ปัญหาในการสืบสวนและดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศภายใต้กฎหมายไทย*

Problems in Investigating and Prosecuting Hackers from Abroad under Thai Laws

กิตสุรณ สังขสุวรรณ์**
นักวิชาการอิสระ
Kitsuron Sangsuvan
Independent Scholar

วันที่รับบทความ 17 ธันวาคม 2564; วันที่แก้ไขบทความ 4 กุมภาพันธ์ 2565; วันที่ตอบรับบทความ 20 กุมภาพันธ์ 2565

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาและวิเคราะห์ปัญหาในการสืบสวนและดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศภายใต้กฎหมายไทย วิธีการในการวิจัยปัญหาดังกล่าวได้ใช้วิธีการวิจัยเชิงคุณภาพ โดยการรวบรวมข้อมูลต่าง ๆ จากตัวบทกฎหมาย หนังสือ บทความวิจัย บทความทางวิชาการ รายงาน ข่าวประจำวัน ทั้งในประเทศไทยและต่างประเทศ ข้อมูลจากเอกสารทั้งหมดนี้ได้ถูกนำมาใช้ในการวิเคราะห์ถึงปัญหาและอุปสรรคในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ ข้อมูลเหล่านี้ยังถูกนำมาใช้ในการอธิบายแนวคิดหรือหลักเกณฑ์ในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศด้วยเช่นกัน

---

* บทความนี้สรุปจากโครงการวิจัยของผู้เขียนเรื่อง **“การดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ”**

** น.บ. มหาวิทยาลัยรามคำแหง; น.บ.ท.; LL.M. (Global Legal Studies) University of Illinois Chicago School of Law, Chicago, Illinois, USA; LL.M. (Intellectual Property) University of Illinois Chicago School of Law, Chicago, Illinois, USA; S.J.D. Indiana University Robert H. McKinney School of Law, Indianapolis, Indiana, USA; อีเมลติดต่อ krit.bond@yahoo.com

การวิจัยพบว่าปัญหาในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศมิได้เกิดจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่อย่างใด ซึ่งในความเป็นจริง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายที่มีประสิทธิภาพ แต่ปัญหาเกิดจากพนักงานเจ้าหน้าที่ขาดความรู้และไม่มีความสามารถในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ นอกจากนี้ ปัญหายังรวมถึงการสืบสวน สอบสวน และรวบรวมพยานหลักฐานดิจิทัลที่อยู่ในต่างประเทศภายใต้พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 และการขอให้ส่งตัวแฮ็กเกอร์ที่อยู่ในต่างประเทศมายังประเทศไทยในฐานะผู้ร้ายข้ามแดนภายใต้พระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551

การวิจัยนี้เสนอวิธีการแก้ไขปัญหาในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศด้วยการพัฒนาศักยภาพและความสามารถของพนักงานเจ้าหน้าที่ในประเทศไทย การเข้าร่วมในความร่วมมือระหว่างประเทศ และการลดขั้นตอนหรือกระบวนการทางกฎหมาย

คำสำคัญ: การเจาะเข้าระบบคอมพิวเตอร์, อาชญากรรมทางเทคโนโลยี, แฮ็กเกอร์

Abstract

The objective of this research is to study and analyze the problems in investigating and prosecuting foreign hackers under Thai laws. Qualitative research has been used as a methodological approach in this research. It has relied on relevant regulations, books, research articles, academic articles, reports, and news from around the world. Knowledge or information based on those documents has been used to analyze the problems and establish conceptions.

This research found that the problems do not result from the Computer-related Crime Act B.E. 2550 (2007). In fact, this Act is the effective regulation. However, the problems result from Thai officers themselves. They do not have sufficient knowledge and capabilities to investigate and prosecute hackers from abroad. In addition, the problems involve the investigation and collection of digital evidence located in other countries. This process has to rely on the Act

on Mutual Assistance in Criminal Matters B.E. 2535 (1992). The problems also include the extradition of foreign hackers under the Extradition Act, B.E. 2551 (2008).

This research offers the resolutions of the problems. Those may include the development of officers' capabilities, participation in international cooperation, and a decrease in legal processes.

Keywords: Hacking, Cybercrime, Hacker

1. บทนำ

การเจาะเข้าระบบคอมพิวเตอร์หรือการแฮ็ก (Hacking) คือ การกระทำด้วยประการใด ๆ เพื่อเข้าถึงหรือบุกรุกระบบคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต[1] การเจาะเข้าระบบคอมพิวเตอร์หรือการแฮ็กถือเป็นอาชญากรรมทางเทคโนโลยีในรูปแบบใหม่ที่เจริญเติบโตขึ้นอย่างรวดเร็ว[2] เนื่องจากกิจกรรมต่าง ๆ ในปัจจุบันได้ดำเนินการด้วยระบบออนไลน์หรือระบบอินเทอร์เน็ตทั้งสิ้น แฮ็กเกอร์จึงใช้ช่องทางออนไลน์หรือระบบอินเทอร์เน็ตในการเจาะเข้าระบบคอมพิวเตอร์ และเมื่ออินเทอร์เน็ตสามารถเชื่อมต่อกิจกรรมต่าง ๆ ได้ทั่วทุกมุมโลก การเจาะเข้าระบบคอมพิวเตอร์จึงกลายเป็นอาชญากรรมข้ามชาติ (Transnational Crime)[3] ที่ก่อให้เกิดความเสียหายต่อประชาชน เศรษฐกิจ ธุรกิจการค้า การเงินการธนาคาร อุตสาหกรรม สาธารณสุข และสังคมในประเทศอื่น ๆ ด้วยเช่นกัน

การเจาะเข้าระบบคอมพิวเตอร์หรือการแฮ็ก ถือเป็นการกระทำผิดทางอาญาตามกฎหมายว่าด้วยการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์โดยเฉพาะ และอาจถือเป็นการกระทำความผิดตามประมวลกฎหมายอาญาในข้อหาอื่น ๆ[4] เช่น ความผิดฐานลักทรัพย์ กรรโชกทรัพย์ รีดเอาทรัพย์ หรือทำให้เสียทรัพย์ นอกจากนี้ กลุ่มแฮ็กเกอร์อาจแบ่งออกเป็น 2 กลุ่ม[5] คือ (1) กลุ่มแฮ็กเกอร์ทั่วไป ซึ่งได้แก่ บุคคลที่มีความรู้และความสามารถในระบบคอมพิวเตอร์[6] และมุ่งหมายหรือลงมือกระทำความผิดต่อผู้เสียหายโดยเฉพาะเจาะจง สำหรับวิธีการที่แฮ็กเกอร์มักใช้ คือ การคาดเดารหัสผ่านของผู้เสียหาย หรือหลอกถามข้อมูลส่วนบุคคลหรือรหัสเพื่อเข้าถึงระบบคอมพิวเตอร์ของผู้เสียหาย และ (2) กลุ่มแฮ็กเกอร์ที่มี

---

[1] Larry Mays, Jeremy Ball, and Laura Fidelie, **Criminal Law: Core Concepts**, First Edition (New York: Wolters Kluwer Law & Business, 2015), p. 235.

[2] Joseph Migga Kizza, **Computer Network Security and Cyber Ethics**, Fourth Edition (North Carolina: McFarland & Company, 2014), p. 114.

[3] Richard Lovely, **Cybercrime** in **International Crime and Justice**, Edited by Mangai Natarajan, First Edition (New York: Cambridge University Press, 2011), p. 160.

[4] Larry Mays, Jeremy Ball, and Laura Fidelie, **Criminal Law: Core Concepts**, p. 235.

[5] Catherine D. Marcum, **Cyber Crime**, Second Edition (New York: Wolters Kluwer, 2019), p. 119.

[6] Ibid.

ความสามารถสูง ซึ่งได้แก่ บุคคลที่มีความรู้และความเชี่ยวชาญในระบบคอมพิวเตอร์อย่างสูง[7] แฮ็กเกอร์กลุ่มนี้มักมุ่งถึงผลร้ายที่อาจเกิดขึ้น อีกทั้งระดับความรุนแรงหรือความเสียหายจากการเจาะเข้าระบบคอมพิวเตอร์ของแฮ็กเกอร์กลุ่มนี้มีสูงด้วยเช่นกัน ตัวอย่างเช่น การเจาะเข้าระบบคอมพิวเตอร์ของธนาคารเพื่อขโมยเงินออกจากธนาคาร แฮ็กเกอร์กลุ่มนี้มีเครื่องมือหรือเทคโนโลยีที่ใช้ในการกระทำความผิดที่ทันสมัย โดยรูปแบบการเจาะเข้าระบบคอมพิวเตอร์ของแฮ็กเกอร์กลุ่มนี้ได้แก่[8] โทรจัน (Trojan),[9] การโจมตีช่องโหว่ในคอมพิวเตอร์ (Cross-Site Scripting (XSS)),[10] การโจมตีโดยปฏิเสธการให้บริการ (Denial-of-Service (DoS)),[11] การสร้างช่องคำสั่งและควบคุมไปยังคอมพิวเตอร์ของเหยื่อ (DNS Tunneling),[12] มัลแวร์ (Malware),[13] ฟิชชิง (Phishing),[14] มัลแวร์เรียกค่าไถ่ (Ransomware),[15] การดึงข้อมูลออกมาจากฐานข้อมูล

---

[7] Ibid.

[8] IBM, **What is A Cyber Attack?** [Online], 15 December 2021. Source: https://www.ibm.com/topics/cyber-attack

[9] โทรจัน (Trojan) คือ โปรแกรมคอมพิวเตอร์ที่ถูกบรรจุเข้าไปในคอมพิวเตอร์ เพื่อลอบเก็บข้อมูลของคอมพิวเตอร์ในเครื่องนั้น

[10] การโจมตีช่องโหว่ในคอมพิวเตอร์ (Cross-Site Scripting (XSS)) คือ การโจมตีโดยการฝังโค้ดเข้าไปกับหน้าเว็บไซต์ที่มีช่องโหว่ เมื่อผู้ใช้โหลดหน้าเว็บเพจ คำสำคัญบางอย่างเช่น ค่าของ Cookie, Username, Password อาจถูกขโมยได้

[11] การโจมตีโดยปฏิเสธการให้บริการ (Denial-of-Service (DoS)) คือ ความพยายามทำให้เครื่องคอมพิวเตอร์หรือเครือข่ายของผู้ใช้บริการไม่สามารถเข้าถึงการให้บริการนั้นได้ เช่น ขัดขวางการเข้าถึงระบบอินเทอร์เน็ต

[12] การสร้างช่องคำสั่งและควบคุมไปยังคอมพิวเตอร์ของเหยื่อ (DNS Tunneling) เป็นเทคนิคมัลแวร์ที่ช่วยให้ผู้โจมตีสร้างช่องคำสั่งและการควบคุมไปยังคอมพิวเตอร์ของเหยื่อ

[13] มัลแวร์ (Malware) คือ โปรแกรมที่ถูกสร้างขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูล

[14] ฟิชชิง (Phishing) คือ เทคนิคการหลอกลวงผ่านทางระบบอินเทอร์เน็ต เพื่อทำให้เหยื่อเปิดเผยข้อมูลสำคัญ เช่น ข้อมูลการทำธุรกรรมทางการเงิน เป็นต้น

[15] มัลแวร์เรียกค่าไถ่ (Ransomware) มักทำการควบคุมไฟล์ของเหยื่อเพื่อไม่ให้เหยื่อเข้าถึงไฟล์ที่ถูกควบคุมไว้ได้ตามปกติ จากนั้นจะมีข้อความเรียกค่าไถ่ไฟล์ที่ได้ถูกควบคุมไว้ หากเหยื่อยอมจ่ายค่าไถ่ แฮ็กเกอร์จะยอมให้เหยื่อเข้าถึงไฟล์นั้น

(Structured Query Language (SQL) Injection),[16] และการโจมตีผ่านช่องโหว่ที่ยังไม่เคยถูกค้นพบ (Zero-Day Exploit)[17]

สำหรับประเทศไทยนั้น แฮ็กเกอร์ที่มีความสามารถสูงได้ลงมือเจาะเข้าระบบคอมพิวเตอร์ในหน่วยงานภาครัฐและเอกชน รวมทั้งประชาชนในประเทศ ที่สำคัญแฮ็กเกอร์เหล่านี้ได้อาศัยอยู่ในต่างประเทศ และได้ทำการโจมตีจากต่างประเทศเข้ามาในประเทศไทย ตัวอย่างเช่น แฮ็กเกอร์ได้ใช้มัลแวร์เรียกค่าไถ่ (Ransomware) ในการเจาะเข้าระบบคอมพิวเตอร์ของโรงพยาบาลเพชรบูรณ์ โดยแฮ็กเกอร์ได้ล็อคข้อมูลคนไข้และเรียกค่าไถ่เป็นเงินจำนวน 6.3 หมื่นล้านบาท[18] หรือแฮ็กเกอร์ได้เจาะเข้าระบบคอมพิวเตอร์เพื่อขโมยเงินออกจากเจ้าของบัญชีธนาคารหรือเจ้าของบัตรเดบิต โดยแฮ็กเกอร์ใช้วิธีขโมยเงินออกจากบัญชีเงินฝากหรือบัตรเดบิตผ่านเครื่องรูดบัตร จำนวนน้อย ๆ แต่หลาย ๆ ครั้ง ทั้งที่เจ้าของบัญชีหรือเจ้าของบัตรเดบิตไม่ได้ทำธุรกรรมทางการเงิน และไม่มี SMS แจ้งเตือนไปยังเจ้าของบัญชีหรือเจ้าของบัตรเดบิตแต่อย่างใด ซึ่งในการตรวจสอบพบว่า แฮ็กเกอร์ที่ลงมือกระทำความผิดประเภทนี้คือแฮ็กเกอร์ที่เป็นชาวต่างชาติ และลงมือกระทำความผิดในต่างประเทศ โดยแฮ็กเกอร์อาจใช้อุปกรณ์พิเศษเพื่อช่วยให้ล่วงรู้ข้อมูลสำคัญในบัตรเดบิต แล้วนำข้อมูลไปทำรายการซื้อสินค้าจากต่างประเทศเพื่อดูดเงินจากบัตรเดบิต โดยใช้กลไกการชำระเงินแบบไร้สัมผัส (Contactless) ที่เชื่อมต่อข้อมูลด้วย WiFi เป็นเครื่องมือในการก่อเหตุ[19]

ในทางปฏิบัติ การสืบสวนหรือตรวจสอบการเจาะเข้าระบบคอมพิวเตอร์นี้ถือเป็นเรื่องยาก เพราะการตรวจสอบติดตามการกระทำความผิดดังกล่าวต้องใช้พนักงานเจ้าหน้าที่ที่มีความรู้

---

[16] การดึงข้อมูลออกมาจากฐานข้อมูล (Structured Query Language (SQL) Injection) คือ การโจมตีโดยอาศัยช่องโหว่ของโปรแกรมเพื่อใส่ SQL เข้าไปในทาง Input ทั้งหลายบน User Interface เพื่อที่จะสามารถดึงข้อมูลออกมาจากฐานข้อมูลได้

[17] การโจมตีผ่านช่องโหว่ที่ยังไม่เคยถูกค้นพบ (Zero-Day Exploit) คือ การโจมตีทางไซเบอร์ขั้นสูงโดยอาศัยช่องโหว่ที่อยู่ใน Hardware หรือ Software ที่ยังไม่เคยถูกค้นพบมาก่อน

[18] ไทยรัฐ ออนไลน์, **รพ. เพชรบูรณ์แจงหลังถูกแฮ็ก ยันข้อมูลที่หลุดไม่กระทบต่อการรักษาคนไข้** [ออนไลน์], 15 ธันวาคม 2564. แหล่งที่มา: https://www.thairath.co.th/news/society/2187423

[19] ผู้จัดการออนไลน์, **แฉ! กลโกงดูดเงินผ่าน “บัตรตื๊ด” บัตรอยู่ในกระเป๋าก็แฮ็กข้อมูลได้** [ออนไลน์], 21 ธันวาคม 2564. แหล่งที่มา: https://mgronline.com/specialscoop/detail/9640000103836

และความเชี่ยวชาญทางคอมพิวเตอร์อย่างมาก ซึ่งโดยทั่วไป พนักงานเจ้าหน้าที่มักเริ่มต้นจากการค้นหาติดตาม Internet Protocol Address (IP Address)[20] จากข้อมูลจราจรทางคอมพิวเตอร์ที่ได้รับจากผู้ให้บริการอินเทอร์เน็ต หากพนักงานเจ้าหน้าที่สามารถค้นพบ IP Address ของแฮ็กเกอร์ได้ พนักงานเจ้าหน้าที่ก็สามารถระบุตัวตนของแฮ็กเกอร์พร้อมพิกัดที่อยู่ได้ แต่อย่างไรก็ตาม แม้พนักงานเจ้าหน้าที่สามารถตรวจสอบ IP Address ที่ใช้ในการก่อเหตุได้ ก็มักเป็น IP Address ปลอมที่สวมรอยมา ซึ่งตามปกติการตรวจสอบมักไม่สามารถสืบไปถึงตัวผู้กระทำความผิดได้ หรือหากสืบไปถึงตัวผู้กระทำความผิดได้ ก็มักพบว่าเป็นการก่อเหตุในต่างประเทศ ซึ่งยากต่อการดำเนินคดี และในปัจจุบันนี้ การเจาะเข้าระบบคอมพิวเตอร์ที่เกิดขึ้นในประเทศไทยมาจากผู้กระทำความผิดหรือแฮ็กเกอร์ที่อยู่ในต่างประเทศจำนวนมาก

การที่พนักงานเจ้าหน้าที่ไม่สามารถปราบปรามหรือดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ ถือเป็นปัญหาในกระบวนการยุติธรรมที่อาจส่งผลกระทบต่อเศรษฐกิจ สังคม และการดำเนินกิจการต่าง ๆ ภายในประเทศ ในขณะเดียวกัน แฮ็กเกอร์ผู้กระทำความผิดย่อมมีความเชื่อมั่นว่าตนเองไม่อาจถูกจับกุมหรือถูกดำเนินคดีได้ แฮ็กเกอร์อาจลงมือกระทำความผิดในประเทศไทยมากขึ้น และคดีเกี่ยวกับการเจาะเข้าระบบคอมพิวเตอร์ย่อมมีจำนวนเพิ่มมากขึ้น ประเทศไทยจึงอาจตกเป็นประเทศกลุ่มเป้าหมายที่ใช้ในการกระทำความผิด ดังนั้น การปราบปรามหรือดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศจึงเป็นเรื่องที่มีความสำคัญและความจำเป็นอย่างมาก

2. วัตถุประสงค์ของการวิจัย

(1) เพื่อศึกษาและพิจารณาประสิทธิภาพของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในการเอาผิดหรือดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ

(2) เพื่อศึกษาและวิเคราะห์วิธีการและปัญหาในการสืบสวน สอบสวน และรวบรวมพยานหลักฐานดิจิทัลจากแฮ็กเกอร์ที่อยู่ในต่างประเทศภายใต้พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535

[20] Internet Protocol Address (IP Address) คือ หมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายที่ใช้โปรโตคอลแบบ TCP/IP

(3) เพื่อศึกษาและวิเคราะห์วิธีการและปัญหาในการขอให้ส่งตัวแฮ็กเกอร์ที่อยู่ในต่างประเทศมายังประเทศไทยในฐานะผู้ร้ายข้ามแดนภายใต้พระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551

(4) เพื่อศึกษาวิธีการและปัญหาในการเก็บรวบรวมและตรวจสอบพยานหลักฐานดิจิทัลบนพื้นฐานของ Digital Forensics[21] เพื่อดำเนินคดีกับแฮ็กเกอร์อยู่ในต่างประเทศ

3. สมมติฐานการวิจัย

ปัญหาในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศไม่ได้เกิดขึ้นจากความล้มเหลวหรือความไม่มีประสิทธิภาพของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่อย่างใด แต่เกิดจากการที่พนักงานเจ้าหน้าที่ไม่มีความสามารถในการติดตาม หรือสืบทราบตัวแฮ็กเกอร์ เนื่องจากแฮ็กเกอร์ในปัจจุบันมีศักยภาพและความสามารถสูงกว่าพนักงานเจ้าหน้าที่มาก พนักงานเจ้าหน้าที่ยังคงไม่เข้าใจถึงวิธีการสืบสวนสอบสวน หรือรวบรวมพยานหลักฐานเพื่อดำเนินคดีกับแฮ็กเกอร์ได้อย่างถูกต้อง นอกจากนี้พนักงานเจ้าหน้าที่ยังมีข้อจำกัดในด้านความรู้ และความเข้าใจในการดำเนินการขอความร่วมมือระหว่างประเทศและการส่งผู้ร้ายข้ามแดน อีกทั้งกระบวนการขอความร่วมมือระหว่างประเทศและการส่งผู้ร้ายข้ามแดนมักมีความล่าช้าและสลับซับซ้อน ส่งผลให้การติดตามตัวหรือดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศจึงเป็นเรื่องที่ยากลำบาก

4. ขอบเขตการวิจัย

การศึกษาปัญหาในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศภายใต้กฎหมายไทยนั้นจำต้องพิจารณาถึงรูปแบบการกระทำผิดของแฮ็กเกอร์และความสามารถของพนักงานเจ้าหน้าที่ จากนั้นต้องศึกษาและพิจารณาถึง (1) บทบัญญัติของกฎหมายที่กำหนดให้การเจาะเข้าระบบคอมพิวเตอร์ของผู้อื่นเป็นการกระทำความผิด ซึ่งได้แก่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยอาจพิจารณารูปแบบและโครงสร้างของพระราชบัญญัติดังกล่าวเพื่อประเมินประสิทธิภาพของกฎหมาย และ (2) บทบัญญัติของ

[21] Digital Forensics มีความหมายคือ วิธีการหรือเทคนิคในการเก็บรวบรวม วิเคราะห์ หรือตรวจพิสูจน์พยานหลักฐานดิจิทัลด้วยวิธีการทางวิทยาศาสตร์

กฎหมายที่เกี่ยวข้องกับการสืบสวนหรือดำเนินคดีแฮ็กเกอร์ผู้กระทำความผิด ซึ่งได้แก่ พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 และพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 โดยพิจารณาถึงปัญหาและอุปสรรคในการขอความช่วยเหลือหรือความร่วมมือในการสืบสวน สอบสวน หรือรวบรวมพยานหลักฐานที่อยู่ในต่างประเทศ และพิจารณาถึงปัญหาและอุปสรรคในการขอให้ส่งแฮ็กเกอร์ที่อยู่ในต่างประเทศในฐานะผู้ร้ายข้ามแดน การศึกษาเหตุปัจจัยเหล่านี้ช่วยทำให้ได้ข้อสรุปและข้อเสนอแนะในการแก้ไขปัญหาการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ

5. วิธีการดำเนินการวิจัย

การศึกษาปัญหาในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศนี้ เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) โดยรวบรวมและศึกษาข้อมูลจากเอกสารต่าง ๆ ซึ่งได้แก่ ตัวบทกฎหมาย หนังสือ บทความวิจัย บทความทางวิชาการ รายงาน ข่าวประจำวัน ทั้งในประเทศไทยและต่างประเทศ ข้อมูลจากเอกสารทั้งหมดนี้ได้ถูกนำมาใช้ในการแสดงและวิเคราะห์ถึงปัญหาและอุปสรรคในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ ข้อมูลเหล่านี้ยังถูกนำมาใช้ในการอธิบายเป็นแนวคิด หรือหลักเกณฑ์ในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศด้วยเช่นกัน

6. ประโยชน์ที่คาดว่าจะได้รับ

การศึกษาปัญหาในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศนี้ ช่วยให้ทราบถึงปัญหาและอุปสรรคในทางกฎหมายที่แท้จริง ซึ่งเกิดขึ้นทั้งในประเทศและต่างประเทศ การศึกษาถึงปัญหานี้ช่วยให้ประชาชนผู้สนใจเข้าใจถึงกระบวนการดำเนินคดีกับแฮ็กเกอร์ และอุปสรรคที่อาจเกิดขึ้น อีกทั้งยังช่วยให้ประชาชนที่ต้องการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศได้พิจารณาและประเมินถึงโอกาสและความเป็นไปได้ในการดำเนินคดี การศึกษาปัญหาดังกล่าวยังอาจช่วยเสริมสร้างมาตรการป้องกันให้แก่ประชาชน โดยประชาชนผู้สนใจควรตระหนักถึงภัยจากแฮ็กเกอร์ที่อยู่ในต่างประเทศ และมีความระมัดระวังการใช้อินเทอร์เน็ตมากยิ่งขึ้น เพราะการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศเป็นเรื่องที่ยากลำบากมาก

7. ผลการวิจัย

อินเทอร์เน็ตเป็นระบบเชื่อมต่อเครือข่ายทั่วโลกเข้าด้วยกัน อินเทอร์เน็ตจึงช่วยให้มนุษย์สามารถติดต่อสื่อสารกันได้แบบไร้พรมแดน[22] แต่อย่างไรก็ตาม อินเทอร์เน็ตได้ถูกนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรมทางเทคโนโลยีที่มีจำนวนมากขึ้น[23] โดยผู้กระทำความผิดใช้อินเทอร์เน็ตและคอมพิวเตอร์ของตนในการเข้าถึงหรือเจาะเข้าระบบคอมพิวเตอร์ของผู้อื่น รวมถึงสมาร์ทโฟน แท็บเล็ต หรือบัญชีผู้ใช้งานในโซเชียลมีเดีย ผู้กระทำความผิดดังกล่าวนี้เรียกว่า “แฮ็กเกอร์” และในปัจจุบันนี้ การเจาะเข้าระบบคอมพิวเตอร์ของผู้อื่นได้ถูกพัฒนากลายเป็นอาชญากรรมข้ามชาติซึ่งส่งผลกระทบต่อประเทศอื่น ๆ ทั่วโลก[24]

การศึกษาและวิจัยพบว่าการจับกุมหรือดำเนินคดีกับแฮ็กเกอร์เป็นเรื่องที่ยากลำบากมาก[25] สภาเศรษฐกิจโลก (World Economic Forum) ได้รายงานทางสถิติว่า โอกาสที่จะประสบความสำเร็จในการจับกุมแฮ็กเกอร์มีเพียง 0.5% เท่านั้น[26] ทั้งนี้เนื่องจากแฮ็กเกอร์ในปัจจุบันนี้มีความเชี่ยวชาญและมีความสามารถสูงมากขึ้นกว่าเดิม แฮ็กเกอร์เหล่านี้ได้ใช้วิธีการใหม่ ๆ หรือเทคโนโลยีที่ทันสมัยในการเจาะเข้าระบบคอมพิวเตอร์ของผู้อื่น[27] อีกทั้งยังใช้วิธีการซ่อนเร้นตัวตนหรือปกปิด IP Address ของตนได้อย่างมีประสิทธิภาพ[28] สิ่งเหล่านี้ทำให้เจ้าหน้าที่ของรัฐไม่สามารถสืบทราบหรือติดตามตัวของแฮ็กเกอร์ได้ หรือในกรณีที่เจ้าหน้าที่ของรัฐสามารถสืบทราบตัวตนของแฮ็กเกอร์หรือทราบ IP Address ของแฮ็กเกอร์ แต่ปรากฏว่าแฮ็กเกอร์ได้

---

[22] Michael Eck, **The Internet: Inside and Out**, First Edition (New York: Rosen Publishing Group, 2002), p. 8.

[23] Samuel C. McQuade, **Encyclopedia of Cybercrime**, First Edition (London: Greenwood Press, 2008), p. 43.

[24] Mikaila Mariel Lemonik, **Law and Justice Around the World: A Comparative Approach**, First Edition (Oakland: University of California Press, 2020), p. 87.

[25] David J. Engebretson, **Technician’s Guide to Physical Security Networking: Enterprise Solutions**, First Edition (Indiana: Author House, 2008), p. 71.

[26] ข่าวไทยพีบีเอส, **ดีอีเอส ล่าแฮ็กเกอร์ขโมยข้อมูล รพ. เพชรบูรณ์ - ปูดกองทัพโดนด้วย** [ออนไลน์], 15 ธันวาคม 2564. แหล่งที่มา: https://news.thaipbs.or.th/content/307715

[27] Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, **Cybercrime and Digital Forensics: Introduction**, First Edition (New York: Routledge, 2015), p. 55.

[28] Kevin Hile, **Cybercrime**, First Edition (Massachusetts: Cengage Learning, 2010), p. 33.

ลงมือกระทำความผิดในต่างประเทศ เจ้าหน้าที่ของรัฐอาจต้องพบความยากลำบากมากขึ้นในการดำเนินคดีแฮ็กเกอร์ที่อยู่ในต่างประเทศ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ถูกตั้งคำถามถึงประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีหรือแฮ็กเกอร์ แต่การศึกษาและวิจัยพบว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายที่มีประสิทธิภาพในการปราบปรามหรือดำเนินคดีกับผู้กระทำความผิดทางเทคโนโลยีหรือแฮ็กเกอร์ โดยพระราชบัญญัติฉบับนี้มีโครงสร้างของกฎหมายอาญาขั้นพื้นฐาน ซึ่งประกอบไปด้วยการกระทำความผิดและบทลงโทษไว้อย่างชัดเจน พระราชบัญญัติฉบับนี้ยังได้กำหนดบทนิยามเพื่ออธิบายความหมายของคำศัพท์ในแต่ละมาตราเพื่อให้เกิดความชัดเจนมากยิ่งขึ้น รวมทั้งยังได้กำหนดอำนาจของพนักงานเจ้าหน้าที่ในการบังคับใช้กฎหมาย เช่น อำนาจการสืบสวน สอบสวน หรือรวบรวมพยานหลักฐาน ที่สำคัญพระราชบัญญัติฉบับนี้ได้กำหนดหลักการบังคับใช้อำนาจตามกฎหมายนอกอาณาเขต (Extraterritorial Jurisdiction) เพื่อเพิ่มประสิทธิภาพในการเอาผิดหรือดำเนินคดีกับผู้กระทำความผิดที่อยู่ในต่างประเทศ นอกจากนี้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้มีการแก้ไขปรับปรุงในปี พ.ศ. 2560 เพื่อให้มีความทันสมัยต่อเหตุการณ์ในปัจจุบัน โดยกำหนดฐานความผิดขึ้นใหม่ แก้ไขฐานความผิดเดิมและกำหนดโทษของความผิดดังกล่าว พระราชบัญญัติฉบับนี้ยังได้ถูกใช้บังคับอย่างแพร่หลาย และมีการนำคดีอันเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เข้าสู่การพิจารณาของศาลฎีกา ดังนั้น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงมิใช่เป็นปัญหาหรืออุปสรรคในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ

การศึกษาและวิจัยพบว่าปัญหาหรืออุปสรรคในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศเกี่ยวข้องกับ (1) ความสามารถของพนักงานเจ้าหน้าที่ (2) กระบวนการสืบสวน สอบสวน และรวบรวมพยานหลักฐานดิจิทัลที่อยู่ในต่างประเทศ และ (3) กระบวนการนำตัวผู้กระทำความผิดมาลงโทษ กล่าวคือ เมื่อพนักงานเจ้าหน้าที่ไม่มีความสามารถหรือขาดเทคโนโลยีที่ทันสมัยในการค้นหาหรือติดตามตัวแฮ็กเกอร์ พนักงานเจ้าหน้าที่ก็ไม่สามารถดำเนินคดีกับแฮ็กเกอร์ได้ หรือหากพนักงานเจ้าหน้าที่ไม่สามารถดำเนินการสืบสวน สอบสวน และรวบรวมพยานหลักฐานดิจิทัลที่อยู่ในต่างประเทศ การดำเนินคดีกับแฮ็กเกอร์ที่อยู่

ในต่างประเทศก็ไม่สามารถทำได้ และหากประเทศผู้รับคำร้องขอปฏิเสธการส่งผู้ร้ายข้ามแดน การนำตัวแฮ็กเกอร์ที่อยู่ในต่างประเทศมารับโทษในประเทศไทยก็ไม่สามารถทำได้

8. อภิปรายผลการวิจัย

8.1 แนวทางการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ

องค์ประกอบสำคัญในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศจำต้องอาศัย (1) บทบัญญัติกฎหมาย และ (2) พยานหลักฐานดิจิทัลบนพื้นฐานของ Digital Forensics

(1) บทบัญญัติกฎหมาย

กฎหมายถือเป็นเครื่องมือสำคัญในการดำเนินคดีกับผู้กระทำความผิด สำหรับการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศนั้นจำต้องอาศัยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 และพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 เป็นเครื่องมือสำคัญในการดำเนินคดี

(2) พยานหลักฐานดิจิทัลบนพื้นฐานของ Digital Forensics

พยานหลักฐานดิจิทัลถือเป็นองค์ประกอบที่สำคัญในการดำเนินคดีอันเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือการเจาะเข้าระบบคอมพิวเตอร์[29] พยานหลักฐานดิจิทัลมีความแตกต่างจากพยานหลักฐานชนิดอื่น ๆ[30] โดยพยานหลักฐานดิจิทัล มีความหมายคือ ข้อมูลที่ได้เก็บรักษาบนสื่อบันทึกข้อมูล หรืออยู่ระหว่างการส่งรับด้วยวิธีการทางอิเล็กทรอนิกส์[31] ข้อมูลเหล่านี้ยังอาจอยู่ในรูปของไฟล์ที่อยู่ในคอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ โทรศัพท์มือถือ

---

[29] Andreas Mitrakas and Damian Zaitch, **Law, Cyber Crime and Digital Forensics: Trailing Digital Suspects** in **Digital Crime and Forensic Science in Cyberspace**, Edited by Panagiotis Kanellis and Others, First Edition (London: IDEA Group Publishing, 2006), p. 269.

[30] Ross M. Gardner and Donna R. Krouskup, **Practical Crime Scene Processing and Investigation**, Third Edition (London: CRC Press, 2018), p. 45.

[31] Richard Boddington, **Practical Digital Forensics**, First Edition (Birmingham: Packt Publishing, 2016), p. 56.

รวมถึงหลักฐานที่เกิดขึ้นจากระบบคอมพิวเตอร์ เช่น ประวัติการเข้าชม[32] ข้อมูลเหล่านี้อาจถูกนำมาใช้เป็นเครื่องมือในการกระทำความผิด บ่งชี้ถึงการกระทำความผิด หรือสามารถเชื่อมโยงกันระหว่างผู้กระทำความผิดกับผู้เสียหาย[33] ที่สำคัญข้อมูลเหล่านี้ยังสามารถนำมาใช้ในการพิจารณาคดีของศาลได้

นอกจากนี้ Digital Forensics ได้ถูกนำมาใช้ในการดำเนินการหรือพิสูจน์ตรวจสอบพยานหลักฐานดิจิทัล[34] Digital Forensics มีความหมายคือ การค้นหา รวบรวม วิเคราะห์ พิจารณา และใช้พยานหลักฐานดิจิทัลในการสืบสวน สอบสวน หรือดำเนินคดีกับผู้กระทำความผิดด้วยวิธีการทางวิทยาศาสตร์[35] ทั้งนี้เนื่องจากพยานหลักฐานดิจิทัลมีลักษณะเปราะบางและสามารถถูกแก้ไขเปลี่ยนแปลงโดยปราศจากร่องรอย Digital Forensics จึงได้ถูกนำมาใช้เพื่อให้พยานหลักฐานดิจิทัลมีความถูกต้อง (Accuracy) และน่าเชื่อถือ (Reliability) Digital Forensics ยังถือเป็นหลักเกณฑ์สำคัญในการดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี โดยประเทศที่พัฒนาแล้วล้วนใช้ Digital Forensics ในการดำเนินการกับพยานหลักฐานดิจิทัลด้วยเช่นกัน

โดยทั่วไป แนวคิดของ Digital Forensics ตั้งอยู่บนพื้นฐานของคำถามว่า “เกิดอะไรขึ้น” บนพยานหลักฐานดิจิทัล[36] โดยคำถามว่า “เกิดอะไรขึ้น” นี้หมายความว่า ได้เกิดการกระทำความผิดขึ้นหรือไม่ มีบุคคลภายนอกที่ไม่ได้อยู่ในพื้นที่ได้เข้าควบคุมคอมพิวเตอร์หรือไม่

---

[32] Don Kerr, John Gammack, and Richard Boddington “Overview of Digital Business Security Issues” in **Digital Business Security Development: Management Technologies**, Edited by Don Kerr, John G. Gammack, and Kay Bryant, First Edition (New York: Business Science Reference, 2010), p. 22.

[33] Alaa Hussein Al-Hamami and Ghossoon M. Waleed Al-Saadoon, **Handbook of Research on Threat Detection and Countermeasures in Network Security**, First Edition (Hershey: Information Science Reference, 2014), p. 144.

[34] Sasa Mrdovic, **IoT Forensics** in **Security of Ubiquitous Computing Systems: Selected Topics**, Edited by Gildas Avoine and Julio Hernandez-Castro, First Edition (Cham: Springer, 2021), p. 216.

[35] Ibid.

[36] Joakim Kavrestad, **Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications**, First Edition (Cham: Springer, 2020), p. 3.

รูปภาพหรือข้อมูลได้หายไปเมื่อใด หรือคอมพิวเตอร์ได้ถูกเจาะเข้าไปในระบบหรือไม่อย่างไร[37] จากนั้นพนักงานเจ้าหน้าที่จะใช้เครื่องมือหรือวิธีการในทางวิทยาศาสตร์ในการแสวงหาคำตอบ นอกจากนี้การตรวจสอบ Digital Forensics อาจแบ่งออกเป็น 3 ขั้นตอนซึ่งได้แก่ (1) การเก็บรวบรวม (2) การวิเคราะห์ และ (3) การรายงานผล

ตัวอย่างการใช้ Digital Forensics ในการสืบสวนหรือค้นหาตัวผู้กระทำความผิดได้แก่ นาย ก. ถูกบริษัทไล่ออกจากงาน นาย ก. จึงได้แอบปล่อยม้าโทรจัน (Trojan Horse) เข้าไปในระบบเครือข่ายคอมพิวเตอร์ของบริษัท ต่อมาบริษัทตรวจพบความผิดปกติและพบม้าโทรจันในระบบเครือข่ายคอมพิวเตอร์ของตน บริษัทจึงได้ให้ผู้เชี่ยวชาญหรือพนักงานเจ้าหน้าที่เข้าทำการตรวจสอบและเก็บรวบรวมพยานหลักฐานดิจิทัลที่เกี่ยวข้องทั้งหมด ผู้เชี่ยวชาญหรือพนักงานเจ้าหน้าที่ได้ใช้วิธีการทางวิทยาศาสตร์ในการตรวจวิเคราะห์และพบว่าม้าโทรจันได้ถูกตั้งค่าให้ส่งข้อมูลต่าง ๆ ของบริษัทไปยัง IP Address ที่ตั้งอยู่ที่บ้านของนาย ก. ดังนั้นจึงเชื่อได้ว่านาย ก. เป็นผู้ปล่อยม้าโทรจันเข้าไปในระบบเครือข่ายคอมพิวเตอร์ของบริษัท

8.2 ประสิทธิภาพของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ถือเป็นกฎหมายสำคัญที่ใช้ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีหรือการเจาะเข้าระบบคอมพิวเตอร์ โดยพระราชบัญญัติฉบับนี้ได้กำหนดขอบเขตเนื้อหา ความผิดและโทษที่ผู้กระทำความผิดต้องได้รับ อำนาจและหน้าที่ของเจ้าพนักงาน นอกจากนี้พระราชบัญญัติฉบับนี้ยังมีบทบัญญัติอันเกี่ยวกับการบังคับใช้กฎหมายนอกอาณาเขต ดังนั้น พระราชบัญญัติฉบับนี้จึงมีประสิทธิภาพที่จะดำเนินคดีกับผู้กระทำความผิดหรือแฮ็กเกอร์ที่อยู่ในต่างประเทศ สำหรับสาระสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีดังต่อไปนี้

(1) ขอบเขตและวัตถุประสงค์ของกฎหมาย

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ถูกกำหนดขึ้นเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีหรือความผิดอันเกี่ยวกับคอมพิวเตอร์ โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[37] Ibid.

ได้กำหนดเหตุผลในการประกาศบังคับใช้กฎหมายฉบับนี้ว่า *“เนื่องจากคอมพิวเตอร์เป็นส่วนสำคัญในการประกอบกิจการและดำรงชีวิตของมนุษย์ หากมีบุคคลใดกระทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งได้เป็นปกติ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไขหรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ ความเสียหายย่อมเกิดขึ้น และกระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน”* ดังนั้น การเจาะเข้าระบบคอมพิวเตอร์หรือการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาตถือเป็นความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งอาจก่อให้เกิดความเสียหายและรบกวนความสงบสุขของประชาชน พระราชบัญญัติฉบับนี้จึงสามารถเอาผิดหรือดำเนินคดีกับการเจาะเข้าระบบคอมพิวเตอร์ได้

(2) บทบัญญัติความผิดอันเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดการกระทำความผิดและโทษที่จะต้องได้รับไว้อย่างชัดเจนในหมวด 1 โดยโทษที่ผู้กระทำความผิดต้องได้รับคือ โทษจำคุกหรือปรับ และเนื่องจากอาชญากรรมทางเทคโนโลยีในปัจจุบันมีหลายรูปแบบ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงได้กำหนดบทบัญญัติอันเป็นความผิดไว้อย่างกว้าง ๆ เพื่อให้ครอบคลุมถึงการกระทำความผิดต่าง ๆ ที่อาจเกิดขึ้น ซึ่งรวมถึงการเจาะเข้าระบบคอมพิวเตอร์ในรูปแบบต่าง ๆ ด้วยเช่นกัน การกำหนดบทบัญญัติอันเป็นความผิดด้วยวิธีการดังกล่าวช่วยเพิ่มประสิทธิภาพในการเอาผิดหรือดำเนินคดีกับผู้กระทำความผิด ตัวอย่างเช่น คำว่า “เข้าถึง” ตามมาตรา 5 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นี้ได้ถูกกำหนดขึ้นอย่างกว้าง ๆ โดยไม่จำกัดวิธีการในการเข้าถึง แฮ็กเกอร์จะใช้วิธีการเข้าถึงในรูปแบบใดไม่สำคัญ หากแต่ผลลัพธ์ออกมาคือแฮ็กเกอร์ได้เข้าไปเกี่ยวข้อง แทรกแซง หรือบุกรุกระบบคอมพิวเตอร์ของผู้อื่น การกระทำนั้นถือเป็นการเข้าถึงทั้งสิ้น ดังนั้นหากแฮ็กเกอร์ใช้โปรแกรมสปายแวร์ (Spyware) เจาะระบบคอมพิวเตอร์ของบริษัทแห่งหนึ่ง แฮ็กเกอร์รายนี้อาจมีความผิดตามมาตรา 5 เพราะการใช้สปายแวร์ในการเจาะระบบคอมพิวเตอร์ถือว่าเป็นการเข้าถึงระบบคอมพิวเตอร์

(3) อำนาจของพนักงานเจ้าหน้าที่

อำนาจของพนักงานเจ้าหน้าที่ถือเป็นเครื่องมือในการบังคับใช้กฎหมายให้มีประสิทธิภาพ[38] ซึ่งหากกฎหมายไม่ได้ให้อำนาจแก่พนักงานเจ้าหน้าที่ในการใช้บังคับ กฎหมายนั้นอาจไม่มีประสิทธิภาพหรือไม่มีผลใช้บังคับ เมื่อเป็นเช่นนี้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดอำนาจของพนักงานเจ้าหน้าที่ในการบังคับใช้กฎหมายไว้ในหมวด 2 โดยพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้มิใช่เจ้าพนักงานทั่วไป แต่ต้องเป็นผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้ และมีคุณสมบัติเป็นไปตามประกาศกฎกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเรื่อง “หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550”

อำนาจของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ถูกกำหนดขึ้นเพื่อให้การบังคับใช้กฎหมายเป็นไปอย่างมีประสิทธิภาพและตรงตามวัตถุประสงค์ของกฎหมาย ต่อมาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ถูกแก้ไขเพิ่มเติมเพื่อให้สอดคล้องกับการป้องกันและปราบปรามการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งก็ได้รวมถึงการเพิ่มประสิทธิภาพในการใช้อำนาจของพนักงานเจ้าหน้าที่ ตัวอย่างเช่น มาตรา 18 (2) และ (3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดให้พนักงานเจ้าหน้าที่สามารถเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ หรือสั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการให้แก่พนักงานเจ้าหน้าที่ และต่อมาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ถูกแก้ไขเพิ่มเติม โดยมาตรา 18 วรรคสาม แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับที่ 2) ได้เพิ่มประสิทธิภาพการใช้อำนาจของพนักงานเจ้าหน้าที่ ด้วยการกำหนดให้ผู้ให้บริการที่ได้รับคำร้องขอดังกล่าวจากพนักงานเจ้าหน้าที่ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกิน 7 วันนับแต่วันที่ได้รับคำร้องขอ แต่อย่างไรก็ตาม การใช้อำนาจของพนักงานเจ้าหน้าที่ดังกล่าวนี้ต้องนำไปใช้เพื่อการสืบสวน

[38] John E. Hess, **Interrogation for Law Enforcement**, Second Edition (New Jersey: Matthew Bender & Company, Inc., 2010), p. 82.

และสอบสวนเท่านั้น และต้องกระทำเฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(4) การบังคับใช้อำนาจตามกฎหมายนอกอาณาเขต (Extraterritorial Jurisdiction)

การบังคับใช้อำนาจตามกฎหมายนอกอาณาเขต คือ การที่รัฐสามารถใช้อำนาจตามกฎหมายภายในของตนบังคับเอากับบุคคลหรือทรัพย์สินที่อยู่นอกเหนือดินแดนของตน[39] แม้การกระทำความผิดนั้นจะไม่ได้เกิดขึ้นภายในดินแดนประเทศของตนก็ตาม แต่เป็นการกระทำความผิดที่รัฐบาลหรือบุคคลในประเทศของตนเป็นผู้เสียหาย หลักการบังคับใช้อำนาจตามกฎหมายนอกอาณาเขตมีความสำคัญเป็นอย่างมากในปัจจุบัน เพราะหลักดังกล่าวนี้ช่วยเพิ่มขอบเขตและประสิทธิภาพในการใช้บังคับกฎหมายให้มีมากยิ่งขึ้น[40] โดยผู้กระทำความผิดที่อยู่ในต่างประเทศไม่สามารถหลบหนีความผิดที่ตนได้เคยกระทำไว้ในประเทศอื่นได้ หลักการบังคับใช้อำนาจตามกฎหมายนอกอาณาเขตยังได้ถูกนำมาใช้ในความผิดอันเกี่ยวกับอาชญากรรมทางเทคโนโลยีมากขึ้น โดยหลักการบังคับใช้อำนาจตามกฎหมายนอกอาณาเขตได้ปรากฏอยู่ในกฎหมายว่าด้วยการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ในหลาย ๆ ประเทศ[41]

สำหรับประเทศไทยนั้น หลักการบังคับใช้อำนาจตามกฎหมายนอกอาณาเขตได้ปรากฏอยู่ในมาตรา 17 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยมาตรา 17 ได้บัญญัติว่า *“ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ... (2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษในราชอาณาจักร”* บทบัญญัติดังกล่าวนี้ได้แสดง

---

[39] Christina Voigt, **Up in the Air: Aviation, the EU Missions Trading Scheme and the Question of Jurisdiction** in **Cambridge Yearbook of European Legal Studies**, Edited by Catherine Barnard, Markus Gehring, and Iyiola Solanke, First Edition (Oregon: Hart Publishing, 2012), p. 496. (Extraterritorial jurisdiction is the legal ability of a state to exercise authority over actors and activities beyond its boundaries.)

[40] Hiromi Sato, **Multilayered Structures of International Criminal Law**, First Edition (Cham: Springer, 2021), p. 141.

[41] Danielle Ireland-Piper, **Extraterritoriality in East Asia: Extraterritorial Criminal Jurisdiction in China, Japan, and South Korea**, First Edition (Massachusetts: Edward Elgar Publishing, 2021), p. 106.

ให้เห็นว่า แม้การกระทำความผิดได้เกิดขึ้นนอกราชอาณาจักรก็ตาม แต่หากผลของการกระทำนั้นได้เกิดขึ้นกับคนไทยหรือรัฐบาลไทยในราชอาณาจักร พระราชบัญญัติฉบับนี้ย่อมมีผลต่อผู้กระทำความผิดที่อยู่นอกราชอาณาจักร โดยพนักงานเจ้าหน้าที่สามารถดำเนินคดีกับผู้กระทำความผิดที่อยู่นอกราชอาณาจักรได้ และเมื่อการเจาะเข้าระบบคอมพิวเตอร์เป็นอาชญากรรมข้ามชาติที่สามารถสร้างความเสียหายให้กับประเทศอื่น มาตรา 17 (2) จึงช่วยให้พนักงานเจ้าหน้าที่สามารถดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ แม้แฮ็กเกอร์ผู้นั้นจะไม่ได้ลงมือกระทำความผิดในราชอาณาจักรก็ตาม

8.3 ปัญหาและอุปสรรคในการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ

(1) ความสามารถของพนักงานเจ้าหน้าที่ในประเทศไทย

การเก็บรวบรวมและพิสูจน์ตรวจสอบพยานหลักฐานดิจิทัลบนพื้นฐานของ Digital Forensics มีความสำคัญต่อการสืบสวน สอบสวน หรือดำเนินคดีกับอาชญากรรมทางเทคโนโลยีเป็นอย่างยิ่ง ดังนั้น Digital Forensics ได้ถูกนำมาใช้ในการสืบสวน สอบสวน หรือรวบรวมพยานหลักฐานดิจิทัลในประเทศไทยด้วยเช่นกัน ตัวอย่างเช่น มาตรา 18 (6) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจในการ “ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวข้องเท่าที่จำเป็น” โดยการตรวจสอบข้อมูลคอมพิวเตอร์นี้ถือเป็นกระบวนการขั้นพื้นฐานของ Digital Forensics

แต่อย่างไรก็ตาม Digital Forensics ยังถือเป็นเรื่องใหม่สำหรับประเทศไทย โดยงานวิจัยเรื่อง “การศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลในงานนิติวิทยาศาสตร์” ได้สรุปผลการวิจัยไว้ว่า ประเทศไทยยังไม่มีวิธีการหรือมาตรฐานในการดำเนินการ Digital Forensics ที่ชัดเจน อีกทั้งยังขาดแคลนเครื่องมือที่ใช้ในการดำเนินการตาม Digital Forensics พนักงานเจ้าหน้าที่ที่ปฏิบัติหน้าที่ยังคงขาดความรู้ความเข้าใจในเรื่อง Digital Forensics เช่น ไม่ทราบถึงวิธีการจัดการกับพยานหลักฐานดิจิทัล ไม่ทราบถึงวิธีการทำให้พยานหลักฐานดิจิทัลมีความถูกต้องและน่าเชื่อถือ หรือไม่ทราบถึงวิธีการเก็บรักษาพยานหลักฐานดิจิทัลให้มีความสมบูรณ์

มากที่สุด[42] ที่สำคัญ พนักงานเจ้าหน้าที่ไม่สามารถวิเคราะห์หรือเชื่อมโยงพยานหลักฐานดิจิทัลที่ปรากฏได้ เช่น ไม่สามารถหาความเชื่อมโยงระหว่างผู้กระทำความผิดกับอุปกรณ์ที่ใช้กระทำความผิดได้ หรือไม่สามารถวิเคราะห์ข้อมูลและเชื่อมโยงข้อมูลเข้ากับผู้กระทำความผิดและผู้เสียหายได้ ดังนั้น พนักงานเจ้าหน้าที่จึงไม่สามารถเก็บรวบรวมหรือดำเนินการใด ๆ กับพยานหลักฐานดิจิทัลได้ หรือหากมีการเก็บรวบรวมหรือดำเนินการดังกล่าว พยานหลักฐานดิจิทัลนั้นก็อาจเป็นพยานหลักฐานที่ไม่มีคุณภาพ

การสืบสวน สอบสวน และรวบรวมพยานหลักฐานดิจิทัลเพื่อดำเนินคดีกับแฮ็กเกอร์ยังถือเป็นเรื่องที่ยากลำบาก เพราะแฮ็กเกอร์ในปัจจุบันมีความเชี่ยวชาญและมีความสามารถสูงในการลงมือกระทำความผิด โดยเฉพาะอย่างยิ่ง แฮ็กเกอร์เหล่านี้มักมีวิธีการในการกระทำความผิดในรูปแบบใหม่และมีประสิทธิภาพมากขึ้นกว่าเดิม และมีความสามารถในการทำลายหรือเปลี่ยนแปลงแก้ไขพยานหลักฐานดิจิทัลจนไม่เหลือร่องรอย รวมถึงมีเครื่องมือที่ใช้ในการซ่อนเร้น IP Address ของตน ตัวอย่างเช่น แฮ็กเกอร์อาจใช้ Proxy ในการหลบซ่อนด้วยการปกปิด IP Address ที่แท้จริงของตนและแสดง IP Address อื่นให้ปรากฏ[43] แฮ็กเกอร์ยังใช้วิธีการเปลี่ยนแปลงข้อมูลจราจรคอมพิวเตอร์และซ่อน IP Address ของตน โดยแฮ็กเกอร์มักนิยมใช้ซอฟต์แวร์สำหรับเปิดใช้งานเพื่อการสื่อสารแบบไม่ระบุตัวตน (The Onion Router หรือ “Tor”) ในการปฏิบัติการดังกล่าว[44] นอกจากนี้แฮ็กเกอร์มักดำเนินกิจกรรมต่าง ๆ บนเว็บไซต์ที่ไม่ปรากฏในฐานข้อมูล (Dark Web) ซึ่งทำให้ยากต่อการติดตาม เพราะเว็บไซต์ดังกล่าวเปิดให้บริการแก่บุคคลเฉพาะกลุ่มและยังใช้โปรแกรมป้องกันการเข้าถึงจากบุคคลภายนอก[45] ดังนั้นพนักงานเจ้าหน้าที่จึงไม่อาจสืบทราบหรือติดตามตัวผู้กระทำความผิดเพราะการติดตาม IP Address ของแฮ็กเกอร์เหล่านี้ต้องใช้เครื่องมือที่ทันสมัยและพนักงาน

---

[42] จิตชนก อินถามา และวงศ์ยศ เกิดศรี, **การศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลในงานนิติวิทยาศาสตร์**, วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ, ปีที่ 7 ฉบับที่ 1 (มิถุนายน 2564), หน้า 134-150.

[43] United Nations Office on Drugs and Crime (UNODC), **Obstacles to Cybercrime Investigations** [Online], 15 December 2021. Source: https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html

[44] Ibid.

[45] Ibid.

เจ้าหน้าที่ที่มีความรู้และความเชี่ยวชาญในคอมพิวเตอร์ แต่ประเทศไทยยังคงขาดแคลนเครื่องมือและบุคลากรที่มีความรู้และความเชี่ยวชาญในเรื่องดังกล่าว

ปัญหาสำคัญอีกประการหนึ่งในการดำเนินคดีกับแฮ็กเกอร์ที่มีความสามารถสูง คือ บุคคลกลุ่มนี้อาศัยอยู่ในต่างประเทศ และได้กระทำความผิดในประเทศไทย หากพนักงานเจ้าหน้าที่ต้องการที่จะสืบสวนหรือดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ พนักงานเจ้าหน้าที่ต้องเก็บรวบรวมพยานหลักฐานดิจิทัลต่าง ๆ ที่อยู่ในต่างประเทศ หากพนักงานเจ้าหน้าที่ไม่สามารถเก็บรวบรวมหรือตรวจสอบพยานหลักฐานดิจิทัลได้ การดำเนินคดีกับผู้กระทำความผิดหรือแฮ็กเกอร์ที่อยู่ในต่างประเทศก็ไม่สามารถทำได้ นอกจากนี้พนักงานเจ้าหน้าที่ต้องอาศัยการขอความช่วยเหลือหรือความร่วมมือระหว่างประเทศในคดีอาญา หากประเทศผู้รับคำร้องขอปฏิเสธให้ความช่วยเหลือหรือความร่วมมือกับประเทศไทยในการสืบสวนสอบสวน และเก็บรวบรวมพยานหลักฐานดิจิทัล พนักงานเจ้าหน้าที่ย่อมไม่สามารถดำเนินคดีกับผู้กระทำความผิดหรือแฮ็กเกอร์ซึ่งอยู่ในต่างประเทศได้ และหากพนักงานเจ้าหน้าที่ต้องการที่จะนำตัวแฮ็กเกอร์ที่อยู่ในต่างประเทศมารับโทษตามกฎหมายไทย พนักงานเจ้าหน้าที่ต้องดำเนินการขอให้ส่งตัวผู้ร้ายข้ามแดน กระบวนการดังกล่าวนี้เป็นเรื่องที่ยากลำบาก สลับซับซ้อน และยังมีอุปสรรคในทางกฎหมายอีกมาก

(2) การขอความช่วยเหลือหรือความร่วมมือระหว่างประเทศในคดีอาญา

โดยทั่วไป การรวบรวมพยานหลักฐานดิจิทัลมีความหมายคือ กระบวนการค้นหา ระบุ รวมรวม ได้มา และรักษาข้อมูลหรือพยานดิจิทัลจากเครื่องคอมพิวเตอร์หรือชุดอุปกรณ์จัดเก็บเพื่อดำเนินคดีกับผู้กระทำความผิด[46] แต่วิธีการสืบสวน สอบสวน และรวบรวมพยานหลักฐานดิจิทัลภายในประเทศและต่างประเทศมีความแตกต่างกัน หากพนักงานเจ้าหน้าสามารถค้นหาหรือระบุ IP Address ของแฮ็กเกอร์ได้ และตรวจสอบพบว่า IP Address ดังกล่าวอยู่ในประเทศไทย พนักงานเจ้าหน้าที่อาจดำเนินการขอให้ศาลออกหมายค้นเพื่อเก็บรวบรวมพยานหลักฐานดิจิทัลอื่น ๆ ประกอบการสืบสวนหรือสอบสวน หากพนักงานเจ้าหน้าที่พบว่า IP Address ของแฮ็กเกอร์อยู่ในต่างประเทศ หรือแฮ็กเกอร์เป็นชาวต่างชาติและก่อเหตุในต่างประเทศ พนักงานเจ้าหน้าที่ไม่สามารถใช้อำนาจตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[46] Kamlesh K. Bajaj and Debjani Nag, **E-Commerce: The Cutting Edge of Business**, Second Edition (New Delhi: Tata McGraw-Hill Publishing Company Limited, 2005), p. 291.

เพื่อเก็บรวบรวมพยานหลักฐานดิจิทัลที่อยู่ในต่างประเทศได้ แต่พนักงานเจ้าหน้าที่อาจขอความช่วยเหลือหรือความร่วมมือระหว่างประเทศในการสืบสวน สอบสวน และรวบรวมพยานหลักฐานดิจิทัล ซึ่งในกรณีดังกล่าวนี้ พนักงานเจ้าหน้าที่อาจใช้วิธีการประสานงานกับต่างประเทศโดยผ่านองค์การตำรวจอาชญากรรมระหว่างประเทศ (International Criminal Police Organization - INTERPOL) วิธีการดังกล่าวนี้ไม่ใช่วิธีการที่เป็นทางการ แต่เป็นเพียงการช่วยเหลือซึ่งกันและกัน ซึ่งอาจไม่เหมาะสมกับการเก็บรวบรวมพยานหลักฐานดิจิทัล และนอกจากนี้ พนักงานเจ้าหน้าที่อาจใช้วิธีการที่เป็นทางการโดยอาศัยพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 เพื่อการสืบสวน สอบสวน และเก็บรวบรวมพยานหลักฐานดิจิทัลที่อยู่ในต่างประเทศ

พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 ได้กำหนดขอบเขตความร่วมมือระหว่างประเทศในการสอบสวนและการสืบพยานหลักฐาน การจัดหาและการให้เอกสารหรือข่าวสารที่อยู่ในความครอบครองของหน่วยงานของรัฐ การจัดส่งเอกสาร การค้นและยึด การสืบหาบุคคล การริบและการยึดทรัพย์สิน ดังนั้นพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 จึงสามารถนำมาใช้ในการสืบสวน สอบสวน และรวบรวมพยานหลักฐานดิจิทัลที่อยู่ในต่างประเทศ และหากพนักงานเจ้าหน้าที่ประสงค์ที่จะขอความช่วยเหลือหรือความร่วมมือจากต่างประเทศ พนักงานเจ้าหน้าที่ต้องเสนอเรื่องต่อผู้ประสานงานกลาง ซึ่งเป็นผู้มีอำนาจหน้าที่ประสานงานในการขอความช่วยเหลือจากต่างประเทศ คำขอความช่วยเหลือจากต่างประเทศและเอกสารทั้งหมดจะต้องทำตามแบบหลักเกณฑ์ วิธีการและเงื่อนไขที่ผู้ประสานงานกลางได้กำหนดไว้ และผู้ประสานงานกลางยังเป็นผู้พิจารณาว่าสมควรจะขอความช่วยเหลือจากต่างประเทศหรือไม่ โดยพิจารณาถึงหลักเกณฑ์ รายละเอียด ข้อเท็จจริง และเอกสารประกอบ หากผู้ประสานงานกลางเห็นสมควรขอความช่วยเหลือจากต่างประเทศ ให้ผู้ประสานงานกลางส่งคำร้องนั้นไปยังประเทศผู้รับคำร้องขอ พนักงานเจ้าหน้าที่ยังต้องปฏิบัติตามพันธกรณีที่ประเทศไทยมีอยู่ต่อประเทศผู้รับคำร้องขอในการใช้ข่าวสารหรือพยานหลักฐานตามวัตถุประสงค์ที่ระบุในคำขอ

แต่อย่างไรก็ตาม พนักงานเจ้าหน้าที่อาจเผชิญปัญหาหรืออุปสรรคในการขอความช่วยเหลือหรือความร่วมมือในการสืบสวน สอบสวน และรวบรวมพยานหลักฐานดิจิทัลที่อยู่ในต่างประเทศ โดยปัญหาหรืออุปสรรคดังกล่าวอาจมีดังต่อไปนี้

(ก) ประเทศผู้รับคำร้องขอไม่มีกฎหมายว่าด้วยการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์

ประเทศส่วนใหญ่บนโลกใบนี้ล้วนมีกฎหมายว่าด้วยการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ แต่ในขณะเดียวกัน ยังคงมีอีกหลายประเทศที่ยังไม่มีกฎหมายว่าด้วยการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ ตัวอย่างเช่น หลายประเทศในทวีปแอฟริกายังคงไม่มีกฎหมายว่าด้วยการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์[47] การที่ประเทศไม่มีกฎหมายฉบับดังกล่าวนี้ย่อมส่งผลให้การสืบสวนหรือสอบสวนความผิดทางเทคโนโลยีหรือการเจาะเข้าระบบคอมพิวเตอร์ระหว่างประเทศเป็นเรื่องที่ยากลำบาก อีกทั้งประเทศเหล่านั้นยังกลายเป็นแหล่งกบดานหรือสร้างผู้กระทำความผิดทางเทคโนโลยีหรือแฮ็กเกอร์[48] เพราะบุคคลเหล่านั้นไม่ถือว่าเป็นผู้กระทำความผิดและไม่ต้องได้รับโทษแต่อย่างใด เมื่อประเทศผู้รับคำร้องขอไม่มีกฎหมายว่าด้วยการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ ประเทศผู้รับคำร้องขออาจไม่ดำเนินการใด ๆ ตามที่พนักงานเจ้าหน้าที่ของประเทศไทยร้องขอ เพราะถือว่าการกระทำนั้นไม่เป็นความผิดในประเทศตน

(ข) ประเทศผู้รับคำร้องขอปฏิเสธให้ความร่วมมือ

ประเทศผู้รับคำร้องขอสามารถปฏิเสธการให้ความช่วยเหลือหรือความร่วมมือในคดีอาญากับประเทศผู้ร้องขอ หากการให้ความช่วยเหลือหรือความร่วมมือในคดีอาญานั้นขัดแย้งกับแนวนโยบายแห่งรัฐ หรือกระทบกระเทือนอำนาจอธิปไตยหรือความมั่นคงของประเทศผู้รับคำร้อง[49] การให้ความช่วยเหลือหรือความร่วมมือระหว่างประเทศในคดีอาญาจึงเป็นเรื่องของดุลยพินิจของประเทศผู้รับคำร้องขอ และในหลาย ๆ กรณีที่เกิดขึ้น แม้ประเทศผู้รับคำร้องขอและประเทศผู้ร้องขอได้ทำสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญา (Treaty on Mutual Legal Assistance in Criminal Matters - MLAT) แต่ประเทศผู้รับคำร้องขอได้ปฏิเสธให้ความช่วยเหลือหรือความร่วมมือในคดีอาญากับประเทศผู้ร้องขอ

---

[47] Ziska Fields, **Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution**, First Edition (Hershey: IGI Global, 2018), p. 369.

[48] Ibid.

[49] Alison Bisset, **Truth Commissions and Criminal Courts**, First Edition (New York: Cambridge University Press, 2012), p. 161.

เพราะมีประเด็นที่ขัดแย้งกับแนวนโยบายแห่งรัฐหรือแนวทางปฏิบัติของประเทศ[50] ตัวอย่างเช่น ประเทศไทยได้ทำสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญา (The Treaty on Mutual Legal Assistance in Criminal Matters among Linked-Minded ASEAN Member Countries - MLAT ASEAN) กับประเทศกลุ่มสมาชิกอาเซียนอีก 9 ประเทศ แต่ในทางปฏิบัตินั้น ประเทศในกลุ่มสมาชิกอาเซียนยังคงปฏิเสธให้ความช่วยเหลือหรือความร่วมมือในคดีอาญา โดยประเทศกลุ่มสมาชิกมักไม่ดำเนินการตามคำร้องขอ ถึงแม้จะมีสนธิสัญญาระหว่างกันก็ตาม เช่น สาธารณรัฐประชาธิปไตยประชาชนลาว ปฏิเสธการส่งหมายนัดตามคำร้องขอของประเทศไทย โดยให้เหตุผลว่าเนื่องจากมีการส่งหมายนัดมาจำนวนมาก จึงไม่สามารถดำเนินการได้ทัน[51]

สำหรับคดีอันเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือการเจาะเข้าระบบคอมพิวเตอร์นั้น แต่ละประเทศมักมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และนโยบายที่เกี่ยวกับอาชญากรรมทางเทคโนโลยีที่แตกต่างกันออกไป และความแตกต่างทางด้านกฎหมายและนโยบายนี้ได้ส่งผลกระทบต่อการให้ความช่วยเหลือหรือความร่วมมือระหว่างประเทศในคดีอาญาด้วยเช่นกัน ตัวอย่างเช่น ประเทศรัสเซียเคยปฏิเสธให้ความช่วยเหลือหรือความร่วมมือในการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีจากประเทศเอสโตเนีย เพราะประเทศรัสเซียมีการประเมินความเสี่ยงในการประกอบอาชญากรรมทางเทคโนโลยีที่แตกต่างไปจากประเทศเอสโตเนีย[52] ดังนั้น แม้ประเทศไทยในฐานะประเทศผู้ร้องขอได้ดำเนินการถูกต้องตามที่พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 กำหนดไว้แล้วก็ตาม แต่ก็มิได้หมายความว่าประเทศผู้รับคำขอต้องดำเนินการตามที่ประเทศไทยร้องขอเสมอไป ประเทศผู้รับคำขออาจปฏิเสธให้ความช่วยเหลือหรือความร่วมมือในการสืบสวนหรือสอบสวนอาชญากรรมทางเทคโนโลยีของประเทศไทยได้ หากคำร้องขอความช่วยเหลือหรือความร่วมมือ

---

[50] พงศ์กุลธร โรจน์วิรุฬห์ วีรพล กุลบุตร และชวนัสถ์ เจนการ, **ปัญหาและอุปสรรคในการดำเนินความร่วมมือระหว่างประเทศในเรื่องทางอาญาในกลุ่มประเทศอาเซียน**, วารสารกระบวนการยุติธรรม, ปีที่ 11 ฉบับที่ 3 (กันยายน 2561), หน้า 113-132.

[51] เรื่องเดียวกัน

[52] Tine Munk, **Policing Virtual Spaces: Public and Private Online Challenges in A Legal Perspective** in **Comparative Policing Form a Legal Perspective**, Edited by Monica den Boer, First Edition (Cheltenham: Edward Elgar Publishing, 2018), p. 240.

ในอาชญากรรมทางเทคโนโลยีของประเทศไทยขัดแย้งกับกฎหมาย นโยบายแห่งรัฐ หรือกระทบกระเทือนความมั่นคงและความปลอดภัยของประเทศผู้รับคำร้องขอ และเมื่อประเทศผู้รับคำขอปฏิเสธให้ความช่วยเหลือหรือความร่วมมือในการสืบสวนหรือสอบสวน พนักงานเจ้าหน้าที่ของรัฐบาลไทยก็ไม่สามารถเก็บรวบรวมพยานหลักฐานดิจิทัลและดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศได้

(ค) ความล่าช้าในการดำเนินการ

ความล่าช้าในการดำเนินการเป็นอีกหนึ่งอุปสรรคในการขอความช่วยเหลือหรือความร่วมมือระหว่างประเทศในคดีอาญา เนื่องจากการขอความช่วยเหลือหรือความร่วมมือระหว่างประเทศในคดีอาญามักกระทำในรูปแบบอย่างเป็นทางการ ความล่าช้าในการดำเนินการจึงมักเกิดขึ้น[53] และอาจเกิดขึ้นจากกระบวนการภายในประเทศผู้ร้องขอ และจากกระบวนการภายในประเทศของผู้รับคำร้องขอ โดยเฉพาะอย่างยิ่ง ความล่าช้าในการดำเนินการมักเกิดขึ้นเนื่องจากการขอความช่วยเหลือหรือความร่วมมือระหว่างประเทศในคดีอาญาไม่ได้กำหนดกรอบระยะเวลาไว้[54] กระบวนการในการดำเนินการจึงมักใช้ระยะเวลานาน เช่น พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 ได้กำหนดวิธีการขอความช่วยเหลือไว้ในส่วนที่ 10 ตั้งแต่มาตรา 36 จนถึงมาตรา 41 แต่ไม่มีบทบัญญัติใดที่กำหนดกรอบระยะเวลาในการดำเนินการ นอกจากนี้ระเบียบของผู้ประสานงานกลางว่าด้วยการให้ความช่วยเหลือและการขอความช่วยเหลือตามกฎหมายว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2537 ก็ไม่ได้กำหนดกรอบระยะเวลาในการดำเนินการไว้ด้วยเช่นกัน ส่งผลให้ระยะเวลาในการดำเนินการจึงอาจขึ้นอยู่กับหน่วยงานของรัฐที่ประสงค์จะขอความช่วยเหลือและผู้ประสานงานกลางนั้นเอง

ความล่าช้าจากกระบวนการภายในประเทศของผู้รับคำร้องขออาจเกิดขึ้น เนื่องจากประเทศผู้รับคำร้องขอต้องตรวจสอบและพิจารณาคำร้องขอและเอกสารต่าง ๆ ที่เกี่ยวข้อง หากประเทศของผู้รับคำร้องเห็นว่าสามารถดำเนินการตามคำร้องขอได้ ก็อาจดำเนินการขั้นต่อไป

---

[53] Klaus von Lampe, **Transnational Crime** in **International and Transnational Crime and Justice**, Edited by Mangai Natarajan, Second Edition (New York: Cambridge University Press, 2019), p. 172.

[54] Ibid.

ด้วยการส่งคำร้องขอนั้นไปยังหน่วยงานที่ดูแลรับผิดชอบหรือที่เกี่ยวข้องกับเรื่องนั้นโดยตรง และหากเรื่องที่ร้องขอความช่วยเหลือหรือความร่วมมือมีความสลับซับซ้อน การดำเนินการตามคำร้องขอย่อมต้องใช้ระยะเวลานาน นอกจากนี้ ประเทศผู้ร้องขอไม่สามารถบังคับหรือกำหนดกรอบระยะเวลาให้ประเทศของผู้รับคำร้องขอปฏิบัติตาม แม้การขอความช่วยเหลือหรือความร่วมมือระหว่างประเทศในคดีอาญาที่ได้ทำขึ้นบนพื้นฐานการให้ความช่วยเหลือซึ่งกันและกันหรือหลักถ้อยทีถ้อยปฏิบัติต่อกัน หรือการขอความช่วยเหลือหรือความร่วมมือระหว่างประเทศในคดีอาญาที่ได้ทำขึ้นบนพื้นฐานสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญา (MLAT) ก็ตาม ดังนั้น การดำเนินการตามคำร้องขอจึงไม่อาจมีกำหนดระยะเวลาที่แน่นอน ซึ่งอาจก่อให้เกิดความล่าช้าขึ้นได้

ความล่าช้าในการดำเนินการส่งผลกระทบต่อการเก็บรวบรวมพยานหลักฐานดิจิทัล เนื่องจากพยานหลักฐานดิจิทัลมักอยู่ในรูปแบบของข้อมูลที่ถูกจัดเก็บไว้ในสื่อบันทึกหรืออุปกรณ์ทางอิเล็กทรอนิกส์ต่าง ๆ เช่น ในเครื่องคอมพิวเตอร์ พยานหลักฐานดิจิทัลเหล่านี้มีความเปราะบางสูงและถูกเปลี่ยนแปลงได้ง่าย[55] อีกทั้งยังอาจถูกทำลายหรือสูญหายได้ตลอดเวลา[56] การเก็บรวบรวมพยานหลักฐานดิจิทัลจึงควรดำเนินการโดยทันทีภายหลังจากการกระทำความผิดได้เกิดขึ้น[57] แต่หากพยานหลักฐานดิจิทัลได้ถูกเก็บรวบรวมภายหลังจากการกระทำความผิดได้เกิดขึ้นเป็นระยะเวลานาน พยานหลักฐานดิจิทัลหรือข้อมูลต่าง ๆ อาจสูญหาย ถูกทำลาย หรือถูกดัดแปลง ซึ่งส่งผลกระทบต่อการดำเนินคดีกับผู้กระทำความผิด ดังนั้น ความล่าช้าในการขอหรือให้ความช่วยเหลือหรือความร่วมมือระหว่างประเทศในคดีอาญาอาจส่งผลกระทบต่อการเก็บรวบรวมพยานหลักฐานดิจิทัล รวมถึงการสืบสวน สอบสวน และดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ[58]

---

[55] James E. Girard, **Criminalistics**, Fifth Edition (Burlington: World Headquarters, 2021), p. 380.

[56] Ibid.

[57] Steve Bunting and Steve Anson, **Mastering Windows Network Forensics and Investigation**, First Edition (Indiana: Wiley Publishing Inc., 2007), p. 13.

[58] Balsing Rajput, **Cyber Economic Crime in India: An Integrated Model for Prevention and Investigation**, First Edition (Cham: Springer, 2021), p. 219.

(ง) ประเทศผู้รับคำร้องขอมีข้อจำกัดในด้านความสามารถ

การเก็บรวบรวมพยานหลักฐานดิจิทัลบนพื้นฐานของ Digital Forensics หรือการดำเนินคดีเกี่ยวกับอาชญากรรมทางเทคโนโลยีจำต้องอาศัยทรัพยากรบุคคล งบประมาณจำนวนมาก ข้อมูลที่มีความทันสมัย ทักษะความรู้ชั้นสูง และเทคโนโลยีสมัยใหม่[59] เพื่อช่วยให้การสืบสวนและสอบสวนอาชญากรรมทางเทคโนโลยีเป็นไปอย่างมีประสิทธิภาพ ตัวอย่างเช่น สำนักงานสอบสวนกลางแห่งประเทศสหรัฐอเมริกาหรือเอฟบีไอ (FBI) ได้ใช้งบประมาณจำนวนมากในการซื้อเครื่องมือหรือซอฟต์แวร์ (Software) เพื่อป้องกันและค้นหาการโจมตีหรือการเจาะเข้าระบบคอมพิวเตอร์ที่มาจากต่างประเทศ[60] แต่อย่างไรก็ตาม หลายประเทศยังคงประสบปัญหาในการขาดแคลนทรัพยากรบุคคล งบประมาณ ผู้เชี่ยวชาญที่มีทักษะความรู้ และเทคโนโลยีสมัยใหม่ที่สามารถสืบสวนและสอบสวนอาชญากรรมทางเทคโนโลยีหรือแฮ็กเกอร์[61] เมื่อเป็นเช่นนี้ หากประเทศผู้รับคำร้องขอไม่มีศักยภาพหรือความสามารถที่เพียงพอในการให้ความช่วยเหลือหรือความร่วมมือ ก็ย่อมมีความเป็นไปได้ที่ประเทศผู้รับคำร้องขอไม่อาจดำเนินการตามที่ประเทศผู้ร้องขอต้องการได้

(3) การขอให้ส่งผู้ร้ายข้ามแดน

การส่งผู้ร้ายข้ามแดน คือ การส่งมอบตัวบุคคลผู้กระทำความผิดจากประเทศผู้รับคำขอไปยังประเทศผู้ร้องขอเพื่อถูกดำเนินคดีอาญาหรือรับโทษทางอาญา[62] แม้ผู้กระทำความผิดได้

---

[59] Jason Sachowski, **Implementing Digital Forensic Readiness: From Reactive to Proactive Process**, Second Edition (New York: CRC Press, 2019), p. 63.

[60] Christopher Wray, **The FBI and the Private Sector: Battling the Cyber Threat Together** [Online], 15 December 2021. Source: https://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-battling-the-cyber-threat-together-012821

[61] Raja Jabir and Omar Alfandi, **Cloud Digital Forensics Evaluation and Crimes Detection** in **Emerging Technologies for Developing Countries: First International EAI Conference, AFRICATEK 2017 Marrakech, Morocco, March 27-28, 2017 Proceedings**, Edited by Fatna Belqasmi and Others, First Edition (Cham: Springer, 2017), p. 179.

[62] Legal Information Institute (LII), **Extradition** [Online], 15 December 2021. Source: https://www.law.cornell.edu/wex/extradition#:~:text=Extradition%20is%20the%20removal%20of,from%20one%20jurisdiction%20to%20another

หลบหนีไปยังประเทศอื่นหรือพำนักอยู่ในประเทศของตนเองก็ตาม โดยทั่วไปการส่งผู้ร้ายข้ามแดนมักกระทำขึ้นบนพื้นฐานของสนธิสัญญาระหว่างประเทศว่าด้วยเรื่องการส่งผู้ร้ายข้ามแดน หรือหากไม่มีสนธิสัญญาระหว่างประเทศ การส่งผู้ร้ายข้ามแดนสามารถกระทำขึ้นได้โดยอาศัยหลักถ้อยทีถ้อยอาศัย ในปัจจุบันนี้ อาชญากรรมทางเทคโนโลยีระหว่างประเทศได้เพิ่มมากขึ้นตามการเปลี่ยนแปลงของโลกและวิวัฒนาการทางเทคโนโลยี[63] การส่งผู้ร้ายข้ามแดนจึงถือเป็นเครื่องมือสำคัญในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีระหว่างประเทศ อีกทั้งการส่งผู้ร้ายข้ามแดนในคดีอันเกี่ยวกับอาชญากรรมทางเทคโนโลยีมักปรากฏให้เห็นอยู่เสมอ ตัวอย่างเช่น Mr. Vladimir Dunaev แฮ็กเกอร์ชาวรัสเซียถูกประเทศสหรัฐอเมริกากล่าวหาว่าได้ใช้ Trickbot Malware ในการโจมตีทางไซเบอร์ช่วงระหว่างปี ค.ศ. 2015 จนถึงปี ค.ศ. 2020 ต่อมา Mr. Vladimir Dunaev ได้ถูกจับกุมที่ประเทศเกาหลีใต้ และถูกส่งตัวในฐานะผู้ร้ายข้ามแดนมายังประเทศสหรัฐอเมริกาเพื่อถูกดำเนินคดีต่อไป[64]

หลักเกณฑ์การส่งผู้ร้ายข้ามแดนของประเทศไทยนั้น ในเบื้องต้นจำต้องพิจารณาว่าประเทศไทยได้ทำสนธิสัญญาส่งผู้ร้ายข้ามแดนไว้กับประเทศอื่นหรือไม่ หากประเทศไทยได้ทำสนธิสัญญาส่งผู้ร้ายข้ามแดนไว้กับประเทศคู่สัญญา ก็จะต้องพิจารณาตามพระราชบัญญัติที่อนุวัติการตามสนธิสัญญากับประเทศนั้น โดยความผิดที่สามารถดำเนินการส่งผู้ร้ายข้ามแดนได้นั้นจะต้องเป็นความผิดตามกฎหมายของทั้งสองประเทศ (Double Criminality) ในกรณีที่ประเทศไทยไม่ได้ทำสนธิสัญญาส่งผู้ร้ายข้ามแดนไว้ การส่งผู้ร้ายข้ามแดนจำต้องเป็นไปตามหลักต่างตอบแทนหรือถ้อยทีถ้อยอาศัย นอกจากนี้การส่งผู้ร้ายข้ามแดนของประเทศไทยต้องเป็นไปตามพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 โดยความผิดที่จะส่งผู้ร้ายข้ามแดนได้ต้องเป็นความผิดอาญาซึ่งกฎหมายของประเทศผู้ร้องขอและกฎหมายไทยกำหนดให้เป็นความผิดอาญาซึ่งมีโทษประหารชีวิตหรือมีโทษจำคุกหรือโทษจำกัดเสรีภาพในรูปแบบอื่นตั้งแต่หนึ่งปีขึ้นไป สำหรับวิธีการร้องขอให้ส่งผู้ร้ายข้ามแดนจากประเทศผู้รับคำร้องขอมายัง

---

[63] Harshit Yadav and Others, **Various Types of Cybercrime and Its Affected Area** in **Emerging Technologies in Data Mining and Information and Security**, Edited by Joao Manuel R.S. Tavares and Others, First Edition (Cham: Springer, 2021), p. 306.

[64] Sean Lyngaas, **Russian Accused of Being Part of Cybercrime Ring Extradited from South Korea to Ohio** [Online], 16 December 2021. Sources: https://edition.cnn.com/2021/10/28/politics/russian-extradited-south-korea-ohio/index.html

ประเทศไทย ให้พนักงานอัยการหรือหน่วยงานที่ประสงค์จะให้มีการส่งผู้ร้ายข้ามแดนเสนอเรื่องต่อผู้ประสานงานกลาง ในกรณีที่ผู้ประสานงานกลางมีคำวินิจฉัยว่าสมควรที่จะจัดทำคำร้องขอให้ส่งผู้ร้ายข้ามแดนจากประเทศผู้รับคำร้องขอ ให้ผู้ประสานงานกลางส่งเรื่องให้พนักงานอัยการจัดทำคำร้องขอส่งผู้ร้ายข้ามแดนและเอกสารประกอบต่อไป และหากประเทศไทยมีสนธิสัญญาส่งผู้ร้ายข้ามแดนกับประเทศผู้รับคำร้องขอ ให้ผู้ประสานงานกลางดำเนินการตามสนธิสัญญา หากประเทศไทยไม่มีสนธิสัญญาส่งผู้ร้ายข้ามแดนกับประเทศผู้รับคำร้องขอให้ผู้ประสานงานกลางดำเนินการโดยผ่านวิธีทางการทูต

สำหรับความผิดอันเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือการเจาะเข้าระบบคอมพิวเตอร์นั้น หากพนักงานเจ้าหน้าที่ต้องการตัวผู้กระทำความผิดหรือแฮ็กเกอร์ที่อยู่ในต่างประเทศมาดำเนินคดีหรือรับโทษตามกฎหมายไทย พนักงานเจ้าหน้าที่ต้องดำเนินการตามพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 ซึ่งในเบื้องต้น ความผิดที่จะส่งตัวผู้ร้ายข้ามแดนให้แก่กันได้นั้นต้องเป็นความผิดของทั้งสองประเทศคือประเทศผู้ร้องขอและประเทศผู้รับคำขอ และโทษขั้นต่ำของฐานความผิดต้องไม่น้อยกว่า 1 ปี เมื่อเป็นเช่นนี้ พนักงานเจ้าหน้าที่จำต้องพิจารณาโทษตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดไว้ โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดโทษจำคุกที่เกิน 1 ปีไว้ในมาตรา 7, 8, 9, 10, 12, และ 12/1 ผู้กระทำความผิดตามมาตราดังกล่าวจึงสามารถถูกส่งตัวกลับมายังประเทศไทยในฐานะผู้ร้ายข้ามแดนได้ แต่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดอัตราโทษจำคุกที่ไม่ถึง 1 ปีไว้ในมาตรา 5 และ 6 โดยมาตรา 5 กำหนดโทษจำคุกไว้ไม่เกิน 6 เดือน ในขณะที่มาตรา 6 กำหนดโทษจำคุกไม่เกิน 1 ปี ดังนั้นผู้กระทำความผิดตามมาตรา 5 และ 6 จึงไม่อาจถูกส่งตัวกลับมายังประเทศไทยในฐานะผู้ร้ายข้ามแดนได้ เว้นแต่การกระทำความผิดตามมาตรา 5 และ 6 เกี่ยวพันกับความผิดที่ให้มีการส่งผู้ร้ายข้ามแดนตามคำร้องขอแล้ว

แต่อย่างไรก็ตาม พนักงานเจ้าหน้าที่อาจเผชิญปัญหาหรืออุปสรรคในการขอให้ส่งผู้ร้ายข้ามแดนหรือแฮ็กเกอร์ที่อยู่ในต่างประเทศ โดยปัญหาหรืออุปสรรคดังกล่าวอาจแบ่งออกเป็นดังต่อไปนี้

(ก) ปัญหาหรืออุปสรรคในประเทศไทย

พนักงานเจ้าหน้าที่ยังคงขาดความรู้ความเข้าใจในขั้นตอนหรือแนวทางปฏิบัติในการเสนอคำร้องขอให้ส่งผู้ร้ายข้ามแดน[65] โดยพนักงานเจ้าหน้าที่มักไม่ทราบว่าต้องใช้เอกสารใดบ้างในการดำเนินการหรือประกอบคำร้องขอ[66] นอกจากนี้ ในการดำเนินการขอให้ส่งผู้ร้ายข้ามแดน การจัดทำคำร้องและนำเสนอเอกสารหรือพยานหลักฐานที่เกี่ยวข้องต้องดำเนินการเป็นภาษาอังกฤษทั้งหมด ตัวอย่างเช่น รายงานการสอบสวน หนังสือคำสั่งฟ้องผู้ต้องหา หมายจับของศาล หรือคำพิพากษาของศาล ต้องทำการแปลเป็นภาษาอังกฤษทั้งหมดเพื่อให้ประเทศผู้รับคำร้องขอได้พิจารณา แต่การดำเนินการแปลเป็นภาษาอังกฤษถือเป็นปัญหาและอุปสรรคของพนักงานเจ้าหน้าที่เป็นอย่างมาก อีกทั้งภาษาอังกฤษที่ใช้ควรต้องเป็นภาษาที่เป็นทางการ พนักงานเจ้าหน้าที่จึงได้แก้ปัญหาด้วยการว่าจ้างแปลเอกสารเป็นภาษาอังกฤษ ซึ่งก็มีค่าใช้จ่ายที่สูงมาก เมื่อเป็นเช่นนี้ พนักงานเจ้าหน้าที่จึงมักไม่ต้องการดำเนินการขอให้ส่งผู้ร้ายข้ามแดน[67]

(ข) ปัญหาหรืออุปสรรคในต่างประเทศ

แม้ประเทศไทยได้ทำสนธิสัญญาส่งผู้ร้ายข้ามแดนกับประเทศอื่น ๆ หรือพนักงานเจ้าหน้าที่ดำเนินการขอส่งผู้ร้ายข้ามแดนตามพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 แล้วก็ตาม แต่ประเทศผู้รับคำร้องขออาจปฏิเสธการส่งตัวผู้ร้ายข้ามแดนมายังประเทศไทย หากการกระทำความผิดเป็นคดีการเมือง หรือผู้กระทำความผิดอาจต้องรับโทษประหารชีวิต จำคุกตลอดชีวิต หรือถูกลงโทษด้วยความทารุณโหดร้าย[68] สำหรับคดีอันเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือการแฮ็กนั้น ประเทศผู้รับคำร้องขออาจปฏิเสธการส่งตัวผู้ร้ายข้ามแดนหรือแฮ็กเกอร์มายังประเทศไทยด้วยเหตุผลดังต่อไปนี้

---

[65] เกชา สุขรมย์, **การส่งผู้ร้ายข้ามแดน: วิธีเอาตัวผู้กระทำผิดที่หลบหนีในต่างประเทศกลับมาเพื่อดำเนินคดีหรือลงโทษ** [ออนไลน์], 16 ธันวาคม 2564. แหล่งที่มา: https://www.fad.go.th/th/articles/108431

[66] เรื่องเดียวกัน

[67] เรื่องเดียวกัน

[68] Joanna Harrington, **Extradition of Transnational Criminals** in **Routledge Handbook of Transnational Criminal Law**, Edited by Neil Boister and Robert J. Currie, First Edition (New York: Routledge, 2015), p. 162.

(ข.1) พยานหลักฐานไม่มีน้ำหนักเพียงพอ

ประเทศผู้รับคำร้องขออาจปฏิเสธการส่งตัวผู้กระทำความผิดหรือแฮ็กเกอร์มายังประเทศไทยได้ ทั้งนี้เนื่องจากการพิจารณาพยานหลักฐานนั้นต้องเป็นไปตามหลักเกณฑ์ของประเทศผู้รับคำร้องขอ หากประเทศผู้รับคำร้องขอได้พิจารณาและพบว่า พยานหลักฐานไม่มีน้ำหนักเพียงพอที่จะพิสูจน์ว่าแฮ็กเกอร์ได้กระทำความผิดในประเทศไทย[69] หรือไม่มีความเกี่ยวข้องหรือเชื่อมโยงกับการกระทำความผิด หรือการเก็บรวบรวมและพิสูจน์ตรวจสอบพยานหลักฐานดิจิทัลไม่ได้กระทำบนพื้นฐานของ Digital Forensics ทำให้พยานหลักฐานดิจิทัลนั้นไม่ถูกต้องและไม่น่าเชื่อถือ ประเทศผู้รับคำร้องขออาจปฏิเสธที่จะปฏิบัติตามคำร้องขอนั้น ดังนั้นหากพนักงานเจ้าหน้าที่ไม่สามารถรวบรวมหรือนำเสนอพยานหลักฐานดิจิทัลที่มีความถูกต้องและมีความน่าเชื่อถือได้ พนักงานเจ้าหน้าที่ก็ไม่อาจขอส่งตัวผู้ร้ายข้ามแดนหรือแฮ็กเกอร์ที่อยู่ในต่างประเทศกลับมายังประเทศไทยได้

(ข.2) การไม่ส่งคนเชื้อชาติของตนเป็นผู้ร้ายข้ามแดน

ประเทศผู้รับคำร้องขออาจไม่ดำเนินการส่งตัวผู้กระทำความผิดหรือแฮ็กเกอร์ที่เป็นคนในเชื้อชาติของตนให้ไปถูกดำเนินคดีหรือรับโทษในประเทศไทย[70] หลักเกณฑ์ดังกล่าวนี้ได้ปรากฏอยู่ในกฎหมายรัฐธรรมนูญของบางประเทศและกฎหมายระหว่างประเทศ ตัวอย่างเช่น มาตรา 61 ของกฎหมายรัฐธรรมนูญแห่งประเทศรัสเซียได้กำหนดว่า *“การส่งประชาชนชาวรัสเซียเป็นผู้ร้ายข้ามแดนไปยังประเทศอื่นเป็นสิ่งต้องห้าม”*[71] มาตรา 16 ของประมวลกฎหมายอาญาแห่งประเทศรัสเซียยังได้กำหนดว่า *“ประชาชนชาวรัสเซียซึ่งได้กระทำความผิดอาญาในดินแดนประเทศอื่น ไม่ต้องถูกส่งตัวเป็นผู้ร้ายข้ามแดนไปยังประเทศนั้น”* ดังนั้น พนักงานเจ้าหน้าที่ต้องพิจารณากฎหมายรัฐธรรมนูญหรือกฎหมายฉบับอื่น ๆ ของประเทศผู้รับคำร้องขอ ว่ามีบทบัญญัติใดที่ห้ามมิให้ส่งประชาชนประเทศของตนไปยังประเทศอื่นในฐานะผู้ร้ายข้ามแดน หากปรากฏว่าประเทศผู้รับคำร้องขอมีกฎหมายที่ห้ามส่งบุคคลในประเทศตนไปถูกดำเนินคดี

---

[69] Michael Abbell, **Extradition to and from the United States 2010**, First Edition (Boston: Martinus Nijhoff, 2010), p. 254.

[70] Carlson Anyangwe, **Criminal Law: The General Part**, First Edition (Bamenda: Langaa RPCIG, 2015), p. 166.

[71] Susan W. Brenner, **Cyberthreats and the Decline of the Nation-State**, First Edition (New York: Routledge, 2014), p. 68.

หรือรับโทษในประเทศอื่น ย่อมมีความเป็นไปได้ว่าประเทศผู้รับคำร้องจะไม่ส่งผู้กระทำความผิดหรือแฮ็กเกอร์ในประเทศตนมายังประเทศไทย

(ข.3) การกระทำความผิดที่ไม่อาจถูกส่งตัวในฐานะผู้ร้ายข้ามแดน

หากการกระทำความผิดที่จะถูกส่งตัวในฐานะผู้ร้ายข้ามแดนมิใช่ความผิดของทั้งสองประเทศ แต่เป็นความผิดเพียงประเทศใดประเทศหนึ่งแต่เพียงประเทศเดียว หรือหากการกระทำความผิดที่จะถูกส่งตัวในฐานะผู้ร้ายข้ามแดนมิใช่ความผิดในประเทศผู้รับคำร้องขอ กรณีดังกล่าวนี้ประเทศผู้รับคำร้องขออาจปฏิเสธการส่งตัวผู้ร้ายข้ามแดนให้แก่ประเทศผู้ร้องขอ เพราะถือว่าไม่ครบเงื่อนไขหรือองค์ประกอบการส่งผู้ร้ายข้ามแดน สำหรับคดีอาชญากรรมทางเทคโนโลยีหรือการเจาะเข้าระบบคอมพิวเตอร์นั้น การกระทำความผิดมักเกี่ยวข้องหรือเชื่อมโยงหลายประเทศ เนื่องจากอินเทอร์เน็ตเชื่อมโยงทั่วทุกมุมโลก หากประเทศผู้รับคำร้องขอไม่มีกฎหมายอันเกี่ยวกับอาชญากรรมทางเทคโนโลยี ประเทศผู้รับคำร้องขออาจปฏิเสธการส่งตัวผู้ร้ายข้ามแดนให้แก่ประเทศผู้ร้องขอ

เมื่อการกระทำความผิดที่จะถูกส่งตัวในฐานะผู้ร้ายข้ามแดนได้ ต้องเป็นความผิดของทั้งสองประเทศ ผู้กระทำความผิดจึงอาจถูกดำเนินคดีและรับโทษตามกฎหมายในประเทศผู้รับคำร้องขอ และหลังจากนั้น ผู้กระทำความผิดไม่ต้องได้รับโทษในฐานความผิดเดียวกันนั้นอีกแต่อย่างใด ตามหลักการไม่ลงโทษซ้ำในความผิดเดียวกัน (Double Jeopardy)[72] เมื่อผู้กระทำความผิดไม่ต้องได้รับโทษซ้ำ ประเทศผู้รับคำร้องขอจึงไม่จำเป็นต้องส่งตัวผู้ร้ายข้ามแดนให้แก่ประเทศผู้ร้องขออีก สำหรับคดีอาชญากรรมทางเทคโนโลยีหรือการเจาะเข้าระบบคอมพิวเตอร์นั้นมักเป็นการกระทำความผิดสองรัฐที่อาจเกี่ยวข้องกับประเทศผู้ร้องขอและประเทศผู้รับคำร้องขอ หากประเทศผู้รับคำร้องขอได้ดำเนินคดีหรือลงโทษผู้กระทำความผิดหรือแฮ็กเกอร์เป็นที่เรียบร้อย ประเทศผู้รับคำร้องอาจปฏิเสธการส่งตัวผู้กระทำความผิดหรือแฮ็กเกอร์ไปยังประเทศผู้ร้องขอ

[72] Ilias Bantekas and Susan Nash, **International Criminal Law**, Third Edition (New York: Routledge, 2009), p. 295.

9. บทสรุปและข้อเสนอแนะ

กฎหมายจะมีประสิทธิภาพหรือประสบความสำเร็จหรือไม่นั้น มิได้อาศัยเพียงบทบัญญัติของกฎหมายที่กำหนดให้การกระทำนั้นเป็นความผิดเพียงเท่านั้น แต่จำต้องอาศัยกระบวนการดำเนินคดีหรือการนำตัวผู้กระทำความผิดมาลงโทษด้วยเช่นกัน ทั้งนี้เพราะกระบวนการยุติธรรมต้องอาศัยเนื้อหาในบทบัญญัติกฎหมายดำเนินการควบคู่กับกระบวนการดำเนินคดีหรือการบังคับใช้กฎหมาย สำหรับปัญหาในการนำตัวแฮ็กเกอร์ที่อยู่ในต่างประเทศมารับโทษตามกฎหมายไทยนั้น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มิได้ถือเป็นอุปสรรคแต่อย่างใด และยังถือว่าเป็นกฎหมายที่มีประสิทธิภาพในการลงโทษผู้กระทำความผิด แต่ปัญหาหรืออุปสรรคเกิดขึ้นจากข้อจำกัดในด้านความสามารถของพนักงานเจ้าหน้าที่ และกระบวนการดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศตามพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 และพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 ปัญหาหรืออุปสรรคดังกล่าวนี้จำเป็นต้องได้รับการแก้ไข เพราะอาจส่งผลให้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กลายเป็นกฎหมายที่ไม่มีประสิทธิภาพ และส่งผลกระทบต่อกระบวนการยุติธรรมในประเทศ โดยปัญหาดังกล่าวควรได้รับการแก้ไขดังต่อไปนี้

(1) การพัฒนาศักยภาพและความสามารถของพนักงานเจ้าหน้าที่ในประเทศไทย

การพัฒนาศักยภาพและความสามารถของพนักงานเจ้าหน้าที่ในการสืบสวนและสอบสวนถือเป็นการเพิ่มประสิทธิภาพในการบังคับใช้กฎหมายอีกประการหนึ่ง และถือเป็นหน้าที่ของรัฐบาลที่ต้องดำเนินการ โดยรัฐบาลควรพัฒนาศักยภาพและความสามารถของพนักงานเจ้าหน้าที่ในการติดตาม ค้นหา หรือสืบสวนแฮ็กเกอร์ที่อยู่ในต่างประเทศ เพราะแฮ็กเกอร์เหล่านี้มีความเชี่ยวชาญและความสามารถสูงในการลงมือกระทำความผิด รัฐบาลควรอบรมหรือพัฒนาความรู้ด้าน Digital Forensics แก่พนักงานเจ้าหน้าที่เพื่อให้การสืบสวน สอบสวน รวบรวม และพิจารณาพยานหลักฐานดิจิทัลเป็นไปตามมาตรฐานสากล รัฐบาลควรจัดหาเครื่องมือหรือเทคโนโลยีที่ทันสมัยในการติดตามค้นหาแฮ็กเกอร์ด้วยเช่นกัน นอกจากนี้ รัฐบาลต้องหาบุคลากรที่มีความรู้ความสามารถในด้านคอมพิวเตอร์มาร่วมงานให้มากขึ้น ในบางกรณี รัฐบาลจำต้องอาศัยบุคลากรภายนอก (Outsource) ที่มีความรู้ความเชี่ยวชาญมาช่วยพนักงานเจ้าหน้าที่ในการสืบสวน สอบสวน หรือรวบรวมพยานหลักฐาน การดำเนินดังกล่าวนี้รัฐบาลอาจต้องใช้งบประมาณจำนวนมาก แต่หากรัฐบาลไม่ดำเนินการใด ๆ พนักงานเจ้าหน้าที่ก็ไม่สามารถ

สืบสวน สอบสวน หรือรวบรวมพยานหลักฐานกับแฮ็กเกอร์ที่อยู่ในต่างประเทศได้อย่างมีประสิทธิภาพ

(2) ความร่วมมือระหว่างประเทศ

เนื่องจากอาชญากรรมทางเทคโนโลยีหรือการเจาะเข้าระบบคอมพิวเตอร์ในปัจจุบันได้กลายเป็นอาชญากรรมข้ามชาติ ความร่วมมือระหว่างประเทศได้ถูกนำมาใช้เป็นเครื่องมือในการแก้ปัญหาดังกล่าว รัฐบาลไทยจึงควรอาศัยความร่วมมือระหว่างประเทศในการพัฒนาความสามารถและเพิ่มประสิทธิภาพในการสืบสวน สอบสวน หรือดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศ ในหลายปีที่ผ่านมา หลาย ๆ ประเทศได้ตกลงกันทำความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยความร่วมมือดังกล่าวนี้มิใช่ความร่วมมือระหว่างประเทศทั่วไป แต่ควรเป็นความร่วมมือสำหรับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีโดยเฉพาะ ซึ่งมีการแลกเปลี่ยนข้อมูลระหว่างกันและการให้ความช่วยเหลือในการรวบรวมพยานหลักฐานดิจิทัลที่จะต้องกระทำด้วยความรวดเร็ว

ความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีอาจอยู่ในรูปแบบของ (1) ความร่วมมือกันระหว่างสองประเทศ (Bilateral Cooperation) ตัวอย่างเช่น ประเทศนิวซีแลนด์และประเทศอินเดียได้ทำการเจรจาในการให้ความร่วมมือทางไซเบอร์ (Bilateral Cyber Dialogue)[73] ความร่วมมือดังกล่าวนี้ช่วยให้การป้องกันอาชญากรรมทางเทคโนโลยีของทั้งสองประเทศเป็นไปอย่างมีประสิทธิภาพ หรือ (2) ความร่วมมือกันระหว่างหลายประเทศ (Multilateral Cooperation) โดยประเทศไทยอาจเข้าร่วมในสนธิสัญญาระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ตัวอย่างเช่น Budapest Convention เป็นสนธิสัญญาระหว่างประเทศฉบับแรกที่ถูกกำหนดขึ้นเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี[74] วัตถุประสงค์ของ Budapest Convention คือ (1) พัฒนากฎหมายภายในของประเทศสมาชิกให้เป็นไปในทิศทางเดียวกัน

---

[73] Apoorva Kaul, **India and New Zealand Agree To Deepen Cooperation in Virtual Bilateral Cyber Dialogue** [Online], 16 December 2021. Source: https://www.republicworld.com/world-news/rest-of-the-world-news/india-and-new-zealand-agree-to-deepen-cooperation-in-virtual-bilateral-cyber-dialogue.html

[74] Council of Europe, **Budapest Convention** [Online], 16 December 2021. Source: https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#/

โดยให้ถือว่าการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลในระบบคอมพิวเตอร์ถือเป็นการกระทำความผิดในคดีอาญา (2) ปรับปรุงวิธีการสืบสวนอาชญากรรมทางเทคโนโลยีและวิธีการเก็บรักษาพยานหลักฐานดิจิทัล และ (3) เพิ่มประสิทธิภาพความร่วมมือระหว่างประเทศ[75] ซึ่งหากประเทศไทยเข้าร่วมเป็นสมาชิก Budapest Convention ประเทศไทยอาจได้รับประโยชน์ในการพัฒนาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้มีความทันสมัยและมีมาตรฐานมากยิ่งขึ้น อีกทั้งยังช่วยให้การสืบสวน สอบสวน และรวบรวมพยานหลักฐานดิจิทัลเป็นไปมีประสิทธิภาพมากยิ่งขึ้น

ประเทศไทยอาจต้องทำสนธิสัญญาส่งผู้ร้ายข้ามแดนและสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญาเพิ่มขึ้น โดยในปัจจุบันนี้ประเทศไทยทำสนธิสัญญาส่งผู้ร้ายข้ามแดนไว้กับ 14 ประเทศ[76] ซึ่งนับว่าน้อยมาก หากต้องการที่จะดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในประเทศต่าง ๆ ได้อย่างครอบคลุม ประเทศไทยอาจต้องพิจารณาทำสนธิสัญญาส่งผู้ร้ายข้ามแดนเพิ่มและสนธิสัญญาส่งผู้ร้ายข้ามแดนในกรณีดังกล่าวนี้อาจเป็นคดีอันเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดอันเกี่ยวกับคอมพิวเตอร์โดยเฉพาะ สนธิสัญญาส่งผู้ร้ายข้ามควรถือเป็นเครื่องมือที่สำคัญ เพราะสนธิสัญญาเป็นข้อตกลงอย่างเป็นทางการที่มีผลผูกพันประเทศคู่สัญญา ส่งผลให้ประเทศคู่สัญญามีหน้าที่ที่จะต้องปฏิบัติตามสนธิสัญญานั้น หากประเทศไทยไม่ทำสนธิสัญญาส่งผู้ร้ายข้ามแดนเพิ่ม การดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศจะกลายเป็นเรื่องยาก เพราะประเทศผู้รับคำร้องขอไม่มีหน้าที่ที่จะต้องส่งผู้กระทำความผิดให้กับประเทศไทย และประเทศผู้รับคำร้องขอมักไม่ส่งบุคคลของประเทศตนให้ไปรับโทษในประเทศอื่น นอกจากนี้ประเทศไทยได้ทำสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญากับประเทศต่าง ๆ รวมทั้งสิ้น 14 ประเทศ[77] และเป็นภาคีสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญาของอาเซียน ประเทศไทยจึงควรทำสนธิสัญญา

---

[75] Council of Europe, **Convention on Cybercrime** [Online], 21 December 2021. Source: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[76] ประเทศที่เป็นคู่สัญญา ได้แก่ อังกฤษ แคนาดา ออสเตรเลีย มาเลเซีย ฟิจิ เบลเยียม อินโดนีเซีย ฟิลิปปินส์ สหรัฐอเมริกา จีน เกาหลีใต้ ลาว บังกลาเทศ และกัมพูชา

[77] กระทรวงการต่างประเทศ, **การแลกเปลี่ยนสัตยาบันสารสนธิสัญญาระหว่างราชอาณาจักรไทยกับยูเครนว่าด้วยความช่วยเหลือซึ่งกันและกันทางกฎหมายในเรื่องทางอาญา** [ออนไลน์], 2 กุมภาพันธ์ 2565. แหล่งที่มา: https://www.mfa.go.th/th/content/5d5bd27c15e39c3060029b77

ว่าด้วยความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญาเพิ่มขึ้นเพื่อให้การสืบสวน สอบสวน และรวบรวมพยานหลักฐานดิจิทัลเป็นไปอย่างมีประสิทธิภาพ

(3) การลดขั้นตอนหรือกระบวนการทางกฎหมาย

การเก็บรวบรวมพยานหลักฐานดิจิทัลหรือข้อมูลต่าง ๆ ต้องดำเนินการด้วยความรวดเร็ว เพื่อไม่ให้ข้อมูลเหล่านั้นสูญหาย ถูกทำลาย หรือถูกเปลี่ยนแปลงแก้ไข การลดขั้นตอนหรือกระบวนการทางกฎหมายจึงเป็นวิธีช่วยให้พนักงานเจ้าหน้าที่สามารถเก็บรวบรวมพยานหลักฐานดิจิทัลได้รวดเร็วมากยิ่งขึ้น และส่งผลให้การบังคับใช้กฎหมายมีประสิทธิภาพมากยิ่งขึ้น เมื่อการสืบสวน สอบสวน หรือรวบรวมพยานหลักฐานดิจิทัลเพื่อดำเนินคดีกับแฮ็กเกอร์ที่อยู่ในต่างประเทศจำต้องดำเนินการผ่านพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 โอกาสที่จะนำตัวผู้กระทำความผิดมารับโทษย่อมมีไม่มาก เพราะกฎหมายดังกล่าวได้กำหนดขั้นตอนและกระบวนการซึ่งอาจก่อให้เกิดความล่าช้า เช่น พนักงานเจ้าหน้าที่ต้องเสนอเรื่องต่อผู้ประสานงานกลาง โดยผู้ประสานงานกลางเป็นผู้พิจารณาว่าสมควรจะขอความช่วยเหลือจากต่างประเทศหรือไม่ ซึ่งกระบวนการดังกล่าวนี้อาจก่อให้เกิดความล่าช้าในการเก็บรวบรวมพยานหลักฐานดิจิทัล ดังนั้นพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงควรได้รับการแก้ไขเพิ่มเติมเพื่อแก้ไขปัญหาดังกล่าว โดยให้อำนาจพนักงานเจ้าหน้าที่สามารถดำเนินการสืบสวนหรือเก็บรวบรวมพยานหลักฐานดิจิทัลที่อยู่ในต่างประเทศโดยตรงได้ในทันที และพนักงานเจ้าหน้าที่ไม่จำเป็นต้องดำเนินการตามพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 อีกต่อไป การแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังกล่าวนี้ มิใช่เป็นการแก้ไขข้อบกพร่องของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่เป็นการแก้ไขเพิ่มเติมเพื่อเพิ่มประสิทธิภาพในการดำเนินคดีกับผู้กระทำความผิดให้มากยิ่งขึ้น เพราะการแก้ไขเพิ่มเติมดังกล่าวนี้มีลักษณะเป็นการลดขั้นตอนหรือกระบวนการทางกฎหมายที่มีความยุ่งยากและสลับซับซ้อนตามพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 และเพิ่มอำนาจให้กับพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 สามารถดำเนินการขอความร่วมมือระหว่างประเทศได้โดยตรง ที่สำคัญกฎหมายทั้งสองนี้เป็นกฎหมายต่างฉบับกัน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ยังคงทำหน้าที่ป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อยู่

เช่นเดิม และมีพนักงานเจ้าหน้าที่มีอำนาจในการสืบสวนและสอบสวนเพื่อใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

บรรณานุกรม

- กระทรวงการต่างประเทศ, **การแลกเปลี่ยนสัตยาบันสารสนธิสัญญาระหว่างราชอาณาจักรไทยกับยูเครนว่าด้วยความช่วยเหลือซึ่งกันและกันทางกฎหมายในเรื่องทางอาญา**, [ออนไลน์], แหล่งที่มา: https://www.mfa.go.th/th/content/5d5bd27c15e39c3060029b77

- เกชา สุขรมย์. **การส่งผู้ร้ายข้ามแดน: วิธีเอาตัวผู้กระทำผิดที่หลบหนีในต่างประเทศกลับมาเพื่อดำเนินคดีหรือลงโทษ** [ออนไลน์], แหล่งที่มา: https://www.fad.go.th/th/articles/108431

- ข่าวไทยพีบีเอส, **ดีอีเอส ล่าแฮ็กเกอร์ขโมยข้อมูล รพ. เพชรบูรณ์ - ปูดกองทัพโดนด้วย** [ออนไลน์], แหล่งที่มา: https://news.thaipbs.or.th/content/307715

- จิตชนก อินถามา และวงศ์ยศ เกิดศรี, **การศึกษาแนวทางการตรวจพิสูจน์หลักฐานทางดิจิทัลในงานนิติวิทยาศาสตร์**, วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ, ปีที่ 7 ฉบับที่ 1 (มิถุนายน 2564).

- ไทยรัฐ ออนไลน์, **รพ. เพชรบูรณ์แจงหลังถูกแฮ็ก ยันข้อมูลที่หลุดไม่กระทบต่อการรักษาคนไข้** [ออนไลน์], แหล่งที่มา: https://www.thairath.co.th/news/society/2187423

- ผู้จัดการออนไลน์, **แฉ! กลโกงดูดเงินผ่าน “บัตรตื๊ด” บัตรอยู่ในกระเป๋าก็แฮ็กข้อมูลได้** [ออนไลน์], แหล่งที่มา: https://mgronline.com/specialscoop/detail/9640000103836

- พงศ์กุลธร โรจน์วิรุฬห์ วีรพล กุลบุตร และชวนัสถ์ เจนการ, **ปัญหาและอุปสรรคในการดำเนินความร่วมมือระหว่างประเทศในเรื่องทางอาญาในกลุ่มประเทศอาเซียน**, วารสารกระบวนการยุติธรรม, ปีที่ 11 ฉบับที่ 3 (กันยายน 2561).

- Alaa Hussein Al-Hamami and Ghossoon M. Waleed Al-Saadoon, **Handbook of Research on Threat Detection and Countermeasures in Network Security**, First Edition (Hershey: Information Science Reference, 2014).

- Alison Bisset, **Truth Commissions and Criminal Courts**, First Edition (New York: Cambridge University Press, 2012).

- Andreas Mitrakas and Damian Zaitch, **Law, Cyber Crime and Digital Forensics: Trailing Digital Suspects** in **Digital Crime and Forensic Science in Cyberspace**, Edited by Panagiotis Kanellis and Others, First Edition (London: IDEA Group Publishing, 2006).

- Apoorva Kaul, **India and New Zealand Agree To Deepen Cooperation in Virtual Bilateral Cyber Dialogue** [Online], Source: https://www.republicworld.com/world-news/rest-of-the-world-news/india-and-new-zealand-agree-to-deepen-cooperation-in-virtual-bilateral-cyber-dialogue.html

- Balsing Rajput, **Cyber Economic Crime in India: An Integrated Model for Prevention and Investigation**, First Edition (Cham: Springer, 2021).

- Carlson Anyangwe, **Criminal Law: The General Part**, First Edition (Bamenda: Langaa RPCIG, 2015).

- Catherine D. Marcum, **Cyber Crime**, Second Edition (New York: Wolters Kluwer, 2019).

- Christina Voigt, **Up in the Air: Aviation, the EU Missions Trading Scheme and the Question of Jurisdiction** in **Cambridge Yearbook of European Legal Studies**, Edited by Catherine Barnard, Markus Gehring, and Iyiola Solanke, First Edition (Oregon: Hart Publishing, 2012).

- Christopher Wray, **The FBI and the Private Sector: Battling the Cyber Threat Together** [Online], Source: https://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-battling-the-cyber-threat-together-012821

- Council of Europe, **Budapest Convention** [Online], Source: https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#/

- Council of Europe, **Convention on Cybercrime** [Online], Source: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

- Danielle Ireland-Piper, **Extraterritoriality in East Asia: Extraterritorial Criminal Jurisdiction in China, Japan, and South Korea**, First Edition (Massachusetts: Edward Elgar Publishing, 2021).

- David J. Engebretson, **Technician's Guide to Physical Security Networking: Enterprise Solutions**, First Edition (Indiana: Author House, 2008).

- Don Kerr, John Gammack, and Richard Boddington, **Overview of Digital Business Security Issues** in **Digital Business Security Development: Management Technologies**, Edited by Don Kerr, John G. Gammack, and Kay Bryant, First Edition (New York: Business Science Reference, 2010).

- Harshit Yadav and Others, **Various Types of Cybercrime and Its Affected Area** in **Emerging Technologies in Data Mining and Information and Security**, Edited by Joao Manuel R.S. Tavares and Others, First Edition (Cham: Springer, 2021).

- Hiromi Sato, **Multilayered Structures of International Criminal Law**, First Edition (Cham: Springer, 2021).

- IBM, **What is A Cyber Attack?** [Online], Source: https://www.ibm.com/topics/cyber-attack

- Ilias Bantekas and Susan Nash, **International Criminal Law**, Third Edition (New York: Routledge, 2009).

- James E. Girard, **Criminalistics**, Fifth Edition (Burlington: World Headquarters, 2021).

- Jason Sachowski, **Implementing Digital Forensic Readiness: From Reactive to Proactive Process**, Second Edition (New York: CRC Press, 2019).

- Joakim Kavrestad, **Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications**, First Edition (Cham: Springer, 2020).

- Joanna Harrington, **Extradition of Transnational Criminals** in **Routledge Handbook of Transnational Criminal Law**, Edited by Neil Boister and Robert J. Currie, First Edition (New York: Routledge, 2015).

- John E. Hess, **Interrogation for Law Enforcement**, Second Edition (New Jersey: Matthew Bender & Company, Inc., 2010).

- Joseph Migga Kizza, **Computer Network Security and Cyber Ethics**, Fourth Edition (North Carolina: McFarland & Company, 2014).

- Kamlesh K. Bajaj and Debjani Nag, **E-Commerce: The Cutting Edge of Business**, Second Edition (New Delhi: Tata McGraw-Hill Publishing Company Limited, 2005).

- Kevin Hile, **Cybercrime**, First Edition (Massachusetts: Cengage Learning, 2010).

- Klaus von Lampe, **Transnational Crime** in **International and Transnational Crime and Justice**, Edited by Mangai Natarajan, Second Edition (New York: Cambridge University Press, 2019).

- Larry Mays Jeremy Ball and Laura Fidelie, **Criminal Law: Core Concepts**, First Edition (New York: Wolters Kluwer Law & Business, 2015).

- Legal Information Institute (LII), **Extradition** [Online], Source: https://www.law.cornell.edu/wex/extradition#:~:text=Extradition%20is%20the%20removal%20of,from%20one%20jurisdiction%20to%20another

- Michael Abbell, **Extradition to and from the United States 2010**, First Edition (Boston: Martinus Nijhoff, 2010).

- Michael Eck, **The Internet: Inside and Out**, First Edition (New York: Rosen Publishing Group, 2002).

- Mikaila Mariel Lemonik, **Law and Justice around the World: A Comparative Approach**, First Edition (Oakland: University of California Press, 2020).

- Raja Jabir and Omar Alfandi, **Cloud Digital Forensics Evaluation and Crimes Detection** in **Emerging Technologies for Developing Countries: First International EAI Conference, AFRICATEK 2017 Marrakech, Morocco, March 27-28, 2017 Proceedings**, Edited by Fatna Belqasmi and Others, First Edition (Cham: Springer, 2017).

- Richard Boddington, **Practical Digital Forensics**, First Edition (Birmingham: Packt Publishing. 2016).

- Richard Lovely, **Cybercrime** in **International Crime and Justice**, Edited by Mangai Natarajan, First Edition (New York: Cambridge University Press, 2011).

- Ross M. Gardner and Donna R. Krouskup, **Practical Crime Scene Processing and Investigation**, Third Edition (London: CRC Press, 2018).

- Samuel C. McQuade, **Encyclopedia of Cybercrime**, First Edition (London: Greenwood Press, 2008).

- Sasa Mrdovic, **IoT Forensics** in **Security of Ubiquitous Computing Systems: Selected Topics**, Edited by Gildas Avoine and Julio Hernandez-Castro, First Edition (Cham: Springer, 2021).

- Sean Lyngaas, **Russian Accused of Being Part of Cybercrime Ring Extradited from South Korea to Ohio** [Online], Sources: https://edition.cnn.com/2021/10/28/politics/russian-extradited-south-korea-ohio/index.html

- Steve Bunting and Steve Anson, **Mastering Windows Network Forensics and Investigation**, First Edition (Indiana: Wiley Publishing Inc, 2007).

- Susan W. Brenner, **Cyberthreats and the Decline of the Nation-State**, First Edition (New York: Routledge, 2014).

- Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, **Cybercrime and Digital Forensics: Introduction**, First Edition (New York: Routledge, 2015).

- Tine Munk, **Policing Virtual Spaces: Public and Private Online Challenges in A Legal Perspective** in **Comparative Policing Form a Legal Perspective**, Edited by Monica den Boer, First Edition (Cheltenham: Edward Elgar Publishing, 2018).

- United Nations Office on Drugs and Crime (UNODC), **Obstacles to Cybercrime Investigations** [Online], Source: https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html

- Ziska Fields, **Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution**, First Edition (Hershey: IGI Global, 2018).