ผลกระทบทางกฎหมายของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ในการคุ้มครองสิทธิส่วนบุคคลจากการส่งสแปม

ชลธิชา สมสอาด[1]
คณาธิป ทองรวีวงศ์[2]

บทคัดย่อ

ในปัจจุบัน ธุรกิจต่างๆ มีการส่งสแปมไปยังผู้บริโภค การกระทำดังกล่าวเป็นการรบกวนสิทธิในความเป็นอยู่ส่วนตัวของบุคคลที่ได้รับการติดต่อซึ่งมิได้คาดหมายและยินยอมในการติดต่อเช่นนั้น งานวิจัยฉบับนี้มุ่งศึกษาระบบกฎหมายไทยปัจจุบันในการปรับใช้เพื่อการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของผู้ถูกรบกวนจากสแปม โดยผู้วิจัยใช้วิธีการวิจัยเชิงคุณภาพ ในการวิเคราะห์เนื้อหารวมทั้งปัญหาการปรับใช้กฎหมายกับการคุ้มครองสิทธิดังกล่าว ผลการวิจัยชี้ให้เห็นว่า ในระบบกฎหมายไทยปัจจุบัน แม้มีกฎหมายหลายฉบับอันอาจนำมาปรับใช้เพื่อการคุ้มครองสิทธิของผู้ถูกรบกวนจากการส่งสแปม โดยเฉพาะพระราชบัญญัติความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 แต่กฎหมายดังกล่าวยังมีปัญหาในเชิงเนื้อหาองค์ประกอบ และขอบเขตหลายประการที่ทำให้ไม่สามารถปรับใช้เพื่อการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวที่ถูกกระทบจากการส่งสแปม ข้อเสนอแนะจากการวิจัย ได้แก่การแก้ไขปัญหาทางกฎหมายที่เกิดขึ้นหลายประการ การบัญญัติกฎหมายขึ้นใหม่ และปรับปรุงแก้ไขกฎหมายที่มีอยู่เดิม

คำสำคัญ: สิทธิส่วนบุคคล สแปม การติดต่อโดยมิได้เรียกร้อง กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อาชญากรรมคอมพิวเตอร์

[1]อาจารย์ประจำหลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยเกษมบัณฑิต
ที่อยู่: 1761 ถนนพัฒนาการ เขตสวนหลวง กทม. 10250
Email: chonthicha.som@kbu.ac.th
[2]ผู้อำนวยการสถาบันกฎหมายสื่อดิจิทัล มหาวิทยาลัยเกษมบัณฑิต
ที่อยู่: 1761 ถนนพัฒนาการ เขตสวนหลวง กทม. 10250
Email: kanathip@yahoo.com

Legal Impacts of the Application of the Computer-Related Offence Act B.E. 2560 on the Protection of Privacy Rights in Case of Spamming

Chonthicha Somsaard[1]
Kanathip Thograweewong[2]

Abstract

Recently, business sectors apply several methods to approach prospective customers, especially "Spam" which is considered an invasion of privacy of the contacted person. This research project aimed to study the application of related Thai laws in relation to violation of privacy rights by Spam. The research approach was qualitative and information was collected from various documents for analytical purposes. It was revealed that there was no specific law in recent Thai legal system to protect the "right not to be contacted by Spam without expectation and consent". Although there were currently various laws which could be applied to unsolicited contact by spam, i.e., the Computer-Related Offence Act B.E. 2560. This research indicated that the content, element, and scope of the laws were inappropriate to be applied to protect the individual privacy rights in case of invasion by Spam. Consequently, the research proposes public policies such as enacting a specific law and amending the existing laws in order to protect privacy rights in case of invasion by Spam.

Key words: Privacy rights, Spam, unsolicited contact, law on computer related offence, computer crime

[1]Lecturer in Master of Law Program, Faculty of Law, Kasem Bundit University
Address: 1761 Pattanakarn Road, Suanluang, Bangkok 10250
Email: chonthicha.som@kbu.ac.th
[2]Director Institute for Digital Media Law, Kasem Bundit University
Address: 1761 Pattanakarn Road, Suanluang, Bangkok 10250
Email: kanathip@yahoo.com

บทนำ

การส่งข้อมูลอิเล็กทรอนิกส์ไปยังผู้รับโดยผู้รับมิได้เรียกร้องเกิดขึ้นอย่างกว้างขวางในปัจจุบัน การส่งข้อมูลดังกล่าวอาจกระทำในหลายรูปแบบ เช่น จดหมายอิเล็กทรอนิกส์ ข้อความทางโทรศัพท์เคลื่อนที่ ข้อความอิเล็กทรอนิกส์ที่ส่งผ่านโปรแกรมประยุกต์ต่างๆ อย่างไรก็ตาม ปัญหาในแง่สิทธิส่วนบุคคลของการส่งข้อมูลดังกล่าวก็คือ ลักษณะของการส่งข้อมูลที่เป็นการติดต่อสื่อสารที่ผู้รับการติดต่อ “มิได้เรียกร้องหรือเชื้อเชิญ” (Unsolicited communication) ซึ่งอาจจำแนกพิจารณาว่ามีลักษณะที่สำคัญสองประการคือ ผู้ติดต่อและผู้รับการติดต่อ มิได้มีความสัมพันธ์กันอยู่ก่อน และผู้รับการติดต่อมิได้ให้ความยินยอมในการติดต่อนั้น(Sorkin, 2001) การติดต่อดังกล่าวส่งผลกระทบต่อสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy) ของผู้รับการติดต่อ หากพิจารณาวัตถุประสงค์ของการติดต่อโดยมิได้เรียกร้องแล้วอาจสามารถจำแนกการติดต่อดังกล่าวได้เป็นสองกลุ่ม คือ การติดต่อเพื่อวัตถุประสงค์เชิงพาณิชย์และการติดต่อเพื่อวัตถุประสงค์ที่มิใช่เชิงพาณิชย์ การส่งข้อมูลดังกล่าวอาจเรียกว่า “สแปม (Spam)” ซึ่งพัฒนามาจากการส่งจดหมายอิเล็กทรอนิกส์ (Spam Email)เป็นการส่งในปริมาณมากไปยังผู้รับหลายราย โดยอาจเรียกว่า “Bulk Email” การส่ง “Spam” นั้นส่งผลกระทบในแง่ของต้นทุนและค่าใช้จ่าย (Cost and expense) ต่อบุคคลหลายฝ่าย เช่น ผู้ให้บริการอินเทอร์เน็ต (Simon, 2004) นายจ้าง (Hansell, 2003) นอกจากนี้ยังส่งผลกระทบต่อสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy) ของผู้รับการติดต่อ ความพยายามแก้ปัญหาการส่งสแปม ปรากฏให้เห็นจากวิธีการทางเทคนิค (Technology-Based Approach) เช่น ผู้ให้บริการระบบจดหมายอิเล็กทรอนิกส์อาจมีการใช้ซอฟท์แวร์ ที่ออกแบบขึ้นสำหรับการคัดกรองจดหมายอิเล็กทรอนิคส์ (Email filtering software) ซึ่งอาจคัดกรองโดยพิจารณาจาก ผู้ส่ง หัวเรื่องที่ส่ง ปริมาณ และลักษณะของการส่ง (Bray, 1996) แต่วิธีการทางเทคนิคก็อาจส่งผลให้จดหมายหรือข้อมูลซึ่งผู้รับต้องการ สูญหายหรือสูญเสียไปในกระบวนการคัดกรองดังกล่าวด้วย ทำให้ผู้รับพลาดโอกาสในการติดต่อสื่อสารหรือการทำธุรกรรมต่างๆ (Bambauer, 2005) นอกจากมาตร การทางเทคนิคดังกล่าวข้างต้น หลายประเทศได้ใช้มาตรการทางกฎหมาย(Legal-Based Approach) เพื่อควบคุมการส่งข้อมูลอิเล็กทรอนิกส์อันมีลักษณะเป็นสแปม สำหรับประเทศไทยมีหลักกฎหมายเกี่ยวกับสแปมครั้งแรกตาม พระราช บัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 2550 ต่อมามีการแก้ไขปรับปรุงในปี พ.ศ. 2560 อย่างไรก็ตาม หลักการควบคุมสแปมตามกฎหมายที่แก้ไขใหม่ยังมีประเด็นปัญหาหลายประการ ดังนั้นงานวิจัยนี้จะได้นำหลักกฎหมายต่างประเทศเกี่ยวกับสแปมมาวิเคราะห์เปรียบเทียบกับหลักกฎหมายมาตรา 11 ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ที่แก้ไขปี พ.ศ. 2560 ในประเด็นต่าง ๆ ที่เกี่ยวข้อง ผลการวิเคราะห์เปรียบเทียบจะนำไปสู่บทสรุปและข้อเสนอแนะเพื่อการปรับปรุงแก้ไขกฎหมายของไทยต่อไป

วัตถุประสงค์ของการวิจัย

1.ศึกษาสภาพการณ์และแนวคิดที่เกี่ยวข้องกับการป้องกันและปราบปรามปัญหา Spam

2. เพื่อศึกษาการปรับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และกฎหมายอื่นของประเทศไทยที่เกี่ยวข้องกับการป้องกันและปราบปรามการข้อมูลอิเล็กทรอนิกส์โดยผู้รับมิได้เรียกร้อง (Spam)

3. เพื่อศึกษาวิเคราะห์เปรียบเทียบพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 กับกฎหมาย “CAN-SPAM Act” ของสหรัฐอเมริกา และ Data Protection Act ของสหราชอาณาจักร เพื่อนำไป สู่การเสนอแนวทางปรับปรุงแก้ไขกฎหมายของประเทศไทยต่อไป

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการศึกษาที่มุ่งเน้นการศึกษากฎหมาย การตีความและปรับใช้กฎหมาย ปัญหาในการบังคับใช้กฎหมาย จึงเป็นการศึกษาเชิงคุณภาพ (Qualitative Research) โดยการศึกษา วิจัยเอกสาร (Documentary Research) จากตัวบทกฎหมายที่เกี่ยวข้อง คำพิพากษาศาลฎีกา คดีที่เกิดขึ้นและบทความวิชาการทั้งในประเทศไทยและต่างประเทศ การวิจัยนี้จะทำการวิเคราะห์เปรียบเทียบ (Comparative analysis) โดยนำกฎหมายของสหรัฐอเมริกาและประเทศอังกฤษมาวิเคราะห์เพื่อเปรียบเทียบกับพระราช บัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ของประเทศไทย

นิยามศัพท์

“Spam” หมายถึง “จดหมายอิเล็กทรอนิกส์หรือข้อความอิเล็กทรอนิกส์ที่ปกปิดหรือปลอมแปลงแหล่งที่มาในการส่งและมิได้เปิดโอกาสให้ผู้รับปฏิเสธการส่งในครั้งต่อไป”

แนวคิดทฤษฎีที่เกี่ยวข้อง

งานวิจัยนี้ได้ทบทวนวรรณกรรมเพื่อศึกษาแนวคิดทฤษฎีเกี่ยวกับสิทธิในความเป็นอยู่ส่วนตัว (Right to Privacy) อันเป็นที่มาของสิทธิที่จะไม่ถูกรบกวนจากการส่ง“Spam”ผลการทบทวนสรุปได้ว่าสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy) สามารถพิจารณาได้จากหลายบริบท กล่าวคือ ในบริบททางปรัชญานั้นพิจารณาที่มาแห่งสิทธิของมนุษย์ทั้งหลายโดยแนวคิดตามธรรมชาติ (Idea of Nature) เพราะธรรมชาติเป็นผู้กำหนดระเบียบอันถูกต้องแห่งจักรวาล (Nature Described the Property of the Universe) (Minogue, 1978) ดังนั้น สิทธิของมนุษย์ทุกคนจึงได้รับการอ้างอิงว่า สิทธิธรรมชาติ (Natural Rights) ในสมัยโรมันมีแนวคิดที่ยอมรับว่าบุคคลแต่ละคนมีเขตแดนของตนเองซึ่งในเขตแดนดังกล่าวนั้นถือเป็นเขตเฉพาะ ตัวของปัจเจกบุคคลแต่ละคนซึ่งปราศจากการสอดเข้ามาเกี่ยวข้องของบุคคลอื่นๆ ในสังคมนั้น (Wacks, 1989) ในบริบททางศาสนานั้น สิทธิในความเป็นส่วนตัวของบุคคลเริ่มพัฒนามาจากการมุ่งเน้นไปที่สิทธิที่เกี่ยวกับเนื้อตัวร่างกาย เช่น การนำใบไม้มาประดิษฐ์เป็นที่ปิดบังส่วนของร่างกายที่ไม่ต้องการให้คนอื่นได้เห็น (Decew, 1997) เมื่อสิทธิในความเป็นอยู่ส่วนตัว เป็นสิทธิที่ติดตัวคนมาตั้งแต่กำเนิด จึงมีลักษณะเช่นเดียวกับสิทธิมนุษยชน (Human Right) ที่เป็นสิทธิที่มีอยู่ในทุกคนอันเนื่องมาจาก

การที่เขาเป็นมนุษย์ ไม่ต้องทำอะไรทั้งสิ้นเพื่อให้ได้มา ขอเพียงได้เกิดเป็นมนุษย์ย่อมมีสิทธิมนุษยชน (Donnelly, 1982) สิทธิในความเป็นอยู่ส่วนตัว มีลักษณะพลวัต (Dynamic) กล่าวคือสามารถเปลี่ยนแปลงไปตามบริบททางสังคม วัฒนธรรม ด้วยเหตุนี้ สิทธิในความเป็นอยู่ส่วนตัว อาจแตกย่อยออกมาเป็นสิทธิต่างๆได้อีกหลายประการตามบริบทต่างๆ เช่น สิทธิในการดำเนินชีวิตและกำหนดความเป็นตัวตนของตนเอง (Self-determination) สิทธิในการติดต่อสื่อสารกับผู้อื่น สิทธิที่จะสมรสหรือสร้างครอบครัว สิทธิในการมีชีวิต สิทธิที่จะเลือกศาสนาและการเมือง เป็นต้น นอกจากนี้เมื่อสังคมเปลี่ยนแปลงไปย่อมเกิดสิทธิในความเป็นส่วนตัวชนิดใหม่ ๆ ขึ้นมาได้ เช่น สิทธิในความเป็นส่วนตัวจากการกระทำต่าง ๆ ที่เกี่ยวข้องกับการขายตรง สิทธิในความเป็นส่วนตัวจากพฤติกรรมต่างๆทางเว็บไซต์เครือข่ายสังคม ดังนั้น การส่งสแปมจึงเป็นการรบกวนสิทธิในความเป็นอยู่ส่วนตัวอีกรูปแบบหนึ่งที่ควรได้รับการศึกษาโดยเฉพาะต่อไป

ผลการวิจัย

ผลการวิจัยโดยวิเคราะห์เปรียบเทียบกฎหมายต่างประเทศ สามารถแยกเป็นประเด็นต่าง ๆ 5 ประเด็นหลัก ดังนี้

ประเด็นที่หนึ่ง การได้มาซึ่งที่อยู่อิเล็กทรอนิกส์

ผลการศึกษาพบว่าขั้นตอนแรกของการส่งสแปม คือ การที่ผู้ส่งได้มาซึ่งข้อมูลที่อยู่อิเล็กทรอนิกส์ ซึ่งแบ่งได้สองกรณีย่อยคือ การได้มาซึ่งข้อมูลที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง และการได้มาซึ่งข้อมูลที่อยู่อิเล็กทรอนิกส์ของผู้รับ

การได้มาซึ่งที่อยู่อิเล็กทรอนิกส์ของผู้ส่งนั้น หากพิจารณาในด้านผู้ส่งสแปม อาจจำแนกลักษณะของข้อมูลในการส่งได้เป็นสองกรณีคือ กรณีที่หนึ่ง ผู้ส่งใช้ข้อมูลตนเองในการส่ง โดยไม่ได้ดำเนินการใดเพื่อปกปิดแหล่งที่มาของการส่ง เช่น การใช้บัญชีที่อยู่จดหมายอิเล็กทรอนิกส์ของตนเอง กรณีที่สอง ผู้ส่งใช้วิธีการเพื่อปกปิดปลอมแปลงแหล่งที่มาของการส่งเพื่อมิให้ทราบว่ามาจากผู้ส่ง เช่น การเข้าถึงบัญชีผู้ใช้จดหมายอิเล็กทรอ นิกส์ของผู้อื่นโดยมิชอบและส่งสแปมจากบัญชีนั้น ประเด็นปัญหาทางกฎหมายในด้านข้อมูลของผู้ส่งจะเกี่ยวข้องกับกรณีที่สอง

กฎหมายเกี่ยวกับสแปมในระดับรัฐบาลกลางของสหรัฐอเมริกา (CAN-SPAM) กำหนดฐานความผิดเกี่ยวกับการฉ้อโกงและกิจกรรมที่เกี่ยวเนื่องกับข้อความพาณิชย์อิเล็กทรอนิกส์ (Fraud and related activity in connection with electronic mail) (Section 4 Public Law 108-187-Dec.. 16, 2003; 15 U.S.C., 770315 U.S.C.,7703) โดยมีความผิดที่สำคัญเกี่ยวกับข้อมูลหรือที่อยู่อิเล็กทรอนิกส์ทางด้านผู้ส่งสแปม 4 ประการ ได้แก่

(1) เข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ และ เจตนาริเริ่มส่งข้อความพาณิชย์อิเล็กทรอนิกส์ไปยังผู้รับจำนวนมากจากเครื่องคอมพิวเตอร์นั้น

(2) ใช้ข้อมูลบ่งชี้ผู้ลงทะเบียนที่แท้จริงอันเป็นเท็จในสาระสำคัญ ในการลงทะเบียนในบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ 5 บัญชีหรือกว่านั้นขึ้นไป หรือลงทะเบียนเป็นผู้ใช้โดเมนเนม 2 โดเมนเนมหรือกว่านั้นขึ้นไป และเจตนาริเริ่มในการส่งข้อความพาณิชย์อิเล็กทรอนิกส์ไปยังผู้รับจำนวนมากจากบัญชีผู้ใช้งานหรือโดเมนเนมดังกล่าว

(3) แสดงตนอันเป็นเท็จว่าเป็นผู้ลงทะเบียนหรือเป็นผู้มีสิทธิตามกฎหมายในการลงทะเบียนอินเตอร์เน็ตโปรโตคอล (IP address) 5 โปรโตคอลหรือกว่านั้นขึ้นไป และเจตนาริเริ่มในการส่งข้อความพาณิชย์อิเล็กทรอนิกส์ไปยังผู้รับจำนวนมากจากอินเตอร์เน็ตโปรโตคอลดังกล่าว

(4) กำหนดฐานความผิดสำหรับการส่งข้อความพาณิชย์อิเล็กทรอนิกส์ที่ถือเป็นการฝ่าฝืนกฎหมายอย่างร้ายแรง (Aggravated Violations Relating to Commercial Electronic Mail) (Section 5 (b) Public Law 108-187-Dec.. 16, 2003; 15 U.S.C., 7704) โดยมีฐานความผิดสำหรับการ “สร้างที่อยู่อิเล็กทรอนิกส์จำนวนมากโดยอัตโนมัติ (Automated creation of multiple electronic mail accounts)” โดยมีองค์ประกอบความผิด “ การส่งข้อความพาณิชย์อิเล็กทรอนิกส์จะถือเป็นการฝ่าฝืนกฎหมายอย่างร้ายแรง หากผู้ส่งใช้สคริปท์หรือวิธีการอัตโนมัติอื่น ๆ ในการลงทะเบียนบัญชีที่อยู่อิเล็กทรอนิกส์หรือบัญชีผู้ใช้งานออนไลน์จำนวนมาก เพื่อใช้ที่อยู่หรือบัญชีดังกล่าวในการส่งข้อความพาณิชย์อิเล็กทรอนิกส์ไปยังผู้รับ”

พฤติกรรมที่เข้าองค์ประกอบความผิด 4 กรณีข้างต้นนั้น นอกจากจัดเป็นการปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งแล้วยังอาจจัดอยู่ในกลุ่มพฤติกรรมการได้มาซึ่งข้อมูลที่ใช้ในการส่ง

ส่วนกฎหมายสหราชอาณาจักรนั้น ไม่ได้กำหนดกฎหมายเฉพาะสำหรับสแปม แต่มีกฎหมายเกี่ยวกับความเป็นส่วนตัวและการสื่อสารอิเล็กทรอนิกส์ (The Privacy and Electronic Communications (EC Directive) Regulations 2003 ซึ่งนำหลักกฎหมายยุโรปมาอนุวัติการได้วาง หลักว่า ห้ามบุคคลใดส่งหรือก่อให้เกิดการสื่อสารเพื่อวัตถุประสงค์ของการทำการตลาดทางตรงโดยจดหมายอิเล็กทรอนิกส์ หาก (ก) ข้อมูลระบุตัวตนของบุคคลซึ่งทำการติดต่อนั้นถูกปลอมหรือปกปิดไว้ (disguised or concealed) (PECR, Section 23) ดังนั้น การส่งสแปมทางจดหมายอิเล็กทรอนิกส์ที่ใช้วิธีปกปิดแหล่งที่มาของผู้ส่งก็จะมีความผิดเฉพาะตามกฎหมายนี้

วิเคราะห์เปรียบเทียบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พบว่าความผิดเฉพาะเกี่ยวกับสแปมตามมาตรา 11 มิได้มีการกำหนดองค์ประกอบที่เกี่ยวเนื่องกับขั้นตอนการได้มาซึ่งข้อมูลของผู้ส่ง อย่างไรก็ตาม หากการได้มาหรือการสร้างขึ้นซึ่งข้อมูลในด้านผู้ส่งมีลักษณะ “ปกปิดหรือปลอมแปลงแหล่งที่มาของการส่ง” อาจเข้าองค์ประกอบความผิด มาตรา 11 วรรคหนึ่ง ได้ ทั้งนี้หากพิจารณาองค์ ประกอบความผิดตามกฎหมาย CAN-SPAM ที่เกี่ยวกับข้อมูลทางด้านผู้ส่งทั้ง 4 กรณี และกฎหมายสหราชอาณาจักรดังกล่าวแล้วเห็นว่า มีลักษณะเป็นการ “ปกปิดหรือปลอมแปลงแหล่งที่มาของการส่ง” อันสามารถเข้าองค์ประกอบมาตรา 11 วรรคหนึ่ง แต่สำหรับฐานความผิดตาม มาตรา 11 วรรคสองและสาม ไม่มีองค์ประกอบเกี่ยวกับการปกปิดหรือปลอมแปลงแหล่งที่มาของการส่ง เนื่องจากพิจารณาที่ “ความเดือดร้อนรำคาญ” ของผู้รับข้อมูลเป็นสำคัญ

แต่หากพิจารณาเฉพาะในส่วนพฤติกรรมการได้มาหรือสร้างขึ้นซึ่งข้อมูลเกี่ยวกับผู้ส่ง โดยยังไม่มีการส่งสแปมนั้น ใน

สหรัฐอเมริกาพบว่า กฎหมาย CAN-SPAM กำหนดความผิดเกี่ยวกับการได้มาหรือสร้างขึ้นซึ่งที่อยู่หรือข้อมูลที่ใช้ในการส่งสแปมโดยมีความเชื่อมโยงกับพฤติกรรมการส่งด้วย เช่น การเข้าถึงคอมพิวเตอร์ของผู้อื่นโดยมิชอบ และ ทำการส่งสแปมจากเครื่องนั้น สำหรับกฎหมายสหราชอาณาจักรก็ต้องเป็นกรณีการปกปิดแหล่งที่มาของผู้ส่งโดยต้องมีการส่งจดหมายอิเล็กทรอนิกส์เช่นกัน ดังนั้น หากมีการเข้าถึงคอมพิวเตอร์ของผู้อื่นโดยมิชอบแต่ไม่เกี่ยวข้องกับการส่งสแปมก็จะไม่อยู่ภายใต้กฎหมายนี้ สำหรับฐานความผิดเฉพาะเกี่ยวกับสแปมตามมาตรา 11 นั้นมี องค์ประกอบในส่วนการกระทำคือ “การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์” ดังนั้นหากมีข้อเท็จจริงเฉพาะในส่วนพฤติกรรมการได้มาหรือสร้างขึ้นซึ่งข้อมูลทางด้านผู้ส่งแต่ยังไม่ได้กระทำการส่งข้อมูลก็ยังไม่เข้าองค์ประกอบความผิดมาตรา 11 ซึ่งลักษณะเช่นนี้คล้ายคลึงกับกฎหมายสหรัฐอเมริกา

ส่วนการได้มาซึ่งที่อยู่อิเล็กทรอนิกส์หรือข้อมูลทางด้านผู้รับนั้น ในด้านข้อมูลของผู้รับการติดต่อนั้น ผู้ทำการส่งสแปมอาจได้มาซึ่งข้อมูลของผู้รับในฐานะเป้าหมายของการส่งด้วยวิธีการต่างๆ เช่น การใช้โปรแกรมหรือวิธีการทางเทคนิคในการได้มา เช่น การใช้โปรแกรมหรือซอฟท์แวร์ที่ออกแบบเฉพาะเพื่อเก็บรวบรวมที่อยู่อิเล็กทรอ นิกส์ (Email harvesting software เช่น “Email Spider” “Email Harvester”) หรือ การได้มาซึ่งที่อยู่อิเล็กทรอนิกส์ของผู้อื่นโดยการสุ่มด้วยวิธีอัตโนมัติ (Automated Mean) เช่น การคาดเดาที่อยู่จดหมายอิเล็กทรอนิกส์ขึ้นด้วยการผสมข้อมูล เช่น ชื่อ ตัวอักษร ตัวเลข เข้าด้วยกัน (Dictionary Attack) ข้อมูลที่ได้มาด้วยวิธีการเหล่านี้อาจมีการ รวบรวมเป็นบัญชีรายชื่อ ซึ่งผู้กระทำการในการได้มาอาจใช้ข้อมูลดังกล่าวเพื่อการส่งสแปมเอง หรือ อาจจำหน่ายบัญชีรายชื่อดังกล่าวให้กับผู้อื่น(Trading list of email address) เพื่อให้นำไปใช้ส่งสแปมต่อไป

กฎหมาย CAN-SPAM ของสหรัฐอเมริกา กำหนดความผิดสำหรับ การส่งข้อความพาณิชย์อิเล็กทรอนิกส์ที่ถือเป็นการฝ่าฝืนกฎหมายอย่างร้ายแรง (Aggravated Violations Relating to Commercial Electronic Mail) ในส่วนที่เกี่ยวกับการได้มาซึ่งข้อมูลผู้รับการติดต่อนั้น มีความผิดฐานเกี่ยวกับการได้มาซึ่งข้อมูลผู้รับด้วยการเก็บข้อมูลที่อยู่อิเล็กทรอนิกส์และการโจมตีระบบแบบสุ่ม (Address Harvesting and Dictionary Attack) ซึ่งมีองค์ประกอบความผิดดังนี้

“ส่งข้อความพาณิชย์อิเล็กทรอนิกส์ โดยผู้ส่งได้รับที่อยู่อิเล็กทรอนิกส์ของผู้รับมาโดยใช้วิธีการอัตโนมัติจากเว็บไซต์หรือบริการออนไลน์ที่ดำเนินการโดยผู้อื่น โดยเว็บไซต์หรือบริการออนไลน์นั้นมีประกาศแจ้งว่าจะไม่ให้ขาย หรือโอนข้อมูลที่อยู่อิเล็กทรอนิกส์ซึ่งเก็บรักษาไว้ในเว็บไซต์หรือบริการออนไลน์นั้นเพื่อใช้หรือเพื่อให้ผู้อื่นสามารถใช้ในการส่งข้อความอิเล็กทรอนิกส์”

“ส่งข้อความพาณิชย์อิเล็กทรอนิกส์ โดยผู้ส่งได้มาซึ่งที่อยู่อิเล็กทรอนิกส์ของผู้รับด้วยการใช้วิธีการอัตโนมัติในการสร้างที่อยู่อิเล็กทรอนิกส์ซึ่งเป็นไปได้ ด้วยการผสมข้อมูล เช่น ชื่อ ตัวอักษร ตัวเลข เข้าด้วยกัน”

สหราชอาณาจักร ไม่ได้กำหนดกฎหมายเฉพาะสำหรับสแปม แต่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Act 1998

หรือ “DPA”) ที่นำมาปรับใช้ได้ โดยกำหนดหลักห้ามผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ดังนั้น การเก็บรวบรวมข้อมูลที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่อนำมาใช้ในการส่งสแปม โดยไม่ได้ขอความยินยอมก่อนจึงเป็นการขัดต่อหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล

วิเคราะห์เปรียบเทียบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 เนื่องจากการได้มาซึ่งที่อยู่อิเล็กทรอนิกส์ของผู้รับอาจเกิดจากการใช้วิธีการกฎหมายต่างประเทศเกี่ยวกับสแปมกำหนดไว้โดยเฉพาะ ก็คือ การใช้ซอฟท์แวร์เก็บรวบรวม ที่อยู่อิเล็กทรอนิกส์ (Address harvesting software) โดยอาจแบ่งรูปแบบของกฎหมายได้สามแนวทาง คือ (1) การกำหนดความผิดตั้งแต่การซื้อขายซอฟท์แวร์หรือโปรแกรม และ (2) ยังไม่กำหนดความผิด ในขั้นตอนการซื้อขายซอฟท์แวร์ แต่มีการกำหนดความผิดในขั้นตอนการส่งสแปมซึ่งผู้ส่งได้ข้อมูลของผู้รับจากการใช้ซอฟท์แวร์ดังกล่าว เช่น กฎหมาย CAN-SPAM (3) กำหนดความผิดสำหรับการได้มาซึ่งข้อมูลเช่นที่อยู่ของผู้รับโดยไม่ได้รับความยินยอมแม้ว่าจะยังไม่ได้นำไปส่งสแปมก็ตาม เช่น กฎหมายสหราชอาณาจักร ในส่วนของ มาตรา 11 มิได้กำหนดความผิดในขั้นตอนการซื้อขายซอฟท์แวร์หรือโปรแกรมที่เกี่ยวข้องกับสแปม อย่างไรก็ตาม มีหลักกฎหมายที่เกี่ยวข้องคือ มาตรา 13 ซึ่งกำหนดความผิดสำหรับผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดมาตรา 11 นอกจากนี้ มาตรา 13 วรรคสาม กำหนดโทษหนักขึ้นสำหรับผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดมาตรา 11 หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา 11 ต่อข้อมูลหรือระบบคอมพิวเตอร์ที่กำหนดไว้ในมาตรา 12 เช่น ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ เป็นต้น แม้ว่ามาตรา 13 กำหนดความผิดสำหรับการจำหน่ายทางเทคนิคหลายวิธีการ โดยวิธีการหนึ่งคือเผยแพร่ชุดคำสั่งเพื่อนำไปใช้ในการส่งสแปมตามมาตรา 11 แต่เมื่อเปรียบเทียบกับกฎหมายต่างประเทศแล้ว เห็นว่ามีข้อแตกต่างหลายประการได้แก่ (1) มาตรา 13 กำหนดความผิดเฉพาะผู้จำหน่ายหรือผู้จัดหาให้ซึ่งซอฟท์แวร์ มิได้กำหนดความผิด สำหรับผู้ซื้อหรือผู้ได้มาซึ่งซอฟท์แวร์ (2) มาตรา 13 มิได้กำหนดจำแนกวิธีการได้มาซึ่งข้อมูลออกเป็นสองวิธีการอย่างชัดเจน (3) มาตรา 13 ใช้กับการจำหน่ายชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อใช้เป็น “เครื่องมือในการกระทำความผิดตามมาตรา 11” ซึ่งมีประเด็นว่า ความผิดมาตรา 13 จะครอบคลุมซอฟท์แวร์ที่ใช้ในขั้นตอนการได้มาซึ่งข้อมูลเพื่อการส่งสแปม โดยยังไม่มีการส่งสแปมได้หรือไม่ เช่น การซื้อขายซอฟท์แวร์ที่สร้างเพื่อใช้ในการเก็บรวบรวมข้อมูลที่อยู่อิเล็กทรอนิกส์ ซึ่งอาจตีความได้สองแนวทางคือ

แนวทางที่หนึ่ง ตีความว่า การได้มาซึ่งข้อมูลผู้รับเพื่อทำการส่งสแปม เป็นส่วนหนึ่งของการส่งสแปม ดังนั้น การจำหน่ายซอฟท์แวร์เพื่อให้ได้มาซึ่งข้อมูลอันจะนำไปใช้กระทำผิดมาตรา 11 จึงเป็นซอฟท์แวร์เพื่อใช้เป็นเครื่องมือกระทำผิดตามมาตรา 11 ซึ่งทำให้ผู้จำหน่ายมีความผิดตามมาตรา 13

แนวทางที่สอง พิจารณาจากข้อเท็จจริงและพฤติกรรมที่เกี่ยวข้องจะเห็นได้ว่า ซอฟท์แวร์หรือโปรแกรมที่จัดทำขึ้นเฉพาะเพื่อใช้ในการเก็บรวบรวมที่อยู่อิเล็กทรอนิกส์ หรือ เพื่อให้ได้มาซึ่งข้อมูลผู้รับการติดต่อ มีลักษณะการทำงานคนละขั้นตอนกับซอฟท์แวร์ที่ใช้เป็นเครื่องมือกระทำความผิดตามมาตรา 11 กล่าวคือ ซอฟท์แวร์ที่ใช้เก็บรวบรวมที่อยู่อิเล็กทรอนิกส์ในเว็บไซต์ต่างๆ นั้น เป็นขั้นตอนการได้มาซึ่งข้อมูลผู้รับการติดต่อ ซึ่งการกระทำในขั้นตอนนี้ยังไม่เป็นความผิดตามมาตรา 11 หรืออาจเป็นเพียงการตระเตรียมกระทำผิดตามมาตรา 11 แต่กฎหมายยังไม่กำหนดเป็นความผิด สำหรับซอฟท์แวร์ที่ใช้ส่งข้อมูลอิเล็กทรอนิกส์หรือซอฟท์แวร์ที่ใช้ส่งสแปม เช่น สคริปท์ที่ใช้ส่งข้อความจำนวนมากไปยังผู้รับในวงกว้าง นั้นเป็นขั้นตอนการกระทำผิดตามมาตรา 11 แล้ว ทั้งนี้เพราะองค์ประกอบความผิดตามมาตรา 11 คือ การ “ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอ นิกส์” ซึ่งหากเปรียบเทียบกับกฎหมายต่าง ประเทศจะเห็นได้ว่ามีการบัญญัติความผิดโดยแยกอย่างชัดเจนระหว่างขั้นตอนการได้มาซึ่งข้อมูลกับขั้นตอนการส่งสแปมโดยใช้ข้อมูลที่ได้มา ดังนั้น การจำหน่ายซอฟท์แวร์เพื่อนำไปใช้ในขั้นเก็บรวบรวมข้อมูลผู้รับเพื่อทำการส่งสแปมจึงไม่เป็นความผิดตามมาตรา 13 หากจะเป็นความผิดก็จะต้องกำหนดไว้อย่างชัดเจนดังเช่นกฎหมายต่างประเทศ ซึ่งผู้วิจัยเห็นด้วยกับการตีความแนวทางที่สองนี้

ประเด็นที่สอง องค์ประกอบเชิงปริมาณและความถี่ของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์

ผลการศึกษาพบว่า กฎหมายเกี่ยวกับสแปมของต่างประเทศ มีการนำองค์ประกอบเกี่ยวกับปริมาณหรือจำนวนของการส่ง และความถี่ หรือช่วงระยะเวลาในการส่ง มากำหนดไว้เป็นเงื่อนไขเบื้องต้นของสแปมที่จะอยู่ภายใต้บังคับของกฎหมาย ดังนั้น การส่งจดหมายหรือข้อมูลคอมพิวเตอร์ที่ไม่อยู่ในขอบเขตด้านปริมาณและความถี่ก็จะไม่ถือว่าเป็นสแปม ทั้งนี้สืบเนื่องจากลักษณะพื้นฐานของสแปมซึ่งเป็นการรบกวนการทำงานของระบบคอมพิวเตอร์และรบกวนสิทธิของบุคคลจะเป็นการส่งในปริมาณมาก (Bulk) หรือส่งไปยังผู้รับจำนวนมาก (Multiple electronic message) องค์ประกอบด้านปริมาณ และความถี่ มีความสัมพันธ์กันจึงมีการบัญญัติควบคู่กันไป

ในส่วนของกฎหมายสหรัฐอเมริกานั้น กฎหมายระดับรัฐบาลกลาง (CAN-SPAM) (Section 4 Public law 108-187--DEC. 16, 2003) กำหนดว่า การส่งจดหมายพาณิชย์อิเล็กทรอนิกส์ไปยังผู้รับจำนวนมาก (Multiple electronic mail)นั้น จะต้องเป็นการส่งข้อความจดหมายพาณิชย์อิเล็กทรอนิกส์มากกว่า 100 ฉบับ ในช่วงระยะเวลา 24 ชั่วโมง หรือมากกว่า 1,000 ฉบับในช่วงระยะเวลา 30 วัน หรือมากกว่า 10,000 ฉบับในช่วงระยะเวลา 1 ปี นอกจากนี้ยังได้กำหนดเกณฑ์ปริมาณการส่งที่จะต้องรับโทษหนักขึ้น หากส่งข้อความจดหมายพาณิชย์อิเล็กทรอนิกส์ เกิน 2,500 ฉบับภายในระยะเวลา 24 ชั่วโมง หรือ 25,000 ภายในระยะเวลา 30 วัน หรือ 250,000 ฉบับ ภายในระยะเวลา 1 ปี

สำหรับกฎหมายระดับมลรัฐอาจมีการกำหนดเกณฑ์ด้านปริมาณและความถี่แตกต่างกันไป เช่น กฎหมายมลรัฐ Virginia กำหนดเกณฑ์การพิจารณาว่า จะต้องมีการส่งมากกว่า 10,000 ฉบับภายในระยะเวลา 24 ชั่วโมง หรือ

100,000 ฉบับภายในระยะเวลา 30 วัน หรือ 1 ล้านฉบับภายในระยะเวลา 1 ปี (Section 18.2-152.3:1 Virginia Title 18.2 Crimes and Offenses generally) กฎหมายมลรัฐ Ohio ใช้เกณฑ์เชิงกำหนดควบคุมสแปมว่าจะต้องเป็นการส่งข้อความหรือจดหมายอิเล็กทรอนิกส์ มากกว่า 10 ฉบับในช่วงระยะเวลา 24 ชั่วโมง หรือ มากกว่า 100 ฉบับในช่วงระยะเวลา 30 วัน หรือ มากกว่า 1,000 ฉบับในช่วงระยะเวลา 1 ปี ซึ่งเป็นการกำหนดเกณฑ์เชิงปริมาณที่ต่ำกว่ากฎหมาย CAN-SPAM อย่างไรก็ตามกฎหมายมลรัฐ Ohio ได้กำหนดเกณฑ์เชิงปริมาณสำหรับการรับโทษหนักขึ้น หากเป็นการส่งในปริมาณเกินกว่า 250 ฉบับในช่วงระยะเวลา 24 ชั่วโมง หรือ มากกว่า 2,500 ฉบับในช่วงระยะเวลา 30 วัน หรือ มากกว่า 25,000 ฉบับในช่วงระยะเวลา 1 ปี สำหรับกฎหมายบางมลรัฐอาจพิจารณาเฉพาะด้านปริมาณโดยไม่กำหนดเกณฑ์ด้านความถี่ เช่น กฎหมายมลรัฐ Louisiana ไม่ได้กำหนดองค์ประกอบด้านความถี่หรือระยะเวลา แต่กำหนดเฉพาะองค์ประกอบเชิงปริมาณว่าจะต้องเป็นจดหมายอิเล็กทรอนิกส์ที่ส่งไปยังผู้รับ มากกว่า 1,000 คน แต่บางมลรัฐไม่ได้นำองค์ประกอบเชิงปริมาณและความถี่มากำหนดไว้

หากพิจารณาแนวทางของกฎหมายสหราชอาณาจักร จะพบว่า กฎหมายเกี่ยวกับความเป็นส่วนตัวและการสื่อสารอิเล็กทรอนิกส์ (The Privacy and Electronic Communications (EC Directive) Regulations 2003") ซึ่งเป็นการนำกฎหมายสหภาพยุโรป (Directive 2002/58/EC) มาบัญญัติเป็นกฎหมายภายในนั้น ไม่ได้กำหนดองค์ประกอบเชิงปริมาณเกี่ยวกับการส่งจดหมายอิเล็กทรอนิกส์ไว้ โดยมีเพียงหลักความยินยอมดังจะได้วิเคราะห์ต่อไป

วิเคราะห์เปรียบเทียบกับพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พบว่า มาตรา 11 วรรคหนึ่ง ไม่กำหนด เกณฑ์เชิงปริมาณและความถี่ องค์ประกอบ "อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ ของบุคคลอื่นโดยปกติสุข" มีความหมายกว้างและไม่ชัดเจน โดยไม่มีการกำหนดเกณฑ์พิจารณา สำหรับประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่ง ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ พ.ศ. 2560 ที่ออกตามความมาตรา 11 วรรคสามนั้น เป็นการกำหนดรายละเอียดสำหรับฐานความผิดที่ 2 (มาตรา 11 วรรคสอง) อย่างไรก็ตาม ในการพิจารณาว่าการส่งสแปมเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของผู้อื่นหรือไม่นั้น อาจนำเกณฑ์ด้านปริมาณและความถี่มาประกอบการพิจารณาได้ แต่ก็ไม่มีความชัดเจนว่าจะใช้ปริมาณและความถี่อย่างไร นอกจากนี้ มาตรา 11 วรรคแรก ไม่กำหนดให้มีการออกประกาศกระทรวงกำหนดรายละเอียดเชิงปริมาณและความถี่ดังเช่นกรณีมาตรา 11 วรรคสอง และวรรคสาม

มาตรา 11 วรรคสองกำหนดองค์ประกอบ "ก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ" โดย มาตรา 11 วรรคสาม กำหนดให้รัฐมนตรีกำหนด "ลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ" ดังนั้นจะเห็นได้ว่า ความผิดฐานนี้เปิดโอกาสให้มีการนำองค์ประกอบในส่วนของ

“ปริมาณ” ในการส่งมาประกอบการพิจารณาว่าการส่งนั้นก่อให้เกิดความเดือดร้อนรำคาญหรือไม่ แต่มีข้อสังเกตว่ามาตรา 11 วรรคสามไม่ได้กำหนดถึง“ความถี่”เมื่อพิจารณา ประกาศกระทรวงฯ พบว่าจากชื่อของประกาศกระทรวงมีการกำหนดทั้ง “ปริมาณและความถี่” แต่เนื้อหาของประกาศกระทรวงฯ กำหนดเฉพาะ “ลักษณะของการส่งที่ไม่ถือเป็นการเดือดร้อนรำคาญ” โดยเฉพาะกรณีผู้ส่งซึ่งมีความสัมพันธ์กับผู้รับ เช่น ผู้ซึ่งเคยมีนิติสัมพันธ์กันมาก่อน แต่ไม่ได้กำหนด “ปริมาณและความถี่” ของการส่งที่จะไม่ถือเป็นการเดือดร้อนรำคาญไว้อย่างชัดเจน ดังเช่นกฎหมายต่างประเทศ

หากเปรียบเทียบกฎหมายสหรัฐอเมริกาจะพบว่า กฎหมายระดับรัฐบาลกลางและกฎหมายบางมลรัฐ มีการกำหนดองค์ประกอบด้านปริมาณและความถี่ไว้อย่างเฉพาะเจาะจงในตัวบทกฎหมาย ในขณะที่สหราชอาณาจักรไม่ได้กำหนดเกณฑ์เชิงปริมาณไว้อย่างชัดเจน สำหรับกฎหมายไทย มาตรา 11 ที่แก้ไขในปี พ.ศ. 2560 มีการเปิดทางให้ประกาศกระทรวงฯ กำหนดรายละเอียดเชิงปริมาณและความถี่ได้จึงคล้ายคลึงกับกฎหมายสหรัฐอเมริกา อย่างไรก็ตาม ในรายละเอียดของประกาศกระทรวงฯ ที่มีผลบังคับใช้ ปี พ.ศ. 2560 นั้น ยังไม่มีการนำองค์ประกอบทั้งด้านปริมาณและความถี่มากำหนดไว้

ประเด็นที่สาม การกำหนดให้จดหมายพาณิชย์อิเล็กทรอนิกส์มีข้อความเตือนว่ามีเนื้อหาเกี่ยวกับเพศและเนื้อหาโฆษณา

ผลการศึกษากฎหมายต่างประเทศพบว่ากฎหมายสหรัฐอเมริกามีหลักการ “แจ้งเตือน” โดยกำหนดหน้าที่ให้ผู้ส่งต้องแจ้งเตือนในส่วนหัวข้อว่าเนื้อหาในจดหมายหรือข้อมูลอิเล็กทรอนิกส์นั้นเกี่ยวข้องกับเรื่องใด ซึ่งมีสองกรณีคือ เนื้อหาเกี่ยวกับเพศ และ เนื้อหาโฆษณา ดังนี้

กรณีเนื้อหาเกี่ยวกับเพศ CAN-SPAM วางหลักห้ามบุคคลใดริเริ่มส่งข้อความจดหมายอิเล็กทรอนิกส์ซึ่งมีเนื้อหาเกี่ยวกับเพศ โดยไม่ระบุเครื่องหมายหรือคำเตือนในส่วนหัวเรื่อง(15 U.S.C., 7704 (d)) สำหรับรายละเอียดเกี่ยวกับเครื่องหมายหรือคำเตือนนั้น กฎหมายให้อำนาจคณะกรรมการการสื่อสารสหรัฐ (FTC) กำหนดโดยในเดือนเมษายน ค.ศ. 2004 คณะกรรมาธิการ FTC ออกกฎเกณฑ์กำหนดให้มีการระบุรายละเอียดต่างๆ รวมทั้งวางข้อจำกัดด้านเนื้อหาสำหรับข้อความที่มีเนื้อหาเกี่ยวกับเพศ (Sexually oriented material) โดยมีหลักว่าหากจดหมายอิเล็กทรอนิกส์นั้นมีข้อความที่มีเนื้อหาเกี่ยวกับเพศ ในส่วนพื้นที่ซึ่งสามารถเข้าดูได้ในชั้นแรก (Initial viewable area) ของจดหมายอิเล็กทรอนิกส์นั้น ต้องเป็นไปตามเงื่อนไข เช่น ต้องมีคำว่า “SEXUALLY-EXPLICIT” ปรากฏอยู่เป็นอักษรแรกของบรรทัดหัวข้อ นอกจากนี้เนื้อหาเกี่ยวกับเพศจะต้องไม่ปรากฏในส่วนหัวเรื่อง อย่างไรก็ตาม การระบุคำเตือนดังกล่าวมีข้อ ยกเว้นสำหรับกรณีที่ ผู้รับจดหมายอิเล็กทรอนิกส์นั้นได้ให้ความยินยอมสำหรับการรับจดหมายดังกล่าวไว้ก่อนแล้ว (Prior affirmative consent) (15 U.S.C., 7704 (d) (2)) บางมลรัฐ เช่น Arkansas กำหนดให้หัวข้อจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาทางเพศอย่างเห็นได้ชัด (Sexually explicit) ต้องระบุคำว่า “ADV:ADULT” ไว้เป็นเก้าตัวอักษรแรกของหัวข้อจดหมายอิเล็กทรอนิกส์ (Arkansas Code, Title 4, Business and Commercial law, Subtitle 7, Consumer protection, Chapter 88,

Deceptive trade practices, Subchapter 6, unsolicited com mercial and sexually explicit electro nic mail prevention act, Section 4-88-603 , 2) For a sexually explicit electronic mail, include in the electronic mail a subject line that contains “ADV:ADULT” as the first nine characters;)

กรณีเนื้อหาเกี่ยวกับการโฆษณา กฎหมายเกี่ยวกับสแปมในระดับมลรัฐ ปรากฏหลักการกำหนดให้การส่งจดหมายหรือข้อความอิเล็กทรอนิกส์ต้องระบุคำเตือนไว้ในหัวเรื่อง (at the beginning of the subject line) สำหรับกรณีที่เป็นจดหมายหรือข้อความเพื่อการโฆษณา เช่น กฎหมายมลรัฐ Arizona กำหนดให้หัวข้อจดหมายอิเล็กทรอนิกส์ ต้องมีคำว่า “ADV” เพื่อบ่งระบุให้ผู้รับทราบว่าเป็นจดหมายเพื่อการพาณิชย์ ข้อสังเกต ประการที่หนึ่ง หลังจากกฎหมาย CAN-SPAM ซึ่งเป็นกฎหมายระดับรัฐบาลกลางมีผลบังคับโดยกฎหมายนี้ไม่ได้มีการกำหนดให้ต้องมีการแจ้งเตือนโฆษณา จึงมีประเด็นว่ากฎหมายระดับมลรัฐที่ขัดแย้งกับหลักการในส่วนนี้จะใช้บังคับได้หรือไม่ ประการที่สอง บางมลรัฐ อาจมีการกำหนดเงื่อนไขการแจ้งเตือนในจดหมายอิเล็กทรอนิกส์ในกฎหมายอื่นที่ไม่ใช่กฎหมาย สแปม เช่น มลรัฐ Kentucky ศาลออกกฎเกณฑ์ควบคุมเฉพาะการส่งข้อมูลอิเล็กทรอนิกส์ของทนายความ หากเป็นการโฆษณาหรือเสนอให้บริการไปยังลูกความ จะต้องระบุว่า THIS IS AN ADVERTISEMENT" ประการที่สาม แม้ว่าไม่ต้องระบุชื่อแจ้งเตือนการโฆษณาในหัวเรื่อง แต่การส่งข้อความโฆษณาก็ยังต้องอยู่ภายใต้หลักทั่วไป ที่ต้องไม่ทำให้เกิดความเข้าใจผิด เช่น ไม่ใช้วิธีการทำให้เข้าใจผิดในแหล่งที่มาของการส่ง ไม่ใช้หัวเรื่องที่ทำให้เกิดความเข้าใจผิด เป็นต้น

กฎหมายสหราชอาณาจักร เกี่ยวกับความเป็นส่วนตัวและการสื่อสารอิเล็กทรอนิกส์ (The Privacy and Electronic Communica tions (EC Directive) Regulations 2003) ซึ่งนำ กฎหมายสหภาพยุโรป (Directive 2002/58/EC) มาบัญญัติเป็นกฎหมายภายในนั้น มุ่งควบคุม สแปมโดยวางหลักความยินยอม แต่ไม่ได้กำหนดหลักการแจ้งเตือนในส่วนหัวข้อของสแปมไว้ดังเช่นกฎหมายสหรัฐอเมริกา

วิเคราะห์เปรียบเทียบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พบว่าแม้ฐานความผิดเกี่ยวกับสแปมตามกฎหมายไทย จะมีการนำหลักการบางอย่างของกฎหมายสหรัฐ โดยเฉพาะหลัก Opt-out และ จดหมายอิเล็กทรอนิกส์ที่เกี่ยวกับธุรกรรมหรือความสัมพันธ์ที่มีมาก่อน (ประกาศกระทรวงฯ ข้อ 4) มากำหนดไว้ในการแก้ไขมาตรา 11 ตามกฎหมายฉบับ พ.ศ. 2560 แต่ไม่ปรากฏว่ามีการนำหลักกฎหมายสหรัฐอเมริกาที่เกี่ยวกับการกำหนดให้ระบุข้อมูลบ่งชี้เนื้อหาหรือคำเตือน มาบัญญัติไว้ด้วย กล่าวคือ มาตรา 11 วรรคแรก และ มาตรา 11 วรรคสอง ไม่ได้กำหนดมาตรการเชิงป้องกันในการกำหนดหน้าที่ให้ผู้ส่งต้องจัดให้มีข้อมูลระบุแจ้งเตือนถึงเนื้อหาในจดหมายหรือในข้อความ

ในส่วนการบ่งระบุว่าจดหมายมีเนื้อหาเกี่ยวกับเพศ ตามกฎหมาย CAN-SPAM อาจไม่เกี่ยวข้องและไม่สามารถนำมาใช้กับกฎหมายไทย เพราะการเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีเนื้อหาเกี่ยวกับเพศ หากเป็นข้อมูลลามกอนาจารแล้วจะเป็นความผิดตามมาตรา 14 ทั้งในกรณีข้อมูลลามกเด็กและผู้ใหญ่ ในขณะที่กฎหมาย

สหรัฐอเมริกาโดยทั่วไปแล้วกำหนดความผิดเฉพาะสื่อลามกเด็ก ดังนั้นข้อมูลคอมพิวเตอร์อันเป็นสื่อลามกผู้ใหญ่โดยทั่วไปแล้วไม่มีความผิด จึงมีหลักการให้แจ้งเตือนดังกล่าว

ในส่วนของการแจ้งเตือนหรือระบุบ่งชี้ว่าจดหมายหรือข้อความนั้นมีเนื้อหาเกี่ยวกับการโฆษณานั้น ตามกฎหมาย CAN-SPAM ซึ่งเป็นกฎหมายระดับรัฐบาลกลางไม่นำมาบัญญัติไว้ แต่การแจ้งเตือนดังกล่าว มีความสำคัญกับสิทธิของผู้บริโภค และสามารถนำมากำหนดในกฎหมายไทยได้ นอกจากกฎหมายสหรัฐอเมริกาแล้ว กฎหมายเฉพาะเกี่ยวกับสแปมของประเทศอื่นมีการนำหลักการนี้มาใช้ เช่น กฎหมายควบคุมสแปมของสิงค์โปร์ กำหนดว่า หากเนื้อหาเป็นการโฆษณาจะต้องมีตัวอักษรระบุว่า “ADV” ในส่วนของหัวข้อ (Spam Control Act, Second Schedule , Section 11) อย่างไรก็ตาม เมื่อพิจารณามาตรา 11 ปัจจุบันแล้ว จะเห็นได้ว่า การส่งจดหมายอิเล็กทรอนิกส์หรือข้อมูล คอมพิวเตอร์ที่มีเนื้อหาโฆษณา ไม่จำต้องระบุคำเตือนหรือข้อมูลบ่งชี้ว่า เนื้อหาในจดหมายหรือข้อความนั้นเกี่ยวข้องกับโฆษณา ในส่วนของการกำหนดให้ระบุข้อมูลบ่งชี้ตัวผู้ส่งที่ถูกต้องนั้นอาจพิจารณาว่าเป็นส่วนหนึ่งของหลัก “opt-out” ตามประกาศกระทรวงฯ ข้อ 5 แต่ตามกฎหมายต่างประเทศมีการบัญญัติแยกหน้าที่การระบุข้อมูลผู้ส่งออกมาจากหน้าที่การระบุข้อมูลเกี่ยวกับการบอกเลิก ทั้งนี้ การระบุข้อมูลผู้ส่งมีวัตถุประสงค์ในการแจ้งข้อมูลให้ผู้รับได้ทราบ และอาจไม่ใช่ที่อยู่อันเดียวกันกับที่ใช้ในการบอกเลิก

เมื่อพิจารณา มาตรา 11 วรรคสองและวรรคสาม จะเห็นได้ว่า การระบุแจ้งเตือนหรือบ่งชี้เนื้อหาจดหมายนั้นว่ามีเนื้อหาเกี่ยวกับการโฆษณา จัดเป็น “ลักษณะข้อมูล” ซึ่งหากมีการระบุไว้อาจทำให้ผู้รับสามารถคาดการณ์และตัดสินใจเกี่ยวกับจดหมายนั้นตั้งแต่แรกโดยไม่ต้องเปิดอ่าน จึงเป็นปัจจัยลดความเดือดร้อนรำคาญได้ โดยตาม มาตรา 11 วรรคสามระบุให้รัฐมนตรีกำหนด “ลักษณะข้อมูล” ที่ไม่ถือว่าเดือดร้อนรำคาญ อย่างไรก็ตาม ประกาศกระทรวงฯ ไม่ได้นำองค์ประกอบดังกล่าวมากำหนด

ประเด็นที่สี่ องค์ประกอบด้านวัตถุประสงค์เชิงพาณิชย์ (Commercial purpose)

ผลการศึกษาพบว่า โดยหลักแล้ว “จดหมายอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์” ที่อยู่ในขอบเขตกฎหมายเกี่ยวกับสแปม จะจำกัดเฉพาะ จดหมายหรือข้อความที่มีวัตถุประสงค์เชิงพาณิชย์ (Commercial electronic message) องค์ประ กอบนี้ทำให้กฎหมายสแปมไม่ครอบคลุมการติดต่อด้วยวัตถุประสงค์อื่นที่มิใช่เชิงการค้าหรือพาณิชย์ เช่น วัตถุประสงค์ความสัมพันธ์ส่วนบุคคล หรือวัตถุประสงค์ที่กฎหมายยกเว้น เช่น การกุศล หน่วยงานของรัฐที่ส่งข้อมูลตามที่กฎหมายกำหนด เป็นต้น ทั้งนี้เนื่องจากการส่งข้อมูลด้วยวัตถุ ประสงค์อื่นอาจเกี่ยวข้องกับกฎหมายอื่นที่มีวัตถุประสงค์เฉพาะและสอดคล้องกับการกระทำนั้น เช่น การติดต่อรบกวนในบริบทความสัมพันธ์ส่วนบุคคลอาจเกี่ยวข้องกับการกลั่นแกล้งรังแกทางอินเทอร์เน็ต หรือการเฝ้าติดตามคุกคามทางอินเทอร์เน็ต (Cyber bullying หรือ Cyber staking) ซึ่งจะอยู่ภายใต้ฐานความผิดเฉพาะที่มีองค์ประกอบแตกต่างจากสแปม

จากการศึกษาพบว่า กฎหมายเกี่ยวกับสแปมของหลายประเทศกำหนดองค์ประกอบ

ของสแปมที่อยู่ภายใต้ขอบเขตกฎหมายว่าจะต้องมีวัตถุประสงค์เชิงพาณิชย์ (Commercial purpose) เช่น

กฎหมายสหรัฐอเมริกา กฎหมายเกี่ยวกับสแปมในระดับรัฐบาลกลาง (CAN-SPAM Act) มีขอบเขตใช้บังคับกับข้อความอิเล็กทรอนิกส์เพื่อการพาณิชย์ (Commercial electronic mail message) ซึ่งนิยามว่า ข้อความอิเล็กทรอนิกส์เพื่อการพาณิชย์ใด ๆ ซึ่งมีวัตถุประสงค์หลักในการโฆษณาทางพาณิชย์หรือส่งเสริมการขายสินค้าหรือบริการทางพาณิชย์ รวมทั้งเนื้อหาบนเว็บไซต์ซึ่งดำเนินการเพื่อวัตถุประสงค์เชิงพาณิชย์ ในระดับมลรัฐนั้น กฎหมายเกี่ยวกับสแปมก็มีการกำหนดขอบเขตใช้เฉพาะข้อความอิเล็กทรอนิกส์เพื่อการพาณิชย์ เช่น กฎหมายมลรัฐ Arizona กำหนดนิยามเกี่ยวกับ “จดหมายพาณิชย์อิเล็กทรอนิกส์โดยผู้รับมิได้เรียกร้อง” (Unsolicited commercial electronic mail)

(Title 44, Trade and Commerce, Chapter 9, Trade practices generally, Article 16, Commercial Electronic mail) กฎหมายมลรัฐ California มีขอบเขตใช้บังคับกับ “จดหมายพาณิชย์อิเล็กทรอนิกส์เพื่อการโฆษณาโดยมิได้เรียกร้อง” (Unsolicited commercial e-mail advertisement) ซึ่งหมายถึง จดหมายพาณิชย์อิเล็กทรอนิกส์เพื่อการโฆษณาโดยมิได้เรียกร้องซึ่งส่งถึงผู้รับ (California business and professional code, Division 7, Part 3, Chapter 1, Article 1.8. Restrictions on Unsolicited Commercial E-mail Advertisers) Section 17529.1)

กฎหมายสหราชอาณาจักร กฎหมายเกี่ยวกับความเป็นส่วนตัวและการสื่อสารอิเล็กทรอนิกส์ (The Privacy and Electronic Communications (EC Directive) Regulations 2003) ซึ่งนำกฎหมายสหภาพยุโรป (Directive 2002/58/EC) มาบัญญัติเป็นกฎหมายภายในนั้น มีขอบเขตเฉพาะใช้กับ “การสื่อสารอิเล็กทรอนิกส์เพื่อวัตถุประสงค์ของการทำการตลาดทางตรง” จึงใช้กับกรณีการส่งสแปมเพื่อวัตถุประสงค์เชิงพาณิชย์เช่นกัน แต่มีขอบเขตจำกัดหรือแคบกว่ากฎหมายสหรัฐอเมริกา เนื่องจากไม่รวมถึงการสื่อสารเชิงพาณิชย์อื่นที่ไม่ใช่การตลาดทางตรง

วิเคราะห์เปรียบเทียบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พบว่า มาตรา 11 วรรคแรก ไม่ได้กำหนดองค์ประกอบเชิงพาณิชย์ ดังนั้น จึงครอบคลุมข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์โดยไม่จำกัดวัตถุประสงค์ หากเข้าองค์ประกอบปกปิดหรือปลอมแปลงแหล่งที่มาของการส่ง และ มีลักษณะเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ก็จะเป็นความผิดมาตรานี้ ซึ่งแตกต่างจากกฎหมายต่างประเทศที่จำกัดเฉพาะข้อความอิเล็กทรอนิกส์ที่มีวัตถุประสงค์เชิงพาณิชย์เท่านั้น สำหรับประกาศกระทรวงฯ นั้นเป็นการขยายความฐานความผิดตามวรรคสอง จึงไม่เกี่ยวข้องกับองค์ประกอบความผิดตามวรรคแรก จะเห็นได้ว่า การกำหนดฐานความผิดวรรคแรกแยกจากวรรคสอง และไม่นำองค์ประกอบเชิงพาณิชย์มากำหนดไว้ ส่งผลให้วรรคแรกอาจครอบคลุมไปถึงการติดต่อเพื่อวัตถุประสงค์ที่ไม่เกี่ยวกับเชิงพาณิชย์ เช่น ความสัมพันธ์ส่วนบุคคล อย่างไรก็ตาม สำหรับ

การส่งข้อความที่ผู้รับและผู้ติดต่อมีความสัมพันธ์ในทางธุรกรรมระหว่างกันมาก่อน (Transactional purpose) ซึ่งประกาศกระทรวงฯ ได้กำหนดรายละเอียดไว้ในฐานะการติดต่อซึ่งไม่เป็นการเดือดร้อนรำคาญตามฐานความผิดวรรคสองนั้น โดยหลักแล้วอาจอยู่ในขอบเขตฐานความผิดวรรคแรกได้

มาตรา 11 วรรคสอง มิได้กำหนดองค์ประกอบเชิงพาณิชย์ ดังนั้นโดยหลักการจึงครอบคลุมการส่งข้อมูลหรือจดหมายอิเล็กทรอนิกส์โดยไม่จำกัดวัตถุประสงค์ อย่างไรก็ตาม จากประกาศกระทรวงฯ ที่ออกตามความมาตรานี้ มีการนำ “องค์ประกอบเชิงพาณิชย์”เข้ามาบัญญัติไว้ด้วยดังจะเห็นได้จาก (1) นิยามของ“ผู้ส่งข้อมูล”ตามประกาศกระทรวงฯ ข้อ 3กำหนดว่า “บุคคลซึ่งมีเจตนาส่งข้อมูล คอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์ ในเบื้องต้นเพื่อประโยชน์ในทางการค้า ไม่ว่าจะเป็นการเสนอขายสินค้าหรือบริการ การลงทุน หรืออสังหาริมทรัพย์ใด ๆ...”(2) องค์ประกอบหลักของความผิดตามวรรคสอง คือ“ลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญ”โดยประกาศกระทรวงฯ ข้อ 4 (4) กำหนดขยายความองค์ประกอบดังกล่าวโดยกำหนดให้การส่งข้อมูลบางกรณี “ไม่ถือว่าก่อให้เกิดความเดือดร้อนรำคาญ”ซึ่งรวมถึง“...การส่งข้อมูล คอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ที่ไม่มีลักษณะผิดกฎหมาย ไม่ละเมิดสิทธิส่วนบุคคล และไม่มีวัตถุประสงค์ในเชิงพาณิชย์...” (3) ประกาศกระทรวงฯ ข้อ 5 กำหนดเงื่อนไขของการปฏิบัติตามหลัก “Opt-out”ว่า “ในกรณีที่เป็นการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ในเชิงพาณิชย์นอกเหนือจากที่ระบุในข้อ 4” กล่าวคือ การส่งข้อมูลที่ไม่ใช่ข้อมูลทางธุรกรรม หรืออาจกล่าวว่า เป็นกรณีที่มีวัตถุประสงค์เชิงพาณิชย์ ดังนั้นในแง่ของผลลัพธ์มีความคล้ายคลึงกับกฎหมายต่างประเทศ กล่าวคือ การส่งสแปมที่เกี่ยวกับวัตถุประสงค์เชิงพาณิชย์ เช่น การชักชวนให้ซื้อสินค้าหรือบริการ จะอยู่ภายใต้กฎหมายเกี่ยวกับสแปม โดยต้องปฏิบัติตามหลักต่างๆ เช่น “Opt-out” สำหรับการส่งสแปมที่ไม่มีวัตถุประสงค์เชิงพาณิชย์จะถือว่าไม่ “เดือดร้อนรำคาญ” และไม่เข้าองค์ประกอบความผิดตามมาตรา 11 วรรคสอง แต่ตามกฎหมายต่างประเทศ กรณีเช่นนี้ไม่อยู่ในขอบเขตของกฎหมายตั้งแต่ในส่วนของนิยาม

การกำหนดองค์ประกอบเชิงพาณิชย์ ทำให้จำแนกการติดต่อวัตถุประสงค์อื่น โดยเฉพาะความสัมพันธ์ส่วนบุคคลออกจากกฎหมายสแปม หากพิจารณากฎหมายต่างประเทศ พบว่า การติดต่อด้วยวัตถุประสงค์นี้ จะไม่อยู่ในขอบเขตของกฎหมายสแปมตั้งแต่ในขั้นตอนการพิจารณานิยามความหมายของ จดหมายหรือข้อความอิเล็กทรอ นิกส์เพื่อการพาณิชย์ แต่ตามมาตรา 11 วรรคสอง นั้น มิได้มีการนิยาม“จดหมายอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์” ไว้เป็นการเฉพาะว่าต้องมีวัตถุประสงค์เชิงพาณิชย์ดังเช่นกฎหมายต่างประเทศ โดยหลักแล้ว การติดต่อรบกวนด้วยวัตถุประสงค์ส่วนบุคคลจึงอยู่ในขอบเขตมาตรา 11 วรรคสอง แม้ประกาศกระทรวงฯ ยกเว้นการติดต่อที่ไม่มีวัตถุประสงค์เชิงพาณิชย์ แต่มีการกำหนดเงื่อนไขอื่นประกอบไปกับองค์ประกอบในเชิงพาณิชย์ด้วย กล่าวคือ “....การส่งข้อมูล คอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์ที่ไม่มีลักษณะผิดกฎหมาย ไม่ละเมิดสิทธิส่วนบุคคล และไม่มีวัตถุประสงค์ในเชิงพาณิชย์...” ทั้งนี้เนื่องจากใช้คำว่า “และ”

จึงอาจตีความว่ากรณีไม่มีวัตถุประสงค์เชิงพาณิชย์จะต้องมีลักษณะไม่ผิดกฎหมายและไม่ละเมิดสิทธิส่วนบุคคลด้วย ซึ่งมีความหมายกว้างกว่ากฎหมายต่างประเทศ ในแง่หนึ่งอาจครอบคลุมความผิดอื่น เช่น กลั่นแกล้งรังแกออนไลน์ เฝ้าติดตามคุกคามออนไลน์ แต่ในอีกแง่หนึ่ง สะท้อนถึงแนวคิดในการใช้กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์อย่างกว้างครอบคลุมพฤติกรรมที่ควรอยู่ภายใต้กรอบแนวคิดและหลักกฎหมายอื่น

องค์ประกอบ“เชิงพาณิชย์”ของจดหมายหรือข้อมูลคอมพิวเตอร์ ทำให้กฎหมายเกี่ยวกับ สแปมมีขอบเขตจำกัดแคบลง โดยไม่ครอบคลุมไปถึงการสื่อสารข้อมูลคอมพิวเตอร์ลักษณะอื่น ๆ ทั้งนี้หากพิจารณาในอีกแง่หนึ่งจะเห็นได้ว่า การส่งข้อมูลคอมพิวเตอร์เป็นวิธีการสื่อสารข้อมูล ซึ่งอาจเป็นการแสดงความคิดเห็นที่ได้รับการคุ้มครองในฐานะเสรีภาพพื้นฐานของประชาชน สำหรับกฎหมายที่จะจำกัดเสรีภาพดังกล่าว ก็จะต้องอยู่ภายใต้เงื่อนไขที่ว่าจะต้องไม่กว้างเกินไป ดังนั้น การกำหนดองค์ประกอบเชิงพาณิชย์เป็นปัจจัยที่ทำให้กฎหมายเกี่ยวกับสแปมไม่กว้างเกินไป เช่น กฎหมายเกี่ยวกับสแปมของมลรัฐ Virginia (Computer crimes: Section 18.2-152.3:1)

กำหนดองค์ประกอบความผิดสำหรับจดหมายอิเล็กทรอนิกส์ซึ่งผู้รับมิได้เรียกร้อง (Unsolicited e-mail) โดยไม่จำกัดว่าต้องเป็นกรณีการส่งในเชิงพาณิชย์ ส่งผลให้ครอบคลุมจดหมายหรือข้อความอิเล็กทรอนิกส์ที่ส่งด้วยวัตถุประสงค์ใดก็ตาม ศาลสูงสุดของมลรัฐตัดสินว่า (Commonwealth of Virginia V. Jeremy Jaynes) กฎหมายดังกล่าว ขัดต่อรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 1 เนื่องจากเป็นการขัดต่อเสรีภาพในการกล่าวข้อความ (Freedom of speech) โดยศาลให้เหตุผลว่ากฎหมายดังกล่าวไม่ได้มีขอบเขตจำกัดอยู่เฉพาะ (Narrowly tailored) จดหมายอิเล็กทรอนิกส์เกี่ยวกับการพาณิชย์ แต่มีขอบเขตรวมถึงจดหมายอิเล็กทรอนิกส์ใด ๆ ที่ผู้รับมิได้เรียกร้อง

ประเด็นที่ห้า การใช้หลัก “Opt-in” “Opt-out”

ผลการศึกษาพบว่ากฎหมายเกี่ยวกับสแปม ของต่างประเทศมีหลักการสองหลักที่แตกต่างกัน คือ

หลัก “Opt-in” มีหลักว่า การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์เพื่อการพาณิชย์หรือการโฆษณา จะต้องขออนุญาตจากผู้รับก่อน หรือเรียกว่า “ความยินยอมก่อนการติดต่อ (Prior consent)”

หลัก “Opt-out” มีหลักว่า หากผู้รับไม่ประสงค์จะได้รับการติดต่อในครั้งต่อไป ก็จะต้องมีกลไกในการให้ผู้รับแจ้งความประสงค์นั้น หรือที่เรียกว่า “บอกเลิกการรับ (Unsubscribe)” และผู้ส่งต้องเคารพเจตนาของผู้รับดังกล่าว ดังนั้น ผู้ส่งข้อมูลไม่จำต้องขอความยินยอมก่อนการส่ง

กฎหมายสหรัฐอเมริกากำหนดหลัก “Opt-out” กล่าวคือ ห้ามมิให้บุคคลใดริเริ่มส่งข้อความจดหมายพาณิชย์อิเล็กทรอนิกส์ เว้นแต่ในข้อความนั้นเป็นไปตามเงื่อนไขดังนี้ (ก) มีข้อมูลบ่งชี้อย่างชัดเจนว่าข้อความนั้นเป็นข้อความโฆษณาหรือติดต่อชักชวนทางธุรกิจ เว้นแต่ ผู้รับได้ให้ความยินยอม (Affirmative consent) (15 U.S.C., 7702 (1) (ข)) มีการแจ้งให้ทราบอย่างชัดเจนถึงโอกาสที่จะแจ้งความประสงค์ไม่รับข้อความต่อไปในอนาคต ทั้งนี้

ภายใต้หลักกฎหมายเกี่ยวกับการแจ้งความประสงค์ดังกล่าวมาแล้ว (15 U.S.C., 7704 (a) (3)) (ค) ที่อยู่ไปรษณีย์ทางกายภาพของผู้ส่งที่ใช้การได้ (a valid physical postal address of the sender)

กฎหมายสหราชอาณาจักร กำหนดหลัก “Opt-in” โดยนำกฎหมายสหภาพยุโรป (Directive 2002/58/EC หรือ “PECD) ดังกล่าวข้างต้น มาบัญญัติเป็นกฎหมายภายใน ได้แก่ กฎหมายเกี่ยวกับความเป็นส่วนตัวและการสื่อสารอิเล็กทรอนิกส์ (The Privacy and Electronic Communications (EC Directive) Regulations 2003 หรือ “PECR”) ซึ่งมีหลักห้ามการติดต่อสื่อสารเพื่อวัตถุประสงค์ของการตลาดทางตรง ตามประเภทของการติดต่อผ่านช่องทางต่างๆ 3 ช่องทางหลักได้แก่ โทรศัพท์ โทรสาร และช่องทางอิเล็กทรอนิกส์ สำหรับการติดต่อทางอิเล็กทรอนิกส์ซึ่งมีหลักว่า “ห้ามบุคคลใดส่งหรือก่อให้เกิดการสื่อสารโดยผู้รับมิได้เรียกร้องเพื่อวัตถุประสงค์ของการทำการตลาดทางตรงโดยใช้จดหมายอิเล็กทรอนิกส์ เว้นแต่ ผู้รับได้ให้ความยินยอมแก่ผู้ส่งไว้ก่อนแล้ว (Previously notified the sender that he consents)

วิเคราะห์เปรียบเทียบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พบว่า มาตรา 11 ตามกฎหมายฉบับก่อนแก้ไขปี 2560 นั้นมีหลักการว่า “ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท” จะเห็นได้ว่า ไม่ได้มีการนำหลักความยินยอม ทั้งกรณี “Opt- in” และ “Opt-out” มากำหนดเป็นองค์ประกอบ อย่างไรก็ตาม การแก้ไขมาตรา 11 ตามกฎหมายฉบับปี พ.ศ. 2560 ทำให้เกิดองค์ประกอบความผิดสองฐานดังนี้ มาตรา 11 วรรคหนึ่ง ความผิดฐานนี้มีองค์ประกอบเช่นเดียวกับมาตรา 11 เดิม โดยไม่มีการแก้ไขถ้อยคำสำหรับองค์ประกอบ “รบกวนการใช้งานระบบคอมพิวเตอร์ของผู้อื่น” ซึ่งไม่มีทั้งหลัก Opt-in และ Opt-out ในองค์ประกอบความผิดฐานนี้ มาตรา 11 วรรคสอง ประกอบกับประกาศกระทรวงฯ จากองค์ประกอบความผิด “เดือดร้อนรำคาญ” และ “เปิดโอกาสให้ผู้รับบอกเลิก” ตามมาตรา 11 วรรคสองประกอบกับประกาศกระทรวงฯ จึงกล่าวได้ว่า ฐานความผิดนี้ไม่ได้ใช้หลัก “Opt-in” ดังเช่นกฎหมายสหราชอาณาจักรและกฎหมายสหภาพยุโรป แต่ใช้หลัก “Opt-out” ซึ่งเป็นแนวทางเดียวกับกฎหมาย CAN-SPAM ของสหรัฐอเมริกา ทำให้ผู้ส่งสามารถส่งจดหมายหรือข้อความไปยังบุคคลที่ตนไม่รู้จักหรือไม่มีความสัมพันธ์กันมาก่อนได้ โดยมีเงื่อนไขตามหลัก “Opt-out”สำหรับประกาศกระทรวงฯ ข้อ 5 (4) ที่กำหนดหลักการ “Opt-out” นั้น วางเงื่อนไขว่าเมื่อผู้รับข้อมูลส่งคำสั่งบอกเลิกไปแล้ว แต่ผู้ส่งฝ่าฝืนส่งข้อมูลซ้ำ ดังนี้ผู้ส่งยังไม่มีความผิด แต่วางเงื่อนไขว่าผู้รับข้อมูลจะต้องส่งคำสั่งบอกเลิกอีกเป็นครั้งที่สอง ทั้งทางจดหมายอิเล็กทรอนิกส์และไปรษณีย์ลงทะเบียน หากผู้ส่งฝ่าฝืนอีกครั้งหรือทำการส่งซ้ำเป็นครั้งที่สาม จึงถือว่าผู้ส่งมีความผิด ซึ่งผลการศึกษาชี้ให้เห็นปัญหาสองประการคือ

ประการที่หนึ่ง การกำหนดกฎหมายเพื่อควบคุมสแปมด้วยระบบ “Opt-out” ดังเช่นแนวทางของกฎหมาย CAN-SPAM ของสหรัฐ

อเมริกานั้น อาจพิจารณาว่าเป็นแนวทางที่ให้น้ำหนักกับการคุ้มครองสิทธิของบุคคลผู้รับการติดต่อน้อยไป เนื่องจากผู้ส่งสามารถทำการติดต่อครั้งแรกโดยไม่ผิดกฎหมาย เพียงแต่ต้องทำตามเงื่อนไขโดยระบุรายละเอียดสำหรับการปฏิเสธ ดังนั้นกฎหมายสแปมของอีกหลายประเทศจึงใช้แนวทาง “Opt-in” สำหรับประกาศกระทรวงฯ ที่กำหนดเงื่อนไขเพิ่มเติมสำหรับการบอกเลิกครั้งที่สอง ทำให้วิพากษ์วิจารณ์ว่าให้น้ำ หนักกับการควบคุมสแปมน้อยกว่ากฎหมายสหรัฐอเมริกา เนื่องจากเปิดโอกาสให้ส่งซ้ำได้ถึงครั้งที่สาม

ประการที่สอง สำหรับการบอกเลิกครั้งแรก ประกาศกระทรวงฯ ไม่ได้กำหนดวิธีการบอกเลิกว่าจะต้องกระทำด้วยวิธีการหรือช่องทางใด อีกทั้งไม่กำหนดว่าจะต้องบอกเลิกด้วยวิธีการที่สามารถยืนยันว่าผู้ส่งได้รับคำสั่งนั้นแล้ว เช่นการใช้ไปรษณีย์ลงทะเบียน แต่ในขั้นตอนการแจ้งครั้งที่สอง ประกาศกระทรวงฯ กำหนดให้ต้องมีการแจ้งด้วยวิธีไปรษณีย์ลงทะเบียน ซึ่งเป็นค่าใช้จ่ายที่ผู้บริโภคต้องรับภาระ โดยเฉพาะอย่างยิ่งการส่งสแปมอาจเกิดขึ้นได้ในทุกขณะโดยผู้ส่งต่างรายกัน ดังนั้น ระบบ “Opt-out” ตามประกาศกระทรวงฯ ซึ่งผู้รับต้องแจ้งครั้งที่สอง ทำให้ผู้รับต้องมีค่าใช้จ่าย และอาจส่งผลให้ผู้รับเลือกที่จะยุติกระบวนการเรียกร้องให้ยกเลิกการส่งสแปม หลักการกำหนดให้ยืนยันด้วยไปรษณีย์ตอบรับไม่ปรากฏในกฎหมายต่างประเทศ เช่น กฎหมาย CAN-SPAM ของสหรัฐอเมริกาด้วย จึงเห็นว่าวัตถุประสงค์ของมาตรา 11 มุ่งคุ้มครองผู้บริโภคให้สามารถใช้สิทธิบอกเลิกโดยง่ายและไม่มีค่าใช้จ่ายทั้งที่เกิดจากผู้ส่งและค่าใช้จ่ายอื่นที่เกี่ยวข้องด้วย โดยนัยนี้จึงเห็นว่าเงื่อนไขตามประกาศกระทรวงฯ อาจไม่สอด คล้องกับเจตนารมณ์ของมาตรา 11

สรุปและข้อเสนอแนะ

จากผลการศึกษาข้างต้นผู้วิจัยมีข้อสรุปและข้อเสนอแนะตามประเด็น ดังนี้

ประเด็นที่หนึ่ง ผลการศึกษาชี้ให้เห็นว่าฐานความผิดสแปมตามมาตรา 11 มิได้มีการกำหนด องค์ประกอบที่เกี่ยวเนื่องกับขั้นตอนการได้มาซึ่งข้อมูลของผู้ส่ง ซึ่งเป็นขั้นตอนแรกที่สำคัญของการได้มาซึ่งที่อยู่ในการส่งสแปม

ผู้วิจัยจึงมีข้อเสนอแนะให้ปรับปรุงแก้ไขกฎหมายโดยเพิ่มเติมหลักการได้มาซึ่งที่อยู่อิเล็กทรอนิกส์ โดยจำแนกเป็นพฤติกรรมต่างๆ เช่น การซื้อขายโปรแกรมสำหรับการเก็บรวบรวมที่อยู่อิเล็กทรอนิกส์ ดังเช่นกฎหมายสหรัฐอเมริกา

ผลการวิจัยชี้ให้เห็นว่า ฐานความผิดสแปมตามมาตรา 11 ไม่ได้กำหนดองค์ประกอบเกี่ยวกับการใช้วิธีอัตโนมัติในการได้มาซึ่งที่อยู่อิเล็กทรอนิกส์ ซึ่งอาจต้องพิจารณาการปรับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฐานอื่นในขณะที่กฎหมายต่างประเทศกำหนดหลักการนี้ไว้ในหมวดสแปมโดยเฉพาะ

ผู้วิจัยจึงมีข้อเสนอแนะให้ปรับปรุงแก้ไขกฎหมายโดยเพิ่มหลักการได้มาซึ่งที่อยู่อิเล็กทรอนิกส์ด้วยวิธีอัตโนมัติไว้ในหมวดความผิดเกี่ยวกับสแปมโดยเฉพาะ โดยอาจเป็นความผิดมาตรา 11/1 เป็นต้น

ประเด็นที่สอง ผลการวิจัยชี้ให้เห็นว่ากฎหมายสหรัฐอเมริกาจะพบว่า กฎหมายระดับรัฐบาลกลางและกฎหมายบางมลรัฐ มีการกำหนดองค์ประกอบด้านปริมาณและความถี่ไว้

อย่างเฉพาะเจาะจงในตัวบทกฎหมาย ซึ่งกฎหมายไทย มาตรา 11 วรรคสามให้รัฐมนตรีออกประกาศกระทรวงฯ กำหนดรายละเอียดประเด็น ปริมาณ และความถี่ไว้ แต่ตามประกาศกระทรวงฯ ยังไม่มีการนำองค์ประกอบทั้งด้านปริมาณและความถี่มากำหนดไว้

ผู้วิจัยจึงมีข้อเสนอแนะให้มีการออกประกาศกระทรวงฯ เพิ่มเติมรายละเอียดเชิงปริมาณและความถี่ของการส่งสแปมดังเช่นกฎหมายต่างประเทศ เช่น สหรัฐอเมริกา ซึ่งบัญญัติไว้ทั้งระดับรัฐบาลกลางและมลรัฐ เป็นต้น

ประเด็นที่สาม ผลการวิจัยชี้ให้เห็นว่ากฎหมายสแปมของต่างประเทศเช่น สหรัฐอเมริกา มีการกำหนดหลักการแจ้งเตือนในหัวเรื่อง กล่าวคือ แจ้งเตือนเนื้อหาเกี่ยวกับเพศและ เนื้อหาโฆษณา แต่ไม่ปรากฏหลักการดังกล่าวตามมาตรา 11 เมื่อพิจารณา มาตรา 11 วรรคสองและวรรคสาม จะเห็นได้ว่า การระบุแจ้งเตือนหรือบ่งชี้เนื้อหาจดหมายนั้นว่ามีเนื้อหาเกี่ยวกับการโฆษณา จัดเป็น “ลักษณะข้อมูล” โดยตาม มาตรา 11 วรรคสามระบุให้รัฐมนตรีกำหนด “ลักษณะข้อมูล”ที่ไม่ถือว่าเดือดร้อนรำคาญ อย่างไรก็ตาม ประกาศกระทรวงฯ ไม่ได้นำองค์ประกอบดังกล่าวมากำหนด จึงเสนอให้มีการเพิ่มเติมหลักดังกล่าวในประกาศกระทรวงฯ

ประเด็นที่สี่ ผลการวิจัยชี้ให้เห็นว่าองค์ประกอบ “เชิงพาณิชย์” ของจดหมายหรือข้อมูลคอมพิวเตอร์ ทำให้กฎหมายเกี่ยวกับสแปมมีขอบเขตจำกัดแคบลง โดยไม่ครอบคลุมไปถึงการสื่อสารข้อมูลคอมพิวเตอร์ลักษณะอื่น ๆ เพื่อมิให้กระทบต่อเสรีภาพในการสื่อสาร โดยกฎหมายต่างประเทศกำหนดองค์ประกอบนี้ในนิยาม อย่างไรก็ตาม มาตรา 11 ไม่ได้กำหนดนิยามจดหมายอิเล็กทรอนิกส์ว่าไม่รวมถึงกรณีจดหมายหรือข้อมูลที่ไม่มีวัตถุประสงค์เชิงพาณิชย์ตั้งแต่ต้น ทำให้โดยหลักแล้วจดหมายหรือข้อมูลทั้งเชิงพาณิชย์และไม่มีวัตถุประสงค์เชิงพาณิชย์อยู่ในขอบเขตมาตรา 11 แม้ประกาศกระทรวงฯ ยกเว้นการติดต่อที่ไม่มีวัตถุประสงค์เชิงพาณิชย์ แต่กำหนดเงื่อนไขอื่นประกอบไปกับ องค์ประกอบในเชิงพาณิชย์ กล่าวคือ“...การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ที่ไม่มีลักษณะผิดกฎหมาย ไม่ละเมิดสิทธิส่วนบุคคล และไม่มีวัตถุประสงค์ในเชิงพาณิชย์...” ทั้งนี้เนื่องจากใช้คำว่า “และ” จึงอาจตีความว่ากรณีไม่มีวัตถุประสงค์เชิงพาณิชย์จะต้องมีลักษณะไม่ผิดกฎหมายและไม่ละเมิดสิทธิส่วนบุคคลด้วย ซึ่งมีความหมายกว้างกว่ากฎหมายต่างประเทศ ในแง่หนึ่งอาจครอบคลุมความผิดอื่น เช่น กลั่นแกล้งรังแกออนไลน์ เฝ้าติดตามคุกคามออนไลน์ แต่ในอีกแง่หนึ่ง สะท้อนถึงแนวคิดในการใช้กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์อย่างกว้างครอบคลุมพฤติกรรมที่ควรอยู่ภายใต้กรอบแนวคิดและหลักกฎหมายอื่น

ผู้วิจัยจึงมีข้อเสนอให้แก้ไขกฎหมาย โดยกำหนดนิยามของ จดหมายอิเล็กทรอนิกส์ ที่อยู่ในขอบเขตมาตรา 11 ว่าหมายถึง “จดหมายอิเล็กทรอนิกส์เพื่อการพาณิชย์” ดังเช่นกฎหมายต่างประเทศ ทำให้การติดต่อในวัตถุประสงค์อื่นไม่ต้องเข้ามาอยู่ในระบบของกฎหมายเกี่ยวกับสแปมตั้งแต่ในชั้นแรก เพื่อให้การติดต่อรบกวนอื่น ๆ อยู่ภายใต้กฎหมายอื่น เช่น กฎหมายอาญา กฎหมายการกลั่นแกล้งออนไลน์ซึ่งมีวัตถุประสงค์ และหลักการที่แตกต่างจากสแปมตามกฎหมายต่างประเทศที่ใช้เฉพาะการติดต่อเชิงพาณิชย์เพื่อการโฆษณาเท่านั้น

ประเด็นที่ห้า ผลการวิจัยชี้ให้เห็นว่า มาตรา 11 ที่แก้ไขปี พ.ศ. 2560 นำหลัก “Opt-out” มาใช้ แต่มีปัญหาว่า เป็นระบบที่ให้การคุ้มครองสิทธิส่วนบุคคลน้อยกว่าหลัก “Opt-in” อีกทั้งกฎหมายไทยยังกำหนดเงื่อนไขให้ต้องบอกเลิกถึงครั้งที่สองซึ่งมากกว่ากฎหมายสหรัฐอเมริกา รวมทั้งกำหนดให้ต้องบอกเลิกครั้งที่สองต้องส่งทางไปรษณีย์ตอบรับอันเกิดค่าใช้จ่ายต่อผู้บริโภค ผู้วิจัยจึงมีข้อเสนอว่า ควรแก้ไขเป็นหลัก “Opt-in” ดังเช่นกฎหมายสหราชอาณาจักรและกฎหมายยุโรป หรือหากคงหลัก “Opt-out” ก็เสนอให้ลดการบอกเลิกเป็นเพียงการแจ้งครั้งแรก และไม่ต้องกำหนดให้ใช้วิธีไปรษณีย์ตอบรับเพื่อลดภาระค่าใช้จ่ายผู้บริโภค

References

Bambauer, E. Derek. (2005). Solving the Inbox Paradox: An Information-based policy Approach to Unsolicited E-mail Advertising, **10 VA.Journal of law & Technology** 5: 8-14.

Bray, Hiawatha. (1996). **Getting Rid of Junk E-Mail**. Boston Globe, Sept. 26.

DeCew , Judith Wagner. (1997). **In Pursuit of Privacy: Law Ethics and The Rise of Technology**. US:Cornell University Press.

Donnelly, Jack. (1982). Human Rights and Human Dignity. **The American Law Review**, 76, No.2 (1982).

Hansell, S. (2003). **Diverging Estimates of the Cost of Spam**. New York Times, July 27.

Hossein Bidgoli (2006) **Handbook of Information Security, Information Warfare, Social, Legal, and International issues, and Security Foundations, U.**S.: John Wiley & Sons, Inc.. Volume 2

Schwabach, Aaron (2014), **Internet and the Law: Technology, Society, and Compromises**, 2nd Edition, ABC-CLIO LLC, .p223.

Sorkin, David. (2001).Technical and Legal Approaches to Unsolicited Electronic Mail. **University of San Francisco Law Review**, Vol. 35. 325

Wacks, Raymond. (1989). **Personal Information: Privacy and the Law**. UK: Oxford Clarendon Press.