อาชญากรรมคอมพิวเตอร์: ศึกษาเฉพาะกรณีการฟิชชิ่งที่เกี่ยวข้องกับการฉ้อโกงประชาชน

รณกร วาพันสุ

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรนิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ปรีดี พนมยงค์
มหาวิทยาลัยธุรกิจบัณฑิตย์
ปีการศึกษา 2566

COMPUTER CRIME: A CASE STUDY OF PHISHING INCIDENTS RELATED TO PUBLIC FRAUD

RONNAKORN VARPANSU

A Thematic Paper Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Laws

Department of Law, Pridi Banomyong Faculty of Law

Dhurakij Pundit University

Academic Year 202

ใบรับรองสารนิพนธ์

คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญานิติศาสตรมหาบัณฑิต

หัวข้อสารนิพนธ์ ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษาเฉพาะกรณีการกระทำความผิดในลักษณะฟิชชิ่ง (PHISHING)

เสนอโดย ว่าที่ร้อยตรี รณกร วาพันสุ

สาขาวิชา นิติศาสตร์

หมวดวิชา กฎหมายอาญาและกระบวนการยุติธรรมทางอาญา

อาจารย์ที่ปรึกษาสารนิพนธ์ อาจารย์ ดร.จิรวุฒิ ลิปิพันธ์

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบสารนิพนธ์แล้ว

..... ประธานกรรมการ

(อาจารย์ ดร.สุรสิทธิ์ แสงวิโรจนพัฒน์)

..... กรรมการและอาจารย์ที่ปรึกษาสารนิพนธ์

(อาจารย์ ดร.จิรวุฒิ ลิปิพันธ์)

..... กรรมการ

(รองศาสตราจารย์อัจฉรียา ชูตินันทน์)

คณะนิติศาสตร์ปรีดี พนมยงค์ รับรองแล้ว

..... รักษาการคณบดีคณะนิติศาสตร์ปรีดี พนมยงค์

(รองศาสตราจารย์พินิจ ทิพย์มณี)

วันที่ 30 เดือน พฤศจิกายน พ.ศ. 2566

หัวข้อสารนิพนธ์ อาชญากรรมคอมพิวเตอร์: ศึกษาเฉพาะกรณีการฟิชชิ่งที่เกี่ยวข้องกับการฉ้อโกงประชาชน
ชื่อผู้เขียน รณกร วาพันสุ
อาจารย์ที่ปรึกษา อาจารย์ ดร.จิรวุฒิ ลิปิพันธ์
หลักสูตร นิติศาสตรมหาบัณฑิต
ปีการศึกษา 2566

บทคัดย่อ

อาชญากรรมทางคอมพิวเตอร์ ในปัจจุบันนั้นมีพื้นฐานมาจากก่ออาชญากรรมแบบเดิมซึ่งมีความร้ายแรงและรวดเร็วมากขึ้น โดยอาศัยเทคโนโลยีเป็นเครื่องมือในการกระทำความผิด อาชญากรรมคอมพิวเตอร์ในปัจจุบันนั้นมีความหลากหลายและรุนแรงมากขึ้น โดยเฉพาะอย่างยิ่งกับการฟิชชิ่ง (phishing) ที่ก่อให้เกิดผลกระทบในวงกว้างแก่ทุกภาคส่วน ซึ่งเมื่อพิจารณาจากกฎหมายของประเทศไทยในปัจจุบันที่แม้จะมีการแก้ไขปรับปรุงเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 ให้มีความชัดเจนและทันสมัยมากเพียงใดก็ยังมีข้อจำกัดในการจับกุมตัวผู้กระทำความผิดมาลงโทษและปัญหาอัตราโทษที่ค่อนข้างต่ำ อันเป็นสิ่งจูงใจให้ผู้กระทำความผิดตัดสินใจกระทำความผิดเนื่องจากเห็นว่าผลประโยชน์คาดหมายสูงกว่าต้นทุนคาดหมาย อีกทั้งในปัจจุบันยังไม่ปรากฏถึงการบัญญัติมาตรการทางกฎหมายใดที่จะสามารถนำมาบังคับใช้ได้กับการกระทำความผิดเกี่ยวกับฟิชชิ่งได้อย่างเฉพาะเจาะจง

จากการศึกษาพบว่ากฎหมายของประเทศสหพันธ์สาธารณรัฐเยอรมนี, สาธารณรัฐฝรั่งเศส และประเทศสหรัฐอเมริกาในส่วนของ รัฐเทนเนสซี, รัฐนิวยอร์ค, รัฐยูทาห์, รัฐแคลิฟอร์เนีย พบว่าในส่วนของประเทศสหพันธ์สาธารณรัฐเยอรมนี และสาธารณรัฐฝรั่งเศส ซึ่งเป็นประเทศที่ถือได้ว่าใช้กฎหมายในระบบเดียวกับระบบกฎหมายของประเทศไทยนั้น ได้บัญญัติเพิ่มเติมฐานความผิดเกี่ยวกับคอมพิวเตอร์ไว้ในประมวลกฎหมายอาญา โดยบัญญัติให้การกระทำต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดยตรงนั้นถือเป็นความผิดพิเศษที่แยกออกจากการกระทำความผิดโดยใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดที่สามารถนำฐานความผิดในประมวลกฎหมายอาญาที่มีอยู่แต่เดิมมาบังคับใช้ได้ และสำหรับในส่วนของรัฐนิวยอร์ค, รัฐยูทาห์ และรัฐแคลิฟอร์เนีย และรัฐเทนเนสซีนั้นได้บัญญัติฐานความผิดฟิชชิ่งขึ้นมาเป็นการเฉพาะ

ด้วยเหตุนี้เอง ประเทศไทยในปัจจุบันจึงควรแก้ไขและปรับปรุงเพิ่มเติมบทบัญญัติให้มีความครอบคลุมถึงลักษณะในการกระทำความผิดมากยิ่งขึ้น นอกจากนี้ผู้เขียนยังเห็นควรเพิ่มโทษจำคุกแก่ผู้ที่กระทำความผิดฐานฟิชชิ่งเพื่อเป็นการรักษาระดับต้นทุนของการกระทำความผิดให้สัมพันธ์กับโทษที่จะได้รับ เหตุเพราะการฟิชชิ่งนั้นมิได้ส่งผลกระทบแค่เฉพาะตัวผู้เสียหายเพียงเท่านั้นแต่ยังรวมไปถึง บุคคลที่โดนผู้กระทำความผิดแอบอ้าง ผู้ให้บริการอินเทอร์เน็ต ตลอดจนหน่วยงานภาครัฐก็ได้รับผลกระทบจากการฟิชชิ่ง

ฉะนั้นจึงควรบัญญัติปรับปรุงและเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติม ให้ครอบคลุมถึงลักษณะของการกระทำความผิดฐานฟิชชิ่ง เพื่อให้ผู้เสียหายจากการฟิชชิ่งทุกรูปแบบได้รับการคุ้มครองตามกฎหมายและผู้กระทำความผิดฐานฟิชชิ่งนั้นได้รับโทษอย่างเหมาะสมกับความผิดที่ได้กระทำต่อไป

คำสำคัญ: ฟิชชิ่ง, อาชญากรรมทางคอมพิวเตอร์, อาชญากรรมทางอินเทอร์เน็ต

อาจารย์ที่ปรึกษา

Thematic Paper Title	COMPUTER CRIME: A CASE STUDY OF PHISHING INCIDENTS RELATED TO PUBLIC FRAUD
Author	Ronnakorn Varpansu
Thematic Paper Advisor	Jirawut Lipipun, Ph.D.
Program	Master of Laws
Academic Year	2023

ABSTRACT

In the present day, computer crimes have evolved from traditional criminal activities, becoming more severe and rapid by leveraging technology as a tool for wrongdoing. Contemporary computer crimes are diverse and increasingly sophisticated, with phishing, in particular, having widespread repercussions across various sectors. When considering the current laws of Thailand, despite recent amendments and additional provisions to the Computer Crime Act (Version 2) B.E. 2560, aiming to provide clarity and modernization, there are still limitations in apprehending and penalizing perpetrators. The relatively low penalties and the current lack of specific legal measures targeting phishing contribute to perpetrators deciding to engage in criminal activities, viewing the expected benefits as outweighing the anticipated costs. Additionally, there is currently no enacted legal measure specifically addressing the offense of phishing.

From the study, it was found that the laws of the Federal Republic of Germany, the French Republic, and the United States, specifically in the states of Tennessee, New York, Utah, and California, have additional provisions regarding computer offenses within their criminal codes. In the case of the Federal Republic of Germany and the French Republic, which are considered countries employing legal systems similar to that of Thailand, they have enacted supplementary bases for computer offenses in their criminal codes. These provisions specifically distinguish offenses against computer systems and computer data, treating them as separate offenses apart from offenses committed using computers as tools. This allows for the enforcement of existing criminal law provisions in cases where computers are used to commit offenses. As for the states of New York, Utah, California, and Tennessee, they have legislated specific offenses related to phishing.

For these reasons, Thailand should now consider amending and further enhancing legislation to encompass the nature of offenses more comprehensively. Additionally, the researcher suggests increasing the prison sentences for those committing phishing offenses to align the severity of the offense with the corresponding penalties. This is because phishing not only impacts the direct victims but also extends to individuals falsely accused by the offenders, internet service providers, and government agencies. Therefore, it is essential to amend and supplement the Computer Crime Act B.E. 2550 and its amendments to explicitly cover the nature of phishing offenses. This ensures legal protection for all forms of phishing victims and imposes appropriate penalties on perpetrators for their wrongful actions.

Keywords: Phishing, Computer Crimes, Cybercrime

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้สำเร็จลุล้วงลงได้ ด้วยความเมตตาและความช่วยเหลือจากบุคคลหลายท่านที่ได้กรุณาให้คำปรึกษาและให้คำแนะนำแก่ผู้เขียน โดยเฉพาะอย่างยิ่งท่านอาจารย์ ดร. จิรวุฒิ ลิปิพันธ์ ที่ได้ให้ความกรุณารับเป็นอาจารย์ที่ปรึกษาสารนิพนธ์ฉบับนี้ พร้อมทั้งได้ให้ข้อเสนอแนะและแนวทางในการปรับปรุงแก้ไขสารนิพนธ์ฉบับนี้ ตลอดจนแนะนำเอกสารและผลงานทางวิชาการต่างๆ ที่เป็นประโยชน์แก่การศึกษาในครั้งนี้ ซึ่งผู้เขียนต้องขอกราบขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ผู้เขียนขอกราบขอบพระคุณท่าน ดร. สุรสิทธิ์ แสงวิโรจนพัฒน์ ที่ได้กรุณารับเป็นประธานกรรมการสอบสารนิพนธ์ และท่านรองศาสตราจารย์ อัจฉรียา ชูตินันทน์ ที่ได้กรุณารับเป็นกรรมการในการสอบสารนิพนธ์ฉบับนี้

นอกจากท่านผู้มีพระคุณที่ผู้เขียนได้กล่าวไปในข้างต้นแล้ว ผู้เขียนขอขอบคุณเพื่อนๆ พี่ๆ ที่ได้ให้กำลังใจและคอยช่วยเหลือในเรื่องต่างๆ ที่เกี่ยวข้องในการทำสารนิพนธ์เป็นอย่างดี

ท้ายที่สุดที่ขาดมิได้ ผู้เขียนขอกราบขอบพระคุณบิดาและมารดาของผู้เขียนที่ได้คอยเลี้ยงดูให้ความช่วยเหลือ และสนับสนุนผู้เขียนเรื่อยมา

คุณค่าและประโยชน์ใดๆ ที่อาจเกิดจากสารนิพนธ์ฉบับนี้ ผู้เขียนขออุทิศแด่บิดามารดาตลอดจนครูบาอาจารณ์และผู้มีพระคุณทั้งหลายที่ให้มีส่วนส่งเสริมสารนิพนธ์ฉบับนี้เสร็จสิ้นลงด้วยดี หากสารนิพนธ์มีข้อผิดพลาดประการใด ผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

รณกร วาพันสุ

สารบัญ

หน้า

สารบัญ (ต่อ)

บทที่ **หน้า**

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

ภาพที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในสังคมปัจจุบันที่ถือได้ว่าเป็นยุคของเทคโนโลยีสารสนเทศและการติดต่อสื่อสาร Information and communications technology (ICT) ความเจริญก้าวหน้าทางเทคโนโลยี ทำให้โลกใบนี้แคบลง ทำให้คนในอีกซีกโลกหนึ่งสามารถ ติดต่อสื่อสารถึงกันได้ภายในเสี้ยวของวินาที การเผยแพร่ขององค์ความรู้ต่างๆ เกิดขึ้นอย่างกว้างขวาง เกิดการ เปลี่ยนแปลงอย่างรวดเร็ว ส่งผลกระทบโดยตรงต่อสภาพของชีวิตความเป็นอยู่ สังคม วัฒนธรรม การเมือง การปกครอง เศรษฐกิจ และความมั่นคงปลอดภัยของประเทศชาติ โดยการติดต่อสื่อสารดังที่ได้กล่าวมานั้นคือรูปแบบการติดต่อสื่อสารผ่านทางอินเทอร์เน็ตซึ่งถือเป็นเทคโนโลยีที่เข้ามาเปลี่ยนแปลงรูปแบบการติดต่อสื่อสารในยุคปัจจุบันเป็นอย่างมาโดยอินเทอร์เน็ตนั้นไม่เพียงแต่จะทำให้มนุษย์นั้นสามารถติดต่อสื่อสารกันได้อย่างรวดเร็วแต่ยังสามารถเป็นแหล่งข้อมูลที่ให้ในการศึกษาค้นคว้าวิจัย และถูกใช้ในการกระทำธุรกรรมทางการเงินเกือบจะทุกประเภทในปัจจุบัน

อินเทอร์เน็ตจึงถือได้ว่าเป็นแหล่งที่ใช้ในการเก็บข้อมูลจำนวนมหาศาลซึ่งใช้ในการค้นคว้าการรับส่งข้อมูลไปมาระหว่างกันอินเทอร์เน็ตจึงเป็นเทคโนโลยีที่ได้รับการพัฒนาขึ้นมาเพื่อให้สามารถใช้ประโยชน์ได้หลากหลายและเป็นที่แพร่หลายในสังคมยุคปัจจุบัน ซึ่งททำให้อินเทอร์เน็ตนั้นมีประโยชน์เป็นอย่างมากในสังคมยุคข่าวสารอย่างในปัจจุบัน ซึ่งจะทำหน้าที่เหมือนห้องสมุดอิเล็กทรอนิกส์ขนาดใหญ่ส่งข้อมูลที่เราต้องการมาให้ถึงที่ภายในไม่กี่วินาทีจากแหล่งข้อมูลทั่วโลก ซึ่งการมีอยู่ของอินเทอร์เน็ตนี้เองทำให้การติดต่อสื่อสาร แสดงความคิดเห็น ซื้อขายหรือการทำธุรกรรมการเงินอื่นๆ รวมถึงการเข้าถึงแหล่งความรู้ขนาดใหญ่ในการสืบค้นข้อมูลเพื่อการศึกษาต่างๆ และการเข้าถึงข้อมูลเพื่อความบันเทิง เป็นไปได้อย่างง่ายดายในยุคปัจจุบัน

อย่างไรก็ตาม แม้อินเทอร์เน็ตจะมีประโยชน์ เป็นอย่างมากในสังคมยุคปัจจุบันแต่ก็ไม่อาจปฏิเสธได้ว่า ในทุกยุคทุกสมัยนั้นย่อมมีกลุ่มคนหรือบุคคลที่ต้องการแสวงหาผลประโยชน์จากการใช้ประโยชน์ของเทคโนโลยีอย่างใดอย่างหนึ่งในการก่ออาชญากรรม หากในยุคนี้เทคโนโลยีเช่นว่านั้นคืออินเทอร์เน็ต อาชญากรเหล่านี้ซึ่งเป็นผู้ที่แสวงหาประโยชน์โดยมิชอบจากการใช้เทคโนโลยีซึ่งถือได้ว่าเป็นการก่ออาชญากรรมทางคอมพิวเตอร์รูปแบบหนึ่ง

อาชญากรรมทางคอมพิวเตอร์ ในปัจจุบันนั้นมีพื้นฐานที่ได้รับการพัฒนามาจากการก่ออาชญากรรมแบบเดิมโดยมีความร้ายแรง และสะดวกรวดเร็วแนบเนียนมากขึ้นกว่าเดิม โดยอาศัยการพัฒนาที่รวดเร็วของเทคโนโลยีในปัจจุบันเป็นเครื่องมือในการก่ออาชญากรรม อาชญากรรมทางคอมพิวเตอร์ในปัจจุบันนั้นมีความหลากหลายมากขึ้นและยิ่งทวีความรุนแรงมากขึ้น โดยเฉพาะรูปแบบการก่ออาชญากรรมผ่านระบบเครือข่ายอินเทอร์เน็ต(ไซเบอร์) หรืออาจกล่าวได้ว่าเป็นอาชญากรรมไซเบอร์ คำว่า “อาชญากรรมไซเบอร์” ในปัจจุบันยังไม่มีนิยามที่เป็นที่ยอมรับอย่างเป็นสากล หากแต่อาจแยกลักษณะร่วมกันได้ เช่น เหตุเกิดในพื้นที่ไซ

เบอร์หรือเครือข่ายอินเทอร์เน็ต ลักษณะการกระทำ ผลของการกระทำ ผู้กระทำ เป้าหมาย วัตถุประสงค์ อุปกรณ์เครื่องมือหรือวิธีการ เป็นต้น และอาจจะกล่าวได้ว่าอาชญากรรมไซเบอร์เป็นส่วนหนึ่งของอาชญากรรมคอมพิวเตอร์ โดยมีองค์ประกอบสำคัญคือเครือข่ายอินเทอร์เน็ตนั่นเอง.[1]อาชญากรรมไซเบอร์ในปัจจุบันนั้นมีหลากหลายและทวีความรุนแรงมากขึ้นก่อให้เกิดความเสียหายมากยิ่งขึ้นโดยเฉพาะอย่างยิ่งคืออาชญากรรมทางคอมพิวเตอร์ในรูปแบบ ฟิชชิ่งสแกม (phishing Scam) ซึ่งก่อให้เกิดความเสียหายต่อระบบเศรษฐกิจของประเทศเป็นจำนวนมหาศาล โดยเฉพาะอย่างยิ่งในประเทศไทยที่มีสถิติเกี่ยวกับการเกิดอาชญากรรมทางคอมพิวเตอร์ตั้งแต่ปี 2561-2564 พบว่ามีผู้ที่ได้รับความเสียหายจากการถูกแฮก เพื่อปรับเปลี่ยน ขโมย ทำลายข้อมูลคอมพิวเตอร์ พบเป็นอันดับที่ 2 โดยมีผู้มาแจ้งความร้องทุกข์จำนวน 585 ราย ความเสียหายรวมประมาณ 67 ล้านบาท และมีแนวโน้มว่าจะเพิ่มขึ้นในปี 2565[2] และสำหรับสถิติเมื่อปี 65 พบว่าอาชญากรรมไซเบอร์ที่เป็นที่น่ากังวลมาจนถึงปีนี้ในไทยคือ Phishing และ Botnet เฉพาะประเทศไทยนับเป็น 2% ของทราฟฟิคทั่วโลกซึ่งถือว่าเป็นเปอเซ็นที่สูงเป็นอย่างมาเมื่อเทียบกับประชากรในประเทศ[3]อีกทั้งจากผลการเก็บข้อมูลของระบบป้องกันฟิชชิ่ง (Anti-Phishing) ของแคสเปอร์สกี้บล็อกลิงก์ฟิชชิ่งพบว่าลิงก์กว่า 11,260,643 รายการในภูมิภาคเอเชียตะวันออกเฉียงใต้ ส่วนในไทยพบการโจมตีกว่า 1,287,283 รายการ[4]ซึ่งแทบจะทั้งหมดเป็นเรื่องเกี่ยวกับฟิชชิ่งสแกม

ฟิชชิ่งสแกม (Phishing Scam) คือการหลอกลวงทางอินเทอร์เน็ต โดยผู้กระทำความผิดจะหลอกให้ผู้ใช้เปิดเผยข้อมูลส่วนตัว เช่น รหัสผ่าน รายละเอียดบัญชีธนาคาร หรือหมายเลขบัตรเครดิตซึ่งโดยทั่วไปการหลอกลวงด้วยวิธีการฟิชชิ่งมักจะเกี่ยวข้องกับการส่งอีเมลปลอมไปยังผู้ใช้เพื่อรวบรวมข้อมูลส่วนบุคคลและใช้งานในภายหลัง อีเมลเหล่านี้มักจะคล้ายกับการสื่อสารอย่างเป็นทางการจากบริษัทที่ถูกกฎหมาย แต่มีลิงก์ที่นำไปสู่เว็บไซต์ปลอมที่ผู้โจมตีควบคุม ฟิชชิ่งเป็นอาชญากรรมทางไซเบอร์ประเภทหนึ่งที่พบได้บ่อยที่สุด และส่งผลกระทบต่อผู้คนนับล้านทั่วโลก มีสาเหตุหลายประการที่ทำให้บางคนอาจตกเป็นเหยื่อของการหลอกลวงแบบฟิชชิ่ง ฟิชชิ่งเป็นอาชญากรรมทางอินเทอร์เน็ตที่ผู้โจมตีส่งอีเมลหลอกลวงไปยังผู้คนเพื่อพยายามให้พวกเขาเปิดเผยข้อมูลส่วนบุคคล อีเมลฟิชชิงนั้นสั้น ส่งจากบัญชีปลอม และโดยทั่วไปแล้วจะขอข้อมูลส่วนบุคคลที่ละเอียดอ่อน เช่น ชื่อผู้ใช้ รหัสผ่าน รายละเอียดบัตรเครดิต หรือรายละเอียดบัญชีธนาคาร การหลอกลวงแบบฟิชชิ่งได้รับความนิยมอย่างมากเนื่องจากผู้โจมตีใช้ความพยายามเพียงเล็กน้อย นักต้มตุ๋นเพียงแค่ต้องส่งอีเมลและรอให้ใครสักคนตกเป็นเหยื่อ การหลอกลวงเหล่านี้สามารถทำกำไรได้มากหากทำงานได้ดีพอ ฟิชชิ่งเป็น

---

[1] กิตติยา พรหมจันทร์, ‘แนวคิดทางอาชญากรรมไซเบอร์กับเงินในบัญชีที่หายไป’ (Bangkokbiznews, 28 ตุลาคม 2564) <www.bangkokbiznews.com-/blogs/columnist/968445> สืบค้นเมื่อ 23 ธันวาคม 2565.

[2] ไทยรัฐออนไลน์, ‘ปอท. ชี้แนวโน้มอาชญากรรมไซเบอร์ ปี 65 มุ่งการแฮกข้อมูล ฉ้อโกงออนไลน์’ (ไทยร้อออนไลน์, 5 มกราคม 2565) <https://www.thairath.co.th/news/crime/227904> สืบค้นเมื่อ 23 ธันวาคม 2565.

[3] โต๊ะข่าวไอที ดิจิทัล, ‘เปิดโฉมหน้า‘ภัยคุกคามโลกออนไลน์ปี66อาชญากรรมไซเบอร์‘ตามสั่ง’มาแน่!!’ (กรุงเทพธุรกิจ, 2 มกราคม 2566) <https://www.bangkokbiznews.com/tech/gadget/1045935> สืบค้นเมื่อ 4 มกราคม 2566.

[4] โต๊ะข่าวไอที ดิจิทัล, ‘แคสเปอร์สกี้ โชว์สถิติ ‘ฟิชชิ่ง’ ภัยร้ายโจมตีองค์กรธุรกิจ’ (กรุงเทพธุรกิจ, 10 มิถุนายน 2565) <https://www.bangkokbiznews.com/tech/gadget/1045935> สืบค้นเมื่อ 5 มกราคม 2566.

การหลอกลวงประเภทหนึ่งที่มีจุดมุ่งหมายเพื่อขโมยข้อมูลส่วนบุคคลจากผู้ใช้คอมพิวเตอร์ที่ไม่สงสัย โดยทั่วไปจะดำเนินการโดยใช้อีเมล์หรือการส่งข้อความ[5]

เมื่อพิจารณาจากขั้นตอนสำคัญของการ ฟิชชิ่ง จะเห็นได้ว่าในขั้นตอนแรกนั้นจะมีการวางแผนเพื่อค้นหาเหยื่อที่มีความเป็นไปได้ที่จะเข้าไปหลอกลวง และเมื่ออาชญากรนั้นได้เหยื่อแล้วก็จะทำการรวบรวมข้อมูลเบื้องต้นของเหยื่อ ซึ่งนำไปสู่ขั้นตอนถัดไปคือการสร้างเว็บไซต์ปลอมซึ่งมีลักษณะที่เหมือนกับเว็บไซต์จริงเพื่อใช้ในการเก็บข้อมูลของเหยื่อโดยเว็บไซต์ดังกล่าวนั้นอาจจะมีหน้าเว็บที่มามารถเข้าไปใช้งานได้จริงซึ่งผู้เสียหายอาจจะกดเข้าไปใช้บริการเว็บปลอมดังกล่าว การโจมตีแบบฟิชชิ่งมักจะกำหนดเป้าหมายเพื่อเปลี่ยนเส้นทางของการเข้าใช้เว็บไซต์ของเหยื่อไปยังเว็บไซต์ปลอมที่พยายามให้เหยื่อกรอกข้อมูลที่สำคัญอย่างยิ่ง เช่น การเข้าสู่ระบบ และรหัสผ่าน ด้วยเหตุนี้เพื่อให้เกิดความสงสัยน้อยที่สุดเท่าที่จะเป็นไปได้ อาชญากรจึงจัดการลิงก์ที่อยู่ในข้อความที่ส่งไปอย่างอันตราย โดยเฉพาะลิงก์ที่เชื่อมโยงกับที่อยู่ของธนาคารในเบราว์เซอร์รุ่นเก่าที่ใช้งานได้อย่างง่าย เช่น Internet Explorer 6 อาชญากรไซเบอร์จะใช้ความสามารถในการซ่อนที่อยู่ของเว็บจริง ในข้อความอีเมล การซ่อนลิงก์จริงนั้นทำได้ง่ายมาก โดยการเชื่อมโยงข้อความ ต่อมาในขั้นตอนที่สามนั้นในส่วนนี้ขึ้นอยู่กับความไม่ตั้งใจของเหยื่อเองคือ การเข้าไปใช้ลิงก์ที่มีการพิมพ์ผิดเช่น paypai.com แทน paypal.com ข้อผิดพลาดมักจะอยู่ในที่จุด (เช่นตั้งชื่อ bank.com.login ของธนาคารแทน bankname.com /login หรือขีดกลางจะใช้แทนเครื่องหมายทับ นอกจากนี้ยังเกิดขึ้นกับคำที่ถูกแทนที่ในสถานที่เช่น login-nazwatwojegobanku.pl โดยปกติแล้วข้อผิดพลาดดังกล่าวจะไม่มีใครสังเกตเห็น[6] และเมื่อเหยื่อนั้นได้กรอกข้อมูลสำคัญในเว็บไซต์ปลอมที่อาชญากรได้สร้างขึ้นมาสำเร็จแล้วนั้นในขั้นตอนสุดท้ายอาชญากรนั้นก็จะนำข้อมูลซึ่งเป็นข้อมูลจริงตามที่เหยื่อนั้นได้กรอกไปในเว็บไซต์ปลอมที่อาชญากรนั้นได้สร้างขึ้นไปใช้ในการเข้าถึงข้อมูลอื่นๆในเว็บไซต์จริงโดยไม่ได้รับอนุญาต หรืออาจนำไปสร้างความเสียหายในด้านอื่นๆซึ่งทำให้เกิดความเสียหายโดยตรงต่อตัวเหยื่อผู้เป็นเจ้าของขอมูลที่แท้จริง ซึ่งการกระทำเช่นนี้เองหากในอดีตอาจเป็นการหลอกถามหรือใช้วิธีการขโมยตัวตนแต่ในปัจจุบันนั้นเทคโนโลยีถูกพัฒนาไปไกลมากทำให้รูปแบบวิธีการการก่ออาชญากรรมนั้นทำได้โดยง่ายและเกิดความเสียหายได้ง่ายและมีมูลค่าความเสียหายที่มหาศาลมากกว่าในอดีตเป็นอย่างมาก ทั้งยังความสะดวกในแง่ของรูปแบบและวิธีการที่ถูกคิดค้นขึ้นมาเพื่อก่ออาชญากรรม

จากเหตุผลในข้างต้นจะเห็นได้ว่าการก่ออาชญากรรมแบบ ฟิชชิ่ง นั้นก่อให้เกิดความเสียหายมากมายต่อประชาชนและเศรษฐกิจ และจากความเสียหายและวิธีการในการก่ออาชญากรรมจึงมีความจำเป็นที่จะต้องใช้กลไกทางกฎหมายในการควบคุมป้องกันและปราบปรามการกระทำผิดเกี่ยวกับ ฟิชชิ่งให้ลดน้อยลงและกำหนดมาตรการรลงโทษที่เหมาะสมอย่างยั่งยืนเพื่อให้อาชญากรนั้นเกิดความยำเกรงต่อการกระทำความผิดและคำนึงถึงผลของโทษที่จะได้รับ แม้ในปัจจุบันจะมีพระราชบัญญัติว่าด้วยการกระทำความผิด

---

[5] Aoo Studio, ‘Phishing (ฟิชชิ่ง) คืออะไร’ (Aoo Studio, 30 ธันวาคม 2564) <https://aoostudio.com/it-security/phishing> สืบค้นเมื่อ 23ธันวาคม 2565.

[6] Bitdefender, ‘ฟิชชิ่ง (PHISHING) คืออะไร?’ (Bitdefender, 25 มีนาคม 2564) <https://www.bitdefender.co.th/post/phishing/> สืบค้นเมื่อ 24 ธันวาคม 2565.

เกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 ซึ่งถูกประกาศใช้เพื่อบังคับแทน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ที่บังคับใช้มาเป็นระยะเวลานานกว่า 10 ปี โดยมีวัตถุประสงค์เพื่อพัฒนากฎหมายให้เท่าทันกับเทคโนโลยีและภัยคุกคามที่เปลี่ยนแปลงไป แต่อย่างไรก็ตามแม้จะมีการพยามแก้ไขปัญหาด้วยการพัฒนากฎหมายให้เท่าทันภัยคุกคามทางไซเบอร์ที่มีการเปลี่ยนแปลงอยู่ตลอดเวลาแต่ก็ไม่ได้ทำให้การกระทำความผิดลดน้อยลงแต่อย่างใดในทางกลับกันกับมีการเพิ่มขึ้นของการกระทำผิดมากขึ้นเรื่อย ๆทั้งยังมีการพัฒนาอยู่ตลอดเวลา

การค้นคว้าอิสระฉบับนี้ จึงมีวัตถุประสงค์มุ่งเน้นที่จะศึกษาถึงข้อบกพร้องในการบังคับใช้มาตราการทางกฎหมาย ในส่วนของมาตรการทางกฎหมายที่ไม่สามารถบังคับใช้ได้ถึงการกระทำความผิดในรูปแบบของฟิชชิ่งได้อย่างมีประสิทธิภาพเท่าที่ควร ซึ่งจากการศึกษาพบว่าทั้งในกฎหมายหลักอย่างกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560ไม่มีบทบัญญัติที่บัญญัติไว้อย่างชัดเจนเกี่ยวกับการกระทำความผิดเกี่ยวกับการกระทำในลักษณะที่เป็นการ ฟิชชิ่ง ซึ่งผลจากการที่ไม่มีบทบัญญัติใดกำหนดไว้ถึงวิธีการหรือลักษณะของการกระทำความผิดเช่นนี้ไว้เป็นการเฉพาะก็ส่งผลทำให้ไม่มีการกำหนดมาตรการที่จะถูกนำมาใช้จัดการกับการกระทำความผิดในลักษณะ ฟิชชิ่ง อย่างเหมาะสมและผลจากการที่ไม่มีการบัญญัติถึงลักษณะของการกระทำในลักษณะ ฟิชชิ่งที่ชัดเจนมากพอจึงทำให้เกิดปัญหาในการตีความของการนำบทบัญญัติมาใช้บังคับ

อย่างไรก็ตาม เมื่อพิจารณาจากสภาพพฤติกรรมการหลอกลวงผู้เสียหายผ่านทางระบบคอมพิวเตอร์พบว่าในการบังคับใช้มาตรการทางกฎหมายอย่างการนำพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 มาตรา 14(1) มาบังคับใช้นั้นยังมีปัญหา อุปสรรคและข้อจำกัดในการบังคับใช้กฎหมายให้มีมีประสิทธิภาพ เช่น องค์ประกอบของการกระทำความผิดตาม มาตรา 14(1) ที่จำกัดไว้เฉพาะการ“นำข้อมูลเข้าสู่ระบบ”และกำหนดเงื่อนไขด้วยเนื้อหาที่นำเข้าว่าต้องเป็นข้อมูลปลอม เท็จ หรือบิดเบือน ซึ่งไม่ครอบคลุมถึงการกระทำในทางอื่นเช่นการกระทำในทางเทคนิค เช่น การแก้ไขเปลี่ยนแปลง ลบ รบกวนกระแสข้อมูล เพื่อให้เกิดความสับสนของผู้ใช้บริการ จากที่ได้กล่าวมาดังตัวอย่างจะเห็นได้ว่า องค์ประกอบการกระทำความผิดของมาตรรา 14(1) นั้นไม่ครอบคลุมไปถึงการกระทำต่อตัวระบบซึ่งมิใช่การกระทำต่อมนุษย์ อีกทั้งพิจารณาถึงบทลงโทษในการกระทำความผิดตาม มาตรา14(1) ที่มีโทษเพียงจำคุกไม่เกิน 5หรือปรับไม่เกิน100,000 บาทหรือทั้งจำทั้งปรับ[7]ซึ่งโทษดังกล่าวนั้นถือได้ว่าน้อยมากเมื่อเทียบกับความเสียหายที่อาชญากรนั้นได้กระทำ

เมื่อพิจารณาถึงจากเหตุผลดังที่ได้กล่าวมาในข้างต้นจะเห็นได้ถึงความไม่ครอบคลุมถึงการกำหนดมาตรการทางกฎหมายที่ใช้ในการควบคุมการกระทำความผิดในการ ฟิชชิ่ง ที่เกิดขึ้นในปัจจุบันรวมไปถึงการกำหนดบทลงโทษต่างๆที่เหมาะสมกับพฤติการแห่งการกระทำ ทั้งยังมีอุปสรรคในการบังคับใช้มาตรการทางกฎหมายต่างๆ ซึ่งในส่วนนี้เองผู้ศึกษาจะได้ทำการศึกษาและเปรียบเทียบกฎหมายไทยและมาตรการทางกฎหมายในต่างประเทศที่ใช้ในการแก้ปัญหาเกี่ยวกับการ ฟิชชิ่ง ได้แก่ กฎหมายของประเทศสหรัฐอเมริกา,

[7] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 มาตรา 14

กฎหมายธุรกิจทั่วไปรัฐนิวยอร์ก(New York General Business),ประมวลกฎหมายธุรกิจรัฐแคลิฟอร์เนีย (California Coad Annotated) ,กฎหมายพาณิชย์และอิเล็กทรอนิกส์รัฐยูทาห์ (UTAH E-COMMERCE INTEGRITY ACT 2018), กฎหมายรัฐเทนเนสซี (Tennessee Coad Annotated),ประมวลกฎหมายของประเทศเยอรมัน (German Criminal Coad) และประมวลกฎหมายของประเทศฝรั่งเศส

1.2 วัตถุประสงค์การศึกษา

1.2.1 เพื่อศึกษาแนวคิดและหลักการทั่วไปเกี่ยวกับการก่ออาชญากรรมคอมพิวเตอร์รวมถึงศึกษารูปแบบและวิธีการในการก่ออาชญากรรมในรูปแบบการ “ฟิชชิ่ง”โดยเฉพาะกรณีการฉ้อโกงประชาชน

1.2.2 เพื่อศึกษาและวิเคราะห์กฎหมายที่เกี่ยวข้องกับการ ฟิชชิ่ง ของไทยและต่างประเทศ

1.2.3 เพื่อศึกษาถึงรูปแบบและแนวทางในการป้องกันและปรับปรุงมาตรการทางกฎหมายและบทบัญญัติต่างๆที่เกี่ยวกับการ ฟิชชิ่ง ที่เป็นการฉ้อโกงประชาชนรวมไปถึงบทลงโทษให้สอดคล้องกับรูปแบบการก่ออาชญากรรมและความเสียหายที่เกิดขึ้น

1.2.4 เพื่อวิเคราะห์กฎหมายของประเทศไทยที่ใช้อยู่ในปัจจุบัน ว่าควรนำมาปรับใช้กับการฟิชชิ่งอันเป็นการฉ้อโกงประชาชนอย่างไร และควรมีการปรับปรุงแก้ไขกฎหมายให้สามารถลงโทษการกระทำความผิดดังกล่าวเพียงใด

1.3 สมมุติฐานการศึกษา

แม้ว่าในปัจจุบันนี้นั้นประเทศไทยจะได้มีการประกาศบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 ที่เป็นการแก้ไขข้อบกพร้องของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ซึ่งประกาศใช้มาอย่างยาวนานเป็นระยะเวลากว่า 10 ปี แต่ไม่ว่าอย่างไรก็ตามแม้ว่าจะมีการแก้ไขบทบัญญัติให้มีความชัดเจนและทันสมัยมากเพียงใดแต่ก็ไม่ปรากฏถึงการบัญญัติกฎหมายหรือมาตรการทางกฎหมายใดที่จะสามารถนำมาบังคับใช้ได้กับการกระทำความผิดเกี่ยวกับ ฟิชชิ่ง ได้อย่างเฉพาะเจาะจง และจากเหตุผลที่ได้กล่าวมาในข้างต้นนั้นแสดงให้เห็นถึงความจำเป็นที่จะต้องมีการศึกษาค้นคว้าเพื่อหาแนวทางในการพัฒนาและปรับปรุงกฎหมายให้มีความทันสมัยและครอบคลุมเพื่อให้เกิดประสิทธิภาพสูงสุดในการดำเนินคดีกับผู้กระทำผิด

1.4 ขอบเขตของการศึกษา

ในการค้นคว้าอิสระครั้งนี้จึงมีวัตถุประสงค์มุ้งเน้นที่จะศึกษาถึงข้อบกพร้องในการบังคับใช้มาตราการทางกฎหมาย ในส่วนของกฎหมายสาระบัญญัติที่ไม่สามารถบังคับใช้ได้ถึงการกระทำความผิดในรูปแบบของ ฟิชชิ่ง ได้อย่างมีประสิทธิภาพเท่าที่ควร อันเนื่องมาจากการที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 นั้นไม่มีการกำหนดบทบัญญัติที่บัญญัติไว้อย่างชัดเจนเกี่ยวกับการกระทำความผิดเกี่ยวกับการกระทำในลักษณะที่เป็นการ ฟิชชิ่ง อันเป็นผลมาจากการที่ไม่มีบทบัญญัติใดกำหนด

ไว้ถึงวิธีการหรือลักษณะของการกระทำความผิดเช่นนี้ไว้เป็นการเฉพาะ จึงส่งผลทำให้ไม่มีการกำหนดมาตรการที่จะถูกนำมาใช้จัดการกับการกระทำความผิดในลักษณะ ฟิชชิ่ง อย่างเหมาะสม และผลจากการที่ไม่มีการบัญญัติถึงลักษณะของการกระทำในลักษณะ ฟิชชิ่ง ที่ชัดเจนมากพอจึงก่อให้เกิดปัญหาในการตีความของการนำบทบัญญัติในกฎหมายอื่นมาใช้บังคับใช้ อีกทั้งในการศึกษาครั้งนี้จะศึกษาไปถึงบทบัญญัติในประมวลกฎหมายอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับ ฟิชชิ่ง และนอกจากการศึกษาบทบัญญัติที่เกี่ยวข้องกับการกระทำผิด ฟิชชิ่ง ในไทยแล้วผู้ศึกษาก็จะได้ศึกษาไปถึงมาตรการทางกฎหมายและบทบัญญัติอื่นๆในกฎหมายต่างประเทศเพื่อนำมาใช้เป็นแนวทางในการบัญญัติมาตราการป้องกันและแก้ไขการกระทำความผิดเกี่ยวกับ ฟิชชิ่ง ในไทยต่อไป.

1.5 วิธีการศึกษา

การดำเนินการศึกษาในครั้งนี้จะดำเนินการด้วยวิธีการศึกษาเชิงคุณภาพ (Qualitative Research) และวิจัยมีลักษณะเป็นการวิจัยทางเอกสาร(Documentary Research) ทั้งขั้น ปฐมภูมิ (Primary document) และขั้นทุติยภูมิ (Secondary document) โดยจะศึกษาและค้นคว้ารวบรวม ข้อมูล จากหนังสือ บทความ วิทยานิพนธ์ เอกสารวิจัย กฎหมาย ระเบียบ ประกาศ กฎกระทรวง และกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับ ฟิชชิ่ง รวมไปถึงการสืบค้นข้อมูลจาจกอินเทอร์เน็ตจากแหล่งข้อมูลที่เกี่ยวข้องทั้งหลาย เพื่อนำมาศึกษา ทำความเข้าในในเนื้อหา และวิเคราะห์พร้อมเปรียบเทียบ

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 เพื่อทำให้ทราบถึงแนวคิดและหลักการทั่วไปเกี่ยวกับการก่ออาชญากรรมคอมพิวเตอร์รวมถึงศึกษารูปแบบและวิธีการในการก่ออาชญากรรมในรูปแบบการ “ฟิชชิ่ง” โดยเฉพาะกรณีการฉ้อโกงประชาชน

1.6.2 เพื่อทำให้ทราบถึงกฎหมายที่เกี่ยวข้องกับการ ฟิชชิ่ง ของไทยและต่างประเทศ

1.6.3 เพื่อทำให้ทราบถึงรูปแบบและแนวทางในการป้องกันและปรับปรุงมาตรการทางกฎหมายและบทบัญญัติต่างๆที่เกี่ยวกับการ ฟิชชิ่ง รวมไปถึงบทลงโทษ ให้สอดคล้องกับรูปแบบการก่ออาชญากรรมและความเสียหายที่เกิดขึ้น

1.6.4 เพื่อทำให้ทราบถึงแนวทางในการปรับใช้กฎหมายกับการฟิชชิ่งอันเป็นการฉ้อโกงประชาชนอย่างไร และควรมีการปรับปรุงแก้ไขกฎหมายให้สามารถลงโทษการกระทำความผิดดังกล่าวเพียงใด

บทที่ 2
แนวคิดและทฤษฎีที่เกี่ยวข้องกับการก่ออาชญากรรมคอมพิวเตอร์ และรูปแบบการก่ออาชญากรรมด้วยวิธีการฟิชชิ่ง

ในบทนี้ผู้ศึกษาจะได้กล่าวถึงแนวคิดและทฤษฎีในการกำหนดความรับผิดทางอาญา และแนวคิดและทฤษฎีที่เกี่ยวข้องกับการฟิชชิ่ง ซึ่งรวมไปถึงหลักการทั่วไปเกี่ยวกับอาชญากรรมคอมพิวเตอร์และรูปแบบการก่ออาชญากรรมด้วยวิธีการฟิชชิ่ง รวมทั้งความหมายของอาชญากรรมคอมพิวเตอร์และการก่ออาชญากรรมทางคอมพิวเตอร์ด้วยวิธีการฟิชชิ่ง พัฒนาการ รูปแบบและลักษณะในการกระทำความผิดซึ่งจะได้กล่าวถึงในบทนี้ตามลำดับต่อไป

2.1 แนวคิดและทฤษฎีในการกำหนดความผิดทางอาญา

2.1.1 แนวคิดในการกำหนดความรับผิดทางอาญา

แนวคิดในการกำหนดความรับผิดทางอาญา คือ แนวคิดที่ถูกนำมาใช้พิจารณาว่าการกระทำหรือไม่กระทำสิ่งใดของคนในสังคมที่ควรจะกำหนดให้เป็นความผิด โดยอาศัยการบัญญัติกฎหมายอาญาให้มีความสอดคล้องกับมาตรฐานทางศีลธรรมของคนในสังคมมาเป็นตัวกำหนดว่าการกระทำใดเป็นความผิด อย่างการกระทำความผิดร้ายแรงที่ผู้คนในสังคมต่างก็รับรู้ได้ว่าการกระทำนั้นเป็นความผิด อาทิ การฆ่าคน การลักขโมย แต่ไม่ว่าอย่างไรก็ดีบางการกระทำที่ถือว่าเป็นการกระทำที่ผิดศีลธรรมอย่างการคบชู้ การดื่มสุรา การพูดโกหก หรือการกระทำใดๆก็แล้วแต่ที่ไม่ได้ก่อให้เกิดผลกระทบต่อสังคมหรือต่อบุคคอื่นแม้จะผิดศีลธรรมแต่ก็ไม่ถือว่าเป็นความผิดในทางกฎหมาย

จากคำกล่าวในข้างต้นอาจกล่าวได้ว่ากฎหมายอาญานั้นมีพื้นฐานในการกำหนดความผิดมาจากมาตรฐานทางศีลธรรม ความเชื่อ และจารีตประเพณีที่ถือปฏิบัติสืบต่อกันมาของคนในสังคม ซึ่งสิ่งเหล่านี้เองเกิดขึ้นมาจากการที่คนในสังคมเป็นผู้กำหนดขึ้นมาเองว่าสิ่งใดควรหรือไม่ควรที่จะกระทำ ด้วยเหตุนี้เองการกำหนดให้การกระทำใดเป็นความผิดในทางอาญาจึงจำเป็นที่จะต้องกำหนดความผิดจากการกระทำ หรือพฤติกรรมที่ถือเป็นความผิดในตัวเอง (Mala in se) โดยพิจารณาจากลักษณะของการการกระทำความผิดเบื่องต้นที่เป็นการกระทำอันขัดต่อศีลธรรมอันดีของผู้คนในสังคม อาทิ การฆ่าผู้อื่น การทำร้ายร่างกายผู้อื่น นอกจากนี้แล้วนั้นการกระทำบางอย่างที่แม้จะไม่ถือเป็นการกระทำที่ขัดศีลธรรม หรือไม่เป็นความผิดในตัวเอง แต่เป็นความผิดตามที่กฎหมายกำหนดอันเนื่องมาจากการพัฒนาทางสังคมและเทคโนโลยีที่ทำให้รูปแบบการก่ออาชญากรรมนั้นมีการเปลี่ยนแปลงไปเกินกว่ารูปแบบการกระทำความผิดอันเป็นความผิดพื้นฐานตามความหมายทางศีลธรรมอันดีของสังคม จึงจำเป็นที่จะต้องมีการกำหนดหลักเกณฑ์เพิ่มเติมเพื่อกำหนดใน

พฤติกรรมบางประเภทที่อาจก่อความเสียหายต่อสังคม กล่าวคือเป็นความผิดที่เกิดขึ้นจากการที่กฎหมายนั้นกำหนดในเป็นความผิด (Mala prohibita)

โดยจากการศึกษาพบว่าในการพิจารณาว่าการกระทำในลักษณะใดควรจะถูกกำหนดให้เป็นความผิดทางอาญาความผิดทางอาญาสามารถพิจารณาได้โดยอ้างอิงจากแนวคิดการพิจารณาการกระทำอันเป็นความผิดทางอาญาของ Prof. Claus Roxin ซึ่งได้แบ่งแนวคิดดังกล่าวเป็น๒ ส่วน[8] กล่าวคือ ในส่วนแรกกฎหมายอาญาถือเป็นเรื่องของการคุ้มครองนิติสมบัติ และในประการที่สองคือกฎหมายอาญาถือเป็นวิถีทางสุดท้าย ดังนี้

2.1.1.1 กฎหมายอาญาถือเป็นเรื่องของการคุ้มครองนิติสมบัติ

ในส่วนนี้จะเป็นส่วนของประเด็นที่ตั้งคำถามว่ารัฐนั้นมีความชอบธรรมในการกำหนดให้กระกระทำใดอย่างใดอย่างหนึ่งเป็นความผิดได้อย่างไร กล่าวคือ เป็นการตั้งคำถามถึงลักษณะของการกระทำความผิดทางอาญาว่าต้องมีคุณสมบัติอย่างไรรัฐจึงจะมีความชอบธรรมในการกำหนดให้การกระทำดังกล่าวเป็นความผิดอาญา ปัญหาจึงมีอยู่ว่าอะไรคือ สิ่งที่กฎหมายประสงค์จะคุ้มครองเหตุเพราะความผิดทางอาญาแต่ละฐานมีสิ่งที่กฎหมายมุ่งที่จะคุ้มครองแตกต่างกันออกไปสิ่งนั้นคือ นิติสมบัติ หรือ คุณธรรมทางกฎหมาย เช่น ในความผิดฐานทำร้ายร่างกาย สิ่งที่กฎหมายมุ้งคุ้มครองคือ ความปลอดภัยของร่างกาย เป็นต้น

อย่างไรก็ดีคำว่า นิติสมบัติ นอกจากจะเป็นเครื่องมือในการใช้ตีความกฎหมายแล้ว ยังมีหน้าที่ช่วยในการกำหนดนโยบายทางอาญาของฝ่ายนิติบัญญัติด้วย เพราะหากนิติสมบัติถูกนำมาใช้เพียงเพื่อตีความทางกฎหมายอย่างเดียว หลักความรับผิดในนิติสมบัติก็แทบจะไร้ความหมาย และไม่ได้มีความสำคัญเกินไปกว่าเครื่องมือที่ใช้ในการตีความกฎหมายให้เป็นไปตามเจตนารมณ์เพียงเท่านั้น ดังนั้น ในการกำหนดนโยบายทางอาญาจากหลักความรับผิดในนิติสมบัติ นั้น Prof. Claus Roxin ได้อธิบายโดยใช้แนวคิดจากทฤษฎีสัญญาประชาคมว่า กฎหมายอาญาถูกกำหนดไว้เพื่อเป็นหลักประกันว่าประชาชนทุกคนจะสามารถใช้ชีวิตได้อย่างเสรีและปลอดภัยภายใต้หลักประกันอันเป็นสิทธิขั้นพื้นฐานที่ได้ถูกรับรองไว้ในรัฐธรรมนูญ หรืออาจกล่าวอีกนัยนึงได้ว่า นิติสมบัติ คือเหตุผลที่ทำให้ต้องบัญญัติความผิดฐานนนั้นๆขึ้นมา[9] และเมื่อพิจารณาจากข้อความในข้างต้นอาจกล่าวโดยสรุปได้ว่านิติสมบัติ คือทุกๆข้อเท็จจริงหรือเป้าหมายที่มีความสำคัญต่อปัจเจกชนแต่ละคนเพื่อให้บุคคลสามารถใช้เสรีภาพของตนได้อย่างเสรี[10]

แต่ไม่ว่าอย่างไรก็ตาม ในความผิดอาญาบางฐานที่รัฐนั้นกำหนดขึ้นมาใช้ในบางความผิดก็มิใช้กรณีที่จะทำให้การดำเนินชีวิตร่วมกันในสังคมของบุคคลเกิดความไม่สงบหรือสูญเสียไปซึ่งเสรีภาพในการดำเนินชีวิต ซึ่งส่งผลให้การกำหนดความผิดฐานนั้นไม่ถูกต้องและนำไปสู่ปัญหาในเรื่องกฎหมายอาญาเฟ้อ ที่

---

[8] สุรสิทธิ์ แสงวิโรจนพัฒน์, ‘หลักเกณฑ์การกำหนดความผิดทางอาญาตามกฎหมายต่างประเทศ’(เมษายน - มิถุนายน 2564) 2 บทบัณฑิตย์ 128.

[9] คัทราวดี สีทองเสือ, ‘คุณธรรมทางกฎหมายในกฎหมายอาญา: ศึกษาความผิดฐานรับของโจร’ (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยลัยธุรกิจบัณฑิตย์ 2557) 2.

[10] สุรสิทธิ์ แสงวิโรจนพัฒน์ (เชิงอรรถ 8) 129.

ถือได้ว่าเป็นสิ่งที่อยู่ตรงข้ามกับแนวคิดในเรื่องการคุ้มครองนิติสมบัติที่สำคัญซึ่ง Prof. Claus Roxin ได้ให้ข้อสังเกตไว้ดังนี้[11]

(1) กฎหมายอาญาที่ละเมิดต่อสิทธิขั้นพื้นฐานหรือกฎหมายอาญาที่มีจุดมุ่งหมายเพียงเพื่อเหตุผลทางการเมืองเพียงอย่างเดียว ไม่ถือเป็นกฎหมายอาญาที่คุ้มครองนิติสมบัติ

(2) เจตนารมณ์ของกฎหมายไม่ถือเป็นนิติสมบัติในทุกกรณี

(3) การกระทำที่ขัดต่อศีลธรรมอันดีไม่ถือว่าเป็นการกระทำที่ละเมิดต่อนิติสมบัติที่จะทำให้สามารถลงโทษบุคคลในทางอาญาได้

(4) การละเมิดต่อศักดิ์ศรีความเป็นมนุษย์ของตนเองหรือของมนุษยชาติ ไม่ถือเป็นเหตุที่จะทำให้สามารถลงโทษทางอาญาได้ทุกกรณี

(5) เฉพาะแค่ความรู้สึกคุกความเท่านั้นที่จะถือเป็นนิติสมบัติที่ได้รับการคุ้มครอง

(6) การจงใจทำร้ายรางการตนเองไม่อาจถือเอามาเป็นเหตุในการลงโทษทางอาญาได้

(7) การใช้กฎหมายอาญาในเชิงสัญลักษณ์ (das symbolische Strafrecht) เป็นสิ่งต้องห้ามในการบังคับใช้กฎหมายอาญา

(8) สิ่งที่คนส่วนใหญ่เห็นว่าไม่ควรทำ ไม่ถือเป็นนิติสมบัติ

(9) สิ่งที่เป็นนามธรรมไม่อาจถูกทำให้เสียหายหรือเสื่อมค่าลงได้ ไม่ถือเป็นนิติสมบัติ

2.1.1.2 กฎหมายอาญาถือเป็นวิธีทางสุดท้าย[12]

สำหรับแนวคิดของหลักการในเรื่องนี้ คือ กฎหมายอาญาจะถูกนำมาใช้ก็ต่อเมื่อไม่มีมาตราการอื่นใดที่จะสามารถนำมาบังคับใช้ได้อย่างมีประสิทธิภาพเพียงพอจะนำมาบังคับใช้กับการกระทำความผิดได้ไม่ว่าจะเป็นมาตราการทางแพ่ง หรือมาตราการทางปกครองก็ตาม ด้วยเหตุนี้เองการบังคับใช้โทษทางอาญาจึงได้ชื่อว่าเป็นมาตราการสุดท้ายของนโยบายในทางสังคม โดยหลักการดังกล่าวมีแนวคิดมาจากหลักความได้สัดส่วน ซึ่งถือเป็นหลักการที่สำคัญยิ่งที่ได้รับการบัญญัติไว้ในรัฐธรรมนูญ กล่าวคือ หากรัฐมีตัวเลือกอย่างอื่นในการนำมาตรการต่างๆ ที่มีความรุนแรงน้อยกว่าการบังคับใช้มาตรการทางอาญา ซึ่งสามารถนำมาบังคับใช้ให้เป็นผลร้ายต่อตัวผู้กระทำความผิด แล้วได้ผลในการคุ้มครองนิติสมบัติที่เท่ากันเมื่อเทียบกับการบังคับใช้มาตราการทางอาญา และด้วยเหตุนี้เองการบังคับใช้มาตราการทางอาญาจึงมิใช้สิ่งที่จำเป็นเสมอไป หากสามารถนำมาตราการอื่นที่ได้ผลเหมือนกันแต่ที่ระดับความรุนแรงน้อยกว่ามาบังคับใช้ได้

---

[11] เพิ่งอ้าง 130.

[12] เพิ่งอ้าง 135.

ประเด็นในเรื่องนี้จึงมีอยู่ว่าเมื่อใดจึงจะควรใช้มาตรการทางอาญา หรือควรใช้มาตรการอื่นในการลงโทษอย่างเช่นการปรับทางพินัย โดยในประเด็นนี้ Prof. Claus Roxin ได้ให้ความเห็นว่าหากสามารถใช้มาตราการอื่นอย่างการปรับทางพินัยแทนการใช้มาตราการทางอาญาก็เพียงพอที่จะสามารถคุ้มครองนิติสมบัติในความผิดเล็กๆ น้อยๆ ที่ไม่ได้มีความเสียหายต่อสังคมมากเท่าไรนักนอกจากนี้การปรับในทางพินัยยังสามารถนำมาบังคับใช้กับกรณีที่แม้จะเป็นความประมาทเพียงเล็กน้อยแต่ก่อให้เกิดความเสียหายต่อสังคม ที่แม้จะเป็นความผิดทางอาญาและต้องใช้มาตราการทางอาญากับกรณีดังกล่าว แต่ Prof. Claus Roxin กลับเห็นต่างว่าการใช้มาตราการปรับทางพินัยก็สามารถที่จะได้ผลคุ้มครองเช่นเดียวกันกับการบังคับใช้มาตรการทางอาญา

ด้วยเหตุนี้เองจึงเป็นที่มาของแนวคิดของวัตถุประสงค์ในการนิติบัญญัติกฎหมายอาญาซึ่งจากการศึกษาพบว่า รองศาสตราจารย์ ดร. อภิรัตน์ เพ็ชรสิริ ได้เรียบเรียงและอธิบายหลักเกณฑ์ในการกำหนดความผิดอาญา โดยมีที่มาจากแนวคิดและวัตถุประสงค์ในการนิติบัญญัติกฎหมายอาญา ไว้ทั้งหมด 6 ประการ[13]ดังนี้

(1) เพื่อคุ้มครองป้องกันซึ่งตัวบุคคล หรือสัตว์ในบางกรณี จากการกระทำที่ไม่พึงประสงค์อย่างร้ายแรงอันมิอาจที่จะให้อภัยได้ ทั้งที่กระทำไปโดยเจตนาหรือไม่เจตนาก็ตาม

(2) เพื่อคุ้มครองป้องกันสภาพจิตใจของผู้คนในสังคมจากการกระทำที่ผิดธรรมชาติและศีลธรรมอันดีของผู้คนในสังคม หรือพฤติกรรมบางประการอันอาจยั่วยุให้เกิดความแตกแยกแก่ผู้คนในสังคม

(3) เพื่อคุ้มครองป้องกันซึ่งทรัพย์สินของบุคคลจากการลักขโมย, ยักยอก, ทำให้เสียทรัพย์หรือรวมกรณีอื่นๆอันเป็นการกระทำที่ละเมิดต่อทรัพย์สินโดยปราศจากอำนาจ

(4) เพื่อคุ้มครองป้องกันผลประโยชน์สาธารณะของคนในสังคมซึ่งรวมไปถึงสภาพบังคับทางอาญาเพื่อเก็บรวบรมภาษีภาษี เช่น ห้ามครอบครองรถยนต์หรือทรัพย์สินบางประการโดยไม่มีทะเบียนและชำระภาษี

(5) เพื่อคุ้มครองป้องกันและรักษาไว้ซึ่งสถาบันทางสังคมซึ่งรวมไปถึงการกำหนดกฎเกณฑ์ในการบังคับให้เกิดความกรุณาอันสมควรเท่าที่จำเป็น

(6) เพื่อให้วิธีการต่างๆสามารถบังคับใช้กับกฎเกณฑ์ต่างๆได้อย่างสอดคล้องกับวัตถุประสงค์ในข้างต้น

---

[13] อภิรัตน์ เพ็ชรศิริ, *ทฤษฎีอาญา ทฤษฎีโทษ และกระบวนการขั้นพื้นฐาน* (พิมพ์ครั้งที่ 4, สำนักพิมพ์วิญญูชน 2562) 49-50.

ทั้งนี้จากหลักเกณฑ์ดังที่ได้กล่าวไปในข้างต้นจะเห็นได้ว่าในการบัญญัติว่าการกระทำใดเป็นความผิดทางอาญานั้นจะต้องมีการกำหนดพฤติกรรมในการกระทำว่าพฤติกรรมใดเป็นการกระทำที่จะถือได้ว่าอยู่ในวัตถุประสงค์ที่กฎหมายอาญามุ่งหวังที่จะกระทำให้บรรลุผล ด้วยเหตุนี้เองจึงได้มีการจึงได้มีการกำหนดทฤษฎีเพื่อที่จะนำมากำหนดของเขตของพฤติกรรม โดยนักวิชาการต่างๆได้มีการคิดค้นหลักเกณฑ์ในการกำหนดพฤติกรรมและทฤษฎีต่างๆขึ้นมามากมายซึ่งเป็นที่รู้จักในชื่อ ทฤษฎีว่าด้วยการกำหนดปริมลฑลของกฎหมายอาญาสารบัญญัติตามทฤษฎีทางอาญา อันเป็นการกำหนดหลักเกณฑ์ว่าด้วยการจำกัด[14] ดังนี้

(1) กฎหมายอาญาต้องบัญญัติขึ้นเพื่อใช้บังคับอย่างเสมอภาค โดยไม่คำนึงถึงประโยชน์ของฝ่ายใดฝ่ายหนึ่ง

(2) ไม่ควรนำกฎหมายอาญามาใช้บังคับโทษแก่การกระทำที่ปราศจากความน่าตำหนิ

(3) การบังคับใช้กฎหมายอาญาต้องถือเป็นมาตรการสุดท้ายเมื่อไม่มีมาตรการใดสามารถที่จะสามารถนำมาใช้บังคับได้อย่างสมควร

(4) การบังคับใช้มาตรการลงโทษทางอาญาต้องสัมพันธ์กันกับผลของความเสียหายที่เกิดขึ้นจากการกระทำความผิด

(5) กฎหมายอาญาต้องไม่ถูกใช้เป็นเครื่องมือในการกำหนดพฤติกรรมหรือเพื่อให้ปฏิบัติตามแนวทางอันเป็นประโยชน์แก่ผู้บังคับใช้กฎหมาย

จากหลักเกณฑ์และทฤษฎีดังที่ได้กล่าวไปในข้างต้นจะเห็นได้ว่าโดยหลักแล้วกฎหมายอาญานั้นถูกกำหนดมาเพื่อใช้บังคับแก่ผู้คนทุกคนในสังคม โดยมีวัตถุประสงค์เพื่อปกป้องบุคคลจากการกระทำอันละเมิดไม่ว่าต่อทรัพย์สินหรือต่อเนื้อตัวร่างกาย ซึ่งรวมไปถึงการกระทำต่อจิตใจด้วย อย่างไรก็ดีการคุ้มครองเช่นว่านี้จำเป็นที่จะต้องกระทำภายใต้ของเขตของกฎหมายอาญาที่จะสามารถนำมาบังคับใช้ได้ ซึ่งจะต้องบังคับใช้โดยคำนึงถึงพฤติกรรมที่เป็นภัยและการใช้การบังคับใช้กฎหมายอาญานั้นต้องเป็นมาตรการสุดท้ายเมื่อไม่มีมาตรการอื่นใดที่จะนำมาบังคับได้อย่างเหมาะสมโดยต้องพิจารณาจากความเสียหายที่เกิดขึ้นจากการกระทำให้สัมพันธ์กับบทลงโทษที่จะได้รับและการบังคับใช้กฎหมายอาญาต้องเป็นไปเพื่อการปกป้องผลประโยชน์ของคนในสังคมเพียงเท่านั้น

2.1.2 หลักความชอบด้วยกฎหมาย

“หลักความชอบด้วยกฎหมายอาญา”[15]หรือ“หลักประกันทางอาญา”[16]หรือ“เอกลักษณ์ของกฎหมายอาญา”[17] มีที่มาจากสุภาษิตในภาษาลาตินที่ว่า “Nullum crimen, nulla poena sine lege”หรือ

---

[14] เพิ่งอ้าง 51-56.

[15] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, ‘หลักความชอบด้วยกฎหมายในกฎหมายอาญา (PRINCIPLE DE LA LEGALITE CRIMINELLE)’ ใน *รวมบทความทางวิชาการเนื่องในโอกาสครบรอบ 84 ปี ศาสตราจารย์ จิตติ ติงศภัทย์* (คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2536) 11.

[16] คณิต ณ นคร, *กฎหมายอาญา ภาคทั่วไป* (พิมพ์ครั้งที่ 7, สำนักพิมพ์วิญญูชน 2563) 89.

[17] เพิ่งอ้าง 89.

ในภาษาอังกฤษคือ “No crime nor punishment without law” ซึ่งหมายความว่า“ไม่มีความผิด ไม่มีโทษโดยไม่มีกฎหมาย” โดยสุภาษิตนี้เองถือได้ว่าเป็นหลักสำคัญในการตีความและบังคับใช้กฎหมายอาญา เนื่องจากกฎหมายอาญานั้นบัญญัติขึ้นเพื่อใช้เป็นเครื่องมือในการกำหนดความประพฤติของคนในสังคม หากละเมิดจะต้องถูกลงโทษและถูกคนในสังคมมองว่าเป็นผู้กระทำความผิดด้วยเหตุนี้เองในการตีความและบังคับใช้กฎหมายอาญาจึงต้องตีความตามตัวอักษรห้ามมิให้เทียบเคียงกฎหมายอื่น

อย่างไรก็ดีในการตีความกฎหมายอาญาจึงจำเป็นต้องคำนึงถึงหลักเกณฑ์ตามสุภาษิตลาตินดังที่ได้กล่าวมาในข้างต้น ซึ่งจากการศึกษาพบว่า Anselm von Feuerbach ได้มีการวางหลักเกณฑ์ที่ซึ่งถือได้ว่าเป็น “หลักประกันในกฎหมายอาญา” ไว้ในหนังสือกฎหมายของเขาที่เขียนขึ้นในปี ค.ศ.1801 ซึ่งได้วางหลักไว้ 3 ประการ ดังนี้[18]

(1) ในการลงโทษต้องมีกฎหมายกำหนดให้ลงโทษได้ (nulla poena sine lege)

(2) การลงโทษต้องขึ้นอยู่กับพฤติกรรมที่กระทำ (nulla poena sine Crmime)

(3) โทษที่จะลงต้องเป็นไปตามกฎหมายกำหนด (Nullum Crime sine poena legali)

จากหลักการข้างต้นจะเห็นได้ว่าในกฎหมายของประเทศไทยนั้นได้มีการบัญญัติหลักเกณฑ์ดังกล่าวไว้ครั้งแรกในกฎหมายลักษณะอาญา รศ.127[19] มาตรา 7 ความว่า “บุคคลควรรับอาญา ต่อเมื่อได้กระทำการอันกฎหมายซึ่งใช้อยู่ในเวลาที่กระทำนั้นบัญญัติว่าเป็นความผิด และกำหนดโทษไว้ และอาญาที่จะใช้ลงโทษผู้กระทำความผิดนั้น ก็ไม่ควรใช้อาญาอย่างอื่นนอกจากอาญาที่ได้บัญญัติไว้ในกฎหมาย”

หลักการดังกล่าวนี้เองถือได้ว่าเป็นหลักการสำคัญที่ได้รับการยอมรับไว้ในกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights) (ICCPR) ข้อที่ 15[20] “บุคคลย่อมไม่ต้องรับผิดทางอาญาเพราะกระทำหรืองดเว้นกระทำการใดซึ่งในขณะที่กระทำไม่เป็นความผิดอาญาตามกฎหมายภายในหรือกฎหมายระหว่างประเทศและจะลงโทษให้หนักกว่าโทษที่มีอยู่ในขณะที่ได้กระทำความผิดอาญาหาได้ไม่...” ซึ่งผลจากกติกานี้เองก่อให้เกิดหลักสำคัญทางอาญาที่ใช้ในการบังคับใช้กฎหมาย

อนึ่ง เนื่องจากกฎหมายอาญานั้นเป็นกฎหมายที่เกี่ยวข้องกับการลงโทษบุคคลที่ได้กระทำความผิดตามที่ได้มีการบัญญัติไว้ในกฎหมายให้เป็นความผิด ซึ่งโทษที่จะลงนั้นมีผลกระทบต่อ เนื้อตัว ร่างกาย และทรัพย์สิน และจากหลักการดังที่ได้กล่าวไปในข้างต้นของกฎหมายอาญาจึงถือได้ว่ามีความสำคัญอย่างยิ่งทั้งใน

---

[18] อภิรัตน์ เพ็ชรศิริ (เชิงอรรถ 13).

[19] ยอร์ช ปาดูซ์, *บันทึกของนายยอร์ช ปาดูซ์ (G.PADOUX) เกี่ยวกับการร่างกฎหมายลักษณะอาญา รศ.127* (สุรศักดิ์ ลิขสิทธิ์วัฒนกุล ผู้แปล, สำนักพิมพ์วิญญูชน 2546).

[20] International Covenant on Civil and Political Rights (adopted16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 15 “No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time when the criminal offence was committed.....”.

ระดับประเทศและในระดับสากลเพราะถือว่าหลักการดังกล่าวนี้นั้นเป็นหลักการที่ได้รับการยอมรับกันโดยทั่วไปในระดับสากล โดยสาเหตุสำคัญที่หลักการนี้มีความสำคัญในทางกฎหมายอาญาเพราะหลักการดังกล่าวนี้นั้นเห็นว่าในการบัญญัติกฎหมายอาญานั้นต้องมีบทบัญญัติที่ชัดเจนวางไว้เป็นกรอบกติกาว่าอย่างไรทำได้ อย่างไรทำไม่ได้ และจะได้รับโทษอย่างไรหากละเมิดกติกาดังกล่าว ซึ่งจากเหตุผลดังที่ได้กล่าวมานี้ประชาชนนั้นจะสามารถพิจารณาและตัดสินใจได้ว่าจะกระทำการใดหรือไม่กระทำการใดและเพื่อเป็นแนวทางในการประพฤติปฏิบัติของประชาชนในรัฐอันเป็นการป้องกันมิให้เกิดการการทำความผิดโดยไม่เจตนาเพราะความไม่รู้กฎหมายกล่าวคือเปรียบเสมือนเป็นการเตือนจากรัฐว่าการกระทำใดทำได้การกระทำใดทำไม่ได้ ด้วยเหตุนี้เองในการบัญญัติกฎหมายอาญาจึงต้องมีความชัดเจนและแน่นอนไม่กำกวมหรือคุมเคลือ เพื่อเป็นการป้องกันการใช้อำนาจและถ่วงดุลอำนาจของภาครัฐไม่ให้ใช้อำนาจตามอำเภอใจ รวมไปถึงเพื่อเป็นการจำแนกกฎหมายและสะท้อนให้เป็นถึงความจำเป็นที่จะต้องบัญญัติกฎหมายไว้เป็นลายลักอักษรเพื่อความชัดเจนในการกำหนดความผิดและโทษก่อนที่จะนำไปใช้บังคับแก่บุคคลใดก็ตาม เพราะถือว่าการกระทำใดก็ตามจะเป็นความผิดได้ต่อเมื่อได้บัญญัติไว้เป็นลายลักษณ์อักษรมีการกำหนดบทลงโทษที่ชัดเจนไว้แล้วเท่านั้น

โดยในประเทศไทยนั้นได้มีการบัญญัติหลักการดังกล่าวไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย ฉบับปี 2560 ในหมวดที่ 3 สิทธิและเสรีภาพของชนชาวไทยว่า “มาตรา 29 บุคคลไม่ต้องรับโทษอาญาเว้นแต่ได้กระทำการอันกฎหมายที่ใช้อยู่ในเวลาที่กระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่บุคคลนั้นจะหนักกว่าโทษที่บัญญัติไว้ในกฎหมายที่ใช้อยู่ในเวลาที่กระทำความผิดมิได้”[21]

นอกจากนี้แล้วยังได้มีการบัญญัติหลักการดังกล่าวไว้ในทำนองเดียวกันในประมวลกฎหมายอาญา มาตรา 2 “บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการอันกฎหมายที่ใช้ในขณะกระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแต่ผู้กระทำความผิดนั้นต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย”[22]

จากที่ได้กล่าวมาในข้างต้นนั้นจะเห็นได้ว่าในการบังคับใช้กฎหมายอาญาจะต้องพิจารณาถึงลักษณะของการกระทำหรือไม่กระทำว่าในช่วงเวลาขณะนั้นมีกฎหมายกำหนดให้การกระทำหรือไม่กระทำนั้นเป็นความผิดหรือไม่และหากพบว่ามีการกำหนดให้เป็นความผิดก็จะต้องดูต่อไปว่ากฎหมายนั้นมีการกำหนดโทษสำหรับการกระทำความผิดนั้นไว้เช่นไร และด้วยเหตุเช่นนี้เองในการที่จะบังคับใช้กฎหมายอาญาทุกครั้งจึงต้องพิจารณาถึงบทบัญญัติในกฎหมายอาญาซึ่งบัญญัติไว้เป็นลายลักษณ์อักษรอย่างชัดเจน โดยในการบังคับโทษนั้นจะบังคับได้แต่เฉพาะความผิดที่เกิดขึ้นภายหลังที่กฎหมายมีผลบังคับใช้เท่านั้น และจากหลักการดังกล่าวนี้เองนอกจากกจะได้รับการยึดถือและปฏิบัติตามกันมาอย่างเคร่งครัดและยาวนาน หลักการดังกล่าวนี้เองยังถือได้ว่าเป็นหลักที่สำคัญที่สุดหลักหนึ่งในกฎหมายอาญา ซึ่งส่งผลให้เกิดผลในทางกฎหมายอาญาหลายประการ กล่าวคือ หลักการดังกล่าวถูกนำมาใช้กับการวินิจฉัยความรับผิดทางอาญาของบุคคล อาทิ หลักการกฎหมายไม่มีผลย้อนหลัง เว้นแต่การย้อนหลังนั้นจะเป็นประโยชน์แก่จำเลย, หลักกฎหมายอาญาต้องบัญญัติ

---

[21] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560.

[22] ประมวลกฎหมายอาญา มาตรา 2.

ไว้เป็นลายลักอักษรณ์เพื่อความชัดเจนในการบังคับใช้และตีความกฎหมายเพราะถือว่าในการบัญญัติกฎหมายอาญานั้นต้องบัญญัติโดยใช้ถ้อคำที่ชัดเจน ไม่กำกวม ไม่คลุมเครือ และการในการตีความกฎหมายต้องตีโดยเคร่งครัดในความความอย่างแคบเพื่อป้องกันการไม่ให้มีการขยายความจนก่อให้เกิดผลร้ายหรือเกิดการลงโทษเกินจำเป็นอันนำไปสู่ความไม่ยุติธรรมในการบังคับใช้กฎหมายอาญา

2.1.3 หลักการกำหนดโทษให้ได้สัดส่วนเหมาะสมกับความผิด

หลักความได้สัดส่วน (Principle of proportionality) เป็นหลักการพื้นฐานภายใต้หลักนิติธรรม (Rule of Law) ที่ได้รับการยอมรับอย่างเป็นสากล โดยเฉพาะอย่างยิ่งเมื่อรัฐต้องการใช้กฎหมายเป็นเครื่องมือในการคุ้มครองสังคมก็จะต้องนำหลักความได้สัดส่วนในกระบวนการยุติธรรมทางอาญามาใช้เป็นหลักเกณฑ์ในการพิจารณาออกมาตราการทางกฎหมายต่างๆ เพื่อปกป้องสิทธิมนุษยชนขั้นพื้นฐานและเพื่อสร้างความสมดุลระหว่าการใช้อำนาจของรัฐกับเสรีภาพของประชาชน เพราะถือว่าการกออกมาตรการทางกฎหมายใดๆก็ตามของภาครัฐจะเป็นผลในการจำกัดสิทธิและเสรีภาพของประชาชนด้วยเหตุนี้เองรัฐจึงต้องพิจารณาถึงความได้สัดส่วนในการออกมาตราการทางกฎหมายต่างๆโดยคำนึงถึงความเหมาะสมและความจำเป็นเป็นหลัก ทั้งยังต้องคำนึงผลกระทบที่จะเกิดขึ้นกับประชาชน ว่าคุ้มค่าหรือไม่ในการออกมาตราการทางกฎหมายนั้นๆ[23]

โดยแนวคิดการกำหนดโทษให้ได้สัดส่วนเหมาะสมกับความผิดมีทฤษฎีที่สนับสนุนแนวคิดอยู่ดังนี้[24]

2.1.3.1 ทฤษฎีเจตจำนงอิสระ (Free will Theory)

ทฤษฎีนี้มีแนวคิดที่ว่า การพิจารณาบทลงโทษผู้กระทำความผิดควรที่จะพิจารณาถึงความความได้สัดส่วนของร้ายแรงในอาชญากรรมที่ตัวผู้กระทำความผิดนั้นได้กระทำลงไป กล่าวคือ การลงโทษต้องไม่มากเกินไปจนมีลักษณะที่โหดร้ายทารุณเกินจำเป็น หรือไม่น้อยเกิดไปจนผู้กระทำความผิดคิดว่าการกระทำความผิดนั้นคุ้มค่าหากลงมือกระทำความผิด โดยทฤษฎีนี้เชื่อว่ามนุษย์มีอิสระในการเลือกทำสิ่งใดๆ ก็ตามที่เห็นว่าเป็นประโยชน์กับตนมากกว่าเป็นผลเสีย เช่นเดียวกับการก่ออาชญากรรมหากผู้กระทำความผิดเห็นว่าโทษที่จะได้รับจากการกระทำความผิดนั้นคุ้มค่าเมื่อเทียบกับประโยชน์ที่จะได้รับจากการกระทำความผิดผู้กระทำความผิดก็จะตัดสินใจเลือกกระทำความผิดนั้นดังนั้น ด้วยเหตุนี้เองในการพิจารณาลงโทษผู้กระทำความผิดจึงต้องพิจารณาถึงความได้สัดส่วนของความร้ายแรงของอาชญากรรมให้สัมพันธ์กับโทษ เพื่อป้องกันไม่ให้เกิดการใช้บทลงโทษเกินจำเป็น หรือทำให้ผู้กระทำความผิดรู้สึกได้ประโยชน์จากการกระความผิด

2.1.3.2 ทฤษฎีอรรถประโยชน์นิยม (Utilitarian Theory)[25]

ทฤษฎีนี้มีแนวคิดที่ว่า การออกกฎหมายต้องสอดคล้องกับกฎของธรรมชาติที่ต้องคำนึงถึงมวลความสุขของคนในสังคมส่วนใหญ่เป็นสำคัญ กล่าวคือ ทฤษฎีนี้เชื่อว่า กฎของธรรมชาตินั้นมีอยู่ด้วยกัน 2 ประการ คือ ประการแรกคือความพอใจ และอีกประการคือความเจ็บปวด โดยกฎทั้งสองประการนี้

---

[23] กิติมา แก้วนะรา,‘หลักความได้สัดส่วนกับการกำหนดโทษทางอาญาที่เหมาะสมสำหรับผู้กระทำความผิดในคดียาเสพติดให้โทษ: ศึกษากรณีแอมเฟตามีน’(วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธุรกิจบัณฑิตย์) 128.

[24] อัจฉรียา ชูตินันทน์, *อาชญาวิทยาและทัณฑวิทยา* (พิมพ์ครั้งที่ 5, สำนักพิมพ์วิญญูชน 2566) 236.

[25] เพิ่งอ้าง 237.

จะเป็นตัวกำหนดพฤติกรรมของมนุษย์เสมอ ดังนั้น ก่อนที่มนุษย์จะทำอะไรจะต้องคำนึงถึงกฎของธรรมชาติสองข้อนี้ก่อนเสมอ การประกอบอาชญากรรมก็เช่นเดียวกัน หากผู้กระทำผิดนั้นคำนึงถึงกฎสองข้อนี้แล้วเห็นว่าผลของการกระทำความผิดทำให้พอใจได้มากกว่าความเจ็บปวดที่จะได้รับเมื่อต้องถูกลงโทษ บุคคลนั้นก็จะตัดสินใจกระทำความผิด ดังนั้น ด้วยเหตุนี้เองในการออกกฎหมายรัฐจึงจำเป็นต้องกำหนดบทลงโทษทางอาญาให้ได้สัดส่วนอย่าเหมาะสมมากพอที่จะทำให้ผู้กระทำความผิดรู้สึกไม่คุ้มค่าเมื่อจะต้องรับโทษ โดยใช้ความสุขของคนในสังคมเป็นเกณฑ์พื้นฐานเรื่อง ความถูกต้องเหมาะสม ที่จะก่อให้เกิดประโยชน์สุขที่จะเกิดแก่ประชาชนในสังคมเป็นสำคัญ

2.1.3.3 ทฤษฎีการลงโทษเพื่อข่มขู่ยับยั้ง (Deterrence Theory)[26]

ทฤษฎีนี้มีวัตถุประสงค์ 2 ประการ คือ ประการแรกเพื่อลดอาชญากรรม หรือการกระทำความผิดซ้ำ ประการที่สองเพื่อข่มขู่และเป็นเยี่ยงอย่างมิให้คนในสังคนทำตาม ในการกำหนดโทษให้ได้สัดส่วนจึงต้องกำหนดตามความเหมาะสมกับระดับความร้ายแรงของการกระทำความผิด โดยการใช้มาตราการลงโทษทางอาญาถือเป็นหนทางสุดท้ายในการบังคับใช้มาตราการทางกฎหมายเพื่อข่มขู่ยับยั้งการกระทำความผิดเพื่อให้คนในสังคมเกิดความกลัวและไม่เอาเป็นเยี่ยงอย่าง และเพื่อเป็นการป้องกันมิให้ผู้กระทำความผิดกลับมากระทำความผิดซ้ำ ซึ่งถือได้ว่าเป็นวัตถุประสงค์หนึ่งของการลงโทษในปัจจุบัน

2.2 แนวทางในการกำหนดความผิดเกี่ยวกับคอมพิวเตอร์ในกฎหมายไทย

จากที่ได้กล่าวมาในหัวข้อข้างต้นเกี่ยวกับการบัญญัติโทษทางอาญาและหลักการกำหนดโทษให้ได้สัดส่วนเหมาะสมกับความผิด ในกฎหมายซึ่งจะถูกนำมาใช้กำหนดการกระทำของคนในสังคมว่าสิ่งใดทำได้และสิ่งใดทำไม่ได้และจะต้องได้รับโทษอย่างไรหากฝ่าฝืนบทบัญญัติดังกล่าวและในการกำหนดบทบัญญัติและโทษนั้นต้องบัญญัติไว้โดยชัดเจนในความหมายอย่างแคบเพื่อไม่ให้เกิดการใช้กฎหมายผิดเจตจำนงค์ของบทบัญญัติ แต่ไม่ว่าอย่างไรก็ตามในการที่จะกำหนดบทบัญญัติให้ชัดเจนครอบคลุมทุกฐานความผิดนั้นคงไม่อาจที่จะกำหนดให้คลอบคลุมทุกฐานความผิดได้ เนื่องจากวิวัฒนาการทางสังคมและเทคโนโลยีที่เปลี่ยนไปรูปแบบในการก่ออาชญากรรมของอาชญากรเองก็มีการพัฒนาและเปลี่ยนแปลงไปตามบริบทของสังคมเช่นกัน โดยเฉพาะอย่างยิ่งในสังคมยุคปัจจุบันที่มีการใช้เทคโนโลยีสารสนเทศกันอย่างแพร่หลาย ด้วยเหตุนี้เองจึงทำให้อาชญากรใช้ช่องทางดังกล่าวในการก่ออาชญากรรมซึ่งในที่นี้ไม่ใช้การกระทำต่อเนื้อตัวร่างกายเหมือนเช่นในอดีตแต่เป็นการก่ออาชญากรรมโดยใช้เทคโนโลยีเข้ามาเป็นเครื่องมือในการใช้ก่ออาชญากรรม ด้วยเหตุนี้เองในการบัญญัติกฎหมายจึงจำเป็นที่จะต้องบัญญัติกฎหมายให้ครอบคลุมไปถึงการกระทำความผิดที่เกิดจากการใช้เทคโนโลยีเข้ามาเพื่อใช้ในการก่ออาชญากรรม

อนึ่ง จากการศึกษาพบว่าในการบัญญัติกฎหมายสำหรับอาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมทางเทคโนโลยีนั้นมีแนวทางในการบัญญัติกฎหมายอยู่สองแนวทาง[27] แนวทางแรกคือการบัญญัติ

---

[26] เพิ่งอ้าง 238.

[27] คณาธิป ทองรวีวงศ์, *กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1* (สำนักพิมพ์นิติธรรม 2563) 74.

กฎหมายเพื่อใช้บังคับโดยเฉพาะกล่าวคือเป็นการกำหนดฐานความผิดเฉพาะเกี่ยวกับอาชญากรรมคอมพิวเตอร์ เช่น ประเทศสหรัฐอเมริกาที่ได้มีการกำหนดกฎหมายเฉพาะในระดับรัฐบาลกลาง (CFAA) ต่อมาในส่วนของแนวทางที่สองคือการนำฐานความผิดที่มีอยู่แล้วในกฎหมายเดิมอันมิได้บัญญัติมาเพื่อใช้กับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มาปรับใช้กับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น ประเทศจีนก่อนการแก้ไขกฎหมายอาญาในปี ค.ศ.1997 ที่ได้มีการนำฐานความผิดทางอาญามาปรับใช้กับฐานความผิดเกี่ยวกับคอมพิวเตอร์

สำหรับในประเทศไทยก่อนที่จะมีการบัญญัติ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นั้นได้มีการนำฐานความผิดในประมวลกฎหมายอาญามาปรับใช้ในฐานความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์โดยอาศัยการพิจารณาจากเจตนาในการกระทำความผิดหรือพฤติการอื่นๆประกอบการพิจารณาซึ่งการนำแนวทางนี้มาปรับใช้นั้นก่อให้เกิดข้อจำกัดในการบังคับใช้กฎหมายอยู่หลายประการโดยเฉพาะอย่างยิ่งในเรื่องข้อจำกัดขององค์ประกอบความผิดที่กำหนดไว้ไม่ครอบคลุมถึงการกระทำความผิดที่เกี่ยวกับการก่ออาชญากรรมทางคอมพิวเตอร์ อีกทั้งฐานความผิดในกฎหมายเดิมนั้นไม่สามารถนำมาปรับใช้กับฐานความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ได้ เช่น โจทย์ฟ้องจำเลยฐานลักทรัพย์จากการขโมยข้อมูลคอมพิวเตอร์ แต่ศาลตัดสินว่าข้อมูลคอมพิวเตอร์ไม่ถือเป็นทรัพย์ (คำพิพากษาฎีกาที่ 5161/2547[28]) และจากสภาพปัญหาการก่ออาชญากรรมคอมพิวเตอร์ที่มีการพัฒนารูปแบบอยู่ตลอดเวลาและได้รับความนิยมจากอาชญากรอย่างแพร่หลายนี้เองทำให้ในหลายๆประเทศพัฒนากฎหมายไปสู่การกำหนดให้อาชญากรรมคอมพิวเตอร์เป็นความผิดเฉพาะ สำหรับในประเทศไทยนั้นได้เลือกที่จะกำหนดการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ให้เป็นความผิดเฉพาะโดยกำหนดไว้ใน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ซึ่งอ้างอิงฐานความผิดมาจากอนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรป และกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศสหรัฐอเมริกา แคนาดา อังกฤษ เป็นต้น

2.3 ความหมายและพัฒนาการของอาชญากรรมคอมพิวเตอร์

2.3.1 ความหมายของอาชญากรรมคอมพิวเตอร์

อาชญากรรมทางคอมพิวเตอร์ (Computer Crime) หมายถึงการกระทำผิดทางอาญาในระบบคอมพิวเตอร์ หรือการใช้คอมพิวเตอร์เพื่อกระทำผิดทางอาญา เช่น ทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลต่างๆ เป็นต้น ซึ่งระบบคอมพิวเตอร์ในที่นี้หมายรวมถึงระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ที่เชื่อมกับระบบดังกล่าวด้วย[29] ซึ่งอาชญากรที่ก่ออาชญากรรมในระบบเครือข่ายคอมพิวเตอร์ เช่น อินเทอร์เน็ต อาจเรียกการ

---

[28] คำพิพากษาฎีกาที่ 5161/2547 <https://deka.in.th/view-411647.html> สืบค้นเมื่อ 8 มีนาคม พ.ศ.2566.

[29] PaPer-BOY, ‘ความหมาย และ อาชญากรคอมพิวเตอร์’ (Gotoknow, 6 กันยายน 2556) <https://www.goto-know.org/posts/372559> สืบค้นเมื่อ 29 ธันวาคม 2565.

ก่ออาชญากรรมเช่นนี้ได้อีกอย่างหนึ่งว่าเป็น อาชญากรรมไซเบอร์ (Cybercrime) โดยอาชญากรที่ก่ออาชญากรรมประเภทนี้มักถูกเรียกว่า แครกเกอร์[30]โดยคำว่า อาชญากรรมทางคอมพิวเตอร์ หรือ Computer Crime ในภาษาอังกฤษมีคำเรียกได้หลายอย่างซึ่งยังคงมีความหมายไปในทำนองเดียวกัน เช่น Computer-Related Crime, Computer Fraud, Cyber Crime, E-Crime, Information Technology Crime, Online Crime, High-Tech Crime, Computer Misuse และ Computer Abuse เป็นต้น[31]โดยคำต่าง ๆเหล่านี้ล้วนแล้วแต่มีความหมายที่สื่อไปในทำนองเดียวกันและสามารถที่จะใช้แทนการได้ (Interchangeably)[32]

ส่วนเรื่องความหมายของคำว่า“อาชญากรรมทางคอมพิวเตอร์”ว่าหมายความถึงพฤติกรรมการกระทำเช่นไรบ้างนั้น อาจกล่าวได้ว่าในปัจจุบันนี้นั้นยังไม่มีคำนิยามที่เป็นสากลที่สามารถถือเอาเป็นมาตรฐานในการกำหนดและตัดสินว่าการกระทำใดคืออาชญากรรมทางคอมพิวเตอร์และมีหลักเกณฑ์ในการกำหนดถึงการกระทำเช่นไรจึงจะถือว่าเป็นการก่ออาชญาทางคอมพิวเตอร์ กระทั้งในปัจจุบันก็ยังไม่มีการนิยามการกระทำดังกล่าวในระดับสากลที่ได้รับการยอมรับโดยทั่วกัน ด้วยเหตุนี้เองจึงเป็นที่ถกเถียงกันในระหว่างนักวิชาและผู้เชี่ยวชาญในวงการเกี่ยวกับเรื่องความหมายของ“อาชญากรรมคอมพิวเตอร์”ซึ่งก็ยังไม่อาจหาข้อยุติได้[33]

อนึ่ง ตามอนุสัญญาว่าด้วยอาชญกรรมไซเบอร์ (Convention on Cybercrime) [34]ของคณะมนตรียุโรปเองก็มิได้มีการบัญญัติถึงนิยามของอาชญากรรมคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ไว้ซึ่งในส่วนนี้นั้นทางผู้เขียนคาดว่าคงเป็นความมุ่งหมายที่จะให้แต่ละประเทศที่ร่วมลงนามกำหนดคำนิยาม หรือขอบเขตของการกำหนดฐานความผิดกันเองโดยอาศัยอนุสัญญาดังกล่าวเป็นแนวทางหรือกรอบกว้าง ๆ เท่านั้น ซึ่งเมื่อพิจารณาจากเจตนารมณ์ของการที่คณะมนตรียุโรปไม่ได้กำหนดลักษณะของการก่ออาชญากรรมทางคอมพิวเตอร์ไว้เป็นบรรทัดฐานคงเป็นเพราะในฐานความผิดทางอาญาของแต่ละประเทศนั้นมีการกำหนดความผิดหรือการกระทำที่เป็นความผิดที่แตกต่างกันไป ด้วยเหตุนี้เองจึงไม่อาจที่จะกำหนดว่าการกระทำใดบ้างที่เป็นการกระทำความผิดทางคอมพิวเตอร์ และหากพิจารณาจากกฎหมายของแต่ละประเทศแล้ว จะพบว่าลักษณะของการกระทำที่บัญญัติให้เป็นความผิดและการแบ่งหมวดหมู่ของความผิด กระทั่งชื่อกฎหมายเองก็มีความหมายที่มีนัยยะสำคัญในการสื่อให้เป็นถึงความหมายของอาชญากรรมประเภทนี้ในลักษณะแคบ

---

[30] แครกเกอร์(Cracker) หมายถึง ผู้ที่มีความรู้และทักษะทางคอมพิวเตอร์เป็นอย่างดีจนสามารถเข้าสู่ระบบได้เพื่อเข้าไปทำลายหรือลบแฟ้มข้อมูล หรือทำให้เครื่องคอมพิวเตอร์เสียหาย รวมทั้งการทำลายระบบปฏิบัติการของเครื่องคอมพิวเตอร์.

[31] องอาจ เทียนหิรัญ, ‘อาชญากรรมคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญา สำหรับการกระทำต่อคอมพิวเตอร์’ (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2546) 11.

[32] ‘Commission of The European Communities’ (European Union) <http://europa.eu.int/SPO/eif/-InternetPoliciesite/Crime/CrimeCommEN.html> สืบค้นเมื่อ 29 ธันวาคม 2565.

[33] องอาจ เทียนหิรัญ (เชิงอรรถ 31) 12.

[34] ‘Convention on Cybercrime (ETS No. 185)’ (The Council of Europe) <https://rm.coe.int/1680081561> สืบค้นเมื่อ 30 ธันวาคม 2565.

กว้างแตกต่างกันไปตามพื้นฐานความผิดอาญาของแต่ละประเทศ เช่น กฎหมายของประเทศมาเลเซียใช้ชื่อว่า "Computer Crime Act" ส่วนประเทศอังกฤษและสิงคโปร์ใช้คำกว้าง ๆ ว่า "กฎหมายที่ว่าด้วยการใช้คอมพิวเตอร์ไปในทางที่มิชอบ " (Computer Misuse Act)หรือในประเทศอินเดียก็เลือกที่จะใช้คำว่า " เทคโนโลยีสารสนเทศ" มาเป็นชื่อกฎหมาย ก็คือ"Information Technology Crime Act" เป็นต้น[35] ซึ่งในส่วนของประเทศไทยนั้นในปัจจุบันก็ได้มีการใช้คำว่า "คอมพิวเตอร์" มาใช้เป็นชื่อในพระราชบัญญัติโดยให้ชื่อว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 (Computer Crimes Act.) ซึ่งถือได้ว่าเป็นบทบัญญัติที่ใช้ในการควบคุมอาชญากรรมทางคอมพิวเตอร์ของประเทศไทยในปัจจุบัน

อย่างไรก็ดีเมื่อพิจารณาจากความเข้าใจของผู้คนโดยทั่วไปในสังคมแล้วนั้นผู้คนส่วนมากมักจะมีความเข้าใจผิดเกี่ยวกับอาชญกรรมทางคอมพิวเตอร์ว่าต้องเป็นการกระทำที่เกิดจากการใช้คอมพิวเตอร์ในการกระทำความผิด แต่ในหลักความจริงคือไม่จำเป็นที่ว่าในการก่ออาชญากรรมทุกกรณีที่ใช้คอมพิวเตอร์แล้วจะต้องเป็นอาชญากรรมคอมพิวเตอร์เสมอไป เพราะในการก่ออาชญากรรมคอมพิวเตอร์นั้นจะต้องเป็นการกระทำต่อระบบคอมพิวเตอร์โดยตรงหรือโดยอ้อมเพื่อผลประโยชน์อย่างใดอย่างหนึ่งในการเข้าถึงคอมพิวเตอร์ โดยประการสำคัญคือผู้ที่ก่ออาชญากรรมประเภทนี้นั้นจะต้องเป็นผู้ที่มีความรู้ทางด้านเทคโนโลยีและการกระทำนั้นต้องเป็นความผิดอาญา ซึ่งต่างจากการก่ออาชญากรรมโดยใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำซึ่งผู้กระทำไม่จำเป็นที่จะต้องมีองค์ความรู้ในเทคโนโลยีมากเท่าไรนัก อีกทั้งในการก่ออาชญากรรมอาจจะเป็นการกระทำความผิดในทางแพ่งหรือทางอาญาก็ได้ เช่น การหลอกลวงผ่านทางแชท

ซึ่งจากการศึกษานั้นพบว่าคำว่าอาชญากรรมคอมพิวเตอร์ได้ถูกนิยามเป็นครั้งแรกในคู่มือกระบวนการยุติธรรมทางอาญา (Criminal Justice Resource Manual 1979) ให้ความหมายอย่างกว้างๆ ว่าเป็นการกระทำใดอันละเมิดต่อกฎหมายที่ใช้ความรู้ด้านเทคโนโลยีคอมพิวเตอร์เป็นปัจจัยสำคัญในการกกระทำความผิดและเพื่อให้การฟ้องร้องดำเนินคดีบรรลุผล[36]

สำหรับในส่วนของการให้นิยามความหมายของอาชญากรรมคอมพิวเตอร์ในประเทศไทยนั้นได้มีการกำหนดให้อาชญากรรมคอมพิวเตอร์มีความหมายถึงการกระทำความผิดตามกฎหมายใดๆซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือในการก่ออาชญากรรม อันก่อให้เกิดความเสียหายต่อผู้เสียหายและผู้กระทำความผิดนั้นได้รับผลประโยชน์อย่างใดอย่างหนึ่งเป็นการตอบแทน อันเป็นเหตุให้การสืบสวนสอบสวนของเจ้าหน้าที่นั้นต้องกระทำไปโดยใช้ความรู้ทางเทคนิคเฉพาะด้านและใช้เทคโนโลยีในการติดตามจับกุมอาชญากร[37]

---

[35] สาวตรี สุขศรี, ‘อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญาวิทยา’ (2560) 2 วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 415, 419.

[36] พิชยุตม์ คูณทอง, ‘การดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ต:ศึกษาเฉพาะกรณีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย 2550) 40.

[37] เอก ศรีเชลียง, ‘อาชญากรรมอิเล็กทรอนิกส์:ศึกษาความสอดคล้องของข่าวอาชญากรรมทางคอมพิวเตอร์ที่ปรากฏในเว็บไซต์ข่าวบีบีซีกับ (ร่าง) พ.ร.บ. ว่าด้วยอาชญากรรมทางคอมพิวเตอร์ไทย’ (สารนิพนธ์ รัฐประศาสนศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย 2545) 28-30.

2.3.2 พัฒนาการของอาชญากรรมทางคอมพิวเตอร์

ในสังคมยุคปัจจุบันนี้นั้นคงไม่อาจปฏิเสธได้ว่า “อาชญากรรมคอมพิวเตอร์” เรื่อยมาจนถึง “อาชญกรรมไซเบอร์ หรืออาชญากรรมทางอินเทอร์เน็ต” เหล่านี้ล้วนแล้วแต่เป็นผลพวงด้านลบที่เกิดขึ้นมาจากพัฒนาการและขยายตัวมาพร้อมๆกับวิวัฒนาการทางเทคโนโลยี โดยเฉพาะอย่างยิ่งกับนวัตกรรมใหม่อย่างคอมพิวเตอร์ และการเชื่อมต่อระหว่างกันจนเกิดเป็นเครือข่ายขนาดเล็ก และใหญ่ตามมากระทั้งในช่วงปลายทศวรรษที่ 60 (ปีค.ศ. 1969) อินเทอร์เน็ตได้ถือกำเนิดขึ้นในขณะที่ด้านหนึ่งถูกใช้เป็น”เครื่องมือ”ในการกระทำความผิด อีกด้านหนึ่งก็ถูกเล็งให้กลายเป็น“เป้าหมายแห่งการกระทำความผิด”ในฐานะที่เป็นอุปกรณ์ หรือช่องทางสำคัญในการเก็บรักษา และ/หรือ รับ-ส่ง ข้อมูลข่าวสาร ทรัพย์สินที่ปัจจุบัน และดูเหมือนว่า จะมีค่ามากกว่าทรัพย์ประเภทที่มีรูปร่างบางอย่างเสียอีก[38]

ด้วยเหตุผลในเรื่องการพัฒนาเทคโนโลยีที่มีความเปลี่ยนแปลงไปตามยุคสมัยนี้เองทำให้ในปัจจุบันนี้นั้นมีเทคโนโลยีต่างๆเกิดขึ้นอย่างมากมายโดยเฉพาะเทคโนโลยีทางด้านคอมพิวเตอร์และการเชื่อมต่ออินเทอเน็ตที่ในยุคนี้นั้นมีการพัฒนาขึ้นมาเพื่อเพิ่มความสะดวกสบายในการดำเนินชีวิตในปัจจุบัน แต่อย่างไรก็ตามแม้ว่าเทคโนโลยีในปัจจุบันนั้นจะมีการพัฒนาให้ทันสมัยมากเท่าไรก็ตามแต่เหรียญก็ย่อมมีสองด้านเสมอทุกอย่างล้วนมีข้อเสียจุดด้อยเสมอ กล่าวคือนอกจากอำนวยความสะดวกในการดำเนินชีวิตแล้วยังถูกใช้เป็นเครื่องมือในการก่ออาชญากรรมคอมพิวเตอร์ของเหล่าอาชญากรอีกด้วย

โดยเมื่อพิจารณาจากบริบทในการก่ออาชญากรรมตั้งแต่อดีจนถึงปัจจุบันนั้นเป็นที่ทราบกันดีว่าในอดีตนั้นคำว่า“อาชญากรรม”มีความหมายถึงการกระทำที่เป็นการละเมิดต่อเนื้อตัวร่างกายหรือเป็นการละเมิดต่อบทบัญญัติของกฎหมาย แต่ไม่ว่าอย่างไรก็ตามด้วยผลพวงจากการที่มนุษย์นั้นได้มีการพัฒนาเทคโนโลยีจนมีความก้าวหน้าเป็นอย่างมากในปัจจุบันทำให้บริบทของการก่ออาชญากรรมนั้นเปลี่ยนแปลงไปตามทิศทางของการพัฒนาเทคโนโลยีและจากคำกล่าวที่ได้กล่าวมาแล้วในข้างต้นว่าเทคโนโลยีในปัจจุบันนั้นแม้จะมีการพัฒนาให้ทันสมัยมากเท่าไรก็ตามแต่เหรียญก็ย่อมมีสองด้านเสมอ ซึ่งนับจากการที่คอมพิวเตอร์นั้นได้ถือกำเนิดขึ้นไม่นานก็มีสิ่งที่เปรียบเสมือนเงาของมนุษย์ตามมานั้นก็คือ อาชญากรรมคอมพิวเตอร์ (Computer crime) ซึ่งถือกำเนิดขึ้นมาจากการที่เครื่องคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ถูกทำลาย โดยเมื่อสังคมเริ่มเห็นคุณค่าว่าสิ่งเหล่านี้มีมูลค่ามาก และส่งผลกระทบสร้างความเสียหายใหญ่หลวงต่อคนจำนวนมาก สังคมจึงค่อยๆ ที่จะเริ่มพัฒนาการกระทำอันละเมิดต่อคอมพิวเตอร์ให้เป็นความผิดและพัฒนาจนเป็นกฎหมายในเวลาต่อมา

จากการศึกษาพบว่าอาชญากรรมคอมพิวเตอร์นั้นเกิดขึ้นครั้งแรกในเดือนกุมภาพันธ์ ค.ศ. 1969[39] โดยในวันนั้นได้เกิดการจลาจลของกลุ่มนักเรียนครั้งใหญ่ที่สุดในแคนาดา โดยเหตุการณ์เริ่มต้นจากการที่นักเรียนได้ทำการประท้วงต่อศาสตราจารย์ท่านหนึ่งที่ถูกกล่าวหาว่าทำการเหยียดเชื้อชาติและเมื่อตำรวจเข้า

---

[38] สาวตรี สุขศรี, ‘ประวัติศาสตร์ อาชญากรรมคอมพิวเตอร์’ (BioLawCom, 7 พฤษภาคม 2552) <http://www.biolawcom.de/article/118> สืบค้นเมื่อ 29 ธันวาคม 2565.

[39] Kabay M. E., *A Brief History of Computer Crime: An Introduction for Students* (School of Graduate Studies Norwich University 2008) 5.

มาถึงก็พบว่ากลุ่มนักเรียนที่ทำการก่อจลาจลนั้นได้ทำการยึดอาคารและเผาทำลายทรัพย์สินรวมไปถึงคอมพิวเตอร์ที่ใช้ในการเก็บข้อมูลของมหาวิทยลัย ซึ่งในท้ายที่สุดเมื่อไฟนั้นได้ดับลงก็พบว่ามีคอมพิวเตอร์ที่ใช้ในการเก็บข้อมูลและทรัพย์สินของมหาวิทยาลัยถูกทำลายเป็นจำนวนมาก จากการประเมินความเสียหายพบว่ามีทรัพย์สินเสียหายเป็นมูลค่าโดยรวมกว่า 2 ล้านดอลลาร์ และ ผลจากการที่เจ้าหน้าที่ตำรวจได้เข้าไประงับเหตุดังกล่าวพบว่ามีนักเรียนกว่า 97 คนถูกจับกุมจากเหตุการณ์การก่อจลาจลดังกล่าว[40]

อนึ่งจากการศึกษาบทความเกี่ยวกับประวัติศาสตร์คอมพิวเตอร์ของ M. E. Kabay[41]พบว่าอาชญากรรมคอมพิวเตอร์ในยุคแรก คือการทำลายคอมพิวเตอร์ทางกายภาพ เช่น การทุบ ทำลาย หรือการกระทำทางกายภาพต่อตัวคอมพิวเตอร์ ซึ่งอาจมีสาเหตุมาจากการเกิดอุบัติเหตุบ้าง หรืออาจเกิดจากการก่อวินาศกรรม เช่นการการเผาทำลาย หรือการจงใจทำให้ใช้งานไม่ได้ และการจารกรรมอุตสาหกรรม ซึ่งต่อมาในช่วงปี ค.ศ. 1960-1970 ได้เกิดการขโมยข้อมูล เปลี่ยนแปลงข้อมูล บุคคล ธุรกิจ และธนาคาร เช่น การปลอมบัตรเครดิต ปลอมบัญชีธนาคาร ซึ่งอาจถือได้ว่าเป็นยุคแรกของ Identity Theft ซึ่งนำไปสู่การกำเนิดอาชีพใหม่อย่าง Dumpster Diver (คนคุ้ยขยะ) ที่ทำหน้าที่ขุดคุ้ยขยะหาข้อมูลที่สามารถนำมาใช้ประโยชน์ในการก่ออาชญากรรมทางคอมพิวเตอร์ได้ อาทิ ใบเสร็จ สำเนาบัตรเครดิต ข้อมูลลูกค้า ข้อมูลธุรกิจ เพื่อนำไปขายต่อให้กับอาชญากรผู้ซึ่งต้องการนำข้อมูลเหล่านั้นมาปลอมแปลงเพื่อใช้งานในการก่ออาชญากรรม โดยอาชีพคนคุ้ยขยะนั้นถือได้ว่าเป็นอาชีพที่สร้างรายได้เป็นอย่างมากในอเมริกาในช่วยยุคดังกล่าว โดยในยุคนั้นมีอาชญากรวัยรุ่นชื่อดังอย่าง Jerry Neal Schneider เป็นผู้นำในการสร้างความเสียหายต่อธุรกิจหลายแห่งจนกระทั่งเริ่มมีการเข้าถึงข้อมูลคอมพิวเตอร์ผ่านเครือข่ายโทรคมนาคมในยุคปี ค.ศ.1980 ซึ่งในยุคนี้นั้นยังไม่มีระบบโครงข่ายอินเทอร์เน็ตเหมือนดังเช่นปัจจุบัน และต่อมาในยุคปี ค.ศ.1990 การทำลายข้อมูลคอมพิวเตอร์จากการส่งไวรัสเข้ามาทางโครงข่ายอินเทอร์เน็ตที่เชื่อออยู่กับคอมพิวเตอร์ ได้ก่อตัวขึ้นพร้อมกับการมาของเทคโนโลยีโครงข่ายอินเทอร์เน็ตที่ได้ถือกำเนิดขึ้นและถูกใช้อย่างแพร่หลายในกลุ่มบุคคลโดยทั่วไป ซึ่งในส่วนนี้เองทำให้จากอาชญากรรมคอมพิวเตอร์ธรรรมดาเกิดการพัฒนารูปแบบวิธีการก่ออาชญากรรมจนในท้ายที่สุดก็กลายเป็น อาชญากรรมไซเบอร์ (Cybercrime) ส่งผลทำให้การทำลายอุปกรณ์คอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ ได้ถูกเปลี่ยนแปลงวิธีการไปตามพัฒนาการทางด้านเทคโนโลยีอันนำไปสู่ช่องทางในการทำความเสียหายผ่านระบบโครงข่ายทางอินเทอร์เน็ต ซึ่งปัจจุบันอาชญากรรมไซเบอร์ได้มีการเติบโตขึ้นอย่างมากเมื่อเทียบกับการก่ออาชญากรรมทางคอมพิวเตอร์อดีต

2.3.3 รูปแบบของการก่ออาชญากรรมทางคอมพิวเตอร์

เทคโนโลยีในสังคมโลกยุคปัจจุบันนี้นั้นแม้จะช่วยอำนวยความสะดวกได้มากเพียงใดก็ตาม สิ่งที่ต้องยอมรับความจริงก็คือ เทคโนโลยีทุกอย่างมีจุดเด่นข้อด้อยของตนทั้งสิ้นทั้งที่มาจากตัวเทคโนโลยีเองและมาจากปัญหาอื่นๆแต่ไม่ว่าอย่างไรก็ตามแม้จะมีการวางวิธีการหรือระบบในป้องกันที่ดีเพียงใดก็ยังต้องพบกับ

---

[40] Concordia University, ‘who we are: History’ (Concordia University, 2008). <http://www.concordia.ca/about/who-weare/ourhistory/sgw.php> สืบค้นเมื่อ 30 ธันวาคม 2565.

[41] Kabay M. E. (เชิงอรรถ 39) 5-6.

ปัญหาการก่ออาชญากรรมทางคอมพิวเตอร์ที่มีให้พบได้อยู่เรื่อย ๆ โดยในปัจจุบันนี้นั้นอาชญากรรมคอมพิวเตอร์ได้มีเกิดขึ้นหลากหลายรูปแบบซึ่งมีทั้งที่มีผลกระทบต่อชีวิต ระบบรักษาความปลอดภัย และระบบเศรษฐกิจ[42]

โดยการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์นั้นสามารถแยกประเภทออกได้เป็น 3 ส่วน ส่วนแรกคือการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ส่วนที่สองคือการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด และส่วนที่สามคือการใช้คอมพิวเตอร์หาประโยชน์โดยไม่ได้รับอนุญาต และจากสามส่วนดังที่ได้กล่าวมาในข้างต้นนี้นั้นสามารถแยกออกมาเป็นประเภทของอาชญากรรมคอมพิวเตอร์ที่สำคัญได้เป็น 9 ประเภท ดังนี้[43]

2.3.3.1 อาชญากรรมที่เป็นการโจรกรรมข้อมูล

หมายถึง การจารกรรมข้อมูลซึ่งรวมไปถึงการจารกรรมข้อมูลจาก internet service provider หรือผู้ให้บริการอินเทอร์เน็ต หรือผู้ที่มีเว็บไซต์ในอินเทอร์เน็ต ซึ่งรวมไปถึงการขโมยข้อมูลเพื่อที่จะใช้ประโยชน์ในการลักลอบใช้บริการ เช่น การขโมยข้อมูลเกี่ยวกับศูนย์โทรศัพท์เพื่อที่จะสามารถควบคุมการใช้โทรศัพท์ของหน่วยงานใดหน่วยงานหนึ่งโดยเอาข้อมูลนั้นมาเป็นประโยชน์คือเป็นการแอบใช้บริการฟรี หรือการขโมยข้อมูลเพื่อนำไปใช้ในการประกอบอาชญากรรมอื่นเพิ่มเติม

2.3.3.2 อาชญากรรมที่เป็นการปล้นข้อมูลหรือการปลอมแปลงข้อมูล

หมายถึง การกระทำความที่เป็นการการละเมิดลิขสิทธิ์ การปลอมแปลง ไม่ว่าจะเป็นการปลอมแปลงเช็ค การปลอมแปลงรูป เสียง หรือการปลอมแปลงสื่อทางคอมพิวเตอร์ที่เรียกว่า มัลติมีเดีย หรือรวมทั้งการปลอมแปลงโปรแกรมคอมพิวเตอร์ โดยคดีที่เกิดขึ้นจากอาชญากรรมประเภทนี้ ได้แก่ MPAA v. Reimerdes: Cracking DVD with DeCss

2.3.3.3 อาชญากรรมที่เป็นการโจมตีทางระบบหรือการก่อการร้าย

หมายถึง การกระทำเพื่อรบกวนผู้ใช้บริการซึ่งไม่เพียงแต่เฉพาะผู้มีจิตใจชั่วร้ายเป็นอาชญากรเท่านั้นที่ทำสิ่งเหล่านี้แต่ยังมีพวกชอบท้าทายทางเทคนิค อยากรู้อยากเห็นว่าสามารถเข้าไปแทรกแซงระบบข้อมูลคอมพิวเตอร์ของผู้อื่นได้มากน้อยเพียงใด นอกจากนั้นยังรวมไปถึงผู้ก่อการร้าย (terrorist) ที่ใช้อินเทอร์เน็ตในการเผยแพร่ข้อมูลข่มขู่ผู้อื่น ที่น่ากลัวที่สุดเกี่ยวกับการก่อการร้ายโดยใช้เครื่องมือสื่อสารผ่านคอมพิวเตอร์คือการเข้าไปแทรกแซงทำลายระบบเครือข่ายของสาธารณูปโภค ซึ่งอย่างที่รู้กันดีอยู่แล้วว่าในปัจจุบันนี้สาธารณูปโภคไม่ว่าจะเรื่องการจ่ายน้ำ จ่ายไฟ หรือการจราจรส่วนใหญ่จะควบคุมโดยระบบคอมพิวเตอร์ ซึ่งผู้ก่อการร้ายพวกนี้สามารถเข้าไปแทรกแซงและทำให้ระบบเหล่านี้ให้ทำงานไม่ได้

---

[42] เฟื่องฟ้า เป็นศิริ, *อาชญากรรมคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง* (สำนักพิมพ์วิญญูชน 2550) 11-13.

[43] อุนิษา เลิศโตมรสกุล และอัณณพ ชูบำรุง, *อาชญากรรมและอาชญาวิทยา* (พิมพ์ครั้งที่ 2, สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย 2561) 161-165.

2.3.3.4 อาชญากรรมที่เป็นฉ้อโกงผ่านทางเครือข่ายคอมพิวเตอร์

หมายถึง การค้าขายหรือชวนลงทุนโดยหลอกลวงผ่านทางเครือข่ายคอมพิวเตอร์ การให้บริการทางคอมพิวเตอร์มีอยู่มากและสามารถทำเงินได้เป็นอย่างดี แต่มีพวกหลอกลวงประกาศโฆษณาโดยไม่ได้ให้บริการจริง หรือชักชวนให้เข้าร่วมลงทุนแต่ไม่ได้มีกิจการเหล่านั้นจริงๆ ซึ่งบางครั้งจะเห็นว่าโฆษณาหลายอย่างดีเกินไปกว่าที่จะเป็นของจริง แต่ก็มีผู้ถูกหลอกหลายราย

2.3.3.5 อาชญากรรมที่เป็นแทรกแซงการส่งข้อมูลผ่านทางเครือข่ายคอมพิวเตอร์

หมายถึง การเข้าแทรกแซงข้อมูลและนำเอาข้อมูลเหล่านั้นมาใช้ประโยชน์ต่อตนโดยมิชอบ เช่น การที่สามารถผ่านอินเทอร์เน็ตเข้าไปแล้วเข้าไปเจาะล้วงเอาความลับเกี่ยวกับรหัสหมายเลขของบัตรเครดิตเพื่อนำมาเป็นประโยชน์ในการก่ออาชญากรรมต่อไปหรือแม้กระทั่งการล้วงความลับทางการค้าซึ่งสามารถทำได้โดยผ่านทางอินเทอร์เน็ตซึ่งอาจเป็นลักษณะของการดักฟังข้อมูลเพื่อที่จะนำมาเป็นประโยชน์กับกิจการของตนเอง

2.3.3.6 อาชญากรรมที่เป็นโจรกรรมผ่านระบบธุรกรรมอิเล็กทรอนนิกส์

หมายถึง การเข้าถึงเครือข่ายคอมพิวเตอร์ของธนาคารโดยมิชอบแล้วใช้โปรแกรมหรือคำสั่งบางอย่างทำการเปลี่ยนแปลงหรือดัดแปลงข้อมูล เพื่อหลอกให้ระบบคอมพิวเตอร์ของธนาคารโอนทรัพย์สินหรือเงินจากบัญชีของผู้เสียหายเข้าไปยังบัญชีที่อาชญากรเตรียมไว้เพื่อใช้รับการโอน ซึ่งการโอนทรัพย์สินดังกล่าวนั้นเกิดขึ้นโดยมิชอบอันเป็นผลจากการดัดแปลงของระบบธนาคารโดยปราศจากสิทธิในการเข้าถึงและเปลี่ยนแปลง

2.3.3.7 อาชญากรรมที่เป็นการใช้เทคโนโลยีเพื่ออำนวยความสะดวก

หมายถึง อาชญากรรมที่เกิดจากการที่อาชญากรเทคโนโลยีทางคอมพิวเตอร์มาใช้เพื่อเพิ่มความสามารถและอำนวยความสะดวกในการกระทำความผิดของตน เช่น อาชญากรทั่วไปที่กระทำความผิดเกี่ยวกับการขนหรือค้ายาเสพติด โดยใช้การสื่อสารผ่านทางคอมพิวเตอร์เพื่อติดต่อกับเครือข่ายอาชญากรรมของตนเพื่อเพิ่มประสิทธิภาพในการประกอบอาชญากรรม ซึ่งรวมไปถึงการใช้คอมพิวเตอร์เพื่อปกปิดและกลบเกลื่อนการกระทำของตนไม่ให้ผู้อื่นล่วงรู้ได้ด้วยการใช้เทคโนโลยีที่เรียกว่า encryption หรือการสื่อสารโดยการเข้ารหัสการสื่อสารโดยการตั้งรหัสขึ้นมาเป็นคำเฉพาะในการติดต่อระหว่างหมู่อาชญากรด้วยกันซึ่งผู้อื่นไม่สามารถเข้าใจได้ด้วยวิธีการปกติ

2.3.3.8 อาชญากรรมที่เป็นการเผยแพร่ข้อมูลที่ไม่เหมาะสม

หมายถึง การใช้คอมพิวเตอร์และเครือข่ายทางอิเทอร์เน็ตซึ่งเป็นเครือข่ายที่สามารถเข้าถึงได้จากทั่วโลกทำการเผยแพร่ภาพที่มาเหมาะสมรวมถึงข้อมูลที่ไม่สมควร ซึ่งการจะเป็นภาพไม่เหมาะสมนั้นหรือข้อมูลไม่สมควรนั้นขึ้นอยู่กับคุณค่าทางวัฒนธรรมของแต่ละสังคมว่าจะรับได้มากน้อยแค่ไหน รวมทั้งการใช้คอมพิวเตอร์เพื่อเผยแพร่ข้อมูลที่ไม่สมควรและเป็นอันตรายต่อสังคม เช่น วิธีการในการก่ออาชญากรรมหรือสูตรในการผลิตระเบิด

2.3.3.9 อาชญกรรมที่เป็นการฟอกเงินผ่านระบบอิเล็กทรอนิกส์

หมายถึง การฟอกเงินทางอิเล็กทรอนิกส์ ซึ่งใช้อุปกรณ์ทางคอมพิวเตอร์และการสื่อสารเป็นเครื่องมือทำให้สามารถกลบเกลื่อนอำพรางตัวตนของผู้กระทำความผิดได้ง่ายขึ้นอันเป็นผลพวงมาจากการพัฒนาเทคโนโลยีที่มีความทันสมัยและสะดวกสะบายมากขึ้น เพราะในปัจจุบันนั้นไม่ได้มีเพียงแค่ธนาคารหลักเท่านั้นที่สามารถรับโอนเงินได้เป็นจำนวนครั้งละมากๆผ่านทางระบบการเงินอิเล็กทรอนิกส์ เพราะธนาคารนอกระบบในปัจจุบันก็สามารถทำได้ทุกอย่างเหมือนที่ธนาคารหลักทำได้จึงทำให้ธนาคารนอกระบบเป็นตัวกลางหลักในการฝากและโอนย้ายเงินที่ผิดกฎหมายได้

2.3.4 ลักษณะและวิธีการของการก่ออาชญากรรมทางคอมพิวเตอร์

การก่ออาชญากรรมทางคอมพิวเตอร์ในปัจจุบันนี้นั้นได้มีการพัฒนารูปแบบการกระทำความผิดเพิ่มมากขึ้นจากในอดีต อันเป็นผลอันเนื่องมาจากพัฒนาเทคโนโลยีที่มีความทันสมัยและรวดเร็วมากขึ้นกว่าในอดีตโดยเฉพาะการประมวลผลของฮาร์ดแวร์และซอฟต์แวร์ที่มีการพัฒนาและอัพเกรดขึ้นมากกว่าในอดีต อีกทันในช่วงปีที่ผ่านมาทั้งโลกตกอยู่ในสถานะการการแพร่ระบาดของเชื้อไวรัส Covid-19 ที่ทำให้ผู้คนในโลกไม่ได้ออกจากบ้าน ดังนั้นทางเดียวที่จะติดต่อโลกภายนอกได้คือการใช้งานเครือข่ายอินเทอร์เน็ตด้วยเหตุนี้เองจึงทำให้เกิดอาชญากรรมทางคอมพิวเตอร์มากขึ้นเป็นพิเศษ

โดยการก่ออาชญากรรมทางคอมพิวเตอร์ในปัจจุบันนั้นสามารถแบ่งลักษณะการกระทำความผิดได้ทั้งหมด 4 ลักษณะ คือ การเจาะระบบรักษาความปลอดภัยทาง, การเจาะเข้าไปในระบบสื่อสารและการรักษาความปลอดภัยของซอฟต์แวร์ข้อมูลต่างๆ, การเจาะเข้าสู่ระบบรักษาความปลอดภัยของระบบปฏิบัติการ (Operating System), การเจาะผ่านระบบรักษาความปลอดภัยส่วนบุคคลผ่านทางระบบอินเทอร์เน็ตเป็นช่องทางในการกระทำความผิด

แต่ไม่ว่าอย่างไรก็ตามแม้ว่าจะมีการพัฒนาเทคโนโลยีที่มีความทันสมัยและรวดเร็วมากขึ้นกว่าในอดีตแต่วิธีการในการก่ออาชญากรรมนั้นไม่ได้เปลี่ยนไปมากนักในแง่วิธีการและพื้นฐานของการกระทำ ซึ่งจากการศึกษาพบว่าโดยทั่วไปแล้วนั้นวิธีการในการประกอบอาชญากรรมทางคอมพิวเตอร์นั้นมีวิธีการที่ถือได้ว่าเป็นพื้นฐานของการกระทำที่สำคัญอยู่ 5 วิธีดังนี้[44]

2.3.4.1 การแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์โดยมิชอบ (Data Diddling)

หมายถึง การเข้าถึงข้อมูลในระบบคอมพิวเตอร์เพื่อทำการแก้ไขหรือเปลี่ยนแปลงข้อมูลระหว่างที่ระบบนั้นกำลังทำการบันทึกโดยไม่มีสิทธิ โดยการเปลี่ยนแปลงดังกล่าวเป็นการกระทำเพื่อให้ตนนั้นได้รับประโยชน์ในทางใดทางหนึ่ง เช่น การที่พนักงานที่มีหน้าที่บันทึกเวลาในการทำงานของพนักงานภายในองค์กรทั้งหมด ทำการแก้ไขตัวเลขชั่วโมงการเข้างานของผู้อื่นมาเป็นของตน

2.3.4.2 การส่งมัลแวร์เพื่อล้วงเอาข้อมูลคอมพิวเตอร์(Trojan Horse Malware)

หมายถึง การส่งเมลหือข้อความที่ฝังมัลแวร์ที่เรียกว่าโทรจันมัลแวร์ไปยังผู้เสียหายและเมื่อผุ้เสียหายเปิดข้อความมัลแวร์นั้นจะถูกโหลดเข้าไปในคอมพิวเตอร์เพื่อทำการล้วงเอาข้อมูลของผู้เสียหาย

---

[44] พิชยุตม์ คูณทอง (เชิงอรรถ 36) 13-16.

เช่น รหัสผ่าน, User Name และข้อมูลส่วนตัวเกี่ยวกับการ Login เข้าสู่ระบบที่ถูกพิมพ์ผ่านคีย์บอร์ดโดยผู้ใช้งานโดยม้าโทรจันนั้นจะทำการบันทึกขอมูลการกรอกรหัสและรวมไปถึงกิจกรรมอื่นๆในคอมพิวเตอร์แล้วจ่งข้อมูลย้อนกลับไปให้อาชญากรที่ส่งมา ซึ่งส่วนใหญ่อาชญากรนั้นจะส่งโปรแกรมม้าโทรจันเข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าวแล้วนำไปใช้ในการเจาะระบบหรือเพื่อโจมตีคอมพิวเตอร์เซิร์ฟเวอร์ต่อไป

2.3.4.3 การแทรปดอร์ (Trap Doors)

หมายถึง การวางกับดักโดยการเขียนโปรแกรมหรือสร้างเว็บไซต์ที่มีลักษณะคล้ายคลึงกับโปรแกรมหรือหน้าเว็บต้นแบบ โดยมีจุดประสงค์เพื่อลวงให้ผู้เสียหายนั้นเกิดความเข้าใจผิดเกี่ยวกับการใช้โปรแกรมหรือเว็บไซต์ที่อาชญากรนั้นสร้างไว้ว่าเป็นของจริง เพื่อทำให้ทราบถึงไอดีและรหัสผ่าน ซึ่งเมื่อผู้เสียหายได้หลงกลและกรอกข้อมูลดังกล่าวนั้นไปแล้วระบบก็จะทำการเก็บข้อมูลเช่นว่านั้นไว้ในไฟล์ลับที่ซ้อนไว้ในโปรแกรมหรือเว็บไซต์ปลอมดังกล่าว

2.3.4.4 การหลอกถาม หรือ อิมเพอร์โซเนชั่น (Impersonation)

หมายถึง การที่อาชญากรนั้นแกล้งทำเป็นว่าตนนั้นเป็นผู้ที่มีหน้าที่ทำการแก้ไข หรือเปลี่ยนแปลงข้อมูล โดยส่วนมากนั้นมักจะอ้างว่าตนนั้นเป็นผู้ที่ได้รับอำนาจ หรือได้รับอนุญาตให้กระทำการอย่างใดอย่างหนึ่งซึ่งวิธีการหลอกถามข้อมูลนั้นก็จะขึ้นอยู่กับเรื่องที่อาชญากรนั้นจะใช้เพื่อหลอกถามข้อมูลเช่น การที่อาชญากรนั้นได้แอบขโมยบัตรกดเงินสดของผู้เสียหายแล้วแกล้งทำเป็นเจ้าหน้าที่ธนาคาร เพื่อโทรหาผู้เสียหายและแจ้งให้ทราบว่าได้มีการพยามใช้บัตรของผู้เสียหายโดย อาชญากรที่แอบอ้างนั้นจะอ้างว่าเพื่อป้องกันเงินในบัญชีของผู้สียหายไม่ให้สูญหายจะต้องทำการเปลี่ยนรหัสผ่านโดยอาชญากรนั้นจะหลอกถามรหัสผ่านเดิมของผู้เสียหาย และเมื่อผู้เสียหายหลงเชื่อให้รหัสไปอาชญากรก็จะทำการโอนเงินออกจากบัญชีของผู้เสียหายจนหมดผ่านระบบธุรกรรมออนไลน์

2.3.4.5 การปลอมแปลงข้อมูลคอมพิวเตอร์(Computer forgery)

หมายถึง การป้อนข้อมูล การแก้ไข หรือการลบข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งส่งผลให้ข้อมูลไม่น่าเชื่อถือมีความน่าเชื่อถือโดยมีเจตนาเพื่อให้ผู้เสียหายเข้าใจว่าข้อมูลนั้นเป็นข้อมูลจริงโดยไม่คำนึงว่าข้อมูลนั้นจะสามารถอ่านและเข้าใจได้โดยตรงหรือไม่ หรือ เป็นการกระทำโดยเจตนาใช้ข้อมูลคอมพิวเตอร์ซึ่งมาจากการปลอมแปลงข้อมูลที่คอมพิวเตอร์ เพื่อจุดประสงค์ในการหลอกลวงผู้เสียหายเพื่อให้ได้มาซึ่งทรัพย์สิน[45] เช่น การแอบอ้างเป็นบุคคล เจ้าหน้าที่ หน่วยงานของรัฐ และหน่วยงานอื่น ๆ ที่ถูกต้องตามกฎหมายเพื่อวัตถุประสงค์ในการฉ้อโกง[46]

---

[45] Anticybercrimep, ‘What is Computer-related Forgery?’ (Anticybercrimep) <https://anticybercrimeph.word-press.com/2015/09/04/computer-related-forgery/> สืบค้นเมื่อ 2 มกราคม 2566.

[46] ‘Cybercrime Module 2 Key Issues: Computer-related offences’ (United Nations Office on Drugs and Crime) <https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/computer-related-offences.html> สืบค้นเมื่อ 2 มกราคม 2566.

2.4 ความหมายและพัฒนาการของการก่ออาชญากรรมคอมพิวเตอร์ประเภทฟิชชิ่ง

2.4.1 ความหมายของการก่ออาชญากรรมคอมพิวเตอร์ประเภทฟิชชิ่ง

Phishing คือ หนึ่งในเทคนิคการโจมตีผ่านทางอินเทอร์เน็ต (Internet) หรือแม้แต่บริการออนไลน์ (On-line) รูปแบบอื่นที่นับวันจะเพิ่มขึ้นเรื่อย ๆ ก็คือการโจมตีในรูปแบบที่เรียกว่าฟิชชิ่ง (Phishing มา จากคำว่า Password + Harvesting + Fishing)[47] ซึ่งเป็นหนึ่งในภัยคุกคามประเภท Fraud ที่มีรูปแบบการหลอกลวงบนโลกออนไลน์ผ่านการแอบอ้างเป็นเว็บไซต์ต่าง ๆ ที่น่าเชื่อถือ เช่น เว็บไซต์ธนาคาร หรือบัญชีโซเชียลมีเดีย ซึ่งโดยทั่วไปอาชญากรไซเบอร์จะแอบอ้างว่าเป็นบริษัทที่มีชื่อเสียง เพื่อน หรือคนรู้จักในการปลอมข้อความและจะแนบลิงก์เพื่อไปยังเว็บไซต์ฟิชชิ่ง[48]ซึ่งใช้เทคนิคในการสร้างหน้าเว็บไซต์ปลอมที่มีหน้าการใช้งานและลักษณะที่ใกล้เคียงกับหน้าเว็บของผู้ให้บริการที่แท้จริง โดยที่ผู้เสียหายนั้นไม่อาจที่จะทราบได้เลยว่าระบบหรือหน้าเว็บไซต์ที่ตนนั้นกำลังใช้งานอยู่นั้นคือระบบหรือหน้าเว็บที่เป็นการทำปลอมขึ้นมาในลักษณะที่เหมือนกับหน้าเว็บจริงของผู้ให้บริการที่แท้จริง ซึ่งการก่ออาชญากรรมฟิชชิ่งนั้นมีลักษณะการกระทำความผิดที่เป็นไปตามความหมายของคำว่า “Fishing” ที่แปลว่า “ตกปลา” ดังนั้น Phishing จึงหมายถึง การปล่อยให้ปลามากินเหยื่อที่ล่อไว้ กล่าวคือ เมื่อผู้ใช้งานคลิกเข้าสู่ระบบ อาชญากรที่สร้างเว็บไซต์ปลอมเหล่านั้นก็จะล้วงข้อมูลส่วนบุคคลของผู้ใช้งานไปทันที ไม่ว่าจะเป็นหมายเลขบัตรเครดิต เลขบัตรประจำตัวประชาชน ตลอดจนรหัสผ่านในการเข้าสู่บัญชีต่าง ๆ การโจมตีรูปแบบนี้มักเป็นที่นิยมและพบได้บ่อยที่สุด โดยเฉพาะในยุคไซเบอร์ที่เราทุกคนต่างใช้อินเทอร์เน็ตกันเป็นกิจวัตรประจำวันเช่นนี้ ทำให้อาชญากรรมลักษณะนี้ทำได้ง่ายมากยิ่งขึ้น[49]โดยเฉพาะอย่างยิ่งในไทยสำหรับสถิติเมื่อปี 65 พบว่าอาชญากรรมไซเบอร์ที่เป็นที่น่ากังวลมาจนถึงปีนี้ในไทย คือ Phishing และ Botnet เฉพาะประเทศไทยนับเป็น 2% ของทราฟฟิคทั่วโลกซึ่งถือว่าเป็นเปอร์เซ็นที่สูงเป็นอย่างมาเมื่อเทียบกับประชากรในประเทศ[50]อีกทั้งจากผลการเก็บข้อมูลของระบบป้องกันฟิชชิ่ง (Anti-Phishing) ของแคสเปอร์สกี้บล็อกลิงก์ฟิชชิ่งพบว่าลิงก์กว่า 11,260,643 รายการในภูมิภาคเอเชียตะวันออกเฉียงใต้ ส่วนในไทยพบการโจมตีกว่า 1,287,283 รายการ[51]

2.4.2 ลักษะณะการหลอกลวงในรูปแบบการฟิชชิ่ง

เมื่อพิจารณาจากลักษณะการหลอกลวงในรูปแบบฟิชชิ่งนั้นอาจถือได้ว่าเป็นภัยคุกคามประเภทการโจมตีวิศวกรรมทางสังคม (Social Engineering Tactics Attackers)[52] กล่าวคือเป็นวิธีการโจมตีทาง

---

[47] พิชยุตม์ คูณทอง (เชิงอรรถ 36) 16.

[48] Microsoft, ‘ปกป้องตัวคุณเองจากฟิชชิ่ง’ (Microsoft) <https://bit.ly/3i6RrFP> สืบค้นเมื่อ 3 ธันวาคม 2566.

[49] PIMLAPAT PHANSUATHONG, ‘ฟิชชิ่ง (PHISHING) คืออะไร? รู้จักภัย 8 ประเภทบนโลกออนไลน์’ (Primal, 25 ตุลาคม 2566) <https://www.primal.co.th/th/seo/what-is-phishing/> สืบค้นเมื่อ 3 ธันวาคม 2566.

[50] โต๊ะข่าวไอที ดิจิทัล (เชิงอรรถ 3).

[51] โต๊ะข่าวไอที ดิจิทัล (เชิงอรรถ 4).

[52] Tom Jagatic and others, *Social Phishing* (School of Informatics Indiana University 2005) 1.

จิตวิทยาที่ไม่จำเป็นต้องใช้ความรู้มากมายเท่าไรนักเพียงแต่อาศัยความเข้าใจในหลักการที่ว่ามนุษนั้นจะตอบสนองต่อการกระทำประเภทใดมากที่สุดและนำการกระทำประเภทนั้นมาใช้ในการหลอกลวงและส่วนใหญ่ก็มักจะได้ผลดี การโจมตีด้วยวิธีทางวิศวกรรมทางสังคม[53] จึงมีความเกี่ยวข้องกับการหลอกให้ผู้คนหลงเชื่อเพื่อที่จะได้ข้อมูลที่สำคัญเพื่อใช้ในการสู่เข้าระบบคอมพิวเตอร์ เช่น การหลอกถามรหัสผ่าน การหลอกให้ส่งข้อมูลที่สำคัญให้ ซึ่งการโจมตีประเภทนี้ไม่จำต้องใช้ความรู้และความเข้าใจอะไรมากนักเกี่ยวกับระบบคอมพิวเตอร์หรือวิศวกรรมทางคอมพิวเตอร์กับการเจาะระบบเลยอันเนื่องมาจากวิศวกรรมทางสังคมนั้นถือว่าเป็นจุดอ่อนที่สำคัญและยากที่จะป้องกันเป็นอย่างมากด้วยเหตุผลอันเนื่องมาจากความแตกต่างในความเป็นมนุษย์นั้นเป็นสิ่งที่ไม่สามารถป้องกันได้เพราะถือว่ามนุษย์นั้นมีเจตจำนงค์อิสระในการดำเนินชีวิตและการเลือกที่จะเชื่ออะไรบางอย่างบนพื้นฐานความเข้าในส่วนบุคคล กล่าวคือมนุษย์ทุกคนนั้นมีความรู้ความเข้าใจในแต่ละเรื่องไม่เท่ากันซึ่งเป็นผลมาจากการเรียนรู้ที่ต่างกันและด้วยเหตุผลนี้เองจึงเป็นเรื่องยากที่จะป้องกันผู้คนในสังคมที่มีความแตกต่างกันจากอาชญากรที่มีจุดประสงค์มุ้งเน้นที่จำทำการหลอกลวงโดยอาศัยวิธีการทางวิศวกรรมทางสังคม โดยรูปแบบการโจมตีแบบวิศวกรรมสังคมโดยส่วนใหญ่นั้นจะใช้โทรศัพท์ถามข้อมูลโดยหลอกว่าตนเป็นผู้ได้รับอนุญาตหรือเป็นผู้มีอำนาจ โดยจะใช้วิธีการหลอกล่อหลายรูปแบบซึ่งอาศัยหลักการทางจิตวิทยา เช่น หลอกลวงว่าผู้ถูกโจมตีเป็นผู้โชคดีได้รับรางวัล โดยอาชญากรอาจใช้รูปแบบทางเทคนิคในการปิดบังเบอร์โทรศัพท์ที่ใช้ในการติดต่อหาผู้เสียหายซึ่งส่วนใหญ่โดยทั่วไปนั้นอาชญากรจะเลือกใช้วิธีการทางเทคโนโลยีคอมพิวเตอร์ในการปลอมแปลงเบอร์ผ่านโปรแกรมปลอมแปลงหมายเลขโทรศัพท์ซึ่งในบางกรณีหมายเลขที่ใช้ในการโทรมาหลอกลวงผู้เสียหายอาจจะเนเบอร์ของสำนักงานหรือหน่วยงานที่อาชญากรนั้นแอบอ้างจริงๆซึ่งสาเหตุที่เป็นเช่นนั้นก็เพราะอาชญากรนั้นใช้โทรแกรมปลอมแปลงหมายเลขเพื่อปลอมหมายเลยและโทรหาผู้เสียหายและการที่ไม่สามารถยืนยันผู้ที่โทรศัพท์เข้ามาว่าเป็นเจ้าหน้าที่หรือผู้ที่ได้รับอนุญาตให้กระทำการเช่นนั้นได้จนทำให้หลงเชื่อและแจ้งข้อมูลส่วนบุคคลของผู้เสียหายให้แก่อาชญากร ซึ่งในการหลอกลวงดังกล่าวข้างต้นนั้นอาจรวมไปถึงการหลอกให้ไปยืนยันการได้รับรางวัลที่เครื่อง ATM และให้ดำเนินการตามขั้นตอนที่อาชญากรบอก ซึ่งโดยมากแล้วมักจะเป็นการหลอกให้โอนเงินไปยังบัญชีที่อาชญากรเปิดไว้เพื่อรับโอนเงิน เช่น รูปแบบการหลอกลวงของแก๊งคอลเซ็นเตอร์ที่หลอกลวงประชาชนซึ่งมีวิธีการดำเนินการอยู่ 2 ลักษณะ คือ จะโทรศัพท์เข้ามาแจ้งว่า ได้รับคืนเงินภาษี หรือ ได้รับรางวัล และการหลอกลวงโดยขู่ว่า เป็นหนี้บัตรเครดิต และฐานข้อมูลกำลังถูกเจาะเข้าระบบ และจะพูดจาหว่านล้อมให้ไปทำธุรกรรมทางตู้เอทีเอ็ม

2.4.3 พัฒนาการของการก่ออาชญากรรมคอมพิวเตอร์ประเภทฟิชชิ่ง

ฟิชชิ่งนั้นแท้จริงแล้วคือการกระทำในลักษณะที่เป็นการหลอกลวงผู้เสียหายเพื่อให้ได้มาซึ่งข้อมูลสำคัญโดยมีพื้นฐานมาจากการใช้หลักการทางจิตวิทยามาหลอกลวงผู้เสียหายแต่เมื่อเป็นการหลอกลวงผ่าน

---

[53] SEVENHORIZON, ‘Social Engineering (การโจมตีแบบวิศวกรรมสังคม)’ (sevenhorizon.wordpress, 3 ธันวาคม 2559) <https://bit.ly/3WGVuaT> สืบค้นเมื่อ 5 มกราคม 2566.

อินเทอร์เน็ต ฟิชเชอร์[54]หรืออาชญากรไซเบอร์ที่ทำการหลอกลวงผู้เสียหายจึงได้มีการอัพเกรดวิธีการในการในการก่ออาชญากรรมจากการก่ออาชญากรรมจากการหลอกลวงทั่วไปเป็นการสร้างเว็บไซต์ปลอมขึ้นมาเพื่อใช้ในการดักเหยื่อหรือผู้เสียหายที่เข้ามาติดเหยื่อหรือเว็บปลอมที่อาชญากรนั้นได้สร้างไว้เพื่อลวงเอาข้อมูลจากผู้เสียหาย โดยที่ผู้เสียหายนั้นเปรียบเสมือนปลาที่เข้ามากินเหยื่อ และเมื่อพิจารณาจากลักษณะการหลอกลวงแล้วจะพบว่ารูปแบบของฟิชชิ่ง ที่มักจะกล่าวถึงนั้นมักจะใช้วิธีการส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเหมือนกับจดหมายอิเล็กทรอนิกส์จากผู้ให้บริการ หรือการเปิดเว็บไซต์ (Web Site) ที่มีลักษณะเช่นเดียวกันกับผู้ให้บริการที่แท้จริง แล้วทำการหลอกเอาข้อมูลสำคัญจากผู้เสียหายด้วยวิธีการผู้เสียหายกรอกข้อมูลสำคัญในเว็บไซต์ปลอมตามที่อาชญากรนั้นได้กำหนดไว้ ซึ่งข้อมูลส่วนใหญ่ที่อาชญากรมักหลอกลวงเพื่อให้ได้มาจากผู้เสียหายส่วนใหญ่มักจะเป็นข้อมูลที่สามารถใช้ในการระบุข้อมูลอัตลักษณ์บุคคล ซึ่งรวมไปถึงข้อมูลสำคัญอย่างอื่นที่สามารถใช้เข้าถึงระบบคอมพิวเตอร์ ข้อมูลบัญชีธุรกรรมอิเล็กทรอนิกส์ ข้อมูลบัตรเครดิต ฯลฯ

จากการศึกษาพบว่าการการก่ออาชญากรรมในรูปแบบฟิชชิ่งครั้งแรกนั้นเกิดขึ้นในช่วงกลางทศวรรษที่ 1990[55] โดยกลุ่มแฮกเกอร์กลุ่มหนึ่งได้ทำการสวมรอยเป็นพนักงานของ AOL[56]ซึ่งในขณะนั้นถือได้ว่าเป็นบริษัทด้านการให้บริการข้อมูลทางเครือข่ายรายใหญ่ในสหรัฐอเมริกา โดยอาชญากรนั้นได้ใช้วิธีการในการก่ออาชญากรรมคือการส่งข้อความโต้ตอบแบบทันทีและอีเมลเพื่อขโมยรหัสผ่านของผู้ใช้และบัญชีของพวกเขา กระทั้งในช่วงต้นของปี 2000 อาชญากรได้หันมาสนให้ความสนใจกับระบบการเงิน โดยเริ่มจากการโจมตีเว็บไซต์สกุลเงินดิจิทัลอย่าง E-Gold เป็นครั้งแรกในปี 2001 และภายในปี 2003 ฟิชเชอร์ได้พัฒนาวิธีการในการก่ออาชญากรรมจากเดิมที่ใช้เพียงการหลอกถามข้อมูลหรือแฮ็กข้อมูลผ่านอีเมลเท่านั้น แต่พอมาในปี2003 ในยุคที่อินเทอร์เน็ตได้รับความนิยมในการใช้งานที่แพร่หลายมากขึ้นในสังคมทั่วไป ด้วยเหตุนี้เองอาชญากรจึงเริ่มที่จะเปลี่ยนรูปแบบในการก่ออาชญากรรมโดยการจดสร้างเว็บไซต์ที่ใช้ชื่อโดเมนที่มีความแตกต่างเล็กน้อยในเว็บไซต์การค้าที่ถูกกฎหมาย เช่น eBay และ PayPal และรวมไปถึงการส่งจดหมายจำนวนมากโดยขอให้ผู้เสียหายมาเยี่ยมชมเว็บไซต์ที่สร้างขึ้นมาเพื่อจุดประสงค์ในการหลอกเอาข้อมูลด้วยการให้ผู้เสียหาย ป้อนรหัสผ่าน และอัปเดตข้อมูลบัตรเครดิต

อนึ่ง จากข้อความดังที่ได้กล่าวมาในข้างต้นว่าในช่วงตั้งแต่ปี2003 ซึ่งถือได้ว่าเป็นยุคที่อินเทอร์เน็ตได้รับความนิยมในการใช้งานที่แพร่หลายมากเป็นอย่างมาก เมื่อเครือข่ายทางสังคมอย่างอินเทอร์เน็ตได้รับ

---

[54] ฟิชเชอร์ คือ ผู้ที่ก่ออาชญากรรมรูปแบบฟิชชิงที่กระทำต่อระบบธนาคารทางอินเทอร์เน็ต โดยใช้กลอุบายทางอินเทอร์เน็ตซึ่งมักมาในรูปแบบของการปลอมแปลงอีเมล หรือข้อความที่สร้างขึ้นเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนตัว

[55] Paul Gillin, ‘The history of phishing’ (Verizon) <https://www.verizon.com/business/-resources/articles/s/the-history-of-phishing/> สืบค้นเมื่อ 5 มกราคม 2566.

[56] AOL ย่อมาจาก American Online, Inc เป็นบริษัทอเมริกันที่ให้บริการทางด้านมัลติมีเดีย ของ Time Warner AOL เป็นผู้ให้บริการข้อมูลทางเครือข่ายรายใหญ่ในสหรัฐอเมริกา ให้บริการในรูปแบบของศูนย์ BBS และให้บริการเข้าใช้อินเทอร์เน็ตนับตั้งแต่ปี1993และนับเป็นศูนย์บริการเครือข่ายขนาดใหญ่ที่สุดในสหรัฐอเมริกา. ‘AOL’ (AOL) <https://g.co/kgs/bpifA3> สืบค้นเมื่อ 5 มกราคม 2566.

ความนิยมในการใช้งานที่แพร่หลายมากขึ้น การก่ออาชญากรรมแบบฟิชชิ่งก็เริ่มที่จะปรับปรุงวิธีการในการรวบรวมข้อมูลส่วนบุคคลเพื่อปรับแต่งข้อความให้สามารถหลอกผู้เสียหายได้แนบเนียนและน่าเชื่อถือมากขึ้น สิ่งนี้เองทำให้เกิดรูปแบบการหลอกลวงแบบสเปียร์ฟิชชิ่ง (Spear Phishing) ซึ่งอาชญากรจะค้นหาข้อมูลเป้าหมายเพื่อปรับแต่งข้อความและเพิ่มโอกาสในการประสบความสำเร็จ และใช้รูปแบบในการหลอกลวงผู้เสียหายโดยใช้รูปแบบอย่างการล่าปลาวาฬ กล่าวคือในการก่ออาชญากรรมในยุคที่ผู้คนมีความรู้ความเข้าใจมากขึ้นทำให้หลอกลวงแบบเดิมมีโอกาสประสบความสำเร็จที่น้อยลง การล่าปลาวาฬจึงหมายถึงการหลอกลวงผู้เสียหายในแบบที่มีการกำหนดเป้าหมายในการก่ออาชญากรรมแบบเฉพาะเจาะจงไปยังผู้บริหารระดับสูงหรือบุคคลที่ร่ำรวย ซึ่งเปรียบได้กับปลาวาฬเพื่อขโมยข้อมูลที่ละเอียดอ่อนหรือโน้มน้าวให้โอนทรัพย์สินหรือเงินจำนวนมากให้กับอาชญากร, เพื่อลดโอกาสในการถูกจับได้, และเพื่อเป็นการเพิ่มโอกาสในการประสบความสำเร็จที่มากขึ้น เนื่องจากความสำเร็จในการก่ออาชญากรรมแบบฟิชชิ่งนั้น จะประสพผลสำเร็จได้ก็ด้วยการใช้เทคนิค Social Engineering แต่ว่าไม่ใช่ผู้ใช้ทุกคนที่จะหลงกลตกหลุมพรางที่ล่อไว้ ดังนั้นความสำเร็จของการใช้วิธีนี้จึงค่อนข้างจำกัด

เมื่อเวลาผ่านไปเทคโนโลยีก็ได้มีการพัฒนามากขึ้นฟิชเชอร์ก็เช่นกันเมื่อเวลาผ่านไปฟิชเชอร์ก็มีความเชี่ยวชาญในวิธีการหลอกลวงมากขึ้นโดยอาชญากรนั้นได้ทำการพัฒนาเทคนิคในการหลอกลวงโดยการปลอมแปลงที่อยู่อีเมลจริง และพัฒนาวิธีการในการส่งอีเมลและแอบอ้างแหล่งที่มาที่เชื่อถือ ทั้งยังขยายขอบเขตของการก่ออาชญากรรมให้ครอบคลุมถึงเครือข่ายทางสังคมออนไลน์ แอพส่งข้อความโต้ตอบแบบทันทีและข้อความ SMS ซึ่งเป็นสิ่งที่ยากต่อการตรวจสอบหรือการคัดกรองอย่างยิ่งและต่อมาอาชญากรก็ได้มีการเริ่มที่จะใช้วิธีการฟิชชิ่งที่กระทำผ่านโทรศัพท์ หรือที่เรียกว่า วิชชิ่ง (Vishing) ซึ่งมาจากคำว่า ว๊อยซ์ (Voice) ซึ่งแปลว่าเสียง เป็นการใช้ ว๊อยซ์ ร่วมกับฟิชชิ่ง โดยมากมักเป็นการหลอกลวงให้ได้มาซึ่งข้อมูลส่วนบุคคลผ่านทางโทรศัพท์นั่นเองซึ่งวิธีการนี้เริ่มปรากฏมากขึ้นในสังคมไทยในปัจจุบัน เช่นการ โทรศัพท์ถึงผู้เสียหายแล้วปลอมตัวว่าเป็นพนักงานจากธนาคารหรือองค์กรบัตรเครดิต ขอตรวจสอบข้อมูลส่วนบุคคลที่สำคัญ หรือแม้แต่หน่วยงานทางการเงินของภาครัฐเองก็ถือได้ว่าเป็นหนึ่งในเหยื่อของอาชญากรประเภทนี้เช่นกัน

นอกจากนี้ยังมีอาชญากรรมคอมพิวเตอร์อีกรูปแบบนึงที่เรียกว่า ฟาร์มมิ่ง(Pharming) ซึ่งเป็นการโจมตีระบบคอมพิวเตอร์รูปแบบนึง ฟาร์มมิ่งคือการเข้าไปเปลี่ยนแปลงเส้นทางของระบบการจับคู่ชื่อให้ตรงกับแอดเดรสที่จะเข้าไป กล่าวคือในขณะที่เสียหายคิดว่าตนนั้นได้เข้าสู่เว็บไซต์ที่พวกเขาต้องการ แต่แท้จริงแล้วผู้เสียหายนั้นกำลังเข้าสู่เว็บไซต์ของไอพีที่มีการล่อลวงเพื่อเอาข้อมูล การใช้วิธีการฟาร์มมิ่งนี้สามารถที่จะสร้างความเสียหายและผลกระทบให้กับผู้ใช้บริการทางออนไลน์ได้ในวงกว้างกว่าเป็นอย่างมากยิ่งไปกว่านั้น ฟาร์มมิ่งไม่ใช่แค่การโจมตีเพียงครั้งเดียวจบเช่น เดียวกับการใช้อีเมล์แบบวิธีการฟิชชิ่ง แต่การฟาร์มมิ่งจะยังคงรออยู่ในระบบจนกว่าผู้ใช้จะเข้าไปยังเว็บไซต์เพื่อใช้บริการเว็บอีกครั้ง

2.4.4 ประเภทของการฟิชชิ่ง(Phishing)[57]

ในการจำแนกประเภทหรือชนิดของการฟิชชิ่งนั้นขึ้นอยู่กับหลักเกณฑ์ในการนำมากำหนดซึ่งจากการศึกษาพบว่ามีหลักเกณฑ์ในการจำแนกประเภทของฟิชชิ่งอยู่ 3 หลักเกณ์ดังนี้

2.4.4.1 หลักเกณฑ์ในการจำแนกประเภทโดยพิจารณาจากช่องทางกระทำผิด

เนื่องจากการ ฟิชชิ่ง นั้นสามารถเกิดได้หลายช่องทาง(Channel) เช่น จดหมายอิเล็กทรอนิกส์ โทรศัพท์ อุปกรณ์คอมพิวเตอร์ ซึ่งสำหรับกรณีที่มีเป่าหมายเป็น คอมพิวเตอร์เคลื่อนที่ หรือ Laptop (Mobile-targeted attacks)จะสามารถจำแนกประเภททการกระทำผิดย่อยไปตามลักษณะของอุปกรณ์ที่เป็นเป้าหมายในการกระทำความผิด โดยจะใช้คำเรียกเจาะจงตามลักษณะของอุปกรณ์นั้นๆ เช่น “Blue jacking” ใช้เรียกสำหรับการกระทำผ่านทางบลูทูธ, “Smishing”ใช้กับการกระทำโดยการส่งข้อความสั่นๆ, และคำว่า “Vishing” ใช้สำหรับการกระทำผ่านโทรศัพท์เคลื่อนที่เป็นต้น

2.4.4.2 หลักเกณฑ์ในการจำแนกประเภทโดยพิจารณาจากวิธีการทางเทคนิค

เนื่องจากการ ฟิชชิ่ง นั้นต้องอาศัยวิธีการทางเทคนิคที่หลากหลายในการก่ออาชญากรรมและด้วยเหตุผลทางด้านเทคนิคในการก่ออาชญากรรมนี้เองทำให้สามารถจำแนกประเภทได้ตามลักษณะของเทคนิคที่ใช้ในการกระทำความผิด ดังนี้[58]

(1) “Deceptive” คือการที่อาชญากรนั้นส่งข้อความบางอย่างไปหาเหยื่อเพื่อโน้มน้าวให้เหยื่อกระทำการบางอย่างตามที่อาชญากรนั้นแนะนำ (Call to action) เช่น การส่งข้อความแจ้งเตือนไปยังเหยื่อเพื่อหลอกว่าคอมพิวเตอร์ของของเหยื่อนั้นเสี่ยงต่อการติดไวรัส โดยทำการแนะนำให้เหยื่อนั้นกรอกรหัสบัตรเครดิตหรือโหลดแอพบางอย่าเพื่อทำการโจรกรรมข้อมูล

(2) “Malware based Phishing” คือการกระทำโดยใช้มัลแวร์เป็นเครื่องมือในการกระทำความผิดซึ่งสามารถจำแนกเป็นประเภทย่อยไปตามประเภทของมัลแวร์ที่ใช้ในการก่ออาชญากรรม เช่น Keylogger ที่เป็นการจดจำการกดแป้นพิมพ์, และWeb Trojan เพื่อสร้างกล่อข้อมูลหลอกให้เหยื่อกรอกข้อมูลสำคัญ

(3) “DNS Based phishing (Pharming)” คือเทคนิคในการแก้ไขเปลี่ยนแปลงข้อมูลในโฮสต์ไฟล์หรือโดเมน ซึ่งจะส่งผลต่อกระบวนการการนำทางในการจับคู่URLในการตอบสนอนต่อการค้นหาของระบบ ทำให้ระบบนั้นเกิดการสับสนและเข้าใจผิดมาจับคู่กับURLปลอมที่อาชญากรนั้นได้เตรียมไว้ โดยผู้เสียหายจะเข้าในว่าหน้าเว็บที่ตนนั้นกำลังใช้งานอยู่คือหน้าเว็บของผู้ให้บริการที่แท้จริงซึ่งส่วนใหญ่หน้าเว็บดังกล่าวที่อาชญากรมักใช้ในการกหลอกผู้เสียหายเพื่อโจรกรรมข้อมูลคือหน้าเว็บไซต์ของธนาคาร เพราะง่ายต่อการหลอกให้เชื่อเพื่อให้ผู้เสียหายกรอกข้อมูลสำคัญ

---

[57] คณาธิป ทองรวีวงศ์, *กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 2 ฯลฯ* (สำนักพิมพ์นิติธรรม 2563) 118-119.

[58] Rasha S. El-Din, Paul Cairns and John Clark, ‘The Human Factor in Mobile Phishing’ <https://www.researchgate.net/publication/298091490> สืบค้นเมื่อ 6 มกราคม 2566.

(4) “Content Injection Phishing” คือการนำเข้าซึ่งชุดคำสั่งข้อมูลที่ไม่พึงประสงค์เข้าสู่ระบบเว็บไซต์ออนไลน์ เช่น การการนำชุดคำสั่งไปใส่ไว้ในเว็บไซต์เพื่อให้ผู้เสียหายนั้นกรอกข้อมูลสำคัญโดยที่ชุดคำสั่งไม่พึงประสงค์นั้นจะเปลี่ยนเส้นทางในการนำส่งข้อมูลไปยังโดเมนของอาชญากรที่อาชญากรนั้นได้สร้างไว้เพื่อใช้ในการเก็บข้อมูลดังกล่าว

(5) “Man in The Middle Phishing” คือการดักจับข้อมูลโดยใช้เทคนิคทางคอมพิวเตอร์ที่มีความซับซ้อนเพื่อดักจับเอาข้อมูลของผู้เสียหายกลางทางระหว่างที่กำลังส่งไปยังผู้ให้บริการ

2.4.4.3 หลักเกณฑ์ในการจำแนกประเภทโดยพิจารณาการกำหนดเป้าหมาย

เนื่องจากการ ฟิชชิ่ง นั้นมีข้อจำกัดในเรื่องความสำเร็จเหตุเพราะในการส่งอีเมลหลอกลวงเหยื่อนั้นอาชญากรจะทำการส่งอีเมลแบบครั้งละมากๆเหมือนการหว่านแหเพื่อจับปลาหรืออาจจะเรียกได้ว่าเป็นการสแปมเมล์เพื่อมุ้งหวังให้มีผู้เสียหายมาติดกับดักที่ตนวางไว้แต่ในบางกรณีอีเมลเช่นว่านั้นก็ไม่สามารถที่จะใช้หลอกลวงกับกลุ่มคนที่มีความรู้ เมื่ออาชญากรรู้เช่นนี้จึงได้มีการพัฒนารูปแบบในการหลอกลวงที่อยู่บนพื้นฐานของการโจมตีทางวิศวกรรมทางสังคมแต่จะเปลี่ยนรูปแบบจากการส่งอีเมล์ครั้งละพัน ๆฉบับไปยังเหยื่อจำนวนมากเป็นการเลือกเหยื่อแบบเฉพาะเจาะจงซึ่งวิธีการดังกล่าวนั้นมี ดังต่อไปนี้[59]

(1) การฟิชชิ่งแบบเจาะจง(Spear Phishing) คือการหลอกลวงแบบมีเป้าหมายชัดเจนในการหลอกลวงโดยฟิชเชอร์นั้นจะทำการศึกษาข้อมูลประวัติและความสนใจเบื่องต้นของเหยื่อเพื่อใช้ในการเขียนอีเมลเพื่อส่งไปยังเหยื่อทั้งนี้เพื่อเป็นการเพิ่มโอกาสในความสำเร็จจากการหลอกลวง ซึ่งโดยทั่วไปฟิชเชอร์มักจะเขียนที่อยู่ ชื่อผู้ส่ง และตำแหน่ง ซึ่งเป็นคนที่เหยื่อนั้นรู้จักหรืออาจเป็นคู่ค้าทางธุรกิจของเหยื่อเพื่อเพิ่มความน่าเชื่อถือ

(2) การฟิชชิ่งแบบพุ่งเป้าเจาะจงไปที่กลุ่มผู้บริหาร (Whaling) คือการหลอกลวงที่มีพื้นฐานและแนวทางเหมือนกับการหลอกลวงแบบเจาะจง (Spear Phishing) เพียงแต่เหยื่อจากการหลอกลวงประเภทนี้จะเป็นกลุ่มผู้บริหารภายในองค์กร(Whales)เนื่องจากเป็นกลุ่มคนที่มีตำแหน่งในการเข้าถึงข้อมูลที่มากกว่าและมีความคุ้มค่าที่จะหลอกกลวงทำให้สิ่งที่อาจได้รับจากการหลอกลวงแบบนี้มีค่ามากขึ้น

(3) การฟิชชิ่งผ่านการแฝงตัวเป็นผู้บริหาร(BEC) คือการหลอกลวงโดยการโจรกรรมและแอบอ้างตัวตนของผู้บริหารระดับองกรค์ (Business Email Compromise)เพื่อใช้ในการหลอกลวงพนักงานภายในองค์กร ลูกค้า และผู้ขายเพื่อใช้ในการเปลี่ยนแปลงเส้นทางในการโอนเงินไปยังบัญชีที่ถูกเตรียมไว้ โดยข้อมูลจาก FBI’s 2019 Internet Crime Report ระบุว่าการโจมตีแบบ (BEC) ถือเป็นการโจมตีที่สร้างความเสียหายกว่า $1.77 billion และยังถือว่าเป็นวีการที่มีประสิทธิภาพมากที่สุดในบรรดาอาชญากรรมไซเบอร์ทั้งหมดในปี 2019[60]

---

[59] Cloud IT Network,’ฟิชชิ่ง (Phishing) คืออะไร?’ (Cloud IT Network, 29 พฤษภาคม 2564) <https://www.clouditnetwork.com/what-is-phishing/> สืบค้นเมื่อ 10 มกราคม 2566.

[60] FBI, ‘2019 Internet Crime Report Released’ (FBI, 11 February 2020) <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120> สืบค้นเมื่อ 10 มกราคม 2566.

(4) โคลนชิ่ง (Clone Phishing) คือการฟิชชิ่งที่ฟิชเชอร์นั้นจะสร้างอีเมล์โดยทำการลอกเรียนแบบเนื้อหาทั้งหมดจากอีเมลของจริง เช่น อีเมลแจ้งเตือนต่างๆจากธนาคาร เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลสำคัญ โดยอาชญากรจะทำการเปลี่ยนลิงค์ที่แนบมากับอีเมลต้นฉบับ นอกจากนั้นอีเมลนี้ยังมักใช้ชื่ออีเมลที่คล้ายคลึงกับต้นฉบับจนยากที่จะสังเกกตุเห็นข้อแตกต่าง

(5) การสโนว์ชู (Snowshoe Spam) คือการใช้เทคนิคSnowshoeในการส่งอีเมลเพื่อหลีกเลี่ยงระบบตรวจจับของกล่องข้อความพี่จะคิดว่าเป็นเมลขยะและคัดแยกไปยังถังขยะและทำให้เหยื่อไม่เห็นอีเมล์นั้น โดยวิธีการก็คือฟิชเชอร์นั้นจะใช้การส่งอีเมล์ที่เป็นการSpamไปทีละน้อยๆโดยการส่งผ่านโดนเมนและIPที่มีความแตกต่างกันออกไป

2.4.5 ขั้นตอนและวิธีการในการฟิชชิ่ง[61]

โดยทั่วไปแล้ววิธีการและเทคนิคในการก่ออาชญากรรมในรูปแบบฟิชชิ่งนั้นเป็นการกระทำที่ตั้งอยู่บนพื้นฐานของการโจมตีระบบคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ต โดยมีวัตถุประสงค์เพื่อการโจรกรรมข้อมูลส่วนบุคคล หรือข้อมูลที่สำคัญอื่นๆตามแต่วัตถุประสงค์ของอาชญากร ซึ่งก่อนที่เหยื่อนั้นจะถูกหลอกลวงและตกเป็นผู้เสียหายในท้ายที่สุดนั้น อาชญากรหรือฟิชเชอร์จะมีการวางแผนเตรียมการก่อนการก่ออาชญากรรม โดยมีขั้นตอนดังต่อไปนี้

2.4.5.1 ขั้นตอนแรกการกำหนดกลุ่มเป้าหมายที่อาชญากรจะใช้แอบอ้าง

ในขั้นตอนนี้ฟิชเชอร์จะทำการกำหนดกลุ่มเป้าหมายในการก่ออาชญากรรมโดยเลือกเหยื่อจากกลุ่มธุรกิจที่เหมาะสม และเป็นเป้าหมายที่มีความเหมาะสมต่อการก่ออาชญากรรม ซึ่งส่วนใหญ่แล้วมักจะเป็นกลุ่มธุรกิจขนาดใหญ่ในต่างประเทศ เช่น ยาฮู (Yahoo) ไมโครซอฟ (Microsoft) เพลพาล (PayPal) หรือหากเป็นในประเทศก็มักจะเป็น ธนาคาร หรือองค์กรขนาดใหญ่ และเมื่อฟิชเชอร์นั้นกำหนดเป้าหมายได้แล้วก็จะนำไปสู่ขั้นตอนถัดไปคือ การค้นหาโดนเมน, ที่อยู่อีเมลของ หรือเบอร์โทรศัพท์ของเหยื่อโดยไม่สนว่าจะได้ข้อมูลเหล่านั้นมาด้วยวิธีการใด

2.4.5.2 ขั้นตอนที่สองการสร้างที่อยู่อีเมลหรือเว็บไซต์ปลอม

ในขั้นตอนนั้นเป็นขั้นตอนที่จะกระทำถัดจากขั้นนตอนแรกคือ เมื่อฟิชเชอร์เลือกเป้าหมายที่ตนจะใช้แอบอ้างได้แล้ว ฟิชเชอร์ก็จะทำการลอกเลียนแบบช่องทางการติดต่อหรือเว็บไซต์ของธุรกิจที่ตนนั้นแอบอ้าง เพื่อใช้ในการสร้างที่อยู่และเว็บไซต์เสมือนจริงขึ้นเพื่อใช้เป็นช่องทางในการฟิชชิ่งโดยจะมีลักษณะที่เหมือนของจริงทั้งการตั้งค่า (Setup) ระบบเว็บไซต์ปลอม รวมถึงการปลอมแปลงลอกเลียนแบบหน้าเว็บเพจ (Web Page) จากเจ้าของที่แท้จริง

---

[61] Tushar Srivastava, ‘Phishing and Pharming-The Deadly Duo’ (SANS Institute, 14 February 2007) <http://www.sans.org/reading-room/whitepapers/ privacy/phishing-pharming-evil-twins-1731> สืบค้นเมื่อ 7 มกราคม 2566.

2.4.5.3 ขั้นตอนที่สามการติดต่อสื่อสารกับผู้เสียหาย

ในขั้นตอนนี้นั้นเป็นกรณีที่ฟิชเชอร์นั้นใช้การส่งอีเมล์หรือการสร้างหน้าเว็บไซต์ปลอมในการใช้หลอกลวงร่วมกันกับการส่งอีเมลเพื่อใช้ในการหลอกลวงผู้เสียหาย ด้วยการส่งอีเมล์หลอกลวงทั้งหมดกระจายไปยังผู้เสียหายตามข้อมูลที่อยู่ของผู้เสียหายที่ฟิชเชอร์นั้นมี ดังนั้น ด้วยวิธีการนี้เองทำให้ในบางครั้งเหยื่อบางรายอาจจะสังเกตุได้ถึงความผิดปกติของอีเมล์ที่ส่งมาเพราะอย่างกรณีที่ฟิชเชอร์นั้นแอบอ้างว่าตนนั้นเป็นตัวแทนธนาคารแห่งหนึ่งซึ่งไม่ใช่ธนาคารที่ลูกค้านั้นใช้บริอยู่ แต่กลับมีอีเมล์ถึงลูกค้าของธนาคารจากธนาคารที่เหยื่อนั้นไม่ได้ใช้บริการทำให้ทราบได้ทันทีว่าอีเมล์นั้นเป็นของปลอมอย่างแน่แท้ แต่ไม่ว่าอย่างไรตามแม้อีเมล์ประเภทนี้จะสังเกตง่ายแต่ก็ใช่ว่าทุกครั้งเหยื่อนั้นจะสังเกตุเพราะในบางครั้งฟิชเชอร์นั้นก็จะใช้วิธีการส่งข้อความมาหลายๆครั้งหรือครั้งละมากๆหรือที่เรียกว่าการสแปม (Email spam) ซึ่งในบางครั้งผู้เสียหายนั้นก็อาจจะกดเข้าไปในเมล์นั้นได้ โดยเมื่อผู้เสียหายนั้นกดเข้าไปยังลิงค์ที่ฟิชเชอร์ได้การวางกับดักเอาไว้และกรอกข้อมูลบางอย่างที่อาจเป็นข้อมูลสำคัญในหน้าเว็บนั้นไปข้อมูลที่ได้ทำการกรอกไปนั้นจะถูกบันทึกเอาไว้ทั้งหมดไม่ว่าจะเป็นบัญชีสำหรับการใช้บริการออรไลน์ไปจนถึงข้อมูลส่วนตัวและข้อมูลบัตรเครดิตซึ่งเป็นการกระทำตามรูปแบบดั้งเดิมที่มักจะใช้ได้ผลเสมอ หรือหากเป็นกรณีการหลอกลวงผ่านโทรศัพท์ก็มักจะใช้วิธีการหลอกถามโดยการอ้านตัวเป็นเจ้าหน้าที่ขอหน่วยงานในภาครัฐหรือเอกชน เช่น ฟิชเชอร์นั้นจะอ้างตัวว่าเป็นตำรวจแล้วทำการถาม ชื่อนามสกุล วันเดือนปีเกิด และข้อมูลส่วนบุคคลสำคัญอื่นๆที่อาชญากรนั้นอาจนำไปใช้ประโยชน์ในการในการสวมรอยหรือใช้ในการทำธุรกรรมอื่นๆ ซึ่งในบางกรณีอาจจะไม่ใช้แค่การได้ไปเพียงข้อมูลส่วนบุคคลเท่านั้นแต่อาขได้ทรัพย์สินไปด้วย เช่น การการส่งข้อความไปยังผู้เสียหายเพื่อแจ้งเปลี่ยนบัญชีเงินฝากในการรับชำระค่าบริการสินค้าเพื่อให้ผู้เสียหายนั้นโอนเงินไปยังบัญชีที่อาชญากรนั้นไปเปิดไว้เพื่อรับโอนโดยเฉพาะซึ่งส่วนใหญ่มันเป็นบัญชีม้าหรือบัญชีปลอมที่ได้มาจากการจ้างเปิดบัญชี ซึ่งในปัจจุบันนั้นวิธีการฟิชชิ่งเช่นนั้นนั้นกำลังเป็นที่นิยมมากในหมู่อาชญากรฟิชชิ่ง เพราะด้วยผลพวงจากการพัฒนาเทคโนโลยีการทำธุรกรรมทางการเงินออนไลน์ที่ทั้งสะดวกรวดเร็วแประหยัดเวลาในการทำธุรกรรม ด้วยเหตุนี้เองการหลอกลวงเช่นนี้จึงเป็นวิธีการที่ได้ผลเป็นอย่างมากในการก่ออาชญากรรมของอาชญากรฟิชชิ่ง

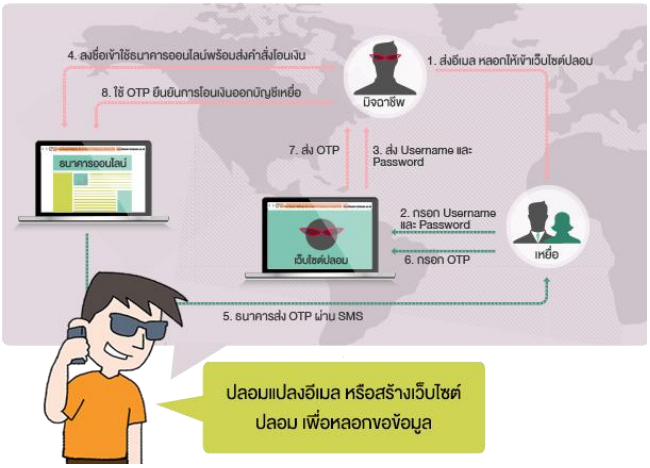
2.4.5.4 ขั้นตอนที่สี่ผลสืบเนื่องจากการได้มาซึ่งข้อมูลส่วนบุคคลเพียงอย่างเดียว

ในขั้นตอนนี้นั้นฟิชเชอร์จะเปลี่ยนจากสถานะจากฟิชเชอร์กลายเป็นอาชญากรคอมพิวเตอร์และสร้างอาชญากรรมอื่นๆ ต่อไป โดยที่อาชญากรนั้นจะนำข้อมูลที่ได้มาจากการฟิชชิ่งไปใช้ในการต่อยอดการก่ออาชญากรรมอื่นๆที่มีพื้นฐานเป็นการหลอกลวงเช่นเดิมแต่อาจเปลี่ยนวิธีการในการหลอกลวง เช่น การแฮกบัญชีในโลกออนไลน์ของผู้เสียหายจากข้อมูลที่ได้มาจากการฟิชชิ่ง หรือการนำข้อมูลส่วนตัวไปซื้อของออนไลน์และจะผลัดเปลี่ยนวิธีการในการใช้ประโยชน์จากข้อมูลไปเรื่อยๆจนกว่าผู้เสียหายนั้นจะเกิดสงสัยหรือรู้ตัว

การทำการฟิชชิ่งนั้นในบางกรณีอาจจะทำครบทั้งสี่ขั้นตอน หรือบางกรณีอาจจะทำเพียงสองหรือสามขั้นตอน ขึ้นอยู่กับแผนการของฟิชเชอร์และความแนบเนียนในการหลอกลวงผู้เสียหายว่าจะสามารถหลอกลวงเพื่อให้ได้ข้อมูลมามากน้อยแค่ไหน

อย่างไรก็ตามในความเป็นจริงแล้วคงจะไม่มีใครให้บัญชีธนาคาร หรือหมายเลขบัตรเครดิตกับผู้อื่นที่ไม่รู้จักหรือไว้ใจ โดยเฉพาะอย่างยิ่งหากรู้ว่าเป็นมิจฉาชีพก็คงไม่มีใครให้ข้อมูลที่มีความสำคัญอย่างยิ่ง แต่เนื่องจากฟิชเชอร์นั้นใช้วิธีการและเทคโนโลยีที่มีความซับซ้อนมาใช้ประกอบการหลอกลวงเพื่อเพิ่มความน่าเชื่อถือและทำให้ผู้เสียหายนั้นหลงเชื่อและให้ข้อมูลส่วนบุคคลไป โดยที่ฟิชเชอร์นั้นในจะใช้เทคนิคในการหลอกลวงด้วยการสร้างหน้าเว็บไซต์ให้มีความเหมือนจริงมาที่สุดรวมทั้งคัดลอกต้นฉบับมาทั้งหมด จากนั้นจะเปลี่ยนลิงค์ (Link) ที่ใช้เชื่อมโยงไปเป็นลิงค์อื่นๆ ที่ต้องการเพื่อให้ผู้เสียหายหลงเข้าไปยังเว็บเพจที่ เตรียมเอาไว โดยที่ลิงค์ที่อยู่ในอีเมล์นั้นเป็นของจริงเพียงแต่ฟิชเชอร์นั้นได้ทำการเปลี่ยนเส้นทางในการเข้าสู้เว็บไซต์ที่ได้เตรียไว้สำหรับการลวงเอาข้อมูลของเหยื่อโดยวิธีการ ฟิชชิ่งแบบนี้เรียกว่าการ Content Injection Phishing

โดยในแนวคิดของจดหมายอิเล็กทรอนิกส์ที่เป็นฟิชชิ่งนั้นจะออกแบบมาให้ผู้เสียหายหลงเชื่อ และมีเหตุให้ผู้เสียหายคลิกโดยอาศัยความรู้สึกที่ทำให้ให้เชื่อและคลิกก่อนที่จะคำนึงถึงเรื่องอื่นๆ ที่จะตามมา โดยอาจมีอุบายว่าเป็นการตรวจสอบบัญชีผู้ใช้(Account) หรือ บอกว่ามีการตรวจพบจากธนาคารว่าบัญชีถูกนำไปใช้โดยผู้อื่นที่ไม่มีสิทธิอย่างไม่ถูกต้องให้ตรวจสอบ หรือเปลี่ยนรหัสผ่านให้เรียบร้อยและตรวจสอบความเป็นเจ้าของตัวจริงโดยการให้กรอกข้อมูลส่วนบุคคล จากนั้นเพื่อมิให้ผู้เสียหายสงสัยก็จะมีการแจ้งขอบคุณที่เปลี่ยนข้อมูลดังกล่าวเพื่อให้ดูแนบเนียนที่สุดและเพื่อไม่ให้เป็นที่สงสัย หรือแม้กระทั้งการสร้างบันทึกว่ามีการซื้อขายหรือทำธุรกรรมนั้นจริงโดยมีข้อความตอบกลับในลักษณะเดียวกันกับการตอบกลับของธนาคาร ดังนั้นเมื่อมีหลายคนเชื่อว่าระบบคอมพิวเตอร์ไม่เคย ผิดพลาดก็จะเชื่อในระบบอัตโนมัติที่คอมพิวเตอร์สั่งมาแล้วก็จะกลายเป็นผู้เสียหายของฟิชเชอร์ในที่สุด[62]



ภาพที่ 2.1 ภาพของตัวอย่างขั้นตอนในการฟิชชิ่งแบบสร้างเว็บไซต์ปลอม[63]

---

[62] วิชญ์ศุทธ์ เมาระพงษ์. ‘ปกป้องข้อมูลสำคัญจากจากการ Phishing’ (สิงหาคม 2552) 152 วารสาร TPA News ข่าว ส.ส.ท., 6-7.

[63] ธนาคารแห่งประเทศไทย, ‘กลโกงธนาคารออนไลน์’ (ธนาคารแห่งประเทศไทย) <https://www.bot.or.th/th/satang-story/fraud/online-fraud.html> สืบค้นเมื่อ 9 มกราคม 2566.

จากภาพตัวอย่างขั้นตอนในการฟิชชิ่งในข้างต้นจะเห็นได้ว่าการฟิชชิ่งนั้นมีกระบวนการที่สำคัญอย่างยิ่งอยู่สามขั้นตอนด้วยกัน คือ 1.ขั้นตอนการส่งข้อความหรือจดหมายอิเล็กทรอนิคที่แอบอ้างสถาบันทางการเงินหรือหน่วยงานที่มีความน่าเชื่อถือเพื่อหลอกลวงผู้เสียหาย 2.ขั้นตอนการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งเป็นที่ปลอมแปลงขึ้นมาเฉพาะเพื่อหลอกให้ผู้เสียหายกรอกข้อมูล 3.ขั้นตอนการนำข้อมูลที่ได้มาจากการหลอกลวงไปใช้ในทางที่มิชอบเพื่อให้ได้ไปซึ้งประโยชน์ในทางทรัพย์สิน

2.5 ผลกระทบจากการก่ออาชญากรรมคอมพิวเตอร์ประเภทฟิชชิ่ง

การหลอกลวงด้วยการฟิชชิ่งนั้นก่อให้เกิดผลกระทบในแง่ลบต่อระบบความปลอดภัยและต่อบุคคล บริษัท และเซิร์ฟเวอร์อินเทอร์เน็ตโดยรวม นอกจากนี้ ผลที่ตามมาจากการหลอกลวงแบบฟิชชิ่งทั้งทางตรงและทางอ้อมยังส่งผลกระทบในวงกว้าง ซึ่งไม่เพียงแต่สร้างความเสียหายให้กับประชาชนทั่วไปและกลุ่มองค์กรทางธุรกิจเพียงเท่านั้น แต่ยังรวมถึงภาครัฐด้วย

2.5.1 ผลกระทบต่อภาครัฐ

การก่ออาชญากรรมคอมพิวเตอร์โดยเฉพาะการก่ออาชญากรรมด้วยวิธีการฟิชชิ่งนั้นถือได้ว่าเป็นการก่ออาชญากรรมทางเศรษฐกิจรูปแบบหนึ่ง[64]ที่มีผลกระทบเป็นอย่างมากต่อรัฐบาลของทุกประเทศทั่วโลก กล่าวคือผลกระทบในแง่ของความเสียหายจากการที่รับนั้นถูกอาชญากรทำการฟิชชิ่งข้อมูลต่างๆในระบบรักษาความปลอดภัยและการปกป้องความลับของชาติ ซึ่งจากที่ได้กล่าวมา ในหัวข้อ 2.2.1 นั้นชี้ให้เห็นว่าผู้ที่จะตกเป็นเหยื่อจากการฟิชชิ่งนั้นไม่ได้จำกัดอยู่แค่ในกลุ่มของประชาชนหรือภาคเอกชนแต่เป็นใครก็ได้ซึ่งรวมถึงหน่วยงานของทางภาครัฐ ด้วยเหตุผลที่ว่าฟิชเชอร์หรืออาชญากรนั้นไม่ได้มุ้งเน้นเพียงแค่การโจรกรรมข้อมูลส่วนบุคคลเพียอย่างเดียวแต่ยังรวมไปถึงการโจรกรรมข้อมูลทุกประเภทที่จะสามารถนำมาใช้ในการนำไปใช้เป็นช่องทางในการก่ออาชญากรรมที่ทำให้เกิดรายได้

โดยเมื่อกล่าวถึงผลกระทบจากการฟิชชิ่งของภาครัฐก็อาจจะกล่าวได้ว่าภาครัฐนั้นประกอบไปด้วยองค์กรต่างๆที่ทำหน้าที่บริหารดูแลประเทศซึ่งองค์กรเหล่านี้เองต่างก็มามาตรรการในการป้องกันการโจมตีหรือโจรกรรมข้อมูลทางไซเบอร์อยู่ แต่อย่างไรก็ตามก็ยังมีบางองกรค์ที่ถื่อได้ว่ามีความเสี่ยงและเสียหายที่สุดเกี่ยวกับฟิชชิ่งคือองค์กรรัฐบาล ทหาร และพลเรือน ซึ่งคาดว่าร้อยละเก้าสิบของการโจมตีที่ก่อให้เกิดความเสียหายมากที่สุดนั้นคือกองทัพและรัฐบาลเพราะถือเป็นหน่วยงานหลักที่จัดการเกี่ยวกับเรื่องภัยความมั่นคงหรือแม้กระทั้งการโจมตีระบบพื้นฐานของประเทศ ตัวอย่างเช่น การโจมตีระบบจัดการข้อมูลผู้ป่วยภายในโรงพยบาลสระบุรี[65] หรือในสหรัฐอเมริกาโรงเรียนเสนาธิการทหารบกที่เวสพอยต์ถูก "โจมตีแบบฟิชชิง" ซึ่ง

---

[64] กุลธิดา อาธิเจริญสุข, ‘การบังคับใช้กฎหมายเกี่ยวกับฟิชชิ่ง’ (2560) 2 วารสารรามคำแหง ฉบับนิติศาสตร์ 3 <https://so05.tci-thaijo.org/index.php/lawjournal/article/view/106759/84496> สืบค้นเมื่อ 9 มกราคม 2566.

[65] ไทยรัฐออนไลน์, ‘แฮ็กโรงพยาบาล-รีดค่าไถ่ เรียกถึง 6.3 หมื่นล้านบาท’ (ไทยรัฐออนไลน์, 10 กันยายน 2563) <https://www.thairath.co.th/news/local/central/1926912> สืบค้นเมื่อ 9 มกราคม 2566.

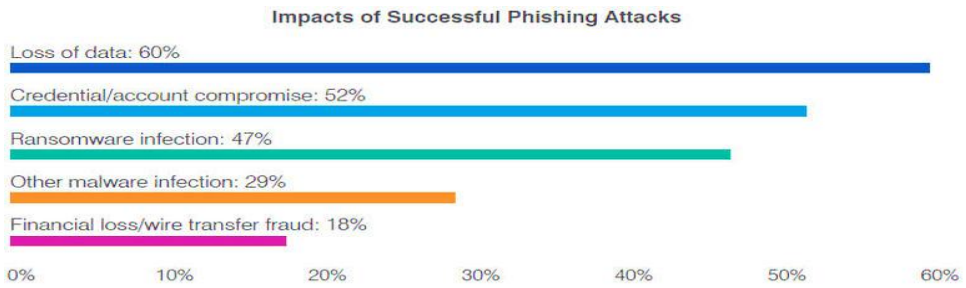
นักเรียนนายร้อยเวสต์พอยต์ส่วนใหญ่ได้รับอีเมลหลอกลวงและถูกหลอกให้เปิดเผยข้อมูลส่วนบุคคล[66]ซึ่งนำไปสู่การนำข้อมูลส่วนบุคคลไปแอบอ้างในการทำผิดต่อไป

2.5.2 ผลกระทบต่อภาคธุรกิจเอกชน

จากที่ได้กล่าวไว้ในหัวข้อ2.3.1ในตอนต้นซึ่งผู้เขียนนั้นได้กล่าวว่าการก่ออาชญากรรมคอมพิวเตอร์โดยเฉพาะการก่ออาชญากรรมด้วยวิธีการฟิชชิ่งนั้นถือได้ว่าเป็นการก่ออาชญากรรมทางเศรษฐกิจรูปแบบหนึ่ง กล่าวคือ ในยุคที่การติดต่อสื่อสารและข้อมูลต่างๆถูกเชื่อมต่อผ่านทางอินเทอร์เน็ตและข้อมูลต่างๆในบริษัทถูกเก็บไว้ในแหล่งเก็บข้อมูลออนไลน์ซึ่งเรียกว่า Could ซึ่งมีระบบการรักษาความปลอดภัยหรือ Fire Wall ที่ใช้ในการดูแลระบบซึ่งการเข้าถึงนั้นจะทำได้เฉพาะบุคคลที่มีหน้าที่ให้เข้าถึงได้เท่านั้น และเมื่อพิจารณาจากสภาพของระบบการประกอบธุรกิจในปัจจุบันอาจเป็นที่ทราบกันดีอยู่แล้วว่าในบุคปัจจุบันนี้ข้อมูลถือเป็นสิ่งสำคัญมากเป็นอันดับหนึ่งต่อการทำธุรกิจใดๆก็ตามด้วยเหตุนี้เองข้อมูลในองค์กรต่างๆจึงตกเป็นเป้าหมายในการฟิชชิ่งจากอาชญากร

โดยจากรายงานในปี 2022 ของ Proofpoint ผู้ให้บริการด้านความปลอดภัยทางอินเทอร์เน็ต พบว่า ในกลุ่มลูกค้าของพวกเขา 57% ถูกฟิชชิงโจมตีข้อมูลของบริษัทได้สำเร็จโดยเพิ่มขึ้นจากปี 2021 มากถึง 55% และจากการสำรวจในปี 2022 พบว่าในกลุ่มลูกค้ามากกว่า 75% ต้องเผชิญกับการโจมตีของฟิชชิงในวงกว้าง ทั้งที่ประสบผลสำเร็จและไม่สำเร็จ[67]

ทั้งนี้การโจมตีแบบกำหนดเป้าหมายได้ลดน้อยลง ทำให้มีโอกาสน้อยกว่าที่จะถูกจับได้ แต่ตอนนี้ cybercriminals ได้ใช้วิธีที่ซับซ้อนมากกว่านั้น ด้วยการค้นคว้าข้อมูลเกี่ยวกับบุคคลสำคัญในบริษัท จากนั้นก็ใช้การโจมตีแบบ spear phishing, BEC รวมทั้งการโจมตีแบบ Whaling ไปที่ CEO หรือบุคคลระดับสูงอื่น ๆ แทน การโจมตีแบบฟิชชิงสามารถส่งผลกระทบต่อบริษัทได้หลายวิธี ดังเช่นผลจากการสำรวจด้านล่างนี้



ภาพที่ 2.2 ภาพของผลสำรวจผลกระทบของธุรกิจจากการฟิชชิ่ง[68]

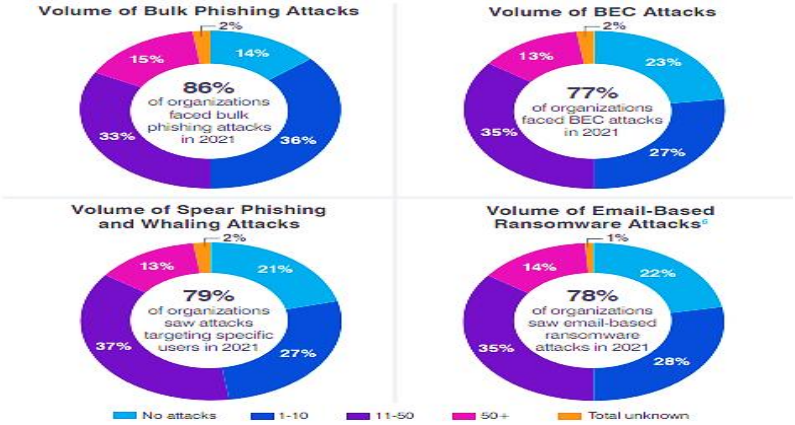
---

[66] Chayanin Kengsuwan, ‘Legal measures for phishing offense’ (Thesis Master of Laws Thammasat University 2012) 20.

[67] Proofpoint,‘2022 State of the Phish’ (Proofpoint) <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish> สืบค้นเมื่อ 10 มกราคม 2566.

[68] เพิ่งอ้าง.

อย่างไรก็ตาม ในปี 2021 ฟิชเชอร์ได้ทำการฟิชชิ่งโดยการหลอกลวงกลุ่มเป้าหมายที่มีความเกี่ยวข้องหรือมีความสำคัญต่อองค์กรทางธุรกิจเพิ่มมากขึ้น โดยที่ 65% ของการสำรวจพบว่า cybercriminals ใช้ Business Email Compromise (BEC) หรือการประนีประนอมทางอีเมลเชิงธุรกิจกับเหยื่อมากขึ้น กล่าวคือ อาชญากรนั้นจะใช้วิธีการแอบอ้างว่าเป็นคู่ค้าทางธุรกิจแล้วขอเปลี่ยนบัญชีธนาคารที่ใช้ในการทำธุรกรรมทางการเงินเพื่อหลอกให้โอนเงินมายังบัญชีดังกล่าวที่เตรียมไว้โดยเฉพาะ ดังจะเห็นได้จากผลสำรวจดังนี้



ภาพที่ 2.3 ภาพของผลการสำรวจการหลอกลวงโดยใช้เทคนิคต่างๆ[69]

2.5.3 ผลกระทบต่อประชาชน

ในสังคมปัจจุบันที่ถือได้ว่าเป็นยุคแห่ง Social Media นั้นเราคงปฏิเสธไม่ได้ว่าเราใช้ชีวิตและทำกิจกรรมต่าง ๆ บนโลกออนไลน์มากขึ้นเมื่อเทียบกับในอดีต ซึ่งมิจฉาชีพเองก็เริ่มใช้ช่องทางดังกล่าวเพื่อแสวงหาผลประโยชน์เช่นเดียวกัน โดยมิจฉาชีพนั้นได้มีการเปลี่ยนแปลงกลวิธีในการหลอกลวงให้มีความแนบเนียนและก่อให้เกิดความเสียหายได้มากยิ่งขึ้นกว่าในอดีต โดยเฉพาะในยุคที่ทุกคนสามารถเข้าถึงเทคโนโลยี และสามารถที่จะตกเป็นเหยื่อจากการแอบอ้างของอาชญากรที่นำเทคโนโลยีมาใช้สร้างความเสียหายให้แก่ประชาชน โดยการกระทำลักษณะดังกล่าวเรียกว่า การฟิชชิ่ง (Phishing) เป็นการหลอกลวงผ่านช่องทางการสื่อสารที่เข้าถึงแต่ละบุคคล เช่น โทรศัพท์ อีเมล Social Media และเว็บไซต์ปลอม เพื่อล่อลวงเอาข้อมูลส่วนบุคคลมาใช้โจรกรรม ซึ่งจะใช้การสร้างสถานการณ์ให้เกิดความกลัว หรือได้รับผลประโยชน์บางอย่าง จนหลงเชื่อทำตามและบอกข้อมูลส่วนบุคคลไป

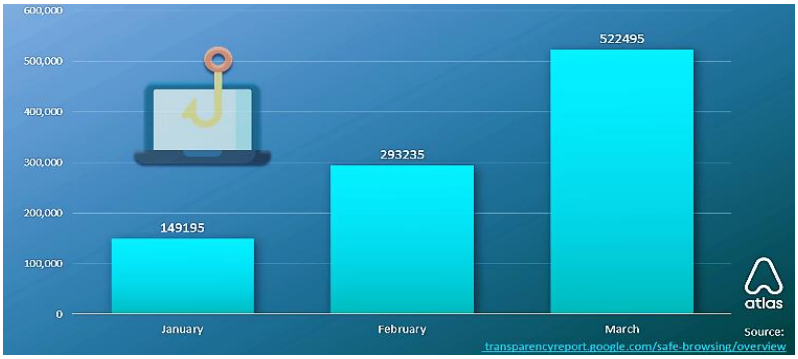
ทั้งนี้จากผลสำรวจของ Google ก็พบว่าในช่วงปี 2022 ที่ผ่านมานี้นั้นมีการเพิ่มขึ้นของเว็บไซต์ฟิชชิง (Phishing) สูงขึ้นถึง 350%[70] ในช่วยที่ไวรัส Covid-19 กำลังแพร่ระบาดซึ่งเป็นเหตุผลให้ผู้คนส่วนมา

---

[69] เพิ่งอ้าง.

[70] Google, ‘Googleรายงานเพื่อความโปร่งใส’ (Google) <https://transparencyreport.google.com/safe-browsing/overview> สืบค้นเมื่อ 10 มกราคม 2566.

เลือกที่จะทำกิจกรรมต่างๆอยู่ภายในที่อยู่อาศัยมากกว่าจะออกไปข้างนอกจึงยิ่งเพิ่มโอกาสในการเกิดอาชญากรรมทางไซเบอร์ ขึ้นสูงตามไปด้วย ทำให้ผู้ที่ไม่คุ้นชินกับระบบออนไลน์อาจตกเป็นเป้าหมายของผู้ไม่หวังดีเหล่านี้ได้ง่ายขึ้น ดังเช่นผลจากการสำรวจด้านล่างนี้



ภาพที่ 2.4 ภาพของผลการสำรวจอัตราการเพิ่มขึ้นของการฟิชชิ่ง[71]

2.6 สภาพปัญหาการก่ออาชญากรรมคอมพิวเตอร์ประเภทฟิชชิ่งในประเทศไทย

ปัญหาการการฟิชชิ่งหรือหลอกลวงทางอินเทอร์เน็ตในประเทศไทยนั้น ก่อให้เกิดผลกระทบต่อภาพรวมในด้านต่างๆทางเศรษฐกิจและสังคมทั้งยังสร้างความเสียหายให้แก่ประเทศเป็นอย่างมากไม่ต่างจากประเทศอื่นๆ เช่นกัน โดยเฉพาะอย่างยิ่งในยุคปัจจุบันนี้ที่การติดต่อสื่อสารของประเทศไทยได้เข้าสู่ยุคเทคโนโลยี 5G อย่างเต็มรูปแบบอันจะเห็นได้จากการที่เราสามารถใช้โทรศัพท์มือถือเพียงเครื่องเดียวในการอำนวยความสะดวกต่างๆ ในการใช้ชีวิตประจำวันหรือการทำงานผ่านช่องทางออนไลน์ เช่น การทำธุรกรรมการเงิน(E - Banking) การซื้อของออนไลน์การประชุมออนไลน์ เป็นต้น

เมื่อการสื่อสารทางออนไลน์มีการเข้าถึงมากยิ่งขึ้นเท่าใด ก็ย่อมจะเกิดปัญหาต่างๆได้มากขึ้นเท่านั้น โดยจะเห็นได้จากการที่ประชาชนตกเป็นเหยื่อการหลอกลวงผ่านทางการใช้บริการออนไลน์เป็นจำนวนมากโดยนับวันยิ่งทวีความรุนแรงและกระจายไปทั่วเท่าที่เทคโนโลยีสามารเข้าถึงได้ โดยมิจฉาชีพเหล่านี้ได้มีการพัฒนารูปแบบวิธีการหลอกลวงให้มีความยุ่งยากซับซ้อน สามารถจับผิดได้ยาก โดยอาศัยการสร้างความน่าเชื่อถือ การสร้างความหวาดกลัว และการชักจูงใจด้วยวิธีต่างๆซึ่งถ้าหากประชาชนหลงเชื่อก็จะทำให้ต้องสูญเสียข้อมูลส่วนตัว รวมไปถึงทรัพย์สินเงินทอง ซึ่งจากการศึกษาข้อมูลภาพรวมจาก สศช. ร่วมกับบริษัทศูนย์วิจัยเพื่อการพัฒนาสังคมและธุรกิจ จำกัด[72] พบว่าการก่ออาชญากรรมเกี่ยวกับการฟิชชิ่งหรือหลอกลวงผ่านอินเทอร์เน็ต ระหว่างเดือนมกราคม ถึง มีนาคม 2565 ในประชากรอายุ ระหว่าง 17-77 ปี จำนวน 5,798

---

[71] เพิ่งอ้าง.

[72] CHANJIRA_YEE, ‘รวบยอด ปัญหา "การหลอกลวงยุคดิจิทัล" ปี 2564 คนไทยโดนโทรหลอกกว่า 6.4 ล้านครั้ง’ (Spring news, 30 พฤษภาคม 2565) <https://www.springnews.co.th/infographic/825198> สืบค้นเมื่อ 11 มกราคม 2566.

ตัวอย่าง 20 จังหวัด ทั่วประเทศ และสัมภาษณ์เชิงลึก 3 กลุ่ม คือ กลุ่มผู้ที่มีประสบการณ์ถูกหลอกลวง 31 คน, กลุ่มภาครัฐและหน่วยงานที่เกี่ยวข้อง 2 คน, กลุ่มภาควิชาการ 4 คน รวมจำนวน 37 คน พบว่า จากกลุ่มตัวอย่างร้อยละ 97.8 ใช้โทรศัพท์มือถือ และร้อยละ 81.5 ใช้งานอินเทอร์เน็ต ซึ่งสะท้อนให้เป็นว่าคนไทยเกือบทั้งประเทศสามารถเข้าถึงโทรศัพท์และอินเทอร์เน็ตอย่างกว้างขวางและสามารถทีจะตกเป็นเหยื่อของอาชญากรได้ทุกเมื่อ และเมื่อพิจารณาประกอบกับผลการวิเคราะห์ของ ศูนย์วิเคราะห์ภัยฟอร์ติการ์ดแล็ปส์ (FortiGuard Labs) ที่ได้ทำการรวบรวมข้อมูล Threat Intelligence และมอนิเตอร์ภัยต่างๆ จากลูกค้าและภัยคุกคามทั่วโลกซึ่งแสดงให้เห็นถึงภัยคุกคามที่ต้องระวังในปีนี้ รวมถึงไทย และแนวโน้มของภัยไซเบอร์ปี 2566 ซึ่งได้ประเมินว่าประเทศไทยนั้นจะประสบกับปัญหาของการเพิ่มขึ้นของจำนวนอาชญากรรมทางคอมพิวเตอร์ประเภทฟิชชิ่ง และ อาชญากรรมไซเบอร์แบบตามสั่ง หรือ Cybercrime-as-a-Service (CaaS) ที่พัฒนาอย่างรวดเร็ว ไปจนถึงการใช้ประโยชน์รูปแบบใหม่จากเป้าหมายใหม่ๆ เช่น ระบบการประมวลผล (Edge) ที่ปลายทาง หรือโลกออนไลน์ต่างๆ[73]

เมื่อพิจารณาถึงสภาพสังคมในยุคปัจจุบันนี้นั้นอาชญากรรมจากการหลอกลางทางคอมพิวเตอร์หรือฟิชชิ่งนั้นได้รับความนิยมกันอย่างแพร่หลายในหมู่อาชญากรในประเทศไทย ดังจะเห็นได้จากข่าวการจับกุมอาชญกรที่ทำการหลอกลวงผ่านโทรศัพท์ซึ่งถือได้ว่าเป็นการฟิชชิ่งรูปแบบหนึ่ง เช่น ข่าวการจับกุมแก๊งคอลเซ็นเตอร์ ที่หลอกลวงผู้เสียหาย โดยการพูดคุยเชิงชู้สาวเพื่อชักชวนมาลงทุน เมื่อเหยื่อสนใจ จะเชิญเข้า “กลุ่มไลน์” อ้างว่า เป็นบริษัทที่ชื่อว่า E-SHIPING.SHOP ซึ่งแท้จริงเป็นบริษัทที่ไม่มีอยู่จริง[74] ซึ่งถือได้ว่าเป็นการหลอกลวงด้วยการ Phishing ประเภท Vishing และ Smishing หรืออย่างข่าวการที่มิจฉาชีพเข้าถึงบัญชีแล้วโอนเงินออกหมด[75] ด้วยวิธีการ Phishing โดยการสร้างหน้าเว็ปปลอมเพื่อลวงให้เหยื่อกรอกข้อมูลบัตรเครดิต เมื่อเหยื่อหลงเชื่อฟิชเชอร์ก็จะทำการโอนเงินจากบัญชีเหยื่อจนหมด หรือการปลอมเว็บไซต์ของกระทรวงการคลัง โดยการสร้างโดเมนปลอมเว็บไซต์กระทรวงการคลัง[76]

---

[73] Digital Life, ‘เปิดภัยไซเบอร์ ปี 66 "แฮกเกอร์ตามสั่ง" มาแน่ ยิ่งผสมความสามารถ AI ยิ่งน่ากลัว’ (Digital Life, 2 มกราคม 2566) <https://www.springnews.co.th/digital-tech/technology/833899> สืบค้นเมื่อ 13 มกราคม 2566.

[74] ทีมข่าวอาชญากรรม, ‘รวบ 4 ผู้ต้องหาแก๊งคอลเซ็นเตอร์นำประสบการณ์จากกัมพูชา ตั้งกลุ่มสตาร์ทอัพตุ๋นเหยื่อในไทยร่วมลงทุน’ (ผู้จัดการออนไลน์, 5 ธันวาคม 2565) <https://mgronline.com/crime/detail/9650000115641> สืบค้นเมื่อ 11 มกราคม 2566.

[75] Drama addict, ‘มิจฉาชีพเข้าถึงบัญชีเขาแล้วโอนเงินออกหมดเลย’ (Facebook) <https://www.facebook.com/141108613290/posts/10161067543448291/?>สืบค้นเมื่อ 11 มกราคม 2566.

[76] ‘คลังเตือนภัยเว็บไซด์กระทรวงการคลังปลอม อย่าคลิก ระวังโดนหลอก’ (รัฐบาลไทย, 1 สิงหาคม 2565) <https://www.thaigov.go.th/news/contents/details/57489> สืบค้นเมื่อ 13 มกราคม 2566.

2.6.1 กรณีตัวอย่างการก่ออาชญากรรมคอมพิวเตอร์ประเภทฟิชชิ่งในประเทศไทย

2.6.1.1 เมื่อวันที่ 13 มกราคม 2566 ที่สถานีตำรวจภูธรเมืองเชียงใหม่ นางสาวบัวลอย อายุ 52 ปี อาชีพเป็นแม่ค้าขายข้าวเหนียวหมูปิ้งในตลาดสดแห่งหนึ่งในตัวเมืองเชียงใหม่ ได้เข้าแจ้งความต่อพนักงานสอบสวนสถานีตำรวจภูธรเมืองเชียงใหม่ว่าถูก "แก๊งคอลเซ็นเตอร์" หลอกอ้างเป็นเจ้าหน้าที่สรรพากรส่งข้อมูลมาให้กรอก จากนั้นได้ดูดเงินภายในบัญชีธนาคารที่ผูกไว้ในแอพพลิเคชั่นในมือถือไปจนเกลี้ยงบัญชี โดยนางสาวบัวลอย เล่าว่าตอนนั้นตนกำลังนั่งขายข้าวเหนียวหมูปิ้งอยู่ในตลาด ได้มีหญิงคนหนึ่งอ้างว่าเป็นเจ้าหน้าที่สรรพากร โทรศัพท์หมายเลข 095-11668xx และเบอร์ 094-99378xx โทรมาหาตนและบอกว่าตนยังไม่ได้ชำระภาษีหลังจากที่ขายของผ่านแอพพลิเคชั่น "เป๋าตัง" จากนั้นปลายสายได้ส่งลิงก์มาให้ทางกล่องข้อความ โดยให้ตนกรอกข้อมูลยืนยันซึ่งขณะนั้นตนเห็นว่าเป็นลิงก์หน้าปกของกรมสรรพากรจึงได้กรอกข้อมูลส่วนตัวลงไป จากนั้นโทรศัพท์มือถือของตนได้ดับลงไปเอง และได้เปิดโทรศัพท์มือถือขึ้นมาใหม่อีกครั้ง จากนั้นแอปฯของธนาคารออมสินแจ้งเตือนมาว่า ตนได้ถอนเงินออกจากบัญชีเงินฝากจำนวน 70,000 บาท เหลือเงินในบัญชีเพียง 26 สตางค์ ทั้งที่ตนไม่ได้กดโอนเงินแต่อย่างใด ตนจึงรีบมาแจ้งความกับเจ้าหน้าที่ตำรวจดังกล่าว

อย่างไรก็ตาม ทางเจ้าหน้าที่ตำรวจได้ตรวจสอบแล้วพบว่า คนร้ายได้ส่งลิงก์ที่ฝังโปรแกรมควบคุมโทรศัพท์ระยะไกล หลังจากที่แก๊งคอลเซ็นเตอร์ได้เข้าไปควบคุมโทรศัพท์มือถือของผู้เสียหายได้แล้ว ก็จะเข้าไปค้นหาแอพพลิเคชั่นของธนาคารที่อยู่ในโทรศัพท์เครื่องนั้น ก่อนที่จะทำการโอนเข้าบัญชีม้าที่เตรียมไว้ไปจนเกลี้ยงบัญชี ทั้งนี้ขอฝากแจ้งเตือนประชาชนว่าอย่าได้หลงเชื่อหากมีคนโทรศัพท์แอบอ้างเป็นเจ้าหน้าที่หน่วยงานของรัฐและส่งลิงก์มาให้กรอกข้อมูล เพราะอาจจะตกเป็นเหยื่อของแก๊งมิจฉาชีพ หรือแก๊งคอลเซ็นเตอร์ได้[77]

ภาพที่ 2.5 ภาพของเว็บไซต์ยื่นภาษีปลอม[78]

---

[77] ธนกร วงศ์นาง, ‘แฉเล่ห์ "แก๊งคอลเซ็นเตอร์" ดูดเงินจากมือถือ เหยื่อรายล่าสุดสูญกว่า 7 หมื่น’ (กรุงเทพธุรกิจ, 13 มกราคม 2566) <https://www.bangkokbiznews.com/news/news-update/1047873> สืบค้นเมื่อ13 มกราคม 2566.

[78] Napaporn Panitchart, ‘อย่าหลงเชื่อ!! เว็บไซต์ ‘กรมสรรพากร’ ปลอม แนะ 3 วิธีสังเกต’ (The Bangkok Insight, 13สิงหาคม 2565) < https://www.thebangkokinsight.com/news/politics-general/politics/926871/> สืบค้นเมื่อ 14 มกราคม 2566.

2.6.1.2 เมื่อวันที่ 28 สิงหาคม 2565 เจ้าหน้าที่ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีตำรวจภูธรภาค5 ได้นำกำลังเข้าตรวจค้นที่บ้านหลังหนึ่งภายในหมู่ 5 ตำบลริมกก อำเภอเมือง จังหวัดเชียงราย ซึ่งเป็นบ้านของแก๊งแอบอ้างธนาคารดังตามหมายค้นของศาลจังหวัดเชียงราย ซึ่งเป็นการบุกค้นบ้านหลังพร้อมกับผู้ต้องหาได้ทั้งหมด 3 คนประกอบด้วย นายมน อายุ 21 ปี ชาว อ.เชียงแสน จ.เชียงราย, นายจักรกฤษณ์ อายุ 23 ปี ชาว อ.เชียงแสน จ.เชียงราย, นางสาวธัณ ณมน อายุ 22 ปี ชาว อ.เชียงแสน จ.เชียงราย โดยทั้งสามทำหน้าที่เป็นแอดมินตอบแชทเพื่อหลอกให้เหยื่อหลอกโอนเงิน ในเข้าจับกุมในครั้งนี้ทางเจ้าหน้าที่ตำรวจได้ขยายผลมาจากการจับกุมตัวนายทักษพล อายุ 22 ปีชาว อ.เชียงแสน จ.เชียงราย เป็นหัวหน้าขบวนการมีหน้าที่หาคนเปิดบัญชี, จัดการการเงิน, ทำเพจเฟซบุ๊กปลอม, ยิงแอดโฆษณา, ควบคุมสั่งการแอดมินที่สามารถจับกุมได้ที่ด่านตรวจแม่โถ ต.แม่เจดีย์ อ.เวียงป่าเป้า จ.เชียงราย เมื่อวันที่ 28 ส.ค. 65 ที่ผ่านมา โดยนายทักษพลตกเป็นผู้ต้องหาตามหมายจับของศาลจังหวัดเชียงใหม่ที่ 731/2565 ในฐานความผิดร่วมกันฉ้อโกงโดยแสดงตนเป็นบุคคลอื่นโดยได้กระทำการแสดงข้อความอันเป็นเท็จต่อประชาชนหรือด้วยการปกปิดความจริงซึ่งควรบอกให้แจ้งแก่ประชาชน โดยทุจริตหรือโดยหลอกลวงนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือ ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จโดยประการที่น่าจะเกิดความเสียหายต่อประชาชน นอกจากนี้ ทางเจ้าหน้าที่ยังได้ขยายผลติดตามจับกุมนางสาวอาทิตยา อายุ 22 ปี ชาวจังหวัดเชียงราย มีหน้าที่เป็นม้าถอนเงินและเป็นผู้ต้องหาตามหมายจับของศาลจังหวัดเชียงใหม่ด้วยจากนั้นเจ้าหน้าที่ตำรวจได้นำตัวผู้ต้องหามาสอบสวน โดยผู้ต้องหารับว่าการกระทำหลอกลวงชาวบ้านมีรุ่นพี่ที่รู้จักเอาทีมงานมาสอน ส่วนการกระทำดังกล่าวนั้นตนได้ทำมาประมาณ 2 เดือนได้เงินมาประมาณ1-2 แสนบาท ส่วนการหาเหยื่อนั้นก็จะหาในแอพพลิเคชั่นเฟซบุ๊กโดยจะเน้นกลุ่มที่ทำงานบริษัททำงานโรงงาน โดยจากการให้ข้อมูลของ พล.ต.ต.วีรชน บุญทวี รอง ผบช.ภ.5 ซึ่งได้เปิดเผยว่าการจับกุมของชุดปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ ตำรวจภูธรภาค 5 นั้น ทางชุดจับกุมได้รับการประสานจากฝ่ายสืบสวนของธนาคารไทยพาณิชย์สำนักงานใหญ่ว่า มีกลุ่มคนร้ายแอบอ้างใช้ภาพของทางธนาคารหลอกลวงประชาชนผ่านเพจเฟสบุ๊คเงินกู้ชื่อว่า "สินเชื่อมณี V. 2" หรือ "จามจุรีช่วยเหลือ V.88" หลอกลวงประชนและได้รับการร้องเรียนจากประชาชนว่าถูกหลอกให้กู้เงิน แต่ไม่ได้เงินจริงโดยจะหลอกเอาค่าดำเนินการและมีผู้เสียหายตกเป็นเหยื่ออีกกว่า 200 รายทั่วประเทศ ซึ่งจากการสืบสวนของเจ้าหน้าที่ตำรวจพบว่า ผู้ต้องหาใช้วิธีสร้างเพจเงินก็ขึ้นมาแล้วยิงแอดโฆษณาไปยังกลุ่มลูกค้าให้ผู้เสียหายกู้เงินในวงเงินไม่เกิน 2 หมื่นบาท อนุมัติเร็วไม่ต้องมีคนค้ำ ไม่ต้องมีหลักทรัพย์ สามารถได้เงินทันทีซึ่งเมื่อผู้เสียหายหลงเชื่อก็จะให้ผู้เสียหายโอนเงินเป็นค่าธรรมเนียมในการดำเนินการประมาณ 300 - 500 บาท และเมื่อผู้เสียหายโอนเงินเสร็จผู้ต้องหาก็จะบล็อกการติดต่อทันที และหากผู้เสียหายรายใดยังหลงเชื่อก็จะคุยหลอก

เอาเงินเรื่อย ๆ โดยอ้างว่าจะสามารถอนุมัติสินเชื่อให้ในยอดเงินที่สูงขึ้น อย่างไรก็ตาม ขบวนการดังกล่าวนั้นทางเจ้าหน้าที่ตำรวจกำลังอยู่ในระหว่างการขยายผลจับกุมผู้ร่วมขบวนการต่อไป[79]

2.7 มาตรการทางกฎหมายที่เกี่ยวข้องกับการฟิชชิ่งอันเป็นการฉ้อโกงประชาชนในประเทศไทย

2.7.1 ประมวลกฎหมายอาญา

เนื่องจากกระทำฟิชชิ่งนั้นถือได้ว่ามีลักษณะที่เป็นการกระทำความผิดทางอาญาประเภทหนึ่ง ดังนั้นจึงต้องนำประมวลกฎหมายอาญาที่เป็นหลักกฎหมายพื้นฐานในการกำหนดความผิดอันมีโทษมาศึกษาวิเคราะห์เพื่อให้เกิดความเข้าใจที่มากยิ่งขึ้น อีกทั้งเมื่อพิจารณาจากลักษณะในการฟ้องคดีกับผู้ที่กระทำผิดทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่คณะกรรมการกฤษฎีกาได้เคยให้ความเห็นไว้ว่าในการฟ้องคดีหากพบว่ากระทำความผิดนั้นเป็นความผิดตามกฎหมายอื่น ก็สามารถที่จะฟ้องผู้กระทำความผิดนั้นในฐานความผิดตามประมวลกฎหมายอื่นได้อีก[80]

โดยในหัวข้อนี้ผู้เขียนจะขอกล่าวถึงเพียงบทบัญญัติที่เกี่ยวข้องกับการฟิชชิ่งเพื่อที่จะได้นำมาวิเคราะห์ว่าการฟิชชิ่งด้วยวิธีการปลอมเว็บไซต์เพื่อให้ได้มาหรือเข้าถึงซึ่งข้อมูลส่วนบุคคลของผู้เสียหายแล้วนำข้อมูลเช่นว่านั้นไปใช้ทางที่ทำให้ได้มาซึ่งประโยชน์ในทางทรัพย์สินนั้นจะถือเป็นการกระทำความผิดฐานฉ้อโกงตามมาตรา 341 และมาตรา343 แค่ไหนเพียงไร ดังนี้

2.7.1.1 ความผิดฐานฉ้อโกง

ความผิดฐานฉ้อโกง คือ ความผิดตามประมวลกฎหมายอาญา มาตรา 341[81]ซึ่งบัญญัติไว้ว่า “ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

“ความผิดฐานฉ้อโกง”[82]เป็นความผิดที่แสดงถึงการเคลื่อนย้าย “สิทธิในทรัพย์”ด้วยการหลอกลวงบุคคลโดยเจตนาทุจริต เพื่อให้ได้ไปซึ่งสิทธินั้นมาเป็นของตน

---

[79] กรุงเทพธุรกิ, ‘ทลายแก๊งแอบอ้างธนาคารดัง หลอกกู้เงินผ่านเฟซบุ๊ก ชาวบ้านตกเป็นเหยื่อ 200 ราย’ (กรุงเทพธุรกิจ, 30 สิงหาคม 2565) <https://www.bangkokbiznews.com/finance/1023775> สืบค้นเมื่อ13 มกราคม 2566.

[80] ความเห็นคณะกรรมการกฤษฎีกา เรื่องเสร็จที่ นร 0901/0507 เรื่อง ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... 3.

[81] ประมวลกฎหมายอาญา มาตรา 341.

[82] คณิต ณ นคร, *กฎหมายอาญาภาคความผิด* (พิมพ์ครั้งที่ 11, สำนักพิมพ์วิญญูชน 2559) 437.

เมื่อพิจารณาจากบทบัญญัติในข้างต้นประกอบกับพฤติกรรมในการประกอบอาชญากรรมคอมพิวเตอร์ประเภทการฟิชชิ่งจะทำให้ทราบได้ว่าพฤติกรรมของการ“ฟิชชิ่ง”โดยทั่วไปแล้วมีจุดประสงค์หลอกลวงหรือปิดบังข้อความที่แท้จริงเพื่อให้ได้มาซึ่งข้อมูลของเหยื่อและนำข้อมูลเช่นว่านั้นไปใช้ทางที่ทำให้ได้มาซึ่งประโยชน์ในทางทรัพย์สิน ด้วยเหตุนี้เองการมาตรานี้จึงมีความเกี่ยวข้องกับการฟิชชิ่ง ซึ่งผู้เขียนจะได้อธิบายความสัมพันธ์ตามองค์ประกอบความผิดดังนี้

องค์ประกอบความผิดที่หนึ่ง “ ผู้ใด หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จหรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง” เมื่อพิจารณาจากองค์ประกอบความผิดดังที่ได้กล่าวไปในข้างต้นจะเห็นได้ว่าในขั้นตอนของการฟิชชิ่งนั้นฟิชเช้อ หรือผู้กระทำฟิชชิ่งนั้นมักจะเลือกใช้วิธีการหลอกลวงเหยื่อด้วยการแสดงข้อความอันเป็นเท็จทั้งหมดหรือบิดเบือนข้อความที่เป็นความจริงบางส่วนเพื่อนำมาใช้ในการหลอกลวงผู้เสียหายโดยใช้วิธีการทางอิเล็กทรอนิกส์ในการแสดงข้อความอันเป็นเท็จเหล่านั้นให้ผู้เสียหายได้ทราบผ่านทางช่องทางต่างๆ ทางอินเทอร์เน็ตเพื่อให้ได้มาซึ่งข้อมูลของผู้เสียหาย อาทิ การส่งจดหมายอิเล็กทรอนิกส์ การสร้างเว็บปลอมที่เลียนแบบเว็บที่แท้จริง และการส่งข้อความSMS ทั้งนี้ในส่วนขององค์ประกอบความผิดในข้อนี้ยังรวมไปถึงการนำข้อมูลของผู้เสียหายที่ได้มาจากการหลอกลวงไปใช้ในการหลอกลวงผู้อื่นต่อก็ถือว่าเป็นความผิดตามองค์ประกอบความผิดนี้เช่นกัน[83]

องค์ประกอบความผิดที่สอง “โดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิ” เมื่อพิจารณาจากองค์ประกอบความผิดดังที่ได้กล่าวไปในข้างต้นจะเห็นได้ว่าโดยเจตนาของการฟิชชิ่งล้วนทำไปเพื่อให้ได้ไปทรัพย์สิน กล่าวคือ โดยพื้นฐานของการกระทำความผิดฐานฟิชชิ่งนั้นตั้งอยู่บนพื้นฐานของการหลอกลวงเพื่อให้ได้ไปซึ่งทรัพย์สินอันเป็นการกระทำความผิดต่อตัวบุคคลโดยตรง แต่ไม่ว่าอย่างไรก็ตามโดยเนื้อแท้ของการฟิชชิ่งนั้นมิใช้การหลอกลวงเพื่อมุ้งประสงค์ที่จะเอาทรัพย์สินจากบุคคลในโดยตรงในขณะที่หลอกลวง แต่เป็นการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลแล้วนำข้อมูลของบุคคลเช่นว่านั้นไปใช้ประโยชน์ในทางอื่นเพื่อให้ได้มาซึ่งทรัพย์สินในภายหลัง โดยไม่จำเป็นที่จะต้องเป็นทรัพย์สินในรูปแบบของเงินหรือสิ่งของมีค่าเสมอไป อาทิ บิทคอยน์

องค์ประกอบความผิดที่สาม “โดยเจตนาทุจริต” สำหรับในส่วนขององค์ประกอบความผิดในข้อนี้นั้น เมื่อพิจารณาจากการกระทำความผิดตามองค์ประกอบความผิดในข้อหนึ่งและข้อสอง จะเห็นได้ว่าการฟิชชิ่งนั้นเป็นการหลอกลวงตามองค์ประกอบความผิดทั้งสองเพราะการ ฟิชชิ่งนั้นมีเจตนาในการกระทำก็เพื่อให้ได้ไปซึ่งทรัพย์สิน กล่าวคือ กรณีที่จะเป็นความผิดฐานฉ้อโกงได้นั้นต้องอาศัยองค์ประกอบที่ผลของการกระทำเป็นหลัก คือ ต้องมีการสูญเสียทรัพย์สิน และการได้ไปซึ่งทรัพย์สินนั้นต้องเป็นกรณีการได้ไปโดยปราศจากความยินยอมอย่างแท้จริง จึงจะถือว่าเป็นความผิด

---

[83] ปัทมาภรณ์ กฤษณายุทธ,‘ความผิดฉ้อโกง: ศึกษากรณีการหลอกลวงทางอินเทอร์เน็ต’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยลัยธรรมศาสตร์ 2551) 84-85.

ดังนั้น เมื่อพิจารณาจากข้อความดังที่ได้กล่าวไปในข้างต้นจะเห็นได้ว่า ฟิชเช้อหรือผู้ที่กระทำการฟิชชิ่งนั้นถือได้ว่ามีเจตนาและมูลเหตุจูงใจในการกระทำความผิด ซึ่งอาจกล่าวได้ว่าฟิชเช้อหรือผู้ที่กระทำการฟิชชิ่งนั้นมีเจตนาทุจริงในการหลอกลวงเพื่อให้ได้มาซึ่งทรัพย์สินอันเป็นความผิดตามมาตรานี้ แต่ไม่ว่าอย่างไรก็ตามหากกรณีการหลอกลวงเพื่อให้ได้ไปซึ่งข้อมูลแต่ยังมิได้นำไปใช้ในการหาประโยชน์ในทางทรัพย์สินที่เป็นสิทธิของผู้เสียหายหรือบุคคลอื่น การหลอกลวงนั้นก็จะยังไม่ถือว่าเป็นการฉ้อโกงตามมาตรานี้ เพราะถือว่าความเสียหายนั้นยังมิได้เกิดขึ้นแก่บุคคล

2.7.1.2 ความผิดฐานฉ้อโกงประชาชน

ความผิดฐานฉ้อโกงประชาชน คือ ความผิดตามประมวลกฎหมายอาญา มาตรา343[84] ซึ่งบัญญัติไว้ว่า “ถ้าการกระทำความผิดตามมาตรา 341 ได้กระทำด้วยการแสดงข้อความอันเป็นเท็จต่อประชาชน หรือด้วยการปกปิดความจริงซึ่งควรบอกให้แจ้งแก่ประชาชน ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำความผิดดังกล่าวในวรรคแรก ต้องด้วยลักษณะดังกล่าวในมาตรา 342[85] อนุมาตราหนึ่งอนุมาตราใดด้วย ผู้กระทำต้องระวางโทษจำคุกตั้งแต่หกเดือนถึงเจ็ดปี และปรับตั้งแต่หนึ่งหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท”

“ความผิดฐานฉ้อโกงประชาชน”เป็นความผิดความผิดที่แสดงถึงการเคลื่อนย้าย “สิทธิในทรัพย์”ด้วยการหลอกลวงประชาชนโดยทุจริต เพื่อให้ได้ไปซึ่งสิทธินั้นมาเป็นของตน

เมื่อพิจารณาจากบทบัญญัติในข้างต้นจะเห็นได้ว่าความผิดฐานฉ้อโกงประชนชนนั้นมีพื้นฐานของการกระทำความผิดมาจากความผิดฐานฉ้อโกงตามมาตรา 341 ที่เป็นการฉ้อโกงบุคคลซึ่งเป็นความผิดเฉพาะตัวและเป็นความผิดอันยอมความได้เพราะถือว่าความเสียหายที่เกิดขึ้นนั้นเป็นเรื่องเฉพาะตัวของบุคคล แต่ในความผิดฐานฉ้อโกงประชาชนนั้นแตกต่างออกไปเพราะการฉ้อโกงประชาชนนั้นถือเป็นเหตุฉกรรณ์อันยอมความมิได้ อีกทั้งเมื่อพิจารณาจากพฤติกรรมในการฟิชชิ่งจะทำให้ทราบได้ว่า“ฟิชชิ่ง”โดยทั่วไปแล้วมีจุดประสงค์หลอกลวงหรือปิดบังข้อความที่แท้จริงเพื่อให้ได้มาซึ่งข้อมูลของเหยื่อและนำข้อมูล ด้วยวิธีการส่งข้อความที่เป็นเท็จนั้นไปยังผู้เสียหายจำนวนครั้งละมากๆ โดยมิได้เลือกอย่างเฉพาะเจาะจงว่าเป็นใคร[86]

---

[84] คณิต ณ นคร (เชิงอรรถ 82) 443.

[85] ประมวลกฎหมายอาญา มาตรา 342 บัญญัติไว้ว่า “ถ้าในการกระทำความผิดฐานฉ้อโกง ผู้กระทำ (1) แสดงตนเป็นคนอื่น หรือ (2) อาศัยความเบาปัญญาของผู้ถูกหลอกลวงซึ่งเป็นเด็ก หรืออาศัยความอ่อนแอแห่งจิตของผู้ถูกหลอกลวง ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

[86] คณิต ณ นคร (เชิงอรรถ82) 444.

อนึ่ง ความผิดในมาตราดังกล่าวนั้นเป็นเรื่องฉ้อโกงด้วยการแสดงข้อความอันเป็นเท็จต่อประชาชน หรือด้วยการปกปิดข้อความจริงซึ่งควรจะบอกให้แจ้งแก่ประชาชน โดยประชาชนในที่นี้หมายถึงบรรดาพลเมืองหรือประชาชนเป็นการทั่วไปทั้งหลาย และไม่ได้ถือเอาจำนวนผู้เสียหายที่ถูกหลอกลวงมากหรือน้อยเป็นเกณฑ์[87] แต่ถือเอาเจตนาการแสดงข้อความอันเป็นเท็จหรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้งแก่ประชาชนโดยทั่วไปเป็นสำคัญ แม้มีคนทราบเพียงคนเดียวก็ผิดฐานนี้ได้[88]

อย่างไรก็ตาม เมื่อพิจารณาจากรูปแบบของการฟิชชิ่งแล้วนอกจากจะเป็นความผิดในฐานฉ้อโกง และฉ้อโกงประชาชนแล้ว การฟิชชิ่งนั้นอาจเป็นความผิดฐานอื่นๆตามพระมวลกฎหมายอาญา และตามพระราชบัญญัติอื่นๆที่มีการกำหนดโทษทางอาญา เป็นต้น อย่างไรก็ดีนอกจากตัวผู้กระทำผิดเองแล้วบุคคลอื่นที่มีส่วนร่วมในการกระทำความผิด ซึ่งเป็นผู้ที่อยู่ในกระบวนการในการกระทำความผิดก็ถือว่ามีความผิดตาม ประมวลกฎหมายอาญามาตรา มาตรา 83[89] หรือหากเป็นผู้บงการให้กระทำการ ก็จะถือว่ามีความผิดตามมาตรา 84[90] และหากเป็นผู้สนับสนุนให้มีการกระทำความผิดก็จะมีความผิดตามมาตรา 86[91] ด้วย

2.7.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขฉบับที่2 พ.ศ.2560

---

[87] ดู คำพิพากษาศาลฎีกาที่ 563/2531.

[88] ดู คำพิพากษาศาลฎีกาที่ 1867/2523.

[89] ประมวลกฎหมายอาญา มาตรา 83 บัญญัติว่า ในกรณีความผิดใดเกิดขึ้นโดยการกระทำของบุคคลตั้งแต่สองคนขึ้นไป ผู้ที่ได้ร่วมกระทำความผิดด้วยกันนั้นเป็นตัวการต้องระวางโทษตามที่กฎหมายกำหนดไว้สำหรับความผิดนั้น

[90] ประมวลกฎหมายอาญา มาตรา 84 บัญญัติว่า ผู้ใดก่อให้ผู้อื่นกระทำความผิดไม่ว่าด้วยการใช้ บังคับ ขู่เข็ญ จ้างวานหรือยุยงส่งเสริม หรือด้วยวิธีอื่นใด ผู้นั้นเป็นผู้ใช้ให้กระทำความผิด ถ้าความผิดมิได้กระทำลงไม่ว่าจะเป็นเพราะผู้ถูกใช้ไม่ยอมกระทำ ยังไม่ได้กระทำ หรือเหตุอื่นใด ผู้ใช้ต้องระวางโทษเพียงหนึ่งในสามของโทษที่กำหนดไว้สำหรับความผิดนั้น

[91] ประมวลกฎหมายอาญา มาตรา 86 บัญญัติว่า ผู้ใดกระทำด้วยประการใด ๆ อันเป็นการช่วยเหลือ หรือให้ความสะดวกในการที่ผู้อื่นกระทำความผิดก่อนหรือขณะกระทำความผิด แม้ผู้กระทำความผิดจะมิได้รู้ถึงการช่วยเหลือหรือให้ความสะดวกนั้นก็ตาม ผู้นั้นเป็นผู้สนับสนุนการกระทำความผิด ต้องระวางโทษสองในสามส่วนของโทษที่กำหนดไว้สำหรับความผิดที่สนับสนุนนั้น

โดยทั่วไปแล้วนั้นผู้ที่กระทำการฉ้อโกงหลอกลวงผู้อื่นเพื่อให้ได้มาซึ่งทรัพย์สิน ผู้ที่กระทำนั้นจะต้องได้รับโทษทางอาญาตามแต่ลักษณะแห่งการกระทำที่ได้บัญญัติให้เป็นความผิดในมาตรานั้นๆ เช่น หากเป็นกรณีการ ฉ้อโกงก็จะถือได้ว่าเป็นความผิดตามประมวลกฎหมายอาญา มาตรา 341 หรือหากเป็นการหลอกลวงเพื่อให้ได้มาซึ่งทรัพย์สินโดยการแสดงตนเป็นบุคคลอื่นก็จะถือเป็นความผิดฐานฉ้อโกงที่ต้องรับโทษหนักขึ้นตาม มาตรา 342 แต่หากเป็นกรณีที่เป็นการฟิชชิ่งที่เป็นทั้งการหลอกลวงและฉ้อโกง หรือในบางกรณีอาจมีการปลอมแปลง โดยจะกระทำผ่านโปรแกรมที่ให้บริการในรูปแบบต่างๆ ผ่านระบบคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ตซึ่งการกระทำความผิดประเภทนี้จะมีลักษณะที่พิเศษแตกต่างไปจากการกระทำความผิดทางกายภายทั่วไปในฐานความผิดอื่นๆ กล่าวคือการฉ้อโกงหลอกลวงผ่านระบบคอมพิวเตอร์หรือการฟิชชิ่ง จะทำให้ข้อมูลอันเป็นเท็จที่ฟิชเชอร์หรือผู้กระทำผิดนั้นสร้างขึ้นมาถูกส่งไปยังเหยื่อได้รวดเร็วขึ้นและสามารถส่งได้ทีละมากๆจนนำไปสู่การเกิดความเสียหายหายต่อประชาชนหรือแม้แต่ตัวภาครัฐเอง อีกทั้งในการควบคุมและกำหนดมาตรการป้องกันการกระทำความผิดทางคอมพิวเตอร์จำเป็นที่จะต้องใช้เทคนิคพิเศษในการแก้ปัญหาทางเทคนิคต่างๆที่เกิดขึ้นจากการกระทำความผิด ด้วยเหตุเช่นนี้จึงจำเป็นที่จะต้องมีการบัญญัติกฎหมายที่จะสามารถนำมาใช้เพื่อควบคุมการกระทำความผิดประเภทนี้ไว้เป็นการเฉพาะ ซึ่งกฎหมายดังกล่าวนั้น ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และแก้ไขฉบับที่2 พ.ศ.2560

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เริ่มต้นการจัดทำร่างพระราชบัญญัติขึ้นเมื่อปี พ.ศ.2541 โดยจัดทำภายใต้การควบคุมของคณะกรรมเทคโนโลยีสารสนเทศแห่งชาติ ซึ่งคณะผู้จัดทำร่างในขณะนั้นได้มีการพิจารณานำกฎหมายต่างประเทศและสนธิสัญญาต่างๆมาใช้ในการศึกษาเพื่อจัดทำร่างพระราชบัญญัติฉบับนี้ อันได้แก่ อนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์(Convention on Cyber Crime 2001) ของสภายุโรป, Computer Misuse Act 1990 ของประเทศสหราชอาณาจักร, Computer Misuse Act 1993 ของประเทศสิงค์โปร, Computer Misuse Act 1997 ของประเทศมาเลเซีย, Unauthorized Computer Access Law 2000 ของประเทศญี่ปุ่น, The Information Technology Act 2000 ของประเทศอินเดีย, German Penal Code ของประเทศเยอรมัน, United States Code ของประเทศสหรัฐอเมริกา โดยพระราชบัญญัติฉบับนี้ได้จัดทำจนแล้วเสร็จและประกาศในพระราชกิจจานุเบกษาเมื่อวันที่ 16 มิถุนายน พ.ศ.2550 และกฎหมายมีผลบังคับใช้ในวันที่ 19 กรกฎาคม พ.ศ.2550 เป็นต้นไป[92]

อนึ่ง เมื่อพิจารณาถึงสาเหตุที่จะต้องมีการบัญญัติพระราชบัญญัติฉบับนี้ก็เพราะว่าในขณะนั้นความแพร่หลายของอาชญากรรมคอมพิวเตอร์เริ่มที่จะเข้ามาสู่ประเทศไทยในขณะนั้น ซึ่งประเทศไทยในขณะนั้นยังไม่มีการกำหนดบทบัญญัติทางกฎหมายในมาใช้ลงโทษหรือกำหนดว่าควรทำเช่นไรกับการกระทำความผิดเช่นนี้เพราะลำพังเพียงฐานความผิดในประมวลกฎหมายอาญาไม่มีศักยภาพพอที่จะนำมาปรับใช้กับฐานความผิดที่กระทำผ่านทางระบบคอมพิวเตอร์เพราะด้วยเหตุที่ว่าในประมวลกฎหมายอาญาไม่ได้มีการบัญญัติฐานความผิดครอบคลุมไปถึงการใช้คอมพิวเตอร์ในการกระทำความผิดเหมือนอย่างใน German Penal

---

[92] มานิตย์ จุมปา, *คำอธิบายกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์* (พิมครั้งที่ 2, สำนักพิมพ์วิญญูชน 2554) 22-23.

Coad ของประเทศเยอรมันที่มีการกำหนดฐานความผิดเกี่ยวกับคอมพิวเตอร์ไว้ในประมวลกฎหมายอาญา ด้วยเหตุนี้เองจึงเป็นที่มาของการจัดทำร่างกฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์จนกระทั้งแล้วเสร็จและมีการประกาศใช้เป็นกฎหมาย[93]

โดยเจตนารมณ์ของกฎหมายฉบับนี้บัญญัติไว้เพื่อใช้ในการกำหนดฐานความผิดและบทลงโทษต่างๆสำหรับบุคคลใดก็ตามที่กระทำการอย่างหนึ่งอย่างใดอันถือได้ว่าเป็นการก่ออาชญากรรมทางคอมพิวเตอร์ [94] หรือใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด และความร่ายแรงนั้นต้องเป็นการกระทำไปในลักษณะที่ก่อให้เกิดความเสียหายต่อ องค์กรหรือหน่วยงานที่เป็นโครงสร้างพื้นฐานของประเทศ เช่น ระบบธนาคาร ระบบจัดการสาธารณูปโภคภายในประเทศ ระบบควบคุมการจราจรทางอากาศ หรือระบบจัดการข้อมูลของสถานพยาบาล เป็นต้น ซึ่งในบางครั้งไม่ใช้แค่การแทรกแซงหรือทำให้ระบบล่มเพียงเท่านั้น แต่อาจก่อให้เกิดผู้เสียชีวิตได้แม้จะไม่ใช่การกระทำทางกายภาพก็ตาม หรือที่เรียกกันว่าการโจมตีทางไซเบอร์ (Cyber attack) อันเข้าข่ายเป็นการก่ออาชญากรรมทางไซเบอร์ที่เป็นการพัฒนามาจากอาชญากรรมทางคอมพิวเตอร์ธรรมดา ซึ่งอาจจะส่งผลกระทบได้ในระดับประเทศ นอกจากนี้แล้ว พระราชบัญญัติฉบับนี้ก็ยังได้มีการกำหนดให้การฉ้อโกง หรือหลอกลวงทางอินเทอร์เน็ต เป็นความผิดตามพระราชบัญญัตินี้อีกด้วย แต่ไม่ว่าอย่างไรก็ตามหลักจากการประกาศบังคับใช้กฎหมายเรื่อยมาก็ได้เกิดปัญหาในเรื่องการตีความบทบัญญัติในเรื่องของการนำเข้าสู่ข้อความอันเป็นเท็จตามมาตรา 14(1) ที่ถูกนำไปใช้อย่างผิดวัตถุประสงค์ในการฟ้องร้องในคดีหมิ่นประมาททางคอมพิวเตอร์ทั้งที่โดยเจตนาที่แท้จริงของมาตรานี้ที่ถูกบัญญัติขึ้นมาก็เพื่ออุดช่องว่างของกฎหมายอาญาเรื่องการปลอมแปลงเอกสาร ซึ่งความผิดฐานปลอมเอกสาร ในประมวลกฎหมายอาญามีความหมายเฉพาะกระดาษหรือวัตถุอื่นใดที่มีรูปร่างและจับต้องได้เท่านั้น ยังไม่สามารถตีความให้ครอบคลุมการปลอมแปลงข้อมูลอิเล็กทรอนิกส์ได้ จนนำมาสู่การแก้ไขพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 โดยเฉพาะอย่างยิ่งในส่วนของมาตรา 14(1) ที่ได้มีการปรับปรุงแก้ไของค์ประกอบของฐานความผิดที่สะท้อนให้เห็นถึงปัญหาตลอดจนความเสียหายที่เกิดขึ้นจากเจตนาทุจริต, หลอกลวง, ฉ้อโกง, และปลอมแปลงทางคอมพิวเตอร์95 ซึ่งมีผลบังคับใช้ใน วันที่24 พฤษภาคม 2560

อย่างไรก็ดี เมื่อนำฐานความผิดตามมาตร 14 มาแยกองค์ประกอบความผิดจะพบว่า มาตราดังกล่าวไม่ได้ถูกออกแบบมาเพื่อใช้กับความผิดฐานหมิ่นประมาท และการเผยแพร่ข้อมูลข่าวสารที่ไม่เป็นความจริงยังไม่ถือเป็นความผิด จนกว่าการเผยแพร่ข้อมูลข่าวสารนั้นจะก่อให้เกิดความเสียหายต่อการรักษาความมั่นคงของรัฐ ความปลอดภัยสาธารณะ หรือ เป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร เป็นต้น

---

[93] ดู หมายเหตุท้ายพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550.

[94] ดู บทที่2, 2.2.3

[95] หนังสือจากนายกรัฐมนตรี เรื่อง เสนอร่างพระราชบัญญัติต่อประธานสภานิติบัญญัติแห่งชาต นร 0503/14561 (26 เมษายน 2559) 5-6.

2.7.2.1 ความผิดฐานนำเข้าข้อมูลคอมพิวเตอร์อันเป็นเท็จ ตามมาตรา 14

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์(ฉบับที่2) พ.ศ.2560 มาตรา 14 บัญญัติไว้ว่า “ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ.

(1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาท ตามประมวลกฎหมายอาญา.

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน.

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา.

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้.

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4) ถ้าการกระทำความผิดตามวรรคหนึ่ง (1) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้”

เมื่อพิจารณาจากบทบัญญัติข้างต้นนี้จะเห็นได้ว่าการกระทำที่เป็นความผิดตามบทบัญญัติมาตรานี้มีพื้นฐานมาจากประมวลกฎหมายอาญาแต่มีข้อแตกต่างในเรื่องการใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ซึ่งต่างจากการกระทำความผิดอาญาทั่วไปที่เป็นการกระทำในทางกายภาพและซึ่งก่อในเกิดผลกระทบต่อเนื้อตัวร่างกาย[96]

โดยเมื่อพิจารณาถึงองค์ประกอบในการกระทำความผิดตามมาตรานี้ จะเห็นได้ว่ามีองค์ประกอบพื้นฐานในการกระทำคือการนำเข้าสู่ระบบซึ่ง “ข้อมูลคอมพิวเตอร์” ซึ่งตามนิยามในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 ได้ให้นิยามของ คำว่า “ระบบคอมพิวเตอร์” และ “ข้อมูลคอมพิวเตอร์” ไว้ดังนี้

---

[96] พรเพรช วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550* (สถาบันพัฒนาข้าราชการฝ่ายตุลาการ ศาลยุติธรรม 2550) 21.

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานของอุปกรณ์เข้าด้วยกัน โดยมีการกำหนดชุดคำสั่ง หรือสิ่งอื่นใดอันเป็นแนวทางในการปฏิบัติงานของอุปกรณ์หรือชุดอุปกรณ์ที่ทำหน้าที่ในการประมวลผลข้อมูลอัตโนมัติ[97]

ดังนั้น คำว่า “ระบบคอมพิวเตอร์” ตามความหมายในพระราชบัญญัตินี้จึงหมายถึงบรรดาอุปกรณ์หรือชุดคำสั่งของอุปกรณ์ทางคอมพิวเตอร์ที่สามารถทำให้อุปกรณ์หรือชุดคำสั่งอื่นๆสามารถทำการประมวลผลร่วมกันได้เองโดยอัตโนมัติตามที่ได้มีการตั้งค่าโปรแกรมหรือชุดคำสั่งไว้แล้ว โดยการทำงานเช่นว่านั้นของระบบปราศจากการควบคุมของมนุษย์ กล่าวคือ ระบบสามารถทำงานได้เองโดยอัตโนมัติโดยที่ไม่จำเป็นต้องมีมนุษย์มาควบคุมตลอดเวลา[98] เช่น Laptop, เครื่องคอมพิวเตอร์เซิร์ฟเวอร์ (Computer server) เป็นต้น นอกจากนี้แล้วยังหมายรวมไปถึง อุปกรณ์ต่างๆที่มีซอร์ฟแวร์ที่ใช้ในการประมวลผลชุดข้อมูลได้อย่างคอมพิวเตอร์ เช่น โทรศัพท์มือถือ เป็นต้น แต่ไม่ว่าอย่างไรก็ตามจากที่ได้กล่าวไปในข้างต้นอุปกรณ์อิเล็กทรอนิกส์บางประเภทก็ไม่ถือเป็นระบบคอมพิวเตอร์เพราะ ไม่สามารถประมวลผลได้เองแต่เมื่อนำไปเชื่อมต่อกับอุปกรณ์อื่นๆที่จะสามารถประมวลผลอัตโนมัติได้ก็จะถือว่าเป็น “ระบบคอมพิวเตอร์” ตามนิยามของพระราชบัญญัตินี้ เช่น หน่วยเก็บข้อมูลแบบฮาดดิสก์ เป็นต้น

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล คำสั่ง ชุดคำสั่ง หรือทรัพยากรอื่นใดในระบบคอมพิวเตอร์ที่จะสามารถเรียกใช้เพื่อนำมาประมวลผลในระบบคอมพิวเตอร์ได้ ซึ่งในที่นี้รวมไปถึงข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ อย่างไรก็ดีหากพิจารณาจากเจตนารมณ์ตามมาตรา 14 อาจกล่าวได้ว่า ข้อมูล ชุดคำสั่ง ข้อความ หรือสิ่งอื่นใดที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ ซึ่งจัดเก็บไว้ในรูบแบบใดก็ตามที่ระบบคอมพิวเตอร์สามารถประมวลผลข้อมูลดังกล่าวได้ก็ถือว่าเป็นข้อมูลคอมพิวเตอร์ตามพระราชบัญญัตินี้

“การนำเข้าสู่ (Upload)” ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 นั้นไม่ได้มีการให้นิยามคำดังกล่าวไว้ แต่เมื่อพิจารณาจากความหมายโดยทั่วไปของคำว่า “นำเข้าสู่ (Upload)” อาจกล่าวได้ว่าเป็นการนำข้อมูลคอมพิวเตอร์เข้าสู่ระบบในรูปแบบใดๆก็ตามอันแสดงแสดงให้เห็นถึงพฤติการณ์ที่ผู้กระทำความผิดเป็นผู้นำข้อมูลคอมพิวเตอร์ไม่ว่าจะสร้างขึ้นใหม่หรือมีอยู่แล้วเข้าสู่ระบบด้วยเจตนาทุจริตหรือเพื่อเป็นการหาประโยชน์แก่ตน เพราะลำพังการสร้างข้อมูลหรือชุกคำสั่งขึ้นมาเพื่อเจตนาในการกระทำความผิดแต่ยังไม่นำเข้าสู่ระบบคอมพิวเตอร์นั้นไม่ถือเป็นความผิดเพราะยังไม่ได้มีการนำเข้าสู่ระบบคอมพิวเตอร์เป็นเพียงการตระเตรียมการเท่านั้น[99]

เมื่อพิจารณาจากที่ได้กล่าวมาในข้างต้นอาจสรุปได้ว่าความผิดตามมาตรานี้นั้นเป็นการนำข้อมูลต่างๆที่อยู่ในรูปแบบข้อมูลทางอิเล็กทรอนิกส์ทุกชนิด เข้าสู่ระบบคอมพิวเตอร์ หรือเครื่องมือ

---

[97] พระราชบัญญัติว่าด้วยการกระทำความเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตร 3.

[98] สำนักพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, *แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์* (สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ 2546) 16.

[99] มานิตย์ จุมปา (เชิงอรรถ 92) 95.

อิเล็กทรอนิกส์ที่สามารถใช้ในการประมวลผลชุดข้อมูลทางอิเล็กทรอนิกส์แล้วแสดงผลออกมาให้เราทราบได้ผ่านหน้าจอแสดงผล

อย่างไรก็ดีนอกจากการกำหนดให้ผู้ที่นำเข้าข้อมูลเข้าสู่ระบบคอมพิวเตอร์ตามความในบทบัญญัติ มาตรา 14 (1)-(5) จะต้องรับผิดตามกฎหมายแล้วนั้นผู้ที่ส่งต่อข้อมูลหรือนำไปเผยแพร่ต่อก็ต้องรับผิดเช่นเดียวกันกับผู้กระทำ หากปรากฏว่าการส่งต่อนั้นกระทำไปโดยรู้อยู่แล้วว่าข้อมูลที่ส่งต่อนั้นมีเนื้อหาที่เป็นความผิดตามมาตรา 14

2.7.2.2 ความผิดฐานดักรับข้อมูลคอมพิวเตอร์ตาม มาตรา 8

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550มาตรา 8 บัญญัติไว้ว่า “ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้ มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือ ทั้งจำทั้งปรับ”[100]

เมื่อพิจารณาจากพฤติกรรมและลักษณะในการประกอบอาชญากรรมคอมพิวเตอร์ประเภทการฟิชชิ่งดังที่ได้กล่าวไว้ในหัวข้อ 2.4.4 จะทำให้ทราบได้ว่าพฤติกรรมของการ “ฟิชชิ่ง” โดยทั่วไปแล้วมีจุดประสงค์เพื่อให้ได้มาซึ่งข้อมูลของเหยื่อ ด้วยเหตุนี้เองการกระทำความผิดประเภทการฟิชชิ่งจึงมีความเกี่ยวข้องกับมาตรา 8[101]ซึ่งผู้เขียนจะได้อธิบายความสัมพันธ์ของฟิชชิ่งตามองค์ประกอบความผิดดังนี้

“โดยมิชอบ”หมายความว่า การกระทำอันเกิดขึ้นด้วยเจตนาทุจริตซึ่งกระทำไปโดยไม่มีสิทธิในการกระทำเช่นนั้น ซึ่งตามนัยของมาตรา8 คือการกระทำโดยอาศัยวิธีการทางอิเล็กทรอนิกส์ซึ่งตัวผู้กระทำมีความสามารถและเทคโนโลยีทางคอมพิวเตอร์ชั้นสูงในการเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ ส่วนบุคคล หรือองค์กร เพื่อดักรับข้อมูลระหว่างอุปกรณ์อิเล็กทรอนิกส์ของเหยื่อและผู้ให้บริการเครือข่าย โดยปราศจากสิทธิในการกระทำเช่นว่านั้น

เมื่อพิจารณาจากบริบทของการฟิชชิ่งที่มีลักษณะขั้นตอนในการหลอกลวงเหยื่อด้วยวิธีการสร้างเว็บไซต์ปลอม หรือการเปลี่ยนเส้นทางการค้นหาของเหยื่อมายังเว็บไซต์ปลอมของผู้กระทำความผิดที่ได้เตรียมการไว้โดยเฉพาะ หรือการส่งลิงค์ข้อความเพื่อหลอกลวงเหยื่อให้หลงเชื่อต่างก็แสดงให้เห็นการกระทำอันเป็นเจตนาโดยมิชอบทั้งสิ้น

“การใช้วิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่ง” หมายความว่า การใช้เทคนิคทางคอมพิวเตอร์ขั้นสูงในการดักรับข้อมูลระหว่างอุปกรณ์อิเล็กทรอนิกส์ซึ่งโดยทั่วไปมักจะกระทำโดยการแทรกแซงการส่งข้อมูลระหว่าอุปกรณ์ในเครือข่ายอินเทอร์เน็ตสาธารณะ (Free Wi-Fi) ที่ไม่ได้มีการกำหนดสิทธิการเข้าใช้เครือข่ายไว้เป็นการเฉพาะ

---

[100] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 8.

[101] ดูประกอบ คำอธิบายมาตรา8 ใน คณาธิป ทองรวีวงศ์, *กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม1: ภาคความผิดต่อระบบและข้อมูลคอมพิวเตอร์*(สำนักพิมพ์นิติธรรม 2563) 260-274.

เมื่อพิจารณาจากบริบทของการฟิชชิงจะเห็นได้ว่าการกระทำในลักษณะนี้ในทางวิชาการนั้นถือได้ว่าเป็นการ ฟิชชิ่ง ชนิดหนึ่งซึ่งมีชื่อเรียกในทางเทคนิคว่า Malware based Phishing หรือ Man-in-the-Middle Phishing

“ข้อมูลคอมพิวเตอร์อันมิได้มีไว้เพื่อประโยชน์สาธารณะ” หมายความว่า ข้อมูลซึ่งห้ามมิให้เผยแพร่โดยมิได้รับอนุญาต ซึ่งหมายรวมไปถึงข้อมูลส่วนบุคคลและข้อมูลอ่อนไหว[102](Sensitive data)

เมื่อพิจารณาจากบริบทของการฟิชชิงจะเห็นได้ว่าข้อมูลที่เป็นเป้าหมายของการฟิชชิ่งล้วนแล้วแต่เป็นข้อมูลส่วนบุคคล และข้อมูลในการยืนยันสิทธิในการเข้าถึงระบบ(credential) ซึ่งมิได้มีไว้เพื่อประโยชน์สาธารณะ นอกจากนี้ข้อมูลมือถือยังถือได้ว่าเป็นข้อมูลส่วนบุคลอีกด้วย

2.7.2.3 ความผิดฐานส่งจดหมายอิเล็กทรอนิกส์ไม่พึงประสงค์ มาตรา 11

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 มาตรา 11 วรรคหนึ่ง บัญญัติไว้ว่า “ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบ คอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ปรับไม่เกินหนึ่งแสนบาท”[103]

เมื่อพิจารณาจากบทบัญญัติและพฤติกรรมในการประกอบอาชญากรรมคอมพิวเตอร์ประเภทการฟิชชิ่งจะเห็นได้ว่าการกระทำความผิดดังบทบัญญัติข้างต้นถือได้ว่าเป็นกระบวนการพื้นฐานในการประกอบอาชญากรรมคอมพิวเตอร์ประเภทฟิชชิ่งกล่าวคือเป็นจุดเริ่มต้นซึ่งถือเป็นพื้นฐานของการฟิชชิ่งคือการส่งจดหมายอิเล็กทรอนิกส์จำนวนมากไปยังอีเมลของผู้เสียหายจำนวนมากโดยไม่เจาะจงผู้เสียหายไว้เป็นการเฉพาะ(Phishing Mail) โดยทั่วไปนั้นการส่งจดหมายอิเล็กทรอนิกส์ประเภทนี้มักจะไม่ปรากฏชื่อผู้ส่ง หรือมีการปกปิด, ปลอมแปลงแหล่งที่มาเพื่อให้เกิดการสับสนและเข้าใจผิดในแหล่งที่มาของจดหมายอิเล็กทรอนิกส์เนื่องจากเป้าหมายของผู้ที่ส่งนั้นเพียงต้องการให้ผู้รับนั้นได้เห็นหรือรับรู้ข้อความเท่านั้น[104] ด้วยเหตุนี้เองการกระทำความผิดตามมาตรา 11 วรรคหนึ่ง จึงมีความเกี่ยวข้องกับการกระทำความผิดประเภทการฟิชชิ่ง

โดยในการกระทำความผิดฐานนี้เมื่อพิจารณาปรับเข้าองค์ประกอบความผิดเกี่ยวกับการฟิชชิ่งซึ่งมีในบางกรณีที่ฟิชเชอร์มีขั้นตอนที่ฟิชเชอร์ประสงค์ติดต่อสื่อสารกับผู้เสียหายในกรณีใช้อีเมล์หรือใช้อีเมล์ร่วมกับเว็บไซต์ปลอมฟิชเชอร์จะส่งจดหมายอิเล็กทรอนิกส์ทั้งหมดออกไปยังผู้เสียหายตามข้อมูลที่มีอยู่ โดยมีทั้งข้อความในจดหมายอิเล็กทรอนิกส์ที่สวยงามเสมือนของจริงโดยไม่เปิดโอกาสให้ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์สามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับ

---

[102] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26.

[103] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์(ฉบับที่2) พ.ศ.2560 มาตรา 11.

[104] สาวตรี สุขศรี, *กฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์และอาชญากรรมทางไซเบอร์* (พิมพ์ครั้งที่ 2, สำนักพิมพ์เดือนตุลา 2563) 265.

ได้ ทั้งนี้เป็นไปตามที่รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนดแนวทางเกี่ยวกับลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการของการส่ง[105]

[105] กุลธิดา อาธิเจริญสุข, ‘การบังคับใช้กฎหมายเกี่ยวกับฟิชชิ่ง’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต สถาบันบัณฑิตพัฒนบริหารศาสตร์ 2559) 135.

บทที่ 3
กฎหมายต่างประเทศที่เกี่ยวกับการฟิชชิ่ง

จากที่ผู้เขียนได้กล่าวไปในบทที่แล้วถึงเรื่องความรับผิดทางอาญา, แนวคิด, ความหมาย, ลักษณะ, และผลกระทบซึ่งรวมไปถึงความเสียหายที่เกิดขึ้นจากการก่ออาชญากรรมคอมพิวเตอร์ในรูปแบบฟิชชิ่ง ดังที่ได้กล่าวไปแล้วนั้น ดังนั้น ในบทนี้ผู้เขียนจะกล่าวถึงเรื่องกฎหมายเกี่ยวกับฟิชชิ่งของประเทศต่างๆ เช่น ประเทศสหรัฐอเมริกา เยอรมัน ฝรั่งเศส และอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ เพื่อให้สามารถดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับฟิชชิ่งได้อย่างเหมาะสม ทั้งนี้เพื่อเป็นการศึกษานำข้อดีของกฎหมายต่างประเทศมาใช้เป็นแนวทางในการปรับปรุงแก้ไขกฎหมายของประเทศไทยที่เกี่ยวข้องกับการก่ออาชญากรรมคอมพิวเตอร์ในรูปแบบฟิชชิ่งให้สามารถบังคับใช้ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

3.1 กฎหมายประเทศสหรัฐอเมริกา

ปัจจุบันในกฎหมายรัฐบาลกลาง (Federal Law) ของประเทศสหรัฐอเมริกายังไม่ได้มีการออกกฎหมายป้องกันฟิชชิ่งที่ถูกนำมาบังคับใช้ในระดับรัฐภายในประเทศโดยตรงจึงทำให้ในปัจจุบันการบังคับใช้กฎหมายเกี่ยวกับฟิชชิ่งในระดับรัฐนั้นอยู่ภายใต้กฎหมาย Identity Theft and Assumption Deterrence Act of 1998 ที่แก้ไขเพิ่มเติมจาก Computer Fraud and Abuse Act of 1984 (CFAA) ซึ่งเป็นกฎหมายเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์ ซึ่งได้รับการบัญญัติไว้ใน United States Code. Title 18 Chapter 47 §1030(a)(4) แต่ไม่ว่าอย่างไรก็ตามเนื่องจากบทบัญญัติเดิมในเรื่องข้อมูลส่วนบุคคลนั้นถูกกำหนดไว้ว่าต้องอยู่ในรูปแบบของเอกสารเท่านั้น ส่งผลให้การฉ้อโกงเอกสารข้อมูลส่วนบุคคล (Identification document) โดยการทำขึ้น ใช้ หรือโอนเอกสารดังกล่าวเป็นความผิดทางอาญาถูกจำกัดไว้เพียงแค่การกระทำต่อตัวเอกสารเพียงเท่านั้น ด้วยเหตุนี้เองจึงได้มีการแก้ไขเพิ่มเติมใน Identity Theft and Assumption Deterrence Act of 1998. §1028(a)(7) ให้มีความครอบคลุมไปถึงการฉ้อโกงข้อมูลส่วนบุคคลของผู้อื่นและนำไปใช้ในทางที่มิชอบเป็นความผิดในทางอาญา ไม่ว่าข้อมูลนั้นจะปรากฏอยู่บนเอกสารหรือไม่ก็ตามโดยมีโทษจำคุกไม่เกิน 10 ปี หรือหากเป็นกรณีให้ความช่วยเหลือกลุ่มก่อการร้ายข้ามชาติมีโทษจำคุกไม่เกิน 25 ปี[106] อย่างไรก็ดีแม้บทบัญญัตินี้มิได้มีการกล่าวถึงการฟิชชิ่งโดยตรงแต่ในองค์ประกอบความผิดของบทบัญญัตินี้ก็ครอบคลุมถึงวิธีการต่างๆที่ฟิชเชอร์นั้นใช้ในการฟิชชิ่ง อาทิ การโจรกรรมข้อมูลประจำตัวบุคคล(Identity Theft) และ

---

[106] U.S. Code Title 18, ch47 §1028(a)(7) the term “knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.”

อาชญากรรมฉ้อฉลอื่นๆ ที่เกี่ยวข้องซึ่งองค์ประกอบความผิดเหล่านี้เองสามารถนำมาปรับใช้เพื่อเอาผิดกับการฟิชชิ่งได้[107]

อนึ่ง นอกจากบทบัญญัติดังที่ได้กล่าวไปในข้างต้นใน §1029[108] ของกฎหมายฉบับเดียวกันนี้เองก็ยังได้กำหนดให้การปลอมแปลงหรือลอกเลียนเครื่องมือที่ใช้ในการเข้าถึง[109] (Access Device) ไม่ว่าจะอยู่ในรูปแบบใดก็ตาม โดยกำหนดให้เป็นความผิดต่อบุคคลที่ผลิต ใช้ หรือค้าเครื่องมือที่ใช้ในการเข้าถึงโดยมีเจตนาฉ้อโกงในการกระทำมีโทษจำคุก 10 ปี อีกทั้งยังกำหนดให้บุคคลที่ผลิต ใช้ หรือค้าซอฟท์แวร์หรือฮาร์ดแวร์ที่ใช้สำหรับการเข้าถึงโดยมิชอบมีโทษจำคุกไม่เกิน 15 ปี หรือทั้งจำทั้งปรับตามที่กฎหมายกำหนดซึ่งรวมไปถึงการยึดทรัพย์ที่มีไว้ใช้หรือเพื่อที่จะใช้ในการกระทำความผิดและเมื่อพิจารณาจากลักษณะในการฟิชชิ่งด้วยวิธีการส่งจดหมายอิเล็กทรอนิกส์จะเห็นได้ว่าจุดมุ่งหมายในการกระทำของ ฟิชเชอร์นั้นคือการหลอกลวงเพื่อให้ได้ไปซึ่งรหัสที่ใช้ในการเข้าถึงข้อมูล เลขประจำตัวบุคคล เลขบัญชีธนาคาร หรือเครื่องมือยืนยันตัวตนอื่นๆ ซึ่งทั้งหมดนี้ล้วนเป็นเครื่องมือที่ใช้ในการเข้าถึงตามความหมายของบทบัญญัติข้างต้น ด้วยเหตุนี้เองบทบัญญัตินี้จึงสามารถที่จะนำมาบังคับใช้กับการพิชชิ่งของฟิชเชอร์ได้[110] แต่ไม่ว่าอย่างไรก็ตามแม้ว่าบทบัญญัติในกฎหมายดังที่ได้กล่าวมาในข้างต้นจะสามารถนำมาใช้ดำเนินคดีกับผู้กระทำความผิดได้แต่ก็สามารถนำมาใช้ได้เพียงบางกรณีเพียงเท่านั้นกล่าวคือจากการศึกษาผู้เขียนพบว่าบทบัญญัติทั้งสามดังที่ได้กล่าวมาในข้างต้นนั้นไม่ได้ถูกบัญญัติมาเพื่อใช้กับการฟิชชิ่งโดยตรงด้วยเหตุนี้เองในปี ค.ศ.2003 จึงได้มีการออกกฎหมาย Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. (CAN-SPAM Act) ซึ่งเป็นกฎหมายที่มีวัตถุประสงค์เพื่อกำหนดฐานบทลงโทษเพิ่มเติมจากใน U.S. Code Title 18, ch47 §1037.และเพื่อใช้ในการควบคุมการส่งจดหมายอิเล็กทรอนิกส์กล่าวคือเป็นกฎหมายที่ใช้ในการควบคุมการส่งจดหมายอิเล็กทรอนิกส์ที่เชิงพานิชย์[111]ที่ไม่พึงประสงค์ อันมีเนื้อหาสำคัญอยู่ที่ §7704 ที่มีเนื้อหาเกี่ยวกับการห้ามมิให้ใช้จดหมายอิเล็กทรอนิกส์เพื่อเป็นเครื่องมือในการหลอกลวงผู้อื่นหรือทำให้เข้าใจผิดในเนื้อหาด้วยการส่งจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาอันเป็นเท็จในสาระสำคัญของข้อความเพื่อหลอกลวงผู้อื่น หรือส่งจดหมายอิเล็กทรอนิกส์ที่มีความเกี่ยวข้องกับการทำธุรกรรมใดๆไปยังคอมพิวเตอร์เครื่องอื่นหากหัวเรื่องหรือเนื้อหาใน

---

[107] สาวตรี สุขศรี (เชิงอรรถ 104) 288.

[108] 18 US Code § 1029.

[109] เครื่องมือที่ใช้ในการเข้าถึง หมายถึง เครื่องมือหรือข้อมูลอื่นใดที่สามารถใช้ในการยืนยันหรือระบุตัวตนของบุคคลเพื่อใช้ในการเข้าถึงบัญชีส่วนบุคคลไม่ว่าจะเป็น บัตรเครดิต รหัสผ่าน เลขประจำตัวประชาชน เลขบัญชีธนาคาร

[110] ดู ผาสุก เจริญเกียรติ, ‘Identity Theft อาชญากรรมใกล้ตัว’ (2552) 1 ดุลพาห 56, 169.

[111] จดหมายอิเล็กทรอนิกส์ที่เชิงพานิชย์ ตามความหมายใน U.S. Code Title 18, ch47 §1037(d)(3) หมายถึง ข้อความอีเมลอิเล็กทรอนิกส์มากกว่า 100 ข้อความในช่วงเวลา 24 ชั่วโมง หรือข้อความอีเมลอิเล็กทรอนิกส์มากกว่า 1,000 ข้อความในช่วงเวลา 30 วัน หรือส่งข้อความอิเล็กทรอนิกส์มากกว่า 10,000 ข้อความในระยะเวลา 1 ปี

จดหมายที่ส่งไปมีลักษณะเป็นเท็จอันนำไปสู่การสำคัญผิดในสาระสำคัญของข้อความ ต้องระวางโทษจำคุกไม่เกิน 5 ปีหรือปรับตามที่กฎหมายกำหนดไว้ใน U.S. Code Title 18, ch47 §1037(b)[112].

3.1.1 กฎหมายของรัฐแคลิฟอร์เนีย

มลรัฐแคลิฟอร์เนียถือได้ว่าเป็นมลรัฐแรกที่มีการบัญญัติกฎหมายต่อต้านฟิชชิ่งขึ้นมาใช้อย่างจริงจัง โดยกฎหมายดังกล่าว คือ California Codes Business and Professions Code Chapter 33 – Anti Phishing Act of 2005 โดยกฎหมายดังกล่าวนี้กำหนดให้ความผิดฐานฟิชชิ่งเป็นความความผิดตั้งแต่ขั้นตอนของการหลอกลวงเหยื่อเพื่อให้ได้ไปซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล โดยไม่จำเป็นว่าข้อมูลดังกล่าวจะต้องถูกนำไปใช้ประโยชน์กล่าวคือในบทบัญญัตินี้นั้นกำหนดให้การหลอกลวงเพื่อให้ได้ไปซึ่งข้อมูลยืนยันตัวบุคคลเป็นความผิด เนื่องจากเจตนารมณ์ของกฎหมาย คือ เพื่อต้องการที่จะคุ้มครองป้องกันข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการทำธุรกรรมทางการเงินซึ่งรวมไปถึงรหัสผ่านที่ใช้ในการเข้าถึงบัญชีส่วนบุคคลหรือธุรกรรมอื่นๆ ซึ่งมีบทบัญญัติสำคัญดังนี้

มาตรา 22948.2[113]

“บุคคลใดกระทำการโดยปราศจากอำนาจหรือได้รับความยินยอมจากผู้ประกอบธุรกิจ โดยการใช้เว็บไซต์ จดหมายอิเล็กทรอนิกส์ หรือบริการอื่นๆทางอินเทอร์เน็ต เพื่อเรียกร้อง ร้องขอ หรือดำเนินการใดๆ อันเป็นการชักจูงบุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล ด้วยการแอบอ้างเป็นตัวแทนทางธุรกิจ ผู้นั้นถือว่ากระทำการมิชอบด้วยกฎหมาย”

มาตรา 22948.3[114]

(A) บุคคลดังต่อไปนี้อาจดำเนินคดีกับบุคคลฝ่าฝืนมาตรา 22948.21

---

[112] U.S. Code Title 18, ch47 §1037(b)Penalties.—The punishment for an offense under subsection (a) is—

(1) a fine under this title, imprisonment for not more than 5 years, or both, if—

(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system.

[113] CA Bus & Prof Code § 22948.2 (2022) “It shall be unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business.”

[114] See. CA Bus & Prof Code § 22948.3 (2022)

(1) บุคคลผู้ซึ่ง (a) มีส่วนร่วมในธุรกิจอินเทอร์เน็ตสาธารณะ หรือเป็นเจ้าของเว็บเพจหรือเป็นเจ้าของเครื่องหมายการค้า และ (b) ได้รับผลกระทบจากการละเมิดมาตรา 22948.2

ภายใต้บทบัญญัติในวรรคนี้ผู้เสียหายอาจเรียกร้องค่าเสียหายได้มากกว่าค่ามูลค่าความเสียหายที่เกิดขึ้น หรือเป็นเงินจำนวน 500,000 ดอลลาร์สหรัฐ

(2) บุคคลที่ได้รับผลกระทบจากการละเมิดมาตรา 22948.2 อาจฟ้องร้องเพื่อดำเนินคดีต่อศาลได้ แต่การฟ้องนั้นจะต้องเป็นการฟ้องบุคคลที่ละเมิดต่อมาตรา 22948.2 เท่านั้น

ภายใต้บทบัญญัติในวรรคนี้ผู้เสียหายตามมาตร 22948.2 อาจเรียกร้องค่าเสียหายเพิ่มเติมได้มากกว่าสามเท่าของความเสียหายแท้จริง หรือ 5,000 ดอลลาร์ ต่อการกระทำละเมิดหนึ่งครั้ง

(B) อัยการสูงสุดหรืออัยการเขตอาจดำเนินคดีเพิ่มเติมกับบุคคลที่กระทำความผิดหรือสมรู้ร่วมคิดในการกระทำความผิดตามมาตรา 22948.2 ได้โดยการกำหนดโทษปรับทางแพ่งเป็นเงินจำนวนไม่เกินกว่า 2,500 ดอลลาร์ ต่อการกระทำละเมิดหนึ่งครั้ง

(C) ภายใต้บทบัญญัตินี้ ศาลอาจดำเนินการอย่างใดอย่างหนึ่งหรือทั้งสองอย่างได้ดังต่อไปนี้

(1) เพิ่มจำนวนมูลค่าความเสียหายที่ผู้เสียหายสามารถเรียกร้องได้เป็นจำนวนสูงสุดไม่เกินกว่าสามเท่าของความเสียหายที่สามารถเรียกร้องได้ภายใต้ (A) ในกรณีที่จำเลยมีส่วนร่วมในการกระทำความผิดตามมาตรา 22948.2

(2) กำหนดจำเลยจ่ายค่าธรรมเนียมศาลและค่าทนายตามที่เหมาะสมในการดำเนินคดีแก่โจทก์

(D) การเรียกร้องค่าเสียหายตามบทบัญญัตินี้ไม่เป็นการตัดสิทธิในการเรียกร้องค่าเสียหายตามกฎหมายอื่น

(E) เพื่อให้เป็นไปตามเจตนารมณ์ของ (1) ในอนุมาตรา (A) ให้ถือว่าการกระทำละเมิดตามมาตรา 22948.2 เพียงครั้งเดียวที่ก่อให้เกิดความเสียหายหลายอย่างเป็นการฝ่าฝืนบทบัญญัติเพียงครั้งเดียว”

3.1.2 กฎหมายของรัฐนิวยอร์ก

ก่อนปี 2006 กฎหมายภายในรัฐนิวยอร์กนั้นไม่ได้มีการบัญญัติกฎหมายที่ใช้บังคับกับการกระทำความผิดเกี่ยวกับการส่งจดหมายสแปมเมลหรือฟิชชิ่งโดยตรง แต่ไม่ว่าอย่างตามเนื่องจากผลกระทบร้ายแรงที่เกิดขึ้นจากการก่ออาชญากรรมประเภทนี้ที่เพิ่มมากขึ้นจึงเป็นเหตุให้ในปี 2006 รัฐนิวยอร์กได้ออกกฎหมายต่อต้านฟิชชิ่ง[115]ซึ่งเป็นส่วนหนึ่งของกฎหมายธุรกิจทั่วไปแห่งรัฐนิวยอร์ก (New York General Business) ซึ่งกำหนดไว้ใน Article 26 – Anti Phishing Act of 2006.[116]โดยกฎหมายดังกล่าวนี้กำหนดให้การใช้อีเมลหรือช่องทางสื่อสารในอินเทอร์เน็ตเป็นเครื่องมือในการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลที่ระบุตัวบุคคล เช่น

---

[115] See 2006 Session Laws of New York, Chapter 64 (A 8025-C).

[116] N.Y. General Business Law, Article 26 (§ 390-B).

หมายเลขประกันสังคม หมายเลขบัญชีธนาคาร หรือหมายเลขบัตรเครดิต เป็นความผิด[117]ซึ่งมีมาตราสำคัญดังนี้

มาตรา 390-B[118]

1. มาตรานี้เรียกว่า กฎหมายต่อต้านฟิชชิ่ง ปี 2006

2. ในมาตรานี้คำต่อไปนี้มีความหมายว่า

“ข้อความอิเล็กทรอนิกส์” หมายถึง ข้อความที่ถูกส่งไปยังที่อยู่อีเมลไม่ซ้ำกันเป็นจำนวนมากโดยไม่จำกัดวิธีการในการส่ง

“ข้อมูลระบุตัวตน” หมายถึง หมายเลขประกันสังคมของบุคคล, เลขที่ใบอนุญาตขับรถ, เลขที่บัญชีธนาคาร, หมายเลขบัตรเครดิตหรือบัตรเดบิต, หมายเลขประจำตัวส่วนบุคคล (PIN), ลายเซ็นอิเล็กทรอนิกส์, ข้อมูลไบโอเมตริกซ์, รหัสผ่านบัญชี หรือ ข้อมูลอื่นใดที่สามารถใช้เพื่อเข้าถึงบัญชีทางการเงินที่ใช้ในการประกอบธุรกรรมทางการเงิน

“อินเทอร์เน็ต” หมายถึง เครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่มีการเชื่อมต่อระหว่างเครือข่ายหลาย ๆ เครือข่ายทั่วโลก โดยมีภาษาที่ใช้สื่อสารกันระหว่างคอมพิวเตอร์ที่เรียกว่า โพรโทคอล (protocol) ซึ่งใช้ในการส่งและรับข้อมูลผ่านทางสายสัญญาณหรือสัญญาณอินเทอร์เน็ต

“เว็บเพจ” หมายถึง การจัดเตรียมข้อความหลายมิติที่จะนำไปสู่ เว็บเพจอื่น ผ่านทางลิงก์ เว็บเบราว์เซอร์จะที่ประสานงานกับทรัพยากรเว็บที่เชื่อมต่อระหว่างเครือข่ายหลายๆ เครือข่ายทั่วโลก

3. บุคคลใดกระทำการผ่านทางเว็บเพจหรือส่งผ่านข้อความอิเล็กทรอนิกส์หรือใช้วิธีการทางอิเล็กทรอนิกส์ในรูปแบบใดๆก็ตามเพื่อร้องขอหรือเพื่อทำให้ทราบถึงข้อมูลที่ระบุตัวตนได้โดยการหลอกลวงหรือทำให้สำคัญผิดว่าเป็นตัวแทนทางธุรกิจ หรือเป็นหน่วยงานของรัฐ โดยปราศจากอำนาจกระทำการหรือได้รับคำยินยอมจากผู้ประกอบธุรกิจหรือหน่วยงานที่แท้จริง บุคคลนั้นถือว่ากระทำการละเมิดต่อกฎหมาย

4. (A) อัยการสูงสุดหรือบุคคลผู้ที่มีส่วนได้เสียในธุรกิจอินเทอร์เน็ตสาธารณะ เจ้าของเว็บเพจหรือเจ้าของเครื่องหมายการค้า และผู้ที่ได้รับความเสียหายจากการกระทำละเมิดต่อบทบัญญัตินี้ สามารถดำเนินการดังต่อไปนี้กับผู้ที่ฝ่าฝืนบทบัญญัตินี้ ได้ดังนี้

(1) กำหนดเงื่อนในการลงโทษต่อบุคคลที่ฝ่าฝืนบทบัญญัติใน 3. และ

(2) เรียกร้องค่าเสียหาย

(2.1) ตามความเสียหายแท้จริงที่เกิดขึ้น หรือ

(2.2) 1,000 ดอลลาร์ ต่อการกระทำละเมิดหนึ่งครั้ง

(B) ในการดำเนินการตาม (A) ศาลอาจจะ

---

[117] Cornell Law School, ‘NEW YORK Commercial Email and Spam’ (Cornell Law School) <https://www.law.-cornell.edu/wex/inbox/new_york> สืบค้นเมื่อ 25 มีนาคม 2566.

[118] NY Gen Bus L § 390-B (2022)

(1) กำหนดค่าเสียหายสูงสุดเป็นจำนวนกว่าสามเท่า จากที่จะต้องได้รับตาม a) ในกรณีที่พบว่าจำเลยมีส่วนร่วมในการกระทำอันเป็นการละเมิดต่อ 3. ในบทบัญญัตินี้

(2) กำหนดให้จำเลยจ่ายค่าธรรมเนียมศาลและค่าทนายตามที่เหมาะสมในการดำเนินคดีแก่โจทก์

5. การเรียกร้องค่าเสียหายตามบทบัญญัตินี้ไม่เป็นการตัดสิทธิในการเรียกร้องค่าเสียหายตามกฎหมายอื่น

อย่างไรก็ดีในกฎหมายของรัฐนิวยอร์กไม่เพียงแค่กำหนดให้การกระทำความฐาน ฟิชชิ่งตาม §390-B Anti Phishing Act of 2006 เป็นความผิดแต่ยังได้มีการกำหนดให้การแอบอ้างเป็นบุคคลอื่นทางเว็บไซต์อินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์เป็นอาชญากรรมระดับสองตามกฎหมายอาญาของรัฐนิวยอร์ก โดยกำหนดไว้ใน New York Penal Law, Article 190 (§ 190.25(4)).[119]

3.1.3 กฎหมายรัฐเทนเนสซี

รัฐเทนเนสซีถือได้ว่าเป็นรัฐที่มีการบัญญัติกฎหมายต่อฟิชชิ่งขึ้นมาใช้อย่างจริงจังโดยบัญญัติไว้ใน Tennessee Code, Title 47, Chapter 18 - CONSUMER PROTECTION Part 52 ANTI - PHISHING ACT OF 2006 ซึ่งเป็นบทบัญญัติที่มีเจตนารมณ์เพื่อใช้ในการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับการฟิชชิ่ง สำหรับบุคคลใดก็ตามที่กระทำการหลอกลวงหรือทำให้เข้าใจผิดเพื่อแสดงตนเป็นผู้แทนหรือบุคคลอื่นโดยปราศจากความยินยอมจากบุคคลดังกล่าวผ่านทางอินเทอร์เน็ต การส่งจดหมายอิเล็กทรอนิกส์หรือวิธีการทางอิเล็กทรอนิกส์อื่นๆซึ่งรวมไปถึงการติดต่อสื่อสารในช่องทางอื่นเพื่อร้องขอหรือกระทำด้วยประการใดๆเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล ซึ่งมีบทบัญญัติสำคัญดังนี้

มาตรา 47-18-2503[120]

(A) การกระทำการหลอกลวงหรือทำให้เข้าใจผิดเพื่อแสดงตนเป็นผู้แทนหรือบุคคลอื่นโดยปราศจากความยินยอมจากบุคคลดังกล่าวผ่านทางอินเทอร์เน็ต การส่งจดหมายอิเล็กทรอนิกส์หรือวิธีการทางอิเล็กทรอนิกส์อื่นๆซึ่งรวมไปถึงการติดต่อสื่อสารในช่องทางอื่นเพื่อร้องขอหรือกระทำด้วยประการใดๆเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล หรือ เอกสารส่วนบุคคล

(B) บุคคลใดกระทำการมิชอบด้วยกฎหมายโดยปราศจากอำนาจหรือความยินยอมจากบุคคลผู้ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล โดยมีเจตนาฉ้อฉลในการใช้ข้อมูลส่วนบุคคลเพื่อตนเองหรือบุคคลอื่นหรือเพื่อจำหน่ายหรือแจกจ่าย

---

[119] N.Y. Penal Law, §190.25(4). “A person is guilty of criminal impersonation in the second degree when.

(4) Impersonates another by communication by internet website or electronic means with intent to obtain a benefit or injure or defraud another, or by such communication pretends to be a public servant in order to induce another to submit to such authority or act in reliance on such pretense.”

[120] Tenn. Code § 47-18-5203.

(1) เพื่อให้ได้มาซึ่งบันทึกหรือข้อมูลที่ช่วยในการเข้าถึงข้อมูลทางการเงิน เอกสารข้อมูลส่วนบุคคลหรือประโยชน์ของบุคคนอื่น

(2) เพื่อให้ได้รับสินค้าหรือบริการโดยการใช้ข้อมูลระบุตัวตนของบุคคลอื่น

(3) เพื่อให้ได้รับเอกสารแสดงระบุตัวตนในนามของบุคคลอื่น

(C) บุคคลใดกระทำการมิชอบด้วยกฎหมายโดยเจตนาฉ้อฉลปราศจากอำนาจหรือความยินยอมจากบุคคลผู้ซึ่งเป็นเจ้าของเว็บเพจหรือเว็บไซต์ เพื่อ

(1) ทำซ้ำหรือเลียนแบบไม่ว่าจะทั้งหมดหรือบางส่วน

(2) ควบคุมหรือเปลี่ยนแปลงเส้นทางในการส่งข้อความอิเล็กทรอนิกส์จาก IP Address ของบุคคลหนึ่งไปยัง IP Address [121]อื่นๆที่กำหนด

(3) ใช้เครื่องหมายการค้า โลโก้ ชื่อ หรือลิขสิทธิ์ของบุคคลอื่นบนหน้าเว็บไซต์โดยปราศจากความยินยอมจากเจ้าของที่แท้จริง หรือ

(4) สร้างการเชื่อมโยงจากหน้าเว็บของบุคคลที่ถูกกำหนด ไปยังหน้าเว็บที่ถูกกำหนดโดยเปลี่ยนเส้นทางการเชื่อมต่อข้อมูลไปยังหน้าเว็บที่ถูกกำหนดไว้

(D) บุคคลใดพยามกระทำการละเมิดต่อบทบัญญัติตามที่ได้กำหนดไว้ในกฎหมายนี้ถือเป็นการกระทำที่มิชอบด้วยกฎหมาย

(E) นอกจากเหนือจากบทลงโทษดังที่บัญญัติไว้ใน § 47-18-5205, บุคคลใดกระทำการโดยเจตนาอันเป็นการละเมิดต่อบทบัญญัติ

(1) ตาม(A),(B)และ(C)ให้ถือว่าเป็นการกระทำความผิดลหุโทษประเภท A[122]

(2) ตาม (D) ให้ถือว่าเป็นการกระทำความผิดลหุโทษประเภท B[123]

มาตรา 47-18-2504[124]

---

[121] IP Address (internet Protocol Address) คือ หมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายที่ใช้โปรโตคอลแบบ TCP/IP สามารถบอกได้ว่าเครื่องคอมพิวเตอร์ตั้งอยู่ที่ไหนซึ่งสามารถระบุได้ผ่าน ip address

[122] ความผิดลหุโทษประเภท A หรือ Class A misdemeanors คือ ประเภทของความผิดลหุโทษทางอาญาที่ร้ายแรงที่สุดหากถูกตัดสินว่ามีความผิด ซึ่งอาจต้องรับโทษจำคุกสูงสุด 11 เดือน 29 วัน ปรับสูงสุด 2,500 ดอลลาร์ หรือทั้งจำทั้งปรับ ตัวอย่างของความผิดทางอาญาประเภท A ได้แก่: ขโมยของมูลค่าน้อยกว่า 1,000 ดอลลาร์, สะกดรอยตาม, ทะเลาะวิวาท, เมาแล้วขับ, ครอบครองอุปกรณ์การเสพ, ครอบครองกัญชาจำนวนไม่มาก, ฝ่าฝืนคำสั่งศาล. Daniel D. Coughlin, ‘Misdemeanor crimes in tennessee’ (Mccbristol, 30 June 2022) <https://www.mccbristol.com/blog/misdemeanor-crimes-in-tennessee/> สืบค้นเมื่อ 28 มีนาคม 2566.

[123] ความผิดลหุโทษประเภท B หรือ Class B misdemeanors คือ ประเภทของความผิดลหุโทษทางอาญาที่มีความรุนแรงน้อยกว่าประเภท A โดยความผิดทางอาญาประเภท B มีโทษจำคุกสูงสุดหกเดือน ปรับไม่เกิน 500 ดอลลาร์ หรือทั้งจำทั้งปรับ ตัวอย่างของความผิดทางอาญาประเภท B ในรัฐเทนเนสซี ได้แก่: ขับรถโดยประมาท, การค้าประเวณี, บุกรุกพื้นที่ส่วนบุคคล. เพิ่งอ้าง.

[124] Tenn. Code § 47-18-5204.

(A) บุคคลดังต่อไปนี้สามารถดำเนินคดีกับบุคคลที่กระทำการละเมิดมาตรา47-18-5203

(1)(a) บุคคลที่:

(i) มีส่วนร่วมในธุรกิจการให้บริการการเข้าถึงอินเทอร์เน็ตแก่สาธารณะ เป็นเจ้าของเว็บเพจ หรือเป็นเจ้าของเครื่องหมายการค้า และ

(ii) ได้รับความเสียหายจากการกระทำละเมิดตามมาตรา 47-18-2503

(1)(b) การเรียกร้องค่าเสียหายของบุคคลตาม (A)(1)(a) (i) สามารถเรียกร้องค่าเสียหายได้มากกว่าจำนวนค่าเสียหายที่เกิดขึ้นจริง หรือ เป็นเงิน 500,000 ดอลลาร์ หรือ

(2)(a) บุคคลที่ได้รับความเสียหายจากการกระทำละเมิดตามมาตรา 47-18-5203 สามารถดำเนินคดีได้เฉพาะกับบุคคลที่กระทำการละเมิดตามมาตรา 47-18-5203 เท่านั้น

(2)(b) การดำเนินคดีภายใต้ (A) (2)(a) ผู้เสียหายอาจร้องขอให้มีการกำหนดบทลงโทษเพิ่มเติมกับบุคคลที่กระทำละเมิดมาตรา 47-18-5203 และ เรียกร้องค่าเสียหายได้มากกว่าสามเท่าของมูลค่าความเสียหายที่เกิดขึ้นจริง หรือ5,000 ดอลลาร์ต่อหนึ่งการกระทำ

(B) อัยการสูงสุดและผู้รายงาน[125]หรืออัยการเขตอาจดำเนินคดีเพิ่มเติมกับบุคคลที่กระทำละเมิดตามมาตรา 47-18-2503 ได้โดยการกำหนดโทษปรับทางแพ่งเป็นเงินจำนวนไม่เกินกว่า 2,500 ดอลลาร์ ต่อการกระทำละเมิดหนึ่งครั้ง

(C) ภายใต้บทบัญญัตินี้ ศาลอาจดำเนินการอย่างใดอย่างหนึ่งหรือทั้งสองอย่างได้ดังต่อไปนี้

(1) เพิ่มจำนวนมูลค่าความเสียหายที่ผู้เสียหายสามารถเรียกร้องได้เป็นจำนวนสูงสุดไม่เกินกว่าสามเท่าของความเสียหายที่สามารถเรียกร้องได้ภายใต้ (A) ในกรณีที่จำเลยมีส่วนร่วมในการกระทำความผิดตามมาตรา 47-18-5203

(2) กำหนดจำเลยจ่ายค่าธรรมเนียมศาลและค่าทนายตามที่เหมาะสมในการดำเนินคดีแก่โจทก์

(D) การเรียกร้องค่าเสียหายตามบทบัญญัตินี้ไม่เป็นการตัดสิทธิในการเรียกร้องค่าเสียหายตามกฎหมายอื่น

(E) เพื่อให้เป็นไปตามเจตนารมณ์ของ (1) ในอนุมาตรา (A) ให้ถือว่าการกระทำละเมิดตามมาตรา 47-18-5203 เพียงครั้งเดียวที่ก่อให้เกิดความเสียหายหลายอย่างเป็นการฝ่าฝืนบทบัญญัติเพียงครั้งเดียว

---

[125] ผู้รายงาน หรือ Reporter คือ บุคลากรของศาลที่ทำหน้าที่บันทึกคำให้การระหว่างการพิจารณาคดีในศาล เช่น การพิจารณาคดีการพิจารณาคดี คำให้การสาบานตน และการฝากขัง ประจักษ์พยาน โดยการถอดความแบบคำต่อคำ จากนั้นผู้รายงานจะจัดทำบันทึกเป็นลายลักษณ์อักษร จากกระบวนการพิจารณาของศาลให้ผู้พิพากษาและทนายความตรวจสอบถูกต้องเมื่อจบการพิจารณาคดี. Cornell Law School,‘Court reporter’ (Cornell Law School) <https://www.law.cornell.edu/wex/court_reporter> สืบค้นเมื่อ 28 มีนาคม 2566.

(F) ผู้ให้บริการอินเทอร์เน็ตไม่ต้องรับผิดภายใต้บทบัญญัติในส่วนนี้หรือกฎหมายของรัฐอื่นใดสำหรับการระบุ ลบ หรือปิดการเข้าถึงเนื้อหาที่อยู่บนหน้าเว็บอินเทอร์เน็ตหรือตำแหน่งออนไลน์อื่น ๆ ที่ผู้ให้บริการดังกล่าวเชื่อโดยสุจริตว่าเป็นการใช้เพื่อประกอบการละเมิดในส่วนนี้

3.1.4 กฎหมายรัฐยูท่า

รัฐยูท่าถือได้ว่าเป็นรัฐที่มีการบัญญัติกฎหมายต่อต้านฟิชชิ่งและฟามมิ่งขึ้นมาใช้อย่างจริงจังโดยบัญญัติไว้ใน Utah Code, Title 13 - Commerce and Trade, Chapter 40 - Utah E-Commerce Integrity Act, Part 2 - Phishing and Pharming ซึ่งเป็นบทบัญญัติที่มีเจตนารมณ์เพื่อใช้ในการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับการฟิชชิ่งและฟามมิ่ง สำหรับบุคคลใดก็ตามที่กระทำการหลอกลวงหรือทำให้เข้าใจผิดเพื่อแสดงตนเป็นผู้แทนทางธุรกิจโดยปราศจากความยินยอมจากเจ้าของธุรกิจดังกล่าวผ่านทางอินเทอร์เน็ต เพื่อร้องขอหรือกระทำด้วยประการใดๆเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล ซึ่งมีบทบัญญัติสำคัญดังนี้

มาตรา 13-40-201[126]

(1) บุคคลใดจะมีความผิดในฐานฟิชชิ่งเมื่อกระทำการโดยเจตนาฉ้อโกงหรือทำร้ายบุคคล โดยใช้ความรู้ในการอำนวยความสะดวกในทางทุจริตหรือทำให้ผู้อื่นได้รับความเสียหาย โดย:

(a) แสดงตนเป็นผู้แทนทางธุรกิจโดยปราศจากอำนาจหรือความยินยอมจากเจ้าของธุรกิจที่แท้จริง และ

(b) กระทำการด้วยวิธีใดๆเพื่อเรียกร้อง ร้องขอ หรือดำเนินการใดๆ อันเป็นการชักจูงบุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล

(2) บุคคลใดจะมีความผิดในฐานฟาร์มมิ่ง[127]เมื่อกระทำการโดยเจตนาฉ้อโกงหรือทำร้ายผู้อื่นโดยใช้ความรู้ในการอำนวยความสะดวกในทางทุจริตหรือทำให้ผู้อื่นได้รับความเสียหายบุคคลนั้น:

(a) สร้างหรือดำเนินการบนเว็บเพจที่แสดงตนว่าเกี่ยวข้องกับธุรกิจที่ถูกต้องตามกฎหมาย โดยปราศจากอำนาจหรือความยินยอมจากเจ้าของธุรกิจที่แท้จริง ซึ่งหน้าเว็บนั้นอาจกระทำการด้วยวิธีใดๆเพื่อเรียกร้อง ร้องขอ หรือดำเนินการใดๆ อันเป็นการชักจูงบุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล หรือ

(b) เปลี่ยนแปลงการตั้งค่าบนคอมพิวเตอร์ของผู้ใช้หรืออุปกรณ์ที่มีลักษณะเดียวกันหรือใช้โปรแกรมซอฟต์แวร์ที่ผู้ใช้อาจค้นหาทางอินเทอร์เน็ต เพื่อทำให้ผู้ใช้อินเทอร์เน็ตพบหน้าเว็บที่ได้เตรียมการไว้โดยการสร้างเว็บเพจและแสดงตนว่าเกี่ยวข้องกับธุรกิจที่ถูกต้องตามกฎหมาย โดยปราศจากอำนาจหรือความยินยอมจากเจ้าของธุรกิจที่แท้จริง ซึ่งหน้าเว็บนั้นอาจกระทำการด้วยวิธีใดๆเพื่อเรียกร้อง ร้องขอ หรือดำเนินการใดๆ อันเป็นการชักจูงบุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล

---

[126] UT Code § 13-40-201 Phishing and pharming.

[127] ฟาร์มมิ่ง (Pharming) คือ การเปลี่ยนลิงค์เว็บไซต์ให้ลิงค์ไปที่เว็บไซต์ปลอมอย่างผิดกฎหมาย และมีเจตนาขโมยข้อมูลส่วนตัวของผู้ใช้ อาทิ รหัสผ่าน หมายเลขบัญชี และข้อมูลสำคัญอื่นๆ.

มาตรา 13-40-401[128]

(1) การดำเนินคดีทางแพ่งกับผู้ที่กระทำละเมิดบทบัญญัติใดๆที่บัญญัติไว้ใน ส่วนที่2เกี่ยวกับการการกระทำความผิดฐานฟิชชิ่งและฟาร์มมิ่ง[129]อาจดำเนินคดีได้โดย:

(a) ผู้ให้บริการอินเทอร์เน็ตที่ได้รับผลกระทบจากการละเมิด

(b) เจ้าของเว็บเพจ เซิร์ฟเวอร์คอมพิวเตอร์ หรือเครื่องหมายการค้าที่ถูกนำมาใช้ในการละเมิดโดยไม่ได้รับอนุญาต หรือ

(c) อัยการสูงสุด

(2) บุคคลผู้ซึ่งเป็นผู้เสียหายและมีอำนาจดำเนินคดีทางแพ่งตาม (1) สามารถเรียกร้องค่าเสียหายจากการกระทำละเมิดตามที่เกิดขึ้นจริง หรือโทษปรับในทางแพ่งไม่เกิน 150,000 ดอลลาร์ ต่อการกระทำละเมิดหนึ่งครั้ง

(3) การกระทำละเมิดบทบัญญัติในส่วนที่2 เกี่ยวกับการการกระทำความผิดฐานฟิชชิ่งและฟาร์มมิ่ง ที่กระทำขึ้นโดยสถาบันการเงินไม่ว่าจะของรัฐหรือเอกชน ให้เป็นไปตามระเบียบข้อบังคับภายในของหน่วยงานหลักที่กำกับดูแลสถาบันการเงินเท่านั้น

3.2 กฎหมายประเทศสหพันธ์สาธารณรัฐเยอรมนี

เนื่องจากประเทศสหพันธ์สาธารณรัฐเยอรมนีเป็นประเทศที่มีการบังคับใช้กฎหมายในระบบเดียวกับประเทศไทย กล่าวคือเป็นประเทศที่ใช้ระบบกฎหมาย Civil Law เช่นเดียวกันกับประเทศไทยทั้งยังถือได้ว่าประเทศสหพันธ์สาธารณรัฐเยอรมนีนั้นเป็นประเทศที่ได้รับการยอมรับว่ามีความเจริญก้าวหน้าเป็นอย่างมากในทางเทคโนโลยีประเทศหนึ่ง ด้วยเหตุนี้เองผู้เขียนจึงได้เลือกที่จะศึกษากฎหมายของประเทศสหพันธ์สาธารณรัฐเยอรมนีเพื่อประโยชน์ในการศึกษาและพัฒนาบทบัญญัติทางกฎหมายที่เกี่ยวข้องกับการฟิชชิ่ง

จากการศึกษาพบว่าประเทศเยอรมนีก่อนที่จะมีการบัญญัติกฎหมายเพิ่มเติมเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ขึ้นมาในการดำเนินคดีกับบุคคลที่กระทำความผิดทางเทคโนโลยีหรือใช้คอมพิวเตอร์เป็นเครื่องมือประกอบในการกระทำความผิด ศาลในขณะนั้นมักจะใช้ฐานความผิดในกฎหมายอาญามาปรับใช้กับการความผิดที่เกิดขึ้นโดยอ้างอิงจากลักษณะในการกระทำความผิด แต่เนื่องจากการก่ออาชญากรรมทางคอมพิวเตอร์ที่ทำให้เกิดความเสียหายและซับซ้อนมากยิ่งขึ้นจึงก่อให้เกิดความจำเป็นที่จะต้องมีการทบทวนกฎหมายและบัญญัติมาตรการทางกฎหมายบางอย่างขึ้นเพื่อใช้บังคับกับการกระทำผิดเกี่ยวกับคอมพิวเตอร์ แต่ไม่ว่าอย่างไรก็ตามเนื่องจากฝ่ายนิติบัญญัติในขณะนั้นได้ดำเนินการแก้ไขและปรับปรุงบทบัญญัติทางกฎหมายภายใต้แนวคิดที่ว่า อาชญากรรมทางคอมพิวเตอร์นั้นเป็นคดีที่มีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ซึ่งในความเห็นของฝ่ายนิติบัญญัติในขณะนั้นเห็นว่าเป็นการกระที่อยู่ในขอบเขตของ

---

[128] UT Code § 13-40-401 Phishing and pharming violations.

[129] UT Code, Title 13, Chapter 40, Part 2 - Phishing and Pharming.

กฎหมายอาญาที่ใช้บังคับอยู่จำไม่จำเป็นที่จะต้องกำหนดให้อาชญากรรมคอมพิวเตอร์เป็นความผิดเฉพาะ[130] และเห็นควรให้แก้ไขโดยการเพิ่มเติมฐานความผิดในกฎหมายอาญาให้เหมาะสมกับยุคสมัยเพียงเท่านั้น

แต่ไม่ว่าอย่างไรก็ดีในปี 2007 ประเทศประเทศสหพันธ์สาธารณรัฐเยอรมนีก็ได้มีการปรับปรุงแก้ไขกฎหมายอาญาเป็นการใหญ่เพื่อให้มีความสอดคล้องและเป็นไปตามข้อกำหนดในอนุสัญญาว่าด้วยอาชญากรรมทางไซเบอร์ (Convention on cybercrime) ของคณะมนตรียุโรป[131] และจากคำกล่าวในข้างต้นที่ว่าเป็นการแก้ไขกฎหมายอาญาเป็นการใหญ่นั้นคือการแก้ไขเพิ่มเติมในฐานความผิดหลักๆที่เกี่ยวข้องกับการก่ออาชญากรรมทางคอมพิวเตอร์ โดยได้เพิ่มฐานความผิดที่เกี่ยวกับคอมพิวเตอร์ไว้ในประมวลกฎหมายอาญาร่วมกับฐานความผิดที่มีอยู่แต่เดิมไว้ในหมวดความผิดเดียวกัน[132]เนื่องจากองค์ประกอบของฐานความผิดนั้นไม่ได้ต่างจากองค์ประกอบในฐานความผิดเดิมมากนักจึงสามารถนำบทบัญญัติเดิมมาปรับใช้กับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้หรือหากความผิดในฐานใดที่มีองค์ประกอบความผิดที่เปลี่ยนไปจากเดิมก็บัญญัติฐานความผิดขึ้นมาใหม่ เช่น ความผิดฐานโจรกรรมหรือปลอมแปลงข้อมูลคอมพิวเตอร์ ก็บัญญัติความผิดเหล่านี้ไว้ในหมวดความผิดเดียวกัน เพื่อให้สะดวกในการบังคับใช้[133]และสอดคล้องกับเจตนารมณ์ของกฎหมายและหลักประกันในทางกฎหมายอาญาที่มีความเป็นเหตุเป็นผลในทุกขั้นตอนของการพิจารณา และที่สำคัญเพื่อเป็นหลักประกันว่าการใช้กฎหมายจะมีความแน่นอนมั่นคงเหมือนกันในทุกกรณี[134] โดยมีบทบัญญัติสำคัญที่เกี่ยวข้องกับการฟิชชิ่งดังนี้

3.2.1 ความผิดฐานจารกรรมข้อมูลคอมพิวเตอร์

ในกฎหมายของประเทศเยอรมนีนั้น การเข้าถึงข้อมูลคอมพิวเตอร์โดยปราศจากโดยปราศจากความยินยอมโดยใช้วิธีที่มิชอบเข้าถึงข้อมูลโดยเจตนาโดยฝ่าฝืนมาตรการป้องกันของข้อมูลนั้นเพื่อเข้าถึงระบบคอมพิวเตอร์ ซึ่งความผิดฐานนี้เพียงแค่เจาะระบบก็เป็นความผิดแล้ว ไม่จำเป็นต้องทำซ้ำหรือโจรกรรมข้อมูลเหล่านั้นออกไปเพราะถือว่ากฎหมายนั้นมุ่งคุ้มครอง ความลับส่วนบุคคล สิทธิส่วนบุคคล และความปลอดภัยของระบบคอมพิวเตอร์[135]

---

[130] กุลธิดา อาธิเจริญสุข (เชิงอรรถ 105) 82.

[131] '... Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (... StrÄndG) (G-SIG: 16019307)' (German Bundestag) <https://dip.bundestag.de/vorgang/.../8366> สืบค้นเมื่อ 30 มีนาคม 2566.

[132] Bettina Weisser, 'Cyber Crime - The Information Society and Related Crimes. National Report on Germany' (2013) Münster Journal of Mathematics, 1.

[133] สาวตรี สุขศรี, 'อาชญากรรมคอมพิวเตอร์/อินเทอร์เน็ตตามกฎหมายอาญาสหพันธ์สาธารณรัฐเยอรมนี' (2556) 3 วารสารนิติศาสตร์, 507-509 <https://opacdb02.dpu.ac.th/cgi-bin/koha/opacdetail.pl-?biblionumber=123953> สืบค้นเมื่อ 30 มีนาคม 2566.

[134] ณัฐสุดา อัคราวัฒนา, 'การกำหนดความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์' (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาลัยธุรกิจบัณฑิตย์ 2560) 42.

[135] เพิ่งอ้าง 82.

อย่างไรก็ตามหากเป็นเพียงการเข้าถึงคอมพิวเตอร์ปราศจากอำนาจเพียงอย่างเดียวโดยมิได้ก่อให้เกิดความเสียหายหรือการกระทำในลักษณะที่เป็นความผิด กล่าวคือเป็นเพียงการเข้าถึงคอมพิวเตอร์เฉยๆมิได้มีการกระทำใดๆต่อข้อมูลหรือระบบคอมพิวเตอร์การกระทำเช่นนี้ไม่ถือว่าเป็นความผิดฐานจารกรรมข้อข้อมูลเพราะฝ่ายนิติบัญญัติของประเทศเยอรมนีเห็นว่าการเข้าถึงคอมพิวเตอร์ปราศจากอำนาจ นั้นเป็นเพียงการพยายามกระทำความผิดเท่านั้นจึงไม่ถือว่าเป็นความผิดอาญาฐานจารกรรมข้อมูล[136]

โดยในเรื่องการจารกรรมข้อมูลนี้เองได้มีการบัญญัติกฎหมายที่เกี่ยวข้องไว้หลายฉบับ แต่ทุกฉบับก็ล้วนมีขอบเขตจำกัดในการบังคับใช้ที่จำกัดทำให้ไม่สามารถครอบคลุมความผิดได้ทุกกรณี ด้วยเหตุนี้เองเพื่อเป็นการอุดช่องว่างของกฎหมายจึงได้มีการบัญญัติมาตรา 202a[137] ไว้ในประมวลกฎหมายอาญาเยอรมนีในเรื่องการจารกรรมข้อมูลความว่า

มาตรา 202a[138] การเข้าถึงข้อมูลโดยมิชอบ

(1) ผู้ใดเข้าถึงโดยปราศจากความยินยอมเพื่อตนเอง หรือผู้อื่น ซึ่งข้อมูลที่ไม่ได้มีไว้สำหรับตนและมีมาตรการป้องกันการโดยเฉพาะถ้าได้กระทำโดยหลีกเลี่ยงการป้องกันนั้น ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับ

(2) ข้อมูลในความหมายของ (1) หมายถึงแต่เฉพาะข่อมูลที่ถูกเก็บไว้ หรือถูกส่งทางอิเล็กทรอนิกส์ ทางคลื่นกระแสแม่เหล็ก หรือทางอื่นที่มีรูปแบบที่ไม่สามารถรับรู้ได้ในทันทีทันที

3.2.2 ความผิดเกี่ยวกับฟิชชิ่ง

ในประเทศเยอรมนีนั้นได้มีการกำหนดให้ความผิดฐานฐานฟิชชิ่งนั้นเป็นความผิดเฉพาะตามบทบัญญัติดังต่อไปนี้

---

[136] กุลธิดา อาธิเจริญสุข (เชิงอรรถ 105) 82.

[137] Section 202a StGB.

Data espionage

(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorized access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.

(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.

[138] StGB. Section 202a Data espionage

(1) Who ever, without being authorized to do so, obtains access, by circumventing the access protection, for themselves or another, to data which were not intended for them and were specially protected against unauthorised access incurs a penalty of imprisonment for a term not exceeding three years or a fine.

(2) For the purposes of subsection (1), data are only those which are stored or transmitted electronically, magnetically, or otherwise in a manner which is not immediately perceptible.

มาตรา 202b[139] ความผิดฐานจารกรรมข้อมูล

ผู้ใดโดยปราศจากความยินยอมใช้วิธีการทางเทคนิคเพื่อดักรับข้อมูล (§202a (2)) ที่มิได้มีไว้สำหรับบุคคลอื่นหรือเพื่อสาธารณะ ซึ่งอยู่ในระหว่างการส่งข้อมูลที่มิได้เปิดเผยต่อสาธารณะหรือจากการแผ่รังสีแม่เหล็กไฟฟ้าของระบบประมวลผลข้อมูล ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับในกรณีที่ความผิดนั้นไม่ต้องรับโทษหนักกว่าตามบทบัญญัติอื่น

มาตรา 202c[140] ความผิดฐานเตรียมการจารกรรมข้อมูลและฟิชชิ่ง

(1) ผู้ใดเตรียมการกระทำความผิดตามมาตรา 202a หรือ 202b โดยการผลิต ได้มาสำหรับตนเองหรือผู้อื่น จำหน่าย จัดหาให้ผู้อื่น เผยแพร่ หรือทำให้แพร่หลายโดยประการอื่นเพื่อทำให้เข้าถึงได้ซึ่ง

(1.1) รหัสผ่านหรือรหัสความปลอดภัยอื่น ๆ ที่ให้การเข้าถึงข้อมูล (มาตรา 202a (2)) หรือ

(1.2) โปรแกรมคอมพิวเตอร์เพื่อวัตถุประสงค์ในการกระทำความผิดนั้น ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับ

(2) ให้นำมาตรา 149 (2) และ (3) มาใช้บังคับ[141]

3.2.3 ความผิดฐานฉ้อโกงคอมพิวเตอร์

ก่อนปี ค.ศ. 1986 นั้นในประมวลกฎหมายอาญาของประเทศเยอรมนีไม่มีการบัญญัติกฎหมายเกี่ยวกับการฉ้อโกงคอมพิวเตอร์ไว้เหตุเพราะนักกฎหมายในประเทศเยอรมนีนั้นมีความเชื่อว่าการที่จะหลอกลวงคอมพิวเตอร์หรือเครื่องจักรนั้นเป็นไปไม่ได้ แต่ไม่ว่าอย่างไรก็ตามเพื่อเป็นการอุดช่องว่างทางกฎหมาย ในปี ค.ศ. 1986 ฝ่ายนิติบัญญัติในขณะนั้นจึงได้กำหนดให้การแก้ไข ดัดแปลง หรือบิดเบือน

---

[139] StGB. Section 202b Phishing

Whosoever unlawfully intercepts data (section 202a (2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment not exceeding two years or a fine, unless the offence incurs a more severe penalty under other provisions.

[140] StGb. Section 202c

Acts preparatory to data espionage and phishing.

(1) Whoever prepares the commission of an offence under section 202a or 202b by producing, acquiring for themselves or another, selling, supplying to another, disseminating, or making available in another way

1. passwords or other security codes which provide access to data(section202a (2))
2. computer programs for the purpose of the commission of such an offence

incurs a penalty of imprisonment for a term not exceeding two years or a fine.

(2) Section 149 (2) and (3) applies accordingly.

[141] See StGB.§ 149 (2),(3)

โปรแกรมหรือข้อมูลคอมพิวเตอร์โดยมีเจตนาเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์ในทางทรัพย์สินเป็นความผิดซึ่งเพิ่มเติมฐานความผิดดังกล่าวโดยการบัญญัติไว้ในประมวลกฎหมายอาญามาตรา 263a และถูกแก้ไขอีกครั้งในปี ค.ศ.2017[142]

มาตรา 263a การฉ้อโกงคอมพิวเตอร์[143]

(1) ผู้ใดโดยเจตนา เพื่อให้ตนเองหรือผู้อื่นได้ประโยชน์ในทางทรัพย์สินใดไม่ชอบด้วยกฎหมายและทำให้ทรัพย์สินของผู้อื่นได้รับความเสียหาย ด้วยการกระทำให้ผลที่แสดงจากการประมวลผลเป็นไปตามความต้องการของตน โดยใช้โปรแกรมที่มีจัดการ ไม่ถูกต้อง โดยใช้ข้อมูลที่ไม่ถูกต้องหรือไม่ครบถ้วนสมบูรณ์ โดยใช้ข้อมูลโดยไม่มีอำนาจ หรือโดยประการอื่นใดโดยไม่ได้รับอนุญาต ต้องระวางโทษไม่เกิน 5 ปีหรือมีโทษปรับ

(2) ให้นำมาตรา 263 (2) ถึง (6) มาใช้บังคับกับการกระทำความผิดตามวรรคแรกโดยอนุโลม”[144]

(3) ผู้ใดตระเตรียมการกระทำความผิดตาม (1) โดย

(3.1) ผลิตโปรแกรมคอมพิวเตอร์โดยมีวัตถุประสงค์เพื่อกระทำการดังกล่าวหรือจัดหาโปรแกรมดังกล่าวไว้ใช้เองหรือผู้อื่น หรือ

(3.2) ผลิต จัดหาไว้สำหรับตนเองหรือผู้อื่น เสนอขาย จัดเก็บ หรือจัดหารหัสผ่านอื่นหรือรหัสความปลอดภัยอื่นที่เหมาะสมแก่การกระทำดังกล่าว ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับ

(4) ในกรณีตามอนุมาตรา (3) ให้นำมาตรา 149 (2) และ (3) มาใช้บังคับ

---

[142] สาวตรี สุขศรี (เชิงอรรถ 104) 155.

[143] Section 263a StGb.

(1) Whoever, with the intention of obtaining an unlawful pecuniary benefit for themselves or a third party, damages the property of another by influencing the result of a data processing operation by incorrectly configuring the computer program, using incorrect or incomplete data, making unauthorised use of data, or taking other unauthorised influence on the processing operation incurs a penalty of imprisonment for a term not exceeding five years or a fine.

(2) Section 263 (2) to (6) applies accordingly.

(3) Whoever prepares an offence under subsection (1) by

1. producing computer programs the purpose of which is to commit such an act or procures such programs for themselves or another, or

2. producing, procuring for themselves or another, offering for sale, storing, or supplying to another passwords or other security codes suited to committing such an act

incurs a penalty of imprisonment for a term not exceeding three years or a fine.

(4) In the cases under subsection (3), section 149 (2) and (3) applies accordingly.

[144] สาวตรี สุขศรี (เชิงอรรถ 104) 155-156.

3.2.4 ความผิดฐานปลอมข้อมูลคอมพิวเตอร์

ตามประมวลกฎหมายอาญาเยอรมนีความผิดฐานปลอมข้อมูลคอมพิวเตอร์นั้นถูกบัญญัติขึ้นมาเพื่ออุดช่องว่างทางกฎหมายของความผิดฐานปลอมแปลงเอกสารเช่นเดียวกันกับประเทศไทย[145]เพราะตามหลักกฎหมายอาญาของเยอรมนีนั้น เอกสารต้องมีลักษณะที่สามารถอ่านและมองเห็นได้ด้วยตา ซึ่งประกอบไปด้วยข้อความต่างๆ ของผู้ประพันธ์ และที่สำคัญที่สุดคือต้องมีลักษณะทางกายภาพ กล่าวคือเอกสารต้องจับต้องได้ แต่หากเป็นกรณีการปลอมข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ในแฟ้มข้อมูลคอมพิวเตอร์ หรือข้อมูลที่ปรากฏอยู่ในจอคอมพิวเตอร์ จะไม่ถือว่าเอกสารตามความหมายในประมวลกฎหมายอาญาด้วยเหตุนี้เองจึงได้มีการบัญญัติมาตรา 269 ขึ้นมาเพื่อบังคับใช้แก่กรณีนี้

มาตรา 269 การปลอมข้อมูลคอมพิวเตอร์[146]

(1) “ผู้ใดกระทำการด้วยเจตนาฉ้อโกงต่อกฎหมาย ทำการบันทึก หรือแก้ไขเปลี่ยนแปลงข้อมูลที่เป็นพยานหลักฐาน เพื่อให้ผู้อื่นหลงเชื่อว่าเอกสารเท็จ หรือปลอมนั้นมีอยู่ หรือเพื่อใช้ประโยชน์จากข้อมูลที่ตนได้บันทึก หรือเปลี่ยนแปลงนั้น ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือมีโทษปรับ”[147]

(2) การพยามกระทำความผิดตามมาตรนี้ผู้กระทำจะต้องรับโทษด้วย

(3) ให้นำมาตรา 267 (3) และ (4) มาใช้บังคับโดยอนุโลม

3.2.5 ผู้มีอำนาจในการดำเนินคดี

ตามประมวลกฎหมายอาญาเยอรมันได้มีการบัญญัติสิทธิในการดำเนินคดีไว้ใน มาตรา77 ดังนี้

มาตรา 77[148]ผู้มีสิทธิยื่นในการยื่นคำฟ้อง

(1) ในความผิดที่ต้องร้องทุกข์กล่าวโทษก่อนผู้เสียหายอาจยืนคำร้องทุกข์ได้เว้นแต่กฎหมายจะบัญญัติไว้เป็นอย่างอื่น

(2) ถ้าผู้เสียหายถึงแก่ความตาย ในกรณีที่กฎหมายบัญญัติไว้ สิทธิในการร้องทุกข์ย่อตกทอดแก่คู่สมรส สามีหรือภรรยาซึ่งเป็นเพศเดียวกัน และบุตร หากผู้เสียหายไม่มีคู่สมรสหรือสามาภรรยาซึ่งเป็นเพศ

---

[145] ‘พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14(1) ยาแรงผิดขนานสำหรับการหมิ่นประมาทออนไลน์’ (iLaw Freedom, 26 สิงหาคม 2557) <https://shorturl.asia/4CXGo> สืบค้นเมื่อ 1 เมษายน 2566.

[146] Section 269 StGB.

Forgery of data of probative value

(1) Whoever, for the purposes of deception in legal commerce, stores or modifies data which are of probative value in such a way that a counterfeit or falsified document would be created upon their retrieval, or whoever uses data stored or modified in such a manner incurs a penalty of imprisonment for a term not exceeding five years or a fine.

(2) The attempt is punishable.

(3) Section 267 (3) and (4) applies accordingly.

[147] ณัฐสุดา อัคราวัฒนา (เชิงอรรถ 134) 60.

[148] Section 77 StGB. Persons entitled to file request.

เดียวกัน หรือบุตร หรือบุคคลเหล่านั้นถึงแก่ความตายก่อนอายุความในการยื่นคำร้องสิ้นสุดลง สิทธินั้นย่อมตกทอดแก่บิดามารดาของผู้เสียหาย ถ้าบิดามารดาถึงแก่ความตายก่อนอายุความในการยื่นคำร้องสิ้นสุดลง ให้สิทธิดังกล่าวตกทอดแก่พี่น้อง และหลานของผู้เสียหาย ถ้าญาติมีส่วนร่วมในการกระทำความผิดหรือคุณสมบัติในฐานะญาติของผู้เสียหายสิ้นสุดลงบุคคลดังกล่าวย่อมถูกตัดสิทธิในการร้องทุกข์ สิทธิ์ในการยื่นคำร้องทุกข์ไม่ตกทอดหากการดำเนินคดีเป็นการขัดหรือแย้งกับเจตนารมณ์ของผู้เสียหาย

(3) ถ้าผู้มีสิทธิยื่นคำร้องทุกข์เป็นผู้ไร้ความสามารถตามกฎหมายหรือเป็นผู้ถูกจำกัดความสามารถตามกฎหมาย ผู้แทนตามกฎหมายซึ่งเป็นผู้จัดการงานอันเป็นการเฉพาะตัวและผู้มีหน้าที่ดูแลบุคคลนั้นๆ มีสิทธิยื่นคำร้องทุกข์ได้

(4) ถ้าผู้เสียหายหลายคนมีสิทธิยื่นคำร้องทุกข์ ผู้สีสิทธิแต่ละคนอาจยื่นคำร้องทุกข์ได้ด้วยตัวเอง

3.3 กฎหมายสาธารณรัฐฝรั่งเศส

เนื่องจากประเทศสาธารณรัฐฝรั่งเศสเป็นประเทศที่มีความสัมพันธ์กับประเทศไทยโดยเฉพาะอย่างยิ่งในเรื่องของระบบประมวลกฎหมายไทยที่ได้นำของประเทศฝรั่งเศสมาใช้เป็นแบบอย่างในการปฏิรูปกฎหมายและที่ปรึกษากฎหมายส่วนใหญ่ก็เป็นชาวฝรั่งเศสนับด้วยเหตุนี้เองในประมวลกฎหมายของไทยนั้นจึงได้รับอิทธิพลทางกฎหมายส่วนหนึ่งมาจากประเทศฝรั่งเศส[149] อีกทั้งยังบังคับใช้กฎหมายในระบบเดียวกับประเทศไทย กล่าวคือเป็นประเทศที่ใช้ระบบกฎหมาย Civil Law เช่นเดียวกันกับประเทศไทยทั้งยังถือได้ว่าประเทศสาธารณรัฐฝรั่งเศสนั้นเป็นประเทศที่มีการพัฒนาและให้ความสำคัญกับกฎหมายเกี่ยวกับอาชญากรรมทางเทคโนโลยีประเทศหนึ่ง ด้วยเหตุนี้เองผู้เขียนจึงได้เลือกที่จะศึกษากฎหมายของประเทศสาธารณรัฐฝรั่งเศสเพื่อประโยชน์ในการศึกษาและพัฒนาบทบัญญัติทางกฎหมายที่เกี่ยวข้องกับการฟิชชิ่ง

ปัจจุบันกฎหมายภายในของสาธารณรัฐฝรั่งเศสนั้นยังมิได้มีการบัญญัติกฎหมายที่เกี่ยวข้องกับการฟิชชิ่งโดยตรง อย่าไรก็ดีฝ่ายนิติบัญญัติของสาธารณรัฐฝรั่งเศสก็ได้มีการออกกฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับอาชญากรรมทางไซเบอร์หลายฉบับตั้งแต่ปี 1988 ซึ่งมีการปรับปรุงอย่างสม่ำเสมอ จนกระทั้งในปี 2004 ได้มีการแก้ไขกฎหมายอาญาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ให้มีความสอดคล้องและเป็นไปตามข้อกำหนดในอนุสัญญาว่าด้วยอาชญากรรมทางไซเบอร์ (Convention on cybercrime)ของคณะมนตรียุโรปตามที่สาธารณรัฐฝรั่งเศสนั้นได้ให้สัตยาบันไว้[150]ซึ่งทำให้การเข้าถึงระบบประมวลผลข้อมูลอัตโนมัติโดยไม่ได้รับอนุญาตถือเป็นความผิด นอกจากนี้ ยังมีการเพิ่มอำนาจและเครื่องมือในการสืบสวนให้กับเจ้าหน้าที่ตำรวจเพื่อจัดการกับการก่ออาชญากรรมทางไซเบอร์อย่างมีประสิทธิภาพทั้งยังได้มีการจัดตั้งศาลเฉพาะที่ใช้ใน

---

[149] วันวิสาข์ ศรีกระจิบ, 'ฝรั่งเศสกับการปฏิรูปกฎหมายไทยตั้งแต่ยุคอาณานิคมจนถึงยุคโลกาภิวัตน์ปัจจุบัน' (วิทยานิพนธ์ อักษรศาสตรมหาบัณฑิต มหาวิทยลัยศิลปากร 2546) ง.

[150] ดู Loi n° 2004-575: Loi pour la confiance dans l'économie numérique

การพิจารณาลงโทษอาชญากรไซเบอร์โดยเฉพาะ[151] ฐานความผิดเกี่ยวกับอาชญากรรมไซเบอร์นั้นรวมไปถึงความผิดที่เกี่ยวข้องกับการเข้าถึงข้อมูลส่วนบุคคล เช่น การแก้ไขหรือเข้าถึงโดยไม่ได้รับอนุญาต[152] โดยบัญญัติไว้ในประมวลกฎหมายอาญาสาธารณรัฐฝรั่งเศส ในส่วนที่เกี่ยวข้องกับการก่ออาชญากรรมทางไซเบอร์ (Le Code pénal, Chapitre III : Des atteintes aux systèmes de traitement automatisé de données) ซึ่งมีบทบัญญัติสำคัญที่เกี่ยวข้องกับการฟิชชิ่ง ดังนี้[153]

3.3.1 ความผิดฐานจารกรรมข้อมูลคอมพิวเตอร์

ในกฎหมายประเทศสาธารณรัฐฝรั่งเศสการจารกรรมข้อมูลหรือการเข้าถึงโดยไม่ได้รับอนุญาตนั้นถือเป็นความผิดตามกฎหมายอาญาฝรั่งเศส ซึ่งได้มีการกำหนดบทลงโทษไว้อย่างชัดแจนสำหรับบุคคลที่เข้าถึงระบบประมวลผลอัตโนมัติโดยไม่ได้รับอนุญาต ดังนี้

มาตรา 323-1[154]

ผู้ใดเข้าถึงโดยเจตนาฉ้อโกงต่อระบบการประมวลผลข้อมูลอัตโนมัติโดย มิชอบไม่ว่าจะทั้งหมดหรือบางส่วนของต้องระวางโทษจำคุก 3 ปีและปรับ 100,000 ยูโร

หากการกระทำความผิดในวรรคหนึ่งนั้นส่งผลให้เกิดการลบล้าง หรือเปลี่ยนแปลงข้อมูลที่อยู่ในระบบ หรือเปลี่ยนแปลงการทำงานของระบบต้องระวางโทษจำคุก 5 ปีและปรับ 150,000 ยูโร

หากการกระทำความผิดตามวรรคหนึ่งและวรรคสองเป็นการกระทำต่อระบบการประมวลผลข้อมูลอัตโนมัติของหน่วงงานของรัฐ ต้องระวางโทษจำคุก7 ปีและปรับ300,000 ยูโร

---

[151] European Union Agency for Criminal Justice Cooperation, ‘Cybercrime’ (European Union Agency for Criminal Justice Cooperation) <www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime> สืบค้นเมื่อ 3 เมษายน 2566.

[152] Claire Bernier, ‘Data Security and Cybercrime in France’ (Lexology) <https://www.lexology.com/library/detail.aspx?g=4db6c38c-be5e-4bce-9044-870c136099a2> สืบค้นเมื่อ 2 เมษายน 2566.

[153] Frédéric Lecomte, ‘Cybersecurity laws and regulations in France 2023’ (ICLG) <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/France> สืบค้นเมื่อ 3 เมษายน 2566.

[154] Le Code pénal, Article 323-1.

Accessing or remaining fraudulently in all or part of an automated data processing system is punishable by three years' imprisonment and a fine of €100,000.

When the result is either the deletion or modification of data contained in the system, or an alteration of the functioning of this system, the penalty is five years' imprisonment and a fine of €150,000.

When the offenses provided for in the first two paragraphs have been committed against an automated personal data processing system implemented by the State, the penalty is increased to seven years' imprisonment and €300,000. fine.

3.3.2 ความผิดเกี่ยวกับการฟิชชิ่ง

ในกฎหมายประเทศฝรั่งเศสในปัจจุบันนั้นยังมิได้มีการบัญญัติให้การฟิชชิ่งนั้นเป็นความผิดเฉพาะ อย่างไรก็ดีในการบังคับใช้กฎหมายเพื่อเอาผิดกับผู้ที่กระทำความผิดเกี่ยวกับฟิชชิ่งนั้นสามารถนำบทบัญญัติในประมวลกฎหมายอาญา และกฎหมายทรัพย์สินทางปัญญามาใช้ในการลงโทษ[155]ผู้กระทำความผิดเกี่ยวกับการฟิชชิ่ง โดยมีบทบัญญัติที่สำคัญดังนี้

มาตรา 226-18[156]

การรวบรวมข้อมูลส่วนบุคคลด้วยวิธีการฉ้อฉล ไม่ยุติธรรม หรือผิดกฎหมายต้องระวางโทษจำคุก 5 ปี และปรับ 300,000 ยูโร

มาตรา 226-4-1[157]

การกระทำเพื่อหรือใช้ข้อมูลอย่างใดอย่างหนึ่งเพื่อช่วยในการเข้าถึงข้อมูลส่วนบุคคลโดยมีจุดประสงค์เพื่อรบกวนความสงบสุขของผู้อื่น หรือบ่อนทำลายเกียรติต้องระวางโทษจำคุก 1 ปี และปรับ 15,000 ยูโร

การกระทำความผิดตามวรรคหนึ่งบนเครือข่ายสื่อสารออนไลน์สาธารณะถือว่ามีโทษเท่ากันเมื่อการกระทำนั้นจุดประสงค์เพื่อแย่งชิงข้อมูลส่วนบุคคลของผู้อื่น

การขโมยข้อมูลส่วนบุคคลของผู้อื่นซึ่งกระทำโดยคู่สมรสหรือหุ้นส่วนคู่ชีวิตของเหยื่อ หรือโดยคู่สัญญาทางแพ่งของเหยื่อการกระทำเหล่านี้มีโทษจำคุกสองปีและปรับ 30,000 ยูโร

มาตรา 313-1[158]

การฉ้อโกง คือ การแสดงตนเป็นบุคคลอื่นโดยเจตนาหลอกลวง หรือทำให้สำคัญผิดในข้อเท็จจริงโดยการใช้กลอุบายหลอกลวง เพื่อให้บุคคลอื่น ส่งเงิน หลักทรัพย์หรือทรัพย์สินใดๆเพื่อให้บริการหรือยินยอมต่อการกระทำที่เป็นภาระผูกพันเป็นการกระทำความผิดฐานการฉ้อโกงต้องระวางโทษจำคุก 5 ปี และปรับ 375,000 ยูโร

---

[155] Claire Bernier (เชิงอรรถที่ 152).

[156] Le Code pénal, Article 226-18.

"Collecting personal data by fraudulent, unfair, or unlawful means is punishable by five years' imprisonment and a fine of 300,000 euros."

[157] Le Code pénal, Article 226-4-1.

[158] Le Code pénal, Article 313-1.

Fraud is the fact, either by the use of a false name or a false capacity, or by the abuse of a true capacity, or by the use of fraudulent maneuvers, of deceiving a natural person or morality and to determine it in this way, to its prejudice or to the prejudice of a third party, to remit funds, securities or any property, to provide a service or to consent to an act operating obligation or discharge.

Fraud is punishable by five years' imprisonment and a fine of 375,000 euros.

มาตรา 323-3[159]

การนำข้อมูลเข้าสู่ระบบการประมวลผลอัตโนมัติอย่างฉ้อฉล การสกัด การถือครอง การทำซ้ำ การส่ง การลบหรือการฉ้อฉลแก้ไขข้อมูลที่มีอยู่มีโทษจำคุกห้าปีและปรับ150,000 ยูโร

เมื่อความผิดนี้เกิดขึ้นกับระบบประมวลผลข้อมูลส่วนบุคคลอัตโนมัติที่ดำเนินการโดยรัฐ โทษจะเพิ่มขึ้นเป็นจำคุก 7 ปี และปรับ 300,000 ยูโร

มาตรา L.713-2[160]

ห้ามมิให้ใช้ เว้นแต่จะได้รับอนุญาตจากเจ้าของเครื่องหมายการค้าที่จดทะเบียน การใช้เครื่องหมายการค้าของบุคคลอื่นในการประกอบธุรกิจสำหรับผลิตภัณฑ์หรือบริการ :

1. เครื่องหมายที่เหมือนกับเครื่องหมายการค้าซึ่งใช้สำหรับผลิตภัณฑ์หรือบริการที่เหมือนกับเครื่องหมายที่จดทะเบียนไว้จากเจ้าของเครื่องหมายการค้าที่แท้จริง

2. เครื่องหมายที่เหมือนหรือคล้ายกับเครื่องหมายการค้าที่ใช้สำหรับสินค้าหรือบริการที่เหมือนหรือคล้ายกับเครื่องหมายที่จดทะเบียนไว้ ซึ่งอาจทำให้ประชาชนทั่วไปเกิดความสับสนและสำคัญผิดระหว่างเครื่องหมายการค้าที่จดทะเบียนกับเครื่องหมายการค้าที่เหมือนทำเลียนแบบ

มาตรา L.713-3[161]

ห้ามมิให้ใช้ เว้นแต่จะได้รับอนุญาตจากเจ้าของเครื่องหมายการค้าที่จดทะเบียนของเครื่องหมายที่เหมือนหรือคล้ายกับเครื่องหมายที่มีชื่อเสียง และใช้กับสินค้าหรือบริการที่เหมือนกัน คล้ายคลึง หรือไม่คล้ายคลึง แก่ผู้ที่เครื่องหมายได้รับการจดทะเบียน หากการใช้เครื่องหมายนี้โดยไม่มีเหตุอันควร เป็นการใช้ประโยชน์จากลักษณะเด่นหรือชื่อเสียงของเครื่องหมายอย่างไม่เป็นธรรม หรือเป็นผลเสียต่อเครื่องหมายนั้น

---

[159] Le Code pénal, Article 323-3.

Fraudulently introducing data into an automated processing system, extracting, holding, reproducing, transmitting, deleting, or fraudulently modifying the data it contains is punishable by five years' imprisonment and €150,000 fine.

When this offense has been committed against an automated personal data processing system implemented by the State, the penalty is increased to seven years' imprisonment and a fine of €300,000.

[160] Code de la propriété intellectuelle. L.713-2

Is prohibited, except authorization of the holder of the mark, the use in the life of the businesses for products or services:

1. A sign identical to the mark and used for products or services identical to those for which the mark is registered.

2. A sign identical or similar to the mark and used for goods or services identical or similar to those for which the mark is registered, if there is, in the mind of the public, a risk of confusion including the risk of association of the sign with the mark.

[161] Code de la propriété intellectuelle. L.713-3

มาตรา L.335-2[162]

งานเขียน บทประพันธ์ดนตรี ภาพวาด หรือการผลิตอื่นใดไม่ว่าจะด้วยวิธีการพิมพ์หรือแกะสลักทั้งหมดหรือบางส่วน อันเป็นการฝ่าฝืนกฎหมายและข้อบังคับที่เกี่ยวข้องกับทรัพย์สินทางปัญญาของผู้สร้าง ถือว่าการกระทำนั้นเป็นการละเมิด และการละเมิดใดๆ ถือเป็นความผิด

การปลอมแปลงผลงานที่ตีพิมพ์ภายในฝรั่งเศสหรือในต่างประเทศมีโทษจำคุก3 ปี และปรับ 300,000 ยูโร

ให้นำบทลงโทษในวรรคสองมาบังคับใช้โดยอนุโลมกระทำความผิดตามวรรคหนึ่งต่อ การส่งออก การนำเข้า การขนถ่าย หรือการมีไว้เพื่อวัตถุประสงค์ดังกล่าวข้างต้นของสิ่งที่ละเมิด

หากการกระทำความผิดตามวรรคหนึ่งเป็นการกระทำโดยกลุ่มบุคคล บทลงโทษจะเพิ่มขึ้นเป็นจำคุก 7 ปี และปรับ 750,000 ยูโร

3.3.3 ผู้มีอำนาจในการดำเนินคดี

เนื่องจากอำนาจในการดำเนินคดีอาญาของประเทศฝรั่งเศสนั้นจัดอยู่ในระบบ ไต่สวนเป็นหลัก (Inquisitorial System)[163] กล่าวคือ อำนาจในการดำเนินคดีนั้นตกเป็นของเจ้าหน้าที่รัฐซึ่งมีหน้าที่สืบหาความจริงและพิสูจน์ความผิดของผู้กล่าวหา เมื่อมีการกระทำความผิดอันเป็นการละเมิดต่อกฎหมายอาญาเกิดขึ้น ผู้ที่ได้รับความเสียหายคือรัฐเนื่องจากการกระทำความผิดนั้นเป็นการละเมิดต่อประโยชน์ของสังคมส่วนรวม แม้ว่าแท้จริงแล้วผู้ที่ได้รับความเสียหายโดยตรงคือผู้เสียหายก็ไม่สิทธิที่จะดำเนินคดีในทางอาญาได้ด้วยตนเอง เหมือนดังเช่นกฎหมายของประเทศไทย

อย่างไรก็ดีแม้ระบบกฎหมายของฝรั่งเศสนั้นจะใช้ระบบกฎหมายเดียวกันกับประเทศไทยแต่ในแง่ของการดำเนินคดีและแนวคิดในการลงโทษผู้กระทำความผิดนั้นค่อนข้างที่จะต่างกับประเทศไทยเหตุเพราะระบบกฎหมายของประเทศฝรั่งเศสนั้นได้รับอิทธิพลมาจากแนวคิดของ ซีซ่า เบ็คคาเรีย (Cesar Beccaria) ที่เห็นว่าเมื่อเกิดการกระทำความผิดของบุคคลใดบุคคลหนึ่งเกิดขึ้นคนภายในสังคมก็จะได้รับความเสียหายไป

---

[162] Code de la propriété intellectuelle. L.335-2

Writings, musical compositions, drawings, paintings, or any other production. Printed or engraved in whole or in part in violation of the laws and regulations concerning the author's property. It is considered a violation and any infringement. regarded as fault.

Forgery of a work published in France or abroad is punishable by three years in prison and a fine of 300,000 euros.

The same penalties will apply for debiting, exporting, importing, transferring, or detaining for the aforementioned purposes of the tort work.

When the offenses listed in this article are committed by gangsters The penalty will increase to 7 years in prison and a fine of 750,000 euros.

[163] อุทัย อาทิเวช, *รวมบทความกฎหมายวิธีพิจารณาความอาญาฝรั่งเศส* (พิมพ์ครั้งที่ 2, สำนักพิมพ์ วิ.เจ. พริ้นติ้ง 2557) 50.

ด้วย กล่าวคือเมื่อมีการกระทำความผิดเกิดขึ้นแม้ความเสียหายโดยตรงจะเกิดแก่ผู้เสียหาย แต่ไม่ว่าอย่างไรก็ตามผลความเสียหายนั้นไม่ได้เกิดขึ้นแค่กับผู้เสียหายเพียงอย่างเดียวแต่ยังส่งผลไปถึงความน่าเชื่อถือและสวัสดิภาพของคนภายในสังคม ดังนั้นรัฐจึงมีความจำเป็นต้องเข้ามาจัดการกับผู้กระทำความผิดซึ่งก่อให้เกิดผลกระทบอย่างร้ายแรงต่อความสงบของสังคม แม้ผู้เสียหายโดยตรงจะละเว้นไม่ดำเนินคดีกับผู้กระทำความผิดด้วยสาเหตุใดๆ ก็ตามก็ไม่สามารถที่จะเป็นเหตุที่ห้ามมิให้รัฐนั้นดำเนินคดีกับผู้กระทำผิด[164]

จากแนวคิดในข้างต้นจึงทำให้ผู้เสียหายในคดีอาญาไม่มีสิทธิที่จะดำเนินคดีด้วยตนเองและถึงแม้ผู้เสียหายจะเสียสิทธิในการดำเนินคดีในทางอาญาแต่ก็ยังมีสิทธิดำเนินคดีในทางแพ่งเพื่อเรียกร้องจากค่าเสียหายที่เกิดขึ้นจากการกระทำความผิดทางอาญา แต่ไม่ว่าอย่างไรก็ตามหากผู้เสียหายประสงค์ที่จะดำเนินในทางอาญากับผู้กระทำความผิดก็สามารถที่จะยื่นคำร้องขอเข้าเป็นคู่ความฝ่ายแพ่งได้โดยอาศัยอำนาจตามมาตราดังต่อไปนี้

มาตรา 1240[165]

ผู้ใดกระทำการที่ก่อให้เกิดความเสียหายแก่ผู้อื่นผู้นั้นต้องชดใช้ค่าเสียหายในความผิดที่ได้กระทำไป.

มาตรา 1[166]

การดำเนินการตามกฎหมายสำหรับบทลงโทษมีขั้นตอนและดำเนินการโดยผู้พิพากษา หรือเจ้าหน้าที่ที่กฎหมายอนุญาต

การดำเนินการนี้อาจเริ่มต้นโดยฝ่ายที่อยู่ภายใต้เงื่อนไขที่กำหนดของบทบัญญัตินี้

มาตรา 2 วรรคแรก[167]

การดำเนินคดีทางแพ่งสามารถกระทำได้โดยผู้เสียหายซึ่งเป็นบุคคลที่ได้รับความเสียหายโดยตรงจากการกระทำความผิดอาญาในฐานความผิดลหุโทษ หรือที่เป็นความผิดต่อส่วนตัว

---

[164] เพิ่งอ้าง 51.

[165] Coad Civil. Article 1240

Any act that causes damage to another shall oblige the person by whose fault it occurred to repair it.

[166] Code of Criminal Procedure. Article 1

Public action for the enforcement of penalties is set in motion and exercised by the magistrates or by the officials to whom it is entrusted by law.

This action can also be initiated by the injured party, under the conditions determined by this code.

[167] Code of Criminal Procedure. Article 2

Civil action aimed at the reparation of the damage suffered because of a felony, a misdemean our or a petty offence is open to all those who have personally suffered damage directly caused by the offence.

ตารางที่ 3.1 ตารางเปรียบเทียบมาตรการที่เกี่ยวข้องกับการฟิชชิ่งในกฎหมายต่างประเทศ

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
มลรัฐแคลิฟอร์เนีย	California Codes Business and Professions Code.	CA Bus & Prof Code § 22948.2 บุคคลใดกระทำการโดยปราศจากอำนาจหรือได้รับความยินยอมจากผู้ประกอบธุรกิจ โดยการใช้เว็บไซต์ จดหมายอิเล็กทรอนิกส์ หรือบริการอื่นๆทางอินเทอร์เน็ต เพื่อเรียกร้อง ร้องขอ หรือดำเนินการใดๆ อันเป็นการชักจูงบุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล ด้วยการแอบอ้างเป็นตัวแทนทางธุรกิจ ผู้นั้นถือว่ากระทำการมิชอบด้วยกฎหมาย	CA Bus & Prof Code §22948.3 (A)บุคคลดังต่อไปนี้อาจดำเนินคดีกับบุคคลฝ่าฝืนมาตรา 22948.21 (1) บุคคลผู้ซึ่ง (a) มีส่วนร่วมในธุรกิจอินเทอร์เน็ตสาธารณะหรือเป็นเจ้าของเว็บเพจ หรือเป็นเจ้าของเครื่องหมายการค้า และ (b) ได้รับผลกระทบจากการละเมิดมาตรา 22948.2 ภายใต้บทบัญญัติในวรรคนี้ ผู้เสียหายอาจเรียกร้องค่าเสียหายได้มากกว่าค่ามูลค่าความเสียหายที่เกิดขึ้นหรือเป็นเงินจำนวน 500,000 ดอลลาร์สหรัฐ (2) บุคคลที่ได้รับผลกระทบจากการละเมิดมาตรา 22948.2 อาจฟ้องร้องเพื่อดำเนินคดีต่อศาลได้ แต่การฟ้องนั้นจะต้องเป็นการฟ้องบุคคลที่ละเมิดต่อมาตรา 22948.2 เท่านั้น ภายใต้บทบัญญัติในวรรคนี้ ผู้เสียหายตามมาตร 22948.2 อาจเรียกร้องค่าเสียหายเพิ่มเติมได้มากกว่าสามเท่าของความเสียหายแท้จริง หรือ 5,000 ดอลลาร์ ต่อการกระทำละเมิดหนึ่งครั้ง (E) เพื่อให้เป็นไปตามเจตนารมณ์ของ (1) ใน	CA Bus & Prof Code §22948.3 (B) อัยการสูงสุดหรืออัยการเขตอาจดำเนินคดีเพิ่มเติมกับบุคคลที่กระทำความผิดหรือสมรู้ร่วมคิดในการกระทำความผิดตามมาตรา 22948.2 ได้โดยการกำหนดโทษปรับทางแพ่งเป็นเงินจำนวนไม่เกินกว่า 2,500 ดอลลาร์ ต่อการกระทำละเมิดหนึ่งครั้ง (C) ภายใต้บทบัญญัตินี้ ศาลอาจดำเนินการอย่างใดอย่างหนึ่งหรือทั้งสองอย่างได้ดังต่อไปนี้ (1) เพิ่มจำนวนมูลค่าความเสียหายที่ผู้เสียหายสามารถเรียกร้องได้เป็นจำนวนสูงสุดไม่เกินกว่าสามเท่าของความเสียหายที่สามารถเรียกร้องได้ภายใต้ (A) ในกรณีที่จำเลยมีส่วนร่วมในการกระทำความผิดตามมาตรา 22948.2 (2)กำหนดจำเลยจ่ายค่าธรรมเนียมศาลและค่าทนายตามที่เหมาะสมในการดำเนินคดีแก่โจทก์ (D)การเรียกร้องค่าเสียหายตามบทบัญญัตินี้ไม่เป็นการตัดสิทธิในการเรียกร้องค่าเสียหายตามกฎหมายอื่น

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
มลรัฐแคลิฟอร์เนีย	California Codes Business and Professions Code.		อนุมาตรา (A) ให้ถือว่าการกระทำละเมิดตามมาตรา 22948.2 เพียงครั้งเดียวที่ก่อให้เกิดความเสียหายหลายอย่างเป็นการฝ่าฝืนบทบัญญัติเพียงครั้งเดียว	
รัฐนิวยอร์ก	New York General Business. Anti Phishing Act of 2006	Article 26 §3903-B 3.บุคคลใดกระทำการผ่านทางเว็บเพจหรือส่งผ่านข้อความอิเล็กทรอนิกส์หรือใช้วิธีการทางอิเล็กทรอนิกส์ในรูปแบบใดๆก็ตามเพื่อร้องขอหรือเพื่อทำให้ทราบถึงข้อมูลที่ระบุตัวตนได้โดยการหลอกลวงหรือทำให้สำคัญผิดว่าเป็นตัวแทนทางธุรกิจ หรือเป็นหน่วยงานของรัฐ โดยปราศจากอำนาจกระทำการหรือได้รับคำยินยอมจากผู้ประกอบธุรกิจหรือหน่วยงานที่แท้จริง บุคคลนั้นถือว่ากระทำการละเมิดต่อกฎหมาย	Article 26 §3903-B 1) กำหนดเงื่อนในการลงโทษต่อบุคคลที่ฝ่าฝืนบทบัญญัติใน (3) และ 2) เรียกร้องค่าเสีย a) ตามความเสียหายแท้จริงที่เกิดขึ้น หรือ b) 1,000 ดอลลาร์ ต่อการกระทำละเมิดหนึ่งครั้ง (B) ในการดำเนินการตาม (A) ศาลอาจจะ 1) กำหนดค่าเสียหายสูงสุดเป็นจำนวนกว่าสามเท่า จากที่จะต้องได้รับตาม a) ในกรณีที่พบว่าจำเลยมีส่วนร่วมในการกระทำอันเป็นการละเมิดต่อ 3. ในบทบัญญัตินี้ 2) กำหนดให้จำเลยจ่ายค่าธรรมเนียมศาลและค่าทนายตามที่เหมาะสมในการดำเนินคดีแก่โจทก์ 5.การเรียกร้องค่าเสียหายตามบทบัญญัตินี้ไม่เป็นการตัดสิทธิในการเรียกร้องค่าเสียหายตามกฎหมายอื่น	Article 26 §3903-B 4. (A) อัยการสูงสุดหรือบุคคลผู้ที่มีส่วนได้เสียในธุรกิจอินเทอร์เน็ตสาธารณะ เจ้าของเว็บเพจ หรือเจ้าของเครื่องหมายการค้า และผู้ที่ได้รับความเสียหายจากการกระทำละเมิดต่อบทบัญญัตินี้

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
รัฐเทนเนสซี	Tennessee Code. ANTI PHISHING ACT OF 2006	§47-18-2503 (A) การกระทำการหลอกลวงหรือทำให้เข้าใจผิดเพื่อแสดงตนเป็นผู้แทนหรือบุคคลอื่นโดยปราศจากความยินยอมจากบุคคลดังกล่าวผ่านทางอินเทอร์เน็ต การส่งจดหมายอิเล็กทรอนิกส์หรือวิธีการทางอิเล็กทรอนิกส์อื่นๆซึ่งรวมไปถึงการติดต่อสื่อสารในช่องทางอื่นเพื่อร้องขอหรือกระทำด้วยประการใดๆเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล หรือ เอกสารส่วนบุคคล (B) บุคคลใดกระทำการมิชอบด้วยกฎหมายโดยปราศจากอำนาจหรือความยินยอมจากบุคคลผู้ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล โดยมีเจตนาฉ้อฉลในการใช้ข้อมูลส่วนบุคคลเพื่อตนเองหรือบุคคลอื่นหรือเพื่อจำหน่ายหรือแจกจ่าย (1) เพื่อให้ได้มาซึ่งบันทึกหรือข้อมูลที่ช่วยในการเข้าถึงข้อมูลทางการเงิน เอกสารข้อมูลส่วนบุคคลหรือประโยชน์ของบุคคนอื่น (2) เพื่อให้ได้รับสินค้าหรือบริการโดยการใช้ข้อมูลระบุตัวตนของบุคคลอื่น (3) เพื่อให้ได้รับเอกสารแสดงระบุตัวตนในนามของบุคคลอื่น (C) บุคคลใดกระทำการมิชอบด้วยกฎหมายโดยเจตนาฉ้อฉลปราศจากอำนาจหรือความยินยอมจากบุคคลผู้ซึ่งเป็น	§47-12-2504 [1](b) การเรียกร้องค่าเสียหายของบุคคลตาม (A)[1](a) (i) สามารถเรียกร้องค่าเสียหายได้มากกว่าจำนวนค่าเสียหายที่เกิดขึ้นจริง หรือ เป็นเงิน 500,000 ดอลลาร์ หรือ [2](b) การดำเนินคดีภายใต้ (A) [2](a) ผู้เสียหายอาจร้องขอให้มีการกำหนดบทลงโทษเพิ่มเติมกับบุคคลที่กระทำละเมิดมาตรา 47-18-5203 และ เรียกร้องค่าเสียหายได้มากกว่าสามเท่าของมูลค่าความเสียหายที่เกิดขึ้นจริง หรือ5,000 ดอลลาร์ต่อหนึ่งการกระทำ	§47-12-2504 A) บุคคลดังต่อไปนี้สามารถดำเนินคดีกับบุคคลที่กระทำการละเมิดมาตรา 47-18-5203 [1](a) บุคคลที่: (i) มีส่วนร่วมในธุรกิจการให้บริการการเข้าถึงอินเทอร์เน็ตแก่สาธารณะ เป็นเจ้าของเว็บเพจ หรือเป็นเจ้าของเครื่องหมายการค้า และ (ii) ได้รับความเสียหายจากการกระทำละเมิดตามมาตรา 47-18-2503 [2](a) บุคคลที่ได้รับความเสียหายจากการกระทำละเมิดตามมาตรา47-18-5203 สามารถดำเนินคดีได้เฉพาะกับบุคคลที่กระทำการละเมิดตามมาตรา 47-18-5203 เท่านั้น

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
รัฐเทนเนสซี	Tennessee Code. ANTI PHISHING ACT OF 2006	เจ้าของเว็บเพจหรือเว็บไซต์เพื่อ (1) ทำซ้ำหรือเลียนแบบไม่ว่าจะทั้งหมดหรือบางส่วน (2) ควบคุมหรือเปลี่ยนแปลงเส้นทางในการส่งข้อความอิเล็กทรอนิกส์จาก IP Address ของบุคคลหนึ่งไปยัง IP Address อื่นๆที่กำหนด (3) ใช้เครื่องหมายการค้า โลโก้ ชื่อ หรือลิขสิทธิ์ของบุคคลอื่นบนหน้าเว็บไซต์โดยปราศจากความยินยอมจากเจ้าของที่แท้จริง หรือ (4) สร้างการเชื่อมโยงจากหน้าเว็บของบุคคลที่ถูกกำหนด ไปยังหน้าเว็บที่ถูกกำหนดโดยเปลี่ยนเส้นทางการเชื่อมต่อข้อมูลไปยังหน้าเว็บที่ถูกกำหนดไว้ (D) บุคคลใดพยามกระทำการละเมิดต่อบทบัญญัติตามที่ได้กำหนดไว้ในกฎหมายนี้ถือเป็นการกระทำที่มิชอบด้วยกฎหมาย (E) นอกจากเหนือจากบทลงโทษดังที่บัญญัติไว้ใน § 47-18-5205, บุคคลใดกระทำการโดยเจตนาอันเป็นการละเมิดต่อบทบัญญัติ (1) ตาม(A),(B)และ(C)ให้ถือว่าเป็นการกระทำความผิดลหุโทษประเภท A (2) ตาม (D) ให้ถือว่าเป็นการกระทำความผิดลหุโทษประเภท B		

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
รัฐเทนเนสซี	Tennessee Code. ANTI PHISHING ACT OF 2006	(F) ผู้ให้บริการอินเทอร์เน็ตไม่ต้องรับผิดภายใต้บทบัญญัติในส่วนนี้หรือกฎหมายของรัฐอื่นใดสำหรับการระบุ ลบ หรือปิดการเข้าถึงเนื้อหาที่อยู่บนหน้าเว็บอินเทอร์เน็ตหรือตำแหน่งออนไลน์อื่น ๆ ที่ผู้ให้บริการดังกล่าวเชื่อโดยสุจริตว่าเป็นการใช้เพื่อประกอบการละเมิดในส่วนนี้		
รัฐยูท่าห์	UTAH E-COMMERCE INTEGRITY ACT2010 GENERAL	§ 13-40-201 (1) บุคคลใดจะมีความผิดในฐานฟิชชิ่งเมื่อกระทำการโดยเจตนาฉ้อโกงหรือทำร้ายบุคคล โดยใช้ความรู้ในการอำนวยความสะดวกในทางทุจริตหรือทำให้ผู้อื่นได้รับความเสียหาย โดย: (a) แสดงตนเป็นผู้แทนทางธุรกิจโดยปราศจากอำนาจหรือความยินยอมจากเจ้าของธุรกิจที่แท้จริง และ (b) กระทำการด้วยวิธีใดๆเพื่อเรียกร้อง ร้องขอ หรือดำเนินการใดๆ อันเป็นการชักจูงบุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล (2) บุคคลใดจะมีความผิดในฐานฟาร์มมิ่งเมื่อกระทำการโดยเจตนาฉ้อโกงหรือทำร้ายผู้อื่นโดยใช้ความรู้ในการอำนวยความสะดวกในทางทุจริตหรือทำให้ผู้อื่นได้รับความเสียหายบุคคลนั้น: (a) สร้างหรือดำเนินการบนเว็บเพจที่แสดงตนว่าเกี่ยวข้อง	§ 13-40-401 (1) การดำเนินคดีทางแพ่งกับผู้ที่กระทำละเมิดบทบัญญัติใดๆที่บัญญัติไว้ใน ส่วนที่2 เกี่ยวกับการการกระทำความผิดฐานฟิชชิ่งและฟาร์มมิ่งอาจดำเนินคดีได้โดย: (2) บุคคลผู้ซึ่งเป็นผู้เสียหายและมีอำนาจดำเนินคดีทางแพ่งตาม (1) สามารถเรียกร้องค่าเสียหายจากการกระทำละเมิดตามที่เกิดขึ้นจริงหรือโทษปรับในทางแพ่งไม่เกิน 150,000 ดอลลาร์ ต่อการกระทำละเมิดหนึ่งครั้ง (3) การกระทำละเมิดบทบัญญัติในส่วนที่2 เกี่ยวกับการการกระทำความผิดฐานฟิชชิ่งและฟาร์มมิ่ง ที่กระทำขึ้นโดยสถาบันการเงินไม่ว่าจะของรัฐหรือเอกชน ให้เป็นไปตามระเบียบข้อบังคับภายในของหน่วยงานหลักที่กำกับดูแลสถาบันการเงินเท่านั้น	§ 13-40-401 (a) ผู้ให้บริการอินเทอร์เน็ตที่ได้รับผลกระทบจากการละเมิด (b) เจ้าของเว็บเพจ เซิร์ฟเวอร์คอมพิวเตอร์ หรือเครื่องหมายการค้าที่ถูกนำมาใช้ในการละเมิดโดยไม่ได้รับอนุญาต หรือ (c) อัยการ

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
รัฐยูท่าห์	UTAH E-COMMERCE INTEGRITY ACT2010 GENERAL	กับธุรกิจที่ถูกต้องตามกฎหมาย โดยปราศจากอำนาจหรือความยินยอมจากเจ้าของธุรกิจที่แท้จริง ซึ่งหน้าเว็บนั้นอาจกระทำการด้วยวิธีใดๆเพื่อเรียกร้อง ร้องขอ หรือดำเนินการใดๆ อันเป็นการชักจูงบุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล หรือ (b) เปลี่ยนแปลงการตั้งค่าบนคอมพิวเตอร์ของผู้ใช้หรืออุปกรณ์ที่มีลักษณะเดียวกันหรือใช้โปรแกรมซอฟต์แวร์ที่ผู้ใช้อาจค้นหาทางอินเทอร์เน็ต เพื่อทำให้ผู้ใช้อินเทอร์เน็ตพบหน้าเว็บที่ได้เตรียมการไว้โดยการสร้างเว็บเพจและแสดงตนว่าเกี่ยวข้องกับธุรกิจที่ถูกต้องตามกฎหมาย โดยปราศจากอำนาจหรือความยินยอมจากเจ้าของธุรกิจที่แท้จริง ซึ่งหน้าเว็บนั้นอาจกระทำการด้วยวิธีใดๆเพื่อเรียกร้อง ร้องขอ หรือดำเนินการใดๆ อันเป็นการชักจูงบุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล		

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
สหพันธ์สาธารณรัฐเยอรมนี	GERMAN CRIMINAL CODE	§ 202a StGb. การเข้าถึงข้อมูลโดยมิชอบ (1) ผู้ใดเข้าถึงโดยมิชอบด้วยกฎหมายเพื่อตนเอง หรือผู้อื่นซึ่งข้อมูลที่ไม่ได้มีไว้สำหรับตนและมีมาตรการป้องกันการโดยเฉพาะถ้าได้กระทำโดยหลีกเลี่ยงการป้องกันนั้น (2) ข้อมูลในความหมายของ (1) หมายถึงแต่เฉพาะข่อมูลที่ถูกเก็บไว้ หรือถูกส่งทางอิเล็กทรอนิกส์ ทางแม่เหล็กหรือทางอื่นที่มีรูปแบบที่ไม่สามารถรับรู้ได้ในทันทีทันที § 202b StGb. ผู้ใดโดยมิชอบด้วยกฎหมายใช้วิธีการทางเทคนิคเพื่อดักรับข้อมูล (§202a (2)) ที่มิได้มีไว้สำหรับบุคคลอื่นหรือเพื่อสาธารณะ ซึ่งอยู่ในระหว่างการส่งข้อมูลที่มิได้เปิดเผยต่อสาธารณะหรือจากการแผ่รังสีแม่เหล็กไฟฟ้าของระบบประมวลผลข้อมูล § 202c StGb. (1) ผู้ใดเตรียมการกระทำความผิดตามมาตรา 202a หรือ 202b โดยการผลิตได้มาสำหรับตนเองหรือผู้อื่นจำหน่าย จัดหาให้ผู้อื่นเผยแพร่ หรือทำให้แพร่หลายโดยประการอื่นเพื่อทำให้เข้าถึงได้ซึ่ง 1.รหัสผ่านหรือรหัสความปลอดภัยอื่น ๆ ที่ให้การเข้าถึงข้อมูล (มาตรา 202a (2)) หรือ	§ 202a StGb. ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับ § 202b StGb. ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับในกรณีที่ความผิดนั้นไม่ต้องรับโทษหนักกว่าตามบทบัญญัติอื่น § 202c StGb. ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับ § 263a StGb. ต้องระวางโทษไม่เกิน 5 ปี หรือมีโทษปรับ หรือจำคุกไม่เกินสามปีหรือปรับ สำหรับกรณีที่เป็นเพียงการตระเตรียมการเพื่อกระทำความผิด § 269 StGb. ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือมีโทษปรับ	§ 77 StGb. (1) ในความผิดที่ต้องร้องทุกข์กล่าวโทษก่อนผู้เสียหายอาจยื่นคำร้องทุกข์ได้เว้นแต่กฎหมายจะบัญญัติไว้เป็นอย่างอื่น (2) ถ้าผู้เสียหายถึงแก่ความตาย ในกรณีที่กฎหมายบัญญัติไว้ สิทธิในการร้องทุกข์ย่อตกทอดแก่คู่สมรส สามีหรือภรรยาซึ่งเป็นเพศเดียวกัน และบุตร หากผู้เสียหายไม่มีคู่สมรสหรือสามาภรรยาซึ่งเป็นเพศเดียวกันหรือบุตร หรือบุคคลเหล่านั้นถึงแก่ความตายก่อนอายุความในการยื่นคำร้องสิ้นสุดลง สิทธินั้นย่อมตกทอดแก่บิดามารดาของผู้เสียหาย ถ้าบิดามารดาถึงแก่ความตายก่อนอายุความในการยื่นคำร้องสิ้นสุดลง ให้สิทธิดังกล่าวตกทอดแก่พี่น้อง และหลานของผู้เสียหาย ถ้าญาติมีส่วนร่วมในการกระทำความผิดหรือคุณสมบัติในฐานะญาติของผู้เสียหายสิ้นสุดลงบุคคลดังกล่าวย่อมถูกตัดสิทธิในการร้องทุกข์ สิทธิ์ในการยื่นคำร้องทุกข์ไม่ตกทอดหากการดำเนินคดีเป็นการขัดหรือแย้งกับเจตนารมณ์ของผู้เสียหาย (3) ถ้าผู้มีสิทธิยื่นคำร้องทุกข์เป็นผู้ไร้ความสามารถตามกฎหมายหรือเป็นผู้ถูกจำกัดความสามารถตามกฎหมาย ผู้แทนตามกฎหมายซึ่งเป็น

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
สหพันธ์สาธารณรัฐเยอรมนี	GERMAN CRIMINAL CODE	2.โปรแกรมคอมพิวเตอร์เพื่อวัตถุประสงค์ในการกระทำความผิดนั้น (2) ให้นำมาตรา 149 (2) และ (3) มาใช้บังคับ **§ 263a StGb.** "(1) ผู้ใดโดยเจตนา เพื่อให้ตนเองหรือผู้อื่นได้ประโยชน์ในทางทรัพย์สินโดยไม่ชอบด้วยกฎหมาย และทำให้ทรัพย์สินของผู้อื่นได้รับความเสียหาย ด้วยการกระทำให้ผลที่แสดงจากการประมวลผลเป็นไปตามความต้องการของตน โดยใช้โปรแกรมที่มีจัดการ ไม่ถูกต้อง โดยใช้ข้อมูลที่ไม่ถูกต้องหรือไม่ครบถ้วนสมบูรณ์ โดยใช้ข้อมูลโดยไม่มีอำนาจ หรือโดยประการอื่นใดโดยไม่ได้รับอนุญาต (2) ให้นำมาตรา 263 (2) ถึง (6) มาใช้บังคับกับการกระทำความผิดตามวรรคแรกโดยอนุโลม” (3) ผู้ใดตระเตรียมการกระทำความผิดตาม (1) โดย 1. ผลิตโปรแกรมคอมพิวเตอร์โดยมีวัตถุประสงค์เพื่อกระทำการดังกล่าวหรือจัดหาโปรแกรมดังกล่าวไว้ใช้เองหรือผู้อื่น หรือ 2. ผลิต จัดหาไว้สำหรับตนเองหรือผู้อื่น เสนอขาย จัดเก็บ หรือจัดหารหัสผ่านอื่นหรือรหัสความปลอดภัยอื่นที่		ผู้จัดการงานอันเป็นการเฉพาะตัวและผู้มีหน้าที่ดูแลบุคคลนั้นๆ มีสิทธิยื่นคำร้องทุกข์ได้ (4) ถ้าผู้เสียหายหลายคนมีสิทธิยื่นคำร้องทุกข์ ผู้สีสิทธิแต่ละคนอาจยื่นคำร้องทุกข์ได้ด้วยตัวเอง

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
สหพันธ์สาธารณรัฐเยอรมนี	GERMAN CRIMINAL CODE	เหมาะสมแก่การกระทำดังกล่าว (4) ในกรณีตามอนุมาตรา (3) ให้นำมาตรา 149 (2) และ (3) มาใช้บังคับ § 269 StGb. (1)ผู้ใดกระทำการด้วยเจตนาฉ้อโกงต่อกฎหมาย ทำการบันทึก หรือแก้ไขเปลี่ยนแปลงข้อมูลที่เป็นพยานหลักฐานเพื่อให้ผู้อื่นหลงเชื่อว่าเอกสารเท็จ หรือปลอมนั้นมีอยู่ หรือเพื่อใช้ประโยชน์จากข้อมูลที่ตนได้บันทึก หรือเปลี่ยนแปลงนั้น (2) การพยามกระทำความผิดตามมาตรานี้ผู้กระทำจะต้องรับโทษด้วย (3) ให้นำมาตรา 267 (3) และ (4) มาใช้บังคับโดยอนุโลม		

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
สาธารณรัฐฝรั่งเศส	FRANCE CRIMINAL CODE - CRIMINAL PROCEDURE CODE - CIVIL COAD - INTELLECTUAL PROPERTY COAD	Le Code pénal Article 226-4-1 การกระทำเพื่อหรือใช้ข้อมูลอย่างใดอย่างหนึ่งเพื่อช่วยในการเข้าถึงข้อมูลส่วนบุคคลโดยมีจุดประสงค์เพื่อรบกวนความสงบสุขของผู้อื่นหรือของผู้อื่น หรือบ่อนทำลายเกียรติ การกระทำความผิดตามวรรคหนึ่งบนเครือข่ายสื่อสารออนไลน์สาธารณะถือว่ามีโทษเท่ากันเมื่อการกระทำนั้นจุดประสงค์เพื่อแย่งชิงข้อมูลส่วนบุคคลของผู้อื่น การขโมยข้อมูลส่วนบุคคลของผู้อื่นซึ่งกระทำโดยคู่สมรสหรือหุ้นส่วนคู่ชีวิตของเหยื่อหรือโดยคู่สัญญาทางแพ่งของเหยื่อการกระทำเหล่านี้ Article 226-18 การรวบรวมข้อมูลส่วนบุคคลด้วยวิธีการฉ้อฉล ไม่ยุติธรรมหรือผิดกฎหมายต้องระวางโทษตามกฎหมาย Article 313-1 การฉ้อโกง คือ การแสดงตนเป็นบุคคลอื่นโดยเจตนาหลอกลวง หรือทำให้สำคัญผิดในข้อเท็จจริง โดยการใช้กลอุบายหลอกลวง เพื่อให้บุคคลอื่น ส่งเงิน หลักทรัพย์หรือทรัพย์สินใดๆเพื่อให้บริการหรือยินยอมต่อการกระทำที่เป็นภาระผูกพันถือเป็นการกระทำความผิดฐานการฉ้อโกง	Le Code pénal Article 226-4-1 ต้องระวางโทษจำคุก 1 ปีและปรับ 15,000 ยูโร หรือจำคุกสองปีและปรับ 30,000 ยูโร สำหรับกรณีการกระทำที่เกิดขึ้นโดยคู่สมรสหรือหุ้นส่วนคู่ชีวิตของเหยื่อ หรือโดยคู่สัญญาทางแพ่งของเหยื่อ Article 226-18 ต้องระวางโทษจำคุก 5 ปีและปรับ 300,000 ยูโร Article 313-1 ต้องระวางโทษจำคุก5ปีและปรับ375,000ยูโร Article 323-1 ต้องระวางโทษจำคุก 3 ปีและปรับ 100,000 ยูโร ต้องระวางโทษจำคุก 5 ปีและปรับ 150,000 ยูโร ต้องได้รับโทษเพิ่มขึ้นต้องระวางโทษจำคุก7 ปีและปรับ 300,000 ยูโร Article 323-3 โทษจำคุกห้าปีและปรับ 150,000 ยูโร หรือหากการกระทำความผิดนั้นเกิดขึ้นต่อหน่วยงานของรัฐโทษจะเพิ่มขึ้นเป็นจำคุก 7 ปีและปรับ 300,000 ยูโร Code de la propriété intellectuelle Article L.335-2 การปลอมแปลงผลงานที่ตีพิมพ์ภายในฝรั่งเศสหรือใน	Code de la Droit civil Article 1240 ผู้ใดกระทำการที่ก่อให้เกิดความเสียหายแก่ผู้อื่นผู้นั้นต้องชดใช้ค่าเสียหายในความผิดที่ได้กระทำไป. Code de procedure pénale Article 1 การดำเนินการตามกฎหมายสำหรับบทลงโทษมีขั้นตอนและดำเนินการโดยฝากหรือเจ้าหน้าที่ที่กฎหมายอนญาติการดำเนินการนี้อาจเริ่มต้นโดยฝ่ายที่อยู่ภายใต้เงื่อนไขที่กำหนดโดยบทบัญญัตินี้ Article 2 การดำเนินคดีทางแพ่งสามารถกระทำได้โดยผู้เสียหายซึ่งเป็นบุคคลที่ได้รับความเสียหายโดยตรงจากการกระทำความผิดอาญาในฐานความผิดลหุโทษ หรือที่เป็นความผิดต่อส่วนตัว

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
สาธารณรัฐฝรั่งเศส	FRANCE CRIMINAL CODE - CRIMINAL PROCEDURE CODE - CIVIL COAD - INTELLECTUAL PROPERTY COAD	Article 323-1 ผู้ใดเข้าถึงหรือฉ้อโกงต่อระบบการประมวลผลข้อมูลอัตโนมัติโดยมิชอบไม่ว่าจะทั้งหมดหรือบางส่วนของ หากการกระทำความผิดในวรรคหนึ่งนั้นส่งผลให้เกิดการลบล้าง หรือเปลี่ยนแปลงข้อมูลที่อยู่ในระบบ หรือเปลี่ยนแปลงการทำงานของระบบ หากการกระทำความผิดตามวรรคหนึ่งและวรรคสองเป็นการกระทำต่อระบบการประมวลผลข้อมูลอัตโนมัติของหน่วงงานของรัฐ Article 323-3 การนำข้อมูลเข้าสู่ระบบการประมวลผลอัตโนมัติอย่างฉ้อฉล การสกัด การถือครอง การทำซ้ำ การส่ง การลบหรือการฉ้อฉลแก้ไขข้อมูลที่มีอยู่ เมื่อความผิดนี้เกิดขึ้นกับระบบประมวลผลข้อมูลส่วนบุคคลอัตโนมัติที่ดำเนินการโดยรัฐ Code de la propriété intellectuelle Article L.335-2 งานเขียน บทประพันธ์ดนตรี ภาพวาด หรือการผลิตอื่นใด ไม่ว่าจะด้วยวิธีการพิมพ์หรือแกะสลักทั้งหมดหรือบางส่วน อันเป็นการฝ่าฝืนกฎหมายและข้อบังคับที่เกี่ยวข้องกับทรัพย์สินทางปัญญาของผู้ประพันธ์ ถือว่าการกระทำ	ต่างประเทศมีโทษจำคุก3 ปี และปรับ 300,000 ยูโร หรือหากการกระทำความผิดตามวรรคหนึ่งเป็นการกระทำโดยกลุ่มบุคคล บทลงโทษจะเพิ่มขึ้นเป็นจำคุก 7 ปี และปรับ 750,000 ยูโร	

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
สาธารณรัฐฝรั่งเศส	FRANCE CRIMINAL CODE - CRIMINAL PROCEDURE CODE - CIVIL COAD - INTELLECTUAL PROPERTY COAD	นั้นเป็นการละเมิดและการละเมิดใดๆ ถือเป็นความผิดให้นำบทลงโทษในวรรคสองมาบังคับใช้โดยอนุโลมกระทำความผิดตามวรรคหนึ่งต่อการส่งออก การนำเข้า การขนถ่าย หรือการกักขังเพื่อวัตถุประสงค์ดังกล่าวข้างต้นของสิ่งที่ละเมิด Article L.713-2 ห้ามมิให้ใช้ เว้นแต่จะได้รับอนุญาตจากเจ้าของเครื่องหมายการค้าที่จดทะเบียน การใช้เครื่องหมายการค้าของบุคคลอื่นในการประกอบธุรกิจสำหรับผลิตภัณฑ์หรือบริการ : 1. เครื่องหมายที่เหมือนกับเครื่องหมายการค้าซึ่งใช้สำหรับผลิตภัณฑ์หรือบริการที่เหมือนกับเครื่องหมายที่จดทะเบียนไว้จากเจ้าของเครื่องหมายการค้าที่แท้จริง 2. เครื่องหมายที่เหมือนหรือคล้ายกับเครื่องหมายการค้าที่ใช้สำหรับสินค้าหรือบริการที่เหมือนหรือคล้ายกับเครื่องหมายที่จดทะเบียนไว้ซึ่งอาจทำให้ประชาชนทั่วไปเกิดความสับสนและสำคัญผิดระหว่างเครื่องหมายการค้าที่จดทะเบียนกับเครื่องหมายการค้าที่เหมือนทำเลียนแบบ		

ตารางที่ 3.1 (ต่อ)

ประเทศ / รัฐ	กฎหมาย	บทบัญญัติ	บทลงโทษ	ผู้มีสิทธิดำเนินคดี
สาธารณรัฐฝรั่งเศส	FRANCE CRIMINAL CODE - CRIMINAL PROCEDURE CODE - CIVIL COAD - INTELLECTUAL PROPERTY COAD	Article L.713-3 ห้ามมิให้ใช้ เว้นแต่จะได้รับอนุญาตจากเจ้าของเครื่องหมายการค้าที่จดทะเบียนของเครื่องหมายที่เหมือนหรือคล้ายกับเครื่องหมายที่มีชื่อเสียง และใช้กับสินค้าหรือบริการที่เหมือนกัน คล้ายคลึง หรือไม่คล้ายคลึง แก่ผู้ที่เครื่องหมายได้รับการจดทะเบียน หากการใช้เครื่องหมายนี้โดยไม่มีเหตุอันควร เป็นการใช้ประโยชน์จากลักษณะเด่นหรือชื่อเสียงของเครื่องหมายอย่างไม่เป็นธรรม หรือเป็นผลเสียต่อเครื่องหมายนั้น		

3.4 มาตรการความร่วมมือระหว่างประเทศ

เนื่องจากลักษณะและรูปแบบอันเป็นพื้นฐานของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นมีลักษณธการกระทำที่ไร้พรมแดนที่อาจมีความเกี่ยวข้องกับหมลายประเทศเพราะในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นอาจเกิดขึ้นที่ไหนก็ได้บนโลกซึ่งทำให้การตามจับกุมตัวผู้กระทำความมาลงโทษเป็นเรื่องที่เกิดขึ้นได้ยากมาก ด้วยเหตุนี้เองการป้องกันหรือแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์จึงเป็นเรื่องที่ไม่อาจที่จะกระทำได้ด้วยการบังคับใช้มาตรการทางกฎหมายที่จำกัดอยู่เฉพาะอาณาเขตของประเทศใดประเทศหนึ่ง ด้วยเหตุนี้เอง จึงทำให้นานาประเทศซึ่งรวมไปถึงองค์กรระหว่างประเทศต่างๆ ทั้งทวิภาคีและพหุภาคี ได้ร่วมกันคิดค้นและพัฒนาแนวทางในการแก้ปัญหาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ไม่ว่าจะเป็นในรูปแบบของ อนุสัญญาระหว่างประเทศ หรือกรอบความร่วมมือระหว่าประเทศ ซึ่งมาตรการต่างๆดังที่ได้กล่าวนี้นั้นผู้เขียนจะได้อธิบายต่อไป ดังนี้

3.4.1 องค์การเพื่อความร่วมมือทางเศรษฐกิจ และพัฒนา

Organization for Economic cooperation and Development หรือ OEDC ถือได้ว่าเป็นองค์กรระหว่างประเทศแรกๆที่ให้กับปัญหาการก่ออาชญากรรมคอมพิวเตอร์ซึ่งในปีค.ศ.1983 OEDC ได้ตั้งคณะทำงานขึ้นมาหนึ่งชุดซึ่งประกอบไปด้วยผู้เชี่ยวชาญด้านการก่ออาชญากรรมคอมพิวเตอร์เพื่อศึกษาและหาแนวทางในการแก้ไขปัญหาการก่ออาชญากรรมทางคอมพิวเตอร์และจัดทำข้อเสนอแนะในการบัญญัติกฎหมาย

ให้กับประเทศในกลุ่มสมาชิกกว่า 38 ประเทศทั่วโลก[168] ทั้งนี้เพื่อให้แนวทางในการกำหนดบทบัญญัติทางกฎหมายของประเทศในกลุ่มสมาชิกเป็นไปในแนวทางเดียวกันเพื่อให้สอดคล้องกับหลักสากลในการส่งตัวผู้ร้ายข้ามแดนหากมีกรณีการก่ออาชญากรรมทางคอมพิวเตอร์ขึ้นในกลุ่มประเทศสมาชิก โดยมีความผิดสำคัญ เช่น การปลอมแปลงข้อมูลคอมพิวเตอร์ การขัดขวางการทำงานของระบบคอมพิวเตอร์[169]

3.4.2 กลุ่มประเทศอุตสาหกรรมชั้นนำโลก

กลุ่มประเทศอุตสาหกรรมชั้นนำโลก (The Group of Eight) หรือ G8 ประกอบไปด้วยประเทศสมาชิก 8 ประเทศ คือ แคนนาดา, ฝรั่งเศส, เยอรมนี, รัสเซีย, อิตาลี, ญี่ปุ่น, สหราชอาณาจักร และสหรัฐอเมริกา ได้จัดตั้งคณะอนุกรรมการว่าด้วยอาชญากรรมทางไซเบอร์ (Subcommittee on High-tech Crimes) ขึ้นในปี ค.ศ.1997[170] เพื่อทำการศึกษาแนวทางในการต่อต้านการก่ออาชญากรรมทางไซเบอร์ และจำแนกประเภทของ High-Tech Crime[171] เพื่อเป็นแนวทางในการกำหนดหลักการเพื่อใช้ในการควบคุมอาชญากรรมทางไซเบอร์ โดยภายหลังการประชุมกลุ่ม ณ กรุงวอชิงตัน ในปีเดียวกันนี้เองก็ได้มีการกำหนดหลักการและแบบแผนในการต่อต้านการก่ออาชญากรรมทางไซเบอร์ เพื่อป้องกันการโจรกรรมข้อมูลและปกป้องระบบคอมพิวเตอร์จากการเข้าถึงโดยมิชอบ[172] โดยมีหลักการที่น่าสนใจ คือ การพัฒนาขีดความสามารถของบุคลากรเพื่อให้มีความรู้ความสามารถในการป้องกันและปราบปรามการก่ออาชญากรรมไซเบอร์ซึ่งรวมไปถึงการการพัฒนาและเพิ่มประสิทธิภาพของเครื่องมือที่จะนำมาใช้ในการป้องกันและปราบปรามการก่ออาชญากรรมทางไซเบอร์ อย่างไรก็ดีหลังจากการประชุมในปี ค.ศ 1997 ก็ได้มีการจักการประชุมและพัฒนามาตรการในการรับมือและปราบปรามต่างๆเรื่อยมา จนกระทั้งในการประชุมกลุ่มปี ค.ศ 1999 ได้มีการกำหนดให้ประเทศสมาชิกต้องเปิดช่องทางการติดต่อสื่อสารเพื่อเป็นเครือข่ายในการติดต่อประสานงานระหว่างประเทศเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์มีเจ้าหน้าที่ปฏิบัติหน้าที่ประสานงานตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์ ซึ่งตั้งแต่ปี ค.ศ 2006 เป็นต้นมาวาระในการประชุมก็มีความมุ่นเน้นที่เพิ่มมากขึ้นอย่างมีนัยสำคัญในการแก้ไขปัญหาการก่ออาชญากรรมประเภทการก่อการร้ายทางไซเบอร์ (Cyberterrorism)[173]

3.4.3 คณะมนตรียุโรป

คณะมนตรีแห่งยุโรป (The Council of Europe) หรือ สภายุโรป ได้มีการจัดตั้งคณะกรรมาธิการซึ่งประกอบไปด้วยผู้เชี่ยวชาญด้านอาชญากรรมคอมพิวเตอร์ (Select Committee of Experts for

---

[168] OECD, 'Who we are' (OECD) <https://www.oecd.org/about/> สืบค้นเมื่อ 15 เมษายน 2566.

[169] สาวตรี ศรีสุข (เชิงอรรถ 104) 50.

[170] เพิ่งอ้าง 51.

[171] กุลธิดา อาธิเจริญสุข (เชิงอรรถ 64) 105.

[172] Claire Bernier (เชิงอรรถ 152).

[173] ดู Marco Gercke, 'understanding cybercrime: Phenomena challenges and legal response' (ITU) <https://www.itu.int/ITUD/cyb/cybersecurity/docs/cybercrime%20legislation%2> สืบค้นเมื่อ 15 เมษายน 2566.

Computer-Related Crime) ขึ้นในปี ค.ศ. 1985 เพื่อศึกษาและกำหนดแนวทางในการบัญญัติกฎหมาย[174] โดยคณะกรรมาธิการได้หารือและจัดทำข้อเสนอ เลขที่ R(89)9[175] ซึ่งมีวัตถุประสงค์เพื่อให้เป็นกรอบแนวทางในการกำหนดฐานความผิดเกี่ยวกับคอมพิวเตอร์ อีกทั้งเพื่อให้เป็นกรอบในการพิจารณาทบทวนปรับปรุงหรือบัญญัติกฎหมายภายในของประเทศสมาชิกให้มีความครอบคลุมถึงลักษณะที่ควรบัญญัติไว้ให้เป็นความผิด[176] ซึ่งครอบคลุมความผิดหลายฐานอันได้แก่ การปลอมแปลงข้อมูลคอมพิวเตอร์, การฉ้อโกงที่เกี่ยวกับคอมพิวเตอร์, การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ, การดักรับข้อมูลคอมพิวเตอร์, การก่อวินาศกรรมทำลายระบบหรือข้อมูลคอมพิวเตอร์ และการโจรกรรมข้อมูลคอมพิวเตอร์ นอกจากนี้ยังรวมไปถึงการใช้และเข้าถึงซอฟต์แวร์โดยมิชอบอีกด้วย[177]

3.4.4 สหภาพยุโรป

สหภาพยุโรป (European Union) หรือ EU ได้มีการพัฒนามาตรการทางกฎหมายขึ้นมาเพื่อใช้เป็นกรอบในการบัญญัติกฎหมายที่ใช้ในการควบคุมและปราบปรามการก่ออาชญากรรมทางไซเบอร์ซึ่งมีผลผูกพันเฉพาะประเทศกลุ่มสมาชิกเท่านั้น แต่ไม่ว่าอย่างไรก็ตามก็ยังมีหลายประเทศในภูมิภาคนอกกลุ่มสมาชิกใช้เป็นเกณฑ์อ้างอิงในการบัญญัติกฎหมายต่างๆภายในประเทศของตน โดยมาตรฐานเช่นว่านี้คือมาตรฐานหรือกรอบทางกฎหมายที่คณะกรรมาธิการยุโรป(European- Commission) ได้นำเสนอต่อสภายุโรป (European Council) เพื่อใช้ในการพิจารณาและประกาศบังคับใช้ภายในประเทศกลุ่มสมาชิก อาทิ ในปี ค.ศ.1998 ได้มีการเสนอ Legal Aspects of Computer-Related Crime in the Information Society COMCRIME Study. ที่มีเนื้อหาที่เกี่ยวข้องกับการก่อความไม่สงบและแนวทางการแก้ไขต่างๆ และต่อมาในปี ค.ศ. 2000 ก็ได้มีการออกมติว่าด้วยการต่อต้านสื่อลามกอนาจารเด็กบนอินเทอร์เน็ต (Council Decision to Combat Child Pornography on the-Internet) ซึ่งอยู่ภายใต้กรอบของมติเดิมที่ออกมาในปี ค.ศ. 1996 ที่เกี่ยวข้องกับการจัดการเนื้อหาที่ผิด กฎหมายและเป็นอันตรายบนอินเทอร์เน็ต ซึ่งรวมไปถึงการส่งเสริมการใช้อินเทอร์เน็ตอย่างปลอดภัย และมติของปี ค.ศ. 1999 เพื่อต่อต้านเนื้อหาที่ผิดกฎหมายและเป็นอันตรายบนเครือข่ายอินเทอร์เน็ตทั่วโลก[178]

---

[174] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, *แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์* (พิมพ์ครั้งที่ 2, สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ 2547) 65.

[175] ดู 'RECOMMENDATION No. R (89) 9' (The Council of Europe) <https://rm.coe.int/09000016804f1094> สืบค้นเมื่อ 15 เมษายน 2566.

[176] ดู 'Computer-related Crime: Recommendation No. R(89)9 on Computer-related Crime and Final Report of the European Committee on Crime Problems' (Office of Justice Programs) <https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-related-crime-recommendation-no-r899-computer-related> สืบค้นเมื่อ 15 เมษายน 2566.

[177] สาวตรี ศรีสุข (เชิงอรรถ 104) 52.

[178] เพิ่งอ้าง 54.

แต่ไม่ว่าอย่างไรก็ตาม มติดังกล่าวไม่ถือเป็นข้อผูกมัดให้รัฐสมาชิกต้องบัญญัติหรือออกมาตรการทางอาญาที่เฉพาะเจาะจงภายในประเทศของตนเพียงแต่ใช้เพื่อเป็นกรอบในการบัญญัติฐานความผิดเพียงเท่านั้น โดยต่อมาในปี ค.ศ. 2001 ก็ได้มีการออกมติจากคณะมนตรีแห่งสหภาพยุโรปว่าด้วยการต่อต้านการฉ้อโกงและการปลอมแปลงการชำระเงินที่ไม่ใช้เงินสด (Framework Decision on Combating Fraud)[179] เพื่อใช้เป็นกรอบแนวทางสำหรับ การออกกฎหมายเพื่อต่อต้านอย่างเป็นทางการ โดยมีพันธะผูกพันให้บรรดารัฐสมาชิกต้องบัญญัติกฎหมายอาญาที่เกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์ ซึ่งรวมไปถึงการผลิตเครื่องมือ เช่น โปรแกรม คอมพิวเตอร์ที่พัฒนาขึ้นเพื่อนำมาใช้กระทำความผิดเรื่องนี้โดยเฉพาะด้วย[180] และต่อมาในปี ค.ศ. 2005 ก็มีได้มีการออกมติซึ่งมุ่งเน้นไปที่การออกทั้งกฎหมายสารบัญญัติ และ กฎหมายวิธีสบัญญัติ เพื่อปกป้องระบบและข้อมูลคอมพิวเตอร์จากการถูกบุกรุก หรือ ถูกรบกวน[181] (Framework Decision on Attacks against Information systems)[182] ทั้งนี้เพื่อให้สอดคล้องและเป็นไปในแนวทางเดียวกัน นอกจากนี้ยังได้กำหนดแนวทางการให้ความร่วมมือทางอาญาระหว่างประเทศสมาชิกอีกด้วย

3.4.5 ความร่วมมือทางเศรษฐกิจเอเชียแปซิฟิก

กลุ่มความร่วมมือทางเศรษฐกิจเอเชียแปซิฟิก (Asia-Pacific Economic Cooperation) หรือ APEC ได้ริเริ่มให้ความสำคัญกับการแก้ปัญหาอาชญากรรมคอมพิวเตอร์อย่างจริงจังตั้งแต่ปี ค.ศ.2001 อันเนื่องมาจากการผลักดันของประเทศสหรัฐอเมริกาที่ต้องการส่งเสริมให้ประเทศต่างๆ ให้ความสำคัญกับปัญหาการก่อการร้าย โดยเฉพาะอย่างยิ่งการก่อการร้ายในรูปแบบของอาชญากรรมคอมพิวเตอร์ที่ส่งผลกระทบอย่างร้ายแรงต่อระบบควบคุมสาธารณูปโภคพื้นฐานของประเทศ กระทั้งในปี ค.ศ. 2002 โดยรัฐมนตรีโทรคมนาคมและสารสนเทศทางเศรษฐกิจของเอเปคได้ออกปฏิญญาเซี่ยงไฮซึ่งรวมไปถึงแถลงการณ์เกี่ยวกับความปลอดภัยของโครงสร้างพื้นฐานด้านข้อมูลและการสื่อสาร ซึ่งภายหลังการออกปฏิญญาเซี่ยงไฮ ในการประชุมกลุ่มครั้งที่ 26 จึงได้มีการจัดทำ APEC Cyber security Strategy ซึ่งประกอบด้วยการพัฒนาในด้านกฎหมายอาชญากรรมไซเบอร์ แนวทางด้านความปลอดภัยและทางเทคนิค การเพิ่มความรับรู้ของสาธารณชน การฝึกอบรมและการศึกษาแนวทางในการป้องกันและปราบปรามการก่ออาชญากรรมทางไซเบอร์[183]

3.4.6 สมาคมประชาชาติแห่งเอเชียงตะวันออกเฉียงใต้

สมาคมประชาชาติแห่งเอเชียงตะวันออกเฉียงใต้ (Association of South East Asian Nations) หรือ อาเซียน (ASEAN) ได้ตระหนักถึงความจำเป็นในการเสริมสร้างความร่วมมือในการต่อต้านอาชญากรรม

---

[179] ดู ‘Combating fraud and counterfeiting of non-cash means of payment’ (EUR-Lex) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001F0413> สืบค้นเมื่อ 16 เมษายน 2566.

[180] EU Framework Decision on Combating Fraud, Article3.

[181] EU Framework Decision on Attacks against Information systems, Article2, 3and4.

[182] ดู ‘On attacks against information systems’ (EUR-Lex) <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32005F0222> สืบค้นเมื่อ 16 เมษายน 2566.

[183] ดู ‘APEC Cyber Security Strategy (2002)’ (Regional Cooperation Council) <https://www.rcc.int/swp/docs/105/apec-cyber-security-strategy-2002> สืบค้นเมื่อ 16 เมษายน 2566.

ทางไซเบอร์ อันเนื่องมาจากการก่ออาชญากรรมไซเบอร์ถือเป็นภัยคุกคามต่อความมั่นคงของชาติอันเป็นผลเสียจากการใช้เทคโนโลยีสารสนเทศและการสื่อสารในทางที่ผิด และถือเป็นการละเมิด ทั้งนี้ อาชญากรรมทางไซเบอร์มีลักษณะเฉพาะและเป็นอาชญากรรมข้ามพรมแดนที่ส่งผลกระทบต่ออธิปไตยของทุกรัฐ ดังนั้นใน การประชุมสุดยอดผู้นำอาเซียน ครั้งที่ 31 ปี ค.ศ.2017 เหล่าผู้นำอาเซียนซึ่งรวมไปถึงประเทศไทยได้ให้การลงนามใน “ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ (ASEAN Declaration to Prevent and Combat Cybercrime)”

โดยปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ได้ให้ความสำคัญกับการปรับปรุงกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์และหลักฐานทางอิเล็กทรอนิกส์ รวมทั้งสนับสนุนการร่างกรอบการทำงานระดับภูมิภาคเพื่อสร้างความร่วมมือระหว่างประเทศสมาชิกและการกำหนดแผนปฏิบัติการระดับชาติในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ รวมถึงการให้ความช่วยเหลือด้านผู้เชี่ยวชาญทางเทคนิคในการป้องกันและต่อต้านอาชญากรรมไซเบอร์ อันเป็นการยกระดับความร่วมมือระหว่างประเทศสมาชิกอาเซียนและประเทศคู่เจรจา รวมทั้งหน่วยงานและองค์กรต่าง ๆ ที่เกี่ยวข้องทั้งในระดับภูมิภาคและนานาชาติ เช่น หัวหน้าตำรวจอาเซียน หัวหน้าตำรวจภาคพื้นยุโรป และองค์การตำรวจสากล นอกจากนี้ ปฏิญญาฯ ยังมีวัตถุประสงค์ในการเสริมสร้างความมั่นคงทางเทคโนโลยี การป้องกัน และความสามารถในการแก้ไขปัญหาเกี่ยวกับอาชญากรรมทางไซเบอร์ และเพื่อพัฒนาขีดความสามารถของอาเซียนในการสร้างและพัฒนาศักยภาพในการต่อสู้กับอาชญากรรมทางไซเบอร์อีกด้วย[184]

[184] สำนักงานคณะกรรมการกฤษฎีกา, ‘ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ และบทวิเคราะห์กฎหมายไทยที่เกี่ยวข้อง’ (LAW FOR ASEAN, 12 มกราคม 2561) <https://lawforasean.-krisdika.go.th/Content/View?Id=349&Type=1> สืบค้นเมื่อ 16 เมษายน 2566.

บทที่ 4
วิเคราะห์การบังคับใช้กฎหมายเกี่ยวกับฟิชชิ่งที่เป็นการฉ้อโกงประชาชน

ฟิชชิ่งถือได้ว่าเป็นอาชญากรรมทางคอมพิวเตอร์ประเภทหนึ่งที่มีแนวโน้มเพิ่มมากขึ้นในปัจจุบันซึ่งก่อให้เกิดความเสียหายต่อหลายภายส่วนโดยเฉพาะอย่างยิ่งในภาคประชาชนที่ตกเป็นเหยื่อจากการหลอกลวงของอาชญกร แม้จะมีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อนำมาใช้ลงโทษกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์โดยเฉพาะแต่ไม่ว่าอย่างไรก็ตามแม่จะมีการประกาศใช้กฎหมายเพื่อควบคุมป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แต่กฎหมายดังกล่าวนี้นั้นก็ไม่สามารถที่จะนำมาบังคับใช้ได้อย่างมีประสิทธิภาพดังจะเห็นได้จากสถิติในปี 2564 มีการแจ้งความอาชญากรรมทางไซเบอร์ทุกประเภททั้งสิ้น 2,069 ครั้ง ส่วนปี 2565 มีภัยคุกคามทั้งหมด 2,279 ครั้ง[185] และมีแนวโน้มคาดว่าในปี 2566 นี้อาจมีจำนวนภัยคุกคามเพิ่มมากขึ้น[186] โดยจากการศึกษาพบว่าปัญหาการก่ออาชญากรรมคอมพิวเตอร์ประเภทฟิชชิ่ง หรือ หลอกลวงให้กรอกข้อมูลทางการเงิน โดยการส่งจดหมายอิเล็กทรอนิกส์แอบอ้างว่าเป็นผู้แทนโดยชอบของธนาคารต้องการให้อัพเดตข้อมูลทางการเงิน หรือโทรศัพท์หาเหยื่อแอบอ้างเป็นเจ้าพนักงานตำรวจแล้วออกอุบายให้โอนเงินเพื่อตรวจสอบ หรือ สร้างเว็ปปลอมที่มีหน้าตาเหมือนกับเว็บที่แท้จริงเพื่อทำให้เหยื่อสับสนและเผลอให้ข้อมูลสำคัญไป โดยปัญหาเหล่านี้เป็นปัญหาที่เกิดขึ้นทั่วโลกและนานาประเทศก็ต่างหาหนทางที่จะจัดการกับปัญหาเหล่านี้โดยเฉพาะอย่างยิ่งในประเทศไทยที่ถือได้ว่าเป็นประเทศหนึ่งที่มีปัญหาการก่ออาชญากรรมมากติดอันดับต้นๆของโลก ด้วยเหตุนี้เองจึงมีความจำเป็นที่จะต้องวิเคราะห์ถึงปัญหาและสภาพในการบังคับใช้กฎหมายในปัจจุบันเพื่อหาแนวทางในการปราบปรามและป้องกันตลอดจนการศึกษาหาแนวทางในการแก้ไขข้อบกพร้องที่เกิดขึ้นในการบังคับใช้กฎหมายซึ่งรวมไปถึงการพิจารณาเกี่ยวกับความเหมาะสมของบทลงโทษ การเรียกร้องค่าเสียหาย และสิทธิของผู้เสียหายเพื่อให้สอดคล้องและเหมาะสมกับสถานะการณ์และผลกระทบที่เกิดขึ้นในปัจจุบัน

4.1 วิเคราะห์การบังคับใช้กฎหมายที่เกี่ยวกับฟิชชิ่งตามประมวลกฎหมายอาญา

กฎหมายอาญานั้นเป็นกฎหมายที่มีความเป็นเอกลักษณ์เฉพาะตัว ซึ่งแตกต่างไปจากกฎหมายอื่นเนื่องจากกฎหมายอาญานั้นเป็นกฎหมายที่เกี่ยวของและกระทบต่อการดำเนินชีวิต โดยมีหลักการสำคัญคือหลัก ไม่มีความผิด ไม่มีโทษ หากไม่มีกฎหมาย ที่แปลมาจากสุภาษิตภาษาละตินว่า Nullum crimem nulla poena sine lege หรือ No Crime Nor Punishment without Law ซึ่งถูกบัญญัติไว้ในประมวลกฎหมาย

---

[185] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ‘สถิติภัยคุกคามประจำปี 2565’ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์) <https://www.etda.or.th/th/Our-Service/thaicert/stat.aspx> สืบค้นเมื่อ 17 เมษายน 2566.

[186] จิราภพ ทวีสูงส่ง, ‘เรื่องใกล้ตัวกว่าที่คิด! “อาชญากรรมทางไซเบอร์” รู้จักไว้..ป้องกันภัยไม่ตกเป็นเหยื่อ’ (Thai PBS, 23 กุมภาพัน 2566) <https://www.thaipbs.or.th/now/content/68> สืบค้นเมื่อ 17 เมษายน 2566.

อาญา มาตรา 2[187] และเนื่องจากกระทำฟิชชิ่งนั้นถือได้ว่ามีลักษณะที่เป็นการกระทำความผิดทางอาญาประเภทหนึ่ง ดังนั้น จึงต้องนำประมวลกฎหมายอาญาที่เป็นหลักกฎหมายพื้นฐานในการกำหนดความผิดอันมีโทษมาศึกษาวิเคราะห์เพื่อให้เกิดความเข้าใจที่มากยิ่งขึ้น อีกทั้งเมื่อพิจารณาจากลักษณะในการฟ้องคดีกับผู้ที่กระทำผิดทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่คณะกรรมการกฤษฎีกาได้เคยให้ความเห็นไว้ว่าในการฟ้องคดีหากพบว่ากระทำความผิดนั้นเป็นความผิดตามกฎหมายอื่น ก็สามารถที่จะฟ้องผู้กระทำความผิดนั้นในฐานความผิดตามประมวลกฎหมายอื่นได้อีก

4.1.1 ความผิดที่เกี่ยวกับการฉ้อโกง

มาตรา 341 ผู้ใด ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี

องค์ประกอบความผิดภายนอก คือ ผู้ใดการหลอกลวง โดยแสดงข้อความอันเป็นเท็จ หรือ ปกปิดข้อความจริงซึ่งควรบอกให้แจ้งแก่ผู้อื่น ทำให้ผู้อื่นหลงเชื่อ และมีการโอนไปซึ่งทรัพย์สิน โดยผู้กระทำได้ทรัพย์สินไป หรือ มีการทำ/ถอน/ทำลายเอกสารสิทธิ

องค์ประกอบความผิดภายใน คือ กระทำโดยรู้สำนึกในการที่กระทำและในขณะเดียวกันผู้กระทำประสงค์ต่อผล หรือย่อมเล็งเห็นผลของการกระทำนั้น เพื่อแสวงหาประโยชน์ที่ไม่ควรได้โดยชอบด้วยกฎหมายสำหรับตนเอง หรือผู้อื่น

เมื่อพิจารณาถึงองค์ประกอบความผิดเปรียบเทียบกับการฟิชชิ่ง ทำให้ทราบได้ว่าการที่ฟิชเช้อนั้นแสดงข้อความอันเป็นเท็จในจดหมายอิเล็กทรอนิกส์หรือเว็บไซต์ปลอมโดยเจตนาเพื่อให้ผู้เสียหายนั้นหลงเชื่อและได้ไปซึ่งขอมูลส่วนบุคคลหรือทรัพย์สินอื่นใด จากผู้เสียหายเพื่อนำไปใช้ในการแสวงหาประโยชน์ในทางทรัพย์สิน หากเป็นกรณีเช่นนี้ก็จะถือว่าครบองค์ประกอบของความผิดฐานฉ้อโกง แต่ไม่ว่าอย่างไรก็ตามในความผิดฐานฉ้อโกงนั้น มีผู้ให้ความเห็นว่ากรณีการที่ฟิชเช้อได้ไปซึ่งข้อมูลส่วนบุคคลนั้นเป็นเพียงการล่วงรู้และคัดลอกเพียงเท่านั้นไม่ได้ทำให้ข้อมูลนั้นหายไปไหน อันมิใช้การตัดกรรมสิทธิ์ในการครอบครองข้อมูลของผู้เสียหาย อีกทั้งหากเป็นกรณีที่ฟิชเช้อนั้นกระทำต่อระบบคอมพิวเตอร์ซึ่งมิใช้ตัวบุคคล แม้จะได้ไปซึ่งข้อมูลส่วนบุคคลและนำไปใช้ประโยชน์ในทางทรัพย์สินก็ไม่ถือว่าเข้าองค์ประกอบความผิด

ดังนั้น การที่จะพิจารณาว่าการฟิชชิ่งนั้นเข้าองค์ประกอบฉ้อโกงหรือไม่ก็อาจจะต้องพิจารณาถึงการตัดกรรมสิทธิ์ในทรัพย์หรือข้อมูลที่ผู้เสียหายนั้นถือครองอยู่

---

[187] ประมวลกฎหมายอาญา มาตรา 2 บัญญัติว่า บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการอันกฎหมายที่ใช้ในขณะกระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่ผู้กระทำความผิดนั้น ต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย ถ้าตามบทบัญญัติของกฎหมายที่บัญญัติในภายหลัง การกระทำเช่นนั้น.

อนึ่ง สำหรับความผิดตามมาตรา 343 นั้นมีองค์ประกอบความผิดพื้นฐานเช่นเดียวกับความผิดฐานฉ้อโกงแต่เพิ่มองค์ประกอบคือ ด้วยการแสดงข้อความอันเป็นเท็จต่อประชาชน หรือด้วยการปกปิดข้อความจริงซึ่งควรจะบอกให้แจ้งแก่ประชาชน โดยประชาชนในที่นี้หมายถึงบรรดาพลเมืองหรือประชาชนเป็นการทั่วไปทั้งหลาย และไม่ได้ถือเอาจำนวนผู้เสียหายที่ถูกหลอกลวงมากหรือน้อยเป็นเกณฑ์[188]แต่ถือเอาเจตนาการแสดงข้อความอันเป็นเท็จหรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้งแก่ประชาชนโดยทั่วไปเป็นสำคัญ แม้มีคนทราบเพียงคนเดียวก็ผิดฐานนี้ได้

4.2 วิเคราะห์การบังคับใช้กฎหมายที่เกี่ยวกับฟิชชิ่งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับที่2 พ.ศ.2560

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นั้นมีวัตถุประสงค์ในการบัญญัติขึ้นมาเพื่อควบคุมและกำหนดโทษต่อการกระทำความผิดเกี่ยวกับคอมพิวเตอร์โดยมีสาระสำคัญอยู่ที่ การมุ่งคุ้มครองและรักษาความปลอดภัยของระบบคอมพิวเตอร์ ซึ่งรวมไปถึงความถูกต้องสมบูรณ์ของข้อมูลและระบบคอมพิวเตอร์ นอกจากนี้ยังรวมไปถึงการควบคุมและเอาผิดกับการเผยแพร่ข้อมูลที่ไม่เหมาะสมในระบบคอมพิวเตอร์ รวมทั้งอำนาจในการกำหนดข้อปฏิบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ซึ่งรวมไปถึงการกำหนดองค์ประกอบในการกระทำความผิดไม่ว่าจะทางตรงหรือทางอ้อมที่เกี่ยวข้องกับการก่ออาชญากรรมคอมพิวเตอร์ในหลายๆรูปแบบ และจากเหตุผลของการบัญญัติพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ดังที่ได้กล่าวมาในข้างต้นจะเห็นได้ว่าคอมพิวเตอร์นั้นเป็นทั้งเป้าหมายและเครื่องมือที่ถูกใช้ประกอบในการกระทำความผิด กล่าวคือคอมพิวเตอร์นั้นเป็นเครื่องมือที่ใช้ในการเก็บข้อมูลสำคัญต่างๆไม่ว่าจะเป็นข้อมูลในระดับบุคคลหรือองค์กรก็ต่างเก็บข้อมูลไว้ในคอมพิวเตอร์กันทั้งนั้นด้วยเหตุนี้เองจึงทำให้คอมพิวเตอร์ตกเป็นเป้าหมายของการโจมตีจากผู้กระทำความผิดซึ่งก็ใช้คอมพิวเตอร์เป็นเครื่องมือประกอบการกระทำความผิดเช่นกันดังจะสังเกตุได้จากมาตราในพระราชบัญญัติที่ล้วนแล้วแต่เป็นข้อกำหนดที่ป้องกันและกำหนดให้การกระทำความผิดต่อคอมพิวเตอร์เป็นความผิดตาม มาตรา5 การเข้าถึงระบบคอมพิวเตอร์ฯ. มาตรา6 การล้วงรู้มาตรการป้องกันการเข้าถึง. มาตรา7 การเข้าถึงข้อมูลคอมพิวเตอร์. มาตรา 8 การดักรับข้อมูลคอมพิวเตอร์. มาตรา9 การรบกวนข้อมูลคอมพิวเตอร์ฯ. มาตรา10 การรบกวนระบบคอมพิวเตอร์มาตรา11 การส่งจดหมายสแปม. มาตรา14 การปลอมแปลงข้อมูลคอมพิวเตอร์หรือเผยแพร่ข้อมูลที่ไม่เหมาะสม. มาตรา16 การตัดต่อดัดแปลงและเผยแพร่ภาพ แต่ไม่ว่าอย่าไรก็ดีแม้จะมีการบัญญัติมาตราขึ้นเพื่อป้องกันและลงโทษผู้กระทำความผิดมากเพียงไรก็มิได้ทำให้การกระทำผิดลงน้อยลงเมื่อเทียบกับอัตราการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มีแนวโน้มเพิ่มมากขึ้นในปัจจุบันโดยเฉพาะอย่างยิ่งกับการก่ออาชญากรรมฟิชชิ่งที่ก่อให้เกิดความเสียหายอย่างร้ายแรงและเป็นวงกว้างเมื่อเทียบกับความผิดอื่น

การฟิชชิ่งนั้นมีขั้นตอนมากมายในการกระทำความผิดซึ่งตัวผู้กระทำความผิดหรือฟิชเชอร์นั้นจะต้องได้รับโทษหากกระทำความผิดนั้นครบองค์ประกอบความผิดในฐานความผิดต่างๆตามพระราชบัญญัติว่าด้วยการกระ

---

[188] ดู คำพิพากษาศาลฎีกาที่ 563/2531.

ทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และฉบับที่2 พ.ศ.2560 ซึ่งในบางกรณีฟิชเชอร์นั้นอาจจะเข้าสู่ระบบคอมพิวเตอร์ของผู้เสียหายเพื่อให้ได้มาซึ่งข้อมูลสำคัญของผู้เสียหายซึ่งในกรณีสมาทโฟนก็ถือได้ว่าเป็นระบบคอมพิวเตอร์เช่นกัน หรือกรณีการส่งอีเมลสแปมเพื่อลวงให้เหยื่อให้ขอมูลสำคัญแก่ผู้กระทำความผิดซึ่งจะถูกนำไปใช้ในการกระทำความผิดอื่นๆต่อ ซึ่งในหัวข้อที่จะได้กล่าวต่อจากนี้ผู้เขียนจะขอกล่าวถึงแต่เฉพาะฐานความผิดที่มีความเกี่ยวข้องกับการกระทำความผิดประเภทฟิชชิ่งซึ่งรวมไปถึงองค์ประกอบความผิดของฐานความผิดเหล่านั้นตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และฉบับที่2 พ.ศ.2560 ซึ่งมีมาตราสำคัญที่ใช้ในการกำหนดโทษแก่ผู้ที่กระทำความผิดฐานฟิชชิ่ง ดังนี้

4.2.1 การดักรับข้อมูล มาตรา8

องค์ประกอบความผิดที่กฎหมายบัญญัติในมาตรานี้ คือ การที่บุคคลใดก็ตามกระทำการด้วยวิธีการทางอิเล็กทรอนิกส์โดยปราศจากอำนาจกระทำการโดยชอบ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์[189]ของผู้อื่นระหว่างที่กำลังส่งผ่านข้อมูลในระบบคอมพิวเตอร์ซึ่งข้อมูลนั้นมิได้มีไว้เพื่อประโยชน์สาธารณะ โดยเจตนา

องค์ประกอบความผิดภายนอกของความผิดนี้ คือ การที่บุคคลใดก็ตามทำการโดยยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นในระหว่างการส่งข้อมูลในระบบคอมพิวเตอร์ โดยมิชอบ

องค์ประกอบความผิดภายในของความผิดนี้ คือ เจตนาในการดักรับไว้ซึ่งข้อมูลของบุคคลอื่นโดยปราศจากอำนาจกระทำการโดยชอบ โดยผู้กระทำจะต้องมีเจตนาในการดักรับข้อมูลอันเป็นเจตนาตามประมวลกฎหมายอาญามาตรา 59

อนึ่ง นอกจากองค์ประกอบความผิดที่ได้กล่าวมาในข้างต้นนี้แล้วการการกระทำความผิดในมาตรานี้เป็นการกระทำผิดที่ผู้กระทำทำไปโดยปราศจากอำนาจ แต่หากผู้ที่กระทำมีอำนาจที่จะกระทำได้โดยชอบก็ย่อมไม่ถือว่าเป็นความผิดตามมาตรนี้[190]

ทั้งนี้ คำว่าข้อมูลคอมพิวเตอร์คอมพิวเตอร์ที่มิได้มีไว้เพื่อประโยชน์สาธารณะ หมายความว่า ข้อมูลที่เป็นเรื่องเฉพาะตนที่ไม่ต้องการเปิดเผยให้ผู้อื่นทราบซึ่งมีมาตรการป้องกันการเข้าถึงอันมิใช่เพื่อสาธารณะโดยไม่จำเป็นว่าข้อมูลดังกล่าวนั้นคือข้อมูลอะไร และเมื่อพิจารณาจากบริบทของการฟิชชิงจะเห็นได้ว่าข้อมูลที่เป็นเป้าหมายของการฟิชชิ่งนั้น ล้วนแล้วแต่เป็นข้อมูลส่วนบุคคล และข้อมูลในการยืนยันสิทธิในการเข้าถึงระบบ (credential) ซึ่งมิได้มีไว้เพื่อประโยชน์สาธารณะทั้งสิ้นซึ่งหมายรวมถึงข้อมูลมือถือที่ถือได้ว่าเป็นข้อมูลส่วนบุคคลอีกด้วย

---

[189] “การดักรับข้อมูลคอมพิวเตอร์” หมายถึง การดักรับโดยใช้วิธีการทางเทคนิคเพื่อลอบ ดักฟัง ตรวจสอบ หรือติดตามเนื้อหาการสื่อสารระหว่าบุคคลหรือระหว่างคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลทางตรงและทางอ้อมซึ่งใช้ในการหาปยะโยชน์อื่นใดอันมิชอบด้วยกฎหมาย. เพิ่งอ้าง 23.

[190] พรเพรช วิชิตชลชัย (เชิงอรรถ 96)24.

4.2.2 การส่งข้อมูลรบกวรการใช้ระบบคอมพิวเตอร์โดยปกติสุข มาตรา11 วรรคหนึ่ง

เจตนารมณ์ในการบัญญัติความผิดฐานนี้ขึ้นมาก็เพื่อเอาผิดกับผู้ที่กระทำการไม่ถึงกับก่อให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์ แต่เป็นการรบกวรการทำงานของระบบคอมพิวเตอร์ กล่าวคือ ความผิดตามนัยของบทบัญญัตินี้คือการส่งข้อความอิเล็กทรอนิกส์จำนวนมากๆไปยังผู้เสียหายอันทำให้การทำงานของระบบคอมพิวเตอร์เกิดการทำงานหนักมากกว่าปกติจนก่อให้เกิดความหน่วงในการใช้งานระบบคอมพิวเตอร์ซึ่งเป็นผลมาจากไฟล์ขยะที่เกิดจากการส่งข้อความอิเล็กทรอนิกส์จำนวนมากๆ โดยมีองค์ประกอบความผิดดังนี้

องค์ประกอบความผิดที่กฎหมายบัญญัติในมาตรานี้ คือ การที่บุคคลใดก็ตามส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุขโดยเจตนา

องค์ประกอบความผิดภายนอกของความผิดนี้ คือ การที่บุคคลใดก็ตามส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

องค์ประกอบความผิดภายในของความผิดนี้ คือ เจตนาในการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข โดยผู้กระทำจะต้องมีเจตนาในการดักรับข้อมูลอันเป็นเจตนาตามประมวลกฎหมายอาญามาตรา 59

อนึ่ง คำว่า “เป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข” มีความหมายว่าการกระทำการด้วยวิธีการทางอิเล็กทรอนิกส์อันเป็นการรบกวนการทำงานของระบบคอมพิวเตอร์ในที่นี้คือการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งมีความรุนแรงของการรบกวนอยู่มากพอสมควรเป็นความรุนแรงที่ต้องใช้มาตรฐานในระดับวิญญูชนเป็นเกณฑ์ในการพิจารณาในทางภาวะวิสัย อันมิใช่การพิจารณาในทางอัตวิสัย[191]

เมื่อพิจารณาถึงลักษณะในการกระทำความผิดของฟิชเชอร์ในการก่ออาชญากรรมประเภทฟิชชิ่งที่เกี่ยวข้องกับการกระทำผิดฐานนนี้ในบางกรณีจะเห็นได้ว่าหนึ่งในช่องทางที่ฟิชเชอร์ใช้ในการติดต่อกับผู้เสียหายคือการติดต่อทางอีเมล์หรือการใช้ร่วมกับเว็บไซต์ปลอมที่สร้างขึ้นมาให้มีรูปแบบเสมือนเว็บไซต์ที่แท้จริงโดยไม่เปิดโอกาสให้ผู้เสียหายนั้นสามารถที่จะปฏิเสธการรับข้อความนั้นได้ เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลของผู้เสียหาซึ่งอาจนำข้อมูลนั้นไปแสวงหาประโยชน์อื่นใด ทั้งนี้ เป็นไปตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่ง ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ พ.ศ.2560

---

[191] ณัฐสุดา อัคราวัฒนา (เชิงอรรถ 134) 109.

4.2.3 การนำเข้าข้อมูลคอมพิวเตอร์อันเป็นเท็จมาตรา 14 (1)

การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จตาม มาตรา 14(1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งเจตนารมณ์ในการบัญญัติมาตรานี้ขึ้นมาก็เพื่อคุ้มครองมิให้บุคคลตกเป็นผู้เสียหายจากการล้อลวงทางคอมพิวเตอร์ ซึ่งมีองค์ประกอบความผิด ดังนี้

องค์ประกอบความผิดที่กฎหมายบัญญัติในมาตรานี้ คือ การที่บุคคลใดก็ตามนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลปลอมหรือบิดเบือนหรือข้อมูลอันเป็นเท็จไม่ว่าจะทั้งหมดหรือแต่บางส่วน โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน โดยเจตนาทุจริตหรือหลอกลวง

องค์ประกอบความผิดภายนอกของความผิดนี้ คือ การที่บุคคลใดก็ตามนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จไม่ว่าจะทั้งหมดหรือแต่บางส่วน

องค์ประกอบความผิดภายในของความผิดนี้ คือ เจตนาที่จะนำเข้าที่จะนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จไม่ว่าจะทั้งหมดหรือแต่บางส่วน โดยผู้กระทำจะต้องมีเจตนาในการนำเข้าสู่ระบบอันเป็นเจตนาตามประมวลกฎหมายอาญามาตรา 59 และมาตรา 1(1)[192] ซึ่งในขณะเดียวกันผู้กระทำความผิดก็ต้องรู้ด้วยว่าข้อมูลที่นำเข้าสู่ระบบนั้นเป็นข้อมูลอันเป็นเท็จ, ปลอม, หรือบิดเบือน

อนึ่ง คำว่า โดยประการที่น่าจะเกิดความเสียหายแก่ประชานชน คือ การนำเข้าข้อมูลคอมพิวเตอร์อันก่อให้เกิดความเสียหาย หากการนำเข้าข้อมูลอันเป็นเท็จแต่ไม่ก่อให้เกิดความเสียหายผู้กระทำก็ไม่ต้องรับผิดในฐานนี้ ซึ่งในประเด็นนี้เองผู้เขียนเห็นว่าเงื่อนไขการลงโทษในองค์ประกอบความผิดฐานนี้นั้นเป็นเพียงเงื่อนไขในการลงโทษทางภาวะวิสัยเพียงเท่านั้นซึ่งผู้กระทำความผิดไม่จำเป็นต้องรู้ถึงความเสียหายที่เกิดขึ้นจากผลของการกระทำความผิดในฐานนี้

แต่ไม่ว่าอย่างไรก็ตามในการบังคับใช้บทบัญญัติในข้างต้นนี้นั้นก็ยังคงมีปัญหาบางประการในเรื่องของการตีความตามบริบทของคำว่า “ข้อมูลอันเป็นเท็จ” ซึ่งมิได้มีการให้คำจำกัดความถึงลักษณะข้อมูลอย่างเฉพาะเจาะจงถึงความหมายของคำว่าข้อมูลอันเป็นเท็จว่าต้องมีองค์ประกอบอย่างไรจึงจะเรียกว่าข้อมูลอันเป็นเท็จ

ทั้งนี้ เมื่อพิจารณาถึงลักษณะในการกระทำความผิดของฟิชเชอร์ในการก่ออาชญากรรมฟิชชิ่งที่เกี่ยวข้องกับการกระทำผิดฐานนี้ในบางกรณีจะเห็นได้ว่าในการใช้อีเมล์ร่วมกับการสร้างเว็บไซปลอมในลักษณะที่เหมือนกับเว็บไซที่แท้จริง ซึ่งอาจทำให้ผู้เสียหายนั้นหลงเชื่อเข้าสู่เว็บดังกล่าวและกรอกข้อมูลลงไปในเว็บ

---

[192] ประมวลกฎหมายอาญา มาตรา 1(1) “โดยทุจริต” หมายความว่า เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น องค์ประกอบของคำว่า “โดยทุจริต” มีดังนี้

(1) แสวงหาประโยชน์ ซึ่งการแสวงหาประโยชน์ในที่นี้ หมายถึง ประโยชน์ในลักษณะที่เป็นทรัพย์สินและประโยชน์ที่มิใช่ทรัพย์สินด้วย

(2) ที่มิควรได้โดยชอบด้วยกฎหมาย หมายถึง ต้องเป็นประโยชน์ที่ผู้แสวงหานั้นไม่มีสิทธิจะได้รับตามกฎหมายในทางกลับกัน ถ้าประโยชน์นั้นผู้แสวงหามีสิทธิจะได้รับตามกฎหมายแล้ว ย่อมมิใช่ทุจริต

(3) สำหรับตนเองหรือผู้อื่น หมายถึง การแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายนั้น เพื่อต้องการเอาประโยชน์เป็นของตนเองหรือของผู้อื่น หรือร่วมกัน

ปลอมที่ถูกเตรียมไว้ซึ่งข้อมูลจะถูกบันทึกไว้ทั้งหมด ซึ่งข้อมูลที่ฟิชเชอร์นั้นได้ไปอาจไม่ใช่แค่เพียงข้อมูลของผู้เสียหายแต่อาจได้ไปซึ่งทรัพย์สินของผู้เสียหายด้วยหากข้อมูลที่ได้ไปนั้นเป็นข้อมูลทางการเงิน[193]

4.3 วิเคราะห์เปรียบเทียบแนวทางการบัญญัติกฎหมายเกี่ยวกับฟิชชิ่ง

จากการศึกษาบทบัญญัติทางกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับฟิชชิ่ง ในหัวข้อนี้ผู้เขียนจะได้นำบทบัญญัติทางกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับฟิชชิ่งของต่างประเทศดังที่ได้กล่าวไปใน บทที่ 3 กล่าวคือ กฎหมายของประเทศสหรัฐอเมริกา,กฎหมายธุรกิจทั่วไปรัฐนิวยอร์ก, ประมวลกฎหมายธุรกิจรัฐแคลิฟอร์เนีย, กฎหมายพาณิชย์และอิเล็กทรอนิกส์รัฐยูทาห์, กฎหมายรัฐเทนเนสซี, ประมวลกฎหมายของประเทศเยอรมัน และประมวลกฎหมายของประเทศฝรั่งเศส โดยจะพิจารณาเฉพาะฐานความผิดที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับฟิชชิ่งโดยเฉพาะซึ่งสามารถแยกรูปแบบในการกระทำความผิดเกี่ยวข้องอันมีลักษณะที่คล้ายคลึงกันได้ ดังนี้

ตารางที่ 4.1 ตารางเปรียบเทียบองค์ประกอบความผิดฐานเข้าสู่ระบบคอมพิวเตอร์และเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ

การเข้าสู่ระบบคอมพิวเตอร์ และ เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	
ประเทศ	**องค์ประกอบความผิดที่กฎหมายบัญญัติ**
สหพันธ์รัฐเยอรมนี	StGB. §220a การที่บุคคลผู้ซึ่งกระทำการโดยปราศจากอำนาจใช้วิธีการมิชอบด้วยกฎหมายเข้าถึงข้อมูล ที่มีการกำหนดมาตรการป้องกันการเข้าถึงซึ่งมิได้มีไว้สำหรับตนเพื่อตนเองหรือผู้อื่น โดยเจตนา
สาธารณรัฐฝรั่งเศส	Penal Coad. Article 323-1 การที่บุคคลใดบุคคลหนึ่งเข้าถึงข้อมูลหรือคงอยู่ในระบบคอมพิวเตอร์ไม่ว่าจะทั้งหมดหรือแต่บางส่วนของระบบประมวลผลข้อมูลอัตโนมัติ โดยเจตนา
ประเทศไทย	**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550** **มาตรา 5** การที่บุคคลใดก็ตามผู้ซึ่งไม่มีอำนาจกระทำการเข้าถึงระบบคอมพิวเตอร์ที่มีการกำหนดมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะและมาตรการเช่นว่านั้นมิได้มีไว้เพื่อตน โดยเจตนา **มาตรา 7** การที่บุคคลใดก็ตามผู้ซึ่งไม่มีอำนาจกระทำการเข้าถึงข้อมูลคอมพิวเตอร์ที่มีการกำหนดมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะและมาตรการเช่นว่านั้นมิได้มีไว้เพื่อตน โดยเจตนา
รัฐแคลิฟอร์เนีย	-

[193] กุลธิดา อาธิเจริญสุข (เชิงอรรถ 64) 136-137.

ตารางที่ 4.1 (ต่อ)

การเข้าสู่ระบบคอมพิวเตอร์ และ เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	
ประเทศ	**องค์ประกอบความผิดที่กฎหมายบัญญัติ**
รัฐนิวยอร์ก	-
รัฐเทนเนสซี	-
รัฐยูท่า	-

เมื่อพิจารณาจากองค์ประกอบความผิดตามที่กฎหมายบัญญัติของแต่ละประเทศดังที่ได้กล่าวมาดังตารางข้างต้นจะเห็นได้ว่าในแต่ละประเทศมีความแตกต่างกันเหตุเพราะในการบัญญัติกฎหมายของแต่ประเทศดังที่ได้กล่าวมานั้นมีจุดประสงค์ในการมุ่งคุ้มครองที่ต่างกัน กล่าวคือ ในบทบัญญัติกฎหมายของ สหพันธ์สาธารณรัฐเยอรมนี มีจุดประสงค์ที่จะมุ่งคุ้มครองการเข้าถึงระบบคอมพิวเตอร์[194]เป็นสำคัญซึ่งเพียงแค่ผู้กระทำความผิดเจาะระบบ หรือเข้าถึงโดยปราศจากอำนาจ หรือเข้าถึงช่องทางที่สามารถที่จะเข้าถึงระบบได้ก็ถือได้ว่าเป็นความผิดแล้ว โดยไม่จำเป็นที่จะต้องมีการทำซ้ำหรือโจรกรรมข้อมูลออกไปเกิดขึ้น[195]

ในส่วนของสาธารณรัฐฝรั่งเศสนั้นก็มีความมุ่งหมายที่จะคุ้มครองการเข้าถึงหรือคงอยู่ในระบบคอมพิวเตอร์โดยมิชอบด้วยกฎหมาย อันมีความคล้ายคลึงกับบทบัญญัติของสหพันธ์สาธารณรัฐเยอรมนี เหตุเพราะเพียงแค่เข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ถือว่าเป็นความผิดตาม มาตรา323-1 แล้วนอกจากนี้แล้วในวรรคสองและวรรคสามของบทบัญญัติมาตรานี้ยังได้มีการบัญญัติเหตุเพิ่มโทษหากเป็นการเข้าถึงเพื่อ แก้ไข ลบ เปลี่ยนแปลงข้อมูลคอมพิวเตอร์ หรือเป็นการกระทำต่อระบบประมวลผลข้อมูลอัตโนมัติที่ดำเนินการโดยภาครัฐ

ในส่วนของประเทศไทยนั้นได้มีการแยกองค์ประกอบการกระทำความผิดออกเป็นสองส่วนโดยบัญญัติไว้เป็น 2 มาตราแยกส่วนการกระทำออกจากกันอย่างชัดเจน โดยในส่วนแรกคือ มาตรา 5 ที่บัญญัติให้การเข้าถึงระบบคอมพิวเตอร์ที่มีการกำหนดมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะและมาตรการเช่นว่านั้นมิได้มีไว้เพื่อตนเป็นความผิด และในส่วนที่สองคือ มาตรา7 ที่บัญญัติให้การเข้าถึงข้อมูลคอมพิวเตอร์ที่มีการกำหนดมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะและมาตรการเช่นว่านั้นมิได้มีไว้เพื่อตนเป็นความผิดเป็นความผิด

ซึ่งหากพิจารณาจากบทบัญญัติของสหพันธ์สาธารณรัฐเยอรมนีและสาธารณรัฐฝรั่งเศสจะเห็นได้ว่ามิได้มีการกำหนดเจตนาในส่วนของการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบไว้โดยเฉพาะในลักษณะเดียวกันกับของประเทศไทย

---

[194] ณัฐสุดา อัคราวัฒนา (เชิงอรรถ 134) 130.

[195] สาวตรี สุขศรี (เชิงอรรถ 133) 510.

สำหรับในส่วนของบทบัญญัติที่เกี่ยวของกับฟิชชิ่งในส่วนของการเข้าสู่ระบบคอมพิวเตอร์ และเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบของ รัฐแคลิฟอร์เนีย, รัฐยูท่า, รัฐนิวยอร์ก และรัฐเทนเนสซี นั้นมิได้มีการกำหนดไว้เพราะในการบังคับใช้มาตรการทางกฎหมายเกี่ยวกับฟิชชิ่งของรัฐดังกล่าวนั้นได้มีการบัญญัติกฎหมายขึ้นมาใช้บังคับโดยเฉพาะกับการกระทำความผิดในรูปแบบฟิชชิ่ง

ตารางที่ 4.2 ตารางเปรียบเทียบองค์ประกอบความผิดฐานดักรับข้อมูลคอมพิวเตอร์

การดักรับข้อมูลคอมพิวเตอร์	
ประเทศ	**องค์ประกอบความผิดที่กฎหมายบัญญัติ**
สหพันธ์รัฐเยอรมนี	StGB. §202b การที่บุคคลใดบุคคลหนึ่งกระทำการโดยปราศจากอำนาจใช้วิธีการทางเทคนิคดักรับข้อมูลอันมิได้มีไว้เพื่อตน ซึ่งอยู่ในระหว่างการรับ-ส่งข้อมูลอันมิได้มีไว้เพื่อสาธารณะ หรือดักรับข้อมูลที่บันทึกในระบบประมวลผลข้อมูล โดยเจตนา
สาธารณรัฐฝรั่งเศส	-
ประเทศไทย	**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 8** การที่บุคคลใดบุคคลหนึ่งกระทำการโดยปราศจากอำนาจใช้วิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นในระหว่างการส่งข้อมูลในระบบคอมพิวเตอร์และข้อมูลเช่นว่านั้นมิได้มีไว้เพื่อสาธารณะหรือเพื่อบุคคลทั่วไป
รัฐแคลิฟอร์เนีย	-
รัฐยูท่า	-
รัฐนิวยอร์ก	-
รัฐเทนเนสซี	-

สำหรับสาธารณรัฐฝรั่งเศส, รัฐแคลิฟอร์เนีย, รัฐยูท่า, รัฐนิวยอร์กและรัฐเทนเนสซี ไม่มีบทบัญญัติสำหรับความผิดในลักษณะนี้

ส่วนบทบัญญัติกฎหมายของ สหพันธ์สาธารณรัฐเยอรมนี มีจุดประสงค์ที่จะมุ่งคุ้มครองข้อมูลคอมพิวเตอร์ที่อยู่ในระหว่างการรับ-ส่งข้อมูลอันมิได้มีไว้เพื่อสาธารณะ หรือข้อมูลที่บันทึกอยู่ในระบบประมวลผลข้อมูล หรือระบบคอมพิวเตอร์ที่มิได้อยู่ในระหว่างการรับ-ส่งข้อมูลด้วย[196]

ในส่วนของบัญญัติกฎหมายของประเทศไทยนั้น องค์ประกอบของการดักรับข้อมูลของผู้อื่นนั้นจะต้องเป็นข้อมูลที่อยู่ในระหว่างการส่งข้อมูลเท่านั้น ซึ่งมิได้หมายรวมถึงข้อมูลคอมพิวเตอร์ที่ถูกจัดเก็บไว้ใน

[196] สาวตรี สุขศรี (เชิงอรรถ 133) 511.

หน่วยเก็บข้อมูลรูปแบบต่างๆ อันมิได้อยู่ในระหว่างการส่งข้อมูล อย่างไรก็ตามข้อมูลเช่นว่านี้ต้องมิใช้ข้อมูลอันมีไว้เพื่อประโยชน์สาธารณะหรือสามารถเข้าถึงได้ทั่วไป ทั้งนี้พิจารณาเจตนาของผู้ที่ส่งข้อมูลคอมพิวเตอร์เช่นว่านี้เป็นหลักว่าต้องการเปิดเผยต่อสาธารณะหรือไม่เพราะถือว่าเจตนาในการส่งข้อมูลนั้นเป็นเรื่องเฉพาะตัว

เมื่อพิจารณาจากองค์ประกอบของบทบัญญัติในข้างต้นจะเห็นได้ว่าในบทบัญญัติทางกฎหมายเกี่ยวกับการดักรับข้อมูลของสหพันธรัฐเยอรมนีนั้นมีเนื้อหาของบทบัญญัติที่ครอบคลุมเป็นอย่างมาก กล่าวคือมีการคุ้มครองข้อมูลคอมพิวเตอร์ที่กว่างกว่าของกฎหมายไทยเป็นอย่างมากโดยคุ้มครองไปถึงข้อมูลที่อยู่ในระหว่างการรับและส่ง ซึ่งรวมไปข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์ด้วย[197]

ตารางที่ 4.3 ตารางเปรียบเทียบองค์ประกอบความผิดฐานเตรียมการหรือดำเนินการเพื่อกระทำความผิดต่อระบบหรือข้อมูลคอมพิวเตอร์

การเตรียมการหรือดำเนินการเพื่อกระทำความผิดต่อระบบหรือข้อมูลคอมพิวเตอร์	
ประเทศ	**องค์ประกอบความผิดที่กฎหมายบัญญัติ**
สหพันธ์รัฐเยอรมนี	StGB. §202c การที่บุคคลใดบุคคลหนึ่งกระทำการโดยปราศจากอำนาจกระทำการเตรียมการใช้วิธีการทางเทคนิคดักรับข้อมูลอันมิได้มีไว้เพื่อตน โดย ผลิต เพื่อตนเองหรือผู้อื่น จำหน่าย จัดหา เผยแพร่ หรือทำให้เข้าถึงซึ่งรหัสผ่านที่ใช้ในการเข้าถึงข้อมูลหรือซอฟแวร์
สาธารณรัฐฝรั่งเศส	Penal Coad. Article 323-3 การที่บุคคลใดบุคคลหนึ่ง แนะนำข้อมูลสำหรับการเข้าถึงระบบประมวลผลอัตโนมัติ โดยมิชอบ
ประเทศไทย	-
รัฐแคลิฟอร์เนีย	-
รัฐยูท่า	-
รัฐนิวยอร์ก	-
รัฐเทนเนสซี	-

เมื่อพิจารณาจากองค์ประกอบความผิดตามที่กฎหมายบัญญัติของแต่ละประเทศดังที่ได้กล่าวมาดังตารางข้างต้นสำหรับบทบัญญัติในส่วนของการเตรียมการหรือดำเนินการเพื่อกระทำความผิดต่อระบบหรือข้อมูลคอมพิวเตอร์จะเห็นได้ว่าในแต่ละประเทศมีความแตกต่างกันเหตุเพราะในการบัญญัติกฎหมายของแต่ประเทศดังที่ได้กล่าวมานั้นมีจุดประสงค์ในการมุ่งคุ้มครองที่ต่างกัน กล่าวคือ ในบทบัญญัติทางกฎหมายของสหพันธ์สาธารณรัฐเยอรมนี มีจุดประสงค์ที่จะมุ่งเอาผิดกับบุคคลที่ใช้วิธีการที่มิชอบเพื่อเข้าถึงระบบ

[197] ณัฐสุดา อัคราวัฒนา (เชิงอรรถ 134) 132.

คอมพิวเตอร์หรือใช้วิธีการทางเทคนิคดักรับข้อมูลที่มิได้มีไว้เพื่อตน หรือเพื่อเตรียมการในการรบกวนการใช้งานระบบประมวลผลข้อมูลของบุคคลอื่น โดยการผลิต เพื่อตนเองหรือผู้อื่น จัดจำหน่าย จัดหา เผยแพร่ หรือทำให้เข้าถึงซึ่งรหัสผ่านที่ใช้ในการเข้าถึงข้อมูลหรือซอฟแวร์ที่มีไว้เพื่อใช้ในการกระทำความผิดดังกล่าว ซึ่งจากที่ได้กล่าวในข้างต้นนี้นั้นจะเห็นได้ว่าในบทบัญญัติของสหพันธ์สาธารณรัฐเยอรมนี มีการกำหนดองค์ประกอบการกระทำความผิดที่มีความชัดเจนเป็นอย่างมากในแง่ของการกระทำ โดยระบุรูปแบบและวิธีการในการกระทำความผิดไว้อย่างชัดเจนซึ่งถือได้ว่าเป็นประโยชน์ในการบังคับใช้กฎหมายเป็นอย่างยิ่ง[198]

ต่อมาในส่วนของสาธารณรัฐฝรั่งเศสบัญญัติให้การแนะนำข้อมูลในการช่วยเหลือเพื่อเข้าถึงระบบประมวลผลข้อมูลอัตโนมัติโดยมิชอบเป็นความผิด อันมีลักษณะที่คล้ายคลึงกับบทบัญญัติของสหพันธรัฐเยอรมนี อย่างไรก็ดีนอกจากความผิดในบทบัญญัติในประมวลกฎหมายอาญาฝรั่งเศส มาตรา323-3 ยังมีการกำหนดลักษณะในการกระทำความผิดเพิ่มเติมที่มีเนื้อหาครอบคลุมไปถึง การนำเข้า เสนอ ถ่ายโอน หรือมีอุปกรณ์ เครื่องมือ ซอฟแวร์ หรือข้อมูลที่มีไว้เพื่อช่วยในการเข้าถึงระบบประมวลผลข้อมูลอัตโนมัติ หรือแนะนำข้อมูลในการเข้าสู่ระบบ หรือลบ หรือเปลี่ยนแปลงข้อมูลในระบบโดยบัญญัติเพิ่มเติมไว้ใน มาตรา 323-3-1 ซึ่งเมื่อพิจารณาจากบทบัญญัติดังที่ได้กล่าวไปจะเห็นได้ว่าบทบัญญัติในประมวลกฎหมายอาญาฝรั่งเศสนั้นได้มีการบัญญัติลักษณะและองค์ประกอบในการกระทำความผิดไว้ค่อนข้างที่จะครอบคลุมและชัดเจนเช่นเดียวกับสหพันธ์สาธารณรัฐเยอรมนี แต่จะแตกต่างกันในส่วนของบทบัญญัติบางประการที่ของสาธารณรัฐฝรั่งเศสนั้นมีบทบัญญัติที่ครอบคลุมกว้างกว่าของเยอรมนี กล่าวคือในบทบัญญัติของฝรั่งเศสนั้นได้บัญญัติครอบคลุมไปการใช้อุปกรณ์หรือเครื่องมือที่ใช้ในการกระทำความผิดด้วย ซึ่งในส่วนนี้สหพันธ์สาธารณรัฐเยอรมนีไม่ได้มีการบัญญัติถึงในส่วนนี้

ในส่วนของบทบัญญัติในประเทศไทยนั้นมิได้มีการบัญญัติบทบัญญัติสำหรับความผิดในลักษณะนี้ไว้ ซึ่งหากอ้างอิงตามประมวลกฎหมายอาญาในส่วนของการตระเตรียมการกระทำความผิดจะเห็นได้ว่าความผิดในชั้นตระเตรียมการนั้นจะต้องมีการบัญญัติฐานความผิดไว้โดยเฉพาะเท่านั้นเพราะถือว่าโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นเป็นโทษทางอาญาที่มีผลกระทบต่อสิทธิต่อสิทธิเสรีภาพของบุคคลโดยตรง[199] ซึ่งในกรณีนี้ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นมิได้มีการบัญญัติไว้

สำหรับในส่วนของรัฐแคลิฟอร์เนีย, รัฐยูท่า, รัฐนิวยอร์ก และรัฐเทนเนสซี ได้มีการกำหนดให้การพยามกระทำความผิดหรือมีเครื่องมือไว้เพื่อกระทำความผิดนั้นเป็นความผิดอันมีโทษ ซึ่งผู้เขียนจะได้กล่าวในประเด็นนี้ในหัวข้อการโจรกรรมข้อมูลส่วนบุคคล

---

[198] ณัฐสุดา อัคราวัฒนา (เชิงอรรถ 134) 138.

[199] สุพิศ ประณีตพลกรัง, *หลักและทฤษฎีทางกฎหมายอาญา* (พิมพ์ครั้งที่ 2, สำนักพิมพ์นิติธรรม 2562) 15.

ตารางที่ 4.4 ตารางเปรียบเทียบองค์ประกอบความผิดฐานฉ้อโกงและหลอกลวงคอมพิวเตอร์

การฉ้อโกงและหลอกลวงคอมพิวเตอร์	
ประเทศ	**องค์ประกอบความผิดที่กฎหมายบัญญัติ**
สหพันธ์รัฐเยอรมนี	**StGB. §263a** การที่บุคคลใดบุคคลหนึ่งกระทำการอย่างหนึ่งอย่างใดต่อการประมวลผลของระบบคอมพิวเตอร์ เพื่อให้ผลลัพธ์ในการประมวลผลเป็นไปในทางที่ตนต้องการเพื่อให้ได้ไปซึ่งประโยชน์ในทางทรัพย์สิน
สาธารณรัฐฝรั่งเศส	**Penal Coad. Article 313-1** การที่บุคคลใดบุคคลหนึ่งแสดงตนเป็นบุคคลอื่นด้วยเจตนาหลอกลวงหรือทำให้สำคัญผิดในข้อเท็จจริง โดยใช้อุบาย ให้บุคคลอื่นส่งมอบทรัพย์ หรือทรัพย์สิน
ประเทศไทย	**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2)พ.ศ.2560** **มาตรา 14(1)** การที่บุคคลใดก็ตามนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลปลอมหรือบิดเบือนหรือข้อมูลอันเป็นเท็จไม่ว่าจะทั้งหมดหรือแต่บางส่วน โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน โดยเจตนาทุจริตหรือหลอกลวง
รัฐแคลิฟอร์เนีย	-
รัฐยูท่า	-
รัฐนิวยอร์ก	-
รัฐเทนเนสซี	-

เมื่อพิจารณาจากองค์ประกอบความผิดตามที่กฎหมายบัญญัติของแต่ละประเทศดังที่ได้กล่าวมาดังตารางข้างต้นสำหรับบทบัญญัติในส่วนของการฉ้อโกงคอมพิวเตอร์จะเห็นได้ว่าในส่วนของ สหพันธรัฐเยอรมนีมีการบัญญัติความผิดฐานฉ้อโกงคอมพิวเตอร์ไว้ในประมวลกฎหมายอาญา มาตรา 263a โดยเป็นการกระทำการอย่างหนึ่งอย่างใดต่อการประมวลผลของระบบคอมพิวเตอร์ เพื่อให้ผลลัพธ์ในการประมวลผลเป็นไปในทางที่ตนต้องการเพื่อให้ได้ไปซึ่งประโยชน์ในทางทรัพย์สิน ซึ่งมิใช้การกระทำต่อตัวบุคคลอันเป็นองค์ประกอบของการฉ้อโกงทั่วไป[200] และจากที่ได้กล่าวในข้างต้นนี้นั้นจะเห็นได้ว่าในบทบัญญัติของสหพันธ์สาธารณรัฐเยอรมนีมีการกำหนดองค์ประกอบการกระทำความผิดที่มีความชัดเจนเป็นอย่างมาก โดยเฉพาะอย่างยิ่งในถ้อยคำของกฎหมายที่กล่าวถึง การกระทำเพื่อให้ผลลัพธ์ในการประมวลผลเป็นไปในทางที่ตนต้องการเพื่อให้ได้ไปซึ่งประโยชน์ในทางทรัพย์สิน ซึ่งในส่วนนี้เองผู้เขียนเห็นว่ามีความน่าสนใจเป็นอย่างมากเพราะในการกำหนดบทบัญญัติเช่นนี้จะส่งผลครอบคลุมไปถึงการกระทำความผิดในทุกรูปแบบและไม่จำกัดวิธีการเหตุเพราะใน

[200] ณัฐสุดา อัคราวัฒนา (เชิงอรรถ 134) 139.

ท้ายที่สุดแล้วไม่ว่าผู้กระทำความผิดจะใช้วิธีการใดในการกระทำต่อระบบคอมพิวเตอร์หากการกระทำนั้นทำไปเพื่อให้ได้ไปซึ่งประโยชน์ในทางทรัพย์สินผู้กระทำก็จะถือว่ามีความผิดตามกฎหมายนี้ด้วย

ต่อมาในส่วนของสาธารณรัฐฝรั่งเศสบัญญัติให้การฉ้อโกงคือ การแสดงตนเป็นบุคคลอื่นด้วยเจตนาหลอกลวงหรือทำให้สำคัญผิดในข้อเท็จจริง โดยใช้อุบาย ให้บุคคลอื่นส่งทรัพย์ หรือทรัพย์สิน เป็นการกระทำผิดฐานฉ้อโกง อันสะท้อนให้เห็นถึงเจตนาของบทบัญญัติที่ต้องการจะปกป้องบุคคลจากการถูกหลอกลวง โดยมีเจตนาเพื่อให้ผู้เสียหายนั้นส่งมอบทรัพย์สินแกตน ซึ่งจากบทบัญญัตินี้จะเห็นได้ว่ามิได้มีการกำหนดลักษณะในการหลอกลวงหรือทำให้สำคัญผิดไว้อย่างชัดเจน ซึ่งจากการศึกษาพบว่าในการบังคับใช้บทบัญญัติในมาตรานี้ของสาธารณรัฐฝรั่งเศสนั้นมิได้จำกัดอยู่แค่การหลอกลวงทั่วไปแต่ยังรวมไปถึงการหลอกลวงบนเครือข่ายสื่อสารออนไลน์อีกด้วย อย่างไรก็ตามเมื่อพิจารณาถึงองค์ประกอบความผิดของสาธารณรัฐฝรั่งเศสจะเห็นได้ว่าค่อนข้างมีความแตกต่างกับความผิดฐานฉ้อโกงคอมพิวเตอร์ตามประมวลกฎหมายอาญา มาตรา 263a ของสหพันธ์รัฐเยอรมนีในแง่ของการกระทำ กล่าวคือในส่วนของ มาตรา 263a นั้นจำกัดไว้เฉพาะการกระทำผิดในกรณีการกระทำการอย่างหนึ่งอย่างใดต่อระบบคอมพิวเตอร์ เพื่อให้ได้ประโยชน์ในทางทรัพย์สินที่สะท้อนให้เห็นถึงเจตนาในการบังคับใช้กับการกระทำผิดต่อระบบคอมพิวเตอร์โดยตรง แต่ในส่วนของมาตรา 313-1 แห่งประมวลกฎหมายอาญาฝรั่งเศสนั้นมิได้มีการกำหนดลักษณะในการหลอกลวง แต่ไม่ว่าอย่างไรก็ดีในบทบัญญัติของทั้งสองประเทศนั้นก็ต่างมีจุดประสงค์ที่เพื่อเอาผิดกับการฉ้อโกงและหลอกลวงโดยใช้คอมพิวเตอร์เป็นเครื่องมือทั้งสิ้น

สำหรับในส่วนของบทบัญญัติในประเทศไทยนั้นบัญญัติให้การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลปลอมหรือบิดเบือนหรือข้อมูลอันเป็นเท็จไม่ว่าจะทั้งหมดหรือแต่บางส่วน โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน โดยเจตนาทุจริตหรือหลอกลวง เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560. มาตรา 14(1) ซึ่งหากพิจารณาจากองค์ประกอบความผิดของมาตรานี้จะเห็นได้ว่าในส่วนของเจตนาในมาตรานี้นั้นสะท้อนให้เห็นถึงเจตนาในการฉ้อโกง กล่าวคือ ในการกระทำความผิดตามมาตรานี้ผู้กระทำต้องมีเจตนา "โดยทุจริต หรือโดยหลอกลวง" ซึ่งคำว่า โดยทุจริต ตามประมวลกฎหมายอาญา หมายความว่า "เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น" ซึ่งสะท้อนให้เห็นถึงเจตนารมณ์ในการเอาผิดกับการกระทำที่มุ่งต่อประโยชน์ทางทรัพย์สิน[201] แม้มิได้บัญญัติในเรื่องการกระทำต่อตัวทรัพย์หรือทรัพย์สินไว้อย่างชัดเจนก็ตามแต่ก็สามารถนำมาตีความในส่วนของเจตนาเพื่อบังคับให้กับการฉ้อโกงได้เช่นกัน แต่ไม่ว่าอย่างไรก็ตามจากการศึกษาพบว่าแม้องค์ประกอบความผิดในมาตรานี้จะสามารถนำมาตีความเอาผิดกับการฉ้อโกงและหลอกลวงได้แต่ก็จำกัดเฉพาะกรณีที่เป็นการกระทำผิดต่อตัวบุคคลอันเป็นองค์ประกอบของการฉ้อโกงทั่วเพียงเท่านั้น ซึ่งในที่นี้ไม่นับรวมไปถึงการกระทำในทางเทคนิคอันเป็นการกระทำต่อตัวระบบอันมิใช้ตัวบุคคล

---

[201] ‘ร่างแก้ไขพ.ร.บ.คอมพิวเตอร์ฯ "ตั้งคณะกรรมการปิดเว็บแม้ไม่ผิดกฎหมาย’ (iLaw, 25 เมษายน 2559) <https://ilaw.or.th/node/4092?fbclid=IwAR383U_Pv0XVzGtc4uyZ7WvgiLkYoQx4oWlGGVgBdZLWDZMgYFL6UJ1n_4E> สืบค้นเมื่อ 5 พฤษภาคม 2566.

อนึ่ง เมื่อพิจารณาถึงองค์ประกอบความผิดของประเทศดังที่ได้กล่าวมาในข้างต้นจะเห็นได้ว่าในบทบัญญัติของประเทศไทยนั้นค่อนข้างที่จะแตกต่างกับบทบัญญัติของต่างประเทศในแง่ของความจริงเท็จของข้อมูลอันเป็นข้อจำกันในการบังคับใช้กฎหมาย เหตุเพราะการที่มาตรา 14(1) กำหนดให้การนำเข้าข้อมูลที่ปลอม, บิดเบือน หรือเป็นเท็จเข้าสู่ระบบนั้นถือเป็นข้อจำกัดในแง่ของเนื้อหาซึ่งสะท้อนให้เห็นถึงปัญหาในการตีความตามกรอบความเข้าใจของมนุษย์เพราะโดยธรรมชาติของการเป็นชุดคำสั่งคอมพิวเตอร์นั้นไม่มีองค์ประกอบในแง่ของเนื้อหาที่ปลอมหรือเท็จ[202] ซึ่งหากพิจารณาจารณาจากบทบัญญัติในส่วนของสหพันธ์รัฐเยอรมนีและสาธารณรัฐฝรั่งเศสจะเห็นได้ว่าไม่ได้มีองค์ประกอบเกี่ยวกับความจริงเท็จของข้อมูลดังเช่นของประเทศไทย[203]

สำหรับรัฐแคลิฟอร์เนีย, รัฐยูท่า, รัฐนิวยอร์กและรัฐเทนเนสซี มิได้มีการบัญญัติบทบัญญัติในลักษณะนี้ไว้เป็นการเฉพาะ

ตารางที่ 4.5 ตารางเปรียบเทียบองค์ประกอบความผิดในการกระทำความผิดต่อข้อมูลส่วนบุคคล

การกระทำความผิดต่อข้อมูลส่วนบุคคล	
ประเทศ	**องค์ประกอบความผิดที่กฎหมายบัญญัติ**
สหพันธ์รัฐเยอรมนี	-
สาธารณรัฐฝรั่งเศส	**Penal Coad. Article 226-4-1** การรวบรวมข้อมูลส่วนบุคคลด้วยวิธีการฉ้อฉลอันมิชอบด้วยกฎหมาย. **Penal Coad. Article 226-18** การกระทำโดยใช้ข้อมูลอย่างใดอย่างหนึ่งเพื่ออำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลซึ่งรวมไปถึงการใช้เครือข่ายสื่อสารออนไลน์เป็นเครื่องมือ อันมีวัตถุประสงค์เพื่อรบกวนความสงบของผู้อื่นหรือเพื่อให้ได้ไปซึ่งข้อมูลส่วนบุคคล
ประเทศไทย	-
รัฐแคลิฟอร์เนีย	**CA Bus & Prof Coad § 22948.2** การที่บุคคลใดบุคคลหนึ่งกระทำการโดยปราศจากความยินยอมหรืออำนาจจากผู้ประกอบธุรกิจ โดยใช้เว็บไซต์ จดหมายอิเล็กทรอนิกส์ หรือบริการอื่นๆบนอินเทอร์เน็ต เรียกร้อง ร้องขอ หรือชักจูงบุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล ด้วยการ

[202] ดู คณาธิป ทองรวีวงศ์ (เชิงอรรถ 50) 247.

[203] เพิ่งอ้าง 35-39.

ตารางที่ 4.5 (ต่อ)

การกระทำความผิดต่อข้อมูลส่วนบุคคล	
ประเทศ	**องค์ประกอบความผิดที่กฎหมายบัญญัติ**
รัฐแคลิฟอร์เนีย	แอบอ้างเป็นผู้แทนทางธุรกิจ
รัฐยูท่า	**UT Code § 13-04-201** การที่บุคคลใดบุคคลหนึ่งกระทำการโดยปราศจากความยินยอมหรืออำนาจจากผู้ประกอบธุรกิจและกระทำการด้วยวิธีการใดๆซึ่งรวมไปถึงการเปลี่ยนแปลงการตั้งค่าบนคอมพิวเตอร์หรืออุปกรณ์ที่ทำงานในลักษณะเดียวกันของบุคคลอื่นหรือใช้ซอฟแวร์เพื่อทำให้ผู้ใช้อินเทอร์เน็ตพบกับหน้าเว็บที่ได้มีการเตรียมไว้โดยปลอมแปลงและลอกเลียนเว็บเพจเพื่อ เรียกร้อง ร้องขอ หรือชักจูง บุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล ด้วยการแสดงตนเป็นผู้แทนทางธุรกิจ
รัฐนิวยอร์ก	**NY Gen Bus Law § 390-B** การที่บุคคลใดบุคคลหนึ่งกระทำการโดยปราศจากความยินยอมหรืออำนาจจากผู้ประกอบธุรกิจหรือหน่วยงานภาครัฐ โดยหลอกลวงหรือทำให้สำคัญผิดว่าเป็นผู้แทนทางธุรกิจ หรือหน่วยงานของรัฐผ่านเว็บเพจ หรือส่งจดหมายอิเล็กทรอนิกส์หรือใช้วิธีการทางอิเล็กทรอนิกส์ เพื่อทำให้ทราบถึง หรือร้องขอ ข้อมูลยืนยันตัวบุคคล
รัฐเทนเนสซี	**Tenn Code § 47-18-2503** การที่บุคคลใดบุคคลหนึ่งกระทำการโดยมิชอบด้วยกฎหมายและปราศจากความยินยอมหรืออำนาจกระทำการ แสดงตนเป็นผู้แทนหรือบุคคลอื่นผ่านทางอินเทอร์เน็ต โดยปลอมแปลงและลอกเลียนเว็บเพจหรือเว็บไซต์ หรือส่งจดหมายอิเล็กทรอนิกส์ หรือใช้วิธีการทางอิเล็กทรอนิกส์ ซึ่งรวมไปถึงการติดต่อสื่อสารในช่องทางอื่น เพื่อร้องขอหรือกระทำด้วยประการใดๆ เพื่อให้ได้มาซึ่งข้อมูล หรือเอกสารส่วนบุคคล และใช้ข้อมูลส่วนบุคคลเช่นว่านี้เพื่อตนเองหรือผู้อื่นหรือเพื่อจำหน่ายหรือแจกจ่าย โดยฉ้อฉล

จากตารางข้างต้นจะเห็นได้ว่า สาธารณรัฐเยอรมนี และประเทศไทย นั้นมิได้มีการบัญญัติบทบัญญัติในลักษณะนี้ไว้เป็นการเฉพาะ

สำหรับในส่วนของสาธารณรัฐฝรั่งเศสได้มีการบัญญัติให้ การรวบรวมข้อมูลส่วนบุคคลด้วยวิธีการฉ้อฉลอันมิชอบด้วยกฎหมาย ตามประมวลกฎหมายอาญาฝรั่งเศส มาตรา 226-4-1 และการกระทำโดยใช้ข้อมูลอย่างใดอย่างหนึ่งเพื่ออำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลซึ่งรวมไปถึงการใช้เครือข่ายสื่อสารออนไลน์เป็นเครื่องมือ อันมีวัตถุประสงค์เพื่อรบกวนความสงบของผู้อื่นหรือเพื่อให้ได้ไปซึ่งข้อมูลส่วนบุคคล ตาม มาตรา226-18 เป็นความผิดตามกฎหมาย ซึ่งเมื่อพิจารณาตามบทบัญญัติในข้างต้นจะเห็นได้ว่า

การกระทำความผิดดังที่ได้กล่าวไปในสองมาตราข้างตนนั้น สะท้อนให้เห็นถึงความพยามที่จะป้องกันการเข้าถึงและรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นโดนปราศจากอำนาจและความยินยอมจากเจ้าของข้อมูลที่แท้จริง

ในส่วนของบัญญัติของรัฐยูท่าได้บัญญัติให้ การกระทำโดยปราศจากความยินยอมหรืออำนาจจากผู้ประกอบธุรกิจและกระทำการด้วยวิธีการใดๆซึ่งรวมไปถึงการเปลี่ยนแปลงการตั้งค่าบนคอมพิวเตอร์หรืออุปกรณ์ที่ทำงานในลักษณะเดียวกันของบุคคลอื่นหรือใช้ซอฟแวร์เพื่อทำให้ผู้ใช้อินเทอร์เน็ตพบกับหน้าเว็บที่ได้มีการเตรียมไว้โดยปลอมแปลงและลอกเลียนเว็บเพจเพื่อ เรียกร้อง ร้องขอ หรือชักจูง บุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล ด้วยการแสดงตนเป็นผู้แทนทางธุรกิจ ไว้ในกฎหมายของรัฐยูท่า (UTAH E-COMMERCE INTEGRITY ACT มาตรา13-04-201 ซึ่งเมื่อพิจารณาจากองค์ประกอบความผิดของมาตรนี้จะเห็นได้ว่าในมาตรานี้นั้นได้แยกองค์ประกอบความผิดไว้เป็น 2 ลักษณะ กล่าวคือในมาตรานี้นั้นนอกจากจะกำหนดให้การอ้างตัวเป็นผู้แทนทางธุรกิจโดยปราศจากความยินยอมเป็นกระทำความผิดฐานฟิชชิ่งยังได้กำหนดให้การฟาร์มมิ่ง[204]เป็นความผิดตามมาตรานี้ด้วย ดังจะเห็นได้จากองค์ประกอบความผิดที่ได้กล่าวไปในส่วนของการใช้ซอฟแวร์เพื่อทำให้ผู้ใช้อินเทอร์เน็ตพบกับหน้าเว็บที่ได้มีการเตรียมไว้โดยปลอมแปลงและลอกเลียนเว็บเพจ อย่างไรก็ดีแม้ว่าในมาตรานี้จะแยกองค์ประกอบความผิดไว้เป็น 2 ลักษณะ แต่เจตนารมณ์ของบทบัญญัติก็เป็นไปเพื่อป้องกันการกระทำการใดๆเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลโดยปราศจากอำนาจและความยินยอมจากเจ้าของข้อมูล

ในส่วนของรัฐแคลิฟอร์เนียได้มีการบัญญัติให้ การกระทำการโดยปราศจากความยินยอมหรืออำนาจจากผู้ประกอบธุรกิจ โดยใช้เว็บไซต์ จดหมายอิเล็กทรอนิกส์ หรือบริการอื่นๆบนอินเทอร์เน็ต เรียกร้อง ร้องขอ หรือชักจูง บุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล ด้วยการแอบอ้างเป็นผู้แทนทางธุรกิจ ไว้ในมาตรา 22948.2 เมื่อพิจารณาจากองค์ประกอบการกระทำของบทบัญญัติดังที่ได้กล่าวไปในข้างต้นนั้นจะเห็นได้ว่าในบทบัญญัตินี้นั้นมีเจตนารมณ์ในการปกป้องข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวตนซึ่งรวมไปถึงเจ้าของธุรกิจที่แท้จริงที่ถูกนำมาแอบอ้างเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลโดยปราศจากอำนาจและความยินยอม นอกจากนี้การพยามกระทำความผิดตามบทบัญญัตินี้ยังถือเป็นการกระทำอันเป็นการละเมิดต่อก็หมายอีกด้วย

ในส่วนของบัญญัติของรัฐนิวยอร์กบัญญัติให้การกระทำการโดยปราศจากความยินยอมหรืออำนาจจากผู้ประกอบธุรกิจหรือหน่วยงานภาครัฐ โดยหลอกลวงหรือทำให้สำคัญผิดว่าเป็นผู้แทนทางธุรกิจ หรือหน่วยงานของรัฐ ผ่านเว็บเพจ หรือส่งจดหมายอิเล็กทรอนิกส์หรือ ใช้วิธีการทางอิเล็กทรอนิกส์ เพื่อทำให้ทราบถึง หรือร้องขอ ข้อมูลยืนยันตัวบุคคล ไว้ในมาตรา 390-B ซึ่งเมื่อพิจารณาจากองค์ประกอบความผิดของมาตรานี้จะเห็นได้ว่าในบทบัญญัตินี้นั้นมีเจตนารมณ์ในการปกป้องข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวตน ซึ่ง

---

[204] ฟาร์มมิ่ง (Pharming) คือ การเปลี่ยนลิงค์เว็บไซต์ที่แท้จริงให้ลิงค์ไปที่เว็บไซต์ปลอมอย่างผิดกฎหมาย และมีเจตนาขโมยข้อมูลส่วนตัวของผู้ใช้ อาทิ รหัสผ่าน หมายเลขบัญชี และข้อมูลสำคัญอื่นๆ

รวมไปถึงเจ้าของธุรกิจที่แท้จริงและหน่วยงานภาครัฐที่ถูกนำมาแอบอ้างเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลโดยปราศจากอำนาจและความยินยอม

ทั้งนี้ จากการศึกษาพบว่าบทบัญญัติของรัฐนิวยอร์กนั้นค่อนข้างที่จะมีลักษณะที่คลายคลึงกับบทบัญญัติของรัฐแคลิฟอร์เนียเป็นอย่างมากในแง่ของการกระทำเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลแต่จะแตกต่างในแง่ของผู้เสียหายในคดี กล่าวคือในบทบัญญัติของรัฐนิวยอร์กนั้นได้กำหนดให้การแอบอ้างเป็นหน่วยงานภาครัฐถือเป็นผู้เสียหายในมาตรานี้ด้วย อย่างไรก็ตามในบทบัญญัติของรัฐนิวยอร์กนั้นมิได้มีการกำหนดให้การเตรียมการกระทำความผิดในมาตรานี้เป็นการกระทำผิดต่อกฎหมายเหมือนดังเช่นบทบัญญัติของรัฐแคลิฟอร์เนีย

ต่อมาในส่วนของบทบัญญัติของรัฐเทนเนสซีได้บัญญัติให้การกระทำการโดยมิชอบด้วยกฎหมายและปราศจากความยินยอมหรืออำนาจกระทำการ แสดงตนเป็นผู้แทนหรือบุคคลอื่นผ่านทางอินเทอร์เน็ต โดยปลอมแปลงและลอกเลียนเว็บเพจหรือเว็บไซต์ หรือส่งจดหมายอิเล็กทรอนิกส์ หรือใช้วิธีการทางอิเล็กทรอนิกส์ ซึ่งรวมไปถึงการติดต่อสื่อสารในช่องทางอื่น เพื่อร้องขอหรือกระทำด้วยประการใดๆ เพื่อให้ได้มาซึ่งข้อมูล หรือเอกสารส่วนบุคคล และใช้ข้อมูลส่วนบุคคลเช่นว่านี้เพื่อตนเองหรือผู้อื่นหรือเพื่อจำหน่ายหรือแจกจ่าย โดยฉ้อฉล ไว้ในมาตรา 47-18-2503 ซึ่งเมื่อพิจารณาจากองค์ประกอบความผิดของมาตรนี้จะเห็นได้ว่าในมาตรานี้นั้นได้แยกองค์ประกอบความผิดไว้เป็น 2 ส่วน ซึ่งในส่วนแรกนั้นกำหนดให้การแสดงตนเป็นผู้แทนหรือบุคคลอื่นผ่านทางอินเทอร์เน็ต โดยปลอมแปลงและลอกเลียนเว็บเพจหรือเว็บไซต์ หรือส่งจดหมายอิเล็กทรอนิกส์ หรือใช้วิธีการทางอิเล็กทรอนิกส์ ซึ่งรวมไปถึงการติดต่อสื่อสารในช่องทางอื่น ด้วยวิธีการใดก็ตามเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลนั้นเป็นความผิดโดยในส่วนนี้จะคล้ายกับกฎหมายของ รัฐนิวยอร์ก รัฐแคลิฟอร์เนีย และรัฐยูทาห์ ต่อมาในส่วนที่สองกำหนดให้การนำข้อมูลที่ได้จากการหลอกลวงในส่วนแรกไปใช้งานต่อเพื่อให้ได้มาซึ่งข้อมูลที่ช่วยในการเข้าถึงแหล่งข้อมูลทางการเงิน เอกสารประจำตัวหรือประโยชน์ของบุคคลอื่นๆ นอกจากนี้การพยามกระทำความผิดตามบทบัญญัตินี้ยังถือเป็นการกระทำอันเป็นการละเมิดต่อกฎหมายอีกด้วย

อนึ่ง นอกจากบทบัญญัติดังที่ได้กล่าวมาในข้างต้นในส่วนของฐานความผิดที่มีความเกี่ยวข้องกับการกระทำผิดด้วยวิธีการฟิชชิ่ง แต่ละประเทศมีการบัญญัติฐานความผิดที่อยู่นอกเหนือจากตารางเปรียบเทียบดังที่ได้กล่าวไปข้างต้น ดังนี้

สำหรับในส่วนของประเทศไทย ยังมีฐานความผิดที่เกี่ยวเกี่ยวข้องกับการกระทำผิดด้วยวิธีการฟิชชิ่ง นอกเหนือจากที่บัญญัติไว้ในตารางอีกเพียงฐานเดียว คือ การส่งข้อมูลคอมพิวเตอร์อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์โดยปกติสุขของบุคคลอื่น ตามมาตรา 11

ส่วนสาธารณรัฐฝรั่งเศส ไม่ได้มีการบัญญัติฐานความผิดที่สามารถนำมาบังคับใช้กับฟิชชิ่งโดยตรงจึงจำเป็นที่จะต้องนำกฎหมายหลายบทมาปรับเพื่อบังคับใช้ โดยหนึ่งในบทบัญญัติสำคัญในการนำมาบังคับใช้กับการกระทำความผิดที่เกี่ยวข้องกับการฟิชชิ่ง คือ ความผิดฐานใช้หรือปลอมแปลงเครื่องหมายการค้าจดทะเบียนโดยไม่ได้รับอนุญาตจากเจ้าของเครื่องหมายการค้าจดทะเบียนที่แท้จริงตาม มาตรา L.335-2 และ L.713-2, L.713-3 แห่งประมวลกฎหมายทรัพย์สินทางปัญญาฝรั่งเศส

4.4 วิเคราะห์เปรียบเทียบบทลงโทษและค่าเสียหาย

ในหัวข้อนี้ผู้เขียนจะได้กล่าวถึงบทลงโทษและค่าเสียหายอันเกิดจากการกระทำความผิดฐานฟิชชิ่ง โดยนำบทบัญญัติทางกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับฟิชชิ่งของต่างประเทศดังที่ได้กล่าวไปใน บทที่ 3 กล่าวคือ กฎหมายของประเทศสหรัฐอเมริกา, กฎหมายธุรกิจทั่วไปรัฐนิวยอร์ก, ประมวลกฎหมายธุรกิจรัฐแคลิฟอร์เนีย, กฎหมายพาณิชย์และอิเล็กทรอนิกส์รัฐยูทาห์, กฎหมายรัฐเทนเนสซี, ประมวลกฎหมายของประเทศเยอรมัน และประมวลกฎหมายของประเทศฝรั่งเศส ซึ่งรวมไปถึงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยด้วย โดยผู้เขียนจะพิจารณาเฉพาะบทลงโทษและค่าเสียหายอันเกิดจากฐานความผิดที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับฟิชชิ่งเท่านั้น

4.3.1 บทลงโทษและค่าเสียหายตามกฎหมายไทย

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14(1) กำหนดระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ สำหรับการกระทำต่อประชาชน และโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับและเป็นความผิดอันยอมความได้ สำหรับกรณีการกระทำต่อบุคคลใดบุคคลหนึ่ง ตามมาตรา 14 วรรคสอง ซึ่งจากการศึกษาพบว่าในบทลงโทษตามบทบัญญัติ มาตรา 14(1) ก่อนการแก้ไข พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 กำหนดให้การกระทำความผิดในมาตรนี้มีโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ โดยไม่แยกว่าการกระทำความผิดตามมาตรานี้นั้นจะก่อให้เกิดความเสียหายต่อประชาชนหรือบุคคลใด

ตารางที่ 4.6 ตารางเปรียบเทียบพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 ในส่วนของมาตรา 14(1)

พ.ร.บ. คอมพิวเตอร์ฯ พ.ศ.2550	**พ.ร.บ. คอมพิวเตอร์ฯ ฉบับที่2 พ.ศ.2560**
ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น หรือประชาชน ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ	ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญาต้องระวางโทษจำคุกไม่เกิน5ปีหรือปรับไม่เกิน 100,000บาท หรือทั้งจำทั้งปรับ

เมื่อพิจารณาบทบัญญัติทั้งสองดังที่กล่าวมาในข้างต้นจะเห็นได้ว่าในการแก้ไขเพิ่มเติม มาตรา 14 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 เป็นการลดบทกำหนดโทษและค่าปรับสำหรับการกระทำความผิดตามมาตรานี้ทั้งที่ในข้อเท็จจริงของการกระทำความผิดเกี่ยวกับฟิชชิ่งนั้นก่อให้ให้เกิดความเสียหายต่อผู้เสียหายและภาพรวมทางเศรษฐกิจของประเทศซึ่งรวมไปถึงหน่วยงานภาครัฐ อีกทั้งในการกระทำผิดฐานฟิชชิ่งนั้นมักจะเป็นคดีที่ไม่มีพยานรู้เห็นและวิธีการในการตามหาตัวผู้กระทำความผิดก็ค่อนข้างที่จะเป็นไปได้ยากเพราะในการกระทำความผิดฐานฟิชชิ่งนั้นสามารถกระทำจากที่ไหนก็ได้ทั่วโลกจึงยากที่จะมีโอกาสหาตัวผู้กระทำความผิดหรือฟิชเชอร์ได้ ด้วยเหตุนี้เองจึงทำให้โอกาสในการกระทำความผิดสำเร็จเพิ่มขึ้นสูงมากขึ้นทำให้โอกาสที่ผู้กระทำความผิดหรือฟิชเชอร์นั้นจะได้รับผลประโยชน์ที่ได้จากการกระทำความผิดสูงมากขึ้นเช่นกัน เมื่อเทียบกับต้นทุนในการกระทำความผิดฐานฟิชชิ่งที่ต่ำมากทั้งยังสามารถกระทำได้ง่ายสามารถแบ่งงานกันทำและค่าใช้จ่ายในการกระทำความผิดแต่ละครั้งก็ไม่ได้สูงมาก

อย่างไรก็ตาม เมื่อพิจารณาถึงบทกำหนดโทษและค่าปรับที่ผู้กระทำความผิดจะได้รับหากถูกดำเนินคดีพบว่าอยู่ในระดับที่ต่ำมากจนเกินไปเมื่อเทียบกับความเสียหายแท้จริงที่เกิดขึ้น ทั้งนี้ เมื่อพิจารณาถึงกระบวนการในการดำเนินคดีกับผู้กระทำความผิดหรือฟิชเชอร์ ในกรณีที่การกระทำความผิดมีบทลงโทษทางกฎหมายทั้งในทางแพ่งและอาญาจะต้องรอให้การพิจารณาทางอาญาแล้วเสร็จเสียก่อนแล้วจึงจะดำเนินคดีในทางแพ่งเพื่อเรียกร้องค่าเสียหายจากการทำละเมิดในทางอาญาต่อได้ นอกจากนี้หากการดำเนินคดีอาญามีระยะเวลาที่นานจนทำให้อายุความในคดีแพ่งหมดลงหากผลจากการดำเนินคดีอาญาตัดสินให้ฝ่ายโจทย์เป็นฝ่ายชนะก็สามารถกลับมาเรียกร้องค่าเสียหายในทางแพ่งอีกครั้งได้แม้อายุความจะหมดไปแล้วก็ตามโดยไม่ถือว่าเป็นการฟ้องซ้ำ ซึ่งในส่วนของค่าเสียหายทางแพ่งนั้นก็เป็นไปตามดุลพินิจของศาลที่ผู้เสียหายนั้นมีหน้าที่นำสืบเพื่อให้ศาลเชื่อได้ว่าความเสียหายนั้นมีมากน้อยเพียงไร อีกทั้งจากการศึกษาพบว่าในปัจจุบันในกฎหมายของประเทศไทยนั้นยังมิได้มีการกำหนดบทบัญญัติในการเรียกค่าเสียหายเพิ่มเติมที่จะทำให้ผู้เสียหายสามารถเรียกร้องค่าเสียหายเพิ่มเติมได้จากค่าเสียหายที่แท้จริงอันเป็นค่าเสียหายเชิงลงโทษ[205]เหมือนอย่างในต่างประเทศที่กำหนดให้สามารถเรียกร้องค่าเสียหายเชิงลงโทษได้ซึ่งผู้เขียนจะได้กล่าวในหัวข้อต่อไป

4.3.2 บทลงโทษและค่าเสียหายตามกฎหมายต่างประเทศ

สำหรับในส่วนของบทลงโทษและค่าเสียหายตามกฎหมายต่างประเทศนั้นในบางประเทศมักมีการกำหนดค่าเสียหายในเชิงลงโทษไว้ อย่างไรก็ตามจากการศึกษาพบว่าไม่ใช้ทุกประเทศที่จะมีการกำหนดค่าเสียหายเชิงลงโทษแก่การกระทำความผิดฐานฟิชชิ่ง โดยในหัวข้อนี้ผู้เขียนจะขอกล่าวถึงทั้งประเทศที่มีการกำหนดค่าเสียหายเชิงลงโทษและประเทศที่ไม่มีการกำหนดค่าเสียหาย เชิงลงโทษ

---

[205] ค่าเสียหายเชิงลงโทษ (Punitive Damages) หรือ “ค่าเสียหายเพื่อเป็นเยี่ยงอย่าง” (Exemplary Damages) คือ ค่าเสียหายทางแพ่งที่ถูกกำหนดขึ้นเพิ่มเติมจากค่าเสียหายที่แท้จริงที่ผู้ถูกกระทำละเมิดได้รับ มีจุดมุ่งหมายเพื่อลงโทษผู้กระทำละเมิดให้เกิดความเข็ดหลาบไม่กล้ากระทำละเมิดเช่นนั้นอีก. มานิตย์ จุมปา, *ความรู้เบื้องต้นเกี่ยวกับกฎหมายสหรัฐอเมริกา* (พิมพ์ครั้งที่ 2, สำนักพิมพ์วิญญชน 2553) 129-130.

สำหรับบทลงโทษและค่าเสียหายในส่วนของสหพันธรัฐเยอรมนีนั้น มิได้มีการบัญญัติค่าเสียหายในเชิงลงโทษไว้ในฐานความผิดฟิชชิ่ง ตามมาตรา 202b แห่งประมวลกฎหมายอาญาเยอรมนี อีกทั้งบทบัญญัติโทษตามมาตราดังกล่าวยังถือว่าน้อยกว่า มาตรา 14(1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 กล่าวคือ มาตรา 202b มีบทบัญญัติโทษ คือ ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับเว้นแต่ความผิดนั้นมีบทลงโทษที่มีโทษสูงกว่าภายใต้ บทบัญญัติอื่นๆ

ต่อมาในส่วนของสาธารณรัฐฝรั่งเศสนั้น ในบทบัญญัติโทษมิได้มีการบัญญัติในเรื่องของค่าเสียหายในเชิงลงโทษไว้ในบทบัญญัติในฐานความผิดที่มีความเกี่ยวข้องกับการกระทำความผิดฐานฟิชชิ่ง อย่างไรก็ดีเนื่องจากประเทศฝรั่งเศสนั้นมิได้มีการมีการบัญญัติฐานความผิดที่สามารถนำมาบังคับใช้กับฟิชชิ่งโดยตรงจึงจำเป็นที่จะต้องนำกฎหมายหลายบทมาปรับเพื่อบังคับใช้ตามแต่พฤติการณ์ในการกระทำความผิด ซึ่งจากการศึกษาพบว่ามีบทบัญญัติที่สามารถนำมาบังคับโทษกับการกระทำความผิดเกี่ยวกับการฟิชชิ่ง ดังนี้

มาตรา 226-18 แห่งประมวลกฎหมายอาญาฝรั่งเศสที่มีบทบัญญัติโทษ คือ ต้องระวางโทษจำคุก 5 ปี หรือปรับ 300,000 ยูโร

มาตรา 226-4-1 แห่งประมวลกฎหมายอาญาฝรั่งเศสที่มีบทบัญญัติโทษ คือ ต้องระวางโทษจำคุก 1 ปี หรือปรับ 150,000 ยูโร หรือหากเป็นกรณีการกระทำที่เกิดขึ้นจากคู่สมรสหรือหุ้นส่วนคู่ชีวิตจะมีโทษเพิ่มขึ้นเป็น ต้องระวางโทษจำคุก 2 ปีหรือปรับ 300,000 ยูโร

มาตรา 313-1 แห่งประมวลกฎหมายอาญาฝรั่งเศสที่มีบทบัญญัติโทษ คือ ต้องระวางโทษจำคุก 5 ปี หรือปรับ 375,000 ยูโร

มาตรา 321-1 แห่งประมวลกฎหมายอาญาฝรั่งเศสที่มีบทบัญญัติโทษ คือ ต้องระวางโทษจำคุก 3 ปี หรือปรับ 100,000 ยูโร ซึ่งอาจขยายไปได้ถึงจำคุก 5 ปี หรือปรับ 150,000 ยูโรหรือหากเป็นกรณีกระทำต่อหน่วยงานภาครัฐ ต้องระวางโทษจำคุก 7 ปีหรือปรับ 300,000 ยูโร

มาตรา 323-3 แห่งประมวลกฎหมายอาญาฝรั่งเศสที่มีบทบัญญัติโทษ คือ ต้องระวางโทษจำคุก 5 ปีหรือปรับ 150,000 ยูโร หรือหากเป็นกรณีกระทำต่อหน่วยงานภาครัฐต้องระวางโทษจำคุก 7 ปีหรือปรับ 300,000 ยูโร

มาตรา L.335-2 แห่งประมวลกฎหมายทรัพย์สินทางปัญญาฝรั่งเศสที่มีบทบัญญัติโทษ คือ ต้องระวางโทษจำคุก 3 ปี หรือปรับ 300,000 ยูโร ซึ่งอาจขยายไปได้ถึงจำคุก 7ปี หรือปรับ 750,000 ยูโร หากเป็นกรณีที่กระทำเป็นกลุ่ม

เมื่อพิจารณาจากบทกำหนดโทษในข้างต้นจะเห็นได้ว่าในประเทศฝรั่งเศสนั้นแม้ว่าจะมิได้มีการกำหนดค่าเสียหายในเชิงลงโทษแต่ได้มีการกำหนดบทเพิ่มโทษ ในกรณีที่เป็นการกระทำผิดต่อภาครัฐดังจะเห็นได้จากบทบัญญัติโทษใน มาตรา 321-1 และ มาตรา 323-3 อย่างไรก็ดีเมื่อพิจารณาถึงบทบัญญัติโทษในการกระทำผิดฐานฟิชชิ่งของสาธารณรัฐฝรั่งเศสและประเทศไทย ทำให้ทราบได้ว่าในบทบัญญัติโทษของสาธารณรัฐฝรั่งเศสนั้นมีการกำหนดบทบัญญัติโทษทั้งจำคุกและโทษปรับที่มากกว่าประเทศไทยอย่างเห็นได้ชัด กล่าวคือมีโทษจำคุกเฉลี่ยอยู่ที่ 3-7 ปี อย่างไรก็ตามในบทกำหนดโทษของสาธารณรัฐฝรั่งเศสไม่เพียงแต่กำหนดโทษที่สูง

กว่าเพียงเท่านั้นแต่ยังได้กำหนดบทเพิ่มโทษสำหรับการกระทำต่อองค์กรภาครัฐ อันสะท้อนให้เห็นถึงการให้ความสำคัญกับการกระทำความผิดต่อระบบประมวลผลข้อมูลของภาครัฐ

ในส่วนของรัฐนิวยอร์กได้มีการกำหนดค่าเสียหายเชิงลงโทษและการชดเชยความเสียหายที่เกิดขึ้นจากการกระทำความผิดไว้ใน มาตรา 390-B แห่งกฎหมายธุรกิจทั่วไป โดยผู้เสียหายหรือผู้ที่ได้รับผลกระทบซึ่งรวมไปถึงผู้ประกอบการธุรกิจที่โดนแอบอ้างจากการกระทำความผิดฐานฟิชชิ่งสามารถเรียกร้องค่าเสียหายได้ตามมูลค่าแท้จริงที่เกิดขึ้น หรือ 1,000 ดอลลาร์ ต่อการละเมิดหนึ่งครั้งและ ศาลอาจกำหนดค่าเสียหายสูงสุดเพิ่มขึ้นได้อีกสามเท่าของในกรณีที่ผู้กระทำความผิดมีส่วนในการเข้าร่วมในการกระทำผิดอันเป็นการฝ่าฝืนบทบัญญัตินี้ ซึ่งรวมไปถึงการที่ศาลกำหนดค่าใช้จ่ายในการดำเนินคดีและค่าธรรมเนียมศาลตามที่เห็นสมควรแก่โจทท์ผู้ชนะคดี อีกทั้งการชดใช้เรียกร้องค่าเสียหายตามบทบัญญัตินี้ไม่ถือว่าเป็นการตัดสิทธิในการเรียกร้องค่าเสียหายตามกฎหมายอื่นเพิ่มเติม

ในส่วนของรัฐแคลิฟอร์เนียได้กำหนดค่าเสียหายเชิงลงโทษและการชดเชยความเสียหายที่เกิดขึ้นจากการกระทำความผิดไว้ใน มาตรา 22948.3 แห่งประมวลกฎหมายรัฐแคลิฟอร์เนีย โดยกำหนดให้ผู้ที่ได้รับผลกระทบและผู้ประกอบการธุรกิจที่โดนแอบอ้างนั้นสามารถฟ้องร้องเรียกค่าเสียหายได้มากกว่าจำนวนค่าเสียหายที่แท้จริงที่เกิดขึ้น หรือเป็นเงินจำนวน 500,000 ดอลลาร์ และผู้ที่ได้รับผลกระทบอาจฟ้องร้องเรียกค่าเสียหายได้มากว่าค่าเสียหายที่แท้จริงเป็นจำนวนกว่าสามเท่าของมูลค่าความเสียหายที่แท้จริง หรือ 5,000 ดอลลาร์ ต่อการละเมิดหนึ่งครั้ง อย่างไรก็ดีพนักงานอัยการหรือทนายความสามารถฟ้องร้องเรียกค่าเสียหายทางแพ่งเพิ่มเติมต่อศาลจากผู้กระทำความผิดได้สูงสุดไม่เกินกว่า 2,500 ดอลลาร์ต่อการละเมิดหนึ่งครั้ง ซึ่งรวมไปถึงการที่ศาลกำหนดค่าใช้จ่ายในการดำเนินคดีและค่าธรรมเนียมศาลตามที่เห็นสมควรแก่โจทท์ผู้ชนะคดี อีกทั้งการชดใช้เรียกร้องค่าเสียหายตามบทบัญญัตินี้ไม่ถือว่าเป็นการตัดสิทธิในการเรียกร้องค่าเสียหายตามกฎหมายอื่นเพิ่มเติม

ในส่วนของรัฐเทนเนสซีได้กำหนดค่าเสียหายเชิงลงโทษและการชดเชยความเสียหายที่เกิดขึ้นจากการกระทำความผิดไว้ใน มาตรา 47-18-2504 แห่งประมวลกฎหมายรัฐเทนเนสซี โดยกำหนดให้ผู้เสียหายและผู้ประกอบการธุรกิจที่โดนแอบอ้างนั้นสามารถฟ้องร้องเรียกค่าเสียหายได้มากกว่าจำนวนค่าเสียหายที่แท้จริงที่เกิดขึ้น หรือเป็นเงินจำนวน 500,000 ดอลลาร์ และผู้ที่ได้รับผลกระทบอาจฟ้องร้องเรียกค่าเสียหายได้มากว่าค่าเสียหายที่แท้จริงเป็นจำนวนกว่าสามเท่าของมูลค่าความเสียหายที่แท้จริง หรือ 5,000 ดอลลาร์ต่อการละเมิดหนึ่งครั้ง อย่างไรก็ดีพนักงานอัยการหรือทนายความสามารถฟ้องร้องเรียกค่าเสียหายทางแพ่งเพิ่มเติมต่อศาลจากผู้กระทำความผิดได้สูงสุดไม่เกินกว่า 2,500 ดอลลาร์ต่อการละเมิดหนึ่งครั้ง ซึ่งรวมไปถึงการที่ศาลอาจกำหนดค่าเสียหายสูงสุดเพิ่มขึ้นได้อีกสามเท่าของในกรณีที่ผู้กระทำความผิดมีส่วนในการเข้าร่วมในการกระทำผิดอันเป็นการฝ่าฝืนบทบัญญัตินี้ และกำหนดค่าใช้จ่ายในการดำเนินคดีและค่าธรรมเนียมศาลตามที่เห็นสมควรแก่โจทท์ผู้ชนะคดี อีกทั้งการชดใช้เรียกร้องค่าเสียหายตามบทบัญญัตินี้ไม่ถือว่าเป็นการตัดสิทธิในการเรียกร้องค่าเสียหายตามกฎหมายอื่นเพิ่มเติม

ในส่วนของรัฐยูท่าได้กำหนดค่าเสียหายเชิงลงโทษและการชดเชยความเสียหายที่เกิดขึ้นจากการกระทำความผิดไว้ในมาตรา13-40-401 แห่งประมวลกฎหมายพานิชย์อิเล็กทรอนิกส์ยูท่าโดยกำหนดให้บุคคลผู้มีอำนาจในการดำเนินคดีสามารถดำเนินคดีทางแพ่งโดยมีสิทธิที่จะเรียกร้องค่าเสียหายได้ตามจำนวนความเสียหายที่เกิดขึ้นจริง หรือปรับในทางแพ่งไม่เกินกว่า 150,000 ดอลลาร์ ต่อการกระทำละเมิดหนึ่งครั้ง

ทั้งนี้ เมื่อพิจารณาจากบทบัญญัติดังที่ได้กล่าวไปในข้างต้นในส่วนของการกำหนดฐานความผิดเกี่ยวกับการกระทำฟิชชิ่ง รัฐนิวยอร์ก, รัฐยูท่า, รัฐแคลิฟอร์เนีย, และรัฐเทนเนสซี จะเห็นได้ว่ามีการกำหนดค่าเสียหายเชิงลงโทษไว้ในบทกำหนดโทษของรัฐอย่างชัดเจนอีกทั้งจากการศึกษาพบว่าในส่วนของรัฐยูท่า, รัฐแคลิฟอร์เนีย, และรัฐเทนเนสซี ได้มีการกำหนดให้มีโทษปรับในทางแพ่งเพิ่มเติมจากโทษปรับแบบปกติ ดังจะเห็นได้จากบทบัญญัติในข้างต้น และเมื่อพิจารณาถึงบทกำหนดโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และฉบับที่2 พ.ศ.2560 ทำให้ทราบได้ว่าในส่วนของการกำหนดโทษต่อการกระทำความผิดเกี่ยวกับฟิชชิ่งในส่วนของประเทศไทยนั้นมีอัตราโทษที่ค่อนข้างข้างที่จะต่ำเป็นอย่างมาก ดังจะสังเกตุได้จากบทบัญญัติโทษในมาตรา 14(1) ที่ถือได้ว่าเป็นบทบัญญัติหลักที่ถูกนำมาใช้กับการกระทำความผิดที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับฟิชชิ่ง กล่าวคือ มีการกำหนดโทษจำคุกไว้เพียงจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ สำหรับการกระทำต่อประชาชน และโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับและเป็นความผิดอันยอมความได้ สำหรับกรณีการกระทำต่อบุคคลใดบุคคลหนึ่ง[206]

อย่างไรก็ตามเมื่อพิจารณาจากทฤษฎีการลงโทษส่วนใหญ่ที่ได้รับการยอมรับโดยทั่วไปจะเห็นได้ว่าในการกำหนดบทลงโทษบุคคลส่วนใหญ่แล้วมักจะเริ่มมาจากการลงโทษทางอาญาซึ่งจากการศึกษาพบว่าในการกำหนดบทลงโทษจากการกระทำความผิดแต่เดิมนั้นมักจะนำแนวคิดในการลงโทษทางอาญามาบังคับใช้กับการกระทำความผิดของบุคคลเพียงอย่างเดียว โดยไม่มีการนำแนวคิดอื่นมาใช้ร่วมด้วยในการลงโทษเพราะถือว่าการจองจำหรือการทำให้เสียเสรีภาของบุคคลนั้นถือเป็นโทษสูงสุดแล้วที่จะสามารถนำมาบังคับต่อบุคคลได้รองจากโทษประหารชีวิต อย่างไรก็ตามเมื่อยุคสมัยเปลี่ยนไปการรูปแบบในการกระทำความผิดและสังคมก็มีความซับซ้อนมากขึ้น การบังคับใช้โทษทางอาญาเองก็มีความจำเป็นที่จะต้องเปลี่ยนแปลงไปตามยุคสมัยและความซับซ้อนของสังคมดุลกัน โดยเฉพาะอย่างยิ่งในการบังคับใช้โทษทางอาญาสำหรับความผิดบางประการ อาทิ ความผิดทางเศรฐกิจ และความผิดทางคอมพิวเตอร์ ที่เป็นไปอย่างไม่มีประสิทธิภาพมากพอที่จะยังยั้งการกระทำความผิดหรือสร้างความยำเกรงให้แก่ผู้กระทำความผิด อาทิ องค์ประกอบความผิด ภาระในการพิสูจน์และระยะเวลาในการดำเนินคดีที่มีอย่างจำกัดด้วยเหตุนี้เองจึงได้มีการนำแนวคิดในการดำเนินคดีโดยใช้มาตรการอื่นใดที่อยู่นอกเหนือไปจากการลงโทษตามแนวคิดทางอาญา อาทิ การนำมาตรการลงโทษทางแพ่งมาบังคับใช้เป็นมาตรการในการลงโทษอย่างนึง โดยนำหลักการอันเป็นประเด็นสำคัญในการลงโทษทางอาญามากำหนดเป็นมาตรการสำคัญที่จะนำมาใช้ในการกำหนดมาตรการซึ่งเป็นผลร้ายต่อตัวผู้กระทำความผิด กล่าวคือ นำโทษปรับมาบังคับใช้อย่างผสมผสานกับการลงโทษทางแพ่งซึ่งมีลักษณะในการลงโทษที่มุ่งเน้นไปที่

---

[206] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 มาตรา14(5).

การชดเชยความเสียหายต่อตัวผู้เสียหายโดยใช้วิธีการและมาตรฐานในการพิสูจน์ในทางแพ่งมาปรับใช้เพราะลำพังเพียงการนำผู้กระทำความผิดมาลงโทษด้วยวิธีการคุมขังอาจไม่เพียงพอเมื่อเทียบกับจำนวนทรัพย์สินที่ผู้เสียหายนั้นสูญไป ซึ่งจากการศึกษาพบว่าในกฎหมายต่างประเทศดังที่ได้กล่าวมาในข้างต้นได้มีการกำหนดหลักเกณฑ์ที่ใช้ในการเรียกร้องค่าเสียหายเพิ่มเติมได้มากกว่าค่าเสียหายที่แท้จริงอันมีวัตถุประสงค์เพื่อเป็นการลงโทษและข่มขู่ยังยั้งไม่ให้ผู้กระทำความผิดกลับมากระทำผิดซ้ำ ซึ่งในส่วนนี้เองผู้เขียนเห็นว่าในการกำหนดบทบัญญัติโทษต่อการกระทำที่เกี่ยวของกับการพิชชิ่งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ควรมีการกำหนดเพิ่มโทษปรับเป็นจำนวนสองเท่าจากผลประโยน์ที่ได้รับเนื่องจากต้นทุนของอาชญากรในการกระทำความผิดนั้นค่อนข้างต่ำ เพราะโอกาสในการถูกดำเนินคดีและจับกุมมีโอกาสที่น้อยเป็นอย่างมากเมื่อเทียบกับคดีในฐานความผิดอื่นอย่างการฉ้อโกงประชาชนด้วยเหตุนี้เองจึงมีความจำเป็นที่จะต้องเพิ่มบทลงโทษเพื่อเป็นการทดแทนโอกาสในการถูกจับกุมที่สูญไป[207] และด้วยเหตุนี้เองผู้เขียนเห็นควรว่าในการแก้ไขบทบัญญัติโทษในส่วนของการกระทำฟิชชิ่งควรมีการกำหนดบทลงโทษที่รุนแรงขึ้นเพื่อเป็นการรักษาระดับต้นทุนของการกระทำความผิดให้สัมพันธ์กับโทษที่จะได้รับเมื่อถูกจับกุม

4.5 วิเคราะห์สิทธิในการดำเนินคดีของผู้เสียหาย

ในส่วนของหัวข้อนี้ผู้เขียนจะได้กล่าวถึงสิทธิในการดำเนินคดีของผู้ได้รับความเสียหายจากการกระทำความผิดเกี่ยวกับฟิชชิ่ง โดยนำบทบัญญัติทางกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับฟิชชิ่งของต่างประเทศดังที่ได้กล่าวไปใน บทที่ 3 กล่าวคือ กฎหมายของประเทศสหรัฐอเมริกา, กฎหมายธุรกิจทั่วไปรัฐนิวยอร์ก, ประมวลกฎหมายธุรกิจรัฐแคลิฟอร์เนีย, กฎหมายพาณิชย์และอิเล็กทรอนิกส์รัฐยูทาห์, กฎหมายรัฐเทนเนสซี, ประมวลกฎหมายของประเทศเยอรมัน และประมวลกฎหมายของประเทศฝรั่งเศส ซึ่งรวมไปถึงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประมวลกฎหมายอาญา ของประเทศไทยด้วย

4.5.1 สิทธิในการดำเนินคดีของผู้เสียหายตามกฎหมายไทย

ในส่วนของผู้ที่มีสิทธิดำเนินคดีตามกฎหมายไทยนั้น กำหนดว่าต้องเป็นผู้ที่ได้รับความเสียหายจากการกระทำผิดทางอาญาฐานใดฐานหนึ่งในประมวลกฎหายอาญา[208]หรือกฎหมายอื่นใดที่บัญญัติโทษทางอาญาไว้ ซึ่งรวมไปถึงผู้ที่มีอำนาจจัดการแทน หรือหากอ้างตามแนวคำพิพากษาศาลฎีกาอาจมีคความหมายถึงกรณีที่มีการกระทำความผิดฐานใดฐานหนึ่งที่เป็นการละเมิดต่อกฎหมายเกิดขึ้นบุคคลผู้ที่ได้รับผลกระทบหรือความเสียหายจากการกระทำอันเป็นการละเมิดต่อกฎหมายซึ่งในที่นี้คือการกระทำความผิดฐานฟิชชิ่ง บุคคลจะถือ

---

[207] ปกป้อง ศรีสนิท, *กฎหมายอาญาชั้นสูง* (พิมพ์ครั้งที่ 3, สำนักพิมพ์วิญญูชน 2563) 107.

[208] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตร2(4) หมายถึง "บุคคลผู้ได้รับความเสียหายเนื่องจากการกระทำความผิดทางอาญาฐานใดฐานหนึ่ง..."

ได้ว่าเป็นผู้เสียหายโดยนิตินัยแม้จะไม่ใช้ผู้ที่ได้รับผลกระทบโดยตรงหรือเป็นเป้าหมาย[209]ก็ตามเพราะในการก่ออาชญากรรมรูปแบบฟิชชิ่งนั้นจำเป็นที่จะต้องมีการแอบอ้างผ่านระบบเครือข่ายคอมพิวเตอร์เพื่อทำการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่จะถูกนำไปใช้ในการกระทำความผิดฐานอื่นเพิ่มเติมเพื่อให้ได้มาซึ่งทรัพย์สิน อย่างไรก็ดีผู้เสียหายในทางนิตินัยยังรวมไปถึงผู้ให้บริการเครือข่ายที่ได้รับผลกระทบจากการกระทำความผิด หรือเจ้าของเว็บเพจที่โดยแอบอ้าง หรือบุคคลที่โดนแอบอ้าง หรือเจ้าของเครื่องหมายการค้าที่ถูกละเมิดโดยการนำเครื่องหมายการค้านั้นไปใช้โดยปราศจากความยินยอม หรืออัยการ

4.5.2 สิทธิในการดำเนินคดีของผู้เสียหายตามกฎหมายต่างประเทศ.

สำหรับในส่วนของประมวลกฎหมายประเทศเยอรมัน ได้กำหนดบทบัญญัติเกี่ยวกับผู้ที่มีสิทธิในการดำเนินคดีไว้ในประมวลกฎหมายอาญาเยอรมัน โดยกำหนดผู้ที่มีสิทธิฟ้องร้องดำเนินคดีจะต้องเป็นผู้เสียหายที่แท้จริง ซึ่งรวมไปถึงผู้แทนผู้เสียหายในกรณีที่ผู้เสียหายนั้นถึงแก่ความตายอันได้แก่ คู่สมรสและบุตร บิดามารดา พี่น้อง และหลานของผู้เสียหาย หรือหากเป็นกรณีที่ผู้เสียหายเป็นบุคคลไร้ความสามารถตามกฎหมาย หรือเป็นผู้ที่ศาลสั่งให้เป็นบุคคลเสมือนไร้ความสามารถ หรือถูกจำกัดสิทธิตามกฎหมาย กรณีนี้ผู้แทนตามกฎหมายซึ่งเป็นผู้จัดการงานเฉพาะตัว และผู้ที่มีหน้าที่ดูแลบุคคลนั้นๆสามารถเป็นผู้ที่มีสิทธิยื่นคำร้องแทนผู้เสียหายได้ นอกจากนี้แล้วผู้เสียหายในคดียังรวมไปถึงพนักงานอัยการที่จะเข้ามามีส่วนในการดำเนินคดีในกรณีที่การกระทำความผิดนั้นเป็นความผิดที่กระทบต่อประโยชน์สาธารณะ โดยอัยการสามารถฟ้องเข้ามาเป็นโจทก์ร่วมกับผู้เสียหายในระหว่างการดำเนินคดีได้ได้ทุกเมื่อ โดยการยื่นคำร้องขอเข้าร่วมเป็นโจทก์กับผู้เสียหายในคดีและเมื่อพนักงานอัยการเข้ามาเป็นโจทก์ร่วมแล้วพนักงานอัยการจะเป็นผู้รับผิดชอบในการดำเนินคดีโดยตรงต่อจากผู้เสียหายส่วนผู้เสียหายนั้นจะลดบทบาทในการดำเนินคดีเป็นรองจากพนักงานอัยการทันที โดยผู้เสียจะกลายเป็นโจทก์ร่วมและมีสิทธิต่างๆในฐานะคู่ความในคดีเพียงเท่านั้น

ต่อมาในส่วนของประเทศฝรั่งเศส ได้กำหนดบทบัญญัติเกี่ยวกับผู้ที่มีสิทธิในการดำเนินคดีไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาสาธารณรัฐฝรั่งเศส โดยกำหนดไว้ในมาตรา 2 วรรคแรก บัญญัติว่าผู้เสียหายต้องเป็นบุคคลที่ได้รับความเสียหายโดยตรงจากการกระทำความผิดอาญา ซึ่งรวมไปถึงผู้ที่เข้ามาจัดการแทนผู้เสียหายในกรณีที่ผู้เสียหายนั้นถึงแก่ความตาย เช่น บิดามารดา บุตรหรือคู่สมรสของผู้เสียหาย[210]อย่างไรก็ตามผู้เสียหายโดยตรงไม่มีอำนาจฟ้องคดีอาญาได้ด้วยตนเอง หากแต่กระทำได้เพียงร้องทุกข์ต่อพนักงานอัยการหรือตำรวจเพื่อให้ทำการสอบสวนความผิดอาญาที่เกิดขึ้นเท่านั้นและถึงแม้ว่าผู้เสียหายจะไม่มีอำนาจฟ้องคดีอาญาได้โดยตรงแต่ก็อาจใช้วิธีทางอ้อม ซึ่งเป็นสิทธิที่สำคัญของผู้เสียหายในคดีอาญาเพื่อให้พนักงานอัยการฟ้องคดีอาญาได้ด้วยวิธีการฟ้องคดีแพ่งเรียกค่าเสียหายที่เกิดขึ้นเนื่องจากการกระทำผิดอาญาดังกล่าวซึ่งจะมีผลในทางกฎหมายให้พนักงานอัยการต้องฟ้องคดีอาญาในการกระทำเดียวกันนั้นต่อไป

ในส่วนของกฎหมายรัฐนิวยอร์ก ได้กำหนดบทบัญญัติเกี่ยวกับผู้ที่มีสิทธิในการดำเนินคดีไว้ในประมวลกฎหมายธุรกิจทั่วไปนิวยอร์ก โดยกำหนดให้ผู้ที่มีสิทธิในการดำเนินคดีจะต้องเป็นผู้ที่ได้รับผลกระทบจากการกระทำความผิดซึ่งในที่นี้คือการกระทำความผิดฐานฟิชชิ่ง อย่างไรก็ดีสิทธิในการดำเนินคดีของผู้เสียหายยังครอบคลุม

---

[209] คณิต ณ นคร, *กฎหมายวิธีพิจารณาความอาญา เล่ม1* (พิมพ์ครั้งที่ 10, สำนักพิมพ์วิญญูชน 2564) 152-154.

[210] อุทัย อาทิเวช (เชิงอรรถ 163) 52-54.

ไปถึง พนักงานอัยการหรือผู้ประกอบธุรกิจให้บริการอินเทอร์เน็ตสาธารณะ เจ้าของเว็บเพจ หรือเจ้าของเครื่องหมายการค้า ซึ่งรวมไปถึงบุคคลผู้ซึ่งได้รับความเสียหายจากการกระทำความผิดฐานฟิชชิ่ง

ในส่วนของกฎหมายรัฐแคลิฟอร์เนีย ได้กำหนดบทบัญญัติเกี่ยวกับผู้ที่มีสิทธิในการดำเนินคดีไว้ในประมวลกฎหมายธุรกิจและวิชาชีพแคลิฟอร์เนีย โดยกำหนดให้ผู้ที่มีสิทธิในการดำเนินคดีจะต้องเป็นผู้ที่ได้รับผลกระทบจากการกระทำความผิดซึ่งในที่นี้คือการกระทำความผิดฐานฟิชชิ่ง อย่างไรก็ดีสิทธิในการดำเนินคดีของผู้เสียหายยังครอบคลุมไปถึง พนักงานอัยการหรือทนายความ หรือผู้ประกอบธุรกิจให้บริการอินเทอร์เน็ตสาธารณะ เจ้าของเว็บเพจ หรือเจ้าของเครื่องหมายการค้า ซึ่งรวมไปถึงบุคคลผู้ซึ่งได้รับความเสียหายจากการกระทำความผิดฐานฟิชชิ่ง

ในส่วนของกฎหมายรัฐเทนเนสซี ได้กำหนดบทบัญญัติเกี่ยวกับผู้ที่มีสิทธิในการดำเนินคดีไว้ในประมวลกฎหมายรัฐเทนเนสซี โดยกำหนดให้ผู้ที่มีสิทธิในการดำเนินคดีจะต้องเป็นผู้ที่ได้รับผลกระทบจากการกระทำความผิดซึ่งในที่นี้คือการกระทำความผิดฐานฟิชชิ่ง อย่างไรก็ดีสิทธิในการดำเนินคดีของผู้เสียหายยังครอบคลุมไปถึง พนักงานอัยการหรือทนายความ หรือผู้ประกอบธุรกิจให้บริการอินเทอร์เน็ตสาธารณะ เจ้าของเว็บเพจ หรือเจ้าของเครื่องหมายการค้า

ในส่วนของกฎหมายรัฐยูทาห์ ได้กำหนดบทบัญญัติเกี่ยวกับผู้ที่มีสิทธิในการดำเนินคดีไว้ในประมวลกฎหมายรัฐยูทาห์ โดยกำหนดให้ผู้ที่มีสิทธิในการดำเนินคดีจะต้องเป็นผู้ที่ได้รับผลกระทบความเสียหายจากการกระกระทำความผิดซึ่งในที่นี้คือการกระทำความผิดฐานฟิชชิ่ง อย่างไรก็ดีสิทธิในการดำเนินคดีของผู้เสียหายยังครอบคลุมไปถึง ผู้ประกอบธุรกิจให้บริการอินเทอร์เน็ตสาธารณะ เจ้าของเว็บเซิร์ฟเวอร์ เจ้าของเซิร์ฟเวอร์ หรือเจ้าของเครื่องหมายการค้าที่ถูกนำไปใช้โดยปราศจากความยินยอม หรือพนักงานอัยการ

อนึ่ง เมื่อพิจารณาจากหมายของประเทศต่างๆดังที่ได้กล่าวไปในข้างต้นจะพบว่าผู้ที่ได้รับผลกระทบจากการกระทำความผิดฐานฟิชชิ่งไม่ได้จำกัดเพียงแค่ผู้เสียหายที่เป็นเจ้าของข้อมูลหรือทรัพย์สินเพียงเท่านั้นที่ได้รับผลกระทบ แต่ยังรวมไปถึงผู้ประกอบธุรกิจเกี่ยวกับการให้บริการด้านอินเทอร์เน็ตสาธารณะ, ผู้ให้บริการเว็บไซต์, และเจ้าของเว็บเพจหรือเจ้าของเครื่องหมายการค้าที่ถูกนำไปแอบอ้าง ด้วยที่ได้รับความเสียหายจากการกระทำความผิดดังกล่าวเพราะการกระทำความผิดฐานฟิชชิ่งนั้นไม่ได้จำกัดอยู่แค่เพียงการกระทำความผิดต่อตัวบุคคลเพียงเท่านั้น นอกจากนี้ยังรวมไปถึงอัยการและผู้แทนผู้เสียหายอีกด้วย

บทที่ 5
บทสรุปและข้อเสนอแนะ

ในบทนี้ผู้เขียนจะได้กล่าวถึงบทสรุปจากการศึกษาปัญหาการบังคับใช้กฎหมายกับการกระทำความผิดที่เกี่ยวข้องกับการกระทำความผิดฐานฟิชชิ่งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และฉบับที่2 พ.ศ.2560 โดยเริ่มศึกษาจากการศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้องกับการก่ออาชญากรรมประเภทการฟิชชิ่ง และโครงสร้างความผิดทางอาญาที่เกี่ยวข้องกับการก่ออาชญากรรมประเภทการฟิชชิ่งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และฉบับที่2 พ.ศ.2560 ซึ่งรวมไปถึงมาตรการทางกฎหมายของต่างประเทศที่เกี่ยวข้องกับการก่ออาชญากรรมประเภทการฟิชชิ่งมาพิจารณาประกอบจนนำมาสู่ข้อสรุปในบทนี้ ดังนี้

5.1 บทสรุป

ในสังคมปัจจุบันที่ถือได้ว่าเป็นยุคของเทคโนโลยีสารสนเทศและการอย่างเต็มตัวเทคโนโลยีอย่างอินเทอร์เน็ตจึงเข้ามามีบทบาทในชีวิตประจำวันของคนส่วนใหญ่ในสังคมทั้งในการค้นหาข้อมูลติดต่อสื่อสารการและทำธุรกรรมทางการเงิน เนื่องจากมีความสะดวกรวดเร็วในการใช้งานอีกทั้งยังมีการพัฒนาอยู่ตลอดเวลาทำให้ทุกสิ่งในสังคมก็เกิดการพัฒนาและปรับตัวเพื่อให้ก้าวทันไปกับการพัฒนาทางเทคโนโลยีที่เป็นไปอย่างรวดเร็ว อย่างไรก็ดีการพัฒนาทางเทคโนโลยีไม่ได้ส่งผลเปลี่ยนแปลงแค่เฉพาะผู้คนในสังคมเพียงเท่านั้นแต่ยังรวมไปถึงผู้กระทำความผิดที่มีการพัฒนารูปแบบการกระทำความผิดเปลี่ยนไปตามความก้าวหน้าทางเทคโนโลยี ซึ่งหนึ่งในการพัฒนารูปแบบในการกระทำความผิด คือ การฟิชชิ่งเนื่องจากมีความสะดวกในการก่ออาชญากรรมและความเสี่ยงในการถูกจับกุมน้อยกว่าการก่ออาชญากรรมในรูปแบบอื่นด้วยเหตุนี้เองฟิชชิ่งจึงเป็นอาชญากรรมที่แพร่หลายในสังคมปัจจุบันที่มีทั้งการพัฒนาวิธีการและรูปแบบที่หลากหลายเพิ่มมากขึ้น ยากแก่การป้องกันและปราบปรามการ

ด้วยเหตุนี้เองทั่วโลกจึงให้ความสำคัญกับการป้องกันและปราบปรามการการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งกับการฟิชชิ่งที่ถือได้ว่าเป็นอาชญากรรมที่มีความร้ายแรงและก่อให้เกิดความเสียหายเป็นวงกล้าวในทุกภาคส่วนตั้งแต่ระดับบุคคลไปจนถึงรัฐบาลและเอกชน และอาจร้ายแรงได้ถึงขั้นทำให้มีผู้เสียชีวิตแม้จะไม่ใช้การกระทำในทางกายภาพก็ตาม อย่างไรก็ดีความเสียหายอันเกิดจากการกระทำความทางคอมพิวเตอร์นั้นไม่ได้จำกัดอยู่แค่เพียงประเทศใดประเทศหนึ่งแต่รวมไปถึงทุกประเทศทั่วโลก เนื่องจากระบบคอมพิวเตอร์นั้นมีโครงข่ายอินเทอร์ที่สามารถเชื่อมต่อกันได้ทั่วโลก ด้วยเหตุนี้เองการกระทำความอย่างการฟิชชิ่งจึงก่อให้เกิดผู้เสียหายเป็นจำนวนมากจากการกระทำความผิดเพียงครั้งเดียว ซึ่งทำให้มูลค่าความเสียหายที่เกิดจากการกระทำความผิดนั้นสูงขึ้นตามไปด้วย

เมื่อพิจารณาจากความเสียหายที่เกิดขึ้นเป็นจำนวนมากจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นจะเห็นได้ว่านาๆประเทศก็ต่างตระหนักถึงผลกระทบและความเสียหายอย่างร้ายแรงที่เกิดขึ้น

จากปัญหานี้ โดยได้กำหนดมาตรการและบทลงโทษทางกฎหมายต่างๆมาเพื่อใช้ป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับฟิชชิ่ง ดังนี้

ตารางที่ 5.1 ตารางเปรียบเทียบมาตรการทางกฎหมายเกี่ยวกับฟิชชิ่งของต่างประเทศ

มาตรการทางกฎหมายเกี่ยวกับฟิชชิ่ง	
ประเทศ	**ความผิดที่กฎหมายบัญญัติ**
สหพันธ์รัฐเยอรมนี	**StGB. §202a** ผู้ใดกระทำการโดยปราศจากอำนาจใช้วิธีการมิชอบด้วยกฎหมายเข้าถึงข้อมูลที่มีการกำหนดมาตรการป้องกันการเข้าถึงซึ่งมิได้มีไว้สำหรับตนเพื่อตนเองหรือผู้อื่น โดยเจตนา ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับ **StGB. §202b** ผู้ใดกระทำการโดยปราศจากอำนาจใช้วิธีการทางเทคนิคดักรับข้อมูลอันมิได้มีไว้เพื่อตน ซึ่งอยู่ในระหว่างการรับ-ส่งข้อมูลอันมิได้มีไว้เพื่อสาธารณะ หรือดักรับข้อมูลที่บันทึกในระบบประมวลผลข้อมูล โดยเจตนา ต้องระวางโทษจำคุกไม่เกินสองหรือปรับในกรณีที่ความผิดนั้นไม่ต้องรับโทษหนักกว่าตามบทบัญญัติอื่น **StGB. §202c** ผู้ใดกระทำการโดยปราศจากอำนาจกระทำการเตรียมการใช้วิธีการทางเทคนิคดักรับข้อมูลอันมิได้มีไว้เพื่อตน โดย ผลิต เพื่อตนเองหรือผู้อื่นจำหน่าย จัดหา เผยแพร่ หรือทำให้เข้าถึงซึ่งรหัสผ่านที่ใช้ในการเข้าถึงข้อมูลหรือซอฟแวร์ ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับ
สาธารณรัฐฝรั่งเศส	**Le code penal. Article 226-4-1.** ผู้ใดกระทำการรวบรวมข้อมูลส่วนบุคคลด้วยวิธีการฉ้อฉลอันมิชอบด้วยกฎหมาย. **Le code penal. Article 226-18.** ผู้ใดกระทำการโดยใช้ข้อมูลอย่างใดอย่างหนึ่งเพื่ออำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลซึ่งรวมไปถึงการใช้เครือข่ายสื่อสารออนไลน์เป็นเครื่องมือ อันมีวัตถุประสงค์เพื่อรบกวนความสงบของผู้อื่นหรือเพื่อให้ได้ไปซึ่งข้อมูลส่วนบุคคล **Le code penal. Article 313-1.** ผู้ใดแสดงตนเป็นบุคคลอื่นด้วยเจตนาหลอกลวงหรือทำให้สำคัญผิดในข้อเท็จจริง โดยใช้อุบาย ให้บุคคลอื่นส่งมอบทรัพย์ หรือทรัพย์สิน **Le code penal. Article 323-3.** ผู้ใด แนะนำข้อมูลสำหรับการเข้าถึงระบบประมวลผลอัตโนมัติ โดยมิชอบ

ตารางที่ 5.1 (ต่อ)

มาตรการทางกฎหมายเกี่ยวกับฟิชชิ่ง	
ประเทศ	**ความผิดที่กฎหมายบัญญัติ**
รัฐแคลิฟอร์เนีย	CA Bus & Prof Coad § 22948.2 ผู้ใดกระทำการโดยปราศจากความยินยอมหรืออำนาจจากผู้ประกอบธุรกิจ โดยใช้เว็บไซต์ จดหมายอิเล็กทรอนิกส์ หรือบริการอื่นๆบนอินเทอร์เน็ต เรียกร้อง ร้องขอ หรือชักจูง บุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล ด้วยการแอบอ้างเป็นผู้แทนทางธุรกิจ
รัฐยูท่า	UT Code § 13-04-201 ผู้ใดกระทำการโดยปราศจากความยินยอมหรืออำนาจจากผู้ประกอบธุรกิจและกระทำการด้วยวิธีการใดๆซึ่งรวมไปถึงการเปลี่ยนแปลงการตั้งค่าบนคอมพิวเตอร์หรืออุปกรณ์ที่ทำงานในลักษณะเดียวกันของบุคคลอื่นหรือใช้ซอฟแวร์เพื่อทำให้ผู้ใช้อินเทอร์เน็ตพบกับหน้าเว็บที่ได้มีการเตรียมไว้โดยปลอมแปลงและลอกเลียนเว็บเพจเพื่อ เรียกร้อง ร้องขอ หรือชักจูง บุคคลอื่นเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวบุคคล ด้วยการแสดงตนเป็นผู้แทนทางธุรกิจ
รัฐนิวยอร์ก	NY Gen Bus Law § 390-B ผู้ใดกระทำการโดยปราศจากความยินยอมหรืออำนาจจากผู้ประกอบธุรกิจหรือหน่วยงานภาครัฐโดหลอกลวงหรือทำให้สำคัญผิดว่าเป็นผู้แทนทางธุรกิจหรือหน่วยงานของรัฐผ่านเว็บเพจหรือส่งจดหมายอิเล็กทรอนิกส์หรือใช้วิธีการทางอิเล็กทรอนิกส์เพื่อทำให้ทราบถึงหรือร้องขอข้อมูลยืนยันตัวบุคคล
รัฐเทนเนสซี	Section Tenn Code § 47-18-2503 ผู้ใดกระทำการโดยมิชอบด้วยกฎหมายและปราศจากความยินยอมหรืออำนาจกระทำการ แสดงตนเป็นผู้แทนหรือบุคคลอื่นผ่านทางอินเทอร์เน็ต โดยปลอมแปลงและลอกเลียนเว็บเพจหรือเว็บไซต์หรือส่งจดหมายอิเล็กทรอนิกส์หรือใช้วิธีการทางอิเล็กทรอนิกส์ซึ่งรวมไปถึงการติดต่อสื่อสารในช่องทางอื่นเพื่อร้องขอหรือกระทำด้วยประการใดๆเพื่อให้ได้มาซึ่งข้อมูล หรือเอกสารส่วนบุคคล และใช้ข้อมูลส่วนบุคคลเช่นว่านี้เพื่อตนเองหรือผู้อื่นหรือเพื่อจำหน่ายหรือแจกจ่าย โดยฉ้อฉล

สำหรับในส่วนของประเทศไทยในยุคที่การก่ออาชญากรรมทางคอมพิวเตอร์ได้รับความนิยมกันอย่างแพร่หลายและมีแนวโนวในการขยายตัวที่รวดเร็วเนื่องจากการเข้ามามีบทบาทของเทคโนโลยีสารสนเทศอย่างอินเทอร์เน็ตที่เข้ามามีบทบาทในชีวิตประจำวันของคนส่วนใหญ่ในสังคมทั้งในการค้นหาข้อมูล,

ติดต่อสื่อสารการและทำธุรกรรมทางการเงิน เนื่องจากมีความสะดวกรวดเร็วในการใช้งานอีกทั้งยังมีการพัฒนาอยู่ตลอดเวลาทำให้ทุกสิ่งในสังคมก็เกิดการพัฒนาและปรับตัวเพื่อให้ก้าวทันไปกับการพัฒนาทางเทคโนโลยีที่เป็นไปอย่างรวดเร็ว อย่างไรก็ดีการพัฒนาทางเทคโนโลยีไม่ได้ส่งผลเปลี่ยนแปลงแค่เฉพาะผู้คนในสังคมเพียงเท่านั้นแต่ยังรวมไปถึงผู้กระทำความผิดที่มีการพัฒนารูปแบบการกระทำความผิดเปลี่ยนไปตามความก้าวหน้าทางเทคโนโลยีซึ่งหนึ่งในการพัฒนารูปแบบในการกระทำความผิดคือการ ฟิชชิ่งเนื่องจากมีความสะดวกในการก่ออาชญากรรมและความเสี่ยงในการถูกจับกุมน้อยกว่าการก่ออาชญากรรมในรูปแบบอื่นด้วยเหตุนี้เองฟิชชิ่งจึงเป็นอาชญากรรมที่แพร่หลายในสังคมปัจจุบันที่มีทั้งการพัฒนาวิธีการและรูปแบบที่หลากหลายเพิ่มมากขึ้นดังจะเห็นได้จากข่าวการพิชชิ่งในปัจจุบัน ตัวอย่างเช่น แม่ค้าขายข้าวเหนียวหมูปิ้งในตัวเมืองเชียงใหม่ถูก "แก๊งคอลเซ็นเตอร์" หลอกส่งข้อมูลมาให้กรอกจากนั้นได้ดูดเงินภายในบัญชีธนาคารที่ผูกไว้ในแอพพลิเคชั่นในมือถือไปจนเกลี้ยงบัญชี[211]

อนึ่ง จากกรณีที่ดังที่ได้กล่าวมาในข้างต้นถือได้ว่าเป็นหนึ่งในรูปแบบและวิธีการของการ ฟิชชิ่งซึ่งแสดงให้เป็นถึงข้อบ่งชี้ที่ว่าฟิชชิ่งนั้นสามารถกระทำได้ง่าย รวดเร็ว และยากต่อการถูกจับกุม อีกทั้งในการบังคับใช้กฎหมายที่เกี่ยวข้องกับการฟิชชิ่งในปัจจุบัน ยังคงมีความสับสนและไม่ชัดเจนในการบังคับใช้กฎหมายจึงทำให้ไม่สามารถนำกฎหมายมาปรับใช้กับการฟิชชิ่งได้อย่างมีประสิทธิภาพเท่าที่ควร ซึ่งโดยทั่วไปแล้วนั้นผู้ที่กระทำการฉ้อโกงหลอกลวงผู้อื่นเพื่อให้ได้มาซึ่งทรัพย์สิน ผู้ที่กระทำนั้นจะต้องได้รับโทษทางอาญาตามแต่ลักษณะแห่งการกระทำที่ได้บัญญัติให้เป็นความผิดในมาตรานั้นๆ เช่น หากเป็นกรณีการ ฉ้อโกงก็จะถือได้ว่าเป็นความผิดตามประมวลกฎหมายอาญาลักษณะ12 หมวด3 มาตรา 341[212] หรือ หากเป็นการหลอกลวงเพื่อให้ได้มาซึ่งทรัพย์สินก็จะเป็นความผิดตามประมวลกฎหมายอาญา ลักษณะ12 หมวด1 มาตรา334[213] แต่หากเป็นกรณีที่เป็นการฟิชชิ่งที่เป็นทั้งการปลอมแปลงและฉ้อโกง หรือในบางกรณีอาจมีการหลอกลวง โดยจะกระทำผ่านโปรแกรมที่ให้บริการในรูปแบบต่างๆ, ผ่านระบบคอมพิวเตอร์หรือเครือข่ายอิเทอร์เน็ตซึ่งการกระทำความผิดประเภทนี้จะมีลักษณะที่พิเศษแตกต่างไปจากการกระทำความผิดทางกายภายทั่วไปในฐานความผิดอื่นๆ กล่าวคือการฉ้อโกงหลอกลวงผ่านระบบคอมพิวเตอร์หรือการฟิชชิ่ง จะทำให้ข้อมูลอันเป็นเท็จที่ฟิชเชอร์ หรือผู้กระทำผิดนั้นสร้างขึ้นมาถูกส่งไปยังเหยื่อได้รวดเร็วขึ้นและสามารถส่งได้ทีละมากๆจนนำไปสู่การเกิดความเสียหายหายต่อประชาชนหรือแม้แต่ตัวภาครัฐเอง อีกทั้งในการควบคุมและกำหนดมาตรการป้องกันการกระทำความผิดทางคอมพิวเตอร์จำเป็นที่จะต้องใช้เทคนิคพิเศษในการแก้ปัญหาทางเทคนิคต่างๆที่เกิดขึ้นจากการกระทำความผิด ซึ่งเมื่อพิจารณาจากมาตรการทางกฎหมายของประเทศไทยที่สามารถนำมา

---

[211] Google (เชิงอรรถ 70).

[212] ประมวลกฎหมายอาญา มาตรา341 “ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

[213] ประมวลกฎหมายอาญา, มาตรา334 “ผู้ใดเอาทรัพย์ของผู้อื่น หรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วยไปโดยทุจริต ผู้นั้นกระทำความผิดฐานลักทรัพย์ ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินหกหมื่นบาท”

บังคับใช้ได้กับการ ฟิชชิ่ง คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยเฉพาะอย่างยิ่งในส่วนของมาตรา 14(1) ที่บัญญัติให้การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา เป็นความผิด อย่างไรก็ตามเมื่อพิจารณาจากองค์ประกอบความผิดของมาตรา 14(1) จะเห็นได้ว่ามาตราดังกล่าวนั้นมีจุดประสงค์มุ้งเน้นไปที่การเอาผิดกับบุคคลใดก็ตามที่นำเข้าข้อมูล ปลอม เท็จ บิดเบือน เข้าสู่ระบบ ซึ่งโดยสภาพแล้วข้อมูลดังกล่าวไม่ได้มีลักษณะในทางเทคนิคที่จะส่งผลกระทบต่อการประมวลผลของข้อมูลหรือระบบคอมพิวเตอร์ในลักษณะที่ทำให้การประมวลผลนั้นเป็นไปตามที่ต้องการหรือไปในทิศทางที่ผู้กระทำนั้นได้ประโยชน์จากการนำเข้าข้อมูล อย่างไรก็ดีเมื่อพิจารณาจากลักษณะของการฟิชชิ่งนั้นจะเห็นได้ว่า ฟิชชิ่งนั้นถือได้ว่าไปเป็นการกระทำความผิดในรูปแบบการฉ้อโกงทางคอมพิวเตอร์ ที่ประกอบไปด้วยขั้นตอนและการกระทำที่หลากหลายวิธี ซึ่งสามารถจำแนกประเภทของการกระทำได้เป็นสองกรณีดังนี้

กรณีที่หนึ่ง การฟิชชิ่ง โดยใช้วิธีการที่มุ้งเน้นไปที่การหลอกลวงบุคคล กล่าวคือเป็นการฟิชชิ่งที่มุ้งเน้นไปที่เนื้อหา (Phishing-related content) ที่มีจุดประสงค์มุ้งเน้นไปที่การหลอกลวงบุคคลหรือจงใจทำให้เข้าใจผิด อันเป็นวิธีการทางวิศวกรรมทางสังคม (Social engineering) อย่างหนึ่งเช่น การสร้างหน้าเว็บปลอมเพื่อลวงให้เหยื่อหลงเชื่อและกรอกข้อมูลส่วนบุคคลที่มีความสำคัญลงไป

กรณีที่สอง การฟิชชิ่ง โดยใช้วิธีการทางเทคนิคเพื่อมุ่งหลอกลวงระบบประมวลผลข้อมูลอัตโนมัติหรือโปรแกรมต่างๆ กล่าวคือ เป็นการฟิชชิ่งที่ไม่ได้เกี่ยวข้องกับการนำเข้าข้อมูลเชิงเนื้อหาแต่ใช้วิธีการทางเทคนิคเพื่อให้บรรลุซึ่งเป้าหมายหรือเพื่อให้ได้มาซึ่งสิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่มิได้มีไว้เพื่อตนอันมีวัตถุประสงค์เช่นเดียวกันกับกรณีแรก คือ เพื่อให้ได้มาซึ่งข้อมูลของเหยื่อ เช่น การเปลี่ยนเส้นทางการเข้าถึงเว็บเพจหรือเว็บไซต์ทางอินเตอร์เน็ตของเหยื่อจากโดเมนหนึ่งไปยังอีกโดเมนหนึ่งที่เตรียมการไว้ โดยมิได้มีการหลอกลวงในด้านเนื้อหา

เมื่อพิจารณาจากกรณีทั้งสองดังที่ได้กล่าวมาในข้างต้นจะเห็นได้ว่าในกรณีแรกนั้นเป็นกรณีการนำเข้าสู่ระบบซึ่งข้อมูลที่ปลอมแปลง เท็จ บิดเบือน โดยมีเจตนาเพื่อหลอกลวงบุคคลซึ่งอยู่ในขอบเขตของมาตรา 14(1) แต่ไม่ว่าอย่างไรก็ตามเมื่อพิจารณาจากกรณีที่สองจะเห็นไปได้ว่ากรณีที่สองนั้นไม่ได้มุ้งเน้นไปที่การหลอกลวงบุคคลหรือทำให้เกิดความเข้าใจผิด และวิธีการที่ใช้ในการฟิชชิ่งนั้นก็ไม่ได้เกี่ยวข้องกับการนำเข้าข้อมูล ปลอม เท็จ บิดเบือน เข้าสู่ระบบคอมพิวเตอร์ตามมาตรา 14(1) กรณีนี้จึงไม่อาจที่จะนำมาตรา 14(1) มาบังคับใช้ได้ แต่ไม่ว่าอย่างไรก็ตามนอกจากกรณีทั้งสองดังที่ได้กล่าไปในข้างต้นนั้นยังมีปัญหาในเรื่องความไม่ครอบคลุมของฐานความผิด และความคลุมเครือของบทบัญญัติจนทำให้ไม่สามารถนำไปปรับเพื่อใช้บังคับกับการกระทำความผิดที่เกี่ยวข้องกับการฟิชชิ่งได้อย่างมีประสิทธิภาพเท่าที่ควรในหลายประการ ดังนี้

ประการแรก ปัญหาความไม่ครอบคลุมของฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และแก้ไขฉบับที่2 พ.ศ.2560 ในส่วนของ มาตรา14(1) บัญญัติไว้ว่า “ ผู้ใดโดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่

ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา ” ซึ่งเมื่อพิจารณาจากลักษณะในการกระทำความผิดของฟิชเชอร์ในการฟิชชิ่งจะพบว่าการกระทำฟิชชิ่งนั้นมักจะอาศัยรูปแบบการแอบอ้าง หรือปลอมแปลงเว็บไซต์เพื่อทำให้ผู้เสียหายเข้าใจผิดและหลงเชื่อว่าเป็นเว็บไซต์ที่แท้จริง อย่างไรก็ดีข้อมูลที่ฟิชเชอร์ใช้ในการแอบอ้างหรือปลอมแปลงเว็บไซต์ในบางกรณีนั้นไม่ถือว่าเป็นข้อมูลคอมพิวเตอร์อันเป็นเท็จเหตุเพราะข้อมูลที่ฟิชเชอร์ใช้ในการนำมาหลอกลวงเหลือนั้นเป็นข้อมูลจริงของตัวผู้เสียหายเองมิใช่การสร้างข้อมูลขึ้นมาใหม่แต่เป็นการนำข้อมูลของผู้เสียหายบางส่วนมาหลอกลวงผู้เสียหายเพื่อให้ได้ไปซึ่งข้อมูลส่วนบุคคลที่ใช้ในการยืนยันตัวตนของผู้เสียหายเพื่อนำไปใช้ในการหาประโยชน์ในทางทรัพย์สินต่อไป ซึ่งในส่วนนี้เองในบทบัญญัติทางกฎหมายของประเทศไทยนั้นยังมิได้มีการบัญญัติให้การขโมยข้อมูลส่วนบุคคลเป็นความผิดไว้เป็นการเฉพาะ แม้ว่าในปัจจุบันจะได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ไว้เพื่อเป็นหลักเกณฑ์ในการกำหนดกลไก หรือมาตรการควบคุมกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นเพียงหลักการทั่วไปและให้คำนิยามข้อมูลส่วนบุคคลไว้เพียงกว้างๆ ในมาตรา 6[214] ทำให้เมื่อเกิดการกระทำความผิดในลักษณะของการโจรกรรมข้อมูลส่วนบุคคล หรือนำข้อมูลส่วนบุคคลไปใช้ในทางที่มิชอบจะต้องนำกฎหมายอื่นที่มีความเกี่ยวข้องหรือใกล้เคียงมาใช้บังคับเป็นกรณีๆ ไป ซึ่งส่งผลกระทบต่อการบังคับใช้กฎหมายอันก่อให้เกิดช่องว่างทางกฎหมายและความสับสนในการบังคับใช้กฎหมายเมื่อเกิดกรณีการกระทำความผิดในลักษณะดังกล่าว

ประการที่สอง ปัญหาทางกฎหมายเกี่ยวกับข้อจำกัดในการบังคับใช้กฎหมายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560 มาตรา 14(1) ที่มีองค์ประกอบของการกระทำผิดที่จำกัดแค่เพียงแค่เฉพาะการ “นำเข้าสู่ระบบ” ที่ไม่ครอบคลุมการกระทำความผิดทางเทคนิคในลักษณะอื่น อาทิ การแก้ไขหรือลบข้อมูล การแทรกแซงการรับส่งข้อมูล ฯลฯ ซึ่งวิธีการทางเทคนิคเหล่านี้ล้วนเป็นวิธีการที่มิใช่การนำเข้าข้อมูลสู่ระบบทั้งสิ้น และด้วยเหตุเช่นนี้เองจึงทำให้องค์ประกอบของฐานความผิดดังที่ได้กล่าวมาในข้างต้นนั้นมีข้อจำกัดในแง้ของเนื้อหาที่จำกัดอยู่เพียงแค่การนำเข้าสู่ระบบซึ่งข้อมูลอันเป็นเท็จ ปลอม หรือบิดเบือน ซึ่งถูกจำกัดอยู่แค่ในกรอบความเข้าใจของมนุษย์เพียงเท่านั้น อีกทั้งยังมีขอบเขตการตีความที่กว้างจนครอบคลุมไปถึงพฤติกรรมอื่นที่มิได้มีความเกี่ยวข้องกับการก่ออาชญากรรมคอมพิวเตอร์ อาทิ การถูกนำไปตีความเพื่อบังคับใช้กับการหมิ่นประมาท(ก่อนการแก้ไข ฉบับที่2 ปี2560) อันมิใช้วัตถุประสงค์ของของฐานความผิดนี้ ซึ่งในส่วนนี้กฎหมายไทยควรที่จะมีการพิจารณาปรับปรุงแก้ไขบทบัญญัติให้มีครอบคลุมกับการกระทำทางเทคนิคให้มีความชัดเจนและครอบคลุมมากยิ่งขึ้น

ประการที่สาม ปัญหาทางกฎหมายเกี่ยวกับการนำเข้าสู่ระบบซึ่งข้อมูลปลอม หรือเท็จ หรือบิดเบือน ซึ่งได้มีการบัญญัติความรับผิดและบทกำหนดโทษไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่2 พ.ศ.2560 มาตรา 14(1) แต่มิได้มีการบัญญัตินิยามคำว่า “ข้อมูลปลอม หรือ

---

[214] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 6 “ข้อมูลส่วนบุคคล หมายความว่าข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”

เท็จ หรือบิดเบือน” ไว้ว่ามีความหมายในลักษณะเช่นไรจึงทำให้มีปัญหาในการตีความและเป็นเรื่องที่ยากที่จะพิจารณาว่าข้อมูลที่นำเข้านั้นเป็นข้อมูล ปลอม เท็จ บิดเบือน หรือไม่ ซึ่งเมื่อพิจารณาการกระทำความผิดฐานฟิชชิ่งตามกฎหมายต่างประเทศแล้วนั้นในส่วนของ กฎหมายของรัฐเทนเนสซี ที่มีหลักการที่ค่อนข้างคล้ายคลึงกับกฎหมายรัฐนิวยอร์ก รัฐแคลิฟอร์เนีย และรัฐยูทาห์ คือการกระทำโดยมิชอบด้วยกฎหมายของบุคคลด้วยวิธีการหลอกลวงหรือทำให้เข้าใจผิดในการแสดงตนเป็นบุคคลอื่นโดยปราศจากอำนาจหรือได้รับความยินยอมจากบุคคลดังกล่าวด้วยวิธีการส่งจดหมายอิเล็กทรอนิกส์หรือวิธีการทางอิเล็กทรอนิกส์อื่นๆ ซึ่งรวมไปถึงการติดต่อสื่อสารแบบไร้สาย เพื่อเรียกร้อง ร้องขอ กระทำการใดๆอันเป็นการชักจูงเพื่อให้ผู้อื่นเปิดเผยข้อมูลการยืนยันตัวตนหรือเอกสารส่วนบุคคลแต่ไม่ว่าอย่างไรก็ดีในส่วนของกฎหมายรัฐยูทาห์ ได้มีการเพิ่มบทบัญญัติในเรื่องการกระทำเพื่อให้ได้ไปซึ่งทรัพย์สิน เพราะเนื่องจากการกระทำฟิชชิ่งนั้นในบางกรณีอาจจะได้ทรัพย์สินไปตั้งแต่ขั้นตอนแรกๆ ทั้งนี้เมื่อพิจารณาจากกฎหมายของรัฐเทนเนสซีทำให้ทราบได้ว่าในกฎหมายของรัฐเทนเนสซีนั้นมีการบัญญัติทางเนื้อหาในบทบัญญัติที่ละเอียดกว่าของหลายๆดังที่กล่าวมาในข้างต้น กล่าวคือในบทบัญญัติกฎหมายของรัฐเทนเนสซีในส่วนของฟิชชิ่งนั้นได้มีการบัญญัติให้การกระทำฟิชชิ่งนั้นเป็นความผิดตั้งแต่ขั้นตอนการตระเตรียมการไปจนถึงกระทำการในทุกขั้นตอนซึ่งรวมไปถึงการฟาร์มมิ่ง ตลอดจนการการกำหนดให้การพยามกระทำความผิดนั้นถือเป็นความผิดอีกด้วย

ประการที่สี่ ปัญหาการกำหนดค่าเสียหายและบทลงโทษเกี่ยวกับการกระทำความผิดเกี่ยวกับฟิชชิ่งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และแก้ไขฉบับที่2 พ.ศ.2560 มาตรา 14(1) บัญญัติไว้ว่า “ผู้ใดกระทำความผิดตามที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุก 5 ปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา” เมื่อพิจารณาจากบทบัญญัติในข้างต้นจะเห็นได้ว่าแม้จะมีการกำหนดบทลงโทษทั้งจำคุกและปรับซึ่งถือมาตรการลงโทษทางอาญาอย่างหนึ่งที่ถูกนำมาใช้เป็นเครื่องมือในการป้องกันและปราบปรามการกระทำความผิดฐานฟิชชิ่ง แต่ไม่ว่าอย่างไรก็ตามแม้จะมีการกำหนดอัตราโทษสำหรับการกระทำความผิดในรูปแบบการฟิชชิ่งไว้ก็ตาม แต่อัตราโทษสำหรับการกระทำความผิดนั้นค่อนข้างที่จะอยู่ในระดับที่ต่ำเมื่อเทียบกับผลประโยชน์ที่ผู้กระทำความผิดนั้นจะได้รับเมื่อพิจารณาถึงผลกระทบที่เกิดขึ้นจากการกระทำความผิดฐานฟิชชิ่งจะทราบได้ว่าผลกระทบที่เกิดขึ้นจากการฟิชชิ่งไม่เพียงแค่ส่งผลไปยังตัวผู้เสียหายโดยตรงแต่ยังรวมไปถึงผู้ประกอบการธุรกิจและผู้ที่ถูกแอบอ้างและภาพรวมทางเศรฐกิจในวงกว้าง อีกทั้งเมื่อพิจารณาถึงลักษณะคดีของการกระทำความผิดฐานฟิชชิ่งที่มักเป็นคดีที่ไม่ค่อยมีพยานรู้เห็นในการกระทำและการที่จะหาตัวฟิชเชอร์นั้นก็เป็นเรื่องที่ค่อนข้างจะมีความยุ้งยากเป็นอย่างยิ่งด้วยข้อจำกัดทางด้านกฎหมายและเทคโนโลยีที่ทำให้โอกาสในการจับกุมตัวผู้กระทำความผิดมาลงโทษนั้นอยู่ในระดับที่ต่ำทำให้โอกาสที่ฟิชเชอร์จะกระทำสำเร็จนั้นมีอยู่ค่อนข้างสูงส่งผลให้โอกาสที่ฟิชเชอร์จะได้รับผลประโยชน์จากการกระทำความผิดก็ย่อมสูงขึ้นด้วยเช่นกันด้วยเหตุนี้เองจึงทำให้ต้นทุนในการกระทำควาผิดของฟิชเชอร์นั้นต่ำมากเมื่อเทียบกับมาตรการลงโทษทาง

อาญาที่จะได้รับหากถูกจับได้ และโดยเฉพาะอย่างยิ่งในการแก้ไขเพิ่มเติม มาตรา 14 ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่2 พ.ศ.2560 ที่เป็นการลดบทกำหนดโทษและค่าปรับซึ่งต่ำอยู่แล้วให้ต่ำไปกว่าเดิม อีกทั้งเมื่อพิจารณาจากถึงบทลงโทษในทางแพ่งบทลงโทษในทางแพ่งที่เป็นไปตามดุลพินิจของศาลในการที่จะตักสินคดีซึ่งผู้เสียหายนั้นมีภาระที่จะต้องนำพิสูจน์ต่อศาลเพื่อให้ศาลนั้นทราบถึงความเสียหายที่แท้จริงที่เกิดแก่ผู้เสียหายว่ามีจำนวนเท่าใด ซึ่งรวมไปถึงการที่กฎหมายนั้นไม่มีการกำหนดหลักเกณฑ์ในการเรียกร้องค่าเสียหายเพิ่มเติมจากค่าเสียหายที่แท้จริงอันเป็นค่าเสียหายในเชิงลงโทษ ซึ่งในส่วนนี้เองเมื่อพิจารณาถึงกฎหมายต่างประเทศในส่วนของรัฐนิวยอร์ก รัฐแคลิฟอร์เนีย รัฐเทนเนสซี และรัฐยูทาห์ ที่ได้มีการกำหนดหลักเกณฑ์เกี่ยวสิทธิในการเรียกร้องค่าเสียหายที่ให้อำนาจแก่ผู้เสียหายในการเรียกร้องค่าเสียหายได้มากเกินกว่าค่าเสียหายที่แท้จริงได้แต่ไม่เกินกว่าจำนวนที่กฎหมายกำหนดไว้ซึ่งค่าเสียหายเช่นนี้เรียกว่าค่าเสียหายเชิงลงโทษ ซึ่งในส่วนนี้เองกฎหมายไทยนั้นควรทีจะมีการพิจารณากำหนดหลักเกณฑ์ในการเรียกร้องค่าเสียหายเพิ่มเติมให้แก่ผู้เสียหายอันเป็นค่าเสียหายเชิงลงโทษแก้ตัวผู้กระทำความผิด ซึ่งรวมไปถึงการกำหนดเพิ่มโทษปรับในทางอาญาให้มีความสัมพันธ์สอดคล้องกับความเสียหายและต้นทุนในการกระทำความผิดของผู้กระทำความผิดเพื่อเป็นการทำให้ผู้กระทำความผิดได้รับความเสียหายทางด้านเศรฐกิจจากการถูกบังคับเอาทรัพย์สินซึ่งจะส่งผลทำให้ผู้กระทำความผิดไม่กลับมากระทำความผิดซ้ำ อีกทั้งการเพิ่มโทษปรับนั้นไม่เป็นการก่อให้เกิดผลกระทบในทางลบที่มากจนเกินไปแก่ผู้กระทำความผิดเมื่อเทียบกับโทษจำคุก

ประการสุดท้าย ปัญหาเรื่องสิทธิในการดำเนินคดีของผู้เสียหายที่ได้รับความเสียหายและผลกระทบจากการฟิชชิ่งที่ยังครอบคลุมไปไม่ถึงเจ้าของเว็บไซต์ หรือเว็บเพจ หรือบุคคลที่ได้รับผลกระทบจากการฟิชชิ่ง ซึ่งหากพิจารณาจารณาจากลักษณะของการกระทำความผิดจะเห็นได้ว่าการฟิชชิ่งนั้นเป็นความผิดที่กระทบต่อภาพรวมของสังคมเป็นอย่างมากเหตุเพราะการก่ออาชญากรรมประเภทนี้สามารถเกิดขึ้นกับใครก็ได้ในสังคม ซึ่งในส่วนนี้เองกฎหมายไทยควรที่จะมีการพิจารณากำหนดให้ผู้เสียหายในคดีที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับฟิชชิ่ง มีความหมายรวมไปถึงสิทธิในการดำเนินคดีที่ครอบคลุมไปถึงเจ้าของเว็บไซต์ หรือเว็บเพจ หรือบุคคลที่ได้รับผลกระทบจากการฟิชชิ่ง เพราะถือว่าเป็นผู้ที่ได้รับความเสียหายจากการฟิชชิ่งด้วยเช่นกัน

5.2 ข้อเสนอแนะ

จากประเด็นปัญหาดังที่ได้กล่าวมาในหัวข้อก่อนนี้ที่ถือได้ว่าเป็นปัญหาที่ทำให้การบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และฉบับที่2 พ.ศ.2560 กับกรณีการฟิชชิ่งนั้นเป็นไปอย่างไม่มีประสิทธิภาพเท่าที่ควรจนนำไปสู่การที่ไม่สามารถนำบทบัญญัติทางกฎหมายมาปรับใช้กับการฟิชชิ่งได้ ด้วยเหตุนี้เองผู้เขียนจึงมีข้อเสนอแนะว่าควรมีการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ให้มีความชัดเจน เข้าใจง่าย สอดคล้องกับหลักกฎหมายสากลสามารถนำมาปรับใช้กับการกระทำความผิดได้อย่างครอบคลุมในทุกขั้นตอนที่เกี่ยวข้องกับการฟิชชิ่งเพื่อเป็นการป้องกันมิให้บทบัญญัติถูกนำไปใช้ผิดวัตถุประสงค์เหมือนอย่างที่ผ่านมา ซึ่งในส่วนนี้เองผู้เขียนมีความเห็น

ว่าควรที่จะนำกฎหมายของรัฐเทนเนสซีมาเป็นแนวทางในการปรับปรุงแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ให้มีความสอดคล้องและเหมาะสมกับขั้นตอนในการกระทำความผิดเกี่ยวกับฟิชชิ่ง ซึ่งรวมไปถึงการกำหนดโทษในทางอาญาให้มีความเหมาะสมกับฐานความผิดฟิชชิ่งมากยิ่งขึ้น และเพื่อเป็นการบรรเทาความเสียหายที่เกิดขึ้นจากการฟิชชิ่งจึงเห็นควรให้นำหลักเกณฑ์ในเรื่องค่าปรับตามมาตรา 76[215] แห่งพระราชบัญญัติลิขสิทธิ์ พ.ศ.2537 ที่กำหนดให้การชำระค่าปรับตามคำพิพากษาต้องจ่ายให้แก่เจ้าของลิขสิทธิ์เป็นจำนวนกึ่งหนึ่งของจำนวนค่าปรับที่ผู้กระทำความผิดนั้นต้องชำระตามคำพิพากษามาปรับใช้ด้วย แต่ทั้งนี้ไม่ถือว่าการได้รับส่วนแบ่งค่าปรับของผู้เสียหายนั้นเป็นการตัดสิทธิในการฟ้องร้องค่าเสียหายในทางแพ่งของเจ้าของลิขสิทธิ์

อนึ่ง ในส่วนของการกำหนดบทบัญญัติโทษของการฟิชชิ่งนั้นผู้เขียนเห็นว่าควรที่จะมีการปรับปรุงแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ให้มีความเหมาะสมกับยุคสมัยและครอบคลุมในทุกลักษณะของการกระทำความผิดที่เกี่ยวข้องกับการฟิชชิ่งด้วยเหตุนี้เองผู้เขียนจึงขอเสนอแนวทางในการปรับปรุงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และฉบับที่2 พ.ศ.2560 โดยเสนอให้ปรับปรุงแก้ไขบทบัญญัติในมาตรา 14(1) เพื่อให้บทบัญญัติมีความครอบคลุมและชัดเจนมากยิ่งขึ้น ซึ่งรวมไปถึงการเพิ่มเติมบทบัญญัติสำหรับการ ฟิชชิ่งเป็นมาตรา14/1 ดังนี้

มาตรา 14(1) โดยทุจริตหรือหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันส่งผลต่อความถูกต้องแท้จริงของข้อมูลคอมพิวเตอร์ เพื่อแก้ไข ระงับยับยั้ง หรือเพื่อให้การประมวลผลข้อมูลนั้นแสดงผลไปในทางที่กำหนด เพื่อให้ได้ไปซึ่งประโยชน์ในทางทรัพย์สินโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

มาตรา 14/1 ผู้ใดโดยเจตนาทุจริตหรือหลอกลวง แสดงตนเป็นบุคคลอื่นหรือผู้แทนบุคคลกระทำการโดยปราศอำนาจหรือความยินยอมผ่านช่องทางอินเทอร์เน็ตด้วยการส่งจดหมายอิเล็กทรอนิกส์หรือใช้วิธีการทางอิเล็กทรอนิกส์ซึ่งรวมไปถึงการติดต่อสื่อสารในช่องทางอื่นๆ เพื่อร้องขอ เรียกร้อง หรือกระทำด้วยประการใดๆ อันเป็นการชักจูงเพื่อให้ได้ไปซึ่งเอกสารหรือข้อมูลส่วนบุคคล ต้องระวางโทษจำคุกไม่เกินสิบปี หรือปรับเป็นจำนวนสองเท่าของผลประโยชน์ที่ได้รับหรือควรจะได้รับจากการกระทำอันฝ่าฝืนต่อบทบัญญัติ ทั้งนี้จำนวนค่าปรับดังกล่าวต้องไม่น้อยกว่าหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

การใช้เอกสารหรือข้อมูลส่วนบุคคลที่ได้มาจากการฝ่าฝืนบทบัญญัติตามวรรคหนึ่งโดยมีเจตนาทุจริตหรือหลอกลวงเพื่อตนเองหรือผู้อื่น เพื่อให้ได้ไปซึ่งประโยชน์ในทางทรัพย์สิน ต้องระวางโทษจำคุกไม่เกินสิบปี หรือปรับเป็นจำนวนสองเท่าของผลประโยชน์ที่ได้รับหรือควรจะได้รับจากการกระทำอันฝ่าฝืนต่อบทบัญญัติ ทั้งนี้จำนวนค่าปรับดังกล่าวต้องไม่น้อยกว่าสองแสนบาทหรือ ทั้งจำทั้งปรับ

---

[215] พระราชบัญญัติลิขสิทธิ์ พ.ศ.2537 มาตรา 76 “ค่าปรับที่ได้ชำระตามคำพิพากษา ให้จ่ายแก่เจ้าของลิขสิทธิ์ หรือสิทธิของนักแสดงเป็นจำนวนกึ่งหนึ่ง แต่ทั้งนี้ไม่เป็นการกระทบกระเทือนถึงสิทธิของ เจ้าของลิขสิทธิ์หรือสิทธิของนักแสดงที่จะฟ้องเรียกค่าเสียหายในทางแพ่งสำหรับส่วนที่เกิน จำนวนเงินค่าปรับที่เจ้าของลิขสิทธิ์หรือสิทธิของนักแสดงได้รับแล้วนั้น”

ผู้เสียหายตามวรรคหนึ่งมีความหมายรวมไปถึงบุคคลผู้ซึ่งได้รับผลกระทบจากการกระทำอันฝ่าฝืนต่อบทบัญญัติ และความผิดดังกล่าวให้ถือว่าเป็นอาญาแผ่นดิน

ค่าปรับที่ได้รับชำระแล้วตามคำพิพากษาให้จ่ายให้กับผู้ที่ได้รับความเสียหายเป็นจำนวนกึ่งหนึ่ง ทั้งนี้ไม่ถือว่าเป็นการตัดสิทธิในการดำเนินคดีทางแพ่งของผู้เสียหายที่จะเรียกร้องค่าเสียหายในส่วนที่เกินออกจากค่าปรับที่ได้รับไปแล้ว

อนึ่ง นอกจากการแก้ไขปรับปรุงมาตรา 14 และเพิ่มบทบัญญัติเป็นมาตรา 14/1 แล้วผู้เขียนยังเห็นควรให้เพิ่มเงื่อนไขในเรื่องการกำหนดค่าเสียหายเชิงลงโทษ (Punitive Damage) มาบังคับใช้กับกรณีการฟิชชิ่งที่เกี่ยวข้องกับการฉ้อโกงประชาชน เพื่อเป็นการป้องปรามการกระทำความผิดที่อาจเกิดขึ้นได้ในอนาคต [216] อีกทั้งโดยลักษณะของค่าเสียหายเชิงลงโทษถือเป็นสภาพบังคับอย่างอื่นนอกเหนือจากโทษทางอาญา จึงสามารถนำมาบังคับใช้ได้กับกรณีการฟิชชิ่งโดยไม่ก่อให้เกิดปัญหากฎหมายอาญาเฟ้อ

เมื่อพิจารณาถึงลักษณะการฟิชชิ่งนั้นจะเห็นได้ว่าเป็นหนึ่งในรูปแบบอาชญากรรมที่สามารถกระทำได้ง่ายเมื่อเทียบกับการก่ออาชญากรรมทางคอมพิวเตอร์ในรูปแบบอื่น ทั้งยังสะดวก รวดเร็ว และมีอัตราในการถูกจับกุมที่ต่ำเป็นอย่างมาก ซึ่งในบางกรณีก็อาจมีผู้กระทำผิดหรือฟิชเชอร์หลายคนร่วมกันในการกระทำความผิดโดยการแบ่งหน้าที่กันในการกระทำความผิด ก่อให้เกิดปัญหาในการนำตัวผู้กระทำความผิดมาลงโทษเพราะเนื่องจากการฟิชชิ่งนั้นเป็นการกระทำผ่านระบบเครื่องข่ายสาระสนเทศในช่องทางต่างๆ ซึ่งรวมไปถึงช่องทางสื่อสารไร้สายทำให้ผู้กระทำความผิดนั้นไม่มีความจำเป็นที่จะต้องอยู่ร่วมกันทำให้ในการจับกุมแต่ละครั้งไม่สามารถจับกุมผู้กระทำความผิดได้ทั้งหมด ด้วยเหตุนี้เองผู้เขียนจึงขอเสนอให้มีการปรับผู้กระทำความผิดเพิ่มเติมจากค่าปรับทางอาญาเป็นค่าปรับในเชิงลงโทษแก่ผู้กระทำความผิด โดยค่าปรับเพิ่มเติมนั้นอาจนำมาแบ่งให้แก่ผู้ที่ได้รับผลกระทบจากการกระทำความผิดซึ่งมิใช่ผู้เสียหายโดยตรงเพื่อเป็นการบรรเทาผลกระทบจากความเสียหายที่เกิดขึ้นจากการกระทำความผิดฐานฟิชชิ่ง และนอกจากการเพิ่มอัตราค่าปรับและโทษซึ่งถือเป็นการเพิ่มต้นทุนให้กับฟิชเชอร์แล้วนั้น การลดโอกาสหรือความน่าจะเป็นในการฟิชชิ่งก็เป็นสิ่งจำเป็นที่จะต้องกระทำควบคู่กันไปกับการบังคับใช้มาตรการทางกฎหมายกับการฟิชชิ่ง โดยการใช้เครื่องมือทางกฎหมายในเชิงปกครองโดยกำหนดให้ทุกภาคส่วนที่มีความเกี่ยวข้องกับการป้องกันและปราบปราบการกระทำความผิดที่เกี่ยวข้องกับการฟิชชิ่งเข้ามามีส่วนร่วมในการบูรณาการความร่วมมือระหว่างองค์กรทั้งภาครัฐและเอกชนในการกำหนดแนวทางป้องกันการกระทำความผิดเกี่ยวกับฟิชชิ่ง เช่น การบัญญัติระเบียบข้อบังคับหรือมาตรการทางกฎหมายที่เหมาะสมกำหนดให้ผู้ให้บริการอินเทอร์เน็ต จะต้องแจ้งเตือนไปยังผู้ใช้บริการถึงความเสี่ยงที่จะถูกโจรกรรมข้อมูลหากพบว่ามีความผิดปกติเกิดขึ้นในระบบของผู้รับบริการเนื่องจากผู้รับบริการบางรายรู้ไม่เท่าทันเทคโนโลยีซึ่งล้วนแล้วแต่เป็นการกระทำในทางเทคนิคทั้งสิ้น ซึ่งรวมไปถึงการแก้ไขกฎหมายสารบัญญัติอื่นๆ ที่เกี่ยวข้องกับการฟิชชิ่งอันเป็นการฉ้อโกงประชาชน เพื่อให้การบังคับใช้

---

[216] ปราโมทย์ เสริมศีลธรรม, *“หลักเกณฑ์ในการกำ หนดโทษทางอาญา” ภายใต้โครงการสนับสนุนสารสนเทศเพื่อการทำงานของสมาชิกรัฐสภา* (สถาบันพระปกเกล้า 2564) 79-80.

มาตราการทางกฎหมายในการป้องกันและปราบปรามฟิชชิ่งเกิดประสิทธิภาพสูงสุดในการป้องกันและปราบปราม

บรรณานุกรม

บรรณานุกรม

กรุงเทพธุรกิจ, ‘ทลายแก๊งแอบอ้างธนาคารดัง หลอกกู้เงินผ่านเฟซบุ๊ก ชาวบ้านตกเป็นเหยื่อ 200 ราย’ (กรุงเทพธุรกิจ, 30 สิงหาคม 2565) <https://www.bangkokbiznews.com/finance/1023775> สืบค้นเมื่อ13 มกราคม 2566.

กิติมา แก้วนะรา,‘หลักความได้สัดส่วนกับการกำหนดโทษทางอาญาที่เหมาะสมสำหรับผู้กระทำความผิดในคดียาเสพติดให้โทษ: ศึกษากรณีแอมเฟตามีน’(วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธุรกิจบัณฑิตย์).

กิตติยา พรหมจันทร์, ‘แนวคิดทางอาชญากรรมไซเบอร์กับเงินในบัญชีที่หายไป’ (Bangkokbiznews, 28 ตุลาคม 2564) <www.bangkokbiznews.com-/blogs/columnist/968445> สืบค้นเมื่อ 23 ธันวาคม 2565.

กุลธิดา อาธิเจริญสุข, ‘การบังคับใช้กฎหมายเกี่ยวกับฟิชชิ่ง’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต สถาบันบัณฑิตพัฒนบริหารศาสตร์ 2559).

_____, ‘การบังคับใช้กฎหมายเกี่ยวกับฟิชชิ่ง’ (2560) 2 วารสารรามคำแหง ฉบับนิติศาสตร์ 3 <https://so05.tci-thaijo.org/index.php/lawjournal/article/view/106759/84496> สืบค้นเมื่อ 9 มกราคม 2566.

เกียรติขจร วัจนะสวัสดิ์, *คำอธิบายกฎหมายอาญาภาค 1* (พิมพ์ครั้งที่ 10, สำนักพิมพ์พลสยามพริ้นติ้ง 2551).

คณาธิป ทองรวีวงศ์, *กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1* (สำนักพิมพ์นิติธรรม 2563).

_____, *กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 2 ฯลฯ* (สำนักพิมพ์นิติธรรม 2563).

คณิต ณ นคร, *กฎหมายอาญา ภาคทั่วไป* (พิมพ์ครั้งที่ 7, สำนักพิมพ์วิญญูชน 2563).

_____, *กฎหมายวิธีพิจารณาความอาญา เล่ม1* (พิมพ์ครั้งที่ 10, สำนักพิมพ์วิญญูชน 2564).

_____, *กฎหมายอาญาภาคความผิด* (พิมพ์ครั้งที่11, สำนักพิมพ์วิญญูชน 2559).

‘คลังเตือนภัยเว็บไซต์กระทรวงการคลังปลอม อย่าคลิก ระวังโดนหลอก’ (รัฐบาลไทย, 1 สิงหาคม 2565) <https://www.thaigov.go.th/news/contents/details/57489> สืบค้นเมื่อ 13 มกราคม 2566.

คัทราวดี สีทองเสือ, ‘คุณธรรมทางกฎหมายในกฎหมายอาญา: ศึกษาความผิดฐานรับของโจร’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยลัยธุรกิจบัณฑิต 2557).

จิราภพ ทวีสูงส่ง, ‘เรื่องใกล้ตัวกว่าที่คิด! “อาชญากรรมทางไซเบอร์” รู้จักไว้..ป้องกันภัยไม่ตกเป็นเหยื่อ’ (Thai PBS, 23 กุมภาพัน 2566) <https://www.thaipbs.or.th/now/content/68> สืบค้นเมื่อ 17 เมษายน 2566.

ณัฐสุดา อัคราวัฒนา, ‘การกำหนดความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาลัยธุรกิจบัณฑิตย์ 2560)

บรรณานุกรม (ต่อ)

โต๊ะข่าวไอที ดิจิทัล, ‘แคสเปอร์สกี้ โชว์สถิติ ‘ฟิชชิ่ง’ ภัยร้ายโจมตีองค์กรธุรกิจ’ (กรุงเทพธุรกิจ, 10 มิถุนายน 2565) <https://www.bangkokbiznews.com/tech/gadget/1045935> สืบค้นเมื่อ 5 มกราคม 2566.

_____, ‘เปิดโฉมหน้า‘ภัยคุกคามโลกออนไลน์’ปี66อาชญากรรมไซเบอร์‘ตามสั่ง’มาแน่!!’ (กรุงเทพธุรกิจ, 2 มกราคม 2566) <https://www.bangkokbiznews.com/tech/gadget/1045935> สืบค้นเมื่อ 4 มกราคม 2566.

ทีมข่าวอาชญากรรม, ‘รวบ 4 ผู้ต้องหาแก๊งคอลเซ็นเตอร์นำประสบการณ์จากกัมพูชา ตั้งกลุ่มสตาร์ทอัพตุ๋นเหยื่อในไทยร่วมลงทุน’ (ผู้จัดการออนไลน์, 5 ธันวาคม 2565) <https://mgronline.com/crime/detail/9650000115641> สืบค้นเมื่อ 11 มกราคม 2566.

ไทยรัฐออนไลน์, ‘ปอท. ชี้แนวโน้มอาชญากรรมไซเบอร์ ปี 65 มุ่งการแฮกข้อมูล ฉ้อโกงออนไลน์’ (ไทยรัฐออนไลน์, 5 มกราคม 2565) <https://www.thairath.co.th/news/crime/2279040> สืบค้นเมื่อ 23 ธันวาคม 2565.

_____, ‘แฮ็กโรงพยาบาล-รีดค่าไถ่ เรียกถึง 6.3 หมื่นล้านบาท’ (ไทยรัฐออนไลน์, 10 กันยายน 2563) <https://www.thairath.co.th/news/local/central/1926912> สืบค้นเมื่อ 9 มกราคม 2566.

ธนกร วงศ์นาง, ‘แฉเล่ห์ "แก๊งคอลเซ็นเตอร์" ดูดเงินจากมือถือ เหยื่อรายล่าสุดสูญกว่า 7 หมื่น’ (กรุงเทพธุรกิจ, 13 มกราคม 2566) <https://www.bangkokbiznews.com/news/news-update/1047873> สืบค้นเมื่อ13 มกราคม 2566.

ธนาคารแห่งประเทศไทย, ‘กลโกงธนาคารออนไลน์’ (ธนาคารแห่งประเทศไทย) <https://www.bot.or.th/th/satang-story/fraud/online-fraud.html> สืบค้นเมื่อ 9 มกราคม 2566.

ปกป้อง ศรีสนิท, *กฎหมายอาญาชั้นสูง* (พิมพ์ครั้งที่ 3, สำนักพิมพ์วิญญูชน 2563).

ปราโมทย์ เสริมศีลธรรม, *“หลักเกณฑ์ในการกำ หนดโทษทางอาญา” ภายใต้โครงการสนับสนุนสารสนเทศเพื่อการทำงานของสมาชิกรัฐสภา* (สถาบันพระปกเกล้า 2564).

ปัทมาภรณ์ กฤษณายุทธ,‘ความผิดฉ้อโกง: ศึกษากรณีการหลอกลวงทางอินเทอร์เน็ต’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยลัยธรรมศาสตร์ 2551).

ผาสุก เจริญเกียรติ, ‘Identity Theft อาชญากรรมใกล้ตัว’ (2552) 1 ดุลพาห.

พรเพรช วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550* (สถาบันพัฒนาข้าราชการฝ่ายตุลาการ ศาลยุติธรรม 2550).

บรรณานุกรม (ต่อ)

พิชยุตม์ คูณทอง, ‘การดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ต:ศึกษาเฉพาะกรณีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย 2550).

พิศวาท สุคนธพันธุ์, *รวมบทความทางวิชาการเนื่องในโอกาสครบรอบ 84 ปี ศาสตราจารย์ จิตติ ติงศภัทย์* (คณะนิติศาสตร์ โรงพิมพ์มหาวิทยาลัยธรรมศาสตร์ 2536).

เฟื่องฟ้า เป็นศิริ, *อาชญากรรมคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง* (สำนักพิมพ์วิญญูชน 2550).

มานิตย์ จุมปา, *ความรู้เบื้องต้นเกี่ยวกับกฎหมายสหรัฐอเมริกา* (พิมพ์ครั้งที่ 2, สำนักพิมพ์วิญญูชน 2553).

_____, *คำอธิบายกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์* (พิมครั้งที่ 2, สำนักพิมพ์วิญญูชน 2554).

ยอร์ช ปาดูซ์, *บันทึกของนายยอร์ช ปาดูซ์ (G.PADOUX) เกี่ยวกับการร่างกฎหมายลักษณะอาญา รศ.127* (สุรศักดิ์ ลิขสิทธิ์วัฒนกุล ผู้แปล, สำนักพิมพ์วิญญูชน 2546).

‘ร่างแก้ไขพ.ร.บ.คอมพิวเตอร์ฯ "ตั้งคณะกรรมการปิดเว็บแม้ไม่ผิดกฎหมาย’ (iLaw, 25 เมษายน 2559) <https://ilaw.or.th/node/4092?fbclid=IwAR383U_Pv0XVzGtc4uyZ7WvgiLkYoQx4oWIGGVgBdZLWDZMgYFL6UJ1n_4E> สืบค้นเมื่อ 5 พฤษภาคม 2566.

วันวิสาข์ ศรีกระจิบ, ‘ฝรั่งเศสกับการปฏิรูปกฎหมายไทยตั้งแต่ยุคอาณานิคมจนถึงยุคโลกาภิวัตน์ปัจจุบัน’ (วิทยานิพนธ์ อักษรศาสตรมหาบัณฑิต มหาวิทยลัยศิลปากร 2546).

วิชญ์ศุทธ์ เมาระพงษ์. ‘ปกป้องข้อมูลสำคัญจากจากการ Phishing’ (สิงหาคม 2552) 152 วารสาร TPA News ข่าว ส.ส.ท.

สาวตรี สุขศรี, *กฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์และอาชญากรรมทางไซเบอร์* (พิมพ์ครั้งที่ 2, สำนักพิมพ์เดือนตุลา 2563).

_____, ‘ประวัติศาสตร์ อาชญากรรมคอมพิวเตอร์’ (BioLawCom, 7 พฤษภาคม 2552) <http://www.biolawcom.de/article/118> สืบค้นเมื่อ 29 ธันวาคม 2565.

_____, ‘อาชญากรรมคอมพิวเตอร์/อินเทอร์เน็ตตามกฎหมายอาญาสหพันธ์สาธารณรัฐเยอรมนี’ (2556) 3 วารสารนิติศาสตร์, 507-509 <https://opacdb02.dpu.ac.th/cgi-bin/koha/opacdetail.pl?biblionumber=123953> สืบค้นเมื่อ 30 มีนาคม 2566.

_____, ‘อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญาวิทยา’ (2560) 2 วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

สุพิศ ประณีตพลกรัง, *หลักและทฤษฎีทางกฎหมายอาญา* (พิมพ์ครั้งที่ 2, สำนักพิมพ์นิติธรรม 2562).

บรรณานุกรม (ต่อ)

สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, ‘หลักความชอบด้วยกฎหมายในกฎหมายอาญา (PRINCIPLE DE LA LEGALITE CRIMINELLE)’ ใน *รวมบทความทางวิชาการเนื่องในโอกาสครบรอบ 84 ปี ศาสตราจารย์ จิตติ ติงศภัทย์* (คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2536).

สุรสิทธิ์ แสงวิโรจนพัฒน์, ‘หลักเกณฑ์การกำหนดความผิดทางอาญาตามกฎหมายต่างประเทศ’(เมษายน - มิถุนายน 2564) 2 บทบัณฑิตย์.

สำนักงานคณะกรรมการกฤษฎีกา, ‘ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ และบทวิเคราะห์กฎหมายไทยที่เกี่ยวข้อง’ (LAW FOR ASEAN, 12 มกราคม 2561) <https://lawforasean.-krisdika.go.th/Content/View?Id=349&Type=1> สืบค้นเมื่อ 16 เมษายน 2566.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ‘สถิติภัยคุกคามประจำปี 2565’ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์) <https://www.etda.or.th/th/Our-Service/thaicert/stat.aspx> สืบค้นเมื่อ 17 เมษายน 2566.

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, *แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์* (พิมพ์ครั้งที่ 2, สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ 2547).

สำนักพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, *แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์* (สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ 2546).

องอาจ เทียนหิรัญ, ‘อาชญากรรมคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญา สำหรับการกระทำต่อคอมพิวเตอร์’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2546).

อภิรัตน์ เพ็ชรศิริ, *ทฤษฎีอาญา ทฤษฎีโทษ และกระบวนการขั้นพื้นฐาน* (พิมพ์ครั้งที่ 4, สำนักพิมพ์วิญญูชน 2562).

อัจฉรียา ชูตินันทน์, *อาชญาวิทยาและทัณฑวิทยา* (พิมพ์ครั้งที่ 5, สำนักพิมพ์วิญญูชน 2566).

อุทัย อาทิเวช, *รวมบทความกฎหมายวิธีพิจารณาความอาญาฝรั่งเศส* (พิมพ์ครั้งที่ 2, สำนักพิมพ์ วี.เจ. พริ้นติ้ง 2557).

อุนิษา เลิศโตมรสกุล และอัณณพ ชูบำรุง, *อาชญากรรมและอาชญาวิทยา* (พิมพ์ครั้งที่ 2, สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย 2561).

เอก ศรีเชลียง, ‘อาชญากรรมอิเล็กทรอนิกส์:ศึกษาความสอดคล้องของข่าวอาชญากรรมทางคอมพิวเตอร์ที่ปรากฏในเว็บไซต์ข่าวบีบีซีกับ (ร่าง) พ.ร.บ. ว่าด้วยอาชญากรรมทางคอมพิวเตอร์ไทย’ (สารนิพนธ์ รัฐประศาสนศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย 2545).

บรรณานุกรม (ต่อ)

Aoo Studio, ‘Phishing (ฟิชชิ่ง) คืออะไร’ (Aoo Studio, 30 ธันวาคม 2564) <https://aoostudio.com/it-security/phishing> สืบค้นเมื่อ 23ธันวาคม 2565.

Bitdefender, ‘ฟิชชิ่ง (PHISHING) คืออะไร?’ (Bitdefender, 25 มีนาคม 2564) <https://www.bitdefender.co.th/post/phishing/> สืบค้นเมื่อ 24 ธันวาคม 2565.

CHANJIRA_YEE, ‘รวบยอด ปัญหา "การหลอกลวงยุคดิจิทัล" ปี 2564 คนไทยโดนโทรหลอกกว่า 6.4 ล้านครั้ง’ (Spring news, 30 พฤษภาคม 2565) <https://www.springnews.co.th/infographic/825198> สืบค้นเมื่อ 11 มกราคม 2566.

Cloud IT Network,’ฟิชชิ่ง (Phishing) คืออะไร?’ (Cloud IT Network, 29 พฤษภาคม 2564) <https://www.clouditnetwork.com/what-is-phishing/> สืบค้นเมื่อ 10 มกราคม 2566.

Digital Life, ‘เปิดภัยไซเบอร์ ปี 66 "แฮกเกอร์ตามสั่ง" มาแน่ ยิ่งผสมความสามารถ AI ยิ่งน่ากลัว’ (Digital Life, 2 มกราคม 2566) <https://www.springnews.co.th/digital-tech/technology/833899> สืบค้นเมื่อ 13 มกราคม 2566.

Drama addict, ‘มิจฉาชีพเข้าถึงบัญชีเขาแล้วโอนเงินออกหมดเลย’ (Facebook) <https://www.facebook.com/141108613290/posts/10161067543448291/?> สืบค้นเมื่อ 11 มกราคม 2566.

Google, ‘Googleรายงานเพื่อความโปร่งใส’ (Google) <https://transparencyreport.google.com/safebrowsing/overview> สืบค้นเมื่อ 10 มกราคม 2566.

Microsoft, ‘ปกป้องตัวคุณเองจากฟิชชิ่ง’ (Microsoft) <https://bit.ly/3i6RrFP> สืบค้นเมื่อ 3 ธันวาคม 2566.

Napaporn Panitchart, ‘อย่าหลงเชื่อ!! เว็บไซต์ ‘กรมสรรพากร’ ปลอม แนะ 3 วิธีสังเกต’ (The Bangkok Insight, 13สิงหาคม 2565) < https://www.thebangkokinsight.com/news/politics-general/politics/926871/> สืบค้นเมื่อ 14 มกราคม 2566.

PaPer-BOY, ‘ความหมาย และ อาชญากรคอมพิวเตอร์’ (Gotoknow, 6 กันยายน 2556) <https://www.goto-know.org/posts/372559> สืบค้นเมื่อ 29 ธันวาคม 2565.

PIMLAPAT PHANSUATHONG, ‘ฟิชชิ่ง (PHISHING) คืออะไร? รู้จักภัย 8 ประเภทบนโลกออนไลน์’ (Primal, 25 ตุลาคม 2566) <https://www.primal.co.th/th/seo/what-is-phishing/> สืบค้นเมื่อ 3 ธันวาคม 2566.

SEVENHORIZON, ‘Social Engineering (การโจมตีแบบวิศวกรรมสังคม)’ (sevenhorizon.wordpress, 3 ธันวาคม 2559) <https://bit.ly/3WGVuaT> สืบค้นเมื่อ 5 มกราคม 2566.

บรรณานุกรม (ต่อ)

Anticybercrimep, ‘What is Computer-related Forgery?’ (Anticybercrimep) <https://anticybercrimeph.word-press.com/2015/09/04/computer-related-forgery/> สืบค้นเมื่อ 2 มกราคม 2566.

‘AOL’ (AOL) <https://ฐ.co/kgs/bpifA3> สืบค้นเมื่อ 5 มกราคม 2566.

‘APEC Cyber Security Strategy (2002)’ (Regional Cooperation Council) <https://www.rcc.int/swp/docs/105/apec-cyber-security-strategy-2002> สืบค้นเมื่อ 16 เมษายน 2566.

Bettina Weisser, ‘Cyber Crime - The Information Society and Related Crimes. National Report on Germany’ (2013) Münster Journal of Mathematics.

Chayanin Kengsuwan, ‘Legal measures for phishing offense’ (Thesis Master of Laws Thammasat University 2012).

Claire Bernier, ‘Data Security and Cybercrime in France’ (Lexology) <https://www.lexology.com/library/detail.aspx?g=4db6c38c-be5e-4bce-9044-870c136099a2> สืบค้นเมื่อ 2 เมษายน 2566.

‘Combating fraud and counterfeiting of non-cash means of payment’ (EUR-Lex) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001F0413> สืบค้นเมื่อ 16 เมษายน 2566.

‘Commission of The European Communities’ (European Union) <http://europa.eu.int/SPO/eif/-InternetPoliciesite/Crime/CrimeCommEN.html> สืบค้นเมื่อ 29 ธันวาคม 2565.

‘Computer-related Crime: Recommendation No. R(89)9 on Computer-related Crime and Final Report of the European Committee on Crime Problems’ (Office of Justice Programs) <https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-related-crime-recommendation-no-r899-computer-related> สืบค้นเมื่อ 15 เมษายน 2566.

Concordia University, ‘who we are: History’ (Concordia University, 2008). <http://www.concordia.ca/about/who-weare/ourhistory/sgw.php> สืบค้นเมื่อ 30 ธันวาคม 2565.

‘Convention on Cybercrime (ETS No. 185)’ (The Council of Europe) <https://rm.coe.int/1680081561> สืบค้นเมื่อ 30 ธันวาคม 2565.

บรรณานุกรม (ต่อ)

Cornell Law School,‘Court reporter’ (Cornell Law School) <https://www.law.cornell.edu/wex/court_reporter> สืบค้นเมื่อ 28 มีนาคม 2566.

_____, ‘NEW YORK Commercial Email and Spam’ (Cornell Law School) <https://www.law.cornell.edu/wex/inbox/new_york> สืบค้นเมื่อ 25 มีนาคม 2566.

‘Cybercrime Module 2 Key Issues: Computer-related offences’ (United Nations Office on Drugs and Crime) <https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/computer-related-offences.html> สืบค้นเมื่อ 2 มกราคม 2566.

Daniel D. Coughlin, ‘Misdemeanor crimes in tennessee’ (Mccbristol, 30 June 2022) <https://www.mccbristol.com/blog/misdemeanor-crimes-in-tennessee/> สืบค้นเมื่อ 28 มีนาคม 2566.

European Union Agency for Criminal Justice Cooperation, ‘Cybercrime’ (European Union Agency for Criminal Justice Cooperation) <www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime> สืบค้นเมื่อ 3 เมษายน 2566.

FBI, ‘2019 Internet Crime Report Released’ (FBI, 11 February 2020) <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120> สืบค้นเมื่อ 10 มกราคม 2566.

Frédéric Lecomte, ‘Cybersecurity laws and regulations in France 2023’ (ICLG) <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/France> สืบค้นเมื่อ 3 เมษายน 2566.

Kabay M. E., *A Brief History of Computer Crime: An Introduction for Students* (School of Graduate Studies Norwich University 2008).

Marco Gercke, ‘understanding cybercrime: Phenomena challenges and legal response’ (ITU) <https://www.itu.int/ITUD/cyb/cybersecurity/docs/cyber-crime%20legislation%2> สืบค้นเมื่อ 15 เมษายน 2566.

OECD, ‘Who we are’ (OECD) <https://www.oecd.org/about/> สืบค้นเมื่อ 15 เมษายน 2566.

‘On attacks against information systems’ (EUR-Lex) <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32005F0222> สืบค้นเมื่อ 16 เมษายน 2566.

Paul Gillin, ‘The history of phishing’ (Verizon) <https://www.verizon.com/business/resources/articles/s/the-history-of-phishing/> สืบค้นเมื่อ 5 มกราคม 2566.

บรรณานุกรม (ต่อ)

Proofpoint,‘2022 State of the Phish’ (Proofpoint)
<https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>
สืบค้นเมื่อ 10 มกราคม 2566.

Rasha S. El-Din, Paul Cairns and John Clark, ‘The Human Factor in Mobile Phishing’
<https://www.researchgate.net/publication/298091490> สืบค้นเมื่อ 6 มกราคม 2566.

‘RECOMMENDATION No. R (89) 9’ (The Council of Europe)
<https://rm.coe.int/09000016804f1094> สืบค้นเมื่อ 15 เมษายน 2566.

‘... Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (... StrÄndG) (G-SIG: 16019307)’ (German Bundestag) <https://dip.bundestag.de/vorgang/.../8366>
สืบค้นเมื่อ 30 มีนาคม 2566.

Tom Jagatic and others, *Social Phishing* (School of Informatics Indiana University 2005).

Tushar Srivastava, ‘Phishing and Pharming-The Deadly Duo’ (SANS Institute, 14 February 2007)
<http://www.sans.org/reading-room/whitepapers/ privacy/phishing-pharming-evil-twins- 1731> สืบค้นเมื่อ 7 มกราคม 2566.

ประวัติผู้เขียน

ชื่อ – นามสกุล นายรณกร วาพันสุ

ประวัติการศึกษา

พ.ศ.2564 - นิติศาสตรบัณฑิต มหาวิทยาลัยมหาสารคาม

ประสบการณ์ทำงาน

พ.ศ. 2566 - นิติกร โรงพยาบาลพระนครศรีอยุธยา