มาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

นางสาวสุธาทิพย์ แก้วศิวะวงศ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2559

Criminal Measures for Online Impersonation

Miss Suthathip Kaewsiwawong

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Laws Program in Laws

Faculty of Law

Chulalongkorn University

Academic Year 2016

หัวข้อวิทยานิพนธ์	มาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต
โดย	นางสาวสุธาทิพย์ แก้วศิวะวงศ์
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร.คณพล จันทน์หอม

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะนิติศาสตร์

(ศาสตราจารย์ ดร.นันทวัฒน์ บรมานันท์)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(ศาสตราจารย์ วีระพงษ์ บุญโญภาส)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(ผู้ช่วยศาสตราจารย์ ดร.คณพล จันทน์หอม)

.....กรรมการภายนอกมหาวิทยาลัย

(พันตำรวจเอก ญาณพล ยั่งยืน)

.....กรรมการภายนอกมหาวิทยาลัย

(ดร.ชาลี วรกุลพิพัฒน์)

สุธาทิพย์ แก้วศิวะวงศ์ : มาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต (Criminal Measures for Online Impersonation) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. ดร.คณพล จันทน์หอม, 179 หน้า.

วิทยานิพนธ์ฉบับนี้มีวัตถุประสงค์เพื่อศึกษาถึงมาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต โดยมุ่งศึกษาเกี่ยวกับลักษณะการกระทำผิด มาตรการทางกฎหมาย และมาตรการบังคับที่ควรนำมาใช้เพื่อป้องกันและปราบปรามการกระทำผิดดังกล่าว

จากการศึกษาพบว่า ในปัจจุบันเทคโนโลยีคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ตเข้ามามีบทบาทสำคัญในการดำเนินชีวิตประจำวันของมนุษย์ การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการกระทำผิดลักษณะหนึ่งซึ่งเกิดขึ้นจากการนำข้อมูลส่วนที่แสดงอัตลักษณ์ส่วนบุคคลของเหยื่อไปใช้แอบอ้างสวมรอยผ่านเว็บไซต์หรือโปรแกรมประยุกต์ที่ใช้งานบนระบบเครือข่ายอินเทอร์เน็ต รวมถึงวิธีการทางอิเล็กทรอนิกส์อย่างอื่น โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และกระทำไปโดยมีวัตถุประสงค์ที่ไม่ชอบด้วยกฎหมาย การกระทำเช่นนี้ถือเป็นการล่วงละเมิดสิทธิในความเป็นตัวตนและสิทธิส่วนบุคคลของผู้ถูกสวมรอยเป็นเหตุให้ผู้ถูกสวมรอยและบุคคลอื่นที่เกี่ยวข้องได้รับความเสียหาย ประเทศไทยต้องประสบกับปัญหาการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต แต่ประเทศไทยยังไม่มีมาตรการทางอาญาเกี่ยวกับการกระทำผิดดังกล่าวอย่างชัดเจนและครอบคลุมเพียงพอ ส่งผลให้ผู้ถูกสวมรอยไม่ได้รับการคุ้มครองอย่างแท้จริง ทั้งนี้ เมื่อศึกษากฎหมายของสหรัฐอเมริกา สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี พบว่าสหรัฐอเมริกามีบทบัญญัติที่วางมาตรการทางอาญาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไว้เป็นการเฉพาะ ส่วนสหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี แม้จะไม่มีบทบัญญัติเฉพาะ แต่มีการกำหนดแนวทางในการนำบทบัญญัติอื่นที่มีอยู่แล้วมาปรับใช้แก่ข้อเท็จจริงที่เกิดขึ้นเป็นรายกรณีไป ส่งผลให้ประเทศเหล่านี้มีมาตรการทางอาญาสำหรับจัดการปัญหาดังกล่าวได้อย่างมีประสิทธิภาพ

ด้วยเหตุที่กล่าวมาข้างต้น จึงเสนอแนะให้ประเทศไทยกำหนดมาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตให้ชัดเจนและเหมาะสม เพื่อให้เจ้าหน้าที่ในกระบวนการยุติธรรมทางอาญามีหลักเกณฑ์ในการดำเนินการทางกฎหมายแก่ผู้กระทำผิด และประชาชนได้รับการคุ้มครองอย่างแท้จริง อันจะส่งผลให้การป้องกันและปราบปรามการกระทำความผิดดังกล่าวเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ

สาขาวิชา นิติศาสตร์ ลายมือชื่อนิสิต .....

ปีการศึกษา 2559 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

5686031634 : MAJOR LAWS
KEYWORDS: ONLINE IMPERSONATION / CRIMINAL MEARSURES / INTERNET / PERSONAL DATA / IDENTITY / RIGHT TO PRIVACY

SUTHATHIP KAEWSIWAWONG: Criminal Measures for Online Impersonation. ADVISOR: ASST. PROF. KANAPHON CHANHOM, Ph.D., 179 pp.

The objective of this thesis is to study the criminal measures for online impersonation crime in order to find which criminal measures and sanctions are applicable to prevent and suppress such crime.

The study showed that computer technology and internet networking system play a very important role in our daily life. Although such technology is useful for various activities, it also opens the door for the criminals to use this technology as a tool to commit crimes. Online impersonation is a crime that a person impersonates other person by using other person's identifying information or personal data via any internet websites, applications, or other electronic means to pretend to be that person without obtaining the consent for the purpose of committing crimes. This behavior infringes the person's right to identity and right to privacy and may cause victims and those who involved to suffer from damages. At present, Thailand is facing a problem of online impersonation, but there are none of criminal measures to prevent such crime and protect the victims effectively. On the contrary, the study showed that the United States has its own provisions imposing criminal measures for online impersonation, whereas, England, Japan, and South Korea do not have any specific laws but they have some guidelines to use the existing laws to prosecute cases involving online impersonation. Their legal measures has proven the effective solutions to solve such problems.

This thesis purposes the implementation of explicit and proper criminal measures related to online impersonation in Thailand in order to take action against the offenders as well as to ensure that people will be truly protected. By doing so would result in the effectiveness of the prevention and suppression of the crime.

Field of Study: Laws Student's Signature .....

Academic Year: 2016 Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ สำเร็จลุล่วงด้วยดีเพราะความอนุเคราะห์อย่างสูงจากท่านผู้ช่วยศาสตราจารย์ ดร.คณพล จันทน์หอม ที่กรุณารับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ โดยท่านได้ชี้แนะแนวทางในการศึกษาวิจัย ให้คำปรึกษา ความเห็น และข้อเสนอแนะอันเป็นประโยชน์อย่างยิ่งต่อการจัดทำวิทยานิพนธ์ฉบับนี้ให้เสร็จสมบูรณ์ ผู้เขียนขอกราบขอบพระคุณท่านผู้ช่วยศาสตราจารย์ ดร.คณพล จันทน์หอม เป็นอย่างสูงที่ให้ความเมตตาและมอบความรู้อันมีค่ายิ่งแก่ผู้เขียนเสมอมา

ผู้เขียนขอกราบขอบพระคุณท่านศาสตราจารย์วีระพงษ์ บุญโญภาส ที่กรุณารับเป็นประธานกรรมการสอบวิทยานิพนธ์ รวมทั้งได้ให้ความเห็นที่เป็นประโยชน์อย่างยิ่งในการเขียนวิทยานิพนธ์ นอกจากนี้ ผู้เขียนขอกราบขอบพระคุณท่านพันตำรวจเอก ญาณพล ยั่งยืน และท่าน ดร.ชาลี วรกุลพิพัฒน์ ที่กรุณาสละเวลาอันมีค่ายิ่งรับเป็นกรรมการผู้ทรงคุณวุฒิ ท่านทั้งสองได้ช่วยชี้แนะแนวทาง ตลอดจนให้ข้อมูลและข้อเสนอแนะแก่ผู้เขียนเพื่อนำไปต่อยอดความรู้และปรับปรุงเนื้อหาของวิทยานิพนธ์ฉบับนี้ให้สมบูรณ์มากยิ่งขึ้น

ในการนี้ ผู้เขียนขอกราบขอบพระคุณคุณพ่อคมศิลป์ แก้วศิวะวงศ์ คุณแม่จุฬาลักษณ์ แก้วศิวะวงศ์ คุณยายสุนงค์ เดชานรากร และขอขอบคุณน้องชาย คุณปิยบุตร แก้วศิวะวงศ์ ที่เป็นกำลังใจสำคัญ และให้การสนับสนุนและส่งเสริมในทุกด้านตลอดระยะเวลาการจัดทำวิทยานิพนธ์ ทำให้ผู้เขียนสามารถจัดทำวิทยานิพนธ์ฉบับนี้จนสำเร็จลุล่วงได้ด้วยดี รวมทั้งขอขอบคุณคุณบัณฑิตย์ นทีรัยไทวะ ที่คอยเป็นกำลังใจและให้คำแนะนำช่วยเหลือด้านข้อมูลและความเห็นทางกฎหมายแก่ผู้เขียนเป็นอย่างดีเสมอมา

นอกจากนี้ ผู้เขียนขอขอบคุณกัลยาณมิตรทุกท่าน ทั้งเพื่อนร่วมชั้นเรียน เจ้าหน้าที่ประจำคณะนิติศาสตร์และบัณฑิตวิทยาลัย ผู้บังคับบัญชา ตลอดจนบุคคลทุกท่านที่ไม่อาจกล่าวนามได้ทั้งหมด ณ ที่นี้ ที่ให้การสนับสนุน ให้ความช่วยเหลือ และคำแนะนำในการศึกษาเล่าเรียนและการจัดทำวิทยานิพนธ์เป็นอย่างดีมาโดยตลอด

ผู้เขียนหวังเป็นอย่างยิ่งว่าวิทยานิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อผู้ที่สนใจศึกษาค้นคว้าไม่มากก็น้อย หากวิทยานิพนธ์ฉบับนี้มีคุณค่าและก่อให้เกิดคุณประโยชน์ประการใด ผู้เขียนขออุทิศความดีความชอบนั้นให้แก่ผู้มีพระคุณของผู้เขียนทุกท่าน แต่หากวิทยานิพนธ์ฉบับนี้บกพร่องหรือผิดพลาดประการใด ผู้เขียนขออภัยมา ณ ที่นี้ และขอน้อมรับไว้แต่เพียงผู้เดียว

สารบัญ

หน้า

หน้า

หน้า

หน้า

สารบัญตาราง

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

นับแต่อดีตจนถึงปัจจุบัน รูปแบบการดำเนินชีวิตของมนุษย์เปลี่ยนแปลงไปตามพัฒนาการของสังคม ผู้คนในยุคสังคมเกษตรกรรมย่อมมีกิจกรรมทางสังคมแตกต่างจากผู้คนในยุคสังคมอุตสาหกรรม เทคโนโลยีที่ได้รับการพัฒนาให้ทันสมัยมากขึ้นส่งผลกระทบโดยตรงต่อกิจกรรมต่าง ๆ ของมนุษย์ ไม่ว่าจะเป็นการติดต่อสื่อสาร การเดินทาง การประกอบอาชีพ การใช้ชีวิตประจำวัน หรือแม้แต่การประกอบอาชญากรรม ในยุคที่เทคโนโลยีทางคอมพิวเตอร์และอินเทอร์เน็ตเฟื่องฟูเช่นนี้ ผู้กระทำผิดจำนวนมากจึงหันมาใช้ช่องทางอิเล็กทรอนิกส์ในการกระทำความผิดมากขึ้น ทำให้เกิดรูปแบบการกระทำความผิดทางคอมพิวเตอร์ที่หลากหลาย ไม่ว่าจะเป็นการมุ่งโจมตีระบบคอมพิวเตอร์โดยตรง หรือการอาศัยระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดก็ตาม

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต (Online Impersonation) เป็นรูปแบบหนึ่งของการกระทำความผิดที่อาศัยระบบคอมพิวเตอร์เป็นเครื่องมือ กล่าวคือ เป็นการใช้ชื่อหรือข้อมูลที่แสดงความเป็นตัวตนของบุคคลอื่นในการส่งจดหมายอิเล็กทรอนิกส์ สร้างข้อความบนเว็บไซต์ สร้างบัญชีผู้ใช้งานเว็บไซต์เครือข่ายสังคมออนไลน์ หรือติดต่อผู้อื่นผ่านทางระบบอินเทอร์เน็ต[1] ผู้กระทำผิดจะอาศัยชื่อหรืออัตลักษณ์ของบุคคลอื่นไปกระทำความผิด หรือทำให้ผู้ที่ถูกสวมรอยหรือบุคคลอื่นใดได้รับความเสียหาย เช่น ใช้ชื่อของดารานักร้องที่มีชื่อเสียงสร้างบัญชีผู้ใช้งานในเว็บไซต์เครือข่ายสังคมออนไลน์ (Social Media or Social Networking) และใช้ชื่อนั้นเพื่อหลอกลวงผู้อื่นให้โอนเงินให้แก่ตน หรือเพื่อทำลายชื่อเสียงของผู้ที่ถูกสวมรอย หรือเพื่อขโมยทรัพย์สิน[2] ดังเช่นที่ปรากฏเป็นข่าวว่าดารานักแสดงคนหนึ่งถูกผู้ไม่ประสงค์ดีสวมรอยเป็นนักแสดงคนดังกล่าวผ่านทางโปรแกรมประยุกต์สำหรับการสนทนา และกระทำการหลอกลวงให้บุคคลอื่นเข้าทำธุรกรรมทางการเงินกับตนเอง เป็นเหตุให้นักแสดงคนดังกล่าวได้รับความเสียหายเนื่องจากการถูกแอบอ้างชื่อและรูปภาพ[3]

---

[1] Webroot, "Discussing Online Impersonation with Your Kids," [Online] Accessed: 2 November 2014. Available from: http://www.webroot.com/us/en/home/resources/tips/ethics-and-legal/ethics-discuss-online-impersonation-with-your-kids

[2] Foh9, "การปลอมแปลงระบบหรือข้อมูลและการสวมรอยเป็นบุคคลอื่น" [ออนไลน์] เข้าถึงเมื่อ 25 มกราคม 2557. แหล่งที่มา: http://foh9.blogspot.com/2012/04/blog-post.html

[3] SpokedarkTV, "มือดีสวมรอยอั้ม พัชราภา ป่วนปลอมไลน์หลอกทำธุรกรรมทางการเงิน" [ออนไลน์] เข้าถึงเมื่อ 26 กุมภาพันธ์ 2558. แหล่งที่มา: http://stars.spokedark.tv/2015/02/19/fake-line/#.VO9BRPmsWSo

การกระทำดังกล่าวข้างต้นย่อมส่งผลกระทบต่อผู้เสียหายหลายประการขึ้นอยู่กับลักษณะของการสวมรอย เช่น การสวมรอยเป็นบุคคลที่มีชื่อเสียงและเขียนข้อความหยาบคายลงบนเว็บไซต์เครือข่ายสังคมออนไลน์ ย่อมทำให้บุคคลผู้ถูกสวมรอยได้รับความเสียหายด้านชื่อเสียงหรือถูกเกลียดชัง หรือการสวมรอยเป็นบุคคลอื่นแล้วหลอกลวงให้บุคคลอีกคนหนึ่งโอนเงินให้แก่ตน ย่อมทำให้ผู้ที่ถูกหลอกลวงได้รับความเสียหายด้านทรัพย์สิน เป็นต้น

อย่างไรก็ตาม แม้ว่าการสวมรอยเป็นบุคคลอื่นเพื่อกระทำความผิดอาญานั้นจะสามารถเอาผิดแก่ผู้กระทำตามฐานความผิดในประมวลกฎหมายอาญาหรือกฎหมายอื่นได้บางฐานความผิดก็ตาม แต่ลักษณะของการกระทำผิดบางกรณีอาจไม่เข้าองค์ประกอบของความผิดที่มีอยู่แล้ว หรือบางกรณีฐานความผิดที่มีอยู่อาจคุ้มครองเพียงผู้เสียหายจากการถูกหลอกลวง แต่ไม่ได้คุ้มครองผู้เสียหายที่ถูกใช้ชื่อหรือข้อมูลส่วนบุคคลในการสวมรอย เช่น กรณีบุคคลหนึ่งสวมรอยเป็นอีกบุคคลหนึ่งและทำการฉ้อโกงบุคคลที่สาม บุคคลที่สามย่อมเป็นผู้เสียหายในความผิดฐานฉ้อโกง แต่บุคคลที่ถูกสวมรอยกลับไม่มีกฎหมายใดคุ้มครองในฐานะเป็นผู้เสียหายของความผิดฐานใดเลย เป็นต้น

วิทยานิพนธ์ฉบับนี้จึงมุ่งศึกษาถึงมาตรการทางอาญาที่เกี่ยวข้องกับการป้องกันและปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต และค้นหาแนวทางในการกำหนดฐานความผิดและมาตรการบังคับที่เหมาะสมสำหรับประเทศไทย เพื่อให้ผู้เสียหายจากการกระทำดังกล่าวได้รับการคุ้มครองสิทธิในความเป็นตัวตนและสิทธิส่วนบุคคลอย่างแท้จริง

1.2 สมมติฐานของการวิจัย

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตก่อให้เกิดความเสียหายต่อผู้ถูกสวมรอยได้หลายด้าน แม้ว่าประเทศไทยจะมีกฎหมายที่สามารถปรับใช้เพื่อลงโทษผู้กระทำผิดได้ในบางกรณี แต่ยังไม่มีบทบัญญัติที่กำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญา รวมทั้งไม่มีการกำหนดมาตรการทางกฎหมายเพื่อให้ผู้เสียหายได้รับการคุ้มครองอย่างแท้จริง ด้วยเหตุนี้จึงสมควรมีมาตรการทางกฎหมายอาญาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเพื่อประโยชน์ในการป้องกันและปราบปรามการกระทำผิดดังกล่าว

1.3 วัตถุประสงค์ของการวิจัย

1.3.1 เพื่อศึกษากฎหมายที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในประเทศไทย สหรัฐอเมริกา สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี

1.3.2 เพื่อศึกษาและวิเคราะห์เปรียบเทียบกฎหมายที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทยกับสหรัฐอเมริกา สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี

1.3.3 เพื่อศึกษาความเหมาะสมของการกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญาในประเทศไทย

1.3.4 เพื่อค้นหามาตรการทางกฎหมายเกี่ยวกับการป้องกันและปราบปรามการกระทำผิดดังกล่าวและแนวทางในการแก้ไขปัญหาที่เกิดขึ้น

1.4 ขอบเขตของการวิจัย

วิทยานิพนธ์ฉบับนี้มุ่งศึกษาถึงสภาพปัญหาการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต รวมถึงที่มา แนวคิด และหลักการในการกำหนดมาตรการทางกฎหมายที่เกี่ยวข้องกับการกระทำความผิดดังกล่าว เฉพาะในส่วนของการสวมรอยเป็นบุคคลธรรมดาที่กระทำผ่านเครือข่ายอินเทอร์เน็ต โดยศึกษาเปรียบเทียบระหว่างกฎหมายของประเทศไทย ศึกษาเฉพาะในส่วนของประมวลกฎหมายอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับที่แก้ไขเพิ่มเติม และร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เท่านั้น เปรียบเทียบกับกฎหมายของสหรัฐอเมริกา สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี เพื่อนำมาวิเคราะห์แนวทางในการป้องกันและปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในประเทศไทย ทั้งนี้ วิทยานิพนธ์ฉบับนี้มีขอบเขตการศึกษาเฉพาะกรณีการกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญาและมาตรการทางกฎหมายที่เกี่ยวข้องกับการกระทำความผิดดังกล่าว

1.5 วิธีดำเนินการวิจัย

ศึกษาวิจัยโดยวิธีวิจัยทางเอกสาร (Documentary Research) ทั้งภาษาไทยและภาษาต่างประเทศจากแหล่งข้อมูลที่เป็นหนังสือ ตำรา บทความ รายงานวิจัย และวิทยานิพนธ์ ตลอดจนข้อมูลจากสื่ออิเล็กทรอนิกส์ในเรื่องที่เกี่ยวข้อง

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ได้ทราบแนวคิด หลักการ และเหตุผลของกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตทั้งในประเทศไทยและต่างประเทศ

1.6.2 ได้ทราบถึงข้อดีและข้อเสียของมาตรการทางกฎหมายเกี่ยวกับการป้องกันและปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในต่างประเทศ

1.6.3 ได้ทราบถึงความเหมาะสมและจำเป็นในการนำมาตรการทางกฎหมายดังกล่าวมาใช้ในประเทศไทย

1.6.4 ได้กำหนดมาตรการทางกฎหมายเกี่ยวกับการป้องกันและปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในประเทศไทย

1.7 เอกสารและงานวิจัยที่เกี่ยวข้อง

เมื่อทบทวนวรรณกรรมที่เกี่ยวข้องและคล้ายคลึงกับเรื่องมาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตแล้วพบว่า มีวรรณกรรมที่กล่าวถึงแนวคิดเกี่ยวกับมาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอยู่บ้าง ดังรายละเอียดต่อไปนี้

นางสาวฐาปณีย์ รติจารุภัทร ได้จัดทำวิทยานิพนธ์ เรื่อง “การกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล”[4] เพื่อค้นหาแนวทางการกำหนดกฎหมายในการป้องกันและปราบปรามการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่เหมาะสมกับประเทศไทย โดยจากการศึกษาพบว่า บทบัญญัติแห่งกฎหมายที่ประเทศไทยมีอยู่ในปัจจุบันยังไม่สามารถนำมาปรับใช้กับการกระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) ได้อย่างครอบคลุม จึงเสนอให้มีการกำหนดฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลให้เป็นความผิดอาญาในกฎหมายไทย โดยกำหนดเป็นกฎหมายเฉพาะซึ่งสามารถปรับใช้ได้เป็นการทั่วไป และมีความครอบคลุมการกระทำผิดทุกกรณี ทั้งนี้ วิทยานิพนธ์ฉบับนี้มุ่งศึกษาภาพรวมของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ซึ่งเกิดขึ้นได้ทั้งทางกายภาพและทางระบบอิเล็กทรอนิกส์ โดยเน้นรายละเอียดเกี่ยวกับการได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลโดยมิชอบด้วยกฎหมาย แต่ยังไม่ได้ศึกษาในรายละเอียดลึกซึ้งเกี่ยวกับการนำข้อมูลดังกล่าวไปใช้เพื่อการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตโดยเฉพาะแต่อย่างใด

ดร.นคร เสรีรักษ์ ได้อธิบายถึงความหมายของสิทธิส่วนบุคคลและลักษณะการละเมิดสิทธิส่วนบุคคลไว้ใน “ความเป็นส่วนตัว ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย” ว่า สิทธิส่วนบุคคล หมายถึง สิทธิที่จะอยู่คนเดียว ปราศจากการ

---

[4] ฐาปนีย์ รติจารุภัทร, "การกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งเป็นเอกลักษณ์บุคคล" (ปริญญานิติศาสตรมหาบัณฑิต, สาขาวิชานิติศาสตร์ คณะนิติศาสตร์, จุฬาลงกรณ์มหาวิทยาลัย, 2555), หน้า.

แทรกแซงโดยบุคคลอื่น รวมไปถึงสิทธิที่จะปกป้องตนเองจากการถูกนำชื่อหรือสิ่งที่บ่งบอกว่าเป็นบุคคลนั้นไปใช้ประโยชน์ทางการค้าหรือการโฆษณาโดยไม่ได้รับความยินยอมโดยชัดแจ้ง การแสวงหาประโยชน์จากเรื่องส่วนตัวเช่นนี้ถือเป็นการละเมิดสิทธิส่วนบุคคลลักษณะหนึ่ง[5] แต่อย่างไรก็ตาม ใน “ความเป็นส่วนตัว ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย” ของ ดร.นคร เสรีรักษ์ ยังไม่มีการอธิบายถึงการนำข้อมูลส่วนบุคคลไปแอบอ้างสวมรอยเป็นบุคคลเจ้าของข้อมูลนั้นผ่านทางระบบเครือข่ายอินเทอร์เน็ต ซึ่งมีวัตถุประสงค์ในการกระทำที่นอกเหนือไปจากเพื่อประโยชน์ทางการค้า

1.8 โครงสร้างวิทยานิพนธ์

วิทยานิพนธ์ เรื่อง มาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต มุ่งศึกษาวิเคราะห์แนวทางการกำหนดมาตรการทางอาญาที่เหมาะสมต่อการป้องกันและปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตสำหรับประเทศไทย โดยมีลำดับการนำเสนอดังนี้

ในบทที่ 2 ผู้เขียนจะนำเสนอถึงแนวคิดและหลักการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต โดยเริ่มศึกษาถึงแนวคิดและหลักการพื้นฐานเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต ประกอบกับแนวคิดและหลักการพื้นฐานเกี่ยวกับสิทธิส่วนบุคคลและข้อมูลส่วนบุคคล เพื่อให้เข้าใจถึงความเชื่อมโยงของการกระทำผิดต่อสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลโดยอาศัยระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือ จากนั้นจะได้ศึกษาถึงการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตโดยละเอียด ตั้งแต่ความหมาย ลักษณะการกระทำ ผลกระทบ ตลอดจนสภาพปัญหาที่เกิดขึ้นจริงในสังคมของผู้ใช้งานอินเทอร์เน็ตทั่วโลก อีกทั้งจะได้ศึกษาถึงแนวคิดและหลักการทางกฎหมายอาญาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต อันได้แก่ การกำหนดให้การกระทำเป็นความผิดอาญา มาตรการบังคับทางอาญา และการคุ้มครองและเยียวยาผู้เสียหาย เพื่อทำให้ทราบหลักการพื้นฐานว่าสมควรกำหนดมาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นดังกล่าวอย่างไรต่อไป

ในบทที่ 3 มุ่งศึกษาถึงมาตรการทางอาญาที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทย โดยจะนำเสนอว่าประเทศไทยมีบทบัญญัติแห่งกฎหมายใดบ้างที่เข้ามาเกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตและแต่ละบทบัญญัติสามารถแก้ไขปัญหาหรือคุ้มครองผู้ถูกสวมรอยอย่างครอบคลุมเพียงพอได้หรือไม่ อย่างไร พร้อมทั้งเสนอให้

---

[5] นคร เสรีรักษ์, ความเป็นส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย (กรุงเทพมหานคร: ฟ้าฮ่าม, 2557), หน้า 37-39.

เห็นถึงสภาพปัญหาและผลกระทบจากการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตที่เกิดขึ้นในประเทศไทย

เมื่อทราบถึงปัญหาที่เกิดจากการบังคับใช้กฎหมายและสภาพปัญหาการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทยในบทที่ 3 แล้วจึงนำไปสู่การค้นหาแนวทางแก้ไขปัญหาดังกล่าว ต่อมาในบทที่ 4 ผู้เขียนจะศึกษาถึงมาตรการทางอาญาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของต่างประเทศ เพื่อค้นหาคำตอบว่าต่างประเทศมีแนวคิดและมาตรการทางกฎหมายสำหรับจัดการกับปัญหาการสวมรอยดังกล่าวไว้หรือไม่ อย่างไร โดยผู้เขียนเลือกทำการศึกษาเฉพาะกฎหมายของสหรัฐอเมริกา สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลีเท่านั้น เพื่อนำข้อมูลที่ได้รับจากการศึกษาค้นคว้าทั้งหมดมาวิเคราะห์เปรียบเทียบมาตรการทางอาญาที่สมควรนำมาปรับใช้ในประเทศไทยต่อไป

หลังจากรวบรวมข้อมูลทั้งกฎหมายไทยและกฎหมายต่างประเทศที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเรียบร้อยแล้ว ในบทที่ 5 ผู้เขียนจะนำข้อมูลดังกล่าวมาประมวลรวมกันและวิเคราะห์ความเหมาะสมในการกำหนดมาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตสำหรับประเทศไทย โดยแบ่งหัวข้อการวิเคราะห์ออกเป็น 3 หัวข้อดังนี้ (1) การวิเคราะห์เปรียบเทียบลักษณะการกระทำความผิด (2) การวิเคราะห์เปรียบเทียบมาตรการทางกฎหมาย และ (3) การวิเคราะห์เปรียบเทียบมาตรการบังคับ เพื่อให้ทราบว่าประเทศไทยควรกำหนดลักษณะการกระทำความผิดอย่างไร ควรมีมาตรการทางกฎหมายอย่างไร และควรกำหนดมาตรการบังคับที่จะลงแก่การกระทำความผิดดังกล่าวอย่างไรตามลำดับ

ในบทที่ 6 ซึ่งเป็นบทสุดท้าย ผู้เขียนจะสรุปภาพรวมของมาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต และเสนอแนะแนวทางการกำหนดมาตรการทางอาญาสำหรับความผิดดังกล่าวที่เหมาะสมและนำไปสู่การป้องกันและปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตสำหรับประเทศไทยต่อไป

บทที่ 2
แนวคิดและหลักการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

นับแต่อดีตจนถึงปัจจุบัน สังคมมนุษย์มีการเปลี่ยนแปลงในด้านต่าง ๆ เป็นอย่างมาก วิถีการดำรงชีวิตแต่เดิมที่ต้องเอาตัวรอดจากภัยธรรมชาติได้พัฒนาเปลี่ยนแปลงเรื่อยมา จนกระทั่งมีการพัฒนาแนวคิดและต่อยอดความรู้เพื่อสร้างสรรค์สิ่งใหม่ ๆ ก่อให้เกิดเทคโนโลยีอันทันสมัย ซึ่งเอื้อประโยชน์ต่อการดำรงชีวิตในปัจจุบันของมนุษย์มากยิ่งขึ้น เทคโนโลยีที่สำคัญเป็นอย่างยิ่งและเป็นหนึ่งในแรงขับเคลื่อนทิศทางของการดำเนินชีวิตในสังคมของมนุษย์ในยุคนี้ก็คือ ระบบคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ต ซึ่งอาจเรียกได้ว่าเป็นรากฐานของการใช้ชีวิตประจำวันในด้านต่าง ๆ มากมาย เช่น การติดต่อสื่อสาร การดำเนินธุรกิจ การค้นคว้าเรียนรู้ การรักษาทางการแพทย์ การสร้างสรรค์สิ่งบันเทิงและงานศิลปะสมัยใหม่ เป็นต้น

ทั้งนี้ แม้ว่าเทคโนโลยีคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตจะเป็นประโยชน์ต่อมนุษย์ในยุคปัจจุบันก็ตาม เหรียญย่อมมีสองด้านเสมอฉันใด เทคโนโลยีเหล่านี้ย่อมมีแง่มุมที่โหดร้ายฉันนั้น บรรดาผู้ไม่ประสงค์ดีจึงอาศัยช่องว่างบางประการมุ่งทำลายหรือสร้างความเสียหายให้แก่ระบบคอมพิวเตอร์ อีกทั้งยังใช้ประโยชน์จากระบบคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ตที่มีความสะดวกสบายเป็นเครื่องมือในการก่ออาชญากรรมหลากหลายรูปแบบ การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการกระทำอีกรูปแบบหนึ่งที่อาศัยระบบเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือในการสร้างความเดือดร้อนรำคาญและละเมิดต่อความเป็นตัวตนของผู้ถูกสวมรอย ส่งผลกระทบและสร้างความเสียหายต่อทั้งผู้ถูกสวมรอยและบุคคลอื่นที่เกี่ยวข้อง ซึ่งผู้กระทำการเช่นนี้สมควรได้รับการลงโทษตามกฎหมาย

ในบทนี้ ผู้เขียนจะขออธิบายถึงแนวคิดและหลักการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต โดยแบ่งเป็น (1) แนวคิดและหลักการพื้นฐานเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต เพื่ออธิบายถึงลักษณะ รูปแบบ และสาเหตุของการเกิดอาชญากรรมคอมพิวเตอร์ (2) แนวคิดและหลักการพื้นฐาน เรื่อง สิทธิส่วนบุคคลและข้อมูลส่วนบุคคล เพื่อชี้ให้เห็นความสำคัญของการคุ้มครองสิทธิส่วนบุคคลและข้อมูลส่วนบุคคล (3) การกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต เพื่ออธิบายถึงลักษณะการกระทำความผิด ผลกระทบและความเสียหายที่เกิดขึ้น รวมทั้งเหตุผลความจำเป็นในการกำหนดให้การกระทำเช่นนี้เป็นความผิดทางอาญา และ (4) แนวคิดและหลักการทางกฎหมายอาญาเกี่ยวกับการกระทำความผิดการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

2.1 แนวคิดและหลักการพื้นฐานเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต

"คอมพิวเตอร์" (Computer) มีความหมายตามพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2542 ว่า *"เครื่องอิเล็กทรอนิกส์แบบอัตโนมัติ ทำหน้าที่เสมือนสมองกลใช้สำหรับแก้ปัญหาต่าง ๆ ทั้งที่ง่ายและซับซ้อน โดยวิธีทางคณิตศาสตร์"* ระบบคอมพิวเตอร์ประกอบด้วยส่วนประกอบสำคัญ 4 ส่วน ส่วนแรกคือ ฮาร์ดแวร์ (Hardware) หมายถึง อุปกรณ์ต่าง ๆ ที่ประกอบเข้ากันเป็นเครื่องคอมพิวเตอร์ แบ่งเป็นหน่วยรับข้อมูล หน่วยประมวลผล และหน่วยแสดงผล ส่วนที่สองคือ ซอฟต์แวร์ (Software) หมายถึง โปรแกรมชุดคำสั่งที่เขียนให้เครื่องคอมพิวเตอร์ทำงานหรือปฏิบัติตาม แบ่งเป็นซอฟต์แวร์ควบคุมระบบ (System Software) และซอฟต์แวร์ประยุกต์ (Application Software) ส่วนที่สามคือ บุคลากร (Peopleware) หมายถึง บุคคลที่เกี่ยวข้องกับการใช้งานคอมพิวเตอร์ และส่วนสุดท้ายคือ ข้อมูลคอมพิวเตอร์ (Data) หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้

การทำงานสอดประสานกันอย่างเป็นระบบของส่วนประกอบในระบบคอมพิวเตอร์ดังกล่าวข้างต้นก่อให้เกิดประโยชน์ต่อการดำเนินชีวิตของผู้คนในสังคมในปัจจุบันอย่างมหาศาล ทั้งภาครัฐและเอกชนในด้านต่าง ๆ เช่น ด้านบริการประชาชนของภาครัฐ ด้านการประกอบธุรกิจการพาณิชย์ทั้งภายในประเทศและต่างประเทศ ด้านการศึกษา ด้านวิทยาศาสตร์และการแพทย์สาธารณสุข ด้านการวิเคราะห์ข้อมูลและเก็บสถิติ ด้านการบันเทิง เป็นต้น[1]

"อินเทอร์เน็ต" (Internet) ย่อมาจากคำศัพท์ภาษาอังกฤษว่า Interconnected Computer Networks ซึ่งหมายถึง เครือข่ายคอมพิวเตอร์หลาย ๆ เครือข่ายที่ถูกเชื่อมต่อเข้าด้วยกัน ไม่ว่าจะเป็นการเชื่อมต่อระบบเครือข่ายภายในท้องถิ่นหรือหน่วยงาน (Local Area Network: LAN) หรือระบบเครือข่ายขนาดใหญ่ครอบคลุมพื้นที่เป็นบริเวณกว้างมากขึ้น (Wide Area Network: WAN) การเชื่อมโยงระบบคอมพิวเตอร์จนกลายเป็นเครือข่ายขนาดใหญ่เช่นนี้ทำให้ผู้ใช้งานคอมพิวเตอร์สามารถติดต่อสื่อสารหรือมีปฏิสัมพันธ์กันผ่านทางระบบอินเทอร์เน็ตได้ แม้ว่าในตอนแรกการเชื่อมโยงระบบคอมพิวเตอร์จะถูกนำมาใช้ประโยชน์เฉพาะในด้านการทหาร ราชการ และการศึกษาเท่านั้น แต่เมื่อกระทรวงกลาโหมแห่งสหรัฐอเมริกาได้พัฒนาระบบเครือข่าย ARPANET

---

[1] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ = Information Technology Law (กรุงเทพมหานคร: นิติธรรม, 2555), หน้า 7.

จนกลายเป็นเครือข่ายสาธารณะแล้ว ระบบเครือข่ายอินเทอร์เน็ตจึงได้ถือกำเนิดขึ้นและถูกพัฒนาต่อมาเพื่อใช้ประโยชน์ทั้งในด้านส่วนบุคคลและการพาณิชย์[2]

เมื่อมนุษย์มีความคิดริเริ่มสร้างสรรค์และนำเทคโนโลยีที่ทันสมัยมาประยุกต์ใช้กับกิจกรรมต่าง ๆ ในชีวิตประจำวันของตน เทคโนโลยีเหล่านั้นจึงกลายเป็นปัจจัยสำคัญในการดำรงชีวิตของมนุษย์ในยุคนี้ ไม่ว่าจะเป็นกิจกรรมที่เกี่ยวข้องกับการหาเลี้ยงชีพ กิจกรรมเพิ่มพูนทักษะความรู้ความชำนาญ หรือแม้แต่กิจกรรมด้านสัมพันธภาพระหว่างบุคคลก็ตาม ซึ่งกำลังเป็นที่นิยมในปัจจุบัน ดังจะเห็นได้จาก ผู้ที่ใช้งานอินเทอร์เน็ตโดยมีจุดประสงค์เพื่อการติดต่อสื่อสารนั้นมีจำนวนเพิ่มมากขึ้นเรื่อย ๆ เสมือนว่าระบบอินเทอร์เน็ตเป็นสายใยที่เชื่อมผู้คนจากทั่วทุกมุมโลกเข้าด้วยกัน ทำให้เกิดเป็นสังคมขนาดใหญ่ขึ้น หรือที่เรียกกันว่า เครือข่ายสังคมออนไลน์ (Online Social Network) ซึ่งเป็นสังคมที่แตกต่างไปจากสังคมแบบดั้งเดิมของมนุษย์ที่มีการสร้างปฏิสัมพันธ์กันต่อหน้าบุคคล แต่ในสังคมออนไลน์นั้นผู้คนมักจะติดต่อสื่อสารกันผ่านหน้าจอเครื่องมืออุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ต จึงทำให้สามารถติดต่อกันได้อย่างไร้พรมแดน ความสะดวกสบายเช่นนี้ก่อให้เกิดประโยชน์ต่อการดำเนินชีวิตของผู้คนทั่วโลกเป็นอย่างมาก ไม่ว่าจะเป็นการใช้งานเพื่อประโยชน์ส่วนบุคคล เช่น การติดต่อพบปะพูดคุยกับคนรู้จักผ่านทางโปรแกรมสนทนา ทำให้ผู้คนที่อยู่ห่างไกลกันสามารถติดต่อสื่อสารกันได้ การเขียนบทความหรือโพสรูปภาพในกระดานสนทนาสาธารณะหรือที่เรียกกันว่าเว็บบอร์ด (Web Board) การค้นหาข้อมูลหรือศึกษาหาความรู้จากบทความออนไลน์นับล้าน ๆ บทความ หรือการใช้งานเพื่อประโยชน์ในเชิงพาณิชย์ เช่น การเปิดร้านค้าขายสินค้าผ่านทางเว็บไซต์ การซื้อสินค้าจากเว็บไซต์ต่างประเทศ การทำธุรกรรมทางการเงินผ่านทางเว็บไซต์ของธนาคาร การลงคลิปวิดีโอในเว็บไซต์ที่ให้ผลตอบแทนเป็นตัวเงินโดยคำนวณจากยอดการเข้าชม เป็นต้น ด้วยเหตุนี้ ระบบอินเทอร์เน็ตจึงกลายมาเป็นส่วนสำคัญของการใช้ชีวิตประจำวัน ธุรกิจ การศึกษา การพาณิชย์ และด้านอื่น ๆ อีกมากมาย

อย่างไรก็ตาม โลกเสมือนจริงบนอินเทอร์เน็ตไม่ได้มีเพียงด้านดีเสมอไป ยังมีบุคคลประสงค์ร้ายที่อาศัยเทคโนโลยีเหล่านี้เป็นเครื่องมือในการกระทำความผิดอีกด้วย ไม่ว่าจะเป็นการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Abuse) ซึ่งเป็นการกระทำที่ผิดต่อจริยธรรม ศีลธรรม หรือจรรยาบรรณ เป็นการสร้างความเดือดร้อนให้กับผู้อื่นที่ยังไม่ถึงขั้นเป็นการกระทำความผิดตามกฎหมาย[3] หรือหากได้กระทำการใดไปจนสร้างความเสียหายให้กับผู้อื่นและเป็นการกระทำที่มี

---

[2] เรื่องเดียวกัน, หน้า 8.

[3] พนิดา พานิชกุล, จริยธรรมทางเทคโนโลยีสารสนเทศ (Ethics in Information Technology) (กรุงเทพมหานคร: เคทีพี คอมพ์ แอนด์ คอนซัลท์, 2553), หน้า 47.

กฎหมายบัญญัติไว้ว่าเป็นความผิด ย่อมเรียกได้ว่าผู้นั้นได้กระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ต

"อาชญากรรมคอมพิวเตอร์" (Computer Crime) หมายถึง การกระทำผิดกฎหมายโดยเจตนาต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ เช่น การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ การกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ เป็นต้น หรือผู้กระทำผิดอาจอาศัยระบบคอมพิวเตอร์หรือระบบเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือในการกระทำความผิด[4] เช่น การหลอกลวงหรือฉ้อโกงผู้อื่นผ่านทางเครือข่ายอินเทอร์เน็ต การเผยแพร่ข้อมูลเท็จทางเครือข่ายอินเทอร์เน็ตโดยมีเจตนาให้ผู้อื่นเสียหาย เป็นต้น ด้วยลักษณะการกระทำความผิดเช่นนี้จะเห็นได้ว่า อาชญากรรมคอมพิวเตอร์จึงเป็นการกระทำความผิดที่แตกต่างไปจากการกระทำความผิดอาญาแบบเดิม กล่าวคือ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือระบบเครือข่ายอินเทอร์เน็ตเป็นการกระทำผิดต่อวัตถุที่ไม่มีรูปร่าง ผู้กระทำความผิดใช้เทคโนโลยีสมัยใหม่เป็นเครื่องมือในการกระทำความผิดทำให้ยากต่อการตรวจพบหรือค้นหาพยานหลักฐาน อีกทั้งยังเป็นการกระทำความผิดที่ไร้พรมแดนอีกด้วย เนื่องจากระบบอินเทอร์เน็ตสามารถเชื่อมโยงผู้ใช้งานได้จากทั่วทุกมุมโลก ดังนั้น ผู้กระทำความผิดและผู้เสียหายอาจมีภูมิลำเนาอยู่คนละประเทศ และอาจสร้างความเสียหายได้อย่างรวดเร็วและเป็นวงกว้างมากกว่าการกระทำความผิดอาญาแบบเดิม[5]

อาชญากรรมคอมพิวเตอร์มีรูปแบบการกระทำที่หลากหลาย เช่น การโจมตีระบบคอมพิวเตอร์ด้วยมัลแวร์หรือไวรัสเพื่อทำลายระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต การเจาะระบบคอมพิวเตอร์ขององค์กรหรือธนาคารต่าง ๆ การสอดแนมข้อมูลคอมพิวเตอร์ของผู้อื่นโดยการใช้โปรแกรมสปายแวร์ (Spyware) การดักรับข้อมูลคอมพิวเตอร์ที่อยู่ในระหว่างส่งภายในเครือข่ายอินทราเน็ตหรืออินเทอร์เน็ต การโจมตีระบบเครือข่าย เซิฟเวอร์ หรือเว็บไซต์ของผู้อื่นด้วยวิธีที่เรียกว่า DOS (Denial of Service Attacks) เป็นสาเหตุให้ระบบเครือข่าย เซิฟเวอร์ หรือเว็บไซต์นั้นล่ม การส่งจดหมายอิเล็กทรอนิกส์ขยะ (Spam Mail) เพื่อก่อกวนหรือสร้างความรำคาญให้กับผู้ใช้งานเว็บไซต์จดหมายอิเล็กทรอนิกส์ การส่งข้อความหรือสิ่งผิดกฎหมายผ่านทางระบบคอมพิวเตอร์ การสร้างและส่งข้อมูลจดหมายอิเล็กทรอนิกส์หรือ

---

[4] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ = Information Technology Law, หน้า 267-268.

[5] เรื่องเดียวกัน, หน้า 268-269.

เว็บไซต์ปลอมเพื่อหลอกลวงผู้อื่นผ่านทางเครือข่ายอินเทอร์เน็ต (Phishing) การขโมยข้อมูลส่วนบุคคลเพื่อนำไปหาผลประโยชน์ทางธุรกิจ (Identity Theft) เป็นต้น

นับวันการกระทำความผิดเหล่านี้ยิ่งมีจำนวนเพิ่มขึ้นเรื่อย ๆ ด้วยสาเหตุสำคัญหลายประการ[6] เช่น ประการแรก เนื่องจากเทคโนโลยีสารสนเทศด้านต่าง ๆ มีความซับซ้อนกว่าสมัยก่อน มีจุดเชื่อมต่อระบบเครือข่ายขององค์กรต่าง ๆ อย่างหลากหลาย เท่ากับเป็นการเพิ่มช่องทางให้ผู้กระทำความผิดเข้าถึงจุดเชื่อมต่อเหล่านั้นได้มากยิ่งขึ้น ประการที่สอง ระบบคอมพิวเตอร์และอินเทอร์เน็ตได้รับการพัฒนาและขยายตัวอยู่เสมอ ทำให้ผู้คนทั่วโลกสามารถแบ่งปันข้อมูลสารสนเทศได้อย่างสะดวกรวดเร็วหรือก่อให้เกิดรูปแบบของการติดต่อสื่อสารใหม่ ๆ ซึ่งการเปลี่ยนแปลงเช่นนี้ย่อมส่งผลให้เกิดความเสี่ยงในการเผชิญหน้ากับการกระทำความผิดรูปแบบใหม่ด้วยเช่นกัน ประการที่สาม ซอฟต์แวร์ที่มีช่องโหว่หลังจากถูกใช้งานเป็นอีกสาเหตุหนึ่งที่ทำให้ผู้ไม่ประสงค์ดีสามารถกระทำความผิดผ่านทางช่องโหว่นั้น ซึ่งผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์อาจตั้งรับการโจมตีของเหล่าแฮกเกอร์ไม่ทัน ผลร้ายจึงตกอยู่กับผู้ใช้งานซอฟต์แวร์

ด้วยเหตุผลดังกล่าวข้างต้น เมื่อระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตได้รับการพัฒนาให้ใช้งานได้อย่างกว้างขวางและสะดวกมากยิ่งขึ้น รูปแบบ วิธีการ หรือช่องทางในการกระทำความผิดทางคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตก็ย่อมมีหลากหลายและเพิ่มจำนวนอาชญากรรมตามไปด้วย การกระทำความผิดในลักษณะนี้ส่งผลกระทบและสร้างความเสียหายให้กับสังคมในหลากหลายแง่มุม ทั้งความเสียหายที่เกิดขึ้นโดยตรงจากการกระทำความผิด เช่น ข้อมูลคอมพิวเตอร์ได้รับความเสียหายหรือถูกทำลาย ระบบคอมพิวเตอร์ภายในองค์กรไม่สามารถให้บริการได้ และความเสียหายที่เกิดขึ้นเนื่องจากการอาศัยระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือ เช่น การถูกหมิ่นประมาทผ่านทางเว็บไซต์ การสูญเสียทรัพย์สินเนื่องจากถูกหลอกลวงทางอินเทอร์เน็ต หรือแม้แต่ความเสียหายเกี่ยวกับข้อมูลส่วนบุคคลและความเป็นส่วนตัวบนโลกอินเทอร์เน็ตก็กลายมาเป็นอีกหนึ่งในประเด็นพิพาทสำคัญที่สร้างปัญหาและความเสียหายให้แก่บุคคลหลายฝ่ายในปัจจุบัน

2.2 แนวคิดและหลักการพื้นฐานเกี่ยวกับสิทธิส่วนบุคคลและข้อมูลส่วนบุคคล

การกระทำความผิดทางคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตบางรูปแบบสามารถส่งผลกระทบต่อสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลของปัจเจกชนในสังคมได้อย่างกว้างขวาง อีกทั้งยังอาจก่อให้เกิดผลร้ายหรือความเสียหายต่อชีวิต ทรัพย์สิน ชื่อเสียง หรือสิทธิด้านอื่น ๆ ของเหยื่อได้อีกด้วย เนื่องจากสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลเป็นสิ่งละเอียดอ่อนและจำเป็นต้องได้รับการรับรองและ

[6] พนิดา พานิชกุล, จริยธรรมทางเทคโนโลยีสารสนเทศ (Ethics in Information Technology), หน้า 47-48.

คุ้มครองตามกฎหมาย มิให้ผู้ใดมาละเมิดหรือสร้างความเสียหายต่อเจ้าของสิทธิหรือข้อมูลนั้นได้ จึงกลายเป็นหลักการสากลที่นานาอารยประเทศได้กำหนดขึ้นเพื่อคุ้มครองสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลอันเป็นสิทธิขั้นพื้นฐานของมนุษย์

2.2.1 ความหมายของสิทธิส่วนบุคคลและข้อมูลส่วนบุคคล

"สิทธิส่วนบุคคลหรือสิทธิในความเป็นส่วนตัว" (Right to Privacy) เป็นสิทธิมนุษยชนขั้นพื้นฐานประเภทหนึ่งซึ่งมนุษย์ทุกคนมีติดตัวมาตั้งแต่เกิด และได้รับการรับรองให้ต้องได้รับความคุ้มครองตามกฎหมาย ดังปรากฏในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 (Universal Declaration of Human Right 1948)[7] สิทธิส่วนบุคคลจึงเป็นสิทธิโดยธรรมชาติของปัจเจกชนที่จะหวงแหนและป้องกันมิให้สมาชิกในสังคมคนอื่นเข้ามารุกล้ำ ก้าวก่าย หรือละเมิดสิทธิประเภทนี้ได้ เป็นสิทธิที่มาจากแนวคิดพื้นฐานที่ว่ามนุษย์ทุกคนมีความเสมอภาคเท่าเทียมกัน ไม่มีใครมีสิทธิส่วนบุคคลเหนือกว่าคนอื่น[8] หรือเรียกได้ว่าเป็นอำนาจอันชอบธรรมของบุคคลที่มีต่อความปลอดภัยในชีวิตร่างกาย ความเป็นอยู่ส่วนตัว ตลอดจนชื่อเสียงเกียรติยศ บุคคลจึงมีสิทธิที่จะดำรงชีวิตอยู่โดยปราศจากการรบกวนหรือทำอันตรายใด ๆ อันเป็นการก่อให้เกิดความเสียหายต่ออำนาจอันชอบธรรมนั้นโดยไม่มีเหตุอันสมควร[9] หรืออีกนัยหนึ่ง ความเป็นส่วนตัวนั้นหมายถึง สถานะที่บุคคลพึงมีในการอยู่ลำพัง ปราศจากการควบคุมหรือล่วงละเมิดโดยบุคคลอื่น

ในต่างประเทศมีนักคิดนักปรัชญาหลายคนได้ให้คำจำกัดความของสิทธิส่วนบุคคลไว้อย่างหลากหลาย ตัวอย่างเช่น Samuel D. Warren และ Louis D. Brandeis ให้คำนิยามของคำว่า Privacy ไว้ว่าหมายถึง สิทธิที่จะอยู่ตามลำพัง Colin J. Bennett เห็นว่า สิทธิส่วนบุคคลต้องปลอดจากการบุกรุกข้อมูลโดยตำรวจ การลอบดักฟัง การถูกรุกรานจากผู้อื่น อีกทั้งยังเป็นสิทธิที่บุคคลสามารถตัดสินใจได้ด้วยตนเองโดยปราศจากการแทรกแซง[10] Alan F. Westin ก็ได้ให้ความหมายของสิทธิส่วนบุคคลไว้ว่า สิทธิของปัจเจกชน กลุ่ม หรือองค์กรในการตัดสินใจว่าข้อมูลของตนจะถูกนำไป

---

[7] UNIVERSAL DECLARATION OF HUMAN RIGHTS 1948 ARTICLE 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[8] นรินทร์ จุ่มศรี, "มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลจากการใช้บริการเครือข่ายสังคมออนไลน์" (นิติศาสตมหาบัณฑิต, คณะนิติศาสตร์ปรีดี พนมยงค์, มหาวิทยาลัยธุรกิจบัณฑิตย์, 2555), หน้า 17.

[9] พนิดา พานิชกุล, จริยธรรมทางเทคโนโลยีสารสนเทศ (Ethics in Information Technology), หน้า 82.

[10] พงษ์ธร สำราญ, สิทธิส่วนบุคคลกับเทคโนโลยี Gps (กรุงเทพมหานคร: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2552), หน้า 16.

เปิดเผยแก่ผู้อื่นได้มากน้อยเพียงใด และหมายความรวมถึงสิทธิในความเป็นอิสระของตนเอง สิทธิในการอยู่ตามลำพัง สิทธิที่จะมีชีวิตอยู่โดยปราศจากการรบกวนหรือละเมิดความเป็นส่วนตัว ตลอดจนสิทธิที่จะไม่เปิดเผยชื่อเสียงเรียงนามหรือความลับส่วนตัว[11]

"ข้อมูลส่วนบุคคล" (Personal Data/Personal Information) เป็นข้อมูลประเภทหนึ่งซึ่งเกี่ยวโยงกับสิทธิส่วนบุคคล หรืออาจกล่าวได้ว่าเป็นข้อมูลที่เกี่ยวข้องกับการดำเนินชีวิตส่วนตัว รวมถึงการแสดงความเห็นใด ๆ เกี่ยวกับความเป็นส่วนตัว[12] หรือหมายถึง ข่าวสารใด ๆ ซึ่งสามารถพิสูจน์หรือชี้ได้เกี่ยวกับเอกชนคนหนึ่ง ๆ เช่น ชื่อ อายุ ที่อยู่ เลขบัตรประจำตัวประชาชน หมายเลขบัตรเครดิต เลขที่บัญชีธนาคาร รูปภาพ ประวัติการศึกษา ข้อมูลทางการแพทย์ ประวัติอาชญากร เป็นต้น นอกจากนี้ยังมีองค์การระหว่างประเทศได้ให้ความหมายของข้อมูลส่วนบุคคลไว้ด้วย เช่น องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) กำหนดขอบเขตความหมายของข้อมูลส่วนบุคคลไว้ให้หมายถึง ข้อมูลใด ๆ ที่เกี่ยวข้องเฉพาะบุคคล หรือสามารถชี้ให้เห็นลักษณะเฉพาะตัวบุคคลเจ้าของข้อมูลได้[13] ส่วนสหภาพยุโรป (European Union) ได้กำหนดคำนิยามของข้อมูลส่วนบุคคลไว้ในมาตรา 2 ของระเบียบรัฐสภาและคณะมนตรีแห่งสหภาพยุโรป 95/46/EC ว่าหมายถึง ข้อมูลข่าวสารใด ๆ ที่ชี้เฉพาะตัวบุคคลหรือสามารถบ่งชี้ลักษณะเฉพาะที่เกี่ยวข้องกับตัวบุคคลธรรมดาที่เป็นเจ้าของข้อมูล ทั้งทางตรงหรือทางอ้อม[14]

สำหรับประเทศไทย ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ได้ร่างคำนิยามของข้อมูลส่วนบุคคลไว้ว่า "ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรมบรรดาที่มีชื่อของบุคคลนั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย"

ทั้งนี้ ข้อมูลส่วนบุคคลถือเป็นส่วนหนึ่งของข้อมูลแสดงอัตลักษณ์ของบุคคล (Identity) หมายความว่า หากข้อมูลใดข้อมูลหนึ่งมีความชัดเจนมากพอที่จะระบุตัวตนของบุคคลใดบุคคลหนึ่งได้เป็นการเฉพาะเจาะจง เป็นข้อมูลที่ชี้ชัดว่าหมายถึงตัวบุคคลนั้นเพียงคนเดียว กรณีนี้เรียกได้ว่าเป็น

---

[11] James Micheal, Privacy and Human Rights : An International and Comparative Study, with Special Reference to Development in Information Technology (Aldershot, Hants: Dartmouth, 1994), p. 1.

[12] David I Bainbridge, Computer and the Law (Great Britain1973), p. 174.

[13] นคร เสรีรักษ์, การคุ้มครองข้อมูลส่วนบุคคล : ข้อเสนอสำหรับประเทศไทย (กรุงเทพมหานคร: ฟ้าฮ่าม, 2558), หน้า 14.

[14] เรื่องเดียวกัน, หน้า 17.

ข้อมูลแสดงอัตลักษณ์ของบุคคล ข้อมูลส่วนบุคคลจะเป็นข้อมูลแสดงอัตลักษณ์ของบุคคลได้ก็ต่อเมื่อข้อมูลส่วนบุคคลนั้นมีความชัดเจนมากพอที่จะระบุตัวตนได้ หรืออาจเกิดจากการใช้ข้อมูลส่วนบุคคลหลายส่วนประกอบกันจนกลายเป็นข้อมูลที่ใช้ระบุตัวตนของบุคคลก็ได้[15]เช่น โดยหลักแล้ว แม้ว่าชื่อจะเป็นข้อมูลส่วนบุคคล แต่ชื่อหนึ่ง ๆ อาจหมายถึงหลายบุคคลได้ แต่หากนำชื่อมาประกอบกับนามสกุล อายุ ที่อยู่ หรือประวัติการศึกษา ฯลฯ จนมากพอที่จะชี้ชัดได้ว่าหมายถึงบุคคลใด ข้อมูลเหล่านั้นย่อมเป็นข้อมูลแสดงอัตลักษณ์ของบุคคล

2.2.2 หลักการคุ้มครองสิทธิส่วนบุคคลและข้อมูลส่วนบุคคล

เนื่องด้วยสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของหลักเรื่องสิทธิและเสรีภาพ ซึ่งเป็นหลักสำคัญของประชาชนทุกคน รัฐจึงจำเป็นต้องมีมาตรการทางกฎหมายเพื่อรับรองและคุ้มครองสิทธิของบุคคลให้ปลอดจากการกระทำที่มิชอบทั้งหลาย ดังที่รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้บัญญัติรับรองสิทธิส่วนบุคคลไว้ในมาตรา 32 ดังนี้

> *“บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใดๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ”*

บทบัญญัติคุ้มครองสิทธิส่วนบุคคลหรือความเป็นส่วนตัวของประเทศไทยดังกล่าวข้างต้นนั้น สอดคล้องกับข้อกำหนดกติกาข้อที่ 17 แห่งกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง ค.ศ. 1966 (Covenant Civil and Political Rights 1966) ใจความว่า *“1. บุคคลจะถูกแทรกแซงในความเป็นส่วนตัว ครอบครัว เคหะสถาน หรือการติดต่อสื่อสารโดยพลการหรือมิชอบด้วยกฎหมายมิได้ และจะถูกลบหลู่เกียรติและชื่อเสียงโดยมิชอบมิได้ 2. บุคคลทุกคนมีสิทธิจะได้รับการคุ้มครองตามกฎหมายไม่ให้ถูกแทรกแซงหรือลบหลู่เช่นว่านั้น”*[16]

นอกจากนี้ สิทธิส่วนบุคคลถือเป็นสิทธิมนุษยชนประเภทหนึ่งซึ่งมนุษย์ทุกคนมีติดตัวมาตั้งแต่เกิด เป็นหลักกฎหมายสากลที่ได้รับการรับรองจากนานาอารยประเทศ ตามที่องค์การสหประชาชาติได้บัญญัติรับรองสิทธิดังกล่าวไว้ในข้อ 12 แห่งปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 (Universal Declaration of Human Rights 1948) ความว่า *“บุคคลใด ๆ ย่อมไม่ถูกแทรกแซงโดย*

---

[15] ฐาปนีย์ รติจารุภัทร, "การกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งเป็นเอกลักษณ์บุคคล," หน้า 16.

[16] พงษ์ธร สำราญ, สิทธิส่วนบุคคลกับเทคโนโลยี Gps, หน้า 17.

พลการในความเป็นอยู่ส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือไม่อาจถูกลบหลู่ในเกียรติยศและชื่อเสียง ทั้งนี้ บุคคลทุกคนย่อมมีสิทธิที่จะได้รับการปกป้องคุ้มครองโดยกฎหมายอันเนื่องจากการก้าวล่วงในสิทธินั้น"[17] ดังนั้นจะเห็นได้ว่า ข้อมูลส่วนบุคคลซึ่งถือเป็นส่วนหนึ่งของสิทธิส่วนบุคคลย่อมต้องได้รับความคุ้มครองด้วย

การคุ้มครองข้อมูลส่วนบุคคลเป็นสิ่งที่นานาชาติให้ความสำคัญเป็นอย่างมาก องค์การระหว่างประเทศหลายองค์การให้ความสนใจในเรื่องดังกล่าวและได้กำหนดหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขึ้นเพื่อเป็นแนวทางในการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลของนานาอารยประเทศต่อไป ดังจะยกตัวอย่างองค์การระหว่างประเทศที่สำคัญ 3 องค์การ ดังนี้

(1) องค์การเพื่อความร่วมมือทางด้านเศรษฐกิจและการพัฒนา (OECD) ได้กำหนด "แนวทางในการคุ้มครองข้อมูลส่วนบุคคลและการส่งข้อมูลส่วนบุคคลข้ามพรมแดน" (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) ซึ่งเป็นหลักเกณฑ์ที่สนับสนุนให้ทุกภาคส่วนร่วมมือกันบริหารจัดการข้อมูลส่วนบุคคล และพิจารณากฎเกณฑ์ที่เป็นอุปสรรคต่อการส่งข้อมูลส่วนบุคคลข้ามพรมแดน[18] ตลอดจนการคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองสิทธิความเป็นส่วนตัว เพื่อให้เกิดความเชื่อมั่นในการติดต่อสัมพันธ์ทางการค้าของผู้ประกอบธุรกิจต่าง ๆ[19]

(2) รัฐสภาแห่งยุโรป (Council of Europe) ได้ประกาศใช้ข้อตกลงของรัฐสภาแห่งยุโรปใน ค.ศ. 1981 ซึ่งมีบทบัญญัติเกี่ยวกับการคุ้มครองสิทธิในความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลในการประมวลผลโดยวิธีอัตโนมัติและการส่งผ่านข้อมูลระหว่างประเทศ โดยมีคณะกรรมการรัฐสภาแห่งยุโรป (The Council of European's Committee) เป็นองค์กรที่ทำหน้าที่ควบคุมดูแลการดำเนินการคุ้มครองการละเมิดสิทธิความเป็นส่วนตัวอันเกิดจากการละเมิดข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย[20]

(3) สหภาพยุโรป (European Union: EU) มีหลักการคุ้มครองข้อมูลส่วนบุคคลโดยออกเป็นระเบียบรัฐสภาและคณะมนตรีแห่งสหภาพยุโรปว่าด้วยการคุ้มครองการประมวลผลและการ

---

[17] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ = Information Technology Law, หน้า 241.

[18] Organisation for Economic Co-operation and Development, "Oecd Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," [Online] Accessed: 13 July 2011. Available from: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[19] นคร เสรีรักษ์, การคุ้มครองข้อมูลส่วนบุคคล : ข้อเสนอสำหรับประเทศไทย, หน้า 14.

[20] เรื่องเดียวกัน, หน้า 17.

ส่งข้อมูลส่วนบุคคล (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data: European Data Protection Directive) อันเป็นหลักเกณฑ์ฉบับแรก เพื่อให้ประเทศสมาชิกของสหภาพยุโรปนำไปใช้เป็นแนวทางในการบัญญัติกฎหมายภายใน รวมถึงให้มีมาตรฐานในการส่งผ่านข้อมูลส่วนบุคคลภายในประเทศสมาชิก[21] โดยมีวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคลและเสรีภาพในการเคลื่อนไหวของข้อมูลของประเทศสมาชิกอย่างเท่าเทียมกัน

(4) องค์การสหประชาชาติ (United Nations) คณะมนตรีเศรษฐกิจและสังคมแห่งสหประชาชาติได้กำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลไว้ในแนวทางการควบคุมข้อมูลส่วนบุคคลที่จัดเก็บด้วยคอมพิวเตอร์ (Guidelines for the Regulation of Computerized Personal Data Files)[22]

(5) กลุ่มความร่วมมือทางเศรษฐกิจเอเชีย-แปซิฟิก (APEC) ได้กำหนดหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคล (APEC Information Privacy Principles) โดยมีวัตถุประสงค์ในการกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลเพื่อป้องกันการใช้ข้อมูลโดยมิชอบและป้องกันความเสียหายที่จะเกิดจากการใช้ข้อมูลโดยมิชอบ ไม่ว่าจะเป็นการสูญหาย เสียหาย การเข้าถึงหรือการทำลายข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การใช้ แก้ไข หรือเปิดเผยโดยมิชอบ[23]

เมื่อองค์การระหว่างประเทศได้วางแนวทางหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไว้แล้ว นานาอารยประเทศจึงรับเอาหลักเกณฑ์ดังกล่าวไปใช้เป็นแนวทางในการตรากฎหมายว่าด้วยการคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคล โดยแต่ละประเทศจะมีพระราชบัญญัติหลากหลายแตกต่างกันไป เช่น กฎหมายคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคลในสหรัฐอเมริกามีทั้งกฎหมายที่มีผลกับรัฐบาลกลางและกฎหมายที่มีผลกับเอกชน เช่น Privacy Act of 1974, Computer Matching and Privacy Protection Act 1988, Electronic Communication Privacy Act of 1986 เป็นต้น ส่วนในประเทศภาคพื้นยุโรปนั้นมีหลายประเทศที่ตราพระราชบัญญัติว่าด้วยการคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคลเช่นเดียวกัน เช่น สาธารณรัฐฝรั่งเศสมีกฎหมาย French Data Protection Act สหพันธ์สาธารณรัฐเยอรมนีมีกฎหมาย Federal Data Protection Act เป็นต้น

---

[21] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ = Information Technology Law, หน้า 246-247.

[22] เรื่องเดียวกัน, หน้า 247.

[23] นคร เสรีรักษ์, การคุ้มครองข้อมูลส่วนบุคคล : ข้อเสนอสำหรับประเทศไทย, หน้า 21-22.

ตัวอย่างของการวางมาตรการและแนวทางในการคุ้มครองสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลในประเทศต่าง ๆ เช่น สหรัฐอเมริกาได้กำหนดหลักการพื้นฐานในการคุ้มครองสิทธิส่วนบุคคลไว้ 4 ประการสำคัญ ได้แก่ ประการแรก คุ้มครองการรุกล้ำความเป็นส่วนตัวของผู้อื่น (Intrusion) ประการที่สอง คุ้มครองการแสวงหาประโยชน์จากความเป็นส่วนตัวของผู้อื่นโดยไม่ได้รับความยินยอม (Appropriation) ประการที่สาม คุ้มครองการเปิดเผยข้อเท็จจริงอันเป็นเรื่องส่วนตัวของบุคคลต่อสาธารณะ (Public Disclosure of Private Fact) และประการที่สี่ คุ้มครองการเผยแพร่ข้อมูลอันเป็นเท็จต่อสาธารณะเพื่อให้บุคคลอื่นได้รับความเสื่อมเสีย (False Light in the Public Eye)[24]

กล่าวโดยสรุป สิทธิส่วนบุคคลและข้อมูลส่วนบุคคลเป็นหนึ่งในสิทธิมนุษยชนขั้นพื้นฐานที่ทุกคนมีมาตั้งแต่เกิด และพึงได้รับการรับรองและคุ้มครองตามกฎหมาย เพื่อมิให้ผู้อื่นมาล่วงละเมิดต่อสิทธินั้นได้ การกระทำอันเป็นการละเมิดต่อสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลและก่อให้เกิดความเสียหายแก่เจ้าของนั้น ย่อมถือเป็นการสร้างความเดือดร้อนรำคาญและความไม่สงบสุขขึ้นในสังคม รัฐจึงสมควรวางนโยบาย แนวทาง หรือมาตรการป้องกันและปราบปรามการละเมิดเช่นนี้

2.3 การกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

เนื่องด้วยเทคโนโลยีด้านคอมพิวเตอร์และอินเทอร์เน็ตได้รับการพัฒนาให้ทันสมัยอยู่ตลอดเวลา อาชญากรคอมพิวเตอร์จึงมีการพัฒนารูปแบบการกระทำผิดให้เป็นไปตามการเปลี่ยนแปลงดังกล่าวเช่นกัน ด้วยเหตุนี้จึงเกิดรูปแบบการกระทำผิดเกี่ยวกับคอมพิวเตอร์รูปแบบใหม่และหลากหลายมากขึ้น การอาศัยระบบเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือในการกระทำความผิดเกี่ยวกับสิทธิส่วนบุคคลหรือข้อมูลส่วนบุคคลถือว่าเป็นการกระทำผิดอีกรูปแบบหนึ่งของอาชญากรรมคอมพิวเตอร์ ซึ่งนับวันจะยิ่งมีจำนวนเพิ่มมากขึ้นอันเนื่องมาจากการเติบโตของสังคมโลกออนไลน์

ในยุคที่ระบบเครือข่ายอินเทอร์เน็ตเฟื่องฟู ผู้พัฒนาซอฟต์แวร์และแพลตฟอร์มต่าง ๆ ได้คิดค้นพร้อมสร้างช่องทางการติดต่อสื่อสารไร้พรมแดนขึ้นเป็นจำนวนมาก ทั้งโปรแกรมประยุกต์สำหรับการสนทนา ระบบจดหมายอิเล็กทรอนิกส์ เว็บไซต์ที่มีจุดประสงค์ในการดำเนินธุรกรรมทางพาณิชย์อิเล็กทรอนิกส์ รวมถึงเว็บไซต์เครือข่ายสังคมออนไลน์รูปแบบต่าง ๆ ซึ่งนับวันจะได้รับการพัฒนาและมีลูกเล่นใหม่ ๆ มากยิ่งขึ้น ด้วยลักษณะที่การใช้งานแพลตฟอร์มเหล่านี้ ผู้ใช้งานไม่ได้ติดต่อสื่อสารกันโดยตรงเฉกเช่นการพบปะพูดคุยในสังคมรูปแบบเดิม แต่เป็นการสื่อสารระยะไกลผ่านทางระบบคอมพิวเตอร์และอินเทอร์เน็ตโดยไม่เห็นหน้าค่าตาของคู่สนทนาอีกฝ่ายหนึ่ง จึงเป็นการง่ายที่ผู้หวังร้ายจะใช้ช่องทางเหล่านี้ในการแสดงตนเป็นบุคคลอื่นเพื่อวัตถุประสงค์ที่ก่อให้เกิดความ

---

[24] พงษ์ธร สำราญ, สิทธิส่วนบุคคลกับเทคโนโลยี Gps, หน้า 28.

เสียหายทั้งต่อเจ้าของตัวตนที่ถูกสวมรอยและบุคคลอื่นที่เกี่ยวข้อง การกระทำเช่นนี้เรียกว่า การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

2.3.1 ความหมายของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการกระทำผิดที่อาศัยเทคโนโลยีคอมพิวเตอร์และอินเทอร์เน็ตเป็นเครื่องมือ ถือเป็นการกระทำผิดรูปแบบหนึ่งของการโจรกรรมข้อมูลแสดงอัตลักษณ์ของบุคคล (Identity Theft) ซึ่งกระทรวงยุติธรรมของสหรัฐอเมริกาได้กำหนดคำนิยามไว้ว่า “Identity Theft และ Identity Fraud คือคำศัพท์ที่ใช้อ้างถึงอาชญากรรมทุกประเภทที่เกิดจากบุคคลใดบุคคลหนึ่งซึ่งได้มาและใช้ข้อมูลส่วนบุคคลของผู้อื่นโดยมิชอบในทางฉ้อโกงหรือหลอกลวง โดยเฉพาะอย่างยิ่งเพื่อให้ได้มาซึ่งผลประโยชน์ทางเศรษฐกิจ” หรือกล่าวอีกนัยหนึ่ง การโจรกรรมข้อมูลแสดงอัตลักษณ์ของบุคคล หมายถึง กรณีที่บุคคลใดบุคคลหนึ่งขโมยข้อมูลสำคัญบางอย่างที่เป็นข้อมูลใช้สำหรับพิสูจน์อัตลักษณ์ของบุคคลอื่น และนำไปใช้ทำธุรกรรมทางการเงินในนามของบุคคลนั้นโดยมิชอบ[25]

อนึ่ง เนื่องจากประเทศไทยยังไม่ได้บัญญัติให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญาจึงจำต้องพิจารณาลักษณะของการกระทำดังกล่าวตามบทบัญญัติทางกฎหมายที่เกี่ยวข้องในต่างประเทศ โดยเฉพาะกฎหมายของสหรัฐอเมริกา เนื่องจากหลายมลรัฐในสหรัฐอเมริกาได้กำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญาและได้กำหนดคำนิยามไว้ ยกตัวอย่างดังต่อไปนี้

ประมวลกฎหมายอาญาของมลรัฐเทกซัสได้ให้ความหมายของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต หรือ Online Impersonation ไว้ว่าหมายถึง การกระทำของบุคคลที่ใช้ชื่อหรือความเป็นตัวตนของผู้อื่นโดยไม่ได้รับความยินยอม เพื่อสร้างหน้าเว็บ ประกาศหรือส่งข้อความบนเว็บไซต์เครือข่ายสังคมออนไลน์เชิงพาณิชย์หรือเว็บไซต์อินเทอร์เน็ตอื่น หรือโปรแกรมจดหมายอิเล็กทรอนิกส์หรือโปรแกรมกระดานข้อความใด ๆ หรือได้ส่งจดหมายอิเล็กทรอนิกส์ ข้อความด่วน ข้อความตัวอักษร หรือการติดต่อสื่อสารอื่นที่คล้ายคลึงกันนี้ซึ่งอ้างถึงชื่อ ที่อยู่ หมายเลขโทรศัพท์ หรือสิ่งอื่นใดที่แสดงข้อมูลอันเป็นอัตลักษณ์ของผู้อื่น โดยมีเจตนาประทุษร้าย หลอกลวง ข่มขู่บุคคลอื่นใด[26]

---

[25] พนิดา พานิชกุล, จริยธรรมทางเทคโนโลยีสารสนเทศ (Ethics in Information Technology), หน้า 90.

[26] TEXAS PENAL CODE § 33.07

ประมวลกฎหมายอาญาของมลรัฐแคลิฟอร์เนียได้ให้ความหมายไว้ว่าหมายถึง การจงใจสวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือผ่านทางเว็บไซต์อินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์อื่นใด โดยไม่ได้รับความยินยอมจากผู้ถูกสวมรอย และมีจุดประสงค์เพื่อประทุษร้าย ข่มขู่ หรือหลอกลวงผู้อื่น[27]

ประมวลกฎหมายอาญาของมลรัฐนิวยอร์กได้ให้ความหมายไว้ว่าหมายถึง การสวมรอยเป็นบุคคลอื่นผ่านการติดต่อสื่อสารทางเว็บไซต์อินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์ โดยเจตนาให้ได้มาซึ่งผลประโยชน์หรือเพื่อทำร้ายหรือหลอกลวงฉ้อโกงผู้อื่น หรืออาศัยช่องทางการติดต่อสื่อสารดังกล่าวทำการอวดอ้างตนเป็นเจ้าหน้าที่รัฐเพื่อโน้มน้าวจูงใจให้ผู้อื่นยอมต่ออำนาจเช่นนั้นหรือกระทำการโดยอาศัยความน่าไว้วางใจจากการอวดอ้างนั้น[28]

จากตัวอย่างคำนิยามข้างต้นจะเห็นได้ว่า ลักษณะสำคัญของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตนั้นประกอบด้วย

(1) ผู้กระทำผิดต้องกระทำด้วยความจงใจหรือมีเจตนากระทำผิด มิใช่เป็นการกระทำผิดโดยประมาทเลินเล่อ

(2) ผู้กระทำผิดไม่ได้รับอนุญาตให้ใช้ชื่อหรือข้อมูลส่วนบุคคลของผู้ถูกสวมรอย

(3) ผู้กระทำผิดกระทำการโดยอาศัยช่องทางบนเว็บไซต์เครือข่ายสังคมออนไลน์หรือวิธีการทางอิเล็กทรอนิกส์ต่าง ๆ

(4) ต้องมีจุดประสงค์เพื่อประทุษร้าย หลอกลวง หรือข่มขู่ผู้อื่น หรือก่อให้เกิดความเสียหายแก่ผู้ถูกสวมรอยเอง

โดยหลักการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตสามารถเกิดขึ้นได้ 2 รูปแบบดังต่อไปนี้

(1) การสร้างหน้าเว็บหรือโพรไฟล์บนสื่อสังคมออนไลน์ปลอม ผู้สวมรอยจะนำข้อมูลส่วนบุคคลที่สามารถระบุตัวตนของผู้อื่นได้อย่างเฉพาะเจาะจงไปใช้เพื่อสร้างหน้าเว็บหรือเปิดใช้งานบัญชีสื่อสังคมออนไลน์ในนามของผู้ถูกสวมรอย และกระทำการต่าง ๆ ผ่านทางหน้าเว็บหรือบัญชีสังคมออนไลน์นั้นเพื่อให้ผู้อื่นหลงเชื่อว่าตนเป็นผู้ที่ถูกสวมรอยจริง

(2) การเข้าถึงบัญชีผู้ใช้งานเว็บไซต์ของผู้ถูกสวมรอยโดยไม่ได้รับอนุญาต (Unauthorized Access) และกระทำการแอบอ้างเป็นเจ้าของบัญชีผู้ใช้งานนั้น การเข้าถึงบัญชีผู้ใช้งานดังกล่าวอาจเกิดจากการขโมยรหัสผ่าน การเจาะระบบคอมพิวเตอร์ หรือวิธีการอื่นใดอันเป็นเหตุให้ผู้กระทำผิดสามารถเข้าใช้งานบัญชีของผู้ถูกสวมรอยได้ และนอกจากจะสวมรอยเป็นเจ้าของ

---

[27] CALIFORNIA PENAL CODE § 528.5

[28] NEW YORK PENAL CODE § 190.25

บัญชีผู้ใช้งานเพื่อวัตถุประสงค์ที่ไม่ชอบด้วยกฎหมาย เช่น การข่มขู่คุกคาม การเฝ้าติดตามรังควาน การหลอกลวงฉ้อโกงแล้ว ผู้กระทำผิดอาจจะขโมยข้อมูลส่วนบุคคล ข้อมูลสำคัญทางการเงิน หรือปล่อยไวรัสเข้าสู่ระบบคอมพิวเตอร์ของผู้ถูกสวมรอยได้อีกด้วย[29] ดังเช่นตัวอย่างกรณีการหลอกลวงผ่านการใช้งานเฟซบุ๊ก (Facebook) ซึ่งบรรดาแฮกเกอร์ได้เข้าทำการยึดบัญชีผู้ใช้งานเฟซบุ๊กและกระทำการสวมรอยเป็นกลุ่มผู้รักษาความปลอดภัยของเฟซบุ๊ก ส่งข้อความไปยังผู้ใช้งานรายอื่นให้หลงเชื่อและกรอกข้อมูลส่วนบุคคลและข้อมูลบัตรเครดิตลงในหน้าเว็บไซต์เฟซบุ๊กปลอม[30]

นอกจากนี้ การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Website Defacement) ซึ่งเป็นการกระทำที่กระทบกระเทือนต่อการรักษาความมั่นคงปลอดภัยของเครื่องบริการเว็บ (Web Server) โปรแกรมสำหรับให้บริการเว็บ (Web Server Software) และโปรแกรมประยุกต์บนเว็บ (Web Application) นั้น อาจเป็นที่มาของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตได้อีกทางหนึ่ง โดยเฉพาะอย่างยิ่งการโจมตีจากเทคนิค Cross-site Scripting ซึ่งเกิดจากช่องโหว่ของเว็บไซต์ที่ไม่มีการคัดกรองหรือตรวจสอบข้อมูลที่ได้รับจากผู้ใช้บริการเว็บไซต์ว่าเป็นข้อมูลที่น่าเชื่อถือหรือไม่ หากมีผู้ไม่หวังดีแทรกคำสั่งต่าง ๆ เข้าไปในหน้าเว็บ เมื่อผู้ใช้บริการเรียกใช้หรือเข้าถึงหน้าเว็บดังกล่าวอาจถูกขโมยข้อมูลสำคัญได้ และผู้กระทำผิดจะนำข้อมูลนั้นไปสวมรอยโดยการเข้าใช้งานบัญชีผู้ใช้งานเว็บไซต์เสมือนว่าเป็นผู้ใช้บริการตัวจริง[31] ทั้งนี้ ในปัจจุบันมีเว็บไซต์ปลอมที่ถูกสร้างขึ้นเพื่อหลอกลวงผู้ใช้บริการเป็นจำนวนมาก ผู้ให้บริการเว็บไซต์จึงควรมีกระบวนการยืนยันตัวตนเว็บไซต์ว่าเป็นเว็บไซต์ที่มีตัวตนอยู่จริง ด้วยการขอใบรับรองอิเล็กทรอนิกส์จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certificate Authority) เพื่อให้ได้กุญแจสาธารณะสำหรับใช้ในการยืนยันตัวตนของเจ้าของหรือผู้รับผิดชอบเว็บไซต์[32] เนื่องจากใบรับรองอิเล็กทรอนิกส์มีประโยชน์หลายประการ ได้แก่ ประการแรก การปกป้องความลับของข้อมูล (Data Confidentiality) เพื่อป้องกันไม่ให้ผู้อื่นที่ไม่ได้รับอนุญาตเข้ามาอ่านข้อมูลอิเล็กทรอนิกส์ ประการที่สอง การตรวจสอบความครบถ้วนของข้อมูล (Data Integrity) เพื่อตรวจสอบว่าข้อมูลถูกต้องครบถ้วนและไม่มีการแก้ไขเปลี่ยนแปลง ประการที่สาม การพิสูจน์ตัวจริง (Authentication) เพื่อยืนยันตัวตนของผู้ส่งข้อมูล

---

[29] Maksim Reznik, "Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation," Touro Law Review 29(2013): 467.

[30] Facecrooks, "Hackers Impersonate Security Team on Facebook," [Online] Accessed: 19 June 2017. Available from: http://facecrooks.com/Scam-Watch/hackers-impersonate-security-team-on-facebook.html

[31] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงเทคโนโลยีและการสื่อสาร, ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (กรุงเทพมหานคร: 2557), หน้า 17.

[32] เรื่องเดียวกัน, หน้า 38.

อิเล็กทรอนิกส์ และประการสุดท้าย การห้ามปฏิเสธความรับผิด (Non-repudiation) เพื่อป้องกันไม่ให้ผู้ส่งข้อมูลอิเล็กทรอนิกส์ปฏิเสธว่าตนไม่ได้ส่งข้อมูลนั้น[33]

2.3.2 ลักษณะการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

ระบบอินเทอร์เน็ตเป็นเครื่องมือสำคัญในการเชื่อมโยงข้อมูลจากทั่วทุกมุมโลกเข้าด้วยกัน การเชื่อมโยงแบบเครือข่ายเช่นนี้ทำให้การติดต่อสื่อสารผ่านทางระบบอินเทอร์เน็ตเป็นไปโดยสะดวกและง่ายดาย ผู้ใช้งานอินเทอร์เน็ตจากทุกประเทศสามารถเข้าถึงข้อมูลและสร้างกิจกรรมผ่านทางระบบดังกล่าวได้โดยไม่มีพรมแดนขวางกั้น ลักษณะเช่นนี้ส่งผลให้เกิดการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตได้จากทุกพื้นที่ที่มีการเชื่อมต่อระบบอินเทอร์เน็ต และมีลักษณะการกระทำผิดที่คล้ายคลึงกันทั่วโลก สามารถสรุปเป็นตัวอย่างโดยสังเขปได้ดังนี้

(1) การสวมรอยเป็นบุคคลอื่นบนเว็บไซต์เครือข่ายสังคมออนไลน์ (Social Networking Sites : SNSs) ซึ่งเกิดขึ้นได้จากหลายสาเหตุ เช่น ความรักใคร่ การเลียนแบบ การขู่ว่าจะเปิดโปงความลับ (Blackmail) หรือเจตนากระทำความผิดอาญาอื่น ๆ เป็นต้น[34] กรณีนี้เกิดขึ้นได้ง่ายและกว้างขวาง เนื่องจากเว็บไซต์เครือข่ายสังคมออนไลน์ได้รับความนิยมเป็นอย่างมากในปัจจุบัน ผู้ใช้งานจำนวนมากเขียนแสดงข้อมูลส่วนบุคคลของตนไว้มากพอที่ผู้กระทำผิดจะสามารถรวบรวมข้อมูลดังกล่าวและนำมาสร้างบัญชีผู้ใช้งานปลอมเพื่อสวมรอยเป็นบุคคลนั้นได้โดยง่าย[35]

เหตุการณ์สวมรอยเป็นบุคคลอื่นที่เกิดขึ้นบ่อยครั้งในการใช้งานเว็บไซต์เครือข่ายสังคมออนไลน์ มักมีเป้าหมายเป็นเพื่อนหรือคนรู้จักของผู้ที่ถูกสวมรอย ผู้กระทำผิดจะสร้างบัญชีผู้ใช้งานเว็บไซต์ในชื่อของผู้เสียหาย รวมทั้งเขียนข้อมูลส่วนบุคคลของผู้เสียหายลงในหน้าประวัติโดยย่อ (Profile) และแสร้งทำเป็นผู้เสียหายเพื่อจะเข้าถึงเพื่อนหรือบุคคลอื่นที่ผู้เสียหายรู้จัก โดยที่ผู้เสียหายไม่อาจทราบได้เลยว่ากำลังถูกสวมรอยอยู่[36] หรือในกรณีที่มีการสร้างบัญชีผู้ใช้งานเครือข่าย

---

[33] ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ, "คำถามที่พบบ่อย" [ออนไลน์] เข้าถึงเมื่อ 19 มิถุนายน 2560. แหล่งที่มา: http://www.nrca.go.th/faq.html

[34] Hiyam S. Ensour, "Online Impersonation a Case Study in the Hashemite Kingdom of Jordan," International Journal of Engineering & Computer Science IJECS-IJENS 13, 05 (2013): 20.

[35] Protect My ID, "Facebook Fraud: Identity Theft through Social Networking," [Online] Accessed: 25 March 2014. Available from: https://www.protectmyid.com/images/education_center/pdf/050TypesofFraud/7_types%20of%20fraud_social%20networking.pdf

[36] ibid.

สังคมออนไลน์ในนามของผู้อื่นและกระทำการต่าง ๆ ในนามของผู้นั้นจนกระทั่งมีชื่อเสียง มีผู้ใช้งานรายอื่นมาติดตามเป็นจำนวนมาก และได้รับผลประโยชน์อันเนื่องมาจากชื่อเสียงนั้น แม้ต่อมาภายหลังจะเปลี่ยนไปใช้ข้อมูลจริงของตนหรือข้อมูลส่วนบุคคลของผู้อื่นแทน ย่อมถือได้ว่าเป็นการสวมรอยเป็นบุคคลอื่นที่ก่อให้เกิดผลประโยชน์แก่ผู้สวมรอยแล้ว เป็นการละเมิดสิทธิในตัวตนและข้อมูลส่วนบุคคลของผู้ถูกสวมรอย

(2) มิตรภาพออนไลน์ (Online Friendship) หมายถึง การผูกสัมพันธ์ฉันมิตรระหว่างผู้ใช้งานอินเทอร์เน็ต โดยเริ่มต้นจากความบริสุทธิ์ใจ แต่ภายหลังกลับข่มขู่ว่าจะเปิดเผยความลับทำให้ผู้อื่นเสื่อมเสียชื่อเสียงหรือเกียรติยศ[37]

(3) การปลอมจดหมายอิเล็กทรอนิกส์ส่วนบุคคลและใช้งานโดยมีจุดประสงค์ในการแก้แค้นหรือหมิ่นประมาทผู้อื่น[38]

(4) การแสดงความคิดเห็นหรือส่งต่อเว็บไซต์ข้อมูลข่าวสารโดยใช้ชื่อปลอม การกระทำเช่นนี้ส่งผลให้ผู้ที่ถูกนำชื่อไปใช้อาจตกเป็นผู้ต้องสงสัยในกรณีที่มีการแสดงความคิดเห็นทางการเมืองหรือศาสนาและก่อให้เกิดความขัดแย้ง ผู้ถูกสวมรอยจำเป็นต้องพิสูจน์ว่าตนมิใช่ผู้ที่แสดงความเห็นดังกล่าวบนเว็บไซต์[39]

(5) การโจรกรรมข้อมูลอันเป็นอัตลักษณ์ส่วนบุคคล (Personal Identity) ของผู้อื่นเพื่อปลอมตัวเป็นผู้นั้น เช่น ชื่อ อายุ เลขประจำตัวประชาชน เป็นต้น ซึ่งเกิดขึ้นได้เมื่อผู้กระทำผิดสามารถเข้าถึงข้อมูลส่วนบุคคลของผู้เสียหายได้โดยวิธีการทางคอมพิวเตอร์[40]

อย่างไรก็ตาม ด้วยลักษณะและรูปแบบการกระทำความผิดที่เกิดจากการนำข้อมูลส่วนบุคคลของผู้อื่นมาแอบอ้างนั้น จึงอาจเกี่ยวโยงหรือคล้ายคลึงกับการกระทำความผิดลักษณะอื่น ๆ ได้หลายฐานความผิดดังต่อไปนี้

(1) การโจรกรรมข้อมูลแสดงอัตลักษณ์ของบุคคล (Identity Theft) มีความแตกต่างจากการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต (Online Impersonation) อยู่หลายประการ เช่น แรงจูงใจเบื้องหลังของผู้กระทำผิดฐานโจรกรรมข้อมูลแสดงอัตลักษณ์ของบุคคล มักจะเป็นการใช้ข้อมูลส่วนบุคคลที่เป็นความลับของผู้อื่นเพื่อให้ได้มาซึ่งผลประโยชน์ทางการเงิน แต่การสวมรอยเป็น

---

[37] Ensour, H. S., "Online Impersonation a Case Study in the Hashemite Kingdom of Jordan," International Journal of Engineering & Computer Science IJECS-IJENS: 21.

[38] ibid.

[39] ibid.

[40] ibid.

บุคคลอื่นบนเครือข่ายอินเทอร์เน็ตนั้นมุ่งไปที่การสร้างความเดือดร้อนเสียหายให้แก่บุคคลอื่นมากกว่าการได้รับผลประโยชน์ เช่น นายขาวสวมรอยเป็นนายเขียวบนเว็บไซต์สังคมออนไลน์ และแสดงข้อความให้นายเขียวได้รับความอับอาย เป็นต้น นอกจากนี้ การโจรกรรมข้อมูลแสดงอัตลักษณ์ของบุคคลยังมีลักษณะเป็นการขโมยข้อมูลส่วนบุคคลที่สำคัญ เช่น หมายเลขบัตรประจำตัวประชาชน หมายเลขบัตรเครดิต เป็นต้น ในขณะที่การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตนั้นเป็นการใช้ข้อมูลส่วนบุคคลของบุคคลอื่นเพื่อกระทำการอันมิชอบด้วยกฎหมายผ่านทางวิธีอิเล็กทรอนิกส์[41] อีกทั้งการสวมรอยดังกล่าวยังป้องกันได้ยากกว่า เนื่องจากผู้กระทำผิดต้องการข้อมูลส่วนบุคคลเพียงเล็กน้อยเท่านั้นก็สามารถสวมรอยเป็นบุคคลอื่นได้แล้ว และผู้ถูกสวมรอยอาจต้องสูญเสียค่าใช้จ่ายจำนวนมากเพื่อจัดการลบล้างข้อมูลที่บิดเบือนไป รวมทั้งการกอบกู้ชื่อเสียงของตนกลับคืนมาอีกด้วย[42] ดังนั้นจึงเห็นได้ว่า การกระทำผิดทั้งสองรูปแบบมีความแตกต่างกันพอสมควร โดยแตกต่างกันทั้งจุดประสงค์ของการกระทำและวิธีการกระทำความผิด

(2) การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตถือเป็นการกระทำรูปแบบหนึ่งของการเฝ้าติดตามทางอินเทอร์เน็ต (Cyberstalking) การคุกคามทางอินเทอร์เน็ต (Cyber Harassment) รวมถึงการกลั่นแกล้งทางอินเทอร์เน็ต (Cyberbullying) ซึ่ง The National Conference of State Legislature แห่งสหรัฐอเมริกาได้กำหนดคำจำกัดความของการเฝ้าติดตามทางอินเทอร์เน็ต (Cyberstalking) ไว้ว่า การใช้อินเทอร์เน็ต จดหมายอิเล็กทรอนิกส์ หรือการสื่อสารทางอิเล็กทรอนิกส์อื่นใด เพื่อเฝ้าติดตาม และให้หมายความรวมถึงรูปแบบพฤติกรรมที่มีลักษณะเป็นการข่มขู่หรือมุ่งประสงค์ร้าย[43] การเฝ้าติดตามทางอินเทอร์เน็ตเป็นการกระทำความผิดผ่านอุปกรณ์สื่อสารอิเล็กทรอนิกส์ซึ่งก่อให้เกิดความเสียหายหรือความเจ็บปวดทางอารมณ์และจิตใจ ในขณะที่การคุกคามทางอินเทอร์เน็ต (Cyber Harassment) นั้นหมายถึง การส่งข้อความจดหมายอิเล็กทรอนิกส์ ข้อความด่วน บล็อก หรือเว็บไซต์ที่มีลักษณะข่มขู่หรือคุกคามไปยังบุคคลใดบุคคลหนึ่งเพื่อรบกวนหรือก่อความเดือดร้อนรำคาญแก่บุคคลนั้น[44] ส่วนการกลั่นแกล้งทางอินเทอร์เน็ต (Cyberbullying) นั้นอาจเป็นการกลั่นแกล้งด้วยวิธีการสวมรอยเป็นบุคคลใดบุคคลหนึ่งผ่านระบบอินเทอร์เน็ตและกระทำ

---

[41] AllClear ID, "Online Impersonation Vs. Identity Theft: Is There a Difference?," [Online] Accessed: 9 November 2014. Updated: 17 December 2012. Available from: https://www.allclearid.com/personal/2012/12/online-impersonatin-vs-identity-theft/

[42] Kori Clanton, "We Are Not Who We Pretend to Be: Odr Alternative to Online Impersonation Statues," Cardozo Journal of Conflict Resolution 16(2014): 331.

[43] ibid.

[44] Cassie Cox, "Protecting Victims of Cyberstalking, Cyberharassment, and Online Impersonation through Prosectutions and Effective Laws," Jurimetrics Journal 54(2014): 280.

การเปิดเผยข้อมูลส่วนบุคคลของผู้ถูกสวมรอย หรือแอบอ้างตัวตนของผู้ถูกสวมรอยเพื่อไปคุกคามผู้อื่นอีกทอดหนึ่ง[45] จะเห็นได้ว่า การกระทำความผิดทั้งสามลักษณะมีจุดประสงค์สำคัญคือ การข่มขู่ มุ่งประสงค์ร้าย ก่อความเดือดร้อนรำคาญ และสร้างความเจ็บปวดทางอารมณ์และจิตใจ ต่อผู้อื่น การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตจึงเป็นเพียงวิธีการหนึ่งที่ผู้กระทำผิดใช้เพื่อเฝ้าติดตามคุกคาม หรือกลั่นแกล้งผู้อื่นผ่านทางอินเทอร์เน็ตเท่านั้น

(3) การหลอกลวงทางอินเทอร์เน็ตรูปแบบหนึ่งที่เกี่ยวข้องกับการขโมยข้อมูลส่วนบุคคลซึ่งเรียกว่า “ฟิชชิ่ง” (Phishing) เป็นการสร้างและใช้จดหมายอิเล็กทรอนิกส์หรือเว็บไซต์ที่ถูกออกแบบมาให้มีลักษณะคล้ายคลึงหรือเสมือนว่าเป็นจดหมายอิเล็กทรอนิกส์หรือเว็บไซต์ขององค์กรธุรกิจ สถาบันทางการเงิน หรือหน่วยงานของรัฐที่มีชื่อเสียง เป็นองค์กรที่ถูกต้องตามกฎหมาย และน่าเชื่อถือไว้วางใจ ผู้กระทำผิดจะสร้างและส่งจดหมายอิเล็กทรอนิกส์หรือเว็บไซต์ปลอมดังกล่าวไปยังผู้เสียหายเพื่อหลอกลวงให้ผู้เสียหายหลงเชื่อและส่งข้อมูลส่วนบุคคล ข้อมูลทางการเงิน หรือข้อมูลที่เป็นความลับมายังผู้กระทำผิด ฟิชชิ่งเป็นวิธีการหนึ่งที่ผู้กระทำผิดที่ต้องการโจรกรรมข้อมูลอันเป็นอัตลักษณ์ส่วนบุคคล (Identity Theft) ใช้เพื่อล้วงเอาข้อมูลส่วนบุคคลผ่านการหลอกลวง ไม่ว่าจะเป็นการหลอกลวงผู้เสียหายจนหลงเชื่อและส่งข้อมูลส่วนบุคคลให้แก่ผู้กระทำผิดเอง หรือหลอกลวงเพื่อให้ผู้กระทำผิดสามารถเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตก็ตาม ในขณะที่การโจรกรรมข้อมูลอันเป็นอัตลักษณ์ส่วนบุคคลนั้นหมายถึง การได้มาและใช้ข้อมูลส่วนบุคคลของผู้อื่นโดยมิชอบหรือใช้เพื่อก่ออาชญากรรมอื่น เช่น ใช้ข้อมูลส่วนบุคคลของผู้อื่นเพื่อให้ได้มาซึ่งสินค้าหรือบริการ หรือใช้ข้อมูลแสดงตัวตนที่แต่งขึ้นมาเพื่อกระทำความผิด เป็นต้น[46]

2.3.3 ผลกระทบที่เกิดจากการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

การสวมรอยเป็นบุคคลอื่นเป็นการกระทำที่ส่งผลกระทบโดยตรงต่อผู้ที่ถูกนำชื่อหรือข้อมูลแสดงอัตลักษณ์ส่วนบุคคลไปใช้ และยังส่งผลกระทบต่อผู้ที่เข้ามาเกี่ยวข้องกับการสวมรอยอีกด้วย นอกจากนี้ ระบบเครือข่ายอินเทอร์เน็ตเป็นระบบที่ทำให้ข้อมูลข่าวสารสามารถแพร่กระจายไปในวงกว้างได้อย่างรวดเร็ว ส่งผลให้การสวมรอยที่เกิดขึ้นในระบบเครือข่ายอินเทอร์เน็ตสามารถสร้างความเสียหายได้มากกว่าการสวมรอยแบบธรรมดา มีผู้ที่ได้รับความเสียหายจำนวนมากขึ้น ดังนี้

---

[45] Colleen M. Koch, "To Catch a Catfish: A Statutory Solution for Victims of Online Impersonation," University of Colorado Law Review 88(2017): 245.

[46] Binational Working Group on Cross-Border Mass Marketing Fraud, "Report on Phishing," [Online] Accessed: 18 June 2017. Available from: https://www.justice.gov/sites/default/files/opa/legacy/2006/11/21/report_on_phishing.pdf

2.3.3.1 ผลกระทบด้านชื่อเสียงของผู้เสียหาย

ลักษณะสำคัญของการสวมรอยเป็นบุคคลอื่นคือ การนำชื่อหรือข้อมูลแสดงตัวตนของบุคคลอื่นไปใช้โดยมิได้รับความยินยอมจากเจ้าของ และกระทำการใด ๆ ในนามของบุคคลอื่นนั้น เป็นเหตุให้ผู้อื่นย่อมเข้าใจผิดว่าผู้ถูกสวมรอยเป็นผู้กระทำเอง ทั้งที่ผู้ถูกสวมรอยไม่ทราบเรื่องเลย หากการกระทำของผู้สวมรอยเป็นสิ่งที่มิชอบด้วยกฎหมายหรือผิดศีลธรรมจรรยาด้วยแล้ว ผู้ถูกสวมรอยอาจถูกตำหนิติเตียน นินทาว่าร้าย หรือถูกดูหมิ่นเกลียดชังจากสังคม ผู้ถูกสวมรอยอาจตกเป็นจำเลยของสังคมโดยที่เขามิได้กระทำผิดอันใดเลยก็เป็นได้ และด้วยเหตุที่การแบ่งปันข่าวสารในระบบเครือข่ายอินเทอร์เน็ตเป็นไปโดยสะดวกรวดเร็ว ผู้ใช้งานอินเทอร์เน็ตจำนวนมากสามารถเข้าถึงแหล่งข้อมูลที่ผู้สวมรอยสร้างขึ้นได้ง่าย ผลเสียหายที่จะเกิดแก่ชื่อเสียงของผู้ถูกสวมรอยจึงมากขึ้นตามไปด้วยเช่นกัน

นอกจากนี้ บางกรณีที่ผู้กระทำผิดสวมรอยเป็นผู้เสียหายและนำชื่อของผู้เสียหายไปก่ออาชญากรรมอื่นอีกต่อหนึ่ง ผู้เสียหายอาจถูกบันทึกชื่อในทะเบียนประวัติอาชญากรหรือผู้ก่อการร้าย โดยที่ผู้เสียหายอาจจะไม่รู้ตัวว่าตนถูกบันทึกชื่อเช่นนั้นลงในฐานข้อมูลของรัฐแล้ว[47] จนกระทั่งผู้เสียหายถูกปฏิเสธการจ้างงานหรือถูกไล่ออกจากงาน เนื่องจากนายจ้างพบเห็นข้อมูลประวัติอาชญากรในชื่อของผู้เสียหาย[48]

2.3.3.2 ผลกระทบด้านทรัพย์สิน

เนื่องด้วยผู้กระทำผิดบางรายมีจุดประสงค์ในการสวมรอยเป็นบุคคลอื่นเพื่อหลอกลวงผู้อื่นและเพื่อให้ตนได้มาซึ่งทรัพย์สินหรือผลประโยชน์ทางการเงินจากเหยื่อ[49] ดังนั้น ผู้เสียหายที่ได้รับผลกระทบนี้จึงต้องสูญเสียทรัพย์สิน สิทธิประโยชน์ทางการเงิน หรือผลประโยชน์อื่น ๆ ไปให้แก่ผู้กระทำผิด

---

[47] Ensour, H. S., "Online Impersonation a Case Study in the Hashemite Kingdom of Jordan," International Journal of Engineering & Computer Science IJECS-IJENS.

[48] Privacy Rights Clearinghouse, "Criminal Identity Theft: What to Do If It Happens to You," [Online] Accessed: 31 October 2014. Available from: https://www.privacyrights.org/consumer-guides/identity-theft-what-do-if-it-happens-you

[49] Ensour, H. S., "Online Impersonation a Case Study in the Hashemite Kingdom of Jordan," International Journal of Engineering & Computer Science IJECS-IJENS: 21.

ยิ่งไปกว่านั้น หากผู้กระทำผิดสามารถเข้าถึงเลขที่บัญชีธนาคารหรือเลขที่บัตรเครดิตของผู้ถูกสวมรอยได้แล้ว ผู้ถูกสวมรอยอาจตกเป็นลูกหนี้ค่าบัตรเครดิตหรือลูกหนี้สินค้าที่ตนไม่ได้ซื้อก็เป็นได้[50]

2.3.3.3 ผลกระทบด้านความเป็นอยู่ของผู้เสียหาย

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอาจส่งผลกระทบที่ร้ายแรงต่อการดำเนินชีวิตของผู้ถูกสวมรอยได้หลายประการ หากเป็นกรณีคุกคาม ข่มขู่ กลั่นแกล้ง หรือก่อความเดือดร้อนรำคาญต่อผู้ถูกสวมรอย ผู้ถูกสวมรอยอาจรู้สึกกลัว สิ้นหวัง ซึมเศร้า หรือแม้แต่ฆ่าตัวตาย[51] ผู้เสียหายที่เป็นเด็กอาจถูกเพื่อนร่วมชั้นเรียนกลั่นแกล้ง กีดกันออกจากกลุ่ม ทำให้มีปัญหาเรื่องการเรียน

เหตุการณ์ร้ายแรงที่เป็นผลมาจากการแสดงตัวตนปลอมผ่านทางโลกไซเบอร์จนกระทั่งเป็นเหตุให้เด็กผู้หญิงคนหนึ่งฆ่าตัวตายในสหรัฐอเมริกานั้นเป็นที่รู้จักกันดีในชื่อคดี Megan Meier เหตุการณ์ดังกล่าวเริ่มต้นขึ้นในเดือนตุลาคม ค.ศ. 2006 เมแกนเป็นเด็กผู้หญิงรูปร่างอ้วน มีความเคารพในตัวเองต่ำ และเป็นโรคซึมเศร้า เมื่อเธอได้รับอนุญาตจากแม่ให้ใช้งานเว็บไซต์ MySpace ได้ เธอได้รับการติดต่อขอเป็นเพื่อนจากบุคคลหนึ่งซึ่งใช้ชื่อแทนตัวเองว่า Josh ในระยะแรก Josh พูดคุยด้วยท่าทีเป็นมิตร แต่ในภายหลัง Josh กลับแสดงท่าทีก้าวร้าวใส่เมแกน และเริ่มตำหนิเมแกนด้วยคำหยาบคาย รวมทั้งชักชวนเพื่อนคนอื่น ๆ มาเขียนข้อความหยาบคายบนหน้าโพรไฟล์ของเมแกนอีกด้วย ในที่สุดเมแกนได้ผูกคอตายในบ้านของเธอและเสียชีวิตในเวลาต่อมา ในภายหลังจึงสืบทราบว่า ผู้ที่ปลอมตัวเป็น Josh นั้นคือแม่ของอดีตเพื่อนร่วมชั้นของเมแกนนั่นเอง ซึ่งปลอมตัวมาเพื่อจับตาดูว่าเมแกนจะพูดอะไรถึงลูกสาวของตนเองบ้าง ทั้งนี้ แม้ว่าคดีของเมแกนจะไม่มีการใช้ชื่อหรือข้อมูลส่วนบุคคลของผู้อื่นไปกระทำการข่มขู่คุกคาม เพียงแต่ตั้งชื่อบัญชีผู้ใช้งาน MySpace ว่า Josh เท่านั้นจึงไม่มีผู้เสียหายที่ถูกสวมรอยก็ตาม แต่คดีนี้เป็นตัวอย่างหนึ่งที่แสดงให้เห็นถึงผลร้ายแรงที่อาจเกิดขึ้นจากการคุกคามผ่านทางระบบอินเทอร์เน็ตได้เป็นอย่างดี เพราะการติดต่อผ่านทางระบบอินเทอร์เน็ตเช่นนี้ ผู้ที่ติดต่อกันไม่อาจเห็นหน้าค่าตาหรืออาจไม่ทราบว่าตัวจริง

---

[50] Reputation.com, "How to Protect Yourself from Online Impersonation," [Online] Accessed: 11 December 2014. Available from: http://www.reputation.com/reputationwatch/articles/how-protect-yourself-online-impersonation

[51] Hemanshu Nigam, "What Can You Can Do to Make Sure an E-Impersonation Bill Gets Passed in Your State?," [Online] Accessed: 11 December 2014. Available from: http://sspblue.com/blog/what-can-you-can-do-to-make-sure-an-e-impersonation-bill-gets-passed-in-your-state/

ของอีกฝ่ายหนึ่งเป็นใคร การหลอกลวง ข่มขู่ คุกคาม หรือการกระทำที่มิชอบอื่น ๆ จึงสามารถเกิดขึ้นได้ง่าย และส่งผลกระทบรุนแรงถึงชีวิตได้ดังเช่นกรณีของเมแกน[52]

2.3.4 สภาพปัญหาการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

ด้วยเหตุที่ความเจริญทางด้านเทคโนโลยีสารสนเทศเข้ามามีบทบาทในการดำเนินชีวิตประจำวันของมนุษย์มากขึ้น จากเดิมที่มนุษย์เคยติดต่อสื่อสารกันผ่านทางการพบปะพูดคุย การส่งจดหมายหรือโทรเลข ปัจจุบันมนุษย์หันมาติดต่อสื่อสารกันผ่านทางระบบอินเทอร์เน็ตมากขึ้น เนื่องจากอินเทอร์เน็ตถือว่าเป็นนวัตกรรมที่สร้างความสะดวกสบายให้แก่ทุกคนสามารถติดต่อกันได้อย่างรวดเร็วและประหยัดทรัพยากรมากขึ้น เป็นเหตุให้ผู้พัฒนาระบบได้สร้างสรรค์เว็บไซต์สำหรับการติดต่อกันทางอินเทอร์เน็ตเพิ่มมากขึ้นและเป็นที่นิยมอย่างมากของผู้ท่องโลกไซเบอร์ เรียกได้ว่าเว็บไซต์เครือข่ายสังคมออนไลน์กลายเป็นแหล่งรวมตัวของมนุษย์ในยุคปัจจุบันจำนวนมาก ทุกคนสามารถติดตามความเคลื่อนไหวของผู้คนรอบตัวได้โดยง่าย ในทางกลับกัน ผู้กระทำผิดก็สามารถสร้างความเสียหายโดยอาศัยรูปแบบของเว็บไซต์เหล่านี้ได้ง่ายเช่นกัน

ปัญหาเรื่องการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตนั้นเป็นปัญหาที่พบเจอได้จากหลายประเทศทั่วโลกที่มีประชากรใช้งานระบบอินเทอร์เน็ต โดยเฉพาะอย่างยิ่ง การใช้งานเว็บไซต์หรือโปรแกรมประยุกต์เกี่ยวกับเครือข่ายสังคมออนไลน์ (Social Networking Sites or Applications) เช่น เฟสบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) อินสตาแกรม (Instagram) หรือกระดานสนทนาต่าง ๆ เป็นต้น รูปแบบของการใช้งานเว็บไซต์หรือโปรแกรมประยุกต์เหล่านี้เอื้อต่อการเสแสร้งแสดงตนเป็นบุคคลอื่น ไม่ว่าจะเป็นบุคคลในจินตนาการหรือบุคคลที่มีตัวตนอยู่จริงก็ตาม หากการแสดงตนเช่นนั้นเกิดขึ้นด้วยเจตนาที่ไม่ดีย่อมก่อให้เกิดความเสียหายแก่ผู้อื่นได้ ทั้งผู้เสียหายที่เป็นบุคคลที่ถูกสวมรอยเองหรือบุคคลอื่นที่เกี่ยวข้องกับการกระทำผิดดังกล่าว

ในส่วนนี้ ผู้เขียนจะอธิบายถึงสภาพปัญหาการกระทำความผิดกรณีสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในต่างประเทศ เพื่อแสดงให้เห็นว่าในปัจจุบันปัญหาดังกล่าวได้เกิดขึ้นจริงทั่วทุกมุมโลกและมีผู้ได้รับความเสียหายหลายด้านแตกต่างกันไป เนื่องจากในปัจจุบันปัญหาการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตกำลังเป็นปัญหาที่หลายประเทศกำลังเผชิญอยู่ โดยเฉพาะประเทศที่มีความเจริญทางด้านระบบโครงข่ายเทคโนโลยีสารสนเทศ เช่น สหรัฐอเมริกา สหราช

---

[52] Jacqueline Vickery, "The Megan Meier Myspace Suicide : A Case Study Exploring the Social Aspects of Convergent Media, Citizen Journalism, and Online Anonymity and Credibility," [Online] Accessed: 25 April 2014. Available from: http://www.online.journalism.utexas.edu/2008/Jaqueline.pdf

อาณาจักร เป็นต้น ทำให้มีจำนวนคดีที่เกิดจากการกระทำความผิดประเภทนี้มากขึ้นเรื่อย ๆ ตัวอย่างเช่น

- กรณีเด็กหญิงวัยรุ่นในมลรัฐเทกซัส สหรัฐอเมริกาถูกจับกุมในข้อหาสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต[53] เหตุการณ์นี้เกิดขึ้นในเมืองแกรนเบอรี่ มลรัฐเทกซัส เมื่อเด็กหญิงวัยรุ่นสองคนได้สร้างบัญชีเฟสบุ๊กปลอมในชื่อของเพื่อนร่วมห้องที่ตกเป็นผู้เสียหายและเจตนาใช้บัญชีดังกล่าวเพื่อทำให้ผู้เสียหายเสื่อมเสียชื่อเสียง โดยการส่งข้อความข่มขู่เพื่อนในเฟสบุ๊กของผู้เสียหาย มารดาของผู้เสียหายได้กล่าวว่า บุตรสาวของตนต้องประสบกับปัญหาร้ายแรงกับเพื่อนร่วมชั้นเรียน ถูกกีดกันทางสังคม และพบเจอการแสดงออกที่ก้าวร้าวจากเพื่อนของเธอ เด็กหญิงสองคนที่กลั่นแกล้งผู้เสียหายรายนี้ถูกจับกุมด้วยข้อหาสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต โดยถูกคุมขังที่เรือนจำนานเกือบสองสัปดาห์เพื่อรอการพิจารณาคดีเข้าสถานพินิจ (Detention Hearing) นับว่าเป็นการจับกุมด้วยข้อหาดังกล่าวเป็นครั้งแรกนับแต่มลรัฐเทกซัสได้บัญญัติกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตใน ค.ศ. 2009

- กรณีชายหนุ่มชาวเมืองลอสแองเจลิสคนหนึ่งได้สร้างบัญชีผู้ใช้งานเว็บไซต์เฟสบุ๊กปลอมมากถึง 130 บัญชีเพื่อคุกคามอดีตคู่รักของตน โดยใส่รูปภาพลามกและข้อมูลติดต่อของหญิงสาวไว้อย่างชัดเจน นับว่าเป็นคดีแรกภายใต้กฎหมายการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของมลรัฐแคลิฟอร์เนีย[54]

- กรณีหญิงชาวเมืองเดมอน มลรัฐเทกซัสได้เจาะระบบเข้าไปยังบัญชีผู้ใช้งานเว็บไซต์ Goodreads ของอดีตคนรักของสามีตน และสร้างหน้าเฟสบุ๊กปลอมขึ้นในนามของผู้เสียหาย ผู้กระทำผิดได้เขียนข้อความเกี่ยวกับผู้เสียหายบนเว็บไซต์ซุบซิบนินทาและส่งจดหมายอิเล็กทรอนิกส์ขู่นายจ้างของผู้เสียหายให้ไล่ผู้เสียหายออกจากงาน[55]

---

[53] Bitdefender, "Teen Girls under Arrest for Online Impersonation," [Online] Accessed: 3 November 2014. Available from: https://www.bitdefender.com/security/pre-teen-teen-girls-under-arrest-for-online-impersonation.html

[54] Ken Dowell, "Digital Deception and the Law," [Online] Accessed: 3 November 2014. Available from: http://offtheleash.net/2014/10/16/digital-deception-and-the-law/

[55] ibid.

- Joseph Cassiere ถูกอดีตเพื่อนร่วมงานสร้างบัญชีทวิตเตอร์ (Twitter) สวมรอยเป็นเขา และทำให้เขาดูเป็นคนโง่เขลาและเป็นพวกกามวิปริต เป็นเหตุให้เขาถูกไล่ออกจากงาน[56]

- ค.ศ. 2008 ณ สหราชอาณาจักร ชายคนหนึ่งถูกอดีตเพื่อนร่วมงานสวมรอยด้วยการสร้างบัญชีเฟสบุ๊กในชื่อของเขาโดยที่เขาไม่ได้ให้ความยินยอม หน้าเฟสบุ๊กดังกล่าวปรากฏข้อมูลส่วนตัวของผู้เสียหาย ไม่ว่าจะเป็นพฤติกรรมทางเพศ สถานะความสัมพันธ์ วันเกิด หรือมุมมองด้านการเมืองและศาสนา ผู้กระทำผิดในคดีนี้ถูกศาลตัดสินในข้อหาละเมิดข้อมูลส่วนบุคคล[57]

- ค.ศ. 2011 นาย Stephen Kirkham ชาวออสเตรเลียได้เข้าถึงบัญชีจดหมายอิเล็กทรอนิกส์ของเพื่อนร่วมงานชื่อนาย Cosimo Tassone และได้ส่งจดหมายอิเล็กทรอนิกส์ฉบับหนึ่งไปยังรายชื่อผู้ติดต่อของนาย Tassone โดยมีรายละเอียดของจดหมายใจความว่า “สวัสดีทุกคน แค่จะบอกว่าฉันเป็นพวกรักร่วมเพศ และฉันกำลังคนมองหาที่เป็นแบบเดียวกันเพื่อจะได้ใช้เวลาอยู่ด้วยกัน” ส่งผลให้นาย Tassone ได้รับความกระทบกระเทือนทางจิตใจเป็นอย่างมากจนไม่สามารถมาทำงานได้เป็นปี ต่อมาเขาได้ฟ้องร้องนาย Kirkham เพื่อเรียกค่าเสียหายในความผิดฐานหมิ่นประมาท มีการสู้คดีกันจนกระทั่งศาลตัดสินให้โจทก์เป็นผู้ชนะและได้รับค่าเสียหายถึง 100,000 ดอลลาร์สหรัฐ[58]

- ราชอาณาจักรเบลเยียมเคยประสบปัญหาเรื่องการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตใน ค.ศ. 2002 มีการสร้างตัวตนปลอมเพื่อใช้งานในกระดานสนทนาบนเว็บไซต์และใช้ตัวตนปลอมดังกล่าวชักชวนให้ผู้ใช้งานกระดานสนทนารายอื่นส่งข้อความเชิงเพศไปยังหมายเลขโทรศัพท์ซึ่งไม่ใช่หมายเลขของผู้กระทำผิด ศาลอาญาแห่งราชอาณาจักรเบลเยียมตัดสินว่าการใช้ตัวตนปลอมดังกล่าวเป็นการฉ้อโกงและการเฝ้าติดตาม (Fraud and Stalking) ในคดีนี้ผู้กระทำผิดถูกพิพากษารอลงอาญาเป็นเวลา 3 ปี และถูกสั่งให้จ่ายค่าเสียหายให้แก่ผู้เสียหาย

- ค.ศ. 2009 ศาลฎีกาแห่งสาธารณรัฐฝรั่งเศสได้มีคำพิพากษาในคดีที่ผู้กระทำผิดเผยแพร่ภาพเปลือยของผู้เสียหายบนระบบเครือข่ายอินเทอร์เน็ตด้วยการใช้ที่อยู่จดหมาย

---

[56] Eric Gardner, "Music Biz Agent Claims Colleague Defamed Him through Twitter Impersonation," [Online] Accessed: 9 December 2014. Available from: http://www.hollywoodreporter.com/thr-esq/music-biz-agent-claims-colleague-725219

[57] In Brief, "What Is the Law on Impersonating Another Person on Facebook?," [Online] Accessed: 9 December 2014. Available from: http://www.inbrief.co.uk/human-rights/impersonating-someone-on-facebook.htm

[58] Kelly Warner Law, "Impersonating Someone on the Internet : Legal or Illegal?," [Online] Accessed: 2 February 2015. Available from: http://kellywarnerlaw.com/impersonating-someone-on-the-internet-law/

อิเล็กทรอนิกส์ของผู้เสียหาย ผู้กระทำผิดมีความผิดตามประมวลกฎหมายอาญาฝรั่งเศส มาตรา 434-23 ฐานโจรกรรมข้อมูลอันเป็นอัตลักษณ์ส่วนบุคคล และละเมิดต่อสิทธิส่วนบุคคล[59]

- ค.ศ. 2007 ศาลประจำเมืองฮัตแวน (Hatvan) ในสาธารณรัฐฮังการีได้ตัดสินคดีเกี่ยวกับโฆษณาปลอมที่ปรากฏบนสื่อออนไลน์ ซึ่งเป็นโฆษณาเกี่ยวกับรถยนต์และบริการทางเพศ โดยมีการนำชื่อเล่นและหมายเลขโทรศัพท์ของผู้เสียหายไปประกอบสื่อโฆษณาดังกล่าว ผู้กระทำผิดทั้งสองคนมีความผิดฐานละเมิดการคุ้มครองข้อมูลส่วนบุคคลและฐานก่อกวนรังควาน ตามมาตรา 177/A แห่งประมวลกฎหมายอาญา และถูกลงโทษปรับเป็นเงินประมาณ 400 ยูโร[60]

- ผู้มีชื่อเสียงคนหนึ่งในราชอาณาจักรเนเธอร์แลนด์เคยประสบปัญหาถูกสวมรอยบนเว็บไซต์เครือข่ายสังคมออนไลน์แห่งหนึ่ง ผู้กระทำผิดได้แสดงอากัปกิริยาผ่านทางบัญชีผู้ใช้งานเว็บไซต์ในลักษณะเหมือนกันกับผู้มีชื่อเสียงคนดังกล่าวด้วยการตอบคำถามและเขียนข้อความต่าง ๆ

- อีกกรณีหนึ่งที่เคยเกิดขึ้นในราชอาณาจักรเนเธอร์แลนด์ ได้แก่ การสร้างตัวตนปลอมโดยการสมัครบัญชีจดหมายอิเล็กทรอนิกส์ด้วยชื่อของผู้เสียหาย และนำบัญชีเหล่านี้ไปใช้ซื้อโทรศัพท์เคลื่อนที่ ก่อกวนผู้อื่น และหลอกลวงฉ้อโกงผ่านทางเว็บไซต์อีเบย์หรือเว็บไซต์ซื้อขายอื่น[61]

กรณีตัวอย่างดังกล่าวข้างต้นเป็นเพียงส่วนหนึ่งของปัญหาที่เกิดขึ้นจากการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ซึ่งแสดงให้เห็นอย่างชัดเจนว่าการกระทำความผิดดังกล่าวก่อให้เกิดผลกระทบด้านลบและเป็นการละเมิดต่อชีวิต ร่างกาย สภาพจิตใจ ทรัพย์สิน ชื่อเสียง ความเป็นส่วนตัวหรือข้อมูลส่วนบุคคล การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการกระทำต่อข้อมูลแสดงอัตลักษณ์ของบุคคล เนื่องจากผู้กระทำผิดนำข้อมูลแสดงอัตลักษณ์ของบุคคลอื่นมาใช้เพื่อให้บุคคลทั่วไปเข้าใจว่าตนเป็นบุคคลที่ถูกสวมรอย จึงถือว่าเป็นการละเมิดในความเป็นตัวตน (Identity) ของผู้เสียหายอย่างร้ายแรง และเป็นการละเมิดสิทธิส่วนบุคคลและข้อมูลส่วนบุคคล เพราะเจ้าของข้อมูลส่วนบุคคลมีอำนาจโดยชอบธรรมที่จะได้รับความเป็นส่วนตัว และอยู่โดยปราศจากการถูกละเมิดหรือถูกรบกวนจากผู้อื่น ด้วยเหตุนี้ รัฐจึงจำเป็นต้องเข้ามาควบคุมดูแลและวางแนวทาง นโยบาย หรือมาตรการทางกฎหมายเพื่อคุ้มครองผู้เสียหายเหล่านี้และป้องกันปราบปราม

---

[59] Neil Robinson *et al.*, Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime : Final Report (2011), pp. 273-274.

[60] ดูคำพิพากษาคดีเพิ่มเติมได้ที่:
http://www.birosag.hu/resource.aspx?ResourceID=OITHAnonim&OEA=1004-H-BJ-2007-3&K=0 และ
http://www.birosag.hu/resource.aspx?ResourceID=OITHAnonim&OEA=0001-H-BJ-2008-138&K=0

[61] Robinson, N. *et al.*, Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime : Final Report.

การกระทำความผิดดังกล่าวด้วยการกำหนดให้การกระทำนั้นเป็นความผิดตามกฎหมายและกำหนดบทลงโทษที่เหมาะสม

อย่างไรก็ตาม รัฐจะบัญญัติให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญาและกำหนดบทลงโทษแก่ผู้กระทำความผิดได้หรือไม่นั้น จำเป็นต้องศึกษาถึงเหตุผลความจำเป็น ที่มา และขอบเขตของการกำหนดฐานความผิดและโทษทางอาญา รวมถึงแนวคิดในการคุ้มครองผู้เสียหายประกอบด้วย เพื่อมิให้เกิดปัญหาในการบังคับใช้กฎหมายอาญาที่เรียกว่า ภาวะกฎหมายอาญาเฟ้อ (Overcriminalization)

2.4 แนวคิดและหลักการทางกฎหมายอาญาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

เมื่อบุคคลใดบุคคลหนึ่งกระทำสิ่งที่เป็นการก่อความเดือดร้อนรำคาญ หรือสร้างความเสียหายต่อผู้อื่น หรือกระทบกระเทือนต่อการใช้ชีวิตอย่างปกติสุขของสมาชิกในสังคม สังคมย่อมมีวิธีการดำเนินการกับบุคคลดังกล่าวเพื่อคืนความสงบสุขให้แก่สังคม กฎหมายเป็นมาตรการที่มีบทบาทสำคัญและทรงประสิทธิภาพสำหรับการดำเนินการเช่นว่านั้น เรียกได้ว่ากฎหมายเป็นหนึ่งในกลไกควบคุมทางสังคม เพื่อจัดการกับบุคคลที่มีพฤติกรรมเบี่ยงเบนในสังคม[62] โดยเฉพาะกฎหมายอาญาซึ่งเป็นเครื่องมือสุดท้ายของกระบวนการยุติธรรมที่จะใช้ลงกับผู้กระทำความผิด การทำความเข้าใจพื้นฐานของมาตรการทางกฎหมายต่าง ๆ จะช่วยให้เข้าใจถึงความจำเป็นในการตรากฎหมายเพื่อคุ้มครองปกป้องสมาชิกในสังคมจากการกระทำผิดกฎหมาย

กฎหมายอาญา คือ กฎหมายที่บัญญัติห้ามมิให้มีการกระทำอย่างหนึ่งอย่างใด หรือบังคับให้มีการกระทำอย่างหนึ่งอย่างใด โดยผู้ที่ฝ่าฝืนหรือไม่ปฏิบัติตามจะต้องได้รับโทษ[63] กล่าวอีกนัยหนึ่งได้ว่ากฎหมายอาญาในเชิงภาษามีความหมายว่า ข้อบังคับที่บัญญัติขึ้นเกี่ยวกับการกระทำที่จะต้องถูกลงโทษ[64] ส่วนกฎหมายอาญาในเชิงเนื้อหาสาระนั้นอธิบายได้ว่า เป็นกฎหมายที่กำหนดว่าการกระทำใดจะเป็นความผิดหรือไม่ หากกระทำความผิดแล้วจะมีสภาพบังคับแก้ผู้กระทำความผิดหรือไม่อย่างไร[65] เพราะฉะนั้น กฎหมายอาญาจึงเป็นสิ่งที่รัฐใช้ควบคุมการกระทำของประชาชนเพื่อก่อให้เกิด

---

[62] คณพล จันทน์หอม, รากฐานกฎหมายอาญา (กรุงเทพมหานคร: วิญญูชน, 2558), หน้า 11.

[63] เกียรติขจร วัจนะสวัสดิ์, คำอธิบายกฎหมายอาญา ภาค 1, พิมพ์ครั้งที่ 10 (กรุงเทพมหานคร: พลสยาม พริ้นติ้ง (ประเทศไทย), 2551), หน้า 1.

[64] คณพล จันทน์หอม, รากฐานกฎหมายอาญา, หน้า 46.

[65] เรื่องเดียวกัน, หน้า 51-52.

ความสงบสุขภายในสังคม ผู้ที่ไม่ปฏิบัติตามกฎหมายอาญาย่อมต้องได้รับโทษซึ่งเป็นเครื่องมือสำคัญในการป้องปรามการกระทำความผิด

จากหลักกฎหมายทั่วไป *"Nullum crimen nulla poena sine lege"* หรือแปลเป็นไทยว่า *"ไม่มีความผิด ไม่มีโทษ หากไม่มีกฎหมาย"* นั้น เป็นหลักสากลที่ทุกประเทศยอมรับและใช้เป็นหลักสำคัญในทางกฎหมายอาญา หมายความว่า รัฐมีอำนาจลงโทษบุคคลใดได้ก็ต่อเมื่อมีกฎหมายบัญญัติให้การกระทำนั้นเป็นความผิดและได้กำหนดบทลงโทษไว้อย่างชัดแจ้ง ดังจะเห็นได้จากรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 เองก็ได้บัญญัติรับรองหลักการดังกล่าวไว้ในมาตรา 29 วรรคหนึ่งว่า *"บุคคลไม่ต้องรับโทษทางอาญา เว้นแต่ได้กระทำการอันกฎหมายที่ใช้อยู่ในเวลาที่กระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่บุคคลนั้นจะหนักกว่าโทษที่บัญญัติไว้ในกฎหมายที่ใช้อยู่ในเวลาที่กระทำความผิดมิได้"* เช่นเดียวกับมาตรา 2 แห่งประมวลกฎหมายอาญาซึ่งบัญญัติว่า *"บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการอันกฎหมายที่ใช้ในขณะกระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่ผู้กระทำความผิดนั้นต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย"*

นอกจากนี้ หลักสำคัญอีกประการหนึ่งของการใช้กฎหมายอาญา คือ กฎหมายอาญาต้องตีความโดยเคร่งครัด กล่าวคือ เมื่อมีกฎหมายกำหนดให้การกระทำหรือไม่กระทำอย่างใดอย่างหนึ่งเป็นความผิดแล้ว ถือว่าเฉพาะกรณีเช่นนั้นเท่านั้นที่เป็นความผิดและผู้กระทำความผิดต้องได้รับโทษเมื่อได้กระทำครบองค์ประกอบความผิด ไม่อาจรวมถึงกรณีอื่น ๆ ที่คล้ายคลึงกัน เนื่องจากการบังคับใช้กฎหมายอาญาที่กำหนดฐานความผิดและบทลงโทษนั้นต้องตีความตามตัวอักษร จึงไม่อาจนำบทบัญญัติทางกฎหมายที่ใกล้เคียงกันมาใช้เป็นผลร้ายต่อบุคคลได้ การตีความเคร่งครัดตามตัวอักษรเช่นนี้ย่อมทำให้กฎหมายอาญามีหลักประกันที่มั่นคงแก่บุคคลผู้อยู่ใต้บังคับแห่งกฎหมายนั้น[66]

หลักประกันในกฎหมายอาญาแบ่งออกเป็น 4 ประการดังต่อไปนี้

(1) การห้ามใช้กฎหมายจารีตประเพณีในกฎหมายอาญา

กฎหมายจารีตประเพณีเป็นกฎหมายที่เกิดจากการยึดถือปฏิบัติติดต่อกันมาอย่างยาวนานจนเป็นที่ยอมรับของผู้คนในสังคม ถือเป็นที่มาของกฎหมายแพ่งประการหนึ่ง แต่กฎหมายอาญาเป็นกฎหมายที่เกิดจากการบัญญัติ การบัญญัติกฎหมายอาญานี้เกิดจากกระบวนการนิติบัญญัติ

---

[66] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์ (กรุงเทพมหานคร: กรุงสยาม พับลิชชิ่ง, 2559), หน้า 16-19.

โดยรัฐสภาอันเป็นการแสดงออกถึงเจตจำนงของประชาชน ด้วยเหตุนี้จึงห้ามใช้กฎหมายจารีตประเพณีในการกำหนดให้การกระทำเป็นความผิดอาญา รวมทั้งการเพิ่มโทษในทางอาญาด้วย[67]

(2) การห้ามใช้กฎหมายที่ใกล้เคียงอย่างยิ่งลงโทษทางอาญาแก่บุคคล

กฎหมายอาญามีหลักเกณฑ์สำคัญคือห้ามใช้กฎหมายใกล้เคียงอย่างยิ่งในทางที่เป็นโทษแก่บุคคล การจะลงโทษทางอาญาแก่บุคคลใดบุคคลหนึ่งจำเป็นต้องให้ฝ่ายนิติบัญญัติเป็นผู้กำหนดหลักเกณฑ์ เพื่อป้องกันไม่ให้มีการนำความรู้สึกในเรื่องผิดถูกของบุคคลอันเป็นเรื่องในทางอัตตวิสัยมาใช้ลงโทษบุคคล ดังนั้นจึงต้องใช้กฎหมายอาญาเท่าที่ไม่เกินเลยขอบเขตของบทบัญญัติที่พึงหาได้จากการตีความกฎหมาย[68]

(3) กฎหมายอาญาต้องบัญญัติให้ชัดเจนแน่นอน

รัฐเป็นผู้ใช้การลงโทษทางอาญากับประชาชน รัฐจึงจำเป็นต้องบัญญัติกฎหมายอาญาให้ชัดเจนมากที่สุด เพื่อเป็นหลักประกันความแน่นอนของกฎหมายว่าตรงตามเจตนารมณ์ของฝ่ายนิติบัญญัติ และเป็นการป้องกันมิให้ผู้บังคับใช้กฎหมายทั้งหลายเลือกใช้กฎหมายตามอำเภอใจ[69]

(4) กฎหมายอาญาไม่มีผลย้อนหลัง

มาตรา 2 บัญญัติถ้อยคำว่า *"...กฎหมายที่ใช้ในขณะกระทำผิด..."* แสดงให้เห็นว่าห้ามใช้กฎหมายอาญาย้อนหลัง หากบุคคลใดบุคคลหนึ่งกระทำการใดที่ในขณะนั้นไม่มีกฎหมายกำหนดให้การกระทำนั้นมีโทษทางอาญา รัฐไม่อาจบัญญัติให้การกระทำนั้นต้องรับโทษทางอาญาย้อนหลังได้[70]

สรุปได้ว่า กฎหมายอาญาต้องประกอบขึ้นด้วย 3 สิ่ง ได้แก่ การกระทำ (Act) ความผิด (Offence) และสภาพบังคับ (Sanction)[71] ดังนั้น หากรัฐประสงค์จะใช้กฎหมายอาญาเพื่อป้องกันและปราบปรามการกระทำความผิด รัฐจำต้องพิจารณาถึงลักษณะสำคัญของกฎหมายอาญาดังกล่าวประกอบกับขอบเขตและความจำเป็นในการกำหนดให้การกระทำใดการกระทำหนึ่งเป็นความผิดอาญาและกำหนดบทลงโทษ

---

[67] คณิต ณ นคร, กฎหมายอาญาภาคทั่วไป, พิมพ์ครั้งที่ 4 (กรุงเทพมหานคร: วิญญูชน, 2554), หน้า 82.

[68] เรื่องเดียวกัน, หน้า 83-84.

[69] เรื่องเดียวกัน, หน้า 87.

[70] เรื่องเดียวกัน, หน้า 90.

[71] คณพล จันทน์หอม, รากฐานกฎหมายอาญา, หน้า 51.

ในหัวข้อนี้ ผู้เขียนจะอธิบายถึงแนวคิดและหลักการทางกฎหมายอาญาเพื่อนำมาพิจารณาว่าสมควรกำหนดมาตรการทางกฎหมายเพื่อป้องกันและปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอย่างไรต่อไป โดยแบ่งหัวข้อการอธิบายออกเป็น 3 ประเด็น ได้แก่ (1) แนวคิดเกี่ยวกับการกำหนดให้การกระทำเป็นความผิดอาญา (2) แนวคิดเกี่ยวกับมาตรการบังคับทางอาญา และ (3) แนวคิดเกี่ยวกับการคุ้มครองและเยียวยาผู้เสียหาย

2.4.1 แนวคิดเกี่ยวกับการกำหนดให้การกระทำเป็นความผิดอาญา

เมื่อมนุษย์อยู่รวมกันเป็นกลุ่มและเกิดปฏิสัมพันธ์ระหว่างกันจนกลายเป็นสังคม แต่ละสังคมย่อมต้องมีวิธีการควบคุมพฤติกรรมของสมาชิกในสังคมให้เป็นไปในแนวทางเดียวกันเพื่อให้เกิดความสงบสุขขึ้น วิธีการควบคุมพฤติกรรมของสมาชิกในสังคมมีหลากหลายวิธี การบัญญัติกฎหมายใช้บังคับพฤติกรรมของสมาชิกในสังคมนั้นเป็นวิธีการหนึ่งที่สำคัญ โดยเฉพาะการบัญญัติเป็นกฎหมายอาญา[72] เนื่องจากกฎหมายอาญาเป็นกฎหมายที่มีผลกระทบต่อสิทธิและเสรีภาพของบุคคลการพิจารณาว่าพฤติกรรมใดควรถูกควบคุมด้วยกฎหมายอาญาและกฎหมายอาญาควรมีขอบเขตในการบังคับใช้มากน้อยเพียงใดจึงเป็นสิ่งสำคัญ

เมื่อบุคคลจะกระทำสิ่งหนึ่งสิ่งใดย่อมต้องมีวัตถุประสงค์ของการกระทำนั้น การบัญญัติกฎหมายทางอาญาก็เช่นเดียวกัน ก่อนที่ผู้บัญญัติกฎหมายจะกำหนดมาตรการใด ๆ ที่มีผลในทางอาญา ผู้นั้นควรต้องคำนึงถึงวัตถุประสงค์หลักของกฎหมายอาญาดังที่ศาสตราจารย์ไนเกล วอล์กเกอร์ (Nigel Walker) ชาวอังกฤษได้ให้ความเห็นไว้ว่า การบัญญัติกฎหมายอาญานั้นต้องบรรลุวัตถุประสงค์อย่างน้อยหกประการดังนี้[73]

(1) การคุ้มครองป้องกันซึ่งตัวบุคคลหรือสัตว์จากการกระทำโดยเจตนา อันเป็นการโหดเหี้ยม ทารุณ หรือการประกอบกรรมทางเพศด้วยวิธีการอันไม่พึงประสงค์ต่าง ๆ คุ้มครองป้องกันบุคคลจากภัยบางประการอันเกิดจากการกระทำโดยไม่เจตนา คุ้มครองป้องกันกลุ่มบุคคลที่อาจถูกชักจูงให้หลงผิดได้โดยง่ายจากการทำร้าย กดขี่หรือขูดรีด อันจะเกิดแต่บุคคลหรือทรัพย์สินของบุคคลเหล่านั้น เช่น ป้องกันภัยบนท้องถนน คุ้มครองผู้เยาว์หรือผู้พิการหรือมีจิตไม่สมประกอบจากการถูกหลอกลวง เป็นต้น

(2) คุ้มครองป้องกันสภาวะจิตใจของสมาชิกในสังคมนั้น ๆ ให้รอดพ้นจากความกระทบกระเทือนจากการกระทำที่ถึงแม้ว่าจะเป็นเรื่องส่วนตัวของบุคคลที่เป็นผู้ใหญ่แล้ว และยินยอม

---

[72] อภิรัตน์ เพ็ชรศิริ, ทฤษฎีอาญา, พิมพ์ครั้งที่ 3 (กรุงเทพมหานคร: วิญญูชน, 2556), หน้า 48.

[73] เรื่องเดียวกัน, หน้า 49.

ต่อการกระทำนั้น แต่ถือว่าผิดธรรมชาติ ป้องกันการกระทำบางประเภทซึ่งเมื่อได้กระทำขึ้นท่ามกลางสาธารณชนแล้ว จะกระทบกระเทือนจิตใจบุคคลอื่นเป็นอย่างมาก รวมทั้งป้องกันพฤติกรรมบางประเภทอันอาจยั่วยุให้เกิดความไม่สงบขึ้นในหมู่ประชาชน เช่น การร่วมประเวณีในระหว่างเครือญาติ การกระทำอนาจาร การกล่าวถ้อยคำหยาบคาย เป็นต้น

(3) คุ้มครองป้องกันซึ่งทรัพย์สินส่วนบุคคลจากการลักขโมย การฉ้อโกง หรือการทำให้เสียทรัพย์ และกรณีอื่น ๆ

(4) คุ้มครองป้องกันสาธารณชนจากความไม่สะดวกสบายต่าง ๆ รวมทั้งใช้สภาพบังคับทางอาญาเพื่อเก็บรวบรวมภาษีอากร เช่น การห้ามมิให้ประชาชนมีรถยนต์หรือทรัพย์สินบางอย่างไว้ในครอบครองโดยไม่มีทะเบียน เป็นต้น

(5) เพื่อป้องกันรักษาไว้ซึ่งสถาบันทางสังคม รวมทั้งเพื่อบังคับให้เกิดความเมตตากรุณาที่จำเป็น เช่น รักษาไว้ซึ่งสถาบันพระมหากษัตริย์ ลงโทษผู้ที่งดเว้นไม่ช่วยเหลือผู้ที่ตกอยู่ในภยันตราย เป็นต้น

(6) เพื่อบังคับใช้วิธีการต่าง ๆ ที่จะทำให้วัตถุประสงค์ทั้งหลายเหล่านี้บรรลุผล เช่น ลงโทษผู้ที่ขัดขวางการปฏิบัติหน้าที่ของเจ้าพนักงานหรือผู้ที่ให้การเป็นเท็จ เป็นต้น

จากแนวคิดทั้ง 6 ประการข้างต้นจะเห็นได้ว่า กฎหมายอาญามีวัตถุประสงค์สำคัญคือการปกป้องคุ้มครองสิทธิและเสรีภาพของสมาชิกในสังคมมิให้ถูกล่วงละเมิดไม่ว่าด้วยวิธีใดเพื่อปกป้องไว้ซึ่งการอยู่ร่วมกันอย่างผาสุก มีความปลอดภัยในชีวิต ร่างกาย ทรัพย์สิน และอื่นๆ อีกทั้งยังประสงค์ให้การดำเนินงานของเจ้าหน้ารัฐเป็นไปอย่างมีประสิทธิภาพและเกิดประสิทธิผลอีกด้วย

อย่างไรก็ตาม กฎหมายอาญาเป็นมาตรการทางกฎหมายที่มีความรุนแรงที่สุด เพราะผู้ที่ฝ่าฝืนกฎหมายอาญาจะต้องถูกจำกัดสิทธิและเสรีภาพบางประการ เช่น นักโทษที่ถูกจำคุกย่อมเสียเสรีภาพในการเดินทาง เป็นต้น ดังนั้นการนำกฎหมายอาญามาใช้บังคับจึงต้องใช้อย่างระมัดระวัง ใช้เฉพาะกับสถานการณ์ที่เหมาะสมและจำเป็นเนื่องจากไม่อาจมีวิธีการอื่นใดที่จะแก้ไขปัญหาได้เหมาะสมเท่ากฎหมายอาญาอีกแล้ว ด้วยเหตุดังกล่าวนักอาชญาวิทยาหลายท่านจึงวางหลักเกณฑ์ข้อจำกัดในการใช้กฎหมายอาญาไว้หลายประการ สรุปพอสังเขปได้ดังต่อไปนี้[74]

(1) กฎหมายอาญานั้นไม่ควรรวมเอาไว้ซึ่งข้อห้ามที่มีจุดประสงค์เพียงเพื่อให้บุคคลเชื่อฟัง และผลของการไม่เชื่อฟังคือผลร้ายในทางแก้แค้นตอบแทนเท่านั้น

(2) ไม่ควรนำกฎหมายอาญามาใช้เพื่อลงโทษพฤติกรรมที่ปราศจากพิษภัย

---

[74] อภิรัตน์ เพ็ชรศิริ, ทฤษฎีอาญา, หน้า 51-62.

(3) ไม่ควรใช้กฎหมายอาญาเพื่อเป็นวิธีการที่นำไปสู่จุดประสงค์ที่สามารถทำให้บรรลุถึงซึ่งจุดประสงค์เช่นเดียวกันนั้น ด้วยวิธีการอื่นที่ทำให้เกิดความทุกขเวทนาน้อยกว่า

(4) ไม่ควรนำกฎหมายอาญามาใช้ เมื่อผลร้ายที่เกิดจากการกระทำผิดนั้นน้อยกว่าผลร้ายที่เกิดจากการลงโทษ

(5) ไม่ควรนำกฎหมายอาญามาใช้ เพื่อจุดประสงค์ที่จะบังคับให้บุคคลประพฤติปฏิบัติตามแนวทางที่จะนำให้เกิดผลประโยชน์แก้ผู้ปฏิบัตินั้นเอง

(6) กฎหมายอาญาไม่ควรรวมไว้ซึ่งข้อห้ามที่ไม่ได้รับการสนับสนุนอย่างจริงจังจากมติมหาชน

(7) กฎหมายอาญาไม่ควรรวมเอาไว้ซึ่งข้อห้ามที่บังคับใช้ไม่ได้

(8) กฎหมายอาญาไม่ควรรวมเอาไว้ซึ่งข้อห้ามบางประการ ซึ่งเมื่อมีการละเมิดข้อห้ามนั้นแล้ว ไม่สามารถพิสูจน์ได้ว่ามีการกระทำความผิดเกิดขึ้นจริง

กล่าวโดยสรุป กฎหมายอาญาเป็นเครื่องมือควบคุมพฤติกรรมของสมาชิกในสังคมให้เป็นไปในทางเดียวกัน เพื่อคุ้มครองป้องกันมิให้เกิดการละเมิดสิทธิและเสรีภาพอันชอบธรรมของแต่ละบุคคล การบัญญัติให้การกระทำใดเป็นความผิดทางอาญาจึงต้องตอบสนองต่อวัตถุประสงค์ของกฎหมายอาญา และต้องไม่เป็นบทบัญญัติที่ขัดต่อหลักเกณฑ์ในการบังคับใช้กฎหมายอาญาอีกด้วย

เมื่อพิจารณาแนวคิดเกี่ยวกับการกำหนดให้การกระทำเป็นความผิดอาญาแล้ว จะเห็นได้ว่าการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการกระทำโดยเจตนาเพื่อละเมิดสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลของผู้ถูกสวมรอยและก่อให้เกิดความเสียหายหลายประการ โดยเฉพาะต่อสภาพจิตใจและชื่อเสียงของผู้ถูกสวมรอย เป็นเหตุให้ไม่สามารถมีความเป็นอยู่เหมือนเช่นปกติดังเดิม นอกจากนี้ยังอาจก่อให้เกิดความไม่สงบสุขขึ้นในสังคม เนื่องมาจากการกระทำความผิดผ่านทางเครือข่ายอินเทอร์เน็ตย่อมส่งผลกระทบกระจายไปในวงกว้าง ดังนั้นจึงควรกำหนดให้การกระทำดังกล่าวเป็นความผิดทางอาญา เพื่อให้ผู้เสียหายได้รับการคุ้มครองตามกฎหมายและเป็นเครื่องมือให้กับเจ้าหน้าที่รัฐในการป้องกันและปราบปรามการกระทำความผิดดังกล่าวอีกประการหนึ่ง

2.4.2 แนวคิดเกี่ยวกับมาตรการบังคับทางอาญา

เมื่อมีการกระทำใดการกระทำหนึ่งที่กฎหมายกำหนดให้เป็นความผิดอาญาเกิดขึ้นย่อมต้องมีสภาพบังคับลงแก่ผู้ที่กระทำความผิดนั้น สภาพบังคับในที่นี้หมายถึง มาตรการบังคับทางอาญา

อันประกอบด้วย โทษ วิธีการเพื่อความปลอดภัย และมาตรการบังคับอย่างอื่น[75] มาตรการบังคับทางอาญาที่สำคัญที่สุด คือ การลงโทษ อันเป็นการกระทำที่ส่งผลร้ายแก่ผู้ที่ต้องรับโทษ ซึ่งอาจจะเป็นผลร้ายต่อร่างกาย จิตใจ หรือทรัพย์สิน[76] ในอดีตมีนักคิดนักปรัชญาหลายท่านได้เสนอแนวความคิดเกี่ยวกับการลงโทษไว้หลายประการ ผู้เขียนจะขอยกตัวอย่างแนวคิดเกี่ยวกับการลงโทษที่สำคัญพอสังเขป ดังนี้[77]

เบคคาเรีย (Beccaria) มีความเห็นว่า การลงโทษต้องไม่มีวัตถุประสงค์เพื่อการแก้แค้น โทษที่จะลงแก่ผู้กระทำผิดต้องเหมาะสมตามลักษณะความผิด ควรกำหนดลักษณะของโทษ ประเภทของโทษ และความหนักเบาของโทษไว้ให้แน่นอน โดยถือหลักการเสมอภาคเท่าเทียมกัน และควรพิจารณากำหนดโทษและลงโทษอย่างเปิดเผย

เจเรมี เบนธัม (Jeremy Bentham) เสนอแนวคิดว่า ควรกำหนดโทษให้สาสมกับความผิด ก่อให้เกิดความเข็ดหลาบ อันจะเป็นเหตุให้คนทั่วไปเกรงกลัวไม่กล้ากระทำผิดตามอย่างจึงเป็นการป้องกันอาชญากรรมอีกทางหนึ่ง ส่วนการกำหนดโทษนั้นไม่ควรกำหนดโทษสำหรับแต่ละความผิดไว้ตายตัว แต่ควรให้ศาลเป็นผู้พิจารณากำหนดโทษให้เหมาะสมเป็นราย ๆ ไป

ต่อมา นักอาชญาวิทยาได้เปลี่ยนแนวคิดและทฤษฎีการลงโทษ โดยเน้นที่การป้องกันอาชญากรรมมากกว่าการแก้แค้นทดแทน ดังเช่นที่ Karl O. Christiansen นักอาชญาวิทยาได้ให้ความเห็นเกี่ยวกับการลงโทษเพื่อป้องกันอาชญากรรมไว้มีสาระสำคัญหลายประการ กล่าวคือ ประการแรก การป้องกันคือจุดมุ่งหมายของการลงโทษและเป็นหนทางสำหรับการสร้างสวัสดิภาพในสังคม ประการที่สอง การละเมิดกฎหมายเป็นเหตุให้ผู้ละเมิดต้องได้รับโทษตามสมควรแก่เหตุ ไม่ว่าจะกระทำไปโดยจงใจหรือประมาทเลินเล่อก็ตาม ประการสุดท้าย การกำหนดโทษมีขึ้นเพื่อประโยชน์ในการป้องกันอาชญากรรม[78]

การลงโทษนั้นมีขึ้นเพื่อวัตถุประสงค์หลายประการดังต่อไปนี้

(1) เพื่อแก้แค้นทดแทน (Retribution)

การลงโทษลักษณะนี้เกิดจากหลักการที่ว่า เมื่อผู้ใดกระทำความผิดหรือกระทำให้ผู้อื่นเดือดร้อนเสียหาย ผู้นั้นต้องถูกลงโทษให้สาสมกับความผิดที่ได้ก่อไว้ เรียกกันทั่วไปว่าเป็นหลัก ตา

---

[75] คณพล จันทน์หอม, รากฐานกฎหมายอาญา, หน้า 51.

[76] อัจฉรียา ชูตินันทน์, อาชญาวิทยาและทัณฑวิทยา, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร: วิญญูชน, 2557), หน้า 130.

[77] ประเทือง ธนิยผล, อาชญาวิทยาและทัณฑวิทยา (กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยรามคำแหง, 2556), หน้า 135.

[78] เรื่องเดียวกัน, หน้า 137.

ต่อตา ฟันต่อฟัน กล่าวคือ หากความผิดเป็นการกระทำที่รุนแรงโหดร้าย ผู้กระทำผิดต้องได้รับผลตอบแทนด้วยการลงโทษที่ทารุณโหดร้ายเช่นกัน แต่ปัจจุบันหลักการลงโทษเพื่อแก้แค้นทดแทนได้เปลี่ยนแปลงไปตามวิวัฒนาการของสังคม จากเดิมที่ใช้วิธีการลงโทษที่ทารุณต่อเนื้อตัวร่างกายก็เปลี่ยนเป็นโทษจำคุกตามความหนักเบาของความผิดแทน[79]

(2) เพื่อยับยั้งการกระทำความผิด (Deterrence)

เมื่อผู้กระทำความผิดถูกลงโทษ ผู้คนในสังคมย่อมเกิดความเกรงกลัวไม่กล้ากระทำความผิด เนื่องจากได้รับรู้ผลแห่งการฝ่าฝืนกฎหมายอย่างเป็นรูปธรรมแล้ว จึงเกิดความตระหนักรู้ถึงโทษของการกระทำผิด รวมทั้งเกิดความกลัวว่าถ้าตนลงมือกระทำผิดไป สังคมจะไม่ยอมรับ และกลัวที่จะถูกจับไปลงโทษ[80] ดังนั้น การลงโทษจึงมีส่วนช่วยยับยั้งทั้งการกระทำความผิดซ้ำของผู้กระทำผิดและการกระทำความผิดของผู้อื่นในอนาคตอีกด้วย

(3) เพื่อตัดผู้กระทำความผิดออกจากสังคม (Incapacitation)

เนื่องจากผู้กระทำความผิดเป็นภัยร้ายของสังคม การกระทำผิดของบุคคลหนึ่งย่อมส่งผลกระทบต่อความสงบสุขของผู้คนในสังคมไม่มากก็น้อย การกันตัวผู้กระทำผิดออกจากสังคมเป็นการชั่วคราวหรือถาวรจะทำให้สังคมปลอดภัยมากยิ่งขึ้น สมาชิกในสังคมพึงพอใจที่ผู้กระทำผิดได้รับการลงโทษ และเป็นการตัดโอกาสหรือจำกัดความสามารถในการกระทำผิด การตัดผู้กระทำความผิดออกจากสังคมมีได้หลายวิธี เช่น ประหารชีวิต จำคุก กักขัง[81]

(4) เพื่อแก้ไขผู้กระทำความผิด (Rehabilitation and Correction)

การลงโทษเพื่อแก้ไขผู้กระทำความผิดมุ่งเน้นให้ผู้กระทำผิดรู้สำนึกและปรับเปลี่ยนแนวคิด ทัศนคติ ตลอดจนรูปแบบการดำรงชีวิต เพื่อให้ผู้กระทำผิดเมื่อพ้นโทษแล้วจะไม่กลับไปกระทำผิดอีก โดยผู้กระทำผิดจะได้รับการอบรม แก้ไขฟื้นฟูทั้งร่างกายและจิตใจ ฝึกอาชีพ เพื่อให้ผู้กระทำผิดสามารถกลับสู่สังคมได้ในที่สุด

(5) เพื่อป้องกันอาชญากรรม (Prevention of Crime)

การลงโทษผู้กระทำผิดเป็นไปตามกฎระเบียบของสังคม ทำให้สังคมเกิดความปลอดภัย ป้องกันมิให้เกิดการกระทำผิดซ้ำหรือการกระทำผิดอื่นในอนาคต เนื่องจากสมาชิกในสังคม

---

[79] เรื่องเดียวกัน, หน้า 138.

[80] Gerald Gardiner, "The Purpose of Criminal Punishment," The Modern Law Review 21, 3 (1958).

[81] ประเทือง ธนิยผล, อาชญาวิทยาและทัณฑวิทยา, หน้า 138.

เห็นตัวอย่างของการฝ่าฝืนกฎหมายแล้วจึงไม่กล้าเอาเยี่ยงอย่าง[82] ดังนั้น การลงโทษที่เหมาะสมจะทำให้อัตราการเกิดอาชญากรรมในสังคมลดลง

กล่าวโดยสรุป การลงโทษเป็นวิธีการปฏิบัติต่อผู้กระทำผิดในลักษณะที่เป็นผลร้ายต่อผู้กระทำผิด โดยมีแนวคิดและวัตถุประสงค์สำคัญเพื่อก่อให้เกิดความสงบสุขในสังคม เพราะการลงโทษมีขึ้นเพื่อยับยั้งมิให้ผู้กระทำผิดกลับไปกระทำผิดซ้ำ ทำให้สมาชิกอื่นในสังคมเกิดความเกรงกลัวไม่กล้าเอาเยี่ยงอย่าง ก่อให้เกิดความปลอดภัยขึ้นในสังคม ป้องกันการเกิดอาชญากรรม และยังเป็นการแก้ไขฟื้นฟูผู้กระทำผิดให้มีโอกาสกลับตัวและสามารถกลับคืนสู่สังคมได้หลังพ้นโทษ

อนึ่ง นอกเหนือจากโทษจะเป็นมาตรการบังคับที่เป็นหลักในกฎหมายอาญาแล้วยังมีมาตรการบังคับอื่นอีก 2 มาตรการ ได้แก่ วิธีการเพื่อความปลอดภัยและมาตรการบังคับทางอาญาอย่างอื่น ซึ่งทั้งสองมาตรการนี้ต่างก็มีวัตถุประสงค์สำคัญเพื่อปกป้องสังคมโดยรวมให้อยู่ในความสงบเรียบร้อย ปลอดภัย และคุ้มครองและรักษาสิทธิของปัจเจกชน[83]

ด้วยเหตุผลดังกล่าวข้างต้น หากมีการกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดทางอาญาแล้วก็สมควรกำหนดมาตรการบังคับทางอาญาที่เหมาะสมกับฐานความผิดดังกล่าวด้วยเช่นกัน ทั้งนี้ ควรกำหนดมาตรการบังคับที่มีวัตถุประสงค์ในการยับยั้งและป้องกันมิให้เกิดการกระทำความผิดเช่นนี้ขึ้นอีกในสังคม บทลงโทษต้องรุนแรงมากพอที่จะทำให้ผู้กระทำความผิดหรือผู้ที่คิดจะกระทำความผิดเกรงกลัวไม่กล้ากระทำความผิดซ้ำ รวมทั้งควรมีมาตรการบังคับทางอาญาอย่างอื่น เช่น การคุมประพฤติ หรือคำสั่งห้ามกระทำการใด ๆ ที่เป็นการล่วงละเมิด เพื่อเป็นหลักประกันความปลอดภัยแก่สิทธิส่วนบุคคลและข้อมูลส่วนบุคคลของประชาชนทุกคนต่อไป

2.4.3 แนวคิดเกี่ยวกับการคุ้มครองและเยียวยาผู้เสียหาย

ตามทฤษฎีอาชญาวิทยาด้านผู้เสียหาย (Victimology) นั้น ผู้เสียหายหรือเหยื่ออาชญากรรม หมายความถึง บุคคลที่ได้รับผลกระทบจากการกระทำความผิด โดยทั่วไปความผิดที่ส่งผลกระทบต่อบุคคลใดบุคคลหนึ่งเป็นการเฉพาะคือการกระทำที่เป็นความผิดอยู่ในตัวเอง หรือ *mala inse* มักเป็นความผิดที่ก่อให้เกิดความเสียหายหรือล่วงละเมิดต่อชีวิต ร่างกาย เสรีภาพ ชื่อเสียง หรือทรัพย์สินของผู้อื่น ผู้ใดที่ได้รับผลกระทบจากการกระทำนี้อาจเป็นผู้เสียหายได้ แต่อย่างไรก็ตาม ยังมีความผิดอีกประเภทหนึ่งเรียกว่า ความผิดที่กฎหมายห้าม หรือ *mala prohibita* ซึ่งส่วนมากมักเป็นความผิดที่รัฐ

---

[82] เรื่องเดียวกัน, หน้า 139.

[83] คณพล จันทน์หอม, รากฐานกฎหมายอาญา, หน้า 53.

เป็นผู้เสียหาย ดังนั้นผู้เสียหายจึงอาจมีได้หลายลักษณะขึ้นอยู่กับว่ากฎหมายได้กำหนดลักษณะของการกระทำความผิดไว้เพื่อคุ้มครองฝ่ายใด

ประมวลกฎหมายวิธีพิจารณาความอาญาได้ให้ความหมายของ “ผู้เสียหาย” ไว้ในมาตรา 2 (4) ว่า *“ผู้เสียหาย หมายถึง บุคคลผู้ได้รับความเสียหายเนื่องจากการกระทำผิดฐานใดฐานหนึ่ง รวมทั้งบุคคลอื่นที่มีอำนาจจัดการแทนได้ ดังบัญญัติไว้ในมาตรา 4, 5 และ 6”* ดังนี้จะเห็นได้ว่าหลักเกณฑ์สำคัญของการเป็นผู้เสียหาย ไม่ว่าผู้เสียหายจะเป็นรัฐหรือเอกชนก็ตาม ได้แก่ มีการกระทำที่กฎหมายบัญญัติว่าเป็นความผิดเกิดขึ้น ผู้เสียหายต้องเป็นบุคคลที่ได้รับความเสียหายโดยตรงจากการกระทำความผิดนั้น และต้องเป็นผู้เสียหายโดยนิตินัย

การพิจารณาว่าบุคคลใดจะเป็นผู้เสียหายโดยตรงหรือไม่ต้องพิจารณาว่า สิทธิที่กฎหมายรับรองและคุ้มครองของบุคคลนั้นถูกกระทบหรือเกิดความเสียหายเนื่องมาจากการกระทำความผิดหรือไม่[84] กรณีเช่นนี้ต้องพิจารณาจากกฎหมายที่บัญญัติฐานความผิดไว้ว่า การที่กฎหมายบัญญัติเช่นนั้นมีขึ้นเพื่อคุ้มครองผู้ใด เนื่องจากเบื้องหลังของบทบัญญัติฐานความผิดแต่ละบทบัญญัติล้วนมีสิ่งที่กฎหมายประสงค์จะคุ้มครอง เป็นสภาพพึงปรารถนาที่กฎหมายต้องการคุ้มครองมิให้ถูกล่วงละเมิด เรียกว่า “คุณธรรมทางกฎหมาย” (Rechtsgut)[85] ซึ่งคุณธรรมทางกฎหมายนี้แตกต่างจากกรรมของการกระทำความผิด เช่น ความผิดฐานพรากผู้เยาว์มีขึ้นเพื่อคุ้มครองสิทธิในการปกครองผู้เยาว์ของบิดามารดาหรือผู้ปกครอง คุณธรรมทางกฎหมายของความผิดฐานนี้คือสิทธิในการปกครองผู้เยาว์ ส่วนกรรมของการกระทำความผิดคือผู้เยาว์ที่ถูกพรากไป ความผิดฐานลักทรัพย์มีขึ้นเพื่อคุ้มครองเจ้าของกรรมสิทธิ์หรือผู้ครอบครอง ส่วนกรรมของการกระทำคือตัวทรัพย์ที่ถูกลักไป เป็นต้น

ในกรณีที่ผู้กระทำผิดได้กระทำความผิดหลายฐานต่อเนื่องกัน ผู้เสียหายในฐานความผิดต่าง ๆ อาจเป็นคนละคนกันได้ ขึ้นอยู่กับว่าคุณธรรมทางกฎหมายมุ่งคุ้มครองบุคคลใด ดังนั้นในคดีที่มีข้อเท็จจริงซับซ้อนจึงต้องแยกพิจารณาการเป็นผู้เสียหายตามความผิดแต่ละฐานไป[86] นอกจากนี้ยังต้องพิจารณาด้วยว่า ในขณะความผิดเกิดขึ้น บุคคลใดที่เป็นผู้เสียหายที่แท้จริงด้วยการพิจารณาว่าคุณธรรมทางกฎหมายของความผิดฐานนั้นมุ่งประสงค์จะคุ้มครองบุคคลใด[87]

---

[84] อุทัย อาทิเวช, คู่มือกฎหมายวิธีพิจารณาความอาญา เล่ม 2 สิทธิของผู้เสียหายในคดีอาญา, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร: วี.เจ.พริ้นติ้ง, 2555), หน้า 17.

[85] คณิต ณ นคร, วิ.อาญาวิพากษ์ (กรุงเทพมหานคร: วิญญูชน, 2552), หน้า 46.

[86] ธานิศ เกศวพิทักษ์, คำอธิบายประมวลกฎหมายวิธีพิจารณาความอาญา ภาค 1-2 (มาตรา 1-156), พิมพ์ครั้งที่ 10 (กรุงเทพมหานคร: กรุงสยาม พับลิชชิ่ง, 2556), หน้า 16-18.

[87] เรื่องเดียวกัน, หน้า 28.

การพิจารณาว่าผู้ใดเป็นผู้เสียหายจากการกระทำความผิดอาญาต้องพิจารณาเป็นขั้นตอนดังนี้ ประการแรก พิจารณาว่าคุณธรรมทางกฎหมายของความผิดอาญาฐานนั้นคืออะไร ประการที่สอง พิจารณาว่าคุณธรรมทางกฎหมายนั้นเป็นคุณธรรมทางกฎหมายที่เป็นส่วนรวมหรือเอกชน กล่าวคือ คุณธรรมทางกฎหมายที่เป็นส่วนรวม เช่น ความปลอดภัยของจราจร การรักษาความลับทางการทหาร เป็นต้น ส่วนคุณธรรมทางกฎหมายที่เป็นส่วนเอกชน เช่น ชีวิต เสรีภาพ กรรมสิทธิ์ เป็นต้น[88] ประการที่สาม ในกรณีที่เป็นคุณธรรมทางกฎหมายที่เป็นส่วนเอกชน จำต้องพิจารณาว่าใครเป็นเจ้าของคุณธรรมทางกฎหมายนั้น เพราะฉะนั้น ผู้ใดที่ถูกล่วงละเมิดคุณธรรมทางกฎหมายอันเนื่องมาจากการกระทำความผิดอาญา ผู้นั้นคือผู้เสียหายในฐานความผิดอาญานั้น[89]

จากแนวทางการพิจารณาประเด็นเรื่องผู้เสียหายดังกล่าวข้างต้น สามารถนำมาพิจารณาเรื่องผู้เสียหายในความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตได้ดังนี้

(1) คุณธรรมทางกฎหมายของความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต คือ สิทธิในความเป็นตัวตน (Right to Identity) ซึ่งเป็นหนึ่งในสิทธิส่วนบุคคลขั้นพื้นฐานที่มนุษย์ทุกคนได้รับมาตั้งแต่เกิด รวมถึงสิทธิส่วนบุคคล (Right to Privacy) ที่จะไม่ถูกแทรกแซงจากบุคคลอื่น หากผู้ใดถูกนำส่วนใดส่วนหนึ่งในความเป็นตัวตนของเขาไปกระทำการบิดเบือนข้อเท็จจริงออกสู่สาธารณะ หรือถูกนำความเป็นตัวตนไปใช้เพื่อหาประโยชน์ใส่ตัวผู้กระทำความผิดโดยไม่ได้รับความยินยอมจากเจ้าของตัวตนนั้น ย่อมเป็นการล่วงละเมิดสิทธิในความเป็นตัวตนและสิทธิส่วนบุคคลอย่างยิ่ง[90]

(2) สิทธิในความเป็นตัวตนอยู่ภายใต้หลักสิทธิส่วนบุคคลซึ่งเป็นสิทธิมนุษยชนขั้นพื้นฐานที่มนุษย์ทุกคนพึงมี ดังนั้น คุณธรรมทางกฎหมายของความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตจึงเป็นคุณธรรมทางกฎหมายที่เป็นส่วนเอกชน

(3) ความเป็นตัวตน (identity) ทำให้บุคคลแต่ละคนมีอัตลักษณ์ที่แตกต่างกันไป ประกอบกับแต่ละบุคคลมีสิทธิที่จะปกป้องตนเองจากการถูกเปิดเผยเรื่องส่วนตัวอย่างไม่เคารพและทำให้อับอาย รวมถึงการถูกนำชื่อหรือสิ่งที่บ่งบอกถึงความเป็นตัวตนของบุคคลนั้นไปใช้ประโยชน์[91]

---

[88] คณิต ณ นคร, วิ.อาญาวิพากษ์, หน้า 47.

[89] เรื่องเดียวกัน, หน้า 49.

[90] David Luyt, "Liability for Impersonating Someone Online," [Online] Accessed: 25 April 2017. Available from: https://www.michalsons.com/blog/liability-impersonating-someone-online/9696

[91] นคร เสรีรักษ์, ความเป็นส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 38.

ดังนั้น เจ้าของคุณธรรมทางกฎหมายอันได้แก่สิทธิในความเป็นตัวตนและสิทธิในความเป็นส่วนตัว คือ ผู้ที่ถูกสวมรอยบนเครือข่ายอินเทอร์เน็ตนั่นเอง

สรุปได้ว่า การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเกิดขึ้นจากการนำข้อมูลส่วนบุคคลที่สามารถใช้ระบุตัวตนของบุคคลอื่นไปใช้เพื่อการแอบอ้างสวมรอย โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล และเป็นการใช้ความเป็นตัวตนของบุคคลอื่นเพื่อให้ได้มาซึ่งประโยชน์อันมิควรได้โดยชอบด้วยกฎหมายหรือเพื่อเจตนาประสงค์ร้ายอื่น ๆ การกระทำเช่นนี้ย่อมเป็นการละเมิดสิทธิในความเป็นตัวตนและสิทธิในความเป็นส่วนตัวอันเป็นคุณธรรมทางกฎหมายของผู้ถูกสวมรอย ด้วยเหตุนี้ ผู้ถูกสวมรอยจึงเป็นผู้เสียหายในความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

แต่อย่างไรก็ตาม การสวมรอยเป็นบุคคลอื่นดังกล่าวหากก่อให้เกิดความเสียหายต่อคุณธรรมทางกฎหมายในความผิดฐานอื่น ๆ ที่เกี่ยวข้อง ย่อมถือได้ว่าเจ้าของคุณธรรมทางกฎหมายนั้นเป็นผู้เสียหายด้วยเช่นกัน ตัวอย่างเช่น หากมีการสวมรอยเป็นบุคคลอื่นผ่านทางเว็บไซต์ซื้อขายสินค้าบนระบบอินเทอร์เน็ต เพื่อกระทำความผิดฐานฉ้อโกง ความผิดฐานฉ้อโกงมีสิทธิในทรัพย์เป็นคุณธรรมทางกฎหมาย ดังนั้นผู้ที่ถูกหลอกลวงและสูญเสียสิทธิในทรัพย์ไปจึงเป็นผู้เสียหายในความผิดฐานฉ้อโกงโดยการแสดงตนเป็นคนอื่น เป็นต้น

กล่าวโดยสรุป จากทฤษฎีและแนวคิดเกี่ยวกับการกำหนดฐานความผิดทางอาญา การกำหนดบทลงโทษ และการคุ้มครองเยียวยาผู้เสียหายดังกล่าวข้างต้น ผู้ที่ถูกนำข้อมูลแสดงอัตลักษณ์ส่วนบุคคลไปใช้เพื่อการสวมรอยแสดงตัวตนเป็นผู้นั้นโดยมีจุดประสงค์ในการก่อให้เกิดความเสียหายใด ๆ ย่อมเป็นการละเมิดสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลซึ่งเป็นสิทธิมนุษยชนขั้นพื้นฐานที่ได้รับการคุ้มครองตามกฎหมาย ผู้นั้นจึงเป็นผู้เสียหายจากการกระทำดังกล่าว ด้วยเหตุนี้จึงสมควรกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดทางอาญาและกำหนดบทลงโทษที่เหมาะสมเพื่อยับยั้งและป้องกันมิให้เกิดการกระทำความผิดเช่นนี้ขึ้นอีก อันเป็นการคุ้มครองปกป้องความสงบสุขของปัจเจกชนและสังคมโดยรวม

บทที่ 3
มาตรการทางอาญาที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทย

ในบทที่ผ่านมาเราได้ศึกษาเกี่ยวกับแนวคิดและหลักการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ทำให้ทราบว่าการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการกระทำที่ล่วงละเมิดต่อสิทธิในความเป็นตัวตน (Right to Identity) และสิทธิส่วนบุคคล (Right to Privacy) และสร้างความเสียหายต่อบุคคลผู้ถูกสวมรอยและบุคคลอื่นได้หลากหลายแง่มุม สมควรที่ต้องนำหลักการทางกฎหมายอาญาเข้ามาพิจารณาเพื่อให้ทราบว่าควรกำหนดให้การกระทำดังกล่าวเป็นความผิดและกำหนดมาตรการบังคับทางอาญาอย่างเหมาะสม

ในบทที่ 3 นี้ ผู้เขียนจะอธิบายถึงมาตรการทางอาญาที่มีอยู่ในปัจจุบันของประเทศไทยซึ่งเกี่ยวข้องการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต โดยแบ่งเป็น (1) กฎหมายที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตตามประมวลกฎหมายอาญา (2) กฎหมายที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตตามพระราชบัญญัติอื่น และ (3) สภาพปัญหาในประเทศไทย เพื่อแสดงให้เห็นถึงความคล้ายคลึงและความแตกต่างขององค์ประกอบความผิด สภาพปัญหาและผลกระทบที่ผู้เสียหายได้รับ ตลอดจนเจตนารมณ์ของการบัญญัติกฎหมายที่มุ่งแก้ไขปัญหาช่องว่างทางกฎหมายที่เกิดขึ้น

3.1 กฎหมายที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตตามประมวลกฎหมายอาญา

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตมีลักษณะการกระทำที่อาจเกิดขึ้นได้หลายรูปแบบ ขึ้นอยู่กับวัตถุประสงค์ของผู้สวมรอย เช่น สวมรอยเป็นบุคคลที่มีชื่อเสียงเพื่ออาศัยชื่อเสียงนั้นหลอกลวงเอาทรัพย์สินของผู้อื่น หรือสวมรอยเป็นบุคคลอื่นเพื่อนำความเป็นตัวตนของบุคคลนั้นไปแสดงพฤติกรรมที่ไม่เหมาะสม เป็นเหตุให้เจ้าของตัวตนเสื่อมเสียชื่อเสียง เป็นต้น รูปแบบที่หลากหลายของการสวมรอยเช่นนี้จึงอาจเกี่ยวโยงกับลักษณะของการกระทำความผิดตามที่บัญญัติไว้ในประมวลกฎหมายอาญาได้หลายฐานความผิด ในหัวข้อนี้ ผู้เขียนจะอธิบายถึงฐานความผิดอาญาที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต โดยแบ่งเป็น 3 ฐานความผิด ได้แก่ (1) ความผิดฐานหมิ่นประมาท (2) ความผิดฐานฉ้อโกง และ (3) ความผิดฐานปลอมเอกสาร

3.1.1 ความผิดฐานหมิ่นประมาท

มนุษย์ทุกคนเกิดมาพร้อมกับศักดิ์ศรีความเป็นมนุษย์ (Human Dignity) อย่างเท่าเทียมกัน อีกทั้งแต่ละรัฐยังมีการสร้างหลักประกันศักดิ์ศรีความเป็นมนุษย์ของพลเมืองด้วยการตราไว้เป็นกฎหมาย ประเทศไทยมีบทบัญญัติคุ้มครองศักดิ์ศรีความเป็นมนุษย์ตามมาตรา 4 แห่งรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ความว่า *"ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาคของบุคคลย่อมได้รับการคุ้มครอง ปวงชนชาวไทยย่อมได้รับความคุ้มครองตามรัฐธรรมนูญเสมอกัน"* ทั้งนี้ "เกียรติ" ถือเป็นส่วนหนึ่งของศักดิ์ศรีความเป็นมนุษย์ในแต่ละบุคคล ซึ่งบุคคลอื่นต้องให้ความเคารพ และจำเป็นต้องได้รับความคุ้มครองตามกฎหมาย เนื่องจากเกียรติเป็นคุณค่าพื้นฐานของมนุษย์ทุกคนจึงถือเป็นคุณธรรมทางกฎหมายประการหนึ่งในกฎหมายอาญา[1] ด้วยเหตุนี้ การล่วงละเมิดเกียรติของบุคคลอื่นเป็นการทำให้คุณค่าที่จะได้รับการยอมรับนับถือลดน้อยลง จึงเป็นสิ่งที่ไม่อาจให้อภัยและต้องมีมาตรการลงโทษผู้กระทำละเมิด ทั้งนี้ ความผิดฐานหมิ่นประมาทเป็นการกระทำความผิดลักษณะหนึ่งอันเป็นการล่วงละเมิดและสร้างความเสียหายต่อชื่อเสียงเกียรติคุณของบุคคลอื่น ประเทศไทยได้กำหนดให้การกระทำดังกล่าวเป็นความผิดตามประมวลกฎหมายอาญา ดังนี้

"มาตรา 326 ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สาม โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ"

ความผิดฐานหมิ่นประมาทเป็นการกระทำความผิดที่มีบุคคลเกี่ยวข้องกัน 3 ฝ่าย ได้แก่ ผู้กระทำความผิด ผู้ที่ถูกใส่ความ และผู้รับทราบข้อความหมิ่นประมาท ผู้กระทำการหมิ่นประมาทและผู้ที่ถูกใส่ความอาจเป็นได้ทั้งบุคคลธรรมดาหรือนิติบุคคลซึ่งมีสภาพบุคคลอยู่ในขณะที่เกิดการกระทำความผิด ทั้งนี้ คำว่า "ผู้อื่น" ซึ่งหมายถึงบุคคลที่ถูกใส่ความนั้น ศาลฎีกาเคยวางแนวทางการวินิจฉัยไว้ว่า ผู้อื่นในที่นี้ต้องทราบว่าหมายถึงผู้ใด แต่ไม่จำเป็นต้องระบุชื่อของผู้นั้น[2] หากมีการใส่ความในลักษณะที่ทำให้บุคคลที่สามเข้าใจได้ว่าผู้ใส่ความหมายถึงใคร ถือว่าผู้ถูกใส่ความเป็นผู้อื่นตามความหมายในมาตรานี้แล้ว ส่วนคำว่า "บุคคลที่สาม" หมายถึง บุคคลที่รับทราบข้อความที่เป็นการใส่ความ โดยบุคคลที่สามจะต้องทราบและเข้าใจข้อความนั้นด้วยจึงจะถือว่าเป็นความผิดสำเร็จฐานหมิ่นประมาท[3]

---

[1] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, พิมพ์ครั้งที่ 11 (กรุงเทพมหานคร: วิญญูชน, 2559), หน้า 240-241.

[2] ไกรฤกษ์ เกษมสันต์, คำอธิบายประมวลกฎหมายอาญา มาตรา 288-มาตรา 366, พิมพ์ครั้งที่ 6 (กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2553), หน้า 180.

[3] เรื่องเดียวกัน, หน้า 182.

สาระสำคัญของความผิดฐานหมิ่นประมาทคือ “การใส่ความ” ซึ่งหมายถึง การยืนยันข้อเท็จจริงซึ่งอาจเป็นความจริงหรือเป็นความเท็จโดยไม่จำกัดวิธีการ ไม่ว่าจะเป็นทางวาจา การแสดงกิริยาอาการใด ๆ การส่งข้อความหรือสัญลักษณ์ต่าง ๆ โดยข้อเท็จจริงที่ถือเป็นการใส่ความต้องเป็นข้อเท็จจริงที่แน่นอน ไม่ใช่ข้อเท็จจริงที่เป็นเพียงคำหยาบคาย เลื่อนลอย หรือเป็นไปไม่ได้ อีกทั้งต้องเป็นข้อเท็จจริงที่ยืนยันอดีตหรือปัจจุบัน[4] ซึ่งการใส่ความเช่นนี้จะเป็นความผิดฐานหมิ่นประมาทได้ต้องมีองค์ประกอบสำคัญอีกประการหนึ่ง คือ การใส่ความผู้อื่นน่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง ซึ่งเป็นพฤติการณ์ประกอบการกระทำความผิด โดยต้องพิจารณาข้อเท็จจริงหลายส่วนประกอบกันตามระดับความรู้ของวิญญูชน เพื่อค้นหาว่าผู้ใส่ความมีเจตนาหรือจุดประสงค์ในการหมิ่นประมาทหรือไม่ ทั้งภาพรวมของข้อความที่แสดงออกมา สถานที่ เวลา โอกาส รวมทั้งประเด็นปัญหาและเป้าหมายที่ผู้ใส่ความต้องการสื่อสารออกไป ดังจะเห็นได้จากแนวคำวินิจฉัยของศาลฎีกาในคำพิพากษาศาลฎีกาที่ 10840/2557[5] ดังนั้น แม้ข้อความที่แสดงออกไปจะเป็นข้อความหยาบคาย ไม่สมควร เสียดสี หรือดูถูกดูแคลนบุคคลอื่น แต่ถ้าข้อความนั้นไม่ถึงขนาดทำให้บุคคลที่ได้รับทราบข้อความเกิดความเกลียดชังหรือดูหมิ่นผู้ที่ถูกใส่ความ ย่อมไม่ใช่การกระทำความผิดฐานหมิ่นประมาท[6]

นอกจากนี้ ความเสียหายต่อชื่อเสียงเกียรติคุณของผู้ถูกใส่ความอาจรุนแรงมากยิ่งขึ้นในกรณีที่ข้อความที่เป็นการใส่ความได้แพร่กระจายออกไปยังสาธารณชน ประมวลกฎหมายอาญาจึงได้บัญญัติความผิดฐานหมิ่นประมาทด้วยการโฆษณาไว้ตามมาตรา 328 ดังนี้

---

[4] ไกรฤกษ์ เกษมสันต์, คำอธิบายประมวลกฎหมายอาญา มาตรา 288-มาตรา 366, หน้า 173-175.

[5] คำพิพากษาศาลฎีกาที่ 10840/2557 การพิจารณาว่าผู้กล่าวใส่ความมุ่งหมายให้คำกล่าวใส่ความสร้างความเสียหายแก่ชื่อเสียงของผู้ถูกใส่ความคนใด นั้น จะพิจารณาแต่เพียงถ้อยคำพูดเฉพาะส่วนใด แยกเป็นส่วนๆ ไม่ได้ หากแต่ต้องพิจารณาภาพรวมที่ผู้ใส่ความกล่าวถึงทั้งหมดรวมกัน อีกทั้งยังอาจต้องพิจารณาถึงสถานที่และเวลาโอกาสรวมทั้งประเด็นปัญหาและเป้าหมายที่ผู้กล่าวใส่ความต้องการสื่อถึงผู้รับฟังคำพูดนั้นประกอบกันด้วย ซึ่งเมื่อนำข้อพิจารณาเช่นว่านี้มาวินิจฉัยประกอบคำพูดอภิปรายของจำเลยในการประชุมสภาผู้แทนราษฎรทั้งหมดแล้วมีข้อความโดยรวมบ่งชี้ชัดแจ้งว่าจำเลยมุ่งหมายใส่ความพาดพิงถึงบริษัทโจทก์ซึ่ง ณ. ภริยาของ ส. ผู้ถูกอภิปรายไม่ไว้วางใจเป็นกรรมการผู้จัดการบริษัทด้วยผู้หนึ่ง และบริษัทโจทก์ได้รับประโยชน์จากการยกเว้นภาษีสรรพสามิต เพราะ ส. ผลักดันให้มีการออกประกาศกรมสรรพสามิตเพื่อเอื้อประโยชน์ให้บริษัทโจทก์นั่นเอง คำกล่าวอภิปรายของจำเลยเช่นนี้ได้ความชัดเจนเพียงพอที่ทำให้ผู้ฟังคำอภิปรายเข้าใจได้ว่าบริษัทที่จำเลยยกตัวอย่างว่าได้รับประโยชน์จากการที่ ส. ผลักดันให้มีการออกประกาศกรมสรรพสามิตยกเว้นภาษีสรรพสามิต คือ บริษัทโจทก์นั่นเอง หาอาจเข้าใจว่าเป็นบริษัทอื่นนอกจากบริษัทโจทก์ไม่ โจทก์จึงเป็นผู้เสียหาย

[6] คำพิพากษาศาลฎีกาที่ 4425/2545 ขณะโจทก์เดินอยู่ที่หน้าหอประชุม จำเลยชี้มือมาที่โจทก์แล้วพูดกับชาวบ้านที่เดินผ่านมาว่า "ระวังทนายสกปรกจะเอาเรื่อง" ซึ่งคำพูดดังกล่าวไม่มีข้อความประกอบให้เห็นว่า โจทก์มีอาชีพทนายความสกปรกในเรื่องอะไรแม้จะเป็นคำเสียดสีโจทก์ว่าเป็นคนน่ารังเกียจ แต่ไม่ถึงขนาดทำให้ผู้ที่รับฟังเข้าใจว่าโจทก์เป็นคนคดโกงขาดความน่าเชื่อถือหรือน่าจะทำให้โจทก์เสียชื่อเสียงถูกดูหมิ่นหรือถูกเกลียดชัง ถ้อยคำที่จำเลยกล่าวจึงไม่เป็นหมิ่นประมาทโจทก์

“มาตรา 328 ถ้าความผิดฐานหมิ่นประมาทได้กระทำโดยการโฆษณาด้วยเอกสาร ภาพวาด ภาพระบายสี ภาพยนตร์ ภาพหรือตัวอักษรที่ทำให้ปรากฏไม่ว่าด้วยวิธีใด ๆ แผ่นเสียง หรือสิ่งบันทึกเสียง บันทึกภาพ หรือบันทึกอักษร กระทำโดยการกระจายเสียง หรือการกระจายภาพ หรือโดยกระทำการป่าวประกาศด้วยวิธีอื่น ผู้กระทำต้องระวางโทษจำคุกไม่เกินสองปี และปรับไม่เกินสองแสนบาท”

คำว่า “โฆษณา” มีความหมายตามพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2542 ว่า *“เผยแพร่ข้อความออกไปยังสาธารณชน; ป่าวร้อง, ป่าวประกาศ”* จะเห็นได้ว่า การหมิ่นประมาทโดยการโฆษณาเป็นการหมิ่นประมาทในลักษณะเดียวกันกับความผิดตามมาตรา 326 แต่การหมิ่นประมาทตามมาตรา 328 ต้องมีลักษณะเพิ่มเติม คือ กระทำโดยการโฆษณาหรือกระทำด้วยวิธีอื่นใดจนเป็นเหตุให้ข้อเท็จจริงที่ใส่ความถูกกระจายออกไปยังบุคคลอื่นในวงกว้าง[7] เป็นการเผยแพร่ข้อความหมิ่นประมาทออกไปยังสาธารณชนหรือประชาชนทั่วไป เท่ากับเป็นการเพิ่มโอกาสให้เกิดความเสียหายต่อผู้ที่ถูกใส่ความได้อย่างกว้างขวางและรุนแรงยิ่งกว่าการหมิ่นประมาทตามมาตรา 326 เนื่องจากมีจำนวนบุคคลอื่นที่รับทราบข้อความหมิ่นประมาทเพิ่มมากขึ้น

อย่างไรก็ตาม ความผิดฐานหมิ่นประมาทด้วยการโฆษณานี้พิจารณาถึงลักษณะของการกระทำที่ทำให้เกิดการแพร่กระจายไปยังสาธารณชนเป็นสำคัญมากกว่าจำนวนบุคคลที่รับทราบข้อความ เช่น การแจกหนังสือพิมพ์ที่มีเนื้อหาใส่ความผู้อื่นถือเป็นการทำให้ข้อความหมิ่นประมาทถูกเผยแพร่ออกไปยังสาธารณชนแล้ว[8] แต่หากเป็นกรณีใส่ความผู้อื่นให้บุคคลกลุ่มใดกลุ่มหนึ่งทราบเท่านั้น ยังไม่ถือว่าเป็นการหมิ่นประมาทด้วยการโฆษณา เช่น การให้สัมภาษณ์ผู้สื่อข่าวหนังสือพิมพ์ด้วยถ้อยคำใส่ความผู้อื่นและหนังสือพิมพ์ตีพิมพ์ข้อความหมิ่นประมาทนั้น ไม่ถือว่าเป็นการหมิ่นประมาทด้วยการโฆษณา[9] หรือการส่งหนังสือที่มีข้อความหมิ่นประมาทไปยังบุคคลเฉพาะกลุ่ม[10] เป็นต้น

---

[7] ไกรฤกษ์ เกษมสันต์, คำอธิบายประมวลกฎหมายอาญา มาตรา 288-มาตรา 366, หน้า 188.

[8] คำพิพากษาศาลฎีกาที่ 4998/2558 การนำหนังสือพิมพ์ไปแจกโดยทราบว่ามีเนื้อหาข้อความหมิ่นประมาทโจทก์ถือได้ว่าเป็นการกระจายข่าวไปสู่สาธารณชนหรือประชาชนทั่วไปแล้ว จึงเป็นการกระทำความผิดฐานหมิ่นประมาทโดยการโฆษณา

[9] คำพิพากษาศาลฎีกาที่ 5599/2530 จำเลยให้สัมภาษณ์ผู้สื่อข่าวหนังสือพิมพ์ด้วยข้อความอันมีมูล เป็นการหมิ่นประมาทโจทก์แล้วหนังสือพิมพ์นำข้อความนั้นไปลงพิมพ์โฆษณา ดังนี้ เมื่อไม่ปรากฏว่าจำเลยได้ใช้บังคับ ขู่เข็ญ จ้างวาน หรือยุยงส่งเสริมให้หนังสือพิมพ์ไปลงพิมพ์ การที่หนังสือพิมพ์นำข้อความนั้นไปลงพิมพ์จึงเป็นเรื่องของหนังสือพิมพ์โดยเฉพาะ คดีโจทก์ไม่มีมูลความผิดฐานหมิ่นประมาทโดยการโฆษณาตามประมวลกฎหมายอาญา มาตรา 328

[10] คำพิพากษาศาลฎีกาที่ 7788/2552 การหมิ่นประมาทโดยการโฆษณาตาม ป.อ. มาตรา 328 ผู้กระทำต้องเผยแพร่ข้อความอันเป็นการหมิ่นประมาทออกไปยังสาธารณชนหรือประชาชนทั่วไป การที่จำเลยส่งหนังสือถึง อ. และบุคคลอื่น ๆ ที่เป็นเจ้าของที่ดินในโครงการบ้านสวนริมทะเลของจำเลยเท่านั้น มีลักษณะเป็นเพียงการแจ้งหรือไขข่าวไปยังเฉพาะกลุ่มบุคคลซึ่งเป็นเจ้าของที่ดินในโครงการดังกล่าวเช่นเดียวกับโจทก์ ยังไม่ถึงกับเป็นการกระจายข่าวไปสู่สาธารณชนหรือประชาชนทั่วไป จึงไม่มีความผิดตามมาตรา 328

จากองค์ประกอบของความผิดฐานหมิ่นประมาทข้างต้น เมื่อนำมาเปรียบเทียบกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตแล้ว พบว่ามีความคล้ายคลึงและความแตกต่างหลายประการดังต่อไปนี้

(ก) ความคล้ายคลึง

คุณธรรมทางกฎหมายของความผิดฐานหมิ่นประมาท คือ เกียรติ กฎหมายให้ความคุ้มครองชื่อเสียงเกียรติคุณของบุคคลมิให้ถูกล่วงละเมิดจากการถูกใส่ความ ในขณะที่การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอาจเกิดผลกระทบหรือสร้างความเสียหายต่อคุณธรรมทางกฎหมายได้หลายประการ ในกรณีที่การสวมรอยดังกล่าวเป็นเหตุให้ผู้ถูกแอบอ้างชื่อต้องเสื่อมเสียชื่อเสียงเกียรติคุณ ก็ถือได้ว่าเป็นการกระทำที่กระทบกระเทือนต่อเกียรติของบุคคลเช่นเดียวกับความผิดฐานหมิ่นประมาท

(ข) ความแตกต่าง

ความผิดฐานหมิ่นประมาทถูกบัญญัติขึ้นเพื่อคุ้มครองชื่อเสียงเกียรติคุณของบุคคลที่ถูกใส่ความ คุณธรรมทางกฎหมายของความผิดฐานนี้คือ เกียรติ แต่สิ่งที่ควรได้รับการคุ้มครองจากการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตนั้นโดยหลักแล้วคือ สิทธิในความเป็นตัวตน สิทธิส่วนบุคคล และข้อมูลส่วนบุคคลของเจ้าของตัวตนที่ถูกสวมรอย แต่อย่างไรก็ตาม การสวมรอยดังกล่าวอาจเกิดขึ้นได้หลายรูปแบบ หากเป็นกรณีที่สวมรอยแล้วแสดงพฤติกรรมที่ไม่เหมาะสมในนามของผู้ถูกสวมรอย จนเป็นเหตุให้ผู้ถูกสวมรอยอาจเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง ก็ถือได้ว่าการกระทำความผิดเช่นนี้มีคุณธรรมทางกฎหมายคือ เกียรติ เช่นเดียวกับความผิดฐานหมิ่นประมาทได้ แต่หากการสวมรอยไม่ได้ทำให้ผู้ถูกสวมรอยได้รับความเสียหายด้านชื่อเสียง เนื่องจากไม่มีการใส่ความต่อบุคคลที่สามหรือต่อประชาชนด้วยการเผยแพร่ข้อความหมิ่นประมาทผ่านระบบเครือข่ายอินเทอร์เน็ต แต่ได้รับความเสียหายด้านอื่น เช่น ถูกติดตามคุกคามหรือรังควาน ได้รับความเดือดร้อนรำคาญ หรือสูญเสียทรัพย์สินหรือตำแหน่งหน้าที่ในการทำงาน กรณีเช่นนี้ย่อมไม่อาจถือได้ว่าผู้ถูกสวมรอยเป็นผู้เสียหายฐานหมิ่นประมาท เพราะคุณธรรมทางกฎหมายไม่ใช่เกียรติเสียแล้ว

อนึ่ง ในกรณีที่ผู้กระทำผิดนำชื่อหรือความเป็นตัวตนของผู้เสียหายไปกระทำการอันเป็นที่เสื่อมเสียต่อชื่อเสียงเกียรติคุณของผู้เสียหายนั้น มีประเด็นที่ควรพิจารณาอีกประการหนึ่ง คือ การสวมรอยในลักษณะเช่นนี้ถือเป็นการใส่ความอันเป็นองค์ประกอบสำคัญของความผิดฐานหมิ่นประมาทหรือไม่ ทั้งนี้ เมื่อพิเคราะห์จากลักษณะการใส่ความแล้วจะเห็นได้ว่า การใส่ความเป็นการยืนยันข้อเท็จจริงที่อ้างถึงบุคคลหนึ่งให้อีกบุคคลหนึ่งรับรู้ หรือกล่าวอีกนัยหนึ่งคือ เป็นการบอก

เล่าข้อเท็จจริงให้บุคคลที่สามได้ทราบ ไม่ว่าจะเป็นด้วยวาจาหรือลายลักษณ์อักษร แต่การสวมรอยเป็นบุคคลอื่นและกระทำการอันเสื่อมเสีย เช่น สวมรอยเป็นบุคคลที่มีชื่อเสียงและกระทำความผิดฐานฉ้อโกงในนามของบุคคลนั้น เป็นเหตุให้ประชาชนทั่วไปไม่พอใจหรือเกลียดชังบุคคลที่ถูกสวมรอย กรณีเช่นนี้เป็นการแสดงออกทางพฤติกรรมที่ทำให้บุคคลที่สามเข้าใจไปเองว่าผู้ถูกสวมรอยเป็นผู้กระทำการอันเสื่อมเสีย มิใช่การบอกเล่าหรือยืนยันข้อเท็จจริงแต่ประการใด ดังนั้น การสวมรอยเป็นบุคคลอื่นที่ส่งผลให้เกิดความเสียหายต่อชื่อเสียงจึงไม่ใช่การใส่ความ และไม่อาจปรับเข้ากับลักษณะการกระทำความผิดฐานหมิ่นประมาทได้ชัดเจนนัก

นอกจากนี้ การสวมรอยเป็นบุคคลอื่นเพื่อใส่ความหมิ่นประมาทบุคคลอีกคนหนึ่งต่อบุคคลที่สามหรือต่อประชาชนผ่านทางระบบเครือข่ายอินเทอร์เน็ต เรียกได้ว่าเป็นการแอบอ้างชื่อของผู้ถูกสวมรอยเพื่อกระทำความผิดฐานหมิ่นประมาทอีกต่อหนึ่ง โดยที่ผู้ถูกสวมรอยอาจรู้หรือไม่รู้ว่าชื่อของตนกลายเป็นชื่อของผู้กระทำความผิดฐานหมิ่นประมาท ในกรณีเช่นนี้ ผู้ถูกสวมรอยย่อมไม่ใช่ผู้ที่ถูกใส่ความ จึงไม่ใช่ผู้เสียหายในความผิดฐานหมิ่นประมาท แต่เป็นผู้เสียหายที่ถูกล่วงละเมิดข้อมูลส่วนบุคคล ตัวอย่างเช่น คำพิพากษาคดีหนึ่งของศาลทหารมณฑลทหารบกที่ 33 จังหวัดเชียงใหม่[11] ซึ่งมีข้อเท็จจริงว่า ผู้กระทำความผิดแอบอ้างใช้ชื่อของ ร. เขียนข้อความหมิ่นประมาทพระมหากษัตริย์บนเว็บไซต์เฟสบุ๊ก เพื่อให้ประชาชนทั่วไปเข้าใจว่า ร. เป็นผู้เขียนข้อความ เป็นเหตุให้ประชาชนกลุ่มหนึ่งร้องทุกข์กล่าวโทษ ร. ในความผิดฐานหมิ่นประมาทพระมหากษัตริย์ตามประมวลกฎหมายอาญามาตรา 112 แต่เมื่อเจ้าหน้าที่ตำรวจได้ควบคุมตัว ร. มาสอบสวนแล้วจึงพบว่า ร. ไม่มีส่วนเกี่ยวข้อง แต่กลับถูกกลั่นแกล้งจากผู้กระทำความผิดด้วยการสร้างเฟสบุ๊กปลอมขึ้นในนามของ ร. ท้ายที่สุดผู้กระทำความผิดยอมรับสารภาพ ผู้พิพากษาศาลทหารมณฑลทหารบกที่ 33 จังหวัดเชียงใหม่มีคำ

[11] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, "ศศิวิมล : โพสต์ข้อความบนเฟซบุ๊ก" [ออนไลน์] เข้าถึงเมื่อ 13 ธันวาคม 2559. แหล่งที่มา: https://freedom.ilaw.or.th/case/681#progress_of_case

พิพากษาว่า ผู้กระทำความผิดมีความผิดตามมาตรา 14 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550[12] ประกอบกับมาตรา 112 แห่งประมวลกฎหมายอาญา[13]

การที่บุคคลหนึ่งทำการสวมรอยเป็นบุคคลอีกคนหนึ่งแล้วได้กระทำในนามของบุคคลนั้นใส่ความผู้อื่นต่อบุคคลที่สาม ผู้ถูกใส่ความจึงเป็นผู้เสียหายในความผิดฐานหมิ่นประมาทที่กระทำลงโดยผู้สวมรอย ส่วนบุคคลที่ถูกสวมรอยย่อมได้รับความเสียหายจากการถูกนำความเป็นตัวตนไปแอบอ้างใส่ความผู้อื่น โดยอาจได้รับความเสียหายด้านชื่อเสียงหรือเสื่อมเกียรติยศ แต่บุคคลที่ถูกสวมรอยไม่ใช่ผู้เสียหายในความผิดฐานหมิ่นประมาท เพราะไม่ใช่ผู้ที่ถูกใส่ความ ดังนั้น บทบัญญัติมาตรานี้จึงคุ้มครองเพียงผู้ที่ถูกใส่ความให้สามารถเอาผิดกับผู้สวมรอยได้ แต่ไม่ได้คุ้มครองบุคคลที่ถูกสวมรอยในกรณีเช่นนี้

ส่วนความผิดฐานหมิ่นประมาทด้วยการโฆษณานั้นมีใจความสำคัญคือลักษณะของการแพร่กระจายข้อความไปยังบุคคลทั่วไปในวงกว้าง ระบบอินเทอร์เน็ตเป็นระบบที่บุคคลทั่วไปสามารถเข้าถึงได้ ทำให้มีบุคคลจำนวนมากที่รับทราบข้อมูลที่อยู่บนระบบอินเทอร์เน็ต หากมีการหมิ่นประมาทผ่านทางระบบอินเทอร์เน็ตแล้วจึงอาจเทียบเคียงได้กับการหมิ่นประมาทด้วยการโฆษณาได้

3.1.2 ความผิดฐานฉ้อโกง

ประมวลกฎหมายอาญาบัญญัติความผิดฐานฉ้อโกงไว้ในมาตรา 341 มีใจความว่า

“ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ”

---

[12] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14 “ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา...”

[13] ประมวลกฎหมายอาญา มาตรา 112 “ผู้ใดหมิ่นประมาท ดูหมิ่น หรือแสดงความอาฆาตมาดร้ายพระมหากษัตริย์ พระราชินี รัชทายาท หรือผู้สำเร็จราชการแทนพระองค์ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี”

สาระสำคัญของลักษณะการกระทำความผิดฐานฉ้อโกง คือ ผู้กระทำความผิดมีเจตนาพิเศษในการหลอกลวงเพื่อให้ได้ไปซึ่งทรัพย์สินหรือทำให้เกิดการทำ ถอน หรือทำลายเอกสารสิทธิตั้งแต่ก่อนหรือในขณะลงมือกระทำความผิด การหลอกลวงดังกล่าวแบ่งเป็น 2 รูปแบบ ได้แก่ การหลอกลวงด้วยการแสดงข้อความอันเป็นเท็จ และการหลอกลวงด้วยการปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง

ในส่วนของการหลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จนั้น หมายถึง การบอกกล่าวข้อเท็จจริงที่ผิดไปจากความเป็นจริงให้ผู้อื่นได้ทราบ ไม่ว่าด้วยวาจา เอกสาร กิริยาท่าทาง หรือวิธีการอื่นใด[14] โดยข้อเท็จจริงดังกล่าวต้องเป็นข้อเท็จจริงที่มีอยู่ในอดีตหรือปัจจุบันเท่านั้น หากกล่าวถึงข้อเท็จจริงในอนาคตอันไม่แน่นอน กรณีจะเป็นความผิดฐานฉ้อโกงได้ก็ต่อเมื่อการแสดงข้อเท็จจริงนั้นเป็นการยืนยันหรือแสดงภาวะแห่งจิตของผู้หลอกลวงว่าเป็นเท็จในขณะที่กล่าวออกมา แต่หากเป็นการกล่าวถึงข้อเท็จจริงในอนาคตหรือการให้คำมั่นย่อมไม่เป็นความผิดฐานฉ้อโกง[15]

ส่วนการปกปิดข้อความจริงซึ่งควรบอกให้แจ้งนั้นเป็นการกระทำการงดเว้นหน้าที่ซึ่งผู้กระทำมีหน้าที่ต้องบอกกล่าวเพื่อป้องกันผล ผลในที่นี้คือมีบุคคลหลงเชื่อคำหลอกลวงนั่นเอง ดังนั้นหากผู้กระทำมีหน้าที่ต้องป้องกันผล ไม่ว่าจะเป็นหน้าที่ตามกฎหมาย หน้าที่ตามสัญญา หรือหน้าที่อันเกิดจากการกระทำครั้งก่อนก็ตาม และผู้นั้นงดเว้นเสียไม่บอกกล่าวข้อความจริง ผู้นั้นย่อมเข้าลักษณะขององค์ประกอบในการกระทำความผิดฐานฉ้อโกงได้[16]

ความผิดฐานฉ้อโกงเป็นความผิดที่ต้องการผล กล่าวคือ เมื่อผู้กระทำได้กระทำการหลอกลวงผู้อื่นโดยแสดงข้อความอันเป็นเท็จแล้วหรือได้กระทำการปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง จะต้องเกิดผลของการกระทำดังกล่าวตามมาจึงจะถือว่าเป็นความผิดฐานฉ้อโกง ได้แก่ ผู้กระทำได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือผู้ถูกหลอกลวงหรือบุคคลที่สามได้ทำ ถอน หรือทำลายเอกสารสิทธิตามที่ตนถูกหลอกลวง ทั้งนี้ ผลที่เกิดขึ้นต้องมีสาเหตุมาจากการถูกหลอกลวงหรือปกปิดข้อความจริงด้วย หากผลเหล่านี้ไม่ได้เกิดขึ้นจากสาเหตุดังกล่าว ย่อมไม่ถือว่าเป็นการกระทำความผิดฐานฉ้อโกง[17]

ทั้งนี้ การได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สามอันจะเป็นความผิดฐานฉ้อโกงได้นั้นต้องเป็นการได้ไปในลักษณะของการโอนกรรมสิทธิ์ในทรัพย์สินนั้นด้วยเป็นสำคัญ

---

[14] จิตติ ติงศภัทิย์, กฎหมายอาญาภาค 2 ตอน 2 และภาค 3 (กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2545), หน้า 308.

[15] ไกรฤกษ์ เกษมสันต์, คำอธิบายประมวลกฎหมายอาญา มาตรา 288-มาตรา 366, หน้า 314.

[16] เรื่องเดียวกัน, หน้า 324.

[17] เรื่องเดียวกัน, หน้า 326.

มิใช่เพียงการโอนการครอบครองทรัพย์สินเท่านั้น โดยความผิดจะสำเร็จเมื่อโอนกรรมสิทธิ์และมีการส่งมอบการครอบครองทรัพย์สินมีรูปร่าง หรือมีการโอนสิทธิในทรัพย์สินที่ไม่มีรูปร่างให้แก่ผู้กระทำความผิดเรียบร้อยแล้ว ดังนั้น การหลอกลวงเพื่อให้ได้ไปซึ่งสิทธิครอบครองจึงเป็นเพียงการลักทรัพย์โดยใช้กลอุบาย มิใช่ความผิดฐานฉ้อโกง[18] ส่วนการทำ ถอน หรือทำลายเอกสารสิทธินั้น คำว่าเอกสารสิทธิเป็นไปตามคำนิยามในมาตรา 1 (9) แห่งประมวลกฎหมายอาญาซึ่งบัญญัติว่า “เอกสารที่เป็นหลักฐานแห่งการก่อ เปลี่ยนแปลง โอน สงวน หรือระงับซึ่งสิทธิ”

ตามที่ได้กล่าวมาแล้ว เมื่อพิจารณาองค์ประกอบของความผิดฐานฉ้อโกงแล้วจะเห็นได้ว่า คุณธรรมทางกฎหมายของความผิดฐานนี้คือ “สิทธิในทรัพย์สิน” (Real Right) การหลอกลวงบุคคลอื่นเพื่อให้ตนได้ไปซึ่งทรัพย์สินถือเป็นการละเมิดต่อสิทธิในทรัพย์สินของบุคคลนั้น เพราะฉะนั้นผู้เสียหายในความผิดฐานนี้จึงได้แก่ ผู้ถูกหลอกลวง กฎหมายอาญามุ่งคุ้มครองบุคคลที่ได้โอนกรรมสิทธิ์และสิทธิครอบครองหรือโอนสิทธิในทรัพย์สินของตนไปให้ผู้กระทำความผิด หรือได้ทำ ถอน หรือทำลายเอกสารสิทธิ อันเนื่องมาจากการถูกหลอกลวง ด้วยเหตุนี้ องค์ประกอบของฐานความผิดดังกล่าวจึงแตกต่างจากการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ซึ่งผู้ที่ได้รับความเสียหายคือบุคคลที่ถูกแอบอ้างชื่อหรือความเป็นตัวตนไปสวมรอยเพื่อกระทำความผิดอื่น ๆ ต่อไป

อนึ่ง ในประมวลกฎหมายอาญามีบทบัญญัติมาตราหนึ่งที่คล้ายคลึงกับการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นอย่างยิ่ง คือ ความผิดฐานฉ้อโกงโดยการแสดงตนเป็นบุคคลอื่นเพื่อหลอกลวงผู้เสียหาย ซึ่งถือเป็นเหตุฉกรรจ์ของความผิดฐานฉ้อโกง ดังที่บัญญัติไว้ในมาตรา 342 (1) แห่งประมวลกฎหมายอาญา ดังนี้ *“มาตรา 342 ถ้าในการกระทำความผิดฐานฉ้อโกง ผู้กระทำ (1) แสดงตนเป็นคนอื่น...ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ”*

จะเห็นได้ว่า ความผิดตามมาตราดังกล่าวเป็นเหตุฉกรรจ์และระวางโทษไว้สูงกว่าความผิดฐานฉ้อโกงธรรมดา เนื่องมาจากพฤติการณ์และลักษณะของการหลอกลวงที่พิเศษเพิ่มมากขึ้น คือ การหลอกลวงโดยการแสดงออกว่าผู้กระทำความผิดเป็นบุคคลอื่น เพื่อให้ผู้ถูกหลอกลวงหลงเชื่อหรือเข้าใจว่าผู้กระทำความผิดเป็นบุคคลอีกคนหนึ่ง มิใช่ตัวของตัวเอง[19] และมิใช่เพียงแต่เข้าใจฐานะ

---

[18] บันทึกท้ายฎีกาที่ 2581/2529 และจิตติ ติงศภัทิย์, กฎหมายอาญาภาค 2 ตอน 2 และภาค 3, หน้า 577-585 และ 856-859.

[19] คำพิพากษาศาลฎีกาที่ 1784/2493 (ประชุมใหญ่) คำว่า "ปลอมตัวเป็นคนอื่น" ตามกฎหมายลักษณะอาญา มาตรา 306 (1) นั้น มุ่งหมายถึงการแสดงตัวให้เขาหลงเชื่อว่าเป็นคนอื่น ซึ่งไม่ใช่ตัวของตัวเอง

ของผู้กระทำผิดไปเท่านั้น เพราะฉะนั้นการแสดงฐานะของตนเองเป็นเท็จหรือการใช้นามแฝงหรือนามสมมติ โดยไม่มีเจตนาจะหลอกลวงผู้อื่นว่าตนเป็นอีกคนหนึ่ง ย่อมไม่เป็นการแสดงตนเป็นคนอื่นตามมาตรานี้[20] เช่น การบอกกล่าวแก่บุคคลอื่นด้วยชื่อเท็จ แม้จะเป็นชื่อของบุคคลอื่นแต่ผู้กระทำไม่มีเจตนาเพื่อทำให้ผู้อื่นเข้าใจผิดว่าตนเป็นบุคคลเจ้าของชื่อนั้น หากแต่ทำไปเพื่อปกปิดชื่อจริงของตน ย่อมไม่เป็นความผิดตามมาตรานี้ ในทางกลับกัน หากเป็นการใช้ชื่อเท็จเพื่อให้เข้าใจว่าผู้กระทำความผิดเป็นบุคคลอีกคนหนึ่ง แม้บุคคลนั้นจะไม่มีตัวตนอยู่จริง ก็ถือว่าเข้าลักษณะการกระทำความผิดนี้แล้ว

จากการศึกษาพบว่า ประเทศไทยมีการกระทำความผิดฐานฉ้อโกงโดยแสดงตนเป็นคนอื่นเกิดขึ้นพอสมควร ตัวอย่างเช่น คำพิพากษาศาลฎีกาที่ 2239/2522 จำเลยใช้เอกสารปลอมอ้างว่าตนเองเป็นเจ้าของรถและขายรถให้แก่ผู้เสียหาย[21] คำพิพากษาศาลฎีกาที่ 20/2546 จำเลยสวมรอยเป็น ส. โดยนำ น.ส.3 ก. ที่ระบุชื่อของ ส. และสำเนาบัตรประชาชนของ ส. มาแสดงต่อผู้เสียหายเพื่อขอกู้ยืมเงิน[22] หรือคำพิพากษาศาลฎีกาที่ 10552/2553 จำเลยหลอกลวงผู้เสียหายด้วยการนำโฉนดที่ดินของผู้อื่นมาแสดงให้ผู้เสียหายเข้าใจว่าจำเลยเป็นบุคคลนั้นและได้ไปซึ่งเงินจากผู้เสียหาย[23]

จำเลยใช้ถ้อยคำหลอกลวงให้เขาหลงเชื่อว่า จำเลยเป็นนายร้อยตำรวจโทประจำกองสอบสวนกลางปทุมวัน (ระบุชื่อ) เมื่อความจริงจำเลยมิใช่เป็นนายร้อยตำรวจประจำกองสอบสวนกลางแล้ว แม้จะไม่ปรากฏว่ามีนายร้อยตำรวจโทชื่อนั้นในกองสอบสวนกลางหรือไม่ ก็ถือว่าเป็นการปลอมตัวตามความหมายในมาตรา 306 (1) แล้ว

[20] ไกรฤกษ์ เกษมสันต์, คำอธิบายประมวลกฎหมายอาญา มาตรา 288-มาตรา 366, หน้า 334-335.

[21] คำพิพากษาศาลฎีกาที่ 2239/2522 จำเลยที่ 1 ที่ 2 กับชายอีกคนหนึ่งซึ่งเป็นผู้ขับรถร่วมกันนำรถยนต์แท็กซี่คันเกิดเหตุมาขายให้ผู้เสียหาย โดยจำเลยที่ 2 อ้างว่าเป็น นาง ส. เจ้าของรถและจำเลยที่ 1 เป็นผู้มอบอำนาจในการโอนรถยนต์ให้แก่ผู้เสียหาย เอกสารเหล่านั้นเป็นเอกสารปลอม จำเลยทั้งสองจึงมีความผิดฐานร่วมกันใช้เอกสารปลอมและฐานฉ้อโกงโดยแสดงตนเป็นคนอื่นแต่การที่จำเลยร่วมกันนำเอกสารปลอมมาใช้ก็โดยมีเจตนาที่จะฉ้อโกงผู้เสียหายนั่นเอง การกระทำของจำเลยทั้งสองจึงเป็นกรรมเดียวเป็นความผิดต่อกฎหมายหลายบท

[22] คำพิพากษาศาลฎีกาที่ 20/2546 การที่จำเลยนำ น.ส.3 ก. ที่ระบุชื่อ ส. และสำเนาบัตรประจำตัวประชาชนของ ส. ซึ่งเลอะเลือนมองเห็นไม่ชัดเจนมาแสดงต่อผู้เสียหายเพื่อขอกู้ยืมเงิน ทำให้ผู้เสียหายหลงเชื่อว่าจำเลยคือ ส. เจ้าของที่ดินตาม น.ส.3 ก. ที่แท้จริง จึงตกลงให้จำเลยกู้ยืมเงินไปนั้น เป็นความผิดฐานฉ้อโกงผู้อื่นโดยการแสดงตนเป็นคนอื่นตามประมวลกฎหมายอาญา มาตรา 342 (1)

[23] คำพิพากษาศาลฎีกาที่ 10552/2553 แม้ตามคำฟ้องโจทก์จะบรรยายว่า จำเลยโดยเจตนาทุจริตหลอกลวงผู้เสียหายที่ 2 ด้วยการแสดงข้อความอันเป็นเท็จและด้วยการแสดงตนเป็นบุคคลอื่น แต่ตามทางพิจารณาที่ได้ความนั้น เป็นเรื่องที่จำเลยหลอกลวง ส. มารดาผู้เสียหายที่ 2 มิใช่หลอกลวงผู้เสียหายที่ 2 ซึ่งเป็นเจ้าของเงินก็ตาม แต่เมื่อผู้เสียหายที่ 2 เป็นเจ้าของเงินที่ให้กู้ และเป็นผู้ทำสัญญากู้ในฐานะผู้ให้กู้เงินที่จำเลยผู้กู้นำโฉนดที่ดินของบุคคลอื่นมาหลอกลวงดังกล่าว เพื่อให้ได้เงินที่กู้ยืมไป ผู้เสียหายที่ 2 ได้รับความเสียหายเนื่องจากการกระทำความผิดของจำเลยแล้ว

จำเลยหลอกลวงด้วยการทำให้ผู้อื่นเข้าใจว่าตนเป็นบุคคลเดียวกับ ป. ผู้มีชื่อในโฉนดที่ดินที่จำเลยนำมาเป็นหลักประกันในการกู้เงินจากผู้เสียหายที่ 2 จากการหลอกลวงดังกล่าวทำให้ได้ไปซึ่งเงินจากผู้เสียหายที่ 2 การกระทำของจำเลยจึงเป็นความผิดฐานฉ้อโกง

เมื่อพิจารณาแล้วจะเห็นได้ว่า การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต โดยมีจุดประสงค์เพื่อหลอกลวงผู้อื่นและได้ไปซึ่งทรัพย์สินของผู้อื่นนั้นมีลักษณะเช่นเดียวกับความผิดฐานฉ้อโกงโดยแสดงตนเป็นคนอื่น หรือกล่าวอีกนัยหนึ่ง การปลอมตนเพื่อหลอกลวงผู้อื่นผ่านทางโลกไซเบอร์เป็นอีกรูปแบบหนึ่งของความผิดฐานฉ้อโกงที่เปลี่ยนแปลงไปตามเทคโนโลยีอันทันสมัยในยุคปัจจุบัน ซึ่งเป็นช่องทางใหม่ในการฉ้อโกงที่สามารถกระทำได้อย่างสะดวกและง่ายดาย แต่อย่างไรก็ตาม ความผิดฐานฉ้อโกงโดยแสดงตนเป็นบุคคลอื่นถูกบัญญัติขึ้นโดยมุ่งคุ้มครองผู้ถูกหลอกลวงเป็นสำคัญ กล่าวคือ ผู้ถูกหลอกลวงเป็นผู้เสียหายตามความผิดฐานนี้ และมีสิทธิร้องทุกข์และดำเนินคดีกับผู้กระทำความผิดได้ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (4)[24] ในขณะที่ผู้เสียหายจากการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ได้แก่ ผู้ถูกสวมรอย ดังนั้น หากผู้กระทำความผิดได้สวมรอยเป็นบุคคลอื่นและกระทำการหลอกลวงฉ้อโกงผู้อื่นผ่านทางเครือข่ายอินเทอร์เน็ตสร้างความเสียหายให้แก่ผู้ถูกหลอกลวง ผู้ถูกหลอกลวงเท่านั้นที่มีสิทธิดำเนินคดีกับผู้กระทำความผิดฐานฉ้อโกงตามมาตรา 342 (1) ได้ แต่ผู้ที่ถูกแอบอ้างสวมรอยนั้นไม่สามารถดำเนินการใด ๆ ได้ เนื่องจากมิใช่ผู้เสียหายตามความผิดฐานนี้นั่นเอง

ข้อพิจารณาดังกล่าวข้างต้นปรากฏในคำพิพากษาศาลฎีกาหลายฉบับ ซึ่งได้วางแนวคำวินิจฉัยไว้ว่า เฉพาะผู้ที่ถูกหลอกลวงและเสียสิทธิในทรัพย์สินไปเท่านั้นที่เป็นผู้เสียหายในความผิดฐานฉ้อโกงโดยการแสดงตนเป็นคนอื่น ส่วนผู้ถูกแอบอ้างชื่อมิใช่ผู้เสียหายในความผิดฐานนี้[25]

นอกจากนี้ ความผิดฐานฉ้อโกงยังมีลักษณะการกระทำความผิดแตกต่างกันไปอีกหลายบทมาตรา เช่น ฉ้อโกงแรงงานตามมาตรา 344 ฉ้อโกงเงินค่าอาหาร ค่าเครื่องดื่ม หรือค่าอยู่ในโรงแรมตามมาตรา 345 ฉ้อโกงให้ผู้อื่นจำหน่ายทรัพย์สินโดยเสียเปรียบตามมาตรา 346 ฉ้อโกงผู้รับประกันวินาศภัยตามมาตรา 347 ทั้งนี้ ความผิดฐานฉ้อโกงที่ถือเป็นเหตุฉกรรจ์ซึ่งอาจก่อให้เกิดความเสียหายได้ในวงกว้าง ได้แก่ ฉ้อโกงประชาชนตามมาตรา 343 ซึ่งมีใจความดังนี้

---

[24] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (4) "ผู้เสียหาย" หมายความถึงบุคคลผู้ได้รับความเสียหายเนื่องจากการกระทำผิดฐานใดฐานหนึ่ง รวมทั้งบุคคลอื่นที่มีอำนาจจัดการแทนได้ ดังบัญญัติไว้ใน มาตรา 4, 5 และ 6

[25] คำพิพากษาศาลฎีกาที่ 2193/2534 “การที่จำเลยนำเช็คที่บริษัท ล. สั่งจ่ายให้โจทก์ร่วม ซึ่งจำเลยได้ปลอมลายมือชื่อของโจทก์ร่วมสลักหลังให้จำเลยแล้วนำไปแสดงต่อเจ้าหน้าที่ของธนาคารตามเช็คเพื่อเรียกเก็บเงินเข้าบัญชีของจำเลย แม้จะเป็นการหลอกลวงโดยแสดงข้อความอันเป็นเท็จหรือปกปิดข้อความจริงที่ควรบอกให้แจ้งก็ตาม แต่ก็เป็นการกระทำต่อธนาคารและเจ้าหน้าที่ของธนาคารโดยตรง ไม่อาจถือได้ว่าเป็นการกระทำต่อโจทก์ร่วม หากโจทก์ร่วมจะได้รับความเสียหายเพราะเสียสิทธิที่จะได้รับเงินตามเช็คไป ก็เป็นความเสียหายที่โจทก์ร่วมได้รับในความผิดฐานปลอมเอกสาร หาใช่ความเสียหายจากการหลอกลวงของจำเลยไม่ โจทก์ร่วมจึงมิใช่ผู้เสียหายในความผิดฐานฉ้อโกงและไม่มีสิทธิร้องทุกข์ในความผิดฐานนี้”

“มาตรา 343 ถ้าการกระทำความผิดตามมาตรา 341 ได้กระทำด้วยการแสดงข้อความอันเป็นเท็จต่อประชาชน หรือด้วยการปกปิดความจริงซึ่งควรบอกให้แจ้งแก่ประชาชน ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำความผิดดังกล่าวในวรรคแรก ต้องด้วยลักษณะดังกล่าวในมาตรา 342 อนุมาตราหนึ่งอนุมาตราใด ผู้กระทำต้องระวางโทษจำคุกตั้งแต่หกเดือนถึงเจ็ดปี และปรับตั้งแต่หนึ่งพันบาทถึงหนึ่งหมื่นสี่พันบาท”

มาตรา 343 เป็นการกระทำความผิดฐานฉ้อโกงประชาชน ซึ่งคำว่า “ประชาชน” มีความหมายตามพจนานุกรมฉบับราชบัณฑิตยสถานว่าหมายถึง บรรดาพลเมืองหรือบุคคลโดยทั่วไป ไม่จำกัดว่าเป็นผู้ใดโดยเฉพาะเจาะจง และไม่ได้ถือเอาจำนวนตัวบุคคลเป็นสำคัญ[26] ดังนั้น การฉ้อโกงประชาชนย่อมเป็นการหลอกลวงบุคคลทั่วไปให้หลงเชื่อด้วยการแสดงข้อความอันเป็นเท็จหรือปกปิดข้อความจริงอันควรบอก โดยมีเจตนาทุจริตเพื่อให้ตนได้ไปซึ่งทรัพย์สินหรือมีการทำ ถอน ทำลายเอกสารสิทธิ นอกจากนี้ มาตรา 343 วรรคสองได้บัญญัติให้การฉ้อโกงประชาชนโดยการแสดงตนเป็นคนอื่นหรือฉ้อโกงประชาชนที่เป็นเด็กหรือผู้ที่มีความอ่อนแอแห่งจิตเป็นเหตุฉกรรจ์ของความผิดฐานฉ้อโกงประชาชนและกำหนดบทลงโทษหนักขึ้นอีกด้วย

การฉ้อโกงประชาชนเป็นการกระทำความผิดที่ส่งผลกระทบต่อสังคมในวงกว้าง เนื่องจากผู้กระทำความผิดได้หลอกลวงประชาชนทั่วไป ราวกับเป็นการวางกับดักเพื่อหลอกล่อเหยื่อโดยไม่จำกัดจำนวนและประเภท หากมีบุคคลใดหลงเชื่อและติดกับก็ย่อมได้รับความเสียหาย ดังปรากฏข้อเท็จจริงในคำพิพากษาศาลฎีกาหลายฉบับ เช่น คำพิพากษาศาลฎีกาที่ 8723/2544 จำเลยหลอกลวงประชาชนว่าเป็นสมาชิกสหกรณ์หอมหัวใหญ่และมีโควต้าเมล็ดพันธุ์หอมหัวใหญ่จำหน่าย เป็นเหตุให้จำเลยได้ไปซึ่งทรัพย์สินจากผู้เสียหาย[27] คำพิพากษาศาลฎีกาที่ 135/2547 จำเลย

---

[26] คำพิพากษาศาลฎีกาที่ 285/2508 การกระทำอันจะเป็นผิดตามประมวลกฎหมายอาญา มาตรา 343 นั้น ผู้กระทำจะต้องกระทำด้วยเจตนาแสดงข้อความอันเป็นเท็จต่อประชาชนโดยทั่วไป จะถือเอาจำนวนผู้เสียหายที่ถูกหลอกลวงมากหรือน้อยและผลเสียหายอันเกิดจากคำหลอกลวงของจำเลยมีมากหรือน้อยเป็นหลักหาได้ไม่ และเมื่อโจทก์มิได้ฟ้องกล่าวหาว่าจำเลยได้หลอกลวงประชาชนโดยทั่วไป จึงเป็นฟ้องที่ไม่ครบองค์ความผิดตามมาตรา 343

[27] คำพิพากษาศาลฎีกาที่ 8723/2544 พฤติการณ์ที่จำเลยพา ว. ไปช่วยจำหน่ายเมล็ดพันธุ์หอมหัวใหญ่และจำเลยไปจำหน่ายเองแต่เพียงลำพัง เพื่อผลประโยชน์ตอบแทนที่จะได้รับเป็นเมล็ดพันธุ์หอมหัวใหญ่ถือได้ว่าเป็นการร่วมมือกับ ว. ในการจำหน่ายเมล็ดพันธุ์หอมหัวใหญ่แล้ว แม้จะไม่ได้รับผลประโยชน์ตอบแทนเป็นเงินก็ตาม การกระทำของจำเลยที่ร่วมกับ ว. หลอกลวงผู้เสียหายทั้งสิบสองและประชาชนว่าเป็นสมาชิกสหกรณ์หอมหัวใหญ่บ้านกาดและมีโควต้าเมล็ดพันธุ์หอมหัวใหญ่จำหน่ายให้แก่ผู้เสียหายทั้งสิบสองและประชาชนด้วยการแสดงข้อความอันเป็นเท็จหรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง ย่อมส่อแสดงให้เห็นถึง

ลงข่าวประกาศอันเป็นความเท็จทางหนังสือพิมพ์เป็นเหตุให้ผู้เสียหายหลงเชื่อและมอบเงินให้จำเลย[28] หรือคำพิพากษาศาลฎีกาที่ 831/2559 จำเลยกับพวกร่วมกันจัดตั้งระบบโทรศัพท์และระบบคอมพิวเตอร์เพื่อดำเนินการติดต่อประชาชนทั่วไปด้วยวิธีการสุ่มหมายเลขโทรศัพท์ และแสดงข้อความอันเป็นเท็จหลอกลวงประชาชนเหล่านั้นว่าตนเป็นเจ้าหน้าที่ธนาคารพาณิชย์หรือเจ้าหน้าที่ของรัฐเพื่อให้ประชาชนหลงเชื่อและดำเนินการธุรกรรมทางการเงินต่าง ๆ ตามที่จำเลยกับพวกต้องการ[29]

จากข้อพิจารณาและข้อสังเกตข้างต้นจะเห็นได้ว่า ความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญากับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตมีความคล้ายคลึงและความแตกต่างกันหลายประการดังต่อไปนี้

(ก) ความคล้ายคลึง

กรณีที่ผู้กระทำความผิดสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต โดยมีจุดประสงค์เพื่อหลอกลวงผู้อื่นให้หลงเชื่อว่าตนเป็นเจ้าของตัวตนที่ถูกสวมรอย และหลอกลวงจนกระทั่งได้ไปซึ่งทรัพย์สินของผู้อื่นนั้น ถือว่าเป็นการกระทำความผิดฐานฉ้อโกงโดยการแสดงตนเป็นคนอื่นตามมาตรา 342 (1) หรืออาจเป็นความผิดฐานฉ้อโกงประชาชนโดยการแสดงตนเป็นคนอื่นตามมาตรา 343 วรรคสอง เนื่องจากการแสดงข้อความอันเป็นเท็จนั้นเป็นการหลอกลวงผ่านเว็บไซต์บนเครือข่ายอินเทอร์เน็ตซึ่งเป็นช่องทางที่ประชาชนทั่วไปสามารถเข้าถึงได้ หรืออาจกล่าวอีกนัยหนึ่ง

เจตนาทุจริตของจำเลยอย่างชัดแจ้งในการที่จะหลอกลวงเอาเงินจากผู้เสียหายทั้งสิบสอง และการหลอกลวงดังว่านั้นจำเลยกับพวกได้ไปซึ่งทรัพย์สินจากผู้เสียหายทั้งสิบสอง จึงเป็นตัวการร่วมกับ ว. กระทำความผิดฐานฉ้อโกงประชาชน

[28] คำพิพากษาศาลฎีกาที่ 135/2547 จำเลยลงข่าวประกาศทางหนังสือพิมพ์ซึ่งเป็นความเท็จโดยทุจริต เป็นเหตุให้ผู้เสียหายที่ 2 ที่ได้อ่านข่าวหลงเชื่อจึงไปติดต่อและมอบเงินให้จำเลย จึงเป็นความผิดฐานฉ้อโกงประชาชน

[29] คำพิพากษาศาลฎีกาที่ 831/2559 การแสดงข้อความอันเป็นเท็จต่อประชาชนในความผิดฐานฉ้อโกงประชาชนตาม ป.อ. มาตรา 343 ถือเอาเจตนาแสดงข้อความอันเป็นเท็จต่อประชาชนเป็นสำคัญ โดยจะเห็นได้จากวิธีการหลอกลวง เมื่อจำเลยทั้งสี่กับพวกจัดตั้งระบบอุปกรณ์โทรศัพท์และระบบคอมพิวเตอร์ในรูปสำนักงานเครือข่ายโทรศัพท์ ขึ้นในต่างประเทศ และใช้การสื่อสารทางเสียงผ่านโครงข่ายอินเตอร์เน็ต ด้วยวิธีการสุ่มหมายเลขโทรศัพท์ของประชาชนที่ปรากฏข้อมูลอยู่ในระบบคอมพิวเตอร์ของจำเลยทั้งสี่กับพวก แล้วโทรศัพท์หรือส่งข้อความทางโทรศัพท์เคลื่อนที่ติดต่อไปยังประชาชนทั่วไป รวมทั้งประชาชนไทยในราชอาณาจักร และแจ้งแก่ผู้ที่ได้รับการติดต่อด้วยข้อความอันเป็นเท็จต่าง ๆ ในลักษณะอ้างตนเองเป็นเจ้าหน้าที่ของธนาคารพาณิชย์และเป็นเจ้าหน้าที่ของรัฐหลอกลวงผู้ได้รับการติดต่อว่า ผู้นั้นเป็นหนี้บัตรเครดิต หรือมียอดการใช้เงินในบัญชีสูงผิดปกติ ให้ไปตรวจดูยอดเงินในบัญชี หรือให้ไปดำเนินการเปลี่ยนแปลงรหัสข้อมูลเกี่ยวกับบัญชีธนาคารที่ประชาชนผู้ถูกหลอกลวงใช้บริการหรือให้ไปดำเนินการใส่รหัสผ่าน หรือรหัสสั่งให้ระงับการทำรายการในบัญชีเงินฝาก บัตรเบิกถอนเงินสดเอทีเอ็มหรือรหัสระงับบัญชีธนาคาร หรือรหัสป้องกันมิให้ข้อมูลรั่วไหล โดยแจ้งว่าเพื่อเป็นการป้องกันมิให้ผู้อื่นเบิกถอนเงินออกจากบัญชีของประชาชนผู้ถูกหลอกลวงได้ ซึ่งเป็นการหลอกลวงเหมือนกัน อันมีลักษณะเป็นการหลอกลวงทั่วไป มิได้มุ่งหมายเจาะจงหลอกลวงคนใดคนหนึ่งเป็นพิเศษ ขึ้นอยู่กับว่าจำเลยทั้งสี่กับพวกจะสุ่มได้หมายเลขโทรศัพท์ของประชาชนใดที่ปรากฏข้อมูลอยู่ในระบบคอมพิวเตอร์ของจำเลยทั้งสี่กับพวกเพื่อทำการหลอกลวง การกระทำของจำเลยทั้งสี่ตามฟ้องจึงเป็นการร่วมกันฉ้อโกงประชาชน

ได้ว่า การแอบอ้างสวมรอยเป็นบุคคลอื่นนั้นเป็นพฤติกรรมเบื้องต้นที่นำไปสู่การหลอกลวงฉ้อโกงในเวลาต่อมา

(ข) ความแตกต่าง

ความผิดฐานฉ้อโกงเป็นการกระทำความผิดที่มุ่งประสงค์ต่อสิทธิในทรัพย์สินของบุคคลอื่น คุณธรรมทางกฎหมายของความผิดฐานนี้จึงเป็นสิทธิในทรัพย์ ดังนั้น ผู้เสียหายในความผิดฐานฉ้อโกงจึงได้แก่ผู้ที่ถูกหลอกลวงและสูญเสียสิทธิในทรัพย์สินหรือได้ทำ ถอน หรือทำลายเอกสารสิทธิเนื่องมาจากการถูกหลอกลวง ในขณะที่การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการกระทำความผิดที่มุ่งประสงค์ต่อการแอบอ้างตัวตนของบุคคลอื่น เป็นการละเมิดต่อความเป็นส่วนตัวและข้อมูลส่วนบุคคลเพื่อให้เจ้าของตัวตนนั้นได้รับความเสียหาย ดังนั้น ผู้เสียหายในการกระทำความผิดนี้จึงได้แก่ บุคคลที่ถูกสวมรอย

กล่าวโดยสรุป ในปัจจุบันนี้ผู้กระทำความผิดฐานฉ้อโกงจำนวนหนึ่งเลือกใช้วิธีสวมรอยเป็นบุคคลอื่น ทำให้ผู้เสียหายหลงเชื่อในความเป็นตัวตนนั้น เพื่อหลอกลวงฉ้อโกงผู้เสียหายผ่านทางระบบเครือข่ายอินเทอร์เน็ต เนื่องจากการติดต่อสื่อสารและการทำธุรกรรมทางการเงินผ่านทางระบบอินเทอร์เน็ตนั้น ทั้งสองฝ่ายไม่จำเป็นต้องพบปะกันต่อหน้า แต่สามารถติดต่อกันโดยที่ไม่ทราบว่าอีกฝ่ายหนึ่งเป็นใคร ลักษณะเช่นนี้จึงเอื้ออำนวยให้เกิดการสวมรอยเป็นบุคคลอื่นผ่านทางเครือข่ายอินเทอร์เน็ตและหลอกลวงฉ้อโกงบุคคลอื่นได้ในวงกว้าง ไม่ว่าจะเป็นการสวมรอยเป็นบุคคลอื่นเพื่อฉ้อโกงทั่วไปหรือฉ้อโกงประชาชนก็ตาม ทั้งนี้ กฎหมายกำหนดให้การฉ้อโกงเป็นความผิดทางอาญาเพื่อมุ่งหมายจะคุ้มครองผู้ที่ถูกหลอกลวง ผู้ถูกหลอกลวงจึงเป็นผู้เสียหายในความผิดฐานนี้ แม้ว่าจะมีการบัญญัติถึงเหตุฉกรรจ์ว่าเป็นการหลอกลวงด้วยการแสดงตนเป็นคนอื่น แต่คนอื่นในที่นี้มิได้รับการคุ้มครองว่าเป็นผู้เสียหายในความผิดฐานฉ้อโกงด้วยแต่อย่างใด ด้วยเหตุนี้ ผู้ถูกสวมรอยในระบบเครือข่ายอินเทอร์เน็ตซึ่งถูกแอบอ้างไปเพื่อการฉ้อโกงจึงไม่ใช่ผู้เสียหายและไม่สามารถดำเนินคดีกับผู้กระทำความผิดฐานฉ้อโกงได้

3.1.3 ความผิดฐานปลอมเอกสาร

ประมวลกฎหมายอาญาบัญญัติฐานความผิดเกี่ยวกับการปลอมเอกสารไว้ ดังนี้

“มาตรา 264 ผู้ใดทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด เติม หรือตัดทอนข้อความ หรือแก้ไขด้วยประการใด ๆ ในเอกสารที่แท้จริง หรือประทับตราปลอม หรือลงลายมือชื่อปลอมในเอกสาร โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ถ้าได้กระทำเพื่อให้ ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็น

เอกสารที่แท้จริง ผู้นั้นกระทำความผิดฐานปลอมเอกสาร ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ...”

วัตถุแห่งการกระทำความผิดตามมาตรา 264 คือ “เอกสาร” ซึ่งเป็นสาระสำคัญขององค์ประกอบแห่งความรับผิด หากวัตถุที่ถูกปลอมแปลงนั้นมิใช่เอกสารในความหมายของประมวลกฎหมายอาญาเสียตั้งแต่ต้น ก็ไม่อาจนำองค์ประกอบแห่งความรับผิดอื่น ๆ มาพิจารณาต่อไปได้ และไม่ถือว่าเป็นการกระทำความผิดฐานปลอมเอกสาร ทั้งนี้ มาตรา 1 (7) แห่งประมวลกฎหมายอาญาได้กำหนดคำนิยามของ “เอกสาร” ไว้ว่า *“กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่นจะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น”*

เมื่อพิจารณาคำนิยามของเอกสารแล้วจะพบลักษณะสำคัญของเอกสาร ดังนี้ “เอกสาร” คือ กระดาษหรือวัตถุอื่นใดเป็นสิ่งที่ใช้รองรับถ้อยคำหรือข้อความที่ทำให้มีความหมายปรากฏขึ้น การปรากฏความหมายเช่นนี้ต้องเกิดจากการกระทำของมนุษย์ มิใช่การปรากฏขึ้นเองโดยสภาพแวดล้อมหรือการทำงานของอุปกรณ์เครื่องมือ ถ้อยคำหรือข้อความที่ปรากฏบนกระดาษหรือวัตถุอื่นใดนั้นต้องแสดงความหมายหรือความคิดของผู้ทำเอกสารออกมาในรูปแบบตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น ซึ่งสามารถอ่านหรือเห็นได้ทางตา แม้ว่าถ้อยคำหรือข้อความนั้นจะเป็นที่เข้าใจได้หรือไม่ก็ตาม หากเป็นสิ่งที่แสดงความคิดของผู้ทำเอกสารแล้วย่อมเรียกได้ว่ามีความหมายปรากฏอยู่ การทำเอกสารอาจเกิดขึ้นได้หลายวิธี เช่น การพิมพ์ ถ่ายภาพ เขียนด้วยมือ การตีตรา การแกะสลัก การพ่นสี เป็นต้น นอกจากนี้ วัตถุที่รองรับความหมายของถ้อยคำหรือข้อความที่จะถือว่าเป็นเอกสารได้จะต้องปรากฏคงทนอยู่ชั่วระยะเวลาหนึ่ง จึงจะเป็นหลักฐานแห่งความหมาย

เอกสารเป็นสิ่งที่มีความสำคัญเป็นอย่างยิ่งในทางกฎหมาย หากเอกสารนั้นสามารถนำไปใช้เป็นพยานหลักฐานได้ แสดงว่าเอกสารนั้นมีความน่าเชื่อถือและมีความมั่นคงในทางกฎหมาย ในทางกลับกัน หากมีการกระทำบางอย่างทำให้ความน่าเชื่อถือและความมั่นคงในทางกฎหมายของเอกสารลดน้อยถอยลง เอกสารนั้นก็ย่อมใช้เป็นพยานหลักฐานไม่ได้ ด้วยเหตุนี้ กฎหมายอาญาจึงมุ่งคุ้มครองคุณธรรมทางกฎหมายของความผิดเกี่ยวกับเอกสาร อันได้แก่ ความมั่นคงและความน่าเชื่อถือในการใช้เอกสารเป็นพยานหลักฐาน[30] โดยมีเจตนารมณ์ในการคุ้มครองเอกสารแบ่งได้เป็น 4 ประการ ได้แก่ การคุ้มครองความแท้จริงแห่งเอกสาร การคุ้มครองความถูกต้องแห่งเอกสาร การคุ้มครองการใช้เอกสาร และการคุ้มครองความปลอดภัยของเอกสาร[31]

---

[30] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, หน้า 662.

[31] เรื่องเดียวกัน, หน้า 240-241.

การคุ้มครองความแท้จริงแห่งเอกสารเป็นการพิจารณาในแง่ของบุคคลผู้ทำเอกสาร กล่าวคือ หากบุคคลนั้นมีอำนาจในการทำเอกสารย่อมแสดงว่าเอกสารที่ถูกจัดทำขึ้นเป็นเอกสารแท้จริง แต่หากบุคคลนั้นไม่มีอำนาจในการทำเอกสารเสียแล้ว ย่อมเรียกได้ว่าเป็นเอกสารปลอม แม้ว่าเอกสารดังกล่าวจะมีเนื้อหาตรงตามความเป็นจริงก็ตาม เอกสารที่ถูกทำขึ้นโดยมีข้อความไม่ตรงกับความเป็นจริงเช่นนี้ถือเป็นเอกสารเท็จ ซึ่งกฎหมายได้ให้ความคุ้มครองเนื้อหาแห่งเอกสารไว้โดยการบัญญัติให้การทำเอกสารเท็จเป็นความผิดทางอาญาในกรณีเฉพาะ เช่น มาตรา 162 ความผิดฐานเจ้าพนักงานทำเอกสารเท็จ มาตรา 267 ความผิดฐานแจ้งให้เจ้าพนักงานจดข้อความเท็จลงในเอกสาร เป็นต้น นอกจากนี้ยังมีคุณธรรมทางกฎหมายที่คุ้มครองการใช้เอกสารและคุ้มครองความปลอดภัยแห่งเอกสาร โดยมองว่า การที่บุคคลใดใช้เอกสารที่เกิดจากการกระทำความผิด ไม่ว่าจะเป็นการปลอมเอกสาร แปลงเอกสาร หรือทำเอกสารเท็จ ย่อมเป็นการกระทบต่อความน่าเชื่อถือของเอกสารนั้น รวมถึงการที่บุคคลกระทำการอันใดที่กระทบต่อความมั่นคงปลอดภัยของเอกสาร ถือว่าขัดต่อวัตถุประสงค์สำคัญของเอกสาร คือ การใช้เอกสารเป็นหลักฐานอ้างอิง กฎหมายจึงบัญญัติให้การกระทำเหล่านี้เป็นความผิดทางอาญา[32]

ความผิดฐานปลอมเอกสารมีลักษณะสำคัญในการกระทำความผิด 2 ประการ คือ การทำเอกสารไม่แท้จริงขึ้นใหม่ เช่น การทำเอกสารปลอมทั้งฉบับหรือแต่บางส่วน และการทำให้เอกสารแท้จริงผิดไปจากเดิม เช่น การเติม ตัดทอน หรือแก้ไขด้วยประการใด ๆ ในเอกสารแท้จริง

อย่างไรก็ตาม แม้ว่าจะมีการกระทำในทางกายภาพดังกล่าวข้างต้นต่อเอกสารก็ตาม แต่การกระทำอาจไม่เป็นความผิดฐานปลอมเอกสารได้ หากขาดองค์ประกอบภายนอกที่สำคัญอีกประการหนึ่ง ได้แก่ “โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน” ซึ่งเป็นพฤติการณ์ประกอบการกระทำ กล่าวคือ การกระทำดังกล่าวมีลักษณะที่น่าจะทำให้ผู้อื่นหรือประชาชนได้รับความเสียหาย ไม่ว่าจะเป็นความเสียหายต่อทรัพย์สิน ชื่อเสียง หรือกระทบต่อความไว้เนื้อเชื่อใจของประชาชน[33] นอกจากนี้ องค์ประกอบภายในที่สำคัญของความผิดฐานปลอมเอกสาร ได้แก่ เจตนา ซึ่งแบ่งเป็น 2 ประเภท ได้แก่ เจตนาธรรมดา คือ ผู้กระทำต้องรู้ข้อเท็จจริงอันเป็นองค์ประกอบของความผิดและประสงค์จะกระทำการบางอย่างที่กฎหมายห้ามไว้ เช่น ผู้กระทำทราบดีว่าตนเองไม่มีอำนาจทำเอกสารนั้น และประสงค์จะทำเอกสารนั้นขึ้นหรือประสงค์จะลงลายมือชื่อปลอม เป็นต้น และเจตนาพิเศษ “เพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง” ซึ่งกฎหมายมิได้กำหนดว่าเป็น

---

[32] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, คำอธิบายความผิดเกี่ยวกับการปลอมและการแปลงตามประมวลกฎหมายอาญา (กรุงเทพมหานคร: วิญญูชน, 2555), หน้า 117-118.

[33] สมศักดิ์ เอี่ยมพลับใหญ่, กฎหมายอาญาภาคความผิดเกี่ยวกับความเท็จ การปลอมและการแปลง (กรุงเทพมหานคร: นิติธรรม, 2554), หน้า 157.

บุคคลใดบุคคลหนึ่งโดยเฉพาะเจาะจง หากผู้กระทำได้กระทำการปลอมเอกสารโดยเจตนาให้บุคคลใด ๆ หลงเชื่อว่าเป็นเอกสารที่แท้จริงแล้ว ก็ย่อมมีความผิดฐานปลอมเอกสาร[34]

ในอดีต ผู้คนมีวิธีการทำเอกสารในรูปแบบดั้งเดิมซึ่งสามารถอ่านหรือมองเห็นด้วยตาเปล่าได้อย่างชัดเจน เช่น การเขียนตัวอักษรลงบนกระดาษด้วยมือ การแกะสลักตราสัญลักษณ์ การพ่นสีเป็นตัวเลขหรือรหัสบนอุปกรณ์เครื่องมือต่าง ๆ เป็นต้น แต่เมื่อโลกก้าวเข้ามาสู่ยุคแห่งเทคโนโลยีสมัยใหม่ การสื่อความหมายผ่านทางถ้อยคำหรือข้อความจึงได้รับการพัฒนาขึ้นให้สามารถแสดงออกซึ่งความคิดด้วยวิธีการทางอิเล็กทรอนิกส์ โดยการป้อนข้อมูลซึ่งมีความหมายผ่านทางระบบคอมพิวเตอร์มีการประมวลผลด้วยโปรแกรมคอมพิวเตอร์และซอฟต์แวร์ และแสดงข้อความหรือรูปภาพผ่านทางหน้าจออุปกรณ์ทางอิเล็กทรอนิกส์ต่าง ๆ เช่น คอมพิวเตอร์ โทรศัพท์มือถือ เครื่องพิมพ์ เครื่องถ่ายเอกสาร เป็นต้น และเนื่องด้วยในปัจจุบันนี้ ผู้คนต่างส่งข้อความหรือรูปภาพเข้าสู่ระบบคอมพิวเตอร์และระบบอินเทอร์เน็ตกันเป็นจำนวนมาก ไม่ว่าจะเป็นการสร้างและเขียนบทความลงเว็บไซต์ การส่งข้อความและแนบไฟล์เอกสารผ่านทางจดหมายอิเล็กทรอนิกส์ การเขียนข้อความลงบนเว็บไซต์เครือข่ายสังคมออนไลน์ต่าง ๆ จึงเป็นที่น่าพิจารณาว่า ข้อมูลที่ถูกนำเข้าสู่ระบบคอมพิวเตอร์และแสดงให้ปรากฏซึ่งความหมายผ่านทางหน้าจออุปกรณ์อิเล็กทรอนิกส์เช่นนี้ ถือว่าเป็นเอกสารตามประมวลกฎหมายอาญาหรือไม่

คำว่า “ข้อมูลคอมพิวเตอร์” มีความหมายตามมาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังนี้ *“ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย”* ซึ่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้ให้ความหมายของคำว่า “ข้อมูลอิเล็กทรอนิกส์” ไว้ตามมาตรา 4 ดังนี้ *“ข้อมูลอิเล็กทรอนิกส์ หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร”*

นอกจากนี้ มาตรา 8 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้กำหนดหลักเกณฑ์การใช้ข้อมูลอิเล็กทรอนิกส์ในฐานะของเอกสารไว้ดังนี้

> *“ภายใต้บังคับบทบัญญัติแห่งมาตรา 9 ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำ*

---

[34] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, คำอธิบายความผิดเกี่ยวกับการปลอมและการแปลงตามประมวลกฎหมายอาญา, หน้า 124.

ข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว”

จากบทบัญญัติข้างต้นจะเห็นได้ว่า ข้อความที่ถูกนำเข้าสู่ระบบคอมพิวเตอร์อาจถือว่าเป็นเอกสารได้ก็ต่อเมื่อข้อความนั้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยมีความหมายคงเดิม ด้วยเหตุนี้ การพิมพ์ข้อความลงบนแพลตฟอร์มออนไลน์ต่าง ๆ เช่น เว็บไซต์ เว็บบอร์ด จึงอาจถือเป็นเอกสารได้ แต่ทั้งนี้ ต้องถือว่าเป็นเอกสารตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เท่านั้น มิใช่เป็นเอกสารตามประมวลกฎหมายอาญา เนื่องจากลักษณะของข้อมูลคอมพิวเตอร์เช่นนี้ไม่ตรงกับลักษณะของเอกสารตามคำนิยามในมาตรา 1 (7) ดังนี้[35]

(1) สิ่งที่ใช้รองรับถ้อยคำ ข้อความ หรือรูปแบบแผนที่แสดงความหมายของเอกสาร คือ กระดาษหรือวัตถุอื่นใด ส่วนสิ่งที่ใช้รองรับข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ คือ สื่อบันทึกข้อมูลอิเล็กทรอนิกส์ต่าง ๆ เช่น ฮาร์ดดิสก์ (Hard Disk) เมโมรีการ์ด (Memory Card) เป็นต้น

(2) การทำให้ปรากฏความหมายในเอกสารเกิดจากการกระทำของมนุษย์เป็นผู้พิมพ์ ถ่ายภาพ หรือใช้วิธีอื่นใดทำให้ปรากฏความหมายนั้น ทำให้บุคคลสามารถอ่านหรือเห็นข้อความหรือสิ่งอื่นที่สื่อความหมายบนกระดาษหรือวัตถุอื่นใดได้ ส่วนการทำให้มีข้อมูลปรากฏขึ้นบนสื่อบันทึกข้อมูลอิเล็กทรอนิกส์นั้นเกิดจากการทำงานโดยอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ ประมวลผลด้วยโปรแกรมหรือซอฟต์แวร์ต่าง ๆ โดยมีมนุษย์เป็นเพียงตัวกลางเชื่อมโยงการทำงาน และมีการแสดงผลของการประมวลผลทางคอมพิวเตอร์ผ่านอุปกรณ์แสดงผล เช่น หน้าจอคอมพิวเตอร์ หน้าจอโทรศัพท์เคลื่อนที่ ดังนั้นจึงกล่าวได้อีกนัยหนึ่งว่า การปรากฏข้อความหรือรูปภาพบนหน้าจออุปกรณ์อิเล็กทรอนิกส์เป็นผลมาจากการทำงานของระบบคอมพิวเตอร์ มนุษย์จึงสามารถอ่านข้อความหรือเห็นรูปภาพนั้นได้ มิได้อ่านหรือเห็นข้อมูลคอมพิวเตอร์ที่อยู่ในสื่อบันทึกอิเล็กทรอนิกส์โดยตรงแต่อย่างใด

(3) ความหมายที่ปรากฏในเอกสาร คือ สิ่งที่ผู้ทำเอกสารได้แสดงความคิดออกมาให้มีความหมาย ไม่ว่าบุคคลอื่นจะเข้าใจหรือไม่ก็ตาม ส่วนความหมายของข้อมูลคอมพิวเตอร์แบ่งได้เป็น 2 ลักษณะ ได้แก่ (1) ข้อมูลที่มนุษย์นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งแสดงถึงความคิดของ

---

[35] พรทิพย์ ตัณฑวนันท์, "อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์" (วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต, คณะนิติศาสตร์, มหาวิทยาลัยธรรมศาสตร์, 2548), หน้า 13-16.

ผู้นำเข้าข้อมูล และ (2) ข้อมูลที่ถูกประมวลผลด้วยระบบคอมพิวเตอร์กลายเป็นภาษาคอมพิวเตอร์ทำให้ระบบคอมพิวเตอร์เข้าใจความหมายและทำงานได้

(4) คำว่า “เป็นหลักฐานแห่งความหมาย” หมายถึง ต้องปรากฏคงทนอยู่ชั่วระยะเวลาหนึ่งจึงจะเป็นเอกสาร มนุษย์สามารถเห็นข้อมูลคอมพิวเตอร์ปรากฏออกมาได้หลายวิธี เช่น การพิมพ์ข้อความหรือรูปภาพลงบนกระดาษหรือวัตถุอื่นใด การแสดงผลข้อมูลคอมพิวเตอร์ทางจอภาพ สำหรับกรณีที่สองนี้ การแสดงผลทางจอภาพเกิดจากวิธีการทางอิเล็กทรอนิกส์ เป็นการทำงานของสัญญาณไฟฟ้าที่ส่งผ่านไปมาตามระบบ ข้อมูลคอมพิวเตอร์ที่อยู่ระหว่างการทำงานของระบบคอมพิวเตอร์เช่นนี้ไม่ถือว่าเป็นหลักฐานแห่งความหมาย เนื่องจากมีการเคลื่อนที่ของข้อมูลได้ตลอดเวลา เมื่อเลื่อน เปลี่ยน ปิด แก้ไข หรือลบข้อมูลที่ปรากฏบนหน้าจอ หรือปิดการทำงานระบบคอมพิวเตอร์ ข้อมูลดังกล่าวก็ไม่สามารถปรากฏเป็นหลักฐานแห่งความหมายที่คงทนให้บุคคลสามารถอ่านหรือเห็นได้ตลอดเวลา จึงไม่เป็นเอกสาร[36]

นอกจากนี้ อาจารย์เข็มชัย ชุติวงศ์ เคยให้ความเห็นไว้ว่า *“ข้อมูลคอมพิวเตอร์มีการสื่อความหมายขึ้นมาบนหน้าจอเหมือนกับเอกสาร แต่ขาดคุณสมบัติของเอกสารอีกข้อหนึ่งคือไม่มีวัตถุรองรับ หากปิดเครื่องไปแล้วข้อความก็จะหายไป แม้จะมีการบันทึกไว้ในเทปบันทึกข้อมูล แต่ก็ไม่สามารถมองเห็นได้ด้วยตาเปล่า ต้องอาศัยอุปกรณ์อื่นช่วยจึงจะอ่านข้อความได้”*[37]

ด้วยเหตุผลดังกล่าวข้างต้น การสร้างข้อความด้วยระบบคอมพิวเตอร์ไม่เป็นเอกสาร ดังนั้น การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตด้วยวิธีการพิมพ์ข้อความหรือใส่รูปภาพลงบนเว็บไซต์ หรือส่งเป็นจดหมายอิเล็กทรอนิกส์ หรือผ่านทางแพลตฟอร์มออนไลน์อื่น ๆ จึงไม่ครบองค์ประกอบความผิดฐานปลอมเอกสารตามประมวลกฎหมายอาญา

3.2 กฎหมายที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตตามพระราชบัญญัติอื่น

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตมีลักษณะและรูปแบบการกระทำความผิดที่เกี่ยวโยงกันหลายส่วน ทั้งเป็นการกระทำโดยอาศัยระบบคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือ และยังเป็นการกระทำต่อสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลของผู้อื่น เพราะฉะนั้นการกระทำดังกล่าวจึงมีกฎหมายที่เกี่ยวข้องและสมควรนำมาพิจารณาหลายฉบับ

---

[36] รัฐสิทธิ์ คุรุสุวรรณ, "ความหมายทางอาญาของคำว่า “เอกสาร”" (วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขาวิชานิติศาสตร์ คณะนิติศาสตร์, จุฬาลงกรณ์มหาวิทยาลัย, 2534), หน้า 127.

[37] การบรรยายวิชา กฎหมายลักษณะพยานหลักฐาน วันอังคารที่ 6 มกราคม 2541, หน้า 157-158.

ในส่วนนี้ผู้เขียนจะอธิบายถึงกฎหมายระดับพระราชบัญญัติที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตจำนวน 2 ฉบับ ได้แก่ (1) พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับที่แก้ไขเพิ่มเติม และ (2) ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

3.2.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับที่แก้ไขเพิ่มเติม

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีขึ้นเพื่อป้องกันและปราบปรามการกระทำที่เกิดขึ้นกับระบบคอมพิวเตอร์ซึ่งทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้หรือทำงานผิดพลาด หรือใช้วิธีการใด ๆ เพื่อล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะลามก ด้วยเหตุที่พระราชบัญญัติดังกล่าวมีเจตนารมณ์ป้องกันมิให้เกิดความเสียหายอันเนื่องมาจากการใช้ระบบคอมพิวเตอร์[38] ดังนั้น พระราชบัญญัติฉบับนี้จึงเกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ซึ่งเป็นการกระทำความผิดที่อาศัยระบบคอมพิวเตอร์เป็นเครื่องมือ โดยมีบทบัญญัติสำคัญที่เกี่ยวข้อง ได้แก่ ความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมหรือเป็นเท็จตามมาตรา 14 (1)

“มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน...”

---

[38] เหตุผลในการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 “เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูลแก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพรข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้”

การกระทำความผิดตามมาตรา 14 (1) เกิดขึ้นเมื่อผู้กระทำความผิดเจตนานำข้อมูลคอมพิวเตอร์ปลอมหรือเท็จเข้าสู่ระบบคอมพิวเตอร์ หมายความว่า ผู้กระทำต้องรู้สำนึกในขณะกระทำและรู้ว่าข้อมูลคอมพิวเตอร์นั้นเป็นข้อมูลคอมพิวเตอร์ปลอมหรือเท็จ[39]

การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ หมายถึง ผู้กระทำความผิดได้นำข้อมูลดังกล่าวเข้าสู่ระบบคอมพิวเตอร์ด้วยวิธีการบันทึกหรือดาวน์โหลดข้อมูลจากแหล่งจัดเก็บที่หนึ่งไปยังระบบคอมพิวเตอร์[40] ไม่ว่าผู้นั้นจะเป็นผู้ที่ทำการปลอมข้อมูลคอมพิวเตอร์หรือไม่ก็ตาม

“ข้อมูลคอมพิวเตอร์ปลอม” หมายถึง ข้อมูลคอมพิวเตอร์ที่ถูกปลอมแปลง โดยอาจเป็นการนำเข้าสู่ระบบคอมพิวเตอร์อย่างถูกต้องหรือไม่ถูกต้องในครั้งแรก หรือเป็นการปลอมแปลงทั้งหมดหรือบางส่วน รวมทั้งการลบข้อมูลโดยการย้ายข้อมูลออกจากสิ่งที่ใช้ในการบันทึกข้อมูลเป็นเหตุให้ข้อมูลนั้นผิดไปจากต้นฉบับ[41] อาจกล่าวอีกนัยหนึ่งได้ว่า ข้อมูลคอมพิวเตอร์ปลอมคือข้อมูลคอมพิวเตอร์ที่ถูกจัดทำขึ้นใหม่ทั้งหมดหรือเพียงบางส่วนโดยผู้ที่ไม่มีอำนาจหรือไม่ได้รับมอบอำนาจให้ทำ เพื่อให้เข้าใจว่าเป็นข้อมูลคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้น

ข้อมูลคอมพิวเตอร์ที่เป็นองค์ประกอบของฐานความผิดตามมาตรา 14 (1) แบ่งออกเป็น 3 ประเภท ได้แก่ (1) ข้อมูลคอมพิวเตอร์ปลอมทั้งหมด หมายถึง ข้อมูลคอมพิวเตอร์ที่ผู้กระทำความผิดได้สร้างขึ้นทั้งหมด โดยมีเจตนาให้ผู้อื่นเข้าใจว่าข้อมูลนั้นเป็นข้อมูลที่แท้จริง และไม่จำเป็นต้องมีข้อมูลคอมพิวเตอร์ที่แท้จริงอยู่ก่อนก็ได้ (2) ข้อมูลคอมพิวเตอร์ปลอมบางส่วน หมายถึง ข้อมูลคอมพิวเตอร์ที่ถูกเปลี่ยนแปลงหรือแก้ไขเฉพาะส่วนใดส่วนหนึ่ง และ (3) ข้อมูลคอมพิวเตอร์อันเป็นเท็จ หมายถึง ข้อมูลคอมพิวเตอร์ที่ไม่ตรงกับข้อมูลจริง[42] ทั้งนี้ ข้อมูลคอมพิวเตอร์อันเป็นเท็จอาจถูกทำขึ้นโดยผู้ที่มีอำนาจหรือไม่มีอำนาจทำข้อมูลนั้นก็ได้ สาระสำคัญไม่ได้อยู่ที่ตัวบุคคลผู้ทำข้อมูลคอมพิวเตอร์ แต่อยู่ที่ข้อมูลคอมพิวเตอร์นั้นไม่ตรงกับความเป็นจริง ต่างจากข้อมูลคอมพิวเตอร์ปลอมซึ่งถูกทำขึ้นโดยผู้ที่ไม่มีอำนาจ แต่ทำขึ้นในนามของผู้อื่น ดังนั้น ข้อมูลคอมพิวเตอร์ปลอมจึงอาจเป็นได้ทั้งข้อมูลที่เป็นความจริงและข้อมูลที่เป็นความเท็จ[43]

---

[39] มานิตย์ จุมปา, คำอธิบายกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (กรุงเทพมหานคร: วิญญูชน, 2553), หน้า 92.

[40] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ = Information Technology Law, หน้า 297.

[41] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, แนวทางการจัดทำกฎหมายอาชญากรรมคอมพิวเตอร์, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร: สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, 2547), หน้า 32.

[42] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ = Information Technology Law, หน้า 297.

[43] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 164-165.

นอกจากนี้ การกระทำจะครบองค์ประกอบความผิดเมื่อได้กระทำไปโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ซึ่งเป็นพฤติการณ์ประกอบการกระทำความผิดฐานนี้ แม้ว่าจะไม่เกิดความเสียหายขึ้นจริงก็ตาม[44]

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น ตามเจตนารมณ์ของผู้ร่างกฎหมายแล้วมีขึ้นเพื่อควบคุมดูแลการกระทำที่ทำให้เกิดความเสียหายต่อระบบในทางเทคนิคเท่านั้น[45] แต่ภายหลังการประกาศใช้พระราชบัญญัติแล้วพบว่ามีการฟ้องร้องคดีตามบทบัญญัติในพระราชบัญญัติดังกล่าวเป็นจำนวนมาก ทั้งที่จริงแล้วสามารถฟ้องร้องเป็นความผิดตามกฎหมายสารบัญญัติอื่นที่เกี่ยวข้องโดยตรงได้ เช่น กรณีการเขียนข้อความหรือโพสรูปภาพใส่ความผู้อื่นบนเว็บไซต์ โดยประการที่น่าจะทำให้ผู้อื่นนั้นถูกดูหมิ่น เกลียดชัง หรือเสื่อมเสียชื่อเสียง เป็นการหมิ่นประมาทในระบบออนไลน์ ซึ่งสามารถนำมาตรา 423 แห่งประมวลกฎหมายแพ่งและพาณิชย์[46] หรือความผิดฐานหมิ่นประมาทด้วยการโฆษณาตามมาตรา 326 ประกอบกับมาตรา 328 แห่งประมวลกฎหมายอาญามาบังคับใช้ได้ ไม่จำเป็นต้องดำเนินคดีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่อย่างใด[47]

ปัญหาสำคัญประการหนึ่งคือ การตีความมาตรา 14 (1) ที่ผิดไปจากเจตนารมณ์ที่แท้จริง กล่าวคือ มาตรา 14 (1) มีขึ้นเพื่ออุดช่องว่างของความผิดฐานปลอมแปลงเอกสารตามกฎหมายอาญา องค์ประกอบของมาตราดังกล่าว คือ การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมซึ่งถูกทำขึ้นโดยผู้ที่ไม่มีอำนาจตามกฎหมายที่จะทำข้อมูลนั้น หรือการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูล

---

[44] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ = Information Technology Law, หน้า 297.

[45] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, "พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14(1) ยาแรงผิดขนานสำหรับการหมิ่นประมาทออนไลน์" [ออนไลน์] เข้าถึงเมื่อ 9 พฤศจิกายน 2557. แหล่งที่มา: https://freedom.ilaw.or.th/blog/

[46] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 423 “ผู้ใดกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนต่อความจริง เป็นที่เสียหายแก่ชื่อเสียงหรือเกียรติคุณของบุคคลอื่นก็ดี หรือเป็นที่เสียหายแก่ทางทำมาหาได้ หรือทางเจริญของเขาโดยประการอื่นก็ดี ท่านว่าผู้นั้นจะต้องใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อความเสียหายอย่างใด ๆ อันเกิดแต่การนั้น แม้ทั้งเมื่อตนมิได้รู้ว่าข้อความนั้นไม่จริง แต่หากควรจะรู้ได้

ผู้ใดส่งข่าวสารอันตนมิได้รู้ว่าเป็นความไม่จริง หากว่าตนเองหรือผู้รับข่าวสารนั้นมีทางได้เสียโดยชอบในการนั้นด้วยแล้ว ท่านว่าเพียงที่ส่งข่าวสารเช่นนั้นหาทำให้ผู้นั้นต้องรับผิดใช้ค่าสินไหมทดแทนไม่”

[47] สาวิตรี สุขศรี, ศิริพล กุศลศิลป์วุฒิ, and อรพิณ ยิ่งยงพัฒนา, อาชญากรรมคอมพิวเตอร์? : งานวิจัยหัวข้อ “ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น (กรุงเทพมหานคร: โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw) ในมูลนิธิอาสาสมัครเพื่อสังคม, 2555), หน้า 82.

แท้จริงที่ถูกทำขึ้นโดยผู้ที่มีอำนาจโดยชอบตามกฎหมาย แต่ต่อมามีการแก้ไขเปลี่ยนแปลงทำให้ข้อมูลนั้นมีความหมายแตกต่างไปจากเดิม[48]

อย่างไรก็ตาม เนื่องด้วยรัฐบาลมีนโยบายในการบริหารประเทศโดยมุ่งพัฒนาและส่งเสริมเศรษฐกิจและสังคมในยุคดิจิทัล (Digital Economy) จึงจำเป็นต้องยกร่างแก้ไขปรับปรุงกฎหมายที่เกี่ยวข้อง ทั้งนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ได้ดำเนินการจัดทำชุดร่างกฎหมายเพื่อการส่งเสริมเศรษฐกิจและสังคม หรือชุดกฎหมายเศรษฐกิจดิจิทัล (Digital Economy) โดยมีกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้เสนอชุดร่างกฎหมายดังกล่าวต่อคณะรัฐมนตรี และคณะรัฐมนตรีได้พิจารณาให้ความเห็นชอบในหลักการของชุดร่างกฎหมายแล้ว เมื่อวันที่ 16 ธันวาคม พ.ศ. 2557 และวันที่ 6 มกราคม พ.ศ. 2558

ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ..) พ.ศ. .... เป็นหนึ่งในกฎหมายที่ถูกยกมาพิจารณาแก้ไขปรับปรุงและถูกรวมอยู่ในชุดร่างกฎหมายเศรษฐกิจดิจิทัล โดยมีวัตถุประสงค์หลักในการแก้ไขปรับปรุงพระราชบัญญัติคือ ต้องการลดปัญหาและข้อจำกัดในการใช้อำนาจของพนักงานเจ้าหน้าที่ รวมทั้งเพื่อให้การป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพมากยิ่งขึ้น เนื่องจากเทคโนโลยีที่พัฒนาก้าวหน้าในปัจจุบันทำให้ปัญหาภัยคุกคามทางคอมพิวเตอร์เพิ่มจำนวนมากขึ้นเรื่อย ๆ อันจะส่งผลกระทบต่อความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ เพิ่มโอกาสสร้างความเสียหายแก่โครงสร้างพื้นฐานของประเทศ และอาจนำไปสู่ปัญหาทางสังคมที่รุนแรงมากขึ้น[49] จึงจำเป็นต้องแก้ไขเพิ่มเติมฐานความผิดบางฐานเพื่อรัฐจะได้มีมาตรการทางกฎหมายที่ชัดเจนในการปกป้องความสงบสุขของสังคม

ทั้งนี้ มาตรา 14 (1) ถูกยกขึ้นพิจารณาแก้ไขปรับปรุงองค์ประกอบของฐานความผิดให้มีความเหมาะสม ชัดเจน และตรงตามเจตนารมณ์แต่เดิมของมาตราดังกล่าว คือมุ่งเอาผิดจากผู้ที่สร้างเว็บไซต์ปลอมเพื่อหลอกลวงฉ้อโกงผู้บริโภคให้หลงเชื่อเข้ามาติดต่อดำเนินธุรกรรมต่าง ๆ (Phishing) รวมถึงการแฝงตัวด้วยการนำข้อมูลคอมพิวเตอร์ปลอมเข้าสู่ระบบคอมพิวเตอร์เพื่อทำลายระบบคอมพิวเตอร์

ตามร่างพระราชบัญญัติฉบับที่คณะรัฐมนตรีรับหลักการนั้น มีการแก้ไขเพิ่มเติมมาตรา 14 (1) ดังนี้

> *“ร่างมาตรา 6 ให้ยกเลิกความในมาตรา 14 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน*

---

[48] เรื่องเดียวกัน, หน้า 82-83.

[49] สำนักงานคณะกรรมการกฤษฎีกา, “บันทึกสำนักงานคณะกรรมการกฤษฎีกาประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ..) พ.ศ. .... เรื่องเสร็จที่ 919/2558,” (เอกสารไม่ตีพิมพ์เผยแพร่)

มาตรา 14 (1) ผู้ใดโดยทุจริตนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จทำให้ได้ไปซึ่งทรัพย์สินหรือข้อมูลส่วนบุคคลของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำความผิดตามวรรคหนึ่ง ได้กระทำด้วยการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จต่อประชาชน ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้"

ต่อมา เมื่อคณะรัฐมนตรีรับหลักการและส่งร่างพระราชบัญญัติไปยังคณะกรรมการกฤษฎีกาเพื่อพิจารณาร่างและส่งกลับมายังคณะรัฐมนตรีพิจารณาให้ความเห็นชอบก่อนส่งต่อไปยังสภานิติบัญญัติแห่งชาติเพื่อพิจารณาร่างนั้น ได้มีการแก้ไขเพิ่มเติมองค์ประกอบของมาตรา 14 (1) อีกครั้งท้ายที่สุด พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ถูกประกาศใช้ในราชกิจจานุเบกษา เล่ม 134 ตอนที่ 10 ก เมื่อวันที่ 24 มกราคม พ.ศ. 2560 โดยมีเหตุผลในการประกาศใช้พระราชบัญญัติดังนี้

"โดยที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็ว และโดยที่มีการจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งมีภารกิจในการกำหนดมาตรฐานและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ สมควรปรับปรุงบทบัญญัติในส่วนที่เกี่ยวกับผู้รักษาการตามกฎหมาย กำหนดฐานความผิดขึ้นใหม่ และแก้ไขฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ตลอดจนกำหนดให้มีคณะกรรมการเปรียบเทียบซึ่งมีอำนาจเปรียบเทียบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และแก้ไขเพิ่มเติมอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้"

ด้วยเหตุผลดังกล่าวข้างต้น มาตรา 14 (1) จึงถูกแก้ไขปรับปรุงให้สามารถบังคับใช้กับการกระทำความผิดเกี่ยวกับข้อมูลคอมพิวเตอร์ได้ตรงตามเจตนารมณ์ของกฎหมายมากยิ่งขึ้น

ทั้งนี้ คณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ..) พ.ศ. .... สภานิติบัญญัติแห่งชาติ ได้ตั้งข้อสังเกตเกี่ยวกับการแก้ไขมาตรา 14 ไว้ ดังนี้ *“เหตุผลที่บัญญัติเพิ่มเติมว่าการกระทำความผิดตามมาตรา 14 (1) อันมิใช่ความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญานั้น เพื่อให้เห็นเจตนารมณ์ที่ชัดเจนว่ากรณีที่การกระทำความผิดดังกล่าวเป็นความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญาแล้วไม่ถือว่าเป็นความผิดตามมาตรา 14 (1)”*[50]

ตารางที่ 1 ตารางเปรียบเทียบการแก้ไขปรับปรุงมาตรา 14 (1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560**
มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน	มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

เมื่อพิจารณามาตรา 14 (1) ที่ถูกแก้ไขใหม่แล้วพบข้อสังเกตหลายประการดังต่อไปนี้

(1) มีการเพิ่มเติมองค์ประกอบของฐานความผิดในส่วนของเจตนาพิเศษ ได้แก่ “โดยทุจริต หรือโดยหลอกลวง” ซึ่งคำว่า “โดยทุจริต” มีความหมายตามมาตรา 1 (1) แห่งประมวล

[50] สำนักกรรมาธิการสำนักงานเลขาธิการวุฒิสภา ปฏิบัติหน้าที่สำนักงานเลขาธิการสภานิติบัญญัติแห่งชาติ, “รายงานของคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ..) พ.ศ. .... สภานิติบัญญัติแห่งชาติ,” 9 ธันวาคม 2559.

กฎหมายอาญา[51] แสดงให้เห็นว่า มาตรา 14 (1) ที่ได้รับการแก้ไขปรับปรุงนั้น มีเจตนารมณ์ในการป้องกันและปราบปรามการกระทำความผิดในลักษณะการทุจริต หลอกลวง หรือฉ้อโกงโดยอาศัยระบบคอมพิวเตอร์เป็นเครื่องมือ ซึ่งเป็นปัญหาที่พบมากในยุคสมัยปัจจุบันที่มีการพัฒนาด้านเทคโนโลยีคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ต ทำให้เกิดการกระทำความผิดเช่นนี้อย่างแพร่หลาย เช่น การสร้างเว็บไซต์หรือส่งจดหมายอิเล็กทรอนิกส์ปลอมไปยังบุคคลอื่น เพื่อหลอกลวงให้หลงเชื่อและกรอกข้อมูลส่วนบุคคล ผู้กระทำความผิดจะนำข้อมูลเหล่านั้นไปใช้ในทางมิชอบและก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล หรือที่เรียกว่า ฟิชชิ่ง (Phishing) รวมถึงการหลอกลวงขายสินค้าออนไลน์ หรือการหลอกลวงในรูปแบบอื่น ๆ ผ่านทางระบบเครือข่ายอินเทอร์เน็ต เป็นต้น

(2) ตามร่างมาตรา 6 ข้างต้นกำหนดให้การกระทำความผิดเป็นเหตุให้ผู้กระทำความผิดได้ไปซึ่งทรัพย์สินหรือข้อมูลส่วนบุคคลของผู้อื่น แม้ว่าในภายหลังคณะกรรมการกฤษฎีกาจะตัดองค์ประกอบนี้ออกไป แต่ก็แสดงให้เห็นว่ามาตรา 14 (1) มีวัตถุประสงค์เน้นไปที่การกระทำที่มุ่งต่อประโยชน์ทางทรัพย์สิน มิใช่การแสดงความคิดเห็นผ่านทางระบบเครือข่ายอินเทอร์เน็ต

(3) นอกจากนี้ เมื่อพิจารณาเนื้อหาของฐานความผิดดังกล่าวแล้วจะเห็นว่ามีพฤติการณ์ประกอบการกระทำคือ “โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน” ซึ่งแตกต่างจากมาตรา 14 (1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งใช้ถ้อยคำว่า “โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน” อีกทั้งมาตรา 14 (1) ใหม่ยังกำหนดให้การกระทำความผิดดังกล่าวที่กระทำต่อปัจเจกชนคนใดคนหนึ่งเป็นความผิดอันยอมความได้ แสดงให้เห็นว่า มาตราดังกล่าวมุ่งคุ้มครองประโยชน์ของสาธารณชนเป็นสำคัญยิ่งกว่าเอกชน เนื่องจากหากเกิดการกระทำความผิดในลักษณะเช่นนี้โดยพุ่งเป้าไปที่ประชาชนซึ่งมีจำนวนมากก็ย่อมมีโอกาสที่จำนวนผู้เสียหายจะเพิ่มสูงขึ้นตามไปด้วย และยังกระทบต่อความสงบสุขของสาธารณชนในภาพรวมมากกว่ากระทำต่อบุคคลใดบุคคลหนึ่งโดยเฉพาะเจาะจง

จากที่กล่าวข้างต้นว่า มาตรา 14 (1) ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มีเจตนารมณ์เพื่อคุ้มครองประโยชน์ของสาธารณชน ด้วยเหตุนี้จึงไม่อาจนำมาปรับใช้กับกรณีการกระทำความผิดฐานหมิ่นประมาทด้วยการอาศัยระบบคอมพิวเตอร์หรือระบบเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือได้ เนื่องจากการกระทำความผิดทั้งสองฐานมีคุณธรรมทางกฎหมายที่แตกต่างกัน กล่าวคือ ความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญามี

---

[51] ประมวลกฎหมายอาญา มาตรา 1 “ในประมวลกฎหมายนี้ (1) "โดยทุจริต" หมายความว่าเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น”

คุณธรรมทางกฎหมายที่มุ่งคุ้มครองชื่อเสียงเกียรติคุณและศักดิ์ศรีของผู้ถูกใส่ความเป็นสำคัญ แต่ความผิดตามมาตรา 14 (1) แห่งร่างพระราชบัญญัตินี้มีคุณธรรมทางกฎหมายที่มุ่งคุ้มครองประโยชน์สาธารณะเป็นสำคัญ[52]

ด้วยเหตุนี้ เมื่อพิจารณาเปรียบเทียบกับลักษณะของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตแล้วจะเห็นได้ว่า การสวมรอยเป็นบุคคลอื่นเกิดขึ้นเมื่อมีการใช้ข้อมูลส่วนบุคคลของผู้อื่นสร้างข้อมูลคอมพิวเตอร์ขึ้นที่ก่อให้เกิดความเสียหายต่อผู้อื่นหรือบุคคลที่สาม ข้อมูลส่วนบุคคลดังกล่าวจึงเป็นข้อมูลที่แท้จริงของบุคคลที่ถูกสวมรอย มิใช่ข้อมูลปลอมที่สร้างขึ้นใหม่หรือมีการแก้ไขเปลี่ยนแปลงข้อมูลดังกล่าว เพราะหากมีการแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคล ข้อมูลนั้นย่อมมิใช่ข้อมูลที่สามารถพิสูจน์ตัวตนของบุคคลที่ถูกสวมรอยได้อีกต่อไป เพราะฉะนั้นการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตจึงไม่ตรงกับองค์ประกอบตามเจตนารมณ์ที่แท้จริงของมาตรา 14 (1)

ทั้งนี้ ในกรณีที่ผู้กระทำความผิดสวมรอยเป็นบุคคลอื่นผ่านเครือข่ายอินเทอร์เน็ตโดยมีเจตนาพิเศษโดยทุจริตหรือหลอกลวงผู้อื่น ย่อมถือได้ว่าเป็นรูปแบบหนึ่งของการกระทำความผิดตามมาตรา 14 (1) แต่อย่างไรก็ตาม การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตนั้นมีขอบเขตของเจตนาพิเศษกว้างกว่าเจตนาพิเศษของมาตรา 14 (1) กล่าวคือ การสวมรอยเป็นบุคคลอื่นอาจเกิดขึ้นโดยมีวัตถุประสงค์เพื่อประทุษร้ายหรือข่มขู่คุกคามผู้อื่นได้อีกด้วย

อนึ่ง การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอาจเกิดขึ้นจากการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของผู้ถูกสวมรอยโดยไม่ได้รับอนุญาตได้อีกทางหนึ่ง กล่าวคือ เมื่อผู้ไม่ประสงค์ดีเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของผู้อื่นที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และสวมรอยเป็นเจ้าของข้อมูลคอมพิวเตอร์นั้นเพื่อกระทำการอย่างหนึ่งอย่างใดที่ไม่ชอบด้วยกฎหมาย ย่อมทำให้ผู้ถูกสวมรอยได้รับความเสียหาย การเข้าถึงโดยมิชอบเช่นนี้เป็นความผิดตามมาตรา 5[53] และมาตรา 7[54] แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และหากมีการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ไม่ว่า

---

[52] สำนักเลขาธิการนายกรัฐมนตรี, “ตารางเปรียบเทียบพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ..) พ.ศ. ....,” 26 เมษายน 2559. (เอกสารไม่ตีพิมพ์เผยแพร่)

[53] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 “ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ”

[54] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 7 “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ”

ทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ถือเป็นความผิดตามมาตรา 9[55] อีกประการหนึ่งด้วย ตัวอย่างเช่น นาย ก. อนุญาตให้ นาย ข. เข้าถึงบัญชีผู้ใช้งานของตนเพื่อลงทะเบียนรายวิชาแทนตน การที่ นาย ข. เข้ารหัสผ่านเพื่อเข้าถึงข้อมูลคอมพิวเตอร์ของ นาย ก. นั้นไม่เป็นความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ เนื่องจาก นาย ข. ได้รับอนุญาตจากเจ้าของข้อมูลคอมพิวเตอร์แล้ว หากต่อมา นาย ข. แอบเข้ารหัสผ่านเพื่อเข้าใช้งานบัญชีของ นาย ก. โดยมีเจตนาถอนรายวิชาของ นาย ก. ออก ทำให้ นาย ก. ได้รับความเสียหาย กรณีเช่นนี้ นาย ข. ย่อมมีความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบตามมาตรา 7 เนื่องจาก นาย ข. ไม่มีอำนาจหรือได้รับอนุญาตจาก นาย ก. แม้ในครั้งแรกจะได้รับอนุญาตก็ตาม แต่เป็นการอนุญาตเพื่อให้ นาย ข. ลงทะเบียนรายวิชาแทน นาย ก. เฉพาะครั้งแรกเท่านั้น เมื่อนาย ข. เข้าถึงข้อมูลคอมพิวเตอร์เกินกว่าที่ตนได้รับอนุญาต ย่อมต้องรับผิด[56] อีกทั้งการถอนรายวิชาเป็นการเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของ นาย ก. โดยมิชอบ จึงเป็นความผิดตามมาตรา 9 อีกด้วย

3.2.2 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มีบทบัญญัติให้การรับรองและคุ้มครองสิทธิส่วนบุคคลของประชาชนชาวไทยไว้ในมาตรา 32 ความว่า

“บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ”

จะเห็นได้ว่า รัฐธรรมนูญฉบับนี้บัญญัติความคุ้มครองสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลไว้อย่างชัดเจน เป็นการรับรองว่าประชาชนทุกคนมีสิทธิส่วนบุคคลอันเป็นสิทธิขั้นพื้นฐานที่ไม่อาจถูกก้าวก่ายหรือล่วงละเมิดได้ รวมถึงคุ้มครองประชาชนจากการถูกแทรกแซงความเป็นส่วนตัวหรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ในทางมิชอบ

ทั้งนี้ รัฐธรรมนูญเป็นเพียงกฎหมายสูงสุดที่ให้การรับรองและคุ้มครองสิทธิทั้งหลายของประชาชนเท่านั้น เพื่อให้การบริหารจัดการบ้านเมืองเป็นไปด้วยความสงบเรียบร้อย จึงจำเป็นต้องมี

---

[55] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 9 “ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

[56] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 140.

กฎหมายระดับพระราชบัญญัติกำหนดกฎเกณฑ์ต่าง ๆ ให้สอดคล้องกับบทบัญญัติตามรัฐธรรมนูญ ดังนั้น เมื่อรัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติรับรองและคุ้มครองสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลไว้แล้ว จึงควรมีกฎหมายระดับพระราชบัญญัติที่เกี่ยวข้องกับเรื่องดังกล่าวด้วย แต่ทว่าในปัจจุบันประเทศไทยยังไม่มีกฎหมายเฉพาะเพื่อคุ้มครองสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลเป็นการทั่วไป มีเพียงกฎหมายเฉพาะเรื่องซึ่งนำมาปรับใช้เฉพาะกรณี เช่น พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 บังคับใช้เพื่อคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานรัฐ พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 บังคับใช้ในเรื่องข้อมูลเครดิตของบุคคล หรือพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 บังคับใช้ในเรื่องข้อมูลการติดต่อสื่อสารระหว่างบุคคล ส่วนกรณีที่มีการละเมิดและสร้างความเสียหายแก่เจ้าของสิทธิส่วนบุคคลหรือข้อมูลส่วนบุคคลก็มีกฎหมายที่เกี่ยวข้องเพื่อแก้ไขเยียวยาปัญหาเฉพาะกรณี เช่น ความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา หรือการชดใช้ค่าสินไหมทดแทนในคดีละเมิดตามประมวลกฎหมายแพ่งและพาณิชย์ เป็นต้น[57]

ด้วยเหตุผลความจำเป็นที่ว่า สิทธิส่วนบุคคลและข้อมูลส่วนบุคคลเป็นสิทธิขั้นพื้นฐานที่สำคัญของมนุษย์ทุกคน และเพื่อป้องกันมิให้สิทธิดังกล่าวถูกกระทบกระเทือนจากการล่วงละเมิด คณะรัฐมนตรีจึงมีมติเห็นชอบให้ปฏิรูปกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเมื่อ พ.ศ. 2539 โดยมอบหมายให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติดำเนินการยกร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลขึ้นตามแนวทางของข้อบังคับสหภาพยุโรป 95/46/EC (European Union Directive 95/46/EC) และกฎหมายต้นแบบจากประเทศต่าง ๆ เช่น Protection of Individuals and Other Subjects with regard to the Processing of Personal Data Act ของสาธารณรัฐอิตาลี Data Protection Act 1998 ของสหราชอาณาจักร Privacy Act 1988 ของเครือรัฐออสเตรเลีย Privacy Act 1993 ของประเทศนิวซีแลนด์ เป็นต้น

ทั้งนี้ ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ได้รับการเสนอต่อสภาผู้แทนราษฎรและหน่วยงานทางฝ่ายนิติบัญญัติต่าง ๆ เพื่อพิจารณาและแก้ไขปรับปรุงเรื่อยมา แต่ยังพิจารณาไม่แล้วเสร็จและยังไม่ได้ประกาศใช้ในราชกิจจานุเบกษา จนกระทั่งรัฐบาลชุดปัจจุบันได้เสนอร่างพระราชบัญญัติดังกล่าวต่อสภานิติบัญญัติแห่งชาติเพื่อพิจารณาเมื่อเดือนตุลาคม พ.ศ. 2557 และได้ยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลขึ้นรวมเป็นส่วนหนึ่งของชุดกฎหมายเศรษฐกิจดิจิทัล ซึ่งคณะรัฐมนตรีได้รับหลักการและส่งให้คณะกรรมการกฤษฎีกาพิจารณาตรวจร่างแล้ว ปรากฏตามเรื่องเสร็จที่ 1135/2558

---

[57] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ = Information Technology Law, หน้า 250.

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มีหลักการและเหตุผล ดังนี้

“ให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าวสามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้”

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... แบ่งออกเป็น 7 หมวด ได้แก่ หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล หมวด 4 ข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล หมวด 5 การร้องเรียน หมวด 6 ความรับผิดทางแพ่ง และหมวด 7 บทกำหนดโทษ

แต่เดิมร่างพระราชบัญญัติดังกล่าวได้กำหนดคำนิยามของ “ข้อมูลส่วนบุคคล” ไว้ในร่างมาตรา 3 ให้หมายความว่า *“ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย”* ต่อมาในการพิจารณาชุดร่างกฎหมายเศรษฐกิจดิจิทัล คณะกรรมการกฤษฎีกาได้แก้ไขปรับปรุงคำนิยามของ “ข้อมูลส่วนบุคคล” ให้หมายความว่า *“ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”*

อนึ่ง นอกจากผู้ที่เป็นเจ้าของข้อมูลส่วนบุคคลจะหมายถึงบุคคลธรรมดาที่เป็นเจ้าของข้อมูลดังกล่าวข้างต้นแล้ว ยังให้หมายความรวมถึง (1) ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ (2) ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ และ (3) ผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

นอกจากนี้ ในส่วนของบทกำหนดโทษนั้น ร่างพระราชบัญญัติฉบับเดิมก่อนเปลี่ยนมาเป็นชุดร่างกฎหมายเศรษฐกิจดิจิทัลได้กำหนดโทษไว้ 2 ประเภท ได้แก่

(1) โทษปรับทางปกครอง กำหนดให้ผู้อำนวยการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการเป็นผู้มีอำนาจปรับทางปกครอง โดยคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิดและความเสียหายที่เกิดจากการกระทำนั้นเป็นสำคัญ

(2) โทษอาญา กำหนดให้ผู้ที่ฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติที่ระบุไว้มีความรับผิดทางอาญาและต้องระวางโทษปรับ รวมทั้งได้กำหนดถึงการกระทำความผิดที่มีทั้งโทษจำคุกและโทษปรับไว้ตามร่างมาตรา 58 ดังนี้

> *“มาตรา 58 ผู้ใดกระทำการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย หรือเพื่อให้ผู้อื่นเสียหาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ*
>
> *ถ้าการกระทำตามวรรคหนึ่งเป็นการเผยแพร่ข้อมูลส่วนบุคคลทางสิ่งพิมพ์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หรือสื่ออิเล็กทรอนิกส์อื่น ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”*

จะเห็นได้ว่า บทบัญญัติข้างต้นเป็นการกำหนดให้การกระทำความผิดต่อข้อมูลส่วนบุคคลของผู้อื่นเป็นเหตุให้ผู้อื่นได้รับความเสียหายเป็นความผิดอาญา พร้อมกับกำหนดอัตราโทษจำคุกและโทษปรับไว้ค่อนข้างสูง เพื่อให้ผู้ที่จะกระทำความผิดเกิดความเกรงกลัว เป็นความพยายามในการยับยั้งมิให้เกิดการล่วงละเมิดข้อมูลส่วนบุคคล

แต่อย่างไรก็ตาม เมื่อร่างพระราชบัญญัติถูกนำเสนอต่อคณะรัฐมนตรีอีกครั้งในฐานะของกฎหมายเศรษฐกิจดิจิทัล พบว่ามีการแก้ไขปรับปรุงหมวด 7 บทกำหนดโทษ โดยตัดบทกำหนดโทษทางปกครองและโทษอาญาออก และเพิ่มเติมบทกำหนดโทษสำหรับผู้ควบคุมข้อมูลส่วนบุคคลที่ฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติมาตราอื่นซึ่งกำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามร่างพระราชบัญญัตินี้ รวมทั้งบทกำหนดโทษแก่บุคคลในกรณีต่าง ๆ เช่น ผู้ที่ต่อสู้หรือขัดขวางพนักงานเจ้าหน้าที่ในการปฏิบัติตามพระราชบัญญัตินี้ ผู้ที่ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้และนำไปเปิดเผยแก่ผู้อื่น เป็นต้น

กล่าวโดยสรุป ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ถูกยกร่างขึ้นเพื่อกำหนดหลักเกณฑ์สำหรับการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามหลักสากล เนื่องจากข้อมูลส่วนบุคคลเป็นสิทธิขั้นพื้นฐานของมนุษย์ที่ได้รับติดตัวมาตั้งแต่เกิด ซึ่งในปัจจุบันเกิดปัญหาการล่วงละเมิดข้อมูลส่วนบุคคลในลักษณะต่าง ๆ เป็นจำนวนมาก สร้างความเสียหายและส่งผลกระทบต่อเจ้าของ

ข้อมูลส่วนบุคคลอย่างกว้างขวาง ด้วยเหตุเช่นว่านี้ ร่างพระราชบัญญัติดังกล่าวจึงมีหลักการสำคัญในการคุ้มครองด้วยการกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ก็ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเสียก่อน นอกจากนี้ ยังกำหนดหลักเกณฑ์เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงสิทธิต่าง ๆ ที่เจ้าของข้อมูลส่วนบุคคลพึงได้รับและมาตรการเยียวยาในกรณีที่ข้อมูลส่วนบุคคลถูกละเมิดอีกด้วย[58]

3.3 สภาพปัญหาในประเทศไทย

ประเทศไทยเป็นอีกประเทศหนึ่งที่มีจำนวนผู้ใช้งานอินเทอร์เน็ตเพิ่มขึ้นเรื่อย ๆ และมีปริมาณการใช้งานเว็บไซต์เครือข่ายสังคมออนไลน์ค่อนข้างสูง คนไทยจำนวนมากที่มีบัญชีผู้ใช้งานเว็บไซต์เหล่านั้นมักเขียนแจ้งข่าวคราวความเคลื่อนไหวของตนลงบนหน้าเว็บไซต์หรือแบ่งปันข้อมูลข่าวสารต่าง ๆ ให้สมาชิกคนอื่นทราบ ทำให้การกระจายข้อมูลข่าวสารเป็นไปอย่างกว้างขวางและรวดเร็ว นอกจากนี้ยังมีการสร้างกิจกรรมต่าง ๆ เกิดขึ้นบนเว็บไซต์อินเทอร์เน็ต เช่น การรวมกลุ่มของผู้คนที่มีความชอบในสิ่งเดียวกัน การแบ่งปันความรู้ รูปภาพ หรือแม้แต่การเขียนโฆษณาสินค้าจากผู้ใช้งานจริง เป็นต้น หากกิจกรรมดังกล่าวได้รับความนิยมจากผู้ใช้งานอินเทอร์เน็ต ผู้ที่สร้างกิจกรรมอาจได้รับความนิยม เป็นที่รู้จัก หรือมีชื่อเสียงไปด้วย เรียกได้ว่าเป็นการสร้างตัวตนของบุคคลคนหนึ่งขึ้นมาในโลกไร้พรมแดน ด้วยเหตุนี้เองจึงมีผู้ไม่หวังดีจำนวนหนึ่งที่อาศัยความเป็นตัวตนของบุคคลประกอบกับความสะดวกรวดเร็วของระบบอินเทอร์เน็ตในการกระทำความผิดด้วยการสวมรอยเป็นบุคคลอื่นและก่อให้เกิดความเสียหายแก่บุคคลนั้นหรือบุคคลอื่นที่เกี่ยวข้อง

ความเสียหายที่เกิดจากการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอาจส่งผลกระทบต่อผู้ถูกสวมรอยและบุคคลที่สามได้หลายด้าน ในส่วนนี้ผู้เขียนจะอธิบายถึงผลกระทบที่เกิดจากการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต พร้อมทั้งเหตุผลสนับสนุนว่ากฎหมายที่มีอยู่ในปัจจุบันของประเทศไทยไม่สามารถปรับใช้กับการกระทำความผิดดังกล่าวได้ทุกกรณี โดยแบ่งผลกระทบออกเป็น 3 ด้านดังต่อไปนี้

---

[58] สำนักงานคณะกรรมการกฤษฎีกา, “บันทึกสำนักงานคณะกรรมการกฤษฎีกาประกอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เรื่องเสร็จที่ 1135/2558,” (เอกสารไม่ตีพิมพ์เผยแพร่)

3.3.1 ผลกระทบด้านชื่อเสียง

ตัวอย่างเหตุการณ์

- ผู้ประกาศข่าวชื่อดังคนหนึ่งถูกผู้ไม่หวังดีนำรูปภาพไปสร้างบัญชีเฟสบุ๊กปลอม และเขียนข้อความที่ไม่เหมาะสม ให้ร้ายองค์กรและบุคคลอื่น รวมทั้งมีข้อความที่ทำให้ผู้ประกาศข่าวคนดังกล่าวเสียหายด้วย[59] ซึ่งเจ้าหน้าที่ตำรวจได้ตั้งข้อหาแก่ผู้กระทำผิดไว้เป็นความผิดตามพระราชบัญญัติการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14 (5) และฐานหมิ่นประมาทด้วยการโฆษณาตามมาตรา 328 แห่งประมวลกฎหมายอาญา[60]

- ดาราตลกชื่อดังคนหนึ่งถูกสวมรอยผ่านทางเว็บไซต์เฟสบุ๊ก โดยผู้สวมรอยได้สร้างแฟนเพจในชื่อของดาราตลกคนดังกล่าว พร้อมทั้งเขียนข้อความและมีภาพประกอบบอกเล่าเรื่องราวที่ดาราตลกรายนี้ทำมาในช่วงเวลาต่าง ๆ อีกทั้งมีการโพสภาพกิจกรรมทางการเมืองและคำหยาบคายต่าง ๆ นอกจากนี้ผู้สวมรอยยังประกาศเชิญชวนให้บุคคลที่ติดตามแฟนเพจบริจาคเงินช่วยกิจกรรมการกุศลและจำหน่ายสินค้าต่าง ๆ อีกด้วย การกระทำดังกล่าวทำให้ดาราตลกรายนี้ได้รับความเสียหายด้านชื่อเสียงเป็นอย่างมาก[61]

3.3.2 ผลกระทบด้านทรัพย์สิน

ตัวอย่างเหตุการณ์

- ภริยาของดารานักแสดงชายคนหนึ่งถูกนำชื่อไปแอบอ้างเพื่อขายสินค้าผ่านทางเครือข่ายสังคมออนไลน์ เช่น เฟสบุ๊ก อินสตาแกรม เป็นต้น และหลอกลวงให้ผู้เสียหายโอนเงินค่าสินค้ามาให้ แต่ไม่ส่งสินค้าให้แก่ผู้เสียหาย[62]

---

[59] ไอที 24 ชั่วโมง, "ถูกคนอื่นปลอมเป็นเราบน Facebook ทำให้เสียหาย แก้ไขอย่างไร?" [ออนไลน์] เข้าถึงเมื่อ 9 ธันวาคม 2557. แหล่งที่มา: http://www.it24hrs.com/2013/how-to-report-facebook-profile-fake/

[60] ทวีพร คุ้มเมธา, รายงานพลเมืองเน็ต 2556 = Thai Netizen's Report 2013 (กรุงเทพมหานคร: เครือข่ายพลเมืองเน็ต, 2557), หน้า 30.

[61] เดลินิวส์, "โน้สอุดมถูกปลอมเฟสบุ๊ก แถมขู่กรรโชกทรัพย์" [ออนไลน์] เข้าถึงเมื่อ 26 กุมภาพันธ์ 2558. แหล่งที่มา: http://www.dailynews.co.th/Content/crime/

[62] ข่าวสด, "หนุ่ม คงกระพัน ควงภรรยาโร่แจ้งกองปราบฯ ถูกแอบอ้างสวมรอยเป็นเมียหลอกขายสินค้าผ่านเฟซบุ๊ก" [ออนไลน์] เข้าถึงเมื่อ 9 ธันวาคม 2558. แหล่งที่มา: http://www.khaosod.co.th/view_newsonline.php?newsid=TVRRd016RTFOVEkyTVE9PQ==

- เฟสบุ๊กชื่อว่า “เงินด่วน ทันใจ” มีการนำรูปภาพของผู้เสียหายไปสร้างเป็นเฟสบุ๊กใหม่ และขึ้นรูปภาพของธนาคารออมสินประกอบเพื่อความน่าเชื่อถือ อีกทั้งสวมรอยเป็นผู้เสียหายเขียนข้อความสนับสนุนเฟสบุ๊กของตนเอง โดยมีจุดประสงค์เพื่อต้มตุ๋นหลอกลวงเงินของบุคคลอื่น[63]

- นางเอกสาวชื่อดังของประเทศไทยถูกสวมรอยในแอพพลิเคชั่น LINE โดยผู้สวมรอยได้ตั้งชื่อผู้ใช้งานเป็นชื่อของนางเอกสาวและใช้รูปภาพของนางเอกสาวประกอบ กระทำการพูดคุยกับบุคคลอื่นเพื่อหลอกลวงให้ทำธุรกรรมทางการเงิน พบว่ามีผู้เสียหายหลงเชื่อหลายราย[64]

3.3.3 ผลกระทบด้านความเป็นส่วนตัว

ตัวอย่างเหตุการณ์

- กรณีนำรูปหญิงสาวคนหนึ่งไปแอบอ้างในเว็บไซต์เฟสบุ๊กและเขียนข้อความเกี่ยวกับการเมือง เป็นเหตุให้เจ้าของรูปถูกผู้ใช้งานอินเทอร์เน็ตจำนวนมากด่าทอและข่มขู่[65]

- นิสิตคนหนึ่งถูกผู้ไม่ประสงค์ดีใช้ข้อมูลและรูปภาพในเฟสบุ๊กสร้างบัญชีผู้ใช้งานเฟสบุ๊กใหม่ ทำการสวมรอยเป็นนิสิตคนดังกล่าวและหลอกลวงขายโทรศัพท์มือถือให้แก่บุคคลอื่นซึ่งเป็นเพื่อนในเฟสบุ๊กของนิสิต รวมทั้งหลอกเอาเงินจากนักร้องคนหนึ่งได้ไปถึง 30,000 บาท กรณีนี้นิสิตคนดังกล่าวได้รับความเสียหายเนื่องจากถูกนำข้อมูลส่วนบุคคลไปใช้กระทำความผิดและมีหมายเรียกจากศาลมาที่บ้านของนิสิตด้วย[66]

ดังนี้จะเห็นได้ว่า การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตนั้น นอกจากจะเป็นการละเมิดสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลของเจ้าของข้อมูลแล้ว ยังส่งผลกระทบต่อทั้งเจ้าของข้อมูลส่วนบุคคลนั้นและผู้อื่นอีกหลายประการ ไม่ว่าจะเป็นความเสียหายต่อชื่อเสียง ผลประโยชน์ ทรัพย์สิน ตำแหน่งหน้าที่การงาน และอื่น ๆ นับได้ว่าเป็นปัญหาที่ควรได้รับการแก้ไขอย่างจริงจัง ตลอดจนหาแนวทางป้องกันและลดอัตราการเกิดอาชญากรรมดังกล่าว ทั้งนี้เพื่อให้สมาชิกในสังคมสามารถดำเนินชีวิตอยู่ได้อย่างปกติสุข

---

[63] Mookook, "เตือนภัยเฟสบุคเงินด่วนทันใจ อย่าได้หลงกลเป็นเหยื่อ" [ออนไลน์] เข้าถึงเมื่อ 26 กุมภาพันธ์ 2558. แหล่งที่มา: http://pantip.com/topic/31691770

[64] SpokedarkTV, "มือดีสวมรอยอั้ม พัชราภา ป่วนปลอมไลน์หลอกทำธุรกรรมทางการเงิน" [ออนไลน์].

[65] ไอที 24 ชั่วโมง, "ผู้ใช้เน็ตระวัง หลังสาวน้อยโดนแอบอ้าง ถูกใช้ภาพมาตัดต่อ แชร์ Facebook โยงการเมือง" [ออนไลน์] เข้าถึงเมื่อ 26 กุมภาพันธ์ 2558. แหล่งที่มา: http://stars.spokedark.tv/2015/02/19/fake-line/#.VO9BRPmsWSo

[66] MThai News, "จับสาวแสบ! สวมรอยเป็นดาวจุฬา หลอกตุ๋นเงิน-ขายมือถือทางเฟสบุ๊ค" [ออนไลน์] เข้าถึงเมื่อ 26 กุมภาพันธ์ 2558. แหล่งที่มา: http://news.mthai.com/hot-news/general-news/96450.html

โดยภาพรวมของการศึกษามาตรการทางอาญาที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทย ทำให้ทราบว่าประเทศไทยยังไม่มีบทบัญญัติที่กำหนดให้การกระทำดังกล่าวเป็นความผิดอาญาไว้โดยตรง อีกทั้งการพิจารณานำบทบัญญัติความผิดฐานอื่น ๆ มาปรับใช้ก็ไม่อาจคุ้มครองผู้ถูกสวมรอยได้อย่างครอบคลุมเพียงพอ จึงสมควรศึกษากฎหมายของต่างประเทศว่ามีการกำหนดมาตรการทางอาญาเพื่อป้องกันและปรามปรามปัญหานี้ไว้อย่างไร เพื่อพิจารณาความเหมาะสมในการนำมาปรับใช้กับประเทศไทยต่อไป

บทที่ 4
มาตรการทางอาญาที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของต่างประเทศ

เมื่อเทคโนโลยีระบบเครือข่ายอินเทอร์เน็ตเจริญก้าวหน้ามากขึ้น การเชื่อมต่อระหว่างผู้คนที่อยู่ต่างสถานที่กันจึงเป็นไปโดยง่าย เกิดเว็บไซต์เครือข่ายสังคมออนไลน์จำนวนมาก กลายเป็นแหล่งรวมตัวของผู้ใช้งานอินเทอร์เน็ตจากทั่วทุกมุมโลก การติดต่อสื่อสารผ่านทางระบบอินเทอร์เน็ตเช่นนี้มีทั้งข้อดีและข้อเสีย ข้อดีของการติดต่อสื่อสารผ่านทางระบบดังกล่าวคือ ความสะดวกรวดเร็วในการส่งข้อมูลระหว่างผู้ใช้งาน และยังเป็นการประหยัดทรัพยากรที่ต้องใช้ในการติดต่อสื่อสารในสมัยก่อนอย่างกระดาษหรือน้ำมันรถอีกด้วย ในทางกลับกัน การติดต่อสื่อสารผ่านทางระบบเครือข่ายอินเทอร์เน็ตก็มีข้อเสียหลายประการ เช่น ส่วนใหญ่แล้วเป็นการติดต่อสื่อสารกันผ่านทางตัวหนังสือหรือรูปภาพ ผู้ใช้งานจึงอาจไม่ทราบว่าบุคคลที่กำลังติดต่อด้วยนั้นแท้ที่จริงแล้วเป็นใคร หรืออาจไม่มีการเปิดเผยตัวตนที่แท้จริงในสังคมออนไลน์ จึงไม่อาจเชื่อถือได้เต็มร้อยว่ากิจกรรมที่ดำเนินการผ่านทางระบบอินเทอร์เน็ตนั้นจะส่งผลดีต่อผู้ใช้งานอย่างแท้จริง ด้วยเหตุนี้ ผู้ไม่ประสงค์ดีจำนวนมากจึงอาศัยช่องทางการติดต่อสื่อสารดังกล่าวเป็นเครื่องมือกระทำความผิดด้วยการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต โดยจะอาศัยตัวตนปลอมนั้นไปกระทำความผิดอย่างอื่นหรือไม่ก็ได้ กรณีเช่นนี้ก่อให้เกิดความเสียหายต่อทั้งเจ้าของข้อมูลที่ถูกนำไปแอบอ้างหรือยังส่งผลเสียหายต่อผู้อื่นที่เข้ามาเกี่ยวข้องหรือเป็นเหยื่อของการสวมรอยนี้ด้วย

ในบทที่ผ่านมา ผู้เขียนได้ศึกษาถึงสภาพปัญหาการสวมรอยบนเครือข่ายอินเทอร์เน็ตของประเทศไทย รวมถึงบทบัญญัติแห่งกฎหมายที่เกี่ยวข้องกับการกระทำความผิดดังกล่าว ทำให้ทราบว่าบทบัญญัติที่มีอยู่ในปัจจุบันของประเทศไทยไม่อาจปรับใช้กับข้อเท็จจริงที่เกิดขึ้นจากการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตได้ครอบคลุมทุกกรณี ดังนั้นจึงสมควรศึกษาว่าต่างประเทศมีกฎหมาย มาตรการ หรือแนวทางในการดำเนินการกับผู้กระทำความผิดฐานนี้อย่างไร เนื่องจากหลายประเทศทั่วโลกต่างเริ่มให้ความสำคัญต่อการแก้ไขปัญหาการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต บางประเทศได้ออกกฎหมายเพื่อบังคับใช้แก่การกระทำความผิดดังกล่าวเป็นการเฉพาะ ในขณะที่อีกหลายประเทศไม่มีการออกกฎหมายเฉพาะสำหรับความผิดดังกล่าว แต่นำกฎหมายที่มีอยู่มาปรับใช้กับข้อเท็จจริงที่เกิดขึ้นเป็นกรณีไป

ในบทนี้ผู้เขียนจะศึกษาถึงมาตรการทางกฎหมายอาญาที่เกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของต่างประเทศจำนวน 4 ประเทศ ได้แก่ สหรัฐอเมริกา สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี เพื่อให้ทราบว่าแต่ละประเทศมีสภาพปัญหา แนวคิด และมาตรการทางกฎหมายในการดำเนินการกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอย่างไร ทั้งนี้ เหตุที่ผู้เขียนสนใจเลือกศึกษากฎหมายของประเทศดังกล่าวเนื่องมาจากว่า สหรัฐอเมริกาเป็นประเทศแรกที่มีมาตรการทางอาญาสำหรับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการเฉพาะด้วยการบัญญัติเป็นฐานความผิดอาญาและกำหนดมาตรการบังคับทั้งทางอาญาและแพ่งไว้ในกฎหมายระดับมลรัฐ ในขณะที่สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลีต่างไม่มีบทบัญญัติกำหนดให้การกระทำดังกล่าวเป็นความผิดเฉพาะ แต่ถึงกระนั้น สหราชอาณาจักรมีการจัดทำคู่มือแนวทางการฟ้องคดีที่เกี่ยวข้องกับสื่อสังคม ซึ่งได้กำหนดหลักเกณฑ์การพิจารณานำกฎหมายที่มีอยู่แล้วมาปรับใช้ ส่วนประเทศญี่ปุ่นและสาธารณรัฐเกาหลีเป็นประเทศในกลุ่มกฎหมายซีวิลลอว์หรือประเทศที่ใช้กฎหมายลายลักษณ์อักษร จึงมีแนวทางการนำบทบัญญัติความผิดฐานอื่นที่เกี่ยวข้องมาปรับใช้แก่การสวมรอยเป็นบุคคลอื่นที่เกิดขึ้นผ่านระบบเครือข่ายอินเทอร์เน็ตเช่นกัน

4.1 สหรัฐอเมริกา

สหรัฐอเมริกาเป็นประเทศที่ประชากรใช้งานอินเทอร์เน็ตเป็นจำนวนมาก เว็บไซต์หรือแอพพลิเคชั่นเครือข่ายสังคมออนไลน์ (Social Networking Sites : SNSs) ที่มีชื่อเสียงและเป็นที่นิยมใช้กันทั่วโลกมักมีแหล่งกำเนิดมาจากสหรัฐอเมริกา เช่น เฟซบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) ยูทูบ (YouTube) จีเมล (Gmail) เป็นต้น ในขณะที่ผู้คนในสังคมอาศัยสิ่งเหล่านี้เป็นเครื่องมือในการสื่อสาร เหล่าอาชญากรก็ใช้สิ่งเหล่านั้นเป็นช่องทางในการกระทำความผิดเช่นเดียวกัน ปรากฏเป็นเหตุการณ์สวมรอยเป็นบุคคลอื่นผ่านวิธีการทางอิเล็กทรอนิกส์ ทั้งนี้ หน่วยงานภาครัฐที่เกี่ยวข้องได้เริ่มตระหนักถึงความสำคัญในการกำหนดมาตรการทางกฎหมายที่ชัดเจนเพื่อป้องกันและปราบปรามการสวมรอยดังกล่าว ในปัจจุบันสหรัฐอเมริกาเป็นประเทศเดียวที่มีกฎหมายระดับมลรัฐเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการเฉพาะ เรียกว่า Online Impersonation Law ในส่วนนี้ ผู้เขียนจะอธิบายถึงประเด็นปัญหาและกฎหมายเฉพาะเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในสหรัฐอเมริกา เพื่อให้ทราบถึงแนวคิดของผู้ยกร่างกฎหมาย สาระสำคัญ

ของบทบัญญัติ องค์ประกอบของฐานความผิด และตัวอย่างการนำบทบัญญัติไปปรับใช้กับการกระทำความผิดที่เกิดขึ้น

4.1.1 ประเด็นปัญหาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในสหรัฐอเมริกา

ปัญหาการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตกลายเป็นภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นในโลกไซเบอร์ของสหรัฐอเมริกาซึ่งนับวันจะมีเพิ่มมากขึ้นเรื่อย ๆ เมื่อพิจารณาลักษณะการกระทำผิดที่เกิดขึ้นจะสามารถแบ่งวิธีการสวมรอยออกเป็น 2 รูปแบบ วิธีการแรกคือ การสร้างบัญชีเว็บไซต์สื่อสังคมออนไลน์ปลอมในนามของบุคคลอื่นและใช้ตัวตนปลอมนั้นในการติดต่อสื่อสารผ่านทางระบบเครือข่ายอินเทอร์เน็ต อีกวิธีการหนึ่งคือ การขโมยรหัสผ่านของเหยื่อหรือเข้าถึงบัญชีของเหยื่อทางอ้อมและสวมรอยเป็นเหยื่อด้วยการใช้งานบัญชีนั้น[1] ซึ่งไม่ว่าจะเป็นการกระทำรูปแบบใดย่อมสร้างความเสียหายแก่เหยื่อได้หลายแง่มุม ทั้งด้านชีวิตความเป็นอยู่ ด้านชื่อเสียงเกียรติคุณ ด้านทรัพย์สินและการเงิน หรือด้านสภาพจิตใจและอารมณ์

คดีที่เป็นที่จับตามองและเป็นจุดเริ่มต้นของความพยายามในการยกร่างกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในสหรัฐอเมริกา คือ คดีของ Megan Meier ซึ่งเมแกนได้ตกเป็นเหยื่อของการแอบอ้างเป็นบุคคลอื่นผ่านทางเว็บไซต์สื่อสังคมออนไลน์ (Social Media) แม้ว่าในคดีดังกล่าวจะไม่ใช่การสวมรอยเป็นบุคคลที่มีตัวตนอยู่จริง แต่ด้วยลักษณะพื้นฐานของการติดต่อสื่อสารผ่านระบบเครือข่ายอินเทอร์เน็ตซึ่งบุคคลสามารถสื่อสารระหว่างกันได้โดยไม่จำเป็นต้องพบปะหน้าค่าตากันโดยตรง ผู้กระทำผิดจึงอาศัยช่องว่างนี้ในการแอบอ้างเป็นบุคคลสมมติและใช้ข้อความข่มขู่คุกคามเมแกน จนกระทั่งเมแกนตัดสินใจปลิดชีวิตตนเอง คดีนี้เป็นหนึ่งในคดีสำคัญที่จุดประกายความตื่นตัวและความตระหนักรู้ถึงภัยอันตรายอันเกิดจากการสวมรอยเป็นบุคคลอื่นบนโลกไซเบอร์ ศาลรัฐบาลกลาง (Federal Court) ของสหรัฐอเมริกาพบว่ามีความยากลำบากในการนำบทบัญญัติที่ยังเคลือบคลุมมาปรับใช้ในคดีนี้ ทั้งนี้ ในครั้งแรก เจ้าหน้าที่ของมลรัฐมิสซูรีตัดสินใจว่าจะไม่ดำเนินการฟ้องร้องจำเลย เนื่องจากไม่มีข้อหาความผิดทางอาญาที่สามารถปรับใช้กับการกระทำความผิดของจำเลย แต่ในภายหลังสำนักงานอัยการแห่งนครลอสแองเจลิสได้ ดำเนินคดีกับจำเลยตาม

[1] Reznik, M., "Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation," Touro Law Review: 457.

พระราชบัญญัติว่าด้วยการฉ้อโกงทางคอมพิวเตอร์และการใช้คอมพิวเตอร์โดยมิชอบ (Computer Fraud and Abuse Act)[2]

นอกจากคดีของ Megan Meier แล้ว ยังมีคดีที่เกิดขึ้นในลักษณะคล้ายคลึงกันอีกเป็นจำนวนมาก ยกตัวอย่างเช่น ในมลรัฐนิวเจอร์ซีย์ Dana Thornton ตกเป็นจำเลยในคดีเกี่ยวกับการสวมรอยเป็นบุคคลอื่น เนื่องจากจำเลยได้สร้างบัญชีเฟซบุ๊กปลอมในนามของอดีตคู่รักซึ่งมีอาชีพเป็นผู้สืบสวนด้านยาเสพติด และเขียนข้อความลงบนหน้าบัญชีเฟซบุ๊กดังกล่าวว่า อดีตคู่รักของตนเสพยาเสพติด ซื้อบริการโสเภณี และเป็นโรคเริม ซึ่งในขณะที่มีการฟ้องร้องคดีนี้ มลรัฐนิวเจอร์ซีย์ยังไม่มีกฎหมายที่กำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตกลายเป็นความผิดทางอาญาไว้โดยตรง แต่อย่างไรก็ตาม ศาลในขณะนั้นปฏิเสธการยกฟ้องโดยให้เหตุผลว่า กฎหมายเกี่ยวกับการโจรกรรมข้อมูลอันเป็นอัตลักษณ์ของบุคคล (Identity Theft Statute) ของมลรัฐนิวเจอร์ซีย์ที่มีอยู่แล้วมีความชัดเจนเพียงพอที่จะใช้บังคับ และถือว่าการกระทำของจำเลยเป็นการทำให้ชื่อเสียงของผู้อื่นเสียหาย[3] ส่วนมลรัฐแคลิฟอร์เนียก็ประสบกับปัญหาการปรับใช้กฎหมายเกี่ยวกับการโจรกรรมข้อมูลอันเป็นอัตลักษณ์ของบุคคลกับคดีลักษณะนี้เช่นกัน ดังจะเห็นได้จากคดีของ In re Rolando S. จำเลยที่เป็นผู้เยาว์เข้าถึงบัญชีเฟซบุ๊กของเหยื่อและเขียนข้อความเชิงกามารมณ์ในนามของเหยื่อส่งไปยังเพื่อนผู้ชาย รวมถึงปรับเปลี่ยนคำอธิบายบนหน้าบัญชีของเหยื่อไปในทางหยาบคาย ศาลอุทธรณ์แห่งมลรัฐแคลิฟอร์เนียพิพากษาให้จำเลยมีความผิดตามกฎหมายเกี่ยวกับการโจรกรรมข้อมูลอันเป็นอัตลักษณ์ของบุคคล (Identity Theft Statute) โดยตัดสินว่าบทบัญญัติดังกล่าวมีเจตนารมณ์กำหนดให้คำว่า “วัตถุประสงค์ที่ไม่ชอบด้วยกฎหมาย” ให้หมายรวมถึงการกระทำที่ถูกห้ามโดยกฎหมายคอมมอนลอว์ด้วย (Common Law) ศาลเห็นว่าข้อความที่จำเลยเขียนลงบนบัญชีเฟซบุ๊กของเหยื่อถือเป็นการหมิ่นประมาท (Libel) ซึ่งเป็นการละเมิดทางแพ่งโดยจงใจ จึงเป็นความผิดตามกฎหมายเกี่ยวกับการโจรกรรมข้อมูลอันเป็นอัตลักษณ์ของบุคคล[4]

อย่างไรก็ตาม แม้ว่ากฎหมายเกี่ยวกับการโจรกรรมข้อมูลอันเป็นอัตลักษณ์ของบุคคล หรือกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ หรือกฎหมายอื่น ๆ ที่เกี่ยวข้องที่มีอยู่แต่เดิมจะสามารถนำมาปรับใช้กับการกระทำความผิดที่เกิดขึ้นดังตัวอย่างข้างต้นก็ตาม แต่ด้วยเนื้อหาของบทบัญญัติที่อาจมีความกำกวม ไม่ครอบคลุม หรือไม่ตรงตามลักษณะการสวมรอยเป็นบุคคลอื่นบน

---

[2] ibid., 462-463.

[3] ibid., 458-460.

[4] ibid., 460-461.

เครือข่ายอินเทอร์เน็ตอย่างชัดแจ้งเท่าไรนัก หลายมลรัฐจึงมีแนวคิดที่จะตรากฎหมายเฉพาะเพื่อกำหนดให้การกระทำดังกล่าวเป็นความผิดทางอาญาพร้อมกำหนดระวางโทษไว้ เพื่อประโยชน์ในการดำเนินคดีและการคุ้มครองผู้เสียหายจากผู้สวมรอยให้ชัดเจนมากยิ่งขึ้น

4.1.2 มาตรการทางกฎหมายที่เกี่ยวข้อง

นับตั้งแต่มลรัฐเทกซัสได้ริเริ่มประกาศใช้กฎหมายเฉพาะเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในชื่อบทบัญญัติว่า Online Impersonation ตั้งแต่ ค.ศ. 2011 เป็นต้นมา (เดิมเมื่อ ค.ศ. 2009 ใช้ชื่อบทบัญญัติว่า Online Harassment) หลายมลรัฐของสหรัฐอเมริกาได้เกิดการตื่นตัวและตระหนักถึงปัญหาภัยคุกคามดังกล่าวมากขึ้น จึงทยอยออกกฎหมายเฉพาะเพื่อกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตกลายเป็นความผิดอาญา พร้อมกำหนดมาตรการบังคับทั้งทางอาญาและแพ่งไว้อย่างชัดเจน อาทิ ผู้แทนมลรัฐโอเรกอนได้ให้ความเห็นในการยกร่างกฎหมาย Online Impersonation ไว้ว่า เนื่องจากในปัจจุบันมลรัฐโอเรกอนไม่มีบทกำหนดโทษทางอาญาสำหรับความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต จึงต้องการกำหนดให้การสื่อสารทางระบบออนไลน์ที่เกิดขึ้นโดยมีเจตนาเพื่อหลอกลวงผู้ได้รับการสื่อสารให้คิดว่าผู้ส่งเป็นบุคคลอื่นกลายเป็นความผิดอาญา จากการสอบถามเจ้าหน้าที่ที่เกี่ยวข้องแล้วพบว่า กฎหมายที่มีอยู่ในปัจจุบันไม่รุนแรงเพียงพอต่อการดำเนินคดีกับผู้กระทำความผิด เหยื่อที่ได้รับความเสียหายด้านชื่อเสียงและความเป็นอยู่ส่วนตัวมักไม่มีหนทางสำหรับการขอความช่วยเหลือเท่าไรนัก การยกร่างบทบัญญัติเป็นการเฉพาะนี้จะทำให้ฝ่ายผู้เสียหายได้รับการเยียวยาและทำให้เจ้าหน้าที่ผู้บังคับใช้กฎหมายมีเครื่องมือในการจัดการกับปัญหานี้อีกด้วย[5]

ด้วยเหตุดังกล่าวข้างต้น สหรัฐอเมริกาจึงมีกฎหมายเฉพาะในระดับมลรัฐที่กำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญา ในส่วนนี้ ผู้เขียนจะอธิบายถึงสาระสำคัญและองค์ประกอบของกฎหมายดังกล่าว พร้อมยกตัวอย่างบทบัญญัติของมลรัฐต่าง ๆ ทั้งที่ได้รับการประกาศใช้บังคับแล้วและร่างกฎหมายที่อยู่ระหว่างดำเนินการยกร่าง

---

[5] Reprentative Cliff Bentz, "Bentz Introduces Bill to Crack Down on Online Impersonation," [Online] Accessed: 4 January 2017. Available from: https://www.oregonlegislature.gov/bentz/Documents/Bentz%20Introduces%20Bill%20to%20Crack%20Down%20on%20Online%20Impersonation.pdf

4.1.2.1 กฎหมายเฉพาะเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต (Online Impersonation)

จากการศึกษาบทบัญญัติความผิดดังกล่าวของมลรัฐต่าง ๆ จะเห็นได้ว่าองค์ประกอบและเนื้อหาสาระของบทบัญญัติมีความคล้ายคลึงกัน ในส่วนนี้ผู้เขียนจะอธิบายถึงสาระสำคัญของบทบัญญัติเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของสหรัฐอเมริกา โดยแบ่งหัวข้อตามองค์ประกอบของบทบัญญัติ ได้แก่ คำนิยาม องค์ประกอบความผิด รูปแบบการกระทำความผิด ความผิดและการกำหนดโทษ การเยียวยาทางแพ่ง ข้อยกเว้น และตัวอย่างบทบัญญัติของมลรัฐต่าง ๆ ดังนี้

4.1.2.1.1 คำนิยาม

ถ้อยคำที่ใช้ในบทบัญญัติแห่งกฎหมายมักมีความหมายหรือคำนิยามเป็นการเฉพาะ เพื่อให้ผู้อ่านกฎหมายหรือผู้ใช้กฎหมายเข้าใจตรงกันและนำบทบัญญัตินั้นไปปรับใช้ได้อย่างเหมาะสมกับข้อเท็จจริงที่เกิดขึ้น ทั้งนี้ เนื่องจากแต่ละมลรัฐของสหรัฐอเมริกามีกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นของตนเอง จึงมีการกำหนดคำนิยามของถ้อยคำในบทบัญญัติไว้เป็นการเฉพาะ คำนิยามที่สำคัญและมักปรากฏในบทบัญญัติของแต่ละมลรัฐมีดังต่อไปนี้

(1) Impersonates or Impersonation หมายถึง การใช้ชื่อหรือข้อมูลอื่นของบุคคลที่มีตัวตนจริงเพื่อกระทำการสวมรอยเป็นบุคคลนั้น ซึ่งทำให้ผู้อื่นอาจเชื่อหรือได้เชื่อโดยมีเหตุอันสมควรว่าผู้กระทำเป็นบุคคลเดียวกันกับบุคคลที่ถูกสวมรอย[6] (Credible Impersonation)

(2) Actual Person หมายถึง บุคคลที่มีชีวิตอยู่ (Living Individual)[7]

(3) Identifying Information หมายถึง ข้อมูลเพียงลำพังหรือรวมกับข้อมูลอื่นแล้วสามารถใช้ระบุตัวตนของบุคคลได้ ประกอบด้วย[8]

---

[6] REVISED CODE OF WASHINGTON § 4.24.790 (1) (c)

[7] REVISED CODE OF WASHINGTON § 4.24.790 (1) (a)

[8] TEXAS PENAL CODE § 32.51

3.1 ชื่อหรือวันเกิด

3.2 ข้อมูลทางชีวภาพที่มีลักษณะเฉพาะ รวมถึงลายพิมพ์นิ้วมือ (Fingerprint) ลายพิมพ์ลักษณะเสียง (Voice Print) ภาพจอประสาทตาหรือม่านตา (Retina or Iris Image)

3.3 หมายเลขประจำตัวทางอิเล็กทรอนิกส์ที่มีลักษณะเฉพาะ ที่อยู่ รหัสเส้นทาง หรือหมายเลขบัญชีสถาบันทางการเงิน

3.4 โทรคมนาคมที่มีการระบุถึงข้อมูลหรือการเข้าถึงอุปกรณ์

3.5 หมายเลขประกันสังคมหรือหมายเลขประจำตัวอื่นใดที่รัฐบาลออกให้

(4) Commercial Social Networking Site หรือ Social Networking Site หมายถึง ธุรกิจ องค์กร หรือหน่วยงานอื่นใดที่ดำเนินงานเกี่ยวกับเว็บไซต์ซึ่งอนุญาตให้บุคคลลงทะเบียนเป็นผู้ใช้งานเพื่อสร้างความสัมพันธ์ส่วนบุคคลกับผู้ใช้งานรายอื่น ผ่านการสื่อสารทางตรงหรือตามเวลาจริงกับผู้ใช้งานรายอื่น หรือสร้างหน้าเว็บหรือโพรไฟล์ที่สาธารณชนหรือบุคคลอื่นสามารถเข้าถึงได้[9] รวมถึงเว็บไซต์บนเครือข่ายอินเทอร์เน็ตที่ให้บริการช่องทางการติดต่อสื่อสารระหว่างผู้ใช้งาน เช่น พื้นที่การประชุมสาธารณะ (Forum) ห้องสนทนา (Chatroom) จดหมายอิเล็กทรอนิกส์ (Electronic Mail) หรือข้อความด่วน (Instant Message)[10] เป็นต้น

(5) Electronic Means หมายถึง การเปิดบัญชีจดหมายอิเล็กทรอนิกส์ หรือการเปิดบัญชีหรือโพรไฟล์เครือข่ายสังคมบนเว็บไซต์ในนามของบุคคลอื่น[11] หรือหมายถึง การเปิดใช้ การเข้าถึง การปรับเปลี่ยน หรือการสร้างบัญชีจดหมายอิเล็กทรอนิกส์ปลอมหรือบัญชีหรือโพรไฟล์ปลอมทางเว็บไซต์บนเครือข่ายอินเทอร์เน็ต หรือการแจ้งประกาศบนเว็บไซต์สื่อสังคมออนไลน์ กระดานข้อความอิเล็กทรอนิกส์ หรือหน้าโฆษณาในระบบออนไลน์[12]

---

[9] TEXAS PENAL CODE § 33.07 (f) (1)

[10] LOUISIANA REVISED STATUES § 14:73.10 B. (4)

[11] CALIFORNIA PENAL CODE § 528.5 (c)

[12] SOUTH CAROLINA HOUSE BILL 3107 § 2

(6) Electronic Bulletin Board หมายถึง เว็บไซต์ที่ออกแบบมาสำหรับเป็นพื้นที่ให้ผู้ใช้งานอินเทอร์เน็ตสามารถแจ้งและตอบสนองต่อประกาศเล็ก ๆ ซึ่งผู้ใช้งานอินเทอร์เน็ตรายอื่นสามารถมองเห็นได้[13] หรือหมายถึง ระบบการติดต่อสื่อสารแบบออนไลน์ที่บุคคลใด ๆ สามารถแบ่งปัน ร้องขอ หรืออภิปรายข้อมูลได้[14]

4.1.2.1.2 องค์ประกอบความผิด

(1) ผู้กระทำความผิดต้องสวมรอยเป็นบุคคลอื่นโดยเจตนา (Intent or Knowingly) หมายถึง ผู้กระทำความผิดมีสำนึกรู้ตัวในขณะกระทำความผิดและจงใจแอบอ้างสวมรอยเป็นบุคคลอื่น

(2) ผู้กระทำความผิดไม่ได้รับความยินยอมจากผู้ที่ถูกสวมรอย (Without Obtaining the Consent) กล่าวคือ ผู้ที่ถูกสวมรอยที่เป็นเจ้าของชื่อหรือข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมแก่ผู้สวมรอยในการนำชื่อหรือข้อมูลส่วนบุคคลไปใช้เพื่อให้ผู้คนทั่วไปเข้าใจหรือเชื่อว่าเป็นการกระทำของผู้ที่ถูกสวมรอย เป็นการสวมรอยโดยปราศจากความยินยอมหรือการได้รับอนุญาต

(3) บุคคลที่ถูกสวมรอยเป็นบุคคลที่มีตัวตนอยู่จริงและยังมีชีวิตอยู่ (Actual Person) เนื่องจากการสวมรอยเป็นบุคคลอื่นนั้นสร้างความเสียหายให้แก่ผู้ที่ถูกสวมรอยได้หลายประการ อาจทำให้ผู้เสียหายได้รับความยากลำบากในการดำรงชีวิต หากกรณีเป็นการแอบอ้างตัวตนของบุคคลที่ไม่มีอยู่จริงหรือไม่มีชีวิตเสียแล้ว ย่อมไม่เกิดความเสียหายแก่บุคคลนั้น

(4) มีเจตนาพิเศษ

นอกเหนือจากเจตนาธรรมดาในการสวมรอยเป็นบุคคลอื่นแล้ว บทบัญญัติเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของสหรัฐอเมริกายังกำหนดถึงเจตนาพิเศษในการสวมรอยไว้อีกด้วย ได้แก่ ประทุษร้าย (Harm) หลอกลวงฉ้อโกง (Defraud) ขู่เข็ญ (Intimidate) ข่มขู่ให้หวาดกลัว (Threaten) ได้มาซึ่งผลประโยชน์ (Obtain a Benefit) ทำความเสียหาย (Injure) คุกคามหรือรังควาน (Harass) และทำให้เสื่อมเสียเกียรติ (Humiliate) แต่อย่างไรก็ตาม มิใช่ว่าการสวมรอยเป็นบุคคลอื่นจะต้องมีเจตนาพิเศษครบทุกเจตนาเสมอไป ขึ้นอยู่กับ

---

[13] REVISED CODE OF WASHINGTON § 4.24.790 (e)

[14] SOUTH CAROLINA HOUSE BILL 3107 SECTION 2

บทบัญญัติของมลรัฐนั้น ๆ ว่าได้กำหนดเจตนาพิเศษไว้อย่างไร เช่น มลรัฐนิวยอร์กกำหนดว่าบุคคลจะมีความผิดอาญาฐานสวมรอยเป็นบุคคลอื่นเมื่อบุคคลนั้นกระทำการสวมรอยโดยมีเจตนาเพื่อให้ได้มาซึ่งผลประโยชน์ หรือเพื่อทำความเสียหาย หรือเพื่อหลอกลวงฉ้อโกงผู้อื่น[15] ในขณะที่มลรัฐแคลิฟอร์เนียกำหนดว่าต้องเป็นการสวมรอยโดยมีวัตถุประสงค์ในการประทุษร้าย ขู่เข็ญ ข่มขู่ให้หวาดกลัว หรือหลอกลวงฉ้อโกง[16] นอกจากนี้ มลรัฐเทกซัสยังแบ่งระดับความผิดฐานสวมรอยเป็นบุคคลอื่นออกเป็น 2 ระดับ กล่าวคือ การกระทำจะเป็นความผิดอาญาอุกฉกรรจ์ระดับสาม (Third Degree Felony) ต้องเกิดจากเจตนาเพื่อประทุษร้าย หลอกลวงฉ้อโกง ข่มขู่ หรือขู่เข็ญ[17] แต่การกระทำที่เป็นความผิดลหุโทษชั้นเอ (Class A Misdemeanor) อาศัยเจตนาพิเศษเพียงสองประการ ได้แก่ เจตนาเพื่อประทุษร้ายหรือเพื่อหลอกลวงฉ้อโกง[18]

(5) เป็นการสวมรอยที่น่าเชื่อถือ (Credible Impersonation) หมายถึง การทำให้บุคคลอื่นหลงเชื่อโดยมีเหตุอันสมควรว่าตนคือผู้ที่ถูกสวมรอย หรือเชื่อว่าตนได้รับมอบอำนาจจากผู้ที่ถูกสวมรอย (Reasonably Believe) การทำให้หลงเชื่อเช่นนี้ต้องเกิดจากเจตนาของผู้กระทำความผิดที่ประสงค์ให้ผู้รับการสื่อสารหลงเชื่อว่าผู้ที่ถูกสวมรอยได้มอบอำนาจหรือเป็นคนถ่ายทอดการสื่อสารนั้นด้วยตนเอง

4.1.2.1.3 รูปแบบการกระทำความผิด

หากพิจารณาในภาพรวมของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตแล้วจะเห็นว่ามีลักษณะเป็นการแอบอ้างชื่อหรือตัวตนของบุคคลอื่น หรือเป็นการปลอมตัวเป็นบุคคลอื่น และมีการติดต่อสื่อสารกับบุคคลที่สามหรือประชาชนทั่วไปผ่านทางเครือข่ายอินเทอร์เน็ต การสวมรอยดังกล่าวมีรูปแบบการกระทำความผิดที่หลากหลาย ดังที่บทบัญญัติเกี่ยวกับความผิดฐานสวมรอยเป็นบุคคลอื่นของมลรัฐต่าง ๆ กำหนดไว้ ดังนี้

(1) การใช้ชื่อหรือความเป็นตัวตนของบุคคลอื่นเพื่อสร้างหน้าเว็บบนเว็บไซต์เครือข่ายสังคมหรือเว็บไซต์อื่น ปรากฏในมาตรา 33.07 ของประมวลกฎหมายอาญาแห่งมลรัฐเทกซัส และมาตรา 73.10 ของประมวลกฎหมายอาญาแห่งมลรัฐลุยเซียนา

---

[15] NEW YORK PENAL CODE § 190.25 (4)

[16] CALIFORNIA PENAL CODE § 528.5 (a)

[17] TEXAS PENAL CODE § 33.07 (a)

[18] TEXAS PENAL CODE § 33.07 (b)

(2) การใช้ชื่อหรือความเป็นตัวตนของบุคคลอื่นเพื่อประกาศหรือส่งข้อความผ่านเว็บไซต์เครือข่ายสังคมหรือเว็บไซต์อื่น โปรแกรมจดหมายอิเล็กทรอนิกส์ หรือโปรแกรมกระดานข้อความ ปรากฏในมาตรา 33.07 ของประมวลกฎหมายอาญาแห่งมลรัฐเทกซัส และมาตรา 73.10 ของประมวลกฎหมายอาญาแห่งมลรัฐลุยเซียนา

(3) การส่งจดหมายอิเล็กทรอนิกส์ ข้อความด่วน ข้อความตัวอักษร หรือการสื่อสารอื่นที่คล้ายคลึงกัน ซึ่งอ้างถึงชื่อ ที่อยู่ เบอร์โทรศัพท์ หรือสิ่งอื่นใดที่เป็นข้อมูลระบุตัวตนของบุคคลอื่น ปรากฏในมาตรา 73.10 ของประมวลกฎหมายอาญาแห่งมลรัฐลุยเซียนา

(4) การแอบอ้างว่าตนเป็นข้าราชการเพื่อจูงใจให้ผู้อื่นยอมต่ออำนาจนั้น ปรากฏในมาตรา 190.25 ของประมวลกฎหมายอาญาแห่งมลรัฐนิวยอร์ก

4.1.2.1.4 ความผิดและการกำหนดโทษ

กฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในมลรัฐต่าง ๆ ของสหรัฐอเมริกากำหนดให้การกระทำดังกล่าวเป็นความผิดทางอาญาและกำหนดระวางโทษจำคุกและโทษปรับ บางมลรัฐกำหนดให้การสวมรอยเป็นบุคคลอื่นเป็นความผิดทางอาญาระดับลหุโทษ (Misdemeanor) ส่วนบางมลรัฐกำหนดให้เป็นความผิดอาญาอุกฉกรรจ์ (Felony)

(1) ความผิดลหุโทษ

มลรัฐนิวยอร์กกำหนดให้การสวมรอยเป็นบุคคลอื่นหรือการแอบอ้างเป็นเจ้าหน้าที่รัฐผ่านทางเว็บไซต์บนเครือข่ายอินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์เป็นความผิดลหุโทษชั้นเอ (Class A Misdemeanor)[19] มลรัฐเซาท์แคโรไลนากำหนดให้การสวมรอยเป็นบุคคลอื่นด้วยเจตนาที่จะก่อความรำคาญหรือประทุษร้ายผ่านทางเว็บไซต์บนเครือข่ายอินเทอร์เน็ตหรือด้วยวิธีการทางอิเล็กทรอนิกส์เป็นความผิดลหุโทษ มีระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือทั้งจำทั้งปรับ[20]

(2) ความผิดอาญาอุกฉกรรจ์

มลรัฐนอร์ทแคโรไลนากำหนดให้การสวมรอยเป็นบุคคลอื่นผ่านเว็บไซต์บนเครือข่ายอินเทอร์เน็ตหรือด้วยวิธีการทางอิเล็กทรอนิกส์โดยมีจุดประสงค์เพื่อประทุษร้าย

---

[19] NEW YORK PENAL CODE § 190.25 (4)

[20] SOUTH CAROLINA HOUSE BILL 3107 § 2

ขู่เข็ญ ข่มขู่ให้หวาดกลัว หรือหลอกลวงฉ้อโกงผู้อื่น เป็นความผิดอาญาอุกฉกรรจ์ชั้น H (Class H Felony) ระวางโทษจำคุก หรือปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือทั้งจำทั้งปรับ[21]

บางมลรัฐได้กำหนดให้การกระทำความผิดรูปแบบหนึ่งเป็นความผิดลหุโทษและอีกรูปแบบหนึ่งเป็นความผิดอาญาอุกฉกรรจ์ไว้ในมาตราเดียวกัน เช่น มลรัฐเทกซัสได้กำหนดให้การสวมรอยด้วยวิธีการสร้างหน้าเว็บบนเว็บไซต์เครือข่ายสังคมหรือเว็บไซต์อื่น หรือการประกาศหรือส่งข้อความผ่านทางเว็บไซต์เครือข่ายสังคมหรือเว็บไซต์อื่นหรือทางโปรแกรมจดหมายอิเล็กทรอนิกส์หรือทางโปรแกรมกระดานข้อความด้วยเจตนาเพื่อประทุษร้าย หลอกลวงฉ้อโกง ข่มขู่ หรือขู่เข็ญผู้อื่นเป็นความผิดอาญาอุกฉกรรจ์ระดับสาม (Third-degree Felony) แต่หากเป็นการส่งจดหมายอิเล็กทรอนิกส์ ข้อความด่วน ข้อความตัวอักษร หรือการสื่อสารอื่นที่คล้ายคลึงกันซึ่งอ้างถึงชื่อ ที่อยู่ หมายเลขโทรศัพท์ หรือสิ่งอื่นใดที่เป็นข้อมูลระบุตัวตนของบุคคลอื่นโดยไม่ได้รับความยินยอมจากบุคคลนั้น โดยมีเจตนาให้ผู้รับสารเชื่อโดยมีเหตุอันสมควรว่าบุคคลอื่นที่ถูกสวมรอยได้มอบอำนาจหรือเป็นผู้ถ่ายทอดการสื่อสารนั้นเอง และมีเจตนาเพื่อประทุษร้ายหรือหลอกลวงผู้หนึ่งผู้ใด ถือเป็นความผิดระดับลหุโทษเท่านั้น เว้นแต่จะได้กระทำไปด้วยเจตนาเพื่อเรียกร้องการตอบสนองจากเจ้าหน้าที่แผนกฉุกเฉิน จะถือว่าเป็นความผิดอาญาอุกฉกรรจ์ระดับสาม

4.1.2.1.5 การเยียวยาทางแพ่ง (Civil Remedy)

หลายมลรัฐไม่ได้กำหนดระวางโทษทางอาญาแก่ผู้กระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไว้แต่เพียงอย่างเดียว แต่ยังกำหนดช่องทางสำหรับการเยียวยาทางแพ่งสำหรับผู้เสียหายไว้อีกด้วย เพื่อเป็นทางเลือกในการบรรเทาความเสียหายที่เกิดขึ้นแก่ผู้ที่ได้รับผลกระทบจากการกระทำความผิด การเยียวยาทางแพ่งที่ปรากฏในบทบัญญัติเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของสหรัฐอเมริกามีหลายประการ เช่น ค่าสินไหมทดแทนความเสียหาย (Compensatory Damages) ค่าเสียหายตามจริง (Actual Damages) ค่าเสียหายเชิงลงโทษ (Punitive Damages) คำสั่งห้ามกระทำการชั่วคราว (Injunctive Relief) คำสั่งให้ชดใช้ด้วยทางอื่นอย่างเป็นธรรม (Equitable Relief) คำสั่งแสดงสิทธิของโจทก์ (Declaratory Relief) รวมถึงค่าทนายความและค่าใช้จ่ายในการดำเนินคดี (Attorney's Fee and Litigation Costs) เป็นต้น

[21] NORTH CAROLINA HOUSE BILL 794 § 1

ตัวอย่างเช่น มลรัฐแคลิฟอร์เนียให้สิทธิแก่ผู้ที่ได้รับความเสียหายหรือสูญเสียจากการสวมรอยเป็นบุคคลอื่นตามมาตรา 528.5 (a) ในการดำเนินคดีทางแพ่งเรียกร้องให้ผู้กระทำความผิดชดใช้ค่าสินไหมทดแทนและให้ศาลมีคำสั่งห้ามจำเลยกระทำการชั่วคราวได้[22] มลรัฐนอร์ทแคโรไลนาได้กำหนดแนวทางการเยียวยาทางแพ่งไว้อย่างชัดเจน โดยให้สิทธิแก่ผู้ที่ถูกนำข้อมูลส่วนบุคคลไปเปิดเผยหรือใช้ในการสวมรอยเป็นบุคคลอื่นสามารถดำเนินคดีทางแพ่งกับผู้ที่เปิดเผยหรือใช้ข้อมูลนั้นได้ และสามารถเรียกร้องให้จำเลยชดใช้ค่าเสียหายตามจริงซึ่งคำนวณจากจำนวนวันที่ถูกละเมิดคูณกับอัตราค่าเสียหายจำนวน 1,000 ดอลลาร์สหรัฐต่อวัน หรือให้ชดใช้เป็นจำนวนเงิน 10,000 ดอลลาร์สหรัฐ อีกทั้งยังสามารถฟ้องเรียกค่าเสียหายเชิงลงโทษ รวมถึงค่าธรรมเนียมทนายความและค่าใช้จ่ายในการดำเนินคดีได้อีกด้วย[23]

4.1.2.1.6 ข้อยกเว้น

มลรัฐเทกซัสกำหนดข้อยกเว้นการกระทำที่ไม่เป็นความผิดตามมาตรา 33.07 หากผู้กระทำเป็นองค์กรใดองค์กรหนึ่งหรือเป็นการกระทำในฐานะลูกจ้างขององค์กรใดองค์กรหนึ่งดังต่อไปนี้ (1) เว็บไซต์เครือข่ายสังคมเชิงพาณิชย์ (2) ผู้ให้บริการอินเทอร์เน็ต (3) บริการคอมพิวเตอร์แบบปฏิสัมพันธ์ (4) ผู้ให้บริการโทรคมนาคม (5) ผู้ให้บริการวิดีโอหรือผู้ให้บริการเคเบิล[24]

มลรัฐเซาท์แคโรไลนากำหนดถึงกรณีที่ไม่สามารถปรับใช้บทบัญญัติมาตรา 37-20-310 แก่กรณีได้ ได้แก่ (1) กรณีที่การสวมรอยเป็นบุคคลอื่นนั้นเป็นเรื่องทางวัฒนธรรม ประวัติศาสตร์ การเมือง ศาสนา การศึกษา เป็นเรื่องที่น่าสนใจพอที่จะเป็นข่าวได้ หรือเพื่อประโยชน์สาธารณะ แต่ไม่จำกัดที่การใช้ในงานศิลปะ คำวิจารณ์ การเสียดสี และการล้อเลียน (2) กรณีที่เป็นการสวมรอยโดยเจ้าหน้าที่ผู้บังคับใช้กฎหมายกระทำการในหน้าที่[25]

---

[22] CALIFORNIA PENAL CODE § 528.5 (e)

[23] NORTH CAROLINA HOUSE BILL 794 § 1

[24] TEXAS PENAL CODE § 33.07 (e)

[25] SOUTH CAROLINA HOUSE BILL 3107 § 2

4.1.2.2 ตัวอย่างบทบัญญัติเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของมลรัฐต่าง ๆ

สหรัฐอเมริกามีบทบัญญัติเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการเฉพาะ ปรากฏตามประมวลกฎหมายอาญาระดับมลรัฐ ซึ่งในปัจจุบันมีหลายมลรัฐที่มีกฎหมายกำหนดให้การกระทำดังกล่าวเป็นความผิดอาญาและกำหนดบทลงโทษไว้ดังต่อไปนี้

4.1.2.2.1 มลรัฐเทกซัส (Texas)

มลรัฐเทกซัสเป็นมลรัฐแรกของสหรัฐอเมริกาที่ดำเนินการยกร่างกฎหมายเฉพาะกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญา ปรากฏตามประมวลกฎหมายอาญาแห่งมลรัฐเทกซัส หมวด 33 อาชญากรรมคอมพิวเตอร์ มาตรา 33.07 ดังนี้[26]

“มาตรา 33.07 การสวมรอยเป็นบุคคลอื่นในระบบออนไลน์ (Online Impersonation)

(a) บุคคลกระทำความผิดอาญาเมื่อบุคคลนั้นใช้ชื่อหรือความเป็นตัวตนของบุคคลอื่นโดยมิได้รับความยินยอมจากบุคคลอื่นนั้นและโดยเจตนาเพื่อประทุษร้าย หลอกลวงฉ้อโกง ขู่เข็ญ หรือข่มขู่บุคคลใด ๆ ให้หวาดกลัว ด้วยวิธีการ:

(1) สร้างหน้าเว็บบนเว็บไซต์เครือข่ายสังคมออนไลน์เชิงพาณิชย์หรือเว็บไซต์อินเทอร์เน็ตอื่น หรือ

(2) ประกาศหรือส่งข้อความผ่านทางเว็บไซต์เครือข่ายสังคมออนไลน์เชิงพาณิชย์หรือเว็บไซต์อินเทอร์เน็ตอื่น ยกเว้นโปรแกรมจดหมายอิเล็กทรอนิกส์หรือโปรแกรมกระดานข้อความ

(b) บุคคลกระทำความผิดอาญาเมื่อบุคคลนั้นส่งจดหมายอิเล็กทรอนิกส์ ข้อความด่วน ข้อความตัวอักษร หรือการติดต่อสื่อสารที่คล้ายคลึงกันนี้ซึ่งอ้างถึงชื่อ ที่อยู่ หมายเลขโทรศัพท์ หรือสิ่งอื่นใดที่แสดงข้อมูลอันเป็นอัตลักษณ์ของผู้อื่น:

(1) โดยปราศจากการได้รับความยินยอมจากผู้อื่นนั้น

---

[26] TEXAS PENAL CODE § 33.07

(2) โดยเจตนาเพื่อก่อให้ผู้รับการสื่อสารมีเหตุอันสมควรที่จะเชื่อได้ว่าผู้อื่นนั้นอนุญาตหรือเป็นผู้ส่งการสื่อสารนั้น และ

(3) โดยเจตนาเพื่อประทุษร้ายหรือหลอกลวงฉ้อโกงบุคคลใด ๆ

(c) การกระทำความผิดตามอนุมาตรา (a) เป็นความผิดอาญาอุกฉกรรจ์ระดับสาม (Felony of the Third Degree) การกระทำความผิดตามอนุมาตรา (b) เป็นความผิดลหุโทษระดับ A (Class A Misdemeanor) เว้นแต่ ผู้กระทำความผิดกระทำโดยมีเจตนาเพื่อเรียกร้องความสนใจจากเจ้าหน้าที่หน่วยฉุกเฉิน กรณีเช่นนี้กำหนดให้เป็นความผิดอาญาอุกฉกรรจ์ระดับสาม

บทบัญญัติดังกล่าวข้างต้นถูกตราเป็นกฎหมายขึ้นในปี 2009 โดยใช้ชื่อว่า Online Harassment ก่อนที่จะมีการแก้ไขปรับปรุงในปี 2011 เปลี่ยนชื่อเป็น Online Impersonation ให้ตรงตามเจตนารมณ์ของกฎหมายที่ต้องการเอาผิดกับผู้ที่สวมรอยเป็นบุคคลอื่นในระบบออนไลน์ โดยมีคดีของ Meigan Meier และคดีระหว่าง Draker v. Schreiber เป็นแรงจูงใจสำคัญ

สภานิติบัญญัติของมลรัฐเทกซัสได้กำหนดให้การกระทำความผิดฐานนี้อาจเป็นได้ทั้งความผิดลหุโทษหรือความผิดอาญาอุกฉกรรจ์ แล้วแต่กรณี ขึ้นอยู่กับว่าผู้กระทำผิดมีเจตนาประสงค์ร้ายมากน้อยเพียงใด หากพิจารณาถ้อยคำที่ใช้ในบทบัญญัติดังกล่าวแล้วจะพบว่ามีข้อแตกต่างที่สำคัญระหว่างการกำหนดให้การกระทำเป็นความผิดลหุโทษหรือความผิดอาญาอุกฉกรรจ์ดังนี้[27]

(1) ความผิดลหุโทษตามอนุมาตรา (b) นั้นกำหนดไว้แต่เพียงว่าผู้กระทำความผิดมีส่วนในการกระจายหรือส่งต่อข้อมูลที่ใช้สำหรับระบุตัวตนของบุคคลอื่น ในขณะที่ความผิดตามอนุมาตรา (a) นั้นกำหนดว่าต้องมีการสร้างเว็บไซต์โดยใช้ชื่อหรือข้อมูลอันเป็นอัตลักษณ์ (name or persona) ของเหยื่อด้วย

(2) ความผิดลหุโทษตามอนุมาตรา (b) ไม่ได้กำหนดว่าผู้กระทำความผิดจะต้องกระทำโดยมีเจตนาเพื่อข่มขู่หรือคุกคาม แต่กำหนดเพียงแต่ว่าผู้กระทำความผิดมีเจตนาจะทำร้ายหรือหลอกลวงเหยื่อเท่านั้น

นอกจากนี้ การใช้ชื่อหรือความเป็นตัวตนของบุคคลอื่นตามอนุมาตรา (a) ไม่ได้จำกัดแค่เพียงการสวมรอยที่มีข้อมูลตรงกันทั้งชื่อและรูปภาพของบุคคลอื่นเท่านั้น (Identical

---

[27] Clanton, K., "We Are Not Who We Pretend to Be: Odr Alternative to Online Impersonation Statues," Cardozo Journal of Conflict Resolution.

Match) ดังนั้น บทบัญญัตินี้จึงปรับใช้ได้อย่างกว้างขวาง สามารถปรับใช้กับกรณีที่รูปภาพของเหยื่อถูกนำไปใช้สร้างโพรไฟล์บนสื่อสังคมออนไลน์ได้ แม้ว่าจะมีการใช้ชื่อปลอมก็ตาม

มลรัฐเทกซัสได้กำหนดมาตรการบังคับทางอาญาแก่การกระทำความผิดดังกล่าวข้างต้นไว้ 2 ประการ ขึ้นอยู่กับพฤติการณ์ว่าเป็นการกระทำความผิดระดับใด ประการแรก ในกรณีที่เป็นการกระทำความผิดตามอนุมาตรา (a) ถือเป็นความผิดอาญาอุกฉกรรจ์ระดับสาม ประมวลกฎหมายอาญาแห่งมลรัฐเทกซัส มาตรา 12.34[28] ได้กำหนดบทลงโทษสำหรับความผิดอาญาอุกฉกรรจ์ระดับสามไว้ว่า ผู้กระทำความผิดต้องระวางโทษจำคุกในเรือนจำของกระทรวงกระบวนการยุติธรรมทางอาญาแห่งมลรัฐเทกซัส (the Texas Department of Criminal Justice) เป็นระยะเวลาไม่น้อยกว่า 2 ปี แต่ไม่เกิน 10 ปี นอกจากโทษจำคุกแล้วผู้กระทำความผิดอาจต้องโทษปรับอีกไม่เกิน 10,000 ดอลลาร์สหรัฐ

ประการที่สอง ในกรณีที่เป็นการกระทำความผิดตามอนุมาตรา (b) ถือเป็นความผิดลหุโทษระดับ A (Class A Misdemeanor) ซึ่งประมวลกฎหมายอาญาแห่งมลรัฐเทกซัส มาตรา 12.21[29] ได้กำหนดบทลงโทษสำหรับความผิดลหุโทษระดับ A ไว้ว่า ผู้กระทำความผิดต้องระวางโทษกักขังในคุก (Confinement in Jail) ไม่เกิน 1 ปี หรือปรับไม่เกิน 4,000 ดอลลาร์สหรัฐ หรือทั้งกักขังทั้งปรับ เว้นแต่เป็นการกระทำความผิดโดยมีเจตนาเพื่อเรียกร้องความสนใจจากเจ้าหน้าที่หน่วยฉุกเฉิน จะกลายเป็นความผิดอาญาอุกฉกรรจ์ระดับสามทันที

นับแต่กฎหมายฉบับนี้ถูกบังคับใช้เมื่อปี 2009 เป็นต้นมา ปรากฏข้อมูลว่ามีการดำเนินคดีเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในมลรัฐเทกซัสเป็นจำนวนพอสมควร ยกตัวอย่างเช่น

(1) คดีของ Victoria Varnes ในปี 2014 ซึ่งจำเลยถูกจับกุมในข้อหาสวมรอยเป็นบุคคลอื่นภายหลังจากที่จำเลยได้สร้างเว็บไซต์ที่มีรูปยั่วยุอารมณ์ในนามของบุคคลอื่น อันเป็นความผิดอาญาอุกฉกรรจ์ระดับสาม และหากจำเลยถูกศาลพิพากษาว่ามีความผิดจริง อาจถูกลงโทษปรับไม่เกิน 10,000 ดอลลาร์สหรัฐ หรือจำคุกไม่เกิน 10 ปี

(2) คดีของ Stacie Keeble ซึ่งตกเป็นเหยื่อของการถูกสวมรอยในโลกออนไลน์ เมื่อจำเลยได้สร้างหน้าเว็บไซต์เฟซบุ๊ก (Facebook) ปลอมขึ้นและใส่รูปตัดต่อใบหน้าของ

---

[28] TEXAS PENAL CODE § 12.34

[29] TEXAS PENAL CODE § 12.21

Stacie กับรูปเปลือยของผู้อื่น โดยจำเลยให้การรับสารภาพในข้อหา Online Impersonation อันเป็นความผิดอาญาอุกฉกรรจ์ระดับสาม และได้รับโทษปรับเป็นจำนวนเงิน 2,500 ดอลลาร์สหรัฐ และรอคุมประพฤติเป็นเวลา 5 ปี เนื่องจากจำเลยไม่เคยมีประวัติอาชญากรรมมาก่อน[30]

4.1.2.2.2 มลรัฐแคลิฟอร์เนีย (California)

เมื่อวันที่ 19 กุมภาพันธ์ ค.ศ. 2010 สภานิติบัญญัติแห่งมลรัฐแคลิฟอร์เนีย ได้ยกร่างพระราชบัญญัติ SB 1411 ขึ้นเพื่อบัญญัติให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญา ดังปรากฏตามประมวลกฎหมายอาญาแห่งมลรัฐแคลิฟอร์เนีย มาตรา 528.5 ดังนี้

“มาตรา 528.5

(a) แม้ว่าจะมีบัญญัติแห่งกฎหมายอื่นปรากฏอยู่ก็ตาม ผู้ใดโดยรู้อยู่แล้วและปราศจากความยินยอมกระทำการสวมรอยเป็นผู้อื่นอย่างน่าเชื่อถือผ่านทางเว็บไซต์อินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์อื่นใด โดยมีจุดประสงค์เพื่อประทุษร้าย ขู่ขวัญ ข่มขู่ให้หวาดกลัวหรือหลอกลวงฉ้อโกงผู้อื่น ผู้นั้นมีความผิดอาญาตามอนุมาตรา d

(b) ภายใต้เจตนารมณ์ของมาตรานี้ การสวมรอยเป็นบุคคลอื่นมีความน่าเชื่อถือเมื่อผู้อื่นมีเหตุอันสมควรให้เชื่อหรือได้กระทำสิ่งที่มีเหตุอันสมควรเชื่อได้ว่าผู้กระทำผิดเคยเป็นหรือเป็นบุคคลที่ถูกสวมรอย

(c) ภายใต้เจตนารมณ์ของมาตรานี้ “วิธีการทางอิเล็กทรอนิกส์” ประกอบด้วย การเปิดใช้งานบัญชีจดหมายอิเล็กทรอนิกส์หรือบัญชีผู้ใช้งานหรือประวัติโดยย่อของเว็บไซต์เครือข่ายสังคมออนไลน์ในนามของผู้อื่น

(d) การกระทำความผิดตามอนุมาตรา a มีโทษปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือจำคุกในคุกประจำท้องถิ่น (imprisonment in a county jail) ไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ”

---

[30] Clanton, K., "We Are Not Who We Pretend to Be: Odr Alternative to Online Impersonation Statues," Cardozo Journal of Conflict Resolution.

ทั้งนี้ สภานิติบัญญัติแห่งมลรัฐแคลิฟอร์เนียได้ระบุเหตุผลของการบัญญัติความผิดฐานดังกล่าวไว้ดังมีใจความสำคัญว่า กฎหมายที่มีอยู่ในปัจจุบันกำหนดให้การสวมรอยเป็นบุคคลอื่นไม่ว่าจะเป็นแบบส่วนตัวหรือทางการล้วนเป็นความผิดอาญา อีกทั้งยังกำหนดให้การเข้าถึง เปลี่ยนแปลง สร้างความเสียหาย ลบ ทำลาย หรือการใช้งานอื่น ๆ ซึ่งข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ โดยจงใจและปราศจากความยินยอม เพื่อวางแผนหรือดำเนินการตามแผนหรือกลอุบายเพื่อฉ้อโกง หลอกลวง หรือขู่กรรโชก หรือควบคุมหรือได้มาซึ่งเงิน ทรัพย์สิน หรือข้อมูลโดยมิชอบ ในกรณีที่มีการละเมิดเช่นว่านั้น นอกจากโทษทางอาญาที่กำหนดไว้โดยเฉพาะแล้ว กฎหมายยังให้สิทธิแก่คู่กรณีฝ่ายที่เสียหายฟ้องผู้กระทำละเมิดเป็นคดีแพ่งได้อีกด้วย

บทบัญญัตินี้กำหนดให้ผู้ใดโดยจงใจและปราศจากการได้รับความยินยอมกระทำการสวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือผ่านทางเว็บไซต์อินเทอร์เน็ตหรือโดยวิธีการทางอิเล็กทรอนิกส์อื่น ๆ โดยมีวัตถุประสงค์เพื่อประทุษร้าย ขู่ขวัญ ข่มขู่ให้หวาดกลัว หรือหลอกลวงฉ้อโกงผู้อื่น ผู้นั้นมีความผิดอาญาระดับลหุโทษ

สำหรับมาตรการบังคับตามกฎหมายนั้น การกระทำความผิดตามอนุมาตรา (a) และ (b) เป็นการสวมรอยบุคคลที่มีตัวตนอยู่จริง นับเป็นความผิดลหุโทษ มีระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือทั้งจำทั้งปรับ นอกจากโทษทางอาญาที่ระบุไว้โดยเฉพาะแล้วยังให้สิทธิแก่ผู้ที่ได้รับความเสียหายหรือสูญเสียสามารถฟ้องผู้ที่ละเมิดบทบัญญัตินี้เป็นคดีแพ่งได้อีกด้วย ได้แก่ ฟ้องร้องเรียกค่าสินไหมทดแทน (Compensatory Damages) หรือขอให้ศาลมีคำสั่งห้ามจำเลยกระทำการชั่วคราว (Injunctive Relief) หรือขอให้ศาลมีคำสั่งให้ชดใช้ด้วยทางอื่นอย่างเป็นธรรม (Equitable Relief)

ตัวอย่างคดีที่เคยเกิดขึ้นและมีการดำเนินคดีตามกฎหมายนี้

(1) คดีของ Jesus Felix ซึ่งให้การรับสารภาพว่าตนได้โพสรูปภาพลามกอนาจารของอดีตแฟนสาวลงบนหน้าเว็บไซต์เฟซบุ๊กเป็นจำนวนมากถึง 130 หน้า เพื่อคุกคามรังควานเหยื่อ ในหน้าเว็บดังกล่าวประกอบไปด้วยข้อมูลติดต่อและรูปภาพลามกอนาจารของเหยื่อ นอกจากนี้จำเลยยังคุกคามมารดาของเหยื่อด้วยการโทรศัพท์ไปหาเป็นจำนวนหลายครั้ง ในคดีนี้จำเลยถูกตัดสินว่ามีความผิดตามมาตรา 528.5 ต้องโทษจำคุกโดยรอลงอาญา 1 ปี และถูกลงโทษคุมประพฤตินาน

5 ปี และทำงานเพื่อสังคมเป็นเวลา 30 วัน นอกจากนี้ ศาลยังมีคำสั่งให้จำเลยต้องอยู่ให้ห่างจากเหยื่อ และห้ามไม่ให้เข้าถึงการใช้อินเทอร์เน็ตในระหว่างระยะเวลาที่ถูกคุมประพฤติ[31]

(2) คดีของ Rolando S. เมื่อ ค.ศ. 2011 ซึ่งศาลตัดสินว่าจำเลยไม่มีความผิดตามมาตรา 528.5 เนื่องจากจำเลยลงมือกระทำความผิดก่อนที่กฎหมายฉบับนี้จะมีผลใช้บังคับ อย่างไรก็ตาม ผู้พิพากษาศาลอุทธรณ์ George L. Orndoff ยืนยันว่า จำเลยมีความผิดภายใต้กฎหมายอื่นที่เกี่ยวข้อง ได้แก่ มาตรา 530.5 แห่งประมวลกฎหมายอาญารัฐแคลิฟอร์เนีย และได้ให้ความเห็นที่น่าสนใจไว้ท้ายคำพิพากษาเกี่ยวกับความแตกต่างระหว่างมาตรา 528.5 และมาตรา 530.5 ว่า มาตรา 528.5 ไม่ได้บัญญัติว่าจำเลยจะต้องมีเจตนาให้ได้มาซึ่งข้อมูลส่วนบุคคลของเหยื่อหรือตั้งใจกระทำโดยมีวัตถุประสงค์ที่ไม่ชอบด้วยกฎหมาย จึงไม่เหมือนกับมาตรา 530.5 ดังนั้น หากผู้ใดเพียงแต่ครอบครองข้อมูลส่วนบุคคลของบุคคลอื่นและใช้ข้อมูลเหล่านั้นเพื่อทำร้าย ขู่ขวัญ ข่มขู่ คุกคาม หรือหลอกลวงผู้อื่น ผู้นั้นอาจต้องรับผิดตามมาตรา 528.5[32]

(3) คดีหนึ่งในศาลสูงประจำท้องถิ่นซานตาคลารา (Santa Clara Superior Court) ใน ค.ศ. 2011[33] มีข้อเท็จจริงที่เกิดขึ้นดังนี้ จำเลยที่ 1 ซึ่งเป็นอดีตชายคนรักของโจทก์ได้ครอบครองรูปภาพส่วนตัวของโจทก์ซึ่งถูกบันทึกภาพไว้โดยยินยอมในระหว่างที่โจทก์และจำเลยที่ 1 มีความสัมพันธ์กัน หลายปีต่อมา จำเลยที่ 2 ซึ่งเป็นหญิงคนรักคนปัจจุบันของจำเลยที่ 1 นำรูปภาพของโจทก์ไปโพสลงบนบัญชีเฟซบุ๊กที่สร้างขึ้นใหม่ในนามของโจทก์ และใช้บัญชีดังกล่าวส่งคำร้องขอเป็นเพื่อน (Friend Request) ไปยังเพื่อน ญาติ และผู้ร่วมงานของโจทก์ ในคดีนี้โจทก์ฟ้องร้องจำเลยในข้อหาสวมรอยเป็นบุคคลบนเครือข่ายอินเทอร์เน็ตหรือโดยวิธีการทางอิเล็กทรอนิกส์ ตามมาตรา 528.5 แต่อย่างไรก็ตาม ศาลไม่ได้ตัดสินพิพากษาตามคำฟ้องของโจทก์ หากแต่ตัดสินให้โจทก์ได้รับชดใช้ค่าเสียหายเป็นจำนวนเงินทั้งสิ้น 190,000 ดอลลาร์สหรัฐ จากคำฟ้องในประเด็นเรื่องความประมาทเลินเล่อ (Negligence) การรุกล้ำเรื่องส่วนตัว (Intrusion into Private Affairs) และการ

---

[31] Without My Consent, "California Penal § 528.5 – Impersonation through Internet or Electronic Means," [Online] Accessed: 23 April 2017. Available from: http://withoutmyconsent.org/50state/31806784

[32] Clanton, K., "We Are Not Who We Pretend to Be: Odr Alternative to Online Impersonation Statues," Cardozo Journal of Conflict Resolution.

[33] [Names Redacted for Privacy], No. 112CV233490 (Santa Clara Co. Super. Ct. Feb. 18, 2014).

เปิดเผยข้อมูลส่วนบุคคลสู่สาธารณะ (Public Disclosure of Private Facts) รวมทั้งได้รับค่าเสียหายเชิงลงโทษ (Punitive Damages) อีก 60,000 ดอลลาร์สหรัฐ[34]

4.1.2.2.3 มลรัฐนิวยอร์ก (New York)

มลรัฐนิวยอร์กได้บัญญัติให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญา ดังปรากฏตามประมวลกฎหมายอาญาแห่งมลรัฐนิวยอร์ก มาตรา 190.25 (4) ดังนี้[35]

“มาตรา 190.25 บุคคลมีความผิดอาญาอุกฉกรรจ์ระดับสองในฐานสวมรอยเป็นบุคคลอื่นเมื่อบุคคลนั้น...

...(4) สวมรอยเป็นบุคคลอื่นผ่านการติดต่อสื่อสารทางเว็บไซต์อินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์ โดยเจตนาให้ได้มาซึ่งผลประโยชน์หรือเพื่อประทุษร้ายหรือหลอกลวงฉ้อโกงผู้อื่น หรืออาศัยช่องทางการติดต่อสื่อสารดังกล่าวทำการอวดอ้างตนเป็นเจ้าหน้าที่รัฐเพื่อโน้มน้าวจูงใจให้ผู้อื่นยอมต่ออำนาจเช่นนั้นหรือกระทำการโดยอาศัยความน่าไว้วางใจจากการอวดอ้างนั้น

การสวมรอยเป็นบุคคลอื่นในระดับสองเป็นความผิดลหุโทษระดับ A”

กฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของมลรัฐนิวยอร์กเกิดจากแนวความคิดของ Andrew Lanza หนึ่งในวุฒิสมาชิกของมลรัฐนิวยอร์ก ซึ่งเคยให้ความเห็นไว้ว่า ปัญหาเรื่องการสวมรอยเป็นบุคคลอื่นในระบบออนไลน์มีความรุนแรงมากยิ่งขึ้น เนื่องจากในปัจจุบันการค้นหาข้อมูลส่วนบุคคลในระบบออนไลน์สามารถทำได้ง่าย รวมถึงเว็บไซต์สื่อสังคมออนไลน์และเว็บไซต์หาคู่ก็มีจำนวนเพิ่มมากขึ้น ผู้กระทำความผิดจึงหาช่องทางที่จะหลอกลวงให้ประชาชนตกเป็นเหยื่อ จึงจำเป็นต้องแสดงให้เห็นถึงความอันตรายของการสวมรอยด้วยการตรากฎหมายนี้มาใช้บังคับ[36]

---

[34] Without My Consent, "Identity Theft," [Online] Accessed: 23 April 2017. Available from: http://withoutmyconsent.org/50state/291858029

[35] NEW YORK PENAL CODE § 190.25

[36] Clanton, K., "We Are Not Who We Pretend to Be: Odr Alternative to Online Impersonation Statues," Cardozo Journal of Conflict Resolution.

เจตนารมณ์ของกฎหมายฉบับนี้จึงมีขึ้นเพื่อยับยั้งมิให้เกิดการนำชื่อหรือข้อมูลส่วนบุคคลของผู้อื่นไปใช้โดยมิชอบ ผู้กระทำความผิดอาจมีวัตถุประสงค์ในการกระทำที่หลากหลาย ตั้งแต่สวมรอยเพื่อข่มขู่คุกคามไปจนถึงกระทำความผิดฐานโจรกรรมข้อมูลอันเป็นอัตลักษณ์ส่วนบุคคล (Identity Theft) ตลอดจนมีเจตนารมณ์ในการยับยั้งคดีเกี่ยวกับการแสดงตัวตนที่บิดเบือนผ่านเครือข่ายอินเทอร์เน็ตที่มีจำนวนมากเกินไปอีกด้วย

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตตามกฎหมายของมลรัฐนิวยอร์กถือเป็นความผิดลหุโทษระดับ A (Class A Misdemeanor) มีระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือทั้งจำทั้งปรับ ตามมาตรา 70.15[37] และมาตรา 80.15[38]

แต่อย่างไรก็ตาม หากกรณีที่เกิดขึ้นไม่สามารถนำกฎหมายฉบับนี้มาปรับใช้ได้ ศาลแห่งมลรัฐนิวยอร์กอาจปรับใช้กฎหมายอื่นที่เกี่ยวข้องแทน เช่น ประมวลกฎหมายอาญา มาตรา 190.77 – 80 ความผิดฐานโจรกรรมข้อมูลอันเป็นอัตลักษณ์ส่วนบุคคล (Identity Theft) หรือ มาตรา 240.25 ความผิดฐานคุกคาม (Harassment)[39]

ทั้งนี้ เนื่องจากมลรัฐเทกซัส มลรัฐแคลิฟอร์เนีย และมลรัฐนิวยอร์ก เป็นมลรัฐในยุคเริ่มแรกที่มีการออกกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ผู้เขียนจึงรวบรวมประเด็นทางกฎหมายที่น่าสนใจเป็นตารางเปรียบเทียบ ดังนี้

[37] NEW YORK PENAL CODE § 70.15

[38] NEW YORK PENAL CODE § 80.05

[39] Clanton, K., "We Are Not Who We Pretend to Be: Odr Alternative to Online Impersonation Statues," Cardozo Journal of Conflict Resolution.

ตารางที่ 2 กฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของมลรัฐเทกซัส มลรัฐแคลิฟอร์เนีย และมลรัฐนิวยอร์ก

มลรัฐ / ประเด็น	มลรัฐเทกซัส Texas Penal Code § 33.07	มลรัฐแคลิฟอร์เนีย California Penal Code § 528.5	มลรัฐนิวยอร์ก New York Penal Code § 190.25
ลักษณะการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต	(a) ใช้ชื่อหรือความเป็นตัวตนของบุคคลอื่นโดยมิได้รับความยินยอมจากบุคคลอื่นนั้นและโดยเจตนาเพื่อประทุษร้าย หลอกลวงฉ้อโกง ขู่ขวัญ หรือข่มขู่บุคคลใด ๆ ให้หวาดกลัว ด้วยการ (1) สร้างหน้าเว็บบนเว็บไซต์เครือข่ายสังคมออนไลน์เชิงพาณิชย์หรือเว็บไซต์อินเทอร์เน็ตอื่น หรือ (2) ประกาศหรือส่งข้อความผ่านทางเว็บไซต์เครือข่ายสังคมออนไลน์เชิงพาณิชย์หรือเว็บไซต์อินเทอร์เน็ตอื่น ยกเว้นโปรแกรมจดหมายอิเล็กทรอนิกส์หรือโปรแกรมกระดานข้อความ	โดยรู้อยู่แล้วและปราศจากความยินยอมกระทำการสวมรอยเป็นผู้อื่นอย่างน่าเชื่อถือผ่านทางเว็บไซต์อินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์อื่นใด โดยมีจุดประสงค์เพื่อประทุษร้าย ขู่ขวัญ ข่มขู่ให้หวาดกลัวหรือหลอกลวงฉ้อโกงผู้อื่น	สวมรอยเป็นบุคคลอื่นผ่านการติดต่อสื่อสารทางเว็บไซต์อินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์ โดยเจตนาให้ได้มาซึ่งผลประโยชน์หรือเพื่อประทุษร้ายหรือหลอกลวงฉ้อโกงผู้อื่น หรืออาศัยช่องทางการติดต่อสื่อสารดังกล่าวทำการอวดอ้างตนเป็นเจ้าหน้าที่รัฐเพื่อโน้มน้าวจูงใจให้ผู้อื่นยอมต่ออำนาจเช่นนั้นหรือกระทำการโดยอาศัยความน่าไว้วางใจจากการอวดอ้างนั้น
	(b) ส่งจดหมายอิเล็กทรอนิกส์ ข้อความด่วน ข้อความตัวอักษร หรือการติดต่อสื่อสารที่คล้ายคลึงกันนี้ซึ่งอ้างถึงชื่อ ที่อยู่ หมายเลขโทรศัพท์ หรือสิ่งอื่นใดที่แสดงข้อมูลอันเป็นอัตลักษณ์ของผู้อื่น (1) โดยปราศจากการได้รับความยินยอมจากผู้อื่นนั้น (2) โดยเจตนาเพื่อก่อให้ผู้รับการสื่อสารมีเหตุอันสมควรที่จะเชื่อได้ว่าผู้อื่นนั้นอนุญาตหรือเป็นผู้ส่งการสื่อสารนั้น และ (3) โดยเจตนาเพื่อประทุษร้ายหรือหลอกลวงฉ้อโกงบุคคลใด ๆ		
มาตรการบังคับทางอาญา	(a) เป็นความผิดอาญาอุกฉกรรจ์ระดับสาม ระวางโทษจำคุก 2-10 ปี หรือปรับไม่เกิน 10,000 ดอลลาร์สหรัฐ (b) เป็นความผิดลหุโทษระดับ A ระวางโทษกักขังในคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 4,000 ดอลลาร์สหรัฐ	ระวางโทษจำคุกไม่เกิน 1 ปีหรือปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือทั้งจำทั้งปรับ	เป็นความผิดลหุโทษระดับ A ระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ

มลรัฐ / ประเด็น	มลรัฐเทกซัส Texas Penal Code § 33.07	มลรัฐแคลิฟอร์เนีย California Penal Code § 528.5	มลรัฐนิวยอร์ก New York Penal Code § 190.25
การเยียวยาทางแพ่ง	ไม่มี	ผู้เสียหายสามารถดำเนินคดีแพ่งเรียกร้องค่าสินไหมทดแทนความเสียหายยื่นคำร้องขอให้ศาลมีคำสั่งห้ามกระทำการชั่วคราว หรือคำสั่งให้ชดใช้ด้วยทางอื่นอย่างเป็นธรรม	ไม่มี
ข้อยกเว้น	ไม่ใช้มาตรานี้บังคับแก่องค์กรหรือลูกจ้างที่ดำเนินการในทางการที่จ้างขององค์กรดังต่อไปนี้ เว็บไซต์ เครือข่ายสังคมออนไลน์เชิงพาณิชย์ ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการคอมพิวเตอร์แบบปฏิสัมพันธ์ ผู้ให้บริการโทรคมนาคม หรือผู้ให้บริการวิดีโอหรือเคเบิล	ไม่มี	ไม่มี

จากตารางข้างต้นจะเห็นได้ว่ามีประเด็นทางกฎหมายที่น่าสนใจหลายประการ ประการแรก กฎหมายของแต่ละมลรัฐกำหนดถึงลักษณะการกระทำความผิดไว้คล้ายคลึงกันและกำหนดให้เป็นความผิดลหุโทษ เว้นแต่มลรัฐเทกซัสที่มีการกำหนดความผิดไว้ 2 ระดับ ขึ้นอยู่กับเจตนาและความร้ายแรงของการกระทำความผิด ประการที่สอง มาตรการทางกฎหมายอาญาที่ใช้บังคับกับผู้กระทำความผิด ได้แก่ โทษจำคุก โทษปรับ และโทษกักขัง ส่วนมาตรการทางแพ่งอันได้แก่ การเยียวยาความเสียหายหรือการร้องขอให้ศาลมีคำสั่งอื่น ๆ นั้น ปรากฏเฉพาะในบทบัญญัติของมลรัฐแคลิฟอร์เนีย ประการสุดท้าย มลรัฐเทกซัสเป็นมลรัฐเดียวในกลุ่มนี้ที่กำหนดข้อยกเว้นมิให้นำบทบัญญัติไปใช้บังคับกับกลุ่มองค์กรหรือกลุ่มบุคคลที่เป็นผู้ให้บริการด้านการสื่อสารทางอิเล็กทรอนิกส์

อย่างไรก็ตาม หลังจากมลรัฐเทกซัส มลรัฐแคลิฟอร์เนีย และมลรัฐนิวยอร์กได้ประกาศใช้กฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ทำให้มลรัฐอื่นเกิดความตื่นตัวในการแก้ไขจัดการปัญหาการสวมรอยเป็นบุคคลอื่นมากยิ่งขึ้น หลายมลรัฐได้ยกร่างกฎหมายเกี่ยวกับการนี้ซึ่งมีรายละเอียดบทบัญญัติที่น่าศึกษาดังต่อไปนี้

4.1.2.2.4 มลรัฐลุยเซียนา (Louisiana)

มลรัฐลุยเซียนาได้บัญญัติให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญา ดังปรากฏตามประมวลกฎหมายอาญาของรัฐลุยเซียนา มาตรา 73.10 ดังนี้

“มาตรา 73.10 การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

A. 1) ผู้ใดจงใจสวมรอยเป็นบุคคลอื่นโดยปราศจากความยินยอมของบุคคลอื่นนั้น โดยมีเจตนาเพื่อประทุษร้าย ขู่ขวัญ ข่มขู่ให้หวาดกลัว หรือหลอกลวงฉ้อโกง ด้วยวิธีการดังนี้

(a) เปิดใช้งานบัญชีจดหมายอิเล็กทรอนิกส์ บัญชีผู้ใช้งานเว็บไซต์เครือข่ายสังคมออนไลน์ หรือเว็บไซต์อินเทอร์เน็ตอื่นใด

(b) ประกาศหรือส่งข้อความผ่านทางเว็บไซต์เครือข่ายสังคมออนไลน์หรือเว็บไซต์อินเทอร์เน็ตอื่นใด

ผู้นั้นมีความผิด

2) ผู้ใดมีเจตนาประทุษร้าย ขู่ขวัญ ข่มขู่ให้หวาดกลัว หรือหลอกลวงฉ้อโกง และส่งจดหมายอิเล็กทรอนิกส์ ข้อความด่วน ข้อความตัวอักษร หรือรูปแบบการติดต่อสื่อสารทางอิเล็กทรอนิกส์อื่นใดซึ่งอ้างถึงชื่อ ที่อยู่ หมายเลขโทรศัพท์ หรือสิ่งอื่นใดที่เป็นข้อมูลอัตลักษณ์ของบุคคลอื่น โดยปราศจากความยินยอมของบุคคลนั้นและมีเจตนาก่อให้ผู้รับการสื่อสารเชื่อว่าบุคคลที่ถูกสวมรอยอนุญาตหรือเป็นผู้ส่งสารที่สื่อมานั้น ผู้นั้นมีความผิด

C. (1) เว้นแต่ที่บัญญัติไว้ในวรรค (2) ของอนุมาตรานี้ ผู้ใดกระทำการฝ่าฝืนบทบัญญัติใด ๆ ที่ปรากฏในมาตรานี้ต้องโทษปรับไม่ต่ำกว่า 250 ดอลลาร์สหรัฐ แต่ไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือจำคุกไม่ต่ำกว่า 10 วัน แต่ไม่เกิน 6 เดือน หรือทั้งจำทั้งปรับ

(2) กรณีผู้กระทำผิดมีอายุต่ำกว่า 17 ปี ให้ดำเนินการจัดการตามบทบัญญัติหมวด 5 แห่งประมวลกฎหมายว่าด้วยเด็ก

D. บทบัญญัติตามมาตรานี้ไม่บังคับใช้กับบุคคลดังต่อไปนี้หรือบุคคลที่รับจ้างทำงานตามทางการที่จ้างให้แก่บุคคลดังต่อไปนี้

(1) เว็บไซต์เครือข่ายสังคมออนไลน์

(2) ผู้ให้บริการคอมพิวเตอร์ที่มีระบบปฏิสัมพันธ์

(3) ผู้ให้บริการการติดต่อสื่อสารทางไกล

(4) ผู้ประกอบการด้านสายเคเบิล

(5) ผู้ให้บริการอินเทอร์เน็ต

(6) เจ้าหน้าที่หรือเจ้าพนักงานบังคับใช้กฎหมาย”

4.1.2.2.5 มลรัฐวอชิงตัน

มลรัฐวอชิงตันถือว่าการสวมรอยเป็นบุคคลอื่นนั้นเป็นการรุกล้ำความเป็นส่วนตัว (Invasion of Privacy) และได้ยกร่างบทบัญญัติเกี่ยวกับการกระทำดังกล่าวไว้ ดังนี้[40]

“มาตรา... การสวมรอยเป็นบุคคลอื่นทางอิเล็กทรอนิกส์ (Electronic Impersonation) – การรุกล้ำความเป็นส่วนตัว (Action for Invasion of Privacy) ...

... (2) บุคคลอาจต้องรับผิดทางแพ่งเนื่องจากการรุกล้ำความเป็นส่วนตัวเมื่อ

(a) บุคคลนั้นสวมรอยเป็นบุคคลอื่นบนเว็บไซต์เครือข่ายสังคมออนไลน์หรือกระดานสนทนาออนไลน์

(b) การสวมรอยเป็นบุคคลอื่นนั้นเกิดด้วยเจตนาและปราศจากความยินยอมของผู้ถูกสวมรอย

(c) บุคคลนั้นเจตนาหลอกลวงหรือก่อให้เกิดความเข้าใจผิดเพื่อรังควาน คุกคาม ข่มขู่ ทำให้เสียเกียรติ หรือหลอกลวงผู้อื่น และ

(d) การสวมรอยนั้นเป็นมูลเหตุใกล้ชิดของความเสียหายที่เกิดแก่ผู้ถูกสวมรอย ความเสียหายนี้อาจประกอบด้วยความเสียหายต่อชื่อเสียงหรือความอัปยศ ความเสียหายต่อตำแหน่งทางอาชีพหรือการเงิน หรือการทำร้ายร่างกาย

(3) (a) ผู้เสียหายจากการถูกสวมรอยตามมาตรานี้อาจฟ้องร้องเพื่อให้ได้รับการชดใช้เยียวยาความเสียหาย ขอให้ศาลมีคำสั่งห้ามจำเลยกระทำการชั่วคราว (Injunctive Relief) หรือขอให้ศาลมีคำสั่งแสดงสิทธิ (Declaratory Relief) ศาลอาจสั่งให้ได้เท่าที่จำเป็น”

---

[40] REVISED CODE OF WASHINGTON § 4.24.790

ผู้ร่างกฎหมายได้ระบุเจตนารมณ์ของการกำหนดฐานความผิดดังกล่าวไว้ในร่างกฎหมาย ดังมีใจความสำคัญว่า สภานิติบัญญัติพบว่า แม้ว่าเว็บไซต์เครือข่ายสังคมออนไลน์และกระดานสนทนาออนไลน์จะสร้างโอกาสอันทรงคุณค่าในการติดต่อประสานงาน แต่ยังเปิดโอกาสให้มีการกระทำที่สร้างความเสียหายแก่บุคคลอื่นได้อีกด้วย แม้ว่าจะมีการแก้ไขเยียวยาทั้งทางแพ่งและทางอาญาสำหรับกรณีฉ้อโกง การสวมรอย และการใช้ความเป็นตัวตนของบุคคลอื่นเพื่อจุดประสงค์ทางการค้าหรือแสวงหากำไรอยู่แล้ว แต่อย่างไรก็ตาม การปรับใช้วิธีการดั้งเดิมเหล่านี้กับการสวมรอยเป็นบุคคลอื่นผ่านทางระบบอินเทอร์เน็ตเพื่อสร้างความเข้าใจผิด หลอกลวง คุกคาม ข่มขู่ หรือกรรโชกนั้นค่อนข้างเป็นเรื่องใหม่และยังไม่ชัดแจ้งนัก ศาลยอมรับการล่วงละเมิดสิทธิความเป็นส่วนตัวของผู้อื่น การล่วงละเมิดความเป็นส่วนตัวประเภทหนึ่งได้แก่ การนำชื่อของผู้อื่นหรือความคล้ายคลึงกับผู้อื่นไปใช้โดยมิชอบ สภานิติบัญญัติประสงค์จะกำหนดเป็นการเฉพาะเจาะจงว่า การล่วงละเมิดความเป็นส่วนตัวอาจประกอบไปด้วยการนำชื่อหรือความคล้ายคลึงกันกับบุคคลอื่นไปใช้โดยมิชอบผ่านทางเว็บไซต์เครือข่ายสังคมออนไลน์และกระดานสนทนาออนไลน์ โดยเจตนาสร้างความเข้าใจผิด หลอกลวง คุกคาม ข่มขู่ หรือกรรโชก[41]

4.1.2.2.6 มลรัฐเซาท์แคโรไลนา

มลรัฐเซาท์แคโรไลนาได้ยกร่างกฎหมายว่าด้วยการป้องกันการสวมรอยเป็นบุคคลอื่นทางดิจิทัล (Digital Impersonation Prevention Act) ขึ้นเมื่อ ค.ศ. 2013 ด้วยการแก้ไขเพิ่มเติมประมวลกฎหมายของมลรัฐเซาท์แคโรไลนา (The Code of Laws of South Carolina, 1976) ปรากฏตามร่างกฎหมายดังนี้[42]

“Article 3 Digital Impersonation Prevention Act

มาตรา 37-20-310.

(A) ภายใต้เจตนารมณ์ของมาตรานี้

(1) “วิธีการทางอิเล็กทรอนิกส์ (Electronic Means)” หมายความว่า การเปิดใช้งาน การเข้าถึง การปรับเปลี่ยน หรือการสร้างบัญชีจดหมายอิเล็กทรอนิกส์ปลอม หรือบัญชีหรือประวัติโดยย่อปลอมบนเว็บไซต์ทางอินเทอร์เน็ต หรือการแจ้งประกาศบนเว็บไซต์เครือข่ายสังคมออนไลน์ กระดานสนทนาอิเล็กทรอนิกส์ หรือหน้าโฆษณาออนไลน์

---

[41] Ibid.

[42] SOUTH CAROLINA HOUSE BILL 3107

(2) “กระดานสนทนาอิเล็กทรอนิกส์ (Electronic Bulletin Board)” หมายถึง ระบบการติดต่อสื่อสารออนไลน์ซึ่งบุคคลอาจแบ่งปัน ร้องขอ หรืออภิปรายข้อมูลได้

(3) “การล้อเล่น (Spoofing)” หมายถึง การปลอมชื่อหรือหมายเลขโทรศัพท์ซึ่งปรากฏบนระบบระบุตัวตนของผู้โทร

(B) แม้ว่าจะมีบทบัญญัติแห่งกฎหมายอื่นปรากฏอยู่ก็ตาม ผู้ใดโดยรู้อยู่แล้วและปราศจากความยินยอมจงใจสวมรอยเป็นบุคคลอื่น โดยมีเจตนาเพื่อรังควานหรือประทุษร้ายผ่านทางเว็บไซต์อินเทอร์เน็ต หรือทางวิธีการทางอิเล็กทรอนิกส์อื่นใด โดยมิใช่เพียงล้อเล่นเท่านั้น ผู้นั้นมีความผิดลหุโทษ จำต้องถูกลงโทษปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ

(C) นอกเหนือจากการเยียวยาทางแพ่งที่เป็นไปได้อื่นใดแล้ว ผู้ที่ได้รับความเสียหายหรือสูญเสียจากการละเมิดตามอนุมาตรา (A) อาจฟ้องร้องผู้กระทำละเมิดเป็นคดีทางแพ่งเพื่อขอให้ชดใช้ค่าสินไหมทดแทน (Compensatory Damages) และขอให้ศาลมีคำสั่งห้ามจำเลยกระทำการชั่วคราว (Injunctive Relief) หรือคำสั่งให้ชดใช้ด้วยทางอื่นอย่างเป็นธรรม (Equitable Relief) อื่นได้”

4.1.2.2.7 มลรัฐนอร์ทแคโรไลนา

เมื่อวันที่ 15 เมษายน 2015 สภานิติบัญญัติแห่งมลรัฐนอร์ทแคโรไลนาได้ยกร่างกฎหมายฉบับหนึ่งขึ้นเพื่อกำหนดให้การสวมรอยเป็นบุคคลอื่นผ่านทางระบบอินเทอร์เน็ตเพื่อจุดประสงค์ที่มิชอบด้วยกฎหมายเป็นความผิดอาญาอุกฉกรรจ์ระดับ H (Class H Felony) โดยเพิ่มเติมฐานความผิดดังกล่าวไว้ในหมวด 14 ของรัฐบัญญัติ ดังนี้[43]

“มาตรา 14-118.8. การสวมรอยเป็นบุคคลอื่นในระบบออนไลน์ (Online Impersonation)

(a) ใช้คำนิยามดังต่อไปนี้

(1) การสวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือ (Credible Impersonation) หมายความว่า กรณีที่ผู้อื่นอาจจะมีเหตุอันสมควรที่จะเชื่อได้ว่า หรือได้เชื่อโดยมีเหตุอันสมควรว่าจำเลยได้เป็นหรือเป็นบุคคลที่ถูกสวมรอย

[43] NORTH CAROLINA HOUSE BILL 794

(2) วิธีการทางอิเล็กทรอนิกส์ (Electronic Means) ประกอบด้วย บัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ บัญชีผู้ใช้งานข้อความด่วน หรือบัญชีผู้ใช้งานหรือโพรไฟล์ของเว็บไซต์เครือข่ายสังคมในนามของผู้อื่น

(b) ผู้ใดโดยรู้อยู่แล้วและไม่ได้รับความยินยอมกระทำการสวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือผ่านทางเว็บไซต์บนเครือข่ายอินเทอร์เน็ตหรือโดยวิธีการทางอิเล็กทรอนิกส์เพื่อประทุษร้าย ข่มขู่คุกคาม หรือหลอกลวงผู้อื่น ผู้นั้นมีความผิดอาญาอุกฉกรรจ์ระดับ H ต้องระวางโทษปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือจำคุก หรือทั้งจำทั้งปรับ

(c) เจ้าของข้อมูลที่ถูกเปิดเผยหรือถูกใช้เนื่องจากวิธีการสวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือนั้นสามารถฟ้องร้องผู้ที่เปิดเผยหรือใช้ข้อมูลนั้นเป็นคดีแพ่ง และมีสิทธิได้รับการเยียวยาจากผู้กระทำผิด ดังนี้

(1) ค่าเสียหายตามจริง (Actual Damages) แต่ไม่น้อยกว่าเบี้ยปรับ ซึ่งคำนวณตามอัตรา 1,000 ดอลลาร์สหรัฐต่อวันที่เกิดการละเมิด หรือ 10,000 ดอลลาร์สหรัฐ

(2) ค่าเสียหายเชิงลงโทษ (Punitive Damages)

(3) ค่าธรรมเนียมทนายความ รวมถึงค่าใช้จ่ายในการดำเนินคดีอื่น ๆ ตามความเหมาะสม

(d) มาตรานี้ไม่ใช้บังคับแก่

(1) เจ้าหน้าที่บังคับใช้กฎหมายในขณะที่เจ้าหน้าที่กำลังปฏิบัติหน้าที่หรือพยายามปฏิบัติหน้าที่

(2) ผู้ที่ได้รับอนุญาตตามหมวด 74C (บริการคุ้มครองความเป็นส่วนตัว) หรือหมวด 74D (ระบบแจ้งเตือน) ของรัฐบัญญัตินี้ ในขณะที่ผู้นั้นเข้าไปมีส่วนร่วมกับการปฏิบัติหน้าที่ตามอาชีพ และไม่ได้เกี่ยวข้องกับการกระทำที่มีวัตถุประสงค์ไม่เหมาะสมดังที่บัญญัติไว้ในมาตรานี้”

กล่าวโดยสรุป สหรัฐอเมริกาเห็นว่าการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นอาชญากรรมที่สร้างความเสียหายต่อประชาชนในหลายมิติ ไม่ว่าจะเป็นความเสียหายต่อชื่อเสียงเกียรติคุณ ความเสียหายต่อทรัพย์สินและการเงิน ความเสียหายที่กระทบกระเทือนต่อการใช้ชีวิตอย่างปกติสุข เช่น การถูกทำร้ายร่างกาย การถูกเลิกจ้าง เป็นต้น อีกทั้งยังเป็นการละเมิดต่อตัวตน

ของบุคคล สิทธิส่วนบุคคล และข้อมูลส่วนบุคคล ด้วยเหตุนี้ หลายมลรัฐจึงมีมาตรการทางกฎหมายสำหรับจัดการปัญหาดังกล่าวด้วยการยกร่างกฎหมายเฉพาะกำหนดให้การสวมรอยเช่นว่านี้เป็นความผิดทางอาญาและกำหนดบทลงโทษไว้สองประเภท ได้แก่ โทษจำคุกและโทษปรับ แต่ทั้งนี้บางมลรัฐได้เพิ่มเติมมาตรการเยียวยาทางแพ่งไว้เพื่อชดเชยความเสียหายของผู้เสียหายอีกด้วย การใช้มาตรการทางกฎหมายเช่นนี้เป็นการให้ความคุ้มครองความปลอดภัยในสิทธิส่วนบุคคล ข้อมูลส่วนบุคคล และสิทธิในการดำรงชีวิตอื่น ๆ ของบุคคล มิให้ถูกล่วงละเมิดจากการถูกนำความเป็นตัวตนไปแอบอ้างสวมรอยเพื่อสร้างความเดือดร้อนแก่สาธารณะต่อไป

4.2 สหราชอาณาจักร

ปัญหาการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตกลายเป็นภัยคุกคามชนิดใหม่ทางโลกไซเบอร์ของสหราชอาณาจักร นอกจากจะเป็นการกระทำที่ล่วงละเมิดต่อข้อมูลส่วนบุคคลแล้วยังเกี่ยวโยงกับการกระทำความผิดอื่นอีกหลายลักษณะ เช่น การข่มขู่คุกคาม การทำให้ชื่อเสียงเสื่อมเสีย การละเมิดในทางเพศ หรือการกระทำความผิดผ่านช่องทางการสื่อสารสาธารณะ เป็นต้น การกระทำที่ไม่ชอบเหล่านี้เริ่มปรากฏมากขึ้นและจำเป็นต้องมีมาตรการทางกฎหมายเข้ามาจัดการกับปัญหาที่เกิดขึ้นอย่างเหมาะสมและมีประสิทธิภาพ

ในหัวข้อนี้ผู้เขียนจะแสดงให้เห็นถึงสภาพปัญหาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตที่เกิดขึ้นในสหราชอาณาจักร และมาตรการทางกฎหมายที่นำมาปรับใช้กับการกระทำความผิดที่เกิดขึ้น อันได้แก่ คู่มือการฟ้องคดีที่เกี่ยวข้องกับการติดต่อสื่อสารที่ส่งผ่านทางสื่อสังคมออนไลน์ (CPS Guidelines on Prosecuting Cases Involving Communication Sent Via Social Media) และแนวทางการปรับใช้บทบัญญัติแห่งกฎหมายอื่นที่เกี่ยวข้อง

4.2.1 ประเด็นปัญหาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในสหราชอาณาจักร

ประชาชนในสหราชอาณาจักรต้องประสบปัญหาเกี่ยวกับการถูกนำข้อมูลส่วนบุคคลไปใช้แอบอ้างสวมรอยบนโลกไซเบอร์เช่นเดียวกันกับสหรัฐอเมริกา การกระทำเช่นว่านี้ส่งผลกระทบต่อการใช้ชีวิตประจำวันในหลายด้าน เช่น ผลกระทบต่อชื่อเสียง การล่วงละเมิดสิทธิส่วนบุคคล ความเสียหายต่อความน่าเชื่อถือในธุรกิจ การละเมิดทรัพย์สินทางปัญญา เป็นต้น ดังเช่นเหตุการณ์การสวม

รอยเป็นผู้บริหารของบริษัทแห่งหนึ่งเพื่อฉ้อโกงเงินทุนของบริษัทด้วยการส่งจดหมายอิเล็กทรอนิกส์ปลอมไปยังพนักงานของบริษัทให้โอนเงินให้ผู้กระทำความผิด[44] หรือตัวอย่างคดีที่เคยเกิดขึ้นในสหราชอาณาจักร เช่นคดีของ Mathew Firsht ใน ค.ศ. 2008 จำเลยซึ่งเป็นอดีตเพื่อนร่วมงานและผู้ช่วยเหลือด้านธุรกิจของผู้เสียหายได้สร้างบัญชีโพรไฟล์เว็บไซต์เฟซบุ๊กในนามของผู้เสียหายโดยปราศจากความยินยอม โพรไฟล์เฟซบุ๊กดังกล่าวประกอบไปด้วยข้อมูลส่วนบุคคลของผู้เสียหาย ทั้งข้อมูลเกี่ยวกับรสนิยมทางเพศ สถานะความสัมพันธ์ วันเกิด และมุมมองทางศาสนาและการเมือง แม้ว่าข้อมูลเหล่านั้นจะไม่ถูกต้องตรงตามความจริงทั้งหมด แต่ศาลถือว่าเป็นข้อมูลที่ผู้เสียหายมีความคาดหวังในความเป็นส่วนตัวโดยชอบด้วยกฎหมาย (Legitimate Expectation of Privacy) ในคดีดังกล่าวศาลได้ตัดสินว่า การสร้างบัญชีโพรไฟล์ปลอมถือเป็นการใช้ข้อมูลส่วนบุคคลโดยมิชอบ นอกจากนี้ ศาลยังพิจารณาว่าการสร้างบัญชีโพรไฟล์ปลอมและสร้างกลุ่มสนทนาในหัวข้อว่าผู้เสียหายเคยโกหกหรือไม่ นับว่าเป็นการเขียนข้อความทำให้ผู้เสียหายเสื่อมเสียชื่อเสียง ถือเป็นการกระทำความผิดฐานหมิ่นประมาทอีกประการหนึ่ง[45]

4.2.2 มาตรการทางกฎหมายที่เกี่ยวข้อง

แม้ว่าเทคโนโลยีที่ทันสมัยจะเข้ามามีบทบาทในการติดต่อสื่อสารของคนในสังคมมากขึ้นและเกิดปัญหาการสวมรอยเป็นบุคคลอื่นผ่านทางเว็บไซต์หรือวิธีการทางอิเล็กทรอนิกส์อื่น ๆ เช่นเดียวกับสหรัฐอเมริกา แต่สหราชอาณาจักรกลับไม่มีกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการเฉพาะแต่อย่างใด โดยทั่วไปแล้ว เพียงแต่การแสร้งทำตัวเป็นบุคคลอื่นไม่ถือเป็นการกระทำที่ผิดกฎหมายในสหราชอาณาจักร เว้นแต่การสวมรอยเช่นนั้นไปเกี่ยวข้องกับการกระทำความผิดอื่น หรือเป็นสาเหตุที่นำไปสู่การกระทำความผิดอื่นต่อไป อาจถือเป็นการกระทำที่ผิดกฎหมายอาญาหรือแพ่งได้ ขึ้นอยู่กับพฤติการณ์ว่าการสวมรอยนั้นกระทบกระเทือนหรือละเมิดสิทธิประเภทใดของผู้เสียหาย ดังนั้น การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในสหราชอาณาจักรจึงอาจเกี่ยวข้องกับความผิดได้หลายกรณี หน่วยงานในกระบวนการยุติธรรมต่างวางแนวทางและมาตรการดำเนินคดีในความผิดดังกล่าวไว้หลายแนวทาง ดังต่อไปนี้

---

[44] PricewaterhouseCoopers LLP and PwC Legal LLP, "Alert: Internet and Impersonation Fraud Utilising the Pricewaterhousecoopers Llp and Pwc Legal Llp Brands," [Online] Accessed: 9 April 2017. Available from: https://www.pwc.co.uk/who-we-are/internet-and-impersonation-fraud.html

[45] In Brief, "What Is the Law on Impersonating Another Person on Facebook?"

4.2.2.1 คู่มือการฟ้องคดีที่เกี่ยวข้องกับการติดต่อสื่อสารที่ส่งผ่านทางสื่อสังคมออนไลน์ (CPS Guidelines on Prosecuting Cases Involving Communication Sent via Social Media)

ในเดือนมีนาคม ค.ศ. 2016 สำนักงานอัยการของสหราชอาณาจักร (Crown Prosecution Service : CPS) ได้ทบทวนคู่มือการฟ้องคดีที่เกี่ยวข้องกับการติดต่อสื่อสารที่ส่งผ่านทางสื่อสังคมออนไลน์ (Guidelines on Prosecuting Cases Involving Communication Sent via Social Media) สำหรับใช้เป็นวิธีปฏิบัติงานของนักกฎหมาย ตำรวจ และอัยการในการดำเนินคดีที่เกิดขึ้นบนเว็บไซต์สื่อสังคมออนไลน์ตามกฎหมายที่มีการใช้บังคับอยู่ โดยไม่ต้องยกร่างกฎหมายเฉพาะขึ้นใหม่ เนื่องจากการติดต่อสื่อสารผ่านทางสื่อสังคมออนไลน์นั้นอาจกลายเป็นความผิดทางอาญาได้ เจ้าหน้าที่ตำรวจและอัยการจึงควรมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ประเมินในเบื้องต้นว่า การกระทำนั้นตรงตามลักษณะความผิดประเภทใดและสามารถดำเนินคดีได้อย่างถูกต้องต่อไป

คู่มือการฟ้องคดีดังกล่าวข้างต้นแบ่งลักษณะการกระทำความผิดทางสื่อสังคมออนไลน์ออกเป็น 4 ประเภทดังต่อไปนี้[46]

ประเภทที่ 1 Credible Threats หมายถึง การติดต่อสื่อสารที่อาจก่อให้เกิดการข่มขู่อย่างน่าเชื่อถือว่าจะใช้ความรุนแรงต่อบุคคลหรือทำให้ทรัพย์สินเสียหาย การกระทำเช่นนี้อาจเป็นความผิดอาญาตามกฎหมายต่าง ๆ หลายฉบับ ขึ้นอยู่กับองค์ประกอบของการกระทำ เช่น กรณีที่เป็นการข่มขู่ว่าจะฆ่าผู้อื่นถือเป็นความผิดตามมาตรา 16 แห่ง Offences against the Person Act 1861 กรณีที่เป็นการข่มขู่ที่ทำให้ผู้อื่นตกอยู่ในความหวาดกลัวต่อความรุนแรงที่อาจเกิดขึ้น ถือเป็นความผิดตามมาตรา 4 แห่ง Protection from Harassment Act 1997 กรณีที่เป็นการข่มขู่ว่าจะใช้ความรุนแรงกับผู้อื่นหรือทำให้ทรัพย์สินเสียหายด้วยการส่งการติดต่อสื่อสารผ่านทางระบบอิเล็กทรอนิกส์ถือเป็นความผิดตามมาตรา 1 แห่ง Malicious Communications Act 1988 หรือกรณีการส่งข้อความที่มีลักษณะข่มขู่คุกคามผ่านทางเครือข่ายโทรคมนาคมสาธารณะถือเป็นความผิดตามมาตรา 127 แห่ง Communications Act 2003 เป็นต้น

---

[46] Crown Prosecuting Service, "Guidelines on Prosecuting Cases Involving Communications Sent Via Social Media," [Online] Accessed: 25 January 2017. Available from: http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/#content

ประเภทที่ 2 Communications Targeting Specific Individuals หมายถึง การติดต่อสื่อสารที่มุ่งเป้าไปที่บุคคลใดบุคคลหนึ่งหรือกลุ่มบุคคลกลุ่มใดกลุ่มหนึ่งเป็นพิเศษ และมีลักษณะการกระทำภายในขอบเขตดังต่อไปนี้

(1) ความผิดเกี่ยวกับการคุกคามหรือติดตาม ตามมาตรา 2 มาตรา 2A มาตรา 4 หรือมาตรา 4A แห่ง Protection from Harassment Act 1997

(2) ความผิดเกี่ยวกับพฤติกรรมที่มีลักษณะควบคุมหรือบีบบังคับ ตามมาตรา 76 แห่ง Serious Crime Act 2015

(3) ความผิดเกี่ยวกับสื่อลามกเพื่อการแก้แค้น ตามมาตรา 33 แห่ง Criminal Justice and Courts Act 2015

(4) ความผิดอื่นที่เกี่ยวข้องกับการสื่อสารที่มุ่งเป้าไปยังบุคคลใดบุคคลหนึ่งโดยเฉพาะเจาะจง เช่น ความผิดตาม Sexual Offences Act 2003 หรือการข่มขู่ว่าจะเปิดโปงความลับ (blackmail) เป็นต้น

ประเภทที่ 3 Breach of Court Orders and Statutory Prohibitions หมายถึง การติดต่อสื่อสารที่อาจกลายเป็นการละเมิดคำสั่งศาลหรือข้อห้ามที่มีกฎหมายกำหนดไว้

ประเภทที่ 4 Communication which are Grossly Offensive, Indecent, Obscene or False หมายถึง การติดต่อสื่อสารที่ไม่เข้าตามประเภทที่ 1 - 3 และมีลักษณะเป็นการละเมิดทางกายภาพ หยาบคาย ลามกอนาจาร หรือเป็นความเท็จ

ลักษณะการกระทำความผิดประเภทที่ 4 เป็นหลักเกณฑ์ที่ได้รับการกำหนดขึ้นใหม่ในครั้งที่มีการทบทวนคู่มือปฏิบัติงานเมื่อ ค.ศ. 2016 เพื่อตอบสนองต่อการดำเนินคดีเกี่ยวกับการสร้างบัญชีสื่อสังคมออนไลน์ปลอมและการแก้แค้นด้วยการส่งรูปภาพหรือวีดิโอลามกอนาจารที่มีจำนวนเพิ่มมากขึ้นเรื่อย ๆ ในการนี้ หากเจ้าหน้าที่ที่เกี่ยวข้องประเมินเหตุการณ์แล้วลงความเห็นว่าการกระทำความผิดมีลักษณะตรงตามประเภทที่ 4 จะมีกฎหมายสำคัญที่เข้ามาเกี่ยวข้องกับกรณีเช่นนี้หลายมาตรา ตัวอย่างเช่น

(1) มาตรา 1 แห่ง Malicious Communications Act 1988[47] เป็นความผิดเกี่ยวกับการส่งการติดต่อสื่อสารไปยังผู้อื่น ซึ่งหยาบคายหรือละเมิดทางกายภาพ หรือแสดงถึงการข่มขู่ หรือเป็นความเท็จ โดยมีเจตนาสร้างความทุกข์ร้อนหรือความวิตกกังวลแก่ผู้รับ

(2) มาตรา 127 แห่ง Communications Act 2003[48] เป็นความผิดอันเกิดจากการส่งหรือก่อให้เกิดการส่งข้อความหรือสิ่งอื่นใดที่มีลักษณะละเมิดทางกายภาพ หรือลามกอนาจาร หรือข่มขู่ให้กลัว ผ่านทางระบบการสื่อสารอิเล็กทรอนิกส์สาธารณะ หรือส่งหรือก่อให้เกิดการส่งข้อความเท็จโดยมีวัตถุประสงค์ก่อความรำคาญ ความไม่สะดวก หรือความวิตกกังวลโดยไม่จำเป็นแก่ผู้อื่น ทั้งนี้ จำเลยจะต้องมีเจตนาหรือตระหนักได้ว่าข้อความนั้นมีลักษณะละเมิดทางกายภาพ ลามกอนาจาร หรือข่มขู่ให้กลัว

คู่มือปฏิบัติงานดังกล่าวได้กำหนดแนวทางการดำเนินคดีเกี่ยวกับบัญชีสื่อสังคมออนไลน์ปลอมหรือที่มีลักษณะล่วงละเมิด (False or Offensive Social Media Cases) ไว้เป็นการเฉพาะ โดยระบุว่า การสร้างบัญชีสื่อสังคมออนไลน์ที่เป็นความเท็จหรือปลอม หรือการสร้างเว็บไซต์หรือโพรไฟล์หรือนามแฝงปลอมหรือมีลักษณะล่วงละเมิด อาจกลายเป็นความผิดอาญาได้ ขึ้นอยู่กับพฤติการณ์และลักษณะการกระทำของผู้กระทำความผิด เช่น การสร้างบัญชีเว็บไซต์เฟซบุ๊กปลอมขึ้นในนามของเหยื่อ เพื่อโจมตีให้เหยื่อได้รับความเสียหายหรือความเดือดร้อนรำคาญ โดยโพรไฟล์ดังกล่าวจะประกอบไปด้วยเนื้อหาที่มีลักษณะล่วงละเมิดทางกายภาพ เป็นความเท็จ คุกคาม หรือลามกน่ารังเกียจ ทั้งนี้ การสร้างโพรไฟล์สื่อสังคมออนไลน์ปลอมหรือที่มีลักษณะล่วงละเมิดดังกล่าวอาจเป็นการกระทำความผิดประเภทที่ 1 ประเภทที่ 2 หรือประเภทที่ 4 ก็ได้ แล้วแต่กรณี

4.2.2.2 ความรับผิดตามกฎหมายอื่น ๆ ที่เกี่ยวข้อง

ตามที่ได้กล่าวมาแล้วข้างต้นว่าสหราชอาณาจักรไม่มีบทบัญญัติกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดเฉพาะ แต่นำบทบัญญัติที่มีอยู่แล้วมาปรับใช้เป็นรายกรณีไป เป็นเหตุให้ผู้สวมรอยอาจถูกดำเนินคดีในความผิดตามกฎหมายอื่น ๆ ที่เกี่ยวข้องได้หลายฉบับดังต่อไปนี้

---

[47] MALICIOUS COMMUNICATIONS ACT 1988 § 1

[48] COMMUNICATIONS ACT 2003 § 127

4.2.2.2.1 Public Order Act 1986

การสร้างเว็บไซต์หรือโพรไฟล์สื่อสังคมออนไลน์ปลอมหรือมีลักษณะล่วงละเมิดข้างต้น อาจกลายเป็นความผิดตาม Public Order Act 1986 ได้อีกประการหนึ่ง ตัวอย่างเช่น คดีพิพาทระหว่าง S v Crown Prosecution Service ของศาลสูงแห่งอังกฤษและเวลส์ (England and Wales High Court) ใน ค.ศ. 2008 จำเลยถูกตัดสินว่ามีความผิดในการคุกคามผู้อื่น ทำให้ผู้อื่นหวาดกลัวหรือเจ็บปวด ตามมาตรา 4A[49] แห่ง Public Order Act 1986 ด้วยการนำเข้ารูปภาพของเหยื่อเข้าสู่เว็บไซต์พร้อมข้อความที่กล่าวหายืนยันว่าเหยื่อเคยถูกตัดสินว่ากระทำความผิดฐานก่อความรุนแรงในอดีต[50]

4.2.2.2.2 Fraud Act 2006

หากเกิดกรณีที่มีการได้รับหรือสูญเสียทางการเงินหรือทรัพย์สินอันเป็นผลเนื่องมาจากบัญชีสื่อสังคมออนไลน์ปลอม อาจถือว่าเป็นการกระทำความผิดตาม Fraud Act 2006 ในฐานความผิดเกี่ยวกับการครอบครอง สร้าง หรือจัดหาสิ่งที่ใช้สำหรับการกระทำความผิดฐานฉ้อโกงตามมาตรา 6 ถึงมาตรา 8 ได้ด้วย กล่าวคือ มาตรา 8 ได้บัญญัติขยายความคำว่า “สิ่ง” (Articles) ที่ใช้ในการกระทำความผิดฐานฉ้อโกงให้หมายรวมถึง โปรแกรมหรือข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์ด้วย[51] ดังนั้น ข้อมูลส่วนบุคคลที่ถูกนำไปใช้เพื่อการสวมรอยบนเครือข่ายอินเทอร์เน็ตด้วยการสร้างเว็บไซต์หรือบัญชีสื่อสังคมออนไลน์ปลอมย่อมกลายเป็นข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์ ผู้ใดที่ครอบครองหรือควบคุมข้อมูลดังกล่าวโดยมีเจตนาใช้ข้อมูลเพื่อการฉ้อโกงจึงมีความผิดตามมาตรา 6[52] ส่วนผู้ใดที่สร้าง ดัดแปลง จัดหา หรือเสนอให้มีการจัดหาข้อมูลเพื่อใช้กระทำการฉ้อโกง ไม่ว่าโดยรู้อยู่แล้วว่าข้อมูลนั้นถูกออกแบบหรือดัดแปลงเพื่อใช้กระทำการฉ้อโกง หรือเจตนาให้ข้อมูลนั้นถูกใช้ในการกระทำหรือสนับสนุนการกระทำการฉ้อโกงก็ตาม ย่อมถือเป็นความผิดตามมาตรา 7[53]

---

[49] PUBLIC ORDER ACT 1986 § 4A

[50] S v Crown Prosecution Service [2008] EWHC 438

[51] FRAUD ACT 2006 § 8

[52] FRAUD ACT 2006 § 6

[53] FRAUD ACT 2006 § 7

4.2.2.2.3 Computer Misuse Act 1990

มาตรา 2 แห่งพระราชบัญญัติดังกล่าวได้บัญญัติให้การเข้าถึงระบบคอมพิวเตอร์โดยมีเจตนาจะกระทำความผิดอื่นหรืออำนวยความสะดวกในการกระทำความผิดอื่นเป็นความผิดอาญา เนื่องจากมาตรา 2 มุ่งประสงค์จะยับยั้งมิให้ผู้กระทำผิดใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดอื่นต่อไป ด้วยเหตุนี้ การใช้ชื่อบัญชีหรือรหัสบัญชีของผู้อื่นโดยไม่ได้รับอนุญาตเพื่อจะเข้าถึงข้อมูลหรือโปรแกรม หรือเพื่อปรับเปลี่ยน ลบ คัดสำเนา หรือย้ายข้อมูลหรือโปรแกรม หรือสวมรอยเป็นบุคคลอื่นโดยการใช้จดหมายอิเล็กทรอนิกส์ โปรแกรมการสนทนาออนไลน์ หรือเว็บไซต์บริการอื่นๆ ในนามของผู้อื่น ย่อมเป็นความผิดตามมาตรานี้ทั้งสิ้น[54]

บทกำหนดโทษสำหรับการกระทำผิดข้างต้นปรากฏในมาตรา 2 (5) ซึ่งวางหลักไว้ว่า ผู้กระทำผิดตามมาตรา 2 นั้น กรณีต้องคำพิพากษาในประเทศอังกฤษและประเทศเวลส์จะต้องโทษจำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินค่าปรับสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ ส่วนกรณีต้องคำพิพากษาในประเทศสกอตแลนด์จะต้องโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินค่าปรับสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ หรือในกรณีเป็นความผิดอุกฉกรรจ์ต้องโทษจำคุกไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ[55]

4.2.2.2.4 Data Protection Act 1998

ตามมาตรา 55 แห่งพระราชบัญญัตินี้ได้กำหนดฐานความผิดเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลไว้ดังมีใจความสำคัญดังนี้ ผู้ใดโดยจงใจหรือประมาทเลินเล่อได้มาหรือเปิดเผยข้อมูลส่วนบุคคลหรือสารสนเทศที่มีข้อมูลส่วนบุคคล หรือจัดหาให้ได้มาซึ่งการเปิดเผยสารสนเทศที่มีข้อมูลส่วนบุคคลของผู้อื่น โดยปราศจากความยินยอมของผู้รักษาข้อมูล ผู้นั้นมีความผิด[56] จากบทบัญญัติมาตรานี้จะเห็นได้ว่าผู้ที่เปิดเผยข้อมูลส่วนบุคคลของผู้อื่นย่อมมีความรับผิดการใช้ชื่อหรือข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ได้รับอนุญาตในการสวมรอยเป็นบุคคลนั้นจึงถือว่าเป็นการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตตามมาตรานี้

---

[54] Wikipedia, "Computer Misuse Act 1990," [Online] Accessed: 5 February 2017. Updated: 29 March 2017. Available from: http://en.wikipedia.org/wiki/Computer_Misuse_Act_1990

[55] COMPUTER MISUSE ACT 1990 § 2 (5)

[56] DATA PROTECTION ACT 1998 § 55 (1) (3)

แต่อย่างไรก็ตาม มาตรา 55 ได้กำหนดข้อยกเว้นให้ไม่ต้องนำบทบัญญัติข้างต้นมาใช้บังคับไว้หลายกรณี ดังนี้

(1) กรณีที่การได้มา เปิดเผย หรือจัดหาข้อมูลส่วนบุคคลมีขึ้นเพื่อป้องกันหรือสืบสวนสอบสวนอาชญากรรม

(2) ผู้กระทำความผิดได้กระทำโดยมีเหตุอันควรเชื่อว่าตนมีสิทธิโดยชอบตามกฎหมายในการได้มาหรือเปิดเผยซึ่งข้อมูลหรือสารสนเทศ หรือจัดให้มีการเปิดเผยข้อมูลของผู้อื่น

(3) ผู้กระทำความผิดได้กระทำโดยมีเหตุอันควรเชื่อว่าตนจะได้รับความยินยอมจากผู้ควบคุมข้อมูล หากผู้ควบคุมข้อมูลทราบถึงการได้มา การเปิดเผย หรือการจัดหาข้อมูลนั้น

(4) ในกรณีที่มีการพิสูจน์ว่าการได้มา การเปิดเผย หรือการจัดหาข้อมูลส่วนบุคคลเป็นไปเพื่อประโยชน์สาธารณะ

ทั้งนี้ มาตรา 60 แห่งพระราชบัญญัตินี้ได้กำหนดหลักเกณฑ์ในการฟ้องคดีและบทลงโทษไว้ว่า ผู้ที่กระทำความผิดตามมาตรา 55 ต้องมีความรับผิดทางอาญาระวางโทษปรับในอัตราสูงสุดไม่เกินที่กฎหมายกำหนด สำหรับคำตัดสินลงโทษแบบรวบรัด (Summary Conviction) หรือโทษปรับ สำหรับคำตัดสินในคดีอาญาอุกฉกรรจ์ (Conviction on Indictment)

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเกิดจากการนำข้อมูลส่วนบุคคลที่ใช้ระบุตัวตนของบุคคลอื่นไปใช้โดยไม่ได้รับความยินยอม อันเป็นความผิดเกี่ยวกับการนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้โดยมิชอบ (Misuse of Private Information) ดังเช่นคดีของ Mathew Firsht ซึ่งถูกนำข้อมูลส่วนบุคคลไปสร้างโพรไฟล์บนเว็บไซต์เฟซบุ๊กโดยไม่ได้รับความยินยอม ข้อมูลส่วนบุคคลเหล่านั้นประกอบไปด้วยชื่อ รสนิยมทางเพศ สถานะความสัมพันธ์ วันเกิด รวมถึงมุมมองทางการเมืองและศาสนา ในคดีนี้ศาลได้ตัดสินว่า ข้อมูลส่วนบุคคลทั้งหมดเป็นข้อมูลที่เจ้าของคาดหวังว่าจะได้รับการคุ้มครองความเป็นส่วนตัวตามกฎหมาย การสร้างโพรไฟล์ปลอมจึงถือว่าเป็นการใช้ข้อมูลส่วนบุคคลโดยมิชอบ

4.2.2.2.5 ความผิดอื่นที่เกี่ยวข้อง

(1) ความผิดฐานหมิ่นประมาท (Defamation)

ในกรณีที่ผู้สวมรอยเขียนข้อความเท็จทำให้บุคคลอื่นหรือธุรกิจใด ๆ ได้รับความเสียหายด้านชื่อเสียงเกียรติคุณ หรือทำให้ได้รับความเกลียดชัง ถูกเยาะเย้ยถากถาง หรือถูกหลบเลี่ยงเสีย อาจถือได้ว่าเป็นความผิดฐานหมิ่นประมาท

(2) ความผิดฐานละเมิดลิขสิทธิ์ (Copyright Infringement)

ตามหลักสากลของกฎหมายลิขสิทธิ์ ผู้ถ่ายภาพย่อมเป็นเจ้าของลิขสิทธิ์ในภาพถ่ายนั้น หากผู้ใดทำซ้ำ ดัดแปลง หรือเผยแพร่ภาพถ่ายโดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์ย่อมมีความผิด ดังนั้น ผู้ใดกระทำการสวมรอยเป็นบุคคลอื่นโดยใช้รูปภาพอันมีลิขสิทธิ์ของผู้อื่นเป็นรูปภาพประกอบเว็บไซต์หรือโพรไฟล์ที่ทำการสวมรอยนั้น ถือว่าเป็นการละเมิดลิขสิทธิ์ได้

(3) กรณีการสวมรอยทางธุรกิจ (Impersonating a Business)

นอกจากการสวมรอยเป็นบุคคลธรรมดาที่มีตัวตนอยู่จริงอาจเป็นความผิดตามกฎหมายแล้ว การสวมรอยในเชิงธุรกิจก็ถือเป็นการกระทำที่ผิดกฎหมายเช่นกัน โดยมีความผิดที่สำคัญ 2 ฐาน ได้แก่ ความผิดฐานละเมิดเครื่องหมายการค้า (Trademarks) และความผิดฐานลวงขาย (Passing Off) กล่าวคือ ในกรณีที่ชื่อของบุคคลหรือธุรกิจได้รับการจดทะเบียนเครื่องหมายการค้าแล้วย่อมได้รับความคุ้มครองมิให้ผู้ใดมาล่วงละเมิดเครื่องหมายการค้านั้นได้ การที่บุคคลอื่นใช้เครื่องหมายการค้านั้นโดยมิชอบจึงเป็นความผิดฐานละเมิดเครื่องหมายการค้า ส่วนความผิดฐานลวงขายตามกฎหมายสหราชอาณาจักร หมายถึง การขายสินค้าหรือให้บริการหรือการดำเนินธุรกิจในลักษณะที่ทำให้ประชาชนทั่วไปหลงเชื่อว่าสินค้า บริการ หรือธุรกิจนั้นเป็นของตน หากมีการสวมรอยด้วยการนำชื่อหรือข้อมูลอื่นใดที่ทำให้ประชาชนหลงเชื่อเช่นว่านั้น เช่น ใช้ชื่อสินค้าเลียนแบบสินค้าของผู้อื่นย่อมเป็นการละเมิดที่ก่อให้เกิดความเสียหายต่อการดำเนินธุรกิจหรือผลประโยชน์ทางธุรกิจของเจ้าของสินค้าหรือบริการ[57]

เมื่อศึกษาถึงมาตรการทางกฎหมายที่สหราชอาณาจักรใช้ในการดำเนินคดีเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตแล้วจะเห็นได้ว่าสามารถนำกฎหมายที่มีอยู่แล้วมาปรับใช้กับการกระทำความผิดที่เกิดขึ้นได้เป็นรายกรณีไป แต่ทั้งนี้ เจ้าหน้าที่ตำรวจ พนักงานอัยการ และนักกฎหมายจำต้องพิจารณาว่าการกระทำความผิดนั้นเป็นไปตามหลักเกณฑ์ในคู่มือการฟ้องคดีที่เกี่ยวข้องกับการติดต่อสื่อสารที่ส่งผ่านทางสื่อสังคมออนไลน์ด้วยหรือไม่ ประการใด เพื่อจะได้นำหลักเกณฑ์ที่ระบุไว้ในคู่มือมาใช้เป็นแนวทางที่ชัดเจนในการอำนวยความยุติธรรมแก่ผู้เสียหายและสาธารณะอย่างมีประสิทธิภาพและเหมาะสมต่อไป

---

[57] ถาวร โพธิ์ทอง, พจนานุกรมกฎหมายและศัพท์ที่เกี่ยวข้อง อังกฤษ-ไทย, พิมพ์ครั้งที่ 3 (กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2550), หน้า 456.

4.3 ประเทศญี่ปุ่น

ในหัวข้อนี้ ผู้เขียนจะอธิบายถึงสภาพปัญหาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นที่เกิดขึ้นในประเทศญี่ปุ่น พร้อมมาตรการทางกฎหมายที่นำมาปรับใช้กับการกระทำความผิดที่เกิดขึ้น

4.3.1 ประเด็นปัญหาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในประเทศญี่ปุ่น

คดีเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในประเทศญี่ปุ่นที่น่าสนใจเกิดขึ้นใน ค.ศ. 2016 ศาลชั้นต้นประจำจังหวัดโอซาก้า (Osaka District Court) มีคำพิพากษาในคดีที่โจทก์ถูกสวมรอยในระบบออนไลน์ ในการฟ้องร้องคดีนี้ โจทก์อ้างในคำฟ้องว่าตนได้รับความเสียหายจากเหตุการณ์ที่เกิดขึ้น และยื่นคำร้องต่อศาลขอให้ศาลมีคำสั่งให้ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider: ISP) เปิดเผยข้อมูลของผู้กระทำความผิดให้โจทก์ทราบ อย่างไรก็ตาม แม้ศาลจะยกคำร้องของโจทก์ แต่ศาลได้ให้ความเห็นเกี่ยวกับสิทธิในตัวตนของบุคคลไว้เป็นครั้งแรกอย่างน่าสนใจ กล่าวคือ ศาลยอมรับว่าโจทก์มีสิทธิที่จะไม่ถูกสวมรอยบนเครือข่ายอินเทอร์เน็ต ผู้พิพากษาเจ้าของคดีให้คำจำกัดความของคำว่า “สิทธิในตัวตน” (Right to Identity) ไว้ว่า เป็นสิทธิในการคงไว้ซึ่งตัวตนเดิมเช่นเดียวกันกับตัวตนที่มีปฏิสัมพันธ์กับผู้อื่น หมายความว่า ทุกคนมีสิทธิที่จะแสดงตัวตนแบบเดียวกันกับทุก ๆ ความสัมพันธ์ที่เกิดขึ้น เป็นตัวตนของบุคคลนั้นอย่างแท้จริง ดังนั้นในกรณีที่ข้อความหรือประกาศใด ๆ ของผู้กระทำความผิดเป็นเหตุให้ผู้อื่นเข้าใจผิดคิดว่าเป็นข้อความของผู้ถูกสวมรอย และก่อให้เกิดความเจ็บปวดทางอารมณ์และจิตใจแก่ผู้ถูกสวมรอย ถือได้ว่าเป็นการล่วงละเมิดสิทธิในตัวตน ซึ่งเป็นสิทธิคนละอย่างกับสิทธิในชื่อเสียงเกียรติคุณ (Right to Reputation) และสิทธิในความเป็นส่วนตัว (Right to Privacy) นอกจากนี้ สิทธิในตัวตนนั้นมีที่มาจากสิทธิในชีวิตและการแสวงหาความสุข (Right to Life and the Pursuit of Happiness) ดังที่รัฐธรรมนูญให้การรับรอง[58]

นอกจากนี้ ยังมีคดีความเกี่ยวกับตัวตนปลอมในระบบออนไลน์อีกเป็นจำนวนมาก ยกตัวอย่างเช่น ใน ค.ศ. 1997 ศาลชั้นต้นประจำจังหวัดเกียวโต (Kyoto District Court) มีคำพิพากษาในคดีที่จำเลยปรับเปลี่ยนข้อมูลที่อยู่ของผู้อื่นเพื่อหลบหนีการค้นหาตัวจากการกระทำความผิดฐานฉ้อโกง

---

[58] The Japan Times, "Court Recognizes ‘Right to Identity’ for First Time in Online Impersonation Ruling," [Online] Accessed: 9 April 2017. Updated: 10 June 2016. Available from: http://www.japantimes.co.jp/news/2016/06/10/national/court-recognizes-right-to-identity-for-first-time-in-online-impersonation-ruling/#.WOpMEPmGPIU

ซึ่งจำเลยได้กระทำลงในนามของผู้อื่นบนระบบกระดานสนทนาออนไลน์แห่งหนึ่ง จำเลยถูกตัดสินให้มีความผิดฐานปลอมแปลง (Forgery) ต้องโทษจำคุก 2 ปี โดยรอลงอาญา 3 ปี พร้อมคุมประพฤติ

4.3.2 มาตรการทางกฎหมายที่เกี่ยวข้อง

ประเทศญี่ปุ่นเป็นประเทศที่ใช้ระบบกฎหมายแบบลายลักษณ์อักษรจึงมีการบัญญัติฐานความผิดลักษณะต่าง ๆ ไว้ทั้งในประมวลกฎหมายอาญาและพระราชบัญญัติอื่น แต่อย่างไรก็ตามประเทศญี่ปุ่นไม่มีกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไว้เป็นการเฉพาะดังเช่นสหรัฐอเมริกา ทั้งยังไม่มีกฎหมายเกี่ยวกับการโจรกรรมข้อมูลแสดงอัตลักษณ์ของบุคคล (Identity Theft) โดยตรงอีกด้วย แต่ศาลและผู้บังคับใช้กฎหมายในประเทศญี่ปุ่นได้นำบทบัญญัติของกฎหมายทั่วไปที่มีอยู่แล้วมาปรับใช้แก่เหตุการณ์ที่เกิดขึ้นเป็นรายกรณีไป โดยพิจารณาถึงลักษณะการกระทำความผิดที่เกิดขึ้นว่าตรงกับกฎหมายใดและนำกฎหมายนั้นมาปรับใช้

หากพิจารณาในแง่มุมของการโจรกรรมข้อมูลแสดงอัตลักษณ์ของบุคคล (Identity Theft) แล้วจะพบว่า การขโมยข้อมูลส่วนบุคคลของผู้อื่นนั้นเป็นความผิดแรกเริ่มที่สามารถนำไปสู่การสวมรอยเป็นผู้นั้นโดยอาศัยข้อมูลที่ได้มา การกระทำความผิดที่เกิดขึ้นภายใต้ชื่อหรือตัวตนของผู้ที่ถูกสวมรอยมีหลากหลายรูปแบบ ไม่ว่าจะเป็นการสร้างตัวตนปลอมบนระบบออนไลน์ เช่น สร้างบัญชีผู้ใช้งานเว็บไซต์เครือข่ายสังคมในนามของบุคคลอื่น หรือการใช้หลักฐานอ้างอิงของบุคคลอื่นโดยมิชอบด้วยกฎหมาย เช่น ใช้ชื่อผู้ใช้งาน (Username) หรือรหัสผ่าน (Password) ของบุคคลอื่นเพื่อส่งจดหมายอิเล็กทรอนิกส์ในนามของบุคคลนั้น แม้ว่าประเทศญี่ปุ่นจะไม่มีกฎหมายเกี่ยวกับการกระทำความผิดในลักษณะดังกล่าวเป็นการเฉพาะ แต่สามารถนำบทบัญญัติที่เกี่ยวข้องอื่น ๆ มาปรับใช้ได้ดังนี้

4.3.2.1 ประมวลกฎหมายอาญา

บทบัญญัติตามประมวลกฎหมายอาญา (Penal Code Act No.45 of 1907) ของประเทศญี่ปุ่นที่อาจนำมาพิจารณาปรับใช้แก่กรณีของการสร้างตัวตนปลอมเพื่อใช้ดำเนินการอย่างใดอย่างหนึ่งให้ได้มาซึ่งทรัพย์สินโดยมิชอบด้วยกฎหมาย หรือกรณีการปลอมแปลงข้อมูลที่ส่งผลกระทบทางด้านกฎหมายนั้น ได้แก่ บทบัญญัติในความผิดฐานฉ้อโกงทางคอมพิวเตอร์ และความผิดฐานปลอมแปลงเอกสารทางคอมพิวเตอร์

4.3.2.1.1 ความผิดฐานฉ้อโกงทางคอมพิวเตอร์ (Computer-related Fraud)

ประมวลกฎหมายอาญาญี่ปุ่นบัญญัติให้การฉ้อโกงทางคอมพิวเตอร์เป็นความผิดอาญาไว้ในหมวด 37 ว่าด้วย การกระทำความผิดฐานฉ้อโกงและกรรโชกทรัพย์ (Crimes of Fraud and Extortion) โดยมีบทบัญญัติที่เกี่ยวข้อง 2 มาตรา ดังนี้

มาตรา 246 ความผิดฐานฉ้อโกง (Fraud)[59]

(1) ผู้ใดฉ้อโกงทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกพร้อมทำงานไม่เกิน 10 ปี

(2) โทษเดียวกันนี้ให้ลงแก่ผู้ที่ได้มาหรือก่อให้บุคคลอื่นได้มาซึ่งผลประโยชน์โดยวิธีการที่ต้องห้ามตามวรรคก่อน

มาตรา 246-2 ความผิดฐานฉ้อโกงทางคอมพิวเตอร์ (Computer Fraud)[60]

นอกเหนือจากที่บัญญัติไว้ในมาตรา 246 ผู้ใดได้มาหรือก่อให้บุคคลอื่นได้มาซึ่งผลประโยชน์โดยการสร้างระเบียนอิเล็กทรอนิกส์ที่เกี่ยวกับการได้มา สูญเสีย หรือแก้ไขเปลี่ยนแปลงสิทธิในทรัพย์สินปลอม ด้วยการป้อนข้อมูลปลอมหรือป้อนคำสั่งโดยไม่ได้รับอนุญาตไปยังคอมพิวเตอร์ที่ใช้ในธุรกิจของผู้อื่น หรือใช้ระเบียนอิเล็กทรอนิกส์ที่เกี่ยวกับการได้มา สูญเสีย หรือแก้ไขเปลี่ยนแปลงสิทธิในทรัพย์สินปลอมเพื่อจัดการธุรกิจของผู้อื่น ต้องระวางถูกลงโทษจำคุกพร้อมใช้แรงงานไม่เกิน 10 ปี

4.3.2.1.2 ความผิดฐานปลอมแปลงเอกสารทางคอมพิวเตอร์ (Computer-related Forgery)

ประมวลกฎหมายอาญาญี่ปุ่นบัญญัติให้การปลอมแปลงเอกสารทางคอมพิวเตอร์เป็นความผิดอาญาไว้ในหมวด 17 ว่าด้วย การกระทำความผิดฐานปลอมเอกสาร (Crimes of Counterfeiting of Documents) โดยมีบทบัญญัติที่เกี่ยวข้อง 2 มาตรา ดังนี้

มาตรา 161 ความผิดฐานใช้เอกสารส่วนบุคคลปลอม (Uttering of Counterfeiting Private Documents)[61]

---

[59] PENAL CODE (ACT NO.45 OF 1907) ARTICLE 246

[60] PENAL CODE (ACT NO.45 OF 1907) ARTICLE 246-2

[61] PENAL CODE (ACT NO.45 OF 1907) ARTICLE 161

(1) ผู้ใดใช้เอกสารหรือภาพวาดปลอมตามสองมาตราก่อนหน้านี้[62] ต้องระวางโทษเช่นเดียวกับผู้ที่ปลอมหรือแปลงเอกสารหรือภาพวาดหรือกรอกข้อมูลเท็จ

(2) ผู้ใดพยายามกระทำความผิดตามที่บัญญัติไว้ในวรรคก่อน ต้องระวางโทษ

มาตรา 161-2 ความผิดฐานสร้างระเบียนอิเล็กทรอนิกส์โดยปราศจากอำนาจ (Unauthorized Creation of Electromagnetic Records)[63]

(1) ผู้ใดโดยเจตนาก่อให้มีการบริหารจัดการกิจการของผู้อื่นโดยไม่สมควรสร้างระเบียนอิเล็กทรอนิกส์โดยไม่มีอำนาจและไม่ชอบด้วยกฎหมาย อันเป็นระเบียนสำหรับการบริหารจัดการที่ไม่สมควรนั้นและเป็นระเบียนที่เกี่ยวข้องกับสิทธิ หน้าที่ หรือการรับรองข้อเท็จจริง ต้องระวางโทษจำคุกพร้อมทำงานไม่เกิน 5 ปี หรือปรับไม่เกิน 500,000 เยน

(2) ในกรณีที่มีการการกระทำความผิดตามวรรคก่อนกับระเบียนอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นโดยหน่วยงานรัฐหรือเจ้าหน้าที่รัฐ ผู้กระทำผิดต้องระวางโทษจำคุกพร้อมทำงานไม่เกิน 10 ปี หรือปรับไม่เกิน 1,000,000 เยน

(3) ผู้ใดโดยมีเจตนาดังที่บัญญัติไว้ในวรรคแรกนำระเบียนอิเล็กทรอนิกส์ซึ่งสร้างขึ้นโดยไม่มีอำนาจและเกี่ยวข้องกับสิทธิ หน้าที่ หรือการรับรองข้อเท็จจริง ไปใช้เพื่อบริหารจัดการกิจการของผู้อื่น ต้องระวางโทษจำคุกในอัตราโทษเดียวกันกับผู้ที่สร้างระเบียนอิเล็กทรอนิกส์เช่นว่านั้น

---

[62] บทบัญญัติดังกล่าว ได้แก่ มาตรา 159 และมาตรา 160 ดังนี้

มาตรา 159 การปลอมเอกสารส่วนบุคคล

(1) ผู้ใดใช้ตราประทับหรือลายมือชื่อของผู้อื่นหรือใช้เอกสารหรือภาพวาดที่เกี่ยวกับสิทธิ หน้าที่ หรือการรับรองข้อเท็จจริง หรือใช้ตราประทับหรือลายมือชื่อของผู้อื่นเพื่อปลอมเอกสารหรือภาพวาดเช่นนั้น ต้องระวางโทษจำคุกพร้อมทำงานตั้งแต่ 3 เดือนขึ้นไป แต่ไม่เกิน 5 ปี

(2) ผู้ใดแปลงเอกสารหรือภาพวาดที่เกี่ยวข้องกับสิทธิ หน้าที่ หรือการรับรองข้อเท็จจริง ซึ่งมีการประทับตราหรือลงลายมือชื่อของผู้อื่น ต้องระวางโทษเดียวกันกับวรรคแรก

(3) นอกจากกรณีที่บัญญัติไว้ในทั้งสองวรรคข้างต้น ผู้ใดปลอมหรือแปลงเอกสารหรือภาพวาดที่เกี่ยวข้องกับสิทธิ หน้าที่ หรือการรับรองข้อเท็จจริง ต้องระวางโทษจำคุกพร้อมทำงานไม่เกิน 1 ปี หรือปรับไม่เกิน 100,000 เยน

มาตรา 160 การทำหนังสือรับรองทางการแพทย์เท็จ

เมื่อแพทย์ทำหนังสือรับรองทางการแพทย์ รายงานการชันสูตรศพ หรือหนังสือรับรองการตายเป็นเท็จ เสนอต่อหน่วยงานของรัฐ ต้องระวางโทษจำคุกโดยไม่ต้องทำงานไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 เยน

[63] PENAL CODE (ACT NO.45 OF 1907) ARTICLE 161-2

(4) ผู้ใดพยายามกระทำความผิดตามที่บัญญัติไว้ในวรรคก่อนหน้า ต้องระวางโทษ

4.3.2.2 พระราชบัญญัติที่มีโทษทางอาญาอื่น ๆ

นอกเหนือจากบทบัญญัติความรับผิดตามประมวลกฎหมายอาญาแล้ว การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในประเทศญี่ปุ่นยังอาจเป็นความผิดตามกฎหมายอื่นที่เกี่ยวข้องได้อีกหลายฉบับ ดังนี้

4.3.2.2.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Act on the Protection of Personal Information: APPI)

ตามมาตรา 2 แห่งพระราชบัญญัติดังกล่าวได้กำหนดคำนิยามของคำว่า “ข้อมูลส่วนบุคคล” (Personal Information) ไว้ว่าหมายถึง ข้อมูลเกี่ยวกับบุคคลที่มีชีวิตอยู่ ซึ่งสามารถใช้ระบุตัวบุคคลเป็นการเฉพาะเจาะจงได้ โดยอาศัยชื่อ วันเกิด หรือการอธิบายอื่นที่มีข้อมูลเหล่านั้น (ประกอบด้วยข้อมูลดังกล่าวซึ่งเอื้อต่อการอ้างอิงถึงข้อมูลอื่น และสามารถใช้ระบุตัวบุคคลเป็นการเฉพาะเจาะจงได้)[64]

ทั้งนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่นยังแบ่งออกเป็นหลายฉบับ ขึ้นอยู่กับกรณีว่าข้อมูลส่วนบุคคลนั้นอยู่ในความครอบครองดูแลของหน่วยงานใด หากข้อมูลส่วนบุคคลอยู่ในความดูแลของหน่วยงานทางปกครอง กรณีต้องอยู่ภายใต้พระราชบัญญัติฉบับที่ 58 ประกาศใช้ ณ วันที่ 30 พฤษภาคม ค.ศ. 2003 ส่วนข้อมูลส่วนบุคคลที่อยู่ในความดูแลของหน่วยงานทางปกครองที่เป็นอิสระหรือองค์กรอื่น ๆ ต้องอยู่ภายใต้พระราชบัญญัติฉบับที่ 59 ซึ่งประกาศใช้ในปี ค.ศ. 2003

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับที่ใช้กับหน่วยงานทางปกครองได้บัญญัติข้อห้ามมิให้มีการนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้เพื่อหาผลประโยชน์ไว้ในมาตรา 53 และ 54 ดังมีใจความว่า ผู้ใดเป็นลูกจ้างหรืออดีตลูกจ้างของหน่วยงานรัฐ หรือบุคคลหรือผู้ประกอบธุรกิจที่ได้รับมอบหมายหน้าที่จากหน่วยงานรัฐให้ดูแลข้อมูลส่วนบุคคล จัดหาข้อมูลส่วนบุคคลที่รักษาไว้เนื่องจากได้รับความนับถือตามหน้าที่การงานนั้นให้แก่บุคคลอื่น หรือจัดสรรข้อมูลนั้น

[64] ACT ON THE PROTECTION OF PERSONAL INFORMATION (ACT NO. 57 OF 2013) ARTICLE 2 (1)

เพื่อก่อให้เกิดประโยชน์ที่มิชอบด้วยกฎหมายแก่ตนเองหรือบุคคลที่สาม ต้องระวางโทษจำคุกพร้อมทำงานไม่เกิน 1 ปี หรือปรับไม่เกิน 500,000 เยน

ส่วนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับที่บังคับใช้กับองค์กรอิสระและหน่วยงานอื่น ๆ นั้นมีบทบัญญัติคุ้มครองข้อมูลส่วนบุคคลไว้ในมาตรา 51 ประกอบมาตรา 53 โดยมีสาระสำคัญของลักษณะการกระทำผิดและอัตราโทษเช่นเดียวกับมาตรา 53 แห่งพระราชบัญญัติฉบับที่ 58 ค.ศ. 2003 ดังได้กล่าวมาแล้วข้างต้น

4.3.2.2.2 พระราชบัญญัติป้องกันการเข้าถึงคอมพิวเตอร์โดยไม่มีอำนาจ (Act on the Prohibition of Unauthorized Computer Access)[65]

การเข้าถึงระบบฐานข้อมูลโดยผิดกฎหมาย (Hacking) เป็นขั้นตอนหนึ่งที่อาจเกิดขึ้นเพื่อสวมรอยเป็นบุคคลอื่นด้วยการอาศัยชื่อบัญชีผู้ใช้งานและรหัสผ่านของบุคคลนั้นโดยไม่มีอำนาจ การเข้าถึงระบบเช่นว่านี้เป็นความผิดตามมาตรา 4 แห่งพระราชบัญญัติป้องกันการเข้าถึงคอมพิวเตอร์โดยไม่มีอำนาจของประเทศญี่ปุ่น[66] ซึ่งแบ่งลักษณะการกระทำความผิดออกเป็น 3 ลักษณะ ได้แก่ (1) การเข้าถึงคอมพิวเตอร์ผ่านทางเครือข่ายสื่อสารทางไกลโดยปราศจากอำนาจโดยใช้ชื่อบัญชีผู้ใช้งานและรหัสผ่านของผู้อื่น (2) การเข้าถึงคอมพิวเตอร์ผ่านเครือข่ายสื่อสารทางไกลโดยปราศจากอำนาจ โดยใช้ข้อมูลหรือคำสั่งที่สามารถหลบเลี่ยงการยับยั้งการเข้าถึงโดยฟังก์ชั่นควบคุมการเข้าถึง และ (3) การเข้าถึงคอมพิวเตอร์ผ่านเครือข่ายสื่อสารทางไกลโดยปราศจากอำนาจ โดยการโจมตีช่องว่างด้านความปลอดภัย ผู้ที่กระทำความผิดดังกล่าวข้างต้นต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 200,000 เยน ส่วนผู้เสียหายสามารถดำเนินคดีทางแพ่งเรียกร้องค่าเสียหายได้

อย่างไรก็ตาม แม้ว่าในภาพรวมนั้นดูเหมือนว่าประเทศญี่ปุ่นจะมีกฎหมายที่นำมาปรับใช้เพื่อปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอยู่แล้วก็ตาม แต่พบว่ายังปรากฏข้อบกพร่องบางประการในการดำเนินการทางกฎหมาย กล่าวคือ ประการแรก เมื่อประชาชนต้องเผชิญหน้ากับความเสียหายที่เกิดขึ้นจากอาชญากรรมในโลกไซเบอร์และรายงานต่อเจ้าหน้าที่ตำรวจ เจ้าหน้าที่ตำรวจเพียงแต่ให้คำปรึกษาและจดบันทึกรายงานเก็บไว้เท่านั้น ไม่มีการเผยแพร่ให้

---

[65] Japan Ministry of Justice, "Act on Prohibition of Unauthorized Computer Access," [Online] Accessed: 21 June 2017. Available from: http://www.japaneselawtranslation.go.jp/law/detail/?id=2250&vm=04&re=02

[66] ACT ON PROHIBITION OF UNAUTHORIZED COMPUTER ACCESS ARTICLE 4

สาธารณชนทั่วไปรับทราบ ประการต่อมา ผู้เสียหายต้องดำเนินการผ่านช่องทางทางการที่รัฐจัดไว้ให้ เช่น การแจ้งความร้องทุกข์ต่อเจ้าหน้าที่ตำรวจท้องถิ่น และการสวมรอยเป็นบุคคลอื่นเช่นนี้มักไม่ได้รับความสนใจมากนัก เว้นแต่เป็นกรณีที่เป็นอันตรายต่อผู้เสียหายอย่างชัดแจ้ง ประการสุดท้าย กระบวนการสืบสวนสอบสวนคดีที่เกิดขึ้นยังคงมีความยุ่งยากซับซ้อน โดยเฉพาะในคดีที่คาบเกี่ยวพื้นที่กระทำความผิดหลายประเทศ ประชาชนในประเทศญี่ปุ่นจำนวนมากไม่ตระหนักถึงคุณค่าของข้อมูลส่วนบุคคล รวมถึงภัยอันตรายอันเกิดจากการใช้ข้อมูลเพื่อการหลอกลวง แม้ว่าจะตรวจพบพยานหลักฐานที่ชัดแจ้ง เช่น ค้นพบหน้าโพรไฟล์ปลอมบนเว็บไซต์เครือข่ายสังคม กลับเป็นการยากยิ่งที่จะขอให้ผู้ดูแลเว็บไซต์นำข้อมูลที่ไม่ชอบออกจากหน้าเว็บ รวมถึงการขอข้อมูลสำคัญสำหรับการสืบสวนสอบสวนคดีจากผู้ดูแลเว็บไซต์ เช่น เลขที่อยู่ไอพี (IP Address) หรือที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้กระทำความผิด ก็มีความยากลำบากเช่นกัน[67]

4.4 สาธารณรัฐเกาหลี

ในหัวข้อนี้ ผู้เขียนจะอธิบายถึงสภาพปัญหาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นที่เกิดขึ้นในสาธารณรัฐเกาหลี รวมถึงมาตรการทางกฎหมายที่เกี่ยวข้องกับการกระทำความผิด

4.4.1 ประเด็นปัญหาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในสาธารณรัฐเกาหลี

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตที่ปรากฏเป็นข่าวในสาธารณรัฐเกาหลีมักจะเป็นการสวมรอยเป็นบุคคลที่มีชื่อเสียงในแวดวงต่าง ๆ เช่น ดารานักร้อง นักการเมือง เป็นต้น โดยผู้กระทำความผิดจะสร้างบัญชีเครือข่ายสังคมออนไลน์ปลอมในนามของบุคคลที่มีชื่อเสียง ประกอบไปด้วยข้อมูลส่วนบุคคลและรูปภาพที่ทำให้ผู้ใช้งานอินเทอร์เน็ตทั่วไปหลงเชื่อว่าบัญชีเครือข่ายสังคมออนไลน์นั้นเป็นของบุคคลที่มีชื่อเสียงตัวจริง จากนั้นผู้กระทำความผิดจะใช้ความน่าเชื่อถือในตัวตนของผู้ถูกสวมรอยไปแสวงหาผลประโยชน์หรือทำให้ผู้อื่นเสียหาย ตัวอย่างเช่น การแอบอ้างว่าเป็นดาราพิธีกรชื่อดังและลงประกาศโฆษณาบนเว็บไซต์เฟซบุ๊ก ให้สัญญาว่าจะให้คูปองอิเล็กทรอนิกส์และของรางวัลแก่ผู้ที่ร่วมแสดงความคิดเห็นต่อประกาศนั้น รวมทั้งลงรูปภาพของผู้ถูกสวมรอยและภริยาเพื่อใช้เป็นเครื่องพิสูจน์ว่าบัญชีเฟซบุ๊กดังกล่าวเป็นของจริงอีกด้วย หรือกรณีที่

---

[67] Robinson, N. *et al.*, Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime : Final Report, p. 372.

ผู้กระทำความผิดใช้ชื่อของผู้ถูกสวมรอยกระทำการกรรโชกทรัพย์และส่งข้อความรังควานเชิงเพศผ่านทางบริการสนทนาด้วยข้อความ[68] เป็นต้น

อนึ่ง สาธารณรัฐเกาหลีมีระบบหมายเลขประจำตัวผู้อยู่อาศัยเรียกว่า Resident Registration Number หรือ RRN ซึ่งเป็นหมายเลขจำนวน 13 หลักเช่นเดียวกันกับหมายเลขประจำตัวประชาชนของประเทศอื่น ใช้สำหรับการระบุตัวประชาชนชาวเกาหลีใต้ในการทำธุรกรรมส่วนตัวต่าง ๆ เช่น ธุรกรรมทางการเงิน การจ้างงาน รวมทั้งใช้ในการยืนยันตัวตนในระบบออนไลน์อีกด้วย ดังนั้น เว็บไซต์ในสาธารณรัฐเกาหลีจำนวนมากจึงกำหนดให้ผู้สมัครขอใช้บริการต้องลงทะเบียนยืนยันตัวตนก่อนจึงจะใช้บริการได้ ข้อกำหนดเช่นนี้ทำให้บัญชีผู้ใช้งานเว็บไซต์กลายเป็นตัวตนในระบบออนไลน์ที่มีความเฉพาะเจาะจง แต่เนื่องจากหมายเลขประจำตัวผู้อยู่อาศัยดังกล่าวอาจปรากฏในฐานข้อมูลบนเครือข่ายอินเทอร์เน็ตและสามารถค้นหาได้โดยง่าย จึงมีแนวโน้มที่จะเกิดการนำหมายเลขประจำตัวของบุคคลอื่นไปใช้ประโยชน์โดยไม่ได้รับอนุญาต การขโมยหมายเลขประจำตัวเช่นนี้กลายเป็นปัญหาสังคมของสาธารณรัฐเกาหลีที่นับวันจะยิ่งรุนแรงมากขึ้น และนำไปสู่การกระทำความผิดอื่นมากมาย เช่น การฉ้อโกงทางการเงิน การสวมรอยเป็นบุคคลอื่น การละเมิดสิทธิส่วนบุคคล และอาชญากรรมอื่น ๆ เป็นต้น[69]

คดีของอดีตประธานาธิบดีโน มู-ฮย็อน (Roh Moo-hyun) ของสาธารณรัฐเกาหลีเป็นตัวอย่างอันชัดเจนที่แสดงให้เห็นถึงการนำหมายเลขประจำตัวของบุคคลอื่นไปใช้ประโยชน์บนระบบออนไลน์ดังที่กล่าวมาแล้วข้างต้นว่าเว็บไซต์ในสาธารณรัฐเกาหลีกำหนดให้ผู้ที่ต้องการใช้บริการต้องลงทะเบียนด้วยการยืนยันหมายเลขประจำตัวของตนเอง ด้วยเหตุนี้จึงมีผู้ใช้งานอินเทอร์เน็ตจำนวนมากได้นำหมายเลขประจำตัวของโน มู-ฮย็อน ไปใช้เพื่อยืนยันตัวตนในการสมัครใช้บริการเว็บไซต์ลามกเว็บไซต์บันเทิง และเว็บไซต์เกมออนไลน์[70]

---

[68] K. Zertuche, "Haha to Take Action against Impersonator," [Online] Accessed: 30 March 2017. Updated: 20 December 2015. Available from: https://www.soompi.com/2015/12/20/haha-to-take-action-against-impersonator/

[69] Motohiro Tsuchiya, "Cyber Security in East Asia Japan and the 2009 Attacks on South Korea and the United States," in Cybersecurity Public Sector Treats and Responses, ed. Kim J. Andreasson (United States of America: CRC Press, 2012), p. 72.

[70] Chosunilbo & Chosun.com, "President, Pm Fall Victim to Online Id Theft," [Online] Accessed: 7 April 2017. Updated: 27 June 2006. Available from: http://english.chosun.com/site/data/html_dir/2006/06/27/2006062761016.html

เมื่อพิจารณาเหตุการณ์ที่เกิดขึ้นข้างต้นแล้วจะเห็นว่า ข้อมูลส่วนบุคคลที่อยู่บนเครือข่ายอินเทอร์เน็ตอาจถูกนำไปใช้ในทางมิชอบได้โดยง่าย ไม่ว่าจะเป็นหมายเลขประจำตัวผู้อยู่อาศัย (Resident Registration Number) ชื่อ รูปภาพ วันเกิด หรือข้อมูลส่วนบุคคลอื่นใดที่สามารถระบุตัวบุคคลเป็นการเฉพาะเจาะจงได้ การนำข้อมูลเหล่านี้ไปใช้ประโยชน์ในการสวมรอยเป็นเจ้าของข้อมูลโดยมีวัตถุประสงค์ที่ไม่ชอบด้วยกฎหมาย เช่น ฉ้อโกง คุกคาม หรือทำให้เสื่อมเสียชื่อเสียง ย่อมก่อให้เกิดความเสียหายแก่บุคคลที่ถูกสวมรอยและประชาชนโดยทั่วไปที่หลงเชื่อ ความเสียหายที่เกิดขึ้นแบ่งออกเป็น 3 ด้าน ได้แก่ (1) ความเสียหายด้านชื่อเสียง (2) ความเสียหายด้านทรัพย์สินหรือการเงิน (3) ความเสียหายด้านความเป็นส่วนตัว

4.4.2 มาตรการทางกฎหมาย

เนื่องด้วยในปัจจุบันสาธารณรัฐเกาหลีไม่มีมาตรการทางกฎหมายเป็นการเฉพาะสำหรับลงโทษผู้ที่สวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ดังนั้นบรรดาผู้เสียหายที่ถูกนำข้อมูลส่วนบุคคลไปแอบอ้างจึงใช้วิธีการแจ้งเตือนผ่านทางสื่อสังคมออนไลน์เป็นการเบื้องต้น โดยการเขียนข้อความชี้แจงว่าตนถูกสวมรอย บัญชีผู้ใช้งานปลอมนั้นไม่ใช่ของตนและตนไม่มีส่วนเกี่ยวข้องกับการกระทำความผิดที่เกิดขึ้นต่อเนื่องจากการสวมรอยแต่อย่างใด อย่างไรก็ตาม การเขียนข้อความชี้แจงให้ประชาชนทั่วไปทราบข้อเท็จจริงและขอร้องให้ผู้กระทำความผิดหยุดการกระทำเสียมักไม่ประสบความสำเร็จเท่าไรนัก ผู้ถูกสวมรอยหลายรายจึงต้องเขียนข้อความในเชิงแจ้งเตือนว่าจะดำเนินการตามกฎหมาย หากผู้กระทำความผิดยังคงกระทำการสวมรอยต่อไป

แม้ว่าสาธารณรัฐเกาหลีจะไม่มีกฎหมายที่กำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดทางอาญาไว้เป็นการเฉพาะก็ตาม แต่ผู้เสียหายจากการสวมรอยเช่นนี้อาจนำกฎหมายอื่นที่เกี่ยวข้องมาปรับใช้ได้เป็นกรณีไป โดยพิจารณาจากลักษณะของการกระทำความผิดและความเสียหายที่เกิดขึ้น กฎหมายที่นำมาปรับใช้กับการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในสาธารณรัฐเกาหลีมีดังต่อไปนี้

4.4.2.1 ประมวลกฎหมายอาญา

หากผู้กระทำความผิดแอบอ้างสวมรอยเป็นบุคคลอื่นเพื่อกระทำการหลอกลวงฉ้อโกงด้วยวิธีการทางคอมพิวเตอร์ ผู้นั้นมีความผิดฐานฉ้อโกงทางคอมพิวเตอร์ (Fraud by Use of

Computer, etc.) ตามมาตรา 347-2 หมวด 39 ความผิดฐานฉ้อโกงและกรรโชกทรัพย์ แห่งประมวลกฎหมายอาญาของสาธารณรัฐเกาหลี ดังนี้

มาตรา 347-2[71] บัญญัติว่า ผู้ใดได้มาซึ่งผลประโยชน์ทางทรัพย์สินหรือทำให้บุคคลที่สามได้ไปซึ่งผลประโยชน์ทางทรัพย์สิน โดยการสร้างข้อมูลที่เป็นการนำเข้าซึ่งข้อมูลสารสนเทศปลอมหรือคำสั่งที่ไม่เหมาะสม หรือนำเข้าหรือปรับเปลี่ยนข้อมูลโดยปราศจากอำนาจ ในหน่วยประมวลผลข้อมูล เช่น คอมพิวเตอร์ หรืออื่น ๆ ต้องระวางโทษจำคุกไม่เกิน 10 ปี หรือปรับไม่เกิน 20 ล้านวอน

4.4.2.2 พระราชบัญญัติที่มีโทษทางอาญาอื่น ๆ

นอกเหนือจากบทบัญญัติความรับผิดตามประมวลกฎหมายอาญาแล้ว การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในสาธารณรัฐเกาหลียังอาจเป็นความผิดตามกฎหมายอื่นที่เกี่ยวข้องได้อีกหลายฉบับ ดังนี้

4.4.2.2.1 พระราชบัญญัติว่าด้วยการจดทะเบียนหมายเลขประจำตัวผู้อยู่อาศัย (Resident Registration Act)

มาตรา 37 แห่งพระราชบัญญัติว่าด้วยการจดทะเบียนหมายเลขประจำตัวผู้อยู่อาศัย ได้กำหนดระวางโทษจำคุกพร้อมใช้แรงงาน (Imprisonment with Labor) เป็นเวลาไม่เกิน 3 ปี หรือปรับไม่เกิน 10 ล้านวอน แก่ผู้ที่กระทำการอันไม่ชอบด้วยกฎหมายดังที่ระบุไว้ในอนุมาตราต่าง ๆ[72] การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการนำข้อมูลส่วนบุคคลของบุคคลอื่นไปใช้โดยไม่ได้รับอนุญาต หากผู้กระทำความผิดนำหมายเลขประจำตัวผู้อยู่อาศัย (Resident Registration Number) ของบุคคลอื่นไปใช้เพื่อสวมรอยเป็นบุคคลนั้น จึงอาจเป็นความผิดตามมาตรา 37 (9) สำหรับกรณีที่เปิดเผยข้อมูลหมายเลขประจำตัวผู้อยู่อาศัย (Resident Registration Number) เพื่อวัตถุประสงค์ในการแสวงหากำไร หรือมาตรา 37 (10) สำหรับกรณีที่ใช้หมายเลขประจำตัวผู้อยู่อาศัย (Resident Registration Number) ของบุคคลที่สามโดยไม่สมควร เว้นแต่ผู้เสียหายเป็นผู้สืบสายเลือดโดยตรง หรือเป็นคู่สมรส หรือเป็นญาติที่อาศัยอยู่ด้วยกัน หรือเป็นคู่สมรสของญาติที่อาศัยอยู่ด้วยกันของผู้กระทำความผิด กรณีเช่นนี้อาจไม่มีการดำเนินคดีหากขัดต่อความประสงค์ของผู้เสียหาย

---

[71] CRIMINAL ACT ARTICLE 374-2

[72] RESIDENT REGISTRATION ACT ARTICLE 37

4.4.2.2.2 พระราชบัญญัติคุ้มครองข้อมูลและการใช้งานเครือข่ายสารสนเทศและการสื่อสาร (Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.) หรือ IT Network Act

พระราชบัญญัติฉบับนี้บังคับใช้กับอุตสาหกรรมด้านเทคโนโลยีสารสนเทศเป็นหลัก โดยมีเจตนารมณ์ส่งเสริมการใช้เครือข่ายข้อมูลสารสนเทศและการสื่อสารเพื่อคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้งานระบบข้อมูลสารสนเทศและการสื่อสารนั้น รวมทั้งเพื่อสร้างสภาพแวดล้อมที่ปลอดภัยและแข็งแรงให้แก่เครือข่ายข้อมูลสารสนเทศและการสื่อสาร เพื่อยกระดับคุณภาพชีวิตของพลเมืองและทำให้สวัสดิการสำหรับประชาชนดีมากยิ่งขึ้น

ความเสียหายที่เกิดขึ้นจากการถูกสวมรอยบนเครือข่ายอินเทอร์เน็ตอาจส่งผลกระทบต่อความน่าเชื่อถือและชื่อเสียงเกียรติคุณของบุคคลที่ถูกสวมรอย มาตรา 70 แห่งพระราชบัญญัติคุ้มครองข้อมูลและการใช้งานเครือข่ายสารสนเทศและการสื่อสาร เป็นบทบัญญัติที่กำหนดให้การหมิ่นประมาทผ่านทางเครือข่ายสารสนเทศและการสื่อสารเป็นความผิดอาญาและกำหนดโทษไว้ ดังนี้

มาตรา 70[73]

(1) ผู้ใดทำให้ผู้อื่นเสื่อมเสียชื่อเสียงด้วยการยืนยันข้อเท็จจริงอย่างเปิดเผยผ่านทางเครือข่ายสารสนเทศและการสื่อสาร โดยมีวัตถุประสงค์เพื่อกล่าวว่าร้ายผู้นั้น ต้องระวางโทษจำคุกธรรมดาหรือจำคุกพร้อมใช้แรงงาน (Imprisonment with or without Prison Labor) ไม่เกิน 3 ปี หรือปรับไม่เกิน 30 ล้านวอน

(2) ผู้ใดทำให้ผู้อื่นเสื่อมเสียชื่อเสียงด้วยการยืนยันข้อเท็จจริงที่เป็นความเท็จอย่างเปิดเผยผ่านทางเครือข่ายสารสนเทศและการสื่อสาร โดยมีวัตถุประสงค์เพื่อกล่าวว่าร้ายผู้นั้น ต้องระวางโทษจำคุกพร้อมใช้แรงงาน (Imprisonment with Prison Labor) ไม่เกิน 7 ปี หรือรอโดยมีข้อจำกัด (Suspension of Qualification) ไม่เกิน 10 ปี หรือปรับไม่เกิน 50 ล้านวอน

(3) ต้องไม่มีการดำเนินคดีการกระทำความผิดตามวรรค 1 และวรรค 2 ที่ขัดต่อความประสงค์ของผู้เสียหาย

---

[73] ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND DATA PROTECTION, ETC. ARTICLE 70

4.4.2.2.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection Act หรือ PIPA)

พระราชบัญญัตินี้เป็นกฎหมายที่ใช้ควบคุมการรวบรวมและการใช้ข้อมูลส่วนบุคคล โดยปรับใช้กับทุกภาคส่วนไม่ว่าจะเป็นหน่วยงานของรัฐหรือองค์กรเอกชนซึ่งเกี่ยวข้องกับการรวบรวม ดำเนินการ และใช้ข้อมูลส่วนบุคคล ทั้งนี้ไม่ได้จำกัดขอบเขตของกฎหมายไว้เพียงภายในสาธารณรัฐเกาหลีเท่านั้น แต่ยังบังคับใช้ครอบคลุมไปถึงองค์กรเอกชนต่างประเทศได้อีกด้วย กฎหมายฉบับนี้ได้กำหนดคำนิยามของคำว่าข้อมูลส่วนบุคคลไว้ว่า หมายถึงข้อมูลที่เกี่ยวข้องกับบุคคลที่ยังมีชีวิตอยู่ ซึ่งบุคคลสามารถระบุตัวตนทั้งโดยตรงหรือโดยอ้อมได้จากการผสมกันของข้อมูลส่วนบุคคลอื่น ๆ อันประกอบด้วย ชื่อนามสกุล หมายเลขลงทะเบียนผู้อยู่อาศัย รูปภาพ

นอกจากนี้ พระราชบัญญัติข้างต้นได้กำหนดให้การกระทำละเมิดข้อมูลส่วนบุคคลบางประการเป็นความผิดอาญาและกำหนดอัตราโทษไว้ เช่น กรณีตัวแทนของบริษัทหรือลูกจ้างถูกพบว่ากระทำการฝ่าฝืนพระราชบัญญัตินี้ในระหว่างการดำเนินธุรกิจในนามของบริษัทผู้อื่น จะต้องถูกลงโทษและบริษัทอาจถูกปรับด้วย โดยผู้ควบคุมข้อมูลหรือบุคคลใดที่ฝ่าฝืนบทบัญญัติ ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 50 ล้านวอน

กล่าวโดยสรุป แม้ว่าสถานการณ์การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของสาธารณรัฐเกาหลี โดยเฉพาะอย่างยิ่งการแอบอ้างเป็นบุคคลที่มีชื่อเสียงบนเว็บไซต์ที่ให้บริการสื่อสังคมออนไลน์จะเพิ่มจำนวนมากขึ้น และสาธารณรัฐเกาหลียังไม่มีมาตรการทางกฎหมายที่ชัดเจนและเป็นการเฉพาะสำหรับจัดการแก้ไขปัญหาเหล่านี้แต่อย่างใด แต่ผู้เสียหายสามารถดำเนินคดีทางอาญากับผู้กระทำความผิดตามลักษณะการกระทำความผิดที่เกิดขึ้นและมีกฎหมายที่ใช้บังคับอยู่ในปัจจุบันกำหนดให้การกระทำนั้นเป็นความผิดได้ รวมทั้งสามารถใช้สื่อสังคมออนไลน์เป็นกระบอกเสียงในการชี้แจงให้ประชาชนทั่วไปรับทราบข้อเท็จจริงที่ถูกต้องและแจ้งเตือนให้ผู้กระทำความผิดยุติการสวมรอย

จากการศึกษาถึงสภาพปัญหาและมาตรการทางกฎหมายที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในสหรัฐอเมริกา สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี ทำให้ทราบว่าการสวมรอยเป็นบุคคลอื่นเป็นปัญหาที่สร้างความเสียหายและกระทบต่อสิทธิของบุคคลในหลายด้าน ไม่ว่าจะเป็นสิทธิในตัวตน สิทธิในความเป็นส่วนตัว สิทธิในข้อมูลส่วนบุคคล รวมถึงสิทธิในการดำรงชีวิตอื่น ๆ เช่น สิทธิที่จะไม่ถูกล่วงละเมิดในความเป็นอยู่ สิทธิในชื่อเสียงเกียรติคุณ

สิทธิในทรัพย์สินและการเงิน เป็นต้น จะเห็นได้ว่าการถูกสวมรอยเป็นการล่วงละเมิดต่อสิทธิทั้งหลายที่กล่าวมา อีกทั้งการสวมรอยที่เกิดขึ้นในระบบเครือข่ายอินเทอร์เน็ตทำให้เกิดความเสียหายแพร่กระจายไปในวงกว้างยิ่งกว่าการสวมรอยแบบดั้งเดิม แต่ละประเทศข้างต้นจึงต้องกำหนดแนวทางและวิธีการจัดการกับปัญหาที่เกิดขึ้น โดยภาพรวมแล้ว มาตรการทางกฎหมายที่ถูกนำมาใช้ในการนี้เป็นมาตรการทางอาญา ซึ่งแบ่งออกเป็น 2 ลักษณะคือ การตรากฎหมายเฉพาะกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความรับผิดทางอาญาและกำหนดระวางโทษจำคุกหรือโทษปรับ ดังเช่นกฎหมายเฉพาะของมลรัฐต่าง ๆ ในสหรัฐอเมริกา และการนำกฎหมายทั่วไปที่เกี่ยวข้องที่มีอยู่แล้วมาปรับใช้แก่กรณีเป็นรายไป ดังเช่นในสหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี โดยเฉพาะสหราชอาณาจักรเองมีคู่มือการปฏิบัติงานเกี่ยวกับการกระทำความผิดดังกล่าวเป็นการเฉพาะ ทำให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถปฏิบัติหน้าที่และบังคับใช้กฎหมายได้อย่างเหมาะสมมากยิ่งขึ้น

บทที่ 5
บทวิเคราะห์เปรียบเทียบมาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

จากการศึกษาในบทที่ 3 เรื่อง มาตรการทางอาญาที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทย จะเห็นได้ว่า ประเทศไทยไม่มีกฎหมายเกี่ยวกับการกระทำความผิดดังกล่าวไว้เป็นการเฉพาะ เมื่อพิจารณาถึงกฎหมายต่าง ๆ ที่เกี่ยวข้อง ได้แก่ ประมวลกฎหมายอาญาในความผิดฐานหมิ่นประมาท ความผิดฐานฉ้อโกง ความผิดฐานปลอมเอกสาร พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับที่แก้ไขเพิ่มเติม และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... พบว่ายังไม่ครอบคลุมลักษณะการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอย่างเพียงพอ รวมถึงไม่สามารถคุ้มครองผู้เสียหายจากการถูกสวมรอยได้อย่างแท้จริง ด้วยเหตุนี้ จึงจำเป็นต้องศึกษาต่อไปในบทที่ 4 เรื่อง มาตรการทางอาญาที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของต่างประเทศ

เมื่อได้ศึกษาถึงมาตรการทางกฎหมายต่าง ๆ ของสหรัฐอเมริกา สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี ทำให้ทราบว่า สหรัฐอเมริกามีกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการเฉพาะ โดยบัญญัติเป็นกฎหมายในระดับมลรัฐ ส่วนอีกสามประเทศยังไม่มีกฎหมายเฉพาะ แต่มีแนวทางในการนำกฎหมายอื่น ๆ ที่มีอยู่แล้วมาปรับใช้ให้เหมาะสมแก่เหตุการณ์ที่เกิดขึ้นเป็นรายกรณีไป

ในบทนี้ ผู้เขียนจะนำมาตรการทางกฎหมายอาญาของสหรัฐอเมริกา สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี มาวิเคราะห์เปรียบเทียบเพื่อเป็นแนวทางว่าประเทศไทยควรกำหนดมาตรการทางอาญาสำหรับกรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอย่างไรจึงจะเหมาะสมและมีประสิทธิภาพสูงสุด โดยแบ่งการวิเคราะห์เปรียบเทียบออกเป็น 3 ส่วน ได้แก่ การวิเคราะห์เปรียบเทียบลักษณะการกระทำความผิด การวิเคราะห์เปรียบเทียบมาตรการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต และการวิเคราะห์เปรียบเทียบมาตรการบังคับเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

5.1 การวิเคราะห์เปรียบเทียบลักษณะการกระทำความผิด

5.1.1 การวิเคราะห์เปรียบเทียบลักษณะการกระทำความผิดของต่างประเทศ

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นพฤติกรรมที่เกิดขึ้นในประเทศต่าง ๆ ทั่วโลก ไม่ว่าประเทศนั้นจะมีการให้คำจำกัดความการกระทำความผิดดังกล่าวไว้หรือไม่ก็ตาม จากการศึกษาถึงลักษณะของการสวมรอยเป็นบุคคลอื่นของต่างประเทศในบทที่ 4 ที่ผ่านมา จะเห็นได้ว่า ในภาพรวม การกระทำดังกล่าวมีองค์ประกอบและรูปแบบการกระทำความผิดที่คล้ายคลึงกันเป็นอย่างมาก ทั้งนี้ พบว่าสหรัฐอเมริกาเป็นเพียงประเทศเดียวที่ให้ความหมายของการสวมรอยเช่นนี้ไว้อย่างชัดเจน ส่วนสหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี ไม่ได้กำหนดคำนิยามของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไว้เป็นการเฉพาะแต่อย่างใด ผู้เขียนจึงเห็นสมควรวิเคราะห์เปรียบเทียบลักษณะการกระทำความผิดดังกล่าวของทั้ง 4 ประเทศ ดังต่อไปนี้

5.1.1.1 สหรัฐอเมริกา

สหรัฐอเมริกาเป็นประเทศเดียวที่มีการให้คำจำกัดความของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต โดยกำหนดไว้ในกฎหมายระดับมลรัฐ โดยส่วนใหญ่แต่ละมลรัฐที่มีการตรากฎหมายนี้จะเรียกการกระทำความผิดนี้ว่า “Online Impersonation” หรือบางมลรัฐอาจใช้คำว่า Internet Impersonation หรือ Digital Impersonation

ในส่วนนี้ผู้เขียนจะขอยกเอาลักษณะการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของมลรัฐเทกซัส มลรัฐแคลิฟอร์เนีย และมลรัฐนิวยอร์ก มาเป็นตัวอย่างให้ทราบว่าการกระทำความผิดดังกล่าวมีองค์ประกอบและรูปแบบการกระทำความผิดอย่างไร

(1) มลรัฐเทกซัส (Texas)

ตามประมวลกฎหมายอาญาแห่งมลรัฐเทกซัส มาตรา 33.07 นั้น การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต หรือตามที่บทบัญญัติใช้คำว่า Online Impersonation มีลักษณะการกระทำความผิดดังที่ระบุไว้ในอนุมาตรา (a) ว่าหมายถึง การกระทำของบุคคลใดบุคคลหนึ่งซึ่งใช้ชื่อหรือตัวตนของบุคคลอื่นโดยไม่ได้รับความยินยอม เพื่อสร้างหน้าเว็บบนเว็บไซต์เครือข่ายสังคมออนไลน์เชิงพาณิชย์ หรือเว็บไซต์อินเทอร์เน็ตอื่น หรือเพื่อเขียนหรือส่งข้อความผ่านทางเว็บไซต์เครือข่ายสังคมออนไลน์เชิงพาณิชย์ หรือเว็บไซต์อินเทอร์เน็ตอื่น หรือผ่านทางโปรแกรมจดหมายอิเล็กทรอนิกส์ หรือโปรแกรมกระดานข้อความ การกระทำเช่นนี้ต้องเกิดจากเจตนาเพื่อประทุษร้าย ฉ้อโกง ข่มขู่ หรือข่มขู่ผู้อื่นให้หวาดกลัว

นอกจากนี้ในอนุมาตรา (b) ได้ระบุถึงลักษณะการกระทำความผิดอีกลักษณะหนึ่ง ได้แก่ การส่งจดหมายอิเล็กทรอนิกส์ ข้อความด่วน ข้อความตัวอักษร หรือการสื่อสารอื่นในทำนองเดียวกันซึ่งอ้างอิงถึงชื่อ ที่อยู่ หมายเลขโทรศัพท์ หรือสิ่งอื่นใดที่สามารถระบุได้ว่าเป็นข้อมูลของบุคคลอื่น ประกอบกับเป็นการส่งโดยไม่ได้รับความยินยอมจากบุคคลอื่น มีเจตนาก่อให้ผู้รับการสื่อสารเชื่อโดยมีเหตุอันสมควรว่าผู้ส่งได้รับอำนาจส่งการสื่อสารนั้นแล้ว และยังต้องมีเจตนาภายในเพื่อประทุษร้ายหรือฉ้อโกงอีกด้วย

(2) มลรัฐแคลิฟอร์เนีย

บทบัญญัติของมลรัฐแคลิฟอร์เนียที่กำหนดถึงการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต คือ มาตรา 528.5 แห่งประมวลกฎหมายอาญาแห่งมลรัฐแคลิฟอร์เนีย โดยบัญญัติถึงลักษณะการกระทำความผิดฐานนี้ว่าหมายถึง การที่ผู้ใดผู้หนึ่งที่จงใจสวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือ (Credibly Impersonate) ผ่านทางเว็บไซต์อินเทอร์เน็ตหรือผ่านวิธีการทางอิเล็กทรอนิกส์อื่น ๆ โดยมีวัตถุประสงค์เพื่อประทุษร้าย ขู่ขวัญ ข่มขู่ให้หวาดกลัว หรือฉ้อโกงผู้อื่น ทั้งนี้ การสวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือ หมายความว่า การสวมรอยที่มีเหตุอันสมควรจะทำให้ผู้อื่นเชื่อหรือได้เชื่อว่าผู้สวมรอยคือผู้ที่ถูกสวมรอยตัวจริง

(3) มลรัฐนิวยอร์ก

ลักษณะการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของมลรัฐนิวยอร์กถูกกำหนดไว้ในประมวลกฎหมายอาญาแห่งมลรัฐนิวยอร์ก มาตรา 190.25 อนุมาตรา 4 โดยกำหนดไว้ว่า เป็นการสวมรอยเป็นบุคคลอื่นด้วยวิธีการสื่อสารทางเว็บไซต์อินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์ โดยมีเจตนาเพื่อให้ได้มาซึ่งผลประโยชน์ หรือเพื่อประทุษร้าย หรือเพื่อฉ้อโกงผู้อื่น

นอกจากนี้ยังหมายรวมถึง การแอบอ้างเป็นเจ้าหน้าที่รัฐด้วยวิธีการสื่อสารข้างต้น เพื่อจูงใจให้ผู้อื่นยินยอมต่ออำนาจของเจ้าหน้ารัฐนั้น หรือกระทำการบางอย่างภายใต้ความน่าเชื่อถือไว้วางใจที่เกิดจากการแอบอ้างดังกล่าว

ตามที่ได้ยกตัวอย่างลักษณะการกระทำความผิดตามกฎหมายเฉพาะของทั้ง 3 มลรัฐข้างต้นนั้น จะเห็นได้ว่า สหรัฐอเมริกาได้กำหนดลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไว้อย่างละเอียด และมักจะมีการกำหนดคำนิยามของถ้อยคำที่ควรทราบไว้อย่างชัดเจน โดยรวมแล้วจะระบุไว้กว้าง ๆ ว่าเป็นการสวมรอยเป็นบุคคลอื่นด้วยการนำข้อมูลส่วนบุคคลของบุคคลอื่นมาใช้ในการติดต่อสื่อสารทางเครือข่ายอินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล และเป็นการสวมรอยที่มีเจตนาเพื่อก่อให้เกิดความเสียหายหรือล่วงละเมิดผู้อื่น ไม่ว่าจะเป็นเจตนาเพื่อประทุษร้าย หลอกลวงฉ้อโกง ข่มขู่คุกคาม หรือให้

ตนได้มาซึ่งผลประโยชน์ที่มิควรได้โดยชอบ ทั้งนี้ มีข้อสังเกตว่า แต่ละมลรัฐจะกำหนดรายละเอียดของการกระทำความผิดที่แตกต่างกันอยู่พอสมควร ดังเช่น มลรัฐเทกซัสกำหนดให้มีการกระทำความผิด 2 ลักษณะ เพื่อประโยชน์ในการกำหนดอัตราโทษที่แตกต่างกัน มลรัฐแคลิฟอร์เนียกำหนดว่าการสวมรอยต้องมีลักษณะที่น่าเชื่อถือ ส่วนมลรัฐนิวยอร์กกำหนดให้การสวมรอยครอบคลุมไปถึงการแอบอ้างตนเป็นเจ้าหน้าที่รัฐเพื่อใช้อำนาจโดยมิชอบอีกด้วย

อนึ่ง จากการศึกษาในบทที่ผ่านมาทำให้ทราบว่าสหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี ไม่มีคำจำกัดความของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไว้เป็นการเฉพาะ แต่เมื่อมีเหตุการณ์ในลักษณะเช่นว่านี้เกิดขึ้น อาจเกี่ยวโยงไปถึงลักษณะของการกระทำความผิดอื่น ๆ ได้หลายประการ ดังนี้

5.1.1.2 สหราชอาณาจักร

ลักษณะการกระทำความผิดที่เกิดขึ้นบ่อยในสหราชอาณาจักร คือ บัญชีสื่อสังคมออนไลน์ที่มีลักษณะปลอมหรือล่วงละเมิด กล่าวคือ เป็นการสร้างบัญชีหรือเว็บไซต์เครือข่ายสังคมออนไลน์ปลอมขึ้น หรือการสร้างโพรไฟล์หรือนามแฝงปลอมที่อาจนำไปสู่การกระทำความผิดทางอาญาได้ ส่วนจะถือว่าเป็นความผิดทางอาญาฐานใดต้องพิจารณาพฤติการณ์ที่เกิดขึ้นเป็นรายกรณี เช่น การสร้างหน้าเว็บไซต์เฟซบุ๊กในนามของเหยื่อ เพื่อมุ่งประทุษร้ายตัวตนของเหยื่อ และหน้าเว็บไซต์นั้นประกอบไปด้วยสิ่งที่มีลักษณะล่วงละเมิด เป็นความเท็จ คุกคาม หรือลามกอนาจาร เป็นต้น ทั้งนี้ สหราชอาณาจักรไม่ได้ระบุไว้อย่างชัดเจนว่าการสร้างบัญชีออนไลน์ปลอมดังกล่าวจะต้องมีขึ้นด้วยเจตนาประการใด ด้วยเหตุนี้ การสวมรอยจะเป็นความผิดหรือไม่จึงขึ้นอยู่กับลักษณะของการกระทำที่เกิดขึ้นว่ามีการกระทบกระเทือนต่อสิทธิของบุคคลอื่นหรือไม่ อย่างไร

5.1.1.3 ประเทศญี่ปุ่น

ลักษณะการกระทำความผิดที่เกิดขึ้นในประเทศญี่ปุ่นมีหลายรูปแบบ โดยภาพรวมแล้วเป็นการกระทำความผิดในนามของบุคคลอื่นผ่านทางระบบเครือข่ายอินเทอร์เน็ต เช่น การอ้างตัวตนปลอมในระบบออนไลน์ด้วยการสร้างบัญชีเว็บไซต์เครือข่ายสังคมออนไลน์ในนามของบุคคลอื่น การใช้หลักฐานรับรองตัวตนของบุคคลอื่นโดยมิชอบด้วยกฎหมายด้วยการใช้บัญชีผู้ใช้งานหรือรหัสผ่านของบุคคลอื่นเพื่อสร้างจดหมายอิเล็กทรอนิกส์ในนามของบุคคลนั้น หรือการนำข้อมูลส่วนบุคคลของผู้อื่นมาสร้างข้อมูลทะเบียนอิเล็กทรอนิกส์โดยไม่มีอำนาจ เป็นต้น

5.1.1.4 สาธารณรัฐเกาหลี

ลักษณะการกระทำความผิดที่เกิดขึ้นในสาธารณรัฐเกาหลีสามารถแบ่งได้เป็น 2 รูปแบบ ได้แก่ การสร้างบัญชีสื่อสังคมออนไลน์ปลอมในนามของบุคคลอื่น และการสมัครใช้งานเว็บไซต์โดยอาศัยเลขประจำตัวผู้อยู่อาศัย (Resident Registration Number: RNN) ของบุคคลอื่น

รูปแบบแรกเป็นพฤติกรรมที่พบเห็นได้ทั่วไปเช่นเดียวกับประเทศอื่น กล่าวคือ ผู้กระทำความผิดจะสร้างบัญชีสื่อสังคมออนไลน์ปลอมขึ้นในนามของบุคคลอื่น ซึ่งมักจะเป็นบุคคลที่มีชื่อเสียงในแวดวงต่าง ๆ ในหน้าบัญชีสื่อสังคมออนไลน์ปลอมจะประกอบไปด้วยข้อมูลส่วนบุคคลและรูปภาพของเหยื่อ ผู้กระทำความผิดจะใช้บัญชีดังกล่าวเขียนข้อความประกาศแจ้งให้ผู้ติดตามหรือประชาชนทั่วไปหลงเชื่อว่าบัญชีนั้นเป็นของจริง และอาจนำไปสู่การกระทำความผิดอื่นต่อไป

รูปแบบที่ 2 เป็นการนำเลขประจำตัวผู้อยู่อาศัยในสาธารณรัฐเกาหลีไปใช้ประโยชน์โดยไม่ได้รับอนุญาต โดยเฉพาะการสมัครใช้บริการเว็บไซต์หรือเกมออนไลน์ เนื่องจากสาธารณรัฐเกาหลีกำหนดให้ผู้ใช้บริการเว็บไซต์หรือเกมออนไลน์ต้องยืนยันตัวตนด้วยการแสดงเลขประจำตัวผู้อยู่อาศัยในขั้นตอนการสมัครใช้บริการ จึงมีคนจำนวนมากที่นำเลขประจำตัวผู้อยู่อาศัยของบุคคลอื่นไปใช้เพื่อการนี้

เมื่อพิจารณาถึงลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของแต่ละประเทศข้างต้นแล้ว สามารถสรุปได้ว่า การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต หมายถึง การใช้ข้อมูลส่วนบุคคลของบุคคลอื่นโดยไม่ได้รับความยินยอม เพื่อก่อให้เกิดการติดต่อสื่อสารผ่านทางระบบเครือข่ายอินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์ เช่น การสร้างบัญชีผู้ใช้งานเว็บไซต์หรือแอพพลิเคชั่นสื่อสังคมออนไลน์ การส่งจดหมายอิเล็กทรอนิกส์ การส่งข้อความสนทนา การใช้งานกระดานข้อความ เป็นต้น เป็นเหตุให้ผู้อื่นเชื่อว่าผู้สวมรอยเป็นผู้ที่ถูกสวมรอยจริง โดยการสวมรอยเช่นนี้ต้องมีวัตถุประสงค์ที่มิชอบด้วยกฎหมาย เช่น สวมรอยเพื่อไปกระทำความผิดอื่น เพื่อประทุษร้าย ข่มขู่คุกคาม หลอกลวงฉ้อโกง หรือทำให้เสื่อมเสียชื่อเสียงเกียรติยศ เป็นต้น

ทั้งนี้ ลักษณะการสวมรอยเป็นบุคคลอื่นของแต่ละประเทศดังกล่าวข้างต้นมีความคล้ายคลึงกันเป็นอย่างมาก อาจมีความแตกต่างอยู่บ้างในรายละเอียดปลีกย่อย ดังแสดงให้เห็นได้ตามตารางเปรียบเทียบต่อไปนี้

ตารางที่ 3 ลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

ประเทศ / ประเด็น	สหรัฐอเมริกา			สหราชอาณาจักร	ประเทศญี่ปุ่น	สาธารณรัฐเกาหลี
	มลรัฐแคลิฟอร์เนีย	มลรัฐเทกซัส	มลรัฐนิวยอร์ก			
ลักษณะการกระทำความผิดที่เข้าข่ายการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต	- สวมรอยเป็นบุคคลอื่นผ่านเว็บไซต์หรือวิธีการทางอิเล็กทรอนิกส์ด้วยวิธีการต่าง ๆ เช่น สร้างหน้าเว็บบนเว็บไซต์เครือข่ายสังคมออนไลน์หรือเว็บไซต์อื่น หรือส่งข้อความผ่านทางเว็บไซต์เครือข่ายสังคมออนไลน์หรือเว็บไซต์อื่น หรือส่งจดหมายอิเล็กทรอนิกส์ หรือสิ่งอื่น ๆ ซึ่งอ้างถึงข้อมูลส่วนบุคคลของผู้อื่น หรือสวมรอยอ้างอำนาจของเจ้าหน้าที่รัฐ - เพื่อให้เกิดผลซึ่งผลประโยชน์ หรือประทุษร้าย ผู้ขู่บังคับ ข่มขู่ให้หวาดกลัว หรือหลอกลวงด้อโกง - กระทำโดยเจตนา - ไม่ได้รับความยินยอมจากผู้ถูกสวมรอย	- สร้างบัญชีหรือเว็บไซต์เครือข่ายสังคมออนไลน์ปลอม - สร้างโพรไฟล์หรือบทสนทนาปลอม - วัตถุประสงค์ของการสวมรอยมีได้หลายประการ เช่น มุ่งประทุษร้ายตัวตนของเหยื่อ หรือมีลักษณะส่วนลบมิด เป็นความเท็จ คุกคาม หรือลามกอนาจาร	- อ้างตัวตนปลอมในระบบออนไลน์ด้วยการสร้างบัญชีเว็บไซต์เครือข่ายสังคมออนไลน์ปลอมขึ้นในนามของบุคคลอื่น - ใช้หลักฐานรับรองตัวตนของบุคคลอื่นโดยมิชอบด้วยกฎหมายด้วยการใช้บัญชีผู้ใช้งานหรือรหัสผ่านของบุคคลอื่นเพื่อสร้างจดหมายอิเล็กทรอนิกส์ในนามของบุคคลนั้น - นำข้อมูลส่วนบุคคลของผู้อื่นมาสร้างข้อมูลทะเบียนอิเล็กทรอนิกส์โดยไม่มีอำนาจ	- สร้างบัญชีสื่อสังคมออนไลน์ปลอมขึ้นในนามของบุคคลอื่น - ใช้แคชประจำตัวผู้อุ่อาศัย (RNN) เพื่อสมัครใช้บริการเว็บไซต์หรือเกมออนไลน์โดยไม่ได้รับอนุญาต

5.1.2 การกำหนดลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทย

หลังจากวิเคราะห์เปรียบเทียบลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของต่างประเทศไปแล้วในหัวข้อที่ 5.1.1 ในส่วนนี้ ผู้เขียนจะวิเคราะห์ถึงการกำหนดลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทย

เมื่อพิจารณาเปรียบเทียบลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของต่างประเทศข้างต้นแล้ว จะเห็นได้ว่าเป็นรูปแบบการสวมรอยที่เกิดขึ้นทั่วไปบนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานอินเทอร์เน็ตในประเทศไทยต่างต้องเผชิญกับความเสี่ยงที่จะถูกนำข้อมูลส่วนบุคคลไปใช้สวมรอยเช่นเดียวกัน แต่ประเทศไทยไม่ได้กำหนดให้การกระทำเช่นนี้เป็นความผิดแต่อย่างใด และมักนำลักษณะการกระทำความผิดอื่นที่ใกล้เคียงหรือเกี่ยวข้องมาปรับใช้ เช่น กรณีที่มีการสวมรอยและทำให้เสื่อมเสียชื่อเสียงนำไปเทียบเคียงกับความผิดฐานหมิ่นประมาท หรือกรณีสวมรอยแล้วหลอกลวงผู้อื่นเพื่อให้ได้ไปซึ่งทรัพย์สิน นำไปเทียบเคียงกับความผิดฐานฉ้อโกง เป็นต้น อย่างไรก็ตาม แม้ว่าการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตจะเป็นส่วนหนึ่งของการกระทำความผิดฐานต่าง ๆ ดังกล่าวจริง แต่ด้วยบทบัญญัติฐานความผิดแต่ละฐานมีคุณธรรมทางกฎหมายที่แตกต่างกัน ทำให้มีผู้เสียหายโดยนิตินัยแตกต่างกันไปด้วย การนำบทบัญญัติเหล่านี้มาปรับใช้แก่กรณีสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตจึงไม่อาจคุ้มครองคุณธรรมทางกฎหมายและผู้เสียหายที่แท้จริงได้อย่างครอบคลุม เช่น ความผิดฐานฉ้อโกงมุ่งคุ้มครองผู้ที่ถูกหลอกลวง แต่ไม่ได้มุ่งคุ้มครองผู้ที่ถูกสวมรอย เป็นต้น

ผู้เขียนมีความเห็นว่าประเทศไทยควรกำหนดลักษณะการกระทำความผิดเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตให้ชัดเจน โดยกำหนดองค์ประกอบ รูปแบบ รายละเอียดของการกระทำให้ครอบคลุมกับเหตุการณ์ที่เกิดขึ้น เพื่อเป็นหลักเกณฑ์ให้เจ้าหน้าที่ที่เกี่ยวข้องและประชาชนทั่วไปทราบว่าการกระทำใดบ้างที่เข้าข่ายเป็นการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ทั้งนี้ จากการวิเคราะห์ลักษณะการกระทำความผิดของต่างประเทศ ทำให้ทราบว่าสหรัฐอเมริกามีกฎหมายระดับมลรัฐที่กำหนดลักษณะการกระทำความผิดนี้ไว้อย่างละเอียดชัดเจน สมควรนำมาเป็นแนวทางในการพิจารณากำหนดลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทยดังต่อไปนี้

5.1.2.1 องค์ประกอบความผิด

(1) ผู้กระทำ ได้แก่ ผู้ที่กระทำโดยรู้อยู่แล้วว่าการกระทำนั้นเป็นการสวมรอยเป็นบุคคลอื่น และได้กระทำไปโดยไม่ได้รับความยินยอมจากผู้ถูกสวมรอย

(2) การกระทำ ในส่วนของการกระทำสามารถแบ่งลักษณะการกระทำออกเป็นหลายรูปแบบ ดังนี้

2.1 สวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือผ่านทางเว็บไซต์อินเทอร์เน็ต โปรแกรมประยุกต์ หรือวิธีการทางอิเล็กทรอนิกส์อย่างอื่น

2.2 สวมรอยเป็นเจ้าหน้าที่รัฐผ่านทางเว็บไซต์อินเทอร์เน็ต โปรแกรมประยุกต์ หรือวิธีการทางอิเล็กทรอนิกส์อย่างอื่น เพื่อโน้มน้าวให้ผู้อื่นยอมต่ออำนาจเช่นว่านั้นหรือแสดงตนให้น่าเชื่อถือ

2.3 สวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือโดยประการที่น่าจะก่อให้เกิดความเสียหายแก่ประชาชน การรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือเป็นการสวมรอยที่กระทบต่อความมั่นคงแห่งราชอาณาจักร

การสวมรอยเป็นบุคคลอื่นเกิดจากการใช้ชื่อหรือข้อมูลแสดงอัตลักษณ์ส่วนบุคคลของผู้อื่นเพื่อแอบอ้างเป็นผู้นั้น และมีลักษณะเป็นที่น่าเชื่อถือแก่ผู้พบเห็น กล่าวคือ มีเหตุอันสมควรให้ผู้อื่นเชื่อได้ว่าผู้กระทำผิดเป็นบุคคลที่ถูกสวมรอยจริง ๆ การแอบอ้างดังกล่าวสามารถเกิดขึ้นได้หลายช่องทางที่เชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ต เช่น การสร้างหน้าเว็บ (Web Pages) การสร้างโพรไฟล์บนเว็บไซต์หรือโปรแกรมประยุกต์ในกลุ่มเครือข่ายสังคมออนไลน์ (Social Networking Sites) การส่งจดหมายอิเล็กทรอนิกส์ ข้อความด่วน หรือข้อความตัวอักษร การใช้งานห้องสนทนา (Chat Room) การใช้งานกระดานสนทนาออนไลน์ (Online Web Board) เป็นต้น

ทั้งนี้ ผู้เขียนเห็นควรให้แบ่งลักษณะการกระทำผิดออกเป็น 3 รูปแบบ ตามแนวคิดการแยกประเภทความผิดฐาน Online Impersonation ของมลรัฐเทกซัส[1] ซึ่งแบ่งเป็นความผิดอาญาอุกฉกรรจ์และความผิดลหุโทษไว้ในบทบัญญัติเดียวกัน ด้วยเหตุผลที่ว่าลักษณะการกระทำผิดแต่ละรูปแบบมีความร้ายแรงหรือผลกระทบที่เกิดขึ้นไม่เท่ากัน ดังนั้น หากพิจารณากำหนดลักษณะการกระทำผิดเป็น 3 รูปแบบ จะทำให้สามารถกำหนดมาตรการบังคับทางอาญาที่เหมาะสมกับความร้ายแรงของแต่ละการกระทำได้โดยสะดวกมากขึ้น

(3) กรรมของการกระทำ ได้แก่ ข้อมูลส่วนบุคคลที่ใช้ระบุตัวตนของผู้ถูกสวมรอย (Identifying Information) เช่น ชื่อนามสกุล วันเกิด รูปภาพประเภทภาพนิ่งและภาพเคลื่อนไหว

[1] TEXAS PENAL CODE § 33.07

วีดิทัศน์ หมายเลขประจำตัว หมายเลขบัญชีผู้ใช้งานอื่น ๆ ที่อยู่อาศัย ที่อยู่จดหมายอิเล็กทรอนิกส์ หมายเลขโทรศัพท์ ประวัติการศึกษา ข้อมูลทางการแพทย์ ประวัติอาชญากร เป็นต้น

ข้อมูลส่วนบุคคลเหล่านี้เมื่อนำมาประกอบกันจะสามารถระบุถึงตัวบุคคลใดบุคคลหนึ่งได้อย่างเฉพาะเจาะจง การสวมรอยเป็นบุคคลอื่นเกิดจากการนำข้อมูลเฉพาะตัวบุคคลไปใช้แอบอ้างแสร้งว่าตนเป็นบุคคลนั้น ดังนั้น ข้อมูลส่วนบุคคลจึงเป็นกรรมของการกระทำ และเนื่องด้วยข้อมูลส่วนบุคคลเป็นหนึ่งในสิทธิส่วนบุคคล จึงส่งผลให้คุณธรรมทางกฎหมายในความผิดฐานนี้ คือ สิทธิในความเป็นตัวตนและสิทธิส่วนบุคคลของผู้ถูกสวมรอยนั่นเอง

(4) เจตนาพิเศษ นอกเหนือจากเจตนาธรรมดาที่ผู้กระทำต้องมีสำนึกรู้ตัวในขณะกระทำการสวมรอยเป็นบุคคลอื่นแล้ว ยังมีเจตนาพิเศษที่เป็นหัวใจสำคัญของความผิดฐานนี้อีกด้วย ตามกฎหมายของสหรัฐอเมริกาปรากฏวัตถุประสงค์ของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไว้หลายกรณี ประกอบกับบทบัญญัติที่ระบุไว้ว่าเกี่ยวข้องกับการปลอมบัญชีผู้ใช้งานสื่อสังคมออนไลน์ตาม CPS Guidelines on Prosecuting Cases Involving Communication Sent via Social Media ของสหราชอาณาจักร ก็มีการกล่าวถึงวัตถุประสงค์ที่ไม่ชอบด้วยกฎหมายไว้เช่นกัน ดังนั้น ผู้เขียนเห็นควรกำหนดเจตนาพิเศษของการกระทำความผิดดังกล่าวให้ครอบคลุม ดังนี้

4.1 เพื่อประทุษร้าย (Harm)

4.2 เพื่อหลอกลวง (Defraud)

4.3 เพื่อขู่เข็ญหรือข่มขู่ให้หวาดกลัว (Intimidate or Threaten)

4.4 เพื่อให้ได้มาซึ่งผลประโยชน์ (Obtain a benefit)

4.5 เพื่อคุกคาม รังควาน หรือก่อความรำคาญ (Harass)

จะเห็นได้ว่า แต่ละกรณีล้วนอาจก่อให้เกิดความเสียหายทั้งต่อชีวิต ร่างกาย ทรัพย์สิน ความเป็นอยู่ ตลอดจนสภาพจิตใจและอารมณ์ของผู้ถูกสวมรอยและผู้เสียหายรายอื่นที่เกี่ยวข้องได้ทั้งสิ้น ประเทศไทยจึงสมควรกำหนดเจตนาพิเศษให้ชัดเจนและครอบคลุมมากที่สุด

5.2 การวิเคราะห์เปรียบเทียบมาตรการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

5.2.1 การวิเคราะห์เปรียบเทียบมาตรการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของต่างประเทศ

จากการศึกษาถึงมาตรการทางกฎหมายที่สหรัฐอเมริกา สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี นำมาบังคับใช้เพื่อป้องกันและปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ทำให้ทราบว่าสหรัฐอเมริกามีการบัญญัติให้การกระทำดังกล่าวเป็นความผิดอาญา โดยบัญญัติไว้ในกฎหมายระดับมลรัฐ ส่วนสหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี ไม่มีบทบัญญัติกำหนดฐานความผิดดังกล่าวไว้เป็นการเฉพาะ แต่จะนำบทบัญญัติแห่งกฎหมายอื่นที่เกี่ยวข้องมาปรับใช้ให้เหมาะสมกับข้อเท็จจริงที่เกิดขึ้น ในหัวข้อนี้ ผู้เขียนจะอธิบายถึงมาตรการทางกฎหมายของต่างประเทศ โดยแบ่งออกเป็น (1) การกำหนดฐานความผิดอาญากรณีสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต และ (2) มาตรการทางกฎหมายทั่วไปที่นำมาปรับใช้กับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

5.2.1.1 การกำหนดฐานความผิดอาญากรณีสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

หลายมลรัฐในสหรัฐอเมริกามีแนวทางนำมาตรการทางกฎหมายมาจัดการกับปัญหาการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตด้วยการตรากฎหมายกำหนดให้การสวมรอยดังกล่าวเป็นความผิดทางอาญา ดังปรากฏตามบทบัญญัติ Online Impersonation ของมลรัฐต่าง ๆ ในส่วนนี้ ผู้เขียนจะขออธิบายถึงมาตรการทางกฎหมายที่มลรัฐเทกซัส มลรัฐแคลิฟอร์เนีย และมลรัฐนิวยอร์กนำมาใช้แก่กรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ดังนี้

(1) มลรัฐเทกซัส

มาตรการทางกฎหมายที่มลรัฐเทกซัสนำมาใช้คือการออกกฎหมายเฉพาะกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดทางอาญา ในชื่อฐานความผิดว่า Online Impersonation ดังปรากฏตามประมวลกฎหมายอาญาแห่งมลรัฐเทกซัส ลักษณะ 7 ความผิดต่อทรัพย์สิน หมวด 33 อาชญากรรมคอมพิวเตอร์ มาตรา 33.07 บทบัญญัตินี้แบ่งลักษณะการกระทำความผิดออกเป็น 2 ลักษณะ ได้แก่

1.1 การใช้ชื่อหรือตัวตนของบุคคลอื่นเพื่อสร้างหน้าเว็บบนเว็บไซต์เครือข่ายสังคมออนไลน์หรือเว็บไซต์อินเทอร์เน็ตอื่น หรือประกาศหรือส่งข้อความบนเว็บไซต์เครือข่ายสังคมออนไลน์ หรือเว็บไซต์อินเทอร์เน็ตอื่น หรือผ่านทางโปรแกรมจดหมายอิเล็กทรอนิกส์ หรือ

โปรแกรมกระดานข้อความ โดยมีเจตนาเพื่อประทุษร้าย หลอกลวงฉ้อโกง ขู่ขวัญ หรือข่มขู่ผู้อื่นให้หวาดกลัว ถือเป็นความผิดอาญาอุกฉกรรจ์ระดับสาม (Felony of the Third Degree)[2]

1.2 การส่งจดหมายอิเล็กทรอนิกส์ ข้อความด่วน ข้อความตัวอักษร หรือการสื่อสารรูปแบบอื่นที่คล้ายคลึงกันนี้ ซึ่งอ้างอิงชื่อ ที่อยู่ หมายเลขโทรศัพท์ หรือสิ่งอื่นที่เป็นข้อมูลในการระบุตัวบุคคลอื่น โดยมีเจตนาเพื่อประทุษร้ายหรือหลอกลวงฉ้อโกงผู้อื่น ถือเป็นความผิดลหุโทษระดับ A (Class A Misdemeanor)[3]

ทั้งนี้ ลักษณะการกระทำความผิดทั้งสองแบบมีองค์ประกอบที่ตรงกันอยู่ประการหนึ่ง คือ การสวมรอยเป็นบุคคลอื่นต้องเกิดขึ้นโดยไม่ได้รับความยินยอมจากผู้ที่ถูกสวมรอย

อนึ่ง มาตรา 33.07 กำหนดข้อยกเว้นห้ามมิให้ฟ้องคดีภายใต้บทบัญญัตินี้ในกรณีที่ผู้กระทำความผิดเป็นองค์กรหรือเป็นลูกจ้างที่ปฏิบัติงานในทางการที่จ้างในองค์กรดังต่อไปนี้ (1) เว็บไซต์เครือข่ายสังคมออนไลน์เชิงพาณิชย์ (2) ผู้ให้บริการอินเทอร์เน็ต (3) ผู้ให้บริการระบบคอมพิวเตอร์แบบปฏิสัมพันธ์ ตามคำนิยามใน U.S.C มาตรา 230 (4) ผู้ให้บริการโทรคมนาคม ตามคำนิยามในมาตรา 51.002 แห่ง Utilities Code หรือ (6) ผู้ให้บริการวิดีโอหรือผู้ให้บริการเครือข่ายเคเบิล ตามคำนิยามในมาตรา 66.002 แห่ง Utilities Code[4]

(2) มลรัฐแคลิฟอร์เนีย

มาตรการทางกฎหมายที่มลรัฐแคลิฟอร์เนียใช้ดำเนินการกับคดีเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตคือการออกกฎหมายเฉพาะ โดยกำหนดเป็นความผิดฐานสวมรอยเป็นบุคคลอื่นผ่านทางอินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์ (Impersonation through Internet or Electronic Means) ไว้ในประมวลกฎหมายอาญา ลักษณะ 13 ความผิดต่อทรัพย์สิน หมวด 8 การปลอมตัวเป็นบุคคลอื่นและการฉ้อโกง (False Personation and Cheating) มาตรา 528.5 โดยกำหนดไว้ว่า ผู้ใดโดยรู้อยู่แล้วกระทำการสวมรอยเป็นบุคคลอื่นที่มีอยู่จริงอย่างน่าเชื่อถือผ่านทางเว็บไซต์บนเครือข่ายอินเทอร์เน็ตหรือโดยวิธีการทางอิเล็กทรอนิกส์อื่นใดโดยไม่มีอำนาจ และมีวัตถุประสงค์เพื่อประทุษร้าย ขู่ขวัญ ข่มขู่ให้หวาดกลัว หรือหลอกลวงฉ้อโกงผู้อื่น ผู้นั้นกระทำความผิดต่อสาธารณชน (Public Offense) และต้องได้รับโทษ[5]

---

[2] TEXAS PENAL CODE § 33.07 (a)

[3] TEXAS PENAL CODE § 33.07 (b)

[4] TEXAS PENAL CODE § 33.07 (e)

[5] CALIFORNIA PENAL CODE § 528.5 (a)

(3) มลรัฐนิวยอร์ก

มลรัฐนิวยอร์กกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดทางอาญาในกลุ่มเดียวกับการสวมรอยเป็นบุคคลอื่นในระดับที่สอง (Criminal Impersonation in the Second Degree) ดังปรากฏในประมวลกฎหมายอาญาแห่งมลรัฐนิวยอร์ก ส่วนที่ 3 ความผิดเฉพาะ ลักษณะ K ความผิดเกี่ยวกับการฉ้อโกง มาตรา 190.25 โดยกำหนดไว้ว่า ผู้ใดสวมรอยเป็นบุคคลอื่นผ่านการติดต่อสื่อสารทางเว็บไซต์บนเครือข่ายอินเทอร์เน็ต หรือวิธีการทางอิเล็กทรอนิกส์ ด้วยเจตนาเพื่อให้ได้มาซึ่งผลประโยชน์ หรือประทุษร้าย หรือหลอกลวงฉ้อโกงผู้อื่น หรืออาศัยวิธีการติดต่อสื่อสารดังกล่าวเพื่อแอบอ้างเป็นเจ้าหน้าที่รัฐเพื่อจูงใจให้ผู้อื่นยินยอมต่ออำนาจเช่นว่านั้น หรือแสดงออกภายใต้ความน่าเชื่อถือจากการแอบอ้างดังกล่าว ผู้นั้นมีความผิดฐานสวมรอยเป็นบุคคลอื่นในระดับที่สอง ถือเป็นความผิดลหุโทษระดับ A (Class A Misdemeanor)[6]

5.2.1.2 มาตรการทางกฎหมายทั่วไปที่นำมาปรับใช้กับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

จากการศึกษาถึงมาตรการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของสหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี ทำให้ทราบว่าทั้งสามประเทศไม่มีกฎหมายที่กำหนดให้การสวมรอยดังกล่าวเป็นความผิดทางอาญาไว้โดยตรงแต่อย่างใด อย่างไรก็ตาม การกระทำความผิดที่เกิดขึ้นอาจเกี่ยวข้องกับลักษณะการกระทำความผิดอื่นตามกฎหมายทั่วไปที่มีอยู่แล้ว ในกรณีเช่นนี้จึงอาจนำบทบัญญัติทางกฎหมายที่เกี่ยวข้องมาปรับใช้แก่กรณีได้ โดยต้องพิจารณาพฤติการณ์ประกอบการกระทำและพิจารณาว่าผู้เสียหายถูกละเมิดสิทธิด้านใดเป็นสำคัญ ในส่วนนี้ ผู้เขียนจะเปรียบเทียบแนวทางการนำกฎหมายทั่วไปมาปรับใช้แก่การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของสหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี โดยแบ่งตามลักษณะความผิดที่เกี่ยวข้อง ดังนี้

(1) ความผิดฐานฉ้อโกง

(ก) สหราชอาณาจักร

Fraud Act 2006 เป็นกฎหมายที่สามารถนำมาปรับใช้กับการนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้ในการสวมรอยเพื่อการฉ้อโกง เนื่องจากมีบทบัญญัติเกี่ยวกับสิ่งที่ใช้สำหรับการกระทำความผิดฐานฉ้อโกง ตามมาตรา 6 – 8 กล่าวคือ มาตรา 8 แห่งพระราชบัญญัตินี้กำหนดให้

[6] NEW YORK PENAL CODE § 190.25 (4)

คำว่า “สิ่ง” (Article) ตามที่ปรากฏในมาตรา 6 และมาตรา 7 หมายรวมถึง โปรแกรมหรือข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์ ดังนั้น การครอบครองหรือควบคุมสิ่งที่ใช้ในการฉ้อโกงตามมาตรา 6 และการสร้าง ดัดแปลง จัดหา หรือเสนอให้มีการจัดหาสิ่งที่ใช้ในการฉ้อโกงตามมาตรา 7 จึงครอบคลุมถึงการครอบครอง ควบคุม สร้าง ดัดแปลง จัดหา หรือเสนอให้มีการจัดหาโปรแกรมหรือข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์เพื่อนำมาใช้กระทำความผิดฐานฉ้อโกง ด้วยเหตุนี้ การสร้างตัวตนปลอมในนามของบุคคลอื่นบนระบบเครือข่ายอินเทอร์เน็ตโดยมีวัตถุประสงค์เพื่อฉ้อโกงจึงอาจเป็นความผิดตามมาตรา 6 – 8 แห่ง Fraud Act 2006 ได้

(ข) ประเทศญี่ปุ่น

ประมวลกฎหมายอาญาของประเทศญี่ปุ่นบัญญัติความผิดฐานฉ้อโกงทางคอมพิวเตอร์ (Computer-related Fraud) ไว้ในหมวด 37 มาตรา 246-2 ความว่า ผู้ใดได้มาหรือก่อให้บุคคลอื่นได้มาซึ่งผลประโยชน์โดยการสร้างระเบียนอิเล็กทรอนิกส์ (Electronic Records) ที่เกี่ยวกับการได้มา สูญเสีย หรือแก้ไขเปลี่ยนแปลงสิทธิในทรัพย์สินปลอม ด้วยการป้อนข้อมูลปลอมหรือป้อนคำสั่งโดยไม่ได้รับอนุญาตไปยังคอมพิวเตอร์ที่ใช้ในธุรกิจของผู้อื่น หรือใช้ระเบียนอิเล็กทรอนิกส์ที่เกี่ยวกับการได้มา สูญเสีย หรือแก้ไขเปลี่ยนแปลงสิทธิในทรัพย์สินปลอมเพื่อจัดการธุรกิจของผู้อื่น

(ค) สาธารณรัฐเกาหลี

ประมวลกฎหมายอาญาของสาธารณรัฐเกาหลีบัญญัติความผิดฐานฉ้อโกงทางคอมพิวเตอร์ (Fraud by Use of Computer, etc.) ไว้ในหมวด 39 ความผิดฐานฉ้อโกงและกรรโชกทรัพย์ มาตรา 347-2 ความว่า ผู้ใดได้มาซึ่งผลประโยชน์ทางทรัพย์สินหรือทำให้บุคคลที่สามได้ไปซึ่งผลประโยชน์ทางทรัพย์สิน โดยการสร้างข้อมูลที่เป็นการนำเข้าซึ่งข้อมูลสารสนเทศปลอมหรือคำสั่งที่ไม่เหมาะสม หรือนำเข้าหรือปรับเปลี่ยนข้อมูลโดยปราศจากอำนาจ ในหน่วยประมวลผลข้อมูล เช่น คอมพิวเตอร์ หรืออื่น ๆ

เมื่อพิจารณาฐานความผิดเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์ของประเทศญี่ปุ่นและสาธารณรัฐเกาหลีแล้วจะเห็นได้ว่า ในกรณีที่มีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตโดยมีวัตถุประสงค์เพื่อการฉ้อโกง ย่อมเป็นการใช้วิธีการทางคอมพิวเตอร์เพื่อให้ได้มาซึ่งผลประโยชน์จากผู้อื่น จึงสามารถนำความผิดฐานฉ้อโกงทางคอมพิวเตอร์มาปรับใช้แก่กรณีได้

(2) ความผิดเกี่ยวกับการใช้งานคอมพิวเตอร์และระบบสื่อสาร

(ก) สหราชอาณาจักร

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอาจเป็นความผิดต่อการใช้งานคอมพิวเตอร์และระบบสื่อสารได้หลายประการ ยกตัวอย่างเช่น

- ในกรณีที่ผู้สวมรอยได้ส่งข้อความซึ่งมีลักษณะหยาบคาย ล่วงละเมิด ข่มขู่ หรือเป็นความเท็จผ่านทางการสื่อสารในระบบอิเล็กทรอนิกส์ โดยมีเจตนาให้ผู้รับสารเกิดความทุกข์ร้อนหรือวิตกกังวล ถือเป็นความผิดตามมาตรา 1 แห่ง Malicious Communications Act 1988

- ในกรณีที่ผู้สวมรอยส่งข้อมูลที่มีลักษณะล่วงละเมิด ลามกอนาจาร หรือข่มขู่ให้หวาดกลัว หรือเพื่อก่อความรำคาญ ความไม่สะดวก ความวิตกกังวลแก่ผู้อื่น ผ่านทางระบบการสื่อสารอิเล็กทรอนิกส์สาธารณะ ถือเป็นความผิดฐานใช้งานเครือข่ายอิเล็กทรอนิกส์สาธารณะอย่างไม่เหมาะสม (Improper Use of Public Electronic Communications Network) ตามมาตรา 127 แห่ง Communications Act 2003

- ในกรณีที่มีการมีการสวมรอยเป็นบุคคลอื่นผ่านทางระบบเครือข่ายอินเทอร์เน็ตหรือใช้วิธีการทางอิเล็กทรอนิกส์โดยมีเจตนาจะกระทำความผิดอื่นหรือเพื่ออำนวยความสะดวกในการกระทำความผิดอื่น ถือว่าเป็นความผิดตามมาตรา 2 แห่ง Computer Misuse Act 1990

(ข) ประเทศญี่ปุ่น

ในบางครั้งก่อนที่จะมีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ผู้กระทำความผิดอาจดำเนินการบางอย่างต่อระบบคอมพิวเตอร์เพื่อให้ได้มาซึ่งสิ่งอำนวยความสะดวกในการสวมรอย เช่น ข้อมูลส่วนบุคคล บัญชีผู้ใช้งาน รหัสผ่าน เป็นต้น พระราชบัญญัติป้องกันการเข้าถึงคอมพิวเตอร์โดยไม่มีอำนาจ (Act on the Prohibition of Unauthorized Computer Access) ได้กำหนดให้การเข้าถึงระบบฐานข้อมูลโดยผิดกฎหมาย (Hacking) เป็นความผิดตามมาตรา 8 โดยแบ่งลักษณะการกระทำความผิดออกเป็น 3 ลักษณะ ดังนี้ (1) การเข้าถึงคอมพิวเตอร์ผ่านทางเครือข่ายสื่อสารทางไกลโดยปราศจากอำนาจ โดยใช้ชื่อบัญชีผู้ใช้งานและรหัสผ่านของผู้อื่น (2) การเข้าถึงคอมพิวเตอร์ผ่านเครือข่ายสื่อสารทางไกลโดยปราศจากอำนาจ โดยใช้ข้อมูลหรือคำสั่งที่สามารถหลบเลี่ยงการยับยั้งการเข้าถึงโดยฟังก์ชั่นควบคุมการเข้าถึง และ (3) การเข้าถึงคอมพิวเตอร์ผ่านเครือข่ายสื่อสารทางไกลโดยปราศจากอำนาจ โดยการโจมตีช่องว่างด้านความปลอดภัย

(ค) สาธารณรัฐเกาหลี

พระราชบัญญัติคุ้มครองข้อมูลและการใช้งานเครือข่ายสารสนเทศและการสื่อสาร (Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. หรือ IT Network Act) ได้บัญญัติเกี่ยวกับการใช้งานเครือข่ายสารสนเทศและการสื่อสารที่ละเมิดต่อชื่อเสียงของบุคคลอื่นไว้ในมาตรา 70 โดยกำหนดให้การทำให้ผู้อื่นเสื่อมเสียชื่อเสียงด้วยการยืนยันข้อเท็จจริง ไม่ว่าจะเป็นความจริงหรือความเท็จ อย่างเปิดเผยผ่านทางเครือข่ายสารสนเทศและการสื่อสาร โดยมีวัตถุประสงค์เพื่อกล่าวว่าร้ายผู้นั้น เป็นการกระทำความผิดฐานหมิ่นประมาท (Defamation) ดังนั้น ในกรณีที่มีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตและการสวมรอยนั้นทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง ย่อมถือว่าเป็นการหมิ่นประมาทผ่านทางเครือข่ายสารสนเทศและการสื่อสารตามมาตรานี้

(3) ความผิดเกี่ยวกับข้อมูลส่วนบุคคล

(ก) สหราชอาณาจักร

การสวมรอยเป็นบุคคลอื่นเกิดจากการนำข้อมูลส่วนบุคคลของผู้ถูกสวมรอยไปใช้แสดงให้ผู้อื่นทั่วไปเข้าใจว่าเป็นการแสดงข้อมูลโดยเจ้าของข้อมูลที่แท้จริง แต่ทว่าเจ้าของข้อมูลส่วนบุคคลที่ถูกสวมรอยไม่ได้ให้ความยินยอมต่อการนำข้อมูลส่วนบุคคลไปใช้เพื่อการนี้ ดังนั้น มาตรา 55 แห่ง Data Protection Act 1998 จึงเป็นบทบัญญัติที่ให้ความคุ้มครองมิให้มีการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบ โดยกำหนดว่า ผู้ใดได้มาหรือเปิดเผยข้อมูลส่วนบุคคลหรือรายละเอียดเกี่ยวกับข้อมูลส่วนบุคคล หรือจัดหาให้ได้มาซึ่งการเปิดเผยข้อมูลส่วนบุคคลของผู้อื่น โดยปราศจากความยินยอมของผู้รักษาข้อมูล ผู้นั้นมีความผิด

(ข) ประเทศญี่ปุ่น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Act on the Protection of Personal Information: APPI) มาตรา 57 – 58 ผู้ใดเป็นลูกจ้างหรืออดีตลูกจ้างของหน่วยงานรัฐหรือบุคคลหรือผู้ประกอบธุรกิจที่ได้รับมอบหมายหน้าที่จากหน่วยงานรัฐให้ดูแลข้อมูลส่วนบุคคล จัดหาข้อมูลส่วนบุคคลที่รักษาไว้เนื่องจากได้รับความนับถือตามหน้าที่การงานนั้นให้แก่บุคคลอื่น หรือจัดสรรข้อมูลนั้นเพื่อก่อให้เกิดประโยชน์ที่มิชอบด้วยกฎหมายแก่ตนเองหรือบุคคลที่สาม

(ค) สาธารณรัฐเกาหลี

ด้วยสาธารณรัฐเกาหลีมีนโยบายยืนยันตัวตนของผู้ใช้งานเว็บไซต์ โปรแกรมประยุกต์ หรือแพลตฟอร์มออนไลน์อื่นบนเครือข่ายอินเทอร์เน็ตด้วยหมายเลขประจำตัวผู้อยู่อาศัย

(Resident Registration Number) ในกรณีที่มีการสวมรอยเป็นบุคคลอื่นด้วยการนำหมายเลขประจำตัวผู้อยู่อาศัยดังกล่าวไปใช้โดยไม่ได้รับอนุญาต ถือเป็นความผิดตามมาตรา 37 แห่งพระราชบัญญัติว่าด้วยการจดทะเบียนหมายเลขประจำตัวผู้อยู่อาศัย (Resident Registration Act)

ตารางที่ 4 มาตรการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

ประเทศ / ประเด็น	สหรัฐอเมริกา			สหราชอาณาจักร	ประเทศญี่ปุ่น	สาธารณรัฐเกาหลี
	มลรัฐเทกซัส	มลรัฐแคลิฟอร์เนีย	มลรัฐนิวยอร์ก			
มาตรการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต	- มีกฎหมายเฉพาะโดยกำหนดเป็นฐานความผิดตาม Texas Penal Code § 33.07 - อยู่ในหมวดอาชญากรรมคอมพิวเตอร์ - แบ่งการกระทำความผิดออกเป็น 2 ระดับ คือ ความผิดอาญาอุกฉกรรจ์ และความผิดลหุโทษ	- มีกฎหมายเฉพาะโดยกำหนดเป็นฐานความผิดตาม California Penal Code § 528.5 - อยู่ในหมวดการปลอมตัวเป็นบุคคลอื่นและการฉ้อโกง (False Personation and Cheating)	- มีกฎหมายเฉพาะโดยกำหนดเป็นฐานความผิดตาม New York Penal Code § 190.25 (4) - เป็นความผิดในกลุ่มการสวมรอยเป็นบุคคลอื่นในระดับที่สอง (Criminal Impersonation in the Second Degree)	- ไม่มีกฎหมายเฉพาะ - ใช้ CPS Guidelines on Prosecuting Cases Involving Communication Sent via Social Media เป็นแนวทางในการดำเนินคดี - ความผิดฐานฉ้อโกง : Fraud Act 2006 - ความผิดเกี่ยวกับการใช้งานคอมพิวเตอร์และระบบสื่อสาร : Malicious Communications Act 1988, Communications Act 2003, Computer Misuse Act 1990 - ความผิดเกี่ยวกับข้อมูลส่วนบุคคล : Data Protection Act 1998	- ไม่มีกฎหมายเฉพาะ - ความผิดฐานฉ้อโกง : Penal Code มาตรา 246-2 ฐานฉ้อโกงทางคอมฯ - ความผิดเกี่ยวกับการใช้งานคอมพิวเตอร์และระบบสื่อสาร : Act on the Prohibition of Unauthorized Computer Access - ความผิดเกี่ยวกับข้อมูลส่วนบุคคล : Act on the Protection of Personal Information	- ไม่มีกฎหมายเฉพาะ - ความผิดฐานฉ้อโกง : Criminal Code มาตรา 347-2 ฐานฉ้อโกงทางคอมฯ - ความผิดเกี่ยวกับการใช้งานคอมพิวเตอร์และระบบสื่อสาร : IT Network Act - ความผิดเกี่ยวกับข้อมูลส่วนบุคคล : Resident Registration Act

จากตารางข้างต้น มลรัฐเทกซัส มลรัฐแคลิฟอร์เนีย และมลรัฐนิวยอร์กมีกฎหมายเฉพาะบัญญัติให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดทางอาญาฐานหนึ่ง โดยบัญญัติไว้ในประมวลกฎหมายอาญาของแต่ละมลรัฐ แต่มีความแตกต่างกันในรายละเอียดของหมวดหมู่ฐานความผิด กล่าวคือ มลรัฐเทกซัสบัญญัติฐานความผิดดังกล่าวไว้ในหมวดความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ มลรัฐแคลิฟอร์เนียบัญญัติไว้ในหมวดความผิดเกี่ยวกับการปลอมตัวเป็นบุคคลอื่นและการฉ้อโกง ส่วนมลรัฐนิวยอร์กบัญญัติไว้ในกลุ่มความผิดเกี่ยวกับการสวมรอยเป็นบุคคลอื่นอันเป็นความผิดอาญาระดับที่สอง

ในทางกลับกัน สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลีไม่มีกฎหมายเฉพาะที่บัญญัติให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นฐานความผิดอาญาแต่อย่างใด แต่เมื่อมีการสวมรอยดังกล่าวเกิดขึ้นจะนำกฎหมายอื่น ๆ ที่มีอยู่แล้วมาพิจารณาปรับใช้ให้เหมาะสมกับลักษณะการกระทำความผิด ด้วยเหตุนี้จึงมีกฎหมายที่เข้ามาเกี่ยวข้องกับการกระทำความผิดนี้เป็นจำนวนมาก ขึ้นอยู่กับแง่มุมในการพิจารณาของบุคคลที่เกี่ยวข้องกับการดำเนินคดีว่าควรนำกฎหมายฉบับใดมาใช้บังคับ อย่างไรก็ตาม ในกลุ่มประเทศที่ไม่มีกฎหมายเฉพาะทั้ง 3 ประเทศข้างต้น มีเพียงสหราชอาณาจักรที่มีการวางแนวทางในการพิจารณากฎหมายที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไว้อย่างชัดเจนเป็นลายลักษณ์อักษร ปรากฏตามคู่มือการฟ้องคดีที่เกี่ยวข้องกับการติดต่อสื่อสารที่ส่งผ่านทางสื่อสังคมออนไลน์ (CPS Guidelines on Prosecuting Cases Involving Communication Sent via Social Media)[7] ของสำนักงานอัยการ (Crown Prosecution Service: CPS)

ทั้งนี้ การจะพิจารณาว่าประเทศไทยควรมีมาตรการทางกฎหมายเพื่อดำเนินการป้องกันและปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอย่างไร จำต้องวิเคราะห์เปรียบเทียบข้อดีและข้อเสียระหว่างการกำหนดฐานความผิดเฉพาะกับการนำกฎหมายที่เกี่ยวข้องมาปรับใช้เสียก่อน ดังปรากฏตามตารางวิเคราะห์เปรียบเทียบต่อไปนี้

[7] Crown Prosecuting Service, "Guidelines on Prosecuting Cases Involving Communications Sent Via Social Media."

ตารางที่ 5 ข้อดีและข้อเสียระหว่างการบัญญัติฐานความผิดอาญาและการนำกฎหมายที่เกี่ยวข้องมาปรับใช้

ประเด็นข้อพิจารณา	การบัญญัติเป็นฐานความผิดอาญา	การนำกฎหมายที่เกี่ยวข้องมาปรับใช้
ข้อดี	1. สามารถกำหนดองค์ประกอบความผิดได้อย่างละเอียด ทำให้ทราบถึงลักษณะการกระทำความผิดและคุณธรรมทางกฎหมายได้อย่างชัดเจน 2. ทำให้การกระทำกลายเป็นความผิดอาญา ส่งผลให้ประชาชนเกิดความเกรงกลัว 3. คุ้มครองผู้เสียหายได้อย่างเหมาะสม ครอบคลุมถึงผู้ที่ถูกสวมรอยและผู้อื่นที่ได้รับความเสียหายจากการสวมรอย 4. สามารถกำหนดมาตรการบังคับที่ชัดเจนและเหมาะสมต่อความร้ายแรงที่เกิดขึ้น 5. มีความเป็นภาวะวิสัย (objective)	1. ไม่จำเป็นต้องบัญญัติฐานความผิดใหม่ เป็นการป้องกันไม่ให้เกิดภาวะกฎหมายอาญาเฟ้อ 2. สามารถปรับใช้กฎหมายที่เกี่ยวข้องได้หลากหลายเพื่อให้สมควรแก่คดีและความเสียหายที่เกิดขึ้น
ข้อเสีย	1. ไม่ครอบคลุมการกระทำความผิดรูปแบบใหม่ที่อาจเกิดขึ้นในอนาคต 2. อาจมีปัญหาเรื่องเขตอำนาจศาล	1. มีกฎหมายที่เกี่ยวข้องเป็นจำนวนมาก อาจยากต่อการพิจารณาปรับใช้กฎหมายให้เหมาะสมกับข้อเท็จจริง 2. กฎหมายบางฉบับอาจไม่สามารถแก้ไขปัญหาได้ตรงประเด็น 3. มีความเป็นอัตตวิสัย (subjective)

จากตารางข้างต้นจะเห็นได้ว่าการบัญญัติฐานความผิดอาญาและการนำกฎหมายที่เกี่ยวข้องมาปรับใช้ต่างก็มีทั้งข้อดีและข้อเสียแตกต่างกันไป ผู้เขียนจะวิเคราะห์ถึงความเหมาะสมของมาตรการทางกฎหมายที่สมควรนำมาใช้ในประเทศไทย ดังนี้

ประการแรก ด้วยกฎหมายอาญามีหลักประกันทางกฎหมาย ห้ามมิให้ใช้กฎหมายใกล้เคียงอย่างยิ่งลงโทษทางอาญาแก่บุคคล และกฎหมายอาญาต้องบัญญัติให้ชัดเจน เพื่อเป็นประกันให้บุคคลที่อยู่ภายใต้กฎหมายนั้นได้รับความคุ้มครองตามเจตนารมณ์ของกฎหมาย ประกอบกับหลักกฎหมายทั่วไปที่ว่า *"ไม่มีความผิด ไม่มีโทษ หากไม่มีกฎหมาย" (Nullum crimen nulla poena sine lege)* จึงยิ่งจำเป็นต้องบัญญัติให้การกระทำเป็นความผิดอาญาจึงจะลงโทษผู้กระทำผิดได้

นอกจากนี้ การที่ศาลนำบทบัญญัติฐานความผิดอื่นมาบังคับใช้แก่ผู้กระทำความผิด นอกจากจะเป็นการไม่ปฏิบัติตามหลักประกันในกฎหมายอาญาแล้ว ยังถือว่าศาลใช้อำนาจตุลาการเกินขอบเขตอีกประการหนึ่ง กล่าวคือ โดยหลักแล้วในการดำเนินคดีอาญา หากไม่ปรากฏว่ามีบทบัญญัติใดกำหนดให้การกระทำเป็นความผิดไว้อย่างชัดแจ้ง ศาลไม่อาจนำกฎหมายใกล้เคียงอย่างยิ่งมาปรับใช้เช่นเดียวกับคดีแพ่งได้

ในส่วนของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตนั้นมีคุณธรรมทางกฎหมาย คือ สิทธิในความเป็นตัวตน (Right to Identity) และสิทธิส่วนบุคคล (Right to Privacy) ผู้เสียหายโดยตรงจากการกระทำดังกล่าวได้แก่ ผู้ถูกสวมรอย ซึ่งการกระทำความผิดโดยอาศัยระบบคอมพิวเตอร์และอินเทอร์เน็ตเป็นเครื่องมือเช่นนี้เกิดขึ้นอย่างง่ายดาย ทำให้ผู้เสียหายได้รับผลกระทบและเกิดความเสียหายได้กว้างขวางและรุนแรงอย่างยิ่ง จึงสมควรต้องมีการกำหนดให้การกระทำเป็นความผิดอาญา เพื่อให้มีหลักประกันในการคุ้มครองคุณธรรมทางกฎหมายของผู้ถูกสวมรอยได้ตรงจุด ผู้ถูกสวมรอยสามารถดำเนินคดีในฐานความผิดดังกล่าวได้ในฐานะผู้เสียหายโดยตรง

ประการที่สอง การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไม่เพียงแต่สร้างความเสียหายแก่ผู้ที่ถูกนำข้อมูลส่วนบุคคลไปใช้แอบอ้างเท่านั้น แต่อาจกระทบต่อบุคคลอื่นที่เข้ามาเกี่ยวพันกับการสวมรอยได้เช่นกัน เช่น ผู้ที่ถูกหลอกลวงและสูญเสียสิทธิในทรัพย์ไป ผู้ที่ถูกทำให้เสื่อมเสียชื่อเสียง เป็นต้น อีกทั้งด้วยลักษณะการกระทำผิดดังกล่าวเองก็อาจตรงกับองค์ประกอบฐานความผิดอื่น ๆ ได้อีกมากมาย เช่น ความผิดฐานฉ้อโกงโดยอาศัยระบบคอมพิวเตอร์[8] ความผิดเกี่ยวกับการคุกคามผู้อื่นผ่านทางระบบสื่อสารอิเล็กทรอนิกส์[9] ความผิดเกี่ยวกับการทำให้ผู้อื่นเสื่อมเสียชื่อเสียงผ่านเครือข่ายสารสนเทศและการสื่อสาร[10] เป็นต้น การนำกฎหมายที่มีอยู่แล้วมาปรับใช้แก่กรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต อาจเกิดปัญหาจากการใช้ดุลพินิจของเจ้าหน้าที่ที่มีความเป็นอัตตวิสัย (Subjective)

---

[8] PENAL CODE ARTICLE ARTICLE 246-2

[9] COMMUNICATIONS ACT 2003 § 127

[10] ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND DATA PROTECTION, ETC. ARTICLE 7

ในกรณีนี้ ควรมีหลักเกณฑ์ที่ชัดเจนแน่นอนสำหรับใช้เป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่ในกระบวนการยุติธรรม ดังเช่นที่สหราชอาณาจักรมีคู่มือการฟ้องคดีที่เกี่ยวข้องกับการติดต่อสื่อสารที่ส่งผ่านทางสื่อสังคมออนไลน์ (CPS Guidelines on Prosecuting Cases Involving Communication Sent Via Social Media) ทำให้เจ้าหน้าที่มีแนวปฏิบัติที่ถูกต้องและชัดเจนเป็นมาตรฐานเดียวกัน ส่งผลให้การดำเนินงานเป็นไปด้วยความเรียบร้อย รวดเร็ว และมีประสิทธิภาพมากยิ่งขึ้น

5.2.2 การกำหนดมาตรการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทย

หลังจากวิเคราะห์เปรียบเทียบมาตรการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของต่างประเทศไปแล้วในหัวข้อที่ 5.2.1 ในส่วนนี้ ผู้เขียนจะวิเคราะห์ถึงการกำหนดมาตรการทางกฎหมายเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทย

เมื่อไม่กี่ปีที่ผ่านมา ประเทศไทยมีเหตุการณ์สวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเกิดขึ้นเป็นจำนวนมาก เช่น เหตุการณ์หนึ่งเจ้าพนักงานตำรวจได้จับกุมผู้กระทำผิดพร้อมตั้งข้อหาว่ากระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประกอบกับความผิดฐานหมิ่นประมาท[11] ซึ่งเป็นการแก้ไขปัญหาที่ไม่ตรงประเด็นเสียทีเดียว การสวมรอยเป็นบุคคลอื่นเช่นนี้ไม่อาจปรับเข้ากับความผิดฐานหมิ่นประมาทได้ทุกกรณี เพราะมีคุณธรรมทางกฎหมายที่ไม่เหมือนกัน สิทธิในความเป็นตัวตนและสิทธิส่วนบุคคลที่จะหวงกันไม่ให้ผู้ใดแทรกแซงความเป็นส่วนตัวของผู้ถูกสวมรอยได้ถูกล่วงละเมิด แต่ประเทศไทยยังไม่มีมาตรการทางกฎหมายที่ให้ความคุ้มครองคุณธรรมทางกฎหมายประการนี้โดยตรงแต่อย่างใด นอกจากนี้ การนำบทบัญญัติฐานความผิดอื่น ๆ มาปรับใช้ก็อาจสามารถให้ความคุ้มครองแก่ผู้เสียหายในความผิดฐานนั้นได้ แต่ผู้ถูกสวมรอยไม่ใช่ผู้เสียหายตามความผิดฐานนั้น จึงไม่ได้รับความคุ้มครอง เช่น กรณีการสวมรอยเป็นบุคคลอื่นเพื่อฉ้อโกง หากมีการดำเนินคดีในความผิดฐานฉ้อโกง ผู้ที่เป็นผู้เสียหายคือผู้ที่ถูกหลอกลวงและเสียสิทธิในทรัพย์ไป หาใช่ผู้ถูกสวมรอยไม่ การนำบทบัญญัติอื่นมาปรับใช้เช่นนี้เกรงว่าจะเป็นการขัดต่อหลักประกันในกฎหมายอาญา เนื่องจากกฎหมายอาญาต้องตีความโดยเคร่งครัดตามตัวอักษรและห้ามนำกฎหมายที่ใกล้เคียงกันมาลงโทษบุคคล

---

[11] ไอที 24 ชั่วโมง, "ถูกคนอื่นปลอมเป็นเราบน Facebook ทำให้เสียหาย แก้ไขอย่างไร?" [ออนไลน์].

การกำหนดมาตรการทางกฎหมายที่เหมาะสมจะส่งผลให้กระบวนการยุติธรรมทางอาญาเป็นไปด้วยความชอบธรรมและมีประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมมากยิ่งขึ้น หัวใจสำคัญของกฎหมายอาญาคือหลักกฎหมายทั่วไป *"Nullum crimen nulla poena sine lege"* หมายความว่า รัฐจะลงโทษบุคคลใดได้ก็ต่อเมื่อมีกฎหมายบัญญัติให้การกระทำนั้นเป็นความผิดและกำหนดบทลงโทษไว้ ด้วยเหตุนี้ ประเทศไทยจึงควรนำมาตรการทางกฎหมายของประเทศสหรัฐอเมริกามาใช้ โดยมีบทบัญญัติกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญา

อนึ่ง เนื่องด้วยการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการกระทำผิดที่มีลักษณะกรรมเดียวผิดกฎหมายหลายบท การกระทำผิดเพียงหนึ่งครั้งอาจเกี่ยวโยงไปถึงการกระทำความผิดฐานอื่น ๆ ได้อีกมากมาย การพิจารณาว่าจะนำบทบัญญัติแห่งกฎหมายใดมาปรับใช้อาจเกิดความสับสนขึ้นได้ ผู้เขียนจึงเห็นว่าประเทศไทยควรนำวิธีการปรับใช้กฎหมายแก่ข้อเท็จจริงของสหราชอาณาจักรมาปรับใช้ด้วยการจัดทำคู่มือแนวทางในการดำเนินคดีเกี่ยวกับการกระทำความผิดลักษณะนี้ รวมถึงลักษณะการกระทำความผิดอื่นที่เกิดขึ้นบนเครือข่ายอินเทอร์เน็ต เพื่อให้เจ้าหน้าที่ในกระบวนการยุติธรรมมีหลักเกณฑ์ในการพิจารณาข้อเท็จจริงที่เกิดขึ้นว่าควรปรับบทกฎหมายใดมาใช้ให้เหมาะสมและถูกต้อง และเพื่อให้มีแนวทางให้การดำเนินการทางกฎหมายเป็นระบบระเบียบ สามารถวิเคราะห์เหตุการณ์และดำเนินการสืบสวนสอบสวนได้อย่างรวดเร็ว ต่อเนื่อง และเป็นธรรม อันจะส่งให้กระบวนการยุติธรรมทางอาญามีประสิทธิภาพมากยิ่งขึ้น

จากหลักการและเหตุผลดังกล่าวข้างต้น ผู้เขียนเห็นควรให้ประเทศไทยกำหนดมาตรการทางกฎหมายดังต่อไปนี้

5.2.2.1 การกำหนดความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

ในปัจจุบันประเทศไทยมีกฎหมายที่เข้ามาเกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอยู่หลายฉบับ แต่กฎหมายเหล่านั้นไม่สามารถคุ้มครองผู้ถูกสวมรอยได้ทุกกรณี จึงสมควรมีบทบัญญัติกำหนดฐานความผิดดังกล่าวเป็นการเฉพาะ ทั้งนี้ เมื่อพิจารณาลักษณะการกระทำผิดจะเห็นได้ว่ามีสองส่วนหลักที่เกี่ยวข้อง ได้แก่ ประการแรก เป็นการกระทำผิดโดยใช้ระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือ และประการที่สอง เป็นการกระทำผิดต่อข้อมูลส่วนบุคคล ดังนั้น กฎหมายของประเทศไทยที่มีความใกล้เคียงอย่างยิ่งกับการกระทำดังกล่าวจึงได้แก่ มาตรา 14 (1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งแก้ไขเพิ่มเติมโดยมาตรา 8 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

อย่างไรก็ตาม เมื่อพิเคราะห์เหตุผลในการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้ว[12] ทำให้ทราบว่า พระราชบัญญัติดังกล่าวมีวัตถุประสงค์สำคัญในการป้องกันและปราบปรามการกระทำความผิดต่อระบบคอมพิวเตอร์หรือการกระทำที่ใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ ซึ่งเป็นการคุ้มครองความมั่นคงปลอดภัยของการใช้งานระบบคอมพิวเตอร์ เทคโนโลยีสารสนเทศและการสื่อสารของประเทศ ในขณะที่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มีเหตุผลและความจำเป็นในการเสนอร่างพระราชบัญญัติ[13] เน้นไปที่การคุ้มครองเจ้าของข้อมูลส่วนบุคคลจากความเสียหายที่เกิดจากการล่วงละเมิดข้อมูลส่วนบุคคล เช่น การนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์หรือเปิดเผยโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เพื่อประโยชน์ในทางการค้าจากการขายข้อมูลส่วนบุคคลนั้นโดยตรงหรือได้รับประโยชน์จากชื่อเสียงของเจ้าของข้อมูลส่วนบุคคล เป็นต้น จึงเห็นได้ว่า ควรกำหนดบทบัญญัติความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไว้ในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... จะมีความเหมาะสมมากที่สุด เพราะคุณธรรมทางกฎหมายของความผิดดังกล่าวประสงค์จะคุ้มครองสิทธิในความเป็นตัวตนและสิทธิส่วนบุคคล ซึ่งข้อมูลส่วนบุคคลถือเป็นหนึ่งในสิทธิส่วนบุคคล จึงสอดคล้องกับเจตนารมณ์ของร่างพระราชบัญญัติที่ประสงค์จะคุ้มครองข้อมูลส่วนบุคคลมิให้ถูกล่วงละเมิด

นอกจากนี้ เมื่อพิจารณาบทกำหนดโทษทางอาญาตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ฉบับเสนอสภานิติบัญญัติแห่งชาติ แล้วจะเห็นได้ว่า ร่างมาตรา 58 กำหนดลักษณะการกระทำผิดไว้อย่างกว้าง ๆ ไม่ได้ระบุเฉพาะเจาะจงว่าเป็นการกระทำต่อข้อมูลส่วนบุคคลในรูปแบบใด เป็นผลให้ไม่ว่าจะเป็นการกระทำเล็กน้อยหรือร้ายแรงเพียงใดก็จะมีระวางโทษเท่ากัน จึงไม่เป็นไปตามหลักความได้สัดส่วนกับความร้ายแรงในการกระทำผิด อีกทั้งการกระทำผิดตามร่างพระราชบัญญัติฉบับดังกล่าวไม่มีบทบัญญัติที่ระบุว่าให้เป็นความผิดอันยอมความได้ เท่ากับว่า

---

[12] เหตุผลในการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 “เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูลแก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพรข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้”

[13] สำนักงานคณะกรรมการกฤษฎีกา, “บันทึกวิเคราะห์สรุปสาระสำคัญของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เรื่องเสร็จที่ 515/2552,” (เอกสารไม่ตีพิมพ์เผยแพร่)

บทบัญญัติที่มีโทษทางอาญาในร่างพระราชบัญญัตินี้ล้วนเป็นความผิดต่อแผ่นดินทั้งสิ้น ทำให้รัฐต้องดำเนินคดีกับผู้กระทำผิดต่อไปแม้ว่าผู้เสียหายจะไม่ติดใจเอาความหรือดำเนินคดีแล้วก็ตาม[14]

อย่างไรก็ตาม เมื่อพิจารณาองค์ประกอบความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตประกอบกับลักษณะการกระทำความผิดที่อาจเกิดขึ้นในประเทศไทย โดยเทียบเคียงกับลักษณะการกระทำความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมาย ตามมาตรา 14 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับที่แก้ไขเพิ่มเติมแล้วนั้น จะเห็นได้ว่า การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตอาจเป็นไปได้ทั้งการสวมรอยเป็นบุคคลธรรมดาสามัญชนทั่วไป และอาจเป็นการสวมรอยเป็นบุคคลสำคัญซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของประเทศ ดังนั้น ผู้เขียนจึงเห็นควรให้แบ่งลักษณะการกระทำความผิดดังกล่าวออกเป็น 2 ลักษณะดังต่อไปนี้

(1) การสวมรอยเป็นบุคคลสำคัญซึ่งเป็นการสวมรอยที่อาจก่อให้เกิดความเสียหายแก่ประชาชน การรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือเป็นการสวมรอยที่กระทบต่อความมั่นคงแห่งราชอาณาจักร ลักษณะการสวมรอยเหล่านี้นอกจากจะส่งผลกระทบต่อผู้ที่ถูกสวมรอยโดยตรงแล้ว ยังกระทบต่อสังคมโดยรวมอีกด้วย รัฐจึงเข้ามาเป็นผู้เสียหายร่วมกับเอกชน ดังนั้นจึงสมควรกำหนดให้การกระทำเช่นนี้เป็นความผิดอาญาต่อแผ่นดิน เพื่อให้รัฐสามารถดำเนินคดีนำตัวผู้กระทำผิดมาลงโทษได้ อันจะเป็นการป้องกันความสงบสุขของสังคมโดยรวม[15]

(2) การสวมรอยเป็นบุคคลทั่วไปที่ไม่ได้กระทบต่อความมั่นคงปลอดภัยของประเทศ แม้ว่าจะการสวมรอยเช่นนี้เป็นการกระทำผิดผ่านทางเครือข่ายอินเทอร์เน็ตซึ่งอาจก่อให้เกิดความเสียหายได้รุนแรงกว่าการกระทำผิดแบบดั้งเดิม แต่อีกส่วนหนึ่งก็เป็นการกระทำผิดต่อสิทธิส่วนบุคคล ซึ่งถือเป็นคุณธรรมทางกฎหมายที่เป็นเรื่องส่วนบุคคลโดยแท้ ผู้เสียหายย่อมได้รับความเสียหายมากกว่ารัฐ สมควรมีบทบัญญัติฐานความผิดที่มุ่งประสงค์จะคุ้มครองผู้เสียหายอย่างแท้จริง อีกทั้งหากผู้เสียหายไม่ติดใจเอาความเสียแล้ว ผู้เสียหายย่อมมีสิทธิที่จะไม่ฟ้องร้องดำเนินคดี และรัฐไม่จำเป็นต้องเข้าไปดำเนินคดีกับผู้กระทำผิดอีกต่อไป ซึ่งเป็นไปตามกรอบความคิดในทางนิติบัญญัติเกี่ยวกับลักษณะของความผิดอันยอมความได้[16]

---

[14] จุฬารัตน์ ยะปะนัน, "ความผิดอาญาแผ่นดินและความผิดอันยอมความได้," จุลนิติ, 2 (2553): 151.

[15] เรื่องเดียวกัน, หน้า 151.

[16] คณิต ณ นคร, กฎหมายอาญาภาคทั่วไป, พิมพ์ครั้งที่ 3 (กรุงเทพมหานคร: วิญญูชน, 2551), หน้า 140.

ด้วยเหตุผลดังกล่าวมาข้างต้น ผู้เขียนจึงมีความเห็นว่า ควรกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญาโดยเฉพาะ โดยกำหนดให้เป็นความผิดอาญาต่อแผ่นดิน ในกรณีที่เป็นการสวมรอยโดยประการที่น่าจะเกิดความเสียหายต่อประชาชนการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือเป็นการสวมรอยที่กระทบต่อความมั่นคงแห่งราชอาณาจักร และกำหนดให้เป็นความผิดอันยอมความได้ ในกรณีที่เป็นการสวมรอยบุคคลใดบุคคลหนึ่งอันถือเป็นเรื่องส่วนบุคคลโดยแท้ เพื่อให้ประเทศไทยมีบทบัญญัติที่คุ้มครองผู้ถูกสวมรอยได้อย่างแท้จริง

ในส่วนของการบัญญัติฐานความผิดนั้น ผู้เขียนเห็นควรนำการบัญญัติความผิดฐาน Online Impersonation ของมลรัฐต่าง ๆ ในสหรัฐอเมริกามาเป็นแนวทาง ดังนี้

(1) ควรแบ่งลักษณะการกระทำความผิดออกเป็น 2 รูปแบบ กล่าวคือ รูปแบบแรก การสวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือผ่านทางเว็บไซต์อินเทอร์เน็ต โปรแกรมประยุกต์ หรือวิธีการทางอิเล็กทรอนิกส์อย่างอื่น และรูปแบบที่สอง การสวมรอยเป็นเจ้าหน้าที่รัฐหรือบุคคลอื่นโดยประการที่น่าจะก่อให้เกิดความเสียหายแก่ประชาชน การรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือเป็นการสวมรอยที่กระทบต่อความมั่นคงแห่งราชอาณาจักรผ่านทางเว็บไซต์อินเทอร์เน็ต โปรแกรมประยุกต์ หรือวิธีการทางอิเล็กทรอนิกส์อย่างอื่น เพื่อโน้มน้าวให้ผู้อื่นยอมต่ออำนาจเช่นว่านั้นหรือแสดงตนให้น่าเชื่อถือ เนื่องจากการกระทำทั้งสองรูปแบบนี้ก่อให้เกิดความเสียหายไม่เท่ากัน การสวมรอยเป็นเจ้าหน้าที่รัฐเพื่อโน้มน้าวจูงใจผู้อื่นให้เชื่อถือในบทบาทอำนาจหน้าที่ของเจ้าหน้าที่รัฐย่อมทำให้ผู้ที่พบเห็นหลงเชื่อและยินยอมต่อการหลอกลวงหรือข่มขู่คุกคามอย่างอื่นที่จะตามมาได้ง่ายกว่าการสวมรอยเป็นบุคคลธรรมดา รวมทั้งการสวมรอยที่กระทบต่อความมั่นคงปลอดภัยของประเทศย่อมสร้างความเสียหายต่อสังคมส่วนรวมได้มากกว่าเช่นกัน จึงควรมีการกำหนดมาตรการบังคับที่รุนแรงกว่ากรณีแรก

(2) ควรกำหนดองค์ประกอบความผิดให้ครอบคลุมและชัดเจน ประกอบด้วย ผู้กระทำ การกระทำ กรรมของการกระทำ เจตนาพิเศษ และพฤติการณ์ประกอบการกระทำ

(3) ควรกำหนดคำนิยามของถ้อยคำสำคัญเพื่อขยายความให้ผู้อ่านกฎหมายสามารถทำความเข้าใจได้อย่างถูกต้อง เพื่อป้องกันปัญหาที่เกิดจากการตีความบทบัญญัติ ตัวอย่างเช่น

- การสวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือ หมายความว่า การใช้ชื่อหรือข้อมูลแสดงอัตลักษณ์ส่วนบุคคลของผู้อื่นในการสวมรอยเป็นผู้นั้น และการสวมรอยเช่นว่านั้นมีเหตุอันสมควรให้ผู้อื่นเชื่อได้ว่าผู้กระทำผิดเป็นบุคคลที่ถูกสวมรอย

- วิธีการติดต่อสื่อสารทางอิเล็กทรอนิกส์ หมายความว่า การดำเนินการใด ๆ เพื่อรับส่งข้อมูลระหว่างผู้ส่งและผู้รับผ่านทางระบบอิเล็กทรอนิกส์ เช่น การเปิดใช้งานบัญชีจดหมายอิเล็กทรอนิกส์ การเปิดใช้งานบัญชีเว็บไซต์เครือข่ายสังคม การสร้างหน้าเว็บ การส่งข้อความในระบบสนทนาออนไลน์

- เว็บไซต์อินเทอร์เน็ต หมายความว่า เว็บไซต์เครือข่ายสังคม เว็บไซต์จดหมายอิเล็กทรอนิกส์ หรือเว็บไซต์อย่างอื่นที่ระบุให้ผู้ใช้งานกรอกข้อมูลส่วนบุคคลเพื่อเข้าถึงการใช้งานเว็บไซต์

(4) ควรกำหนดมาตรการบังคับทางอาญา รวมถึงมาตรการเยียวยาทางแพ่งให้เหมาะสมกับความร้ายแรงแห่งการกระทำ

5.2.2.2 การจัดทำคู่มือแนวทางการดำเนินคดี

ดังที่กล่าวมาแล้วข้างต้น การจัดทำคู่มือแนวทางสำหรับการดำเนินคดีเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตจะเป็นประโยชน์ต่อการปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้องในทุกกระบวนการของการดำเนินคดีอาญา รวมถึงเป็นแหล่งข้อมูลให้ประชาชนทั่วไปศึกษาถึงโทษทัณฑ์ของการกระทำผิดอันเป็นการยับยั้งมิให้เกิดการกระทำความผิดได้อีกทางหนึ่ง ในการนี้ผู้เขียนเห็นควรให้นำคู่มือการฟ้องคดีที่เกี่ยวข้องกับการติดต่อสื่อสารที่ส่งผ่านทางสื่อสังคมออนไลน์ (CPS Guidelines on Prosecuting Cases Involving Communication Sent Via Social Media) ของสำนักงานอัยการของสหราชอาณาจักร (CPS: Crown Prosecuting Service) มาเป็นแนวทางในการจัดทำคู่มือการดำเนินคดีที่เหมาะสมกับประเทศไทย ดังนี้

(1) ควรจำแนกลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตให้เป็นไปตามวัตถุประสงค์ในการกระทำความผิด เช่น สวมรอยเพื่อฉ้อโกง สวมรอยเพื่อข่มขู่คุกคาม สวมรอยเพื่อทำให้ผู้ถูกสวมรอยเสียชื่อเสียง หรือสวมรอยเป็นเจ้าหน้าที่รัฐเพื่อแสร้งใช้อำนาจโดยมิชอบ เป็นต้น ทั้งนี้ เพื่อเป็นหลักเกณฑ์เบื้องต้นในการพิจารณาว่าข้อเท็จจริงที่เกิดขึ้นตรงกับลักษณะการกระทำความผิดกลุ่มใด ทำให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถประเมินในเบื้องต้นได้ว่าสมควรนำบทบัญญัติแห่งกฎหมายฉบับใดบ้างมาใช้บังคับแก่กรณี

(2) ภายหลังจำแนกกลุ่มลักษณะการกระทำความผิดได้อย่างครอบคลุมแล้ว ควรระบุหลักเกณฑ์การพิจารณาปรับใช้กฎหมายในแต่ละกลุ่มไว้โดยละเอียด เพื่อให้ทราบว่าหากเกิด

การสวมรอยเป็นบุคคลอื่นในลักษณะเช่นนั้นแล้ว ต้องพิจารณานำบทบัญญัติแห่งกฎหมายใดมาปรับใช้จึงจะถูกต้องและเป็นธรรมมากที่สุด เช่น เมื่อเกิดการสวมรอยเป็นบุคคลอื่นเพื่อฉ้อโกง ให้พิจารณานำประมวลกฎหมายอาญา มาตรา 342 (1) ฐานฉ้อโกงโดยแสดงตนเป็นคนอื่น หรือมาตรา 343 วรรคสอง ฐานฉ้อโกงประชาชนโดยแสดงตนเป็นคนอื่น มาปรับใช้ เป็นต้น

(3) ควรกำหนดขั้นตอนและกระบวนการในการดำเนินคดีความผิดฐานดังกล่าวให้ชัดเจน ตั้งแต่ชั้นสืบสวนสอบสวนจนถึงการฟ้องคดี รวมทั้งข้อสังเกต ข้อควรระวัง และเทคนิคในการดำเนินคดี เพื่อใช้เป็นหลักเกณฑ์มาตรฐานในการปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้อง

5.3 การวิเคราะห์เปรียบเทียบมาตรการบังคับสำหรับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

5.3.1 การวิเคราะห์เปรียบเทียบมาตรการบังคับสำหรับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของต่างประเทศ

5.3.1.1 มาตรการบังคับกรณีเป็นความผิดเฉพาะ

(1) มลรัฐเทกซัส

ดังที่ได้กล่าวมาแล้วข้างต้น ความผิดฐาน Online Impersonation ตามประมวลกฎหมายอาญาแห่งมลรัฐเทกซัสแบ่งลักษณะการกระทำความผิดออกเป็น 2 ลักษณะ จึงมีการกำหนดมาตรการบังคับทางอาญาไว้ 2 รูปแบบเช่นกัน กล่าวคือ การกระทำความผิดตามอนุมาตรา (a) ถือเป็นความผิดอาญาอุกฉกรรจ์ระดับสาม (Felony of the Third Degree) ระวางโทษจำคุกในเรือนจำของกระทรวงกระบวนการยุติธรรมทางอาญาแห่งมลรัฐเทกซัส (Texas Department of Criminal Justice) เป็นระยะเวลาไม่น้อยกว่า 2 ปี แต่ไม่เกิน 10 ปี นอกจากโทษจำคุกแล้วผู้กระทำความผิดอาจต้องโทษปรับอีกไม่เกิน 10,000 ดอลลาร์สหรัฐ ตามมาตรา 33.07 ประกอบมาตรา 12.34

ส่วนการกระทำความผิดตามอนุมาตรา (b) ถือเป็นความผิดลหุโทษระดับ A (Class A Misdemeanor) ระวางโทษกักขังในคุก (Confinement in Jail) ไม่เกิน 1 ปี หรือปรับไม่เกิน 4,000 ดอลลาร์สหรัฐ หรือทั้งกักขังทั้งปรับ ตามมาตรา 33.07 ประกอบมาตรา 12.21 เว้นแต่เป็นการกระทำความผิดโดยมีเจตนาเพื่อเรียกร้องความสนใจจากเจ้าหน้าที่หน่วยฉุกเฉิน จะถือว่าเป็นความผิดอาญาอุกฉกรรจ์ระดับสาม

(2) มลรัฐแคลิฟอร์เนีย

ตามมาตรา 528.5 นั้น มลรัฐแคลิฟอร์เนียกำหนดมาตรการบังคับทางอาญาไว้ 2 ลักษณะ ผู้กระทำความผิดต้องระวางโทษจำคุกในคุกประจำท้องถิ่น (Imprisonment in a County Jail) ไม่เกิน 1 ปีหรือปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือทั้งจำทั้งปรับ แต่อย่างไรก็ตาม นอกจากบทบัญญัติดังกล่าวจะกำหนดโทษทางอาญาไว้แล้ว ยังสร้างทางเลือกในการเยียวยาทางแพ่งไว้ให้แก่ผู้เสียหายอีกด้วย ดังที่กำหนดไว้ในอนุมาตรา (e) ว่า นอกเหนือจากการเยียวยาทางแพ่งอื่นที่ผู้เสียหายสามารถร้องขอได้แล้ว ผู้ที่ได้รับความเสียหายหรือสูญเสียจากการล่วงละเมิดสวมรอยเป็นบุคคลอื่น อาจดำเนินคดีแพ่งเรียกร้องค่าสินไหมทดแทนความเสียหาย (Compensatory Damages) ยื่นคำร้องขอให้ศาลมีคำสั่งห้ามกระทำการชั่วคราว (Injunctive Relief) หรือคำสั่งให้ชดใช้ด้วยทางอื่นอย่างเป็นธรรม (Equitable Relief) ได้ตามสมควรแก่กรณี

3) มลรัฐนิวยอร์ก

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในมลรัฐนิวยอร์กถือเป็นความผิดลหุโทษระดับ A (Class A Misdemeanor) ซึ่งมีโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ เป็นไปตามประมวลกฎหมายอาญาแห่งมลรัฐนิวยอร์ก มาตรา 190.25 ประกอบมาตรา 70.15 และมาตรา 80.05

5.3.1.2 มาตรการบังคับกรณีเป็นความผิดทั่วไป

(1) ความผิดฐานฉ้อโกง

(ก) สหราชอาณาจักร

บุคคลที่กระทำความผิดตามมาตรา 6 แห่ง Fraud Act 2006 ฐานครอบครองหรือควบคุมสิ่งที่ใช้ในการฉ้อโกง หากศาลมีคำพิพากษาว่าเป็นความผิดโทษเบา จะต้องระวางโทษจำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินอัตราค่าปรับสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ หรือในกรณีที่เป็นความผิดอาญาโทษหนัก ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ ส่วนผู้ที่กระทำความผิดตามมาตรา 7 ฐานสร้างหรือจัดหาสิ่งที่ใช้สำหรับการฉ้อโกง ในกรณีที่ศาลพิพากษาให้เป็นความผิดอาญาโทษเบา ต้องระวางโทษจำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินอัตราค่าปรับสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ หรือในกรณีที่เป็นความผิดอาญาโทษหนักต้องระวางโทษจำคุกไม่เกิน 10 ปี หรือปรับ หรือทั้งจำทั้งปรับ

(ข) ประเทศญี่ปุ่น

ผู้กระทำความผิดตามมาตรา 246-2 ความผิดฐานฉ้อโกงทางคอมพิวเตอร์ (Computer-related Fraud) ต้องระวางโทษจำคุกพร้อมใช้แรงงานเป็นระยะเวลาไม่เกิน 10 ปี

(ค) สาธารณรัฐเกาหลี

ผู้กระทำความผิดตามมาตรา 347-2 ความผิดฐานฉ้อโกงทางคอมพิวเตอร์ (Fraud by Use of Computer, etc.) ต้องระวางโทษจำคุกไม่เกิน 10 ปี หรือปรับไม่เกิน 20 ล้านวอน

(2) ความผิดเกี่ยวกับการใช้งานคอมพิวเตอร์และระบบสื่อสาร

(ก) สหราชอาณาจักร

Malicious Communications Act 1988 มาตรา 1 (4) บัญญัติบทลงโทษไว้ 2 ประการ ได้แก่ ประการแรก อนุมาตรา (a) กำหนดถึงคำตัดสินลงโทษบนฐานของคำฟ้องคดีอาญาอุกฉกรรจ์ (Conviction on Indictment) ให้มีโทษจำคุกไม่เกิน 2 ปี หรือปรับ หรือทั้งจำทั้งปรับ ประการที่สอง อนุมาตรา (b) คำตัดสินลงโทษอย่างรวบรัด (Summary Conviction) ให้มีโทษจำคุกไม่เกิน 12 เดือน หรือปรับ หรือทั้งจำทั้งปรับ

Communications Act 2003 มาตรา 127 ผู้ใดมีความผิดตามมาตรานี้ ต้องถูกลงโทษตามคำตัดสินลงโทษอย่างรวบรัด (Summary Conviction) จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับที่ 5 ของมาตรฐานค่าปรับ หรือทั้งจำทั้งปรับ

Computer Misuse Act 1990 มาตรา 2 (5) แบ่งอัตราโทษตามพื้นที่ของประเทศในเครือสหราชอาณาจักรที่ถูกศาลตัดสินพิพากษาลงโทษ ดังนี้ ประเทศอังกฤษและประเทศเวลส์มีระวางโทษจำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินอัตราค่าปรับสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ ส่วนในประเทศสกอตแลนด์มีระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินอัตราค่าปรับสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ แต่หากเป็นกรณีที่เป็นความผิดอาญาอุกฉกรรจ์จะมีระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ

(ข) ประเทศญี่ปุ่น

พระราชบัญญัติป้องกันการเข้าถึงคอมพิวเตอร์โดยไม่มีอำนาจ (Act on the Prohibition of Unauthorized Computer Access) กำหนดให้ผู้กระทำความผิดฐานการเข้าถึงระบบฐานข้อมูลโดยผิดกฎหมาย (Hacking) ตามมาตรา 8 ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 200,000 เยน ส่วนผู้เสียหายสามารถดำเนินคดีทางแพ่งเรียกร้องค่าเสียหายได้

(ค) สาธารณรัฐเกาหลี

การกระทำความผิดฐานหมิ่นประมาทผ่านทางระบบเครือข่ายสารสนเทศและการสื่อสารตามมาตรา 70 แห่งพระราชบัญญัติคุ้มครองข้อมูลและการใช้งานเครือข่ายสารสนเทศและการสื่อสาร (Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.) มี 2 ลักษณะและมีบทกำหนดโทษที่แตกต่างกันค่อนข้างมาก กล่าวคือ ในกรณีที่เป็นการหมิ่นประมาทโดยกล่าวอ้างข้อเท็จจริงทั่วไป ต้องระวางโทษจำคุกธรรมดาหรือจำคุกพร้อมใช้แรงงานเป็นระยะเวลาไม่เกิน 3 ปี หรือปรับไม่เกิน 30 ล้านวอน ส่วนกรณีที่เป็นการหมิ่นประมาทโดยกล่าวอ้างข้อเท็จจริงที่เป็นความเท็จ ต้องระวางโทษจำคุกพร้อมใช้แรงงาน (Imprisonment with Prison Labor) ไม่เกิน 7 ปี หรือรอโดยมีข้อจำกัด (Suspension of Qualification) ไม่เกิน 10 ปี หรือปรับไม่เกิน 50 ล้านวอน

(3) ความผิดเกี่ยวกับข้อมูลส่วนบุคคล

(ก) สหราชอาณาจักร

การกระทำความผิดฐานได้มา เปิดเผย หรือจัดหาข้อมูลส่วนบุคคลโดยมิชอบตามมาตรา 55 แห่ง Data Protection Act 1998 นั้น มีการกำหนดมาตรการบังคับไว้ในมาตรา 60 ว่า ผู้ที่กระทำความผิดต้องระวางโทษปรับในอัตราสูงสุดไม่เกินที่กฎหมายกำหนด สำหรับคำตัดสินลงโทษแบบรวบรัด (Summary Conviction) หรือโทษปรับ สำหรับคำตัดสินในคดีอาญาอุกฉกรรจ์ (Conviction on Indictment)

(ข) ประเทศญี่ปุ่น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Act on the Protection of Personal Information: APPI) กำหนดให้ผู้กระทำความผิดต้องระวางโทษจำคุกพร้อมทำงานไม่เกิน 1 ปี หรือปรับไม่เกิน 500,000 เยน

(ค) สาธารณรัฐเกาหลี

พระราชบัญญัติว่าด้วยการจดทะเบียนหมายเลขประจำตัวผู้อยู่อาศัย (Resident Registration Act) มาตรา 37 กำหนดให้ผู้กระทำความผิดเกี่ยวกับการใช้หรือเปิดเผยหมายเลขประจำตัวผู้อยู่อาศัยโดยไม่ได้รับอนุญาต ให้มีโทษจำคุกพร้อมใช้แรงงาน (Imprisonment with Labor) เป็นระยะเวลาไม่เกิน 3 ปี หรือปรับไม่เกิน 10 ล้านวอน

ตารางที่ 6 มาตรการบังคับสำหรับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต

ประเทศ / ประเด็น	สหรัฐอเมริกา			สหราชอาณาจักร	ประเทศญี่ปุ่น	สาธารณรัฐเกาหลี
	มลรัฐเทกซัส	มลรัฐแคลิฟอร์เนีย	มลรัฐนิวยอร์ก			
มาตรการบังคับเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต	Texas Penal Code § 33.07 กำหนดดังนี้ (1) กรณีตาม (a) เป็นความผิดอาญาอุกฉกรรจ์ระดับสาม ระวางโทษจำคุกไม่น้อยกว่า 2 ปี แต่ไม่เกิน 10 ปี และอาจต้องโทษปรับอีกไม่เกิน 10,000 ดอลลาร์สหรัฐ (2) กรณีตาม (b) เป็นความผิดอุกฉกรรจ์ระดับ A ระวางโทษกักขังในคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 4,000 ดอลลาร์สหรัฐ หรือทั้งกักขังทั้งปรับ	California Penal Code § 528.5 กำหนดระวางโทษจำคุกในคุกประจำท้องถิ่น ไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือทั้งจำทั้งปรับ - ผู้เสียหายสามารถดำเนินคดีแพ่งเพื่อเรียกค่าสินไหมทดแทนความเสียหาย หรือยื่นคำร้องขอให้ศาลมีคำสั่งห้ามกระทำการชั่วคราว หรือคำสั่งให้ชดใช้ด้วยทางอื่นอย่างเป็นธรรม	New York Penal Code § 190.25 (4) กำหนดระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ	- ความผิดฐานฉ้อโกง : Fraud Act 2006 แบ่งเป็นความผิดโทษบาและความผิดโทษหนัก โดยกำหนดระวางโทษจำคุก/ปรับ/ทั้งจำทั้งปรับ - ความผิดเกี่ยวกับการใช้งานคอมพิวเตอร์และระบบสื่อสาร : มีทั้งคำตัดสินลงโทษแบบรวบรัดและคำตัดสินลงโทษคดีอาญาอุกฉกรรจ์ โดยกำหนดระวางโทษจำคุก/ปรับ/ทั้งจำทั้งปรับ - ความผิดเกี่ยวกับข้อมูลส่วนบุคคล : Data Protection Act 1998 มีทั้งคำตัดสินลงโทษแบบรวบรัดและคำตัดสินลงโทษคดีอาญาอุกฉกรรจ์ ระวางโทษปรับ	- ความผิดฐานฉ้อโกง : มาตรา 246-2 ฐานฉ้อโกงทางคอมฯ ระวางโทษจำคุกพร้อมใช้แรงงานเป็นระยะเวลาไม่เกิน 10 ปี - ความผิดเกี่ยวกับการใช้งานคอมพิวเตอร์และระบบสื่อสาร : ระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 500,000 เยน - ผู้เสียหายสามารถดำเนินคดีแพ่งเรียกค่าเสียหายได้ - ความผิดเกี่ยวกับข้อมูลส่วนบุคคล : ระวางโทษจำคุกพร้อมใช้แรงงานไม่เกิน 1 ปี หรือปรับไม่เกิน 500,000 เยน	- ความผิดฐานฉ้อโกง : มาตรา 347-2 ฐานฉ้อโกงทางคอมฯ ระวางโทษจำคุกไม่เกิน 10 ปี หรือปรับไม่เกิน 20 ล้านวอน - ความผิดเกี่ยวกับการใช้งานคอมพิวเตอร์และระบบสื่อสาร : ระวางโทษจำคุกต่ำสุดไม่เกิน 3 ปี สูงสุดไม่เกิน 10 ปี หรือปรับต่ำสุดไม่เกิน 30 ล้านวอน สูงสุดไม่เกิน 50 ล้านวอน - ความผิดเกี่ยวกับข้อมูลส่วนบุคคล : ระวางโทษจำคุกพร้อมใช้แรงงาน เป็นระยะเวลาไม่เกิน 3 ปี หรือปรับไม่เกิน 10 ล้านวอน

จากตารางข้างต้นจะเห็นได้ว่า มาตรการบังคับที่ต่างประเทศนำมาใช้มีทั้งมาตรการลงโทษทางอาญาและมาตรการเยียวยาทางแพ่ง กล่าวคือ สหรัฐอเมริกากำหนดวิธีการลงโทษสำหรับความผิดฐาน Online Impersonation ไว้ 2 วิธีการ ได้แก่ โทษจำคุกและโทษปรับ และกำหนดอัตราโทษเฉลี่ยอยู่ที่จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000 ดอลลาร์สหรัฐ หรือทั้งจำทั้งปรับ ส่วนสหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี มีการกำหนดวิธีการลงโทษสำหรับความผิดอื่นที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไว้ 2 วิธีการ ได้แก่ โทษจำคุกและโทษปรับ โดยมีข้อสังเกตว่าในกลุ่มความผิดฐานฉ้อโกงที่กระทำผ่านระบบคอมพิวเตอร์และกลุ่มความผิดเกี่ยวกับข้อมูลส่วนบุคคล ประเทศญี่ปุ่นและสาธารณรัฐเกาหลีจะกำหนดอัตราโทษปรับค่อนข้างสูงมาก แสดงให้เห็นว่า การกระทำความผิดลักษณะดังกล่าวมีความร้ายแรงและสร้างความเสียหายได้มากจึงจำเป็นต้องกำหนดอัตราโทษที่รุนแรงเพื่อเป็นการยับยั้งการกระทำผิด ทำให้บุคคลเกิดความเกรงกลัว ไม่กล้ากระทำผิด

นอกเหนือจากมาตรการลงโทษทางอาญาแล้ว บางประเทศได้กำหนดมาตรการเยียวยาทางแพ่งไว้เป็นช่องทางแก่ผู้เสียหายที่จะเรียกร้องให้ตนได้รับชดใช้ความเสียหาย รวมถึงการร้องขอให้ศาลมีคำสั่งอื่น ๆ ที่จะอำนวยความเป็นธรรมแก่ผู้เสียหายได้อีกด้วย

5.3.2 การกำหนดมาตรการบังคับสำหรับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทย

หลังจากวิเคราะห์เปรียบเทียบมาตรการบังคับสำหรับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของต่างประเทศไปแล้วในหัวข้อที่ 5.3.1 ในส่วนนี้ ผู้เขียนจะวิเคราะห์ถึงการกำหนดมาตรการบังคับสำหรับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของประเทศไทย

เมื่อเกิดการกระทำผิดขึ้นในสังคม นอกจากผู้กระทำผิดจะสร้างความเสียหายให้แก่ผู้เสียหายแล้ว ยังเป็นการทำลายความสงบเรียบร้อยและศีลธรรมอันดีของประชาชนและสังคมส่วนรวมด้วยอีกประการหนึ่ง[17] การนำมาตรการทางอาญามาบังคับใช้จึงเป็นไปเพื่อความปลอดภัยและความสงบสุขของสังคม เนื่องจากการลงโทษมีวัตถุประสงค์หลายประการ ไม่ว่าจะเป็นเพื่อแก้แค้นทดแทน เพื่อตัดผู้กระทำผิดออกจากสังคม เพื่อยับยั้งการกระทำความผิด เพื่อแก้ไขผู้กระทำผิด และเพื่อป้องกันอาชญากรรม เพราะฉะนั้นประเทศไทยจึงควรนำแนวทางมาตรการทางอาญาของต่างประเทศสำหรับการกระทำผิดกรณีสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตที่เหมาะสมมาปรับใช้ ดังนี้

---

[17] ประเทือง ธนิยผล, อาชญาวิทยาและทัณฑวิทยา, หน้า 134.

5.3.2.1 โทษจำคุก

การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตตามกฎหมายของสหรัฐอเมริกา รวมถึงกฎหมายเกี่ยวกับข้อมูลส่วนบุคคลของสหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี ล้วนแล้วแต่มีการกำหนดโทษจำคุกไว้ทั้งสิ้น เพื่อทำให้บุคคลในสังคมเกิดความเกรงกลัวอันจะเป็นการยับยั้งมิให้เกิดการกระทำความผิด แต่ทั้งนี้ มลรัฐเทกซัสมีการกำหนดอัตราโทษสำหรับการสวมรอยเป็นบุคคลอื่นไว้ 2 ระดับ กล่าวคือ การสวมรอยที่เข้าลักษณะเป็นความผิดอาญาอุกฉกรรจ์ให้ต้องได้รับโทษจำคุกเป็นระยะเวลานานกว่าการสวมรอยที่เข้าลักษณะเป็นความผิดลหุโทษ การจำแนกระดับความผิดและอัตราโทษเช่นนี้เป็นไปตามหลักความได้สัดส่วน เพราะผู้ที่กระทำความผิดที่สร้างความเสียหายหรือส่งผลกระทบต่อผู้อื่นมากกว่าก็สมควรได้รับโทษหนักกว่า เพราะฉะนั้น ผู้เขียนจึงเห็นควรให้ประเทศไทยนำแนวทางการกำหนดอัตราโทษจำคุกตามสัดส่วนความร้ายแรงแห่งการกระทำผิดมาปรับใช้ โดยกำหนดให้การสวมรอยเป็นเจ้าหน้าที่รัฐหรือการสวมรอยที่กระทบต่อความมั่นคงปลอดภัยของประเทศมีระวางโทษจำคุกเป็นระยะเวลานานกว่าการสวมรอยเป็นบุคคลธรรมดา เนื่องจากการสวมรอยดังกล่าวย่อมสร้างความน่าเชื่อถือและทำให้ประชาชนทั่วไปหลงเชื่อและยินยอมต่อการอำนาจที่เสแสร้งนั้นได้ง่ายกว่า และสร้างความเสียหายต่อความสงบสุขของสังคมโดยรวมได้มากกว่าอีกด้วย

5.3.2.2 โทษปรับ

กฎหมายของต่างประเทศมีการกำหนดโทษปรับสำหรับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตมาพร้อมกับโทษจำคุก ซึ่งผู้เขียนเห็นว่าประเทศไทยควรนำวิธีการลงโทษปรับมาใช้เช่นเดียวกัน เพราะโทษปรับสามารถใช้แทนโทษจำคุกระยะสั้นได้ ทำให้ผู้กระทำผิดที่ไม่ได้มีจิตใจชั่วร้ายหรือสันดานเป็นอาชญากรไม่ต้องเข้าคุก และสามารถกำหนดอัตราค่าปรับให้เหมาะสมกับผู้กระทำผิดแต่ละระดับชั้นได้[18] ทั้งนี้ การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการกระทำที่นำข้อมูลส่วนบุคคลไปใช้ในทางที่ผิดผ่านระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต ซึ่งสร้างความเสียหายได้มาก จึงจำต้องกำหนดอัตราค่าปรับให้สูงมากพอที่จะสามารถทดแทนความผิดแก่รัฐและทำให้ผู้อื่นเกิดความเกรงกลัวไม่กล้ากระทำความผิด นอกจากนี้ควรกำหนดโทษปรับสำหรับการสวมรอยเป็นเจ้าหน้าที่รัฐหรือการสวมรอยที่กระทบต่อความมั่นคงปลอดภัยของประเทศให้หนักกว่าการสวมรอยเป็นบุคคลธรรมดา เนื่องจากกรณีแรกสามารถก่อให้เกิดความเสียหายต่อส่วนรวมได้มากกว่าดังที่กล่าวมาแล้วข้างต้น

[18] เรื่องเดียวกัน, หน้า 154.

(3) มาตรการคุมประพฤติ

จากการศึกษาวิจัยพบว่า ในคดีสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตในสหรัฐอเมริกา ศาลเคยมีคำพิพากษาลงโทษปรับผู้กระทำผิดพร้อมกำหนดเงื่อนไขคุมประพฤติสำหรับผู้กระทำผิดที่ไม่เคยมีประวัติอาชญากรรมมาก่อน[19] ผู้เขียนเห็นว่าประเทศไทยควรนำมาตรการคุมประพฤติตามแบบอย่างของสหรัฐอเมริกามาปรับใช้ เนื่องจากการคุมประพฤติทำให้ผู้กระทำผิดมีโอกาสในการแก้ไขปรับปรุงตนเองโดยอาศัยอิทธิพลจากสังคมรอบข้าง ไม่ตัดอิสรภาพของผู้กระทำผิดในการประกอบอาชีพการงาน อีกทั้งยังเป็นการป้องกันมิให้เกิดการกระทำความผิดซ้ำอันจะส่งผลดีต่อการคุ้มครองปกป้องสังคมจากอาชญากรรมอีกทางหนึ่ง[20] ทั้งนี้ ควรกำหนดเงื่อนไขในการคุมประพฤติให้เหมาะสมกับลักษณะการกระทำของผู้กระทำผิดแต่ละราย เช่น กรณีสวมรอยเป็นบุคคลอื่นเพื่อคุกคามผู้เสียหาย ควรกำหนดเงื่อนไขให้ผู้กระทำผิดต้องอยู่ให้ห่างจากผู้เสียหาย หรือห้ามมิให้ผู้กระทำผิดเข้าถึงการใช้อินเทอร์เน็ตในระยะเวลาที่ถูกคุมประพฤติ[21] เป็นต้น

นอกเหนือจากมาตรการทางอาญาที่สมควรนำมาปรับใช้ดังกล่าวข้างต้น ประเทศไทยควรมีมาตรการเยียวยาทางแพ่ง (Civil Remedy) เพื่อบรรเทาความเดือดร้อน ความทุกข์ใจ และความเสียหายอันเกิดจากการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต เพราะผลกระทบที่เกิดขึ้นจากการสวมรอยนั้นไม่ใช่เพียงแต่ก่อความเสียหายต่อสิทธิส่วนบุคคลเท่านั้น แต่ยังกระทบต่อสภาพจิตใจ การดำเนินชีวิต ความปลอดภัยในชีวิตและร่างกาย ตลอดจนชื่อเสียงเกียรติคุณอีกด้วย ประเทศไทยจึงควรนำกฎหมายของสหรัฐอเมริกามาปรับใช้ โดยกำหนดให้ผู้เสียหายมีสิทธิได้รับการเยียวยาทางแพ่ง รวมถึงมีสิทธิร้องขอให้ศาลมีคำสั่งที่เป็นธรรมแก่ตนได้ ได้แก่ ค่าสินไหมทดแทนความเสียหาย (Compensatory Damages) ค่าเสียหายตามจริง (Actual Damages) ค่าเสียหายเชิงลงโทษ (Punitive Damages) คำสั่งห้ามกระทำการชั่วคราว (Injunctive Relief) คำสั่งให้ชดใช้ด้วยทางอื่นอย่างเป็นธรรม (Equitable Relief) คำสั่งแสดงสิทธิของโจทก์ (Declaratory Relief) รวมถึงค่าทนายความและค่าใช้จ่ายในการดาเนินคดี (Attorney’s Fee and Litigation Costs)

กล่าวโดยสรุป การนำแนวทางกำหนดมาตรการบังคับทั้งทางอาญาและแพ่งของต่างประเทศมาปรับใช้ให้เหมาะสมและสอดคล้องกับสภาวการณ์ของประเทศไทย จะช่วยให้ผู้คนในสังคมเกรงกลัวการกระทำผิด เป็นการยับยั้งมิให้เกิดการกระทำความผิดซ้ำ สามารถป้องกันและปราบปรามการสวม

---

[19] Clanton, K., "We Are Not Who We Pretend to Be: Odr Alternative to Online Impersonation Statues," Cardozo Journal of Conflict Resolution.

[20] ประเทือง ธนิยผล, อาชญาวิทยาและทัณฑวิทยา, หน้า 217-218.

[21] Without My Consent, "California Penal § 528.5 – Impersonation through Internet or Electronic Means."

รอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตที่เกิดขึ้นในประเทศไทย รวมทั้งสามารถให้ความคุ้มครองและชดใช้เยียวยาความเสียหายแก่ผู้เสียหายได้อย่างเป็นธรรมและมีประสิทธิภาพมากยิ่งขึ้น อันจะเป็นประโยชน์ต่อการรักษาความสงบสุขและศีลธรรมอันดีของประชาชนต่อไป

บทที่ 6
บทสรุปและข้อเสนอแนะ

จากสมมติฐานของวิทยานิพนธ์ที่ว่า “การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตก่อให้เกิดความเสียหายต่อผู้ถูกสวมรอยได้หลายด้าน แม้ว่าประเทศไทยจะมีกฎหมายที่สามารถปรับใช้เพื่อลงโทษผู้กระทำผิดได้ในบางกรณี แต่ยังไม่มีบทบัญญัติที่กำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญา รวมทั้งไม่มีการกำหนดมาตรการทางกฎหมายเพื่อให้ผู้เสียหายได้รับการคุ้มครองอย่างแท้จริง ด้วยเหตุนี้จึงสมควรมีมาตรการทางกฎหมายอาญาเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเพื่อประโยชน์ในการป้องกันและปราบปรามการกระทำผิดดังกล่าว” เมื่อได้ศึกษาวิจัยแล้วปรากฏว่า สมมติฐานที่ผู้เขียนตั้งไว้ในเบื้องต้นเป็นสิ่งที่ถูกต้อง เพราะมาตรการทางอาญาที่ประเทศไทยมีอยู่ในปัจจุบันยังไม่สามารถป้องกันและปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตได้อย่างมีประสิทธิภาพ ดังนั้น ผู้เขียนจะสรุปและเสนอแนะแนวทางการแก้ไขดังต่อไปนี้

6.1 บทสรุป

ด้วยความเจริญก้าวหน้าทางด้านเทคโนโลยีคอมพิวเตอร์และอินเทอร์เน็ตที่เพิ่มมากขึ้นอย่างไม่หยุดยั้ง ส่งผลให้ระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเข้ามามีบทบาทในชีวิตประจำวันของมนุษย์ยุคปัจจุบันเป็นอย่างมาก ผู้คนส่วนใหญ่มักใช้เทคโนโลยีดังกล่าวเป็นเครื่องมือในการดำเนินกิจกรรมต่าง ๆ มากมาย ทั้งที่เป็นกิจกรรมส่วนบุคคลและส่วนรวม ไม่ว่าจะเป็นการสร้างคุณประโยชน์ในด้านการเมือง เศรษฐกิจ สังคม การศึกษา การเกษตร ฯลฯ แต่ทว่าเหรียญมีสองด้านเสมอ ในทางกลับกัน ผู้ที่ไม่ประสงค์ดีก็ได้ใช้ช่องทางเทคโนโลยีดังกล่าวเพื่อแสวงหาผลประโยชน์โดยมิชอบหรือเพื่อก่ออาชญากรรมอื่น ๆ การกระทำความผิดโดยอาศัยระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือนั้นกระทบกระเทือนต่อสิทธิต่าง ๆ และสามารถสร้างความเสียหายที่แพร่กระจายเป็นวงกว้างยิ่งกว่าการกระทำความผิดรูปแบบเดิม สิทธิส่วนบุคคลเป็นหนึ่งในสิทธิที่ถูกล่วงละเมิดจากการกระทำความผิดผ่านระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตได้โดยง่าย การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการกระทำความผิดรูปแบบหนึ่งที่ผู้ไม่ประสงค์ดีได้ใช้ข้อมูลส่วนบุคคลและความเป็นตัวตนของบุคคลอื่นไปแอบอ้างเพื่อวัตถุประสงค์ที่ไม่ชอบด้วยกฎหมาย เช่น หลอกลวง ฉ้อโกง ประทุษร้าย ข่มขู่ คุกคาม เป็นต้น การกระทำเช่นนี้ถือว่าเป็นการล่วงละเมิดสิทธิในความเป็นตัวตนของบุคคล (Right to Identity) และสิทธิในความเป็นส่วนตัว (Right to Privacy)

ของบุคคลที่ไม่อาจถูกแทรกแซงได้ อีกทั้งยังก่อให้เกิดความเสียหายแก่ผู้ถูกสวมรอยและผู้เสียหายอื่นที่เข้ามาเกี่ยวข้องอีกด้วย

ประเทศไทยต้องประสบกับปัญหาการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเช่นเดียวกับประเทศอื่น ๆ ทั่วโลก สภาพปัญหาที่เกิดขึ้นในประเทศไทยโดยส่วนใหญ่มักเกี่ยวข้องกับการใช้งานเว็บไซต์หรือโปรแกรมประยุกต์ (Application) ที่ต้องใช้งานผ่านเครือข่ายอินเทอร์เน็ต เช่น เว็บไซต์เครือข่ายสังคม (Social Networking Sites) เว็บไซต์ธุรกรรมทางการเงิน เว็บไซต์ซื้อขายสินค้าออนไลน์ โปรแกรมประยุกต์สำหรับการสนทนาบนโทรศัพท์เคลื่อนที่ เป็นต้น การสวมรอยเป็นบุคคลอื่นผ่านช่องทางเหล่านี้ก่อให้เกิดความเสียหายต่อชื่อเสียงเกียรติคุณ ทรัพย์สิน และการดำเนินชีวิตในด้าน ต่าง ๆ ของทั้งผู้ถูกสวมรอยและผู้เสียหายอื่นที่เกี่ยวข้อง นอกจากนี้ยังถือเป็นการล่วงละเมิดสิทธิในความเป็นตัวตนและสิทธิในความเป็นส่วนตัวอย่างร้ายแรงอีกด้วย

จากสภาพปัญหาที่เกิดขึ้น ประเทศไทยยังไม่มีมาตรการทางกฎหมายอาญาเพื่อป้องกันและปราบปรามการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตโดยตรง หากแต่เมื่อเกิดการกระทำความผิดดังกล่าว เจ้าหน้าที่ในกระบวนการยุติธรรมทางอาญาจะนำบทบัญญัติที่เกี่ยวข้องมาปรับใช้แทน เช่น หากการสวมรอยเป็นบุคคลอื่นมีขึ้นเพื่อหลอกลวงให้ได้ไปซึ่งทรัพย์สินของผู้อื่น ถือเป็นการกระทำความผิดฐานฉ้อโกง เป็นต้น ทั้งนี้ จากการศึกษาวิจัย พบว่า การนำกฎหมายที่มีอยู่แล้วมาปรับใช้กับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตไม่สามารถปราบปรามการกระทำความผิดและคุ้มครองผู้เสียหายได้อย่างครอบคลุมเพียงพอ ดังนี้

(1) ความผิดฐานหมิ่นประมาทมีคุณธรรมทางกฎหมาย คือ เกียรติ แต่คุณธรรมทางกฎหมายที่ผู้ถูกสวมรอยถูกล่วงละเมิด คือ สิทธิในความเป็นตัวตนและสิทธิส่วนบุคคล อีกทั้งการสวมรอยเป็นบุคคลอื่นไม่ถือเป็นการใส่ความ ดังนั้นจึงไม่อาจนำความผิดฐานหมิ่นประมาทมาปรับใช้กับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตได้ชัดเจนนัก

(2) แม้ว่าจะมีการบัญญัติความผิดฐานฉ้อโกงโดยแสดงตนเป็นบุคคลอื่นไว้ก็ตาม แต่เนื่องจากคุณธรรมทางกฎหมายในความผิดฐานดังกล่าว คือ สิทธิในทรัพย์ และผู้เสียหายที่บทบัญญัตินี้ประสงค์จะคุ้มครอง คือ ผู้ที่ถูกหลอกลวงและสูญเสียสิทธิในทรัพย์ไป มิใช่ผู้ที่ถูกนำความเป็นตัวตนหรือข้อมูลส่วนบุคคลไปใช้แอบอ้างแต่อย่างใด ดังนั้น ในกรณีที่มีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตโดยมีเจตนาเพื่อฉ้อโกง ผู้ที่ถูกสวมรอยจึงไม่สามารถดำเนินการฟ้องคดีภายใต้ความผิดฐานฉ้อโกงได้

(3) การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการสร้างข้อมูลขึ้นในระบบคอมพิวเตอร์ให้แสดงผลผ่านทางหน้าจอของอุปกรณ์อิเล็กทรอนิกส์ และมีการส่งผ่านข้อมูลตาม

กลไกภายในระบบเครือข่ายอินเทอร์เน็ต แต่การกระทำเช่นนี้หาใช่การสร้างเอกสารไม่ เพราะมีลักษณะและคุณสมบัติไม่ตรงตามคำนิยามของเอกสารตามประมวลกฎหมายอาญา ดังนั้น การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตจึงไม่เป็นความผิดฐานปลอมเอกสาร

(4) ตามมาตรา 14 (1) แห่งพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับที่แก้ไขเพิ่มเติม นั้น ในระยะแรกเริ่ม บทบัญญัตินี้มีวัตถุประสงค์เพื่ออุดช่องว่างของความผิดฐานปลอมแปลงเอกสารตามประมวลกฎหมายอาญา แต่กลับถูกนำมาปรับใช้กับการหมิ่นประมาทในระบบออนไลน์เสียเป็นส่วนใหญ่ การปรับใช้เช่นนี้ถือว่าขัดต่อเจตนารมณ์ของกฎหมาย แม้ต่อมาได้มีการแก้ไขปรับปรุงมาตรา 14 (1) ด้วยการเพิ่มเติมองค์ประกอบความผิดในส่วนของเจตนาพิเศษ ได้แก่ “โดยทุจริตหรือโดยหลอกลวง” แต่บทบัญญัตินี้ยังคงมุ่งคุ้มครองประโยชน์สาธารณะเป็นหลักมากกว่าสิทธิส่วนบุคคล ดังนั้น ผู้เขียนจึงเห็นว่าไม่อาจนำมาตรา 14 (1) มาปรับใช้กับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตได้อย่างครอบคลุมนัก เพราะการกระทำผิดดังกล่าวกระทบกระเทือนต่อสิทธิส่วนบุคคลเป็นสำคัญ อีกทั้งเจตนาพิเศษของการสวมรอยเป็นบุคคลอื่นยังรวมไปถึงเพื่อการประทุษร้าย คุกคาม หรือข่มขู่ให้หวาดกลัวอีกด้วย

(5) ตามร่างมาตรา 58 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ฉบับที่เสนอต่อสภานิติบัญญัติแห่งชาตินั้น ได้กำหนดความผิดและโทษอาญาแก่ผู้ที่กระทำการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย หรือเพื่อให้ผู้อื่นเสียหาย และหากเป็นการเผยแพร่ข้อมูลส่วนบุคคลผ่านทางสื่ออิเล็กทรอนิกส์จะต้องระวางโทษหนักกว่าเดิมเกือบเท่าตัว ผู้เขียนมีความเห็นว่า การยกร่างบทบัญญัติเช่นนี้เป็นการกำหนดความผิดที่กว้างเกินไป อีกทั้งยังไม่มีการกำหนดให้มีการกระทำที่เป็นความผิดอันยอมความได้ ทั้งที่จริงแล้วการกระทำผิดต่อข้อมูลส่วนบุคคลในบางกรณีอาจไม่กระทบหรือส่งผลเสียหายต่อรัฐอย่างชัดเจนนัก หากแต่เป็นการล่วงละเมิดคุณธรรมทางกฎหมายที่เป็นส่วนตัวของผู้เสียหายโดยแท้เสียมากกว่า

เมื่อศึกษาวิจัยกฎหมายที่เกี่ยวข้องกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตของต่างประเทศ ทำให้ทราบว่าแต่ละประเทศต่างประสบกับปัญหาการกระทำผิดนี้เช่นเดียวกัน เป็นเหตุให้ต้องมีมาตรการทางอาญาสำหรับป้องกันและปราบปรามปัญหาที่เกิดขึ้น ทั้งนี้ สหรัฐอเมริกาเป็นเพียงประเทศเดียวที่มีบทบัญญัติในกฎหมายระดับมลรัฐกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญา ในขณะที่สหราชอาณาจักร ประเทศญี่ปุ่น และสาธารณรัฐเกาหลี ไม่มีบทบัญญัติทางกฎหมายเป็นการเฉพาะ แต่ได้นำกฎหมายอื่นที่เกี่ยวข้องมาปรับใช้เป็นกรณีไป มาตรการทางกฎหมายเหล่านี้เกิดขึ้นจากพื้นฐานของประชาชนในแต่ละประเทศซึ่งแตกต่างกัน ไม่ว่าจะเป็นด้านแนวความคิด เศรษฐกิจ และวัฒนธรรม ผู้เขียนจึงเห็นควรวิเคราะห์มาตรการทางกฎหมายของต่างประเทศเพื่อพิจารณานำแนวคิดและหลักการที่เหมาะสมมาปรับใช้กับประเทศไทย ดังนี้

(1) ลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตปรากฏอย่างชัดเจนที่สุดในบทบัญญัติฐานความผิดที่เรียกว่า Online Impersonation ตามประมวลกฎหมายอาญาระดับมลรัฐในสหรัฐอเมริกา โดยระบุถึงองค์ประกอบความผิดไว้อย่างครบถ้วน ได้แก่ ผู้กระทำ ลักษณะหรือรูปแบบการกระทำ กรรมของการกระทำ เจตนาพิเศษ พฤติการณ์ประกอบการกระทำ และคำนิยามของถ้อยคำที่สำคัญ การกำหนดรายละเอียดของการกระทำผิดไว้อย่างชัดแจ้งเช่นนี้เป็นประโยชน์ต่อการพิจารณาว่าการกระทำใดเข้าข่ายเป็นการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตหรือไม่ ด้วยเหตุนี้ ประเทศไทยจึงควรนำรายละเอียดของลักษณะการกระทำความผิดฐาน Online Impersonation มาเป็นแนวทางในการกำหนดมาตรการทางกฎหมายที่ครอบคลุมและเหมาะสมกับการกระทำผิดที่เกิดขึ้น

(2) มาตรการทางกฎหมายของต่างประเทศแบ่งออกเป็น 2 ลักษณะ ได้แก่ การกำหนดให้การกระทำผิดเป็นความผิดอาญา และการนำกฎหมายอื่นที่เกี่ยวข้องมาปรับใช้ ในส่วนนี้ประเทศไทยควรกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญาเช่นเดียวกันกับสหรัฐอเมริกา เพื่อทำให้ผู้ถูกสวมรอยได้รับความคุ้มครองสิทธิในความเป็นตัวตนและสิทธิส่วนบุคคลอันไม่อาจล่วงละเมิดได้อย่างแท้จริง นอกจากนี้ ในกรณีที่การสวมรอยเป็นบุคคลอื่นเกี่ยวข้องกับการกระทำความผิดอื่น เป็นเหตุให้มีผู้เสียหายนอกเหนือจากผู้ถูกสวมรอยและทำให้มีกฎหมายหลายฉบับเข้ามาเกี่ยวข้อง ประเทศไทยจึงควรนำแนวทางการจัดทำคู่มือการดำเนินคดีเกี่ยวกับลักษณะความผิดดังกล่าวตามแบบอย่างของสหราชอาณาจักรมาปรับใช้ เพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องมีหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการดำเนินการทางกฎหมายต่อไป

(3) บทบัญญัติความผิดฐาน Online Impersonation ของมลรัฐต่าง ๆ ในสหรัฐอเมริกามีการกำหนดมาตรการบังคับไว้ทั้งทางอาญาและแพ่ง มาตรการบังคับทางอาญา ได้แก่ โทษจำคุก โทษปรับ และการคุมประพฤติ ส่วนมาตรการบังคับทางแพ่งจะช่วยบรรเทาความเสียหายที่เกิดขึ้นและสร้างเกราะคุ้มครองผู้เสียหายอย่างเป็นธรรม เช่น สิทธิในการเรียกค่าสินไหมทดแทนความเสียหาย (Compensatory Damages) ค่าเสียหายเชิงลงโทษ (Punitive Damages) หรือยื่นคำร้องต่อศาลให้มีคำสั่งห้ามกระทำการชั่วคราว (Injunctive Relief) คำสั่งให้ชดใช้ด้วยทางอื่นอย่างเป็นธรรม (Equitable Relief) เป็นต้น ประเทศไทยจึงควรนำแนวทางมาตรการบังคับของสหรัฐอเมริกามาปรับใช้ เพื่อลงโทษผู้กระทำผิดและคุ้มครองเยียวยาผู้เสียหาย

หากประเทศไทยกำหนดลักษณะการกระทำความผิดไว้อย่างชัดเจน รวมทั้งมีมาตรการทางกฎหมายและมาตรการบังคับที่เหมาะสม จะช่วยให้ประเทศไทยมีหลักเกณฑ์ในการดำเนินคดีเกี่ยวกับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตที่มีประสิทธิภาพ และก่อให้เกิดประสิทธิผลในการป้องกันและปราบปรามการกระทำผิด รวมทั้งสามารถคุ้มครองผู้เสียหายได้เป็นอย่างดียิ่ง

6.2 ข้อเสนอแนะ

จากบทสรุปที่ผู้เขียนอธิบายไปข้างต้น จะเห็นได้ว่า ประเทศไทยยังไม่มีมาตรการทางกฎหมายที่เหมาะสมและครอบคลุมสำหรับการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ในหัวข้อนี้ ผู้เขียนจะนำเสนอข้อเสนอแนะเพื่อเป็นแนวทางให้ประเทศไทยมีมาตรการทางกฎหมายที่สามารถป้องกันและปราบปรามการกระทำผิดดังกล่าว และคุ้มครองผู้เสียหายได้อย่างมีประสิทธิภาพ ดังนี้

6.2.1 ขอเสนอให้ประเทศไทยกำหนดลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตให้ชัดเจน ซึ่งประกอบไปด้วย ผู้กระทำ ลักษณะหรือรูปแบบการกระทำ กรรมของการกระทำ เจตนาพิเศษ พฤติการณ์ประกอบการกระทำ และคำนิยามของถ้อยคำ ที่สำคัญ โดยกำหนดให้มีรายละเอียดที่ชัดเจนและครอบคลุมเพียงพอที่จะทำให้ทราบถึงคุณธรรมทางกฎหมายอันเป็นเจตนารมณ์เบื้องหลังที่กฎหมายประสงค์จะคุ้มครองตามแนวทางดังต่อไปนี้

(1) ผู้กระทำ ได้แก่ ผู้ที่กระทำโดยรู้อยู่แล้วว่าการกระทำนั้นเป็นการสวมรอยเป็นบุคคลอื่น และได้กระทำไปโดยไม่ได้รับความยินยอมจากผู้ถูกสวมรอย

(2) การกระทำ จำแนกออกเป็น 3 รูปแบบตามความเสียหายและระดับผลกระทบที่อาจเกิดขึ้น ได้แก่ รูปแบบที่หนึ่ง การสวมรอยเป็นบุคคลอื่นอย่างน่าเชื่อถือผ่านทางเว็บไซต์อินเทอร์เน็ต โปรแกรมประยุกต์ หรือวิธีการทางอิเล็กทรอนิกส์อย่างอื่น และรูปแบบที่สอง การสวมรอยเป็นเจ้าหน้าที่รัฐผ่านทางเว็บไซต์อินเทอร์เน็ต โปรแกรมประยุกต์ หรือวิธีการทางอิเล็กทรอนิกส์อย่างอื่น เพื่อโน้มน้าวให้ผู้อื่นยอมต่ออำนาจเช่นว่านั้นหรือแสดงตนให้น่าเชื่อถือ และรูปแบบที่ 3 การสวมรอยเป็นบุคคลอื่นโดยประการที่น่าจะก่อให้เกิดความเสียหายแก่ประชาชน การรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือเป็นการสวมรอยที่กระทบต่อความมั่นคงแห่งราชอาณาจักร

การกระทำที่ถือว่าเป็นการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเกิดขึ้นจากการนำชื่อหรือข้อมูลแสดงอัตลักษณ์ส่วนบุคคลของผู้อื่นไปใช้แอบอ้างสวมรอยเป็นผู้นั้นโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ซึ่งการสวมรอยต้องมีลักษณะเป็นที่น่าเชื่อถือ (Credibly Impersonate) กล่าวคือ มีเหตุอันสมควรให้ผู้อื่นหลงเชื่อว่าผู้กระทำผิดเป็นบุคคลที่ถูกสวมรอยตัวจริง อีกทั้งการสวมรอยต้องเกิดขึ้นผ่านการใช้งานเว็บไซต์ โปรแกรมซอฟต์แวร์ โปรแกรมประยุกต์ หรือแพลตฟอร์มอย่างอื่นที่เชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ต เช่น การสร้างหน้าเว็บ (Web Pages) การสร้างโพรไฟล์บนเว็บไซต์หรือโปรแกรมประยุกต์ในกลุ่มเครือข่ายสังคมออนไลน์ (Social

Networking Sites) การส่งจดหมายอิเล็กทรอนิกส์ ข้อความด่วน หรือข้อความตัวอักษร การใช้งานห้องสนทนา (Chat Room) การใช้งานกระดานสนทนาออนไลน์ (Online Web Board) เป็นต้น

(3) กรรมของการกระทำ ได้แก่ ข้อมูลส่วนบุคคลที่ใช้ระบุตัวตนของผู้ถูกสวมรอย (Identifying Information) เช่น ชื่อนามสกุล วันเกิด รูปภาพประเภทภาพนิ่งและภาพเคลื่อนไหววีดิทัศน์ หมายเลขประจำตัว หมายเลขบัญชีผู้ใช้งานอื่น ๆ ที่อยู่อาศัย ที่อยู่จดหมายอิเล็กทรอนิกส์ หมายเลขโทรศัพท์ ประวัติการศึกษา ข้อมูลทางการแพทย์ ประวัติอาชญากร เป็นต้น ซึ่งถือเป็นสิทธิส่วนบุคคลอย่างหนึ่งที่ต้องได้รับความคุ้มครองตามกฎหมาย

(4) เจตนาพิเศษ ควรกำหนดเจตนาพิเศษของการกระทำความผิดดังกล่าวให้ครอบคลุมวัตถุประสงค์ของการสวมรอยเป็นบุคคลอื่นที่อาจเกิดขึ้น ได้แก่ เพื่อประทุษร้าย (Harm) เพื่อหลอกลวง (Defraud) เพื่อขู่เข็ญหรือข่มขู่ให้หวาดกลัว (Intimidate or Threaten) เพื่อให้ได้มาซึ่งผลประโยชน์ (Obtain a benefit) เพื่อคุกคาม รังควาน หรือก่อความรำคาญ (Harass)

นอกจากนี้ การกำหนดลักษณะการกระทำความผิดควรใช้ถ้อยคำที่กระชับ รัดกุม ประชาชนทั่วไปสามารถอ่านและเข้าใจได้ตรงกัน มิให้เกิดปัญหาในการตีความตัวบทกฎหมาย เพื่อประโยชน์ในการนำไปกำหนดไว้ในฐานความผิดต่อไป

6.2.2 ขอเสนอให้ประเทศไทยกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญา โดยกำหนดให้เป็นความผิดอาญาต่อแผ่นดินสำหรับกรณีการสวมรอยเป็นเจ้าหน้าที่รัฐหรือบุคคลใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อประชาชนหรือส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือเป็นการสวมรอยที่กระทบต่อความมั่นคงแห่งราชอาณาจักร รวมทั้งกำหนดให้เป็นความผิดอันยอมความได้สำหรับกรณีการสวมรอยเป็นบุคคลธรรมดาทั่วไป เพื่อให้ได้ฐานความผิดที่มีคุณธรรมทางกฎหมาย คือ สิทธิในความเป็นตัวตนและสิทธิส่วนบุคคล ผู้ที่ถูกล่วงละเมิดสิทธิดังกล่าวจากการถูกนำความเป็นตัวตนหรือข้อมูลส่วนบุคคลไปใช้ในทางมิชอบโดยปราศจากความยินยอมผ่านทางเครือข่ายอินเทอร์เน็ตจะได้รับความคุ้มครองให้มีฐานะเป็นผู้เสียหายตามกฎหมายอาญา และสามารถดำเนินคดีกับผู้กระทำผิดได้

ทั้งนี้ เห็นควรแก้ไขเพิ่มเติมฐานความผิดดังกล่าวไว้ในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เนื่องจากร่างพระราชบัญญัติดังกล่าวมีเจตนารมณ์ในการตราขึ้นเพื่อแก้ไขเยียวยาความเสียหายที่เกิดจากการล่วงละเมิดสิทธิในข้อมูลส่วนบุคคลเป็นหลัก จึงสอดคล้องกับวัตถุประสงค์ของคุณธรรมทางกฎหมายในความผิดฐานดังกล่าวที่ต้องการคุ้มครองสิทธิส่วนบุคคลของเจ้าของข้อมูลที่ถูกนำไปใช้เพื่อสวมรอย

6.2.3 ขอเสนอให้มีการจัดทำคู่มือแนวทางการดำเนินงานในคดีสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต โดยกำหนดรายละเอียดเกี่ยวกับคำนิยาม ลักษณะการกระทำความผิด มาตรการทางกฎหมาย แนวทางการพิจารณาการปรับใช้กฎหมายอื่น ๆ ที่เกี่ยวข้อง ตลอดจนขั้นตอนการดำเนินการทางกฎหมายของเจ้าหน้าที่ในกระบวนการยุติธรรม ตามแนวทางดังต่อไปนี้

(1) ควรจำแนกลักษณะการกระทำความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตออกเป็นกลุ่ม ๆ ตามวัตถุประสงค์ในการกระทำความผิด เพื่อเป็นหลักเกณฑ์เบื้องต้นในการพิจารณาว่าข้อเท็จจริงที่เกิดขึ้นตรงกับลักษณะการกระทำความผิดกลุ่มใด ทำให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถประเมินในเบื้องต้นได้ว่าสมควรนำบทบัญญัติแห่งกฎหมายฉบับใดบ้างมาใช้บังคับแก่กรณี

(2) ควรระบุหลักเกณฑ์การพิจารณาปรับใช้กฎหมายในแต่ละกลุ่มไว้โดยละเอียด เพื่อให้ทราบว่าหากเกิดการสวมรอยเป็นบุคคลอื่นในลักษณะเช่นนั้นแล้ว ต้องพิจารณานำบทบัญญัติแห่งกฎหมายใดมาปรับใช้จึงจะถูกต้องและชอบธรรม

(3) ควรกำหนดขั้นตอนและกระบวนการในการดำเนินคดีความผิดฐานดังกล่าวให้ชัดเจน ตั้งแต่ชั้นสืบสวนสอบสวนจนถึงการฟ้องคดี รวมทั้งข้อสังเกต ข้อควรระวัง และเทคนิคในการดำเนินคดี เพื่อใช้เป็นหลักเกณฑ์มาตรฐานในการปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้อง

พร้อมกันนี้ ควรเผยแพร่คู่มือดังกล่าวให้สาธารณชนรับทราบ เพื่อให้เจ้าพนักงานตำรวจ พนักงานอัยการ ศาล เจ้าหน้าที่ในกระบวนการยุติธรรมอื่น ๆ ตลอดจนประชาชนได้รับทราบมาตรการทางกฎหมายและขั้นตอนการดำเนินคดีความผิดฐานสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต อีกทั้งเพื่อให้เจ้าหน้าที่มีหลักเกณฑ์และแนวทางการพิจารณาดำเนินการที่ชัดเจนและเป็นมาตรฐานเดียวกัน

6.2.4 ขอเสนอให้ประเทศไทยกำหนดมาตรการบังคับทางอาญาและทางแพ่งเท่าที่จำเป็นตามสมควรแก่ความร้ายแรงของการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ต ในส่วนของมาตรการบังคับทางอาญา ขอเสนอให้ใช้วิธีการลงโทษจำคุกและโทษปรับ โดยกำหนดอัตราโทษสำหรับการสวมรอยเป็นเจ้าหน้าที่รัฐหรือบุคคลใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อประชาชนหรือส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือเป็นการสวมรอยที่กระทบต่อความมั่นคงแห่งราชอาณาจักร ให้หนักกว่าการสวมรอยเป็นบุคคลธรรมดาทั่วไป เพราะการสวมรอยในกรณีแรกนั้นอาศัยอำนาจและความน่าเชื่อถือของตำแหน่งหน้าที่มาจูงใจให้ผู้อื่นหลงเชื่อในการสวมรอย หรือเป็นการสวมรอยที่กระทบต่อความมั่นคงปลอดภัยของประเทศหรือความมั่นคงแห่ง

ราชอาณาจักร จึงมีแนวโน้มที่จะเกิดความเสียหายและส่งผลกระทบต่อส่วนรวมได้มากกว่า จึงควรกำหนดอัตราโทษหนักกว่าตามหลักความได้สัดส่วน ทั้งนี้ การกำหนดบทลงโทษที่สมควรแก่ความร้ายแรงนี้เป็นไปเพื่อลงโทษผู้กระทำผิดให้เกิดความหลาบจำ และทำให้ผู้อื่นเกิดความเกรงกลัว ซึ่งถือเป็นการยับยั้งมิให้เกิดการกระทำผิดขึ้นในอนาคต รวมทั้งขอเสนอให้มีการคุมประพฤติ เพื่อให้ผู้กระทำผิดมีโอกาสได้เรียนรู้ที่จะแก้ไขปรับปรุงตนเอง มิให้เกิดการกระทำความผิดซ้ำ โดยควรกำหนดเงื่อนไขการคุมประพฤติให้เหมาะสมกับผู้กระทำผิดแต่ละราย เช่น ให้ผู้กระทำผิดต้องจ่ายค่าชดเชยแก่ผู้เสียหาย ห้ามผู้กระทำผิดไม่ให้เข้าไปยุ่งเกี่ยวกับผู้เสียหาย ห้ามเข้าถึงการใช้งานอินเทอร์เน็ตในระหว่างถูกคุมประพฤติ หรือทำงานบริการสังคม เป็นต้น

ในส่วนของมาตรการบังคับทางแพ่ง ขอเสนอให้กำหนดทางเลือกสำหรับการเยียวยาบรรเทาความเสียหายทางแพ่ง อันได้แก่ สิทธิของผู้เสียหายในการเรียกร้องค่าสินไหมทดแทนความเสียหาย (Compensatory Damages) ค่าเสียหายตามจริง (Actual Damages) ค่าเสียหายเชิงลงโทษ (Punitive Damages) หรือสิทธิในการขอให้ศาลมีคำสั่งห้ามจำเลยกระทำการชั่วคราว (Injunctive Relief) คำสั่งให้ชดใช้ด้วยทางอื่นอย่างเป็นธรรม (Equitable Relief) คำสั่งแสดงสิทธิของโจทก์ (Declaratory Relief) รวมถึงให้ผู้เสียหายมีสิทธิได้รับค่าทนายความและค่าใช้จ่ายในการดำเนินคดี (Attorney's Fee and Litigation Costs) จากจำเลยคืนภายหลังคดีถึงที่สุด

หลังจากศึกษาวิจัยเกี่ยวกับมาตรการทางอาญากรณีการสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตจนสิ้นสุดแล้ว สามารถสรุปใจความสำคัญได้ว่า การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นการกระทำผิดต่อสิทธิในความเป็นตัวตน (Right to Identity) และสิทธิส่วนบุคคล (Right to Privacy) ของผู้ถูกสวมรอย อีกทั้งยังก่อให้เกิดความเสียหายต่อผู้ถูกสวมรอยและบุคคลอื่นที่เข้ามาเกี่ยวข้องอีกหลายแง่มุม การนำหลักการทางกฎหมายอาญาเข้ามาพิจารณาเพื่อค้นหามาตรการทางกฎหมายที่เหมาะสมสำหรับการป้องกันและปราบปรามการกระทำผิดดังกล่าวทำให้ทราบว่า การกำหนดให้การสวมรอยเป็นบุคคลอื่นบนเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญาและกำหนดมาตรการบังคับทางอาญาที่เหมาะสมจะช่วยจัดการปัญหาที่เกิดขึ้นได้ แต่อย่างไรก็ตาม แม้ว่ารัฐจะบัญญัติกฎหมายหรือมีมาตรการทางกฎหมายที่ดีเพียงใด หากขาดความร่วมมือจากประชาชนและบุคลากรในทุกภาคส่วนของสังคม กฎหมายหรือมาตรการทางกฎหมายเหล่านั้นก็ไม่อาจบรรลุผลสัมฤทธิ์อย่างที่ควรจะเป็นได้ ดังนั้น นอกเหนือจากการกำหนดแนวนโยบายทางอาญาที่มีประสิทธิภาพในการปราบปรามผู้กระทำผิดแล้ว ทุกคนในสังคมควรมีจิตสำนึกที่ดีและมีความเกรงกลัวต่อกฎหมายอันจะเป็นการยับยั้งมิให้เกิดการกระทำความผิด ซึ่งถือเป็นหลักการสำคัญในการป้องกันอาชญากรรมนั่นเอง

รายการอ้างอิง

ภาษาไทย

หนังสือ

เกียรติขจร วัจนะสวัสดิ์. คำอธิบายกฎหมายอาญา ภาค 1. พิมพ์ครั้งที่ 10. กรุงเทพมหานคร: พลสยาม พริ้นติ้ง (ประเทศไทย), 2551.

ไกรฤกษ์ เกษมสันต์. คำอธิบายประมวลกฎหมายอาญา มาตรา 288-มาตรา 366. พิมพ์ครั้งที่ 6. กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2553.

คณพล จันทน์หอม. รากฐานกฎหมายอาญา. กรุงเทพมหานคร: วิญญูชน, 2558.

คณิต ณ นคร. กฎหมายอาญาภาคความผิด. พิมพ์ครั้งที่ 11. กรุงเทพมหานคร: วิญญูชน, 2559.

———. กฎหมายอาญาภาคทั่วไป. พิมพ์ครั้งที่ 3. กรุงเทพมหานคร: วิญญูชน, 2551.

———. กฎหมายอาญาภาคทั่วไป. พิมพ์ครั้งที่ 4. กรุงเทพมหานคร: วิญญูชน, 2554.

———. วิ.อาญาวิพากษ์. กรุงเทพมหานคร: วิญญูชน, 2552.

จิตติ ติงศภัทิย์. กฎหมายอาญาภาค 2 ตอน 2 และภาค 3. กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2545.

ถาวร โพธิ์ทอง. พจนานุกรมกฎหมายและศัพท์ที่เกี่ยวข้อง อังกฤษ-ไทย. พิมพ์ครั้งที่ 3. กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2550.

ทวีพร คุ้มเมธา. รายงานพลเมืองเน็ต 2556 = Thai Netizen's Report 2013. กรุงเทพมหานคร: เครือข่ายพลเมืองเน็ต, 2557.

ธานิศ เกศวพิทักษ์. คำอธิบายประมวลกฎหมายวิธีพิจารณาความอาญา ภาค 1-2 (มาตรา 1-156). พิมพ์ครั้งที่ 10. กรุงเทพมหานคร: กรุงสยาม พับลิชชิ่ง, 2556.

นคร เสรีรักษ์. การคุ้มครองข้อมูลส่วนบุคคล : ข้อเสนอสำหรับประเทศไทย. กรุงเทพมหานคร: ฟ้าฮ่าม, 2558.

———. ความเป็นส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย. กรุงเทพมหานคร: ฟ้าฮ่าม, 2557.

ประเทือง ธนิยผล. อาชญาวิทยาและทัณฑวิทยา. กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยรามคำแหง, 2556.

พงษ์ธร สำราญ. สิทธิส่วนบุคคลกับเทคโนโลยี Gps. กรุงเทพมหานคร: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2552.

พนิดา พานิชกุล. จริยธรรมทางเทคโนโลยีสารสนเทศ (Ethics in Information Technology). กรุงเทพมหานคร: เคทีพี คอมพ์ แอนด์ คอนซัลท์, 2553.

มานิตย์ จุมปา. คำอธิบายกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์. กรุงเทพมหานคร: วิญญูชน, 2553.

สมศักดิ์ เอี่ยมพลับใหญ่. กฎหมายอาญาภาคความผิดเกี่ยวกับความเท็จ การปลอมและการแปลง. กรุงเทพมหานคร: นิติธรรม, 2554.

สราวุธ ปิติยาศักดิ์. กฎหมายเทคโนโลยีสารสนเทศ = Information Technology Law. กรุงเทพมหานคร: นิติธรรม, 2555.

สาวิตรี สุขศรี, ศิริพล กุศลศิลป์วุฒิและอรพิณ ยิ่งยงพัฒนา. อาชญากรรมคอมพิวเตอร์? : งานวิจัยหัวข้อ “ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น. กรุงเทพมหานคร: โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw) ในมูลนิธิอาสาสมัครเพื่อสังคม, 2555.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงเทคโนโลยีและการสื่อสาร. ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์. กรุงเทพมหานคร: 2557.

สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. แนวทางการจัดทำกฎหมายอาชญากรรมคอมพิวเตอร์. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, 2547.

สุเนติ คงเทพ. คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์. กรุงเทพมหานคร: กรุงสยาม พับลิชชิ่ง, 2559.

สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. คำอธิบายความผิดเกี่ยวกับการปลอมและการแปลงตามประมวลกฎหมายอาญา. กรุงเทพมหานคร: วิญญูชน, 2555.

อภิรัตน์ เพ็ชรศิริ. ทฤษฎีอาญา. พิมพ์ครั้งที่ 3. กรุงเทพมหานคร: วิญญูชน, 2556.

อัจฉรียา ชูตินันทน์. อาชญาวิทยาและทัณฑวิทยา. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: วิญญูชน, 2557.

อุทัย อาทิเวช. คู่มือกฎหมายวิธีพิจารณาความอาญา เล่ม 2 สิทธิของผู้เสียหายในคดีอาญา. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: วี.เจ.พริ้นติ้ง, 2555.

วารสาร

จุฬารัตน์ ยะปะนัน. ความผิดอาญาแผ่นดินและความผิดอันยอมความได้. จุลนิติ, 2 (2553).

วิทยานิพนธ์

ฐาปนีย์ รติจารุภัทร. การกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งเป็นเอกลักษณ์บุคคล. ปริญญานิติศาสตรมหาบัณฑิต, สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2555.

นรินทร์ จุ่มศรี. มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลจากการใช้บริการเครือข่ายสังคมออนไลน์. นิติศาสตมหาบัณฑิต, คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์. 2555.

พรทิพย์ ตัณฑวนันท์. อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์. วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. 2548.

รัฐสิทธิ์ คุรุสุวรรณ. ความหมายทางอาญาของคำว่า “เอกสาร”. วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2534.

สื่ออิเล็กทรอนิกส์

Foh9. การปลอมแปลงระบบหรือข้อมูลและการสวมรอยเป็นบุคคลอื่น [ออนไลน์]. 2555. แหล่งที่มา: http://foh9.blogspot.com/2012/04/blog-post.html [เข้าถึงเมื่อ 25 มกราคม 2557]

Mookook. เตือนภัยเฟสบุคเงินด่วนทันใจ อย่าได้หลงกลเป็นเหยื่อ [ออนไลน์]. 2558. แหล่งที่มา: http://pantip.com/topic/31691770 [เข้าถึงเมื่อ 26 กุมภาพันธ์ 2558]

MThai News. จับสาวแสบ! สวมรอยเป็นดาวจุฬา หลอกตุ๋นเงิน-ขายมือถือทางเฟสบุ๊ค [ออนไลน์]. แหล่งที่มา: http://news.mthai.com/hot-news/general-news/96450.html [เข้าถึงเมื่อ 26 กุมภาพันธ์ 2558]

SpokedarkTV. มือดีสวมรอยอั้ม พัชราภา ป่วนปลอมไลน์หลอกทำธุรกรรมทางการเงิน [ออนไลน์]. 2558. แหล่งที่มา: http://stars.spokedark.tv/2015/02/19/fake-line/#.VO9BRPmsWSo [เข้าถึงเมื่อ 26 กุมภาพันธ์ 2558]

ข่าวสด. หนุ่ม คงกระพัน ควงภรรยาโร่แจ้งกองปราบฯ ถูกแอบอ้างสวมรอยเป็นเมียหลอกขายสินค้าผ่านเฟซบุ๊ก [ออนไลน์]. 2558. แหล่งที่มา: http://www.khaosod.co.th/view_newsonline.php?newsid=TVRRd016RTFOVEkyTVE9PQ== [เข้าถึงเมื่อ 9 ธันวาคม 2558]

เดลินิวส์. โน้สอุดมถูกปลอมเฟสบุ๊ก แถมขู่กรรโชกทรัพย์ [ออนไลน์]. 2558. แหล่งที่มา: http://www.dailynews.co.th/Content/crime/ [เข้าถึงเมื่อ 26 กุมภาพันธ์ 2558]

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ. คำถามที่พบบ่อย [ออนไลน์]. แหล่งที่มา: http://www.nrca.go.th/faq.html [เข้าถึงเมื่อ 19 มิถุนายน 2560]

ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์. พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14(1) ยาแรงผิดขนานสำหรับการหมิ่นประมาทออนไลน์ [ออนไลน์]. 2557. แหล่งที่มา: https://freedom.ilaw.or.th/blog/ [เข้าถึงเมื่อ 9 พฤศจิกายน 2557]

———. ศศิวิมล : โพสต์ข้อความบนเฟซบุ๊ก [ออนไลน์]. แหล่งที่มา: https://freedom.ilaw.or.th/case/681#progress_of_case [เข้าถึงเมื่อ 13 ธันวาคม 2559]

ไอที 24 ชั่วโมง. ถูกคนอื่นปลอมเป็นเราบน Facebook ทำให้เสียหาย แก้ไขอย่างไร? [ออนไลน์]. 2557. แหล่งที่มา: http://www.it24hrs.com/2013/how-to-report-facebook-profile-fake/ [เข้าถึงเมื่อ 9 ธันวาคม 2557]

———. ผู้ใช้เน็ตระวัง หลังสาวน้อยโดนแอบอ้าง ถูกใช้ภาพมาตัดต่อ แชร์ Facebook โยงการเมือง [ออนไลน์]. 2558. แหล่งที่มา: http://stars.spokedark.tv/2015/02/19/fake-line/#.VO9BRPmsWSo [เข้าถึงเมื่อ 26 กุมภาพันธ์ 2558]

ภาษาอังกฤษ

หนังสือ

Bainbridge, D. I. Computer and the Law. Great Britain: 1973.

Micheal, J. Privacy and Human Rights : An International and Comparative Study, with Special Reference to Development in Information Technology. Aldershot, Hants: Dartmouth, 1994.

Robinson, N.และคณะ. Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime : Final Report. 2011.

Tsuchiya, M. Cyber Security in East Asia Japan and the 2009 Attacks on South Korea and the United States. In Edited by Andreasson, K. J., Cybersecurity Public Sector Treats and Responses. United States of America: CRC Press, 2012.

วารสาร

Clanton, K. We Are Not Who We Pretend to Be: Odr Alternative to Online Impersonation Statues. Cardozo Journal of Conflict Resolution 16 (2014).

Cox, C. Protecting Victims of Cyberstalking, Cyberharassment, and Online Impersonation through Prosectutions and Effective Laws. Jurimetrics Journal 54 (2014).

Ensour, H. S. Online Impersonation a Case Study in the Hashemite Kingdom of Jordan. International Journal of Engineering & Computer Science IJECS-IJENS 13, 05 (2013).

Gardiner, G. The Purpose of Criminal Punishment. The Modern Law Review 21, 3 (1958): 211-235.

Koch, C. M. To Catch a Catfish: A Statutory Solution for Victims of Online Impersonation. University of Colorado Law Review 88 (2017).

Reznik, M. Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation. Touro Law Review 29 (2013).

สื่ออิเล็กทรอนิกส์

AllClear ID. Online Impersonation Vs. Identity Theft: Is There a Difference? [Online]. Available from: https://www.allclearid.com/personal/2012/12/online-impersonatin-vs-identity-theft/ [9 November 2014. 17 December 2012]

Binational Working Group on Cross-Border Mass Marketing Fraud. Report on Phishing [Online]. 2006. Available from: https://www.justice.gov/sites/default/files/opa/legacy/2006/11/21/report_on_phishing.pdf [18 June 2017.

Bitdefender. Teen Girls under Arrest for Online Impersonation [Online]. 2012. Available from: https://www.bitdefender.com/security/pre-teen-teen-girls-under-arrest-for-online-impersonation.html [3 November 2014.

Chosun.com, C. President, Pm Fall Victim to Online Id Theft [Online]. 2006. Available from: http://english.chosun.com/site/data/html_dir/2006/06/27/2006062761016.html [7 April 2017. 27 June 2006]

Crown Prosecuting Service. Guidelines on Prosecuting Cases Involving Communications Sent Via Social Media [Online]. 2016. Available from:

http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/#content [25 January 2017.

Dowell, K. Digital Deception and the Law [Online]. 2014. Available from: http://offtheleash.net/2014/10/16/digital-deception-and-the-law/ [3 November 2014.

Facecrooks. Hackers Impersonate Security Team on Facebook [Online]. 2012. Available from: http://facecrooks.com/Scam-Watch/hackers-impersonate-security-team-on-facebook.html [19 June 2017.

Gardner, E. Music Biz Agent Claims Colleague Defamed Him through Twitter Impersonation [Online]. 2014. Available from: http://www.hollywoodreporter.com/thr-esq/music-biz-agent-claims-colleague-725219 [9 December 2014.

In Brief. What Is the Law on Impersonating Another Person on Facebook? [Online]. Available from: http://www.inbrief.co.uk/human-rights/impersonating-someone-on-facebook.htm [9 December 2014.

K. Zertuche. Haha to Take Action against Impersonator [Online]. 2015. Available from: https://www.soompi.com/2015/12/20/haha-to-take-action-against-impersonator/ [30 March 2017. 20 December 2015]

Kelly Warner Law. Impersonating Someone on the Internet : Legal or Illegal? [Online]. 2014. Available from: http://kellywarnerlaw.com/impersonating-someone-on-the-internet-law/ [2 February 2015.

Luyt, D. Liability for Impersonating Someone Online [Online]. 2011. Available from: https://www.michalsons.com/blog/liability-impersonating-someone-online/9696 [25 April 2017.

Ministry of Justice, J. Act on Prohibition of Unauthorized Computer Access [Online]. Available from: http://www.japaneselawtranslation.go.jp/law/detail/?id=2250&vm=04&re=02 [21 June 2017.

Nigam, H. What Can You Can Do to Make Sure an E-Impersonation Bill Gets Passed in Your State? [Online]. 2011. Available from: http://sspblue.com/blog/what-

can-you-can-do-to-make-sure-an-e-impersonation-bill-gets-passed-in-your-state/ [11 December 2014.

Organisation for Economic Co-operation and Development. Oecd Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [Online]. 2013. Available from: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [13 July 2011.

PricewaterhouseCoopers LLP and PwC Legal LLP. Alert: Internet and Impersonation Fraud Utilising the Pricewaterhousecoopers Llp and Pwc Legal Llp Brands [Online]. Available from: https://www.pwc.co.uk/who-we-are/internet-and-impersonation-fraud.html [9 April 2017.

Privacy Rights Clearinghouse. Criminal Identity Theft: What to Do If It Happens to You [Online]. Available from: https://www.privacyrights.org/consumer-guides/identity-theft-what-do-if-it-happens-you [31 October 2014.

Protect My ID. Facebook Fraud: Identity Theft through Social Networking [Online]. 2010. Available from: https://www.protectmyid.com/images/education_center/pdf/050TypesofFraud/7_types%20of%20fraud_social%20networking.pdf [25 March 2014.

Reprentative Cliff Bentz. Bentz Introduces Bill to Crack Down on Online Impersonation [Online]. 2015. Available from: https://www.oregonlegislature.gov/bentz/Documents/Bentz%20Introduces%20Bill%20to%20Crack%20Down%20on%20Online%20Impersonation.pdf [4 January 2017.

Reputation.com. How to Protect Yourself from Online Impersonation [Online]. Available from: http://www.reputation.com/reputationwatch/articles/how-protect-yourself-online-impersonation [11 December 2014.

The Japan Times. Court Recognizes 'Right to Identity' for First Time in Online Impersonation Ruling [Online]. 2016. Available from: http://www.japantimes.co.jp/news/2016/06/10/national/court-recognizes-right-to-identity-for-first-time-in-online-impersonation-ruling/#.WOpMEPmGPIU [9 April 2017. 10 June 2016]

Vickery, J. The Megan Meier Myspace Suicide : A Case Study Exploring the Social Aspects of Convergent Media, Citizen Journalism, and Online Anonymity and Credibility [Online]. 2008. Available from: http://www.online.journalism.utexas.edu/2008/Jaqueline.pdf [25 April 2014.

Webroot. Discussing Online Impersonation with Your Kids [Online]. Available from: http://www.webroot.com/us/en/home/resources/tips/ethics-and-legal/ethics-discuss-online-impersonation-with-your-kids [2 November 2014.

Wikipedia. Computer Misuse Act 1990 [Online]. 2017. Available from: http://en.wikipedia.org/wiki/Computer_Misuse_Act_1990 [5 February 2017. 29 March 2017]

Without My Consent. California Penal § 528.5 – Impersonation through Internet or Electronic Means [Online]. Available from: http://withoutmyconsent.org/50state/31806784 [23 April 2017.

———. Identity Theft [Online]. Available from: http://withoutmyconsent.org/50state/291858029 [23 April 2017.

ภาคผนวก

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวสุธาทิพย์ แก้วศิวะวงศ์ เกิดเมื่อวันที่ 25 มีนาคม พ.ศ. 2532 ที่กรุงเทพมหานคร สำเร็จการศึกษาชั้นประถมศึกษาจากโรงเรียนประชานิเวศน์ ชั้นมัธยมศึกษาจากโรงเรียนสวนกุหลาบวิทยาลัยนนทบุรี และปริญญานิติศาสตรบัณฑิต เกียรตินิยมอันดับสอง จากคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ปีการศึกษา 2555 และได้รับประกาศนียบัตรหลักสูตรวิชาว่าความ รุ่นที่ 38 จากสำนักฝึกอบรมวิชาว่าความ สภาทนายความแห่งประเทศไทย ปัจจุบันกำลังศึกษาต่ออยู่ในชั้นปริญญามหาบัณฑิต หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย และประกอบอาชีพพนักงานรัฐวิสาหกิจ ตำแหน่งนิติกรประจำฝ่ายกฎหมาย การประปานครหลวง