกรรมอื่น ๆ สำหรับงานเกี่ยวกับการกระทำผิดทางคอมพิวเตอร์

2. ต้าน สกัดกั้น และจำกัดการเข้าถึง การเผยแพร่ข้อมูลข่าวสาร ที่มีเนื้อหาผิดต่อระเบียบกฎหมายของ สปป.ลาว

3. เฝ้าระวัง ติดตาม ตรวจตรา แนะนำ แจ้งเตือน และโต้ตอบทุกเหตุการณ์ฉุกเฉินที่เกิดขึ้นทางระบบคอมพิวเตอร์

4. โฆษณา เผยแพร่นิติกรรม และวิธีป้องกันภัยทางระบบคอมพิวเตอร์

5. แจ้งความต่อองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชน

6. เข้าร่วม และร่วมมือกับองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชนในการดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์

7. แจ้งให้ผู้บริการอำนวยความสะดวก และสนองข้อมูนเกี่ยวกับการกระทำผิด

8. ประสานงานรวมมือกับศูนย์สกัดกั้น และแก้ไขเหตุการณ์ฉุกเฉินทางระบบคอมพิวเตอร์ของต่างประเทศ

9. พัฒนาด้านบุคลากรเกี่ยวกับงานความปลอดภัยระบบคอมพิวเตอร์

10. สรุป และรายงานการจัดตั้งปฏิบัติหน้าที่ของตนต่อรัฐบาลอย่างเป็นปกติ

11. ปฏิบัติสิทธิ และหน้าที่อื่นตามที่ได้กำหนดไว้ในระเบียบกฎหมาย

**มาตรา 51 สิทธิ และหน้าที่ของแผนกไปรษณีย์ โทรคมนาคม และการสื่อสารแขวง (จังหวัด) นคร**

ในการเข้าร่วมการดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์ แผนกไปรษณีย์ โทรคมนาคม และการสื่อสารแขวง (จังหวัด) นคร มีสิทธิ และหน้าที่ตามขอบเขตความรับผิดชอบของตน ดังนี้

1. โฆษนา เผยแพร่นิติกรรม และวิธีป้องกันภัยทางระบบคอมพิวเตอร์

2. แจ้งความต่อองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชน

3. เข้าร่วม และร่วมมือกับองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชนในการดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์

4. แจ้งให้ผู้ให้บริการอำนวยความสะดวก และสนองข้อมูนเกี่ยวกับการกระทำผิด

5. ประสานงานร่วมมือกับศูนย์สกัดกั้น และแก้ไขเหตุการณ์ฉุกเฉินทางระบบคอมพิวเตอร์ของต่างประเทศ ตามการเห็นดีของกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร

6. พัฒนาทางด้านบุคคลกร ด้านงานความปลอดภัยระบบคอมพิวเตอร์

7. สรุป และรายงานการจัดตั้งปฏิบัติงานของตนต่อกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร และองค์การปกครองแขวง (จังหวัด) นคร อย่างเป็นปกติ

8. ปฏิบัติสิทธิ และหน้าที่อื่น ๆ ตามที่ได้กำหนดไว้ในระบบกฎหมาย

**มาตรา 52 สิทธิ และหน้าที่ของห้องการไปรษณีย์ โทรคมนาคม และการสื่อสารเมือง (อำเภอ) เทศบาล**

ในการเข้าร่วมการดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์ ห้องการไปรษณีย์ โทรคมนาคม และการสื่อสาร เมือง (อำเภอ) และเทศบาลมีสิทธิ และหน้าที่ตามขอบเขตความรับผิดชอบของตน ดังนี้

1. โฆษนา เผยแพร่นิติกรรม และวิธีป้องกันภัยทางระบบคอมพิวเตอร์

2. แจ้งความต่อองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชน

3. เข้ารวม และร่วมมือกับองค์การสืบสวนสอบสวนของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชนในการดำเนินคดีการกระทำผิดทางระบบคอมพิวเตอร์

4. แจ้งให้ผู้ให้บริการอำนวยความสะดวก และสนองข้อมูลเกี่ยวกับการกระทำผิด

5. สรุป และรายงานการจัดตั้งปฏิบัติงานของตนต่อแผนกไปรษณีย์ โทรคมนาคมและการสื่อสารและองค์การปกครองเมือง (อำเภอ) เทศบาล อย่างเป็นปกติ

6. ปฏิบัติสิทธิ และหน้าที่อื่น ๆ ตามที่ได้กำหนดไว้ในกฎหมาย

**มาตรา 53 สิทธิ และหน้าที่ของแขนงการอื่น**

ในการดำเนินคดีการกระทำความผิดทางระบบคอมพิวเตอร์แขนงการอื่นมีหน้าที่อำนวยความสะดวก และให้ความร่วมมือแก่เจ้าหน้าที่สืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือพนักงานอัยการตามขอบเขตสิทธิ และความรับผิดชอบของตน

## หมวดที่ 2
## การตรวจตรา

**มาตรา 54 องค์การตรวจตรา**

องค์การตรวจตรางานการกระทำผิดทางระบบคอมพิวเตอร์ ประกอบด้วย

1. องค์การตรวจตราภายใน ซึ่งหมายถึงองค์การเดียวกันกับองค์การคุ้มครองงานการกระทำผิดทางระบบคอมพิวเตอร์ตามที่ได้กำหนดไว้ใน มาตรา 48 ของกฎหมายฉบับนี้

2. องค์การตรวจตราภายนอก ได้แก่ สภาแห่งชาติ องค์การตรวจสอบแห่งรัฐ และองค์การตรวจตารัฐบาล และต้านการฉ้อราชบังหลวง

**มาตรา 55 เนื้อในการตรวจตรา**

เนื้อในการตรวจตรางานการกระทำความผิดทางระบบคอมพิวเตอร์มี ดังนี้

1. การปฏิบัตินโยบาย และระเบียบกฎหมายเกี่ยวกับงานการกระทำความผิดทางระบบคอมพิวเตอร์

2. การจัดตั้ง และการดำเนินงานขององค์การคุ้มครองงานการกระทำความผิดทางระบบคอมพิวเตอร์

3. การดำเนินคดีต่อผู้กระทำความผิดทางระบบคอมพิวเตอร์

4. ความรับผิดชอบ การประพฤติ และแบบแผนวิธีการทำงานของเจ้าหน้าที่สืบสวนสอบสวนของเจ้าหน้าที่ตำรวจ

5. การปฏิบัติสนธิสัญญา และสัญญาสากลเกี่ยวกับงานการกระทำผิดทางระบบคอมพิวเตอร์ที่ สปป.ลาว เป็นภาคี

**มาตรา 56 รูปการ การตรวจตรา**

การตรวจตราตามเนื้อหาที่ได้กำหนดไว้ใน มาตรา 55 ของกฎหมายฉบับนี้ให้ดำเนินด้วยรูปการ ดังนี้

1. การตรวจตราอย่างเป็นระบบปกติ

2. การตรวจตราโดยมีการแจ้งให้รู้ล่วงหน้า

3. การตรวจตราแบบกะทันหัน

4. การตรวจตราตามการมอบหมาย

การตรวจตราอย่างเป็นระบบปกติ หมายถึง การตรวจตราที่ดำเนินไปตามแผนการอย่างเป็นประจำและมีกำหนดเวลาอันแน่นอน

การตรวจตราโดยมีการแจ้งให้รู้ล่วงหน้า หมายถึง การตรวจตรานอกแผนการ เมื่อเห็นว่ามีความจำเป็นซึ่งแจ้งให้ผู้ที่จะถูกตรวจตราทราบล่วงหน้า

การตรวจตราแบบกะทันหัน หมายถึง การตรวจตราโดยเร่งด่วนซึ่งมิได้แจ้งให้ผู้ถูกตรวจตราทราบล่วงหน้า

การตรวจตราตามการมอบหมาย หมายถึง การตรวจตราในกรณีรับใช้งานเฉพาะกิจอย่างใดอย่างหนึ่ง โดยการมอบหมายของรัฐบาล

ในการดำเนินการตรวจตราเกี่ยวกับการใช้ระบบคอมพิวเตอร์เจ้าหน้าที่ขององค์การตรวจตราต้องปฏิบัติให้ถูกต้องตามระเบียบกฎหมายอย่างเข้มงวด

## ภาคที่ 10
## นโยบายต่อผู้มีผลงาน และมาตรการต่อผู้ละเมิด

**มาตรา 57 นโยบายต่อผู้มีผลงาน**

บุคคล นิติบุคคลหรือองค์กรที่มีผลงานดีเด่นในการจัดตั้งปฏิบัติกฎหมายฉบับนี้จะได้รับการยกย่อง และนโยบายอื่นตามระเบียบการ

**มาตรา 58 มาตรการต่อผู้ละเมิด**

บุคคล นิติบุคคล หรือองค์กร ที่ละเมิดกฎหมายฉบับนี้ จะถูกกล่าวเตือน ศึกษาอบรมลงวินัย ปรับ ใช้แทนค่าเสียหายทางแพ่ง หรือถูกลงโทษทางอาญา ตามแต่กรณีเบาหรือหนัก ตามที่ได้กำหนดไว้ในระเบียบกฎหมาย

**มาตรา 59 มาตรการศึกษาอบรม**

บุคคล นิติบุคคล หรือองค์กรใดองค์กรหนึ่ง ที่ละเมิดกฎหมายฉบับนี้ ที่ก่อให้เกิดความเสียหายต่ำกว่า 10,000,000 กีบ จะถูกตักเตือน ศึกษาอบรม

**มาตรา 60 มาตรการทางวินัย**

พนักงาน และเจ้าหน้าที่ ที่ละเมิดกฎหมายฉบับนี้ในการดำเนินคดีเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ ซึ่งมีลักษณะเบาบาง ที่ไม่เป็นการกระทำผิดทางอาญา และก่อความเสียหาย

ที่มีมูลค่าต่ำกว่า 10,000,000 กีบ แต่ไม่จงใจรายงาน หลบหลีกการกระทำผิด จะถูกลงวินัยตามแต่ละกรณี ดังนี้

- ติเตียน กล่าวเตือนความผิดตามระเบียบรัฐกร (นิติกร) พร้อมทั้งบันทึกไว้ในประวัติของผู้กระทำความผิด
- หยุดการเลื่อนชั้น ขั้นเงินเดือน และการยกย่อง
- ปลดตำแหน่งหรือโยกย้ายไปรับหน้าที่อื่น ที่มีตำแหน่งต่ำกว่าเดิม
- ให้ออกจากราชการ โดยไม่ได้รับนโยบายใด ๆ

**มาตรา 61 มาตรการทางแพ่ง**

บุคคลหรือองค์กรที่ละเมิดกฎหมายฉบับนี้ ซึ่งได้ก่อความเสียหายแก่ผู้อื่น จะต้องใช้แทนค่าเสียหายที่ตนได้กระทำ

**มาตรา 62 มาตรการทางอาญา**

บุคคลใดที่ละเมิดกฎหมายฉบับนี้ ซึ่งเป็นการกระทำผิดทางอาญา จะถูกลงโทษตามกฎหมายอาญา ตามแต่ละกรณีเบาหรือหนัก รวมทั้งทดแทนค่าเสียหายที่ตนได้กระทำขึ้น

1. การเข้าถึงระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต ต้องระวางโทษจำคุกตั้งแต่ 3 เดือน ถึง 2 ปี และปรับตั้งแต่ 10,000,000 กีบ ถึง 40,000,000 กีบ
2. การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต ต้องระวางโทษจำคุกตั้งแต่ 1 เดือน ถึง 1 ปี และปรับตั้งแต่ 5,000,000 กีบ ถึง 20,000,000 กีบ
3. การดักสกัดเอาข้อมูลในระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต ต้องระวางโทษจำคุกตั้งแต่ 3 เดือน ถึง 2 ปี และปรับตั้งแต่ 10,000,000 กีบ ถึง 40,000,000 กีบ
4. การทำรายข้อมูลคอมพิวเตอร์ ต้องระวางโทษจำคุกตั้งแต่ 3 ปี ถึง 7 ปี และปรับตั้งแต่ 20,000,000 กีบ ถึง 60,000,000 กีบ
5. การรบกวนระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกตั้งแต่ 1 ปี ถึง 5 ปี และปรับตั้งแต่ 5,000,000 กีบ ถึง 25,000,000 กีบ
6. การปลอมแปลงข้อมูลทางระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกตั้งแต่ 1 ปี ถึง 5 ปี และปรับตั้งแต่ 10,000,000 กีบ ถึง 50,000,000 กีบ
7. การผลิตเครื่องมือกระทำผิดทางระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกตั้งแต่ 5 เดือน ถึง 1 ปี และปรับตั้งแต่ 5,000,000 กีบ ถึง 20,000,000 กีบ
8. การเผยแพร่สื่อลามกอนาจาร ต้องระวางโทษจำคุกตั้งแต่ 5 เดือน ถึง 1 ปี หรือกักกันและปรับตั้งแต่ 200,000 กีบ ถึง 5,000,000 กีบ

9. การตัดต่อรูป ภาพเคลื่อนไหวและเสียง ต้องระวางโทษจำคุกตั้งแต่ 3 เดือน ถึง 1 ปี หรือกักกัน และปรับตั้งแต่ 500,000 กีบ ถึง 1,000,000 กีบ

10. การกระทำผิดเกี่ยวกับสื่อสังคมออนไลน์ ต้องระวางโทษจำคุกตั้งแต่ 3 เดือน ถึง 1 ปี หรือกักกัน และปรับตั้งแต่ 200,000 กีบ ถึง 1,000,000 กีบ

## ภาคที่ 11
## บทบัญญัติสุดท้าย

**มาตรา 63 การจัดตั้งปฏิบัติ**

รัฐบาลแห่งสาธารณรัฐประชาธิปไตย ประชาชนลาว เป็นผู้จัดตั้งกฎหมายฉบับนี้

**มาตรา 64 ผลศักดิ์สิทธิ์**

กฎหมายฉบับนี้มีผลศักดิ์สิทธิ์ ภายหลัง 120 วัน นับแต่วันประธานประเทศแห่งสาธารณรัฐประชาธิปไตยประชาชนลาว ได้ออกรัฐดำรัฐประกาศใช้เป็นต้นไป

ประธานสภาแห่งชาติ

# ภาคผนวก ข

# ร่างกฎหมายว่าด้วยการต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

สาธารณรัฐ ประชาธิปไตย ประชาชนลาว

สันติภาพ เอกราช ประชาธิปไตย เอกภาพ วัฒนาถาวร

สภาแห่งชาติ เลขที่…...../สภช

นครหลวงเวียงจันทน์, วันที่.../…./….

## ร่างกฎหมาย
## ว่าด้วยการต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

## ภาคที่ 1
## บทบัญญัติทั่วไป

**มาตรา 1 วัตถุประสงค์**

กฎหมายฉบับนี้กำหนดหลักการ ระเบียบการ และมาตรการเกี่ยวกับการคุ้มครอง ติดตาม ตรวจสอบงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ เพื่อทำให้งานดังกล่าวมีประสิทธิผลเพื่อต้าน สกัดกั้น จำกัด และกำจัดอาชญากรรม ปกป้องระบบฐานข้อมูล ระบบเซิฟเวอร์ ข้อมูลทางระบบคอมพิวเตอร์ รับประกันความมั่นคงของชาติ ความสงบ และความเป็นระเบียบเรียบร้อยของสังคม สามารถเชื่อมโยงกับภูมิภาค และสากล เป็นส่วนหนึ่งในการปกปักษ์รักษา และพัฒนาเศรษฐกิจ-สังคม ให้เจริญก้าวหน้า

**มาตรา 2 การต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์**

การต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ หมายถึง การจำกัด กำจัด ปราบปราม ลบล้างทุกการกระทำที่เป็นอาชญากรรมทางระบบคอมพิวเตอร์ โดยการตรวจตรา การศึกษาอบรม ปฏิบัติวินัย และการลงโทษตามกฎหมาย และระเบียบการ

**มาตรา 3 การอธิบายศัพท์**

คำศัพท์ที่ใช้ในกฎหมายฉบับนี้มีความหมาย ดังนี้

1. **อาชญากรรมทางระบบคอมพิวเตอร์** หมายถึง การกระทำผิดทางระบบคอมพิวเตอร์ที่สร้างความเสียหายให้แก่บุคคล นิติบุคคล และองค์กร ตามพฤติกรรมที่ได้กำหนดไว้ในมาตรา 8 ของกฎหมายฉบับนี้

2. **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์อิเล็กทรอนิกส์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมต่อระบบการปฏิบัติการเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่น ๆ เพื่อให้อุปกรณ์อิเล็กทรอนิกส์หรือชุดอุปกรณ์ของคอมพิวเตอร์ ทำหน้าที่ประมวลผลข้อมูลแบบอัตโนมัติในคอมพิวเตอร์เครื่องหนึ่งหรือหลายเครื่องที่เชื่อมต่อเข้าหากันผ่านเครือข่ายคอมพิวเตอร์ และเครือข่ายอินเทอร์เน็ต

3. **โปรแกรม** หมายถึง ระบบคำสั่งหรือชุดคำสั่ง ที่ระบบคอมพิวเตอร์สามารถปฏิบัติได้เพื่อทำให้เกิดผลได้รับตามที่ได้กำหนดไว้

4. **ระบบเซิฟเวอร์ (Server system)** หมายถึง ระบบให้บริการผ่านระบบคอมพิวเตอร์ ประกอบด้วย ระบบฐานข้อมูล เว็บเซิฟเวอร์ เมลเซิฟเวอร์ ไฟล์เซิฟเวอร์ และอื่น ๆ

5. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ โปรแกรมหรือระบบฐานข้อมูล ข้อมูลส่วนบุคคล ข้อมูลจราจรทางระบบคอมพิวเตอร์ ในรูปแบบที่สามารถประมวลผล และทำให้ระบบคอมพิวเตอร์ทำงานได้

6. **ระบบฐานข้อมูล (Database System)** หมายถึง ระบบข้อมูลที่เก็บรักษาในรูปแบบอิเล็กทรอนิกส์ที่สามารถคุ้มครอง ปรับปรุง และใช้ได้

7. **ข้อมูลส่วนบุคคล** หมายถึง ข้อมูลที่เกี่ยวข้องหรือบ่งบอกถึงลักษณะหรือตัวตน การเคลื่อนไหวของบุคคล นิติบุคคลหรือองค์กรโดยทางตรงหรือทางอ้อม

8. **ข้อมูลจราจรทางระบบคอมพิวเตอร์** หมายถึง ข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการสื่อสารผ่านระบบคอมพิวเตอร์ ซึ่งถูกสร้างขึ้นโดยระบบคอมพิวเตอร์ที่เป็นส่วนหนึ่ง ในเชื่อมโยงการสื่อสารที่บ่งบอกถึงผู้ส่ง ต้นทาง สื่อกลาง เส้นทาง ปลายทาง วัน เวลา ขนาด กำหนดเวลาของการสื่อสาร ชนิดการบริการ และอื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

9. **ผู้ให้บริการ** หมายถึง ผู้ให้บริการด้านการสื่อสารข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์ และผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์

10. **การประมวลข้อมูลแบบอัตโนมัติ** หมายถึง กระบวนการคำนวณปรุงแต่งข้อมูลในระบบคอมพิวเตอร์ โดยโปรแกรมคอมพิวเตอร์

11. **โปรแกรมประสงค์ร้าย (Malicious Code)** หมายถึง ชุดคำสั่งคอมพิวเตอร์ที่สร้างขึ้นเพื่อทำลายระบบคอมพิวเตอร์หรือขโมยข้อมูลคอมพิวเตอร์

12. **ไวรัส** หมายถึง โปรแกรมหรือชุดคำสั่งที่สามารถแพร่กระจายและสร้างความเสียหายแก่ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์

13. **เว็ปไซต์ปลอม (Phishing)** หมายถึง เว็ปไซต์ที่สร้างขึ้นมาใหม่คล้ายคลึงกันเว็ปไซต์เดิมเพื่อหลอกลวงเอาข้อมูลจากผู้ใช้บริการ

14. **ช่องโหว่ (Vulnerability)** หมายถึง ข้อบกพร่องของโปรแกรมหรือซอฟแวร์ที่ไม่สมบูรณ์ และไม่ได้รับการปรับปรุง ทำให้ผู้ประสงค์ร้ายสามารถใช้ช่องโหว่ดังกล่าวเข้าทำลายระบบ ขโมยข้อมูล เปลี่ยนแปลงข้อมูล และอื่น ๆ

15. **ข้อมูลผู้ใช้บริการ** หมายถึง ข้อมูลที่นำไปสู่ผู้ใช้บริการที่อยู่ไปรษณีย์ ที่อยู่ทางอิเล็กทรอนิกส์ ที่อยู่ทางด้านภูมิลำเนา เลขหมายอินเทอร์เน็ต เบอร์โทรศัพท์หรือรหัสอื่นที่ใช้เข้าในระบบคอมพิวเตอร์

16. **มาตรการป้องกันเฉพาะ** หมายถึง การใช้เครื่องมือหรือโปรแกรมคอมพิวเตอร์พิเศษเพื่อต้าน และสกัดกั้นการเข้าถึงระบบคอมพิวเตอร์ของผู้ใช้บริการ

17. **สื่อสังคมออนไลน์** หมายถึง การสื่อสารผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อเผยแพร่ข้อมูลข่าวสารสู่สาธารณะ ด้วยการใช้วัตถุอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารอื่น

18. **ภาพเคลื่อนไหว** หมายถึง การสร้าง การแต้ม การวาดภาพขึ้นใหม่ที่มีผลใกล้เคียงกับตัวจริง ซึ่งมีการเคลื่อนไหวโดยผ่านอุปกรณ์อิเล็กทรอนิกส์ เช่น หนังการ์ตูน

**มาตรา 4 นโยบายของรัฐเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์**

รัฐส่งเสริมการใช้เทคโนโลยีที่ทันสมัยในงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ให้มีความปลอดภัย สะดวกรวดเร็ว และยุติธรรม พร้อมทั้งปกป้องสิทธิผลประโยชน์อันชอบธรรมของผู้ให้บริการ ผู้ใช้บริการระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ถูกต้องตามกฎหมาย และระเบียบการ

รัฐสร้างเงื่อนไข และอำนวยความสะดวกให้แก่การจัดตั้งปฏิบัติงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ด้วยการสนองงบประมาน จัดตั้งบุคลากร พาหนะ อุปกรณ์ก่อสร้างพื้นฐานโครงร่าง เพื่อทำให้งานดังกล่าวมีประสิทธิผล

รัฐผลักดันบุคคล นิติบุคคล และองค์กร ให้เข้าร่วมในงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์โดยการโฆษณาเผยแพร่ จัดการฝึกอบรม จัดกิจกรรม แจ้งเตือน และมีนโยบายอื่นที่เหมาะสม

รัฐส่งเสริมบุคคล นิติบุคคลทั้งภายในและต่างประเทศ สามารถลงทุนเข้าในงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

นอกจากงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ รัฐยังส่งเสริมให้ทุกแขนงการ รวมทั้งภาครัฐและเอกชน มีการใช้ข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์ให้เกิดประโยชน์ มีส่วนร่วมในงานสร้าง พัฒนาเศรษฐกิจ-สังคม ให้มีประสิทธิผลสูง

**มาตรา 5 หลักการเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์**

งานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ต้องรับประกันหลักการ ดังนี้

1. ความสอดคล้องกับแนวทางนโยบาย กฎหมาย แผนยุทธศาสตร์ แผนพัฒนาเศรษฐกิจ-สังคมของชาติ
2. ความมั่นคงของชาติ ความสงบ ความเป็นระเบียบเรียบร้อยของสังคม และจารีตประเพณีอันดีงามของชาติ
3. การรักษาความลับของชาติ ความลับทางราชการ ของบุคคล นิติบุคคล และองค์กร
4. ความเป็นเอกภาพ ปลอดภัย สะดวกรวดเร็ว และยุติธรรม
5. เอาการต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ เป็นต้นตอ และถือเอาการแก้ไขปัญหาเป็นสำคัญ
6. การปกป้องสิทธิ และผลประโยชน์อันชอบธรรมของผู้ให้บริการ ผู้ใช้บริการระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ตามกฎหมาย และระเบียบการ
7. การปฏิบัติตามสัญญาสากล และสนธิสัญญาที่ สปป.ลาว เป็นภาคี

**มาตรา 6 ขอบเขตการใช้กฎหมาย**

กฎหมายฉบับนี้ใช้สำหรับบุคคล นิติบุคคล และองค์กรทั้งภายใน และต่างประเทศที่ดำรงชีวิต เคลื่อนไหว ใช้ระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์อยู่ สปป.ลาว

**มาตรา 7 การร่วมมือสากล**

รัฐเปิดกว้าง และส่งเสริมการประสานงานร่วมมือกับต่างประเทศ ภาคพื้น และสากลเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ด้วยการแลกเปลี่ยนบทเรียน ข้อมูลข่าวสาร การยกระดับวิชาการ ความรู้ และความสามารถของบุคลากร การสนองข้อมูล การพิสูจน์ข้อมูล และการยืนยันข้อมูล โดยสอดคล้องกับกฎหมาย ระเบียบการของ สปป.ลาว สัญญาสากล และสนธิสัญญาที่ สปป.ลาว เป็นภาคี

# ภาคที่ 2
# พฤติกรรมที่เป็นอาชญากรรมทางระบบคอมพิวเตอร์

**มาตรา 8 พฤติกรรมที่เป็นอาชญากรรมทางระบบคอมพิวเตอร์**

พฤติกรรมที่เป็นอาชญากรรมทางระบบคอมพิวเตอร์ มีดังนี้

1. การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์
2. การเข้าถึงระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต
3. การตัดต่อเนื้อหา รูป ภาพเคลื่อนไหว เสียง และวิดีโอ โดยไม่ได้รับอนุญาต
4. การดักรับข้อมูลในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต
5. การสร้างความเสียหายผ่านสื่อสังคมออนไลน์
6. การเผยแพร่สิ่งลามกผ่านระบบคอมพิวเตอร์
7. การรบกวนระบบคอมพิวเตอร์
8. การปลอมแปลงข้อมูลคอมพิวเตอร์
9. การทำลายข้อมูลคอมพิวเตอร์
10. การดำเนินกิจการเกี่ยวกับเครื่องมืออาชญากรรมทางระบบคอมพิวเตอร์
11. การใช้ระบบคอมพิวเตอร์เข้าในการก่อการร้าย
12. การเล่นการพนันที่ต้องห้ามผ่านระบบคอมพิวเตอร์

**มาตรา 9 การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์**

การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ หมายถึง การนำเอามาตรการป้องกันเฉพาะไปเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งสร้างความเสียหายให้แก่บุคคล นิติบุคคล และองค์กรที่เกี่ยวข้อง

**มาตรา 10 การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต**

การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต หมายถึง การใช้อุปกรณ์อิเล็กทรอนิกส์เข้าถึงระบบคอมพิวเตอร์ ที่มีมาตรการป้องกันเฉพาะหรือเพื่อขโมยข้อมูลทางด้านการค้า ข้อมูลด้านการเงิน และความลับ และข้อมูลอื่นของบุคคล นิติบุคคล องค์กร

**มาตรา 11 การตัดต่อเนื้อหา รูป ภาพเคลื่อนไหว เสียง และวิดีโอโดยไม่ได้รับอนุญาต**

การตัดต่อเนื้อหา รูป ภาพเคลื่อนไหว เสียง และวิดีโอโดยไม่ได้รับอนุญาต หมายถึง การสร้างขึ้นใหม่ การเพิ่มเติมหรือการดัดแปลงจากต้นฉบับด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่น เพื่อเผยแพร่ผ่านระบบคอมพิวเตอร์ ซึ่งสร้างความเสียหายให้แก่บุคคล นิติบุคคล และองค์กรที่เกี่ยวข้อง

**มาตรา 12 การดักรับข้อมูลในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต**

การดักรับข้อมูลในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต หมายถึง การดักรับข้อมูลที่กำลังรับหรือส่งผ่านระบบคอมพิวเตอร์ ด้วยการใช้เครื่องมือทางด้านอิเล็กทรอนิกส์

**มาตรา 13 การสร้างความเสียหายผ่านสื่อสังคมออนไลน์**

การสร้างความเสียหายผ่านสื่อสังคมออนไลน์ แสดงออกด้วยการกระทำ ดังนี้

1. การเอาข้อมูลคอมพิวเตอร์ที่มีลักษณะใส่ร้ายป้ายสี หมิ่นประมาท ใช้คำศัพท์ไม่สุภาพเข้าสู่ระบบคอมพิวเตอร์

2. การเอาข้อมูลที่มีลักษณะใช้ความรุนแรง ข้อมูลที่ไม่เป็นความจริงเข้าสู่ระบบคอมพิวเตอร์

3. การเอาข้อมูลคอมพิวเตอร์ที่เป็นการทำร้ายความมั่นคงของชาติ ความสงบ ความเป็นระเบียบเรียบร้อยของสังคม และจารีตประเพณีอันดีงามของชาติ

4. การเอาข้อมูลคอมพิวเตอร์ที่มีลักษณะชวนเชื่อ ยุยง และส่งเสริมประชาชนต่อต้านรัฐบาลหรือแบ่งแยกความสามัคคี

5. การโฆษณาค้าขายยาเสพติด อาวุธสงคราม อาวุธเคมี ค้ามนุษย์ ค้าประเวณี ค้าโสเภณี และสิ่งที่ผิดกฎหมาย

6. การเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ ตามที่ได้กำหนดไว้ใน มาตรา 11 และมาตรา 14 ของกฎหมายฉบับนี้ รวมทั้งข้อ 1, 2, 3, 4 และข้อ 5 ของมาตรานี้

**มาตรา 14 การเผยแพร่สิ่งลามกผ่านระบบคอมพิวเตอร์**

สิ่งลามก หมายถึง รูป ภาพเคลื่อนไหว เสียง วิดีโอ และข้อมูลที่มีเนื้อหาซึ่งแสดงออกอย่างชัดเจนเกี่ยวกับอวัยวะเพศ และพฤติกรรมทางเพศของคน

การเผยแพร่สิ่งลามกผ่านระบบคอมพิวเตอร์ การซื้อขาย การแจกจ่าย การส่งต่อ การเผยแพร่ และการแนะนำข้อมูลดังที่ได้กำหนดไว้ในวรรคหนึ่งข้างต้นผ่านระบบคอมพิวเตอร์

**มาตรา 15 การรบกวนระบบคอมพิวเตอร์**

การรบกวนระบบคอมพิวเตอร์ หมายถึงการกระทำ ดังนี้

1. การสร้าง และใช้โปรแกรมคอมพิวเตอร์ ไวรัสหรือเครื่องมืออื่น เพื่อขัดขวางหรือทำลายการปฏิบัติงานของระบบคอมพิวเตอร์

2. การส่งข้อมูลระบบคอมพิวเตอร์หรือจดหมายทางอิเล็กทรอนิกส์ โดยมีการปกปิดที่อยู่หรือแหล่งที่มาของผู้ส่ง เพื่อรบกวนและ/หรือทำลายการปฏิบัติงานของระบบคอมพิวเตอร์

**มาตรา 16 การปลอมแปลงข้อมูลคอมพิวเตอร์**

การปลอมแปลงข้อมูลคอมพิวเตอร์ หมายถึง การใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ เพื่อเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ด้วยการกระทำ ดังนี้

1. การป้อนข้อมูล การเปลี่ยนแปลงข้อมูล การปลอมแปลงที่อยู่ทางอิเล็กทรอนิกส์หรือการลบข้อมูลในระบบคอมพิวเตอร์ ที่ส่งผลให้ข้อมูลทางระบบคอมพิวเตอร์อย่างใดอย่างหนึ่งเปลี่ยนแปลงจากข้อมูลเดิมโดยเจตนา

2. การป้อน และการเปลี่ยนแปลงข้อมูลธุรกรรมทางการเงิน ทางการค้า ความลับ และข้อมูลอื่นของบุคคล นิติบุคคล องค์กร โดยไม่ได้รับอนุญาต

3. การสร้างเว็บไซต์ปลอมเพื่อหลอกลวงให้ผู้ใช้บริการระบบคอมพิวเตอร์หรืออินเทอร์เน็ตป้อนข้อมูลบัญชีเงินฝาก รหัสบัตรเครดิต รหัสใช้อินเทอร์เน็ต และข้อมูลอื่น

**มาตรา 17 การทำลายข้อมูลคอมพิวเตอร์**

การทำลายข้อมูลคอมพิวเตอร์ หมายถึง การลบ การดัดแปลง และ/หรือ การปลอมแปลงข้อมูลคอมพิวเตอร์หรือข้อมูลในระบบคอมพิวเตอร์เพื่อทำให้ข้อมูลหรือระบบคอมพิวเตอร์นั้นเสียหาย

**มาตรา 18 การดำเนินกิจการเกี่ยวกับเครื่องมืออาชญากรรมทางระบบคอมพิวเตอร์**

การดำเนินกิจการเกี่ยวกับเครื่องมืออาชญากรรมทางระบบคอมพิวเตอร์ หมายถึง การผลิต มีไว้ครอบครอง ซื้อขาย จำหน่าย โฆษณา เผยแพร่หรือแนะนำเครื่องมือดังกล่าว เช่น โปรแกรมคอมพิวเตอร์หรือการออกแบบข้อมูลคอมพิวเตอร์ เป็นต้น เพื่อก่ออาชญากรรมทางระบบคอมพิวเตอร์

**มาตรา 19 การใช้ระบบคอมพิวเตอร์ในการก่อการร้าย**

การใช้ระบบคอมพิวเตอร์ในการก่อการร้าย หมายถึง การแนะนำวิธีสร้าง และใช้อาวุธสงคราม ยุทธวิธีในการก่อการร้ายผ่านระบบคอมพิวเตอร์ เพื่อสร้างความเสียหายให้แก่ความมั่นคงของชาติ และความเป็นระเบียบเรียบร้อยของสังคม

**มาตรา 20 การเล่นพนันที่ต้องห้ามผ่านระบบคอมพิวเตอร์**

การเล่นพนันที่ต้องห้ามผ่านระบบคอมพิวเตอร์ หมายถึง การพนันแบบหนึ่งโดยใช้ระบบคอมพิวเตอร์หรืออินเทอร์เน็ต เพื่อสร้างสิ่งอำนวยความสะดวก บริการเป็นเจ้ามือรับพนัน สร้างความไม่สงบให้แก่สังคม และปรากฏการณ์ถดถอยทางการเงินอื่น ๆ

# ภาคที่ 3
# การต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

## หมวดที่ 1
## การต้านอาชญากรรมทางระบบคอมพิวเตอร์

**มาตรา 21 การต้านอาชญากรรมทางระบบคอมพิวเตอร์**

การต้านอาชญากรรมทางระบบคอมพิวเตอร์ มีดังนี้

1. การแจ้งเตือน
2. การให้คำปรึกษา
3. การแจ้งเหตุฉุกเฉิน
4. การดำเนินการแก้ไข
5. การโต้ตอบ

**มาตรา 22 การแจ้งเตือน**

กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร เป็นผู้แจ้งภัยอันตรายที่เกิดขึ้นในระบบคอมพิวเตอร์ และอินเทอร์เน็ต เป็นต้น การแจ้งเตือนเว็บไซต์ โปรแกรมประสงค์ร้าย การแจ้งช่องโหว่ของระบบคอมพิวเตอร์ การหลอกลวงทางจดหมายอิเล็กทรอนิกส์ และอื่น ๆ

ผู้ให้บริการระบบคอมพิวเตอร์ต้องแจ้งเตือน และกำหนดเงื่อนไขในการเข้าถึงระบบคอมพิวเตอร์ เพื่อจำกัดหรือไม่อนุญาตให้ผู้ใช้บริการทั่วไปเข้าถึงระบบคอมพิวเตอร์

**มาตรา 23 การให้คำปรึกษา**

การให้คำปรึกษา หมายถึง กระบวนการสนทนา แลกเปลี่ยนความคิดเห็น ระหว่าง แขนงการไปรษณีย์โทรคมนาคม และการสื่อสาร กับผู้ขอคำปรึกษา เพื่อให้คำแนะนำ วิธีการแก้ไขทางด้านเทคนิค เพื่อลดการสูญเสียข้อมูล การรบกวนข้อมูล การยุติการทำงานของระบบคอมพิวเตอร์ การสกัดกั้นการกระจายไวรัสคอมพิวเตอร์ และการเข้าทำลายข้อมูลในระบบคอมพิวเตอร์

**มาตรา 24 การแจ้งเหตุฉุกเฉิน**

บุคคล นิติบุคคล และองค์กรทั้งภายใน และต่างประเทศ ที่ดำรงชีวิต เคลื่อนไหว และใช้ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์อยู่ สปป.ลาว ต้องแจ้งเหตุฉุกเฉินที่เกิดขึ้นกับระบบคอมพิวเตอร์ของตนหรือต่อแขนงการไปรษณีย์ โทรคมนาคม และการสื่อสาร

การแจ้งเหตุฉุกเฉิน สามารถดำเนินด้วยวิธีการ ดังนี้

1. คำร้องตามแบบพิมพ์
2. โทรศัพท์สายด่วน แฟกซ์
3. จดหมายอิเล็กทรอนิกส์
4. วิธีการอื่น

**มาตรา 25 การดำเนินการแก้ไข**

ภายหลังที่ได้รับแจ้งเหตุฉุกเฉินแล้ว กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสารต้องค้นคว้าพิจารณาคำร้อง และแจ้งตอบพร้อมทั้งแนะนำวิธีการแก้ไข ภายในกำหนดเวลา 5 วันทำงานราชการ

ในกรณีจำเป็น และเร่งด่วน กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร ต้องดำเนินการแก้ไขทางเทคนิควิชาการ ตามการร้องขอของผู้เกี่ยวข้องอย่างทันท้วงที่

**มาตรา 26 มาตรการในการโต้ตอบ**

กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร ใช้มาตรการโต้ตอบ ดังนี้

1. แจ้งให้ยุติการกระทำ
2. ตัดเนื้อหาการนำเสนอ
3. ปิดการใช้บริการชั่วคราวหรือถาวร
4. ถอนใบอนุญาต

## หมวดที่ 2
## การสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

**มาตรา 27 การสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์**

การสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ มีดังนี้

1. การจัดตั้งโฆษณาเผยแพร่
2. การฝึกอบรม
3. การให้ความรู้เกี่ยวกับความปลอดภัยทางระบบคอมพิวเตอร์
4. การสร้างกิจกรรมป้องกันข้อมูล
5. การเฝ้าละวังเหตุฉุกเฉิน
6. การเก็บสถิติ

**มาตรา 28 การจัดตั้งโฆษณา**

กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสารเป็นผู้สร้างคู่มือ แผนภาพติดผนัง (สติ๊กเกอร์) แผ่นโฆษณา สื่อสิ่งพิมพ์ และวิดีโอเกี่ยวกับการเฝ้าละวัง ป้องกันภัยทางระบบคอมพิวเตอร์ ประสานสมทบกับแขนงการอื่น องค์การปกครองท้องถิ่น โฆษณาเผยแพร่ ในขอบเขตทั่วประเทศ

**มาตรา 29 การฝึกอบรม**

แขนงการไปรษณีย์ โทรคมนาคม และการสื่อสาร ประสานสมทบกับแขนงการอื่น และองค์การปกครองท้องถิ่นที่เกี่ยวข้อง จัดฝึกอบรมให้แก่พนักงาน เจ้าหน้าที่ที่เกี่ยวข้องเกี่ยวกับงานต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ รวมทั้งงานสืบสวน-สอบสวน

**มาตรา 30 การให้ความรู้เกี่ยวกับความปลอดภัยทางระบบคอมพิวเตอร์**

กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร เป็นหน่วยงานหลักในการประสานสมทบกับภาคส่วนที่เกี่ยวข้อง กำหนดมาตรการเฉพาะในการรักษาความปลอดภัยทางระบบคอมพิวเตอร์ และให้ความรู้เกี่ยวกับมาตรการดังกล่าวแก่สังคม

กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสารเป็นเจ้าการประสานสมทบกับกระทรวงศึกษาธิการ และกีฬา นำเอาวิชาการเรียนด้านความปลอดภัยทางระบบคอมพิวเตอร์บรรจุเข้าในหลักสูตรการเรียน-การสอนแต่ชั้นมัธยมต้นขึ้นไป

**มาตรา 31 การสร้างกิจกรรมป้องกันข้อมูล**

เพื่อรับประกันความปลอดภัยทางระบบคอมพิวเตอร์ และการป้องกันข้อมูลคอมพิวเตอร์ แขนงการไปรษณีย์ โทรคมนาคม และการสื่อสาร แขนงการป้องกันความสงบ ผู้ให้บริการ และผู้รักษาข้อมูล ต้องสร้างกิจกรรมให้ความรู้ด้านความปลอดภัย การใช้ระบบคอมพิวเตอร์ เพื่อให้รู้เทคนิค และวิธีป้องกันข้อมูล อยู่ตามองค์การจัดตั้งของรัฐ เอกชน และสถานการศึกษา

**มาตรา 32 การเฝ้าระวังเหตุฉุกเฉิน**

แขนงการไปรษณีย์ โทรคมนาคม และการสื่อสาร เป็นผู้เฝ้าระวังเหตุฉุกเฉิน ด้วยการติดตาม ตรวจสอบ แนะนำ แจ้งเตือน ป้องกัน และโต้ตอบภัยอันตราย ที่เกิดขึ้นทางระบบคอมพิวเตอร์

**มาตรา 33 การเก็บสถิติ**

แขนงการไปรษณีย์ โทรคมนาคม และการสื่อสาร และแขนงการป้องกันความสงบ ต้องเก็บสถิติ และสร้างฐานข้อมูลเกี่ยวกับอาชญากรรมทางระบบคอมพิวเตอร์ พร้อมทั้งศึกษาค้นคว้าเป็นแต่ละระยะเพื่อค้นหาเงื่อนไข และสาเหตุที่พาให้เกิดอาชญากรรมทางระบบคอมพิวเตอร์

# หมวดที่ 3
# ศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์

**มาตรา 34 ศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์**

เพื่อทำให้การคุ้มครอง ติดตาม ตรวจตรา ต้าน สกัดกั้น จำกัด และกำจัดอาชญากรรมปกป้องระบบฐานข้อมูล ระบบเซิฟเวอร์ ข้อมูลคอมพิวเตอร์ และสามารถเชื่อมโยงกับภูมิภาค และสากล รัฐจัดตั้งศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์ โดยเขียนย่อว่า “สกค”

ศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์ หมายถึง หัวหน้าวิชาการหนึ่งมีฐานะเทียบเท่ากรม ซึ่งอยู่ภายใต้โครงประกอบการจัดตั้งของกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร มีภาระบทบาทเป็นเสนาธิการให้กระทรวงดังกล่าว ในการสกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์

**มาตรา 35 สิทธิและหน้าที่ของศูนย์สกัดกั้นและแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์**

ในการคุ้มครองงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์ มีสิทธิและหน้าที่ ดังนี้

1. ค้นคว้าผลักดันแผนยุทธศาสตร์ นโยบาย เป็นแผนการ แผนงาน และโครงการของตนเพื่อนำเสนอต่อกระทรวง และจัดตั้งปฏิบัติแผนดังกล่าว

2. ค้นคว้าระเบียบการต่าง ๆ เกี่ยวกับการคุ้มครองงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

3. โฆษณา เผยแพร่กฎหมาย และระเยียบการเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

4. สร้างแผนการเคลื่อนไหว และงบประมาณประจำปีเพื่อเสนอต่อกระทรวงพิจารณารับรอง

5. ค้นคว้าเสนอปรับปรุงภาระบทบาทหน้าที่ และโครงประกอบการองค์กรของศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์ เสนอการแต่งตั้งหรือปลดตำแหน่งงานขั้นรองหัวหน้าศูนย์ลงมา และการบรรจุซับซ้อนพนักงานต่อกระทรวง

6. ค้นคว้านำเสนอการยกย่องต่อบุคคล และนิติบุคคล ที่มีผลงานในการเข้าดำเนินงานต้านและสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

7. สร้าง ฝึกอบรม ยกระดับ และพัฒนาบุคลากรเกี่ยวกับงานด้านความปลอดภัยทางระบบคอมพิวเตอร์

8. เฝ้าระวัง ติดตาม ตรวจตรา แนะนำ แจ้งเตือน และโต้ตอบทุกเหตุการณ์ฉุกเฉินทางระบบคอมพิวเตอร์

9. แจ้งเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ต่อหน่วยงานที่เกี่ยวข้อง

10. ประสานงาน และให้การร่วมมือกับหน่วยงานที่เกี่ยวข้อง ในการดำเนินคดีทางระบบคอมพิวเตอร์ การดำเนินงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

11. แจ้งให้ผู้ให้บริการ และผู้รักษาข้อมูล อำนวยความสะดวก และสนองข้อมูลเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์

12. ค้นคว้านำเสนอแผนการประสานงาน ร่วมมือกับต่างประเทศ ภูมิภาค และสากลเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ต่อกระทรวง และจัดตั้งปฏิบัติแผนการดังกล่าว

13. สรุป และรายงานการดำเนินงานของตนต่อกระทรวงอย่างเป็นปกติ

14. ใช้สิทธิ และปฏิบัติหน้าที่อื่นตามที่ได้กำหนดไว้ในกฎหมาย และระเบียบการ

## ภาคที่ 4
## การร่วมมือสากลในการต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

**มาตรา 36 หลักการพื้นฐานในการร่วมมือ**

การร่วมมือสากลในการต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ระหว่างองค์การที่มีสิทธิอำนาจของ สปป.ลาว และต่างประเทศให้ปฏิบัติตามหลักการ เคารพเอกราชอำนาจอธิปไตย และผืนแผ่นดินอันครบถ้วนของกัน ไม่แทรกแซงงานภายในของกันและกัน เสมอภาพต่างฝ่ายต่างได้รับผลประโยชน์ และสอดคล้องกับสัญญาสากล และสนธิสัญญาที่ สปป.ลาว เป็นภาคี

**มาตรา 37 การร่วมมือทางด้านเทคนิควิชาการ**

การร่วมมือสากลทางด้านเทคนิควิชาการ ในการสกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์มีเนื้อหาหลัก ดังนี้

1. การแลกเปลี่ยนข้อมูลข่าวสารทางด้านเทคนิควิชาการในการต้าน และสกัดกั้นเหตุฉุกเฉินทางระบบคอมพิวเตอร์

2. การระงับหรือแจ้งให้ยุติการทำลายทางระบบคอมพิวเตอร์

3. การประสานกับผู้ให้บริการอยู่ต่างประเทศ เกี่ยวกับการใช้สื่อสังคมออนไลน์ ที่มีเนื้อหาตามที่ได้กำหนดไว้ในมาตรา 13 ของกฎหมายฉบับนี้

4. การให้การช่วยเหลือซึ่งกันและกันในการเฝ้าระวัง สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์ในงานสำคัญ เป็นต้น กองประชุมระดับชาติ ภูมิภาค และสากลรวมทั้งงานมหกรรมต่าง ๆ

**มาตรา 38 การช่วยเหลือซึ่งกันและกันทางกฎหมาย**

การร้องขอให้การช่วยเหลือซึ่งกันและกันทางกฎหมาย หมายถึง การร้องขอให้ทำการสืบสวน-สอบสวน ใช้มาตรการสกัดกั้น ออกคำสั่งให้เก็บรักษา และป้องกันข้อมูลทางระบบคอมพิวเตอร์ รวมทั้งข้อมูลจราจรทางระบบคอมพิวเตอร์ การสืบค้น การบ่งตัว และชี้ตัวผู้กระทำผิด การยึดหรือการอายัดอุปกรณ์หรือเครื่องมือที่ใช้ และเกี่ยวพันถึงการกระทำผิด การขอหลักฐานเพิ่มเติมเกี่ยวกับการกระทำผิด และการส่งผู้ร้ายข้ามแดน

สำหรับกลไก และขั้นตอนของการช่วยเหลือซึ่งกันและกันทางกฎหมายนั้น ให้ปฏิบัติตามกฎหมาย และระเบียบการที่เกี่ยวข้องของ สปป.ลาว สัญญาสากล และสนธิสัญญาที่ สปป.ลาว เป็นภาคี

**มาตรา 39 เนื้อหาของการร้องขอการช่วยเหลือซึ่งกันและกันทางกฎหมาย**

การร้องขอการช่วยเหลือซึ่งกัน และกันทางกฎหมายมีเนื้อหาหลัก ดังนี้

1. จุดประสงค์ ความจำเป็น และสภาพความเป็นจริงในการร้องขอ
2. ข้อมูลที่สำคัญสำหรับการยืนยัน การติดตาม และการบ่งตัวผู้กระทำผิดทางระบบคอมพิวเตอร์ ที่ต้องการเก็บรักษาหรือป้องกันเฉพาะ
3. การสรุปย่อเกี่ยวกับข้อมูลทางระบบคอมพิวเตอร์หรือข้อมูลจราจรทางระบบคอมพิวเตอร์ที่ต้องการเก็บรักษาหรือป้องกันเฉพาะ
4. เอกสารอ้างอิงทางด้านนิติกรรมเกี่ยวกับการกระทำของผู้ต้องหา
5. องค์การหรือเจ้าหน้าที่ที่เกี่ยวข้อง สามารถขอข้อมูลเพิ่มเติมจากประเทศที่ร้องขอการช่วยเหลือทางกฎหมาย

**มาตรา 40 การรักษาความลับ**

องค์การที่มีสิทธิเกี่ยวข้องของ สปป.ลาว ต้องรักษาความลับของประเทศที่ร้องขอการช่วยเหลือทางกฎหมาย

# ภาคที่ 5
# ข้อห้าม

**มาตรา 41 ข้อห้ามทั่วไป**

ห้ามบุคคล นิติบุคคล หรือองค์กรมีพฤติกรรม ดังนี้

1. มีพฤติกรรมตามที่ได้กำหนดไว้ในมาตรา 8 ของกฎหมายฉบับนี้

2. ทำลายหรือสร้างความเสียหายให้แก่อุปกรณ์อิเล็กทรอนิกส์ คอมพิวเตอร์ และสิ่งอำนวยความสะดวกต่าง ๆ ในการแลกเปลี่ยนข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์

3. มีพฤติกรรมอื่น ที่เป็นการละเมิดกฎหมาย และระเบียบการ

**มาตรา 42 ข้อห้ามสำหรับผู้ให้บริการ**

ห้ามผู้ให้บริการมีพฤติกรรม ดังนี้

1. ลบข้อมูลจราจรทางระบบคอมพิวเตอร์ก่อน 90 วันในกรณีเชื่อมต่อ และก่อน 360 วันในกรณีไม่เชื่อมต่อ

2. ลบข้อมูลผู้ใช้บริการระบบคอมพิวเตอร์ที่สร้างความเสียหายก่อน 90 วัน

3. สนองข้อมูลที่ไม่ถูกต้องให้เจ้าหน้าที่ และพนักงานที่เกี่ยวข้อง

4. เปิดเผยข้อมูลของผู้ใช้บริการโดยไม่ได้รับอนุญาต

5. สร้างเงื่อนไขหรืออำนวยความสะดวกให้แก่การก่ออาชญากรรมทางระบบคอมพิวเตอร์

6. มีพฤติกรรมอื่นที่เป็นการละเมิดกฎหมาย และระเบียบการ

**มาตรา 43 ข้อห้ามสำหรับเจ้าหน้าที่ และพนักงานที่เกี่ยวข้อง**

ห้ามเจ้าหน้าที่ และพนักงานที่เกี่ยวข้องมีพฤติกรรม ดังนี้

1. เปิดเผยความลับของรัฐ ความลับทางราชการ ของบุคคล นิติบุคคลหรือองค์กรผ่านทางระบบคอมพิวเตอร์

2. หน่วงเหนี่ยว และปลอมแปลงเอกสารเกี่ยวกับข้อมูลที่เป็นการกระทำผิดทางระบบคอมพิวเตอร์

3. ใช้หน้าที่ตำแหน่ง เพื่อผลประโยชน์ส่วนตัว ครอบครัว และพวกพ้อง

4. ละเลยหน้าที่ความรับผิดชอบที่องค์กรมอบหมายให้

5. มีพฤติกรรมอื่น ที่เป็นการละเมิดระเบียบกฎหมาย และระเบียบการ

# ภาคที่ 6
# การสืบสวน-สอบสวนคดีทางระบบคอมพิวเตอร์

**มาตรา 44 สาเหตุที่พาให้เปิดการสืบสวน-สอบสวน**

สาเหตุที่พาให้เปิดการสืบสวน-สอบสวนคดีทางระบบคอมพิวเตอร์มี ดังนี้

1. มีการแจ้งความ การรายงาน การร้องฟ้องของบุคคล นิติบุคคลหรือองค์กรเกี่ยวกับพฤติกรรมที่เป็นอาชญากรรมทางระบบคอมพิวเตอร์

2. มีการเข้ามอบตัวของผู้กระทำผิด

3. พบเห็นร่องรอย ข้อมูล หลักฐานของพฤติกรรมตามที่ได้กำหนดไว้ในมารตรา 8 ของกฎหมายฉบับนี้

**มาตรา 45 ขั้นตอนการสืบสวน-สอบสวนคดีทางระบบคอมพิวเตอร์**

ขั้นตอนการสืบสวน-สอบสวนคดีทางระบบคอมพิวเตอร์ให้ปฏิบัติ ดังนี้

1. การแจ้งความ การรายงานหรือการร้องฟ้อง
2. การเปิดการสืบสวน-สอบสวน
3. การดำเนินการสืบสวน-สอบสวน
4. การสรุปการสืบสวน-สอบสวน และการประกอบสำนวนคดี

**มาตรา 46 การแจ้งความ การรายงาน หรือการฟ้องร้อง**

การแจ้งความ การลายงานหรือการฟ้องร้องเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ให้แจ้งหรือยื่นต่อองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำตรวจหรือองค์การอัยการประชาชน

องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชนต้องพิจารณาการแจ้งความ การรายงานหรือการฟ้องร้อง ไม่ให้เกิน 5 วันทำงานราชการ นับแต่วันได้รับการแจ้งความ การรายงานหรือการฟ้องร้องเป็นต้นไป ในกรณีมีความยุ่งยากสับสน การกำหนดเวลาดังกล่าวไม่ให้เกิน 10 วันทำงานราชการ

**มาตรา 47 การเปิดการสืบสวน-สอบสวน**

ในกรณีที่มีข้อมูลหลักฐานรัดกุมเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ หัวหน้าองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือหัวหน้าองค์การอัยการประชาชน ต้องออกคำสั่งเปิดการสืบสวน-สอบสวนในขอบเขตสิทธิและหน้าที่ของตน ตามที่ได้กำหนดไว้ในกฎหมายว่าด้วยการกำเนินคดีอาญา

ในกรณีจำเป็น เร่งด่วน และมีข้อมูลที่ยืนยันได้ว่ากำลังมีการตระเตรียมหรือก่ออาชญากรรมทางระบบคอมพิวเตอร์ หัวหน้าองค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือหัวหน้าองค์การ

อัยการประชาชนต้องออกคำสั่งให้เก็บรักษา และป้องกันข้อมูลทางคอมพิวเตอร์หรือข้อมูลจราจรทางระบบคอมพิวเตอร์

ผู้ให้บริการหรือภาคส่วนที่คุ้มครองข้อมูลมีพันธะเก็บรักษา และปกป้องข้อมูลดังกล่าวไว้อย่างรีบด่วนจนกว่าจะสิ้นสุดการดำเนินคดี เพื่อรับประกันไม่ให้ข้อมูลมีการเปลี่ยนแปลงหรือเสียหาย

**มาตรา 48 การดำเนินการสืบสวน-สอบสวน**

องค์การสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจหรือองค์การอัยการประชาชน ต้องประสานงานกับหน่วงงานไปรษณีย์ โทรคมนาคม และการสื่อสาร และภาคส่วนที่เกี่ยวข้อง เพื่อดำเนินการค้นหาข้อมูลหลักฐานและที่มาของอาชญากรรมทางระบบคอมพิวเตอร์ เพื่อเป็นหลักฐานให้แก่การสืบสวน-สอบสวน

การดำเนินการสืบสวน-สอบสวนคดีทางระบบคอมพิวเตอร์ ต้องใช้วิธีการสืบสวน-สอบสวน มาตรการสกัดกั้น และกำหนดเวลาในการสืบสวน-สอบสวน ตามที่ได้กำหนดไว้ในกฎหมายว่าด้วยการดำเนินคดีอาญา

**มาตรา 49 การสรุปการสืบสวน-สอบสวน และการประกอบสำนวนคดี**

ภายหลังสิ้นสุดการสืบสวน-สอบสวนของเจ้าหน้าที่ตำรวจ ถ้ามีข้อมูลหลักฐานที่รัดกุมว่าการละเมิดนั้น เป็นการกระทำผิดทางระบบคอมพิวเตอร์ องค์การสืบสวน-สอบสวนต้องสรุป และประกอบสำนวนคดีส่งให้องค์การอัยการประชาชนพิจารณาสั่งฟ้องต่อศาล

ในกรณีองค์การอัยการประชาชน หากเป็นผู้ดำเนินการสืบสวน-สอบสวนก็ต้องสรุปประกอบสำนวนคดี และออกคำสั่งฟ้องต่อศาล เพื่อพิจารณาตัดสินตามกฎหมาย

# ภาคที่ 7
# การคุ้มครอง และการตรวจตรา

## หมวดที่ 1
## การคุ้มครอง

**มาตรา 50 องค์การคุ้มครอง**

รัฐบาลเป็นผู้คุ้มครองงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์อย่างรวมศูนย์ และเป็นเอกภาพ ในขอบเขตทั่วประเทศ โดยมอบให้กระทรวงไปรษณีย์ โทรคมนาคม และ

การสื่อสาร เป็นผู้รับผิดชอบโดยตรง และเป็นเจ้าการประสานสมทบกับกระทรวงป้องกันประเทศ (กระทรวงกลาโหม)กระทรวงป้องกันความสงบ (กระทรวงมหาดไทย) กระทวงวิทยาศาสตร์ และเทคโนโลยี กระทรวงแถลงข่าว วัฒนธรรม และท่องเที่ยว กระทรวงอื่น และองค์การปกครองส่วนท้องถิ่นที่เกี่ยวข้อง

องค์การคุ้มครองงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ประกอบด้วย

1. กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร
2. แผนกไปรษณีย์ โทรคมนาคม และการสื่อสารแขวง (จังหวัด) นครหลวงเวียงจันทน์
3. ห้องการไปรษณีย์ โทรคมนาคม และการสื่อสารเมือง (อำเภอ) เทศบาล

**มาตรา 51 สิทธิและหน้าที่ของกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร**

ในการคุ้มครองงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ กระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร มีสิทธิ และหน้าที่ ดังนี้

1. เสนอรัฐบาลพิจารณาสร้าง และปรับปรุงแผนยุทศาสตร์ นโยบาย กฎหมาย ระเบียบการเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์
2. รับรองแผนการ แผนงาน และโครงการเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ตามการเสนอของศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์
3. รับรองแผนงานการดำเนินงาน และงบประมาณประจำปี ตามการเสนอของศูนย์สกัดกั้นและแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์
4. รับรองระเบียบการต่าง ๆ ที่จำเป็นในการดำเนินการของศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์
5. พิจารณารับรองการค้นคว้า ปรับปรุงภารบทบาท และโครงสร้างองค์กรศูนย์สกัดกั้นและแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์
6. เสนอนายกรัฐมลตรีแต่งตั้งหรือปลดตำแหน่งหัวหน้าศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์
7. แต่งตั้งหรือปลดตำแหน่งรองหัวหน้าศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์ หัวหน้า และรองหัวหน้าแผนกศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์
8. พิจารณารับรองการรับ การบรรจุซับซ้อนพนักงานขั้นเทียบเท่ารองกรมลงมารวมทั้งการปฏิบัตินโยบายยกย่อง และวินัยต่อพนักงาน
9. ติดตามตรวจตราการดำเนินงานของศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์

10. สรุป และลายงานการเคลื่อนไหวงานของตนต่อรัฐบาลอย่างปกติ

11. ใช้สิทธิ และปฏิบัติหน้าที่อื่นตามที่ได้กำหนดไว้ในกฎหมาย และระเบียบการ

**มาตรา 52 สิทธิ และหน้าที่ของแผนกไปรษณีย์ โทรคมนาคม และการสื่อสารแขวง (จังหวัด) นคร (นครหลวงเวียงจันท์)**

ในการคุ้มครองงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ แผนกไปรษณีย์ โทรคมนาคม และการสื่อสาร แขวง นคร มิสิทธิ และหน้าที่ตามขอบเขตความรับผิดชอบของตน ดังนี้

1. โฆษณาเผยแพร่แผนยุทศาสตร์ นโยบาย กฎหมาย ระเบียบการเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ แล้วจัดตั้งปฏิบัติ

2. ขึ้นแผนสร้าง ฝึกอบรม ยกระดับ และพัฒนาบุคลากรเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ แล้วเสนอต่อหน่วยงานบังคับบัญชาต่อไป

3. แจ้งเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ ต่อองค์การสืบสวน-สอบสวน และองค์การอัยการประชาชน

4. ประสานสมทบ และให้การร่วมมือกับองค์การสืบสวน-สอบสวน และองค์การอัยการประชาชนในการดำเนินคดีทางระบบคอมพิวเตอร์

5. แจ้งต่อผู้ให้บริการ ผู้รักษาข้อมูล อำนวยความสะดวก และสนองข้อมูลเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์

6. ประสานสมทบกับแผนกการอื่นที่เกี่ยวข้อง ในการดำเนินงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

7. ประสานงานร่วมมือกับศูนย์สกัดกั้น และแก้ไขเหตุฉุกเฉินทางระบบคอมพิวเตอร์ของกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร

8. เก็บสถิติเกี่ยวกับอาชญากรรมทางระบบคอมพิวเตอร์

9. ประสานงาน ร่วมมือกับต่างประเทศ ภูมิภาค และสากลเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ตามการมอบหมาย

10. สรุป และรายงานการดำเนินงานของตนต่อกระทรวงไปรษณีย์ โทรคมนาคม และการสื่อสาร และองค์กรปกครองแขวง นคร อย่างปกติ

11. ใช้สิทธิ และปฏิบัติหน้าที่อื่นตามที่ได้กำหนดไว้ในกฎหมาย และระเบียบการ

**มาตรา 53 สิทธิและหน้าที่ของห้องการไปรษณีย์ โทรคมนาคม และการสื่อสาร เมือง (อำเภอ) เทศบาล**

ในการคุ้มครองงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ห้องการไปรษณีย์ โทรคมนาคม และการสื่อสาร เมือง (อำเภอ) เทศบาล มีสิทธิ และหน้าที่ตามขอบเขตความรับผิดชอบของตน ดังนี้

1. เผยแพร่แผนยุทศาสตร์ นโยบาย ระเบียบการเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ แล้วจัดตั้งปฏิบัติ

2. ขึ้นแผน สร้าง ฝึกอบรม ยกระดับ และพัฒนาบุคลากรเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ แล้วเสนอต่อหน่วยงานบังคับบัญชาต่อไป

3. แจ้งเกี่ยวกับการกระทำผิดทางระบบคอมพิวเตอร์ ต่อองค์การสืบสวน-สอบสวนหรือองค์การอัยการประชาชน

4. ประสานสมทบ และให้การร่วมมือกับองค์การสืบสวน-สอบสวนหรือองค์การอัยการประชาชนในการดำเนินคดีทางระบบคอมพิวเตอร์

5. ประสานสมทบกับห้องการอื่นที่เกี่ยวข้อง ในการเคลื่อนไหวต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

6. เก็บสถิติเกี่ยวกับอาชญากรรมทางระบบคอมพิวเตอร์

7. สรุป และรายงานการดำเนินงานของตนต่อแผนกไปรษณีย์ โทรคมนาคม และการสื่อสาร และองค์การปกครองเมือง เทศบาล อย่างปกติ

8. ใช้สิทธิ และปฏิบัติหน้าที่อื่นตามที่ได้กำหนดไว้ในกฎหมาย และระเบียบการ

**มาตรา 54 สิทธิ และหน้าที่ของแขนงการอื่น**

ในการคุ้มครองงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ แขนงการอื่นที่เกี่ยวข้อง ได้แก่ แขนงการป้องกันประเทศ ป้องกันความสงบ วิทยาศาสตร์ และเทคโนโลยี แถลงข่าว วัฒนธรรม และท่องเที่ยว มีสิทธิ และหน้าที่เข้าร่วม ให้การร่วมมือในการต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ รายงาน และสนองข้อมูลเกี่ยวกับอาชญากรรมดังกล่าว ตามขอบเขตความรับผิดชอบของตน

# หมวดที่ 2

# การตรวจตรา

**มาตรา 55 องค์การตรวจตรา**

องค์การตรวจตรางานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ ประกอบด้วย

1. องค์การตรวจตราภายใน ซึ่งหมายถึงองค์การเดียวกันกับองค์การคุ้มครองงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ตามที่ได้กำหนดไว้ใน มาตรา 48 ของกฎหมายฉบับนี้

2. องค์การตรวจตราภายนอก ได้แก่ สภาแห่งชาติ องค์การตรวจสอบแห่งรัฐ และองค์การตรวจตารัฐบาลและต้านการฉ้อราชบังหลวง แนวลาวสร้างชาติ และองค์การจัดตั้งมหาชน

**มาตรา 56 เนื้อในการตรวจตรา**

เนื้อในการตรวจตรางานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ มีดังนี้

1. การปฏิบัติแผนยุทศาสตร์ นโยบาย กฎหมาย และระเบียบการเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

2. การจัดตั้งและการดำเนินงานขององค์การคุ้มครองงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์

3. การปฏิบัติตามสนธิสัญญาและสัญญาสากลเกี่ยวกับงานต้าน และสกัดกั้นอาชญากรรมทางระบบคอมพิวเตอร์ที่ สปป.ลาว เป็นภาคี

**มาตรา 57 รูปการการตรวจตรา**

การตรวจตราดำเนินด้วยรูปการ ดังนี้

1. การตรวจตราอย่างเป็นระบบปกติ
2. การตรวจตราโดยมีการแจ้งให้ล่วงหน้า
3. การตรวจตราแบบกะทันหัน

การตรวจตราอย่างเป็นระบบปกติ หมายถึง การตรวจตราที่ดำเนินไปตามแผนการอย่างเป็นประจำและมีกำหนดเวลาอันแน่นอน

การตรวจตราโดยมีการแจ้งให้ล่วงหน้า หมายถึง การตรวจตรานอกแผนการ เมื่อเห็นว่ามีความจำเป็นซึ่งแจ้งให้ผู้ที่จะถูกตรวจตราทราบล่วงหน้า

การตรวจตราแบบกะทันหัน หมายถึง การตรวจตราโดยเร่งด่วนซึ่งมิได้แจ้งให้ผู้ถูกตรวจตราทราบล่วงหน้า

ในการดำเนินการตรวจตราให้ปฏิบัติถูกต้องตามกฎหมาย และระเบียบการอย่างเข้มงวด

# ภาคที่ 8
# นโยบายต่อผู้มีผลงาน และมาตรการต่อผู้ละเมิด

**มาตรา 58 นโยบายต่อผู้มีผลงาน**

บุคคล นิติบุคคลหรือองค์กรที่มีผลงานดีเด่นในการปฏิบัติตามกฎหมายฉบับนี้ ได้แก่ การรายงาน การให้ความร่วมมือ การสนองข้อมูลเกี่ยวกับพฤติกรรมที่เป็นอาชญากรรมทางระบบคอมพิวเตอร์ จะได้รับการยกย่องและนโยบายอื่นตามระเบียบการ

**มาตรา 59 มาตรการต่อผู้ละเมิด**

บุคคล นิติบุคคล หรือองค์กรที่ละเมิดกฎหมายฉบับนี้ ได้แก่ ข้อห้าม จะถูกศึกษาอบรม กล่าวเตือน ลงวินัย ปรับ ใช้แทนค่าเสียหายทางแพ่ง หรือถูกลงโทษทางอาญา ตามแต่กรณีเบาหรือหนัก ตามที่ได้กำหนดไว้ในกฎหมาย และระเบียบ

**มาตรา 60 มาตราการศึกษาอบรม**

บุคคล นิติบุคคล หรือองค์กรที่ละเมิดกฎหมายฉบับนี้ ซึ่งเป็นการละเมิดครั้งแรก และก่อความเสียหายไม่มากมายจะถูกศึกษาอบรม และกล่าวเตือน

**มาตรา 61 มาตรการทางวินัย**

เจ้าหน้าที่ และพนักงานที่เกี่ยวข้องที่ได้ละเมิดกฎหมายฉบับนี้ ซึ่งไม่เป็นการกระทำผิดทางอาญา จะถูกลงวินัยตามแต่ละกรณี ดังนี้

1. ติเตียน กล่าวเตือนความผิดตามระเบียบการพร้อมทั้งบันทึกไว้ในประวัติของผู้กระทำความผิด
2. หยุดชั่วคราวการเลื่อนชั้น ขั้นเงินเดือนและการยกย่อง
3. ปลดตำแหน่งหรือโยกย้ายไปรับหน้าที่อื่น ที่มีตำแหน่งต่ำกว่าเดิม
4. ให้ออกจากราชการ โดยไม่ได้รับนโยบายใด ๆ

ผู้ถูกลงวินัย ต้องส่งคืนทรัพย์สินที่ตนได้มาจากการปฏิบัติหน้าที่ของตนที่ไม่ถูกต้องนั้นให้องค์กรอย่างคบถ้วน

**มาตรา 62 มาตรการปรับ**

บุคคล นิติบุคคล หรือองค์กรที่ละเมิดกฎหมายฉบับนี้ จะถูกปรับในกรณี ดังนี้

1. สนองข้อมูลที่ไม่ถูกต้องให้เจ้าหน้าที่ และพนักงานที่เกี่ยวข้อง ซึ่งไม่สร้างความเสียหายให้แก่ผู้ใดผู้หนึ่ง
2. หน่วงระยะเวลาในการสนองข้อมูลให้เจ้าหน้าที่ และพนักงานที่เกี่ยวข้อง

3. ลบข้อมูลในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของผู้อื่นที่ไม่ได้รับอนุญาตจากผู้ที่เกี่ยวข้อง

4. กรณีอื่นที่ได้กำหนดไว้ในกฎหมาย และระเบียบการเกี่ยวกับการละเมิดทางบริหาร

อัตราค่าปรับตามแต่ละกรณีได้กำหนดไว้ในระเบียบการเฉพาะ

**มาตรา 63 มาตรการทางแพ่ง**

บุคคล นิติบุคคล หรือองค์กรที่ละเมิดกฎหมายฉบับนี้ ซึ่งได้สร้างความเสียหายแก่ผู้อื่นต้องใช้แทนค่าเสียหายที่ตนได้กระทำขึ้น

**มาตรา 64 มาตรการทางอาญา**

บุคคลใดที่ได้กระทำผิดในฐานการกระทำผิดต่อไปนี้จะถูกลงโทษ ดังนี้

1. การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกตั้งแต่ 1 เดือน ถึง 1 ปี และปรับตั้งแต่ 1,000,000 กีบ ถึง 4,000,000 กีบ

2. การเข้าถึงระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต ต้องระวางโทษจำคุกตั้งแต่ 3 เดือน ถึง 1 ปี และปรับตั้งแต่ 2,000,000 กีบ ถึง 5,000,000 กีบ

3. การตัดต่อเนื้อหา รูป ภาพเคลื่อนไหว เสียง และวิดีโอโดยไม่ได้รับอนุญาต ต้องระวางโทษจำคุกตั้งแต่ 3 เดือน ถึง 2 ปี และปรับตั้งแต่ 3,000,000 กีบ ถึง 10,000,000 กีบ

4. การดักรับข้อมูลในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ต้องระวางโทษจำคุกตั้งแต่ 3 เดือน ถึง 2 ปี และปรับตั้งแต่ 4,000,000 กีบ ถึง 20,000,000 กีบ

5. การสร้างความเสียหายผ่านสื่อสังคมออนไลน์ ต้องระวางโทษจำคุกตั้งแต่ 3 เดือน ถึง 3 ปี และปรับตั้งแต่ 4,000,000 กีบ ถึง 25,000,000 กีบ

6. การเผยแพร่สิ่งลามกผ่านระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกตั้งแต่ 1 ปี ถึง 3 ปี และปรับตั้งแต่ 5,000,000 กีบ ถึง 30,000,000 กีบ

7. การรบกวนระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกตั้งแต่ 1 ปี ถึง 5 ปี และปรับตั้งแต่ 5,000,000 กีบ ถึง 40,000,000 กีบ

8. การปลอมแปลงข้อมูลคอมพิวเตอร์ ต้องระวางโทษจำคุกตั้งแต่ 1 ปี ถึง 5 ปี และปรับตั้งแต่ 5,000,000 กีบ ถึง 30,000,000 กีบ

9. การทำลายข้อมูลคอมพิวเตอร์ ต้องระวางโทษจำคุกตั้งแต่ 3 ปีถึง 5 ปี และปรับตั้งแต่ 10,000,000 กีบถึง 50,000,000 กีบ

10. การดำเนินกิจการเกี่ยวกับเครื่องมืออาชญากรรมทางระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกตั้งแต่ 3 ปี ถึง 5 ปี และปรับตั้งแต่ 10,000,000 กีบ ถึง 50,000,000 กีบ

11. การใช้ระบบคอมพิวเตอร์ในการก่อการร้าย ต้องระวางโทษจำคุกตั้งแต่ 5 ปี ถึง 10 ปี และปรับตั้งแต่ 50,000,000 กีบ ถึง 400,000,000 กีบ

12. การเล่นการพนันที่ต้องห้ามผ่านระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกตั้งแต่ 1 ปี ถึง 3 ปี และปรับตั้งแต่ 5,000,000 กีบ ถึง 30,000,000 กีบ

## ภาคที่ 9
## บทบัญญัติสุดท้าย

**มาตรา 65 การจัดตั้งปฏิบัติ**

รัฐบาลแห่งสาธารณรัฐประชาธิปไตยประชาชนลาว เป็นผู้จัดตั้งปฏิบัติกฎหมายฉบับนี้

**มาตรา 66 ผลศักดิ์สิทธิ์**

กฎหมายฉบับนี้มีผลศักดิ์สิทธิ์ นับแต่วันที่ประธานประเทศแห่งสาธารณรัฐประชาธิปไตยประชาชนลาว ได้ออกรัฐดำรัฐประกาศใช้ และภายหลังได้ลงจดหมายเหตุทางราชการ 15 วัน

ข้อกำหนด บทบัญญัติใดที่ขัดกับกฎหมายฉบับนี้ล้วนแต่ถูกยกเลิก

**ประธานสภาแห่งชาติ**

# ประวัติผู้เขียน

# ประวัติผู้เขียน

| | |
|---|---|
| **ชื่อ** | นางเกมอุรา ไชยวงศ์ |
| **วัน เดือน ปีเกิด** | 5 เมษายน 2521 |
| **สถานที่อยู่ปัจจุบัน** | บ้านเลขที่ 269 หน่วยที่ 25 บ้านโคกชาย<br>เมืองหาดซายฟอง นครหลวงเวียงจันทน์<br>สาธารณรัฐประชาธิปไตยประชาชนลาว |
| **ประวัติการศึกษา** | |
| 2549 | ปริญญาตรี นิติศาสตรบัณฑิต<br>กฎหมายการปกครอง มหาวิทยาลัยแห่งชาติ |
| 2540 | ประกาศนียบัตรสาขาบัญชี<br>โรงเรียนรัตนะ นครหลวงเวียงจันทน์ |
| **ประวัติการทำงาน** | |
| 2552-ปัจจุบัน | หัวหน้าแผนกนโยบาย กรมจัดตั้งและพนักงาน<br>กระทรวงยุติธรรม |
| 2549-2552 | รองหัวหน้าแผนกนโยบาย กรมจัดตั้งและพนักงาน<br>กระทรวงยุติธรรม |
| 2541-2549 | เจ้าหน้าที่บริหาร กรมจัดตั้งและพนักงาน<br>กระทรวงยุติธรรม |