# ปัญหาของการดำเนินคดีอาญา ศึกษากรณีการค้น การยึด พยานหลักฐาน ที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

**นางสาววรรณิศา คำฟูบุตร**

การศึกษาค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตร์มหาบัณฑิต
วิชาเอกกฎหมายอาญาและกระบวนการยุติธรรม สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2564

# The problem of criminal prosecution : A case study of search, seizure, and evidence from the commission of computer crimes

**Ms. Wannisa Kumfubut**

An Independent Study Submitted in Partial Fulfillment of the Requirements for

the Degree of Master of Laws in Criminal Law and Criminal Justice

School of Law

Sukhothai Thammathirat Open University

2021

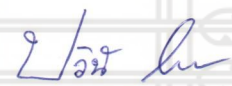
| | |
|---|---|
| **หัวข้อการศึกษาค้นคว้าอิสระ** | ปัญหาของการดำเนินคดีอาญา ศึกษากรณีการค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ |
| **ชื่อและนามสกุล** | นางสาววรรณิศา คำฟูบุตร |
| **วิชาเอก** | กฎหมายอาญาและกระบวนการยุติธรรม |
| **สาขาวิชา** | นิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช |
| **อาจารย์ที่ปรึกษา** | รองศาสตราจารย์อาจารี มีอินทร์เกิด มีสิทธิ์ |

การศึกษาค้นคว้าอิสระนี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 11 สิงหาคม 2565

คณะกรรมการสอบการศึกษาค้นคว้าอิสระ

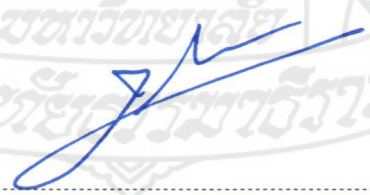
..... ประธานกรรมการ

(รองศาสตราจารย์อาจารี มีอินทร์เกิด มีสิทธิ์)



..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร. ปวินี ไพรทอง)



.....

(รองศาสตราจารย์วรวุฒิ เทพทอง)

ประธานกรรมการประจำสาขาวิชานิติศาสตร์

**ชื่อการศึกษาค้นคว้าอิสระ** ปัญหาของการดำเนินคดีอาญา ศึกษากรณีการค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

**ผู้ศึกษา** นางสาววรรณิศา คำฟูบุตร **รหัสนักศึกษา** 2614003453 **ปริญญา** นิติศาสตรมหาบัณฑิต

**อาจารย์ที่ปรึกษา** รองศาสตราจารย์อาจารี มีอินทร์เกิด มีสิทธิ์ **ปีการศึกษา** 2564

## บทคัดย่อ

การศึกษาค้นคว้าอิสระนี้มีวัตถุประสงค์เพื่อ (1) ศึกษารูปแบบการกระทำความผิดที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด (2) ศึกษาการควบคุม การค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ตามกฎหมายไทยและกฎหมายต่างประเทศ (3) ศึกษาบทบัญญัติกฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทยและกฎหมายต่างประเทศ (4) ศึกษาถึงปัญหาในการดำเนินคดีอาญาในส่วนของการควบคุม การค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ตามกฎหมายไทยเปรียบเทียบกฎหมายต่างประเทศ (5) ศึกษาแนวทางแก้ไข ปรับปรุงและพัฒนาบทบัญญัติกฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ให้มีประสิทธิภาพ

การศึกษาค้นคว้าอิสระนี้ เป็นการวิจัยเชิงคุณภาพ ด้วยวิธีวิจัยเอกสารจากตัวบทกฎหมาย ตำราทางวิชาการ งานวิจัย คำพิพากษาศาลฎีกา บทความในวารสารหรือนิตยสารทางกฎหมาย ข้อมูลจากเว็บไซต์ทางอินเตอร์เน็ตทั้งของประเทศไทยและของต่างประเทศเกี่ยวกับการดำเนินคดีกับผู้ที่กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ เพื่อนำมาเป็นข้อมูลในการวิเคราะห์ปัญหา เปรียบเทียบ สรุปและข้อเสนอแนะ

จากการศึกษาพบว่า (1) รูปแบบของอาชญากรรมทางคอมพิวเตอร์แตกต่างไปตามความประสงค์ของอาชญากรว่าต้องการให้เกิดความเสียหายรูปแบบใด ซึ่งรูปแบบการกระทำความผิดเปลี่ยนไปตามวิวัฒนาการทางเทคโนโลยี (2) ประเทศไทยที่กำหนดให้การค้นของเจ้าพนักงานในที่รโหฐานต้องมีหมายค้นเช่นเดียวกับสหรัฐอเมริกาและสหพันธ์สาธารณรัฐเยอรมนี (3) กฎหมายการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทยกับกฎหมายของสหรัฐอเมริกามีความคล้ายคลึงกันโดยมีบทบัญญัติกฎหมายเฉพาะแตกต่างจากสหพันธ์สาธารณรัฐเยอรมนีไม่มีกฎหมายเฉพาะแต่บัญญัติเพิ่มเติมในกฎหมายอาญา (4) ปัญหาการดำเนินคดีอาญา กรณีการค้น การยึด พยานหลักฐานและปัญหาการซ้ำซ้อนระหว่างพนักงานเจ้าหน้าที่กับพนักงานสอบสวน (5) ผู้ศึกษาเห็นควรมีการจัดตั้งสำนักงานอัยการคดีอาชญากรรมทางเทคโนโลยีเป็นผู้มีอำนาจในการพิจารณาคำร้องการค้น การยึด พยานหลักฐานทางคอมพิวเตอร์ และแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 29 วรรค 2 กำหนดให้อำนาจในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นอำนาจของพนักงานเจ้าหน้าที่เป็นผู้ดำเนินการเพื่อไม่ให้เกิดความยุ่งยากในการประสานงาน

**คำสำคัญ** การดำเนินคดีอาญา พยานหลักฐาน ความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

**Independent study title**: The problem of criminal prosecution: A case study of search, seizure, and evidence from the commission of computer crimes.
**Author :** Miss Wannisa Kumfubut; **ID** : 2614003453 ; **Degree** : Master of Laws ;
**Independent Study advisors** : Arjaree Meeintarakerd Meesidhi, Associate Professor;
**Academic Year** : 2021

## Abstract

The objectives of this independent study are: (1) to study crime patterns that are using computers as a tool to commit crimes; (2) to study the control, the search, and the seizure of evidence involving the commission of crimes relating to computer crimes according to Thai law and foreign laws (3) Study the legal provisions related to criminal prosecution relating to computer crimes according to Thai law and foreign laws (4) Study the problems in a criminal prosecution of the control, the search, the seizure of witnesses evidence involving criminal offenses related to computer crimes according to Thai law compare to foreign laws. (5) Study the solutions, improvement, and development of legal provisions related to criminal prosecution of computer crimes to be effective.

This independent study is qualitative research by means of documentary research from the law academic textbooks, research papers, the judgments of the Supreme Court, and articles in legal journals or magazines from both Thai and foreign, internet websites about the prosecution of people who commit crimes related to computer crimes, to be used as data for problem analysis, comparison, conclusions, and giving recommendations.

This study found that (1) the pattern of computer crime differed according to the intentions of the criminals to determine what kind of damage they want. The pattern of crime has changed according to the evolution of technology. (2) In Thailand requires that officers who search in private places have a search warrant as same as in the United States and Germany. (3) Criminal prosecution laws on computer crimes in Thailand and United States law are similar in that they have specific Acts. In Germany is no specific law, but additional provisions in Criminal Code. (4) Problems of criminal prosecution regarding searches, seizure, evidence, and duplication between competent officials and investigators. (5) I, the researcher, recommend that there should be established a Technology Crime Prosecutor's Office to be permitted the search and seizure in the case of computer crimes, and shall amend the Cybercrime and Computer-related Crimes Act 2007, Section 29, paragraph 2 stipulates the power to arrest, control, search, conduct investigations, and prosecute offenders according to the Cybercrime and Computer-related Crimes Act 2007 is the authority of the competent official to act in order to avoid the problem of coordination.

**Keywords:** criminal prosecution, evidence, computer crimes

# กิตติกรรมประกาศ

งานวิจัยเล่มนี้สำเร็จได้เนื่องจากได้รับความช่วยเหลือและความกรุณาจากบุคคลหลายฝ่าย ผู้วิจัยขอกราบขอบพระคุณรองศาสตราจารย์อาจารี มีอินทร์เกิด มีสิทธิ์ ที่ได้เสียสละเวลาอันมีค่า เป็นอาจารย์ที่ปรึกษา และคอยให้คำแนะนำ คำปรึกษา แก้ไขความบกพร่อง ตรวจสอบการศึกษาวิจัยนี้จนสำเร็จได้

นอกจากนี้ ผู้วิจัยขอขอบพระคุณ คณาจารย์ทุกท่านที่ได้ให้วิชาความรู้แก่ผู้วิจัย รวมถึงผู้ที่เป็นเจ้าของงานเขียนในหนังสือ วารสาร บทความ ในเรื่องที่เกี่ยวข้องกับงานวิจัยเล่มนี้ ที่ผู้วิจัยได้ศึกษาค้นคว้าและอ้างอิงถึงผลงานทางวิชาการ ซึ่งเป็นประโยชน์ในการศึกษาค้นคว้างานวิจัยเล่มนี้เป็นอย่างยิ่ง

วรรณิศา คำฟูบุตร

11 สิงหาคม 2565

# สารบัญ

# สารบัญ (ต่อ)

หน้า

# สารบัญตาราง

หน้า



# บทที่ 1
# บทนำ

## 1. ความเป็นมาและความสำคัญของปัญหา

การพัฒนาระบบเทคโนโลยีให้มีความก้าวหน้ากับสภาพสังคมในปัจจุบัน และนำเทคโนโลยีมาใช้ในการติดต่อสื่อสาร การเผยแพร่และรับข้อมูลข่าวสารผ่านเครือข่ายอินเตอร์เน็ต เนื่องจากมีความสะดวกรวดเร็วและสามารถเข้าถึงความเคลื่อนไหวในสังคมได้ทันต่อเหตุการณ์ ไม่ว่าจะอยู่ใกล้หรือไกลเพียงใดก็ตาม ทำให้คอมพิวเตอร์ โทรศัพท์ และอุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการติดต่อสื่อสารมีความสำคัญมากต่อมนุษย์ในยุคปัจจุบัน นอกเหนือจากการนำเทคโนโลยีมาใช้ในการติดต่อสื่อสารระหว่างกันแล้ว มนุษย์ยังนำมาใช้ในการทำธุรกรรมผ่านทางสื่ออิเล็กทรอนิกส์ ทำให้บุคคลที่ไม่ต้องพบปะกันแต่สามารถทำธุรกรรมต่างๆด้วยกันได้ ไม่ว่าจะเป็นการซื้อขาย การตกลงทำธุรกิจ การแลกเปลี่ยนข้อมูล โดยผ่านทางคอมพิวเตอร์ โทรศัพท์ และอุปกรณ์อิเล็กทรอนิกส์อื่นๆ

เมื่อการติดต่อสื่อสารและการเผยแพร่หรือรับข้อมูลข่าวสารผ่านเครือข่ายอินเตอร์เน็ตเป็นที่นิยมมากในสังคมปัจจุบัน จึงทำให้มีบุคคลใช้เป็นช่องทางในการกระทำความผิดก่ออาชญากรรมโดยใช้ระบบคอมพิวเตอร์ โทรศัพท์ และอุปกรณ์อิเล็กทรอนิกส์อื่นๆผ่านทางเครือข่ายอินเตอร์เน็ต ซึ่งสามารถกระทำได้หลากหลายรูปแบบ ไม่ว่าจะเป็นการหลอกลวงผ่านการติดต่อทางสื่ออิเล็กทรอนิกส์ การเข้าถึงระบบหรือข้อมูลของผู้อื่น การทำลายข้อมูล การทำลายระบบ การสร้างขึ้น ตัดต่อ เติมหรือการเปลี่ยนแปลงข้อมูล การดักรับข้อมูล การส่งข้อความรบกวน การแสดงข้อมูลอันเป็นเท็จ การส่งต่อข้อมูลที่ผิดกฎหมาย เป็นต้น การกระทำดังกล่าวนั้นอาจทำให้เกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศและอาจก่อให้เกิดความหวาดกลัวและตื่นตระหนกแก่ประชาชน

การดำเนินคดีกับผู้ที่กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์นั้นประเทศไทยได้นำกฎหมายวิธีพิจารณาความอาญามาใช้บังคับกับกระบวนการ ในการแสวงหาข้อเท็จจริงและพยานหลักฐานในการนำตัวผู้กระทำความผิดมาลงโทษ แต่เนื่องจากการก่ออาชญากรรมทางคอมพิวเตอร์มีวิธีการที่ซับซ้อนและผู้กระทำความผิดมักเป็นบุคคลที่มีความรู้ใน

ด้านเทคโนโลยีเป็นอย่างดี และไม่สามารถหาตัวตนที่อยู่แน่นอนได้ ซึ่งต้องใช้กระบวนการในการสืบค้นตัว หากบุคคลเหล่านั้นไม่ได้อยู่ในราชอาณาจักรไทย จะทำให้ลำบากในการเข้าถึงตัวผู้กระทำความผิด แม้จะมีการแต่งตั้งพนักงานเจ้าหน้าที่ให้มีอำนาจตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เพื่อสืบสวนสอบสวนหาพยานหลักฐานที่เกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด และให้มีอำนาจควบคุมดูแลเว็บไซต์ที่เกิดจากการกระทำความผิดก็สามารถควบคุมได้เพียงชั่วคราว เนื่องจากเครือข่ายอินเตอร์เน็ตสามารถแพร่กระจายข่าวสารได้อย่างรวดเร็ว จึงทำให้เกิดความไม่มั่นใจในเรื่องการปิดกั้นเว็บไซต์บางเนื้อหาว่าสามารถจะปิดกั้นได้ทั้งหมดและก่อให้เกิดปัญหาในการป้องกันการก่ออาชญากรรมทางคอมพิวเตอร์และการดำเนินคดี การจับ การควบคุม การค้น และการรวบรวมพยานหลักฐาน เนื่องจากพยานหลักฐานอิเล็กทรอนิกส์มีความแตกต่างจากพยานหลักฐานทั่วไป เป็นเพียงข้อมูลในระบบซึ่งง่ายต่อการแก้ไข เปลี่ยนแปลงและทำลาย และการค้นและรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ต้องได้รับคำสั่งอนุญาตจากศาล ก่อให้เกิดความล่าช้าในการเข้าถึงพยานหลักฐานและทำให้ผู้กระทำความผิดสามารถแก้ไขเปลี่ยนแปลงและทำลายพยานหลักฐานได้ ซึ่งกระทบต่อความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ที่จะต้องนำสืบในชั้นศาลเพื่อประกอบในการพิจารณาคดีตัดสินลงโทษผู้กระทำความผิด

จะเห็นได้ว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และบทบัญญัติกฎหมายวิธีพิจารณาความอาญาไม่สามารถครอบคลุมไปถึงอาชญากรรมทางคอมพิวเตอร์ได้เท่าที่ควร รวมทั้งปัญหาในกรณีที่หากพบการกระทำความผิดที่ไม่เกี่ยวกับหมายค้นจะสามารถดำเนินการกับคอมพิวเตอร์เครื่องนั้นได้หรือไม่ และในกรณีการค้นในที่รโหฐานต้องทำในเวลากลางวัน แต่หากเป็นข้อมูลหรือพยานหลักฐานอิเล็กทรอนิกส์ พนักงานเจ้าหน้าที่จะทำการค้นในกรณีฉุกเฉินได้หรือไม่ จึงเป็นปัญหาและอุปสรรคต่อการดำเนินคดีกับผู้กระทำความผิดเพื่อให้กระบวนการในการดำเนินคดี การแสวงหาข้อเท็จจริงและการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ ในความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มีประสิทธิภาพมากยิ่งขึ้น จึงจำเป็นที่จะต้องหาแนวทางการแก้ไขพัฒนา

## 2. วัตถุประสงค์การวิจัย

2.1 เพื่อศึกษารูปแบบการกระทำความผิดที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด

2.2 เพื่อศึกษาการควบคุม การค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ตามกฎหมายไทยและกฎหมายต่างประเทศ

2.3 เพื่อศึกษาบทบัญญัติกฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทยและกฎหมายต่างประเทศ

2.4 เพื่อศึกษาถึงปัญหาในการดำเนินคดีอาญาในส่วนของการควบคุม การค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ตามกฎหมายไทยเปรียบเทียบกฎหมายต่างประเทศ

2.5 เพื่อศึกษาแนวทางแก้ไข ปรับปรุงและพัฒนาบทบัญญัติกฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ให้มีประสิทธิภาพ

## 3. กรอบแนวคิดการวิจัย

การศึกษาปัญหาของบทบัญญัติกฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทยและกฎหมายต่างประเทศ โดยมีทฤษฎีที่สนับสนุนได้แก่ ทฤษฎีรูปแบบกระบวนการยุติธรรมทางอาญาแบ่งออกเป็น 2 ระบบ คือ ทฤษฎีการควบคุมอาชญากรรม (The Crime Control Model) และทฤษฎีกระบวนนิติธรรม (The Due Process Model) หลักการดำเนินคดีที่เป็นธรรม (Rights to Fair Trial) เป็นหลักการพื้นฐานที่สำคัญ ซึ่งจะนำไปสู่ การดำเนินคดีอาญาที่เป็นธรรม

## 4. สมมติฐานการวิจัย

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และบทบัญญัติกฎหมายวิธีพิจารณาความอาญาที่ประเทศไทยนำมาใช้บังคับกับการดำเนินคดีกับผู้ที่กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ไม่สามารถครอบคลุมไปถึงการดำเนินคดีอาญากับผู้กระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ได้เท่าที่ควร ในสภาพ

สังคมของประเทศไทยในปัจจุบันที่เทคโนโลยีมีความก้าวหน้าประกอบกับการก่ออาชญากรรมทางคอมพิวเตอร์ที่มีความสลับซับซ้อนยากต่อการแสวงหาข้อเท็จจริงและพยานหลักฐาน ในการนำตัวผู้กระทำความผิดมาลงโทษ จึงควรแก้ไขปรับปรุงบทบัญญัติกฎหมายในส่วนที่เกี่ยวข้องกับความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ โดยศึกษาแนวคิด ทฤษฎี และหลักเกณฑ์ของกฎหมายไทยและกฎหมายต่างประเทศ เพื่อนำมาเป็นแนวทางในการปรับแก้ให้กฎหมายที่เกี่ยวข้องกับการดำเนินคดีกับผู้ที่กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

## 5. ขอบเขตของการวิจัย

การศึกษาถึงรูปแบบการกระทำความผิดที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด แนวคิด ทฤษฎีของการรวมรวมและการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ตามกฎหมายไทย และปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และบทบัญญัติกฎหมายวิธีพิจารณาความอาญา พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ที่ประเทศไทยนำมาใช้ในการดำเนินคดีกับผู้ที่กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ โดยศึกษาเปรียบเทียบกับหลักเกณฑ์แนวทางของกฎหมายต่างประเทศ

## 6. นิยามศัพท์เฉพาะ

**6.1 อาชญากรรมทางคอมพิวเตอร์** หมายความว่า การกระทำผิดทางอาญาในระบบคอมพิวเตอร์ หรือการใช้คอมพิวเตอร์ โทรศัพท์ หรืออุปกรณ์อิเล็กทรอนิกส์อื่นๆผ่านทางเครือข่ายอินเตอร์เน็ตเพื่อกระทำผิดทางอาญา

**6.2 ข้อมูลคอมพิวเตอร์** หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ โทรศัพท์ หรืออุปกรณ์อิเล็กทรอนิกส์อื่นๆ ในสภาพที่อาจประมวลผลได้

**6.3 พยานหลักฐานอิเล็กทรอนิกส์** หมายความว่า ข้อมูลคอมพิวเตอร์ที่นำมาเป็นหลักฐานในการพิสูจน์ข้อเท็จจริงในการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

**6.4 พนักงานเจ้าหน้าที่** หมายความว่า พนักงานเจ้าหน้าที่ ซึ่งได้รับการแต่งตั้งให้มีอำนาจตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

**6.5 เจ้าพนักงาน** หมายความว่า เจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญา

## 7. ประโยชน์ที่คาดว่าจะได้รับ

7.1 เพื่อให้ทราบถึงรูปแบบการกระทำความผิดที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด

7.2 เพื่อทำให้ทราบถึงการควบคุม การค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ตามกฎหมายไทยและกฎหมายต่างประเทศ

7.3 เพื่อให้ทราบถึงบทบัญญัติกฎหมายที่เกี่ยวข้องการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทยและกฎหมายต่างประเทศ

7.4 เพื่อให้ทราบถึงปัญหาในการดำเนินคดีอาญาในส่วนของการควบคุม การค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ตามกฎหมายไทยเปรียบเทียบกฎหมายต่างประเทศ

7.5 เพื่อให้ทราบถึงแนวทางแก้ไข ปรับปรุงและพัฒนาบทบัญญัติกฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ให้มีประสิทธิภาพ

# บทที่ 2
# แนวคิด ทฤษฎีเกี่ยวกับการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

ปัจจุบันในประเทศไทยมีการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์อย่างแพร่หลายที่เกิดเป็นคดีสำคัญและสร้างความเสียหายต่อประเทศที่รุนแรงมากขึ้นตามการพัฒนาของระบบเทคโนโลยีที่มีความก้าวหน้า ก่อให้เกิดรูปแบบอาชญากรรมทางคอมพิวเตอร์ในรูปแบบต่างๆขึ้นมากมาย ซึ่งในการดำเนินคดีนำตัวผู้กระทำความผิดมาลงโทษนั้นกระทำได้โดยยาก เนื่องจากการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์แตกต่างจากการกระทำความผิดทางอาญาทั่วไป ผู้กระทำความผิดมีเพียงอุปกรณ์อิเล็กทรอนิกส์ที่สามารถเชื่อมต่อเครือข่ายอินเตอร์เน็ตก็สามารถกระทำความผิดได้ไม่ว่าจะอยู่ที่ใดบนโลก การปราบปรามหรือป้องกันการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์จึงมีข้อจำกัดในด้านการแสวงหาพยานหลักฐานในการนำตัวผู้กระทำความผิดมาลงโทษ

ดังนั้น จึงจำเป็นที่จะต้องศึกษาแนวคิด ทฤษฎีเกี่ยวกับการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ความหมาย รูปแบบของการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ และทฤษฎีที่เกี่ยวกับการให้อำนาจรัฐในการดำเนินคดีอาญา เพื่อให้เกิดความเข้าใจและหาแนวทางในการแก้ไขพัฒนาให้การดำเนินคดีความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มีประสิทธิภาพต่อไป

## 1. แนวคิดการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

อาชญากรรมทางคอมพิวเตอร์ ถือว่าเป็นอาชญากรรมรูปแบบหนึ่งที่สร้างผลกระทบแก่ผู้ที่ได้รับความเสียหายอย่างร้ายแรง ไม่ว่าจะความเสียหายทางด้านข้อมูลส่วนบุคคล ด้านเศรษฐกิจและด้านวัฒนธรรม ในการนำข้อมูลส่วนบุคคลมาเผยแพร่ให้เกิดความเสียหาย หรือการเข้าถึงข้อมูลของผู้อื่น ซึ่งอาชญากรรมทางคอมพิวเตอร์สามารถเป็นต้นทางที่ทำให้เกิดการก่ออาชญากรรมทางด้านอื่น ๆ ขึ้นมา เนื่องจากการเข้าถึงข้อมูลได้ง่าย และการดำเนินคดีกับผู้ที่กระทำความผิดที่กระทำได้ยาก

**1.1 ความหมายของอาชญากรรมทางคอมพิวเตอร์**

นิยาม อาชญากรรมทางคอมพิวเตอร์ ในความหมายอย่างกว้าง หมายถึง การกระทำที่ผิดกฎหมายใด ๆ ซึ่งอาศัยหรือมีความเกี่ยวเนื่องกับระบบหรือเครือข่ายทางคอมพิวเตอร์ โดยการใช้ระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ให้ได้รับความเสียหายโดยตรงคือ การกระทำความผิดโดยการสร้างความเสียหายต่อระบบหรือข้อมูลคอมพิวเตอร์ เช่นการเข้าสู้ระบบคอมพิวเตอร์เพื่อทำลาย แก้ไข หรือเปลี่ยนแปลงข้อมูล และได้รับความเสียหายโดยอ้อมคือ การใช้ระบบคอมพิวเตอร์เป็นช่องทางในการกระทำความผิดอื่น เช่น การติดต่อซื้อขายสิ่งผิดกฎหมายทางอินเทอร์เน็ต[1]

สำนักงานตำรวจแห่งชาติ ได้กำหนดนิยาม อาชญากรรมทางคอมพิวเตอร์ หมายถึง การกระทำใดๆ ก็ตามที่เกี่ยวกับการใช้คอมพิวเตอร์อันทำให้บุคคลอื่นได้รับความเสียหายและผู้กระทำได้รับผลประโยชน์ตอบแทน และการทำผิดกฎหมายซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือ และการสืบสวนของเจ้าหน้าที่ จำเป็นต้องใช้ความรู้ทางด้านเทคโนโลยีคอมพิวเตอร์ในการนำผู้กระทำความผิดมาดำเนินคดี

สำนักงานตำรวจแห่งชาติได้แบ่งส่วนราชการ โดยได้จัดตั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อยป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวน ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์[2]

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้กำหนดนิยามอาชญากรรมทางคอมพิวเตอร์ไว้เป็นการเฉพาะ แต่ได้อธิบายลักษณะของอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ 2 ลักษณะ ได้แก่[3]

1. อาชญากรรมที่กระทำต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ โดยการเข้าไปแทรกแซง ทำลาย ทำให้เปลี่ยนแปลง ทำให้เสียหายในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

---

[1] ญาณพล ยั่งยืน, อาชญากรรมทางคอมพิวเตอร์, ศูนย์ข้อมูลสารสนเทศ สำนักงานตำรวจแห่งชาติ, หน้า 4

[2] กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี.ประวัติหน่วยงาน. สืบค้นเมื่อวันที่ 22 เมษายน 2564. จากเว็บไซต์: (https:// https://tcsd.go.th/เกี่ยวกับหน่วยงาน/)

[3] สำนักงานศาลยุติธรรม, คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550, พิมพ์ครั้งที่ 1 : โรงพิมพ์ดอกเบี้ย, 2550, หน้า 72

2. การใช้คอมพิวเตอร์เป็นเครื่องมือประกอบอาชญากรรมซึ่งเป็นอาชญากรรมที่มีผลกระทบร้ายแรงและขยายวงกว้างเพราะการแพร่หลายของข้อมูลคอมพิวเตอร์นั้นไม่มีพรมแดน

ดังนั้น จึงสรุปได้ว่า อาชญากรรมทางคอมพิวเตอร์ หมายถึง การกระทำใดๆที่ผิดกฎหมาย โดยการใช้เทคโนโลยีคอมพิวเตอร์เป็นส่วนสำคัญในการกระทำความผิดหรือใช้เป็นช่องทางในการกระทำความผิดตามกฎหมายอื่น และในการสืบสวนสอบสวนของเจ้าหน้าที่เพื่อนำผู้กระทำมาดำเนินคดีต้องใช้ความรู้ทางเทคโนโลยีคอมพิวเตอร์ ซึ่งการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อระบบหรือข้อมูลคอมพิวเตอร์ หรือเป็นเหตุให้ผู้อื่นให้ได้รับความเสียหายจากการกระทำดังกล่าว

**1.2 รูปแบบของการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์**

เมื่อเทคโนโลยีเข้ามามีบทบาทสำคัญในชีวิตของมนุษย์ เป็นเหตุให้อาชญากรใช้เป็นช่องทางในการกระทำความผิด ก่ออาชญากรรมโดยใช้ระบบคอมพิวเตอร์ โทรศัพท์ และอุปกรณ์อิเล็กทรอนิกส์อื่นๆ ผ่านทางเครือข่ายอินเตอร์เน็ต โดยอาชญากรรมทางคอมพิวเตอร์ได้เกิดขึ้นอย่างแพร่หลายในปัจจุบัน และสร้างความเสียหายเป็นวงกว้าง ซึ่งรูปแบบของอาชญากรรมทางคอมพิวเตอร์จะแตกต่างไปตามความประสงค์ของอาชญากรว่าต้องการให้เกิดความเสียหายในรูปแบบใด จึงได้มีการแบ่งรูปแบบอาชญากรรมทางคอมพิวเตอร์ ดังนี้[4]

1. การขโมยข้อมูลทางอินเตอร์เน็ต รวมถึงการขโมยประโยชน์ ในการลักลอบใช้บริการ
2. การปกปิดความผิดของตัวเอง โดยใช้ระบบการสื่อสาร
3. การละเมิดลิขสิทธิ์ ปลอมแปลงรูปแบบเลียนแบบระบบ ซอฟแวร์โดยมิชอบ
4. การเผยแพร่ภาพ เสียง ลามก อนาจาร และข้อมูลที่ไม่ เหมาะสม
5. การฟอกเงิน
6. การก่อกวนระบบคอมพิวเตอร์
7. การหลอกลวงให้ร่วมค้าขาย หรือ ลงทุนปลอม
8. การลักลอบใช้ข้อมูลเพื่อแสวงหาผลประโยชน์ในทางมิชอบ
9. การใช้คอมพิวเตอร์ในการโอนบัญชีผู้อื่นเป็นของตัวเอง

อาชญากรรมทางคอมพิวเตอร์ เป็นอาชญากรรมที่แสวงหาผลประโยชน์ส่วนตัวและก่อให้เกิดความเสียหายต่อบุคคล หรือองค์กร ผ่านทางเครือข่ายอินเทอร์เน็ต ซึ่งรูปแบบการ

---

[4] Todsapol Aryuyune,/ อาชญากรรมคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง,/2016,/สืบค้นเมื่อวันที่ 23 เมษายน 2564.จากเว็บไซต์: (https:// www.slideshare.net/TodsapolAryuyune/7-62768502)

กระทำความผิดเปลี่ยนไปตามวิวัฒนาการทางเทคโนโลยี และมีรูปแบบใหม่ๆ เกิดขึ้นอยู่ตลอดเวลา ยกตัวอย่างเช่น

Hacker (แฮกเกอร์) คือ อาชญากรที่มีความรู้ในระบบคอมพิวเตอร์เป็นอย่างดี และต้องมีความเชี่ยวชาญด้านคอมพิวเตอร์และอินเทอร์เน็ตเป็นอย่างมาก สามารถเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยเจาะผ่านระบบรักษาความปลอดภัยของคอมพิวเตอร์เพื่อดูข้อมูลหรือความลับขององค์กรต่างๆ แล้วนำไปก่อให้เกิดความเสียหายแก่ผู้ใช้งานระบบ

Sniffer (สนิฟเฟอร์) คือ โปรแกรมดักเก็บข้อมูลในระบบคอมพิวเตอร์ที่จะคอยดักฟังการสนทนากันในเครือข่าย โดยการแฝงมากับอีเมล การดาวน์โหลดภาพ เพลง หรือการคลิกลิงค์ เพื่อเข้าเว็บไซต์ต่างๆ เมื่อเข้ามาแล้วโปรแกรมสนิฟเฟอร์จะเข้ามาฝังตัวอยู่ในเครื่องเพื่อดักเก็บข้อมูลเครือข่ายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง แต่ไม่สามารถอ่านข้อมูลได้ในทันทีต้องมีการแปลงข้อมูลจากตัวเลขให้เป็นภาษาเขียน ซึ่งผู้กระทำความผิดมักจะใช้เพื่อดักเก็บข้อมูลสำคัญ เช่น รหัสผ่าน หรือเลขบัญชีธนาคาร

Spam Mail (สแปมเมล) หรือ Junk Mail (อีเมลขยะ) คือ การส่งอีเมลมาจากบุคคลที่ไม่รู้จักและส่งไปหาบุคคลอื่นเป็นจำนวนมาก ภายในอีเมลจะมีเนื้อหาที่สร้างความดึงดูดและกระตุ้นให้ผู้ที่ได้รับเปิดอีเมล์ เช่นการแจ้งข่าวว่าถูกรางวัล การขอความช่วยเหลือ ข้อความชักชวนให้เข้าเว็บไซต์ลามก ซึ่งผู้กระทำจะใช้เป็นช่องทางในการส่งไวรัสหรือสนิฟเฟอร์ แนบมากับอีเมล หากผู้ได้รับเปิดอ่านอีเมล์หรือลิงค์ที่แนบมากับอีเมล์จะทำให้ไวรัสหรือสนิฟเฟอร์เข้าไปฝังตัวภายในคอมพิวเตอร์อย่างรวดเร็ว ซึ่งอาจเป็นเหตุให้คอมพิวเตอร์ทำงานขัดข้อง หรือถูกขโมยข้อมูลที่สำคัญออกไปจากอีเมล์ และในกรณีที่ผู้ได้รับอีเมล์หลงเชื่อข้อความหลอกลวงโอนเงินให้แก่ผู้กระทำความผิดหรือส่งต่อข้อความให้แก่ผู้อื่นเป็นจดหมายลูกโซ่ก่อให้เกิดความเสียหายเป็นจำนวนมาก

Spy ware (สปายแวร์) คือ โปรแกรมที่แฝงเข้ามาในเครื่องคอมพิวเตอร์ โดยจะแอบซ่อนมากับโฆษณาสินค้าเป็นป๊อปอัพที่ขึ้นมาตามเว็บไซต์ต่างๆ ส่วนใหญ่จะเป็นโฆษณาผลิตภัณฑ์หรือภาพลามกอนาจาร ซึ่งจะหลอกล่อให้กดเข้าไปดู และเมื่อโปรแกรมแฝงเข้ามาในเครื่องแล้วจะทำให้คอมพิวเตอร์ทำงานช้าลงกว่าปรกติ เนื่องจากสปายแวร์จะเปิดใช้โปรแกรมบางอย่างโดยที่ผู้ใช้ไม่รู้ตัว จึงทำให้การรับส่งข้อมูลผ่านอินเตอร์เน็ตช้าและการเชื่อมต่อของอินเตอร์เน็ตไม่เสถียร และยังทำให้ข้อมูลส่วนบุคคลของผู้ใช้งานถูกนำออกไปโดยที่ไม่รู้ตัว

Phishing Mail หรือ Fishing แปลว่าการตกปลา หมายถึงการกระทำของอาชญากรที่เหมือนการนำเหยื่อมาล่อให้ปลามาติดกับ โดยอาชญากรจะใช้วิธีการปลอมแปลงอีเมลเพื่อหลอกให้หลงเข้าไปยังเว็บไซต์ปลอมที่สร้างขึ้นผ่านลิงค์ที่มากับอีเมล์นั้น ซึ่งอาจทำทีว่าข้อมูลเกี่ยวกับระบบ

คอมพิวเตอร์กำลังมีปัญหา จึงต้องรวบรวมข้อมูลที่เสียหายไป โดยให้กรอกข้อมูลในเว็บไซต์ที่แนบมากับอีเมล ภายในเว็บไซต์จะสอบถามข้อมูลเกี่ยวกับการเงินหรือข้อมูลหมายเลขบัตรเครดิต เพื่อจะนำไปปลอมแปลงหรือแอบอ้างในการทำธุรกรรมทางการเงินและโจรกรรมทรัพย์สิน ส่วนมากนั้นจะแอบอ้างว่าเป็นอีเมลของธนาคาร หากลูกค้าของธนาคารหลงเชื่อและกรอกข้อมูลจะเกิดความเสียหายแก่ลูกค้าและธนาคารเป็นอย่างมาก

Botnet (บอทเน็ต) หรือ Robot Network คือ เครื่องมือที่อาชญากรใช้ในการก่ออาชญากรรมทางคอมพิวเตอร์ โดยอาชญากรจะส่งสิ่งที่เปรียบเสมือนปืนกลเข้าไปฝังในเครื่องคอมพิวเตอร์จำนวนมากโดยเจ้าของไม่รู้ตัว หลังจากนั้นจะสั่งให้คอมพิวเตอร์ยิงโจมตีเป้าหมายพร้อมๆ กันจากคอมพิวเตอร์หลายๆ เครื่อง โดยการควบคุมของอาชญากรเพียงคนเดียว แต่เป็นอาชญากรรมที่สร้างความเสียหายอย่างร้ายแรง สามารถทำลายระบบการทำงานของทั้งองค์กรหยุดชะงักพร้อมๆ กันได้ และได้ข้อมูลสำคัญขององค์กรนั้น ส่วนมากบอทเน็ตจะใช้ในการหาผลประโยชน์ของอาชญากรในการต่อรองกับองค์กรเพื่อสั่งไม่ให้ทำลายระบบ [5]

จากการศึกษารูปแบบอาชญากรรมทางคอมพิวเตอร์จะเห็นได้ว่ารูปแบบของอาชญากรรมทางคอมพิวเตอร์จะแตกต่างไปตามความประสงค์ของอาชญากรว่าต้องการให้เกิดความเสียหายรูปแบบใด ซึ่งรูปแบบการกระทำความผิดเปลี่ยนไปตามวิวัฒนาการทางเทคโนโลยี และมีรูปแบบใหม่ๆ ที่มีความสลับซับซ้อนมากขึ้น ผู้กระทำความผิดมักเป็นบุคคลที่มีความรู้ในด้านเทคโนโลยีเป็นอย่างดี และไม่สามารถหาตัวตนที่อยู่แน่นอนได้ หากบุคคลเหล่านั้นไม่ได้อยู่ในราชอาณาจักรไทย จะทำให้ลำบากในการเข้าถึงตัวผู้กระทำความผิด ซึ่งต้องใช้กระบวนการในการสืบค้นตัว จึงต้องสืบค้นจากพยานหลักฐานอิเล็กทรอนิกส์ เพื่อให้เข้าถึงตัวผู้กระทำความผิด และนำตัวผู้กระทำความผิดมาลงโทษ

**1.3 พยานหลักฐานอิเล็กทรอนิกส์**

พยานหลักฐานอิเล็กทรอนิกส์ถือเป็นสิ่งสำคัญที่จะนำไปสู่การนำตัวผู้กระทำความผิดทางอาชญากรรมทางคอมพิวเตอร์มาลงโทษ เนื่องจากเป็นพยานหลักฐานที่สำคัญในการที่จะเข้าถึงตัวผู้กระทำความผิดมากที่สุด เพื่อให้การดำเนินคดีกับผู้ที่กระทำความผิดอาชญากรรมทางคอมพิวเตอร์มีประสิทธิภาพ พนักงานสอบสวนต้องมีความเข้าใจและเชี่ยวชาญในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์

---

[5] คลิ๊กผิดถึงติดคุก, กรุงเทพมหานคร, พิมพ์ครั้งที่ 1 : ซีเอส ล๊อกซอินโฟ, 2551 หน้า 24-55

***1.3.1 พยาน*** หมายถึง หลักฐานเครื่องพิสูจน์ข้อเท็จจริง ผู้ที่รู้เห็นเหตุการณ์หรือข้อเท็จจริงที่ใช้เป็นหลักฐานเครื่องพิสูจน์ได้ บุคคลซึ่งให้การในเรื่องหรือสิ่งที่ตนได้เห็นได้ยิน หรือได้รับรู้มาโดยวิธีอื่น[6]

***1.3.2 พยานหลักฐาน*** ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 หมายถึง พยานวัตถุ พยานเอกสาร หรือพยานบุคคล ตลอดจนหลักฐานต่างๆ ซึ่งอาจจะเป็นเครื่องพิสูจน์การกระทำผิดได้[7] จึงหมายถึงสิ่งสามารถพิสูจน์ข้อเท็จจริงที่กล่าวอ้างขึ้นในการดำเนินคดี คู่ความจะกล่าวอ้างข้อเท็จจริงของตนเพื่อสนับสนุนหรือแก้ข้อกล่าวหาของตน คู่ความจะต้องหาทางพิสูจน์ข้อกล่าวอ้างของตนให้ศาลเชื่อ โดยการนำพยานหลักฐานมายืนยันข้อเท็จจริง ซึ่งๆ พยานหลักฐานอาจเป็นบุคคลผู้เห็นเหตุการณ์ หรือเอกสาร วัตถุต่าง พยานหลักฐานในคดีอาญาถือเป็นสิ่งที่สำคัญมาก เนื่องจากเป็นเครื่องมือในการพิสูจน์การกระทำความผิด

***1.3.3 ข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์*** ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 ได้กำหนดนิยาม ข้อมูลอิเล็กทรอนิกส์ หมายถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายทางอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร[8] ส่วนในพระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2550 มาตรา 3 ได้กำหนดนิยาม ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย[9] ความหมายของคำว่า ข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์ จึงมีความหมายกว้างขวางครอบคลุมไปถึงข้อมูลทุกชนิดที่ทำขึ้นด้วยวิธีการทางอิเล็กทรอนิกส์ ไม่ใช่แค่ข้อความตัวอักษรหรือตัวเลขแต่รวมไปถึงเสียง

ความหมายของคำว่าพยานหลักฐานอิเล็กทรอนิกส์ จึงหมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ได้ ซึ่งข้อมูลดังกล่าวสามารถพิสูจน์ข้อเท็จจริงที่กล่าวอ้างขึ้นหรือสามารถพิสูจน์การกระทำความผิดได้

---

[6] พจนานุกรไทย.com,/คำหมวดหมู่อักษร พ ความหมายของคำว่า ‘พยาน’,/2014,/สืบค้นเมื่อวันที่ 30 เมษายน 2564.จากเว็บไซต์: (https://พจนานุกรมไทย.com/30-192-ความหมาย-พยาน.html)

[7] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226

[8] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4

[9] พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2550 มาตรา 3

ในปัจจุบันข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์มีการนำมาใช้ในการจัดเก็บข้อมูลกันอย่างแพร่หลาย ไม่ว่าจะเป็นข้อมูลในการติดต่อสื่อสารระหว่างบุคคล หรือการทำธุรกรรมผ่านทางอิเล็กทรอนิกส์ ในการซื้อขายสินค้าและบริการ การชำระเงิน และธุรกรรมด้านการเงินต่างๆ ข้อมูลดังกล่าวจึงมีความเสี่ยงที่จะตกเป็นเป้าหมายของการกระทำความผิดหรือถูกใช้เป็นเครื่องมือในการกระทำความผิดหรือเป็นอุปกรณ์ในการจัดเก็บข้อมูลที่เกี่ยวข้องกับการกระทำความผิด ข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์จึงถือได้ว่าเป็นพยานหลักฐานที่มีความสำคัญในการพิสูจน์ความผิดในคดีอาญาไม่น้อยไปกว่าพยานหลักฐานต่างๆ แต่ลักษณะของพยานหลักฐานอิเล็กทรอนิกส์สามารถถูกเปลี่ยนแปลงได้ง่าย การรวบรวมพยานหลักฐานและการจัดเก็บพยานหลักฐานจึงต้องเป็นไปด้วยความระมัดระวัง เพื่อไม่ให้เกิดข้อโต้แย้งในการอ้างอิงและการรับฟังพยานหลักฐานในชั้นศาล

พยานหลักฐานอิเล็กทรอนิกส์อาจจัดเป็นพยานเอกสารหรือพยานวัตถุตามวัตถุประสงค์ในการใช้อ้างในคดี หากมีวัตถุประสงค์หากมีวัตถุประสงค์ยืนยันความถูกต้องแท้จริงของเนื้อความด้วยการนำข้อมูลอิเล็กทรอนิกส์ที่บันทึกไว้ในระบบคอมพิวเตอร์ประมวลผลผ่านชุดคำสั่งและอุปกรณ์ต่างๆ โดยนำออกมาในรูปของสิ่งพิมพ์เอกสาร และมีเนื้อหาตรงกันกับที่แสดงอยู่สิ่งพิมพ์นั้นจัดเป็นพยานเอกสาร แต่หากการใช้อ้างข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์เพื่อมุ่งยืนยันความมีอยู่ของข้อมูลอิเล็กทรอนิกส์ด้วยการนำระบบคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ที่บันทึกข้อมูลไว้มานำสืบด้วยการแสดงออกในรูปแบบที่เข้าใจได้ และทำให้เห็นว่าเป็นข้อมูลที่ระบบคอมพิวเตอร์แสดงออกมาเป็นข้อมูลถูกต้องแท้จริง ไม่มีการแก้ไข หรือทำลายให้เกิดความเสียหาย ก็จะจัดเป็นพยานวัตถุ

การรวบรวมพยานหลักฐานเล็กทรอนิกส์ กฎหมายประเทศไทยนั้นพนักงานสอบสวนมีอำนาจรวบรวมพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 เป็นบทกฎหมายทั่วไปแต่บทกฎหมายดังกล่าวมิได้บัญญัติเกี่ยวกับการรวบรวมพยานหลักฐานเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์ไว้โดยตรง ในคดีอาญาบางประเภทความผิดมีกฎหมายบัญญัติเอาไว้โดยเฉพาะเจาะจงในเรื่องของอำนาจของพนักงานสอบสวนหรือเจ้าพนักงานผู้มีอำนาจรวบรวมพยานหลักฐานและจัดเก็บพยานหลักฐาน พนักงานสอบสวนหรือเจ้าพนักงานเหล่านั้นจะต้องปฏิบัติให้เป็นไปตามบทบัญญัติกฎหมายเฉพาะที่กำหนดอำนาจไว้ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 เป็นต้น แต่การรวบรวมพยานหลักฐานเล็กทรอนิกส์ อาจมีปัญหาและอุปสรรคเนื่องจากอาชญากรรมทางคอมพิวเตอร์นั้น

ยากต่อการตรวจพิสูจน์การกระทำความผิดและการกระทำความผิดเป็นไปอย่างรวดเร็วสร้างความเสียหายเป็นวงกว้าง การสืบสวนสอบสวนจึงต้องกระทำโดยพนักงานสอบสวนหรือบุคคลที่ต้องมีความเชี่ยวชาญ และปัญหาในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในกรณีที่มีความจำเป็นที่จะต้องออกหมายค้น ตามประมวลกฎหมายวิธีพิจารณาความอาญาของไทยการออกหมายค้นต้องระบุถึงสิ่งที่จะค้น และแหล่งที่อยู่ของสิ่งที่จะค้น ซึ่งข้อมูลคอมพิวเตอร์ในบางกรณีไม่อาจระบุได้ว่าอยู่ในรูปแบบใด และเก็บไว้ที่ใด เป็นสิ่งไม่มีรูปร่าง การที่จะใช้อำนาจในการค้นพนักงานเจ้าหน้าที่จะต้องทำโดยวิธีใด และหากพบการกระทำความผิดอื่นที่ไม่เกี่ยวกับหมายค้นจะสามารถดำเนินการได้หรือไม่ และจะถือว่าการเจอสิ่งผิดกฎหมายนั้นเป็นความผิดซึ่งหน้าตามประมวลกฎหมายอาญาได้หรือไม่ ในกรณีการค้นในที่รโหฐานต้องทำในเวลากลางวัน แต่หากเป็นข้อมูลหรือพยานหลักฐานอิเล็กทรอนิกส์ พนักงานเจ้าหน้าที่จะทำการค้นในกรณีฉุกเฉินได้หรือไม่ จึงเป็นปัญหาที่จะต้องหาแนวทางการแก้ไขพัฒนาต่อไป

การรับฟังพยานหลักฐานอิเล็กทรอนิกส์ ศาลมีอำนาจใช้ดุลพินิจรับฟังและชั่งน้ำหนักพยานหลักฐานอิเล็กทรอนิกส์ตามที่กฎหมายกำหนด ซึ่งในปัจจุบันกฎหมายไทยยังไม่มีบทบัญญัติเกี่ยวกับการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญาเป็นการเฉพาะ การรับฟังพยานหลักฐานอิเล็กทรอนิกส์จึงเป็นไปตามหลักการรับฟังพยานหลักฐานทั่วไป ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจาเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่ไม่ได้เกิดขึ้นจากการจูงใจ มีคามั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน” แต่กรณีที่มีกฎหมายเฉพาะอื่นที่ได้บัญญัติหลักเกณฑ์และวิธีการในการได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ไว้ การรวบรวมพยานหลักฐานนั้นจะต้องปฏิบัติให้ถูกต้องตามหลักเกณฑ์และวิธีการดังกล่าวนอกเหนือไปจากหลักเกณฑ์ทั่วไปตามประมวลกฎหมายวิธีพิจารณาความอาญาด้วย ไม่เช่นนั้นย่อมถือว่าเป็นการได้พยานหลักฐานอิเล็กทรอนิกส์มาโดยมิชอบ ศาลมีอำนาจไม่รับฟังได้ เนื่องจากพยานหลักฐานอิเล็กทรอนิกส์ มีความเสี่ยงที่จะถูกแก้ไขเปลี่ยนแปลง และสูญหาย อย่างง่ายดาย โดยเฉพาะข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ที่มีการส่งผ่านทางระบบคอมพิวเตอร์หลายทอด พยานหลักฐานอิเล็กทรอนิกส์ที่ศาลจะรับฟังจึงต้องเป็นพยานหลักฐานที่เนื้อหาไม่มีการเปลี่ยนแปลง ข้อมูลเป็นไปตามเจตนารมณ์ที่แท้จริงของผู้สร้างข้อมูล ไม่ว่าผู้สร้างข้อมูลจะเป็นมนุษย์หรือคอมพิวเตอร์[10]

---

[10] สมคิด สายเจริญ ,พยานหลักฐานดิจิทัลในคดีอาญา Digital Evidence in Criminal Cases , สำนักงานอัยการสูงสุด,หน้า 8

## 2. ทฤษฎีเกี่ยวกับการให้อำนาจเจ้าหน้าที่รัฐในการดำเนินคดีอาญา

การดำเนินคดีอาญาเป็นกระบวนการบังคับใช้กฎหมายอาญาโดยมีพนักงานสอบสวน พนักงานอัยการ ทนายความ ศาล และราชทัณฑ์ ปฏิบัติหน้าที่เชื่อมโยงกันเพื่อให้เกิดความสมดุลทางกฎหมายและความยุติธรรมในทางอาญา การดำเนินคดีอาญามีวัตถุประสงค์เพื่อค้นหาความจริงเพื่อชี้ขาดตัดสินคดีให้ผู้กระทำความผิดได้รับโทษเป็นไปตามกระบวนการยุติธรรมทางอาญา ซึ่งปัจจุบันประเทศไทยมีการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์อย่างแพร่หลายที่เกิดเป็นคดีสำคัญและสร้างความเสียหายต่อประเทศที่รุนแรงมากขึ้น ตามการพัฒนาของระบบเทคโนโลยีที่มีความก้าวหน้า ก่อให้เกิดรูปแบบอาชญากรรมทางคอมพิวเตอร์ในรูปแบบต่างๆขึ้นมากมาย ซึ่งการดำเนินคดีนำตัวผู้กระทำความผิดมาลงโทษนั้น กระทำได้โดยยาก เนื่องจากการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์แตกต่างจากการกระทำความผิดทางอาญาทั่วไป ผู้กระทำความผิดมีเพียงอุปกรณ์อิเล็กทรอนิกส์ที่สามารถเชื่อมต่อเครือข่ายอินเตอร์เน็ตก็สามารถกระทำความผิดได้ไม่ว่าจะอยู่ที่ใดบนโลก การปราบปรามหรือป้องกันการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์จึงมีข้อจำกัดในด้านการแสวงหาพยานหลักฐานเพื่อหาตัวผู้กระทำความผิดมาลงโทษ ในอดีตประเทศไทยยังขาดกฎหมายที่ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ทำให้การทำงานของเจ้าหน้าที่ในการรวบรวมพยานหลักฐานหรือดำเนินคดีกับผู้ที่กระทำความผิดไม่อาจกระทำได้อย่างมีประสิทธิภาพ เพราะการดำเนินการของเจ้าหน้าที่ของรัฐต้องอยู่ภายใต้หลักการของนิติรัฐและหลักการดำเนินคดีที่เป็นธรรม

หลักการดำเนินคดีที่เป็นธรรม (Rights to Fair Trial) เป็นหลักการพื้นฐานของความยุติธรรมและสันติภาพ เป็นเครื่องมือสำคัญของรัฐในการดำรงรักษาไว้ซึ่งความสงบเรียบร้อยของสังคมเป็นเครื่องมือที่จะป้องกันการใช้อำนาจตามอำเภอใจและเป็นหลักประกันว่าประชาชนจะได้รับการปฏิบัติด้วยกระบวนการทางกฎหมายที่แน่นอน คาดหมายได้และเป็นธรรมซึ่งเป็นหลักการพื้นฐานของหลักการปกครองโดยกฎหมาย[11]

หลักนิติรัฐมีหลักการสำคัญในการจำกัดอำนาจของรัฐโดยกฎหมาย การทำให้รัฐต้องผูกพันอยู่กับหลักการพื้นฐานและคุณค่าทางกฎหมาย รัฐต้องดำเนินการในด้านต่างๆเพื่อให้เกิดความเป็นธรรมขึ้นอย่างแท้จริงในสังคม โดยกำหนดให้องค์กรของรัฐทุกองค์กรต้องผูกพันกับ

---

[11] วรเจตน์ ภาคีรัตน์.(2557).เอกสารประกอบการบรรยายเรื่องหลักนิติรัฐ.พิมพ์ครั้งที่ 2. กรุงเทพมหานคร:โครงการตำราและเอกสารประกอบการสอนคณะนิติศาสตร์,2557,หน้า 6

หลักการประกันสิทธิขั้นพื้นฐาน ทั้งกับกฎหมายและความยุติธรรมเจ้าหน้าที่ของรัฐจะกระทำการใดอันเป็นการกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนจะต้องมีกฎหมายให้อำนาจหน้าที่แก่เจ้าหน้าที่รัฐ หากไม่มีกฎหมายให้อำนาจเจ้าหน้าที่รัฐจะกระทำการใดอันเป็นการกระทบต่อสิทธิเสรีภาพของประชาชนไม่ได้[12]

เมื่อไม่มีกฎหมายใดกำหนดให้อำนาจหน้าที่แก่เจ้าหน้าที่ในการรวบรวมพยานหลักฐานหรือดำเนินคดีกับผู้ที่กระทำความผิดอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์จึงต้องนำกฎหมายวิธีพิจารณาความอาญามาบังคับใช้ โดยพนักงานสอบสวนต้องใช้อำนาจตามมาตรา 132 ประมวลกฎหมายวิธีพิจารณาความอาญาในการออกหมายเรียกเอกสารหรือพยานบุคคลที่เกี่ยวข้องเพื่อให้ข้อมูลทางโทรคมนาคมหรือข้อมูลทางอินเตอร์เน็ต

การตรากฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นการกำหนดความผิดเกี่ยวกับคอมพิวเตอร์ไว้เป็นการเฉพาะและให้อำนาจแก่พนักงานเจ้าหน้าที่เป็นการเฉพาะในการการรวบรวมพยานหลักฐานหรือดำเนินคดีกับผู้ที่กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ซึ่งการควบคุม การค้น การยึดพยานหลักฐานที่เกิดจากการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์เป็นหนึ่งในการดำเนินคดีอาญาที่สำคัญเพื่อที่จะนำมาเป็นพยานหลักฐานเสนอต่อศาลในการรับฟังเพื่อการพิจารณาตัดสินลงโทษผู้กระทำความผิด การรับฟังพยานหลักฐานเป็นขั้นตอนในการกลั่นกรองหรือคัดเลือกพยานหลักฐาน โดยมีทฤษฎีที่สนับสนุนได้แก่ ทฤษฎีรูปแบบกระบวนการยุติธรรมทางอาญาแบ่งออกเป็น 2 ระบบ ได้แก่

**2.1 ทฤษฎีการควบคุมอาชญากรรม (The Crime Model)**

ทฤษฎีการควบคุมอาชญากรรมมีแนวคิดในเชิงอนุรักษ์นิยม ซึ่งทฤษฎีนี้มีหลักการที่สำคัญคือ อำนาจรัฐเป็นใหญ่เหนือเสรีภาพของบุคคล โดยให้อำนาจเจ้าหน้าที่ของรัฐในการป้องกันและปราบปรามอาชญากรรมอย่างเต็มที่แม้อาจจะมีการก้าวล่วงสิทธิเสรีภาพปัจเจกบุคคล แต่เพื่อให้บรรลุเป้าหมายในการควบคุมอาชญากรรม และสร้างความสงบเรียบร้อยในสังคม กฎหมายและแนวนโยบายของรัฐก็ให้เจ้าหน้าที่ของรัฐกระทำได้ การควบคุมปราบปรามอาชญากรรมเป็นหน้าที่อันสำคัญที่สุดของกระบวนการยุติธรรมทางอาญา การที่จะรักษาความสงบสุขของสังคมจะต้องมีการควบคุมอาชญากรรมอย่างเข้มข้น กระบวนการดำเนินคดีต้องรวดเร็ว คดีอาญาที่เข้าสู่ระบบความยุติธรรมตามทฤษฎีนี้จะดำเนินตามขั้นตอนต่างๆที่กำหนดไว้อย่างสม่ำเสมอ ไม่ว่าจะเป็นการสืบสวนก่อนทำการจับกุม การสืบสวนภายหลังการจับกุม การเตรียมคดีเพื่อฟ้องยังศาล การพิจารณาคดี การพิพากษาลงโทษผู้กระทำความผิด และการปล่อยตัวจำเลย

---

[12] เรื่องเดียวกัน.

ขั้นตอนต่างๆจะดำเนินไปอย่างต่อเนื่อง ส่วนการกลั่นกรองคดีจะดำเนินการตามขั้นตอนต่างๆ ตามลำดับ การวินิจฉัยคดีให้เสร็จสิ้นไปตั้งแต่ขั้นตอนต้นๆของกระบวนการถือว่าเป็นวิธีการที่มีประสิทธิภาพมากที่สุด ทำให้ผู้ต้องหาที่เป็นผู้บริสุทธิ์จะถูกกลั่นกรองออกไป ผู้ที่กระทำความผิดก็จะถูกดำเนินคดีอย่างรวดเร็ว โดยทฤษฎีนี้เชื่อว่าตำรวจและพนักงานอัยการสามารถวินิจฉัยความถูกผิดของขั้นตอนได้ ซึ่งความมุ่งหมายของทฤษฎีนี้คือขั้นตอนในกระบวนการยุติธรรมจะต้องรวบรัดและมีประสิทธิภาพ และการค้นหาข้อเท็จจริงในชั้นตำรวจและพนักงานอัยการต้องเพียงพอเชื่อถือได้[13]

**2.2 ทฤษฎีกระบวนการนิติธรรม (The Due Process Model)**

ทฤษฎีนี้มีหลักการมุ่งคำนึงถึงสิทธิของผู้ต้องหาและคุ้มครองสิทธิเสรีภาพของบุคคลเป็นสำคัญสันนิษฐานไว้ก่อนว่า ผู้ถูกกล่าวหาเป็นผู้บริสุทธิ์ อำนาจของเจ้าพนักงานจะต้องถูกจำกัดเพื่อป้องกันมิให้มีการใช้อำนาจโดยมิชอบกระทบต่อสิทธิเสรีภาพของประชาชน จึงต้องมีกฎหมายจำกัดอำนาจของเจ้าพนักงานในการปฏิบัติหน้าที่เกี่ยวกับมาตรการบังคับ เช่น การจับ การค้น ซึ่งหากฝ่าฝืนก็มีการกำหนดโทษ เจ้าพนักงานจะต้องปฏิบัติตามกฎหมายโดยเคร่งครัด เพื่อให้เกิดความเป็นธรรมภายใต้หลักกฎหมาย อำนาจของเจ้าพนักงานและกระบวนการของรัฐจะต้องถูกควบคุมโดยการจำกัดอำนาจของรัฐ เนื่องจากทฤษฎีนี้ไม่เชื่อว่าการควบคุมอาชญากรรมจะมีประสิทธิภาพอย่างแท้จริง โดยเฉพาะการค้นหาข้อเท็จจริงโดยเจ้าพนักงานตำรวจและพนักงานอัยการอาจมีการสร้างพยานหลักฐานขึ้นใหม่ จึงไม่เห็นด้วยในการแสวงหาพยานหลักฐานอย่างไม่เป็นทางการของทฤษฎีควบคุมอาชญากรรม ทฤษฎีกระบวนนิติธรรมเห็นว่าต้องให้มีการพิจารณาคดีหรือไต่สวนข้อกล่าวหาอย่างเป็นทางการและเปิดเผยทั้งในปัญหาข้อเท็จจริงและข้อกฎหมายในศาลยุติธรรมที่เป็นกลาง[14]

ทฤษฎีควบคุมอาชญากรรมเป็นแนวคิดโบราณในทุกประเทศเป็นแนวคิดที่ส่งผลถึงการรับฟังพยานหลักฐานในคดีอาญาที่เจ้าพนักงานของรัฐสามารถแสวงหาพยานหลักฐานได้อย่างกว้างขวางส่วนทฤษฎีนิติธรรมเป็นทฤษฎีที่ตอบโต้การใช้อำนาจรัฐที่กระทบต่อสิทธิเสรีภาพของบุคคลโดยตรง ซึ่งทฤษฎีนิติธรรมขยายตัวแทรกเข้าไปในกฎหมายทั่วโลก โดยในประเทศที่เจริญแล้วเป็นส่วนใหญ่จะมีแนวคิดทางทฤษฎีนิติธรรมมากกว่าทฤษฎีควบคุมอาชญากรรม

---

[13] ประธาน วัฒนพานิช, ระบบความยุติธรรมทางอาญา : แนวคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม, วารสารนิติศาสตร์, ปีที่ 9, (กันยายน-พฤศจิกายน 2520).หน้า 151

[14] ธีสุทธิ์ พันธ์ฤทธิ์.(2551).การรับฟังพยานหลักฐานคดีอาญา.กรุงเทพมหานคร:วิญญูชน, 2551, หน้า 13-15

จากการศึกษาทฤษฎีรูปแบบกระบวนการยุติธรรมทางอาญา กฎหมายที่เกี่ยวกับดำเนินคดีอาญากับผู้กระทำความผิดทางอาชญากรรมทางคอมพิวเตอร์ของประเทศไทยได้มีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นกฎหมายที่กำหนดความผิดเกี่ยวกับคอมพิวเตอร์ไว้เป็นการเฉพาะและได้กำหนดให้อำนาจของพนักงานเจ้าหน้าที่ในการดำเนินคดีกับผู้ที่กระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ที่ไม่ต้องขออนุญาตศาลเป็นอำนาจในการเข้าถึงข้อมูลทั่วไป แต่อำนาจในการเข้าถึงข้อมูลคอมพิวเตอร์หรือการเจาะระบบคอมพิวเตอร์ ต้องได้รับอนุญาตจากศาลก่อน เป็นการให้อำนาจศาลในการตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่ และมีบทกำหนดโทษกรณีพนักงานเจ้าหน้าที่กระทำการฝ่าฝืนกฎหมายที่กระทบต่อสิทธิเสรีภาพของประชาชน นอกจากนี้ประเทศไทยได้นำกฎหมายวิธีพิจารณาความอาญามาใช้ในการแสวงหาข้อเท็จจริงและพยานหลักฐานในการนำตัวผู้กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มาลงโทษ การจับ การค้น การควบคุม ต้องได้รับอนุญาตจากศาลก่อน ซึ่งเป็นไปตามแนวคิดทฤษฎีกระบวนการนิติธรรมที่คุ้มครองสิทธิเสรีภาพของบุคคลเป็นสำคัญ การจำกัดอำนาจของเจ้าหน้าที่รัฐมิให้ใช้อำนาจโดยมิชอบกระทบต่อสิทธิของประชาชน แต่ก็ทำให้เกิดปัญหาในการดำเนินคดีอาญาการค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ การจำกัดอำนาจของเจ้าหน้าที่รัฐโดยการกำหนดขั้นตอนในการเข้าถึงพยานหลักฐานต้องยื่นคำร้องและขออนุญาตจากศาลก่อน ก่อให้เกิดความล่าช้าในการค้นและการยึดพยานหลักฐานอิเล็กทรอนิกส์ ปัญหาในการขอออกหมายค้นที่พนักงานเจ้าหน้าที่จะต้องปฏิบัติตามที่กฎหมายบัญญัติเพื่อให้ได้พยานหลักฐานทางคอมพิวเตอร์อย่างถูกต้องตามกฎหมาย โดยต้องมีหมายค้นในการออกหมายค้นกฎหมายกำหนดให้ศาลเป็นผู้มีอำนาจในการพิจารณาตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐแต่เพียงผู้เดียว

พยานหลักฐานอิเล็กทรอนิกส์ เป็นข้อมูลที่สามารถทำลายหรือแก้ไขได้โดยง่ายและใช้ระยะเวลาสั้น ผู้กระทำความผิดมักมีความรู้ความเชี่ยวชาญทางคอมพิวเตอร์ เมื่อรู้ถึงการค้นพยานหลักฐานก็จะทำลายหรือแก้ไขได้ทันที การสืบค้นจึงต้องใช้ความรวดเร็ว ในการดำเนินคดีกับผู้กระทำความผิดทางคอมพิวเตอร์ ผู้ศึกษาเห็นว่าการค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ควรให้อำนาจแก่เจ้าหน้าที่รัฐในการดำเนินการแสวงหาพยานหลักฐานในการดำเนินคดีกับผู้กระทำความผิดอย่างเต็มที่ เพื่อให้บรรลุเป้าหมายของการควบคุมและปราบปรามอาชญากรรมตามแนวคิดทฤษฎีการควบคุมอาชญากรรม

# บทที่ 3
# กฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทยและกฎหมายต่างประเทศ

การกระทำความผิดอาชญากรรมทางคอมพิวเตอร์มีความแตกต่างจากการกระทำความผิดรูปแบบทั่วไปที่การดำเนินคดีของเจ้าพนักงานไม่มีความยุ่งยากซับซ้อนพยานหลักฐานสามารถเห็นได้ชัดเจน แต่การกระทำความผิดอาชญากรรมทางคอมพิวเตอร์เป็นการนำเทคโนโลยีเข้ามามีส่วนสำคัญในการกระทำความผิดวิธีการกระทำความผิดมีความยุ่งยากซับซ้อน ผู้กระทำมักมีความรู้ ความเชี่ยวชาญด้านเทคโนโลยีเป็นอย่างดี ในการดำเนินคดีกับผู้ที่กระทำความผิดจึงต้องใช้วิธีการที่แตกต่างจากการกระทำความผิดในรูปแบบทั่วไป เพื่อให้ได้ข้อมูลพยานหลักฐานอิเล็กทรอนิกส์ จึงต้องมีกฎหมายกำหนดให้อำนาจเจ้าพนักงานในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ กฎหมายที่ใช้ในการดำเนินคดีกับผู้ที่กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในเรื่องการควบคุม การค้น การยึด ในประเทศไทยที่สำคัญคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และประมวลกฎหมายวิธีพิจารณาความอาญา

## 1. กฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทย

### 1.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ถือว่าเป็นกฎหมายอาญาเฉพาะเรื่องฉบับหนึ่ง เกิดจากปัญหาการทำงานของเจ้าหน้าที่ในการดำเนินคดีกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือใช้คอมพิวเตอร์กระทำความผิดที่ไม่อาจกระทำได้อย่างมีประสิทธิภาพ ซึ่งเมื่อมีการตรากฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ได้มีการกำหนดความผิดเกี่ยวกับคอมพิวเตอร์ไว้เป็นการเฉพาะและให้อำนาจแก่เจ้าหน้าที่เป็นการเฉพาะ ทำให้การบังคับใช้กฎหมายในการดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์มีประสิทธิภาพ

มากยิ่งขึ้น โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ ดังนี้[15]

***1.1.1 การเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 ได้กำหนดโทษสำหรับผู้ใดที่เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ ยกตัวอย่างการกระทำความผิดรูปแบบนี้ คือ แฮกเกอร์ (Hacker) อาชญากรรมที่เจาะเข้าไปในระบบคอมพิวเตอร์ของคนอื่นเพื่อแอบดูข้อมูล หรือล้วงความลับขององค์กรต่างๆแล้วนำไปก่อความเสียหาย

***1.1.2 การล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นไปเปิดเผยโดยมิชอบ***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 6 ได้กำหนดโทษสำหรับผู้ใดที่ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ ยกตัวอย่างการกระทำความผิดรูปแบบนี้คือ ม้าโทรจัน (Trojan Horse) เป็นโปรแกรมที่ออกแบบให้แฝงเข้าไปสู่ระบบคอมพิวเตอร์ของผู้อื่นเพื่อล้วงเอาความลับของระบบคอมพิวเตอร์และไม่มีการทำสำเนาตัวเองแต่จะใช้การพรางตัวและหลอกล่อ ซึ่งจะแฝงเข้าสู่คอมพิวเตอร์ของผู้ใช้หลายหลายรูปแบบเพื่อดักจับ ติดตามหรือเปิดทางให้แฮกเกอร์เข้าโจมตีระบบ

***1.1.3 การเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 7 ได้กำหนดโทษสำหรับผู้ใดที่เข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ ยกตัวอย่างการกระทำความผิดรูปแบบนี้คือ สนิฟเฟอร์ (Sniffer) เป็นโปรแกรมดักเก็บข้อมูลในระบบคอมพิวเตอร์จะแฝงมากับอีเมล การดาวน์โหลดภาพหรือเพลง สนิฟเฟอร์จะคอยฝังตัวอยู่ในเครื่องเพื่อดักฟังการสนทนากันในเครือข่ายแต่ไม่สามารถอ่านข้อมูลทันที จะต้องมีการแปลงข้อมูลจากตัวเลขให้เป็นภาษาเขียน เป็นเครื่องมือ

---

[15] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ประเภทหนึ่งที่แฮกเกอร์นิยมใช้เพื่อส่งมาดักเก็บข้อมูลสำคัญ เช่น รหัสผ่าน บัญชีธนาคาร จากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์หนึ่ง

***1.1.4 การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่น***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 8 ได้กำหนดโทษสำหรับผู้ใดที่กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

***1.1.5 การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 9 ได้กำหนดโทษสำหรับผู้ใดที่ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ ยกตัวอย่างการกระทำความผิดรูปแบบนี้คือ การทำลาย แก้ไข เปลี่ยนแปลง หรือทำให้ข้อมูลของผู้อื่นเสียหาย เช่น กรณีบุคคลใดไม่พอใจกับการกระทำของอีกฝ่าย จึงต่อต้านด้วยการเข้าไปขัดขวาง ทำร้ายระบบเว็บไซต์ของฝ่ายตรงข้าม ให้บุคคลอื่นๆ ใช้งานไม่ได้

***1.1.6 การทำให้ระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 10 ได้กำหนดโทษสำหรับผู้ใดที่กระทำการโดยมิของเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ ยกตัวอย่างการกระทำความผิดรูปแบบนี้คือ หนอนอินเตอร์เน็ต (Worm) เป็นไวรัสคอมพิวเตอร์ที่สามารถคัดลอกตัวเองและแพร่กระจายจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครือข่ายอื่นๆ โดยผ่านระบบอินเตอร์เน็ตในรูปแบบของอีเมลหรือไฟล์ หากผู้ใช้ได้เปิดโปรแกรมที่ติดเชื้อเหล่านั้นไวรัสดังกล่าวจะแพร่กระจายไปอย่างรวดเร็วและเป็นวงกว้าง

***1.1.7 การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นซึ่งเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 11 ได้กำหนดโทษสำหรับผู้ใดที่ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว ซึ่งเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท ยกตัวอย่างการกระทำความผิดรูปแบบนี้ คือ สแปมเมล (Spam Mail) เป็นอีเมลขยะมาจากบุคคลที่ไม่รู้จักและส่งไปหาบุคคลอื่นเป็นจำนวนมาก ซึ่งภายในอีเมลจะมีเนื้อหาเกี่ยวกับการโฆษณาเพื่อขายสินค้า การแจ้งข่าวสารว่าถูกรางวัล การขอความช่วยเหลือ การชักชวนให้เข้าเว็บไซต์ลามก ซึ่งมีลักษณะเป็นจดหมายลูกโซ่ เมื่อกดอ่านไวรัสจะเข้าไปฝังตัวอยู่ในคอมพิวเตอร์อย่างรวดเร็ว ผลที่ตามมาคือจะถูกขโมยข้อมูลสำคัญออกไปจากอีเมลและถูกหลอกให้เสียเงินหากหลงเชื่อจดหมายลูกโซ่ต่างๆ

***1.1.8 การแต่งตั้งพนักงานเจ้าหน้าที่จากผู้ที่มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 28 กำหนดให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์ โดยได้มีประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดคุณสมบัติของพนักเจ้าหน้าที่ ต้องมีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์ สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์ วิทยาศาสตร์วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์ ผ่านการอบรมทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) สืบสวน สอบสวน และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) และต้องมีคุณสมบัติอื่นอย่างหนึ่งอย่างใด ดังต่อไปนี้ รับราชการหรือเคยรับราชการไม่น้อยกว่าสองปีในตำแหน่งเจ้าหน้าที่ตรวจพิสูจน์พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์หรือพยานหลักฐานอิเล็กทรอนิกส์ หรือสำเร็จการศึกษาทางวิศวกรรมศาสตร์ วิทยาศาสตร์วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์ ในระดับปริญญาตรี และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสี่ปี หรือในระดับปริญญาโท หรือสอบไล่ได้เป็นเนติบัณฑิตตามหลักสูตรของสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสามปี หรือในระดับปริญญาเอก หรือมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงาน ตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสองปี

หรือเป็นบุคคลที่ทำงานเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือมีประสบการณ์ในการดำเนินคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ไม่น้อยกว่าสองปี

กรณีที่มีความจำเป็นเพื่อประโยชน์ของทางราชการในการสืบสวนและสอบสวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จำเป็นต้องมีบุคลากรซึ่งมีความรู้ ความชำนาญหรือประสบการณ์สูงเพื่อดำเนินการสืบสวนและสอบสวนการกระทำผิดหรือคดีเช่นว่านั้น หรือเป็นบุคลากรในสาขาที่ขาดแคลนรัฐมนตรีอาจยกเว้นคุณสมบัติดังกล่าว ไม่ว่าทั้งหมดหรือบางส่วนสำหรับการบรรจุและแต่งตั้งบุคคลใดเป็นการเฉพาะก็ได้[16]

***1.1.9 การประสานงานในเรื่องการจับ ควบคุม ค้น การสืบสวนและสอบสวนระหว่างพนักงานเจ้าหน้าที่กับพนักงานสอบสวนผู้รับผิดชอบ***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 29 ได้บัญญัติให้อำนาจพนักงานเจ้าหน้าที่ให้มีฐานะเป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญาคือ มีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษและมีอำนาจในการสืบสวนสอบสวน แต่เฉพาะความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เท่านั้น

การประสานงานระหว่างพนักงานเจ้าหน้าที่กับเจ้าพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาว่าผู้ใดจะต้องรับผิดชอบในเรื่องใดในขั้นตอนของการสืบสวนและสอบสวน ซึ่งทั้งสองฝ่ายต่างมีอำนาจเช่นกัน เนื่องจากพระราชบัญญัตินี้ไม่ได้ตัดอำนาจหน้าที่ของเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และพระราชบัญญัตินี้มิได้กำหนดรายละเอียดไว้ จึงได้กำหนดให้นายกรัฐมนตรีและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการเพื่อให้เกิดความชัดเจนที่จะประสานการปฏิบัติหรือดำเนินการตามอำนาจหน้าที่ของแต่ละฝ่ายต่อไป

**1.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560**

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ได้มีการแก้ไขเพิ่มเติมกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เนื่องจากได้มีการจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งมีภารกิจในการกำหนดมาตรฐานและ

---

[16] ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

มาตรการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เฝ้าระวังติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ พระราชบัญญัตินี้จึงได้กำหนดให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่เพื่อปฏิบัติการตามพระราชบัญญัตินี้ และได้แก้ไขเพิ่มเติมการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้มีความเหมาะสมยิ่งขึ้นในการดำเนินคดีการควบคุม การค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ดังนี้[17]

***1.2.1 การกำหนดการกระทำความผิดเกี่ยวกับคอมพิวเตอร์***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560มาตรา 14 ได้กำหนดความผิดของผู้ที่กระทำความผิดเกี่ยวกับการนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ ได้แก่

*1) การกระทำโดยทุจริตหรือโดยหลอกลวง* นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา แต่หากเป็นการกระทำที่มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

*2) การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ* โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

*3) การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ* อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

*4) การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ* ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

*5) การเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์* โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)

---

[17] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

การกระทำความผิดดังกล่าวต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ การกำหนดความผิดของผู้ให้บริการที่ให้ความร่วมมือ ยินยอมหรือรู้เห็นเป็นใจให้มีการกระทำความผิดดังกล่าวในระบบคอมพิวเตอร์ที่อยู่ในความดูแลของตนต้องระวางโทษเช่นเดียวกับผู้กระทำความผิด เว้นแต่ผู้ให้บริการจะพิสูจน์ว่าได้ปฏิบัติตามประกาศของรัฐมนตรี ผู้นั้นไม่ต้องรับผิด

***1.2.2 การให้อำนาจพนักงานเจ้าหน้าที่ซึ่งไม่ต้องขออนุญาตศาล***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560มาตรา 18 (1)-(3) ได้กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจในการสืบสวนสอบสวนนอกเหนือจากอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา เพื่อประโยชน์ในการสืบสวนสอบสวนในกรณีที่มีเหตุอันควรเชื่อว่าได้มีการกระทำความผิดตามพระราชบัญญัตินี้หรือในกรณีที่มีการร้องขอจากพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาในบรรดาความผิดอาญาที่ได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือส่วนหนึ่งในการกระทำความผิดตามกฎหมายอื่น ซึ่งสามารถกระทำได้เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิดโดยไม่จำต้องขออนุญาตศาล ดังนี้

*1) มีอำนาจเรื่องทั่วไปในการรวบรวมพยานหลักฐาน*ซึ่งอาจทำโดยวิธีการมีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือหรือส่งเอกสาร ข้อมูลทั่วไปไม่รวมถึงข้อมูลคอมพิวเตอร์

*2) มีอำนาจเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลที่เกี่ยวข้อง*

*3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการหรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่* ผู้ให้บริการมีหน้าที่ต้องเก็บข้อมูลเกี่ยวกับผู้ใช้บริการ เช่น ข้อมูลรหัสประจำตัวผู้ใช้บริการ

การไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ดังกล่าว เป็นความผิดตามมาตรา 27 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ต้องระวางโทษปรับไม่เกินสองแสนบาทและปรับเป็นรายวันไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

***1.2.3 การใช้อำนาจของพนักงานเจ้าหน้าที่ซึ่งต้องขออนุญาตศาล***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มาตรา 18 (4)-(8) กำหนดการใช้อำนาจของพนักงานเจ้าหน้าที่ในการสืบสวนสอบสวน

เพื่อหาพยานหลักฐานการกระทำความผิด ซึ่งมาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ได้กำหนดการใช้อำนาจของพนักงานเจ้าหน้าที่ต้องขออนุญาตศาลตามวิธีการที่กฎหมายบัญญัติไว้ก่อน

*1) การทำสำเนาข้อมูลคอมพิวเตอร์* ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อว่ามีการกระทำความผิดและต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์เกินความจำเป็น ในกรณีที่ระบบคอมพิวเตอร์มิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่ การทำสำเนาข้อมูลคอมพิวเตอร์หรือข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งได้แก่การเจาะระบบเพื่อให้ทราบถึงระบบคอมพิวเตอร์ที่ใช้ในการกระทำความผิดเพื่อให้ได้พยานหลักฐานเกี่ยวกับการกระทำความผิดที่กระทำผ่านระบบคอมพิวเตอร์ ซึ่งเป็นการสืบสวนหาตัวผู้กระทำความผิด เมื่อพนักงานเจ้าหน้าที่ได้ไปกระทำจากระบบคอมพิวเตอร์ถือว่าเป็นการล่วงล้ำเข้าไปในข้อมูลคอมพิวเตอร์ พนักงานเจ้าหน้าที่จะกระทำได้ก็ต่อเมื่อได้รับอนุญาตจากศาลก่อน

*2) การสั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์* ส่งมอบข้อมูลคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

*3) การตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์* ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใดอันเป็นหลักฐานหรือใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็น

*4) การใช้อำนาจในการตรวจสอบและเข้าถึงข้อมูลคอมพิวเตอร์* พนักงานเจ้าหน้าที่อาจพบปัญหาซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลคอมพิวเตอร์ได้เนื่องจากมีรหัสป้องกันการเข้าถึงข้อมูลจึงกำหนดให้อำนาจพนักงานเจ้าหน้าที่ดำเนินการถอดรหัสลับหรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับทำการถอดรหัสลับ

*5) การใช้อำนาจในการยึดอายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำผิด* พนักงานเจ้าหน้าที่ต้องได้รับอนุญาตจากศาลและจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์ไว้เป็นหลักฐานและจะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ หากมีกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานเกินสามสิบวัน พนักงานเจ้าหน้าที่ต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายระยะเวลาการยึดหรืออายัด แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือ

หลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยเร็ว

การยึดระบบคอมพิวเตอร์ คือการนำระบบคอมพิวเตอร์มาอยู่ในความครอบครองของพนักงานเจ้าหน้าที่

การอายัดระบบคอมพิวเตอร์ คือการที่พนักงานเจ้าหน้าที่สั่งระงับการใช้ระบบคอมพิวเตอร์นั้นและให้ระบบคอมพิวเตอร์นั้นอยู่ในความควบคุมของพนักงานเจ้าหน้าที่

***1.2.4 การให้อำนาจศาลในการตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560มาตรา 19 เป็นบทบัญญัติที่ให้อำนาจศาลในการควบคุมและตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่เฉพาะการใช้อำนาจตามมาตรา 18 (4)-(8) ที่จะต้องยื่นคำร้องขออนุญาตต่อศาลเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการ ซึ่งจะต้องเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เท่านั้นที่มีอำนาจและต้องยื่นคำร้องด้วยตนเอง

การยื่นคำร้องจะต้องยื่นต่อศาลที่มีเขตอำนาจตามพระธรรมนูญศาลยุติธรรมและกฎหมายว่าด้วยการจัดตั้งศาล การยื่นคำร้องในคดีความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งเป็นคดีอาญาจึงต้องยื่นต่อศาลชั้นต้นที่มีอำนาจพิจารณาพิพากษาคดีอาญาและมีเขตอำนาจในคดีที่บุคคลใดกระทำหรือกำลังจะกระทำความผิด คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

การพิจารณาคำร้องของพนักงานเจ้าหน้าที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์กำหนดให้ศาลพิจารณาคำร้องโดยเร็ว ถ้าศาลเห็นสมควรให้มีการไต่สวนคำร้องก่อนมีคำสั่งก็ได้เป็นอำนาจทั่วไปของศาลตามประมวลกฎหมายวิธีพิจารณาความอาญาและเป็นการสั่งคำร้องคำขอในคดีอาญาซึ่งผู้พิพากษาคนเดียวมีอำนาจตามพระธรรมนูญศาลยุติธรรม

เมื่อได้รับคำสั่งอนุญาตจากศาลให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีคำสั่งอนุญาตคำร้องภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ

***1.2.5 มาตรการปิดกั้นเว็บไซต์ที่เป็นความผิดตามกฎหมายอื่นหรือที่มีลักษณะขัดต่อศีลธรรมอันดีของประชาชน***

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ได้บัญญัติยกเลิกมาตรา 20 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ

คอมพิวเตอร์ พ.ศ.2550 และได้แก้ไขให้อำนาจศาลในการมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาค 2 ลักษณะ 1 หรือลักษณะ 1/1แห่งประมวลกฎหมายอาญา และข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา หรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนและเจ้าหน้าที่ตามกฎหมายนั้น หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาได้ร้องขอ

จะเห็นได้ว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ได้มีการแก้ไขเพิ่มเติมกฎหมายฉบับเดิม คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในหลายประการ อาทิ กำหนดฐานความผิดขึ้นใหม่ และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลาย หรือลบข้อมูลคอมพิวเตอร์ และแก้ไขเพิ่มเติมอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้น รวมทั้งในส่วนของผู้รักษาการตามกฎหมาย เนื่องมาจาก พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็ว และมีการจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งมีภารกิจในการกำหนดมาตรฐานและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ

**1.3 กฎหมายวิธีพิจารณาความอาญา**

กฎหมายวิธีพิจารณาความอาญาเป็นกฎหมายที่ว่าด้วยหลักเกณฑ์และวิธีการในการให้อำนาจหน้าที่แก่เจ้าพนักงานของรัฐในกระบวนการยุติธรรมทางอาญาและศาลในการร่วมมือกันค้นหาความจริงอันเกี่ยวกับการกระทำความผิดและการนำตัวผู้กระทำความผิดกฎหมายอาญามาดำเนินการพิจารณาและลงโทษตามบทบัญญัติของกฎหมาย ซึ่งประเทศไทยได้นำกฎหมายวิธีพิจารณาความอาญามาใช้บังคับกับกระบวนการในการแสวงหาข้อเท็จจริงและพยานหลักฐานในการนำตัวผู้กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ด้วย

กฎหมายวิธีพิจารณาความอาญาได้บัญญัติให้อำนาจเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญาเพื่อให้การดำเนินคดีอาญาสามารถได้มาซึ่งพยานหลักฐานที่จะ

พิสูจน์ความผิดและลงโทษผู้กระทำความผิดที่แท้จริงได้ ประมวลกฎหมายวิธีพิจารณาความอาญาจึงกำหนดขอบเขตของการปฏิบัติงานของเจ้าพนักงานในการจับ การควบคุม การค้นพยานหลักฐานที่เกิดจากการกระทำความผิดทางอาญา ดังนี้[18]

***1.3.1 การจับโดยเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญา***

การจับโดยเจ้าพนักงานไม่ว่าเป็นพนักงานฝ่ายปกครองหรือตำรวจพนักงานสอบสวนกำหนดให้มีกระบวนการตรวจสอบโดยองค์กรศาล ซึ่งศาลจะตรวจสอบเหตุแล้วจึงออกหมายจับ แต่ในกรณีที่มีการกระทำความผิดซึ่งหน้าหรือเหตุจำเป็นอย่างอื่นที่ไม่สามารถออกหมายจับได้ทัน กฎหมายอนุญาตให้จับโดยไม่มีหมายจับได้

*1) การจับโดยมีหมายจับ* หมายจับต้องออกโดยศาลและอาศัยเหตุที่จะออกหมายจับ มาตรา 66 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ได้กำหนดเหตุในการออกหมายจับไว้ คือ เมื่อมีหลักฐานตามสมควรว่าบุคคลใดน่าจะได้กระทำความผิดอาญาซึ่งมีอัตราโทษอย่างสูงเกินสามปี หรือเมื่อมีหลักฐานตามสมควรว่าบุคคลใดน่าจะได้กระทำความผิดอาญาและมีเหตุควรเชื่อว่าจะหลบหนี หรือไปยุ่งเหยิงกับพยานหลักฐานหรือก่อเหตุอันตรายประการอื่น หรือถ้าบุคคลนั้นไม่มีที่อยู่เป็นหลักแหล่งหรือไม่มาตามหมายเรียกหรือตามนัดโดยไม่มีข้อแก้ตัวอันควร

*2) การจับโดยไม่มีหมายจับพนักงานฝ่ายปกครองหรือตำรวจไม่สามารถกระทำได้* ซึ่งมาตรา 78 แห่งประมวลกฎหมายวิธีพิจารณาความอาญาได้กำหนดเหตุยกเว้นให้พนักงานฝ่ายปกครองหรือตำรวจสามารถกระทำได้โดยไม่มีหมายจับ คือ

*(1) เมื่อบุคคลนั้นได้กระทำผิดซึ่งหน้า* ความผิดซึ่งเห็นกำลังกระทำหรือพบในอาการใดซึ่งแทบจะไม่มีความสงสัยเลยว่าได้กระทำความผิดมาแล้วสดๆ ความผิดซึ่งหน้านั้นเจ้าพนักงานผู้จับจะต้องเป็นผู้พบเห็นเอง

*(2) เมื่อเจ้าพนักงานพบบุคคลโดยมีพฤติการณ์อันควรสงสัยว่าผู้นั้นน่าจะก่อเหตุร้ายให้เกิดอันตรายแก่บุคคลหรือทรัพย์สินของผู้อื่น* โดยมีเครื่องมือ อาวุธ หรือวัตถุอย่างอื่นอันสามารถใช้ในการกระทำความผิด

*(3) เมื่อมีเหตุที่จะออกหมายจับตามมาตรา 66 (2)* แห่งประมวลกฎหมายวิธีพิจารณาความอาญา แต่มีเหตุจำเป็นเร่งด่วนที่ไม่อาจขอศาลออกหมายจับบุคคลนั้นได้

*(4) การจับผู้ต้องหาหรือจำเลยที่หนีหรือจะหลบหนีในระหว่างถูกปล่อยชั่วคราว*

---

[18] บทบัญญัติกฎหมายวิธีพิจารณาความอาญา

***1.3.2 การควบคุมอำนาจเจ้าพนักงานในตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 2 (21) แห่งประมวลกฎหมายวิธีพิจารณาความอาญา*** ได้นิยามคำว่า “ควบคุม” หมายถึง การควบคุมหรือกักขังผู้ถูกจับโดยพนักงานฝ่ายปกครองหรือตำรวจในระหว่างสืบสวนหรือสอบสวน การควบคุมนั้นพนักงานฝ่ายปกครองหรือตำรวจและพนักงานสอบสวนต้องเป็นไปตามหลักมาตรา 87 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งจะควบคุมได้เท่าที่จำเป็นตามพฤติการณ์แห่งคดีและไม่เกินระยะเวลาที่กฎหมายกำหนดซึ่งขึ้นอยู่กับความร้ายแรงของความผิดที่ผู้ต้องหาถูกกล่าวหา

***1.3.3 อำนาจเจ้าพนักงานในการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญา***

*1) การค้นที่รโหฐานเพื่อค้นหาบุคคลซึ่งถูกหน่วงเหนี่ยวกักขังในที่รโหฐานหรือบุคคลที่มีหมายให้จับได้* และการค้นหาสิ่งของซึ่งอาจเป็นวัตถุหรือพยานหรือมีไว้หรือได้มาโดยการกระทำผิดหรือใช้ในการกระทำผิด การค้นนั้นพนักงานฝ่ายปกครองหรือตำรวจ และพนักงานสอบสวนต้องมีหมายค้นหรือคำสั่งศาล เว้นแต่ในกรณีที่ตามมาตรา 92 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา พนักงานฝ่ายปกครองหรือตำรวจสามารถค้นได้โดยมิต้องมีหมายค้นหรือคำสั่งของศาล

(1) เมื่อมีเสียงหรือพฤติการณ์แสดงให้เห็นว่ามีเหตุร้ายเกิดขึ้นในที่รโหฐานนั้น

(2) เมื่อปรากฏความผิดซึ่งหน้ากำลังกระทำลงในที่รโหฐาน

(3) เมื่อบุคคลที่ได้กระทำความผิดซึ่งหน้าขณะที่ถูกไล่จับหนีเข้าไปหรือมีเหตุควรสงสัยว่าได้เข้าไปซุกซ่อนตัวอยู่ในที่รโหฐานนั้น

(4) เมื่อมีพยานหลักฐานว่าสิ่งของที่มีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิดหรือได้ใช้หรือมีไว้เพื่อใช้ในการกระทำความผิด หรืออาจเป็นพยานหลักฐานพิสูจน์การกระทำความผิดได้ซ่อนหรืออยู่ในนั้นหากกว่าจะเอาหมายค้นเกรงว่าสิ่งของนั้นจะถูกโยกย้ายหรือทำลายเสียก่อน

(5) เมื่อที่รโหฐานนั้นผู้จะต้องถูกจับเป็นเจ้าบ้านและการจับนั้นมีหมายจับหรือจับตามมาตรา 78 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

2) *การค้นตัวบุคคล บทบัญญัติกฎหมายมาตรา 93 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา* บัญญัติห้ามการค้นบุคคลในที่สาธารณะ โดยมีข้อยกเว้นให้พนักงานฝ่ายปกครองหรือตำรวจเป็นผู้ค้นได้ เมื่อมีเหตุอันควรสงสัยว่าบุคคลนั้นมีสิ่งของในความครอบครองเพื่อจะใช้ในการกระทำความผิด หรือได้สิ่งของมาโดยการกระทำความผิด หรือมีสิ่งของซึ่งมีไว้เป็นความผิด

การค้นตัวในที่รโหฐาน บทบัญญัติกฎหมายมาตรา 100 วรรคสอง แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ให้อำนาจพนักงานผู้มีอำนาจค้นที่รโหฐานเมื่อมีเหตุอันควรสงสัยว่าบุคคลซึ่งอยู่ในที่ค้นได้เอาสิ่งของที่ต้องการพบซุกซ่อนในร่างกาย เจ้าพนักงานมีอำนาจค้นตัวผู้นั้นได้ และการค้นตัวผู้ที่ถูกจับเพื่อหาสิ่งของที่อาจใช้เป็นพยานหลักฐานเจ้าพนักงานสามารถกระทำได้

การจัดการตามหมายค้นนั้นเจ้าพนักงานที่มีชื่อในหมายค้นหรือผู้รักษาการแทนเท่านั้นที่มีอำนาจไปจัดการตามหมายค้น เจ้าพนักงานผู้ค้นต้องแสดงความบริสุทธิ์ก่อนและให้ค้นต่อหน้าผู้ครอบครองสถานที่หรือบุคคลในครอบครัวของผู้นั้นหรือค้นต่อหน้าบุคคลที่เจ้าพนักงานได้ร้องขอมาเป็นพยาน และโดยหลักการค้นต้องค้นเพื่อหาตัวคนหรือสิ่งของที่ต้องการค้นเท่านั้น เว้นแต่ในกรณีที่ค้นหาสิ่งของโดยไม่จำกัดสิ่ง เจ้าพนักงานผู้ค้นมีอำนาจยึดสิ่งของใดๆซึ่งน่าจะใช้เป็นพยานหลักฐานเพื่อประโยชน์หรือยันผู้ต้องหาหรือจำเลย

จะเห็นได้ว่าประเทศไทยได้นำกฎหมายวิธีพิจารณาความอาญามาใช้บังคับกับกระบวนการในการแสวงหาข้อเท็จจริงและพยานหลักฐานในการนำตัวผู้กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มาลงโทษ แม้จะมีการแต่งตั้งพนักงานเจ้าหน้าที่ให้มีอำนาจหน้าที่เป็นพิเศษ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เพื่อสืบสวนสอบสวนหาพยานหลักฐานที่เกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ แต่พระราชบัญญัติดังกล่าวก็มิได้ตัดอำนาจของเจ้าพนักงานตามกฎหมายอื่นที่ให้อำนาจแก่เจ้าพนักงานประเภทนั้นๆในทำนองเดียวกัน ในการดำเนินการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนิน คดีกับผู้ที่กระทำความผิด พนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 มาตรา 29 กำหนดให้มีฐานะเป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญา หมายความว่ามีอำนาจทั้งปวงตามที่กำหนดไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาที่กำหนดไว้สำหรับพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่เช่นเดียวกัน จึงทำให้พนักงานเจ้าหน้าที่และพนักงานตามประมวลกฎหมายอาญามีอำนาจซ้ำซ้อนกันในเรื่องการมีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ การจับ ควบคุม การค้น อำนาจในการทำสำนวนการสืบสวนสอบสวน ในความผิดที่มีความเกี่ยวพันกันระหว่างความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และความผิดตามกฎหมายอื่น

**1.4 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547**

กระทรวงยุติธรรมได้มีการปรับปรุงอำนาจหน้าที่โดยจัดให้มีกรมสอบสวนคดีพิเศษ อยู่ภายใต้สังกัดกระทรวงยุติธรรม ก่อตั้งขึ้นเมื่อวันที่ 3 ตุลาคม 2545 ตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ.2545 ใช้ชื่อภาษาอังกฤษว่า “DEPARTMENT OF SPECIAL INVESTIGATION” มีชื่อย่อว่า “DSI” เพื่อรับผิดชอบในการดำเนินการเกี่ยวกับคดีอาญาบางประเภทที่กำหนดให้อยู่ในอำนาจหน้าที่และคดีดังกล่าวจำเป็นต้องมีผู้เชี่ยวชาญเฉพาะด้านเป็นผู้ดำเนินการสืบสวนและสอบสวน โดยกำหนดอำนาจหน้าที่ของเจ้าหน้าที่ดังกล่าว เพื่อให้การป้องกันและปราบปรามการกระทำความผิดอาญาเป็นไปอย่างมีประสิทธิภาพ พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ได้กำหนดให้มีพนักงานสอบสวนคดีพิเศษ เจ้าหน้าที่คดีพิเศษ และวิธีการสืบสวนและสอบสวนคดีพิเศษ เพื่อปฏิบัติหน้าที่ดังกล่าวเป็นการเฉพาะ[19]

ประกาศ กคพ. (ฉบับที่ 7) พ.ศ. 2562 เรื่อง กำหนดรายละเอียดของลักษณะของการกระทำความผิดที่เป็นคดีพิเศษ ตามมาตรา 21 วรรคหนึ่ง (1) แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 กำหนดในบัญชีท้ายประกาศ ข้อ 13 คดีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติม ที่มีผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศด้านความมั่นคงและบริการภาครัฐที่สำคัญ ด้านการเงิน ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภคหรือด้านสาธารณสุข หรือกระทบต่อความมั่นคงของประเทศซึ่งความผิดดังกล่าวอาจส่งผลกระทบต่อความสงบเรียบร้อยและศีลธรรมอันดีและก่อให้เกิดความเสียหายร้ายแรง[20] ซึ่งมีบทกำหนดโทษในมาตรา ดังต่อไปนี้

1. มาตรา 5 การเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง

2. มาตรา 6 การล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นไปเปิดเผยโดยมิชอบ

3. มาตรา 7 การเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง

---

[19] Dsi กรมสอบสวนคดีพิเศษ,/ เกี่ยวกับดีเอสไอ/2559,/สืบค้นเมื่อวันที่ 21 กันยายน 2565.จากเว็บไซต์: (https://www.dsi.go.th/th/Detail/History-of-DSI)

[20] บัญชีท้ายประกาศ กคพ. (ฉบับที่ 7) พ.ศ. 2562 เรื่อง กำหนดรายละเอียดของลักษณะของการกระทำความผิดที่เป็นคดีพิเศษ

4. มาตรา 8 การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่น

5. มาตรา 9 การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

6. มาตรา 10 การทำให้ระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

7. มาตรา 11 การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นซึ่งเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

8. มาตรา 12 การกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 หรือมาตรา 11 เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

9. มาตรา 14 การกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ ดังต่อไปนี้

1. การกระทำโดยทุจริตหรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ

2. การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

3. การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

4. การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

5. การเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)

10. มาตรา 17 ผู้กระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

กรมสอบสวนคดีพิเศษจึงมีอำนาจในการสอบสวนคดีอาญาซึ่งเป็นความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ที่มีลักษณะของการกระทำความผิดที่เป็นคดีพิเศษ ซึ่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ได้กำหนดให้มีพนักงานสอบสวนคดีพิเศษและเจ้าหน้าที่คดีพิเศษ มีอำนาจในการสืบสวนและสอบสวนคดีพิเศษ ดังนี้[21]

***1.4.1 การเป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่***

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 23 กำหนดให้การปฏิบัติหน้าที่เกี่ยวกับคดีพิเศษให้พนักงานสอบสวนคดีพิเศษมีอำนาจสืบสวนและสอบสวนคดีพิเศษ และเป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมาย วิธีพิจารณาความอาญา มีอำนาจในการจับ ผู้มีหมายจับในคดีพิเศษเท่านั้นและนำส่งพนักงานสอบสวนคดีพิเศษผู้มีอำนาจหน้าที่เกี่ยวข้องดำเนินการตามกฎหมาย ส่วนเจ้าพนักงานคดีพิเศษ จะมีฐานะเป็นพนักงานฝ่ายปกครองหรือตำรวจตามประมวลกฎหมายวิธีพิจารณาความอาญา ต่อเมื่อพนักงานสอบสวนคดีพิเศษ ได้มอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับคดีพิเศษ

กรณีที่มีเหตุอันควรสงสัยว่าคดีความผิดทางอาญาใดเป็นคดีพิเศษให้พนักงานสอบสวนคดีพิเศษมีอำนาจสืบสวนคดีดังกล่าวได้ ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 23/1

***1.4.2 การเข้าไปในเคหสถานหรือสถานที่ใด ๆ เพื่อตรวจค้น โดยไม่มีหมายค้น***

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 24 (1) กำหนดให้อำนาจพนักงานสอบสวนคดีพิเศษเข้าไปในเคหสถานหรือสถานที่ใด ๆ เพื่อตรวจค้น เมื่อมีเหตุสงสัยตามสมควรว่ามีบุคคลกระทำความผิดที่เป็นคดีพิเศษหลบซ่อนอยู่ หรือมีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรืออาจใช้เป็นพยานหลักฐานได้ ประกอบกับมีเหตุอันควรเชื่อว่าการเนิ่นช้ากว่าจะเอาหมายค้นบุคคลนั้นจะหลบหนีไป หรือทรัพย์สินนั้นจะถูกโยกย้าย ซุกซ่อน ทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิม

***1.4.3 การค้นบุคคลหรือยานพาหนะ***

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 24 (2) กำหนดให้อำนาจพนักงานสอบสวนคดีพิเศษ มีอำนาจค้นบุคคลหรือยานพาหนะที่มีเหตุสงสัยตามสมควรว่ามีทรัพย์สิน ซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้

---

[21] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547

***1.4.4 การมีหนังสือสอบถามหรือเรียกหน่วยงานหรือบุคคลมาให้ถ้อยคำ***

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 24 (3) และ (4) กำหนดให้อำนาจพนักงานสอบสวนคดีพิเศษ มีอำนาจมีหนังสือสอบถามหรือเรียกให้สถาบันการเงิน ส่วนราชการ องค์การ หรือหน่วยงานของรัฐ หรือรัฐวิสาหกิจ ส่งเจ้าหน้าที่ที่เกี่ยวข้อง หรือเรียกบุคคลใด ๆ มาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชีเอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

***1.4.5 การยึดหรืออายัดทรัพย์สินที่ค้นพบ***

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 24 (5) กำหนดให้อำนาจพนักงานสอบสวนคดีพิเศษ มีอำนาจยึดหรืออายัดทรัพย์สินที่ค้นพบหรือที่ส่งดังกล่าวไว้ในข้อ 1-4

***1.4.6 การให้อำนาจศาลในการตรวจสอบการใช้อำนาจของพนักงานสอบสวนคดีพิเศษ***

การใช้อำนาจในการสืบสวนสอบสวนของพนักงานสอบสวนคดีพิเศษในข้อ 1-5 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 24 วรรคสอง กำหนดให้พนักงานสอบสวนคดีพิเศษแสดงความบริสุทธิ์ก่อนการเข้าค้น รายงานเหตุผลและผลการตรวจค้นเป็นหนังสือต่อผู้บังคับบัญชาเหนือขึ้นไป และบันทึกเหตุสงสัยและเหตุอันควรเชื่อที่ทำให้สามารถเข้าค้นได้เป็นหนังสือให้ไว้แก่ผู้ครอบครองเคหสถานหรือสถานที่ค้น กรณีค้นในเวลากลางคืนภายหลังพระอาทิตย์ตก พนักงานสอบสวนคดีพิเศษผู้เป็นหัวหน้าในการเข้าค้นต้องเป็นข้าราชการพลเรือนตำแหน่งตั้งแต่ระดับ 7 ขึ้นไป และพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 24 วรรคสาม กำหนดให้พนักงานคดีสอบสวนคดีพิเศษผู้เป็นหัวหน้าในการเข้าค้นส่งสำเนาบันทึกเหตุสงสัยและเหตุอันควรเชื่อ และสำเนาบันทึกการตรวจค้นและบัญชีทรัพย์ที่ยึดหรืออายัดต่อศาลจังหวัดที่มีอำนาจเหนือท้องที่ที่ทำการค้น หรือศาลอาญาในเขตกรุงเทพมหานคร ภายใน 48 ชั่วโมงหลังการสิ้นสุดการค้น

***1.4.7 การเข้าถึงข้อมูลอิเล็กทรอนิกส์***

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 กำหนดให้อำนาจพนักงานสอบสวนคดีพิเศษ ซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือ จะยื่นคำขอฝ่ายเดียวต่ออธิบดี ผู้พิพากษาศาลอาญา เพื่อมีคำสั่งอนุญาตให้ได้มาซึ่ง เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด กรณีมีเหตุอันควรเชื่อได้ว่า ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ

การพิจารณาอนุญาตตามคำขออธิบดีผู้พิพากษาศาลอาญาจะพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็น ได้แก่กรณีที่มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ และมีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว และไม่อาจใช้วิธีการอื่นที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้ อธิบดีผู้พิพากษาศาลอาญาจะสั่งอนุญาตได้คราวละไม่เกินสิบเก้าวันโดยกำหนดเงื่อนไขใด ๆ ก็ได้ หากในภายหลังที่มีคำสั่งอนุญาต ปรากฏข้อเท็จจริงว่าเหตุผลและความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อาจเปลี่ยนแปลงคำสั่งได้ตามที่เห็นสมควร

***1.4.8 การแฝงตัว***

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 27 กำหนดให้อำนาจพนักงานสอบสวนคดีพิเศษ มีอำนาจให้บุคคลใดจัดทำเอกสารหรือหลักฐานใดขึ้นหรือเข้าไปแฝงตัวในองค์กรหรือกลุ่มคนใด เพื่อประโยชน์ในการสืบสวนสอบสวน และให้ถือว่าเป็นการกระทำโดยชอบ

***1.4.9 การประสานการปฏิบัติหน้าที่ในคดีพิเศษระหว่างหน่วยงานของรัฐที่เกี่ยวข้อง***

ข้อบังคับ กคพ. ว่าด้วยการปฏิบัติหน้าที่ในคดีพิเศษระหว่างหน่วยงานของรัฐที่เกี่ยวข้อง พ.ศ. 2547 ได้กำหนดให้กรมสอบสวนคดีพิเศษและหน่วยงานที่เกี่ยวข้องประสานงานเพื่อป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคดีพิเศษ โดยกำหนดให้กรมสอบสวนคดีพิเศษรับคำร้องทุกข์ หรือคำกล่าวโทษ ในคดีความผิดอาญาอันเป็นคดีพิเศษเท่านั้น กรณีที่มีการร้องทุกข์ หรือกล่าวโทษในการกระทำความผิดอาญาอันเป็นคดีพิเศษต่อพนักงานสอบสวนของสำนักงานตำรวจหรือเจ้าหน้าที่สืบสวนของหน่วยงานอื่นของรัฐ ให้พนักงานสอบสวนหรือเจ้าหน้าที่ดำเนินการรับคำร้องทุกข์หรือคำกล่าวโทษ ดำเนินการสืบสวนสอบสวนตามหน้าที่จนกว่าจะมีการส่งมอบสำนวนการสอบสวนให้กรมสอบสวนคดีพิเศษภายใน 15 วันนับแต่วันที่มีการรับ คำร้องทุกข์หรือคำกล่าวโทษ เมื่อส่งสำนวนการสอบสวนแล้วให้มีการหารือเกี่ยวกับรายละเอียดกรดำเนินการ เพื่อให้เกิดการประสานความร่วมมือระหว่างพนักงานสอบสวนคดีพิเศษกับพนักงานสอบสวนหรือเจ้าหน้าที่ผู้มีอำนาจสอบสวน[22]

---

[22] ข้อบังคับ กคพ. ว่าด้วยการปฏิบัติหน้าที่ในคดีพิเศษระหว่างหน่วยงานของรัฐที่เกี่ยวข้อง พ.ศ. 2547

***1.4.10 การสอบสวนร่วมกันหรือการปฏิบัติหน้าที่ร่วมกันในคดีพิเศษระหว่างพนักงานสอบสวนคดีพิเศษกับพนักงานอัยการหรืออัยการทหาร***

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 32 ประกอบกับข้อบังคับ กคพ. ว่าด้วยหลักเกณฑ์และวิธีการเกี่ยวกับการสอบสวนร่วมกันหรือการปฏิบัติหน้าที่ร่วมกันในคดีพิเศษระหว่างพนักงานสอบสวนคดีพิเศษกับพนักงานอัยการหรืออัยการทหาร พ.ศ. 2547 โดยกำหนดให้คดีพิเศษที่ต้องดำเนินการสอบสวนร่วมกัน ได้แก่ คดีพิเศษในมาตรา 21 วรรคหนึ่ง (1) (ค) คดีความผิดทางอาญาที่มีลักษณะเป็นการกระทำความผิดข้างชาติที่สำคัญหรือเป็นการกระทำขององค์กรอาชญากรรม หรือ (ง) คดีความผิดทางอาญาที่มีผู้ทรงอิทธิพลที่สำคัญเป็นตัวการผู้ใช้หรือผู้สนับสนุน หรือคดีพิเศษที่ กคพ. มีมติให้ต้องดำเนินการสอบสวนร่วมกัน[23]

การปฏิบัติหน้าที่ร่วมกัน หมายถึง การมีพนักงานอัยการหรืออัยการทหารให้คำแนะนำและตรวจสอบพยานหลักฐานตั้งแต่ชั้นเริ่มการสอบสวนในคดีพิเศษ โดยให้เริ่มดำเนินการนับแต่โอกาสแรกเท่าที่จะพึงกระทำได้ ซึ่งพนักงานสอบสวนคดีพิเศษเป็นผู้รับผิดชอบในการสอบสวน โดยพนักงานอัยการหรืออัยการทหารให้คำแนะนำ และตรวจสอบพยานหลักฐานว่าเป็นประโยชน์ในการสอบสวนหรือการฟ้องคดีหรือไม่

จะเห็นได้ว่าพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ได้กำหนดให้อำนาจแก่พนักงานสอบสวนคดีพิเศษและเจ้าพนักงานคดีพิเศษ ในการดำเนินการแสวงหาข้อเท็จจริงและพยานหลักฐานในการนำตัวผู้กระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มาลงโทษ ในความผิดที่มีลักษณะเป็นคดีพิเศษเกี่ยวกับการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ที่มีผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศด้านความมั่นคงและบริการภาครัฐที่สำคัญ ด้านการเงิน ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภคหรือด้านสาธารณสุข หรือกระทบต่อความมั่นคงของประเทศ ซึ่งความผิดดังกล่าวอาจส่งผลกระทบต่อความสงบเรียบร้อยและศีลธรรมอันดีและก่อให้เกิดความเสียหายร้ายแรง และให้มีฐานะเป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา มีอำนาจในการจับผู้มีหมายจับในคดีพิเศษ การค้นโดยไม่มีหมายค้น การเข้าถึงข้อมูลอิเล็กทรอนิกส์และการแฝงตัว การประสานการปฏิบัติหน้าที่ในคดีพิเศษระหว่างหน่วยงานของรัฐที่เกี่ยวข้อง การ

---

[23] ข้อบังคับ กคพ. ว่าด้วยหลักเกณฑ์และวิธีการเกี่ยวกับการสอบสวนร่วมกันหรือการปฏิบัติหน้าที่ร่วมกันในคดีพิเศษระหว่างพนักงานสอบสวนคดีพิเศษกับพนักงานอัยการหรืออัยการทหาร พ.ศ.2547

สอบสวนร่วมกันหรือการปฏิบัติหน้าที่ร่วมกันในคดีพิเศษระหว่างพนักงานสอบสวนคดีพิเศษกับพนักงานอัยการ

**1.5 หน่วยงานที่มีอำนาจดำเนินคดีกับผู้ที่กระทำความผิดทางคอมพิวเตอร์ของประเทศไทย**

เนื่องจากประเทศไทยมีกฎหมายที่เกี่ยวกับการดำเนินคดีกับผู้ที่กระทำความผิดทางอาชญากรรมทางคอมพิวเตอร์หลายฉบับ โดยในแต่ละฉบับได้กำหนดให้อำนาจแก่เจ้าหน้าที่รัฐหลายฝ่ายในการดำเนินคดีกับผู้ที่กระทำความผิดทางอาชญากรรมทางคอมพิวเตอร์ ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ซึ่งให้อำนาจแก่พนักงานเจ้าหน้าที่ในการดำเนินการควบคุม การค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายวิธีพิจารณาความอาญาที่ให้อำนาจแก่พนักงานสอบสวนในการดำเนินคดีกับผู้ที่กระทำความผิดทางอาญา และพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 กำหนดให้อำนาจแก่พนักงานสอบสวนคดีพิเศษในการสืบสวนสอบสวนแสวงหาข้อเท็จจริงและพยานหลักฐานกับผู้ที่กระทำความผิดอาชญากรรมทางคอมพิวเตอร์ ในความผิดที่มีลักษณะเป็นคดีพิเศษ ซึ่งในแต่ละหน่วยงานนั้นมีอำนาจหน้าที่ในลักษณะที่คล้ายกัน ดังนี้

***1.5.1 กรมสอบสวนคดีพิเศษ (DEPARTMENT OF SPECIAL INVESTIGATION : DSI)***

มีภารกิจและหน้าที่ความรับผิดชอบเกี่ยวกับการป้องกัน การปราบปราม การสืบสวนและการสอบสวนคดีความผิดทางอาญาที่ต้องดำเนินการสืบสวนและสอบสวนโดยใช้วิธีการพิเศษตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 กำหนดให้อำนาจแก่ พนักงานสอบสวนคดีพิเศษ ซึ่งเป็นอำนาจที่นอกเหนือจากที่กำหนดไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา และพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ มีอำนาจในการสืบสวนสอบสวน แสวงหาข้อเท็จจริงและพยานหลักฐานในการนำตัวผู้กระทำความผิดอาชญากรรมทางคอมพิวเตอร์ ในความผิดที่มีลักษณะเป็นคดีพิเศษ โดยกำหนดให้มีอำนาจการเข้าไปในเคหสถานหรือสถานที่ใด ๆ เพื่อตรวจค้น โดยไม่มีหมายค้น อำนาจค้นบุคคลหรือยานพาหนะ อำนาจยึดหรืออายัดทรัพย์สินที่ค้นพบ อำนาจในการเข้าถึงเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่ง ส่งทางไปรษณีย์โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด มีอำนาจให้บุคคลใดจัดทำเอกสารหรือหลักฐานใดขึ้นหรือเข้าไปแฝงตัวในองค์กรหรือกลุ่มคนใด เพื่อประโยชน์ในการสืบสวนสอบสวน และให้ถือว่าเป็นการกระทำโดยชอบ

***1.5.2 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี Technology Crime Suppression Division (TCSD)***

เป็นหน่วยงานที่จัดตั้งขึ้นตามโครงสร้างใหม่ เมื่อวันที่ 7 กันยายน 2552 ตามพระราชกฤษฎีกาแบ่งส่วนราชการ สำนักงานตำรวจแห่งชาติพ.ศ.2552 กฎกระทรวงแบ่งส่วนราชการเป็น กองบังคับการ หรือส่วนราชการอย่างอื่น ในสำนักงานตำรวจแห่งชาติ พ.ศ.2552 ระเบียบสำนักงานตำรวจแห่งชาติ ว่าด้วยการกำหนดอำนาจหน้าที่ของส่วนราชการ สำนักงานตำรวจแห่งชาติ พ.ศ.2552 แบ่งส่วนกองกำกับการ 1 มีหน้าที่เกี่ยวกับการกระทำผิดที่มุ่งต่อระบบคอมพิวเตอร์เป็นเป้าหมาย กองกำกับการ 2 มีหน้าที่เกี่ยวกับการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำผิด กองกำกับการ 3 มีหน้าที่เกี่ยวกับการนำเข้าเผยแพร่ข้อมูลคอมพิวเตอร์ สู่ระบบคอมพิวเตอร์ที่เป็นความผิด และกลุ่มงานสนับสนุนคดีเทคโนโลยี มีหน้าที่เกี่ยวกับปฏิบัติการโต้ตอบในเชิงรุกโดยฉับพลันทางอินเตอร์เน็ต และสนับสนุนคดีเทคโนโลยี และมีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อยป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวน ปฏิบัติงานตามประมวลกฎหมาย วิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์[24]

***1.5.3 กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) Cyber Crime Investigation Bureau (CCIB)***

เป็นหน่วยงานที่จัดตั้งขึ้น เมื่อวันที่ 9 กันยายน 2563 ตามพระราชกฤษฎีกาแบ่งส่วนราชการสสำนักงานตำรวจแห่งชาติ (ฉบับที่ 5) พ.ศ.2563 กฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการอย่างอื่นในสำนักงานตำรวจแห่งชาติ (ฉบับที่ 17) พ.ศ.2563 ระเบียบสำนักงานตำรวจแห่งชาติ ว่าด้วยการกำหนดอำนาจหน้าที่ของส่วนราชการ สำนักงานตำรวจแห่งชาติ (ฉบับที่ 24) พ.ศ.2563[25]

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี มีอำนาจหน้าที่ในการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี ดังนี้[26]

---

[24] กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี,/ประวัติหน่วยงาน/2552,/สืบค้นเมื่อวันที่ 22 กันยายน 2565. จากเว็บไซต์: (https://www.tcsd.go.th/เกี่ยวกับหน่วยงาน)

[25] กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี,/ประวัติความเป็นมา/2563/สืบค้นเมื่อวันที่ 22 กันยายน 2565.จากเว็บไซต์: (https://www.ccib.go.th/เกี่ยวกับหน่วยงาน/ประวัติหน่วยงาน)

[26] กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี,/ประวัติความเป็นมา/2563/สืบค้นเมื่อวันที่ 22 กันยายน 2565. จากเว็บไซต์: (https://www.ccib.go.th/เกี่ยวกับหน่วยงาน/อำนาจหน้าที่)

1. เป็นฝ่ายอำนวยการด้านยุทธศาสตร์ให้สำนักงานตำรวจแห่งชาติ ในการวางแผน ควบคุม ตรวจสอบ ให้คำแนะนำ และเสนอแนะการปฏิบัติงาน ตามอำนาจหน้าที่ของกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีและหน่วยงานในสังกัด

2. ดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วราชอาณาจักร

3. ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่น อันเป็นความผิดทางอาญาเกี่ยวกับอาชญากรรมทางเทคโนโลยีและความผิดอื่นที่เกี่ยวเนื่อง

4. ดำเนินการเกี่ยวกับการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี โดยการใช้เทคโนโลยีสารสนเทศและเครื่องมือพิเศษ สนับสนุนส่วนราชการ หรือหน่วยงานอื่นในการสืบสวนสอบสวน รวมทั้งสนับสนุนการพัฒนาบุคลากรด้านการสืบสวนสอบสวนของสำนักงานตำรวจแห่งชาติ ให้มีความรู้ ความสามารถในการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี

5. ดำเนินการเกี่ยวกับการรวบรวมข้อมูล ตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี

6. ดำเนินการเกี่ยวกับการพิสูจน์หลักฐานดิจิทัล การตรวจสถานที่เกิดเหตุ และเก็บรวบรวมพยานหลักฐานดิจิทัลเพื่อสนับสนุนการปฏิบัติงานสืบสวนสอบสวนของหน่วยงานต่าง ๆ

7. ส่งเสริมและสนับสนุนให้ท้องถิ่น ชุมชน และประชาชนมีส่วนร่วมในกิจกรรมของตำรวจเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี รวมทั้งประสานความร่วมมือกับหน่วยงานของรัฐหรือองค์กรอื่นที่เกี่ยวข้องกับงานป้องกันและปราบปราม และงานสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี ทั้งในประเทศและต่างประเทศ

## 2. กฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายต่างประเทศ

ในสถานการณ์ปัจจุบันพบว่าในหลายองค์กร ไม่ว่าจะเป็นเอกชนหรือหน่วยงานของรัฐถูกจารกรรมข้อมูลบ่อยครั้ง สะท้อนให้เห็นปัญหาอาชญากรรมทางคอมพิวเตอร์ที่มีเพิ่มมากขึ้น เป็นอันตรายต่อทุกคนและสร้างความเสียหายในวงกว้าง ซึ่ง Cybercrime Magazine ประเมินว่ามีความ

เสียหายจากอาชญากรรมทางคอมพิวเตอร์ทั่วโลกสูงถึง 6 ล้านล้านดอลลาร์สหรัฐ และระบุว่าตั้งแต่มีการแพร่ระบาดของโรคโควิด-19 จำนวนอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้นถึง 6 เท่า โดยสถิติองค์กรธุรกิจถูกจารกรรมข้อมูลในปี 2021 เกิดขึ้นในทุก 11 วินาที Cyber security Ventures คาดว่าต้นทุนของอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้น 15% ต่อปี ทำให้ในปี 2025 ต้นทุนอาชญากรรมบนอินเทอร์เน็ตจะสูงถึง 10.5 ล้านล้านดอลลาร์สหรัฐฯ สอดคล้องกับผลสำรวจของ Accenture ในปี 2019 ที่สัมภาษณ์ผู้บริหาร 2,647 คน 355 บริษัท 16 อุตสาหกรรม ใน 11 ประเทศ พบว่า ทุกองค์กรจัดสรรงบประมาณแก้ปัญหาจากการถูกจารกรรมข้อมูลเพิ่มขึ้น มีการจัดอันดับผ่าน Global Cyber security Exposure Index 2020 (CEI) (ดัชนีความปลอดภัยทางไซเบอร์ทั่วโลก) ประเทศไทยถูกจัดอันดับความปลอดภัยทางอินเตอร์เน็ตอยู่ที่ 38 ของโลก จากการจัดอันดับ 85 ประเทศ ซึ่งอยู่ในอันดับ 3 ของอาเซียน การแก้ปัญหาที่เกิดจากการก่ออาชญากรรมทางคอมพิวเตอร์ ในส่วนมากองค์กรที่ถูกจารกรรมข้อมูลมักจะแก้ปัญหา โดยการยินยอมให้ในสิ่งที่อาชญากรต้องการ ไม่ว่าจะเป็นเงิน หรือทรัพย์สิน ซึ่งถือว่าเป็นการแก้ปัญหาในปลายเหตุ การป้องกันไม่ให้เกิดอาชญากรรมทางคอมพิวเตอร์จึงถือเป็นสิ่งสำคัญ และการดำเนินคดีกับผู้ที่กระทำความผิดก็เป็นการป้องกันไม่ให้อาชญากรนำมาใช้ในการแสวงหาประโยชน์โดยมิชอบ[27]

**2.1 กฎหมายของสหรัฐอเมริกา**

ประเทศสหรัฐอเมริกา เป็นประเทศที่มีการพัฒนาในด้านเทคโนโลยีมาอย่างยาวนาน เนื่องจากสหรัฐอเมริกามีนโยบายส่งเสริมด้านเทคโนโลยี การส่งเสริมการแลกเปลี่ยนข้อมูลและเพิ่มศักยภาพการแข่งขันและพัฒนาเศรษฐกิจด้านดิจิทัล โดยให้ความสำคัญในการเข้าถึงระบบอินเทอร์เน็ตให้เป็นทางเลือกของผู้บริโภคและประชาชน พร้อมทั้งมีมาตรการด้านความปลอดภัยเพื่อสร้างความมั่นใจสำหรับการเข้าใช้ระบบอินเทอร์เน็ตที่สอดคล้องกับกฎหมาย ซึ่งมุ่งเน้นด้านการป้องกัน โดยให้ภาคเอกชนเข้ามามีส่วนร่วมในการป้องกันความปลอดภัยทางอินเทอร์เน็ตให้กับระบบเศรษฐกิจและประชาชน

กฎหมายที่เกี่ยวกับการกระทำความผิดทางอาชญากรรมทางคอมพิวเตอร์ของสหรัฐอเมริกา มีมาตั้งแต่ปี ค.ศ.1984 คือ กฎหมาย Computer Fraud and Abuse Act (CFAA) มีผลบังคับใช้ในปี 1986 โดยสภาคองเกรสเห็นว่าสหรัฐอเมริกามีความก้าวหน้าทางเทคโนโลยี ทำให้เกิดการกระทำความผิดในรูปแบบใหม่ๆ จากการพัฒนาของเทคโนโลยี จึงได้มีการตรากฎหมายฉบับ

---

[27] สิทธิพล วิบูลย์ธนากุล,/ อาชญากรรมบนอินเทอร์เน็ต ก่อต้นทุนทางเศรษฐกิจแค่ไหน/2564,/ สืบค้นเมื่อวันที่ 19 มกราคม 2565. จากเว็บไซต์: (https://www.bangkokbiznews.com/business/962481)

ดังกล่าว เพื่อเป็นกฎหมายหลักในการดำเนินคดีกับการกระทำความผิดทางคอมพิวเตอร์ กฎหมายฉบับดังกล่าวมีการแก้ไขหลายครั้ง โดยแก้ไขครั้งล่าสุดคือปี 2008 เพื่อให้ครอบคลุมกับการกระทำความผิดทางคอมพิวเตอร์ในหลากหลายรูปแบบ[28]

การกระทำที่ถือว่าเป็นความผิดตามกฎหมาย Computer Fraud and Abuse Act (CFAA) ได้บัญญัติไว้ใน CFAA 18 U.S.C. มาตรา 1030 ได้แก่

1. Section (a)(1) ผู้ใดเข้าสู่ระบบคอมพิวเตอร์โดยรู้ว่าไม่มีอำนาจ และได้ไปซึ่งข้อมูลนั้น โดยมีเหตุอันควรเชื่อได้ว่าข้อมูลนั้นอาจใช้ไปเพื่อการอันเป็นภัยต่อความมั่นคงของรัฐ หรือเพื่อประโยชน์ของชาติอื่น ผู้กระทำความผิดตามอนุมาตรานี้จะถูกลงโทษปรับหรือจำคุกไม่เกิน 10 ปีหรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 20 ปี

2. Section (a)(2) ผู้ใดเจตนาเข้าสู่ระบบคอมพิวเตอร์โดยปราศจากอำนาจ เพื่อให้ได้มาซึ่งข้อมูลทางการเงินหรือเข้าสู่ข้อมูลของสถาบันการเงิน ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำความผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

3. Section (a)(3) ผู้ใดมีเจตนาเข้าสู่คอมพิวเตอร์ของรัฐบาล โดยปราศจากอำนาจ และปลอมแปลง หรือแสร้งทำเป็นว่าเป็นพนักงานของรัฐบาลเพื่อทำการเปิดระบบประมวลผลอันก่อให้เกิดความเสียหายต่อรัฐบาลสหรัฐ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำความผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

4. Section (a)(4) ผู้ใดเข้าสู่ระบบคอมพิวเตอร์ของรัฐบาล โดยรู้ว่าไม่มีอำนาจเพื่อผลประโยชน์ใด ๆ ด้วยเจตนาที่จะฉ้อโกง หรือได้ไปซึ่งสิ่งมีค่าใด ๆ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำความผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี[29]

สหรัฐอเมริกา ได้มีมาตรการทางกฎหมายในการป้องกัน ปราบปราม อาชญากรรมทางอิเล็กทรอนิกส์ ให้ความสำคัญกับความปลอดภัยทางไซเบอร์ในรัฐ มีมาตรการการป้องกันและปราบปรามการกระทำความผิดทางคอมพิวเตอร์ โดยรัฐบาลสหรัฐอเมริกามีการจัดตั้งหน่วยงานเกี่ยวกับการดำเนินคดีกับผู้ที่กระทำความผิดทางคอมพิวเตอร์ ดังนี้

---

[28] NACDL,/ CFAA Background/2020,/สืบค้นเมื่อวันที่ 8 มิถุนายน 2565.จากเว็บไซต์: (https://www.nacdl.org/Content/CFAABackground)

[29] NACDL,/ Computer Fraud and Abuse Act (CFAA)/2020,/สืบค้นเมื่อวันที่ 8 มิถุนายน 2565.จากเว็บไซต์: (https://www.nacdl.org/Landing/ComputerFraudandAbuseAct)

1. ศูนย์รับเรื่องร้องเรียนอาชญากรรมทางอินเทอร์เน็ตของ FBI (the Internet Crime Complaint Center) มีภารกิจการจัดให้มีการรายงานที่น่าเชื่อถือและสะดวกแก่สาธารณชนในการส่งข้อมูลไปยังสำนักงานสืบสวนกลางแห่งสหรัฐอเมริกาเกี่ยวกับกิจกรรมที่ต้องสงสัยว่าเป็นอาชญากรทางอิเล็กทรอนิกส์ และทางศูนย์รับเรื่องร้องเรียนจะดำเนินการวิเคราะห์และสืบสวนตามกฎหมายต่อไป[30]

2. Cyber security Infrastructure Security Agency (CISA) มีบทบาทในการรักษาความปลอดภัยทางไซเบอร์ จากภัยคุกคามทางไซเบอร์ หรือจากการที่บุคคลนำเทคโนโลยีมาใช้ในการขโมยข้อมูล หรือมาขัดขวาง ทำลาย คุกคามการทำงานของรัฐบาลหรือพลเมืองของประเทศสหรัฐอเมริกา[31]

ในส่วนของการค้น ยึดพยานหลักฐานที่เกิดจากการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ มีการให้อำนาจแก่

อัยการ ยกตัวอย่าง รัฐแมสซาชูเซตส์ (Massachusetts) เป็นรัฐหนึ่งในเขตนิวอิงแลนด์ ในสหรัฐอเมริกา ให้ความสำคัญกับความปลอดภัยทางไซเบอร์ในรัฐ มีมาตรการการป้องกันและปราบปรามการกระทำความผิดทางคอมพิวเตอร์ให้อำนาจในการสืบสวนและดำเนินคดีกับผู้ที่กระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ แก่สำนักงานอัยการสูงสุด ซึ่งได้มีการจัดตั้งแผนก Enterprise, Major และ Cyber Crimes (EMCCD) ดำเนินการสืบสวนและดำเนินคดีอาญาที่ซับซ้อนซึ่งเกี่ยวข้องกับหลักฐานดิจิทัล ให้คำปรึกษาหารือเกี่ยวกับอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยี และการตรวจสอบหลักฐานทางนิติวิทยาศาสตร์ของหลักฐานดิจิทัล มีการสร้างห้องปฏิบัติการหลักฐานดิจิทัล ให้บริการสำนักงานอัยการสูงสุด ตลอดจนหน่วยงานบังคับใช้กฎหมายในท้องถิ่นและของรัฐอื่นๆ ที่ต้องการความช่วยเหลือ[32]

พนักงานสืบสวนสอบสวน เพื่อให้สามารถเข้าถึงพยานหลักฐานได้อย่างรวดเร็ว ป้องกันการทำลายพยานหลักฐานของผู้กระทำความผิด โดยมีการสืบสวนทาง ไซเบอร์ของหน่วยสืบราชการลับของสหรัฐอเมริกา (United States Secret Service) มีเป้าหมายปกป้องโครงสร้าง

---

[30] FBI (the Internet Crime Complaint Center) IC3,/ Mission Statement/2000,/สืบค้นเมื่อวันที่ 8 มิถุนายน 2565.จากเว็บไซต์: (https://www.ic3.gov/Home/About)

[31] CYBERSECURITY,/ CISA's Role in Cyber security /2000,/สืบค้นเมื่อวันที่ 8 มิถุนายน 2565. จากเว็บไซต์: (https://www.cisa.gov/cybersecurity)

[32] Mass.gov,/ The Attorney General's Enterprise, Major, and Cyber Crimes Division /2022,/ สืบค้นเมื่อวันที่ 8 มิถุนายน 2565.จากเว็บไซต์: (https://www.mass.gov/the-attorney-generals-enterprise-major-and-cyber-crimes-division)

พื้นฐานทางการเงินของประเทศและรักษาสภาพแวดล้อมที่ปลอดภัยสำหรับชาวอเมริกันในการทำธุรกรรมทางการเงิน มีภารกิจคือการตรวจสอบอาชญากรรมทางการเงินที่ซับซ้อนซึ่งเปิดใช้งานทางไซเบอร์ ที่อาจส่งผลกระทบในวงกว้างต่อบุคคล องค์กร ชุมชน และประเทศชาติ มีหน้าที่รับผิดชอบในการตรวจจับ สืบสวน และจับกุมบุคคลที่ละเมิดกฎหมายบางประการที่เกี่ยวข้องกับระบบการเงิน มีการใช้สินทรัพย์ดิจิทัลมากขึ้นเพื่ออำนวยความสะดวกในการก่ออาชญากรรมที่หลากหลาย ซึ่งรวมถึงแผนการฉ้อโกงต่างๆ ในขณะที่สหรัฐอเมริกาเป็นผู้นำในการกำหนดมาตรฐานสำหรับการควบคุมและดูแลการใช้สินทรัพย์ดิจิทัลเพื่อต่อต้านการฟอกเงินและต่อต้านการจัดหาเงินทุนเพื่อการก่อการร้าย มีการปฏิบัติงานโดยมีศูนย์ภารกิจกระจายตามพื้นที่ เพื่อให้การติดตามและประสานงาน การสืบสวนทั้งในประเทศและต่างประเทศ มีประสิทธิภาพ เนื่องจากการรักษาความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพต้องใช้แนวทางแบบองค์รวมเพื่อให้องค์กรมีความยืดหยุ่นมากขึ้นต่อการโจมตีทางไซเบอร์ หน่วยสืบราชการลับได้พัฒนาการวางแผนรับมือเหตุการณ์ทางไซเบอร์เพื่อช่วยองค์กรในการจัดเตรียม ป้องกัน และตอบสนองต่อการโจมตีทางไซเบอร์[33]

แต่เพื่อเป็นการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐหรือผู้มีอำนาจหน้าที่ไม่ให้ยึดพยานหลักฐานโดยผิดกฎหมายหรือขัดกับรัฐธรรมนูญแห่งสหรัฐอเมริกา การค้นและการยึดพยานหลักฐานอิเล็กทรอนิกส์ ที่อยู่ในความครอบครองของบุคคลใดในที่รโหฐานต้องมีหมายค้นและมีเหตุอันควรหรือมีความสมเหตุสมผลที่จะขอให้ศาลออกหมายค้นหรือยึด แต่เพื่อให้การเข้าถึงพยานหลักฐานอิเล็กทรอนิกส์ได้อย่างรวดเร็วทันต่อการทำลายพยานหลักฐานของอาชญากร จึงมีการกำหนดข้อยกเว้นในกรณีที่ไม่ต้องขอหมายค้น ได้แก่

1. ความยินยอม โดยความยินยอมสามารถแสดงออกได้หลายรูปแบบ เช่นการ กดตกลงแถบข้อความแจ้งเตือน หรือในกรณีที่มีผู้ใช้หลายคนใน User เดียว เมื่อได้รับความยินยอมจากผู้ใช้คนเดียวก็เพียงพอ ซึ่งความยินยอมอาจกำหนดเงื่อนไขของเรื่องที่ยินยอมและระยะเวลาได้ และจะเพิกถอนเมื่อใดก็ได้

2. กรณีมีเหตุฉุกเฉิน เพื่อป้องกันการทำลายพยานหลักฐานเจ้าหน้าที่รัฐหรือผู้มีอำนาจหน้าที่ สามารถตรวจค้น ณ ขณะนั้นเพื่อรักษาข้อมูลนั้นไว้ หรือยึดอุปกรณ์เก็บข้อมูลอิเล็กทรอนิกส์

---

[33] United States Secret Service,/ Cyber Investigations/2000,/สืบค้นเมื่อวันที่ 8 มิถุนายน 2565.จากเว็บไซต์: (https://www.secretservice.gov/investigation/cyber)

ในการค้นพยานหลักฐานอิเล็กทรอนิกส์จะต้องทำการค้นหาฮาร์ดแวร์ หรือฮาร์ดดิสก์ ในการปฏิบัติหน้าที่ของพนักงานสอบสวนของสหรัฐอเมริกา จะต้องเป็นการค้นหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์โดยไม่ขัดต่อหลักการไม่รับฟังพยานหลักฐาน ซึ่งได้มาโดยการค้นที่มิชอบ (Exclusionary Rule) ตามรัฐธรรมนูญสหรัฐอเมริกาซึ่งคุ้มครองสิทธิความปลอดภัยในร่างกายและเคหสถาน กฎหมายว่าด้วยวิธีพิจารณาความอาญาของสหรัฐอเมริกา ซึ่งบัญญัติว่า

เจ้าพนักงานผู้มีอำนาจหรือพนักงานอัยการต้องขอหมายค้น

1. หมายค้นต้องออกโดยศาล Magistrate ของมลรัฐ หรือศาลของสหรัฐ สำหรับการค้นสิ่งของหรือค้นหาหาบุคคลในเขตอำนาจศาล

2. หมายค้นออกโดยศาล Magistrate สำหรับกรณีการสิ่งของหรือค้นหาบุคคลในเขตอำนาจศาลหรือค้นสิ่งของที่ถูกโยกย้ายหรือบุคคลหลบหนีออกนอกเขตก่อนจะถูกดำเนินการตามกฎหมาย[34]

จะเห็นได้ว่าเจ้าหน้าที่ของรัฐจะทำการค้นพยานหลักฐานอิเล็กทรอนิกส์ได้ก็ต่อเมื่อมีหมายค้นและมีเหตุอันควรหรือมีความสมเหตุสมผลที่จะขอให้ศาลออกหมายค้น หมายค้นดังกล่าวจะต้องออกโดยผู้พิพากษา แม้ในกรณีของการค้นข้อมูลอิเล็กทรอนิกส์ซึ่งเป็นพยานหลักฐานที่มีลักษณะพิเศษที่อาจถูกแก้ไขเปลี่ยนแปลงได้เจ้าพนักงานของรัฐก็จะต้องทำการค้นโดยมีหมายเพราะกระบวนการในการออกหมายเป็นมาตรการในการตรวจสอบการใช้ดุลพินิจของเจ้าหน้าที่เพื่อให้เจ้าหน้าที่ปฏิบัติหน้าที่โดยไม่ขัดกับรัฐธรรมนูญ ถึงแม้จะไม่ได้เข้าไปค้นในที่รโหฐานแต่การเข้าไปตรวจสอบระบบอินเทอร์เน็ตหรือเข้าไปในเครือข่ายของผู้อื่น ก็ถือว่าเป็นการละเมิดสิทธิของบุคคลตามรัฐธรรมนูญ

**2.2 กฎหมายของสหพันธ์สาธารณรัฐเยอรมนี**

สหพันธ์สาธารณรัฐเยอรมนี เป็นประเทศที่ใช้นิติวิธีของระบบประมวลกฎหมาย (Civil law) เช่นเดียวกับประเทศไทย แนวคิดของสหพันธ์สาธารณรัฐเยอรมนีไม่มีบทบัญญัติพิเศษโดยเฉพาะที่จะลงโทษผู้กระทำความผิดทางอาชญากรรมทางอิเล็กทรอนิกส์ ซึ่งจะเน้นไปในทางปราบปรามการกระทำความผิดโดยอาศัยคอมพิวเตอร์เป็นเครื่องมือ เนื่องจากตามนิติวิธีของระบบประมวลกฎหมาย (Civil law) การกระทำใดที่เป็นความผิดทางอาญาและกระทบคุณธรรมทางกฎหมายจะต้องบัญญัติความผิดและมาตรการบังคับทางอาญาไว้ในประมวลกฎหมายอาญา ด้วยเหตุ

---

[34] ปัณฑ์ณัฐ ขันเขต, วิทยานิพนธ์ปริญญานิติศาสตร์มหาบัณฑิต คณะนิติศาสตร์สถาบันบัณฑิตพัฒนาบริหารศาสตร์, 2559, หน้า 24-25

ที่ว่ากฎหมายอาญาต้องการ “หลักความชัดเจนแน่นอน” เนื่องจากการลงโทษทางอาญาเป็นมาตรการที่รุนแรงที่สุดของรัฐที่ใช้กับประชาชนในรัฐและเป็นเรื่องที่กระทบต่อชีวิต และสิทธิเสรีภาพของประชาชนโดยตรง

เมื่อสหพันธ์สาธารณรัฐเยอรมนีได้รับผลกระทบจากการก่ออาชญากรรมทางคอมพิวเตอร์เพิ่มมากขึ้น ฝ่ายนิติบัญญัติของสหพันธ์สาธารณรัฐเยอรมนีมีแนวความคิดว่าคดีอาชญากรรมทางคอมพิวเตอร์ โดยเฉพาะคดีที่มีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดนั้นเป็นการกระทำที่อยู่ในขอบเขตของกฎหมายอาญาที่ใช้บังคับอยู่แล้ว จึงได้บัญญัติความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์ เพิ่มไว้ในประมวลกฎหมายอาญา ความผิดที่กระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยตรงอันเป็นฐานความผิดพิเศษเกี่ยวกับคอมพิวเตอร์โดยเฉพาะ ซึ่งมีองค์ประกอบความผิดที่เปลี่ยนแปลงไปจากความผิดดั้งเดิม ก็บัญญัติเป็นฐานความผิดเพิ่มเติม ส่วนที่เป็นการกระทำความผิดประเภทที่อาศัยคอมพิวเตอร์เป็นเครื่องมือ โดยไม่มีองค์ประกอบความผิดแตกต่างไปจากความผิดดั้งเดิมที่กำหนดไว้ในประมวลกฎหมายอาญา โดยบัญญัติความผิดใหม่เพิ่มเติมเข้าไว้ในประมวลกฎหมายอาญา ได้แก่ ความผิดฐานจารกรรมข้อมูล ความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูล ความผิดฐานก่อวินาศกรรมทางคอมพิวเตอร์ความผิดฐานปลอมข้อมูลทางคอมพิวเตอร์ และความผิดฐานฉ้อโกงทางคอมพิวเตอร์

ประมวลกฎหมายอาญาสหพันธ์สาธารณรัฐเยอรมนี German Criminal Code 1974 แก้ไขเพิ่มเติม (StGB: Strafgesetzbuch) มีบทบัญญัติกำหนดฐานความผิดพิเศษเกี่ยวกับคอมพิวเตอร์ ซึ่งกำหนดไว้ใน Chapter 15 Violation of privacy of personal and private sphere โดยเฉพาะดังนี้

1. มาตรา 202a การจารกรรมข้อมูล

(1) ผู้ใดโดยไม่ได้รับอนุญาต ได้เข้าถึงโดยการหลีกเลี่ยงการป้องกันการเข้าถึงสำหรับตนเองหรือผู้อื่น ไปยังข้อมูลที่ได้รับการปกป้องเป็นพิเศษจากการเข้าถึงโดยไม่ได้รับอนุญาต ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับ

(2) เพื่อวัตถุประสงค์ของอนุมาตรา (1) ข้อมูลเป็นเพียงข้อมูลที่จัดเก็บหรือส่งทางอิเล็กทรอนิกส์หรือในลักษณะอื่นที่ไม่สามารถรับรู้ได้ในทันที[35]

2. มาตรา 202b การดักรับข้อมูลโดยมิชอบ ผู้ใดโดยไม่ได้รับอนุญาตให้ดำเนินการดังกล่าว ตาม (มาตรา 202a (2)) ซึ่งไม่ได้รับอนุญาต ไม่ว่าจะเพื่อตนเองหรือผู้อื่น โดยวิธีการ

---

[35] Section 202a StGB Data espionage

ทางเทคนิคจากการส่งข้อมูลที่ไม่เปิดเผยต่อสาธารณะหรือจากสถานที่ประมวลผลข้อมูล ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับ เว้นแต่ความผิดจะมีโทษหนักกว่านั้นตามบทบัญญัติอื่น[36]

3. มาตรา 202c การเตรียมการเพื่อจารกรรมข้อมูลและดักข้อมูล

(1) ผู้ใดเตรียมการกระทำความผิดตามมาตรา 202a หรือ 202b โดยได้มาเอง หรืออย่างอื่น ขาย จัดหาให้ผู้อื่น เผยแพร่หรือจัดให้มีในลักษณะอื่น ได้แก่

1. รหัสผ่านหรือรหัสความปลอดภัยอื่น ๆ ที่ให้การเข้าถึงข้อมูล (มาตรา 202a (2)) หรือ

2. โปรแกรมคอมพิวเตอร์เพื่อกระทำความผิดดังกล่าวต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับ

(2) มาตรา 149 (2) และ (3) ให้ใช้บังคับตามนั้น[37]

4. มาตรา 263a การฉ้อโกงทางคอมพิวเตอร์

(1) ผู้ใดโดยเจตนาเพื่อให้ได้มาซึ่งผลประโยชน์โดยมิชอบด้วยกฎหมายสำหรับตนเองหรือบุคคลอื่น ให้เกิดความเสียหายต่อทรัพย์สินของผู้อื่นโดยกระทำต่อผลการดำเนินการประมวลผลข้อมูลโดยกำหนดค่าโปรแกรมคอมพิวเตอร์ไม่ถูกต้อง ใช้ข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์ นำไปใช้โดยไม่ได้รับอนุญาต ของข้อมูลหรือการใช้อิทธิพลอื่น ๆ โดยไม่ได้รับอนุญาตในการประมวลผลต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับ

(2) มาตรา 263 (2) ถึง (6) ให้ใช้บังคับตามนั้น

(3) ผู้ใดจัดทำความผิดตามอนุมาตรา (1) โดยผลิตโปรแกรมคอมพิวเตอร์โดยมีวัตถุประสงค์เพื่อกระทำการดังกล่าว หรือจัดหาโปรแกรมดังกล่าวสำหรับตนเองหรือผู้อื่น หรือผู้ใดเสนอขายโปรแกรมดังกล่าว หรือถือหรือจัดส่งให้ผู้อื่น ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับ

(4) ในกรณีตามอนุมาตรา (3) มาตรา 149 (2) และ (3) ให้ใช้บังคับตามนั้น[38]

5. มาตรา 269 การปลอมแปลงข้อมูลซึ่งเป็นพยานหลักฐาน ความมั่นคงและความเชื่อถือในการใช้เป็นพยานหลักฐาน ความถูกต้องแท้จริงของข้อมูล

(1) ผู้ใด เพื่อวัตถุประสงค์ในการหลอกลวงทางการค้าตามกฎหมาย จัดเก็บหรือแก้ไขข้อมูลซึ่งมีมูลค่าที่พิสูจน์ได้ในลักษณะที่เอกสารปลอมแปลงหรือปลอมจะถูกสร้างขึ้น

---

[36] Section 202b StGB Phishing

[37] Section 202c StGB Acts preparatory to data espionage and phishing

[38] Section 263a StGB Computer fraud

เมื่อมีการค้นคืน หรือใครก็ตามที่ใช้ข้อมูลที่จัดเก็บหรือแก้ไขในข้อมูลดังกล่าว ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับ

(2) การพยายามกระทำความผิดต้องระวางโทษ

(3) มาตรา 267 (3) และ (4) ให้ใช้บังคับตามนั้น[39]

6. มาตรา 303a การลบ ปิดกั้นการทำงาน ทำให้ใช้ประโยชน์ไม่ได้ หรือแก้ไขเปลี่ยนแปลงข้อมูลโดยมิชอบ

(1) ผู้ใดลบ ระงับ ทำให้ใช้ไม่ได้หรือเปลี่ยนแปลงข้อมูลโดยมิชอบด้วยกฎหมาย (มาตรา 202a (2)) ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับ

(2) การพยายามกระทำความผิดต้องระวางโทษ[40]

7. มาตรา 303b การก่อวินาศกรรมคอมพิวเตอร์ ความปลอดภัยของระบบประมวลผลข้อมูล ความมั่งคงของประเทศ

(1) ผู้ใดขัดขวางการดำเนินการประมวลผลข้อมูลที่มีความสำคัญอย่างมากต่อผู้อื่นโดย

1. กระทำความผิดตามมาตรา 303ก (1)

2. การป้อนหรือส่งข้อมูล (มาตรา 202a (2)) โดยมีเจตนาที่จะส่งผลเสียต่อผู้อื่นหรือ

3. ทำลาย ทำให้เสียหาย ทำให้ใช้ไม่ได้ ลบหรือเปลี่ยนแปลงระบบประมวลผลข้อมูลหรือผู้ให้บริการข้อมูล ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับ

(2) หากการดำเนินการประมวลผลข้อมูลมีความสำคัญอย่างยิ่งต่อธุรกิจ องค์กร หรือหน่วยงานของผู้อื่น บทลงโทษคือจำคุกไม่เกินห้าปีหรือปรับ

(3) การพยายามกระทำความผิดต้องระวางโทษ

(4) ในกรณีร้ายแรงโดยเฉพาะตามอนุมาตรา (2) โทษจำคุกตั้งแต่หกเดือนถึง 10 ปี กรณีร้ายแรงโดยเฉพาะอย่างยิ่งมักเกิดขึ้นเมื่อผู้กระทำความผิด

1. ทำให้เกิดความสูญเสียทางการเงินครั้งใหญ่

2. กระทำการในเชิงพาณิชย์หรือเป็นสมาชิกของกลุ่มที่มีจุดประสงค์เพื่อก่อวินาศกรรมคอมพิวเตอร์อย่างต่อเนื่องหรือ

---

[39] Section 269 StGB Forgery of data intended to provide proof

[40] Section 303a StGB Data tampering

3. การกระทำความผิดเป็นอันตรายต่ออุปทานของประชากรด้วยสินค้าหรือบริการที่สำคัญหรือความมั่นคงของสหพันธ์สาธารณรัฐเยอรมนี

(5) มาตรา 202c ให้ใช้กับการกระทำความผิดตามอนุมาตรา (1)[41]

การกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ในการดำเนินกระบวนการทางวิธีพิจารณาความอาญาในประเทศเยอรมนี การสอบสวนและการรวบรวมพยานหลักฐาน มีวิธีการและหลักเกณฑ์เป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศเยอรมนี (The Code of Criminal Procedure)

บทบัญญัติเกี่ยวกับการค้นและการยึดพยานหลักฐานซึ่งใช้บังคับรวมถึงการค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

1. มาตรา 102 การตรวจค้นสถานที่และตัวผู้ต้องหา

การตรวจค้นร่างกาย การตรวจค้นทรัพย์สิน ส่วนตัว และสถานที่อื่น ๆ ของผู้กระทำความผิดหรือผู้มีส่วนร่วม ถูกสงสัยว่ากระทำความผิดหรือจัดการข้อมูลที่ถูกขโมย หรือถูกสงสัยว่าช่วยเหลือตามข้อเท็จจริงหรือขัดขวางการดำเนินคดี หรือการลงโทษหรือการจัดการของที่ขโมยมาอาจกระทำได้เพื่อความมุ่งหมายในการจับกุม รวมทั้งในกรณีที่อาจสันนิษฐานได้ว่าการค้นหาจะนำไปสู่การค้นพบหลักฐาน[42]

2. มาตรา 103 การค้นหาสถานที่ของบุคคลอื่น

(1) การค้นในส่วนที่เกี่ยวกับบุคคลอื่นจะยอมได้เฉพาะเพื่อวัตถุประสงค์ในการจับกุมผู้ต้องหาหรือเพื่อติดตามร่องรอยของการกระทำความผิดหรือเพื่อยึดสิ่งของบางอย่าง และเฉพาะในกรณีที่ข้อเท็จจริงว่าผู้ต้องหากระทำความผิด อยู่ในสถานที่ที่จะตรวจค้น เพื่อประโยชน์ในการจับกุมผู้ต้องหาซึ่งต้องสงสัยว่ากระทำความผิดตามมาตรา 89a หรือมาตรา 89c (1) ถึง (4) แห่งประมวลกฎหมายอาญาหรือตามมาตรา 129a รวมทั้งมาตรา 129b (1) แห่งประมวลกฎหมายอาญาด้วย ประมวลกฎหมายหรือความผิดอย่างหนึ่งอย่างใดที่กำหนดไว้ในบทบัญญัติดังกล่าว การตรวจค้นของเอกชนและสถานที่อื่น ๆ ให้กระทำได้หากตั้งอยู่ในอาคารที่อาจสันนิษฐานได้ว่าผู้ต้องหาอยู่ในสถานที่นั้น

(2) ข้อจำกัดของอนุมาตรา (1) ประโยค 1 ไม่ใช้บังคับกับสถานที่ซึ่งผู้ต้องหาถูกจับกุมหรือที่เขาเข้าไปในระหว่างการไล่ล่า[43]

---

[41] Section 303b StGB Computer sabotage

[42] Section 102 Search of accused's premises and person

[43] Section 103 Search of other persons' premises

3. มาตรา 104 การค้นในเวลากลางคืน

(1) สถานที่ส่วนตัว สถานที่ประกอบธุรกิจ และทรัพย์สินที่ปิดล้อม อาจถูกค้นในเวลากลางคืนได้เฉพาะเพื่อตามหาบุคคลที่ถูกจับในการกระทำ ในสถานการณ์เร่งด่วน หรือเพื่อวัตถุประสงค์ในการจับกุมนักโทษที่หลบหนีไปอีกครั้ง

(2) ข้อจำกัดนี้ไม่ใช้บังคับกับสถานที่ซึ่งทุกคนสามารถเข้าถึงได้ในเวลากลางคืนหรือที่ตำรวจรู้จักในฐานะที่พักพิงหรือสถานที่รวบรวมผู้กระทำความผิด เป็นคลังทรัพย์สินที่ได้มาจากการกระทำความผิด หรือเป็นที่หลบซ่อนสำหรับการเล่นการพนัน การค้ามนุษย์อย่างผิดกฎหมายในยาเสพติดหรืออาวุธ หรือการค้าประเวณี

(3) เวลากลางคืน ให้นับรวมในช่วงเวลาตั้งแต่ 1 เมษายน ถึง 30 กันยายน เวลาระหว่าง 21.00 น. ถึง 04.00 น. และในช่วงเวลาตั้งแต่ 1 ตุลาคม ถึง 31 มีนาคม ให้นับเวลาระหว่าง 21.00 น. ถึง 06.00 น.[44]

4. มาตรา 105 ขั้นตอนการค้น

(1) การตรวจค้นอาจทำได้โดยผู้พิพากษาเท่านั้น และในกรณีเร่งด่วนสำนักงานอัยการและพนักงานสอบสวน (มาตรา 152 แห่งพระราชบัญญัติรัฐธรรมนูญของศาล) การค้นตามมาตรา 103 (1) ให้ผู้พิพากษาสั่ง ในกรณีเร่งด่วน ให้สำนักงานอัยการมีอำนาจสั่งการตรวจค้นดังกล่าวได้

(2) ถ้าจะต้องค้นสถานที่ของเอกชน สถานที่ประกอบธุรกิจ หรือทรัพย์สินที่ปิดล้อมโดยที่ไม่มีผู้พิพากษาหรือพนักงานอัยการ ให้เรียกเจ้าหน้าที่เทศบาลหรือสมาชิกสองคนของชุมชนในเขตที่ทำการค้นนั้นเข้ามา ถ้าเป็นไปได้เพื่อช่วย ผู้ที่ถูกเรียกเข้ามาเป็นสมาชิกในชุมชนจะต้องไม่ใช่เจ้าหน้าที่ตำรวจหรือพนักงานสอบสวนของสำนักงานอัยการ

(3) หากจำเป็นต้องดำเนินการค้นหาในอาคารอย่างเป็นทางการหรือในสถานที่ติดตั้งหรือสถานที่ของกองกำลังสหพันธรัฐซึ่งไม่เปิดให้ประชาชนทั่วไปร้องขอให้ดำเนินการ การค้นหาดังกล่าว หน่วยงานที่ขอมีสิทธิเข้าร่วมได้ ไม่จำเป็นต้องมีคำขอดังกล่าวหากมีการค้นหาในสถานที่ซึ่งมีบุคคลอื่นอาศัยอยู่โดยเฉพาะนอกเหนือจากสมาชิกของกองกำลังสหพันธรัฐ[45]

---

[44] Section 104 Night-time search

[45] Section 105 Procedure for searches

5. มาตรา 106 การเรียกผู้ครองครองสถานที่ค้น

(1) ผู้ครอบครองสถานที่หรือผู้ครอบครองสิ่งของที่จะค้นอาจอยู่ในการตรวจค้นก็ได้ หากไม่อยู่ ให้เรียกตัวแทน ญาติผู้ใหญ่ ผู้ที่อาศัยอยู่ในบ้านหรือเพื่อนบ้าน ถ้าเป็นไปได้ จะถูกเรียกให้ช่วยเหลือ

(2) ในกรณีตามมาตรา 103 (1) ให้แจ้งวัตถุประสงค์ในการค้นหาให้ทราบแก่ผู้ครอบครองหรือบุคคลที่ถูกเรียกเข้ามาช่วยเหลือก่อนที่การค้นหาจะเริ่มต้นขึ้น บทบัญญัตินี้ไม่ใช้บังคับกับผู้อยู่อาศัยในสถานที่ที่ระบุไว้ในมาตรา 104 (2)[46]

6. มาตรา 107 การแจ้งเหตุผลในการค้นหา เมื่อเสร็จสิ้นการค้นหาผู้ที่ได้รับผลกระทบจะต้องได้รับแจ้งเป็นลายลักษณ์อักษรพร้อมระบุเหตุผลในการค้นหา (มาตรา 102 และ 103) และในกรณีตามมาตรา 102 ให้ระบุความผิด เมื่อได้รับการร้องขอ จะได้รับรายการสิ่งของซึ่งถูกอายัดหรือยึดไว้คืน หากไม่พบสิ่งที่น่าสงสัย ให้จัดทำใบรับรองการค้น[47]

7. มาตรา 127 การจับ โดยให้อำนาจแก่เจ้าพนักงานและราษฎรในการจับบุคคลในกรณีจำเป็นเร่งด่วน โดยไม่ต้องขอให้ศาลออกหมายจับก่อน ดังนี้[48]

(1) การจับเมื่อพบความผิดซึ่งหน้า เพื่อรักษาความสงบเรียบร้อยในบ้านเมืองและการนำตัวบุคคลมาดำเนินคดีอาญา หลักเกณฑ์ในการจับเมื่อพบความผิดซึ่งหน้ามีการพบผู้กระทำความผิดในขณะที่กระทำความผิดอยู่หรือขณะกำลังถูกไล่ตามอยู่ หรือไม่สามารถระบุตัวตนของผู้กระทำความผิดได้ หรือมีพฤติการณ์ว่าผู้กระทำความผิดจะหลบหนี ซึ่งการจับเมื่อพบความผิดซึ่งหน้าสามารถใช้กำลังได้เท่าที่จำเป็นและได้สัดส่วนเพื่อจะทราบตัวผู้ถูกจับและขัดขวางมิให้หลบหนี

(2) การจับโดยอาศัยเหตุจำเป็นเร่งด่วน ให้อำนาจเฉพาะอัยการและตำรวจ กรณีที่ปรากฏเหตุว่าหากรอไปขอหมายจากศาลอาจก่อให้เกิดความเสียหายได้

(3) การจับเพื่อการดำเนินคดีแบบเร่งรัด ให้อำนาจแก่อัยการและตำรวจ กรณีที่การกระทำความผิดนั้นสามารถดำเนินคดีแบบเร่งรัดได้ และศาลจะมีคำพิพากษาลงโทษผู้กระทำความผิดโดยไม่ช้า และผู้ถูกจับจะไม่มาปรากฏตัวในการพิจารณาคดีของศาล

การดำเนินคดีที่เกิดจากการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ของสหพันธ์สาธารณรัฐเยอรมนี มีการให้อำนาจแก่

---

[46] Section 106 Calling in occupant of premises to be searched

[47] Section 107 Notification of reason for search; inventory

[48] Section 127 Provisional arrest

1. อัยการ การดำเนินคดีอาญาชั้นสอบสวนเป็นความรับผิดชอบของอัยการ เมื่ออัยการสงสัยว่ามีการกระทำความผิดอาญาเกิดขึ้น ไม่ว่าจะด้วยการร้องทุกข์หรือด้วยวิธีการอื่นใด อัยการมีหน้าที่ต้องแสวงหาข้อเท็จจริงเพื่อนำไปสู่การตัดสินใจว่าจะฟ้องคดีอาญาหรือไม่ อัยการมีหน้าที่ในการรวบรวมข้อเท็จจริงทั้งที่เป็นโทษต่อผู้ถูกกล่าวหาและที่เป็นคุณต่อผู้ถูกกล่าวหา และมีหน้าที่รับผิดชอบการนำสืบพยานหลักฐาน การสอบสวนคดีอาญาของอัยการครอบคลุมไปจนถึงข้อเท็จจริงที่สำคัญต่อการกำหนดโทษด้วย ตามประมวลกฎหมายวิธีพิจารณาความอาญาของสหพันธ์สาธารณรัฐเยอรมนี (The Code of Criminal Procedure) โดยให้อำนาจอัยการในการสอบสวนข้อเท็จจริงเพื่อพิจารณาในการฟ้องคดี และสืบหาพฤติการณ์และข้อเท็จจริงทั้งที่เป็นโทษและเป็นคุณของผู้ถูกกล่าวหาซึ่งบัญญัติไว้ในมาตรา 160[49]

การดำเนินคดีอาญาในชั้นสอบสวนของสหพันธ์สาธารณรัฐเยอรมนี มีหลักการพื้นฐานอยู่ว่า อัยการมีความเป็นอิสระในการที่จะเลือกใช้มาตรการบังคับในทางอาญามาตรการใดก็ได้ และจะใช้มาตรการใดก่อนหรือหลังก็ได้ หรือที่เรียกกันว่า “หลักความเป็นอิสระในการจัดรูปแบบการสอบสวน” บัญญัติไว้ในมาตรา 161 มีอำนาจในการเรียกข้อมูลจากหน่วยงานใดๆ ในการสอบสวนคดีอาญาด้วยวิธีการใดๆ โดยจะดำเนินการด้วยตนเองหรือให้ตำรวจดำเนินการก็ได้ ซึ่งตำรวจมีหน้าที่ปฏิบัติตามคำสั่งอัยการและมีอำนาจเรียกข้อมูลจากหน่วยงานอื่นด้วยเช่นกัน ยกตัวอย่างเช่น ในคดีลักทรัพย์ในเคหะสถาน อัยการสามารถสั่งให้ตำรวจสอบปากคำผู้เสียหายเกี่ยวกับจำนวน แหล่งที่มา ราคา ตำหนิและวิธีการเก็บรักษาทรัพย์ที่ถูกลักไป รวมไปถึงว่ามีผู้ใดบ้างหรือไม่ที่รู้ที่ซ่อนของทรัพย์นั้น รวมถึงเวลาเกิดเหตุและการรับรู้เหตุการณ์อื่นๆ เช่น เสียงหรือแสงไฟ เป็นต้น นอกจากนั้น อัยการยังสามารถขอให้ตำรวจตรวจหาร่องรอยต่างๆ โดยเฉพาะอย่างยิ่งลายนิ้วมือในที่เกิดเหตุ อาจมีการสอบปากคำผู้ที่อยู่ในบ้านนั้นว่าได้ยินหรือได้เห็นอะไรบ้างหรือไม่ รวมไปถึงผู้ที่อาศัยอยู่ในบริเวณใกล้เคียง หรือร้านขายของเก่า หรืออาจมีการลงโฆษณาในหนังสือพิมพ์เพื่อหาเบาะแสของทรัพย์ที่ถูกขโมยไปก็ได้ นอกจากนี้อัยการยังมีอำนาจในการสั่งการตรวจค้นในกรณีเร่งด่วนได้ การค้นในส่วนที่เกี่ยวกับบุคคลอื่น เพื่อวัตถุประสงค์ในการจับกุมผู้ต้องหาหรือเพื่อติดตามร่องรอยของการกระทำความผิดหรือเพื่อยึดสิ่งของบางอย่างและเฉพาะในกรณีที่ข้อเท็จจริงว่าผู้ต้องหากระทำความผิด อยู่ในสถานที่ที่จะตรวจค้น เพื่อประโยชน์ในการจับกุมผู้ต้องหาซึ่งต้องสงสัยว่ากระทำความผิดซึ่งบัญญัติไว้ในมาตรา 105 (1) ประกอบกับมาตรา 103 (1)[50]

---

[49] กรรภิรมย์ โกมลาร.(2561).วารสารวิชาการ คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย.ปีที่ 10 ฉบับที่ 1 มิถุนายน 2561, หน้า 13-14

[50] เรื่องเดียวกัน.

2. สำนักงานตำรวจอาชญากรรมแห่งสหพันธ์สาธารณรัฐเยอรมนี Bundeskriminalamt (BKA) เป็นหน่วยงานตำรวจสืบสวนกลางของสหพันธ์สาธารณรัฐเยอรมนี ซึ่งอยู่ภายใต้สังกัดกระทรวงมหาดไทย มีอำนาจประสานงานความร่วมมือระหว่างสหพันธ์รัฐและกองกำลังตำรวจของรัฐ การสืบสวนคดีอาชญากรรมระหว่างประเทศ การก่อการร้าย และคดีอื่น ๆ ที่เกี่ยวข้องกับความมั่นคงของชาติ การต่อต้านการก่อการร้าย การคุ้มครองสมาชิกของสถาบันรัฐธรรมนูญและพยานของรัฐบาลกลาง เมื่อได้รับการร้องขอจากหน่วยงานของรัฐที่เกี่ยวข้องหรือรัฐมนตรีกระทรวงมหาดไทยของรัฐบาลกลาง หน่วยงานดังกล่าวจะรับผิดชอบในการสอบสวนกรณีขนาดใหญ่บางกรณี นอกจากนี้ อัยการสูงสุดของเยอรมนียังสามารถสั่งให้สอบสวนกรณีที่เป็นผลประโยชน์สาธารณะเป็นพิเศษ ซึ่งในสำนักงานได้มีการจัดตั้งแผนก Cybercrime มีหน้าที่หลักในการสืบสวนในด้านอาชญากรรมทางคอมพิวเตอร์ การสืบสวนบุคคลและเครือข่ายที่กำหนดเป้าหมายที่มีชื่อเสียงในสหพันธ์สาธารณรัฐเยอรมนีการรวบรวมและวิเคราะห์ข้อมูลเพื่อช่วยในการตรวจสอบอย่างต่อเนื่อง การต่อสู้กับการโจมตีทางไซเบอร์กับโครงสร้างพื้นฐานและสถาบันที่สำคัญของรัฐบาลเยอรมัน การให้คำปรึกษาในการพัฒนากลยุทธ์และกรอบกฎหมายในการต่อสู้กับอาชญากรรมทางอินเทอร์เน็ต[51]

สหพันธ์สาธารณรัฐเยอรมนีให้ความสำคัญกับการคุ้มครองสิทธิส่วนบุคคลและสิทธิเสรีภาพของประชาชน เห็นได้จากการบัญญัติกฎหมายที่เกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ได้บัญญัติรวมไว้ในประมวลกฎหมายอาญา เพื่อให้มีความชัดเจนแน่นอน โดยมุ่งเน้นการปราบปรามอาชญากรรมที่กระทำความผิดโดยอาศัยคอมพิวเตอร์เป็นเครื่องมือ ในส่วนของการค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ การปฏิบัติหน้าที่ของเจ้าพนักงานหรือเจ้าหน้าที่ตำรวจ และอัยการ เป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญาของสหพันธ์สาธารณรัฐเยอรมนี(The Code of Criminal Procedure) ซึ่งจะกระทำได้ก็แต่อาศัยอำนาจแห่งกฎหมาย การค้นเคหสถานจะกระทำได้ก็แต่โดยคำสั่งของผู้พิพากษา และการค้นจะต้องกระทำในลักษณะที่กฎหมายบัญญัติไว้เท่านั้น

---

[51] Federal Criminal Police Office (Germany),/ 2014,/สืบค้นเมื่อวันที่ 24 มิถุนายน 2565.จากเว็บไซต์: (https://en.wikipedia.org/wiki/Federal_Criminal_Police_Office_(Germany)

## 3. ศึกษาวิเคราะห์เปรียบเทียบกฎหมายไทยและกฎหมายต่างประเทศ

### 3.1 กฎหมายไทยเปรียบเทียบกับกฎหมายของสหรัฐอเมริกา

เมื่อเปรียบเทียบกฎหมายการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทยกับกฎหมายสหรัฐอเมริกามีความคล้ายคลึงกันโดยมีบทบัญญัติกฎหมายที่ดำเนินการกับผู้ที่กระทำความผิดทางคอมพิวเตอร์ ในกฎหมายไทยมีบทบัญญัติพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ในสหรัฐอเมริกาก็มีบัญญัติกฎหมาย Computer Fraud and Abuse Act (CFAA) กำหนดการเข้าถึงข้อมูลคอมพิวเตอร์ ซึ่งเน้นไปในทางกำหนดโทษกับผู้ที่กระทำความผิดเช่นเดียวกับบทบัญญัติกฎหมายไทย

การดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ในสหรัฐอเมริกามีการจัดตั้งหน่วยงานศูนย์รับเรื่องร้องเรียนอาชญากรรมทางอินเทอร์เน็ตของ FBI (the Internet Crime Complaint Center) มีภารกิจอำนวยความสะดวกให้ประชาชนสามารถรายงานเกี่ยวกับกิจกรรมที่ต้องสงสัยว่าเป็นอาชญากรทางอิเล็กทรอนิกส์ และหน่วยงาน Cyber security Infrastructure Security Agency (CISA) มีบทบาทในการรักษาความปลอดภัยทางไซเบอร์จากภัยคุกคามทางไซเบอร์ การค้น การยึดพยานหลักฐานที่เกิดจากการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ มีการให้อำนาจแก่ อัยการ และพนักงานสืบสวนสอบสวน ในการค้นพยานหลักฐานอิเล็กทรอนิกส์ การกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ ในส่วนประเทศไทยมีการจัดตั้งหน่วยงานกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี Technology Crime Suppression Division (TCSD) มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อยป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวน ปฏิบัติงานตามประมวลกฎหมาย วิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์[52] และได้มีการจัดตั้งหน่วยงานกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) Cyber Crime Investigation Bureau (CCIB) มีอำนาจหน้าที่ ในการวางแผน ควบคุม ตรวจสอบ ให้คำแนะนำ และเสนอแนะการปฏิบัติงาน ดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วราชอาณาจักร ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อันเป็นความผิดทางอาญาเกี่ยวกับอาชญากรรมทางเทคโนโลยี ดำเนินการเกี่ยวกับการสืบสวน

---

[52] กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี,/ประวัติหน่วยงาน/2552,/สืบค้นเมื่อวันที่ 9 มิถุนายน 2565. จากเว็บไซต์: (https://www.tcsd.go.th/เกี่ยวกับหน่วยงาน)

สอบสวนคดีอาชญากรรมทางเทคโนโลยีโดยการใช้เทคโนโลยีสารสนเทศและเครื่องมือพิเศษสนับสนุนส่วนราชการ หรือหน่วยงานอื่นในการสืบสวนสอบสวน ดำเนินการเกี่ยวกับการรวบรวมข้อมูล ตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี ดำเนินการเกี่ยวกับการพิสูจน์หลักฐานดิจิทัล การตรวจสถานที่เกิดเหตุและเก็บรวบรวมพยานหลักฐานดิจิทัลเพื่อสนับสนุนการปฏิบัติงานสืบสวนสอบสวนของหน่วยงานต่าง ๆ[53] และในกรณีที่มีการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ ในความผิดที่มีลักษณะเป็นคดีพิเศษ ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ประเทศไทยกำหนดให้อำนาจแก่พนักงานสอบสวนคดีพิเศษ (DSI) ในการดำเนินการสืบสวนสอบสวนโดยใช้วิธีการพิเศษ

การค้นและยึดคอมพิวเตอร์และการได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์ในการสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ในสหรัฐอเมริกา กฎหมายว่าด้วยวิธีพิจารณาความอาญาของสหรัฐอเมริกา ให้อำนาจพนักงานสอบสวนและอัยการในการค้นหาพยานหลักฐานที่อยู่ในความครอบครองของบุคคลใดในที่รโหฐานต้องมีหมายค้นและมีเหตุอันควรหรือมีความสมเหตุสมผลที่จะขอให้ศาลออกหมายค้น เนื่องจากสหรัฐอเมริกาให้ความสำคัญต่อการคุ้มครองการล่วงละเมิดต่อสิทธิส่วนบุคคล ไม่ให้เจ้าหน้าที่ตำรวจค้นและยึดพยานหลักฐานโดยผิดกฎหมายหรือขัดกับรัฐธรรมนูญ แต่ก็มีการกำหนดข้อยกเว้นในกรณีที่ไม่ต้องขอหมายค้น ในกรณีที่ได้รับความยินยอมจากเจ้าของข้อมูล หรือ ในกรณีมีเหตุฉุกเฉิน เพื่อป้องกันการทำลายพยานหลักฐาน ในส่วนของประเทศไทย บทบัญญัติกฎหมายวิธีพิจารณาความอาญาในประเทศไทยที่กำหนดให้การค้นของเจ้าพนักงานในที่รโหฐานต้องมีหมายค้น แต่บทบัญญัติพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ในประเทศไทย กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจในการสืบสวนสอบสวนนอกเหนือจากอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งได้กำหนดอำนาจของพนักงานเจ้าหน้าที่ที่ไม่ต้องขออนุญาตศาล ได้แก่ อำนาจเรื่องทั่วไปในการรวบรวมพยานหลักฐานซึ่งอาจทำโดยวิธีการมีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือหรือส่งเอกสาร ข้อมูลทั่วไปไม่รวมถึงข้อมูลคอมพิวเตอร์ อำนาจเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลที่เกี่ยวข้อง สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการหรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงาน

---

[53] กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี,/ อำนาจหน้าที่/2020,/สืบค้นเมื่อวันที่ 9 มิถุนายน 2565. จากเว็บไซต์: (https://www.ccib.go.th/เกี่ยวกับหน่วยงาน/อำนาจหน้าที่)

เจ้าหน้าที่ และกำหนดการใช้อำนาจของพนักงานเจ้าหน้าที่ต้องขออนุญาตศาลตามวิธีการที่กฎหมายบัญญัติไว้ก่อน ได้แก่ การเจาะระบบเพื่อให้ทราบถึงระบบคอมพิวเตอร์ที่ใช้ในการกระทำความผิด เพื่อให้ได้พยานหลักฐานเกี่ยวกับการกระทำความผิดที่กระทำผ่านระบบคอมพิวเตอร์ การสั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลหรืออุปกรณ์ให้แก่พนักงานเจ้าหน้าที่ ดำเนินการถอดรหัสลับหรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับทำการถอดรหัสลับ การใช้อำนาจในการยึดอายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำผิด และในกรณีที่มีการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ ในความผิดที่มีลักษณะเป็นคดีพิเศษ ที่มีผลกระทบและสร้างความเสียหายอย่างร้ายแรง ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ประเทศไทยกำหนดให้อำนาจแก่พนักงานสอบสวนคดีพิเศษ (DSI) ในการดำเนินการสืบสวนสอบสวนโดยใช้วิธีการพิเศษ ได้แก่ อำนาจการเข้าไปในเคหสถานหรือสถานที่ใด ๆ เพื่อตรวจค้น โดยไม่มีหมายค้น อำนาจในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ และมีอำนาจให้บุคคลใดจัดทำเอกสารหรือหลักฐานใดขึ้นหรือเข้าไปแฝงตัวในองค์กรหรือกลุ่มคนใด เพื่อประโยชน์ในการสืบสวนสอบสวน และการกระทำดังกล่าวถือว่าเป็นการกระทำโดยชอบ

**3.2 กฎหมายไทยเปรียบเทียบกับกฎหมายสหพันธ์สาธารณรัฐเยอรมนี**

เมื่อเปรียบเทียบกฎหมายการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทยกับกฎหมายสหพันธ์สาธารณรัฐเยอรมนี ประเทศไทยได้มีการตรากฎหมาย ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งได้มีการกำหนดฐานความผิดเกี่ยวกับคอมพิวเตอร์และกำหนดให้อำนาจแก่เจ้าหน้าที่เป็นการเฉพาะในการดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว แตกต่างจากสหพันธ์สาธารณรัฐเยอรมนีซึ่งฝ่ายนิติบัญญัติมีแนวคิดว่าการกระทำใดที่เป็นความผิดทางอาญาและกระทบคุณธรรมทางกฎหมายจะต้องบัญญัติความผิดและมาตรการบังคับทางอาญาไว้ในประมวลกฎหมายอาญา เพื่อให้เกิดความชัดเจน ในส่วนคดีอาชญากรรมทางคอมพิวเตอร์ จึงได้มีการบัญญัติไว้ในประมวลกฎหมายอาญาสหพันธ์สาธารณรัฐเยอรมนี German Criminal Code 1974 เนื่องจากคดีที่มีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดนั้นเป็นการกระทำที่อยู่ในขอบเขตของกฎหมายอาญาที่ใช้บังคับอยู่แล้ว จึงได้บัญญัติความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์ เพิ่มไว้ในประมวลกฎหมายอาญา ซึ่งลักษณะของฐานความผิดมีความคล้ายกับกฎหมายประเทศไทย

การรวบรวมพยานหลักฐานในคดีเกี่ยวกับคอมพิวเตอร์ของสหพันธ์สาธารณรัฐเยอรมนีไม่มีกฎหมายเฉพาะมารองรับ กระบวนการจับ การค้น การควบคุม มีวิธีการและหลักเกณฑ์เป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญาของสหพันธ์สาธารณรัฐเยอรมนี (The Code of Criminal Procedure) แตกต่างจากประเทศไทยที่มีกฎหมายบัญญัติให้อำนาจแก่เจ้าหน้าที่ ทั้งในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และประมวลกฎหมายวิธีพิจารณาความอาญา แต่การใช้อำนาจของเจ้าหน้าที่จะกระทำได้ก็แต่อาศัยอำนาจแห่งกฎหมาย และศาลจะเป็นผู้มีอำนาจในการตรวจสอบ และจะต้องกระทำในลักษณะที่กฎหมายบัญญัติไว้เท่านั้น แต่ก็มีข้อยกเว้นในการจับบุคคล โดยไม่ต้องขอให้ศาลออกหมายจับก่อนเมื่อพบความผิดซึ่งหน้า เพื่อรักษาความสงบเรียบร้อยในบ้านเมือง หรือการจับโดยอาศัยเหตุจำเป็นเร่งด่วน การจับเพื่อการดำเนินคดีแบบเร่งรัด ให้อำนาจแก่อัยการและตำรวจ กรณีที่การกระทำความผิดนั้นสามารถดำเนินคดีแบบเร่งรัดได้ คล้ายกับกฎหมายไทยในมาตรา 78 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ให้อำนาจพนักงานฝ่ายปกครองหรือตำรวจสามารถกระทำได้โดยไม่มีหมายจับเมื่อมีหลักฐานหรือมีเหตุอันควรเชื่อตามสมควร นอกจากนั้นพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มาตรา 18 (1)-(3)ได้ให้อำนาจพนักงานเจ้าหน้าที่ซึ่งไม่ต้องขออนุญาตศาล ในการสืบสวนสอบสวนบรรดาความผิดอาญาที่ได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือส่วนหนึ่งในการกระทำความผิดตามกฎหมายอื่น ได้แก่ อำนาจเรื่องทั่วไปในการรวบรวมพยานหลักฐาน อำนาจเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลที่เกี่ยวข้อง สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการหรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการ

การดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ในสหพันธ์สาธารณรัฐเยอรมนี การสอบสวนได้ให้อำนาจแก่อัยการสืบหาพฤติการณ์และข้อเท็จจริงเพื่อพิจารณาในการฟ้องคดีและมีอำนาจในการเรียกข้อมูลจากหน่วยงาน ในการสอบสวน ซึ่งจะดำเนินการด้วยตนเองหรือให้ตำรวจดำเนินการก็ได้ มีการบัญญัติให้อำนาจอัยการในการดำเนินคดีอาญาในชั้นสอบสวนมีความเป็นอิสระในการที่จะเลือกใช้มาตรการบังคับในทางอาญามาตรการใดก็ได้ และจะใช้มาตรการใดก่อนหรือหลังก็ได้ และมีอำนาจในการสั่งการตรวจค้นในกรณีเร่งด่วนได้ แตกต่างจากประเทศไทยในขั้นตอนการดำเนินการสืบสวนสอบสวนจะเป็นหน้าที่ของตำรวจในการสืบหาพยานหลักฐานเพื่อเสนอให้อัยการเป็นผู้พิจารณาฟ้องคดี แต่หากพยานหลักฐานไม่เพียงพออัยการสามารถให้ตำรวจสืบหาพยานเพิ่มเติมได้ อัยการจะไม่ดำเนินการสืบหา

พยานหลักฐานโดยตรง สหพันธ์สาธารณรัฐเยอรมนีได้มีสำนักงานตำรวจอาชญากรรมแห่งสหพันธรัฐเยอรมนี Bundeskriminalamt (BKA) เป็นหน่วยงานตำรวจสืบสวนกลางของเยอรมนี มีหน้าที่หลักในการสืบสวนในด้านอาชญากรรมทางคอมพิวเตอร์ เช่นเดียวกับประเทศไทยมีการจัดตั้งหน่วยงานกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี Technology Crime Suppression Division (TCSD) และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) Cyber Crime Investigation Bureau (CCIB) ที่ดำเนินการเกี่ยวกับการสืบสวนสอบสวนและป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วราชอาณาจักร และกรณีที่มีการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ ในความผิดที่มีลักษณะเป็นคดีพิเศษ ที่มีผลกระทบและสร้างความเสียหายอย่างร้ายแรง ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ประเทศไทยกำหนดให้อำนาจแก่พนักงานสอบสวนคดีพิเศษ (DSI)

**3.3 ตารางเปรียบเทียบกฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทยและกฎหมายต่างประเทศ**

| | กฎหมายไทย | กฎหมายสหรัฐอเมริกา | กฎหมายสหพันธ์สาธารณรัฐเยอรมนี |
|---|---|---|---|
| กฎหมายเกี่ยวกับการการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ | 1.พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550<br>2.พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560<br>3.บทบัญญัติกฎหมายวิธีพิจารณาความอาญา<br>4. พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 | บัญญัติกฎหมาย Computer Fraud and Abuse Act (CFAA) | ไม่มีกฎหมายเฉพาะ ได้บัญญัติความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์ เพิ่มเติมในประมวลกฎหมายอาญาสหพันธ์สาธารณรัฐเยอรมนี German Criminal Code 1974 และการดำเนินคดีเป็นไปตามหลักเกณฑ์ในประมวลกฎหมายวิธีพิจารณาความอาญาของสหพันธ์สาธารณรัฐเยอรมนี (The Code of Criminal Procedure) |
| ผู้มีอำนาจเกี่ยวกับการดำเนินคดีกับผู้ที่กระทำความผิดทางคอมพิวเตอร์ | - พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์<br>- เจ้าพนักงาน ตามประมวลกฎหมายอาญา<br>-กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีTechnologyCrimeSuppression Division (TCSD) | - ศูนย์รับเรื่องร้องเรียนอาชญากรรมทางอินเทอร์เน็ตของ FBI (the Internet Crime Complaint Center)<br>- Cybersecurity Infrastructure Security Agency (CISA) | - พนักงานอัยการ : การดำเนินคดีอาญาชั้นสอบสวนเป็นความรับผิดชอบของอัยการ มีอิสระในการที่จะเลือกใช้มาตรการบังคับในทางอาญา หลักความเป็นอิสระในการจัดรูปแบบการสอบสวน<br>- สำนักงานตำรวจอาชญากรรมแห่งสหพันธ์สาธารณรัฐเยอรมนี Bundeskriminalamt (BKA) ในสำนักงานได้มีการจัดตั้งแผนก |

| | กฎหมายไทย | กฎหมายสหรัฐอเมริกา | กฎหมายสหพันธ์สาธารณรัฐเยอรมนี |
|---|---|---|---|
| | -กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) Cyber Crime Investigation Bureau (CCIB)<br>-กรมสอบสวนคดีพิเศษ ( DEPARTMENT OF SPECIAL INVESTIGATION : DSI) | | Cybercrime มีหน้าที่หลักในการสืบสวนในด้านอาชญากรรมทางคอมพิวเตอร์ |
| ข้อยกเว้นในกรณีที่ไม่ต้องขอหมายจับ หมายค้น | - การกระทำความผิดซึ่งหน้าหรือเหตุจำเป็นอย่างอื่นที่ไม่สามารถออกหมายจับได้ทัน<br>- การค้น ตามประมวลกฎหมายวิธีพิจารณาความอาญา<br>1. เมื่อมีเสียงหรือพฤติการณ์แสดงให้เห็นว่ามีเหตุร้าย<br>2. เมื่อปรากฏความผิดซึ่งหน้ากำลังกระทำลงในที่รโหฐาน<br>3. เมื่อบุคคลที่ได้กระทำความผิดซึ่งหน้าขณะที่ถูกไล่จับหนีเข้าไปหรือมีเหตุควรสงสัยว่าได้เข้าไปซุกซ่อนตัวอยู่ในที่รโหฐานนั้น<br>4. เพื่อป้องกันการทำลายพยานหลักฐาน<br>5. เมื่อที่รโหฐานนั้นผู้จะต้องถูกจับเป็นเจ้าบ้านและการจับนั้นมีหมายจับหรือจับตามมาตรา 78 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา<br>-พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มาตรา 18 (1)-(3) ได้ให้อำนาจพนักงานเจ้าหน้าที่ซึ่งไม่ต้องขออนุญาตศาล<br>-พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 24 (1) การเข้าไปในเคหสถานหรือสถานที่ใด ๆ เพื่อตรวจค้น โดยไม่มีหมายค้น | 1.ความยินยอม<br>2. กรณีมีเหตุฉุกเฉินเพื่อป้องกันการทำลายพยานหลักฐาน | - กรณีเร่งด่วน ให้สำนักงานอัยการมีอำนาจสั่งการตรวจค้นได้<br>- การจับบุคคล โดยไม่ต้องขอให้ศาลออกหมายจับก่อนเมื่อพบความผิดซึ่งหน้า เพื่อรักษาความสงบเรียบร้อยในบ้านเมือง หรือการจับโดยอาศัยเหตุจำเป็นเร่งด่วน การจับเพื่อการดำเนินคดีแบบเร่งรัด ให้อำนาจแก่อัยการและตำรวจ กรณีที่การกระทำความผิดนั้นสามารถดำเนินคดีแบบเร่งรัดได้ |

# บทที่ 4
# ปัญหาทางกฎหมายของการดำเนินคดีอาญา ศึกษากรณีการค้น การยึด พยานหลักฐาน ที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

ปัญหาในการดำเนินคดีอาญากับผู้ที่กระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ เป็นปัญหาที่เกิดกับผู้ที่บังคับใช้กฎหมายทั่วโลก เนื่องจากการก่ออาชญากรรมทางคอมพิวเตอร์มีความยากต่อการตรวจพบพยานหลักฐาน และยากต่อการพิสูจน์ความรับผิด การกระทำความผิดมีวิธีการที่ซับซ้อนและผู้กระทำความผิดมักเป็นบุคคลที่มีความรู้ในด้านเทคโนโลยีเป็นอย่างดี และไม่สามารถหาตัวตนที่อยู่แน่นอนได้ทำให้ลำบากในการเข้าถึงตัวผู้กระทำความผิด

จะเห็นได้ว่าปัญหาในการดำเนินคดีกับผู้ที่กระทำความผิด การแสวงหาข้อเท็จจริงและพยานหลักฐาน เพื่อนำมาค้นหาความจริงอันเกี่ยวกับการกระทำความผิดและการนำตัวผู้กระทำความผิดมาดำเนินการพิจารณาและลงโทษตามบทบัญญัติของกฎหมายไทยยังคงมีปัญหาอยู่ จึงจำเป็นที่จะต้องวิเคราะห์ถึงสภาพปัญหาและมาตรการทางกฎหมายที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของต่างประเทศ เพื่อศึกษาแนวคิดในการค้น การยึดของกฎหมายต่างประเทศ เพื่อเป็นแนวทางในการแก้ไขปัญหากฎหมายเกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทย

## 1. ปัญหาการดำเนินคดีอาญา กรณีการค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

การกระทำความผิดทางคอมพิวเตอร์เป็นการกระทำความผิดที่ผู้กระทำมีความรู้ความเชี่ยวชาญทางคอมพิวเตอร์ จึงเป็นเรื่องยากในการสืบค้นพยานหลักฐาน เนื่องจากพยานหลักฐานอิเล็กทรอนิกส์ เป็นข้อมูลที่สามารถทำลายหรือแก้ไขได้โดยง่ายและใช้ระยะเวลาสั้น ผู้กระทำความผิดสามารถรู้ถึงการค้นพยานหลักฐานก็จะทำลายหรือแก้ไขได้ทันที การสืบค้นจึงต้องใช้ความรวดเร็วและความชำนาญของเจ้าหน้าที่

จากการศึกษาแนวคิดทฤษฎีรูปแบบกระบวนการยุติธรรมทางอาญาและกฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทยยังมีปัญหาในส่วนของความล่าช้าของการค้นและการยึดพยานหลักฐานอิเล็กทรอนิกส์ ซึ่งการค้นหาพยานหลักฐานเป็นเครื่องมือในการดำเนินคดีอาญาที่สำคัญและจำเป็น เพื่อให้ได้มาซึ่งพยานหลักฐาน เป็นการดำเนินการของเจ้าพนักงานของรัฐที่กฎหมายอนุญาตให้เข้าไปแสวงหาพยานหลักฐานต่างๆ จากตัวบุคคล สิ่งของ ในกรณีของการกระทำความผิดทางคอมพิวเตอร์เพื่อที่จะได้ของพยานหลักฐานมีความจำเป็นที่จะต้องตรวจค้น ข้อมูลทางคอมพิวเตอร์ เครื่องคอมพิวเตอร์จากผู้ใช้งานหรือผู้ครอบครองคอมพิวเตอร์หรือข้อมูลในระบบคอมพิวเตอร์ ซึ่งตามกฎหมายไทยในส่วนของการค้นและการยึดพยานหลักฐานทางคอมพิวเตอร์ได้มีการบัญญัติไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และบทบัญญัติกฎหมายวิธีพิจารณาความอาญา

การค้นข้อมูลอิเล็กทรอนิกส์เพื่อให้ได้มาของพยานหลักฐานโดยไม่มีการรุกล้ำเข้าไปในที่รโหฐานแต่ก็ถือว่าเป็นการล่วงล้ำเข้าไปในพื้นที่ส่วนบุคคลของผู้อื่นก็ต้องใช้หมายค้นเช่นเดียวกัน บทบัญญัติกฎหมายวิธีพิจารณาความอาญามาตรา 92 การค้นในที่รโหฐาน พนักงานฝ่ายปกครองหรือตำรวจ และพนักงานสอบสวนต้องมีหมายค้นหรือคำสั่งศาล แม้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์(ฉบับที่ 2) พ.ศ. 2560 มาตรา 18 (1)-(3) ได้กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจในการสืบสวนสอบสวนนอกเหนือจากอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา การให้อำนาจพนักงานเจ้าหน้าที่ซึ่งไม่ต้องขออนุญาตศาลแต่ก็เป็นอำนาจเรื่องทั่วไปโดยวิธีการมีหนังสือสอบถามหรือเรียกบุคคลมาให้ถ้อยคำหรือส่งคำชี้แจ้งเป็นหนังสือหรือเอกสาร แต่ไม่รวมถึงข้อมูลคอมพิวเตอร์ ในการเข้าถึงข้อมูลคอมพิวเตอร์เพื่อให้ทราบถึงระบบคอมพิวเตอร์ที่ใช้ในการกระทำความผิดเพื่อให้ได้พยานหลักฐานเกี่ยวกับการกระทำความผิดที่กระทำผ่านระบบคอมพิวเตอร์ ซึ่งเป็นการสืบสวนหาตัวผู้กระทำความผิดเมื่อพนักงานเจ้าหน้าที่ได้ไปกระทำจากระบบคอมพิวเตอร์ถือว่าเป็นการล่วงล้ำเข้าไปในข้อมูลคอมพิวเตอร์ พนักงานเจ้าหน้าที่จะกระทำได้ก็ต่อเมื่อได้รับอนุญาตจากศาลก่อน ตามมาตรา 18 (4)-(8)

การใช้อำนาจในการยึดอายัดระบบคอมพิวเตอร์พนักงานเจ้าหน้าที่จะกระทำได้เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำผิด และต้องได้รับอนุญาตจากศาลและจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์ไว้เป็นหลักฐานและจะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ หากมี

กรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานเกินสามสิบวัน พนักงานเจ้าหน้าที่ต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายระยะเวลาการยึดหรืออายัด แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยเร็ว

การยื่นคำร้องจะต้องยื่นต่อศาลที่มีเขตอำนาจตามพระธรรมนูญศาลยุติธรรมและกฎหมายว่าด้วยการจัดตั้งศาล การยื่นคำร้องในคดีความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งเป็นคดีอาญาจึงต้องยื่นต่อศาลชั้นต้นที่มีอำนาจพิจารณาพิพากษาคดีอาญาและมีเขตอำนาจในคดีที่บุคคลใดกระทำหรือกำลังจะกระทำความผิด ถ้าศาลเห็นสมควรให้มีการไต่สวนคำร้องก่อนมีคำสั่งก็ได้ เมื่อได้รับคำสั่งอนุญาตจากศาลให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีคำสั่งอนุญาตคำร้องภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เท่านั้นที่มีอำนาจและต้องยื่นคำร้องด้วยตนเอง ตามมาตรา 19

ปัญหาในการขอออกหมายค้นที่พนักงานเจ้าหน้าที่จะต้องปฏิบัติตามที่กฎหมายบัญญัติเพื่อให้ได้พยานหลักฐานทางคอมพิวเตอร์อย่างถูกต้องตามกฎหมาย โดยต้องมีหมายค้นในการออกหมายค้นกฎหมายกำหนดให้ศาลเป็นผู้มีอำนาจในการพิจารณาตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่เพียงผู้เดียวแต่ขั้นตอนในการดำเนินการขอหมายค้นและการอนุมัติหมายค้นของศาลเป็นขั้นตอนที่ล่าช้า พยานหลักฐานทางคอมพิวเตอร์อาจถูกเปลี่ยนแปลงหรือทำลาย แม้ประเทศไทยจะมีการจัดตั้งหน่วยงานกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) Cyber Crime Investigation Bureau (CCIB) และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี TechnologyCrime Suppression Division (TCSD) แต่ก็ยังไม่สามารถแก้ปัญหาในการดำเนินคดีอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ได้เท่าที่ควร การสืบสวนติดตามผู้กระทำความผิดอย่างต่อเนื่องการพิสูจน์ตัวบุคคลผู้ส่งและผู้รับข้อมูลทางคอมพิวเตอร์เป็นเรื่องที่ยาก และส่วนใหญ่แล้วการกระทำความผิดเกิดขึ้นในสถานที่ปกปิดมิดชิดเจ้าหน้าที่ตำรวจจึงจำเป็นต้องมีหมายค้นเข้าไปตรวจสอบการกระทำความผิดขั้นตอนและการรวบรวมพยานหลักฐาน ในการขอหมายค้นจากศาลต้องใช้ระยะเวลานานพอสมควร ซึ่งระยะเวลาที่พนักงานสอบสวนใช้ในการขอหมายศาลก็จะเป็นระยะเวลาที่จะเปิดโอกาสให้ผู้กระทำความผิดทำลายพยานหลักฐานได้

ปัจจุบันกฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทย เป็นไปตามแนวคิดทฤษฎีกระบวนการนิติธรรมที่คุ้มครองสิทธิเสรีภาพของบุคคลเป็นสำคัญ จำกัดอำนาจของเจ้าหน้าที่รัฐมิให้ใช้อำนาจโดยมิชอบกระทบต่อสิทธิ

ของประชาชน พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์และกฎหมายวิธีพิจารณาความอาญา กำหนดให้เจ้าหน้าที่รัฐต้องปฏิบัติหน้าที่เกี่ยวกับมาตรการบังคับทางอาญา ในการจับ การค้น การควบคุม ต้องปฏิบัติตามกฎหมายอย่างเคร่งครัด ถือเป็นการป้องกันการใช้อำนาจรัฐไม่ให้กระทบต่อสิทธิเสรีภาพของประชาชน แต่ในการแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์แตกต่างจากพยานหลักฐานทั่วไป เป็นข้อมูลที่สามารถทำลายหรือแก้ไขได้โดยง่ายและใช้ระยะเวลาสั้น ผู้กระทำความผิดมีความรู้ความเชี่ยวชาญทางคอมพิวเตอร์ การค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ควรให้อำนาจแก่เจ้าหน้าที่รัฐในการดำเนินการแสวงหาพยานหลักฐานในการดำเนินคดีกับผู้กระทำความผิดอย่างเต็มที่ แม้มีการก้าวล่วงสิทธิเสรีภาพบุคคล แต่เพื่อให้บรรลุเป้าหมายในการควบคุมอาชญากรรม และสร้างความสงบเรียบร้อยในสังคม ให้การดำเนินคดีเป็นไปอย่างรวดเร็ว ไม่ว่าจะเป็นการสืบสวนก่อนทำการจับกุม การสืบสวนภายหลังการจับกุม การเตรียมคดีเพื่อฟ้องยังศาล การพิจารณาคดี การพิพากษาลงโทษผู้กระทำความผิด และการปล่อยตัวจำเลย ขั้นตอนต่างๆควรจะดำเนินไปอย่างต่อเนื่อง การกลั่นกรองคดีจะดำเนินการตามขั้นตอนต่างๆตามลำดับ การวินิจฉัยคดีให้เสร็จสิ้นไปตั้งแต่ขั้นตอนต้นๆของกระบวนการถือว่าเป็นวิธีการที่มีประสิทธิภาพมากที่สุด ทำให้ผู้ต้องหาที่เป็นผู้บริสุทธิ์จะถูกกลั่นกรองออกไป ผู้ที่กระทำความผิดก็จะถูกดำเนินคดีอย่างรวดเร็ว เจ้าหน้าที่รัฐและพนักงานอัยการสามารถวินิจฉัยความถูกผิดของขั้นตอนได้ ตามแนวคิดทฤษฎีการควบคุมอาชญากรรม เช่นเดียวกับสหพันธ์สาธารณรัฐเยอรมนี กฎหมายวิธีพิจารณาความอาญาของสหพันธ์สาธารณรัฐเยอรมนี (The Code of Criminal Procedure) ให้อำนาจอัยการในการสอบสวนข้อเท็จจริงเพื่อพิจารณาในการฟ้องคดี และสืบหาพฤติการณ์และข้อเท็จจริงทั้งที่เป็นโทษและเป็นคุณของผู้ถูกกล่าวหา การดำเนินคดีอาญาในชั้นสอบสวนของสหพันธ์สาธารณรัฐเยอรมนี มีหลักการพื้นฐานอยู่ว่า อัยการมีความเป็นอิสระในการที่จะเลือกใช้มาตรการบังคับในทางอาญามาตรการใดก็ได้ โดยนำ “หลักความเป็นอิสระในการจัดรูปแบบการสอบสวน” มาใช้ในการดำเนินคดีอาญาในการสืบสวนสอบสวนอย่างเต็มที่ และอัยการยังมีอำนาจในการสั่งการตรวจค้นในกรณีเร่งด่วนได้ ทำให้การดำเนินคดีอาญาเป็นไปอย่างรวดเร็ว

## 2. ปัญหาการซ้ำซ้อนระหว่างพนักงานเจ้าหน้าที่กับพนักงานสอบสวน ในการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 29 บัญญัติว่า ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มีฐานะเป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญา จึงมีอำนาจทั้งปวงตามประมวลกฎหมายวิธีพิจารณาความอาญากำหนด แต่มีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จึงไม่ได้ตัดอำนาจของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา เพียงแต่พนักงานสอบสวนไม่มีอำนาจหน้าที่ตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กำหนดไว้โดยเฉพาะเท่านั้น ยกตัวอย่างเช่น อำนาจของพนักงานเจ้าหน้าที่ ตามมาตรา 18 ถึงมาตรา 21 พนักงานสอบสวนจึงยังมีอำนาจอื่นที่ไม่ได้บัญญัติไว้เป็นอำนาจของพนักงานเจ้าหน้าที่โดยเฉพาะ

เมื่อพนักงานเจ้าหน้าที่และพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจซ้ำซ้อนกันในบางเรื่อง และในความผิดที่เกิดขึ้นนั้นมักมีความเกี่ยวพันกันระหว่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และความผิดตามกฎหมายอื่น ในการดำเนินคดีจึงต้องมีการประสานงาน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มิได้ระบุกำหนดรายละเอียดไว้อย่างชัดเจน กำหนดให้นายกรัฐมนตรีและรัฐมนตรีกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการ ซึ่งเมื่อวันที่ 30 พฤศจิกายน 2550 ได้มีการจัดทำระเบียบว่าด้วยการจับ ควบคุม การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิด ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนด

คำนิยาม “การปฏิบัติหน้าที่ร่วมกัน” หมายความว่า การที่พนักงานเจ้าหน้าที่และหรือพนักงานสอบสวนได้ให้ความเห็นหรือคำแนะนำ และหรือตรวจสอบพยานหลักฐานตั้งแต่ชั้นเริ่มการสอบสวนในคดีโดยให้เริ่มดำเนินการนับแต่โอกาสแรกเท่าที่จะพึงกระทำได้ และ “การสอบสวนร่วมกัน” หมายความว่า การสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในส่วนอำนาจในการรับคำร้องทุกข์หรือคำกล่าวโทษ ระเบียบว่าด้วยการจับ ควบคุม การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิด ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดให้พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนเป็นผู้รับคำร้องทุกข์ หรือคำกล่าวโทษในกรณีที่มีการกระทำความผิดเกิดขึ้น หรืออ้าง หรือเชื่อว่าได้เกิดขึ้นภายในเขตอำนาจของตนหรือผู้ต้องหามีที่อยู่หรือถูกจับภายในเขตอำนาจของตน และเป็นความผิดที่บัญญัติไว้ในหมวด 1 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในกรณีที่พนักงานสอบสวนได้รับคำร้องทุกข์ หรือคำกล่าวโทษ แล้ว ให้พนักงานสอบสวนประสานงานกับพนักงานเจ้าหน้าที่เพื่อประโยชน์ในการแสวงหาพยานหลักฐานประกอบการกระทำความผิดในการจับ ควบคุม และค้น เมื่อพนักงานเจ้าหน้าที่ประสานมายังพนักงานสอบสวนผู้รับผิดชอบแล้ว ให้พนักงานสอบสวนผู้รับผิดชอบดำเนินการตามอำนาจหน้าที่ต่อไป ให้พนักงานเจ้าหน้าที่ผู้รับผิดชอบดำเนินการแสวงหาพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดตามที่บัญญัติไว้ในหมวด 1 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยให้มีการปฏิบัติหน้าที่ร่วมกัน และการสอบสวนร่วมกัน และมีหน้าที่ส่งมอบพยานหลักฐานที่รวบรวมได้ทั้งหมดให้กับพนักงานสอบสวนผู้รับผิดชอบ จนกว่าการสอบสวนในคดีนั้นจะเสร็จสิ้น เมื่อพนักงานสอบสวนผู้รับผิดชอบในการสอบสวน เห็นว่าการสอบสวนเสร็จสิ้นแล้วให้พนักงานสอบสวนเป็นผู้ทำความเห็นในรายงานความเห็นทางคดี และลงลายมือชื่อ และส่งสำนวนการสอบสวนไปยังพนักงานอัยการในท้องที่ที่มีเขตอำนาจ เพื่อพิจารณาสั่งการต่อไป

จะเห็นได้ว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และระเบียบว่าด้วยการจับ ควบคุม การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิด ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มิได้กำหนดระบุอำนาจหน้าที่ของพนักงานเจ้าหน้าที่และพนักงานสอบสวนอย่างชัดเจน แต่จะเน้นไปในทางประสานความร่วมมือระหว่างกัน ซึ่งเมื่อกฎหมายมิได้ระบุอำนาจหน้าที่ไว้อย่างชัดเจนทำให้เกิดปัญหาในการปฏิบัติหน้าที่ที่ซ้ำซ้อนกัน เนื่องจากกฎหมายกำหนดให้อำนาจแก่เจ้าหน้าที่รัฐหลายฝ่ายให้มีอำนาจดังกล่าว เพื่อให้เกิดความชัดเจนแน่นอนแก่ประชาชนและเจ้าหน้าที่รัฐผู้ปฏิบัติงาน จึงเห็นควรกำหนดให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์มี

อำนาจในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี Technology Crime Suppression Division (TCSD) และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) Cyber Crime Investigation Bureau (CCIB) เนื่องจากเป็นหน่วยงานที่จัดตั้งขึ้นเพื่อดำเนินคดีกับผู้ที่กระทำความผิดทางอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะ และมีการแต่งตั้งพนักงานเจ้าหน้าที่จากผู้ที่มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 28 ประกอบกับประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเรื่องหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยมีอำนาจในการดำเนินคดีกับผู้ที่กระทำความผิดทางคอมพิวเตอร์ไม่ว่าจะเป็นอำนาจในการจับ การค้น การควบคุม การทำสำนวนการสอบสวน การรับคำร้องทุก และคำกล่าวโทษ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งเป็นกฎหมายหลักในการกำหนดความผิดและให้อำนาจแก่พนักงานเจ้าหน้าที่

# บทที่ 5
# บทสรุปและข้อเสนอแนะ

## 1. บทสรุป

การก่ออาชญากรรมทางอิเล็กทรอนิกส์เป็นอาชญากรรมที่เกิดขึ้นอย่างแพร่หลาย และมีการพัฒนาไปอย่างรวดเร็วและส่งผลร้ายอย่างกว้างขวาง เนื่องจากเป็นอาชญากรรมที่กระทำได้โดยง่ายผู้กระทำสามารถกระทำได้แม้มีอินเตอร์เน็ต อีกทั้งในปัจจุบันมีการนำสกุลเงินดิจิทัลมาใช้ในการซื้อขายแลกเปลี่ยนหรือใช้ในการลงทุนประกอบธุรกิจ อาชญากรจึงใช้ช่องทางดังกล่าวในการกระทำความผิด ก่อให้เกิดความเสียหายทางด้านเศรษฐกิจอย่างรุนแรง นอกจากนั้นยังมีการนำสื่ออิเล็กทรอนิกส์มากระทำความผิดในรูปแบบต่างๆ ไม่ว่าจะเป็น การล่วงละเมิดทางไซเบอร์ (Cyber harassment) การกลั่นแกล้งทางอินเทอร์เน็ต (Cyber bullying) การคุกคามทางไซเบอร์ (Cyber threats) หรือการสะกดรอยตามรังควานทางไซเบอร์ (Cyber stalking) ส่งผลต่อความปลอดภัยในชีวิตและทรัพย์สินทั้งสิ้น จึงต้องมีมาตรการที่จะนำมาใช้บังคับกับผู้ที่กระทำความผิดอย่างชัดเจน และมีการดำเนินคดีให้ได้ผู้ที่กระทำความผิดมารับโทษอย่างรวดเร็ว

ปัญหาในการดำเนินคดีอาญากับผู้ที่กระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ เป็นปัญหาที่เกิดกับผู้ที่บังคับใช้กฎหมายทั่วโลก เนื่องจากการก่ออาชญากรรมทางอิเล็กทรอนิกส์มีความยากต่อการตรวจพบพยานหลักฐาน และยากต่อการพิสูจน์ความรับผิด การกระทำความผิดมีวิธีการที่ซับซ้อนและผู้กระทำความผิดมักเป็นบุคคลที่มีความรู้ในด้านเทคโนโลยีเป็นอย่างดี และไม่สามารถหาตัวตนที่อยู่แน่นอนได้ทำให้ลำบากในการเข้าถึงตัวผู้กระทำความผิด และจากการศึกษาบทบัญญัติกฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทยและวิเคราะห์กับบทบัญญัติกฎหมายของสหรัฐอเมริกาและกฎหมายของสหพันธ์สาธารณรัฐเยอรมนี พบว่า แม้ว่าประเทศไทยจะมีกฎหมายอาชญากรรมคอมพิวเตอร์จะมีผลบังคับใช้แล้วคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 แต่หน่วยงานฝ่ายกระบวนการยุติธรรมก็ยังไม่สามารถนำกฎหมายมาจัดการกับผู้กระทำความผิดได้ เนื่องจากกฎหมายดังกล่าวไม่สามารถครอบคลุมไปถึงอาชญากรรมทางคอมพิวเตอร์ได้เท่าที่ควร พระราชบัญญัติดังกล่าวได้กำหนดให้มีพนักงานเจ้าหน้าที่แต่ก็ไม่ได้ตัด

อำนาจเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญาเพียงแต่เจ้าพนักงานตามประมวลกฎหมายอาญาไม่มีอำนาจหน้าที่ตามที่พระราชบัญญัตินี้กำหนดไว้โดยเฉพาะเท่านั้น แต่เจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญายังมีอำนาจหน้าที่ซึ่งไม่ได้มีการบัญญัติไว้โดยเฉพาะ พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจซ้ำซ้อนกันในเรื่องการมีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ การจับ ควบคุม การค้น อำนาจในการทำสำนวนการสืบสวนสอบสวน ในความผิดที่มีความเกี่ยวพันกันระหว่างความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และความผิดตามกฎหมายอื่น

หลักเกณฑ์การใช้อำนาจของพนักงานเจ้าหน้าที่ที่ทำให้เกิดความล่าช้าในการเข้าถึงพยานหลักฐานทางอิเล็กทรอนิกส์ การต้องได้การอนุญาตจากศาลถึงจะมีอำนาจในการดำเนินการได้ ซึ่งการเข้าถึงพยานหลักฐานทางอิเล็กทรอนิกส์มีความซับซ้อนจำเป็นต้องใช้ความรวดเร็วในการเข้าถึง การดำเนินการขอหมายค้นหรือการยื่นคำร้องเพื่อขออนุญาตจากศาลจึงก่อให้เกิดความล่าช้า

จากปัญหาข้างต้นจึงเห็นควร ทำการศึกษาและวิเคราะห์ปัญหาทางกฎหมาย ซึ่งมีประเด็นดังนี้

**1.1 ปัญหาการดำเนินคดีอาญา กรณีการค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์**

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และประมวลกฎหมายวิธีพิจารณาความอาญา ได้บัญญัติระบุขอบเขตอำนาจของพนักงานเจ้าหน้าที่ในการควบคุม การค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดทางอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มีข้อจำกัดอยู่มาก จึงควรกำหนดวิธีการ กระบวนการ และเงื่อนไขการใช้อำนาจของพนักงานเจ้าหน้าที่ในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ ให้มีอำนาจในการดำเนินการโดยเร็วเพื่อป้องการการแก้ไขเปลี่ยนแปลงพยานหลักฐานทางอิเล็กทรอนิกส์ของผู้กระทำความผิด ถึงแม้ประเทศไทยจะมีการจัดตั้งหน่วยงานกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี TechnologyCrime Suppression Division (TCSD) และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) Cyber Crime Investigation Bureau (CCIB) มีอำนาจหน้าที่ในการปฏิบัติพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 แต่ในส่วนของอำนาจในการเข้าถึงพยานหลักฐานจะกระทำได้

ต่อเมื่อได้รับอนุญาตจากศาลก่อนเป็นขั้นตอนที่ทำให้เกิดความล่าช้าในการยื่นคำร้องต่อศาลเพื่อพิจารณา เนื่องจากในแต่ละวันมีคดีขึ้นสู่ศาลอย่างมากไม่ว่าจะคดีแพ่งหรือคดีอาญาและในส่วนของคำร้องที่ศาลต้องพิจารณาซึ่งต้องใช้ระยะเวลา เพื่อตรวจสอบความถูกต้อง แต่คดีที่เกิดจากการกระทำความผิดทางอิเล็กทรอนิกส์พยานหลักฐานเป็นข้อมูลที่สามารถแก้ไขเปลี่ยนแปลงได้ตลอดเวลาการเข้าถึงพยานหลักฐานจึงต้องรวดเร็ว จึงควรให้อำนาจแก่เจ้าหน้าที่รัฐในการดำเนินการแสวงหาพยานหลักฐานในการดำเนินคดีกับผู้กระทำความผิดอย่างเต็มที่ แม้มีการก้าวล่วงสิทธิเสรีภาพบุคคล แต่เพื่อให้บรรลุเป้าหมายในการควบคุมอาชญากรรม และสร้างความสงบเรียบร้อยในสังคมผู้ที่กระทำความผิดก็จะถูกดำเนินคดีอย่างรวดเร็ว เจ้าหน้าที่รัฐและพนักงานอัยการสามารถวินิจฉัยความถูกผิดของขั้นตอนได้ ผู้ศึกษาเห็นควรกำหนดให้อำนาจแก่พนักงานอัยการในการตรวจสอบการพิจารณาคำร้องการค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ตามแนวคิด“หลักความเป็นอิสระในการจัดรูปแบบการสอบสวน” ของสหพันธ์สาธารณรัฐเยอรมนี

**1.2 ปัญหาการซ้ำซ้อนระหว่างพนักงานเจ้าหน้าที่กับพนักงานสอบสวน** ในการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์

ประเทศไทยมีการจัดตั้งหน่วยงานกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี TechnologyCrime Suppression Division (TCSD) มีอำนาจหน้าที่ ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวน ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์ และหน่วยงานกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) Cyber Crime Investigation Bureau (CCIB) หรือตำรวจไซเบอร์ มีอำนาจหน้าที่ดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วราชอาณาจักร ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่น อันเป็นความผิดทางอาญาเกี่ยวกับอาชญากรรมทางเทคโนโลยีและความผิดอื่นที่เกี่ยวเนื่อง และดำเนินการเกี่ยวกับการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี ซึ่งทั้งสองหน่วยงานมีอำนาจหน้าที่ที่คล้ายคลึงกัน อีกทั้งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ไม่ได้ตัดอำนาจเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญา ไม่ว่าจะเป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ ยังมีอำนาจในการรับแจ้งความร้องทุกข์ จับกุม ทำสำนวนการสอบสวนได้ ระเบียบว่าด้วยการจับ ควบคุม การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิด ตาม

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มิได้กำหนดระบุอำนาจหน้าที่ของพนักงานเจ้าหน้าที่และพนักงานสอบสวนอย่างชัดเจน แต่จะเน้นไปในทางประสานความร่วมมือระหว่างกัน ซึ่งเมื่อกฎหมายมิได้ระบุอำนาจหน้าที่ไว้อย่างชัดเจนทำให้เกิดปัญหาในการปฏิบัติหน้าที่ที่ซ้ำซ้อนกัน เนื่องจากกฎหมายกำหนดให้อำนาจแก่เจ้าหน้าที่รัฐหลายฝ่าย

## 2. ข้อเสนอแนะ

จากการศึกษาเปรียบเทียบ วิเคราะห์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมายการดำเนินคดีอาญาการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของสหรัฐอเมริกา และสหพันธ์สาธารณรัฐเยอรมนี ผู้ศึกษาจึงขอเสนอแนะแนวทางในการแก้ไขปัญหาในประเด็นต่าง ๆ ดังต่อไปนี้

**2.1 ปัญหาการดำเนินคดีอาญา กรณีการค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์**

ผู้ศึกษาเห็นสมควรให้มีการจัดตั้งสำนักงานอัยการคดีอาชญากรรมทางเทคโนโลยี เพื่อให้มีอำนาจในการดำเนินคดีอาญาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ โดยกำหนดให้พนักงานอัยการมีอำนาจสืบหาพฤติการณ์และข้อเท็จจริงทั้งที่เป็นโทษและเป็นคุณของผู้ถูกกล่าวหาได้ด้วยตนเองหรือให้กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี TechnologyCrime Suppression Division (TCSD) และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) Cyber Crime Investigation Bureau (CCIB) ดำเนินการก็ได้ เพื่อพิจารณาในการฟ้องคดีและมีอำนาจในการเรียกข้อมูลจากหน่วยงาน ในการสืบสวนสอบสวนในคดีอาชญากรรมทางเทคโนโลยี เพื่อช่วยให้การดำเนินคดีให้เกิดความเป็นธรรม สะดวกรวดเร็วมากขึ้น และเห็นควรแก้ไขกฎหมายในส่วนของอำนาจหน้าที่ที่ต้องขออนุญาตศาล โดยให้พนักงานอัยการเป็นผู้มีอำนาจในการพิจารณาคำร้อง ในกรณีที่จำเป็น เร่งด่วน หรือเกรงว่าพยานหลักฐานจะถูกแก้ไขเปลี่ยนแปลงหรือสูญหาย กำหนดให้อำนาจในการตรวจสอบการพิจารณาคำร้องการค้น การยึด พยานหลักฐานที่เกิดจากการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ แก่พนักงานอัยการในการพิจารณาคำร้องของพนักงานเจ้าหน้าที่หรือพนักงานสอบสวนในการค้น การยึด พยานหลักฐานอิเล็กทรอนิกส์ เพื่อให้เกิดความรวดเร็วในการพิจารณาคำร้อง และเป็นหลักประกันในการใช้ดุลพินิจของเจ้าหน้าที่

**2.2 ปัญหาการซ้ำซ้อนระหว่างพนักงานเจ้าหน้าที่กับพนักงานสอบสวน ในการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์**

ผู้ศึกษาเห็นสมควรให้มีการแก้ไขเพิ่มเติมกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 29 วรรค 2 เดิมที่บัญญัติไว้ว่า “ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป”

ขอแก้ไขเพิ่มเติมใน วรรค 2 โดยใช้ถ้อยคำใหม่ดังนี้ “ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ผู้รับผิดชอบดำเนินการตามอำนาจหน้าที่ต่อไป”

เนื่องจากการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ได้กำหนดให้อำนาจแก่พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา รวมถึงพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ มีอำนาจเช่นเดียวกับพนักงานเจ้าหน้าที่ ซึ่งมีอำนาจซ้ำซ้อนกันจึงเห็นควรกำหนดให้อำนาจในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นอำนาจของพนักงานเจ้าหน้าที่เป็นผู้ดำเนินการ ได้แก่กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี TechnologyCrime Suppression Division (TCSD) และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) Cyber Crime Investigation Bureau (CCIB) เนื่องจากเป็นหน่วยงานที่จัดตั้งขึ้นเพื่อดำเนินคดีกับผู้ที่กระทำความผิดทางอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะ เพื่อไม่ให้เกิดความยุ่งยากในการประสานงาน และเพื่อให้เกิดความชัดเจนแน่นอนแก่ประชาชนและเจ้าหน้าที่ผู้ปฏิบัติงาน

# บรรณานุกรม

# บรรณานุกรม


กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี. (2552). *ประวัติหน่วยงาน*. สืบค้นจาก https:// https://tcsd.go.th/เกี่ยวกับหน่วยงาน/

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี. (2563). *อำนาจหน้าที่*. สืบค้นจาก https://www.ccib.go.th/เกี่ยวกับหน่วยงาน/อำนาจหน้าที่

ธีสุทธิ์ พันธ์ฤทธิ์. (2551). *การรับฟังพยานหลักฐานคดีอาญา*. กรุงเทพมหานคร:วิญญูชน.

ปัณฑ์ณัฐ ขันเขต. (2559). *ปัญหากฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในชั้นพนักงานสอบสวน*. (วิทยานิพนธ์ปริญญานิติศาสตร์มหาบัณฑิต). สถาบันบัณฑิตพัฒนาบริหารศาสตร์, กรุงเทพมหานคร.

พจนานุกรไทย.com. (2557). *คำหมวดหมู่อักษร พ ความหมายของคำว่า 'พยาน'*.สืบค้นจาก https://พจนานุกรมไทย.com/30-192-ความหมาย-พยาน.html

วรเจตน์ ภาคีรัตน์.(2557). *เอกสารประกอบการบรรยายเรื่องหลักนิติรัฐ*. (พิมพ์ครั้งที่ 2). กรุงเทพมหานคร:โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์.

สมคิด สายเจริญ. (2557). *พยานหลักฐานดิจิทัลในคดีอาญา Digital Evidence in Criminal Cases.* สำนักงานอัยการสูงสุด.

สิทธิพล วิบูลย์ธนากุล. (2564). อาชญากรรมบนอินเทอร์เน็ตก่อต้นทุนทางเศรษฐกิจแค่ไหน. สืบค้นจาก https://www.bangkokbiznews.com/business/962481

CYBERSECURITY. (2000). *CISA's Role in Cybersecurity*. สืบค้นจาก https://www.cisa.gov/cybersecurity

Dsi กรมสอบสวนคดีพิเศษ,/ เกี่ยวกับดีเอสไอ/2559,/. สืบค้น https://www.dsi.go.th/th/Detail/History-of-DSI

FBI (the Internet Crime Complaint Center) IC3. (2000). *Mission Statement.* สืบค้นจาก https://www.ic3.gov/Home/About

Federal Criminal Police Office (Germany). (2014). สืบค้นจาก https://en.wikipedia.org/wiki/Federal_Criminal_Police_Office_(Germany)

Mass.gov. (2022). *The Attorney General's Enterprise, Major, and Cyber Crimes Division*. สืบค้นจาก https://www.mass.gov/the-attorney-generals-enterprise-major-and-cyber-crimes-division

NACDL. (2022). *CFAA Background.*สืบค้นจาก https://www.nacdl.org/Content/CFAABackground

Todsapol Aryuyune. (2559). *อาชญากรรมคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง*. สืบค้นจาก https:// www.slideshare.net/TodsapolAryuyune/7-62768502

United States Secret Service. (2000). *Cyber Investigations.* สืบค้นจาก https://www.secretservice.gov/investigation/cyber

# ประวัติผู้ศึกษา

| | |
|---|---|
| **ชื่อ** | นางสาววรรณิศา คำฟูบุตร |
| **วัน เดือน ปีเกิด** | 13 มกราคม 2537 |
| **สถานที่เกิด** | อำเภอเมือง จังหวัดลำปาง |
| **ประวัติการศึกษา** | นิติศาสตร์บัณฑิต มหาวิทยาลัยธรรมศาสตร์ ปี 2559 |
| **สถานที่ทำงาน** | ศาลแขวงลำปาง อำเภอเมือง จังหวัดลำปาง |
| **ตำแหน่ง** | นิติกร |