ปัญหาของการเปิดเผยและส่งมอบข้อมูลภายใต้มาตรา 70 วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

นายชิตพล พงศ์วชิราพร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2565

PROBLEM OF DISCLOSE AND PROVIDE DATA UNDER SECTION 70 PARAGRAPH TWO OF CYBERSECURITY ACT B.E. 2562 (2019)

Mr. Chittapon Pongvachiraporn

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Laws in Laws
FACULTY OF LAW
Chulalongkorn University
Academic Year 2022

หัวข้อวิทยานิพนธ์	ปัญหาของการเปิดเผยและส่งมอบข้อมูลภายใต้มาตรา 70 วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
โดย	นายชิตพล พงศ์วชิราพร
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร.ณัชพล จิตติรัตน์

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

..... คณบดีคณะนิติศาสตร์
(ผู้ช่วยศาสตราจารย์ ดร.ปารีณา ศรีวนิชย์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ศาสตราจารย์ ดร.คณพล จันทน์หอม)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ดร.ณัชพล จิตติรัตน์)

..... กรรมการ
(อาจารย์ ดร.ปราโมทย์ เสริมศีลธรรม)

..... กรรมการภายนอกมหาวิทยาลัย
(พันตำรวจเอก ดร.ศักดิ์วุฒิ วิบูลสมัย)

ชิตพล พงศ์วชิราพร : ปัญหาของการเปิดเผยและส่งมอบข้อมูลภายใต้มาตรา 70 วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (PROBLEM OF DISCLOSE AND PROVIDE DATA UNDER SECTION 70 PARAGRAPH TWO OF CYBERSECURITY ACT B.E. 2562 (2019)) อ.ที่ปรึกษาหลัก : ผศ. ดร.ณัชพล จิตติรัตน์

วิทยานิพนธ์ฉบับนี้มีวัตถุประสงค์เพื่อศึกษาปัญหาและกฎหมายเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งเป็นการกำหนดมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ รวมทั้งศึกษาแนวคิด มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทยและในต่างประเทศ เพื่อเสนอแนะแนวทางในการพัฒนามาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้มีความเหมาะสม

จากการศึกษาพบว่า การที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดข้อยกเว้นในการเปิดเผยและส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่นได้เป็นการให้อำนาจแก่เจ้าหน้าที่รัฐในการแสวงหาพยานหลักฐาน ซึ่งข้อมูลต่าง ๆ ที่ได้มาตามพระราชบัญญัติ ฯ ย่อมเป็นข้อมูลอิเล็กทรอนิกส์เป็นส่วนใหญ่ จึงถือได้ว่าเป็นมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ประการหนึ่ง เนื่องจากมาตรการในการแสวงหาพยานหลักฐานเป็นมาตรการที่เป็นการกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน จึงจำเป็นต้องมีหลักเกณฑ์ที่เหมาะสมในการใช้อำนาจของเจ้าหน้าที่รัฐ และในปัจจุบันยังไม่มีบทบัญญัติของกฎหมายกำหนดหลักเกณฑ์ในการปฏิบัติเกี่ยวกับการใช้อำนาจดังกล่าว ย่อมอาจก่อให้เกิดปัญหาในทางปฏิบัติได้

ด้วยเหตุผลที่กล่าวไปข้างต้น ผู้เขียนจึงเสนอแนะให้มีการแก้ไขมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งเป็นการกำหนดมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ โดยให้มีการกำหนดหลักเกณฑ์ที่เหมาะสมแก่การเปิดเผยหรือส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่น เพื่อเป็นบรรทัดฐานให้เจ้าหน้าที่รัฐได้ใช้เป็นแนวทางในการปฏิบัติ และเป็นการคุ้มครองสิทธิเสรีภาพของประชาชน

สาขาวิชา	นิติศาสตร์	ลายมือชื่อนิสิต .....
ปีการศึกษา	2565	ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

6085963034 : MAJOR LAWS
KEYWORD: Electronic Evidence, Obtained Electronic Evidence, Cybersecurity

Chittapon Pongvachiraporn : PROBLEM OF DISCLOSE AND PROVIDE DATA UNDER SECTION 70 PARAGRAPH TWO OF CYBERSECURITY ACT B.E. 2562 (2019). Advisor: Asst. Prof. NATCHAPOL JITTIRAT, Ph.D.

This thesis aims to study the problems and doctrines of measures for cybersecurity, which is relate to measures for obtaining electronic evidence. The thesis also studies the concepts, measures for cybersecurity and measures for obtaining electronic evidence in Thailand and foreign countries and propose the appropriate of measures for obtaining electronic evidence under Cybersecurity Act B.E. 2562 (2019)

According to the research, Cybersecurity Act B.E. 2562 (2019) stipulates exceptions for the benefit litigation against an offender under other laws. It empowered state official to obtaining evidence. Most of the data obtained under this Act are electronic evidence. Therefore, it can be regards as one of the measures for obtaining electronic evidence. Since the evidence obtaining measure is a measure that affects the rights and the liberty of the people, it is necessary to have appropriate criteria for exercising the power of state officials. At present, there is no provision of the law prescribing the rules for the exercise of such power, it may cause problems in practice.

As a consequence, the author of this thesis suggests measures for cybersecurity, which is relate to measures for obtaining electronic evidence should be revised by appropriate criteria for the disclose or send data for the benefit litigation against an offender under other laws. The proposed to be criterion for state officials to use as a guideline in practice and to protect rights and liberties of the people.

Field of Study: Laws Student's Signature .....
Academic Year: 2022 Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงเป็นอย่างดีเพราะความเมตตาอย่างสูงจากอาจารย์และผู้ทรงคุณวุฒิหลายท่าน โดยเฉพาะท่านผู้ช่วยศาสตราจารย์ ดร.ณัชพล จิตติรัตน์ ที่ได้กรุณารับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ฉบับนี้ โดยท่านได้ให้คำแนะนำ ชี้แนะประเด็นในการศึกษา ตลอดจนตรวจสอบแก้ไขข้อบกพร่องในการจัดทำวิทยานิพนธ์ตั้งแต่เริ่มต้นจนจบ ผู้เขียนจึงขอกราบขอบพระคุณท่านอาจารย์เป็นอย่างสูงที่ให้ความเมตตากรุณาผู้เขียนตลอดมา ขอกราบขอบพระคุณท่านศาสตราจารย์ ดร.คณพล จันทน์หอม ที่กรุณารับเป็นประธานกรรมการสอบวิทยานิพนธ์ ท่านอาจารย์ ดร.ปราโมทย์ เสริมศีลธรรม และท่านพันตำรวจเอก ดร.ศักดิ์วุฒิ วิบูลสมัย ที่กรุณารับเป็นกรรมการผู้ทรงคุณวุฒิ โดยท่านอาจารย์ได้ชี้แนะประเด็นการศึกษา และช่วยปรับปรุงแนวทางในการจัดทำวิทยานิพนธ์ฉบับนี้ให้มีความสมบูรณ์มากยิ่งขึ้น

ผู้เขียนขอกราบขอบพระคุณเจ้าหน้าที่ประจำหลักสูตรนิติศาสตรมหาบัณฑิต และเจ้าหน้าที่ห้องสมุด คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัยทุกท่านที่ให้ความรู้ ให้ความอนุเคราะห์ และอำนวยความสะดวกในการจัดทำวิทยานิพนธ์ด้วยดีตลอดมา

นอกจากนี้ ผู้เขียนขอกราบขอบพระคุณบุคคลสำคัญ ซึ่งเป็นผู้ให้โอกาสในการศึกษารวมทั้งเป็นแรงผลักดันสนับสนุนให้ผู้เขียนสามารถจัดทำวิทยานิพนธ์เล่มนี้จนสำเร็จลุล่วง ได้แก่ คุณเฉียบชัย และคุณน้ำผึ้ง พงศ์วชิราพร บิดามารดาผู้เป็นที่เคารพรัก คุณภัทรมาศ ฉันทนานุวัฒน์ บุคคลสำคัญซึ่งคอยช่วยเหลือและให้กำลังใจในการจัดทำวิทยานิพนธ์ของผู้เขียนเสมอมา และเพื่อน ๆ ทุกคนที่คอยช่วยเหลือ ถามไถ่และให้กำลังใจตลอดการจัดทำวิทยานิพนธ์ รวมไปถึงเพื่อน ๆ ที่คอยอยู่เคียงข้างในช่วงเวลาที่เหนื่อยล้าจากการใช้ชีวิตและจัดทำวิทยานิพนธ์ฉบับนี้ทุก ๆ ท่าน

สุดท้ายนี้ ผู้เขียนหวังเป็นอย่างยิ่งว่าวิทยานิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อบุคคลในสังคม และบุคคลในวงวิชาการด้านกฎหมาย คุณความดีที่เกิดมีขึ้นจากวิทยานิพนธ์ฉบับนี้ ผู้เขียนขอมอบให้แก่บุคคลทุกท่านที่ได้กล่าวมาทั้งหมด ตลอดจนท่านผู้จัดทำที่ผู้เขียนนำมาอ้างอิงและเรียบเรียงเป็นวิทยานิพนธ์ฉบับนี้ หากวิทยานิพนธ์ฉบับนี้มีข้อผิดพลาดและบกพร่องประการใด ผู้เขียนต้องกราบขออภัย ณ ที่นี้ และขอน้อมรับไว้แต่เพียงผู้เดียว

ชิตพล พงศ์วชิราพร

สารบัญ

หน้า

สารบัญตาราง

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันที่มีการพัฒนาของเทคโนโลยีอยู่ตลอดเวลา อินเตอร์เน็ตได้ทำให้เกิดยุคของการติดต่อสื่อสารที่ไร้พรมแดน ซึ่งเทคโนโลยีอินเตอร์เน็ตดังกล่าวก่อให้เกิดประโยชน์แก่สังคมโลกมากมาย แต่ในขณะเดียวกันก็ทำให้เกิดรูปแบบของการกระทำความผิดทางอาญารูปแบบใหม่ขึ้นนั่นก็คือ อาชญากรรมทางคอมพิวเตอร์ ซึ่งเป็นอาชญากรรมที่ส่งผลกระทบต่อชีวิตและความเป็นอยู่ของประชาชนเป็นวงกว้าง เนื่องมาจากรูปแบบอาชญากรรมที่ใช้เทคโนโลยีสมัยใหม่ คอมพิวเตอร์ เครือข่ายอินเตอร์เน็ต และอุปกรณ์อิเล็กทรอนิกส์เป็นช่องทางในการกระทำความผิด[1] เมื่อเครือข่ายอินเตอร์เน็ตได้เข้ามามีส่วนในการให้บริการทางด้านโครงสร้างพื้นฐานที่สำคัญของประเทศ จึงทำให้อาชญากรรมทางคอมพิวเตอร์สามารถส่งผลกระทบต่อโครงสร้างพื้นฐานที่สำคัญของประเทศได้เช่นเดียวกัน ซึ่งภัยคุกคามนี้ในปัจจุบันเรียกกันว่า “ภัยคุกคามทางไซเบอร์” แม้ว่าในช่วงหลายปีที่ผ่านมานานาประเทศจะได้มีการกำหนดฐานความผิดใหม่ซึ่งเป็นฐานความผิดเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แต่การกำหนดฐานความผิดดังกล่าวและการให้อำนาจแก่เจ้าหน้าที่รัฐในการดำเนินคดีและจับกุมผู้กระทำความผิดภายหลังที่การกระทำความผิดเกิดขึ้นแล้วนั้น อาจไม่สามารถรักษาไว้ซึ่งความสงบเรียบร้อยในสังคมได้ เนื่องจากอาชญากรรมทางคอมพิวเตอร์ หรือที่เรียกว่าอาชญากรรมไซเบอร์หรือภัยคุกคามไซเบอร์ เป็นการโจมตีหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ ในบางกรณีอาจส่งผลกระทบให้เกิดความเสียหายเป็นวงกว้างต่อประเทศได้[2] ดังนั้น จึงมีความจำเป็นที่รัฐจะต้องมีมาตรการในการรักษาความปลอดภัยไซเบอร์โดยเฉพาะมาตรการทั้งก่อนและหลังจากที่เกิดภัยคุกคามไซเบอร์ขึ้นแล้ว เพื่อเป็นการลดขอบเขตความเสียหายที่อาจเกิดขึ้นได้จากภัยคุกคามไซเบอร์

ประเทศไทยได้เพ่งเล็งถึงปัญหาเกี่ยวกับภัยคุกคามไซเบอร์ และได้มีการศึกษาแนวทางในการแก้ไขปัญหาและรับมือต่อภัยคุกคามไซเบอร์ดังกล่าว จึงได้ประกาศใช้พระราชบัญญัติการรักษาความ

---

[1] ฐกฤต แก้วทับทิม, "การขยายตัวขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโควิด-19," วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์ กรกฎาคม - ธันวาคม 2564, ฉบับที่ 2 ปีที่ 7 (2565): หน้า 164.

[2] จิตสุภา ฤทธิผลิน, "กลยุทธ์การคืนสภาพได้ทางไซเบอร์ : แนวทางสำคัญในการดำเนินงานขององค์กรในยุคดิจิทัล," วารสารวิชาการ กสทช. ประจำปี 2564 (2564): หน้า 163 - 164.

มั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เมื่อวันที่ 28 พฤษภาคม พ.ศ. 2562 โดยมีวัตถุประสงค์เพื่อเป็นการยกระดับการรักษาความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure หรือ CII) ให้มีประสิทธิภาพมากยิ่งขึ้น พร้อมทั้งยังมีการกำหนดมาตรการในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงของรัฐ เศรษฐกิจ และความสงบเรียบร้อยภายในประเทศขึ้นอีกด้วย นอกจากการจัดตั้งหน่วยงานเพื่อบังคับใช้กฎหมายและกำหนดมาตรการต่าง ๆ ให้หน่วยงานพื้นฐานสำคัญทางสารสนเทศต้องดำเนินการตามแล้ว พระราชบัญญัติ ฯ ดังกล่าวยังได้ให้อำนาจแก่เจ้าหน้าที่รัฐในการเข้าถึงข้อมูลต่าง ๆ ของประชาชน รวมไปถึงมีอำนาจในการเรียกบุคคลมาให้ข้อมูล และเข้าตรวจสอบสถานที่อันเป็นเคหสถานของประชาชนได้ด้วย ซึ่งอำนาจดังกล่าวกำหนดโดยแบ่งไปตามระดับความร้ายแรงของภัยคุกคามไซเบอร์ที่เกิดหรืออาจจะเกิดขึ้นได้

เมื่อพิจารณามาตรการต่าง ๆ ในการเข้าถึงข้อมูลตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ จะเห็นได้ว่าได้มีการแบ่งออกเป็น 3 ระดับด้วยกัน ได้แก่ มาตรการในกรณีของภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง มาตรการในกรณีของภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และมาตรการในกรณีของภัยคุกคามทางไซเบอร์ในระดับวิกฤติ

(1) มาตรการในกรณีของภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงไม่ได้ให้อำนาจเป็นพิเศษแก่เจ้าหน้าที่รัฐแต่อย่างใด คงกำหนดเพียงว่าให้เจ้าหน้าที่รัฐทำการรวบรวม ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบ รวมไปถึงการสนับสนุน ให้ความช่วยเหลือ หรือประสานงานในการป้องกัน รับมือ และลดความเสี่ยงเท่านั้น[3]

(2) มาตรการในกรณีของภัยคุกคามไซเบอร์ในระดับร้ายแรง กฎหมายได้ให้อำนาจแก่เจ้าหน้าที่รัฐในการมีหนังสือขอความร่วมมือให้บุคคลที่เกี่ยวข้องมาให้ข้อมูลหรือให้ส่งข้อมูลเป็นหนังสือ และการมีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของบุคคลใดเพื่อประโยชน์ในการดำเนินการ[4] ซึ่งมีลักษณะเป็นการขอความร่วมมือ อีกทั้งยังได้ให้อำนาจในการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์[5] ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ[6] ซึ่งมีเหตุอันควรเชื่อ

---

[3] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 59

[4] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 62

[5] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 65 (5) และ 66 (2)

ได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ โดยในการเข้าถึงข้อมูลดังกล่าวจะต้องยื่นคำร้องต่อศาลโดยระบุเหตุอันควรเชื่อได้ว่ามีบุคคลใดบุคคลหนึ่งกำลังก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

(3) มาตรการในกรณีของภัยคุกคามไซเบอร์ในระดับวิกฤติ ซึ่งกฎหมายกำหนดให้เจ้าหน้าที่รัฐมีอำนาจดำเนินการใด ๆ ได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าโดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากได้ดำเนินการไปแล้วให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว รวมถึงมีอำนาจขอข้อมูลที่เป็นปัจจุบันและต่อเนื่อง (Real Time) จากผู้ที่เกี่ยวข้องกับภัยคุกคามไซเบอร์

จากมาตรการดังกล่าวข้างต้น จะเห็นได้ว่า นอกจากเป็นมาตรการที่ให้อำนาจแก่เจ้าหน้าที่รัฐในการเข้าถึงข้อมูลต่าง ๆ ของประชาชน และสามารถจัดเก็บหรือรวบรวมข้อมูลต่าง ๆ เหล่านั้นมาใช้เพื่อประโยชน์ในการดำเนินการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์แล้ว ยังได้กำหนดให้สามารถนำเอาข้อมูลต่าง ๆ เหล่านั้นไปใช้ในการดำเนินคดีต่าง ๆ ได้อีกด้วย โดยหลักการนำข้อมูลไปใช้ประกอบการดำเนินคดีปรากฏอยู่ในมาตรา 70 ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งมาตรา 70 ได้กำหนดห้ามมิให้เจ้าหน้าที่รัฐเปิดเผยหรือส่งมอบข้อมูลต่าง ๆ ซึ่งได้มาจากมาตรการตามพระราชบัญญัติฉบับนี้ หากฝ่าฝืนย่อมมีความผิด และอาจต้องระวางโทษจำคุกสูงสุด 3 ปี อย่างไรก็ตาม ในมาตรา 70 วรรคสอง ได้มีการกำหนดข้อยกเว้นที่เจ้าหน้าที่รัฐสามารถเปิดเผยหรือส่งมอบข้อมูลดังกล่าวได้ แบ่งออกเป็น 3 กรณี ดังนี้

(1) การเปิดเผยหรือส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้

(2) การเปิดเผยหรือส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายฉบับอื่น

(3) การเปิดเผยหรือส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจโดยมิชอบ

เมื่อพิจารณากรณีที่เป็นข้อยกเว้นในการเปิดเผยหรือส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายฉบับอื่น ๆ มีลักษณะเป็นการให้อำนาจแก่เจ้าหน้าที่รัฐใน

---

[6] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 66 (4)

การแสวงหาพยานหลักฐาน ซึ่งข้อมูลต่าง ๆ ที่ได้มาตามพระราชบัญญัติฉบับนี้ ย่อมมีลักษณะเป็นข้อมูลอิเล็กทรอนิกส์เป็นสำคัญ กรณีดังกล่าวจึงถือได้ว่าเป็นมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ประการหนึ่ง ซึ่งมาตรการในการแสวงหาพยานหลักฐานโดยทั่วไปจะต้องมีกฎหมายกำหนดหลักเกณฑ์และขอบเขตในการใช้อำนาจของเจ้าหน้าที่รัฐไว้อย่างชัดเจน เนื่องจากมาตรการในการแสวงหาพยานหลักฐานเป็นมาตรการที่กระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน

มาตรการในการแสวงหาพยานหลักฐานที่สำคัญ ได้แก่ การค้นและการยึด ซึ่งโดยทั่วไปแล้วเจ้าหน้าที่รัฐจะทำการค้นหรือยึดสิ่งใดได้จะต้องมีการยื่นคำร้องต่อศาลเพื่อขอออกหมายค้นเสียก่อน ในคำร้องจึงต้องประกอบไปด้วยเหตุอันควรเชื่อได้ว่าสิ่งที่จะทำการค้นหรือยึดนั้นมีความเกี่ยวข้องกับการกระทำความผิด ซึ่งหลักการดังกล่าวถือเป็นหลักการสำคัญและเป็นสากลในการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐาน แต่เมื่อพิจารณาถึงหลักเกณฑ์ต่าง ๆ ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ จะเห็นได้ว่า แม้จะมีการนำหลักการเกี่ยวกับการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐมาใช้ประกอบมาตรการในการเข้าถึงข้อมูลต่าง ๆ ของประชาชน เช่น หลักนิติธรรมโดยมีการกำหนดบทบัญญัติเกี่ยวกับการใช้อำนาจของเจ้าหน้าที่รัฐไว้อย่างชัดเจน และมีการกำหนดบทลงโทษในกรณีที่เจ้าหน้าที่รัฐไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย หรือการใช้อำนาจหน้าที่โดยมิชอบ หลักการคุ้มครองสิทธิเสรีภาพของประชาชน เช่น หลักการตรวจสอบการใช้อำนาจรัฐ โดยได้มีการนำหลักเหตุอันควรเชื่อมาประกอบการใช้อำนาจของเจ้าหน้าที่รัฐที่เกี่ยวข้องกับการเข้าถึงข้อมูลของประชาชน

อย่างไรก็ตาม แม้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ จะได้มีการบัญญัติให้นำหลักการที่สำคัญต่าง ๆ มาประกอบกับการใช้อำนาจหน้าที่ของเจ้าหน้าที่รัฐ แต่หลักการต่าง ๆ เหล่านั้น ก็เป็นเพียงหลักการใช้อำนาจเกี่ยวกับการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์เป็นสำคัญเท่านั้น กล่าวคือ กำหนดให้เจ้าหน้าที่รัฐต้องมีการยื่นคำร้องต่อศาลก่อนดำเนินการ โดยคำร้องดังกล่าวจะต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ขึ้น เป็นต้น แต่หากการใช้มาตรการดังกล่าวเป็นผลให้ เจ้าหน้าที่รัฐได้ไปซึ่งข้อมูลที่เกี่ยวกับการกระทำความผิดตามกฎหมายอื่น แล้วนั้น จะเห็นได้ว่าคำร้องดังกล่าวย่อมไม่มีการระบุเหตุอันควรเชื่อว่าบุคคลใดบุคคลหนึ่งกำลังกระทำความผิดตามกฎหมายอื่น ซึ่งมีความเชื่อมโยงกับข้อมูลดังกล่าวที่ได้มาแต่อย่างใด จากที่กล่าวมาข้างต้นเป็นกรณีภัยคุกคามไซเบอร์ในระดับร้ายแรง ซึ่งเจ้าหน้าที่รัฐจะต้องมีการยื่นคำร้องต่อศาลเพื่อดำเนินมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ หากเป็นกรณีของภัยคุกคามไซเบอร์ในระดับวิกฤติ

กฎหมายให้อำนาจแก่เจ้าหน้าที่รัฐในการดำเนินการใด ๆ ได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าโดยไม่ต้องยื่นคำร้องต่อศาล และกำหนดให้ภายหลังจากได้ดำเนินการไปแล้วให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็วเท่านั้น เหตุที่เป็นเช่นนี้เพราะในกรณีของภัยคุกคามไซเบอร์ในระดับวิกฤติ หากปล่อยให้เวลาล่วงเลยไปอาจส่งผลกระทบและสร้างความเสียหายเป็นวงกว้างได้

การที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ได้กำหนดให้อำนาจแก่เจ้าหน้าที่รัฐในลักษณะที่แตกต่างไปจากมาตรการในการแสวงหาพยานหลักฐานทั่วไป เป็นผลมาจากการชั่งน้ำหนักระหว่างการใช้อำนาจของเจ้าหน้าที่รัฐอย่างเต็มที่เพื่อรักษาไว้ซึ่งความสงบสุขของสังคมตามแนวความคิดของทฤษฎีการควบคุมอาชญากรรม (Crime Control Theory) กับการคุ้มครองสิทธิเสรีภาพของประชาชนเป็นสำคัญตามแนวความคิดของทฤษฎีความชอบด้วยกระบวนการทางกฎหมาย (Due Process Theory) ซึ่งการรักษาความมั่นคงปลอดภัยไซเบอร์ในกรณีที่มีความจำเป็นและเร่งด่วน จำเป็นต้องให้อำนาจแก่รัฐอย่างเต็มที่ในการดำเนินการต่าง ๆ เพราะไม่เช่นนั้นแล้ว อาจทำให้การดำเนินการล่าช้าและทำให้ไม่สามารถรักษาไว้ซึ่งความปลอดภัยไซเบอร์ได้ อย่างไรก็ดี การกำหนดข้อยกเว้นให้สามารถเปิดเผยหรือส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายฉบับอื่นได้นั้น การกระทำความผิดดังกล่าวอาจเป็นคนละกรณีกับภัยคุกคามไซเบอร์ที่เกิดขึ้น โดยในบางฐานความผิดอาจมีความเกี่ยวข้องเชื่อมโยงกัน แต่ในบางฐานความผิดอาจไม่มีความเกี่ยวเชื่อมโยงกันแต่อย่างใดก็ได้ ยิ่งไปกว่านั้นฐานความผิดตามกฎหมายอื่น อาจเป็นฐานความผิดที่ไม่ได้มีความรุนแรงมากเพียงพอที่จะมีความเหมาะสมในการใช้มาตรการพิเศษ ดังเช่นมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในการเข้าถึงข้อมูลต่าง ๆ เนื่องจากโดยปกติแล้วอำนาจของเจ้าหน้าที่รัฐในการแสวงหาพยานหลักฐานย่อมเปลี่ยนแปลงไป ขึ้นอยู่กับความร้ายแรงของความความผิดที่เกิดขึ้นนั้น ๆ ซึ่งข้อยกเว้นดังกล่าวเป็นข้อยกเว้นที่มีลักษณะครอบคลุมอย่างกว้างและสามารถใช้ได้กับทุกฐานความผิดที่ได้มีการบัญญัติไว้ในกฎหมายฉบับต่าง ๆ ของประเทศไทย อันอาจส่งผลให้ไม่เป็นไปตามหลักทั่วไปของการแสวงหาพยานหลักฐานที่เหมาะสมกับฐานความผิดนั้น ๆ และอาจเป็นการกระทบกระเทือนสิทธิเสรีภาพของประชาชนเกินสมควร

ในปัจจุบันยังไม่มีบทบัญญัติของกฎหมายที่กำหนดหลักเกณฑ์เกี่ยวกับการบังคับใช้ข้อยกเว้นในการที่สามารถเปิดเผยหรือส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายฉบับอื่นได้แต่อย่างใด เมื่อพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ได้มีการ

ประกาศใช้แล้ว บทบัญญัติดังกล่าวก็ย่อมมีผลบังคับใช้เช่นเดียวกัน การที่ไม่มีบทบัญญัติกำหนดหลักเกณฑ์ที่ชัดเจน ย่อมอาจก่อให้เกิดปัญหาในทางปฏิบัติได้

ดังนั้น จากปัญหาดังกล่าวข้างต้น ผู้เขียนจึงเห็นควรศึกษาและวิเคราะห์มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ที่เกี่ยวข้อง เพื่อวิเคราะห์หาแนวทางในการกำหนดบทบัญญัติที่เหมาะสมเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทยตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ และให้สอดคล้องกับหลักการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐ และหลักการคุ้มครองสิทธิเสรีภาพของประชาชน

1.2 สมมติฐาน

การที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 70 วรรคสอง กำหนดข้อยกเว้นในการเปิดเผยและส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่น มีลักษณะเป็นการให้อำนาจแก่เจ้าหน้าที่รัฐในการแสวงหาพยานหลักฐาน ซึ่งโดยลักษณะของข้อมูลต่าง ๆ ที่ได้มาตามพระราชบัญญัติดังกล่าว ย่อมมีลักษณะเป็นข้อมูลอิเล็กทรอนิกส์เป็นสำคัญ จึงถือได้ว่าเป็นมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ประการหนึ่ง เมื่อมาตรการในการแสวงหาพยานหลักฐานเป็นมาตรการที่เป็นการกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน จึงควรมีการแก้ไขบทบัญญัติของกฎหมาย โดยมีการกำหนดหลักเกณฑ์ที่เหมาะสม โดยเฉพาะหลักการค้นโดยไม่มีหมายภายใต้หลักการเห็นได้โดยประจักษ์ (Plain view) มาปรับใช้กับการใช้อำนาจของเจ้าหน้าที่รัฐ ตามมาตรา 70 วรรคสอง ที่ได้กำหนดข้อยกเว้นของการเปิดเผยและส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่น และเพื่อให้เป็นไปตามหลักการทั่วไปว่าด้วยการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้มีการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐ และไม่เป็นการกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนเกินสมควร

1.3 วัตถุประสงค์ของการศึกษาวิจัย

1.3.1 เพื่อศึกษาแนวความคิด ลักษณะ และวัตถุประสงค์ของมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์

1.3.2 เพื่อศึกษาหลักกฎหมายและคำพิพากษาเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามกฎหมายไทยและกฎหมายต่างประเทศ

1.3.3 เพื่อวิเคราะห์ศึกษาเปรียบเทียบวัตถุประสงค์ มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทยและต่างประเทศ

1.3.4 เพื่อเสนอแนะแนวทางแก้ไขและปรับปรุงพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.4 ขอบเขตการศึกษา

ศึกษาแนวความคิด ทฤษฎี หลักกฎหมาย และคำพิพากษาเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ เพื่อนำข้อมูลที่ได้มาทำการวิเคราะห์ เปรียบเทียบ และเสนอมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ให้เหมาะสมและสอดคล้องกับเจตนารมย์ของกฎหมาย และสามารถกำหนดมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ได้อย่างเหมาะสม สอดคล้องกับหลักการคุ้มครองสิทธิเสรีภาพของประชาชน

1.5 วิธีการศึกษาวิจัย

วิทยานิพนธ์ฉบับนี้ใช้วิธีการวิจัยทางเอกสาร โดยศึกษาค้นคว้าจากเอกสาร ข้อมูล ตำรา และเอกสารต่าง ๆ ที่เกี่ยวข้องทั้งภาษาไทยและภาษาต่างประเทศ เช่น หนังสือ บทความ วิทยานิพนธ์ รวมทั้งเอกสารอื่น ๆ ตลอดจนตัวบทกฎหมายทั้งของประเทศไทยและต่างประเทศ รวมทั้งข้อมูลทางอิเล็กทรอนิกส์

1.6 ประโยชน์ที่คาดว่าจะได้รับจากการศึกษาวิจัย

1.6.1 ทำให้ทราบแนวความคิด ลักษณะ และวัตถุประสงค์ของมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์

1.6.2 ทำให้ทราบถึงหลักกฎหมายและคำพิพากษาเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามกฎหมายไทยและกฎหมายต่างประเทศ

1.6.3 ทำให้สามารถวิเคราะห์ศึกษาเปรียบเทียบวัตถุประสงค์ มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทยและต่างประเทศ

1.6.4 ทำให้สามารถเสนอแนะแนวทางแก้ไขและปรับปรุงพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.7 งานวิจัยที่เกี่ยวข้อง

(1) การค้นคว้าอิสระ เรื่อง การตรวจสอบและถ่วงดุลอำนาจเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดย นางสาวอนัญพร สกุลเมฆา นิติศาสตรมหาบัณฑิต สาขากฎหมายอาญา คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีการศึกษา 2562

โดยการค้นคว้าอิสระฉบับดังกล่าวได้ทำการศึกษาวิจัยเกี่ยวกับการถ่วงดุลอำนาจของเจ้าหน้าที่รัฐซึ่งกฎหมายรักษาความมั่นคงปลอดภัยไซเบอร์เป็นกฎหมายที่บัญญัติขึ้นเพื่อวางมาตรการในการรับมือและป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นหรืออาจจะเกิดขึ้นในอนาคต เพื่อให้ได้มาซึ่งข้อมูลต่าง ๆ ที่จะใช้ในการรักษาความมั่นคงปลอดภัยไซเบอร์ภายในประเทศได้อย่างทันท่วงที ซึ่งพระราชบัญญัติ ฯ ของประเทศไทยได้ให้อำนาจแก่เจ้าหน้าที่ในการดำเนินมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งอำนาจดังกล่าวเป็นอำนาจที่ส่งผลกระทบต่อสิทธิและเสรีภาพของประชาชนโดยตรง จึงจำเป็นต้องมีการกำหนดหลักเกณฑ์การใช้อำนาจของเจ้าหน้าที่รัฐที่ชัดเจนและตรวจสอบการใช้อำนาจได้ เพื่อเป็นหลักประกันในการคุ้มครองสิทธิเสรีภาพของประชาชน ซึ่งได้มีการเสนอแนะการแก้ปัญหาดังกล่าว ดังนี้[7]

ประการแรก ควรมีการคุ้มครองผู้เปิดเผยข้อมูล โดยกฎหมายควรมีการกำหนดให้มีความละเอียดครอบคลุมมากยิ่งขึ้น ไม่ว่าจะเป็นในกรณีของการเปิดเผยข้อมูลทางวิชาชีพ ความลับทางการค้า นอกเหนือไปจากในเรื่องของการละเมิดและผิดสัญญาที่ได้มีการกำหนดไว้ในพระราชบัญญัติ ฯ แล้ว และควรมีการกำหนดห้ามไม่ให้สามารถนำข้อมูลที่ได้มาตามอำนาจในพระราชบัญญัติ ฯ ไปใช้เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่น โดยข้อมูลที่ได้จะต้องใช้เป็นพยานหลักฐานเฉพาะความผิดฐานต่าง ๆ ที่ได้มีการกำหนดไว้ในพระราชบัญญัติ ฯ เท่านั้น และควรมีการกำหนดให้มีการลบหรือทำลายข้อมูลส่วนบุคคลหรือข้อมูลที่ทำให้ระบุตัวตนของบุคคลได้ที่ไม่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดให้เจ้าหน้าที่ต้องทำลายข้อมูลอื่นที่ไม่เกี่ยวข้องโดยตรงกับกฎหมายที่ให้อำนาจไว้ภายในระยะเวลาที่เหมาะสมด้วย

---

[7] อนัญพร สกุลเมฆา, "การตรวจสอบและถ่วงดุลอำนาจเจ้าพนักงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562" (นิติศาสตรมหาบัณฑิต สาขากฎหมายอาญา, คณะนิติศาสตร์, มหาวิทยาลัยธรรมศาสตร์, 2562), หน้า 67 - 70.

ประการที่สอง บทบัญญัติที่ให้ดุลพินิจแก่เจ้าหน้าที่รัฐในกรณีที่มีเหตุอันควรเชื่อได้ว่าเป็นผู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ ให้เจ้าหน้าที่รัฐสามารถใช้มาตรการต่าง ๆ ได้นั้น เพื่อเป็นการควบคุมการใช้ดุลพินิจดังกล่าวให้อยู่ในขอบเขต จึงควรกำหนดให้บุคคลที่ได้รับคำสั่งมีสิทธิที่จะปฏิเสธก่อนได้ และเมื่อมีการปฏิเสธไม่ให้ความยินยอมโดยปราศจากเหตุอันสมควร เจ้าหน้าที่รัฐจะต้องแจ้งต่อ กกม. เพื่อพิจารณาทบทวนคำสั่งอีกครั้งหนึ่ง

ประการที่สาม ในกรณีของการที่ให้อำนาจแก่เจ้าหน้าที่รัฐในการเข้าตรวจค้นสถานที่ซึ่งพระราชบัญญัติ ฯ ไม่ได้กำหนดให้สิทธิแก่บุคคลผู้ซึ่งถูกรบกวนในการปฏิเสธคำสั่งหรือมีการกำหนดหลักเกณฑ์ในการตรวจสอบถ่วงดุลการใช้อำนาจดังกล่าวเอาไว้ การใช้อำนาจดังกล่าว ถือเป็นการละเมิดสิทธิของประชาชน จึงควรมีการบัญญัติให้เจ้าหน้าที่รัฐต้องขออนุญาตจากศาลก่อนดำเนินการเพื่อเป็นการตรวจสอบถ่วงดุลการใช้อำนาจโดยองค์กรตุลาการ

ประการที่สี่ นอกจากการตรวจสอบถ่วงดุลอำนาจโดยองค์กรตุลาการแล้ว ควรกำหนดให้มีการตรวจสอบถ่วงดุลอำนาจโดยองค์กรอัยการอีกชั้นหนึ่งด้วย กล่าวคือ ให้ กกม. ยื่นคำร้องต่อพนักงานอัยการเพื่อให้พนักงานอัยการเข้ามามีบทบาทในการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐในการเข้าตรวจค้นสถานที่นั้น ๆ โดยกำหนดให้พนักงานอัยการมีหน้าที่ขอออกหมายอาญาต่อศาล จากนั้นจึงให้ศาลพิจารณาออกหมายอีกครั้งหนึ่ง ส่วนในกรณีของภัยคุกคามทางไซเบอร์ในระดับวิกฤตินั้น คณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจในการดำเนินการได้ทันทีเท่าที่จำเป็น โดยจะต้องยื่นคำร้องต่อพนักงานอัยการ เพื่อพิจารณาการขอออกหมายอาญา ภายหลังจากการดำเนินการดังกล่าวไปแล้ว จึงให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว หากไม่ได้รับอนุญาตจากศาลให้คำสั่งดังกล่าวสิ้นผลไป

ประการที่ห้า ตามพระราชบัญญัติ ฯ กำหนดให้สามารถอุทธรณ์คำสั่งได้เฉพาะกรณีของภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น จึงควรมีการแก้ไขให้สามารถอุทธรณ์คำสั่งอันเกี่ยวกับมาตรการในการรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรงและในระดับวิกฤติได้ด้วย โดยกำหนดให้สามารถอุทธรณ์คำสั่งดังกล่าวได้ภายใน 30 วัน นับแต่วันที่ได้รับคำสั่ง

ซึ่งการค้นคว้าอิสระฉบับดังกล่าวเน้นการศึกษาเปรียบเทียบบทบัญญัติแห่งกฎหมายและหลักเกณฑ์ในการดำเนินการของรัฐเป็นหลัก โดยกล่าวถึงปัญหาการตรวจสอบถ่วงดุลอำนาจตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ว่าตามพระราชบัญญัติดังกล่าวมีปัญหาใน

การตรวจสอบถ่วงดุลการใช้อำนาจในกรณีใดบ้าง ไม่ว่าจะเป็นปัญหาของมาตรการที่อาจส่งผลกระทบต่อสิทธิเสรีภาพของประชาชน ปัญหาการล่วงละเมิดสิทธิความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล สิทธิความเป็นส่วนตัวในการติดต่อสื่อสาร สิทธิความเป็นส่วนตัวในการอยู่หรือพักอาศัย ปัญหาการตรวจสอบการใช้อำนาจรัฐ เช่น การตรวจสอบภายในองค์กร และการตรวจสอบภายนอกองค์กรโดยองค์กรตุลาการ องค์กรอัยการ หรือโดยประชาชน เปรียบเทียบกับบทบัญญัติแห่งกฎหมายของประเทศสหรัฐอเมริกา และประเทศสิงคโปร์ที่มีการนำหลักการต่าง ๆ ในการคุ้มครองสิทธิเสรีภาพของประชาชนมาประกอบการดำเนินการต่าง ๆ เกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มากกว่าและชัดเจนกว่า โดยได้นำหลักการของกฎหมายต่างประเทศไม่ว่าจะเป็นประเทศสหรัฐอเมริกาหรือประเทศสิงคโปร์มาประกอบกับแนวความคิดในการคุ้มครองสิทธิเสรีภาพของประชาชน เพื่อนำมาปรับใช้กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศไทย[8]

เมื่อพิจารณาประเด็นข้อเสนอแนะทั้ง 5 ประการดังกล่าวแล้ว ประการที่สำคัญที่เกี่ยวข้องกับวิทยานิพนธ์ฉบับนี้ของผู้เขียนได้แก่ประการที่ 1 ซึ่งเกี่ยวกับมาตรา 70 ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ในประเด็นที่มีลักษณะทำให้บทบัญญัติดังกล่าวสามารถนำมาใช้เป็นมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ประการหนึ่งของเจ้าหน้าที่รัฐ โดยในมาตรา 70 วรรคสอง กำหนดว่า “ความในวรรคแรกไม่ให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือกฎหมายอื่น หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ” ซึ่งข้อเสนอแนะของการค้นคว้าอิสระฉบับดังกล่าวเสนอให้แก้ไขมาตรา 70 วรรคสอง ดังนี้ “ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด และมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดอื่นตามพระราชบัญญัติฉบับนี้ หรือผู้กระทำความผิดตามกฎหมายอื่น ผู้ใดฝ่าฝืนต้องระวางโทษ...”

เมื่อผู้เขียนได้ทำการศึกษาเพิ่มเติมมีความเห็นว่า ในการแก้ไขบทบัญญัติมาตรา 70 ที่กำหนดให้สามารถเปิดเผยหรือส่งมอบข้อมูลซึ่งได้มาเหล่านั้นเพื่อประโยชน์ในการดำเนินคดีกับ

---

[8] Ibid., หน้า 45 - 62.

ผู้กระทำความผิดตามกฎหมายอื่น จะต้องมีการพิจารณาเปรียบเทียบกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศว่าได้มีการกำหนดหลักเกณฑ์ในลักษณะดังกล่าวเอาไว้หรือไม่ และมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีลักษณะเป็นการแสวงหาพยานหลักฐานดังกล่าวมีความเหมือนหรือแตกต่างจากมาตรการในต่างประเทศหรือไม่ นอกจากนี้ การที่จะพิจารณาถึงความเหมาะสมของข้อกำหนดให้สามารถเปิดเผยหรือส่งมอบข้อมูลซึ่งได้มาเหล่านั้นเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่นได้

อีกทั้งจะต้องพิจารณาเปรียบเทียบกับมาตรการในการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาอันเป็นหลักการพื้นฐานเพื่อให้เห็นถึงแนวความคิดเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานในประเทศ เพื่อให้สามารถพิจารณาได้อย่างเหมาะสมว่าการกำหนดในลักษณะดังกล่าวมีความสอดคล้องกับแนวคิดและหลักการตามประมวลกฎหมายวิธีพิจารณาความอาญาของไทยหรือไม่

นอกจากนี้ยังควรที่พิจารณาเปรียบเทียบมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติไซเบอร์ ฯ กับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของต่างประเทศเพื่อให้ทราบถึงหลักการต่าง ๆ เกี่ยวกับการแสวงหาพยานพยานหลักฐาน ไม่ว่าจะเป็นหลักการในการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐ หรือหลักการในการคุ้มครองสิทธิเสรีภาพของประชาชนต่าง ๆ ว่ามีการกำหนดไว้เช่นไร และมีหลักการที่เหมาะสมจะนำมาปรับใช้กับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศไทยหรือไม่

โดยวิทยานิพนธ์ของผู้เขียนฉบับนี้จะให้ความสำคัญในการศึกษาเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของประเทศไทยเป็นสำคัญ โดยเฉพาะมาตรการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ว่าในปัจจุบันการที่กำหนดให้สามารถเปิดเผยหรือส่งมอบข้อมูลซึ่งได้มาเหล่านั้นเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่นมีหลักการต่าง ๆ ประกอบการใช้อำนาจดังกล่าวซึ่งมีลักษณะเป็นการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ เพราะสามารถนำข้อมูลซึ่งได้มาตามมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ไปใช้เป็นพยานหลักฐานในฐานความผิดอื่น ๆ ได้ อันเป็นการกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน จึงควรที่จะได้มีการศึกษาเพื่อเสนอแนะแนวทางแก้ไขที่เหมาะสมต่อไป

(2) วิทยานิพนธ์ เรื่อง ปัญหาทางกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญา โดย นางสาวกุลนิดา ผิตินาวิน นิติศาสตรมหาบัณฑิต กลุ่มวิชากฎหมายอาญาและกระบวนการยุติธรรมทางอาญา คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม ปีการศึกษา 2564

โดยวิทยานิพนธ์ฉบับดังกล่าวได้ทำการศึกษาวิจัยเกี่ยวกับปัญหาการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญา โดยทำการศึกษาแนวคิดหลักการ และบทบัญญัติกฎหมายของต่างประเทศที่เกี่ยวข้องกับปัญหาดังกล่าว ได้แก่ ประเทศสหรัฐอเมริกา ประเทศอังกฤษ และเครือรัฐออสเตรเลีย รัฐควีนส์แลนด์ เพื่อนำมาวิเคราะห์และเสนอแนะแนวทางในการปรับปรุงแก้ไขกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทย เนื่องจากการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญาของพนักงานสอบสวนเป็นกระบวนการที่สำคัญอย่างยิ่ง และพยานหลักฐานอิเล็กทรอนิกส์มีลักษณะเฉพาะแตกต่างไปจากพยานหลักฐานทั่วไป ซึ่งอาจเป็นข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองตามรัฐธรรมนูญ แต่บทบัญญัติกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญาทั่วไปตามประมวลกฎหมายวิธีพิจารณาความอาญา กลับมีเพียงบทบัญญัติกำหนดอำนาจและขอบเขตการใช้อำนาจของพนักงานสอบสวนเป็นการทั่วไป แม้จะมีกฎหมายพิเศษฉบับอื่นที่กำหนดอำนาจในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ของเจ้าหน้าที่รัฐตามกฎหมายพิเศษอื่น แต่ก็ไม่ครอบคลุมและมีประสิทธิภาพมากพอ อีกทั้งยังขาดมาตรการเกี่ยวกับการตรวจสอบความถูกต้องแท้จริงของพยานหลักฐานที่ได้มา และแนวทางขั้นตอนปฏิบัติงานในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ ซึ่งอาจทำให้การดำเนินงานด้านการรวบรวมพยานหลักฐานไม่เป็นไปตามมาตรฐาน และส่งผลต่อความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ในคดี จึงมีปัญหาที่จำเป็นต้องทำการศึกษา 3 ประการ ดังนี้

ประการที่หนึ่ง ปัญหาการกำหนดบทบัญญัติเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในประมวลกฎหมายอาญา เนื่องจากข้อมูลหรือสารสนเทศจากอุปกรณ์อิเล็กทรอนิกส์และระบบเครือข่ายออนไลน์อาจเป็นประโยชน์ในการสืบสวนความผิดทางอาญาและนำมาใช้เป็นพยานหลักฐานเพื่อพิสูจน์ข้อเท็จจริงในคดีได้ แต่มาตรการตามประมวลกฎหมายวิธีพิจารณาความอาญาไม่ครอบคลุมไปถึงพยานหลักฐานอิเล็กทรอนิกส์ การจะใช้อำนาจเพื่อเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ไม่สามารถใช้เพียงแค่อำนาจในการยึดและค้นได้ จำเป็นต้องมีอำนาจพิเศษบางประการเพื่อเข้าถึงพยานหลักฐานเหล่านั้น แม้จะมีการบัญญัติอำนาจในการรวบรวม

พยานหลักฐานอิเล็กทรอนิกส์ไว้ในกฎหมายพิเศษอื่น ก็ยังคงขาดประสิทธิภาพในการดำเนินการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ พนักงานสอบสวนจำเป็นต้องขอความร่วมมือกับเจ้าหน้าที่รัฐตามกฎหมายพิเศษและหน่วยงานที่เกี่ยวข้อง และกฎหมายพิเศษหลายฉบับที่ได้มีการกำหนดรายละเอียดไว้แตกต่างกันก็อาจทำให้เกิดความขัดข้องและยากลำบากต่อการเก็บรวบรวมพยานหลักฐานโดยไม่จำเป็น อีกทั้งยังทำให้ต้องใช้ระยะเวลานานที่จะนำพยานหลักฐานอิเล็กทรอนิกส์เข้าสู่สำนวนการสอบสวนได้

ประการที่สอง ปัญหาเกี่ยวกับอำนาจและขอบเขตอำนาจของพนักงานสอบสวนในการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ แม้ว่าพนักงานสอบสวนจะมีอำนาจในการรวบรวมพยานหลักฐานได้ทุกชนิดเท่าที่จะสามารถพิสูจน์ข้อเท็จจริงในคดีได้ แต่เนื่องด้วยบทบัญญัติในประมวลกฎหมายวิธีพิจารณาความอาญาอาจเป็นการจำกัดการค้นหาความจริงของพนักงานสอบสวน โดยเฉพาะในกรณีของพยานหลักฐานอิเล็กทรอนิกส์ ที่จำเป็นต้องใช้เทคโนโลยีหรือความรู้ความสามารถเกี่ยวกับเทคโนโลยีเข้ามาช่วยในการเก็บรวบรวมและตรวจพิสูจน์พยานหลักฐาน การที่พนักงานสอบสวนต้องใช้ดุลพินิจในการเก็บรวบรวมพยานหลักฐานตามอำนาจที่บัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาเท่านั้น อาจทำให้ไม่สามารถรวบรวมพยานหลักฐานได้ครบถ้วน การขาดบทกำหนดอำนาจที่เหมาะสมเพื่อใช้เก็บรวบรวมพยานหลักฐานอาจส่งผลร้ายต่อการดำเนินกระบวนการยุติธรรมทางอาญา อีกทั้งการเก็บรวบรวมพยานหลักฐานอาจเป็นการก้าวล่วงเข้าไปในสิทธิส่วนบุคคล การกำหนดขอบเขตของการก้าวล่วงเข้าไปในสิทธิส่วนบุคคลเช่นนั้น จะสามารถกระทำได้มากน้อยเพียงใดจึงควรที่จะต้องอยู่ภายใต้บังคับของกฎหมายซึ่งมีการบัญญัติไว้อย่างชัดเจน

ประการที่สาม ปัญหาเกี่ยวกับแนวทางขั้นตอนในการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ เนื่องจากพยานหลักฐานอิเล็กทรอนิกส์จำเป็นต้องใช้กระบวนการที่เหมาะสมเพื่อเก็บรวบรวมและใช้กระบวนการตรวจพิสูจน์ทางดิจิทัล อันจะทำให้พยานหลักฐานที่ได้มานั้นมีน้ำหนักและสามารถใช้เป็นหลักฐานที่ศาลยอมรับฟังได้ แม้กฎหมายของไทยจะมีกฎหมายที่บัญญัติถึงการรักษาความน่าเชื่อถือและการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ไว้ แต่กลับไม่มีการกำหนดกฎหมายเกี่ยวกับกระบวนการขั้นตอนหรือมาตรฐานการปฏิบัติงานในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ของพนักงานสอบสวน และให้การใช้อำนาจเพื่อรวบรวมพยานหลักฐานเป็นไปตามดุลพินิจของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญารวมถึงกฎหมายเฉพาะอื่น

เท่านั้น ทำให้การใช้อำนาจของพนักสอบสวนปราศจากบทบัญญัติที่กำหนดวิธีการปฏิบัติที่ชัดเจนและไม่มีผลบังคับใช้ในกรณีที่พนักงานสอบสวนปฏิบัติหน้าที่โดยมิชอบ หรือไม่เป็นไปตามหลักเกณฑ์ที่เหมาะสม การกำหนดหลักเกณฑ์หรือแนวปฏิบัติให้ชัดเจนย่อมเพิ่มประสิทธิภาพในการเก็บรักษาพยานหลักฐานอิเล็กทรอนิกส์และการตรวจสอบพยานหลักฐานอิเล็กทรอนิกส์ในการดำเนินคดีอาญา

จากปัญหาทั้งสามประการข้างต้น จึงควรมีการกำหนดกฎหมายเกี่ยวกับหลักเกณฑ์และแนวทางในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ให้ชัดเจน โดยนำบทบัญญัติเกี่ยวกับการได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ของต่างประเทศมาปรับใช้อย่างเหมาะสม ไม่ว่าจะเป็นประเทศสหรัฐอเมริกาที่ปรากฏอยู่ในหลักเกณฑ์วิธีพิจารณาความอาญาของรัฐบาลกลาง (Federal Rules of Criminal Procedure) และกฎหมายฉบับอื่น ๆ ที่เกี่ยวข้อง ประเทศอังกฤษที่ปรากฏอยู่ในกฎหมายอำนาจและความรับผิดชอบของเจ้าหน้าที่ตำรวจ ค.ศ. 1984 (Police and Criminal Evidence Act 1984 : PACE) และรัฐควีนส์แลนด์ เครือรัฐออสเตรเลีย ที่ปรากฏอยู่ในกฎหมายอำนาจและความรับผิดชอบของเจ้าหน้าที่ตำรวจ ค.ศ. 2020 (Police Power and Responsibilities Act 2020) มาปรับใช้กับบทบัญญัติของประเทศไทย เพื่อให้ประเทศไทยมีบทบัญญัติที่เกี่ยวกับการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์โดยเฉพาะในประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งเป็นกฎหมายทั่วไป โดยได้มีข้อเสนอแนะให้มีการแก้ไขในประเด็นต่าง ๆ ดังนี้

ข้อเสนอแนะในการแก้ไขกฎหมาย ได้แก่

ประการแรก ควรมีการเพิ่มบทบัญญัติเกี่ยวกับการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในประมวลกฎหมายวิธีพิจารณาความอาญาอาญา

ประการที่สอง ควรมีการเพิ่มบทบัญญัติเกี่ยวกับอำนาจของพนักงานสอบสวนในการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในประมวลกฎหมายวิธีพิจารณาความอาญา

ประการที่สาม ควรมีการเพิ่มบทบัญญัติเกี่ยวกับขอบเขตของการใช้อำนาจของพนักงานสอบสวนในการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา

ประการที่สี่ ควรมีการเพิ่มกฎกระทรวงกำหนดเกี่ยวกับรายละเอียดและขั้นตอนในการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ของพนักงานสอบสวนเพิ่มเติมจากประมวลกฎหมายวิธีพิจารณาความอาญา

ข้อเสนอแนะเชิงนโยบาย ได้แก่

ประการแรก ควรมีการพัฒนาบุคลากรให้มีความรู้ ความเข้าใจ และความสามารถในการปฏิบัติงานด้านการเก็บรวบรวมและตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ โดยให้อยู่ภายใต้มาตรฐานเดียวกันและทัดเทียมกับมาตรฐานสากล รวมถึงการพัฒนาอุปกรณ์ ตลอดจนองค์ความรู้ทางเทคโนโลยีสารสนเทศ เพื่อให้พนักงานสอบสวนและผู้ที่เกี่ยวข้องสามารถดำเนินกระบวนการยุติธรรมได้อย่างมีประสิทธิภาพ

ประการที่สอง ควรมีการจัดการศึกษาอบรมพนักงานสอบสวน เจ้าหน้าที่พิสูจน์หลักฐาน และหน่วยงานที่เกี่ยวข้องกับกระบวนการยุติธรรมทางอาญา ให้มีความรู้เบื้องต้นเกี่ยวกับพยานหลักฐานอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศในยุคสมัยใหม่ อีกทั้งหน่วยงานภาครัฐควรจัดทรัพยากรเพื่อรองรับสนับสนุนงานสอบสวนได้อย่างเพียงพอและมีประสิทธิภาพ และจัดให้มีการอบรมหรือฝึกปฏิบัติในด้านการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ให้กับพนักงานสอบสวนและเจ้าหน้าที่ที่มีอำนาจในการเก็บรวบรวมพยานหลักฐาน

วิทยานิพนธ์ฉบับดังกล่าว ได้มีการศึกษามาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ทั้งในประเทศไทยและต่างประเทศ เพื่อแสวงหาแนวทางที่เหมาะสมแก่การปรับใช้กับบทบัญญัติทั่วไปเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ อำนาจและขอบเขตอำนาจในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ รวมไปถึงรายละเอียดของขั้นตอนในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ของประเทศไทย โดยมีการเสนอแนะให้แก้ไขเพิ่มเติมบทบัญญัติในประมวลกฎหมายวิธีพิจารณาความอาญา เพิ่มเติมบทบัญญัติเพื่อกำหนดรายละเอียดของขั้นตอนในการดำเนินงาน รวมไปถึงข้อเสนอแนะในเชิงนโยบาย โดยมีการนำบทบัญญัติและหลักเกณฑ์ต่าง ๆ ที่มีความเหมาะสมของต่างประเทศมาปรับใช้แก่บทบัญญัติของประเทศไทย ส่วนวิทยานิพนธ์ของผู้เขียนฉบับนี้ แม้จะได้มีการศึกษามาตรการเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในต่างประเทศเช่นเดียวกันกับวิทยานิพนธ์ฉบับข้างต้น แต่ได้มีการศึกษาเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วย เพื่อเสนอแนะแนวทางแก้ไขเกี่ยวกับบทบัญญัติตามพระราชบัญญัติ

การรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรา 70 วรรคสอง ที่กำหนดให้เจ้าหน้าที่รัฐสามารถเปิดเผยและส่งมอบข้อมูลต่าง ๆ ซึ่งได้มาตามมาตรการต่าง ๆ ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่น อันมีลักษณะเป็นการให้อำนาจแก่เจ้าหน้าที่รัฐในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ อันอาจกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนเกินสมควร ให้มีความเหมาะสมมากยิ่งขึ้น โดยนำหลักเกณฑ์เกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของต่างประเทศที่มีความคล้ายคลึงกับมาตรการในการแสวงหาพยานหลักฐานบททั่วไปตามประมวลกฎหมายวิธีพิจารณาความอาญามาปรับใช้ประกอบกับการเปิดเผยและส่งมอบข้อมูลดังกล่าว

บทที่ 2
แนวความคิดและทฤษฎีเกี่ยวกับการแสวงหาพยานหลักฐาน

การแสวงหาพยานหลักฐานเป็นกระบวนการที่สำคัญในกระบวนการยุติธรรมทางอาญาเพื่อพิสูจน์ถึงข้อเท็จจริงในคดี มาตรการในการแสวงหาพยานหลักฐานของเจ้าหน้าที่รัฐถูกบัญญัติไว้ในกฎหมายฉบับต่าง ๆ หลายฉบับด้วยกัน ไม่ว่าจะเป็นประมวลกฎหมายวิธีพิจารณาความอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 เป็นต้น ซึ่งมาตรการในการแสวงหาพยานหลักฐานเหล่านี้เป็นมาตรการที่กระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชน[9] ดังนั้น ในกำหนดมาตรการทางกฎหมายที่ให้อำนาจแก่เจ้าหน้าที่รัฐว่าจะเป็นมาตรการที่มุ่งเน้นในการควบคุมอาชญากรรมเป็นหลัก หรือมุ่งเน้นในการคุ้มครองสิทธิเสรีภาพของประชาชนเป็นหลัก ย่อมขึ้นอยู่กับกระบวนการยุติธรรมทางอาญาของประเทศนั้น ๆ ว่าจะมีรูปแบบในการดำเนินกระบวนยุติธรรมทางอาญาในลักษณะใด ซึ่งลักษณะของกระบวนการยุติธรรมทางอาญาดังกล่าวย่อมส่งผลต่อหลักเกณฑ์ในการจำกัดและตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐ ในบทนี้จะศึกษาในเรื่องของแนวคิดและทฤษฎีที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานในกระบวนการยุติธรรมและการจำกัดและตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ เพื่อใช้เป็นรากฐานในการศึกษาและเปรียบเทียบแนวคิดเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานตามมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยและต่างประเทศต่อไป

2.1 แนวคิดเกี่ยวกับการแสวงหาพยานหลักฐานในกระบวนการยุติธรรมทางอาญา

กระบวนการยุติธรรมทางอาญา (Criminal Justice) คือ รากฐานของสังคมรัฐ เป็นกระบวนการสำคัญในการรักษาสังคมให้เที่ยงธรรม สงบสุข และปลอดภัย ด้วยการบังคับใช้กฎหมายและคุ้มครองสิทธิเสรีภาพของประชาชน[10] กระบวนการยุติธรรมทางอาญาประกอบไปด้วย 2 แนวคิดหลักด้วยกัน คือ แนวคิดว่าด้วยการปราบปรามอาชญากรรมเพื่อรักษาไว้ซึ่งความสงบเรียบร้อยในสังคม และแนวคิดว่าด้วยการคุ้มครองสิทธิและเสรีภาพของประชาชน ซึ่งทั้งสองแนวคิดนี้ต่างแสดง

---

[9] นารี กิตติสมบูรณ์สุข, "การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์" (นิติศาสตรมหาบัณฑิต, นิติศาสตร์, มหาวิทยาลัยธุรกิจบัณฑิต, 2548), หน้า 5.

[10] อุทัย อาทิเวช, กฎหมายวิธีพิจารณาความอาญาและพยานชั้นสูง (นนทบุรี: สำนักพิมพ์ มหาวิทยาลัยสุโขทัยธรรมาธิราช), หน้า 5 - 6.

ออกมาผ่านรูปแบบของนโยบายของรัฐในการดำเนินกระบวนการยุติธรรมทางอาญา ซึ่งมีจุดมุ่งหมายเพื่อรักษาไว้ซึ่งความสงบเรียบร้อยของสังคม และในขณะเดียวกันจะต้องคำนึงถึงสิทธิและเสรีภาพของประชาชนโดยไม่ละเมิดสิทธิเสรีภาพของประชาชนเกินความเหมาะสมหรือเกินสมควร ในแต่ละประเทศย่อมมีหลักการเกี่ยวกับการแสวงหาพยานหลักฐานที่เหมือนและแตกต่างกันไปแล้วแต่ว่าประเทศนั้นให้ความสำคัญกับสิ่งใดเป็นหลัก ระหว่างมุ่งเน้นในการคุ้มครองสิทธิและเสรีภาพของประชาชนเป็นสำคัญหรือมุ่งเน้นในการปราบปรามอาชญากรรมเพื่อรักษาไว้ซึ่งความสงบเรียบร้อยในสังคมเป็นสำคัญ

ศาสตราจารย์ เฮอร์เบิร์ต แพคเกอร์ (Professor Herbert Packer) นักนิติศาสตร์ชาวอเมริกัน ได้ศึกษาและวิเคราะห์รูปแบบกระบวนการยุติธรรมทางอาญา โดยแยกเป็น 2 ทฤษฎีที่สำคัญ[11] ได้แก่ ทฤษฎีการควบคุมอาชญากรรม (Crime Control Theory) และทฤษฎีความชอบด้วยกระบวนการทางกฎหมาย (Due Process Theory) ซึ่งทั้งสองทฤษฎีนี้มีแนวคิดอันเป็นรากฐานของมาตรการในการดำเนินกระบวนการยุติธรรมทางอาญาที่แตกต่างกันอย่างชัดเจน ดังจะได้อธิบายต่อไป

2.1.1 ทฤษฎีการควบคุมอาชญากรรม

ทฤษฎีการควบคุมอาชญากรรม (Crime Control Theory) มุ่งเน้นในประสิทธิภาพของกระบวนการยุติธรรม ให้ความสำคัญในการควบคุม ระงับ และปราบปรามอาชญากรรมเป็นหลักเพื่อรักษาไว้ซึ่งความสงบเรียบร้อยในสังคม[12] การรักษาไว้ซึ่งความสงบสุขในสังคมเป็นหน้าที่ที่สำคัญที่สุดของกระบวนการยุติธรรมทางอาญา ซึ่งการที่จะรักษาไว้ซึ่งความสงบสุขในสังคมได้นั้น กระบวนการยุติธรรมจะต้องมีความรวดเร็ว รวบรัด และมีประสิทธิภาพ ในกรณีที่ผู้ต้องหาบริสุทธิ์จะต้องถูกกลั่นกรองออกไปอย่างรวดเร็ว และผู้ที่กระทำความผิดก็จะต้องถูกดำเนินคดีอย่างรวดเร็วเช่นเดียวกัน[13] หากรัฐไม่สามารถปราบปรามหรือควบคุมอาชญากรรมได้อย่างรวดเร็วและมี

---

[11] ธีสุทธิ์ พันธ์ฤทธิ์, การรับฟังพยานหลักฐานคดีอาญา : บทวิเคราะห์และวิจารณ์, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2558), หน้า 5.

[12] ประธาน วัฒนพานิช, "ระบบความยุติธรรมทางอาญา : แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม," 9, 2 (2520): หน้า 150.

[13] ธีสุทธิ์ พันธ์ฤทธิ์, การรับฟังพยานหลักฐานคดีอาญา : บทวิเคราะห์และวิจารณ์, หน้า 3.

ประสิทธิภาพ รัฐย่อมไม่สามารถรักษาไว้ซึ่งความสงบเรียบร้อยในสังคมได้ และทำให้สิทธิและเสรีภาพของประชาชนถูกคุกคามโดยอาชญากรรมที่เกิดขึ้น[14]

ด้วยเหตุที่ทฤษฎีการควบคุมอาชญากรรมให้ความสำคัญกับการควบคุมและปราบปรามอาชญากรรมอย่างรวดเร็ว รวบรัด และมีประสิทธิภาพ มาตรการในการแสวงหาพยานหลักฐานตามทฤษฎีนี้จึงกำหนดให้เจ้าหน้าที่รัฐมีอำนาจในการรวบรวมและแสวงหาพยานหลักฐานอย่างกว้างขวาง[15] เพื่อให้องค์กรหรือหน่วยงานต่าง ๆ ในกระบวนการยุติธรรมทางอาญาสามารถดำเนินการไปได้อย่างรวดเร็ว รวบรัด และมีประสิทธิภาพในการควบคุมและปราบปรามอาชญากรรมเพื่อรักษาไว้ซึ่งความสงบสุขในสังคม สิทธิและเสรีภาพของประชาชน ผู้ต้องหา หรือบุคคลอื่น ๆ ที่เกี่ยวข้องกับอาชญากรรมจึงได้รับความคุ้มครองในขอบเขตที่จำกัด มีความสำคัญรองลงมาจากอำนาจของเจ้าหน้าที่รัฐในการควบคุมและปราบปรามอาชญากรรม แม้การกระทำของเจ้าหน้าที่รัฐในกระบวนการยุติธรรมทางอาญาจะกระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชนก็ตาม แต่เพื่อความสงบสุขของสังคมแล้วก็ย่อมสามารถกระทำได้

โดยสรุปแล้วสามารถจำแนกหลักการและแนวคิดที่สำคัญของทฤษฎีการควบคุมอาชญากรรมออกได้เป็นหลายประการด้วยกัน ดังนี้[16]

(1) การปราบปรามอาชญากรรมเป็นหน้าที่ที่สำคัญที่สุดของกระบวนการยุติธรรมทางอาญา เพราะความเป็นระเบียบเรียบร้อยเป็นสิ่งที่จำเป็นและสำคัญที่สุดสำหรับสังคมเสรีประชาธิปไตย

(2) กระบวนการยุติธรรมทางอาญาควรมุ่งเน้นในการพิสูจน์ถึงสิทธิของเหยื่อจากอาชญากรรมมากกว่าการที่จะมุ่งคุ้มครองสิทธิของผู้กระทำความผิด

---

[14] ประธาน วัฒนพานิช, "ระบบความยุติธรรมทางอาญา : แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม," หน้า 150.

[15] ธีสุทธิ์ พันธ์ฤทธิ์, การรับฟังพยานหลักฐานคดีอาญา : บทวิเคราะห์และวิจารณ์, หน้า 4.

[16] Flaviu Ciopec, "Crime Control or Due Process? Which Are the Tendencies in Romanian Criminal Justice?," ใน Journal of Eastern-European Criminal Law(Faculty of Law West University of Timisoara, 2017), pp. หน้า 193 - 194.

(3) ควรให้อำนาจแก่เจ้าหน้าที่ตำรวจและพนักงานอัยการในการดำเนินการอย่างกว้างขวาง เพื่อให้ง่ายต่อการสืบสวนสอบสวน การจับกุม การค้น การยึด และการดำเนินคดีเพื่อพิพากษาลงโทษผู้กระทำความผิด

(4) กฎเกณฑ์ที่กำหนดขึ้นโดยมีวัตถุประสงค์ที่เฉพาะเจาะจงในการยับยั้ง หรือเป็นอุปสรรคต่อการทำงานของหน่วยงานในกระบวนการยุติธรรมทางอาญาไม่ควรถูกบัญญัติขึ้นมา

(5) กระบวนการยุติธรรมทางอาญาควรดำเนินการอย่างรวดเร็ว รวบรัด และมีประสิทธิภาพ

(6) หากเจ้าหน้าที่ตำรวจเสนอให้ทำการจับกุม และพนักงานอัยการได้ยื่นฟ้องจำเลยเป็นคดีต่อศาล จำเลยควรถูกสันนิษฐานว่ามีความผิดจริงตามคำฟ้อง เพราะการสืบสวนสอบสวนข้อเท็จจริงต่าง ๆ ของเจ้าหน้าที่ตำรวจและพนักงานอัยการมีความน่าเชื่อถือสูง

2.1.2 ทฤษฎีความชอบด้วยกระบวนการทางกฎหมาย

ทฤษฎีความชอบด้วยกระบวนการทางกฎหมาย (Due Process Theory) มุ่งเน้นในเรื่องความเป็นธรรมในกระบวนการยุติธรรม ให้ความสำคัญในตัวบทบัญญัติของกฎหมาย และยึดหลักการคุ้มครองสิทธิและเสรีภาพของประชาชนเป็นหลัก มากกว่าประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรม ดังนั้นการใช้อำนาจของเจ้าหน้าที่รัฐ และกระบวนการของรัฐจะต้องดำเนินการตามขั้นตอนต่าง ๆ ที่กฎหมายบัญญัติไว้โดยเคร่งครัดและสามารถตรวจสอบได้ในทุก ๆ ขั้นตอน การกระทำใดที่เป็นการละเมิดสิทธิและเสรีภาพของประชาชนต้องมีบทบัญญัติของกฎหมายให้อำนาจไว้อย่างชัดเจน[17] ซึ่งเป็นไปตามแนวความคิดของหลักนิติธรรม (The Rule of Law) เพื่อไม่ให้เจ้าหน้าที่รัฐใช้อำนาจหรือดุลพินิจได้อย่างกว้าง และเป็นการกระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชนเกินสมควร เนื่องจากในการดำเนินการในการค้นหาข้อเท็จจริงซึ่งกระทำโดยเจ้าหน้าที่ตำรวจ พนักงานอัยการ หรือเจ้าหน้าที่ฝ่ายปกครอง ส่วนใหญ่เป็นการดำเนินการในที่รโหฐาน ซึ่งอาจใช้วิธีการหลอกลวง ขู่เข็ญ หรือกระทำการใด ๆ อันมีลักษณะเป็นการ

[17] ประธาน วัฒนพานิช, "ระบบความยุติธรรมทางอาญา : แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม," หน้า 152.

กระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชนอย่างร้ายแรง โดยที่กฎหมายไม่ได้มีการบัญญัติให้อำนาจไว้[18]

ในประเทศที่มีรูปแบบกระบวนการยุติธรรมทางอาญาไปในทิศทางของทฤษฎีความชอบด้วยกระบวนการทางกฎหมายหรือหลักนิติธรรม จะกำหนดบทบัญญัติของกฎหมาย กฎเกณฑ์ หรือมาตรการเกี่ยวกับการแสวงหาพยานหลักฐานอยู่บนพื้นฐานของการคุ้มครองสิทธิและเสรีภาพของประชาชน บทบัญญัติของกฎหมาย กฎเกณฑ์ หรือมาตรการใดที่เป็นการแทรกแซงหรือกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนมากเกินไปจะไม่ถูกนำมาใช้ หรือหากถูกนำมาใช้จะต้องมีการจำกัดอำนาจของเจ้าหน้าที่เจ้าหน้าที่รัฐ และจะต้องมีการตรวจสอบการใช้อำนาจเสมอ[19] ดังนั้น ในการใช้อำนาจของเจ้าพนักงาของรัฐจะต้องปฏิบัติตามบทบัญญัติของกฎหมายโดยเคร่งครัดและไม่สามารถใช้อำนาจได้อย่างกว้างขวาง

โดยสรุปแล้วสามารถจำแนกหลักการและแนวคิดที่สำคัญของทฤษฎีความชอบด้วยกระบวนการทางกฎหมายออกได้เป็นหลายประการด้วยกัน ดังนี้[20]

(1) หน้าที่ที่สำคัญที่สุดของกระบวนการยุติธรรมทางอาญาคือการจัดหาและให้ความเป็นธรรมขั้นพื้นฐานทางกฎหมายให้แก่บุคคลทุกคน

(2) กระบวนการยุติธรรมทางอาญาควรมุ่งเน้นให้ความสำคัญกับสิทธิของจำเลยเป็นหลัก ไม่ใช่สิทธิของเหยื่อ เพราะในรัฐธรรมนูญมักจะมีบทบัญญัติเกี่ยวกับการคุ้มครองสิทธิของผู้ต้องหาไว้โดยชัดแจ้ง

(3) ควรจำกัดอำนาจในการดำเนินการต่าง ๆ ของเจ้าหน้าที่ตำรวจและพนักงานอัยการเพื่อป้องกันการใช้อำนาจหน้าที่ดังกล่าวโดยมิชอบ อันจะเป็นการละเมิดสิทธิเสรีภาพของประชาชน

(4) สิทธิของประชาชนตามรัฐธรรมนูญไม่ใช่กฎเกณฑ์ที่กำหนดขึ้นโดยมีวัตถุประสงค์ที่เฉพาะเจาะจงบางอย่างเท่านั้น แต่หน่วยงานในกระบวนการยุติธรรมทางอาญาจะต้องรับผิดชอบต่อ

---

[18] ธีสุทธิ์ พันธ์ฤทธิ์, การรับฟังพยานหลักฐานคดีอาญา : บทวิเคราะห์และวิจารณ์, หน้า 4.

[19] Ibid., หน้า 4.

[20] Flaviu Ciopec, "Crime Control or Due Process? Which Are the Tendencies in Romanian Criminal Justice?," หน้า 194.

กฎระเบียบ ขั้นตอน และแนวทางการปฏิบัติเพื่อให้มั่นใจว่าจะมีความเป็นธรรมและมีความสม่ำเสมอในการดำเนินกระบวนการยุติธรรมทางอาญา

(5) กระบวนการยุติธรรมทางอาญาควรมีลักษณะเป็นอุปสรรคต่อการดำเนินการต่าง ๆ มีลักษณะเป็นขั้นตอนตามลำดับเพื่อป้องกันการใช้อำนาจหน้าที่โดยมิชอบของหน่วยงานในกระบวนการยุติธรรมทางอาญา และปกป้องผู้บริสุทธิ์หรือลงโทษผู้มีความผิดตามข้อเท็จจริง

(6) กระบวนการยุติธรรมทางอาญาไม่ควรถือว่าบุคคลใดมีความผิดเพียงเพราะข้อเท็จจริง บุคคลควรถูกตัดสินว่ามีความผิดก็ต่อเมื่อการใช้อำนาจต่าง ๆ ของหน่วยงานในกระบวนการยุติธรรมทางอาญาเป็นไปอย่างถูกต้องตามขั้นตอนของกฎหมาย ไม่ว่าจะเป็นขั้นตอนในการสืบสวนสอบสวนเพื่อหาข้อเท็จจริง หรือขั้นตอนในการพิจารณาคดีก็ตาม

ดังนั้น การที่รัฐจะกำหนดนโยบายในการดำเนินกระบวนการยุติธรรมทางอาญาในลักษณะใดย่อมขึ้นอยู่กับว่ารัฐนั้น ๆ ให้ความสำคัญในประสิทธิภาพของกระบวนการยุติธรรมเป็นสำคัญ หรือจะให้ความสำคัญกับการคุ้มครองสิทธิและเสรีภาพของประชาชนเป็นสำคัญ เพราะมาตรการในการแสวงหาพยานหลักฐานเป็นจุดเริ่มต้นของกระบวนการยุติธรรมทางอาญา การจะพิสูจน์ข้อเท็จจริงว่าบุคคลใดได้กระทำความผิดจริง หรือบุคคลใดเป็นผู้บริสุทธิ์นั้น จะต้องพิจารณาจากพยานหลักฐานเป็นสำคัญ หากพยานหลักฐานชิ้นใดมีคุณค่าในเชิงพิสูจน์ (Probative Value)[21] สูง แต่การจะได้พยานหลักฐานชิ้นนั้นมาจำเป็นต้องแทรกแซงสิทธิและเสรีภาพของประชาชนเกินสมควร หากรัฐให้ความสำคัญในการควบคุมอาชญากรรมเป็นสำคัญย่อมให้อำนาจเจ้าหน้าที่รัฐอย่างกว้างขวางเพื่อนำพยานหลักฐานดังกล่าวเข้ามาสู่กระบวนการยุติธรรมทางอาญาเพื่อลงโทษผู้กระทำความผิดโดยเร็ว แต่หากรัฐให้ความสำคัญกับสิทธิและเสรีภาพของประชาชนเป็นสำคัญ นโยบายทางอาญาของรัฐอาจทำให้เจ้าหน้าที่รัฐไม่สามารถนำพยานหลักฐานดังกล่าวเข้าสู่กระบวนการยุติธรรมทางอาญาเพื่อพิสูจน์ถึงข้อเท็จจริงในคดีได้ ดังนั้นในหลายประเทศจึงได้มีการกำหนดนโยบายทางอาญาเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานโดยผสมผสานรูปแบบของทฤษฎีทางกระบวนการยุติธรรมทั้งสองไม่ว่าจะเป็นทฤษฎีการควบคุมอาชญากรรม หรือทฤษฎีความชอบด้วยกระบวนการทางกฎหมายเข้า

[21] จรัญ ภักดีกุล, กฎหมายลักษณะพยานหลักฐาน, พิมพ์ครั้งที่ 11 (กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2559), หน้า 302.

ด้วยกัน เพื่อสร้างความสมดุลระหว่างประโยชน์ของรัฐในการรักษาความสงบเรียบร้อยของสังคม และการคุ้มครองสิทธิเสรีภาพของประชาชน เพื่อให้เหมาะสมและเกิดประโยชน์สูงสุดแก่รัฐและประชาชน

2.2 แนวความคิดเกี่ยวกับหลักนิติรัฐและหลักนิติธรรม

"หลักนิติรัฐ" (Legal State) หรือ "หลักนิติธรรม" (Rule of Law) เป็นหลักการหนึ่งที่เป็นหลักประกันสิทธิและเสรีภาพของประชาชนให้พ้นจากการใช้อำนาจในทางที่ผิดของเจ้าหน้าที่รัฐ หน่วยงานของรัฐ หรือตัวรัฐเอง โดยหลักนิติรัฐเป็นหลักการพื้นฐานในระบบกฎหมายของประเทศเยอรมนี คำว่า "นิติรัฐ" เป็นคำที่แปลมาจากภาษาเยอรมนีว่า "Rechtsstaat" ซึ่งประกอบขึ้นจากคำสองคำ คือ คำว่า "Recht"[22] ที่แปลว่า "กฎหมาย" และคำว่า "Staat" ที่แปลว่า "รัฐ"[23] โดยการปกครองในนิติรัฐนั้น กฎหมายจะต้องไม่เปิดโอกาสให้ผู้ปกครองใช้อำนาจตามอำเภอใจ ภายใต้กฎหมายบุคคลทุกคนจะต้องเสมอภาคซึ่งกันและกัน[24] และบุคคลจะต้องสามารถทราบก่อนล่วงหน้าว่ากฎหมายมุ่งประสงค์จะบังคับให้ตนกระทำหรือไม่ให้กระทำสิ่งใด ผลร้ายอันเกิดจากการฝ่าฝืนกฎหมายคืออะไร ทั้งนี้เพื่อที่บุคคลจะได้ปฏิบัติให้ถูกต้องสอดคล้องกับกฎหมาย

แนวความคิดพื้นฐานดังกล่าวก่อให้เกิดหลักการต่าง ๆ ในทางกฎหมายตามมา เช่น หลักไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย[25] (nulla poena sine lege) หลักการห้ามลงโทษซ้ำซ้อน หลักการห้ามตรากฎหมายกำหนดโทษย้อนหลังแก่บุคคล เป็นต้น[26] ดังนั้น เมื่อแนวความคิดพื้นฐานของนิติรัฐ คือ การจำกัดอำนาจของรัฐโดยกฎหมาย การทำให้รัฐต้องผูกพันอยู่กับหลักการพื้นฐานและคุณค่าทางกฎหมายโดยไม่อาจบิดพริ้ว ด้วยเหตุนี้ หลักนิติรัฐจึงไม่ได้มีความหมายแค่เพียงการบังคับให้รัฐต้องคุ้มครองสิทธิเสรีภาพของบุคคลเพียงเท่านั้น แต่ยังเรียกร้องให้รัฐต้องดำเนินการใน

---

[22] คำว่า Recht ในภาษาเยอรมนีสามารถแปลว่า "สิทธิ" ได้ด้วย

[23] สุวิทย์ ปัญญาวงศ์, กฎหมายมหาชน, พิมพ์ครั้งที่ 2, บรรณาธิการ, (กรุงเทพมหานคร: วิญญูชน, 2561), หน้า 85 - 86. อ้างในอนัญพร สกุลเมฆา, "การตรวจสอบและถ่วงดุลอำนาจเจ้าพนักงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562," หน้า 7.

[24] เสาวนีย์ อัศวโรจน์, "สิทธิมนุษยชนกับกฎหมายปกครอง : การคุ้มครองสิทธิเสรีภาพของประชาชน," วารสารกระบวนการยุติธรรม Journal of Thai Justice System เล่มที่ 1 ปีที่ 3 มกราคม - มีนาคม 2553 (2553): หน้า 63.

[25] "หลักไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย" เป็นแนวคิดของนักปรัชญาทางตะวันตก แนวคิดนี้เป็นหลักสากล ในทางกฎหมาย ซึ่งมีอิทธิพลต่อกฎหมายของไทยมาจนกระทั่งปัจจุบัน เกิดขึ้นเพื่อให้ความเป็นธรรมกับบุคคลที่กระทำการสิ่งใดสิ่งหนึ่งผ่านมาแล้ว แต่ในขณะนั้น ไม่มีกฎหมายใดบัญญัติว่าสิ่งที่กระทำเป็นความผิดเอาไว้ หากมีการบัญญัติกฎหมายในภายหลังว่าการกระทำในอดีตนั้นเป็นความผิด และต้องรับโทษจะต้องนำตัวบุคคลดังกล่าวมาลงโทษ จะเป็นการละเมิดหลักดังกล่าวซึ่งไม่สามารถกระทำได้

[26] วรเจตน์ ภาคีรัตน์, "หลักนิติธรรมและหลักนิติรัฐ," จุลนิติ ม.ค. - ก.พ. 55(2555): หน้า 50 - 51.

ด้านต่าง ๆ เพื่อให้เกิดความเป็นธรรมขึ้นอย่างแท้จริงในสังคม ด้วยวัตถุประสงค์ดังกล่าวจะบรรลุได้ก็แต่โดยการสร้างระบบการคุ้มครองสิทธิเสรีภาพของบุคคลที่มีประสิทธิภาพ และการยอมรับให้มีองค์กรตุลาการขึ้นมาโดยเฉพาะ (ศาลรัฐธรรมนูญ) โดยให้องค์กรดังกล่าวพิทักษ์ปกป้องคุณค่าในรัฐธรรมนูญ ซึ่งรัฐธรรมนูญของเยอรมนีหลังสงครามโลกครั้งที่สองที่เรียกว่า “กฎหมายพื้นฐาน” (Grundgesetz) ได้ดำเนินรอยตามแนวทางของหลักนิติรัฐ และได้มีการบัญญัติให้หลักนิติรัฐเป็นหลักการพื้นฐานของรัฐธรรมนูญฉบับดังกล่าว[27]

ส่วน “หลักนิติธรรม” เป็นหลักการพื้นฐานสำคัญของรัฐธรรมนูญของประเทศอังกฤษ ซึ่งตั้งอยู่บน 2 หลักการที่สำคัญ ได้แก่ หลักอำนาจสูงสุดในทางนิติบัญญัติเป็นของรัฐสภา และหลักนิติธรรม[28] โดยนักกฎหมายรัฐธรรมนูญของประเทศอังกฤษที่มีบทบาทมากที่สุดคนหนึ่งในการช่วยพัฒนาหลักนิติธรรมก็คือ A.V. Dicey โดย Dicey เห็นว่าหลักนิติธรรม หมายถึง การที่บรรดาการกระทำทั้งหลายทั้งปวงของรัฐและฝ่ายปกครองจะต้องอยู่ภายใต้บังคับของกฎหมาย จะต้องไม่มีการกระทำการก้าวล่วงสิทธิและเสรีภาพของประชาชนตามอำเภอใจ หากปรากฏว่ารัฐหรือฝ่ายปกครองกระทำการขัดต่อกฎหมาย การกระทำดังกล่าวย่อมต้องถูกฟ้องคดียังศาลยุติธรรมได้ เพราะรัฐหรือเจ้าหน้าที่รัฐจะมีสิทธิพิเศษใด ๆ เหนือกว่าประชาชนไม่ได้ ซึ่งหลักนิติธรรมตามแนวความคิดของ Dicey มุ่งเน้นไปที่ความผูกพันต่อกฎหมายของฝ่ายบริหาร ไม่ได้เรียกร้องให้ฝ่ายนิติบัญญัติให้ต้องผูกพันต่อกฎเกณฑ์อื่นใดในการตรากฎหมาย การที่ Dicey ให้ความหมายของหลักนิติธรรมในแง่ที่ทุกคนต้องอยู่ภายใต้กฎหมายและภายใต้ศาลเดียวกันตามหลักความเสมอภาคต่อหน้ากฎหมาย ส่งผลให้เป็นการปฏิเสธการจัดตั้งศาลปกครองขึ้นมาเป็นอีกระบบศาลหนึ่ง โดย Dicey เห็นว่าหากจัดตั้งให้มีศาลปกครองหรือองค์กรอื่นซึ่งไม่ใช่ศาลยุติธรรมหรือศาลธรรมดาทำหน้าที่ตัดสินคดีปกครอง[29] จะส่งผลให้บรรดาข้าราชการต่าง ๆ ที่ถูกฟ้องในศาลปกครองว่ากระทำการโดยไม่ชอบด้วยกฎหมาย ย่อมอยู่ในฐานะที่ได้เปรียบกว่าประชาชนทั่วไป ซึ่ง Dicey เห็นว่าไม่ถูกต้อง แนวความคิดนี้ได้รับการยึดถือและเดินรอยตามในบรรดาประเทศที่ได้รับอิทธิพลจากระบบกฎหมายอังกฤษมาจนถึงปัจจุบัน[30]

---

[27] Ibid., หน้า 54.

[28] บรรเจิด สิงคะเนติ, หลักกฎหมายมหาชน หลักนิติธรรม/นิติรัฐในฐานะ "เกณฑ์" จำกัดอำนาจรัฐ, พิมพ์ครั้งที่ 3 (กรุงเทพมหานคร: วิญญูชน, 2560), หน้า 25.

[29] ณ เวลานั้นในประเทศฝรั่งเศสได้มีการจัดตั้งศาลปกครองขึ้นมาเป็นอีกระบบศาลหนึ่งคู่ขนานกันไปกับศาลยุติธรรม

[30] วรเจตน์ ภาคีรัตน์, "หลักนิติธรรมและหลักนิติรัฐ," จุลนิติ: หน้า 60 - 61.

2.2.1 หลักนิติธรรมในการจำกัดอำนาจของเจ้าหน้าที่รัฐ

ตามที่รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 26 วรรคหนึ่ง ได้บัญญัติว่า “การตรากฎหมายที่มีผลเป็นการจำกัดสิทธิหรือเสรีภาพของบุคคล ต้องเป็นไปตามเงื่อนไขที่บัญญัติไว้ในรัฐธรรมนูญ ในกรณีที่รัฐธรรมนูญมิได้บัญญัติเงื่อนไขไว้ กฎหมายดังกล่าวต้องไม่ขัดต่อหลักนิติธรรม ไม่เพิ่มภาระหรือจำกัดสิทธิหรือเสรีภาพของบุคคลเกินสมควรแก่เหตุ และจะกระทบต่อศักดิ์ศรีความเป็นมนุษย์ของบุคคลมิได้ รวมทั้งต้องระบุเหตุผลความจำเป็นในการจำกัดสิทธิและเสรีภาพไว้ด้วย” จากบทบัญญัติดังกล่าวย่อมนำมาสู่ความผูกพันของรัฐว่าการตรากฎหมายและการปฏิบัติหน้าที่ของผู้ใช้อำนาจรัฐต้องเป็นไปตามหลักนิติธรรม[31] สำหรับหลักนิติธรรมในประเทศไทยสามารถจำแนกได้เป็น 2 ประการด้วยกัน คือ 1. หลักนิติธรรมโดยเคร่งครัด และ 2. หลักนิติกรรมโดยทั่วไป

หลักนิติธรรมโดยเคร่งครัด หรือหลักนิติธรรมในความหมายอย่างแคบ หมายถึง หลักพื้นฐานแห่งกฎหมาย ที่กฎหมาย กระบวนการยุติธรรม หรือการกระทำใด ๆ จะต้องไม่ฝ่าฝืน ขัด หรือแย้งต่อหลักนิติธรรม โดยหลักนี้จะถูกล่วงละเมิดมิได้ หากฝ่าฝืน ขัด หรือแย้งต่อหลักนิติธรรม ย่อมไม่มีผลบังคับใช้[32] โดยหลักนิติธรรมโดยเคร่งครัด หรือหลักนิติธรรมในความหมายอย่างแคบมีหลักการสำคัญที่เกี่ยวข้อง ดังนี้

1) หลักความเป็นอิสระ และความเป็นกลางของผู้พิพากษาตุลาการ

2) กฎหมายต้องใช้บังคับเป็นการทั่วไป

3) กฎหมายต้องมีการประกาศใช้ให้ประชาชนทราบ

4) กฎหมายอาญาต้องไม่มีผลย้อนหลังในทางที่เป็นโทษ

5) ผู้ต้องหาหรือจำเลยในคดีอาญาต้องมีสิทธิในการต่อสู้คดี

6) เจ้าหน้าที่รัฐจะใช้อำนาจได้เท่าที่กฎหมายให้อำนาจ

7) กฎหมายจะยกเว้นความรับผิดให้แก่การกระทำที่ยังไม่เกิดขึ้นไม่ได้

---

[31] บรรเจิด สิงคะเนติ, หลักกฎหมายมหาชน หลักนิติธรรม/นิติรัฐในฐานะ "เกณฑ์" จำกัดอำนาจรัฐ, หน้า 59.

[32] เขตไท ลังการ์พินธ์, "หลักนิติธรรมของประเทศอังกฤษ และประเทศไทย : ความหมายและสาระสำคัญ," วารสารนิติศาสตร์ มหาวิทยาลัยนเรศวร ปีที่ 9, ฉบับที่ 2 พฤศจิกายน 2558 (2558): หน้า 31.

หลักนิติธรรมโดยทั่วไป หรือหลักนิติธรรมในความหมายอย่างกว้าง หมายถึง ลักษณะที่ดีของกฎหมาย กระบวนการยุติธรรมหรือการกระทำใด ๆ ที่อาจเรียกอีกอย่างหนึ่งว่าอุดมคติของกฎหมายและกระบวนการยุติธรรม โดยจะครบถ้วนหรือขาดตกบกพร่องไปบ้างก็ยังบังคับใช้ได้ตราบที่ไม่ขัดต่อหลักนิติธรรมโดยเคร่งครัด[33] โดยหลักนิติธรรมโดยทั่วไป หรือหลักนิติธรรมในความหมายอย่างกว้างมีหลักการสำคัญที่เกี่ยวข้อง ดังนี้

1) กฎหมายที่ดีต้องมีความชัดเจน

2) กฎหมายที่ดีต้องไม่ขัดแย้งกันเอง

3) กฎหมายที่ดีต้องมีเหตุผล

4) กฎหมายที่ดีต้องนำไปสู่ความเป็นธรรม

5) กฎหมายที่ดีต้องคุ้มครองสิทธิมนุษยชน ศักดิ์ศรีความเป็นมนุษย์ หรือสิทธิขั้นพื้นฐาน

6) กฎหมายที่ดีต้องทันสมัย และสามารถรับต่อความเปลี่ยนแปลงของสังคม เศรษฐกิจ การเมือง และวัฒนธรรม

7) กฎหมายที่ดีต้องบัญญัติตามกระบวนการและขั้นตอนที่กฎหมายบัญญัติไว้

8) กฎหมายที่ดีต้องไม่มีผลย้อนหลังเป็นผลร้าย หรือกระทบต่อสิทธิ หน้าที่ หรือความรับผิดของบุคคล

9) กฎหมายที่ดีต้องมีบทลงโทษที่เหมาะสม และได้สัดส่วนกับความผิด

10) กฎหมายที่ดีต้องมีการบังคับใช้อย่างมีประสิทธิภาพ และส่งเสริมให้ประชาชนมีความรู้ และเคารพกฎหมาย

11) กระบวนการนิติบัญญัติต้องเป็นกระบวนการที่เปิดเผย โปร่งใส และตรวจสอบได้

12) กระบวนการยุติธรรมที่ดีต้องเปิดโอกาสให้มีการอุทธรณ์

---

[33] Ibid., หน้า 35.

13) กระบวนการยุติธรรมที่ดีต้องเปิดโอกาสให้ประชาชนเข้าถึงได้โดยสะดวก ไม่ชักช้า ด้วยค่าใช้จ่ายที่เหมาะสม

14) กระบวนการยุติธรรมที่ดีต้องส่งเสริมให้มีกระบวนการยุติธรรมทางเลือก

15) นักกฎหมาย ผู้ที่เกี่ยวข้องในกระบวนการยุติธรรม และเจ้าหน้าที่รัฐที่ดีต้องมีความเป็นอิสระและความเป็นกลางในการปฏิบัติหน้าที่

16) นักกฎหมาย ผู้ที่เกี่ยวข้องในกระบวนการยุติธรรม และเจ้าหน้าที่รัฐที่ดีต้องซื่อสัตย์สุจริต ยึดหลักธรรม เมตตาธรรม และสันติธรรม

หลักการนิติธรรมเป็นหลักการพื้นฐานที่มีสถานะเป็นหลักการในระดับรัฐธรรมนูญ ซึ่งมีทั้งหลักการย่อยต่าง ๆ ที่ปรากฏอยู่ในรัฐธรรมนูญ และหลักการย่อยต่าง ๆ ที่มิได้ปรากฏอยู่ในรัฐธรรมนูญ อีกทั้งยังเป็นหลักการที่ช่วยในการตีความบทบัญญัติของกฎหมาย และยังเป็นหลักการที่นำมาอุดช่องว่างของกฎหมายในกรณีที่ไม่มีกฎเกณฑ์ในทางกฎหมายที่นำมาบังคับใช้ในเรื่องนั้น ๆ อีกด้วย[34] เมื่อพิจารณาหลักสำคัญต่าง ๆ ของหลักนิติธรรมที่กล่าวมาข้างต้นแล้ว หลักนิติธรรมจึงมีขึ้นเพื่อจำกัดอำนาจรัฐ และคุ้มครองสิทธิเสรีภาพของประชาชนอันเป็นหัวใจสำคัญของการปกครองในระบอบประชาธิปไตย[35]

2.2.2 ผลของการละเมิดหลักนิติรัฐหรือหลักนิติธรรม

ดังที่ได้กล่าวไปแล้วว่า หลักนิติธรรมเป็นหลักการในระดับรัฐธรรมนูญ ดังนั้น การกระทำใด ๆ ขององค์กรของรัฐที่ขัดกับหลักนิติธรรม โดยหลักการแล้วย่อมมีผลเป็นการขัดกับรัฐธรรมนูญ แต่จะต้องพิจารณาว่าการกระทำนั้นเป็นการกระทำในลักษณะใด และการกระทำเหล่านั้นอยู่ภายใต้การตรวจสอบของศาลหรือไม่ โดยอาจแบ่งการกระทำของรัฐออกได้ ดังนี้[36]

1) การกระทำที่มีลักษณะเป็นบทบัญญัติของกฎหมาย ในกรณีที่ขัดหรือแย้งกับหลักนิติธรรมบทบัญญัติดังกล่าวย่อมไม่สามารถบังคับใช้ได้[37] ส่วนการที่จะมีผลไม่ให้บังคับใช้จะมีผลจาก

---

[34] บรรเจิด สิงคะเนติ, หลักกฎหมายมหาชน หลักนิติธรรม/นิติรัฐในฐานะ "เกณฑ์" จำกัดอำนาจรัฐ, หน้า 67 - 68

[35] เขตไท ลังการ์พินธ์, "หลักนิติธรรมของประเทศอังกฤษ และประเทศไทย : ความหมายและสาระสำคัญ," วารสารนิติศาสตร์ มหาวิทยาลัยนเรศวร: หน้า 42.

[36] บรรเจิด สิงคะเนติ, หลักกฎหมายมหาชน หลักนิติธรรม/นิติรัฐในฐานะ "เกณฑ์" จำกัดอำนาจรัฐ, หน้า 67 - 68.

[37] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 5

อดีต ปัจจุบัน หรือในอนาคต ย่อมขึ้นอยู่กับบทบัญญัติดังกล่าวว่าขัดหรือแย้งในระดับที่รุนแรง หรือบกพร่องเพียงเล็กน้อย ซึ่งอาจกำหนดเงื่อนไขให้สามารถดำเนินการแก้ไขเปลี่ยนแปลงบทบัญญัติดังกล่าวในอนาคตได้

2) การกระทำที่เป็นการกระทำทางนโยบาย หรือการกระทำทางการเมือง ในกรณีที่ขัดกับหลักนิติธรรมย่อมเป็นการกระทำที่ขัดกับรัฐธรรมนูญ ซึ่งจะนำไปสู่การตรวจสอบทางการเมือง หรือนำไปสู่กระบวนการถอดถอนผู้ดำรงตำแหน่งทางการเมือง หรือกรณีที่เกี่ยวโยงกับการทุจริตหรือประพฤติมิชอบของฝ่ายการเมืองย่อมเป็นเหตุนำไปสู่การฟ้องร้องต่อศาลฎีกาแผนกคดีอาญาของผู้ดำรงตำแหน่งทางการเมืองได้หากการกระทำดังกล่าวเข้าองค์ประกอบความผิดที่กำหนดไว้[38]

3) การกระทำที่เป็นการกระทำทางปกครอง ไม่ว่าจะเป็นการออกกฎ คำสั่ง หรือการกระทำอื่นใด ในกรณีที่ขัดกับหลักนิติธรรมถือว่าเป็นการกระทำที่ขัดต่อรัฐธรรมนูญ ถือว่าเป็นการกระทำที่ไม่ชอบด้วยกฎหมาย ศาลปกครองย่อมมีอำนาจออกคำบังคับเพื่อกำหนดว่าจะให้มีผลย้อนหลังหรือไม่ หรือมีผลไปในอนาคต หรือจะกำหนดให้มีเงื่อนไขอย่างใดอย่างหนึ่งตามความเป็นธรรมแห่งคดีขึ้นอยู่กับระดับความรุนแรงของการกระทำดังกล่าว[39]

ดังนั้น หลักนิติรัฐและหลักนิติธรรมจึงเป็นหลักการพื้นฐานที่สำคัญของรัฐ เป็นหลักการที่มีขึ้นเพื่อคุ้มครองสิทธิเสรีภาพของประชาชน การที่รัฐจะดำเนินการใด ๆ จะต้องอยู่ภายใต้กรอบของกฎหมาย และหากรัฐใช้อำนาจโดยมิชอบ ประชาชนย่อมสามารถฟ้องร้องดำเนินคดีต่อรัฐได้[40] การที่สิทธิเสรีภาพของประชาชนจะได้รับการคุ้มครอง หรือรักษาไว้โดยปราศจากการแทรกแซงโดยมิชอบจากรัฐ รัฐจะต้องนำหลักนิติรัฐและหลักนิติธรรมมาเป็นหลักการสำคัญในการดำเนินกาต่าง ๆ ของรัฐ เพราะหลักการทั้งสองต่างก็เป็นหลักการที่มุ่งให้เกิดความยุติธรรม และสันติสุขในสังคม[41]

2.3 แนวความคิดเกี่ยวกับการคุ้มครองสิทธิเสรีภาพของประชาชน

หลักการคุ้มครองสิทธิเสรีภาพเป็นหลักการพื้นฐานในการปกครองระบอบประชาธิปไตย และเป็นสิ่งที่ควบคู่มากับการเกิดของรัฐธรรมนูญในประเทศต่าง ๆ ที่ปกครองด้วยระบอบประชาธิปไตย

---

[38] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 3 วรรคสอง และ มาตรา 5

[39] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 71 วรรคหนึ่ง (1) และ วรรคสอง

[40] ผ่องพรรณ ไพพรรณรัตน์, หลักนิติธรรมกับการคุ้มครองสิทธิเสรีภาพของประชาชน (สำนักงานศาลรัฐธรรมนูญ), หน้า 2 - 7.

[41] วรเจตน์ ภาคีรัตน์, "หลักนิติธรรมและหลักนิติรัฐ," จุลนิติ: หน้า 16 - 17.

เป็นหลัก เพราะเจตนารมย์ในการร่างรัฐธรรมนูญขึ้นมาก็เพื่อที่จะให้ความคุ้มครองสิทธิและเสรีภาพตลอดจนความเสมอภาคของบุคคล ดังจะเห็นได้จากคำประกาศสิทธิมนุษยชนและพลเมืองของประเทศฝรั่งเศส ปี ค.ศ. 1798 ข้อ 16 ที่กำหนดว่า “สังคมใดไม่มีการให้หลักประกันในการคุ้มครองสิทธิเสรีภาพ หรือไม่มีการแบ่งแยกการใช้อำนาจอธิปไตย จะถือว่ามีรัฐธรรมนูญไม่ได้”[42] และหลักการดังกล่าวได้กลายมาเป็นหลักการพื้นฐานที่สำคัญของรัฐธรรมนูญในประเทศต่าง ๆ[43]

ในช่วงก่อนการเปลี่ยนแปลงการปกครอง พ.ศ. 2475 ในประเทศไทย แนวความคิดทางด้านสิทธิและเสรีภาพตามแนวความคิดตะวันตกยังไม่เป็นที่แพร่หลายในประเทศไทยเท่าใดนัก การคุ้มครองสิทธิเสรีภาพจึงยังไม่มีลักษณะเป็นการรับรองและคุ้มครองตามกฎหมายแต่อย่างใด การดำเนินความสัมพันธ์ของบุคคลในสังคม หรือการปฏิบัติระหว่างผู้ปกครองและผู้อยู่ใต้ปกครองจะใช้หลักศาสนาและหลักจารีตประเพณีเป็นปัจจัยกำหนด[44] จนกระทั่งเมื่อได้มีการเปลี่ยนแปลงการปกครอง และได้มีการประกาศใช้รัฐธรรมนูญถาวรฉบับแรกของประเทศไทย จึงได้มีการนำหลักการคุ้มครองสิทธิและเสรีภาพมาบัญญัติไว้ ดังนี้ “บุคคลย่อมมีเสรีภาพบริบูรณ์ในการนับถือศาสนาหรือลัทธิใด ๆ และมีเสรีภาพในการปฏิบัติพิธีกรรมตามความเชื่อของตน เมื่อไม่เป็นปฏิปักษ์ต่อหน้าที่ของพลเมืองและไม่เป็นการขัดต่อความสงบเรียบร้อยหรือศีลธรรมของประชาชน” และ “ภายในบังคับแห่งกฎหมาย บุคคลย่อมมีเสรีภาพบริบูรณ์ในร่างกาย เคหสถาน ทรัพย์สิน การพูด การเขียน การโฆษณา การศึกษาอบรม การประชุมโดยเปิดเผย การตั้งสมาคม การอาชีพ”[45]

ในปัจจุบันประเทศไทยยังคงคำนึงถึงหลักการคุ้มครองสิทธิและเสรีภาพของประชาชนเป็นประการสำคัญ ดังจะเห็นได้จากรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 4 ที่บัญญัติไว้ว่า “ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาคของบุคคลย่อมได้รับความคุ้มครอง”

---

[42] “A society in which the observance of the law is not assured, nor the separation of powers defined, has no constitution at all.”

[43] กองบรรณาธิการสำนักกฎหมาย, "หลักสิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย : แนวความคิดและภาคปฏิบัติ," จุลนิติ ม.ค. - ก.พ. 54: หน้า 1

[44] คณะกรรมการศึกษาแนวทางแก้ไขเพิ่มเติมรัฐธรรมนูญ สำนักงานเลขาธิการสภาผู้แทนราษฎร, แนวทางแก้ไขรัฐธรรมนูญ เรื่อง สิทธิเสรีภาพ และหน้าที่ของชนชาวไทย, พิมพ์ครั้งที่ 1 (กรุงเทพมหานคร: สำนักงานเลขาธิการสภาผู้แทนราษฎร, 2549), หน้า 5.

[45] กองบรรณาธิการสำนักกฎหมาย, "หลักสิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย : แนวความคิดและภาคปฏิบัติ," จุลนิติ: หน้า 2.

2.3.1 การคุ้มครองสิทธิความเป็นส่วนตัว

สิทธิเสรีภาพขั้นพื้นฐานในการใช้ชีวิตของบุคคลซึ่งรัฐมีหน้าที่ที่จะต้องให้ความคุ้มครองอย่างยิ่ง คือ สิทธิในความเป็นส่วนตัว (Rights to Privacy) หรือสิทธิส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐานของบุคคลที่ไม่อาจถูกพรากไปโดยบุคคลใดได้ และรัฐจะต้องให้การรับรองและคุ้มครองสิทธิดังกล่าว สิทธิในความเป็นส่วนตัวหรือสิทธิส่วนบุคคล ในทางวิชาการได้ให้หมายความว่า สิทธิของบุคคลที่จะอยู่ลำพังโดยปราศจากบุคคลอื่นรบกวน และเป็นสิทธิที่บุคคลจะคาดหมายได้ว่าข้อมูลส่วนบุคคลของตนจะไม่ถูกเปิดเผยต่อบุคคลที่สามหรือต่อสาธารณะโดยปราศจากความยินยอม ซึ่งการเปิดเผยนั้นอาจส่งผลให้บุคคลดังกล่าวได้รับความเดือนร้อน อับอาย หรือได้รับความทุกข์ใจ ทรมานใจ ซึ่งข้อมูลข่าวสารส่วนบุคคลนี้หมายความรวมถึงข้อเท็จจริง รูปภาพ ไม่ว่าจะเป็นภาพถ่ายหรือในลักษณะอื่นใด[46] ประเภทของสิทธิในความเป็นส่วนตัวที่ได้รับผลกระทบจากการดำเนินกระบวนการยุติธรรมทางอาญาของรัฐอาจแบ่งพิจารณาได้ดังนี้ ความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล (Information Privacy) ความเป็นส่วนตัวในเนื้อตัวและร่างกาย (Bodily Privacy) ความเป็นส่วนตัวในการสื่อสาร (Communication Privacy) และความเป็นส่วนตัวในเคหสถาน (Territorial Privacy)[47] อย่างไรก็ตามสิทธิในความเป็นส่วนตัวย่อมได้รับผลกระทบจากการใช้อำนาจของรัฐเกี่ยวกับการแสวงหาพยานหลักฐานอยู่เสมอ ดังนั้น สิทธิส่วนบุคคลจึงย่อมได้รับความคุ้มครองจากการดำเนินกระบวนการยุติธรรมทางอาญาของรัฐอยู่เป็นลำดับแรก ๆ เสมอ

2.3.2 การตรวจสอบการใช้อำนาจรัฐ

นอกจากหลักการคุ้มครองสิทธิเสรีภาพขั้นพื้นฐานที่ได้มีการบัญญัติรับรองไว้ในรัฐธรรมนูญแล้ว การตรวจสอบการใช้อำนาจของรัฐก็เป็นหลักการสำคัญในการคุ้มครองสิทธิเสรีภาพของประชาชนเช่นเดียวกัน กล่าวคือ เป็นการตรวจสอบการใช้อำนาจของบุคคล หรือองค์กรซึ่งเป็นผู้แทนในการใช้อำนาจรัฐไม่ให้ใช้อำนาจผิดวัตถุประสงค์ของบทบัญญัติของกฎหมาย และเป็นการป้องกันการใช้อำนาจโดยมิชอบ และการใช้อำนาจตามอำเภอใจของเจ้าหน้าที่รัฐ แนวคิดการตรวจสอบการใช้อำนาจรัฐมีขึ้นก็เพื่อคุ้มครองสิทธิเสรีภาพของประชาชนไม่ให้ถูกละเมิด หรือได้รับ

---

[46] วนิดา แสงสารพันธ์, "สิทธิส่วนบุคคล กับความคุ้มครองตามกฎหมาย," LAW FOR YOU: หน้า 78 - 79.

[47] ทิพาพร นะมาตร์, "สิทธิความเป็นอยู่ส่วนตัว : ศึกษากรณีสิทธิความเป็นอยู่ส่วนตัวของบุคคลสาธารณะ" (นิติศาสตรมหาบัณฑิต, สาขาวิชานิติศาสตร์, มหาวิทยาลัยธุรกิจบัณฑิต, 2551), หน้า 31 - 32.

ความกระทบกระเทือนจากการใช้อำนาจรัฐเกินสมควรจนกระทบกระเทือนต่อสาระสำคัญของสิทธิและเสรีภาพนั้น ๆ หากพิจารณาจากเกณฑ์การแบ่งองค์กรผู้ใช้อำนาจรัฐ สามารถแบ่งประเภทของการควบคุมและตรวจสอบการใช้อำนาจรัฐออกได้เป็น 2 กรณี ได้แก่ การตรวจสอบภายในองค์กรและการตรวจสอบภายนอกองค์กร มีรายละเอียดดังนี้[48]

(1) การตรวจสอบภายในองค์กร เป็นการตรวจสอบการใช้อำนาจทางการบริหารและการปกครองในระดับต่าง ๆ เมื่อกฎหมายได้มอบหมายและให้อำนาจไว้แก่ฝ่ายปกครอง จึงต้องมีการกำหนดวิธีการควบคุมการใช้อำนาจดังกล่าวไว้ด้วย เพื่อเป็นการป้องกันการใช้อำนาจและหน้าที่โดยมิชอบ หรือขาดความยุติธรรมอันจะก่อให้เกิดความเดือดร้อนแก่ประชาชน หรือแม้กระทั่งผลของการใช้อำนาจ และหน้าที่ของผู้ปกครองไม่เป็นไปตามเจตนารมย์ของกฎหมาย วิธีการควบคุมตรวจสอบการใช้อำนาจภายในองค์กรมีอยู่ 2 วิธีการด้วยกัน ดังนี้

(1.1) การควบคุมโดยผู้บังคับบัญชาหรือผู้กำกับดูแล โดยการควบคุมบังคับบัญชา เป็นกรณีที่ผู้บังคับบัญชาใช้อำนาจทั่วไปตามหลักของอำนาจบังคับบัญชาที่มีอยู่เหนือผู้ใต้บังคับบัญชา เพื่อควบคุมดูแล และตรวจสอบความชอบด้วยกฎหมาย และความเหมาะสมในการใช้ดุลพินิจต่าง ๆ ในการกระทำทางปกครองของผู้ใต้บังคับบัญชา หากการกระทำดังกล่าวไม่ชอบด้วยกฎหมาย หรือชอบด้วยกฎหมายแต่ไม่มีความเหมาะสม ผู้บังคับบัญชาย่อมมีอำนาจยกเลิก เพิกถอน หรือสั่งแก้ไขเปลี่ยนแปลงการกระทำทางปกครองดังกล่าวของผู้ใต้บังคับบัญชาได้

ส่วนการกำกับดูแล เป็นกรณีที่องค์กรฝ่ายปกครองในราชการส่วนกลางหรือส่วนภูมิภาคใช้อำนาจตรวจสอบความชอบด้วยกฎหมายขององค์กรปกครองส่วนท้องถิ่น เช่น กรุงเทพมหานคร หรือเทศบาลต่าง ๆ ตลอดจนการกระทำขององค์กรมหาชน เช่น ธนาคารแห่งประเทศไทย องค์การสื่อสารมวลชนแห่งประเทศไทย เป็นต้น หากองค์กรฝ่ายปกครองส่วนกลางหรือองค์กรฝ่ายปกครองส่วนภูมิภาคเห็นว่าการกระทำขององค์กรปกครองส่วนท้องถิ่นหรือการกระทำขององค์กรมหาชนไม่ชอบด้วยกฎหมาย องค์กรปกครองส่วนกลางหรือองค์กรปกครองส่วนภูมิภาคมีอำนาจไม่อนุมัติให้การกระทำนั้นมีผลบังคับ หรืออาจยกเลิก เพิกถอนการกระทำนั้นได้

---

[48] ยุทธพร อิสรชัย, "การตรวจสอบการใช้อำนาจรัฐ," [Online] Accessed: 10/05/2566. Available from: http://wiki.kpi.ac.th/index.php?title=การตรวจสอบการใช้อำนาจรัฐ

(1.2) การอุทธรณ์ หรือการร้องทุกข์ ซึ่งการอุทธรณ์มีลักษณะใกล้เคียงกับการร้องทุกข์มาก หากแต่ต่างกันที่ว่าการอุทธรณ์คำสั่ง หรือคำวินิจฉัยทั่วไปจะมีเรื่องของระยะเวลาเกี่ยวข้องด้วย โดยสามารถดำเนินการอุทธรณ์คำสั่ง หรือคำวินิจฉัยของเจ้าหน้าที่รัฐได้ภายในระยะเวลาที่กำหนดไว้ ส่วนการร้องทุกข์เป็นกระบวนการทางกฎหมายที่ใช้ในการควบคุมการใช้อำนาจของหน่วยงานรัฐ และของเจ้าหน้าที่รัฐ จุดประสงค์ของการร้องทุกข์นั้นก็เพื่อให้มีการยกเลิกเพิกถอน หรือมีการเปลี่ยนแปลงคำสั่งที่หน่วยงานรัฐหรือเจ้าหน้าที่รัฐได้ออกไว้โดยไม่ถูกต้องหรือไม่ชอบ

(2) การตรวจสอบภายนอกองค์กร แบ่งออกเป็นการควบคุมทางการเมือง การควบคุมโดยองค์กรอิสระตามรัฐธรรมนูญ และการควบคุมโดยองค์กรตุลาการ ซึ่งมีรายละเอียดดังนี้

(2.1) การควบคุม และการตรวจสอบในทางการเมือง เป็นการเยียวยาความบกพร่องในการใช้อำนาจรัฐวิธีหนึ่ง เพราะโดยหลักการแล้วองค์กรนิติบัญญัติมีอำนาจหน้าที่สำคัญ 2 ประการ คือ หน้าที่ในทางนิติบัญญัติ อันได้แก่ การออกกฎหมาย และหน้าที่ในการควบคุมฝ่ายบริหารทั้งในฐานะรัฐบาล และในฐานะฝ่ายปกครองให้เป็นไปตามนโยบายที่แถลงไว้ต่อรัฐสภาและตามกฎหมาย บทบาทและอำนาจหน้าที่ขององค์กรนิติบัญญัติในเรื่องการควบคุม และตรวจสอบการใช้อำนาจรัฐนั้นมีความแตกต่างกันไปในแต่ละประเทศ โดยขึ้นอยู่กับลักษณะของระบอบการเมืองการปกครองของประเทศนั้น ๆ เป็นสำคัญ เช่น ในระบบการปกครองแบบรัฐสภาอาจใช้วิธีการขอเปิดอภิปรายเพื่อลงมติไม่ไว้วางใจในการตั้งคณะกรรมาธิการ หรือการตั้งกระทู้ถาม เป็นต้น อย่างไรก็ตามการควบคุม และตรวจสอบโดยทางการเมืองมีข้อจำกัดอยู่หลายประการด้วยกัน เช่น การที่ฝ่ายบริหารคุมเสียงข้างมากในสภา หรือการที่พรรคฝ่ายค้านจะสนใจต่อความบกพร่องเฉพาะกรณีที่ทำให้เกิดปัญหาต่อเสถียรภาพของรัฐบาลเท่านั้น ดังนั้น การควบคุม และตรวจสอบโดยทางการเมืองจึงมีความเหมาะสมเฉพาะกับการตรวจสอบในเชิงนโยบายหรือควบคุม และตรวจสอบเฉพาะประเด็นที่เป็นปัญหาสำคัญ ๆ เท่านั้น

(2.2) การควบคุม และตรวจสอบโดยองค์กรอิสระ เป็นการมอบหมายให้องค์กรอิสระดังกล่าวมีอำนาจในการควบคุม และตรวจสอบภายในขอบเขตอำนาจขององค์กรนั้น ๆ เช่น ผู้ตรวจการเงินแผ่นดินก็จะมีอำนาจในการควบคุม และตรวจสอบเรื่องการเงินการคลังของหน่วยงานของรัฐต่าง ๆ หรือกรณีของผู้ตรวจการแผ่นดินของรัฐสภาก็จะมีอำนาจในการตรวจสอบการ

กระทำขององค์กรรัฐทั้งหลาย ส่วนขอบเขตอำนาจขององค์กรอิสระจะมีอำนาจมากน้อยเพียงใด ย่อมขึ้นอยู่กับบทบัญญัติของรัฐธรรมนูญ และบทบัญญัติกฎหมายว่าจะมีการบัญญัติให้องค์กรอิสระนั้น ๆ มีอำนาจอย่างไร และเพียงใด

(2.3) การควบคุม และตรวจสอบโดยองค์กรฝ่ายตุลาการ เป็นการควบคุมและตรวจสอบที่สำคัญที่สุด เพราะเป็นระบบการควบคุม และตรวจสอบที่ให้หลักประกันแก่ประชาชนได้มากที่สุด ด้วยเหตุนี้จึงมีการกล่าวกันว่า “รัฐใดรัฐหนึ่งไม่อาจถือได้ว่าเป็นนิติรัฐ หากรัฐนั้นปราศจากการควบคุม และตรวจสอบโดยองค์กรตุลาการ” ทั้งนี้ เพราะองค์กรตุลาการมีหลักประกันความเป็นอิสระของตุลาการ นอกจากนี้ องค์กรตุลาการยังมีวิธีพิจารณาเพื่อเป็นการคุ้มครองความเป็นธรรมในการดำเนินกระบวนพิจารณาต่าง ๆ การควบคุมและตรวจสอบโดยองค์กรตุลาการอาจแยกออกได้เป็น 2 ระบบ คือ ระบบศาลเดี่ยว และระบบศาลคู่

2.3.3 หลักเหตุอันควรเชื่อและหลักเหตุอันควรสงสัย

หลักเหตุอันควรเชื่อ (Probable Cause) และหลักเหตุอันควรสงสัย (Reasonable Suspicion) เป็นหลักการที่กำหนดขึ้นมาเพื่อคุ้มครองสิทธิเสรีภาพของประชาชนจากการใช้อำนาจหน้าที่ของเจ้าหน้าที่รัฐ เพื่อเป็นการรับประกันว่าเจ้าหน้าที่รัฐจะใช้อำนาจหน้าที่ต่าง ๆ ที่กฎหมายบัญญัติไว้อย่างถูกต้อง เหมาะสม และสมควร หลักการทั้งสองปรากฏให้เห็นอย่างเด่นชัดอยู่ในหลักการของกระบวนยุติธรรมทางอาญาในประเทศสหรัฐอเมริกา ซึ่งนอกจากในประเทศสหรัฐอเมริกาแล้ว หลักการทั้งสองก็ยังปรากฏอยู่ในหลักของกระบวนการยุติธรรมทางอาญาของประเทศอื่น ๆ รวมทั้งในประเทศไทยด้วย โดยมักจะปรากฏอยู่ในเรื่องของมาตรการในการแสวงหาพยานหลักฐานต่าง ๆ โดยเฉพาะการจับและการค้น ซึ่งในบทบัญญัติของประเทศไทยได้ปรากฏอยู่ในเรื่องของเหตุแห่งการค้นเช่นเดียวกัน

หลักเหตุอันควรเชื่อ (Probable Cause) หมายถึง กรณีที่บุคคลมีเหตุผลที่จะเชื่อว่ามีอาชญากรรมที่ได้เกิดขึ้นแล้ว กำลังอยู่ในขั้นตอนของการลงมือก่ออาชญากรรม หรืออยู่ในขั้นตอนของการตระเตรียมการเพื่อก่ออาชญากรรม ซึ่งหลักเหตุอันควรเชื่อเป็นหลักการสำคัญที่ประเทศสหรัฐอเมริกาได้นำมาประกอบกับการใช้อำนาจหน้าที่ของเจ้าหน้าที่รัฐเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐาน หากเจ้าหน้าที่ตำรวจหรือเจ้าหน้าที่รัฐอื่นซึ่งมีอำนาจหน้าที่ที่จะสามารถทำการค้น หรือจับกุมได้ มีเหตุอันควรเชื่อได้ว่ามีบุคคลใดได้ลงมือก่ออาชญากรรมขึ้นแล้ว มีเหตุอันควร

เชื่อได้ว่ามีบุคคลใดกำลังก่ออาชญากรรมอยู่ หรือมีเหตุอันควรเชื่อได้ว่ามีบุคคลใดกำลังตระเตรียมการเพื่อก่ออาชญากรรม ก็เพียงพอสำหรับการที่จะทำการค้น หรือการออกหมายสำหรับทำการจับกุมแล้ว ส่วนการทำการจับกุมนั้น หากเจ้าหน้าที่ตำรวจหรือเจ้าหน้าที่รัฐอื่นที่มีอำนาจหน้าที่เห็นว่ามีการก่ออาชญากรรมเกิดขึ้น ก็ถือว่าเพียงพอสำหรับการทำการจับกุมเช่นกัน เพราะการเห็นด้วยตาก็ถือว่าเป็นเหตุอันควรเชื่ออย่างหนึ่งเช่นเดียวกัน[49]

หลักเหตุอันควรสงสัย (Reasonable Suspicion) เป็นหลักการที่ศาลฎีกาของประเทศสหรัฐอเมริกาได้ให้คำจำกัดความไว้ โดยหมายถึง “ข้อสรุปทั่วไปเกี่ยวกับพฤติกรรมของมนุษย์ที่ผู้คนปฏิบัติจริง” นอกจากนี้ ยังได้มีการจำกัดความเหตุอันควรสงสัยว่าเป็นกรณีที่ต้องการมากกว่า “ลางสังหรณ์ที่ไม่มีความชัดเจน” เหตุอันควรสงสัยต้องอาศัยข้อเท็จจริงหรือสถานการณ์ที่ทำให้มีความสงสัยที่เพียงพอว่ามีเหตุการณ์ใดเหตุการณ์หนึ่งได้เกิดขึ้น ซึ่งมากกว่าสิ่งซึ่งสมมติขึ้นมาเอง หรือการคาดเดาเพียงอย่างเดียว หลักเหตุอันควรสงสัย จึงหมายถึง กรณีที่บุคคลที่มีเหตุผลจะสงสัยว่าได้มีบุคคลใดได้ลงมือก่ออาชญากรรมขึ้นแล้ว มีบุคคลใดกำลังก่ออาชญากรรมอยู่ หรือมีบุคคลใดกำลังจะก่ออาชญากรรมในไม่ช้า ซึ่งหลักเหตุอันควรสงสัยเป็นหลักการสำคัญที่ประเทศสหรัฐอเมริกาได้นำมาประกอบการใช้อำนาจหน้าที่ของเจ้าหน้าที่รัฐเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานเช่นเดียวกัน หากเจ้าหน้าที่ตำรวจหรือเจ้าหน้าที่รัฐอื่นซึ่งมีอำนาจหน้าที่มีเหตุอันควรสงสัยก็สามารถที่จะทำการค้นตัวผู้ต้องสงสัย หรือกักตัวผู้ต้องสงสัยได้ชั่วคราว แต่เหตุอันควรสงสัยนี้ ไม่เพียงพอที่จะเป็นเหตุให้เจ้าหน้าที่รัฐจะทำการค้นหาบุคคล หรือค้นยานพาหนะ และไม่เพียงพอที่จะเป็นเหตุให้เจ้าหน้าที่รัฐทำการจับกุม หรือขอหมายสำหรับทำการค้นได้ดังเช่นเหตุอันควรเชื่อ[50]

หลักเหตุอันควรเชื่อ (Probable Cause) และหลักเหตุอันควรสงสัย (Reasonable Suspicion) มีความคล้ายคลึงกันอย่างมาก ซึ่งมักทำให้เกิดความสับสนและนำไปใช้ หรือปฏิบัติอย่างผิดวัตถุประสงค์ เมื่อหลักการทั้งสองเกี่ยวข้องกับอำนาจหน้าที่ของเจ้าหน้าที่รัฐในการดำเนินการต่าง ๆ โดยเฉพาะในการดำเนินการของเจ้าหน้าที่ตำรวจ ในสถานการณ์เช่นเดียวกัน หลักการทั้งสองหลักการนี้ย่อมส่งผลลัพธ์ที่แตกต่างกันทั้งต่อสิทธิของบุคคล ต่อมาตรการที่เหมาะสม และต่อผลลัพธ์ที่

---

[49] Maricopa County, "Probable Cause Versus Reasonable Suspicion," [Online] Accessed: 17/8/2564. Available from: https://www.maricopa.gov/919/Probable-Cause-Versus-Reasonable-Suspici

[50] บรรเจิด สิงคะเนติ, หลักพื้นฐานเกี่ยวกับสิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์, พิมพ์ครั้งที่ 5 (กรุงเทพมหานคร: วิญญูชน, 2558), หน้า 28.

เกิดขึ้นในสถานการณ์นั้น ๆ หลักเหตุอันควรสงสัยเป็นขั้นตอนก่อนหลักเหตุอันควรเชื่อ กล่าวคือ เมื่อมีเหตุอันควรสงสัยว่าจะมีการก่ออาชญากรรมเกิดขึ้น สถานการณ์จะขยายไปสู่เหตุอันควรเชื่อเมื่อเห็นได้ว่ามีความใกล้เคียงที่สุดที่จะมีการก่ออาชญากรรมเกิดขึ้น[51]

จากการศึกษาเห็นว่า กระบวนการยุติธรรมทางอาญาเป็นกระบวนการที่สำคัญอันจะรักษาไว้ซึ่งความสงบสุขให้แก่สังคม อย่างไรก็ตาม มาตรการต่าง ๆ ในกระบวนการยุติธรรมทางอาญาเป็นการให้อำนาจแก่รัฐในการดำเนินการต่าง ๆ ซึ่งกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน เพราะประชาชนจำเป็นต้องสละสิทธิเสรีภาพบางประการเพื่อแลกมากับการใช้อำนาจของรัฐในการรักษาไว้ซึ่งความสงบสุขในสังคม ดังนั้น การที่รัฐจะใช้อำนาจในลักษณะที่เป็นการกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนจึงจำเป็นที่จะต้องมีมาตรการในการควบคุมและตรวจสอบให้การใช้อำนาจเป็นไปอย่างถูกต้องและเหมาะสม หากรัฐใดมุ่งที่จะรักษาไว้ซึ่งความสงบสุขในสังคมเป็นหลัก การใช้อำนาจของรัฐย่อมเป็นการลดทอนสิทธิเสรีภาพที่มากยิ่งขึ้น แต่หากรัฐใดมุ่งที่จะรักษาไว้ซึ่งสิทธิเสรีภาพของประชาชนเป็นสำคัญ การใช้อำนาจของรัฐเพื่อรักษาไว้ซึ่งความสงบสุขของสังคมย่อมเป็นไปได้โดยยากเนื่องด้วยหลักเกณฑ์เกี่ยวกับการใช้อำนาจ ในปัจจุบัน นานาประเทศได้มีการผสมผสานรูปแบบของกระบวนการยุติธรรมทางอาญาทั้งสองเข้าด้วยกัน จึงได้เกิดเป็นหลักการต่าง ๆ ในการตรวจสอบการใช้อำนาจของรัฐ ประเทศใดที่มุ่งคุ้มครองสิทธิเสรีภาพของประชาชนเป็นสำคัญย่อมมีขั้นตอนในการตรวจที่ละเอียดและรัดกุม เพื่อให้การใช้อำนาจของรัฐเป็นไปเพียงเท่าที่มีความจำเป็นเท่านั้น ส่วนประเทศใดที่มุ่งรักษาไว้ซึ่งความสงบสุขของสังคมย่อมมีการตรวจสอบการใช้อำนาจรัฐที่น้อยลงมา เพื่อให้รัฐสามารถใช้อำนาจของตนได้อย่างรวดเร็วและมีประสิทธิภาพ รัฐจึงจำเป็นต้องมีการชั่งน้ำหนักระหว่างสิทธิเสรีภาพของประชาชนและการใช้อำนาจของรัฐเพื่อดำรงไว้ซึ่งความสงบสุขในสังคมว่าในกรณีเช่นใดควรจะมีการใช้อำนาจและมีมาตรการในการตรวจสอบการใช้อำนาจอย่างไร ซึ่งในบทต่อไปจะทำการศึกษาหลักกฎหมายที่เกี่ยวข้องกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามกฎหมายไทยและกฎหมายต่างประเทศ

---

[51] Ibid., หน้า 28.

บทที่ 3
แนวความคิดและกฎหมายเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทย

"ภัยคุกคามทางไซเบอร์" หรือ "Cyber Threats" หมายถึง การกระทำหรือการดำเนินการใด ๆ ผ่านการใช้ระบบสารสนเทศ หรือเครือข่ายที่ก่อให้เกิดผลเสียต่อระบบข้อมูลเครือข่าย หรือข้อมูลภายใน[52] เป็นภัยคุกคามที่ส่งผลกระทบในทุกภาคส่วน ไม่ว่าจะเป็นทางเศรษฐกิจ หรือความมั่นคงของประเทศ ภัยคุกคามทางไซเบอร์ที่สำคัญ คือ "อาชญากรรมทางไซเบอร์" หรือ "Cyber Crime" ซึ่งหมายถึง อาชญากรรมที่มีการกำหนดให้คอมพิวเตอร์เป็นเป้าหมายของการก่ออาชญากรรม หรือใช้เป็นเครื่องมือในการกระทำความผิด โดยอาชญากรไซเบอร์อาจใช้เทคโนโลยีทางคอมพิวเตอร์ในการเข้าถึงข้อมูลส่วนบุคคล ความลับทางการค้า หรือใช้อินเตอร์เน็ตเพื่อแสวงหาประโยชน์ต่าง ๆ หรือเพื่อวัตถุประสงค์ในทางที่ไม่ชอบ นอกจากนี้อาชญากรไซเบอร์ยังสามารถใช้คอมพิวเตอร์เพื่อการสื่อสาร หรือจัดการ หรือจัดเก็บเอกสาร หรือข้อมูลต่าง ๆ เป็นต้น[53]

ปัจจุบันภัยคุกคามไซเบอร์ได้เกิดขึ้นอย่างต่อเนื่อง และยังมีความรุนแรงเพิ่มขึ้นกว่าในอดีต อันสร้างความเสียหายให้แก่ประชาชน สังคม ตลอดจนประเทศชาติ ไม่ว่าจะในประเทศที่พัฒนาแล้วหรือในประเทศที่กำลังพัฒนาก็ตาม ดังจะเห็นได้จากเหตุการณ์ภัยคุกคามทางไซเบอร์ที่สำคัญในหลาย ๆ กรณีที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานสำคัญ (Critical Infrastructures) ของประเทศ เช่น เหตุการณ์ช่วงระหว่างวันที่ 6 - 12 พฤษภาคม พ.ศ. 2564 ที่มีการโจมตีทางไซเบอร์ครั้งใหญ่ที่เกิดขึ้นกับบริษัทท่อส่งน้ำมันรายใหญ่ของประเทศสหรัฐอเมริกา ที่ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ (Ransomware) ทำให้บริษัทดังกล่าวต้องมีการหยุดการขนส่งน้ำมันบางส่วนลงชั่วคราวเพื่อแก้ไขปัญหาที่เกิดขึ้นซึ่งสร้างความเสียหายเป็นอย่างมาก การโจมตีดังกล่าวเป็นการปฏิบัติการขององค์กรอาชญากรรมข้ามชาติที่มุ่งโจมตีเป้าหมายที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ[54] เหตุการณ์การโจมตีทางไซเบอร์ในลักษณะนี้ไม่ใช่เหตุการณ์ที่เกิดขึ้นเป็นครั้งแรก และไม่ใช่เหตุการณ์

---

[52] สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, "[ออนไลน์] เข้าถึงเมื่อ 15/07/2566. แหล่งที่มา: https://www.sec.or.th/TH/Pages/CYBERRESILIENCE-KNOWLEDGECYBER.aspx

[53] Mehak Aneja, "Role of Judiciary in Cyber Crime," Supremo Amicus 18, July, 2020 (2020).

[54] ปริญญา หอมเอนก, "[ออนไลน์] เข้าถึงเมื่อ 12/11/65. แหล่งที่มา: https://www.bangkokbiznews.com/columnist/1000806

การโจมตีทางไซเบอร์ที่จะเกิดขึ้นเป็นครั้งสุดท้าย หากแต่ยังคงเกิดขึ้นในหลายประเทศทั่วโลกในตลอดระยะเวลาหลายปีที่ผ่านมา จึงเป็นสาเหตุที่นานาประเทศจำเป็นที่จะต้องมีการกำหนดมาตรการ หรือกฎหมายโดยเฉพาะเพื่อรับมือต่อภัยคุกคามทางไซเบอร์ที่เกิดขึ้นหรืออาจจะเกิดขึ้นในอนาคต ประเทศไทยได้ตระหนัก และรับรู้ถึงความร้ายแรงของภัยคุกคามทางไซเบอร์ดังกล่าว จึงเป็นเหตุผลให้มีความจำเป็นที่จะต้องมีการกำหนดมาตรการทางกฎหมายเพื่อป้องกันต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต และเป็นการกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ หน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญต่าง ๆ รวมไปถึงความสงบเรียบร้อยภายในประเทศ

ในบทนี้จะกล่าวถึงแนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์เป็นประการแรก เพื่อให้ทราบถึงความสำคัญของการกำหนดมาตรการที่เหมาะสมต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ประการที่สองกล่าวถึงกฎหมายที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประการสุดท้ายจะกล่าวถึงมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทย เพื่อให้ทราบถึงหลักเกณฑ์ต่าง ๆ ที่ให้อำนาจแก่เจ้าหน้าที่รัฐอันมีลักษณะเป็นการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ รวมไปถึงหลักเกณฑ์ในการคุ้มครองสิทธิเสรีภาพของประชาชนภายใต้มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์

3.1 แนวความคิดเกี่ยวกับอาชญากรรมไซเบอร์

อาชญากรรมไซเบอร์เป็นผลพวงด้านลบที่เกิดขึ้น พัฒนา และขยายตัวมาพร้อมกับวิวัฒนาการ และความก้าวหน้าทางเทคโนโลยีสารสนเทศที่เกิดขึ้นบนโลกใบนี้ นับตั้งแต่มีการกำเนิดคอมพิวเตอร์เครื่องแรกบนโลกเป็นต้นมา จนกระทั่งการถือกำเนิดของอินเทอร์เน็ตขึ้นเป็นครั้งแรกในปี ค.ศ. 1969 จนเชื่อมต่อกันเป็นเครือข่ายสารสนเทศขนาดใหญ่ดังเช่นในปัจจุบัน แม้ว่าระบบเครือข่ายสารสนเทศที่มีความก้าวหน้าจะสร้างประโยชน์มากมายให้แก่มนุษย์ แต่ในขณะเดียวกันระบบเครือข่ายสารสนเทศก็ถูกใช้เป็นเครื่องมือในการก่ออาชญากรรม หรือตกเป็นเป้าหมายในการก่ออาชญากรรมเช่นเดียวกัน

3.1.1 วิวัฒนาการของอาชญากรรมไซเบอร์

ในอดีตการก่ออาชญากรรมโดยใช้คอมพิวเตอร์ยังไม่ได้มีลักษณะเป็นอาชญากรรมทางไซเบอร์ที่ส่งผลกระทบอย่างรุนแรงต่อระบบเครือข่าย หรือระบบสารสนเทศดังเช่นในปัจจุบัน การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้มีวิวัฒนาการขึ้นมาตามระยะเวลา และความก้าวหน้าของเทคโนโลยี โดยในบทนี้ผู้เขียนจะแบ่งวิวัฒนาการของทั้งอาชญากรรมไซเบอร์และมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ออกเป็นช่วงทศวรรษต่าง ๆ สามช่วงระยะเวลาด้วยกัน โดยมีรายละเอียดดังนี้

1) ช่วงทศวรรษที่ 1940 ถึงทศวรรษที่ 1960 ภายหลังจากการถือกำเนิดขึ้นของคอมพิวเตอร์เครื่องแรกในปี ค.ศ. 1943 ถือเป็นเวลาเกือบสองทศวรรษที่ในช่วงระยะเวลาดังกล่าวไม่มีการโจมตีทางไซเบอร์เกิดขึ้น เหตุผลเป็นเพราะในช่วงระยะเวลาดังกล่าวการเข้าถึงคอมพิวเตอร์นั้นเป็นไปได้โดยยาก และจำกัดอยู่แต่เพียงบุคคลจำนวนน้อยเท่านั้น ประกอบกับยังไม่มีการเกิดขึ้นของระบบเครือข่ายคอมพิวเตอร์ อย่างไรก็ตาม ในปี ค.ศ. 1949 ปรากฏทฤษฎีที่เป็นรากฐานของไวรัสคอมพิวเตอร์ในปัจจุบันโดย John von Neuman ผู้บุกเบิกด้านคอมพิวเตอร์ได้คาดหมายไว้ว่าโปรแกรมคอมพิวเตอร์นั้นสามารถทำที่จะซ้ำได้[55] ต่อมาในช่วงปลายทศวรรษที่ 1950 ซึ่งเป็นยุคเริ่มต้นของการใช้โทรศัพท์ ได้เกิดคำว่า “Phone Phreaking”[56] ขึ้น ซึ่งหมายถึง กลุ่มที่ออกแบบระบบเสียงย้อนกลับที่ใช้ในการกำหนดเส้นทางการโทรทางไกลด้วยการสร้างโทนเสียงเหล่านี้ขึ้นใหม่ ซึ่ง Phreaks สามารถสลับการโทรจากทางโทรศัพท์มือถือทำให้สามารถโทรฟรีได้ทั่วโลก ซึ่ง ณ ขณะนั้นผู้ให้บริการด้านโทรคมนาคมไม่มีทางที่จะหยุดการแพร่ระบาดของการกระทำดังกล่าวได้ ภายหลัง Phone Phreaking ได้หมดไปในช่วงปลายทศวรรษที่ 1980[57]

ต่อมาในช่วงกลางทศวรรษที่ 1960 คอมพิวเตอร์ยังคงมีเมนเฟรม (Mainframe) ขนาดใหญ่ซึ่งถูกจัดเก็บไว้อย่างปลอดภัย โดยคอมพิวเตอร์ยังคงมีราคาสูงมากทำให้การเข้าถึงเป็นไปได้โดยยากแม้แต่สำหรับโปรแกรมเมอร์ก็ตาม อย่างไรก็ตาม ในช่วงระยะเวลาดังกล่าวก็มีการจู่โจม

---

[55] Katie Chadd, "The History of Cybercrime and Cybersecurity, 1940-2020," [Online] Accessed: 14/11/65. Available from: https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/

[56] Phreaking เป็นคำแสลงที่กำหนดขึ้นเพื่ออธิบายกิจกรรมของผู้ศึกษาทดลองหรือสำรวจระบบโทรคมนาคม เช่น อุปกรณ์และระบบที่เชื่อมต่อกับเครือข่ายโทรศัพท์สาธารณะ คำว่า Phreak เป็นการสะกดคำว่า Freak ด้วย Ph- จากคำว่า Phone

[57] Katie Chadd, "The History of Cybercrime and Cybersecurity, 1940-2020."

เจาะระบบ (Hacking) ซึ่งในช่วงแรกผู้ที่ทำการเจาะระบบได้ส่วนใหญ่เป็นนักเรียนที่กระทำไปเพราะความอยากรู้อยากเห็นเท่านั้น ในช่วงปลายของทศวรรษดังกล่าว เมื่อคอมพิวเตอร์เริ่มมีขนาดที่เล็กลงและมีต้นทุนในการผลิตที่ลดลง ประกอบกับเป็นช่วงที่เกิดเทคโนโลยีอินเตอร์เน็ตขึ้นเป็นครั้งแรก โดยเกิดขึ้นในปี ค.ศ. 1969 บริษัทขนาดใหญ่จึงได้เริ่มลงทุนในเทคโนโลยีคอมพิวเตอร์เพื่อจัดเก็บ และจัดการกับข้อมูลเพื่อความปลอดภัยในข้อมูลจึงได้มีการเริ่มใช้ระบบรหัสผ่าน[58] โดยในช่วงทศวรรษที่ 1940 ที่เกิดคอมพิวเตอร์เครื่องแรกขึ้น จนถึงช่วงปลายของทศวรรษที่ 1960 อาชญากรรมที่เกิดจากการใช้คอมพิวเตอร์เป็นเพียงการกระทำที่เป็นอันตรายต่อข้อมูลซึ่งเป็นความลับอันส่งผลกระทบต่อความเป็นส่วนตัวของบุคคลเท่านั้น[59]

2) ช่วงทศวรรษที่ 1970 ถึงทศวรรษที่ 1980 โดยในช่วงทศวรรษที่ 1970 เกิดโครงการวิจัย ARPANET (the Advance Research Projects Agency Network) ซึ่งเป็นเครือข่ายคอมพิวเตอร์ของกระทรวงกลาโหมประเทศสหรัฐอเมริกาที่ใช้ในงานวิจัยทางด้านการทหาร โครงการดังกล่าวได้เริ่มต้นวิจัยถึงความปลอดภัยไซเบอร์ที่เหมาะสม ซึ่งผลของการเริ่มต้นวิจัยโครงการดังกล่าวได้ก่อให้เกิดหนอนคอมพิวเตอร์ (Computer Worm)[60] ตัวแรกของโลกขึ้น โดยนักวิจัย Bob Thomas ได้สร้างโปรแกรมคอมพิวเตอร์ที่ชื่อว่า Creep โปรแกรมดังกล่าวสามารถเคลื่อนที่ผ่านระบบเครือข่ายของ ARPANET ได้ โดยทิ้งร่องรอยเส้นทางไว้ ซึ่งร่องรอยดังกล่าวอ่านได้ว่า “ฉันคือ Creeper จับฉันสิถ้าคุณทำได้” (I’m creeper, catch me if you can) ซึ่ง Ray Thompson ผู้ประดิษฐ์ระบบอีเมล ได้เขียนโปรแกรม Reaper เพื่อไล่ตามและลบโปรแกรม Creeper โดยโปรแกรม Reaper ไม่ได้เป็นเพียงตัวอย่างแรกของซอฟต์แวร์สำหรับป้องกันไวรัสเท่านั้น แต่ยังเป็นโปรแกรมจำลองตัวเองตัวแรกอีกด้วย จึงทำให้โปรแกรม Reaper ได้ชื่อว่าเป็น Computer Worm ตัวแรกของ

---

[58] Ibid.

[59] สาวตรี สุขศรี, กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2563), หน้า 62 - 63.

[60] Worm เป็นโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้สามารถแพร่กระจายตัวเองจากคอมพิวเตอร์เครื่องไปยังคอมพิวเตอร์อีกเครื่องได้โดยอาศัยระบบเน็ตเวิร์ค ซึ่งสามารถแพร่กระจายได้ด้วยตนเอง และแพร่กระจายได้อย่างรวดเร็วและทำความเสียหายรุนแรงกว่า Virus มาก

โลก[61] และต่อมาใน ค.ศ. 1987 ได้มีการเกิดโปรแกรมป้องกันไวรัสในเชิงพาณิชย์ขึ้นเป็นครั้งแรกด้วยเช่นกัน[62]

นอกจากนี้ในช่วงทศวรรษดังกล่าวยังได้เริ่มมีการถกเถียงเพื่อหาทางแก้ปัญหาเกี่ยวกับอาชญากรรมคอมพิวเตอร์ เนื่องจากผลกระทบของอาชญากรรมคอมพิวเตอร์มิได้จำกัดขอบเขตอยู่แค่เพียงข้อมูลส่วนบุคคลอีกต่อไป แต่เริ่มส่งผลกระทบถึงระบบเศรษฐกิจด้วย ความผิดสำคัญที่เกิดขึ้นบ่อยครั้ง เช่น การบิดเบือนเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ (Computer Manipulation) การก่อวินาศกรรมคอมพิวเตอร์ (Computer Sabotage) การเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ (Unauthorized Access to Information) รวมทั้งปัญหาการละเมิดลิขสิทธิ์ซอฟต์แวร์ และการลักลอบทำซ้ำผลงานสร้างสรรค์ดิจิทัลอันมีลิขสิทธิ์ เป็นต้น[63]

3) ช่วงทศวรรษที่ 1990 จนถึงปัจจุบัน นับแต่ช่วงปลายทศวรรษที่ 1980 จนถึงปี ค.ศ. 1996 ได้เกิดไวรัสคอมพิวเตอร์จำนวนมากผ่านการใช้เทคนิคและนวัตกรรมใหม่ ๆ ทำให้เกิดความท้าทายสำหรับนักพัฒนาโปรแกรมป้องกันไวรัสที่จะต้องพัฒนาความสามารถของโปรแกรมป้องกันอยู่เสมอ อีกทั้งในช่วงปลายของทศวรรษที่ 1990 ที่การใช้อีเมลได้แพร่หลายมากขึ้น แม้ว่าจะเป็นการปฏิวัติของวงการการสื่อสาร แต่ในขณะเดียวกันก็เป็นช่องทางใหม่สำหรับการโจมตีของไวรัสคอมพิวเตอร์ต่าง ๆ ด้วย ซึ่งจำนวนของไวรัสและมัลแวร์ (Malware) ใหม่ได้มีจำนวนที่เพิ่มขึ้นเป็นอย่างมาก จากในช่วงทศวรรษที่ 1990 ที่มีจำนวนเพียงหลักหมื่น ได้เพิ่มขึ้นเป็นกว่าห้าล้านกรณีในปี ค.ศ. 2007 จึงเป็นที่ชัดเจนว่าจำเป็นต้องมีมาตรการในการปกป้องและรักษาความปลอดภัยไซเบอร์[64]

นับตั้งแต่ทศวรรษที่ 1990 เป็นต้นมา อาชญากรรมคอมพิวเตอร์ไม่ได้ส่งผลกระทบต่อเพียงแค่ข้อมูลส่วนบุคคล หรือระบบเศรษฐกิจเท่านั้น แต่ยังส่งผลกระทบต่อสิ่งที่กฎหมายมุ่งจะคุ้มครองด้วย โดยผู้กระทำความผิดอาจมีเป้าหมายเพื่อสร้างความเสียหายต่อสาธารณประโยชน์ สังคม หรือแม้กระทั่งต่อชีวิตร่างกาย เป็นต้น ด้วยการพัฒนาของเทคโนโลยีส่งผลให้ลักษณะของการกระทำ

---

[61] Katie Chadd, "The History of Cybercrime and Cybersecurity, 1940-2020."

[62] Bogdan Popa, "Did You Know: The First Antivirus Product Was Launched in 1987," [Online] Accessed: 12/11/65. Available from: https://news.softpedia.com/news/did-you-know-the-first-antivirus-product-was-launched-in-1987-528883.shtml

[63] สาวตรี สุขศรี, กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์, หน้า 64 - 65.

[64] Katie Chadd, "The History of Cybercrime and Cybersecurity, 1940-2020."

ความผิดมีลักษณะที่แตกต่างไปจากเดิม กล่าวคือ จากเดิมที่ผู้กระทำความผิดกระทำต่อระบบคอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์เครื่องใดเครื่องหนึ่ง หรือใช้คอมพิวเตอร์ส่วนบุคคลเป็นเครื่องมือกลับกลายเป็นการทำความผิดโดยอาศัยเครือข่ายคอมพิวเตอร์ซึ่งเชื่อมโยงคอมพิวเตอร์จำนวนมากเข้าไว้ด้วยกัน ส่งผลให้ความเสียหายที่เกิดขึ้นขยายขอบเขตกว้างออกไป[65] จึงอาจกล่าวได้ว่ารูปแบบของการกระทำความผิดมีการพัฒนาจากลักษณะของอาชญากรรมคอมพิวเตอร์ที่อาจส่งผลกระทบต่อบุคคลใดบุคคลหนึ่ง กลายเป็นอาชญากรรมไซเบอร์ที่ส่งผลต่อบุคคลเป็นจำนวนมาก และอาจสร้างความเสียหายเป็นวงกว้างให้แก่ประเทศได้ ดังนั้นเพื่อรับมือต่อภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลา มาตรการในการรักษาความมั่นคงปลอดไซเบอร์จึงเป็นสิ่งจำเป็นที่รัฐจะนำมาใช้เพื่อป้องกันและตอบโต้ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

3.1.2 ความหมายของอาชญากรรมไซเบอร์

แม้ปัจจุบันในทางวิชาการจะมีการให้คำนิยามของคำว่า “อาชญากรรมคอมพิวเตอร์” (Computer Crime) และ “อาชญากรรมไซเบอร์” (Cybercrime) ที่หลากหลายและแตกต่างกันไป แต่ยังไม่มีคำนิยามใดคำนิยามหนึ่งที่เป็นที่ยอมรับโดยทั่วไป[66] ตัวอย่างของความหมายของอาชญากรรมคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ เช่น

“กิจกรรมของอาชญากรซึ่งมีคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์เป็นวิธีการหลักในการกระทำความผิดหรือฝ่าฝืนกฎหมาย” (Criminal activities in which computers or computer networks are the principal means of committing an offense.)[67]

“กิจกรรมต้องห้ามตามกฎหมายซึ่งอาศัยคอมพิวเตอร์เป็นสื่อและสามารถกระทำผ่านเครือข่ายโดยส่งผลระหว่างประเทศ”[68]

“กิจกรรมใดซึ่งคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ถูกใช้เป็นเครื่องมือ หรือตกเป็นเป้าหมาย หรือเป็นสภาพแวดล้อมของการประกอบอาชญากรรม”[69]

---

[65] สาวตรี สุขศรี, กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์, หน้า 65 - 68.

[66] คณาธิป ทองรวีวงศ์, กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1 (กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2563), หน้า 7.

[67] Nir Kshetri, "Positive Externality, Increasing Returns, and the Rise in Cybercrimes,"(2009). อ้างใน คณาธิป ทองรวีวงศ์, กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1, หน้า 8.

[68] Chris Hale, "Cybercrime: Facts & Figures Concerning This Global Dilemma," Crime & Justice International 18, 65 (2545). อ้างใน คณาธิป ทองรวีวงศ์, กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1, หน้า 8.

“อาชญากรรมที่กระทำในพื้นที่เสมือน ซึ่งข้อมูลเกี่ยวกับบุคคล เหตุการณ์ หรือเรื่องราวต่าง ๆ ถูกแสดงออกมาในรูปของตัวเลขหรือสัญลักษณ์และส่งผ่านเครือข่าย” (Cybercrime is crime committed in a virtual space and a virtual space fashioned in a way that information are represented in mathematical, symbol or any other way and transferred through local and global networks.)[70]

แม้ความหมายหรือคำนิยามของคำว่า อาชญากรรมคอมพิวเตอร์ และอาชญากรรมไซเบอร์ที่ยกตัวอย่างมาข้างต้นจะได้มีการให้ความหมาย และคำนิยามไว้หลากหลายแตกต่างกันไป แต่จะเห็นได้ว่ามีองค์ประกอบร่วมกันบางประการ เช่น สถานที่หรือสภาพแวดล้อมของการกระทำความผิดซึ่งเกี่ยวข้องกับพื้นที่ไซเบอร์ หรือเครือข่ายคอมพิวเตอร์ ลักษณะของการกระทำ ผลกระทบ บุคคลผู้ถูกกระทำ เป้าหมาย วัตถุประสงค์ อุปกรณ์ เครื่องมือ หรือวิธีการ เป็นต้น[71] ทำให้พอที่จะจำกัดความได้ว่า อาชญากรรมทางไซเบอร์ หมายถึง การกระทำความผิดโดยใช้อุปกรณ์อิเล็กทรอนิกส์ ไม่ว่าจะเป็นคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ กระทำบนคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์

3.2 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

นับตั้งแต่ประเทศไทยได้มีการประกาศให้บังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประเทศไทยมีสถิติการคุกคามทางไซเบอร์ที่ลดลงอย่างต่อเนื่อง ดังปรากฏตามตารางซึ่งเป็นการจัดเก็บข้อมูลโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[72]

---

[69] David L. Carter, "Computer Crime Categories: How Techno-Criminals Operate," FBI Law Enforcement Bulletin 64, 7 (2538). อ้างใน คณาธิป ทองรวีวงศ์, กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1, หน้า 8.

[70] Nureni Ayofe Azeez and Oluwaseyi Osunade, "Approach to Solving Cybercrime and Cybersecurity," International Journal of Computer Science and Information Security (IJCSIS) 3, 1 (2552). อ้างใน คณาธิป ทองรวีวงศ์, กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1, หน้า 9.

[71] คณาธิป ทองรวีวงศ์, กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1, หน้า 9.

[72] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, "สถิติภัยคุกคาม," [Online] Accessed: 11/11/65. Available from: https://www.etda.or.th/th/Our-Service/thaicert/stat.aspx

ตารางที่ 1 : สถิติภัยคุกคามทางไซเบอร์ตั้งแต่ปี พ.ศ. 2560 ถึง พ.ศ. 2564

ปี	พ.ศ. 2560	พ.ศ. 2561	พ.ศ. 2562	พ.ศ. 2563	พ.ศ. 2564
จำนวนของภัยคุกคามทางไซเบอร์	3,237 กรณี	2,520 กรณี	2,470 กรณี	2,250 กรณี	2,069 กรณี

นอกจากข้อมูลของสถิติภัยคุกคามทางไซเบอร์ในตารางข้างต้นแล้ว สถิติของภัยคุกคามทางไซเบอร์ในปี พ.ศ. 2565 โดยนับตั้งแต่เดือนมกราคมถึงเดือนกันยายน มีสถิติของภัยคุกคามไซเบอร์ที่เกิดขึ้นทั้งสิ้น 1,884 กรณีด้วยกัน[73] แม้จำนวนสถิติของภัยคุกคามไซเบอร์ในประเทศไทยจะลดลงในทุก ๆ ปี แต่มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ก็ยังคงเป็นมาตรการจำเป็นที่รัฐจะต้องให้ความสำคัญ และกำหนดมาตรการหรือนโยบายที่มีความเหมาะสมต่อไปในอนาคต

ประเทศไทยได้เล็งเห็นถึงความสำคัญของการพัฒนาเศรษฐกิจดิจิทัลภายในประเทศ จึงได้มีการกำหนดกรอบนโยบายเศรษฐกิจดิจิทัลเพื่อเศรษฐกิจและสังคม หรือ Digital Economy ขึ้น โดยในส่วนของกฎหมายได้มีการจัดทำชุดร่างกฎหมายเพื่อการส่งเสริมเศรษฐกิจและสังคม หรือเรียกสั้น ๆ ว่า “ชุดกฎหมายเศรษฐกิจดิจิทัล”[74] ซึ่งในชุดกฎหมายดังกล่าว ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นกฎหมายสำคัญที่มีวัตถุประสงค์เพื่อกำหนดมาตรการในการรักษาความปลอดภัยไซเบอร์ โดยในภายหลังได้มีการประกาศใช้บังคับเมื่อวันที่ 28 พฤษภาคม พ.ศ. 2562 ใช้ชื่อว่า “พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562” มีรายละเอียดอันเป็นสาระสำคัญ 3 ประการด้วยกัน ดังนี้

1) กำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐมีมาตรฐาน และมีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

[73] Ibid.

[74] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, "ร่างกฎหมายเศรษฐกิจดิจิทัล," [Online] Accessed: 11/11/65. Available from: https://ictlawcenter.etda.or.th/de_laws

2) มีการเฝ้าระวังภัยคุกคามทางไซเบอร์ และมีแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ

3) มีการร่วมมือ และประสานงานระหว่างกันกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อมีภัยร้ายแรงที่ทำให้การให้บริการที่สำคัญไม่สามารถทำงานได้ จนทำให้เกิดความเดือนร้อนแก่ประชาชน

นอกจากสาระสำคัญทั้ง 3 ประการแล้ว ยังปรากฏหลักการและเหตุผลในการประกาศใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ซึ่งปรากฏอยู่ในหมายเหตุท้ายพระราชบัญญัติ ดังนี้

“โดยที่ปัจจุบันการให้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเตอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกัน หรือรับมือภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควรกำหนดลักษณะของภารกิจ หรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐ และหน่วยงานเอกชนที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการ และมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกัน และการรับมือภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องตราพระราชบัญญัตินี้”

นอกจากรายละเอียดอันเป็นสาระสำคัญ รวมไปถึงหลักการและเหตุผลในการตราพระราชบัญญัติ ฯ แล้ว ยังปรากฏมาตรการต่าง ๆ ที่ให้อำนาจแก่เจ้าหน้าที่รัฐในการดำเนินการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์หลายประการด้วยกัน โดยสามารถแบ่งออกได้เป็น 3 ประการตามระดับความร้ายแรงของภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น หรือเกิดขึ้น โดยอำนาจของรัฐในการดำเนินการดังกล่าวจะมีลักษณะเป็นการให้อำนาจอย่างกว้างขวางหรือไม่ก็แปรผันตรงกับระดับความร้ายแรงของภัยคุกคามทางไซเบอร์นั้น ๆ โดยมีรายละเอียดที่สำคัญ ดังนี้

1) อำนาจในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ตาม มาตรา 59 ซึ่งไม่ได้ให้อำนาจเป็นพิเศษแก่เจ้าหน้าที่รัฐแต่อย่างใด คงกำหนดเพียงว่าให้เจ้าหน้าที่รัฐทำการรวบรวม ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบ รวมไปถึงการสนับสนุนให้ความช่วยเหลือ หรือประสานงาน ในการป้องกัน รับมือ และลดความเสี่ยงเท่านั้น[75]

2) อำนาจในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงตาม มาตรา 62 ซึ่งให้อำนาจแก่เจ้าหน้าที่รัฐในการเข้าถึงข้อมูล 2 ประการด้วยกัน ได้แก่ การมีหนังสือขอความร่วมมือให้บุคคลที่เกี่ยวข้องมาให้ข้อมูลหรือให้ส่งข้อมูลเป็นหนังสือ และการมีหนังสือขอข้อมูลเอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของบุคคลใดเพื่อประโยชน์ในการดำเนินการ[76]

อำนาจของในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรงตาม มาตรา 65 (5) และ มาตรา 66 (2) และ (4) ซึ่งให้อำนาจแก่เจ้าหน้าที่รัฐในการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์[77] ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ[78] ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ โดยในการเข้าถึงข้อมูลดังกล่าวจะต้องยื่นคำร้องต่อศาลโดยระบุเหตุอันควรเชื่อได้ว่ามีบุคคลใดบุคคลหนึ่งกำลังก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

และ 3) อำนาจในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤต ตาม มาตรา 68 ซึ่งกำหนดให้มีอำนาจดำเนินการใด ๆ ได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าโดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากได้ดำเนินการไปแล้วให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว รวมถึงมีอำนาจขอข้อมูลที่เป็นปัจจุบันและต่อเนื่อง (Real Time) จากผู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์

เมื่อพิจารณาอำนาจของเจ้าหน้าที่รัฐทั้ง 3 ประการข้างต้น จะเห็นได้ว่าในกรณีที่เป็นการขอความร่วมมือโดยตรงจากบุคคลซึ่งมีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เจ้าหน้าที่รัฐ

---

[75] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 59

[76] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 62

[77] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 65 (5) และ 66 (2)

[78] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 66 (4)

สามารถดำเนินการไปได้โดยทันที ส่วนในกรณีที่เป็นการใช้อำนาจเพื่อเข้าถึงข้อมูลต่าง ๆ ของประชาชนที่มีลักษณะเป็นการกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน เจ้าหน้าที่รัฐจะต้องดำเนินการตามบทบัญญัติของกฎหมายโดยเคร่งครัด เช่น ในการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ มาตรา 65 กำหนดให้ต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้บุคคลดำเนินการตามคำร้อง โดยคำร้องที่ยื่นต่อศาลจะต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำ หรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง เป็นต้น จะเห็นได้ว่าโดยทั่วไปแล้วในการที่เจ้าหน้าที่รัฐจะเข้าถึงข้อมูลต่าง ๆ ของประชาชนได้นั้น หากไม่ใช่กรณีที่ขอความร่วมมือจากประชาชน เจ้าหน้าที่รัฐจะต้องดำเนินการตามขั้นตอนต่าง ๆ ที่ได้มีการกำหนดไว้ และยังไม่การกำหนดบทลงโทษในกรณีที่เจ้าหน้าที่อำนาจโดยมิชอบอีกด้วย ซึ่งขั้นตอนต่าง ๆ เหล่านี้เป็นขั้นตอนในการควบคุมและตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐ ซึ่งได้มีการนำแนวความคิดตามทฤษฎีต่าง ๆ มาปรับใช้ ไม่ว่าจะเป็นหลักนิติรัฐหรือหลักนิติธรรม หลักการตรวจสอบการใช้อำนาจรัฐ หลักเหตุอันควรเชื่อและเหตุอันควรสงสัย รวมไปถึงหลักการในการคุ้มครองสิทธิเสรีภาพของประชาชนอื่น ๆ เป็นต้น

อย่างไรก็ตาม ในกรณีที่จำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ซึ่งมีความร้ายแรงเป็นอันมากดังเช่นในกรณีของภัยคุกคามทางไซเบอร์ในระดับวิกฤติตามที่ได้มีการกำหนดไว้ในพระราชบัญญัติ ฯ เจ้าหน้าที่รัฐมีอำนาจในการดำเนินการใด ๆ เท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้โดยไม่ต้องยื่นคำร้องต่อศาล แต่ภายหลังจากการดำเนินการดังกล่าวแล้วให้แจ้งรายละเอียดการดำเนินการต่อศาลที่มีเขตอำนาจโดยเร็ว ซึ่งกรณีของภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีความจำเป็นเร่งด่วนนี้ เป็นกรณีที่หากไม่ดำเนินการทันทีอาจจะทำให้ส่งผลกระทบและเกิดความเสียหายเป็นวงกว้างได้ จึงมีความจำเป็นที่จะต้องให้อำนาจแก่เจ้าหน้าที่รัฐเป็นพิเศษในการดำเนินมาตรการต่าง ๆ เพื่อเป็นการป้องกันและเยียวยาความเสียหายที่อาจเกิดขึ้น

จากมาตรการดังกล่าวข้างต้น ซึ่งเป็นมาตรการที่ให้อำนาจแก่เจ้าหน้าที่รัฐในการเข้าถึงข้อมูลต่าง ๆ ของประชาชนได้ และสามารถจัดเก็บหรือรวบรวมข้อมูลต่าง ๆ เหล่านั้นมาใช้เพื่อประโยชน์ในการดำเนินการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์แล้ว ข้อมูลต่าง ๆ เหล่านั้นยังสามารถนำไปใช้ประกอบการดำเนินคดีต่าง ๆ ได้อีกด้วย โดยหลักการนำ

ข้อมูลไปใช้ประกอบการดำเนินคดีปรากฏอยู่ในมาตรา 70 ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

“มาตรา 70 ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นหรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจโดยมิชอบ”

เมื่อพิจารณาบทบัญญัติดังกล่าวจะเห็นได้ว่า โดยทั่วไปแล้วมาตรา 70 ห้ามมิให้เจ้าหน้าที่รัฐเปิดเผยหรือส่งมอบข้อมูลต่าง ๆ ที่ได้มาตามมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ แต่ก็ได้มีข้อยกเว้นปรากฏอยู่ใน มาตรา 70 วรรคสอง ซึ่งกำหนดให้สามารถเปิดเผยหรือส่งมอบข้อมูลซึ่งได้มาเหล่านั้นเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัติ ฯ ผู้กระทำความผิดตามกฎหมายอื่น หรือการดำเนินคดีกับเจ้าหน้าที่รัฐเกี่ยวกับการใช้อำนาจโดยมิชอบได้ ซึ่งทำให้นอกจากข้อมูลซึ่งได้มาตามมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์จะนำมาใช้เพื่อเหตุผลในการดำเนินการตามมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และนำมาใช้พยานหลักฐานในการดำเนินคดีตามฐานความผิดต่าง ๆที่ได้กำหนดไว้ในพระราชบัญญัติ ฯ แล้ว ยังสามารถนำไปใช้เป็นพยานหลักฐานในการดำเนินคดีในฐานความผิดตามกฎหมายอื่นได้อีกด้วย ซึ่งข้อมูลส่วนใหญ่ที่ได้มาตามมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์มักจะเป็นข้อมูลซึ่งอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์เป็นส่วนใหญ่ ส่งผลให้มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย เมื่อพิจารณาประกอบกับมาตรา 70 วรรคสองแล้ว ย่อมถือได้ว่าเป็นมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์มาตรการหนึ่งของประเทศไทย

3.3 มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทย

มาตรการในการแสวงหาพยานหลักฐานของประเทศไทยปรากฏอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา โดยมาตรการที่สำคัญได้แก่การค้น ซึ่งการค้นนั้น โดยหลักจะกระทำได้ต่อเมื่อมี

หมายค้นเท่านั้น[79] โดยเหตุที่จะออกหมายค้นได้นั้นประมวลกฎหมายวิธีพิจารณาความอาญา ได้บัญญัติไว้ในมาตรา 69 ดังนี้

มาตรา 69 บัญญัติว่า “เหตุที่จะออกหมายค้นได้มีดังต่อไปนี้

(1) เพื่อพบและยึดสิ่งของซึ่งจะเป็นพยานหลักฐานประกอบการสอบสวน ไต่สวนมูลฟ้องหรือพิจารณา

(2) เพื่อพบและยึดสิ่งของซึ่งมีไว้เป็นความผิด หรือได้มาโดยผิดกฎหมาย หรือมีเหตุอันควรสงสัยว่าได้ใช้หรือตั้งใจจะใช้ในการกระทำความผิด

(3) เพื่อพบและช่วยบุคคลซึ่งได้ถูกหน่วงเหนี่ยวหรือกักขังโดยมิชอบด้วยกฎหมาย

(4) เพื่อพบบุคคลซึ่งมีหมายให้จับ

(5) เพื่อพบและยึดสิ่งของตามคำพิพากษาหรือตามคำสั่งศาล ในกรณีที่จะพบหรือจะยึดโดยวิธีอื่นไม่ได้แล้ว”

นอกจากเหตุแห่งการค้นแล้ว ยังได้มีการบัญญัติในเรื่องของการค้นในที่รโหฐานที่สำคัญไว้ ซึ่งปรากฏอยู่ในมาตรา 92 และ 98 โดยในมาตรา 98 ได้กำหนดเกี่ยวกับหลักเกณฑ์ในการค้นในที่รโหฐาน ดังนี้

มาตรา 98 บัญญัติว่า “การค้นในที่รโหฐานนั้นจะค้นได้แต่เฉพาะเพื่อหาตัวคนหรือสิ่งของที่ต้องการค้นเท่านั้น แต่มีข้อยกเว้นดังนี้

(1) ในกรณีที่ค้นหาสิ่งของโดยไม่จำกัดสิ่ง เจ้าพนักงานผู้ค้นมีอำนาจยึดสิ่งของใด ๆ ซึ่งน่าจะใช้เป็นพยานหลักฐานเพื่อประโยชน์หรือยันผู้ต้องหาหรือจำเลย

(2) เจ้าพนักงานซึ่งทำการค้นมีอำนาจจับบุคคลหรือสิ่งของอื่นในที่ค้นนั้นได้เมื่อมีหมายต่างหากหรือในกรณีความผิดซึ่งหน้า”

ส่วนมาตรา 92 ได้กำหนดข้อยกเว้นสำหรับการค้นในที่รโหฐานเอาไว้ ดังนี้

---

[79] ประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 57 วรรคแรก “ภายใต้บังคับแห่งบทบัญญัติในมาตรา 78 มาตรา 79 มาตรา 80 มาตรา 92 และมาตรา 94 แห่งประมวลกฎหมายนี้ จะจับ ขัง จำคุก หรือค้นในที่รโหฐานหาตัวคนหรือสิ่งของ ต้องมีคำสั่งหรือหมายของศาลสำหรับการนั้น”

มาตรา 92 บัญญัติว่า “ห้ามมิให้ค้นในที่รโหฐานโดยไม่มีหมายค้นเว้นแต่พนักงานฝ่ายปกครองหรือตำรวจเป็นผู้ค้น และในกรณีต่อไปนี้

(1) เมื่อมีเสียงร้องให้ช่วยมาจากข้างในที่รโหฐาน

(2) เมื่อปรากฏความผิดซึ่งหน้ากำลังกระทำลงในที่รโหฐาน

(3) เมื่อบุคคลที่ได้กระทำความผิดซึ่งหน้า ขณะที่ถูกไล่จับหนีเข้าไปหรือมีเหตุอันแน่นแฟ้นควรสงสัยว่าได้เข้าไปซุกซ่อนตัวอยู่ในที่รโหฐานนั้น

(4) เมื่อมีความสงสัยตามสมควรว่าสิ่งของที่ได้มาโดยการกระทำความผิดได้ซ่อนหรืออยู่ในนั้น ประกอบทั้งต้องมีเหตุอันควรเชื่อว่าเนื่องจากการเนิ่นช้ากว่าจะเอาหมายค้นมาได้สิ่งของนั้นจะถูกโยกย้ายเสียก่อน

(5) เมื่อที่รโหฐานนั้นผู้จะต้องถูกจับเป็นเจ้าบ้าน และการจับนั้นมีหมายจับหรือจับตามมาตรา 78

เมื่อพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ค้นด้วยตนเองไม่ต้องมีหมายค้นก็ได้ แต่ต้องเป็นกรณีที่อาจออกหมายค้นหรือค้นได้ตามประมวลกฎหมายนี้”

เมื่อพิจารณาบทบัญญัติข้างต้นจะเห็นได้ว่าการค้นนั้นต้องเป็นไปเพื่อเหตุดังที่ได้กำหนดไว้ในกฎหมายเท่านั้น โดยการค้นจะต้องมีหมายค้นเสมอ เว้นแต่เข้าข้อยกเว้นที่กฎหมายกำหนดไว้ตามมาตรา 92 (1) ถึง (5) ที่ให้อำนาจเจ้าหน้าที่รัฐทำการค้นโดยไม่ต้องมีหมายได้ ซึ่งเมื่อพิจารณาตามข้อยกเว้นข้างต้นจะเห็นได้ว่า การค้นโดยไม่มีหมายจะกระทำได้ต่อเมื่อเป็นกรณีที่มีพฤติการณ์หรือข้อมูลที่เกี่ยวข้องกับการกระทำความผิด เพื่อเป็นการตรวจสอบและจำกัดอำนาจในการแสวงหาพยานหลักฐานของเจ้าหน้าที่รัฐซึ่งทำการค้น อันเป็นไปตามรัฐธรรมนูญแห่งราชอาณาจักรไทย ฯ ในหลักการคุ้มครองในความเป็นอยู่ส่วนตัว และในข้อมูลส่วนตัวใด ๆ ตามมาตรา 32 ซึ่งการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะเท่านั้น และในหลักการคุ้มครองสิทธิเสรีภาพในมาตรา 33 การล่วงละเมิดหรือรุกกล้ำเคหสถานของบุคคลจะกระทำมิได้ เว้นแต่ได้รับอนุญาตจากเจ้าของเคหสถานหรือ

อาศัยอำนาจตามบทบัญญัติของกฎหมาย โดยรายละเอียดในการขอออกหมายค้นจากศาลจะต้องมีรายละเอียด ดังต่อไปนี้[80]

(1) ต้องระบุลักษณะสิ่งของที่ต้องการหาและยึด หรือชื่อตัว ชื่อสกุล รูปพรรณ อายุของบุคคลที่ต้องการหา และสถานที่ที่จะค้น ระบุบ้านเลขที่ ชื่อตัว ชื่อสกุลและสถานะของเจ้าของหรือผู้ครอบครองเท่าที่ทราบ หากไม่สามารถระบุบ้านเลขที่ที่จะค้นได้ ให้ทำแผนที่ของสถานที่ที่จะค้นและบริเวณใกล้เคียงแทน

(2) ต้องระบุเหตุที่จะออกหมายค้น ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 69 พร้อมสำเนาเอกสารซึ่งสนับสนุนเหตุแห่งการออกหมายค้น

(3) แนบแบบพิมพ์หมายค้นที่กรอกข้อความครบถ้วนแล้วพร้อมสำเนา รวมทั้งเอกสารอื่นที่เกี่ยวข้อง เช่น บันทึกคำร้องทุกข์ หนังสือมอบอำนาจให้ร้องทุกข์ เป็นต้น มาท้ายคำร้อง

แม้ตามประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศไทยจะไม่ได้มีการกำหนดเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ไว้โดยเฉพาะ แต่ก็ได้มีการกำหนดมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ไว้ในกฎหมายฉบับอื่น ๆ อีก ไม่ว่าจะเป็นพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฯ พระราชบัญญัติการสอบสวนคดีพิเศษ ฯ เป็นต้น

อย่างไรก็ตาม ประมวลกฎหมายวิธีพิจารณาความอาญาไม่ได้มีการกำหนดมาตรการเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ไว้โดยเฉพาะ แต่มีปรากฏอยู่ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ซึ่งมีวัตถุประสงค์ในการสืบสวน สอบสวน และแสวงหาพยานหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิดมาลงโทษเป็นหลัก[81] และมีบทบัญญัติที่เกี่ยวข้องกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ปรากฏอยู่ใน มาตรา 18 และ 19 ดังนี้

มาตรา 18 บัญญัติว่า “ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอ

---

[80] ข้อบังคับของประธานศาลฎีกาว่าด้วยหลักเกณฑ์และวิธีการเกี่ยวกับการออกคำสั่งหรือหมายอาญา พ.ศ. 2548 มาตรา 11

[81] คณาธิป ทองรวีวงศ์, กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1, หน้า 637 - 639.

ตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิด หรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น

พนักงานสอบสวนอาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริงดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่รีบรวบรวมข้อเท็จจริงและหลักฐานแล้วแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (1) (2) และ (3) ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงานเจ้าหน้าที่กำหนดซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่ ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดระยะเวลาที่ต้องดำเนินการที่เหมาะสมกับประเภทของผู้ให้บริการก็ได้”

มาตรา 19 บัญญัติว่า “การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) และ (8) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา 18 (4) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา 18 (8) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้วพนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง”

เมื่อพิจารณาบทบัญญัติดังกล่าวสามารถสรุปมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ออกได้เป็นสองประการด้วยกัน ดังนี้

(1) มาตรา 18 (1) (2) และ (3) ให้อำนาจแก่เจ้าหน้าที่รัฐในการมีหนังสือสอบถามหรือเรียกให้บุคคลที่เกี่ยวข้องกับการกระทำความผิดมาให้ข้อมูล ส่งคำชี้แจงเป็นหนังสือ ส่งเอกสาร ข้อมูลหรือหลักฐานต่าง ๆ[82] เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการที่เกี่ยวข้อง[83] และสั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่กฎหมายกำหนดให้ต้องเก็บรักษาไว้ หรือข้อมูลที่อยู่ในการครอบครองหรือควบคุมของผู้ให้บริการแก่เจ้าพนักงาของรัฐ[84] โดยผู้ที่ได้รับการร้องขอข้างต้นจะต้องดำเนินการตามคำร้องขอโดยไม่ชักช้า เว้นแต่กรณีที่มีเหตุสมควรต้องได้รับอนุญาตจากเจ้าหน้าที่รัฐจึงจะไม่ดำเนินการตามการร้องขอดังกล่าวได้[85]

(2) มาตรา 18 (4) (5) (6) (7) และ (8) ให้อำนาจแก่เจ้าหน้าที่รัฐในการทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด[86] สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวแก่เจ้าหน้าที่รัฐ[87] ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อ

---

[82] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 (1)

[83] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 (2)

[84] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 (3)

[85] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 วรรคท้าย

[86] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 (4)

[87] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 (5)

สืบสวนหาตัวผู้กระทำความผิด[88] ถอดรหัสข้อมูลลับของข้อมูลคอมพิวเตอร์ หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้าถึงรหัสลับของข้อมูลดังกล่าว ทำการถอดรหัสลับหรือให้ความร่วมมือในการถอดรหัสลับ[89] ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดเกี่ยวกับการกระทำความผิด[90] โดยการใช้อำนาจดังกล่าวข้างต้น เจ้าหน้าที่รัฐจะต้องยื่นคำร้องต่อศาลเพื่อมีคำสั่งอนุญาตให้ดำเนินการตามคำร้อง โดยคำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่จะสามารถระบุได้ด้วย[91]

นอกจากการสืบสวนและสอบสวนความผิดข้างต้นแล้ว ในมาตรา 18 วรรคสอง ได้วางหลักเกณฑ์ในกรณีที่พนักงานสอบสว สามารถร้องขอให้ดำเนินการตามมาตรา 18 วรรคหนึ่ง ได้ เพื่อประโยชน์ในการสืบสวนสอบสวนความผิดอาญาตามกฎหมายอื่น โดยกำหนดไว้ดังนี้ “เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิด หรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวนอาจจะร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริงดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่รีบรวบรวมข้อเท็จจริงและหลักฐานแล้วแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป”[92]

จากการศึกษาจะเห็นได้ว่า ในปัจจุบันมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นมาตรการสำคัญที่ควรจะได้มีการนำมาปรับใช้ในประเทศ เพราะอาชญากรรมไซเบอร์เป็นอาชญากรรมที่ส่งผลกระทบเป็นวงกว้างต่อสังคม และโครงสร้างทางสารสนเทศที่สำคัญต่าง ๆ ของประเทศ แม้การที่ประเทศไทยได้มีการประกาศให้บังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์จะเป็นสิ่งที่เหมาะสมกับสถานการณ์โลกในปัจจุบัน แต่อย่างไรก็ตาม เมื่อพิจารณา

---

[88] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 (6)

[89] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 (7)

[90] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 (8)

[91] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 19

[92] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 วรรคสอง

บทบัญญัติกฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานในประเทศไทย ซึ่งเป็นการให้อำนาจแก่เจ้าหน้าที่รัฐในการดำเนินการเพื่อรวบรวมพยานหลักฐานมาพิสูจน์ข้อเท็จจริงในคดี อันเป็นการดำเนินการที่กระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนอย่างไม่สามารถหลีกเลี่ยงได้ ดังนั้น ในการที่เจ้าหน้าที่รัฐจะใช้อำนาจดังกล่าว จะต้องเป็นไปตามหลักเกณฑ์ต่าง ๆ ที่กฎหมายได้บัญญัติไว้เท่านั้น ซึ่งการบัญญัติหลักเกณฑ์ดังกล่าวก็เป็นไปเพื่อตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐว่าเป็นไปโดยถูกต้องและสมควรหรือไม่ การที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศไทย ได้มีการกำหนดให้สามารถเปิดเผยและส่งมอบข้อมูลต่าง ๆ ที่ได้มาตามมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่นได้ซึ่งมีลักษณะเป็นการให้อำนาจแก่เจ้าหน้าที่รัฐในการแสวงหาพยานหลักฐาน จึงควรที่จะมีการตรวจสอบการใช้อำนาของเจ้าหน้าที่รัฐอย่างเหมาะสม เพื่อไม่ให้เป็นการกระทบกระเทือนสิทธิเสรีภาพของประชาชนเกินสมควร อันเป็นไปตามหลักการในการแสวงหาพยานหลักฐานทั่วไปซึ่งปรากฏอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา

บทที่ 4
มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในต่างประเทศ

เมื่อได้ศึกษาแนวความคิดและกฎหมายเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทยแล้ว ในบทนี้จะศึกษาถึงมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในต่างประเทศ เพื่อนำมาพิจารณาเปรียบเทียบกับกฎหมายเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทยว่าแต่ละประเทศมีแนวความคิด วัตถุประสงค์ และลักษณะของการกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์อย่างไร มีวิธีการใดที่เหมาะสมแก่การนำมาปรับใช้และพัฒนากฎหมายเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย ประเทศที่ผู้เขียนจะนำมาศึกษาเปรียบเทียบมี 3 ประเทศ ประกอบด้วย ประเทศสหรัฐอเมริกา ประเทศสิงคโปร์ และเครือรัฐออสเตรเลีย รัฐควีนส์แลนด์เครือรัฐออสเตรเลีย

4.1 ประเทศสหรัฐอเมริกา

ภายหลังเหตุการณ์ 9/11 สภาด้านความมั่นคงและคณะกรรมการของรัฐที่เกี่ยวข้องกับการข่าวกรองของประเทศสหรัฐอเมริกา (Senate Select Committee on Intelligence และ House Permanent Select Committee on Intelligence) ได้ทำการตรวจสอบระบบข่าวกรองของประเทศทั้งระบบ ทำให้ประเทศสหรัฐอเมริกาได้กำหนดยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ขึ้นมาใหม่[93] โดยได้มีการประกาศใช้กฎหมายความปลอดภัยไซเบอร์ ค.ศ. 2015 (Cybersecurity Act 2015) โดยได้กำหนดกลไกเกี่ยวกับการแบ่งปันข้อมูลระหว่างภาครัฐและภาคเอกชนเป็นสำคัญ[94] แบ่งออกเป็น 2 หมวดใหญ่ ๆ ด้วยกัน ได้แก่ หมวดที่ 1 กฎหมายการแบ่งปันข้อมูลความปลอดภัยไซเบอร์

---

[93] เศรษฐพงค์ มะลิสุวรรณ, "Cybersecurity ยักษ์ใหญ่ยังเคยล้ม จึงน่าศึกษาเป็นบทเรียน," [Online] Accessed: 10/11/65. Available from: https://www.beartai.com/article/beartai-ict/66506

[94] Sullivan & Cromwell LLP, "The Cybersecurity Act of 2015 : Congress Passes and President Signs Long-Anticipated Measure Setting Framework for Sharing Cyber Threat Information with Federal Government and Private Sector,"(2558). หน้า 1

ค.ศ. 2015 (Cybersecurity Information Sharing Act of 2015) และหมวดที่ 2 ความก้าวหน้าด้านความปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Advancement)

4.1.1 มาตรการในการรักษาความปลอดภัยไซเบอร์

ในต้นปี ค.ศ. 2013 ประธานาธิบดีโอบามาได้มีคำสั่ง Executive Order (EO) 13636, “Improving Critical Infrastructure Cybersecurity”[95] เพื่อให้มีการพัฒนามาตรการในการรักษาความปลอดภัยแก่โครงสร้างพื้นฐานทางสารสนเทศที่สำคัญของประเทศ จึงได้มีการตรากฎหมายการแบ่งปันข้อมูลความปลอดภัยไซเบอร์ ค.ศ. 2015 (Cybersecurity Information Sharing Act of 2015) ขึ้น โดยมีวัตถุประสงค์เพื่อพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ผ่านการแลกเปลี่ยน และแบ่งปันข้อมูลข่าวสารทางไซเบอร์ระหว่างรัฐบาลกลางและหน่วยงานอื่น ๆ เช่น ภาคเอกชน องค์กร หน่วยงานในระดับมลรัฐ รวมถึงหน่วยงานโครงสร้างพื้นฐานสำคัญ เป็นต้น โดยมีกระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security) เป็นหน่วยงานที่รับผิดชอบในการประสานงาน[96] โดยมีอำนาจในการออกมาตรการในการตรวจสอบป้องกันและส่งข้อมูลที่เกี่ยวข้องไปยังหน่วยงานอื่น ๆ ซึ่งระบบที่มีการแบ่งปันข้อมูลต้องเป็นระบบอัตโนมัติ และส่งข้อมูลแบบปัจจุบันและต่อเนื่อง (Real Time) เพื่อที่จะสามารถนำข้อมูลดังกล่าวไปใช้ประโยชน์ในการรับมือ ป้องกัน และบรรเทาความเสียหายจากภัยคุกคามไซเบอร์[97] โดยสามารถส่งข้อมูลดังกล่าวไปยังหน่วยงานราชการอื่นที่กฎหมายกำหนดได้[98]

กฎหมายการแบ่งปันข้อมูลความปลอดภัยไซเบอร์ ฯ ได้มีข้อกำหนดเกี่ยวกับข้อมูลที่ได้มาจากมาตรการตามกฎหมายฉบับนี้ต่อหน่วยงาน องค์กร หรือบุคคลที่ได้รับข้อมูลโดยเฉพาะใน

---

[95] The White House, "Executive Order -- Improving Critical Infrastructure Cybersecurity," [Online] Accessed: 11/11/56. Available from: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity#

[96] อนัญพร สกุลเมฆา, "การตรวจสอบและถ่วงดุลอำนาจเจ้าพนักงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562," หน้า 38.

[97] Cybersecurity Information Sharing Act 2015, Section 105 (a) (3)

[98] อนัญพร สกุลเมฆา, "การตรวจสอบและถ่วงดุลอำนาจเจ้าพนักงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562," หน้า 39.

เรื่องของการเปิดเผย การเก็บรักษา หรือการใช้งานข้อมูลดังกล่าว โดยจะต้องเป็นไปเพื่อการดังต่อไปนี้[99]

(1) เพื่อวัตถุประสงค์ด้านความปลอดภัยไซเบอร์

(2) เพื่อการตรวจสอบภัยคุกคามด้านความปลอดภัยไซเบอร์ หรือการหาช่องโหว่เกี่ยวกับการรักษาความปลอดภัยไซเบอร์

(3) เพื่อตอบสนอง ป้องกัน หรือบรรเทาผลกระทบจากภัยคุกคามไซเบอร์ ที่อาจก่อให้เกิดความเสียหายแก่ชีวิต หรือความเสียหายแก่ร่างกายอย่างร้ายแรง ความเสียหายทางเศรษฐกิจอย่างร้ายแรง รวมถึงการกระทำที่เกี่ยวเนื่องกับกฎหมายการก่อการร้าย

(4) เพื่อตอบสนอง สืบสวน ดำเนินคดี ป้องกัน หรือบรรเทาความเสียหายในการแสวงหาประโยชน์ในทางเพศ และภัยคุกคามต่อความปลอดภัยทางร่างกายใด ๆ ที่เกิดจากความผิดตามที่ระบุไว้ในข้อก่อนหน้านี้[100]

นอกจากนี้ยังได้มีข้อกำหนดเกี่ยวกับการคุ้มครองบุคคลที่ดำเนินการตามกฎหมายฉบับนี้ รวมไปถึงการคุ้มครองข้อมูลส่วนบุคคล ซึ่งสามารถแบ่งออกได้ดังต่อไปนี้[101]

(1) การแบ่งปันหรือรับข้อมูลตามที่ดำเนินการตามกฎหมายฉบับนี้ หรือการแบ่งปันข้อมูลกับรัฐบาลกลางภายใต้กระบวนการของกระทรวงความมั่นคง ฯ ย่อมไม่มีความรับผิดใด ๆ ในทางแพ่ง

(2) การแบ่งปันข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์กับรัฐบาลกลางจะไม่ถือว่าเป็นการสละเอกสิทธิ์หรือสละความคุ้มครองใด ๆ ที่กำหนดโดยกฎหมาย รวมถึงการป้องกันความลับทางการค้า และการแบ่งปันข้อมูลที่บ่งบอกถึงภัยคุกคามไซเบอร์ และมาตรการในการป้องกัน จะได้รับการยกเว้นจากการถูกเปิดเผยตามกฎหมายเสรีภาพด้านข้อมูลข่าวสาร (Freedom of Information Act)

---

[99] Sullivan & Cromwell LLP, "The Cybersecurity Act of 2015 : Congress Passes and President Signs Long-Anticipated Measure Setting Framework for Sharing Cyber Threat Information with Federal Government and Private Sector," หน้า 5.

[100] Cybersecurity Information Sharing Act 2015, Section 105 (5)

[101] Sullivan & Cromwell LLP, "The Cybersecurity Act of 2015 : Congress Passes and President Signs Long-Anticipated Measure Setting Framework for Sharing Cyber Threat Information with Federal Government and Private Sector," หน้า 8.

หรือกฎหมายว่าด้วยเสรีภาพด้านข้อมูลข่าวสารของรัฐบาลกลาง รัฐ มลรัฐ และการแบ่งปันข้อมูล ดังกล่าวจะถือเป็นข้อมูลทางพาณิชย์ การเงิน โดยข้อมูลดังกล่าวจะเป็นกรรมสิทธิ์ของหน่วยงานที่ให้ข้อมูล ไม่ใช่กรรมสิทธิ์ของรัฐบาลกลาง[102]

(3) กฎหมายฉบับนี้ไม่ได้เป็นการกำหนดหน้าที่ในการแบ่งปันข้อมูลเกี่ยวกับความปลอดภัยไซเบอร์ หรือหน้าที่ในการเตือน หรือดำเนินการใด ๆ จากการได้รับข้อมูลดังกล่าว และไม่ได้กำหนดความรับผิดต่อหน่วยงานใด ๆ ที่ไม่ประสงค์จะเข้าร่วมในการแบ่งปันข้อมูล

(4) ข้อมูลที่ได้รับจากการแบ่งปันข้อมูล หากพบว่าเป็นข้อมูลส่วนบุคคล หรือข้อมูลที่สามารถระบุตัวตนได้ ซึ่งไม่เกี่ยวข้องโดยตรงกับการรักษาความมั่นคงปลอดภัยไซเบอร์ จะต้องถูกนำออกจากระบบข้อมูลของกระทรวงความมั่นคง ฯ[103] และหากมีข้อมูลที่ไม่เกี่ยวข้องโดยตรงกับที่กฎหมายได้ให้อำนาจไว้ รัฐจะต้องทำลายข้อมูลดังกล่าวภายในระยะเวลาที่เหมาะสม[104]

(5) กำหนดมาตรการลงโทษสำหรับเจ้าหน้าที่รัฐ พนักงานหรือตัวแทนของหน่วยงานของรัฐบาลกลางในกรณีที่เกี่ยวข้องกับการแสดงเจตนากระทำการภายใต้หมวดนี้โดยไม่ได้รับอนุญาต[105]

4.1.2 มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์

ประเทศสหรัฐอเมริกาได้มีการวางหลักเกณฑ์เกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ไว้โดยเฉพาะ ซึ่งปรากฏอยู่ในคำพิพากษาของศาลและบทบัญญัติอื่นที่เกี่ยวข้อง สามารถแบ่งออกได้เป็น 2 ประการด้วยกัน ได้แก่ มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยมีหมาย และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยไม่มีหมาย ซึ่งมีรายละเอียดที่สำคัญดังต่อไปนี้

---

[102] Cybersecurity Information Sharing Act 2015, Section 105 (d)

[103] Cybersecurity Information Sharing Act 2015, Section 105 (d) (2)

[104] Cybersecurity Information Sharing Act 2015, Section 105 (b) (3) (B)

[105] อนัญพร สกุลเมฆา, "การตรวจสอบและถ่วงดุลอำนาจเจ้าพนักงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562," หน้า 42.

4.1.2.1 มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยมีหมาย

ภายหลังจากที่ได้มีการให้สัตยาบันรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 4 (The Fourth Amendment) ได้สร้างความเปลี่ยนแปลงให้แก่ระบบกระบวนการยุติธรรมทางอาญาในประเทศสหรัฐอเมริกาเป็นอันมาก โดยประเทศสหรัฐอเมริกาได้ให้ความคุ้มครองในเรื่องสิทธิในความเป็นส่วนตัว (Rights of Privacy) ของประชาชนอย่างกว้างขวาง อีกทั้งยังจำกัดอำนาจของเจ้าหน้าที่รัฐในการค้นและยึดทรัพย์สินซึ่งจะกระทำได้ต่อเมื่อมีหมายจากศาล และศาลจะออกหมายให้แก่เจ้าหน้าที่รัฐก็ต่อเมื่อเจ้าหน้าที่รัฐมีเหตุอันควรเชื่อ (Probable Clause) เท่านั้น จึงเป็นหน้าที่ของเจ้าหน้าที่รัฐที่จะต้องแสดงให้ศาลเห็นถึงเหตุอันควรเชื่อดังกล่าวเพื่อที่ศาลจะได้ทำการอนุมัติให้สามารถดำเนินการตามคำขอได้ ด้วยเหตุนี้จึงทำให้เจ้าหน้าที่รัฐไม่สามารถเข้าไปค้นและยึดสิ่งของในสถานที่ต่าง ๆ ได้โดยอิสระ โดยการค้นและยึดจะชอบด้วยหลักการในรัฐธรรมนูญ ฯ หากเป็นการค้นและยึดที่ไม่ละเมิดความคาดหวังที่สมเหตุสมผลในความเป็นส่วนตัวของประชาชน (Reasonable Expectation of Privacy)[106] ซึ่งศาลสูงได้อธิบายไว้ในคำพิพากษาฉบับหนึ่งว่า “สิ่งที่บุคคลเปิดเผยโดยเจตนาต่อสาธารณะ แม้ในบ้านพักอาศัยหรือที่ทำงานย่อมไม่อยู่ภายใต้ความคุ้มครองตามรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 4 แต่สิ่งที่บุคคลพยายามรักษาไว้ซึ่งความเป็นส่วนตัวแม้จะอยู่ในที่สาธารณะก็อาจได้รับความคุ้มครองตามรัฐธรรมนูญ ฯ”[107] ดังนั้น การคุ้มครองสิทธิในความเป็นส่วนตัวตามแนวคิดของรัฐธรรมนูญ ฯ จึงไม่ได้ขึ้นอยู่กับสิทธิในสถานที่หรือทรัพย์สินที่ถูกล่วงละเมิดนั้น ๆ แต่ขึ้นอยู่กับว่าบุคคลมีความคาดหวังที่สมเหตุสมผลในความเป็นส่วนตัวของประชาชนที่จะได้รับความคุ้มครองจากการล่วงละเมิดของเจ้าหน้าที่รัฐหรือไม่ ด้วยเหตุนี้เจ้าหน้าที่รัฐจึงไม่สามารถทำการค้นสถานที่หรือยึดทรัพย์สินของประชาชนตามอำเภอใจได้ แต่จะต้องดำเนินการตามหลักเกณฑ์ของกฎหมาย โดยในเรื่องของเหตุแห่งการค้นและยึดที่เจ้าหน้าที่รัฐสามารถกระทำได้นั้นแบ่งออกเป็นสองกรณีด้วยกันคือ

---

[106] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[107] What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

(1) กรณีทั่วไป เจ้าหน้าที่รัฐจะต้องขอหมายค้นจากศาลทุกกรณี เว้นแต่กรณีที่มีหลักเกณฑ์ของกฎหมายกำหนดไว้โดยชัดแจ้งว่าไม่จำต้องขอหมายค้นก่อนก็สามารถดำเนินการค้นไปได้

(2) กรณีพิเศษ เมื่อมีเหตุการณ์บางอย่างเกิดขึ้น หลักเกณฑ์ของกฎหมายอาจกำหนดให้เจ้าหน้าที่รัฐสามารถทำการค้นสถานที่และยึดทรัพย์สินได้โดยไม่จำเป็นต้องขอหมายจากศาลก่อน แต่การดำเนินการดังกล่าวเจ้าหน้าที่รัฐจะต้องทราบถึงข้อเท็จจริง หรือพฤติการณ์ที่เกี่ยวข้องกับอาชญากรรม หรือข้อมูลเกี่ยวกับสิ่งของที่ต้องการยึด แล้วจึงพิจารณาว่าเหตุดังกล่าวเป็นกรณีพิเศษที่ถือว่ามีเหตุผลสมควรที่จะทำการค้นหรือยึดหรือไม่

ในการที่เจ้าหน้าที่รัฐจะมีคำร้องขอออกหมายค้นนั้น โดยทั่วไปกฎหมายของประเทศสหรัฐอเมริกากำหนดหลักเกณฑ์ให้ศาลเป็นองค์กรผู้มีอำนาจออกหมายค้นตามคำร้องขอของเจ้าหน้าที่ตำรวจหรือพนักงานอัยการ โดยกฎข้อ 41 (c)[108] ของหลักเกณฑ์วิธีพิจารณาความอาญาของรัฐบาลกลาง (Federal Rules of Criminal Procedure) ได้กำหนดให้ผู้พิพากษา (magistrate judge) อาจออกหมายค้นให้แก่เจ้าหน้าที่รัฐเพื่อพบสิ่งของหรือบุคคลในกรณีดังต่อไปนี้

(1) เพื่อพบพยานหลักฐานในการกระทำความผิด

(2) เพื่อพบสิ่งของซึ่งมีไว้เป็นความผิด สิ่งของซึ่งได้จากการกระทำความผิดหรือสิ่งของอื่นใดที่ครอบครองโดยผิดกฎหมาย

(3) เพื่อพบทรัพย์ที่ทำไว้ หรือมีไว้เพื่อใช้ในการกระทำความผิด หรือใช้ในการกระทำความผิด

(4) เพื่อพบบุคคลที่ต้องการจับกุม หรือบุคคลที่ถูกหน่วงเหนี่ยวกักขังโดยไม่ชอบด้วยกฎหมาย

---

[108] Federal Rules of Criminal Procedure, Rule 41. (c) Persons or Property Subject to Search or Seizure. A warrant may be issued for any of the following:

(1) evidence of a crime;

(2) contraband, fruits of crime, or other items illegally possessed;

(3) property designed for use, intended for use, or used in committing a crime; or

(4) a person to be arrested or a person who is unlawfully restrained.

ในกรณีของการมีคำร้องขอออกหมายเพื่อทำการค้นสถานที่หรือยึดสิ่งของต่อศาลนั้น เจ้าหน้าที่ตำรวจหรือพนักงานอัยการจะต้องแสดงเหตุแห่งการค้นให้ศาลพิจารณาประกอบการตัดสินใจในการออกหมาย ซึ่งเหตุดังกล่าวอาจประกอบไปด้วย รายละเอียดของการกระทำความผิดอาญาที่เกิดขึ้นหรือกำลังจะเกิดขึ้น รายละเอียดของสถานที่ที่ต้องการตรวจค้น รายละเอียดของสิ่งของที่ต้องการยึด รายละเอียดของผู้ต้องสงสัยหรือบุคคลที่เกี่ยวข้อง เป็นต้น

ส่วนการขอออกหมายค้นสำหรับการค้นคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ต่าง ๆ มีหลักเกณฑ์ในการขอออกหมายค้นเช่นเดียวกับกรณีของการขอออกหมายค้นทั่วไป โดยเจ้าหน้าที่ตำรวจหรือพนักงานอัยการจะต้องระบุรายละเอียดเกี่ยวกับสิ่งที่ต้องการค้นหรือยึด โดยจะต้องระบุรายละเอียดต่าง ๆ เช่นเดียวกับการขอหมายค้นหรือยึดในกรณีทั่วไป ไม่ว่าจะเป็นรายละเอียดของการกระทำความผิดอาญาที่เกิดขึ้นหรือกำลังจะเกิดขึ้น รายละเอียดของสถานที่ที่ต้องการตรวจค้น รายละเอียดของสิ่งของที่ต้องการยึด รายละเอียดของผู้ต้องสงสัยหรือบุคคลที่เกี่ยวข้อง เป็นต้น และจะต้องระบุถึงอุปกรณ์อิเล็กทรอนิกส์ซึ่งสร้างหรือจัดเก็บข้อมูลอิเล็กทรอนิกส์นั้น ๆ อยู่ ไม่ว่าจะอยู่ในรูปแบบใด หรือเรียกว่าอะไร รวมไปถึงรูปแบบของคอมพิวเตอร์หรือที่จัดเก็บข้อมูลอิเล็กทรอนิกส์ (เช่น ฮาร์ดดิสก์ หรืออุปกรณ์ที่สามารถจัดเก็บข้อมูลดังกล่าวได้) รูปแบบใด ๆ ของการทำด้วยมือ (เช่น การเขียน วาดภาพ ระบายสี) รูปแบบใด ๆ ทางกลไก (เช่น การพิมพ์ หรือตีพิมพ์) และรูปแบบใด ๆ ของรูปถ่าย (เช่น ไมโครฟิล์ม ไมโครฟิช ภาพพิมพ์ สไลด์ ฟิล์มขาวดำ วิดีโอเทป ภาพถ่ายเคลื่อนไหว) เป็นต้น ซึ่งโดยทั่วไปศาลจะอนุญาตให้เจ้าหน้าที่รัฐทำการยึดอุปกรณ์คอมพิวเตอร์ได้ก็ต่อเมื่อเจ้าหน้าที่รัฐมีเหตุผลที่สมเหตุสมผลว่าคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ที่ต้องการทำการค้นหรือยึดนั้น อยู่ ณ สถานที่ หรืออยู่ในอุปกรณ์ดังกล่าวดังที่ได้อธิบายไว้ตามรายละเอียดในหมายจริง[109] ซึ่งสิ่งที่เจ้าหน้าที่รัฐต้องมุ่งเน้นในการอธิบายถึงก็คือข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บอยู่ในอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ มากกว่าตัวอุปกรณ์อิเล็กทรอนิกส์ เพราะสิ่งที่จะทำการยึดภายใต้หมายนั้นมักเป็นข้อมูลอิเล็กทรอนิกส์ในรูปแบบต่าง ๆ ซึ่งมีความเกี่ยวข้องกับการก่ออาชญากรรม

---

[109] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," ed. 3(Washington, D.C: Office of Legal Education Executive Office for United States Attorneys, 2552). หน้า 74

อย่างไรก็ตาม ในบางกรณีเจ้าหน้าที่ตำรวจหรือพนักงานอัยการอาจไม่ต้องระบุรายละเอียดดังที่กล่าวไปก็ได้ เพราะการที่ศาลจะออกหมายค้นหรือยึดให้นั้น ศาลจะพิจารณาโดยอาศัยสามัญสำนึกทั่วไป (Commonsensical) และรูปแบบในทางปฏิบัติ (Practical) มากกว่ารูปแบบทางเทคนิคที่มากเกินไป[110] โดยศาลสูงของประเทศสหรัฐอเมริกาได้วางหลักเกณฑ์ไว้ในคำพิพากษาหลายฉบับด้วยกัน เช่น เมื่อเจ้าหน้าที่รัฐไม่สามารถทราบรูปแบบที่แน่นอนของอุปกรณ์ซึ่งจัดเก็บข้อมูลไว้ก่อนที่จะทำการค้นหา การอธิบายในรูปแบบทั่วไปก็เป็นการเพียงพอที่ศาลจะออกหมายค้นหรือยึดให้ได้[111] แม้หมายจะอธิบายถึงสิ่งที่ต้องการยึดอย่างกว้าง ๆ หรืออธิบายไว้เพียงแต่ในรูปแบบทั่วไป โดยไม่เฉพาะเจาะจงก็สามารถบังคับใช้ได้ หากคำอธิบายดังกล่าวในหมายมีลักษณะที่เฉพาะเจาะจงในลักษณะและสถานการณ์เช่นนั้นภายใต้การสอบสวนของเจ้าหน้าที่ตำรวจ[112] คำอธิบายทั่วไปถึงอุปกรณ์คอมพิวเตอร์ที่จะทำการยึดก็เพียงพอแล้ว เพราะในทางปฏิบัตินั้นย่อมไม่สามารถที่จะระบุอย่างเฉพาะเจาะจงได้ว่าต้องการจะยึดฮาร์ดแวร์หรือซอฟต์แวร์อะไรเพื่อที่จะได้มาซึ่งรูปภาพอย่างแม่นยำว่ารูปภาพดังกล่าวบรรจุอยู่ในส่วนใดของฮาร์ดแวร์หรือซอฟต์แวร์[113] ในกรณีทั่วไปนั้นการขอหมายโดยระบุว่าต้องการยึดข้อมูลทั้งหมดนั้นไม่เพียงพอต่อการที่ศาลจะอนุมัติหมายค้นหรือยึดให้ แต่การขอไฟล์ที่เก็บไว้ทั้งหมดในบัญชีเครือข่ายของ AOL เพื่อทำการค้นหาบัญชีสื่อลามกอนาจารนั้นย่อมเพียงพอที่ศาลจะอนุมัติหมายค้นให้ได้ เพราะในทางปฏิบัติข้อมูลทั้งหมดจำเป็นที่จะต้องถูกตรวจสอบเพื่อพิจารณาว่าข้อมูลใดบ้างที่เป็นสื่อลามกอนาจาร[114] เป็นต้น

การตรวจสอบคอมพิวเตอร์เพื่อหาหลักฐานในการกระทำความผิดทางอาญาเป็นกระบวนการที่ใช้เวลานาน และถึงแม้ว่าเจ้าหน้าที่รัฐจะทราบข้อมูลที่เฉพาะเจาะจงเกี่ยวกับไฟล์ที่ต้องการค้นหา แต่ไฟล์ดังกล่าวอาจจะใส่ชื่อไว้ไม่ตรง อาจจะเข้ารหัสไว้ อาจเก็บไว้ในไฟล์ลับหรือซ่อนอยู่ใน slack space[115] ซึ่งทำให้ไฟล์ดังกล่าวไม่เป็นที่สะดุดตา และทำการตรวจสอบได้ยาก

---

[110] Ibid., หน้า 75 - 76.

[111] United States v. Ventresca, 380 U.S. 102, 108 (1965)

[112] United States v. Logan, 250 F.3d 350, 365 (6th Cir. 2001)

[113] United States v. Lacy, 119 F.3d 742, 746-47 (9th Cir. 1997)

[114] United States v. London, 66 F.3d 1227, 1238 (1st Cir. 1995)

[115] Slack space คือ พื้นที่ว่างส่วนที่เหลือของ cluster หลังจากใช้ในการเก็บข้อมูลแล้ว เช่น ในกรณีที่ต้องการเก็บไฟล์ที่มีขนาด 1200 bytes และกำหนดให้ระบบปฏิบัติการมีขนาด cluster เท่ากับ 2048 bytes (4 sectors) ไฟล์ที่เก็บจะกินพื้นที่ไป 1200 bytes และจะเหลือพื้นที่อีก 848 bytes ซึ่งปกกติแล้วระบบจะไม่นำไปใช้ในการเก็ยไฟล์อื่น พื้นที่ดังกล่าวเรียกว่า slack space ซึ่งเป็นพื้นที่ ๆ สามารถทำการซ่อนไฟล์ต่าง ๆ เพื่อไม่ให้เป็นที่สะดุดตา

ยิ่งไปกว่านั้น พยานหลักฐานของการก่ออาชญากรรมที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์นั้น ไม่ได้อยู่ในรูปแบบของไฟล์เสมอไป โดยอาจอยู่ในระบบปฏิบัติการที่ถูกสร้างขึ้นเป็นพิเศษ หรือพยานหลักฐานซึ่งเป็นข้อมูลอิเล็กทรอนิกส์นั้นอาจยากที่จะค้นหาหรือเรียกคืนหากไม่มีเครื่องมือที่เหมาะสมและระยะเวลาที่เหมาะสมในการดำเนินการ ซึ่งอาจใช้เวลาเป็นวันหรือสัปดาห์ในการหาข้อมูลที่เฉพาะเจาะจงเพื่ออธิบายในการขอหมาย เนื่องจากอุปกรณ์จัดเก็บข้อมูลของคอมพิวเตอร์มักจะบรรจุไปด้วยข้อมูลจำนวนมหาศาล[116]

นอกจากนี้การที่ต้องใช้ระยะเวลานานในการตรวจสอบคอมพิวเตอร์เพื่อหาพยานหลักฐานเกี่ยวกับการกระทำความผิดอาญา ยังส่งผลกระทบต่อการตรวจค้นคอมพิวเตอร์หรืออุปกรณ์เก็บข้อมูลในสถานที่ต่าง ๆ ด้วย เพราะเจ้าหน้าที่รัฐไม่สามารถคาดหมายได้ว่าจะต้องใช้ระยะเวลายาวนานเท่าใดในการดำเนินการ และในบางสถานการณ์การขอขยายระยะเวลาในการตรวจค้นอาจไม่มีเหตุผลเพียงพอ[117] ในคำพิพากษาของศาลสูงฉบับหนึ่งเกี่ยวกับการค้นเอกสารซึ่งเป็นกระดาษจำนวนมาก ตามธรรมเนียมปฏิบัติแล้วศาลจะอนุญาตให้เจ้าหน้าที่รัฐนำเอกสารดังกล่าวออกจากพื้นที่ตรวจค้นเพื่อนำไปตรวจสอบและพิจารณาว่าเอกสารใดบ้างที่อยู่ภายใต้ขอบเขตของหมาย[118] ด้วยเหตุผลเช่นเดียวกัน ศาลได้อนุญาตให้เจ้าหน้าที่รัฐสามารถที่จะนำคอมพิวเตอร์ออกจากสถานที่ซึ่งทำการตรวจค้นเพื่อทำการตรวจสอบได้[119] โดยศาลสูงได้มีคำพิพากษาเกี่ยวกับกรณีดังกล่าวไว้หลายฉบับด้วยกัน เช่น การยึดคอมพิวเตอร์ทั้งหมดนั้นสมเหตุสมผลเพราะคำให้การที่ว่า “เป็นธรรมแล้วที่นำทั้งระบบออกจากจุดตรวจค้น เพราะระยะเวลาและผู้เชี่ยวชาญในการควบคุมสภาพแวดล้อมนั้นจำเป็นสำหรับการวิเคราะห์ข้อมูลอย่างเหมาะสม”[120] เพราะปัญหาทางเทคนิคในการตรวจค้นคอมพิวเตอร์ในที่พักอาศัยของผู้ต้องสงสัย รวมไปถึงเนื้อหาของข้อมูลในคอมพิวเตอร์ จึงมีเหตุผลสมควรเพียงพอที่จะอนุญาตให้เจ้าหน้าที่ตำรวจเคลื่อนย้ายคอมพิวเตอร์ดังกล่าวเพื่อตรวจค้นไฟล์ที่เกี่ยวข้องกับการกระทำความผิดได้[121] เนื่องจากหมายนั้นจำกัดประเภทของเอกสารและบันทึกต่าง ๆ

---

[116] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 76 - 79

[117] United States v. Santarelli, 778 F.2d 609, 615-16 (11th Cir. 1985)

[118] United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997)

[119] United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999)

[120] United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000)

[121] Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001)

ที่จะทำการยึดได้ไว้อย่างชัดเจน จึงอนุญาตให้ยึดคอมพิวเตอร์ทั้งเครื่องเพื่อทำการตรวจสอบ[122] เป็นต้น และยิ่งไปกว่านั้น ในบางกรณีการพยายามจะทำการตรวจค้นสื่อบันทึกข้อมูล ณ สถานที่ทำการค้นอาจทำให้มีความเสี่ยงเพิ่มมากขึ้นที่จะก่อความเสียหายแก่พยานหลักฐานนั้น ดังนั้น แนวทางปฏิบัติที่ดีที่สุดสำหรับการตรวจค้นสื่อบันทึกข้อมูลนอกสถานที่ซึ่งผู้ตรวจสอบทางนิติวิทยาศาสตร์สามารถรับรองความสมบูรณ์ของข้อมูลได้จึงเป็นแนวทางที่สำคัญ[123]

นอกจากการตรวจค้นข้อมูลอิเล็กทรอนิกส์ในคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ซึ่งจัดเก็บข้อมูลอิเล็กทรอนิกส์ไว้แล้ว เจ้าหน้าที่ตำรวจหรือพนักงานอัยการอาจขอให้ศาลออกหมายจำนวนมากในการตรวจค้นแบบเครือข่ายก็ได้ ในกรณีที่มีเหตุผลอันควรเชื่อว่าการตรวจค้นแบบเครือข่ายจะทำให้สามารถดึงข้อมูลที่จัดเก็บไว้ในหลาย ๆ สถานที่ได้ โดยในกฎข้อ 41 (b) ของหลักเกณฑ์วิธีพิจารณาความอาญาของรัฐบาลกลาง (Federal Rules of Criminal Procedure) วางหลักไว้ว่า ผู้พิพากษา (Magistrate Judge) ในเขตอำนาจหนึ่งอาจออกหมายค้นสำหรับ “การค้นทรัพย์สิน.....ภายในเขตอำนาจ” หรือ “การค้นทรัพย์สิน.....นอกเขตอำนาจ หากทรัพย์สินนั้น.....อยู่ในเขตอำนาจขณะดำเนินการขอหมาย แต่อาจย้ายออกนอกเขตอำนาจก่อนที่หมายค้นจะมีผล”[124] โดยในกฎข้อ 41 ตอนหนึ่งได้ให้ความหมายของคำว่า “ทรัพย์สิน”[125] (Property) ว่า ทรัพย์สินหมายความรวมถึง “ข้อมูล” (Information) ด้วย และศาลฎีกาได้ถือว่าทรัพย์สินตามความในกฎข้อ 41 นั้น หมายความรวมถึงทรัพย์สินที่จับต้องไม่ได้ เช่น ข้อมูลคอมพิวเตอร์ด้วย[126] แม้ว่าศาลจะไม่ได้กล่าวถึงเรื่องดังกล่าวไว้โดยตรง แต่ข้อความที่ใช้ในกฎข้อ 41 ประกอบกับการตีความคำว่า “ทรัพย์สิน” ดังกล่าวของศาลฎีกา อาจจำกัดการค้นข้อมูลคอมพิวเตอร์ซึ่งอยู่ในเขตอำนาจซึ่งหมายค้นนั้นได้ถูกออก[127]

---

[122] United States v. Giberson, 527 F.3d 882, 886 (9th Cir. 2008)

[123] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 76 - 79

[124] Federal Rules of Criminal Procedure, Rule 41. (b)

[125] Federal Rules of Criminal Procedure, Rule 41. (a) (2) (A) “Property” includes documents, books, papers, any other tangible objects, and information.

[126] United States v. New York Tel. Co., 434 U.S. 159, 170 (1977)

[127] United States v. Walters, 558 F. Supp. 726, 730 (D.Md. 1980) (กล่าวถึงคำจำกัดในกรณีที่เกี่ยวข้องกับบันทึกทางโทรศัพท์)

ในกรณีที่คอมพิวเตอร์เครื่องหนึ่งเกี่ยวข้องกับอาชญากรรมหลายประเภท ฮาร์ดไดรฟ์ของคอมพิวเตอร์เครื่องดังกล่าวที่เจ้าหน้าที่รัฐทำการยึดมาเพื่อตรวจสอบเกี่ยวกับการกระทำความผิดหนึ่ง อาจมีพยานหลักฐานเกี่ยวกับการกระทำความผิดอื่น ๆ ก็เป็นได้ ซึ่งเจ้าหน้าที่รัฐมีอำนาจแค่เฉพาะการค้นหาพยานหลักฐานในการกระทำความผิดตามหมายดังกล่าวเท่านั้น ในกรณีเช่นนี้ เจ้าหน้าที่รัฐจะต้องขอหมายเพื่อค้นหรือยึดอีกฉบับสำหรับพยานหลักฐานที่พบในภายหลัง[128] เช่น ในกรณีที่พนักงานสอบสวนได้รับหมายในการค้นคอมพิวเตอร์ของจำเลยเพื่อหาบันทึกเกี่ยวกับการค้ายาเสพติด โดยในขณะที่พนักงานสอบสวนทำการตรวจค้นที่ ณ สถานีตำรวจ กลับพบรูปภาพลามกอนาจารของของเด็ก เมื่อพนักงานสอบสวนพบภาพดังกล่าวจึงทำการหยุดการค้นหาบันทึกเกี่ยวกับการค้ายาเสพติด และทำการค้นฮาร์ดไดรฟ์ทั้งหมดเพื่อหาภาพลามกอนาจารของเด็กแทน ในกรณีเช่นนี้ The Tenth Circuit จะระงับการค้นหาภาพลามกอนาจารของเด็ก เนื่องจากการค้นภาพลามากอนาจารของเด็กในภายหลังนั้นอยู่นอกเหนือขอบเขตของหมายที่พนักงานสอบสวนได้รับ[129] ในกรณีเช่นนี้พนักงานสอบสวนจะต้องทำการขอหมายค้นใหม่จากศาลในกรณีของการกระทำความผิดเกี่ยวกับสื่อลามกอนาจารของเด็กก่อนที่จะทำการค้นหาภาพดังกล่าวในฮาร์ดไดรฟ์ของจำเลย มิเช่นนั้นย่อมเป็นการดำเนินการที่ไม่ชอบด้วยกฎหมาย[130]

นอกจากรายละเอียดของสิ่งซึ่งต้องการจะทำการค้นและยึดตามหมายแล้ว ข้อ 41 (e) (2) (A)[131] ของหลักเกณฑ์วิธีพิจารณาความอาญาของรัฐบาลกลาง (Federal Rules of Criminal Procedure) ยังได้กำหนดในเรื่องเนื้อหาของหมายไว้เพิ่มเติมดังนี้

---

[128] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 90

[129] United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)

[130] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 90

[131] Federal Rules of Criminal Procedure, Rule 41. (e) (2) (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and

“หมายสำหรับการค้นและยึดบุคคลหรือทรัพย์สิน ยกเว้นกรณีของหมายสำหรับติดตามอุปกรณ์ หมายจะต้องระบุตัวบุคคลหรือทรัพย์สินที่จะทำการค้น จะต้องระบุตัวบุคคลหรือทรัพย์สินที่จะทำการยึด และกำหนดตัวผู้พิพากษาที่จะทำการส่งหมายคืน โดยหมายจะต้องมีคำสั่งให้เจ้าหน้าที่รัฐดำเนินการดังต่อไปนี้

(1) ดำเนินการตามหมายภายในระยะเวลาที่กำหนด โดยจะต้องไม่เกิน 14 วัน

(2) ดำเนินการตามหมายในช่วงเวลากลางวัน เว้นแต่ว่าผู้พิพากษาจะมีเหตุผลอันสมควรอนุญาตอย่างชัดแจ้งให้ดำเนินการในช่วงเวลาอื่นได้

(3) ดำเนินการส่งคืนหมายให้แก่ผู้พิพากษาที่ได้รับมอบหมายตามหมายดังกล่าว”

ซึ่งหมายภายใต้กฎข้อ 41 (e) (2) (A) อาจให้อำนาจในการยึดสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ ยึดหรือคัดลอกข้อมูลที่จัดเก็บด้วยระบบอิเล็กทรอนิกส์ หรืออื่น ๆ ตามที่หมายได้มีการระบุไว้ โดยหมายดังกล่าวนั้นอาจให้อำนาจแก่เจ้าหน้าที่รัฐในการตรวจสอบสื่อหรือข้อมูลในภายหลังเพื่อให้สอดคล้องกับรายละเอียดตามหมายได้ อย่างไรก็ตาม ระยะเวลาในการดำเนินการตามกฎข้อ 41 (e) (2) (A) และข้อ 41 (f) (1) (A)[132] นั้น หมายถึง ระยะเวลาในการยึดหรือคัดลอกสื่อหรือข้อมูล ณ สถานที่ทำการตรวจค้นเท่านั้น แต่ไม่ได้ระบุถึงระยะเวลาในการตรวจสอบสื่อหรือข้อมูลดังกล่าวในภายหลังนอกสถานที่ที่ทำการตรวจค้น ในกรณีนี้ศาลสูงเห็นว่าไม่มีบทบัญญัติข้อใดของรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 4 (The Fourth Amendment) หรือกฎข้อ 41 ที่ระบุอย่างชัดเจนถึงระยะเวลาในการวิเคราะห์ทางวิทยาศาสตร์ (Forensic Analysis) และศาลได้มีคำพิพากษาสนับสนุนถึงกรณีดังกล่าวว่า กระบวนการตรวจสอบทางวิทยาศาสตร์นั้นใช้เวลาหลายเดือนหลังจากที่

(iii) return the warrant to the magistrate judge designated in the warrant.

[132] Federal Rules of Criminal Procedure, Rule 41. (f) (1) (A) *Noting the Time.* The officer executing the warrant must enter on it the exact date and time it was executed.

ผู้ตรวจสอบได้รับคอมพิวเตอร์หรือข้อมูลจากการค้นและยึด[133] โดยจะเห็นได้จากคำพิพากษาของศาลสูง เช่น ล่าช้าเป็นระยะเวลา 10 เดือน[134] ล่าช้าเป็นระยะเวลา 6 สัปดาห์[135]

4.1.2.2 มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยไม่มีหมาย

การค้นโดยไม่มีหมายที่ล่วงล้ำความคาดหวังในความเป็นส่วนตัวจะต้องเป็นไปตามรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 4 (The Fourth Amendment)[136] โดยมีหลักเกณฑ์ที่เจ้าหน้าที่รัฐจะสามารถทำการค้นและยึดคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ เพื่อนำมาเป็นพยานหลักฐานประกอบการพิจารณาคดีหลายประการด้วยกัน สามารแบ่งออกเป็นข้อได้ดังต่อไปนี้

(1) การค้นและยึดโดยความยินยอม[137] เจ้าหน้าที่รัฐอาจค้นสถานที่หรือวัตถุโดยไม่ต้องมีหมายค้นหรือแม้กระทั่งเหตุอันควรเชื่อ (Probable Clause) หากผู้มีอำนาจยินยอมโดยสมัครใจที่จะให้ทำการค้น[138] โดยผู้มีอำนาจในการให้ความยินยอมอาจเป็นเจ้าของตามความเป็นจริงหรือตามที่ปรากฏ[139] การให้ความยินยอมนั้นอาจเป็นการให้ความยินยอมโดยชัดแจ้งหรือโดยปริยายก็ได้[140] สำหรับขอบเขตของความยินยอมในการค้นนั้น โดยทั่วไปแล้วจะกำหนดโดยความชัดแจ้งของวัตถุประสงค์และจำกัดด้วยขอบเขตของความยินยอมที่ได้ให้ไว้[141] โดยมาตรฐานในการวัดขอบเขตของความยินยอมภายใต้รัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 4 (The Fourth Amendment) คือความสมเหตุสมผลตามวัตถุประสงค์ ซึ่งจำเป็นต้องมีการพิจารณาข้อเท็จจริงอย่างละเอียดว่ามีเหตุผลเพียงพอที่เจ้าหน้าที่รัฐจะเชื่อว่าขอบเขตของความยินยอมนั้นครอบคลุมถึงวัตถุที่ต้องการทำการค้น

---

[133] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 91 - 92

[134] United States v. Burns, 2008 WL 4542990, at *8-9 (N.D. Ill. Apr. 29, 2008), United States v. Gorrell, 360 F. Supp. 2d 48,55 n.5 (D.D.C. 2004)

[135] United States v. Hernandez, 183 F. 3d 468, 480 (D.P.R. 2002)

[136] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 15

[137] Ibid., หน้า 15 - 27.

[138] Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973)

[139] See United States v. Buckner, 473 F.3d 551, 555 (4th Cir. 2007).

[140] United States v. MilianRodriguez, 759 F.2d 1558, 1563-64 (11th Cir. 1985)

[141] United States v. Pena, 143 F.3d 1363, 1368 (10th Cir. 1998

หรือไม่[142] หากมีการกำหนดขอบเขตของความยินยอมไว้อย่างชัดแจ้งก่อนหรือระหว่างการค้น เจ้าหน้าที่รัฐจะต้องเคารพขอบเขตตามความยินยอมดังกล่าว[143]

(2) การค้นและยึดในสถานการณ์เร่งด่วน ซึ่งสถานการณ์เร่งด่วนนั้นเป็นข้อยกเว้นของการค้นโดยมีหมาย เจ้าหน้าที่รัฐจึงสามารถค้นและยึดโดยไม่มีหมายได้ในกรณีที่ถือว่าเป็นสถานการณ์เร่งด่วน โดยทั่วไปแล้ว เจ้าหน้าที่รัฐจะกระทำการค้นและยึดได้เมื่อมีสถานการณ์อย่างใดอย่างหนึ่งต่อไปนี้ คือ[144]

(2.1) พยานหลักฐานนั้นอยู่ในอันตรายที่ใกล้จะถึงจากการถูกทำลาย

(2.2) ประชาชนตกอยู่ในอันตรายที่ใกล้จะถึง

(2.3) เจ้าหน้าที่ตำรวจซึ่งอยู่ในระหว่างการไล่ล่าผู้ต้องสงสัย

(2.4) ผู้ต้องสงสัยน่าจะหลบหนีไปได้ก่อนที่เจ้าหน้าที่รัฐจะขอหมายค้นได้

ในการพิจารณาว่ามีสถานการณ์เร่งด่วนที่จำเป็นจะต้องทำการค้นโดยไม่มีหมายหรือไม่นั้น เจ้าหน้าที่รัฐจะต้องพิจารณาถึงระดับความเร่งด่วนที่เกี่ยวข้อง ระยะเวลาที่จำเป็นในการดำเนินการขอหมาย พยานหลักฐานดังกล่าวจะถูกลบหรือทำลายหรือไม่ ความเป็นไปได้ที่จะเกิดอันตรายในสถานที่ที่มีพยานหลักฐานอยู่ สถานการณ์ที่ผู้ครอบครองสิ่งผิดกฎหมายรู้ถึงการตามล่าของเจ้าหน้าที่รัฐ และความพร้อมในการทำลายของผิดกฎหมาย

(3) การค้นในเหตุการณ์ที่ทำการจับกุมโดยชอบด้วยกฎหมาย ในการจับกุมโดยชอบด้วยกฎหมายนั้น เจ้าหน้าที่รัฐสามารถทำการค้น (Full Search) บุคคลผู้ถูกจับได้ และรวมไปถึงการค้นหาพื้นที่โดยรอบบุคคลผู้ถูกจับได้โดยไม่ต้องมีหมาย เช่น ในกรณีที่เจ้าหน้าที่ตำรวจทำการตรวจค้นสถานที่เกิดเหตุเพื่อจับกุมผู้กระทำความผิดเกี่ยวกับการจราจรได้พบซองบุหรี่ซึ่งมีลักษณะยับ

---

[142] Florida v. Jimeno, 500 U.S. 248, 251 (1991)

[143] Vaughn v. Baldwin, 950 F.2d 331, 333-34 (6th Cir. 1991)

[144] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 27 - 28

ยู่ยี่อยู่ในกระเป๋าเสื้อด้านซ้ายของผู้ต้องสงสัย เจ้าหน้าที่ตำรวจจึงเปิดซองบุหรี่ดังกล่าวโดยไม่ทราบว่าข้างในบรรจุสิ่งใดไว้ จึงทำให้พบเฮโรอีนจำนวน 40 แคปซูล ซึ่งศาลฎีกาถือว่าการตรวจค้นดังกล่าวนั้นได้รับอนุญาต แม้ว่าเจ้าหน้าที่ตำรวจจะไม่มีเหตุผลที่ชัดเจนในการตรวจค้นซองบุหรี่ดังกล่าวก็ตาม[145] สำหรับขอบเขตชั่วคราวที่อนุญาตสำหรับการค้นในเหตุการณ์ที่ทำการจับกุมแตกต่างกันไปตามวัตถุที่ทำการตรวจค้นว่าวัตถุดังกล่าวเป็นวัตุที่เกี่ยวข้องกับบุคคลผู้ถูกจับกุม ณ ขณะทำการจับกุมหรือไม่ เช่น เสื้อผ้า กระเป๋าสตางค์ หรือทรัพย์สินส่วนตัวอื่น ๆ ที่อยู่ใกล้ตัวผู้ถูกจับกุม เช่น กระเป๋าเดินทาง[146] ในสองคดีของศาลฎีกาได้แสดงให้เห็นถึงความแตกต่างนี้ โดยในคดีแรกแสดงให้เห็นถึงความสำคัญของระยะเวลาที่อนุญาตให้ทำการค้นวัตถุที่เกี่ยวข้องในเหตุการณ์ที่ทำการจับกุม โดยจะต้องดำเนินการค้นทันที[147] ในทางกลับกัน ในคดีที่สอง ศาลเห็นว่าเจ้าหน้าที่รัฐไม่สามารถตรวจค้นตู้เก็บรองเท้าในเหตุการณ์ที่ทำการจับกุมได้ เนื่องจากเจ้าหน้าที่รัฐได้ทำการค้นตู้เก็บรองเท้าซึ่งอยู่ห่างจากสถานที่ทำการจับกุมภายหลังจากที่ทำการจับกุมเป็นเวลา 90 นาที[148]

การค้นในเหตุการณ์ที่ทำการจับกุม ซึ่งในอดีตได้เริ่มต้นจากการค้นวิทยุติดตามตัว (Pagers) และปัจจุบันได้ขยายไปยังการค้นโทรศัพท์มือถือ ศาลได้เห็นด้วยกับแนวทางทั่วไปว่าหลักการของการค้นในเหตุการณ์ที่ทำการจับกุมนำมาใช้กับอุปกรณ์พกพาอิเล็กทรอนิกส์ด้วย

ในหลาย ๆ กรณีในช่วงทศวรรษที่ผ่านมาได้อนุมัติการค้นวิทยุติดตามตัวในเหตุการณ์ที่ทำการจับกุมไม่ว่าจะเป็นในคดี United States v. Brookes, 2005 WL 1940124, at *3 (D.V.I. Jun. 16, 2005), คดี Yu v. United States, 1997 WL 423070, at *2 (S.D.N.Y. Jul. 29, 1997), คดี United States v. Thomas, 114 F.3d 403, 404 n.2 (3d Cir. 1997) (dicta), คดี United States v. Reyes, 922 F. Supp. 818, 833 (S.D.N.Y. 1996), คดี United States v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995), คดี United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993) หรือ คดี United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996) และยิ่งไปกว่านั้นในช่วงระยะเวลาที่ผ่านมาไม่นาน ในหลาย ๆ คำพิพากษาของศาลได้สนับสนุนการค้นโทรศัพท์มือถือในเหตุการณ์ที่ทำการจับกุมเช่นเดียวกัน ไม่ว่าจะเป็นในคดี United States v. Finley,

---

[145] United States v. Robinson, 414 U.S. 218, 235 (1973)

[146] United States v. Chadwick, 433 U.S. 1, 15 (1977)

[147] United States v. Edwards, 415 U.S. 800, 808-09 (1974)

[148] United States v. Chadwick, 433 U.S. 1, 15 (1977)

477 F.3d 250, 259-60 (5th Cir. 2007), คดี United States v. Valdez, 2008 WL 360548, at *2-4 (E.D. Wis. Feb. 8, 2008), คดี United States v. Curry, 2008 WL 219966, at *10 (D. Me. Jan. 23, 2008), คดี United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1278-79 (D. Kan. 2007), คดี United States v. Dennis, 2007 WL 3400500, at *7-8 (E.D. Ky. Nov. 13, 2007), คดี United States v. Mendoza, 421 F.3d 663, 666-68 (8th Cir. 2005), คดี United States v. Brookes, 2005 WL 1940124, at *3 (D.V.I. Jun. 16, 2005) หรือ คดี United States v. Cote, 2005 WL 1323343, at *6 (N.D. Ill. May 26, 2005) นอกจากนี้ศาลอุทธรณ์ในคดีหนึ่งได้อนุมัติการตรวจค้นสมุดรายชื่ออิเล็กทรอนิกส์ในเหตุการณ์ที่ทำการจับกุมในคดี United States v. Goree, 2002 WL 31050979, at *5-6 (6th Cir. Sept. 12, 2002) ด้วยเช่นกัน[149]

อย่างไรก็ตาม ศาลไม่เห็นด้วยว่าการค้นโทรศัพท์มือถือในเหตุการณ์ที่ทำการจับกุมนั้นเหมือนกับในกรณีของการค้นตู้เก็บรองเท้าในคดี United States v. Chadwick หรือการค้นทรัพย์สินส่วนบุคคลในคดี United States v. Edwards มีเพียงศาลอุทธรณ์ในคดีเดียวเท่านั้นที่พิจารณาว่าปัญหาที่ถือได้ว่าโทรศัพท์มือถือที่พบในทันทีของบุคคลซึ่งเป็นจำเลยถือเป็นทรัพย์สินส่วนบุคคลที่เกี่ยวข้องกับบุคคลผู้ถูกจับ ดังจะเห็นได้จาก คดี United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007), คดี United States v. Wurie, 2009 WL 1176946, at *5 (D. Mass. 2009), คดี United States v. Brookes, 2005 WL 1940124, at *3 (D.V.I. Jun. 16, 2005) หรือ คดี United States v. Cote, 2005 WL 1323343, at *6 (N.D. Ill. May 26,2005) อย่างไรก็ตาม ในสองคดีของศาลแขวงได้ทำการเปรียบเทียบในกรณีของโทรศัพท์มือถือกับคดีของการค้นตู้เก็บรองเท้าในคดี United States v. Chadwick และได้ถือว่าการค้นหาโทรศัพท์มือถือไม่ได้เกิดขึ้นพร้อมกับรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 4 โดยในคดี United States v. Lasalle, 2007 WL 1390820, at *7 (D. Haw. May 9, 2007) ได้ปฏิเสธการค้นโทรศัพท์มือถือที่เกิดขึ้นภายหลังการจับกุมนานจำเลยกว่าสองชั่วโมง ในคดี United States v. Park, 2007 WL 1521573, at *5-9 (N.D. Cal. May 23, 2007) ได้ปฏิเสธการค้นโทรศัพท์มือถือที่เกิดขึ้นภายหลังการจับกุมจำเลยนานกว่า 90 นาที และในคดี United States v. Wall, 2008 WL 5381412, at *3-4 (S.D. Fla. Dec.

[149] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 31 - 32

22, 2008) การค้นโทรศัพท์มือถือที่สถานีตำรวจภายหลังการจับกุมไม่สามารถพิสูจน์ได้ว่าเป็นการค้นในเหตุการณ์ที่ทำการจับกุม[150]

ในปัจจุบันศาลยังไม่ได้มีการระบุว่าสื่ออิเล็กทรอนิกส์ที่มีความจุขนาดใหญ่ เช่น คอมพิวเตอร์พกพาในปัจจุบันอาจถูกค้นในเหตุการณ์ที่ทำการจับกุม (แม้ว่าการตรวจสอบในช่วงระยะเวลาสั้น ๆ อาจทำได้ในบางกรณี โดยเฉพาะการตรวจสอบด้วยอุปกรณ์ทางวิทยาศาสตร์ที่ออกแบบมาสำหรับใช้ในการตรวจสอบในสถานที่เกิดเหตุ) การค้นโดยวิธีการทางวิทยาศาสตร์ที่สมบูรณ์ (Complete Forensic Search) จำเป็นต้องใช้ข้อมูลภายในคอมพิวเตอร์ โดยทำการคัดลอกแล้วจึงค้นหาโดยใช้เครื่องมือที่ออกแบบมาสำหรับการวิเคราะห์ทางวิทยาศาสตร์ (Forensic Analysis) และการค้นโดยวิธีการทางวิทยาศาสตร์ที่สมบูรณ์ดังกล่าวอาจไม่สามารถนำมาปรับใช้กับเหตุการณ์ดังเช่นในกรณีของคดี United States v. Chadwick ได้ อย่างไรก็ตามเจ้าหน้าที่รัฐอาจทำการยึดคอมพิวเตอร์พกพาดังกล่าวในการค้นในเหตุการณ์ที่ทำการจับกุม และภายหลังจากทำการยึดแล้วจึงทำการขอหมายค้นเพื่อทำการค้นอย่างละเอียดในภายหลัง[151] (นอกจากนี้ โทรศัพท์มือถือนั้นมีลักษณะที่คล้ายคลึงกับคอมพิวเตอร์มากขึ้นเรื่อย ๆ ในปัจจุบันจึงอาจรวมเข้าเป็นอุปกรณ์ประเภทเดียวกัน การค้นหาทางวิทยาศาสตร์ที่สมบูรณ์ของโทรศัพท์มือถืออาจเปิดเผยหลักฐานมากกว่าการค้นสั้น ๆ ในเหตุการณ์ที่ทำการจับกุม[152])

(4) หลักการเห็นได้โดยประจักษ์ (Plain View) พยานหลักฐานของอาชญากรรมที่เกิดขึ้นอาจถูกยึดได้โดยไม่ต้องมีหมายศาลภายใต้หลักการเห็นได้โดยประจักษ์ ซึ่งเป็นข้อยกเว้นในการค้นที่ต้องมีหมายศาล ในการอาศัยข้อยกเว้นดังกล่าวนี้ เจ้าหน้าที่รัฐต้องอยู่ในตำแหน่งหรือสถานที่ที่ชอบด้วยกฎหมายในการสังเกตและเข้าถึงพยานหลักฐาน และเบาะแสดังกล่าวจะต้องปรากฏอย่างชัดเจนในขณะนั้น[153] แม้ว่าบางครั้งเจ้าหน้าที่รัฐจะเข้ามาพร้อมเบาะแสบนหน้าจอคอมพิวเตอร์ แต่การปรับใช้หลักภายใต้การเห็นได้โดยประจักษ์ ส่วนใหญ่จะเกิดขึ้นเมื่อเจ้าหน้าที่รัฐตรวจสอบคอมพิวเตอร์ตามหมายค้นและค้นพบหลักฐานของอาชญากรรมแยกต่างหากซึ่งอยู่

---

[150] Ibid., หน้า 32 - 33.

[151] Ibid., หน้า 33 - 34.

[152] Wayne Jansen and Rick Ayers, Guidelines on Cell Phone Forensics (National Institute of Standards and Technology No. 800-101, 2007)

[153] Horton v. California, 496 U.S. 128, 136 (1990)

นอกเหนืออำนาจของหมายค้นเดิม เช่น ในคดี United States v. Wong, 334 F.3d 831, 838 (9th Cir. 2003) เจ้าหน้าที่รัฐได้ค้นพบสื่อลามกอนาจารเด็กในฮาร์ดไดรฟ์ขณะที่ทำการค้นหลักฐานของคดีฆาตกรรมในฮาร์ดไดรฟ์โดยชอบด้วยกฎหมาย

ภายใต้หลักการเห็นได้โดยประจักษ์กับคอมพิวเตอร์ส่วนใหญ่จะเกี่ยวข้องกับกรณีที่เจ้าหน้าที่รัฐพบภาพซึ่งไม่เหมาะสมในคอมพิวเตอร์ในขณะทำการตรวจค้น แต่ในบางสถานการณ์ ชื่อที่เกี่ยวข้องกับไฟล์โดยเฉพาะภาพลามากอนาจารเด็กสามารถใช้ในการกล่าวโทษได้เช่นกัน เช่น ในคดี Compare Commonwealth v. Hinds, 768 N.E.2d 1067, 1073 (Mass. 2002) ที่ปรากฏว่าเจ้าหน้าที่ได้ทำการค้นหาพยานหลักฐานโดยชอบด้วยกฎหมายในคดีข่มขืนสามารถทำการเปิดและยึดไฟล์ภาพที่มีชื่อไม่เหมาะสมในทางเพศได้ ซึ่งอยู่ภายใต้หลักการเห็นได้โดยประจักษ์และสามารถใช้ในการกล่าวโทษได้

สิ่งสำคัญของข้อยกเว้นภายใต้หลักการเห็นได้โดยประจักษ์ ไม่สามารถแสดงให้เห็นถึงการละเมิดความคาดหวังในความเป็นส่วนตัวที่สมเหตุสมผลได้ ข้อยกเว้นดังกล่าวอนุญาตในการยึดพยานหลักฐานที่เจ้าหน้าที่รัฐได้รับอนุญาตให้ตรวจสอบเท่านั้นตามรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 4 (The Fourth Amendment) ซึ่งหมายความว่าเจ้าหน้าที่รัฐไม่สามารถพึ่งพาข้อยกเว้นภายใต้หลักการเห็นได้โดยประจักษ์เพื่อแสดงให้เห็นถึงการเปิดภาชนะซึ่งถูกปิดที่ไม่ได้รับอนุญาตให้ทำการตรวจสอบ[154] โดยศาลมีข้อสรุปที่แตกต่างกันว่าไฟล์แต่ละไฟล์ที่ถูกเก็บไว้ในคอมพิวเตอร์นั้น ควรถือเป็นภาชนะปิดที่แยกต่างหากจากกัน ซึ่งความแตกต่างนี้มีส่วนสำคัญสำหรับขอบเขตของหลักการเห็นได้โดยประจักษ์ ซึ่งศาลส่วนใหญ่นั้นวิเคราะห์ว่าไฟล์คอมพิวเตอร์เป็นภาชนะที่จัดเก็บแยกต่างหากจากกัน[155] เมื่อแต่ละไฟล์ถือว่าเป็นภาชนะปิดที่แยกจากกัน เจ้าหน้าที่รัฐจึงไม่สามารถอาศัยหลักการเห็นได้โดยประจักษ์ เพื่อเปิดไฟล์อื่นบนคอมพิวเตอร์ อย่างไรก็ตาม คำพิพากษาของ Fifth Circuit ในคดี United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2001) และคดี United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002), vacated on other grounds, 537 U.S. 802 (2002), aff'd, 359 F.3d 356, 358 (5th Cir. 2004) แนะนำให้หลักการเห็นได้โดยประจักษ์สำหรับไฟล์เดียวบนคอมพิวเตอร์ หรืออุปกรณ์จัดเก็บข้อมูลควรที่จะ

---

[154] United States v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996)

[155] Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001), United States v. Carey, 172 F.3d 1268, 1273-75 (10th Cir. 1999)

สามารถเป็นพื้นฐานสำหรับการค้นหาที่ครอบคลุมมากขึ้น ในสองกรณีข้างต้น ศาลถือว่าเมื่อได้มีการค้นส่วนหนึ่งของคอมพิวเตอร์หรืออุปกรณ์จัดเก็บข้อมูลโดยไม่มีหมายแล้ว จำเลยย่อมไม่ได้รับการสงวนไว้ซึ่งความคาดหวังในความเป็นส่วนตัวที่สมเหตุสมผล (Reasonable Expectation of Privacy) ในเนื้อหาที่เหลือของคอมพิวเตอร์หรืออุปกรณ์จัดเก็บข้อมูลได้อีกต่อไป[156] ดังนั้น การค้นคอมพิวเตอร์หรืออุปกรณ์จัดเก็บข้อมูลโดยผู้บังคับใช้กฎหมายจึงมีขอบเขตกว้างมากขึ้น โดยไม่ละเมิดต่อรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 4 (The Fourth Amendment) ซึ่งเหตุผลดังกล่าวนำไปใช้ในกรณีที่ไฟล์ถูกจัดวางไว้ในลักษณะที่เห็นได้โดยประจักษ์ด้วย[157]

(5) การค้นในสถานที่จัดเก็บ (Inventory searches) เจ้าหน้าที่รัฐซึ่งบังคับใช้กฎหมายจะทำการเก็บสิ่งของซึ่งยึดได้มาเป็นประจำ โดยการค้นสิ่งของดังกล่าวต่อไปนี้จะเรียกว่า “การค้นในสถานที่จัดเก็บ” การค้นในสถานที่จัดเก็บเหล่านี้ย่อมสมเหตุสมผลและอยู่ภายใต้ข้อยกเว้นของการค้นโดยไม่ต้องมีหมายศาล เมื่อเป็นไปตามเงื่อนไขสองประการด้วยกัน ได้แก่ ประการแรก การค้นต้องเป็นไปตามวัตถุประสงค์ที่ชอบด้วยกฎหมาย และไม่ใช่เพื่อวัตถุประสงค์ในการสอบสวน เช่น เพื่อปกป้องเจ้าของทรัพย์สินขณะถูกควบคุมตัว เพื่อประกันในกรณีของการอ้างสิทธิ์ในทรัพย์สินที่สูญหาย หรือเพื่อป้องกันเจ้าหน้าที่ตำรวจจากอันตราย เป็นต้น ซึ่งมีน้ำหนักมากกว่าการรุกล้ำสิทธิภายใต้รัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 4 (The Fourth Amendment)[158] ประการที่สอง การค้นต้องเป็นไปตามขั้นตอนที่เป็นมาตรฐาน[159]

(6) การค้นบริเวณชายแดน (Border Searches) เพื่อปกป้องความสามารถของรัฐบาลในการตรวจสอบสิ่งของผิดกฎหมายและทรัพย์สินอื่น ๆ ที่อาจเข้าหรือออกจากประเทศสหรัฐอเมริกาโดยผิดกฎหมาย ศาลฎีกาได้ยอมรับข้อยกเว้นพิเศษสำหรับการค้นหาที่เกิดขึ้น ณ บริเวณชายแดนของประเทศสหรัฐอเมริกาโดยไม่มีหมาย ตามที่ศาลได้มีการวางแนวทางไว้ การค้นตามปกติ ณ บริเวณชายแดนนั้นไม่จำเป็นต้องมีหมาย เหตุอันควรเชื่อ (Probable Cause) หรือแม้กระทั่งเหตุอันควรสงสัย (Reasonable Suspicion) ว่าการค้นอาจเปิดเผยถึงสิ่งของผิดกฎหมาย

---

[156] United States v. Slanina, 283 F.3d 670, 676-77 (5th Cir. 2002)

[157] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 35 - 36

[158] Illinois v. Lafayette, 462 U.S.640, 644 (1983), South Dakota v. Opperman, 428 U.S. 364, 369-70 (1976)

[159] Colorado v. Bertine, 479 U.S. 367, 374 n.6 (1987), Florida v. Wells, 495 U.S. 1, 4-5 (1990)

หรือพยานหลักฐาน[160] อย่างไรก็ตามสำหรับการค้นที่ล่วงล้ำโดยเฉพาะเจาะจงอย่างน้อยจะต้องมีเหตุอันควรสงสัย[161] กฎเหล่านี้นำมาใช้ต่อประชาชนและทรัพย์สินทั้งที่เข้าและออกจากประเทศสหรัฐอเมริกา[162]

คดีเกี่ยวกับการค้น ณ บริเวณชายแดนของศาลฎีกาแสดงให้เห็นว่าเหตุอันควรสงสัยไม่จำเป็นสำหรับการค้นทรัพย์สิน ณ บริเวณชายแดนโดยไม่ทำลายตัวทรัพย์สินนั้น นอกจากนี้ศาลยังพิจารณาว่า การค้นถังเชื้อเพลิงของรถยนต์บริเวณชายแดนไม่ต้องการเหตุอันควรสงสัยเช่นเดียวกัน โดยศาลได้ให้เหตุผลไว้ว่า “เหตุผลที่อาจสนับสนุนความสงสัยระดับหนึ่งในกรณีของการค้นหาบุคคลที่ล่วงล้ำอย่างมาก เช่น ศักดิ์ศรีและผลประโยชน์ในความเป็นส่วนตัวของบุคคลที่ถูกค้นนั้น ไม่นำไปใช้กับยานพาหนะ”[163] แม้ว่าผลประโยชน์ในความเป็นส่วนตัวในถังน้ำมันจะน้อยกว่าในทรัพย์สินอื่น ๆ เช่น คอมพิวเตอร์ ซึ่งศาลได้วิเคราะห์ไว้ในคดีข้างต้นนั้น ไม่ได้จำกัดอยู่แค่เฉพาะถังน้ำมันหรือยานพาหนะเท่านั้น เพื่อตอบสนองต่อข้อโต้แย้งของจำเลยที่กล่าวอ้างว่ารัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 4 (The Fourth Amendment) ปกป้องทรัพย์สินมากเท่ากับความเป็นส่วนตัว ศาลให้ความสำคัญกับการที่ถังน้ำมันนั้นไม่ได้รับความเสียหายทางกายภาพ และสรุปว่า “เป็นความจริงที่ว่าในขณะที่ทำการค้นบางครั้งทรัพย์ได้รับความเสียหายมากจนต้องการผลลัพธ์ที่แตกต่างจากเดิม ซึ่งในกรณีนี้ไม่ใช่หนึ่งในนั้น” ศาลอุทธรณ์ในคำพิพากษาคดี United States v. Camacho, 368 F.3d 1182, 1183 (9th Cir. 2004) ได้ตั้งข้อสังเกตว่า “ศาลฎีกาได้ทำให้เห็นชัดเจนแล้วว่าเจ้าหน้าที่รัฐไม่จำต้องมีเหตุอันควรสงสัยในการค้นทรัพย์สิน ณ บริเวณชายแดนโดยไม่ทำให้เกิดความเสียหายแก่ตัวทรัพย์สินนั้น”[164]

นับตั้งแต่คดี United States v. Flores-Montano เป็นต้นมา ศาลได้ยึดถือการค้นคอมพิวเตอร์ ณ บริเวณชายแดนโดยไม่จำต้องมีเหตุอันควรสงสัย (Reasonable Suspicion) ในการค้น ในคดี United States v. Arnold, 523 F.3d 941, 946 (9th Cir. 2008)

---

[160] United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985)

[161] Thornton v. United States, 541 U.S. 615, 632 (2004)

[162] UnitedStates v. Oriakhi, 57 F.3d 1290, 1297 (4th Cir. 1995)

[163] United States v. Flores-Montano, 541 U.S. 149 (2004)

[164] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 38

Ninth Circuit ถือว่า “เหตุอันควรสงสัยไม่เป็นสำหรับเจ้าหน้าที่ศุลกากรในการค้นคอมพิวเตอร์พกพาหรืออุปกรณ์จัดเก็บข้อมูลอิเล็กทรอนิกส์ส่วนบุคคลอื่น ๆ” ในการยึดถือแนวทางดังกล่าว ศาลในคดี United States v. Arnold ได้ปฏิเสธข้อโต้แย้งของจำเลยอย่างชัดเจน ซึ่งก่อนหน้านั้นได้ถูกรับรองโดยศาลแขวงว่า การค้นคอมพิวเตอร์พกพานั้นเป็นการล่วงล้ำมากกว่าการค้นทรัพย์สินทั่วไป เช่นเดียวกับการค้นที่พักอาศัยเนื่องจากมีความจุขนาดใหญ่ อย่างไรก็ตามศาลในคดี United States v. Arnold พบว่าไม่มีความแตกต่างตามเหตุผลระหว่างการค้นกระเป๋าเดินทางของนักเดินทาง ณ บริเวณชายแดนโดยไม่มีเหตุอันควรสงสัยและการค้นคอมพิวเตอร์พกพาบริเวณชายแดนโดยไม่มีเหตุอันควรสงสัย นอกจากนี้ยังได้มีคำพิพากษาที่สนับสนุนหลักการดังกล่าว ได้แก่ คดี United States v. Hampe, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007) ได้ปฏิเสธการวิเคราะห์ของศาลแขวงในคดี United States v. Arnold และถือว่าการค้นไฟล์คอมพิวเตอร์บริเวณชายแดนนั้นไม่ต้องอาศัย**เหตุอันควรสงสัยในการค้นแต่อย่างใด นอกจากนี้ในคดี** United States v. Ickes, 393 F.3d 501, 506-07 (4th Cir. 2005) the Fourth Circuit ยังอนุญาตให้มีการค้นคอมพิวเตอร์และดิสก์ภายในรถยนต์ของจำเลยภายใต้ข้อยกเว้นในการค้น ณ บริเวณชายแดน[165]

(7) การคุมประพฤติและการได้รับทัณฑ์บน บุคคลที่ถูกคุมประพฤติ ได้รับทัณฑ์บน หรือได้รับการปล่อยตัวภายใต้การดูแลย่อมได้รับความคาดหวังในความเป็นส่วนตัว (Expectation of Privacy) ที่น้อยลงจากบุคคลทั่วไป และอาจถูกค้นได้โดยไม่ต้องมีหมายขึ้นอยู่กับเหตุอันควรสงสัย (Reasonable Suspicion) หรือความเป็นไปได้โดยไม่ต้องมีความสงสัยโดยเฉพาะเจาะจง ในคดี United States v. Knights, 534 U.S. 112, 122 (2001) ศาลฎีกาได้พิจารณาความถูกต้องของการค้นที่อยู่อาศัยของผู้ถูกคุมประพฤติโดยไม่มีหมาย โดยอาศัยเพียงเหตุอันควรสงสัย ซึ่งเงื่อนไขของการคุมประพฤติกำหนดให้ผู้ถูกคุมประพฤติจะถูกส่งตัวไปเพื่อทำการค้นได้ตลอดเวลา โดยมีหรือไม่มีหมายหรือเหตุอันควรสงสัย ซึ่งศาลไม่ได้อาศัยการวิเคราะห์ความต้องการพิเศษ (Special Needs) ของคดี Griffin v. Wisconsin, 483 U.S. 868 (1987) การค้นในกรณีของการคุมประพฤติก่อนหน้านี้ศาลได้ใช้**รัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่** 4 (The Fourth Amendment) วิเคราะห์และพิจารณาพฤติการณ์แวดล้อมของการค้นทั้งหมด และศาลได้ตั้งข้อสังเกตว่าผู้ถูกคุมประพฤติได้รับความคาดหวังในความเป็นส่วนตัวที่ลดลง ซึ่งเป็นประโยชน์ต่อ

---

[165] Ibid., หน้า 38 - 40.

รัฐบาลในการป้องกันการกระทำความผิดซ้ำ และเพื่อให้ผู้ถูกคุมประพฤติสามารถกลับไปอาศัยอยู่ในสังคมได้ เนื่องจากรัฐบาลกังวลว่าผู้ถูกคุมประพฤติมีแนวโน้มที่จะกระทำผิด และปกปิดอาชญากรรมมากกว่าประชาชนทั่วไป เพื่อเป็นการสร้างสมดุลปัจจัยเหล่านี้ ศาลได้ยอมรับว่าการค้นในกรณีของการคุมประพฤติและการได้รับทัณฑ์บนนั้น ต้องการเพียงเหตุอันควรสงสัยก็เพียงพอที่เจ้าหน้าที่รัฐจะสามารถทำการค้นผู้ถูกคุมประพฤติได้[166]

ในคดี Samson v. California, 547 U.S. 843, 857 (2006)[167] ศาลฎีกาได้ขยายขอบเขตจากคดี United States v. Knights โดยถือว่ารัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 4 (The Fourth Amendment) นั้นไม่ได้ห้ามการค้นในกรณีของการได้รับทัณฑ์บนโดยปราศจากข้อสงสัย เช่นเดียวกับคดี United States v. Knights ศาลได้ใช้พฤติการณ์แวดล้อมทั้งหมดและพิจารณาข้อตกลงทัณฑ์บนว่าอนุญาตให้ทำการค้นโดยปราศจากข้อสงสัย ผลประโยชน์ของรัฐบาลในการกำกับดูแลผู้ได้รับทัณฑ์บน และเป้าหมายของรัฐบาลในการลดการกระทำความผิดซ้ำ อย่างไรก็ตาม ศาลในคดี Samson v. California ไม่ได้ทำให้ชัดเจนว่าแนวทางดังกล่าวขยายไปถึงผู้ถูกคุมประพฤติด้วยหรือไม่ และศาลตั้งข้อสังเกตว่าผู้ถูกทัณฑ์บนมีความคาดหวังในความเป็นส่วนตัวที่น้อยกว่าผู้ถูกคุมประพฤติ[168]

ตามแนวทางของคดี United States v. Knights และ คดี Samson v. California The Sixth Circuit ยึดถือแนวทางการค้นโดยไม่มีหมายสำหรับการค้นคอมพิวเตอร์ของผู้ถูกคุมประพฤติโดยอาศัยเหตุอันควรสงสัย (Reasonable Suspicion) ว่าผู้ถูกคุมประพฤติได้ฝ่าฝืนการคุมประพฤติโดยอาศัยอินเตอร์เน็ต โดยในคดี United States v. Herndon, 501 F.3d 683, 692 (6th Cir. 2007)[169] ได้มีคำพิพากษาส่วนหนึ่งว่า ในการคุมประพฤติสำหรับความผิดในการแสวงหาประโยชน์ทางเพศจากผู้เยาว์นั้น ผู้ถูกคุมประพฤติอยู่ภายใต้เงื่อนไขเฉพาะในการใช้อินเตอร์เน็ต และกำหนดให้ต้องอนุญาตให้เจ้าหน้าที่คุมประพฤติค้นคอมพิวเตอร์ได้ตลอดเวลาสำหรับการใช้อินเตอร์เน็ต ภายหลังจากที่ผู้ถูกคุมประพฤติแจ้งกับเจ้าหน้าที่คุมประพฤติว่าได้ใช้อินเตอร์เน็ตเพื่อหา

---

[166] Ibid., หน้า 40.

[167] Samson v. California, 547 U.S. 843, 857 (2006)

[168] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 40

[169] United States v. Herndon, 501 F.3d 683, 692 (6th Cir. 2007)

งาน เจ้าหน้าที่คุมประพฤติได้ไปที่บ้านพักของผู้ถูกคุมประพฤติ และได้ค้นคอมพิวเตอร์และฮาร์ดไดรฟ์พกพาจนพบกับภาพอนาจารเด็ก ซึ่งศาลได้ตัดสินว่าการค้นในคดี United States v. Herndon นั้นเป็นการค้นที่เหมาะสม เนื่องจากผู้ถูกคุมประพฤตินั้นย่อมมีความคาดหวังที่สมเหตุสมผลในความเป็นส่วนตัวที่ลดลงอย่างมาก ด้วยเงื่อนไขของการคุมประพฤติ และมีค่ามากกว่าสำหรับรัฐบาลในการป้องกันการกระทำความผิดซ้ำ The Sixth Circuit ได้สรุปว่า การตรวจค้นของเจ้าหน้าที่พิสูจน์หลักฐานเป็นไปอย่างเหมาะสม เพราะสำหรับการค้นดังกล่าวนั้นต้องการเพียงเหตุอันควรสงสัยเท่านั้น นอกจากนี้ได้มีคำพิพากษาในคดี United States v. Yuknavich, 419 F.3d 1302, 1311 (11th Cir. 2005)[170] ได้ยืนยันหลักการค้นคอมพิวเตอร์ผู้ถูกคุมประพฤติโดยไม่ต้องมีหมาย แม้ในกรณีที่ไม่มีเงื่อนไขที่ชัดเจนที่ผู้ถูกคุมประพฤติต้องส่งคอมพิวเตอร์ดังกล่าวไปทำการตรวจค้น[171]

4.2 ประเทศสิงคโปร์

ประเทศสิงคโปร์ได้เล็งเห็นถึงปัญหาภัยคุกคามไซเบอร์ที่อาจส่งผลกระทบต่อเศรษฐกิจและสังคม จึงได้เริ่มให้ความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยในปี ค.ศ. 2005 ได้จัดทำแผนแม่แบบด้านความมั่นคงปลอดภัยไซเบอร์ฉบับแรก คือ Infocomm Security Masterplan 2005 - 2007 เป็นแบบแผนในการประสานงานระหว่างภาครัฐและภาคเอกชนในการรับมือกับภัยคุกคามไซเบอร์ ต่อมาภายหลังได้มีการประกาศใช้แผนแม่แบบการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ฉบับที่ 2 และ 3 ในปี ค.ศ. 2008 และ ค.ศ. 2013 ตามลำดับ[172] ซึ่งในตลอดช่วงระยะเวลาหลายปี ประเทศสิงคโปร์ได้มีการพัฒนามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ในด้านต่าง ๆ ได้มีการจัดตั้งหน่วยงานเฉพาะขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น และได้มีการประกาศใช้กฎหมายความมั่นคงปลอดภัยไซเบอร์ ค.ศ. 2018 (Cybersecurity Act 2018) ในวันที่ 2 มีนาคม ค.ศ. 2018

---

[170] United States v. Yuknavich, 419 F.3d 1302, 1311 (11th Cir. 2005)

[171] Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." หน้า 41

[172] กัลยา ชินาธิวร, "ความสำเร็จของสิงคโปร์: กรณีศึกษาเพื่อประกอบการพัฒนาแนวทางการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย" (การฝึกอบรมหลักสูตรนักบริหารการทูต รุ่นที่ 11 ปี 2562, สถาบันการต่างประเทศเทวะวงศ์วโรปการ กระทรวงกาต่างประเทศ, 2562), หน้า 25 - 26.

4.2.1 มาตรการในการรักษาความปลอดภัยไซเบอร์

ในปี ค.ศ. 2018 ประเทศสิงคโปร์ได้มีการประกาศใช้กฎหมายความมั่นคงปลอดภัยไซเบอร์ ค.ศ. 2018 (Cybersecurity Act 2018) ซึ่งมีวัตถุประสงค์เพื่อกำหนดให้มีมาตรการป้องกัน จัดการ และตอบสนองต่อภัยคุกคามไซเบอร์ โดยได้มีการกำหนดมาตรการเชิงป้องกัน รับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์ทั้งก่อนเกิดและภายหลังจากเกิดภัยคุกคามทางไซเบอร์ขึ้นแล้ว กำหนดมาตรฐานทางเทคนิคให้ผู้ที่เกี่ยวข้องกับหน่วยงานโครงสร้างพื้นฐานสำคัญต้องปฏิบัติตาม รวมไปถึงให้อำนาจหน่วยงานที่จัดตั้งขึ้นในการดำเนินการเพื่อป้องกัน รับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์ กฎหมายความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศสิงคโปร์มีสาระสำคัญที่ใกล้เคียงกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศไทยเป็นอย่างมาก โดยได้มีการแบ่งระดับภัยคุกคามทางไซเบอร์ออกเป็น 3 ระดับด้วยกัน และได้ให้อำนาจแก่เจ้าหน้าที่รัฐในการเข้าถึงข้อมูลต่าง ๆ ตามมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ ซึ่งอำนาจในการเข้าถึงข้อมูลต่าง ๆ นี้แปรผันตรงกับระดับความร้ายแรงของภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นหรือเกิดขึ้น

เมื่อพิจารณาบทบัญญัติในหมวดที่ 4 ที่กล่าวถึงการตอบสนองต่อภัยคุกคามต่อการรักษาความปลอดภัยไซเบอร์ จะเห็นถึงแนวคิดและหลักการที่มีความคล้ายคลึงกับแนวคิดและหลักการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศไทยเป็นอย่างมาก โดยเฉพาะการบัญญัติให้อำนาจแก่เจ้าหน้าที่รัฐในการเข้าถึงข้อมูลต่าง ๆ ของประชาชน ทั้งบทบัญญัติที่มีลักษณะเป็นการขอความร่วมมือเพื่อขอข้อมูลที่จำเป็นจากประชาชน รวมไปถึงบทบัญญัติที่มีลักษณะเป็นการออกคำสั่งให้ประชาชนต้องปฏิบัติตาม แต่ก็มีหลักการและแนวคิดที่แตกต่างกันอยู่เช่นกัน โดยเฉพาะในเรื่องของการคุ้มครองบุคคล ซึ่งมีรายละเอียดที่สำคัญดังนี้

(1) ในกรณีของภัยคุกคามทางไซเบอร์ในระดับทั่วไป (Cybersecurity Incidents) ซึ่งอยู่ภายใต้บทบัญญัติมาตรา 19 ให้อำนาจแก่เจ้าหน้าที่รัฐในการเรียกบุคคลมาให้ข้อมูล[173] การมีหนังสือขอข้อมูลต่าง ๆ[174] เพื่อวัตถุประสงค์ในการสอบสวนเกี่ยวกับภัยคุกคามไซเบอร์ หากบุคคลที่ได้รับหนังสือดังกล่าวไม่ปฏิบัติตามข้อกำหนด เจ้าหน้าที่อาจรายงานเหตุดังกล่าวไปยังผู้พิพากษา (Magistrate) เพื่อออกคำสั่งให้บุคคลดังกล่าวปฏิบัติตามข้อกำหนดที่ได้รับเป็นลายลักษณ์อักษร

---

[173] Cybersecurity Act 2018, Section 19. (2) (a)

[174] Cybersecurity Act 2018, Section 19. (2) (b) และ (c)

ดังกล่าว[175] และได้กำหนดข้อยกเว้นสำหรับบุคคลที่อยู่ภายใต้สิทธิ สิทธิพิเศษ การให้ความคุ้มครอง ภาระผูกพัน หรือข้อจำกัด ที่กำหนดไว้ภายใต้บทบัญญัติของกฎหมาย สัญญา หรือกฎเกณฑ์ในการประกอบวิชาชีพไว้เช่นเดียวกันว่าไม่จำเป็นต้องเปิดเผยข้อมูลใด ๆ เว้นแต่กรณีที่สิทธิต่าง ๆ ดังกล่าวข้างต้นไม่สามารถอ้างในการไม่เปิดเผยข้อมูลได้ กรณีเช่นนี้ก็จำต้องเปิดเผยข้อมูลตามข้อกำหนดในหนังสือให้แก่กรรมาธิการหรือเจ้าหน้าที่รัฐซึ่งได้รับมอบหมายทราบ โดยบุคคลที่ถูกสอบสวนตามมาตรานี้ หากเปิดเผยข้อมูลโดยสุจริตและมีความระมัดระวังตามสมควร ไม่ถือว่าเป็นการผิดต่อภาระผูกพันต่าง ๆ ตามที่กล่าวถึงข้างต้น[176]

(2) กรณีของภัยคุกคามไซเบอร์ในระดับร้ายแรง (Serious Cybersecurity Incidents) นอกจากให้อำนาจแก่เจ้าหน้าที่รัฐในการเรียกบุคคลมาให้ข้อมูล และการมีหนังสือขอข้อมูลแล้ว ยังมีอำนาจในการเข้าถึง ตรวจสอบการทำงานของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์เพื่อค้นหาข้อมูลใด ๆ ได้[177] สามารถทำสำเนา ดึงข้อมูล[178] ทำการสแกนคอมพิวเตอร์หรือระบบคอมพิวเตอร์[179] รวมไปถึงการเข้าไปตรวจสอบสถานที่ใด ๆ โดยมีหนังสือบอกกล่าวเป็นลายลักษณ์อักษรตามสมควรแก่ผู้เป็นเจ้าของ หรือผู้ครอบครองสถานที่ใด ๆ เพื่อเข้าไปในสถานที่ดังกล่าว[180] นอกจากนี้ยังมีอำนาจในการยึดคอมพิวเตอร์ใด ๆ หรืออุปกรณ์อื่น ๆ เพื่อวัตถุประสงค์การตรวจสอบหรือวิเคราะห์เพิ่มเติมในอนาคต[181] โดยในการยึดนั้นจะต้องได้รับความยินยอมจากผู้เป็นเจ้าของก่อนถึงจะทำการยึดได้ อย่างไรก็ตาม ในกรณีที่ผู้เป็นเจ้าของไม่ยินยอมให้ทำการยึด หากกรรมาธิการเห็นว่าการใช้อำนาจเป็นสิ่งจำเป็นสำหรับการสอบสวน ไม่มีวิธีการที่เป็นการรบกวนน้อยกว่าเพื่อให้บรรลุวัตถุประสงค์ของการสอบสวน และภายหลังจากปรึกษากับผู้เป็นเจ้าของและคำนึงถึงความสำคัญของคอมพิวเตอร์หรืออุปกรณ์อื่น ๆ ที่มีต่อธุรกิจหรือการดำเนินงานของผู้เป็นเจ้าของ ประโยชน์จากการใช้อำนาจนั้นมีมากกว่าความเสียหายที่จะกระทบต่อผู้เป็นเจ้าของ และกรรมาธิการได้มีหนังสืออนุญาตให้ทำการยึดเป็นลายลักษณ์อักษร เจ้าหน้าที่รัฐย่อสามารถทำการยึดคอมพิวเตอร์ใด ๆ หรืออุปกรณ์

---

[175] Cybersecurity Act 2018, Section 19. (5)

[176] Cybersecurity Act 2018, Section 19. (6)

[177] Cybersecurity Act 2018, Section 20. (2) (c)

[178] Cybersecurity Act 2018, Section 20. (2) (g)

[179] Cybersecurity Act 2018, Section 20. (2) (f)

[180] Cybersecurity Act 2018, Section 20. (2) (d)

[181] Cybersecurity Act 2018, Section 20. (2) (h)

อื่น ๆ เพื่อการตรวจสอบหรือวิเคราะห์เพิ่มเติมได้ โดยภายหลังจากที่เสร็จสิ้นการตรวจสอบหรือวิเคราะห์เพิ่มเติมคอมพิวเตอร์หรืออุปกรณ์อื่น ๆ แล้ว จะต้องดำเนินการส่งคืนคอมพิวเตอร์ หรืออุปกรณ์อื่น ๆ ให้แก่ผู้เป็นเจ้าของทันที[182]

(3) กรณีของภัยคุกคามไซเบอร์ในระดับฉุกเฉิน (Emergency Cybersecurity Measures and Requirement) ได้ให้อำนาจแก่เจ้าหน้าที่รัฐในการใช้มาตรการใด ๆ ที่เห็นว่าจำเป็นและเหมาะสมได้ทั้งสิ้น[183] มีการบัญญัติคุ้มครองผู้เปิดเผยข้อมูลไว้[184] ซึ่งบุคคลที่ได้ให้ข้อมูลแก่เจ้าหน้าที่รัฐตามมาตรการ และข้อกำหนดด้านความปลอดภัยไซเบอร์ในกรณีฉุกเฉินโดยสุจริต ไม่ถือว่ากระทำความผิดหรือฝ่าฝืนข้อกำหนดตามกฎหมาย สัญญา หรือมาตรฐานทางวิชาชีพนั้น ๆ[185] นอกจากนี้ยังได้มีการกำหนดการคุ้มครองข้อมูลที่อาจนำไปพยานหลักฐานในกระบวนการดำเนินคดีทางแพ่งหรือทางอาญา[186] กล่าวคือ ในกรณีที่ความผิดใดถูกเปิดเผยระหว่างหรือจากการใช้มาตราการต่าง ๆ ภายใต้มาตรานี้ โดยระบุว่า ข้อมูลใด ๆ ที่ได้จากมาตรการภายใต้มาตรการเกี่ยวกับภัยคุกคามทางไซเบอร์ในระดับฉุกเฉินนี้ ไม่สามารถใช้เป็นพยานหลักฐานในการดำเนินคดีแพ่งหรือคดีอาญาใด ๆ ได้ และพยานในคดีแพ่งหรือคดีอาญาไม่มีหน้าที่ในการเปิดเผยชื่อ ที่อยู่ หรือรายละเอียดอื่น ๆ ของผู้แจ้งข้อมูล หรือเพื่อตอบคำถามใด ๆ ที่คำตอบจะนำไปสู่ หรืออาจนำไปสู่การค้นพบชื่อ ที่อยู่ หรือรายละเอียดอื่น ๆ ของผู้ให้ข้อมูล หากหนังสือ เอกสาร ข้อมูล หรือผลผลิตจากคอมพิวเตอร์ใด ถูกยอมรับเป็นหลักฐาน หรือความรับผิดต่อการสอบสวนในการดำเนินคดีแพ่งหรือคดีอาญาประกอบด้วยรายการใด ๆ ซึ่งมีการระบุชื่อ หรือรูปพรรณของผู้ให้ข้อมูล หรืออาจนำไปสู่การค้นพบผู้ให้ข้อมูล ศาลต้องทำให้รายการเหล่านั้นถูกปกปิดจากจากถูกพบ หรือทำการลบเท่าที่จำเป็นเพื่อปกป้องผู้ให้ข้อมูลจากการถูกค้นพบ[187]

เมื่อพิจารณาบทบัญญัติของประเทศสิงคโปร์จะเห็นได้ว่าแม้จะให้อำนาจแก่เจ้าหน้าที่ในการเข้าถึงข้อมูลต่าง ๆ ของประชาชนได้ แต่ก็ได้กำหนดหลักเกณฑ์ในการคุ้มครองผู้ให้

---

[182] Cybersecurity Act 2018, Section 20. (5)

[183] Cybersecurity Act 2018, Section 23. (2)

[184] Cybersecurity Act 2018, Section 23. (7)

[185] อนัญพร สกุลเมฆา, "การตรวจสอบและถ่วงดุลอำนาจเจ้าพนักงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562," หน้า 31.

[186] Ibid., หน้า 32.

[187] Cybersecurity Act 2018, Section 23. (10)

ข้อมูลว่าจะไม่มีความผิดในกรณีต่าง ๆ โดยเฉพาะในกรณีของมาตรการและข้อกำหนดด้านความปลอดภัยไซเบอร์ในกรณีฉุกเฉินที่ให้อำนาจแก่เจ้าหน้าที่ในการใช้มาตรการใด ๆ ที่เห็นว่าจำเป็นและเหมาะสมได้ทั้งสิ้น ซึ่งได้กำหนดคุ้มครองว่าในกรณีที่ข้อมูลที่ได้มานั้นเป็นการเปิดเผยการกระทำความผิดใด ๆ จะไม่สามารถนำมาใช้เป็นพยานหลักฐานในการดำเนินคดีแพ่งหรือคดีอาญาใด ๆ ได้ ซึ่งถือได้ว่าเป็นการจำกัดขอบเขตการใช้อำนาจของเจ้าหน้าที่รัฐลง โดยให้อำนาจต่าง ๆ ตามกฎหมายฉบับนี้เป็นไปเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เท่านั้น

4.2.2 มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์

มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศสิงคโปร์ถูกวางหลักไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศสิงคโปร์ (Criminal Procedure Code 2010) มีรายละเอียดที่สำคัญ ดังนี้

ในการแสวงหาพยานหลักฐานต่าง ๆ หากเจ้าหน้าที่ตำรวจเห็นว่าเอกสารหรือสิ่งใด ๆ จำเป็น (Necessary) หรือน่าพึงพอใจ (Desirable) สำหรับการสอบสวน การพิจารณา หรือการดำเนินการใด ๆ ตามประมวลกฎหมายวิธีพิจารณาความอาญานี้ เจ้าหน้าที่ตำรวจอาจออกคำสั่งเป็นหนังสือให้บุคคลซึ่งครอบครอง หรือมีอำนาจในเอกสารหรือสิ่งใดจัดทำเอกสารหรือส่งสิ่งดังกล่าวให้แก่เจ้าหน้าที่ตำรวจ หรือให้อำนาจแก่เจ้าหน้าที่ตำรวจในการเข้าถึงข้อมูลเหล่านั้น[188] หากเอกสารหรือสิ่งเหล่านั้นถูกจัดเก็บอยู่ในคอมพิวเตอร์หรือเข้าถึงได้โดยอาศัยคอมพิวเตอร์เท่านั้น เจ้าหน้าที่ตำรวจอาจออกคำสั่งเป็นหนังสือเพื่อใช้อำนาจเช่นเดียวกันได้[189] ศาลจะออกหมายค้นให้แก่เจ้าหน้าที่ตำรวจในกรณีที่บุคคลที่ได้รับคำสั่งเป็นหนังสือจากเจ้าหน้าที่ตำรวจไม่ปฏิบัติตามคำสั่ง หรือในกรณีที่ไม่ทราบว่าบุคคลใดเป็นผู้ครอบครองเอกสารหรือสิ่งเหล่านั้น หรืออาจออกหมายเรียกเพื่อให้บุคคลที่ได้รับคำสั่งมาตามหมายเรียก เป็นต้น[190] ในหมายค้นจะต้องระบุชื่อของเจ้าหน้าที่ผู้ดำเนินการตามหมายคนเดียวหรือหลายคนแล้วแต่กรณี ไม่ว่าจะเป็นเจ้าหน้าที่ตำรวจหรือบุคคลใดที่ศาลเห็นสมควร หากศาลเห็นว่าเหมาะสมอาจระบุสถานที่โดยเฉพาะเจาะจงสำหรับการค้นหา หรือตรวจสอบ และระบุบุคคลที่

---

[188] Criminal Procedure Code, when search warrant may be issued, Section 20. (1) (a)

[189] Criminal Procedure Code, when search warrant may be issued, Section 20. (1) (b)

[190] Criminal Procedure Code, when search warrant may be issued, Section 24.

ถูกตั้งข้อหาที่จะดำเนินการตามหมายเพื่อค้นหรือตรวจสอบในสถานที่เฉพาะเจาะจงดังกล่าว และศาลจะต้องกำหนดจำนวนวันที่หมายค้นดังกล่าวจะมีผลบังคับใช้[191]

นอกจากอำนาจในการค้นในกรณีต่าง ๆ ข้างต้นแล้ว ในการยึดนั้นก็ได้มีการวางหลักเกณฑ์ไว้ด้วยเช่นกัน โดยเจ้าหน้าที่ตำรวจอาจยึด ห้ามไม่ให้กำจัด หรือซื้อขายทรัพย์สินใด ๆ ในกรณีที่ทรัพย์สินดังกล่าวได้ใช้ในการกระทำความผิด ในกรณีที่สงสัยว่าจะใช้หรือมีการใช้ทรัพย์สินดังกล่าวในการกระทำความผิด หรือทรัพย์สินซึ่งต้องสงสัยว่าเป็นพยานหลักฐานในการกระทำความผิด[192] โดยเจ้าหน้าที่ตำรวจอาจใช้อำนาจตามมาตรานี้ โดยไม่ต้องคำนึงถึงบทบัญญัติในกฎหมายอื่นที่เกี่ยวข้องกับการยึดแต่อย่างใด[193] และเนื่องจากในมาตรานี้ไม่ได้มีการกล่าวถึงข้อกำหนดที่ให้เจ้าหน้าที่ตำรวจต้องยื่นคำร้องเพื่อขอหมายศาลก่อน จึงสามารถตีความได้ว่าเจ้าหน้าที่ตำรวจสามารถดำเนินการไปโดยใช้ดุลพินิจของตนเองได้โดยไม่ต้องขอหมายค้นจากศาลแต่อย่างใด

นอกจากการค้นสถานที่ ค้นตัวบุคคล และการยึดทรัพย์สินต่าง ๆ ดังที่ได้กล่าวไปข้างต้นแล้ว ประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศสิงคโปร์ยังได้บัญญัติถึงกรณีของอำนาจในการเข้าถึงคอมพิวเตอร์ไว้ในมาตรา 39 โดยเฉพาะด้วย โดยเจ้าหน้าที่ตำรวจหรือผู้มีอำนาจในการสอบสวนผู้กระทำความผิดซึ่งถูกจับอาจกระทำการดังต่อไปนี้ได้ตลอดเวลา[194]

(1) เข้าถึงและตรวจสอบ (ในหรือจากประเทศสิงคโปร์) การดำเนินการของคอมพิวเตอร์ (ไม่ว่าจะในหรือนอกประเทศสิงคโปร์) ที่เจ้าหน้าที่ตำรวจหรือผู้มีอำนาจมีเหตุอันสมควรที่จะสงสัยว่า (Reasonable Cause to Suspect) ว่าเป็นหรือถูกใช้ หรือประกอบด้วย หรือมีหลักฐานที่เกี่ยวข้องกับความผิดที่สามารถจับกุมได้

(2) ใช้คอมพิวเตอร์ดังกล่าวในหรือจากประเทศสิงคโปร์ หรือทำให้คอมพิวเตอร์ดังกล่าวใช้ในหรือจากประเทศสิงคโปร์เพื่อค้นหาข้อมูลใด ๆ ที่มีอยู่หรือพร้อมใช้งานในคอมพิวเตอร์ดังกล่าว และเพื่อทำสำเนาข้อมูลดังกล่าว

---

[191] Criminal Procedure Code, when search warrant may be issued, Section 26.

[192] Criminal Procedure Code, when search warrant may be issued, Section 35. (1)

[193] Criminal Procedure Code, when search warrant may be issued, Section 35. (4)

[194] Criminal Procedure Code, when search warrant may be issued, Section 39. (1)

(3) ป้องกันไม่ให้บุคคลอื่นเข้าถึงหรือใช้คอมพิวเตอร์ดังกล่าว (รวมถึงการเปลี่ยนชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลรับรองความถูกต้องอื่น ๆ ที่จำเป็นสำหรับการเข้าถึงคอมพิวเตอร์) หรือ

(4) สั่งบุคคลใด ๆ เพื่อหยุดการเข้าถึงหรือใช้ หรือการใช้งานใด ๆ ซึ่งคอมพิวเตอร์ดังกล่าว หรือเข้าถึงหรือใช้คอมพิวเตอร์เครื่องใด ๆ ภายใต้เงื่อนไขใด ๆ ซึ่งกำหนดโดยเจ้าหน้าที่ตำรวจหรือผู้มีอำนาจ

ในกรณีที่เจ้าหน้าที่ตำรวจมีเหตุอันควรสงสัย (Reasonable Suspicion) ว่าบุคคลใดใช้หรือได้ใช้คอมพิวเตอร์ที่เกี่ยวข้องกับความผิดที่เจ้าหน้าที่ตำรวจหรือเจ้าหน้าที่ผู้มีอำนาจได้ทำการจับกุม หรือบุคคลใด ๆ ที่รับผิดชอบหรือเกี่ยวข้องกับการทำงานของคอมพิวเตอร์ หรือบุคคลใดที่เจ้าหน้าที่ตำรวจหรือผู้มีอำนาจเชื่ออย่างมีเหตุผลว่ารู้หรือสามารถเข้าถึงชื่อผู้ใช้ รหัสผ่าน หรือการรับรองความถูกต้องอื่น ๆ ที่จำเป็นสำหรับการเข้าถึงคอมพิวเตอร์ดังกล่าวได้[195] บุคคลดังกล่าวจะต้องให้ความช่วยเหลือแก่เจ้าหน้าที่ตำรวจหรือบุคคลผู้มีอำนาจในการเข้าถึงคอมพิวเตอร์ และช่วยเหลือในการป้องกันไม่ให้บุคคลภายนอกเข้าถึงหรือใช้คอมพิวเตอร์ รวมไปถึงช่วยเหลือในการเปลี่ยนชื่อผู้ใช้ รหัสผ่าน หรือการรับรองความถูกต้องอื่น ๆ เท่าที่จำเป็นเพื่อเข้าถึงคอมพิวเตอร์ดังกล่าว[196]

4.3 เครือรัฐออสเตรเลีย รัฐควีนส์แลนด์

เครือรัฐออสเตรเลีย (Commonwealth of Australia) มีการปกครองในระบบสหพันธรัฐ (Federal Government) โครงสร้างการปกครองภายนอกประกอบด้วย รัฐบาลกลาง (the Commonwealth Government) หรือ รัฐบาลสหพันธรัฐ (the Federal Government) ซึ่งจัดทำภารกิจในระดับชาติ โครงสร้างการปกครองระดับรองลงมา คือ การปกครองระดับมลรัฐ ซึ่งมีอยู่ทั้งสิ้น 6 รัฐและ 2 ดินแดน แต่ละรัฐจะมีสภา ฝ่ายบริหาร ฝ่ายตุลาการ รวมถึงการมีรัฐธรรมนูญเป็นของตนเอง

4.3.1 มาตรการในการรักษาความปลอดภัยไซเบอร์

เมื่อวันที่ 6 สิงหาคม ค.ศ. 2020 รัฐบาลกลางของประเทศออสเตรเลียได้มีการประกาศยุทธศาสตร์ความปลอดภัยไซเบอร์ ค.ศ. 2020 (Australia's Cyber Security Strategy 2020) เพื่อให้โลกออนไลน์มีความปลอดภัยมากยิ่งขึ้นสำหรับประชาชนชาวออสเตรเลีย ธุรกิจของ

---

[195] Criminal Procedure Code, when search warrant may be issued, Section 39. (2)

[196] Criminal Procedure Code, when search warrant may be issued, Section 39. (2A)

ภาคเอกชน และการให้บริการที่จำเป็น โดยจะจัดให้มีการดำเนินการที่เป็นหลักการสำคัญดังต่อไปนี้[197]

(1) มีการดำเนินการโดยรัฐบาลกลางเพื่อเสริมสร้างการปกป้องประชาชนชาวออสเตรเลีย ธุรกิจของภาคเอกชน การให้บริการที่จำเป็นจากภัยคุกคามอันมีความสลับซับซ้อน

(2) มีการดำเนินการโดยภาคธุรกิจเพื่อรักษาความปลอดภัยต่อผลิตภัณฑ์และบริการและปกป้องผู้บริโภคจากช่องโหว่ทางไซเบอร์ที่ทราบถึงการมีอยู่ของช่องโหว่นั้น

(3) มีการดำเนินการโดยชุมชนเพื่อสร้างแนวปฏิบัติที่ปลอดภัยในพฤติกรรมทางออนไลน์ และการซื้ออย่างชาญฉลาดของผู้บริโภค

แม้ยุทธศาสตร์ความปลอดภัยไซเบอร์ ฯ จะเป็นความคิดริเริ่มของรัฐบาลกลางออสเตรเลีย แต่รัฐ รัฐบาลท้องถิ่น ตลอดจนภาคธุรกิจ สถาบันการศึกษา พันธมิตรระหว่างประเทศและชุมชน ล้วนแล้วแต่มีบทบาทที่สำคัญในการเสริมสร้างความปลอดภัยไซเบอร์ของประเทศออสเตรเลีย นอกจากนี้ตามที่ระบุไว้ในยุทธศาสตร์ความปลอดภัยไซเบอร์ ฯ รัฐบาลกลางออสเตรเลียมีพันธกิจที่จะต้องปกป้องบริการที่จำเป็นของประชาชนชาวออสเตรเลีย โดยการยกระดับความปลอดภัย และความยืดหยุ่นของโครงสร้างพื้นฐานที่สำคัญต่าง ๆ ได้มีการจัดตั้งคณะกรรมการที่ปรึกษาอุตสาหกรรมความปลอดภัยไซเบอร์ (The Cyber Security Industry Advisory Committee) เพื่อช่วยแนะนำการดำเนินการตามยุทธศาสตร์ และจะมีบทบาทอย่างต่อเนื่องในการกำหนดมาตรการในการดำเนินการทั้งระยะสั้นและระยะยาวภายใต้ยุทธศาสตร์ดังกล่าว[198]

4.3.2 มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์

เนื่องจากเครือรัฐออสเตรเลียมีรัฐบาลทำหน้าที่บริหารราชการแผ่นดิน 3 ระดับ ได้แก่ รัฐบาลระดับเครือรัฐหรือรัฐบาลกลาง รัฐบาลแห่งรัฐ และรัฐบาลท้องถิ่น ซึ่งรัฐในแต่ละรัฐของประเทศออสเตรเลียมีอธิปไตยเป็นของตนเอง ดังนั้นแต่ละรัฐจึงมีบทบัญญัติของกฎหมายที่แยกเป็นเอกเทศออกจากกัน โดยผู้เขียนจะทำการศึกษาในส่วนของมาตรการในการแสวงหาพยานหลักฐาน

---

[197] The Department of Home Affairs Australia Government, [Online] Accessed: 17/07/66. Updated: 27/02/66. Available from: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australias-cyber-security-strategy-2020

[198] Ibid.

อิเล็กทรอนิกส์ของรัฐควีนส์แลนด์ เครือรัฐออสเตรเลีย ซึ่งเป็นรัฐหนึ่งในเครือรัฐออสเตรเลีย โดยมีรายละเอียดที่สำคัญดังต่อไปนี้

รัฐควีนส์แลนด์ เครือรัฐออสเตรเลีย ได้มีการกำหนดมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยเฉพาะไว้ในพระราชบัญญัติอำนาจหน้าที่ของเจ้าหน้าที่ตำรวจ ค.ศ. 2020 (Police Powers and Responsibilities Act 2020) ซึ่งเป็นบทบัญญัติที่มีขึ้นเพื่อกำหนดอำนาจหน้าที่ และความรับผิดชอบของเจ้าหน้าที่ตำรวจของกรมตำรวจแห่งรัฐควีนส์แลนด์ (Queensland Police Service : QPS)

4.3.2.1 การค้นสถานที่โดยมีหมาย

การค้นสถานที่โดยมีหมายปรากฏอยู่ในบทที่ 7 ว่าด้วยการค้น การได้มาซึ่งเอกสาร การเข้าถึงภาพดิจิทัล หรือข้อมูลอื่น และสถานที่เกิดเหตุ (Chapter 7 - Search warrants, obtaining documents, accessing registered digital photos and other information, and crime scenes) ในกรณีของการแสวงหาพยานหลักฐานทั่วไปกำหนดว่าเจ้าหน้าที่ตำรวจอาจขอหมายเพื่อเข้าค้นสถานที่ (หมายค้น) เพื่อให้ได้มาซึ่งพยานหลักฐานที่อาจจะเป็นพยานหลักฐานที่เกิดขึ้นในขณะที่กระทำความผิด หรือที่อาจได้มาจากพยานหลักฐานที่ยึดมาจากการค้น หรืออาจเป็นยานพาหนะ หรือทรัพย์สินอื่นที่เจ้าหน้าที่ตำรวจเชื่อว่าจะสามารถใช้เป็นพยานหลักฐานที่อาจใช้พิสูจน์ถึงการกระทำความผิดได้[199] โดยผู้มีอำนาจออกหมายค้นจะออกหมายค้นได้ต่อเมื่อแสดงให้เป็นที่พอใจแก่ผู้มีอำนาจออกหมายว่าพยานหลักฐานหรือทรัพย์สินดังกล่าวที่ต้องเข้าทำการตรวจค้น มีเหตุอันควรเชื่อที่จะสงสัย (Reasonable grounds for suspecting) ว่าพยานหลักฐาน ทรัพย์สิน หรือสิ่งของต้องห้ามอยู่ ณ สถานที่นั้น หรืออาจจะถูกนำมาอยู่ในสถานที่นั้นภายใน 72 ชั่วโมง[200]

ส่วนมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในคำสั่งในหมายค้นเกี่ยวกับข้อมูลอุปกรณ์ที่ได้มาจากอุปกรณ์ดิจิทัลตามมาตรา 154 และอำนาจของเจ้าหน้าที่ภายหลังจากอุปกรณ์ดิจิทัลถูกยึดตาม มาตรา 154A ซึ่งอยู่ภายใต้บทที่ 7 ว่าด้วยการค้น การได้มาซึ่งเอกสาร การเข้าถึงภาพดิจิทัล หรือข้อมูลอื่น และสถานที่เกิดเหตุ

มาตรา 154 บัญญัติว่า “คำสั่งในหมายค้นเกี่ยวกับข้อมูลอุปกรณ์ที่ได้มาจากอุปกรณ์ดิจิทัล

---

[199] Police Powers and Responsibilities Act 2020, Section 150.

[200] Police Powers and Responsibilities Act 2020, Section 151.

(1) หากผู้ออกหมาย คือ ผู้พิพากษาของศาลท้องถิ่นหรือศาลสูง ผู้ออกหมายอาจมีคำสั่งในหมายค้นกำหนดให้บุคคลที่เกี่ยวข้องให้กระทำการดังต่อไปนี้ต่ออุปกรณ์ดิจิทัล ณ สถานที่ที่ถูกทำการตรวจค้น

(a) ให้เจ้าหน้าที่ตำรวจเข้าถึงอุปกรณ์ดิจิทัล

(b) ให้ชุดข้อมูลเพื่อเข้าถึงอุปกรณ์แก่เจ้าหน้าที่ตำรวจเพื่อเข้าถึงข้อมูลอุปกรณ์ดิจิทัล หรือให้ความร่วมมือที่จำเป็นเพื่อให้เจ้าหน้าที่ตำรวจสามารถเข้าถึงข้อมูลอุปกรณ์จากอุปกรณ์ดิจิทัลได้

(c) อนุญาตให้เจ้าหน้าที่ตำรวจ

(i) ใช้ข้อมูลที่ได้จากอุปกรณ์เพื่อเข้าถึงข้อมูลอุปกรณ์ หรือ

(ii) ตรวจสอบข้อมูลอุปกรณ์เพื่อหาว่าข้อมูลนั้นอาจเป็นพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิด หรือ

(iii) ทำสำเนาอุปกรณ์ที่อาจเป็นพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิด รวมไปถึงการใช้อุปกรณ์ดิจิทัลอื่น หรือ

(iv) แปลงข้อมูลอุปกรณ์ที่อาจเป็นพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดให้อยู่ในรูปแบบเอกสาร หรือรูปแบบอื่นที่ทำให้เจ้าหน้าที่ตำรวจสามารถเข้าใจข้อมูลได้

(2) หากผู้ออกหมาย คือ ผู้พิพากษาของศาลท้องถิ่นหรือศาลสูง ผู้ออกหมายอาจมีคำสั่งในหมายค้นถึงบุคคลที่เกี่ยวข้องให้กระทำการตามอนุมาตรา (1) (b) หรือ (c) ต่ออุปกรณ์ดิจิทัลที่ถูกยึด และนำออกจากสถานที่ที่ถูกทำการตรวจค้น หลังจากที่อุปกรณ์ดังกล่าวถูกนำออกมาแล้ว

(3) คำสั่งที่สั่งภายใต้อนุมาตรา (2) ต้องมีข้อความดังต่อไปนี้

(a) เวลาหรือระยะเวลาที่บุคคลที่เกี่ยวข้องต้องให้ข้อมูลหรือให้ความร่วมมือแก่เจ้าหน้าที่ตำรวจตาม (1) (b) และ

(b) สถานที่ที่บุคคลที่เกี่ยวข้องต้องให้ข้อมูลหรือให้ความร่วมมือ และ

(c) เงื่อนไขใด ๆ ที่ทำให้ได้มาซึ่งข้อมูลหรือความร่วมมือ และ

(d) ความขัดข้องในการปฏิบัติตามที่อาจเกิดขึ้นจากการจัดการภายใต้ประมวลกฎหมายอาญา มาตรา 205A”

นอกจากหมายค้นจะให้อำนาจแก่เจ้าหน้าที่ตำรวจในการทำการตรวจค้นสถานที่แล้ว ตามบทบัญญัติในมาตรานี้ หมายค้นอาจมีคำสั่งที่เกี่ยวข้องกับข้อมูลที่ได้จากอุปกรณ์ดิจิทัลในสถานที่ที่ถูกทำการตรวจค้น บุคคลที่เกี่ยวข้องจะต้องให้เจ้าหน้าที่ตำรวจเข้าถึงอุปกรณ์ดิจิทัลและข้อมูลต่าง ๆ ในอุปกรณ์ดิจิทัล เรียกชุดข้อมูลเพื่อการเข้าถึงข้อมูลในอุปกรณ์ดิจิทัลดังกล่าว รวมไปถึงให้เจ้าหน้าที่ตำรวจทำการตรวจสอบ ทำสำเนา แปลงรูปแบบข้อมูลดิจิทัล ให้เจ้าหน้าที่ตำรวจสามารถเข้าใจข้อมูลได้ บุคคลซึ่งฝ่าฝืนคำสั่งเกี่ยวกับข้อมูลอุปกรณ์ที่ได้มาจากอุปกรณ์ดิจิทัลโดยไม่มีเหตุผลอันสมควรจะถือว่ามีความผิดทางอาญา ระวางโทษจำคุกสูงสุด 5 ปี[201]

มาตรา 154A บัญญัติว่า “คำสั่งภายหลังจากอุปกรณ์ดิจิทัลถูกยึด

(1) มาตรานี้จะใช้บังคับหาก

(a) อุปกรณ์ดิจิทัลถูกยึดภายใต้หมายค้นและถูกนำออกจากสถานที่ที่ถูกทำการตรวจค้น

(b) ทั้งสองกรณี

(i) หมายค้นไม่มีคำสั่งที่สั่งภายใต้ มาตรา 154 (1) หรือ (2) หรือ

(ii) หมานค้นมีคำสั่งที่สั่งภายใต้ มาตรา 154 (1) หรือ (2) แต่มีการกำหนดเพิ่มเกี่ยวกับการเข้าถึงข้อมูลสำหรับเจ้าหน้าที่ตำรวจเพื่อให้เข้าถึงข้อมูลอุปกรณ์ที่อาจเป็นพยานหลักฐานที่เกี่ยวกับการกระทำความผิด

(2) ในคำขอของเจ้าหน้าที่ตำรวจนั้น ศาลท้องถิ่นหรือศาลสูงอาจมีคำสั่งให้บุคคลที่เกี่ยวข้องกระทำการตาม มาตรา 154 (1) (b) หรือ (c)

(3) คำขอที่ทำภายใต้อนุมาตรา (2)

(a) อาจทำในเวลาใดก็ได้หลังจากที่ออกหมายแล้ว และ

(b) จะต้องทำ

---

[201] Criminal Code Act, Section 205A

(i) หากมีการออกหมายค้นโดยผู้พิพากษาศาลสูงถึงผู้พิพากษาศาลสูง หรือ

(ii) หากมีการออกหมายค้นโดยผู้พิพากษาศาลท้องถิ่นถึงผู้พิพากษาศาลท้องถิ่น

(4) คำขอที่ทำภายใต้อนุมาตรา (2) ต้องมีข้อความดังต่อไปนี้

(a) เวลาหรือระยะเวลาที่บุคคลที่เกี่ยวข้องต้องให้ข้อมูลหรือให้ความร่วมมือแก่เจ้าหน้าที่ตำรวจตาม (1) (b) และ

(b) สถานที่ที่บุคคลที่เกี่ยวข้องต้องให้ข้อมูลหรือให้ความร่วมมือ และ

(c) เงื่อนไขใด ๆ ที่ทำให้ได้มาซึ่งข้อมูลหรือความร่วมมือ และ

(d) ความขัดข้องในการปฏิบัติตามที่อาจเกิดขึ้นจากการจัดการภายใต้ประมวลกฎหมายอาญา มาตรา 205A

(5) ศาลท้องถิ่นหรือศาลสูงอาจมีคำสั่งตามอนุมาตรา (2) ในกรณีที่แน่ใจว่ามีเหตุอันควรเชื่อที่จะควรสงสัยว่าข้อมูลอุปกรณ์จากอุปกรณ์ดิจิทัลอาจเป็นพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิด”

ตามบทบัญญัติมาตรานี้ ภายหลังจากที่อุปกรณ์ดิจิทัลถูกยึดมาจากการค้นในสถานที่ที่ถูกทำการตรวจค้นแล้ว เจ้าหน้าที่ตำรวจมีอำนาจในการเข้าถึงอุปกรณ์ดิจิทัลและข้อมูลต่าง ๆ ในอุปกรณ์ดิจิทัล เรียกชุดข้อมูลเพื่อการเข้าถึงข้อมูลในอุปกรณ์ดิจิทัลดังกล่าว รวมไปถึงให้เจ้าหน้าที่ตำรวจทำการตรวจสอบ ทำสำเนา แปลงรูปแบบข้อมูลดิจิทัล ให้เจ้าหน้าที่ตำรวจสามารถเข้าใจข้อมูลได้เช่นเดียวกันกับในกรณีที่เจ้าหน้าที่ตำรวจทำการตรวจค้นอุปกรณ์ดิจิทัล ณ สถานที่ที่ถูกทำการตรวจค้น อีกทั้งคำสั่งที่เกี่ยวข้องกับข้อมูลที่ได้จากอุปกรณ์ดิจิทัล บุคคลซึ่งฝ่าฝืนคำสั่งเกี่ยวกับข้อมูลอุปกรณ์ที่ได้มาจากอุปกรณ์ดิจิทัลโดยไม่มีเหตุผลอันสมควรจะถือว่ามีความผิดทางอาญา ระวางโทษจำคุกสูงสุด 5 ปี[202]

อย่างไรก็ตาม การที่เจ้าหน้าที่ตำรวจจะขอออกหมายค้นต่อศาลท้องถิ่นหรือศาลสูงเพื่อดำเนินการในการค้นอุปกรณ์ดิจิทัลต่าง ๆ นั้น จะขอหมายค้นได้ก็แต่เฉพาะในกรณีที่มีเหตุ

---

[202] Criminal Code Act, Section 205A

อันควรเชื่อที่จะสงสัยว่าจะพบพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิด วัตถุที่ต้องห้ามจากการเข้าทำการตรวจค้นในสถานที่นั้น หรืออาจถูกนำไปไว้ในสถานที่นั้นภายใน 72 ชั่วโมง[203] เมื่อได้มีการขอหมายค้นแล้ว ผู้ออกหมายค้นอาจมีคำสั่งเกี่ยวกับการแสวงหาพยานหลักฐานดิจิทัลจากอุปกรณ์ดิจิทัลที่ถูกทำการยึดดังกล่าว

4.3.2.2 การค้นอุปกรณ์ดิจิทัลที่สถานที่เกิดเหตุหรือถูกยึดจากสถานที่เกิดเหตุ

การค้นอุปกรณ์ดิจิทัลที่สถานที่เกิดเหตุหรือถูกยึดจากสถานที่เกิดเหตุตามมาตรา 178A ปรากฏอยู่ในบทที่ 7 ว่าด้วยการค้น การได้มาซึ่งเอกสาร การเข้าถึงภาพดิจิทัล หรือข้อมูลอื่น และสถานที่เกิดเหตุ

มาตรา 178A บัญญัติว่า “คำสั่งเกี่ยวกับอุปกรณ์ดิจิทัลที่สถานที่เกิดเหตุหรือถูกยึดจากสถานที่เกิดเหตุ

(1) ในคำขอของเจ้าหน้าที่ตำรวจ ผู้พิพากษาของศาลท้องถิ่นหรือศาลสูงอาจมีคำสั่งให้บุคคลที่เกี่ยวข้องกระทำการตามอนุมาตรา (2) ต่ออุปกรณ์ดิจิทัลที่

(a) อยู่ในสถานที่เกิดเหตุ

(b) ถูกยึดจากสถานที่เกิดเหตุตาม มาตรา 176 (1) (j)

(2) บุคคลที่เกี่ยวข้องอาจถูกกำหนดให้กระทำการ

(a) มอบอุปกรณ์ให้เจ้าหน้าที่ตำรวจเข้าถึง หรือ

(b) มอบข้อมูลหรือให้ความร่วมมือที่จำเป็นในการเข้าถึงอุปกรณ์ให้แก่เจ้าหน้าที่ตำรวจเพื่อให้เจ้าหน้าที่ตำรวจสามารถเข้าถึงอุปกรณ์ หรือ

(c) อนุญาตเจ้าหน้าที่ตำรวจให้

(i) ใช้ข้อมูลในการเข้าถึงอุปกรณ์เพื่อเข้าถึงอุปกรณ์ หรือ

(ii) ตรวจสอบข้อมูลอุปกรณ์เพื่อหาว่าข้อมูลนั้นอาจเป็นพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดในสถานที่เกิดเหตุซึ่งเป็นจุดเริ่มต้นของความผิด

---

[203] Police Powers and Responsibilities Act 2020, Section 151.

(iii) ทำสำเนาข้อมูลอุปกรณ์ที่อาจเป็นพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดในสถานที่เกิดเหตุซึ่งเป็นจุดเริ่มต้นของความผิด รวมถึงการใช้อุปกรณ์ดิจิทัลอื่นหรือ

(iv) แปลงข้อมูลอุปกรณ์ที่อาจเป็นพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดในสถานที่เกิดเหตุซึ่งเป็นจุดเริ่มต้นของความผิดให้อยู่ในรูปแบบเอกสาร หรือรูปแบบอื่นที่ทำให้เจ้าหน้าที่ตำรวจสามารถเข้าใจข้อมูลได้

(3) ศาลท้องถิ่นหรือศาลสูงอาจมีคำสั่งในกรณีที่แน่ใจว่ามีเหตุอันควรเชื่อที่จะควรสงสัยว่าข้อมูลอุปกรณ์จากอุปกรณ์ดิจิทัลอาจเป็นพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดจากการกระทำความผิดในสถานที่เกิดเหตุ

(4) คำสั่งต้องมีข้อความดังต่อไปนี้

(a) เวลาหรือระยะเวลาที่บุคคลที่เกี่ยวข้องต้องให้ข้อมูลหรือให้ความร่วมมือแก่เจ้าหน้าที่ตำรวจตาม (2) (b) และ

(b) สถานที่ที่บุคคลที่เกี่ยวข้องต้องให้ข้อมูลหรือให้ความร่วมมือ และ

(c) เงื่อนไขใด ๆ ที่ทำให้ได้มาซึ่งข้อมูลหรือความร่วมมือ และ

(d) ความขัดข้องในการปฏิบัติตามที่อาจเกิดขึ้นจากการจัดการภายใต้ประมวลกฎหมายอาญา มาตรา 205A

(5) เมื่อคำขอเกี่ยวกับคำสั่งอาจถูกกำหนดโดยไม่มีระยะเวลาจำกัด คำขออาจถูกยื่นในเวลาเดียวกับที่เจ้าหน้าที่ตำรวจได้ไปรับมอบอำนาจให้ไปตรวจสถานที่เกิดเหตุและผู้พิพากษาหรือเจ้าหน้าที่ฝ่ายปกครองอาจใส่ไว้ในคำสั่งให้ตรวจสถานที่เกิดเหตุ”

ตามบทบัญญัติในมาตรานี้ อุปกรณ์ดิจิทัลที่เจ้าหน้าที่ตำรวจมีอำนาจในการเก็บข้อมูล คือ อุปกรณ์ดิจิทัลที่พบในสถานที่เกิดเหตุหรือถูกยึดจากสถานที่เกิดเหตุ บุคคลที่เกี่ยวข้องจะต้องให้เจ้าหน้าที่ตำรวจเข้าถึงอุปกรณ์ดิจิทัลและข้อมูลในอุปกรณ์ดิจิทัล ให้ชุดข้อมูลเพื่อเข้าถึงข้อมูลในอุปกรณ์ดิจิทัล รวมถึงให้ตรวจสอบ ทำสำเนา หรือแปลงรูปแบบข้อมูลดิจิทัล ให้เจ้าหน้าที่ตำรวจสามารถเข้าใจข้อมูลได้ โดยจะมีคำสั่งดังกล่าวได้ต่อเมื่อมีเหตุอันควรเชื่อที่จะสงสัยว่าจะพบพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิด บุคคลซึ่งฝ่าฝืนคำสั่งเกี่ยวกับข้อมูลอุปกรณ์ที่ได้มา

จากอุปกรณ์ดิจิทัลโดยไม่มีเหตุผลอันสมควรจะถือว่ามีความผิดทางอาญา ระวางโทษจำคุกสูงสุด 5 ปี[204]

จากการศึกษาจะเห็นได้ว่ามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของต่างประเทศมีความแตกต่างกันไปตามแนวความคิดเกี่ยวกับกระบวนการยุติธรรมทางอาญาของในประเทศนั้น ๆ สำหรับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ สามารถที่จะจำแนกออกได้เป็น 2 รูปแบบด้วยกัน ได้แก่ มาตรการที่มีลักษณะเป็นการร่วมมือกันระหว่างภาครัฐและภาคเอกชน และมาตรการที่มีลักษณะเป็นการให้อำนาจแก่รัฐในการดำเนินการเป็นหลัก โดยมีข้อสังเกตหลักอยู่ที่การเข้าถึงข้อมูลต่าง ๆ ของประชาชน ซึ่งมาตรการที่มีลักษณะเป็นการร่วมมือกันระหว่างภาครัฐและภาคเอกชนจะไม่มีมาตรการใด ๆ ที่เป็นการให้อำนาจแก่รัฐในการเข้าถึงข้อมูลต่าง ๆ แต่จะเป็นความสมัครใจของเจ้าของข้อมูลที่จะส่งข้อมูลให้แก่รัฐหรือหน่วยงานที่เกี่ยวข้องหรือไม่ ดังเช่นที่ปรากฏในมาตรการประเทศสหรัฐอเมริกาและเครือรัฐออสเตรเลีย ส่วนมาตรการที่มีลักษณะเป็นการให้อำนาจแก่รัฐในการดำเนินการ กำหนดให้รัฐเป็นผู้ใช้อำนาจต่าง ๆ ไม่ว่าจะเป็นการเข้าถึงข้อมูลคอมพิวเตอร์ ยึด ตรวจค้นคอมพิวเตอร์ ระบบคอมพิวเตอร์ต่าง ๆ รวมไปถึงการเข้าทำการตรวจค้นสถานที่ด้วย เป็นต้น ดังที่ปรากฏในมาตรการของประเทศสิงคโปร์ ซึ่งมาตรการต่าง ๆ เหล่านี้ย่อมกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน จึงจำเป็นต้องมีมาตรการในการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐเป็นสำคัญ โดยประเทศสิงคโปร์ได้มีการกำหนดห้ามมิให้นำข้อมูลซึ่งได้มาจากมาตรการในการรักาความมั่นคงปลอดภัยไซเบอร์ไปใช้กับดำเนินคดีต่าง ๆ ไม่ว่าจะเป็นคดีแพ่งหรือคดีอาญาก็ตาม

ส่วนมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของต่างประเทศปรากฏอยู่ในบทบัญญัติกฎหมายเกี่ยวกับการสืบสวนสอบสวนต่าง ๆ ซึ่งมีหลักเกณฑ์ในการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐอยู่อย่างชัดเจน ในประเทศสหรัฐอเมริกา หรือรัฐควีนส์แลนด์ เครือรัฐออสเตรเลียก็ตาม ส่วนในประเทศสิงคโปร์มีรูปแบบของแสวงหาพยานหลักฐานที่แตกต่างไปจากประเทศอื่น ๆ ซึ่งให้อำนาจแก่เจ้าหน้าที่ตำรวจเป็นผู้เริ่มต้นในการสืบสวนสอบสวนเพื่อแสวงหาพยานหลักฐานต่าง ๆ โดยไม่จำต้องมีการตรวจสอบการใช้อำนาจโดยองค์กรตุลาการก่อน แต่มาตรการดังกล่าวก็เป็นมาตรการที่อยู่ภายใต้ความสมัครใจของบุคคลที่ปฏิบัติหรือไม่ปฏิบัติตามคำสั่งของเจ้าหน้าที่ตำรวจ หากไม่ปฏิบัติตามเจ้าหน้าที่ตำรวจจำเป็นต้องยื่นคำร้องต่อศาลเพื่อให้มีคำสั่งให้ปฏิบัติตามอีกครั้งหนึ่ง

---

[204] Criminal Code Act, Section 205A

เมื่อได้ศึกษามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ทั้งในประเทศไทยและต่างประเทศแล้ว ในบทต่อไปจะได้ทำการวิเคราะห์ประเด็นปัญหาต่าง ๆ เกี่ยวกับมาตรา 70 วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางที่เหมาะสมแก่การแก้ไขบทบัญญัติดังกล่าว

บทที่ 5
วิเคราะห์มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์

เมื่อได้ศึกษามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทยและในต่างประเทศ ได้แก่ ประเทศสหรัฐอเมริกา ประเทศสิงคโปร์ และเครือรัฐออสเตรเลีย รัฐควีนส์แลนด์ เครือรัฐออสเตรเลียแล้ว ในบทนี้ผู้เขียนจะวิเคราะห์ใน 3 ประเด็นด้วยกัน โดยจะทำการวิเคราะห์มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์เปรียบเทียบกับ (1) มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ในต่างประเทศ (2) มาตรการในการแสวงหาพยานหลักฐานในประเทศไทย และ (3) มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในต่างประเทศ โดยมีรายละเอียดดังนี้

5.1 วิเคราะห์เปรียบเทียบมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ในต่างประเทศ

ภัยคุกคามไซเบอร์เป็นภัยคุกคามที่มีรากฐานมาจากอาชญากรรมทางคอมพิวเตอร์ หรืออาชญากรรมทางไซเบอร์ ในปัจจุบันนานาประเทศได้มีการกำหนดกรอบของมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันหรือจำกัดความเสียหายที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ ประเทศไทยซึ่งได้เล็งเห็นถึงปัญหาเกี่ยวกับภัยคุกคามไซเบอร์จึงได้มีการศึกษาแนวทางในการแก้ไขปัญหาและรับมือต่อภัยคุกคามไซเบอร์ดังกล่าว ภายหลังจึงได้มีการประกาศใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีเหตุผลหรือวัตถุประสงค์เพื่อป้องกัน รับมือต่อภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที โดยกำหนดหน้าที่แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐ และหน่วยงานของเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ไม่ให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ จัดตั้งหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน และกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง

5.1.1 วัตถุประสงค์ของมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์

จากเหตุผลและวัตถุประสงค์ของการประกาศใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ข้างต้นจะเห็นได้ว่ามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์เป็น

มาตรการที่มีขึ้นเพื่อป้องกัน รับมือต่อภัยคุกคามทางไซเบอร์เป็นสำคัญ โดยได้มีการกำหนดมาตรการต่าง ๆ ซึ่งให้อำนาจแก่เจ้าหน้าที่รัฐในการดำเนินการเพื่อให้เป็นไปตามวัตถุประสงค์ของพระราชบัญญัติ ฯ โดยสามารถเปรียบเทียบวัตถุประสงค์ของมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยและต่างประเทศเป็นตารางได้ ดังนี้

ตารางที่ 2 : ตารางเปรียบเทียบวัตถุประสงค์ของมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยและต่างประเทศ

ประเทศ	วัตถุประสงค์ของมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์
ไทย	กำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างมีเอกภาพและต่อเนื่อง
ประเทศสหรัฐอเมริกา	พัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ผ่านการแลกเปลี่ยนและแบ่งปันข้อมูลข่าวสารทางไซเบอร์ระหว่างรัฐบาลกลางและหน่วยงานอื่น ๆ เช่น ภาคเอกชน องค์กร รวมถึงหน่วยงานโครงสร้างพื้นฐานสำคัญ หรือหน่วยงานในระดับมลรัฐ เป็นต้น
ประเทศสิงคโปร์	กำหนดหรืออนุญาตให้มีมาตรการป้องกัน จัดการ และตอบสนองต่อภัยคุกคามและเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ เพื่อกำกับผู้เป็นเจ้าของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อกำกับผู้ให้บริการด้านการรักษาความปลอดภัยไซเบอร์ และสิ่งที่เกี่ยวข้องกับ

	ข้อความข้างต้น และเพื่อให้เป็นผลสืบเนื่องต่อการแก้ไขกฎหมายลายลักษณ์อักษรฉบับอื่น ๆ
เครือรัฐออสเตรเลีย	เพื่อให้โลกออนไลน์มีความปลอดภัยมากยิ่งขึ้นสำหรับประชาชนชาวออสเตรเลีย ธุรกิจของภาคเอกชน และการให้บริการที่จำเป็น โดยจะจัดให้มีการดำเนินการที่เป็นหลักการสำคัญ ได้แก่ มีการดำเนินการโดยรัฐบาลกลางเพื่อเสริมสร้างการปกป้องประชาชนชาวออสเตรเลีย ธุรกิจของภาคเอกชน การให้บริการที่จำเป็นจากภัยคุกคามอันมีความสลับซับซ้อน มีการดำเนินการโดยภาคธุรกิจเพื่อรักษาความปลอดภัยต่อผลิตภัณฑ์และบริการ และปกป้องผู้บริโภคจากช่องโหว่ทางไซเบอร์ที่ทราบถึงการมีอยู่ของช่องโหว่นั้น และมีการดำเนินการโดยชุมชนเพื่อสร้างแนวปฏิบัติที่ปลอดภัยในพฤติกรรมทางออนไลน์ และการซื้ออย่างชาญฉลาดของผู้บริโภค

เมื่อพิจารณาวัตถุประสงค์ของมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ จะเห็นได้ว่ามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์มีวัตถุประสงค์หลักเพื่อส่งเสริมและสร้างความปลอดภัยให้แก่โลกไซเบอร์เป็นสำคัญ โดยประเทศสหรัฐอเมริกาได้มีการบังคับใช้กฎหมายการแบ่งปันข้อมูลความปลอดภัยไซเบอร์ ซึ่งอยู่ในหมวดที่ 1 ของกฎหมายความปลอดภัยไซเบอร์ โดยกฎหมายการแบ่งปันข้อมูลความปลอดภัยไซเบอร์ ฯ มีวัตถุประสงค์เพื่อพัฒนามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ผ่านการแลกเปลี่ยนและแบ่งปันข้อมูลข่าวสารทางไซเบอร์ ระหว่างรัฐบาลกลางและหน่วยงานอื่น ๆ เช่น ภาคเอกชน องค์กร รวมถึงหน่วยงานโครงสร้างพื้นฐานสำคัญ หรือหน่วยงานในระดับมลรัฐ เป็นต้น และกำหนดให้กระทรวงความมั่นคงแห่งมาตุภูมิเป็นหน่วยงานที่รับผิดชอบในการประสานงาน มีอำนาจในการออกมาตรการตรวจสอบป้องกันและส่งข้อมูลที่เกี่ยวข้องไปยังหน่วยงานอื่น ๆ ซึ่งระบบที่มีการแบ่งปันข้อมูลต้องเป็นระบบอัตโนมัติ และส่งข้อมูลแบบปัจจุบันและต่อเนื่อง (Real Time) เพื่อที่จะสามารถนำไปใช้ประโยชน์ในการรับมือ ป้องกัน และบรรเทาความเสียหายจากภัยคุกคามไซเบอร์ได้อย่างทันท่วงที

ประเทศสิงคโปร์ได้มีการประกาศใช้กฎหมายความมั่นคงปลอดภัยไซเบอร์ ค.ศ. 2018 โดยมีวัตถุประสงค์เพื่อกำหนดหรืออนุญาตให้มีมาตรการป้องกัน จัดการ และตอบสนองต่อภัย

คุกคามและเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ เพื่อกำกับผู้เป็นเจ้าของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการด้านการรักษาความปลอดภัยไซเบอร์ และสิ่งที่เกี่ยวข้องกับข้อความข้างต้น และเพื่อให้เป็นผลสืบเนื่องต่อการแก้ไขกฎหมายลายลักษณ์อักษรฉบับอื่น ๆ

และเครือรัฐออสเตรเลียได้มีการประกาศยุทธศาสตร์ความปลอดภัยไซเบอร์ ค.ศ. 2020 (Australia's Cyber Security Strategy 2020) เพื่อให้โลกออนไลน์มีความปลอดภัยมากยิ่งขึ้นสำหรับประชาชนชาวออสเตรเลีย ธุรกิจของภาคเอกชน และการให้บริการที่จำเป็น

จากการศึกษาจะเห็นได้ว่า วัตถุประสงค์ในการกำหนดมาตรการในการรักษาความปลอดภัยไซเบอร์ในต่างประเทศรวมไปถึงประเทศไทย มีวัตถุประสงค์ไปในทิศทางเดียวกัน คือ เพื่อรักษาความมั่นคงปลอดภัยในโลกไซเบอร์ โดยจะกำหนดหน้าที่แก่หน่วยงานโครงสร้างพื้นฐานที่สำคัญของประเทศไม่ว่าจะเป็นหน่วยงานรัฐหรือหน่วยงานเอกชนก็ตาม ให้รายงานภัยคุกคามไซเบอร์ที่ตนทราบแก่หน่วยงานรัฐ และกำหนดหน้าที่ในการพัฒนามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ต่าง ๆ ให้ต้องดำเนินการตามกรอบหรือแนวทางด้วย ซึ่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ก็ได้มีการบัญญัติขึ้นโดยมีวัตถุประสงค์เช่นเดียวกันกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศอื่น ๆ

อย่างไรก็ตาม แม้วัตถุประสงค์ในการกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของนานาประเทศจะไปในทิศทางเดียวกัน แต่มาตรการที่ได้มีการกำหนดไว้แตกต่างกันอย่างชัดเจน ดังจะได้กล่าวต่อไป

5.1.2 มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์

ภัยคุกคามไซเบอร์นั้นมีรากฐานมาจากอาชญากรรมคอมพิวเตอร์ โดยในแรกเริ่มนานาประเทศได้เริ่มต้นจากการกำหนดฐานความผิดใหม่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ขึ้นเพื่อให้เกิดอำนาจสืบสวนสอบสวน และอำนาจในการแสวงหาพยานหลักฐานแก่เจ้าหน้าที่ผู้มีอำนาจหน้าที่ในประเทศของตนเพื่อหาตัวผู้กระทำความผิดมาลงโทษ แต่เมื่อในภายหลังการสืบสวนสอบสวนเพื่อหาตัวผู้ก่ออาชญากรรมคอมพิวเตอร์นั้นเป็นมาตรการที่ไม่ทันท่วงที กล่าวคือ เป็นมาตรการที่ดำเนินการภายหลังจากพบการกระทำความผิดขึ้น จึงได้มีแนวคิดเกี่ยวกับการจัดการปัญหาดังกล่าวก่อนที่จะเกิดความเสียหายเป็นวงกว้าง นั่นก็คือ มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีวัตถุประสงค์เพื่อจัดการกับปัญหาภัยคุกคามตั้งแต่ก่อนที่ภัยคุกคามดังกล่าวจะเกิดขึ้นรวมไปถึงการ

จำกัดความเสียหายที่อาจเกิดขึ้นจากภัยคุกคามดังกล่าว กล่าวคือ เป็นการรับมือ ป้องกัน และลดความเสี่ยงจากการสร้างความเสียหายของภัยคุกคามไซเบอร์ ซึ่งในประเทศต่าง ๆ ที่ผู้เขียนได้ทำการศึกษาล้วนแล้วแต่มีมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งสิ้น แต่มาตรการดังกล่าวก็มีความแตกต่างกันไปตามหลักการและแนวความคิดของแต่ละประเทศ โดยสามารถเปรียบเทียบมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยและต่างประเทศเป็นตารางได้ ดังนี้

ตารางที่ 3 : ตารางเปรียบเทียบมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยและต่างประเทศ

มาตรการในการรักษาความปลอดภัยไซเบอร์	**ประเทศไทย**	**ประเทศสหรัฐอเมริกา**	**ประเทศสิงคโปร์**	**เครือรัฐออสเตรเลีย**
มาตรการที่มีลักษณะเป็นการร่วมมือระหว่างภาครัฐและภาคเอกชน	มี	มี	มี	มี
มาตรการที่มีลักษณะเป็นการให้อำนาจแก่รัฐในการเข้าถึงข้อมูลต่าง ๆ ของประชาชน	มี	ไม่มี	มี	ไม่มี
มาตรการที่มีลักษณะเป็นการให้อำนาจรัฐในการแสวงหาพยานหลักฐาน	มี	ไม่มี	ไม่มี	ไม่มี

ประเทศไทยได้มีการบัญญัติพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ฯ ขึ้นเพื่อกำหนดมาตรการต่าง ๆ โดยเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยสามารถแบ่งออกได้เป็น 2 ลักษณะด้วยกัน ได้แก่ มาตรการที่เป็นความร่วมมือระหว่างภาครัฐและเอกชน โดยกำหนดหน้าที่เบื้องต้นแก่หน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญภายในประเทศเพื่อพัฒนาแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศร่วมกัน และมาตรการที่ให้อำนาจแก่เจ้าหน้าที่รัฐในการเข้าถึงข้อมูลต่าง ๆ ของประชาชนเพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยไซเบอร์ โดยอำนาจของเจ้าหน้าที่รัฐที่มีลักษณะเป็นการได้ไปซึ่งข้อมูลจากประชาชนสามารถแบ่งออกได้เป็น 3 ประการด้วยกันดังนี้

(1) มาตรการในกรณีของภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงไม่ได้ให้อำนาจเป็นพิเศษแก่เจ้าหน้าที่รัฐแต่อย่างใด คงกำหนดเพียงว่าให้เจ้าหน้าที่รัฐทำการรวบรวม ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบ รวมไปถึงการสนับสนุน ให้ความช่วยเหลือหรือประสานงาน ในการป้องกัน รับมือ และลดความเสี่ยงเท่านั้น[205]

(2) มาตรการในกรณีของภัยคุกคามทางไซเบอร์ในระดับร้ายแรงได้ให้อำนาจแก่เจ้าหน้าที่รัฐในการมีหนังสือขอความร่วมมือให้บุคคลที่เกี่ยวข้องมาให้ข้อมูลหรือให้ส่งข้อมูลเป็นหนังสือ และการมีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของบุคคลใดเพื่อประโยชน์ในการดำเนินการ[206] ซึ่งมีลักษณะเป็นการขอความร่วมมือ อีกทั้งยังได้ให้อำนาจในการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์[207] ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ[208] ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ โดยในการเข้าถึงข้อมูลดังกล่าวจะต้องยื่นคำร้องต่อศาลโดยระบุเหตุอันควรเชื่อได้ว่ามีบุคคลใดบุคคลหนึ่งกำลังก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

(3) มาตรการในกรณีของภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ซึ่งกำหนดให้เจ้าหน้าที่รัฐมีอำนาจดำเนินการใด ๆ ได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าโดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากได้ดำเนินการไปแล้วให้แจ้งรายละเอียดการ

---

[205] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 59

[206] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 62

[207] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 65 (5) และ 66 (2)

[208] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 66 (4)

ดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว รวมถึงมีอำนาจขอข้อมูลที่เป็นปัจจุบันและต่อเนื่อง (Real Time) จากผู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์

ในประเทศสหรัฐอเมริกามีมาตรการทางกฎหมายในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เน้นไปที่การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานตามกฎหมายการแบ่งปันข้อมูลความปลอดภัยไซเบอร์ ค.ศ. 2015 (Cybersecurity Information Sharing Act 2015) โดยกฎหมายดังกล่าวจะไม่ได้เป็นการบังคับให้หน่วยงานที่เกี่ยวข้องจะต้องเข้าร่วมในการแลกเปลี่ยนข้อมูล และได้มีการจำกัดอำนาจของเจ้าหน้าที่ รวมไปถึงคุ้มครองบุคคลที่ดำเนินการตามกฎหมายฉบับนี้ และคุ้มครองข้อมูลส่วนบุคคล ได้แก่ การแบ่งปันข้อมูลตามกฎหมายบับนี้ย่อมไม่มีความรับผิดในทางแพ่ง ไม่ถือว่าเป็นการสละเอกสิทธิ์หรือสละความคุ้มครองใด ๆ ที่กำหนดโดยกฎหมาย หากพบข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้องหรือข้อมูลที่ไม่เกี่ยวข้องโดยตรงกับที่กฎหมายให้อำนาจไว้จะต้องดำเนินการนำออกจากระบบ และกำหนดโทษสำหรับบุคคลที่กระทำภายใต้กฎหมายนี้โดยไม่ได้รับอนุญาต

ส่วนหลักกฎหมายของประเทศสิงคโปร์ได้มีการกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ในกฎหมายความมั่นคงปลอดภัยไซเบอร์ ค.ศ. 2018 (Cybersecurity Act 2018) ซึ่งมีความคล้ายคลึงกับบทบัญญัติของประเทศไทยเป็นอันมาก ได้ให้อำนาจแก่เจ้าหน้าที่ในการเข้าถึงข้อมูลต่าง ๆ ของประชาชน ในกรณีต่าง ๆ ดังนี้

(1) กรณีของภัยคุกคามไซเบอร์ในระดับทั่วไป ให้อำนาจในการเรียกบุคคลมาให้ข้อมูล การขอข้อมูล โดยการเรียกบุคคลหรือการขอข้อมูลนั้น ผู้ได้รับคำสั่งสามารถที่จะไม่เปิดเผยข้อมูลได้หากมีภาระผูกพันตามกฎหมาย สัญญา หรือกฎเกณฑ์ใดกำหนดไว้ และหากเปิดเผยข้อมูลโดยสุจริตและมีความระมัดระวังตามสมควรไม่ถือว่าเป็นการผิดต่อภาระผูกพันต่าง ๆ ข้างต้น

(2) กรณีของภัยคุกคามไซเบอร์ในระดับร้ายแรง มีอำนาจเข้าถึง ตรวจสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อค้นหาข้อมูลใด ๆ ได้ ทำสำเนา ดึงข้อมูล หรือโปรแกรม รวมไปถึงการเข้าไปตรวจสอบสถานที่ใด ๆ และยึดคอมพิวเตอร์หรืออุปกรณ์ใด ๆ โดยอำนาจนี้ไม่มีข้อกำหนดที่มีลักษณะเป็นการคุ้มครองดังเช่นอำนาจก่อนหน้า โดยอำนาจเหล่านี้อยู่บนหลักการว่าเจ้าหน้าที่จะต้องมีเหตุอันควรสงสัยว่าเป็นหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(3) กรณีของภัยคุกคามทางไซเบอร์ในระดับฉุกเฉินซึ่งได้ให้อำนาจในการใช้มาตรการใด ๆ ที่เห็นว่าจำเป็นและเหมาะสมได้ทั้งสิ้น มีการบัญญัติคุ้มครองผู้เปิดเผยข้อมูลไว้ โดยบุคคลที่ได้ให้ข้อมูลแก่เจ้าหน้าที่ตามมาตรการและข้อกำหนดด้านความปลอดภัยไซเบอร์ในกรณี

ฉุกเฉินโดยสุจริต ไม่ถือว่ากระทำความผิดหรือฝ่าฝืนข้อกำหนดตามกฎหมาย สัญญา หรือมาตรฐานทางวิชาชีพนั้น ๆ

นอกจากนี้ยังได้มีการกำหนดการคุ้มครองข้อมูลที่อาจนำไปเป็นพยานหลักฐานในการดำเนินคดีแพ่งหรือคดีอาญา กล่าวคือ ในกรณีที่ความผิดใดถูกเปิดเผยระหว่างหรือจากการใช้มาตราการต่าง ๆ ภายใต้มาตรานี้ โดยระบุว่า ข้อมูลใด ๆ ที่ได้จากมาตรการภายใต้มาตรการเกี่ยวกับภัยคุกคามทางไซเบอร์ในระดับฉุกเฉินนี้ ไม่สามารถใช้เป็นพยานหลักฐานในการดำเนินคดีแพ่งหรือคดีอาญาใด ๆ ได้ และพยานในคดีแพ่งหรือคดีอาญาไม่มีหน้าที่ในการเปิดเผยชื่อ ที่อยู่ หรือรายละเอียดอื่น ๆ ของผู้แจ้งข้อมูล หรือเพื่อตอบคำถามใด ๆ ที่คำตอบจะนำไปสู่ หรืออาจนำไปสู่การค้นพบชื่อ ที่อยู่ หรือรายละเอียดอื่น ๆ ของผู้ให้ข้อมูล หากหนังสือ เอกสาร ข้อมูล หรือผลผลิตจากคอมพิวเตอร์ใด ถูกยอมรับเป็นหลักฐาน หรือความรับผิดต่อการสอบสวนในการดำเนินคดีแพ่งหรือคดีอาญา ประกอบด้วยรายการใด ๆ ซึ่งมีการระบุชื่อ หรือรูปพรรณของผู้ให้ข้อมูล หรืออาจนำไปสู่การค้นพบผู้ให้ข้อมูล ศาลต้องทำให้รายการเหล่านั้นถูกปกปิดจากจากถูกพบ หรือทำการลบเท่าที่จำเป็นเพื่อปกป้องผู้ให้ข้อมูลจากการถูกค้นพบ

และในเครือรัฐออสเตรเลียจัดให้มีมาตรการในการดำเนินการที่เป็นหลักการสำคัญดังต่อไปนี้

(1) มีการดำเนินการโดยรัฐบาลกลางเพื่อเสริมสร้างการปกป้องประชาชนชาวออสเตรเลีย ธุรกิจของภาคเอกชน การให้บริการที่จำเป็นจากภัยคุกคามอันมีความสลับซับซ้อน

(2) มีการดำเนินการโดยภาคธุรกิจเพื่อรักษาความปลอดภัยต่อผลิตภัณฑ์และบริการ และปกป้องผู้บริโภคจากช่องโหว่ทางไซเบอร์ที่ทราบถึงการมีอยู่ของช่องโหว่นั้น

(3) มีการดำเนินการโดยชุมชนเพื่อสร้างแนวปฏิบัติที่ปลอดภัยในพฤติกรรมทางออนไลน์ และการซื้ออย่างชาญฉลาดของผู้บริโภค

เมื่อพิจารณามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยและต่างประเทศทำให้สามารถสรุปได้ว่า โดยลักษณะของมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์สามารถจำแนกออกได้เป็น 2 รูปแบบด้วยกัน ได้แก่ มาตรการที่มีลักษณะเป็นการร่วมมือระหว่างภาครัฐและภาคเอกชน และมาตรการที่มีลักษณะเป็นการให้อำนาจแก่รัฐในการดำเนินการต่าง ๆ โดยมาตรการที่มีลักษณะเป็นการร่วมมือระหว่างภาครัฐและภาคเอกชนเป็นมาตรการซึ่งเป็นหลักการในการดำเนินมาตรการต่าง ๆ เพื่อรักษาความปลอดภัยไซเบอร์อันปรากฏอยู่ในมาตรการของทุก ๆ ประเทศรวมถึงประเทศไทยด้วย โดยอาจมีการกำหนดหน้าที่แก่หน่วยงานโครงสร้างพื้นฐานที่

สำคัญของประเทศให้มีการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของตน และอาจกำหนดหน้าที่แก่หน่วยงานโครงสร้างพื้นฐานที่สำคัญให้มีหน้าที่ต้องรายงานเหตุการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์แก่รัฐหรือหน่วยงานที่เกี่ยวข้อง หรืออาจมีการกำหนดแนวทางในการดำเนินการอื่น ๆ ซึ่งมีลักษณะเป็นการร่วมมือระหว่างภาครัฐและภาคเอกชน

สำหรับมาตรการที่มีลักษณะเป็นการให้อำนาจแก่รัฐในการดำเนินการต่าง ๆ ปรากฏอยู่แต่เฉพาะมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยและประเทศสิงคโปร์เท่านั้น โดยได้มีการกำหนดให้รัฐมีอำนาจในการเข้าถึงข้อมูลต่าง ๆ ของประชาชนได้ ซึ่งลักษณะของอำนาจในการเข้าถึงข้อมูลของประชาชนมีความแตกต่างกันไปในขึ้นอยู่กับระดับความร้ายแรงของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยมีตั้งแต่อำนาจที่มีลักษณะเป็นการขอความร่วมมือจากประชาชน อำนาจที่มีลักษณะเป็นการเข้าถึงข้อมูลต่าง ๆ ของประชาชนโดยมีการตรวจสอบการใช้อำนาจก่อนดำเนินการ รวมไปถึงอำนาจในการเข้าถึงข้อมูลต่าง ๆ ของประชาชนโดยไม่มีการตรวจสอบอำนาจก่อนดำเนินการ แต่ให้มีการตรวจสอบภายหลังดำเนินการแทน

จากการศึกษาวัตถุประสงค์และมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศไทยและประเทศต่าง ๆ ทำให้เห็นว่ามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์มีลักษณะที่แตกต่างจากมาตรการในกระบวนการยุติธรรมทางอาญาทั่วไป กล่าวคือ มาตรการในกระบวนการยุติธรรมทางอาญาทั่วไปเป็นกระบวนการที่มุ่งเน้นในการนำตัวผู้กระทำความผิดมาลงโทษ ดังนั้น ในกระบวนการยุติธรรมทางอาญาจึงมีการกำหนดมาตรการในการสืบสวนและสอบสวนไว้เพื่อให้เจ้าหน้าที่รัฐสามารถรวบรวมพยานหลักฐานมาเพื่อใช้ประกอบการดำเนินคดีต่อผู้กระทำความผิด ซึ่งหลักการในการได้มาซึ่งพยานหลักฐานหรือการแสวงหาพยานหลักฐาน เป็นหลักการที่กระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชน หากเจ้าหน้าที่จะดำเนินการอันใดที่เป็นการกระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชนจะต้องมีกฎหมายบัญญัติไว้โดยชัดเจน นอกจากนี้ยังจำเป็นต้องมีมาตรการในการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐ โดยมาตรการที่เป็นสากลได้แก่ การตรวจสอบการใช้อำนาจโดยองค์กรตุลาการ หรือการตรวจสอบโดยผู้บังคับบัญชา หรือผู้กำกับดูแล เช่น การแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศไทย โดยหลักแล้วพนักงานสอบสวนจะต้องยื่นคำร้องต่อศาลเพื่อขอหมายจากศาล โดยคำร้องจะต้องแสดงเหตุผลที่สมควรที่ศาลจะอนุมัติหมายดังกล่าวไว้ด้วย และในกรณีตามกฎหมายที่กำหนดฐานความผิดพิเศษ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก็กำหนดให้เจ้าหน้าที่จะต้องยื่นคำร้องต่อศาลเพื่อมีคำสั่งอนุญาตให้ดำเนินการตามคำร้อง โดยคำร้อง

ต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่จะสามารถระบุได้ด้วย

ส่วนมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ไม่ได้มีวัตถุประสงค์เพื่อมุ่งเน้นในการสืบสวนสอบสวนเพื่อนำตัวผู้กระทำความผิดมาลงโทษ แต่มุ่งเน้นในการรักษาไว้ซึ่งความปลอดภัยต่อหน่วยงานสารสนเทศที่สำคัญของประเทศเป็นหลัก ดังจะเห็นได้จากมาตรการที่มีความพิเศษซึ่งมีความแตกต่างจากมาตรการในกระบวนการยุติธรรมทางอาญาทั่วไป ไม่ว่าจะเป็นการกำหนดความร่วมมือระหว่างภาครัฐ และภาคเอกชนเพื่อดำเนินมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ การกำหนดห้ามมิให้นำข้อมูลซึ่งได้มาจากมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ไปใช้เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิด ดังที่ปรากฏอยู่ในมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศสิงคโปร์ กล่าวคือ กำหนดให้ใช้ข้อมูลได้เฉพาะเพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์เท่านั้น แต่ในประเทศไทยได้มีการกำหนดหลักเกณฑ์ที่แตกต่างออกไปเป็นอย่างมาก กล่าวคือ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศไทยกำหนดให้เจ้าหน้าที่รัฐสามารถนำข้อมูลที่ได้มาตามมาตรการพิเศษในการรักษาความมั่นคงปลอดภัยไซเบอร์ไปใช้เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายฉบับอื่นได้ ซึ่งปรากฏอยู่ในมาตรา 70 วรรคสอง ซึ่งเป็นข้อยกเว้นของหลักการเกี่ยวกับการห้ามมิให้นำข้อมูลไปใช้เพื่อประโยชน์อื่นนอกจากการรักษาความมั่นคงปลอดภัยไซเบอร์

เมื่อพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศไทยได้มีการกำหนดให้สามารถนำข้อมูลที่ได้มาตามมาตรการพิเศษในการรักษาความมั่นคงปลอดภัยไซเบอร์ไปใช้เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายฉบับอื่นได้ เนื่องจากบทบัญญัติดังกล่าวได้มีการเปลี่ยนแปลงหลักการทั่วไปเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งเป็นมาตรการที่มีความพิเศษแตกต่างจากมาตรการในกระบวนการยุติธรรมทางอาญาทั่วไป กลับกลายเป็นมาตรการที่ให้อำนาจแก่เจ้าหน้าที่รัฐในการแสวงหาพยานหลักฐาน โดยเฉพาะข้อมูลอันมีลักษณะเป็นพยานหลักฐานอิเล็กทรอนิกส์ ซึ่งเป็นข้อมูลที่ได้มาจากมาตรการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่นนี้ จึงจำเป็นที่จะต้องมีการกำหนดหลักเกณฑ์ที่เหมาะสมในการปฏิบัติตามบทบัญญัติดังกล่าว เนื่องจากมาตรการในการแสวงหาพยานหลักฐานเป็นมาตรการที่กระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน เพราะพยานหลักฐานอิเล็กทรอนิกส์ต่าง ๆ สามารถนำไปสู่การพิสูจน์การกระทำความผิดและลงโทษประชาชนได้ จึงควรมีการนำหลักการตรวจสอบการใช้อำนาจของ

เจ้าหน้าที่รัฐ และหลักการคุ้มครองสิทธิเสรีภาพของประชาชนต่าง ๆ มาประกอบการใช้อำนาจตามมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยที่มีลักษณะเป็นการให้อำนาจแก่เจ้าหน้าที่รัฐในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์

5.2 วิเคราะห์เปรียบเทียบมาตรการในการแสวงหาพยานหลักฐานในประเทศไทย

เมื่อพิจารณาบทบัญญัติในพระราชบัญญัติการรักษาความมั่นปลอดภัยไซเบอร์ ฯ สามารถแบ่งมาตรการในการแสวงหาพยานหลักฐานออกได้เป็น 2 ประการด้วยกัน ได้แก่ มาตรการในการแสวงหาพยานหลักฐานในกรณีของภัยคุกคามทางไซเบอร์ในระดับร้ายแรงและในระดับวิกฤติ โดยมีรายละเอียดดังนี้

(1) มาตรการในการแสวงหาพยานหลักฐานในกรณีของภัยคุกคามทางไซเบอร์ในระดับร้ายแรงได้ให้อำนาจแก่เจ้าหน้าที่รัฐในการมีหนังสือขอความร่วมมือให้บุคคลที่เกี่ยวข้องมาให้ข้อมูลหรือให้ส่งข้อมูลเป็นหนังสือ และการมีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของบุคคลใดเพื่อประโยชน์ในการดำเนินการ[209] ซึ่งมีลักษณะเป็นการขอความร่วมมือ อีกทั้งยังได้ให้อำนาจในการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์[210] ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ[211] ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ โดยในการเข้าถึงข้อมูลดังกล่าวจะต้องยื่นคำร้องต่อศาลโดยระบุเหตุอันควรเชื่อได้ว่ามีบุคคลใดบุคคลหนึ่งกำลังก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

เมื่อเปรียบเทียบกับมาตรการในการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 98 (2) จะเห็นได้ว่ามีความคล้ายคลึงกันเป็นอย่างมาก กล่าวคือ เป็นกรณีที่ต้องมีการยื่นคำร้องต่อศาลก่อนการดำเนินการ ไม่ว่าจะเป็นค้นตามประมวลกฎหมายวิธีพิจารณาความอาญา หรือการเข้าถึงข้อมูลคอมพิวเตอร์ต่าง ๆ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และในขณะที่ดำเนินการตามหมายนั้นได้พบเหตุที่กฎหมายกำหนดไว้ โดยตามประมวลกฎหมายวิธีพิจารณาความอาญาคือคือพบความผิดซึ่งหน้า กำหนดให้เจ้าหน้าที่รัฐสามารถทำการจับหรือยึดสิ่งของได้ ส่วนตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ได้กำหนดให้สามารถเปิดเผยหรือส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีตามความผิดอื่นได้

---

[209] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 62

[210] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 65 (5) และ 66 (2)

[211] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 66 (4)

(2) มาตรการในการแสวงหาพยานหลักฐานในกรณีของภัยคุกคามทางไซเบอร์ในระดับวิกฤติ กำหนดให้เจ้าหน้าที่ของรัฐมีอำนาจดำเนินการใด ๆ ได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าโดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากได้ดำเนินการไปแล้วให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว รวมถึงมีอำนาจขอข้อมูลที่เป็นปัจจุบันและต่อเนื่อง (Real Time) จากผู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์

เมื่อเปรียบเทียบกับมาตรการในการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 98 (2) จะเห็นได้ว่ามีความแตกต่างกัน กล่าวคือ มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในกรณีของภัยคุกคามทางไซเบอร์ในระดับวิกฤติไม่ได้มีการกำหนดให้เจ้าหน้าที่รัฐต้องยื่นคำร้องต่อศาลหรือดำเนินการใด ๆ อันลักษณะเป็นการตรวจสอบการใช้อำนาจก่อนแต่ประการใด โดยกำหนดเพียงให้แจ้งรายละเอียดการดำเนินการต่อศาลในภายหลังเท่านั้น

จากการศึกษาจะเห็นได้ว่า มาตรการแสวงหาพยานหลักฐานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์กับมาตรการในการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มีหลักการที่แตกต่างกันหลายประการด้วยกัน แสดงให้เห็นว่ามาตรการในการแสวงหาพยานหลักฐานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ไม่ได้เป็นไปตามหลักการและแนวความคิดของการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา โดยเป็นมาตรการที่มีลักษณะโน้มเอียงไปในทางของทฤษฎีการควบคุมอาชญากรรม (Crime control theory) มากกว่าทฤษฎีความชอบด้วยกระบวนการทางกฎหมาย (Due process theory) อย่างชัดเจน ซึ่งการที่บทบัญญัติของกฎหมายใดได้กำหนดมาตรการให้อำนาจแก่เจ้าหน้าที่รัฐอย่างกว้างขวางมากเกินไปย่อมส่งผลกระทบต่อสิทธิเสรีภาพของประชาชน โดยเฉพาะมาตรการในการแสวงหาพยานหลักฐานกรณีของภัยคุกคามไซเบอร์ในระดับวิกฤติ จึงสมควรที่จะมีการกำหนดหลักการเกี่ยวกับการตรวจสอบการใช้อำนาจ และการคุ้มครองสิทธิเสรีภาพของประชาชนมาประกอบเพื่อให้สอดคล้องกับหลักการในการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาอันเป็นหลักการพื้นฐานของกระบวนการยุติธรรมทางอาญาในประเทศไทย และเพื่อไม่ให้เป็นการให้อำนาจแก่เจ้าหน้าที่รัฐมากเกินไป อันอาจส่งผลกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนเกินสมควร

5.3 วิเคราะห์เปรียบเทียบมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในต่างประเทศ

มาตรการในการแสวงหาพยานหลักฐานเป็นมาตรการสำคัญในกระบวนการยุติธรรมทางอาญาอันมีวัตถุประสงค์เพื่อนำผู้กระทำความผิดมาลงโทษ โดยมาตรการในการแสวงหา

พยานหลักฐานเป็นมาตรการที่กระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนอย่างไม่สามารถหลีกเลี่ยงได้ ดังนั้น ในการใช้อำนาจของเจ้าหน้าที่รัฐเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานจึงจำเป็นต้องมีหลักการในการตรวจสอบการใช้อำนาจต่าง ๆ ของเจ้าหน้าที่รัฐเพื่อเป็นการคุ้มครองสิทธิเสรีภาพของประชาชนไม่ให้ถูกกระทบกระเทือนเกินสมควร

ประเทศสหรัฐอเมริกาได้วางหลักเกณฑ์เกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ไว้โดยเฉพาะ สามารถแบ่งออกไปเป็น 2 ประการด้วยกัน

(1) การค้นและยึดพยานหลักฐานอิเล็กทรอนิกส์โดยมีหมาย โดยทั่วไปแล้วเจ้าหน้าที่รัฐจะต้องขอหมายค้นจากศาลทุกกรณี เว้นแต่กรณีที่มีหลักเกณฑ์ของกฎหมายกำหนดไว้โดยชัดแจ้งว่าไม่จำต้องขอหมายค้นก่อนก็สามารถดำเนินการค้นไปได้ และในกรณีพิเศษ เมื่อมีเหตุการณ์บางอย่างเกิดขึ้น หลักเกณฑ์ของกฎหมายอาจกำหนดให้เจ้าหน้าที่รัฐสามารถทำการค้นสถานที่และยึดทรัพย์สินได้โดยไม่จำเป็นต้องขอหมายจากศาลก่อน แต่การดำเนินการดังกล่าวเจ้าหน้าที่รัฐจะต้องทราบถึงข้อเท็จจริง หรือพฤติการณ์ที่เกี่ยวข้องกับอาชญากรรม หรือข้อมูลเกี่ยวกับสิ่งของที่ต้องการยึด แล้วจึงพิจารณาว่าเหตุดังกล่าวเป็นกรณีพิเศษที่ถือว่ามีเหตุผลสมควรที่จะทำการค้นหรือยึดหรือไม่

ในการที่เจ้าหน้าที่รัฐจะมีคำร้องขอออกหมายค้นจะต้องยื่นคำร้องขอต่อศาล โดยหมายค้นจะต้องมีวัตถุประสงค์เพื่อพบสิ่งของหรือบุคคลซึ่งเป็นพยานหลักฐานในการกระทำความผิด มีไว้เป็นความผิด มีไว้เพื่อใช้ในการกระทำความผิด หรือเป็นบุคคลที่ต้องการจับกุม เป็นต้น ซึ่งหมายค้นจะต้องแสดงเหตุแห่งการค้นให้ศาลพิจารณาประกอบการตัดสินใจในการออกหมาย ซึ่งเหตุดังกล่าวอาจประกอบไปด้วย รายละเอียดของการกระทำความผิดอาญาที่เกิดขึ้นหรือกำลังจะเกิดขึ้น รายละเอียดของสถานที่ที่ต้องการตรวจค้น รายละเอียดของสิ่งของที่ต้องการยึด รายละเอียดของผู้ต้องสงสัยหรือบุคคลที่เกี่ยวข้อง เป็นต้น

ส่วนการขอออกหมายค้นสำหรับการค้นคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ต่าง ๆ มีหลักเกณฑ์ในการขอออกหมายค้นเช่นเดียวกับกรณีของการขอออกหมายค้นทั่วไป และจะต้องระบุถึงอุปกรณ์อิเล็กทรอนิกส์ซึ่งสร้างหรือจัดเก็บข้อมูลอิเล็กทรอนิกส์นั้น ๆ อยู่ ไม่ว่าจะอยู่ในรูปแบบใด หรือเรียกว่าอะไร รวมไปถึงรูปแบบของคอมพิวเตอร์หรือที่จัดเก็บข้อมูลอิเล็กทรอนิกส์ รูปแบบใด ๆ ของการทำด้วยมือ รูปแบบใด ๆ ทางกลไก และรูปแบบใด ๆ ของรูปถ่าย เป็นต้น

นอกจากการตรวจค้นข้อมูลอิเล็กทรอนิกส์ในคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ซึ่งจัดเก็บข้อมูลอิเล็กทรอนิกส์ไว้แล้ว เจ้าหน้าที่ตำรวจหรือพนักงานอัยการอาจขอให้ศาลออกหมายจำนวนมากในการตรวจค้นแบบเครือข่ายก็ได้ และในกรณีที่คอมพิวเตอร์เครื่องหนึ่งเกี่ยวข้องกับอาชญากรรมหลายประเภท ฮาร์ดไดรฟ์ของคอมพิวเตอร์เครื่องดังกล่าวที่เจ้าหน้าที่รัฐทำการยึดมาเพื่อตรวจสอบเกี่ยวกับการกระทำความผิดหนึ่ง อาจมีพยานหลักฐานเกี่ยวกับการกระทำความผิดอื่น ๆ ก็เป็นได้ ซึ่งเจ้าหน้าที่รัฐมีอำนาจแค่เฉพาะการค้นหาพยานหลักฐานในการกระทำความผิดตามหมายดังกล่าวเท่านั้น ในกรณีเช่นนี้ เจ้าหน้าที่รัฐจะต้องขอหมายเพื่อค้นหรือยึดอีกฉบับสำหรับพยานหลักฐานที่พบในภายหลัง

(2) การค้นและยึดพยานหลักฐานอิเล็กทรอนิกส์โดยไม่มีหมาย สามารถแบ่งออกได้เป็นหลายกรณี ดังต่อไปนี้

(2.1) การค้นและยึดโดยความยินยอม เจ้าหน้าที่รัฐอาจค้นสถานที่หรือวัตถุโดยไม่ต้องมีหมายค้นหรือแม้กระทั่งเหตุอันควรเชื่อ

(2.2) การค้นและยึดในสถานการณ์เร่งด่วน ซึ่งสถานการณ์เร่งด่วนนั้นเป็นข้อยกเว้นของการค้นโดยมีหมาย เจ้าหน้าที่รัฐจึงสามารถค้นและยึดโดยไม่มีหมายได้ในกรณีที่ถือว่าเป็นสถานการณ์เร่งด่วน เช่น พยานหลักฐานนั้นอยู่ในอันตรายที่ใกล้จะถึงจากการถูกทำลาย ประชาชนตกอยู่ในอันตรายที่ใกล้จะถึง เจ้าหน้าที่ตำรวจซึ่งอยู่ในระหว่างการไล่ล่าผู้ต้องสงสัย ผู้ต้องสงสัยน่าจะหลบหนีไปได้ก่อนที่เจ้าหน้าที่รัฐจะขอหมายค้นได้ เป็นต้น

(2.3) การค้นในเหตุการณ์ที่ทำการจับกุมโดยชอบด้วยกฎหมาย ในการจับกุมโดยชอบด้วยกฎหมายนั้น เจ้าหน้าที่รัฐสามารถทำการค้นบุคคลผู้ถูกจับได้ และรวมไปถึงการค้นหาพื้นที่โดยรอบบุคคลผู้ถูกจับได้โดยไม่ต้องมีหมาย

(2.4) หลักการเห็นได้โดยประจักษ์ โดยเจ้าหน้าที่รัฐต้องอยู่ในตำแหน่งหรือสถานที่ที่ชอบด้วยกฎหมายในการสังเกตและเข้าถึงพยานหลักฐาน และเบาะแสดังกล่าวจะต้องปรากฏอย่างชัดเจนในขณะนั้น

(2.5) การค้นในสถานที่จัดเก็บ เจ้าหน้าที่รัฐซึ่งบังคับใช้กฎหมายจะทำการเก็บสิ่งของซึ่งยึดได้มาเป็นประจำ โดยการค้นสิ่งของดังกล่าวต่อไปนี้จะเรียกว่า “การค้นในสถานที่จัดเก็บ” การ

ค้นในสถานที่จัดเก็บเหล่านี้ย่อมสมเหตุสมผลและอยู่ภายใต้ข้อยกเว้นของการค้นโดยไม่ต้องมีหมายศาล แต่ต้องไม่ใช่เพื่อวัตถุประสงค์ในการสอบสวน

(2.6) การค้นบริเวณชายแดน การค้นตามปกติ ณ บริเวณชายแดนนั้นไม่จำเป็นต้องมีหมาย เหตุอันควรเชื่อ หรือแม้กระทั่งเหตุอันควรสงสัย แต่การค้นที่ล่วงล้ำโดยเฉพาะเจาะจงอย่างน้อยจะต้องมีเหตุอันควรสงสัย

(2.7) การคุมประพฤติและการได้รับทัณฑ์บน บุคคลที่ถูกคุมประพฤติ ได้รับทัณฑ์บนหรือได้รับการปล่อยตัวภายใต้การดูแลย่อมได้รับความคาดหวังในความเป็นส่วนตัวที่น้อยลงจากบุคคลทั่วไป และอาจถูกค้นได้โดยไม่ต้องมีหมายขึ้นอยู่กับเหตุอันควรสงสัย หรือความเป็นไปได้โดยไม่ต้องมีความสงสัยโดยเฉพาะเจาะจง

ส่วนในประเทศสิงคโปร์ได้มีการกำหนดมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศสิงคโปร์ โนในการแสวงหาพยานหลักฐานต่าง ๆ หากเจ้าหน้าที่ตำรวจเห็นว่าเอกสารหรือสิ่งใดจำเป็นสำหรับการสอบสวน การพิจารณา หรือการดำเนินการใด ๆ ตามประมวลกฎหมายวิธีพิจารณาความอาญา เจ้าหน้าที่ตำรวจอาจออกคำสั่งเป็นหนังสือให้บุคคลซึ่งครอบครอง หรือมีอำนาจในเอกสารหรือสิ่งใดจัดทำเอกสารส่งหรือสิ่งดังกล่าวให้แก่เจ้าหน้าที่ตำรวจ หรือให้อำนาจแก่เจ้าหน้าที่ตำรวจในการเข้าถึงข้อมูลเหล่านั้น หากเอกสารหรือสิ่งเหล่านั้นถูกจัดเก็บอยู่ในคอมพิวเตอร์หรือเข้าถึงได้โดยอาศัยคอมพิวเตอร์เท่านั้น เจ้าหน้าที่ตำรวจอาจออกคำสั่งเป็นหนังสือเพื่อใช้อำนาจเช่นเดียวกันได้ ศาลจะออกหมายค้นให้แก่เจ้าหน้าที่ตำรวจในกรณีที่บุคคลที่ได้รับคำสั่งเป็นหนังสือจากเจ้าหน้าที่ตำรวจไม่ปฏิบัติตามคำสั่ง หรือในกรณีที่ไม่ทราบว่าบุคคลใดเป็นผู้ครอบครองเอกสารหรือสิ่งเหล่านั้น หรืออาจออกหมายเรียกเพื่อให้บุคคลที่ได้รับคำสั่งมาตามหมายเรียก เป็นต้น โดยในหมายค้นจะต้องระบุชื่อของเจ้าหน้าที่ผู้ดำเนินการตามหมายคนเดียวหรือหลายคนแล้วแต่กรณี ไม่ว่าจะเป็นเจ้าหน้าที่ตำรวจหรือบุคคลใดที่ศาลเห็นสมควร หากศาลเห็นว่าเหมาะสมอาจระบุสถานที่โดยเฉพาะเจาะจงสำหรับการค้นหา หรือตรวจสอบ และระบุบุคคลที่ถูกตั้งข้อหาที่จะดำเนินการตามหมายเพื่อค้นหรือตรวจสอบในสถานที่เฉพาะเจาะจง สำหรับการยึดเจ้าหน้าที่ตำรวจอาจยึด ห้ามไม่ให้กำจัด หรือซื้อขายทรัพย์สินใด ๆ ในกรณีที่ทรัพย์สินดังกล่าวได้ใช้ในการกระทำความผิด ในกรณีที่สงสัยว่าจะใช้หรือมีการใช้ทรัพย์สินดังกล่าวในการกระทำความผิด หรือทรัพย์สินซึ่งต้องสงสัยว่าเป็นพยานหลักฐานในการกระทำความผิด ซึ่งเจ้าหน้าที่ตำรวจสามารถดำเนินการไปโดยใช้ดุลพินิจของตนเองได้โดยไม่ต้องขอหมายค้นจากศาลแต่อย่างใด นอกจากมาตรการข้างต้นแล้ว ประเทศสิงคโปร์ยังได้กำหนดมาตรการในกรณีของ

อำนาจในการเข้าถึงคอมพิวเตอร์ไว้โดยเฉพาะด้วย โดยเจ้าหน้าที่รัฐสามารถเข้าถึง ตรวจสอบ ใช้ ป้องกันไม่ให้บุคคลอื่นเข้าถึง ซึ่งคอมพิวเตอร์ของผู้ถูกจับกุมได้

และในรัฐควีนส์แลนด์ เครือรัฐออสเตรเลีย ได้มีการกำหนดมาตรการในการแสวงหาพยานหลักฐานไว้โดยเฉพาะในพระราชบัญญัติอำนาจหน้าที่ของเจ้าหน้าที่ตำรวจ ฯ สำหรับการค้นสถานที่โดยมีหมายค้น นอกจากเจ้าหน้าที่ตำรวจจะสามารถทำการตรวจค้นสถานที่ได้แล้ว หมายค้นอาจมีคำสั่งที่เกี่ยวข้องกับข้อมูลที่ได้จากอุปกรณ์ดิจิทัลในสถานที่ที่ถูกทำการตรวจค้น บุคคลที่เกี่ยวข้องจะต้องให้เจ้าหน้าที่ตำรวจเข้าถึงอุปกรณ์ดิจิทัลและข้อมูลต่าง ๆ ในอุปกรณ์ดิจิทัล เรียกชุดข้อมูลเพื่อการเข้าถึงข้อมูลในอุปกรณ์ดิจิทัลดังกล่าว รวมไปถึงให้เจ้าหน้าที่ตำรวจทำการตรวจสอบ ทำสำเนา แปลงรูปแบบข้อมูลดิจิทัล ให้เจ้าหน้าที่ตำรวจสามารถเข้าใจข้อมูลได้ โดยการที่เจ้าหน้าที่ตำรวจจะขอออกหมายค้นต่อศาลท้องถิ่นหรือศาลสูงเพื่อดำเนินการในการค้นอุปกรณ์ดิจิทัลต่าง ๆ นั้น จะต้องมีเหตุอันควรเชื่อที่จะสงสัยว่าจะพบพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิด วัตถุที่ต้องห้ามจากการเข้าทำการตรวจค้นในสถานที่นั้น หรืออาจถูกนำไปไว้ในสถานที่นั้นภายใน 72 ชั่วโมง นอกจากนี้ เจ้าหน้าที่ตำรวจยังมีอำนาจในการเก็บข้อมูลอุปกรณ์ดิจิทัลที่พบในสถานที่เกิดเหตุ หรือถูกยึดจากสถานที่เกิดเหตุได้ด้วย โดยคำสั่งที่อนุญาตให้เจ้าหน้าที่ตำรวจดำเนินการดังกล่าวจะต้องมีเหตุอันควรเชื่อที่จะสงสัยว่าจะพบพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดด้วยเช่นเดียวกัน

โดยกรณีของมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของต่างประเทศสามารถแบ่งพิจารณาออกได้เป็น มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยมีหมาย และโดยไม่มีหมาย โดยมีรายละเอียดตามตารางต่อไปนี้

ตารางที่ 4 : ตารางเปรียบเทียบมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยมีหมายและโดยไม่มีหมายในประเทศไทยและต่างประเทศ

ประเทศ	มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยมีหมาย	มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยไม่มีหมาย
ประเทศสหรัฐอเมริกา	ปรากฏอยู่ในคำพิพากษาของศาลและบทบัญญัติอื่นที่เกี่ยวข้อง โดยแบ่งออกเป็นกรณีทั่วไป และกรณีพิเศษ	(1) การค้นและยึดโดยความยินยอม (2) การค้นและยึดในสถานการณ์เร่งด่วน (3) การค้นในเหตุการณ์ที่ทำการจับกุมโดยชอบด้วยกฎหมาย (4) การค้นภายใต้หลักการเห็นได้โดยประจักษ์ (5) การค้นในสถานที่จัดเก็บ (6) การค้นบริเวณชายแดน (7) การค้นบุคคลซึ่งถูกคุมประพฤติและการได้รับทัณฑ์บน
ประเทศสิงคโปร์	ปรากฏอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศสิงคโปร์ ศาลจะออกหมายค้นให้แก่เจ้าหน้าที่ตำรวจในกรณีที่บุคคลที่ได้รับคำสั่งเป็นหนังสือจากเจ้าหน้าที่ตำรวจไม่ปฏิบัติตามคำสั่ง หรือในกรณีที่ไม่ทราบว่าบุคคลใดเป็นผู้ครอบครองเอกสารหรือสิ่งเหล่านั้น หรืออาจออกหมายเรียกเพื่อให้บุคคลที่ได้รับคำสั่งมาตามหมายเรียก เป็นต้น	ปรากฏอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศสิงคโปร์ ในกรณีที่เจ้าหน้าที่ตำรวจเห็นว่าเอกสารหรือสิ่งใด ๆ จำเป็น หรือน่าพึงพอใจ สำหรับการสอบสวน การพิจารณา หรือการดำเนินการใด ๆ ตามประมวลกฎหมายวิธีพิจารณาความอาญานี้ เจ้าหน้าที่ตำรวจอาจออกคำสั่งเป็นหนังสือให้บุคคลซึ่งครอบครอง หรือมีอำนาจในเอกสาร หรือสิ่งใดจัดทำเอกสารส่งหรือสิ่งดังกล่าวให้แก่เจ้าหน้าที่ตำรวจ หรือให้อำนาจแก่

		เจ้าหน้าที่ตำรวจในการเข้าถึงข้อมูลเหล่านั้น หากเอกสารหรือสิ่งเหล่านั้นถูกจัดเก็บอยู่ในคอมพิวเตอร์หรือเข้าถึงได้โดยอาศัยคอมพิวเตอร์เท่านั้น เจ้าหน้าที่ตำรวจอาจออกคำสั่งเป็นหนังสือเพื่อใช้อำนาจเช่นเดียวกันได้
เครือรัฐออสเตรเลีย รัฐควีนส์แลนด์	ปรากฏอยู่ในพระราชบัญญัติอำนาจหน้าที่ของเจ้าหน้าที่ตำรวจ ค.ศ. 2020 โดยหมายค้นอาจมีคำสั่งที่เกี่ยวข้องกับข้อมูลที่ได้จากอุปกรณ์ดิจิทัลในสถานที่ที่ถูกทำการตรวจค้น บุคคลที่เกี่ยวข้องจะต้องให้เจ้าหน้าที่ตำรวจเข้าถึงอุปกรณ์ดิจิทัลและข้อมูลต่าง ๆ ในอุปกรณ์ดิจิทัล เรียกชุดข้อมูลเพื่อการเข้าถึงข้อมูลในอุปกรณ์ดิจิทัลดังกล่าว รวมไปถึงให้เจ้าหน้าที่ตำรวจทำการตรวจสอบ ทำสำเนา แปลงรูปแบบข้อมูลดิจิทัล ให้เจ้าหน้าที่ตำรวจสามารถเข้าใจข้อมูลได้ และอุปกรณ์ดิจิทัลที่พบในสถานที่เกิดเหตุหรือถูกยึดจากสถานที่เกิดเหตุ บุคคลที่เกี่ยวข้องจะต้องให้เจ้าหน้าที่ตำรวจเข้าถึงอุปกรณ์ดิจิทัลและข้อมูลในอุปกรณ์ดิจิทัล ให้ชุดข้อมูลเพื่อเข้าถึงข้อมูลในอุปกรณ์ดิจิทัล รวมถึงให้ตรวจสอบ ทำสำเนา หรือแปลงรูปแบบข้อมูลดิจิทัลให้เจ้าหน้าที่ตำรวจสามารถเข้าใจข้อมูลได้ โดยจะมีคำสั่งดังกล่าวได้ต่อเมื่อมีเหตุอันควรเชื่อที่จะสงสัยว่าจะพบพยานหลักฐานที่เกี่ยวข้องกับการ	ไม่มีการกำหนดมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยไม่มีหมาย

	กระทำความผิด	

นอกจากนี้ยังสามารถเปรียบเทียบหลักการเกี่ยวกับการขอหมายค้นตามมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของต่างประเทศ ซึ่งสามารถแบ่งพิจารณาออกเป็นเหตุแห่งการขอหมายค้น และรายละเอียดที่ต้องระบุในการขอหมายค้น โดยมีรายละเอียดตามตารางต่อไปนี้

ตารางที่ 5 : ตารางเปรียบหลักเกณฑ์เกี่ยวกับการขอหมายค้นในประเทศไทยและต่างประเทศ

ประเทศ	**เหตุแห่งการขอหมายค้น**	**รายละเอียดที่ต้องระบุในการขอหมายค้น**
ประเทศสหรัฐอเมริกา	เพื่อพบพยานหลักฐานในการกระทำความผิด เพื่อพบสิ่งของซึ่งมีไว้เป็นความผิด สิ่งของซึ่งได้จากการกระทำความผิด หรือสิ่งของอื่นใดที่ครอบครองโดยผิดกฎหมาย เพื่อพบทรัพย์ที่ทำไว้ หรือมีไว้เพื่อใช้ในการกระทำความผิด หรือใช้ในการกระทำความผิด เพื่อพบบุคคลที่ต้องการจับกุม หรือบุคคลที่ถูกหน่วงเหนี่ยวกักขังโดยไม่ชอบด้วยกฎหมาย	ต้องระบุรายละเอียดเกี่ยวกับสิ่งที่ต้องการค้นหรือยึด โดยจะต้องระบุรายละเอียดต่าง ๆ เช่นเดียวกับการขอหมายค้นหรือยึดในกรณีทั่วไป ไม่ว่าจะเป็นรายละเอียดของการกระทำความผิดอาญาที่เกิดขึ้นหรือกำลังจะเกิดขึ้น รายละเอียดของสถานที่ที่ต้องการตรวจค้น รายละเอียดของสิ่งของที่ต้องการยึด รายละเอียดของผู้ต้องสงสัยหรือบุคคลที่เกี่ยวข้อง เป็นต้น และจะต้องระบุถึงอุปกรณ์อิเล็กทรอนิกส์ซึ่งสร้างหรือจัดเก็บข้อมูลอิเล็กทรอนิกส์นั้น ๆ อยู่ ไม่ว่าจะอยู่ในรูปแบบใด หรือเรียกว่าอะไร รวมไปถึงรูปแบบของคอมพิวเตอร์หรือที่จัดเก็บข้อมูลอิเล็กทรอนิกส์ (เช่น ฮาร์ดดิสก์หรืออุปกรณ์ที่สามารถจัดเก็บข้อมูลดังกล่าวได้) รูปแบบใด ๆ ของการทำด้วยมือ (เช่น การเขียน วาดภาพ ระบายสี) รูปแบบใด ๆ ทางกลไก (เช่น การพิมพ์หรือตีพิมพ์) และรูปแบบใด ๆ ของรูปถ่าย (เช่น ไมโครฟิล์ม ไมโครฟิช ภาพพิมพ์

		สไลด์ ฟิล์มขาวดำ วิดีโอเทป ภาพถ่าย เคลื่อนไหว) เป็นต้น
ประเทศสิงคโปร์	ศาลจะออกหมายค้นให้แก่เจ้าหน้าที่ตำรวจในกรณีที่บุคคลที่ได้รับคำสั่งเป็นหนังสือจากเจ้าหน้าที่ตำรวจไม่ปฏิบัติตามคำสั่ง หรือในกรณีที่ไม่ทราบว่าบุคคลใดเป็นผู้ครอบครองเอกสารหรือสิ่งเหล่านั้น หรืออาจออกหมายเรียกเพื่อให้บุคคลที่ได้รับคำสั่งมาตามหมายเรียก	ในหมายค้นจะต้องระบุชื่อของเจ้าหน้าที่ผู้ดำเนินการตามหมายคนเดียวหรือหลายคนแล้วแต่กรณี ไม่ว่าจะเป็นเจ้าหน้าที่ตำรวจหรือบุคคลใดที่ศาลเห็นสมควร หากศาลเห็นว่าเหมาะสมอาจระบุสถานที่โดยเฉพาะเจาะจงสำหรับการค้นหา หรือตรวจสอบ และระบุบุคคลที่ถูกตั้งข้อหาที่จะดำเนินการตามหมายเพื่อค้นหรือตรวจสอบในสถานที่เฉพาะเจาะจงดังกล่าว และศาลจะต้องกำหนดจำนวนวันที่หมายค้นดังกล่าวจะมีผลบังคับใช้
เครือรัฐออสเตรเลีย รัฐควีนส์แลนด์	เพื่อให้ได้มาซึ่งพยานหลักฐานที่อาจจะเป็นพยานหลักฐานที่เกิดขึ้นในขณะที่กระทำความผิด หรือที่อาจได้มาจากพยานหลักฐานที่ยึดมาจากการค้น หรืออาจเป็นยานพาหนะ หรือทรัพย์สินอื่นที่เจ้าหน้าที่ตำรวจเชื่อว่าจะสามารถใช้เป็นพยานหลักฐานที่อาจใช้พิสูจน์ถึงกากระทำความผิดได้	พยานหลักฐาน ทรัพย์สิน หรือสิ่งของต้องห้ามดังกล่าวที่ต้องเข้าทำการตรวจค้นมีเหตุอันควรเชื่อที่จะสงสัยอยู่ ณ สถานที่นั้น หรืออาจจะถูกนำมาอยู่ในสถานที่นั้นภายใน 72 ชั่วโมง

สำหรับประเด็นในเรื่องของการเปรียบเทียบมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในต่างประเทศกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ เมื่อพิจารณามาตรการของต่างประเทศแล้วจะเห็นได้ว่าล้วนแล้วแต่มีการนำหลักการเกี่ยวกับหมายค้นอันเป็นหลักการในการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐโดยองค์กรตุลาการมาประกอบการใช้อำนาจเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ทั้งสิ้น โดยอาจมีรายละเอียดที่แตกต่างกันไปในแต่ละประเทศ

ประเทศสหรัฐอเมริกามีการกำหนดมาตรการเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ไว้อย่างชัดเจนทั้งกรณีที่ต้องทำการค้นโดยมีหมายค้น และกรณีที่สามารถทำการค้นได้โดยไม่ต้องมีหมายค้น และได้มีการระบุเหตุแห่งการออกหมายค้น และรายละเอียดที่ต้องระบุไว้ในหมายค้น ซึ่งหลักการทั่วไปเช่นเดียวกับหลักการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาของไทย อย่างไรก็ตามในกรณีของการค้นโดยไม่มีหมายนั้น หากเปรียบเทียบหลักการในกรณีการค้นภายใต้หลักการเห็นได้โดยประจักษ์ (Plain view) กับการค้นตามมาตรา 98 (2) นั้นมีความคล้ายคลึงกันเป็นอย่างมาก โดยมีสาระสำคัญดังต่อไปนี้

การค้นภายใต้หลักการเห็นได้โดยประจักษ์ เป็นข้อยกเว้นในการค้นที่ต้องมีหมายศาล ในการอาศัยข้อยกเว้นดังกล่าวนี้ เจ้าหน้าที่รัฐจะต้องอยู่ในตำแหน่งหรือสถานที่ที่ชอบด้วยกฎหมายในการสังเกตและเข้าถึงพยานหลักฐาน และเบาะแสดังกล่าวจะต้องปรากฏอย่างชัดเจนในขณะนั้น ซึ่งการปรากฏอย่างชัดเจนได้มีการวางหลักว่า อาจหมายถึง ชื่อของไฟล์ที่มีความเกี่ยวข้องกับภาพลามกอนาจารเด็ก หรือมีชื่อไฟล์ที่ไม่เหมาะสมในทางเพศ เป็นต้น สำหรับข้อปฏิบัติในการค้นภายใต้หลักการเห็นได้โดยประจักษ์ ถือว่าเมื่อได้มีการค้นส่วนหนึ่งส่วนใดของคอมพิวเตอร์ หรืออุปกรณ์จัดเก็บข้อมูลโดยไม่มีหมายแล้ว จำเลยย่อมไม่ได้รับการสงวนไว้ซึ่งความคาดหวังในความเป็นส่วนตัวที่สมเหตุสมผล (Reasonable Expectation of Privacy) ในเนื้อหาที่เหลือของคอมพิวเตอร์หรืออุปกรณ์จัดเก็บข้อมูลได้อีกต่อไป

เมื่อพิจารณาเปรียบเทียบกับมาตรการในการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 98 (2) ในกรณีของการค้นได้โดยไม่มีหมาย หากในขณะทำการค้นตามเหตุอย่างหนึ่งแล้วพบเหตุเกี่ยวกับกรณีของความผิดซึ่งหน้า เช่น ขณะที่เจ้าหน้าที่รัฐตรวจค้นยาเสพติดตามหมายค้นของศาลภายในบ้านของจำเลย พบอาวุธปืนไม่มีทะเบียนซุกซ่อนภายในบ้าน แม้หมายค้นจะระบุให้ค้นหายาเสพติด แต่การครอบครองอาวุธปืนไม่มีทะเบียนก็เป็นความผิดซึ่งหน้า เจ้าหน้าที่รัฐย่อมมีอำนาจจับกุมจำเลยได้ และสามารถยึดอาวุธปืนดังกล่าวได้ด้วย[212] จากตัวอย่างข้างต้น จะเห็นได้ว่าในการค้นเคหสถาน เจ้าหน้าที่รัฐย่อมสามารถค้นส่วนใดส่วนหนึ่งของเคหสถานได้โดยอาศัยอำนาจตามหมายค้น หากขณะดำเนินการค้นพอเหตุเกี่ยวกับความผิดซึ่งหน้า เจ้าหน้าที่รัฐย่อมมีอำนาจในการทำการยึดและจับกุมได้ ซึ่งมีหลักการเช่นเดียวกับการค้นภายใต้หลักการเห็นได้

---

[212] สหรัฐ กิติ ศุภกร, หลักและคำพิพากษา : กฎหมายวิธีพิจารณาความอาญา, พิมพ์ครั้งที่ 14, บรรณาธิการ, (กรุงเทพมหานคร: บริษัท อมรินทร์พริ้นติ้งแอนด์พับบลิชชิ่ง จำกัด (มหาชน), 2565), หน้า 357.

โดยประจักษ์ แสดงให้เห็นถึงความสอดคล้องของแนวความคิดเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานของประเทศไทยและประเทศสหรัฐอเมริกาอย่างชัดเจน

เมื่อพิจารณาเปรียบเทียบกับมาตราการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์จะเห็นได้ว่ามีความแตกต่างกันอยู่ เบื้องต้นเจ้าหน้าที่รัฐที่จะทำการค้นโดยไม่มีหมายภายใต้หลักการเห็นได้โดยประจักษ์ (Plain view) จะต้องมีอำนาจในการเข้าตรวจค้นตามหมายซึ่งได้มีการอนุมัติจากศาลก่อน แล้วในขณะค้นได้พบเจอข้อมูลอื่นใดที่เป็นความผิดอีก โดยมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในกรณีของภัยคุกคามทางไซเบอร์ในระดับร้ายแรงก็มีหลักการที่คล้ายคลึงกัน กล่าวคือ ในการที่เจ้าหน้าที่รัฐจะทำการเข้าถึงข้อมูลต่าง ๆ ภายในคอมพิวเตอร์ จะต้องมีการยื่นคำร้องต่อศาลโดยระบุเหตุตามที่กำหนดไว้เพื่อให้ศาลมีคำสั่งอนุญาตให้ทำการเข้าถึงได้เสียก่อน เมื่อเจ้าหน้าที่รัฐได้เข้าถึง หรือได้ทำการยึดคอมพิวเตอร์ดังกล่าวมาตรวจสอบ ภายหลังพบเจอข้อมูลที่ผิดกฎหมาย กรณีเช่นนี้ย่อมเป็นไปตามหลักการเดียวกับการค้นโดยไม่มีหมายภายใต้หลักการเห็นได้โดยประจักษ์

อย่างไรก็ตาม มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในกรณีของภัยคุกคามไซเบอร์ในระดับวิกฤติไม่ได้มีการกำหนดขั้นตอนในยื่นคำร้องต่อศาลก่อนดำเนินการแต่อย่างใด คงกำหนดแต่เพียงว่าให้เจ้าหน้าที่รัฐดำเนินการใด ๆ ไปก่อน และภายหลังจากดำเนินการจึงแจ้งรายละเอียดของการดำเนินการแก่ศาล ซึ่งมาตรการดังกล่าวไม่ได้เป็นไปตามหลักการค้นโดยไม่มีหมายภายใต้หลักการเห็นได้โดยประจักษ์ เนื่องจากในการใช้อำนาจนั้น ไม่ได้มีการตรวจสอบการใช้อำนาจโดยองค์กรตุลาการเลย กรณีของข้อมูลต่าง ๆ ที่ได้มาภายใต้มาตรการในการแสวงหาพยานหลักฐานกรณีของภัยคุกคามทางไซเบอร์ในระดับวิกฤติ จึงไม่สมควรที่จะสามารถเปิดเผยหรือส่งมอบเพื่อประโยชน์ในการดำเนินคดีต่อผู้กระทำความผิดตามกฎหมายอื่นได้

รัฐควีนส์แลนด์ เครือรัฐออสเตรเลีย ได้มีการกำหนดมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยมีหมายเอาไว้อย่างชัดเจน แต่ไม่ได้มีการกำหนดในกรณีของการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยไม่มีหมายเอาไว้ นอกจากนี้ยังได้กำหนดเหตุแห่งการขอออกหมายค้นอย่างชัดเจนเช่นเดียวกัน และการขอออกหมายค้นเจ้าหน้าที่รัฐจะต้องระบุรายละเอียดต่าง ๆ ที่กฎหมายกำหนดไว้ ซึ่งมาตรการข้างต้นมีความคล้ายคลึงกับมาตรการในการแสวงหาพยานหลักฐานในกรณีที่ต้องมีหมายตามประมวลกฎหมายวิธีพิจารณาความอาญาของไทย จึงมีขอบเขตของการให้อำนาจแก่เจ้าหน้าที่รัฐในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ที่แคบกว่ามาตรการในการ

แสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศไทย

ส่วนในประเทศสิงคโปร์นั้น ดังที่ได้กล่าวไปแล้วว่าหลักการในการแสวงหาพยานหลักฐานของประเทศสิงคโปร์มีความแตกต่างจากหลักการทั่วไป โดยในเบื้องต้นจะอาศัยหลักความยินยอมในการขอข้อมูลจากประชาชน หากประชาชนไม่ยินยอมจึงค่อยมีการยื่นเพื่อขอหมายต่อศาล แต่ก็ได้มีข้อกำหนดเกี่ยวกับรายละเอียดที่ต้องระบุไว้ในการขอหมายค้นอย่างละเอียดและชัดเจนเช่นเดียวกันกับในประเทศอื่น ๆ โดยที่มาตรการของประเทศสิงคโปร์ไม่ปรากฏเหตุแห่งการขอหมายค้นดังเช่นในประเทศไทย ประเทศสหรัฐอเมริกา หรือรัฐควีนส์แลนด์ เครือรัฐออสเตรเลีย เนื่องจากมาตรการในการแสวงหาพยานหลักฐานโดยทั่วไปของประเทศสิงคโปร์นั้นเริ่มต้นจากการมีคำสั่งโดยเจ้าหน้าที่ตำรวจ แล้วจึงดำเนินการขอหมายจากศาลในกรณีที่บุคคลดังกล่าวไม่ดำเนินการตามคำสั่งของเจ้าหน้าที่ตำรวจ

จากการศึกษาจะเห็นได้ว่า มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในประเทศสหรัฐอเมริกา และเครือรัฐออสเตรเลีย รัฐควีนส์แลนด์ เครือรัฐออสเตรเลีย ได้ยืนยันหลักการที่สำคัญเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐาน ซึ่งก็คือหลักการตรวจสอบการใช้อำนาจโดยองค์กรตุลาการผ่านการขอหมายค้นจากศาล โดยเจ้าหน้าที่รัฐจะทำการค้นโดยไม่มีหมายได้ก็แต่กรณีที่มีบทบัญญัติโดยชัดแจ้งให้กระทำได้เท่านั้น ซึ่งกรณีของข้อยกเว้นที่ทำการค้นได้โดยไม่มีหมายมักจะเป็นกรณีที่เจ้าหน้าที่รัฐสามารถเห็นหรือเข้าถึงการกระทำความผิดหรือทรัพย์ซึ่งมีไว้เป็นความผิดได้โดยง่าย ดังเช่นข้อยกเว้นที่ปรากฏอยู่ในมาตรการในการแสวงหาพยานหลักฐานโดยไม่มีหมายค้นของประเทศสหรัฐอเมริกา รวมถึงมาตรการในการแสวงหาพยานหลักฐานโดยไม่มีหมายค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาของไทย เนื่องจากมาตรการในการแสวงหาพยานหลักฐานเป็นมาตรการที่กระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน การที่เจ้าหน้าที่รัฐจะใช้อำนาจดังกล่าวจึงจำเป็นที่จะต้องมีการตรวจสอบการใช้อำนาจเสียก่อน ซึ่งมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศไทยในกรณีของภัยคุกคามในระดับร้ายแรงที่แม้จะมีการกำหนดให้ต้องยื่นคำร้องต่อศาลการดำเนินการต่าง ๆ อันเป็นการกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน แต่ก็มีช่องว่างที่ทำให้มีความแตกต่างจากกรณีของการค้นโดยไม่มีหมายที่ปรากฏอยู่ในมาตรการของประเทศต่าง ๆ อย่างชัดเจน กล่าวคือ ณ เวลาที่เจ้าหน้าที่รัฐได้ไปซึ่งคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ อาจไม่ทราบถึงการมีอยู่ของข้อมูลที่เกี่ยวข้องกับการกระทำความผิดอื่นซึ่งไม่มีความเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

เลยก็ได้ แต่เจ้าหน้าที่รัฐก็สามารถได้ไปซึ่งข้อมูลดังกล่าว และภายหลังหากมีการทำการตรวจค้นคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์แล้วข้อมูลเกี่ยวกับการกระทำความผิดอื่นดังกล่าว ก็สามารถเปิดเผยหรือส่งมอบเพื่อประโยชน์ในการดำเนินคดีอื่น ๆ ได้

นอกจากนี้เมื่อพิจารณามาตรการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยไม่มีหมายของประเทศสหรัฐอเมริกา ในกรณีของการค้นโดยไม่มีหมายภายใต้หลักการเห็นได้โดยประจักษ์ (Plain view) ซึ่งมีหลักการ แนวคิด รวมไปถึงข้อกำหนดในทางปฏิบัติที่มีลักษณะคล้ายคลึงกับมาตรการในการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศไทยเป็นอันมาก ผู้เขียนจึงเห็นควรให้มีการนำหลักการค้นโดยไม่มีหมายภายใต้หลักการเห็นได้โดยประจักษ์มาเป็นหลักเกณฑ์ประกอบการใช้มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศไทย

บทที่ 6
บทสรุปและข้อเสนอแนะ

6.1 บทสรุป

มาตรการในการแสวงหาพยานหลักฐานเป็นมาตรการที่กระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน แม้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จะไม่ได้มีวัตถุประสงค์เพื่อการสืบสวนสอบสวนดังเช่นมาตรการทางอาญาอื่น ๆ แต่เมื่อพิจารณาจากบทบัญญัติในมาตรา 70 ที่กำหนดว่า “กำหนดให้สามารถเปิดเผยหรือส่งมอบข้อมูลต่าง ๆ เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่นได้” ทำให้มาตรการต่าง ๆ ที่ได้ไปซึ่งข้อมูลอิเล็กทรอนิกส์มีลักษณะเป็นมาตรการที่ให้อำนาจแก่เจ้าหน้าที่รัฐในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ เมื่อมาตรการในการแสวงหาพยานหลักฐานเป็นมาตรการที่กระทบกระเทือนต่อสิทธิเสรีภาพของประชาชน จึงควรที่จะได้มีการนำหลักการในการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐและหลักการคุ้มครองสิทธิเสรีภาพของประชาชนต่าง ๆ มาประกอบการใช้อำนาจ

วัตถุประสงค์ในการกำหนดมาตรการในการรักษาความปลอดภัยไซเบอร์ในต่างประเทศรวมถึงประเทศไทย ล้วนแล้วแต่มีวัตถุประสงค์ไปในทิศทางเดียวกัน คือ เพื่อรักษาความมั่นคงปลอดภัยในโลกไซเบอร์ โดยจะกำหนดหน้าที่แก่หน่วยงานโครงสร้างพื้นฐานที่สำคัญของประเทศไม่ว่าจะเป็นหน่วยงานรัฐหรือหน่วยงานเอกชนก็ตาม ให้รายงานภัยคุกคามไซเบอร์ที่ตนทราบแก่หน่วยงานรัฐ และกำหนดหน้าที่ในการพัฒนามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ต่าง ๆ ให้ต้องดำเนินการตามกรอบหรือแนวทางด้วย ซึ่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ก็ได้มีการบัญญัติขึ้นโดยมีวัตถุประสงค์เช่นเดียวกันกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศอื่น ๆ

มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์สามารถแบ่งออกได้เป็น 2 ลักษณะด้วยกัน ได้แก่ มาตรการที่เป็นความร่วมมือระหว่างภาครัฐและเอกชน โดยกำหนดหน้าที่เบื้องต้นแก่หน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญภายในประเทศเพื่อพัฒนาแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศร่วมกัน และมาตรการที่ให้อำนาจแก่เจ้าหน้าที่รัฐในการเข้าถึงข้อมูลต่าง ๆ ของประชาชนเพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยไซเบอร์ ซึ่งประเทศไทยได้มีการ

กำหนดมาตรการไปในลักษณะที่เป็นการให้อำนาจแก่เจ้าหน้าที่รัฐในการดำเนินการเป็นหลัก โดยให้อำนาจในการเข้าถึงข้อมูลตามหลักเกณฑ์ต่าง ๆ ที่ปรากฏอยู่ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ

จากการศึกษาวัตถุประสงค์และมาตรการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในประเทศไทยและประเทศต่าง ๆ ทำให้เห็นว่ามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์มีลักษณะที่แตกต่างจากมาตรการในกระบวนการยุติธรรมทางอาญาทั่วไป กล่าวคือ มาตรการในกระบวนการยุติธรรมทางอาญาทั่วไปเป็นกระบวนการที่มุ่งเน้นในการนำตัวผู้กระทำความผิดมาลงโทษ ดังนั้น ในกระบวนการยุติธรรมทางอาญาจึงมีการกำหนดมาตรการในการสืบสวนและสอบสวนไว้เพื่อให้เจ้าหน้าที่รัฐสามารถรวบรวมพยานหลักฐานมาเพื่อใช้ประกอบการดำเนินคดีต่อผู้กระทำความผิด ซึ่งหลักการในการได้มาซึ่งพยานหลักฐานหรือการแสวงหาพยานหลักฐาน เป็นหลักการที่กระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชน หากเจ้าหน้าที่จะดำเนินการอันใดที่เป็นการกระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชนจะต้องมีกฎหมายบัญญัติไว้โดยชัดเจน นอกจากนี้ยังจำเป็นต้องมีมาตรการในการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐ โดยมาตรการที่เป็นสากลก็คือการตรวจสอบการใช้อำนาจโดยองค์กรตุลาการ หรือการตรวจสอบโดยผู้บังคับบัญชาหรือผู้กำกับดูแล

เมื่อเปรียบเทียบมาตรการในการแสวงหาพยานหลักฐานในการแสวงหาพยานหลักฐานในประเทศไทยกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ สามารถแบ่งพิจารณามาตรการในการแสวงหาพยานหลักฐานออกได้เป็น 2 ประการด้วยกัน

(1) มาตรการในการแสวงหาพยานหลักฐานในกรณีของภัยคุกคามทางไซเบอร์ในระดับร้ายแรงและมาตรการในการค้นโดยมีหมายจะมีการกำหนดให้มีการตรวจสอบการใช้อำนาจโดยองค์กรตุลาการ มีการนำแนวความคิดเกี่ยวกับเหตุอันควรสงสัย และดำเนินรอยตามหลักการของหลักนิติรัฐ แต่มาตรการในการแสวงหาพยานหลักฐานในกรณีของภัยคุกคามทางไซเบอร์มีลักษณะที่เป็นการให้อำนาจแก่เจ้าหน้าที่รัฐมากกว่าหลักการในการค้นตามมาตรา 98 (2) ได้แก่ ลักษณะของการได้ไปซึ่งข้อมูล โดยในมาตรการในการแสวงหาพยานหลักฐานย่อมได้ไปซึ่งข้อมูลทั้งหมดที่บรรจุอยู่ในคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ที่ต้องการค้น และสามารถเก็บข้อมูลดังกล่าวไว้ได้ ซึ่ง ณ เวลา

ที่ได้ไปซึ่งข้อมูลที่เกี่ยวกับความผิดอื่น เจ้าหน้าที่รัฐอาจจะไม่ทราบถึงการมีอยู่ของข้อมูลนั้นเลย และการที่จะหาข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์ เจ้าหน้าที่รัฐย่อมที่จะต้องทำการตรวจค้นทุกส่วนของระบบจัดเก็บข้อมูลของคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์นั้นซึ่งอาจเป็นเหตุที่ทำให้พบข้อมูลซึ่งเป็นความผิดตามกฎหมายอื่นในภายหลัง อีกทั้งความผิดที่เป็นเหตุในการได้ไปซึ่งข้อมูลย่อมไม่มีความเกี่ยวข้องกับรายละเอียดที่ปรากฏตามคำร้องที่ได้ยื่นต่อศาลตามมาตรการในการแสวงหาพยานหลักฐานกรณีของภัยคุกคามทางไซเบอร์ในระดับร้ายแรง การกำหนดทุกความผิดตามกฎหมายอื่นนั้น ซึ่งกว้างกว่าที่กำหนดไว้ในกรณีของการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาที่จำกัดอยู่แต่เฉพาะกรณีของความผิดซึ่งหน้า

(2) มาตรการในการแสวงหาพยานหลักฐานในกรณีของภัยคุกคามทางไซเบอร์ในระดับวิกฤติให้อำนาจที่กว้างขวางกว่ากรณีของการค้นโดยไม่มีหมายเป็นอันมาก เนื่องจากสามารถทำการเข้าถึงข้อมูลได้ในทุก ๆ กรณี ไม่ได้มีการกำหนดเหตุที่จะค้นโดยไม่มีหมายได้ดังเช่นในประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งการใช้อำนาจในลักษณะดังกล่าวไม่ได้มีการตรวจสอบการใช้อำนาจ หรือนำหลักการคุ้มครองสิทธิเสรีภาพมาประกอบการใช้อำนาจแต่อย่างใด คงมีเพียงการที่ต้องแจ้งต่อศาลภายหลังจากการดำเนินการเท่านั้น ซึ่งอาจเป็นการกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนเกินสมควร อีกทั้งเหตุที่เป็นการละเมิดต่อสิทธิโดยการนำข้อมูลส่วนบุคคลไปใช้ก็แต่โดยอำนาจตามกฎหมายที่ตราขึ้นเพื่อประโยชน์สาธารณะเท่านั้น แม้การรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับวิกฤติจะเป็นการดำเนินการเพื่อประโยชน์สาธารณะ แต่การเปิดเผยหรือส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีในกรณีเป็นความผิดตามกฎหมายอื่นนั้น ไม่ได้มีลักษณะเป็นมาตรการเพื่อประโยชน์สาธารณะ

เมื่อเปรียบเทียบมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในต่างประเทศกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของประเทศไทย จะเห็นได้ว่าการค้นภายใต้หลักการเห็นได้โดยประจักษ์ (Plain view) ของประเทศสหรัฐอเมริกากับการค้นตามมาตรา 98 (2) นั้นมีความคล้ายคลึงกันเป็นอย่างมาก แสดงให้เห็นถึงความสอดคล้องของแนวความคิดเกี่ยวกับมาตรการในการแสวงหาพยานหลักฐานของประเทศไทยและประเทศสหรัฐอเมริกาอย่างชัดเจน

นอกจากนี้เมื่อพิจารณาเปรียบเทียบกับมาตราการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ จะเห็นได้ว่ามีความแตกต่าง

กันอยู่ เบื้องต้นเจ้าหน้าที่รัฐที่จะทำการค้นโดยไม่มีหมายภายใต้หลักการเห็นได้โดยประจักษ์ (Plain view) จะต้องมีอำนาจในการเข้าตรวจค้นตามหมายซึ่งได้มีการอนุญาตจากศาลก่อน แล้วในขณะค้นได้พบเจอข้อมูลอื่นใดที่เป็นความผิดอีก โดยมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในกรณีของภัยคุกคามทางไซเบอร์ในระดับร้ายก็มีหลักการที่คล้ายคลึงกัน กล่าวคือ ในการที่เจ้าหน้าที่จะทำการเข้าถึงข้อมูลต่าง ๆ ภายในคอมพิวเตอร์ จะต้องมีการยื่นคำร้องต่อศาลโดยระบุเหตุตามที่กำหนดไว้เพื่อให้ศาลมีคำสั่งอนุญาตให้ทำการเข้าถึงได้เสียก่อน เมื่อเจ้าหน้าที่รัฐได้เข้าถึง หรือได้ทำการยึดคอมพิวเตอร์ดังกล่าวมาตรวจสอบ ภายหลังพบเจอข้อมูลที่ผิดกฎหมาย กรณีเช่นนี้ย่อมเป็นไปตามหลักการเดียวกับการค้นโดยไม่มีหมายภายใต้หลักการเห็นได้โดยประจักษ์

อย่างไรก็ตาม มาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในกรณีของภัยคุกคามไซเบอร์ในระดับวิกฤติไม่ได้มีการกำหนดขั้นตอนในยื่นคำร้องต่อศาลก่อนดำเนินการแต่อย่างใด คงกำหนดแต่เพียงว่าให้เจ้าหน้าที่รัฐดำเนินการใด ๆ ไปก่อน และภายหลังจากดำเนินการจึงแจ้งรายละเอียดของการดำเนินการแก่ศาล ซึ่งมาตรการดังกล่าวไม่ได้เป็นไปตามหลักการค้นโดยไม่มีหมายภายใต้หลักการเห็นได้โดยประจักษ์ เนื่องจากในการใช้อำนาจนั้น ไม่ได้มีการตรวจสอบการใช้อำนาจโดยองค์กรตุลาการเลย กรณีของข้อมูลต่าง ๆ ที่ได้มาภายใต้มาตรการในการแสวงหาพยานหลักฐานกรณีของภัยคุกคามทางไซเบอร์ในระดับวิกฤติ จึงไม่สมควรที่จะสามารถเปิดเผยหรือส่งมอบเพื่อประโยชน์ในการดำเนินคดีต่อผู้กระทำความผิดตามกฎหมายอื่นได้

ดังนั้น จากการศึกษาเปรียบเทียบมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ ของไทย เปรียบเทียบกับมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ เปรียบเทียบกับมาตรการในการแสวงหาพยานหลักฐานของประเทศไทยตามประมวลกฎหมายวิธีพิจารณาความอาญา และเปรียบเทียบกับมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของต่างประเทศ เห็นว่า มาตรา 70 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ฯ สมควรได้รับการแก้ไข ควรมีการนำหลักการของมาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์โดยไม่มีหมายในกรณีการค้นภายใต้หลักการเห็นได้โดยประจักษ์ (Plain view) มาประกอบการใช้อำนาจตามมาตรา 70 โดยกำหนดให้สามารถเปิดเผยและส่งมอบข้อมูลซึ่งได้มาตามพระราชบัญญัตินี้เฉพาะกรณีที่ได้รับการยินยอมโดยเจ้าของข้อมูล หรือกรณีที่ได้มีการยื่นคำร้องต่อศาลในการดำเนินการเพื่อให้ได้ข้อมูลมาเท่านั้น ส่วนในกรณีที่ไม่ได้มีการดำเนินการตามสองประการข้างต้น ดังเช่นในกรณีของภัยคุกคามทางไซเบอร์ใน

ระดับวิกฤติ ผู้เขียนมีความเห็นว่า มาตรการต่าง ๆ ในกรณีของภัยคุกคามทางไซเบอร์ในระดับวิกฤติเป็นมาตรการที่ให้อำนาจมากกว่าการดำเนินการทั่วไปในทางอาญาเป็นอย่างมาก เนื่องจากไม่มีการตรวจสอบก่อนการใช้อำนาจแต่อย่างใด ซึ่งเหตุที่มีการให้อำนาจเช่นนั้นเป็นเพราะความสำคัญของประโยชน์สาธารณะที่เจ้าหน้าที่ของรัฐจะต้องจัดการกับภัยคุกคามไซเบอร์ที่อาจสร้างความเสียหายเป็นวงกว้าง เมื่อการเปิดเผยหรือส่งมอบข้อมูลไม่ได้มีวัตถุประสงค์เพื่อประโยชน์สาธารณะดังเช่นในกรณีข้างต้น จึงไม่สมควรที่นำข้อมูลซึ่งได้มาจากมาตรการพิเศษมาเพื่อใช้ประโยชน์แก่การกระทำอื่นใดของรัฐอีก

6.2 ข้อเสนอแนะ

จากการศึกษามาตรการในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ผู้เขียนเห็นควรที่จะแก้ไขพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 70 เนื่องจากบทบัญญัติดังกล่าวเป็นบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่รัฐในลักษณะที่เป็นการแสวงหาพยานหลักฐาน แต่ไม่มีมาตรการในการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐที่เหมาะสม อันอาจกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนเกินสมควร ดังนี้

เสนอให้มีแก้ไขพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 70 โดยกำหนดให้การเปิดเผยหรือส่งมอบข้อมูลเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่น จะต้องปรากฏว่าเจ้าหน้าที่รัฐที่ดำเนินการขอข้อมูลดังกล่าวไปใช้ จะต้องปฏิบัติตามกฎหมายว่าการค้นโดยชอบด้วยกฎหมายแล้ว เพื่อให้เป็นไปตามหลักการเกี่ยวกับการแสวงหาพยานหลักฐาน โดยแก้ไขให้มีข้อความดังนี้

“ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัติฉบับนี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษ...

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นหรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจโดยมิชอบ

ความในวรรคสองมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามกฎหมายอื่น ในกรณีที่ได้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการมาตามมาตรา 68”

บรรณานุกรม

ภาษาต่างประเทศ

Mehak Aneja. Role of Judiciary in Cyber Crime. Supremo Amicus 18, July, 2020 (2020): 519-525.

David L. Carter. Computer Crime Categories: How Techno-Criminals Operate. FBI Law Enforcement Bulletin 64, 7 (2538).

Katie Chadd. The History of Cybercrime and Cybersecurity, 1940-2020 [Online]. 2563. Available from: https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/ [14/11/65.

Flaviu Ciopec. "Crime Control or Due Process? Which Are the Tendencies in Romanian Criminal Justice?" In Journal of Eastern-European Criminal Law: Faculty of Law West University of Timisoara, 2017.

Criminal Division Computer Crime and Intellectual Property Section, U.S. Department of Justice. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." edited by 3. Washington, D.C: Office of Legal Education Executive Office for United States Attorneys, 2552.

Maricopa County. Probable Cause Versus Reasonable Suspicion [Online]. Available from: https://www.maricopa.gov/9 1 9 / Probable-Cause-Versus-Reasonable-Suspici [17/8/2564.

The Department of Home Affairs Australia Government. [Online]. 2020. Available from: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australias-cyber-security-strategy-2020 [17/07/66. 27/02/66]

Chris Hale. Cybercrime: Facts & Figures Concerning This Global Dilemma. Crime & Justice International 18, 65 (2545).

The White House. Executive Order -- Improving Critical Infrastructure Cybersecurity [Online]. 2556. Available from: https://obamawhitehouse.archives.gov/the-

press-office/2 0 1 3 / 0 2 / 1 2 / executive-order-improving-critical-infrastructure-cybersecurity# [11/11/56.

Nir Kshetri. "Positive Externality, Increasing Returns, and the Rise in Cybercrimes." 2009.

Sullivan & Cromwell LLP. "The Cybersecurity Act of 2 0 1 5 : Congress Passes and President Signs Long-Anticipated Measure Setting Framework for Sharing Cyber Threat Information with Federal Government and Private Sector." 2558.

Nureni Ayofe Azeez and Oluwaseyi Osunade. Approach to Solving Cybercrime and Cybersecurity. International Journal of Computer Science and Information Security (IJCSIS) 3, 1 (2552).

Bogdan Popa. Did You Know: The First Antivirus Product Was Launched in 1 9 8 7 [Online]. 2 5 6 3 . Available from: https://news.softpedia.com/news/did-you-know-the-first-antivirus-product-was-launched-in-1987-528883.shtml [12/11/65.

ภาษาไทย

กองบรรณาธิการสำนักกฎหมาย. หลักสิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย : แนวความคิดและภาคปฏิบัติ. จุลนิติ ม.ค. - ก.พ. 54.

นารี กิตติสมบูรณ์สุข. การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์. นิติศาสตรมหาบัณฑิต, นิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิต. 2548.

ฐกฤต แก้วทับทิม. การขยายตัวขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโควิด-19. วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์ กรกฎาคม - ธันวาคม 2564, ฉบับที่ 2 ปีที่ 7 (2565).

กัลยา ชินาธิวร. ความสำเร็จของสิงคโปร์: กรณีศึกษาเพื่อประกอบการพัฒนาแนวทางการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย. การฝึกอบรมหลักสูตรนักบริหารการทูต รุ่นที่ 11 ปี 2562 สถาบันการต่างประเทศเทวะวงศ์วโรปการ กระทรวงกาต่างประเทศ. 2562.

คณาธิป ทองรวีวงศ์. กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1. กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2563.

ทิพาพร นะมาตร์. สิทธิความเป็นอยู่ส่วนตัว : ศึกษากรณีสิทธิความเป็นอยู่ส่วนตัวของบุคคลสาธารณะ. นิติศาสตรมหาบัณฑิต, สาขาวิชานิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิต. 2551.

สุวิทย์ ปัญญาวงศ์. กฎหมายมหาชน. 2, พ., บรรณาธิการ. กรุงเทพมหานคร: วิญญูชน, 2561.

ธีสุทธิ์ พันธ์ฤทธิ์. การรับฟังพยานหลักฐานคดีอาญา : บทวิเคราะห์และวิจารณ์. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2558.

ผ่องพรรณ ไพพรรณรัตน์. หลักนิติธรรมกับการคุ้มครองสิทธิเสรีภาพของประชาชน. สำนักงานศาลรัฐธรรมนูญ.

จรัญ ภักดีกุล. กฎหมายลักษณะพยานหลักฐาน. พิมพ์ครั้งที่ 11. กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2559.

วรเจตน์ ภาคีรัตน์. หลักนิติธรรมและหลักนิติรัฐ. จุลนิติ ม.ค. - ก.พ. 55(2555).

เศรษฐพงค์ มะลิสุวรรณ. Cybersecurity ยักษ์ใหญ่ยังเคยล้ม จึงน่าศึกษาเป็นบทเรียน [Online]. 2558. Available from: https://www.beartai.com/article/beartai-ict/66506 [10/11/65.

จิตสุภา ฤทธิผลิน. กลยุทธ์การคืนสภาพได้ทางไซเบอร์ : แนวทางสำคัญในการดำเนินงานขององค์กรในยุคดิจิทัล. วารสารวิชาการ กสทช. ประจำปี 2564(2564).

เขตไท ลังการ์พินธ์. หลักนิติธรรมของประเทศอังกฤษ และประเทศไทย : ความหมายและสาระสำคัญ. วารสารนิติศาสตร์ มหาวิทยาลัยนเรศวร ปีที่ 9, ฉบับที่ 2 พฤศจิกายน 2558 (2558).

ประธาน วัฒนพานิช. ระบบความยุติธรรมทางอาญา : แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม. 9, 2 (2520): 150.

สหรัฐ กิติ ศุภกร. หลักและคำพิพากษา : กฎหมายวิธีพิจารณาความอาญา. 14, พ., บรรณาธิการ. กรุงเทพมหานคร: บริษัท อมรินทร์พริ้นติ้งแอนด์พับบลิชชิ่ง จำกัด (มหาชน), 2565.

อนัญพร สกุลเมฆา. การตรวจสอบและถ่วงดุลอำนาจเจ้าพนักงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. นิติศาสตรมหาบัณฑิต สาขากฎหมายอาญา, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. 2562.

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. [ออนไลน์]. แหล่งที่มา: https://www.sec.or.th/TH/Pages/CYBERRESILIENCE-KNOWLEDGECYBER.aspx [เข้าถึงเมื่อ 15/07/2566]

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. ร่างกฎหมายเศรษฐกิจดิจิทัล [Online]. Available from: https://ictlawcenter.etda.or.th/de_laws [11/11/65.

———. สถิติภัยคุกคาม [Online]. 2565. Available from: https://www.etda.or.th/th/Our-Service/thaicert/stat.aspx [11/11/65.

คณะกรรมการศึกษาแนวทางแก้ไขเพิ่มเติมรัฐธรรมนูญ สำนักงานเลขาธิการสภาผู้แทนราษฎร. แนวทางแก้ไขรัฐธรรมนูญ เรื่อง สิทธิ เสรีภาพ และหน้าที่ของชนชาวไทย. พิมพ์ครั้งที่ 1. กรุงเทพมหานคร: สำนักงานเลขาธิการสภาผู้แทนราษฎร, 2549.

บรรเจิด สิงคะเนติ. หลักกฎหมายมหาชน หลักนิติธรรม/นิติรัฐในฐานะ "เกณฑ์" จำกัดอำนาจรัฐ. พิมพ์ครั้งที่ 3. กรุงเทพมหานคร: วิญญูชน, 2560.

———. หลักพื้นฐานเกี่ยวกับสิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์. พิมพ์ครั้งที่ 5. กรุงเทพมหานคร: วิญญูชน, 2558.

สาวตรี สุขศรี. กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2563.

วนิดา แสงสารพันธ์. สิทธิส่วนบุคคล กับความคุ้มครองตามกฎหมาย. LAW FOR YOU.

ปริญญา หอมเอนก. [ออนไลน์]. 2565. แหล่งที่มา: https://www.bangkokbiznews.com/columnist/1000806 [เข้าถึงเมื่อ 12/11/65]

เสาวนีย์ อัศวโรจน์. สิทธิมนุษยชนกับกฎหมายปกครอง : การคุ้มครองสิทธิเสรีภาพของประชาชน. วารสารกระบวนการยุติธรรม Journal of Thai Justice System เล่มที่ 1 ปีที่ 3 มกราคม - มีนาคม 2553 (2553).

อุทัย อาทิเวช. กฎหมายวิธีพิจารณาความอาญาและพยานชั้นสูง. นนทบุรี: สำนักพิมพ์มหาวิทยาลัยสุโขทัยธรรมาธิราช.

ยุทธพร อิสรชัย. การตรวจสอบการใช้อำนาจรัฐ [Online]. Available from: http://wiki.kpi.ac.th/index.php?title=การตรวจสอบการใช้อำนาจรัฐ [10/05/2566.

ประวัติผู้เขียน

ชื่อ-สกุล	ชิตพล พงศ์วชิราพร
วัน เดือน ปี เกิด	11 มิถุนายน 2534
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษา	สำเร็จการศึกษาชั้นมัธยมศึกษาจากโรงเรียนสาธิตมหาวิทยาลัยศรีนครินทรวิโรฒ ประสานมิตร (ฝ่ายมัธยม) และสำเร็จการศึกษาชั้นปริญญาตรีนิติศาสตรบัณฑิต จากคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย จากนั้นได้เข้าศึกษาต่อในหลักสูตรนิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์ หมวดวิชากฎหมายอาญาและกระบวนการยุติธรรมทางอาญา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย