ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยความรับผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 กับการส่งอีเมลเชิงพาณิชย์ในลักษณะสแปม (spam)

นางสาวชัญญารักษ์ แซ่ห่าน

เอกัตศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรมหาบัณฑิต
สาขาวิชากฎหมายเศรษฐกิจ
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2560

หัวข้อเอกัตศึกษา	ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยความรับผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 กับการส่งอีเมลเชิงพาณิชย์ในลักษณะสแปม (spam)
โดย	นางสาวชัญญารักษ์ แซ่ห่าน
รหัสประจ ตัว	5986166034
หลักสูตร	ศิลปศาสตรมหาบัณฑิต สาขาวิชากฎหมายเศรษฐกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
หมวดวิชา	กฎหมายธุรกิจทั่วไป
อาจารย์ที่ปรึกษา	อาจารย์ ดร. ณัชพล จิตติรัตน์
ปีการศึกษา	2560

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้เอกัตศึกษาฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรมหาบัณฑิต สาขาวิชากฎหมายเศรษฐกิจ

ลงชื่อ.....อาจารย์ที่ปรึกษา

(อาจารย์ ดร. ณัชพล จิตติรัตน์)

ชัญญารักษ์ แซ่ห่าน : ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยความรับผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 กับการส่งอีเมลเชิงพาณิชย์ในลักษณะสแปม (spam) อาจารย์ที่ปรึกษา : ดร. ณัชพล จิตติรัตน์, 106 หน้า

เอกัตศึกษาฉบับนี้มีวัตถุประสงค์เพื่อศึกษาปัญหาเกี่ยวกับบังคับใช้พระราชบัญญัติว่าด้วยความรับผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 กับการส่งอีเมลเชิงพาณิชย์ในลักษณะสแปม (spam) รวมทั้งศึกษาทฤษฎี แนวคิด และมาตรการทางกฎหมายที่เกี่ยวข้องกับการกระทาความผิดเกี่ยวกับสแปมปัจจุบันทั้งในประเทศไทยและต่างประเทศ เพื่อนามาวิเคราะห์เปรียบเทียบ และเพื่อเสนอแนะแนวทางในการเพิ่มเติมบทบัญญัติกฎหมายที่เหมาะสม รวมไปถึงแนวทางในการใช้อีเมลเชิงพาณิชย์เพื่อการโฆษณาให้เกิดประสิทธิภาพสูงสุด ในขณะที่ยังสามารถปกป้องสิทธิความความเป็นอยู่ส่วนบุคคลของผู้บริโภคได้อย่างเป็นธรรม

จากการศึกษาพบว่าปัจจุบัน พระราชบัญญัติว่าด้วยความรับผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ยังไม่สามารถคุ้มครองสิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภคได้เพียงพอ เนื่องจากไม่มีหลักเกณฑ์ที่แน่ชัดในเรื่องการตั้งชื่อหัวเรื่องของอีเมล (Heading) ซึ่งกระทบต่อสิทธิในการรับรู้คาพรรณนาที่ถูกต้องและเพียงพอของผู้รับ เนื่องจากผู้รับไม่สามารถตัดสินใจก่อนเปิดอ่านอีเมลเชิงพาณิชย์เหล่านั้นได้ ซึ่งนอกจะทาให้สิ้นเปลืองข้อมูลอินเทอร์เน็ต ยังมีความเสี่ยงในการติดไวรัสหรือมัลแวร์อีกด้วย ยิ่งไปกว่านั้นกฎหมายยังไม่ได้กาหนดขนาด ความถี่ และปริมาณในการส่งที่เหมาะสมกับอัตราการส่งผ่านข้อมูลระบบเครือข่ายอินเทอร์เน็ตในปัจจุบัน ทาให้ผู้รับมีโอกาสได้รับอีเมลเชิงพาณิชย์เป็นจานวนมากจนรบกวนการใช้งานพื้นที่ในกล่องข้อความของตนอย่างปกติสุข และยังทาให้ผู้ให้บริการอินเทอร์เน็ต (ISPs) หรือผู้ดูแลระบบต้องแบกรับภาระค่าใช้จ่ายในการบริหารจัดการหรือขยายแบนด์วิดท์ (Bandwidth) หรือเซิร์ฟเวอร์ (server) เพื่อรองรับกับปริมาณข้อมูลโฆษณาที่มีจานวนมากกว่าครึ่งของอีเมลทั้งหมดบนระบบอินเทอร์เน็ต อีกทั้งยังต้องเป็นฝ่ายจัดหาพัฒนาระบบหรือมาตรการในการป้องกันสแปมเมลให้ทันสมัยอยู่เสมอเพื่อรองรับกับปัญหาที่เกิดขึ้น

อย่างไรก็ตาม การที่ผู้ประกอบการต้องขอความยินยอมก่อนทาการส่งอีเมลโฆษณาโดยใช้หลัก Opt-in เพียงอย่างเดียว เป็นการจากัดสิทธิในการโฆษณามากเกินไปเช่นกัน ดังนั้นจึงควรพิจารณาปรับใช้หลัก inferred consent ในกรณีเป็นการโฆษณาสินค้าอื่นที่มีลักษณะใกล้เคียงกับสินค้าเดิมที่ผู้รับให้คายินยอมไว้โดยเปิดช่องทางให้ผู้รับนั้นสามารถบอกปฏิเสธการรับได้โดยง่าย เพื่อเพิ่มอิสระให้แก่ผู้ประกอบการและส่งเสริมความคล่องตัวในการท ทการตลาด

กิตติกรรมประกาศ

เอกัตศึกษาฉบับนี้สำเร็จลุล่วงไปได้ด้วยการให้ความช่วยเหลือแนะนำของอาจารย์ ดร. ณัชพล จิตติรัตน์ ซึ่งเป็นอาจารย์ที่ปรึกษาที่ได้กรุณาที่ให้คำแนะนำข้อคิดเห็น ตรวจสอบ และแก้ไขร่างเอกัตศึกษามาโดยตลอด ผู้เขียนจึงขอกราบขอบพระคุณไว้ ณ โอกาสนี้

ผู้เขียนขอขอบคุณ นางสาว นิชา ทรงธีระปัญญา และนาย พิสิษฐ์ เมธาธรรม ที่ได้ช่วยตรวจแก้ไขเอกัตศึกษาฉบับนี้ให้ถูกต้องสมบูรณ์ยิ่งขึ้น และคอยให้กำลังใจตลอดมาจนเอกัตศึกษาฉบับนี้สำเร็จลุล่วงไปด้วยดี

ท้ายนี้ผู้เขียนขอขอบคุณมารดา และครอบครัว ที่ให้ความเข้าใจและเปิดโอกาสให้ได้รับการศึกษา ผู้เขียนขอให้เป็นกตเวทิตาแด่ มารดา ครอบครัวของผู้เขียน ตลอดจนผู้เขียนหนังสือและบทความต่างๆที่ให้ความรู้แก่ผู้เขียน หากเอกัตศึกษาฉบับนี้มีความบกพร่องประการใด ผู้เขียนขอน้อมรับความผิดพลาดไว้แต่เพียงผู้เดียว

นางสาวชัญญารักษ์ แซ่ห่าน

สารบัญ

หน้า

บทที่ 1 บทน า

1.1 ที่มาและความส าคัญของปัญหา..... 1

1.2 สมมติฐานของการศึกษา..... 3

1.3 วัตถุประสงค์ในการศึกษา..... 3

1.4 ขอบเขตของการศึกษา..... 3

1.5 วิธีการศึกษาวิจัย..... 4

1.6 ประโยชน์ที่คาดว่าจะได้รับ..... 4

บทที่ 2 การกระท าความผิดฐานอีเมลเชิงพาณิชย์ในลักษณะสแปม (spam)

2.1 ที่มาของการกระท าผิดเกี่ยวกับสแปม (spam) 5

2.1.1 ความหมายของสแปม (spam) 6

2.1.2 จุดก าเนิดของสแปม (spam) 7

2.1.3 ลักษณะและประเภทของสแปม (spam) 9

2.1.3.1 ลักษณะโดยทั่วไปของสแปมเมล (spam mail)..... 9

2.1.3.2 ประเภทของสแปม (spam) 11

2.2 แนวความคิดที่เกี่ยวกับกระทาความผิดในลักษณะสแปม (spam) 12

2.3 ปัญหาอันเกิดจากการกระท าความผิดเกี่ยวกับสแปม (spam) 13

2.3.1 การละเมิดสิทธิสิทธิในความเป็นอยู่ส่วนบุคคล (Rights of Privacy) 13

2.3.2 ต้นทุนในการด าเนินธุรกิจของผู้ประกอบการ..... 16

2.3.3 ความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน..... 17

2.3.4 ความรับผิดทางอาญา..... 19

2.4 บทบาทของภาครัฐในการหามาตรการควบคุมการกระท าความผิดฐานส่งข้อมูลหรืออีเมลในลักษณะสแปม (spam) 21

2.4.1 ลักษณะของหลักเกณฑ์ Opt-in และ Opt-out 21

2.4.2 จุดประสงค์ที่ภาครัฐจ าเป็นต้องเข้ามาแทรกแซงการส่งข้อมูลหรืออีเมลในลักษณะสแปม (spam) 22

2.5 การใช้อีเมลในลักษณะสแปมเพื่อจุดประสงค์เชิงพาณิชย์ในปัจจุบัน..... 24

2.5.1 สถานการณ์การตลาด e-commerce ในปัจจุบัน..... 25

2.5.2 สถิติการท าสแปมเมลและฟิชชิ่ง (spam mail & phishing) 29

บทที่ 3 กฎหมายเกี่ยวกับการกระทำผิดในรูปแบบสแปม (spam) ของประเทศไทย

3.1 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 33

3.1.1 วัตถุประสงค์ของพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ 34

3.2 การกำหนดความผิดและบทลงโทษของความผิดแต่ละประเภทของผู้ใช้งานคอมพิวเตอร์ 35

3.3 การกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ 38

3.4 การกำหนดอำนาจหน้าที่ของผู้ให้บริการ 40

3.5 สาระสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 41

3.6 สรุปสาระสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 47

3.6.1 ขอบเขตในการส่งสแปมเมล (spam mail) 47

3.6.2 การดูแลและป้องกันข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ 48

3.6.3 การกระทำอันเป็นความผิดฐานหมิ่นประมาท 49

3.6.4 ผู้ให้บริการ 49

3.6.5 การคุ้มครองความเสียหายต่อบุคคลธรรมดา 49

3.6.6 การลงโทษผู้กระทำความผิด 50

3.6.7 การเชื่อมโยงความร่วมมือของพนักงานเจ้าหน้าที่ในทุกภาคส่วน 50

3.6.8 พนักงานเจ้าหน้าที่ 50

บทที่ 4 กฎหมายเกี่ยวกับการกระทำผิดในรูปแบบสแปม (spam) ในต่างประเทศ

4.1 ความหมายของการกระทำความผิดในลักษณะสแปม (spam) 51

4.2 กฎหมายต่อต้านการกระทำความผิดเกี่ยวกับสแปมในประเทศสหรัฐอเมริกา 53

4.2.1 ที่มาของ CAN-SPAM 54

4.2.2 จุดประสงค์ของกฎหมาย CAN-SPAM 56

4.2.3 การนิยามของคำศัพท์ที่เกี่ยวข้อง 56

4.2.4 ลักษณะของอีเมลที่ถูกควบคุมการส่งโดย CAN-SPAM 58

4.2.5 สาระสำคัญของกฎหมาย CAN-SPAM 59

4.2.6 หน้าที่ของภาคธุรกิจในใช้อีเมลเชิงพาณิชย์เพื่อโฆษณาประชาสัมพันธ์ 62

4.2.7 การกระทำที่เป็นความผิดตามกฎหมาย CAN-SPAM 63

4.2.8 บทลงโทษของการกระทำความผิดตามกฎมาย CAN-SPAM 63

4.3 กฎหมายต่อต้านการกระท าความผิดเกี่ยวกับสแปมในสหภาพยุโรป..... 64
4.3.1 ระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
(Data Protection Directive 95/46/EC) 65
4.3.2 ระเบียบว่าด้วยสิทธิส่วนบุคคลในระบบโทรคมนาคม
(Telecommunications Privacy Directives 97/66/EC) 66
4.3.3 ระเบียบว่าด้วยการพาณิชย์อิเล็กทรอนิกส์
(E-Commerce Directive 2000/31/EC) 67
4.3.4 ระเบียบว่าด้วยความเป็นส่วนตัวทางอิเล็กทรอนิกส์
(E-Privacy Directive 2002/58/EC)..... 67
4.4 สรุปความแตกต่างของหลักเกณฑ์ในการบังคับใช้กฎหมายต่อต้านการกระท าความผิด
เกี่ยวกับสแปมในสหรัฐอเมริกาและสหภาพยุโรป..... 68

บทที่ 5 วิเคราะห์มาตรการในการบังคับใช้พระราชบัญญัติว่าด้วยการกระท าผิดเกี่ยวกับคอมพิวเตอร์ในประเทศไทย

5.1 หลักเกณฑ์พิจารณาการกระท าความผิดเกี่ยวกับสแปม (spam) 72
5.1.1 วิเคราะห์ข้อดี-ข้อเสียของหลักเกณฑ์ Opt-in และ Opt-out..... 77
5.1.2 โทษและอัตราโทษ..... 82
5.1.3 สถานการณ์ในการบังคับใช้พระราชบัญญัติว่าด้วยการกระทาความผิดเกี่ยวกับ
คอมพิวเตอร์ในประเทศไทย..... 83
5.2 ข้อที่นักการตลาดพึงระวังในการใช้อีเมลเชิงพาณิชย์เพื่อท าการตลาด..... 88
5.2.1 การศึกษากลุ่มลูกค้าเป้าหมายเพื่อให้เกิดประสิทธิภาพในการสื่อสาร..... 89
5.2.2 การสร้างเนื้อหาที่เหมาะสมและเกิดประสิทธิภาพในการจูงใจผู้บริโภค..... 90
5.2.3 ขนาดและจ านวนอีเมลเชิงพาณิชย์ที่เหมาะสมส าหรับการส่งออกในแต่ละครั้ง..... 92
5.3 การคุ้มครองสิทธิในความเป็นอยู่ส่วนบุคคล (Rights of privacy) ของผู้บริโภค..... 94

บทที่ 6 บทสรุปและข้อเสนอแนะ

6.1 บทสรุป..... 97
6.2 ข้อเสนอแนะ..... 102

บรรณานุกรม..... 107

สารบัญตาราง

		หน้า
ตารางที่ 1	เปรียบเทียบความแตกต่างของพระราชบัญญัติฯปี2550 กับปี2560.....	41
ตารางที่ 2	สรุปความแตกต่างของหลักเกณฑ์ในการบังคับใช้กฎหมายต่อต้านการกระท า ความผิดเกี่ยวกับสแปมเมลในสหรัฐอเมริกาและสหภาพยุโรป.....	69
ตารางที่ 3	องค์ประกอบทางความผิดฐานส่งสแปมเมล.....	77
ตารางที่ 4	เปรียบเทียบลักษณะของหลักเกณฑ์ Opt-in และ Opt-out.....	78

สารบัญรูปภาพ

		หน้า
ภาพที่ 1	ข่าวตีกทรุดขณะก่อสร้างจากหนังสือพิมพ์ผู้จัดการออนไลน์	18
ภาพที่ 2	ผลส าจจจ าจนผู้ใช้อินเทอร์เน็ตในประเทศไทยประจ ไตรมาสแรกปี 2559	26
ภาพที่ 3	สัดส่วนธุรกิจพาณิชย์อิเล็กทรอนิกส์จ าแนกตามขนาดของธุรกิจประจ าปี2557	26
ภาพที่ 4	มูลค่า e-commerce ในประเทศไทยปี 2557-2560	27
ภาพที่ 5	ตัวอย่างโฟลเดอร์ Promotion ในอีเมล	28
ภาพที่ 6	จ านวนอีเมลที่โปรแกรม Antivirus ดักจับว่าเป็นสแปม ไตรมาสที่ 1-2 ปี2560	29
ภาพที่ 7	ตัวอย่างอีเมลที่แผงมัลแวร์เข้ามาในไฟล์แนบ	30
ภาพที่ 8	ตัวอย่างอีเมลที่หลอกให้ผู้รับคลิกลิงก์ที่หลอกว่าเป็นวิธีแก้ไขมัลแวร์	30
ภาพที่ 9	ประเภทของอีเมล Phishing ที่สามารถตรวจจับได้ในไตรมาสที่สอง ปี2560	31
ภาพที่ 10	ตัวอย่างหน้าเว็บไซต์ปลอม	32
ภาพที่ 11	ผลลัพธ์จากการวิจัยโดยใช้แบบสอบถามเรื่องการท าการตลาดผ่านอีเมล (e-mail marketing) กับประชากรชาวมาเลเซีย 70 คน โดยมหาวิทยาลัย University of Malaya และ Multimedia University	79
ภาพที่ 12	Infographic แสดงผลการส ารวจเกี่ยวกับรูปแบบการโฆษณาที่ได้รับความเชื่อถือจากผู้บริโภค “Global Trust in Advertising 2015” โดยบริษัทนีลเส็น (Nielsen) ประเทศไทย	80
ภาพที่ 13	แผนภาพสรุปการพิจารณาความผิดฐานท าสแปมมลในประเทศไทย	81
ภาพที่ 14	ตัวอย่างจากแอปพลิเคชันของ Watsons ที่ระบุให้ผู้ลงทะเบียนต้องท าการยินยอมในการรับข่าวสารอย่างน้อย 2 ช่องทาง	85
ภาพที่ 15	ตัวอย่างแอปพลิเคชัน 11 street และ Pomelo ที่ใส่เครื่องหมายในช่องยินยอมเพื่อรับข้อมูลข่าวสารเอาไว้ล่วงหน้า	86
ภาพที่ 16	ตัวอย่างลักษณะการพาดหัวข่าวเพื่อจุดประสงค์ในการคลิกเบต	88
ภาพที่ 17	ผลการส ารวจความยาวของหัวเรื่อง (subject) อีเมลที่ส่งผลต่ออัตราการเปิดอ่านโดยผู้รับ	91
ภาพที่ 18	ข้อดีของการท าตลาดออนไลน์	104
ภาพที่ 19	ตัวอย่างจากแอปพลิเคชัน Shopee ที่ใช้รูปแบบ Double Opt-in ในการลงทะเบียนและ Subscribe	105

บทที่ 1

บทน า

1.1 ที่มาและความส คัญของปัญหา

ปัจจุบันการใช้คอมพิวเตอร์และอินเทอร์เน็ต มีความสาคัญต่อชีวิตประจาวันของมนุษย์เป็นอย่างมาก เพราะอินเทอร์เน็ตคือเทคโนโลยีที่ท ให้เกิดการติดต่อสื่อสารอย่างรวดเร็วและทั่วถึง อีกทั้งยังสามารถใช้ค้นคว้าหาข้อมูลข่าวสารต่างๆในทั่วทุกมุมโลกได้อย่างทันยุคทันเหตุการณ์ แต่ถึงแม้อินเทอร์เน็ตจะมีข้อดีอยู่มากมาย ถ้าผู้ใช้งานใช้ในทางที่ผิดเพื่อแสวงหาผลประโยชน์ส่วนตน หรือใช้งานอย่างประมาทเลินเล่อ เทคโนโลยีนี้อาจกลายเป็นดาบสองคมย้อนมาทาร้ายผู้ใช้งานได้เช่นกัน ยกตัวอย่างเช่น การใช้สื่อคอมพิวเตอร์ในทางที่ไม่เหมาะสมและก่อให้เกิดความเสียหายแก่ผู้อื่นเกิดขึ้นมากมาย ไม่ว่าจะเป็นการใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลเท็จเพื่อให้เกิดความวุ่นวายในสังคม หรือการส่งต่อข้อมูลที่มีลักษณะลามกอนาจาร การตัดต่อภาพของผู้อื่นในทางเสียหายแล้วเผยแพร่ลงบนสื่อสังคมออนไลน์ (Social Media)

เนื่องจากปัญหาการใช้เทคโนโลยีคอมพิวเตอร์ในทางมิชอบ ก่อให้เกิดความเสียหายและกระทบกระเทือนต่อเศรษฐกิจ สังคม ความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน รัฐบาลจึงได้ประกาศใช้พระราชบัญญัติว่าด้วยการกระทาผิดเกี่ยวกับคอมพิวเตอร์ โดยคณะรัฐมนตรียกร่างเสนอต่อสภานิติบัญญัติแห่งชาติและประกาศในราชกิจจานุเบกษาเมื่อวันที่ 18 มิถุนายน 2550 มีผลบังคับใช้เมื่อวันที่ 18 กรกฎาคม 2550 ซึ่งต่อมามีการเปิดรับฟังความเห็นจากประชาชนอยู่เสมอ จนในที่สุดจึงมีการปรับแก้ไขบทบัญญัติ เพื่อให้สามารถรองรับกับการพัฒนาที่รวดเร็วของเทคโนโลยีและพฤติกรรมการใช้อินเทอร์เน็ตของผู้บริโภค

ต่อมามีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ซึ่งได้แก้ไขเพิ่มเติมบทบัญญัติและอัตราโทษ อีกทั้งยังกาหนดให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมออกประกาศเพิ่มเติมเพื่อกาหนดมาตรการทางกฎหมายให้มีความชัดเจนมากขึ้น ซึ่งบทบัญญัติที่มีผลกระทบต่อการส่งอีเมลเชิงพาณิชย์ ได้แก่ มาตรา 4 ว่าด้วยเรื่องการส่งอีเมลไม่พึงประสงค์อันเป็นการก่อให้เกิดความเดือดร้อนราคาญ โดยมีการเพิ่มวรรคสองต่อจากมาตรา 11 ของพระราชบัญญัติฯเดิม ดังต่อไปนี้ “ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิด ความเดือดร้อนราคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับ สามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกิน 200,000 บาท ให้รัฐมนตรีออกประกาศกาหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของ ข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนราคาญแก่ผู้รับและลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย” ดังนั้น ผู้ใดที่ทาการส่งข้อมูลหรืออีเมลโฆษณา หรือโพสต์ข้อความ

โฆษณาบนสื่อสังคมออนไลน์ของคนอื่น ไม่ว่าจะเป็นเฟสบุ๊กหรืออินสตาแกรมโดยที่เจ้าของไม่ได้ให้คายินยอมต่อกระทาการดังกล่าว จะเข้าข่ายการส่งข้อมูลอิเล็กทรอนิกส์อันก่อให้เกิดความรคาญ ซึ่งถือเป็นการกระท าผิดตามพระราชบัญญัติข้างต้น

ในยุคที่ช่องทางการทาการตลาดไม่ได้จากัดอยู่เพียงแค่สื่อสิ่งพิมพ์ โทรทัศน์ วิทยุ หรือป้ายโฆษณากลางแจ้งเหมือนสมัยก่อน เทคโนโลยีด้านการโฆษณาประชาสัมพันธ์และพฤติกรรมการรับข้อมูลของผู้บริโภคได้ก้าวเข้ามาอยู่ในโลกอินเทอร์เน็ต ดังจะเห็นได้จากมูลค่าการเติบโตของตลาดพาณิชย์อิเล็กทรอนิกส์ (e-commerce) ของประเทศไทยปี 2560 เทียบกับปี 2559 ที่มีแนวโน้มการเติบโตอย่างต่อเนื่องกว่า 9.86% โดยสถาบัน ETDA คาดการณ์มูลค่ารวมของตลาดพาณิชย์อิเล็กทรอนิกส์ (e-commerce) ในปี 2560 ไว้สูงถึง 2,812,592.03 ล้านบาท[1] ซึ่งอัตราการเติบโตนี้มีผลทาให้การแข่งขันในตลาดออนไลน์ทวีความรุนแรงมากขึ้นไปด้วยเช่นกัน ผู้ประกอบการต่างพยายามหาช่องทางที่มีประสิทธิภาพในการติดต่อสื่อสารกับผู้บริโภค เพื่อสร้างการรับรู้ (awareness) ความสนใจ (interest) และกระตุ้นการซื้อ (motivation)

แม้ว่าเทคโนโลยีจะเข้ามาช่วยให้การสื่อสารทางตรงไปยังผู้บริโภคสามารถทาได้ง่ายขึ้น แต่การส่งข้อความโฆษณาเหล่านั้นออกไปโดยไม่ได้รับความยินยอมจากผู้รับล่วงหน้าจะถือว่าเป็นสแปมหรือไม่ ยังคงเป็นประเด็นที่แต่ละประเทศมีความเห็นแตกต่างกัน หากเป็นการโฆษณาสินค้าที่น่าสงสัย สื่อลามกอนาจาร บริการที่ก้ากึ่งผิดกฎหมาย หรือจดหมายลูกโซ่ คงจะไม่ยากอะไรที่ประชาชนทั่วไปจะทราบว่านั่นคือการกระทาที่มีความผิดทางกฎหมาย แต่สิ่งหนึ่งที่ผู้ใช้งานอินเตอร์เน็ตส่วนใหญ่อาจลืมตระหนักไป คือ ถึงสินค้านั้นจะเป็นสิ่งถูกกฎหมายก็ตาม แต่หากการด าเนินกิจกรรมการโฆษณาทาโดยไม่เหมาะสม หรือเข้าข่ายเป็นการรุกรานสิทธิความเป็นอยู่ส่วนบุคคล หรือก่อให้เกิดภาระค่าใช้จ่ายจากการรับโฆษณาที่ผู้รับไม่ต้องการนั้น ย่อมเป็นการกระทาที่เอาผิดตามกฎหมายได้ด้วยเช่นกัน

ถึงแม้การเผยแพร่โฆษณาด้วยวิธีทาสแปมจะเป็นวิธีที่ใช้ต้นทุนต่า แต่ภาระค่าใช้จ่ายในการส่งข้อมูลที่เกิดขึ้นส่วนใหญ่กลับตกไปเป็นของผู้รับหรือผู้ให้บริการ (Service Provider) ที่ต้องเสียค่าอินเทอร์เน็ต ค่าบริการจัดการ เสียเวลาในการคัดกรองข้อมูล เสียพื้นที่เซิร์ฟเวอร์ในการจัดเก็บ และยังต้องเสียค่าใช้จ่ายในการพัฒนาระบบป้องกัน กลั่นกรองข้อมูลที่ไม่พึงประสงค์เหล่านี้เพื่อป้องกันผลกระทบที่จะเกิดกับผู้ใช้งานอีกด้วย ยิ่งไปกว่านั้นการได้รับข้อความสแปมเป็นจานวนมากย่อมทาให้ผู้ใช้เกิดความรู้สึกด้านลบ และถือได้ว่าเป็นการรบกวนสิทธิในความเป็นอยู่ส่วนบุคคล (Rights of Privacy) ของผู้รับ ดังนั้น นักการตลาดที่ดีจึงควรทาความเข้าใจถึงวิธีการโฆษณาที่ก่อให้เกิดประสิทธิภาพสูงสุด สอดคล้องกับกฎหมาย และไม่ทาให้ผู้บริโภครู้สึกร คาญ เพื่อสร้างภาพลักษณ์ที่ดีต่อตัวสินค้า รวมทั้งป้องกันไม่ให้เกิดทัศนคติแง่ลบกับการโฆษณาที่เข้าข่ายเป็นสแปม

---

[1] สานักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA), ผลสารวจพฤติกรรมผู้ใช้อินเทอร์เน็ตและมูลค่าอีคอมเมิร์ซ [ออนไลน์]. แหล่งที่มา: https://www.etda.or.th/content/value-of-e-commerce-survey-in-thailand-2017.html [เข้าถึงเมื่อ 24 พฤษภาคม, 2017]

1.2 สมมติฐานในการวิจัย

พระราชบัญญัติว่าด้วยความรับผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 ยังไม่สามารถคุ้มครองสิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภคได้เพียงพอและยังขาดความชัดเจน จึงทาให้ผู้ประกอบการไม่สามารถน มาอ้างอิงเพื่อเป็นหลักเกณฑ์ในการส่งอีเมลเชิงพาณิชย์ ดังนั้น จึงควรเพิ่มหลักเกณฑ์เรื่องการแสดงหัวเรื่อง (Heading) กาหนดเกณฑ์ของจานวน ความถี่ ปริมาณ ขนาดของข้อมูลโฆษณา และปรับใช้หลัก inferred consent เพื่อช่วยอานวยความสะดวกและส่งเสริมการทากิจกรรมทางการตลาดของภาคธุรกิจ และเพื่อปกป้องสิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภคได้อย่างเป็นธรรม

1.3 วัตถุประสงค์การศึกษา

1.3.1 เพื่อทราบถึงแนวคิดและทฤษฎีที่เกี่ยวข้องกับกระทาความผิดเกี่ยวกับสแปม และการใช้มาตรการทางกฎหมายเพื่อป้องกันการกระท าผิดดังกล่าว

1.3.2 เพื่อทราบถึงกฎหมายและมาตรการทางกฎหมายในการต่อต้านการกระทาความผิดเกี่ยวกับสแปมของต่างประเทศ อันได้แก่ สหรัฐอเมริกา และสหภาพยุโรป

1.3.3 เพื่อวิเคราะห์เปรียบเทียบหลักเกณฑ์ที่ใช้ในการก หนดมาตรการทางกฎหมายเกี่ยวกับการต่อต้านการกระท าความผิดเกี่ยวกับสแปม (หลัก Opt-in และ Opt-out)

1.3.4 เพื่อทราบถึงขอบเขตการส่งอีเมลเชิงพาณิชย์ที่ไม่ก่อให้เกิดความเดือดร้อนราคาญแก่ผู้รับข้อมูล

1.3.5 เพื่อทราบถึงผลกระทบจากพระราชบัญญัติว่าด้วยการกระทาผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 ที่มีต่อการส่งอีเมลเชิงพาณิชย์ในปัจจุบัน

1.3.6 เพื่อเสนอแนะแนวทางในการกาหนดมาตรการทางกฎหมายที่เหมาะสมเพื่อให้เกิดความเป็นธรรมต่อผู้ประกอบการที่ต้องการทาการตลาดผ่านอีเมล

1.3.7 เพื่อเสนอแนะแนวทางในการส่งอีเมลเชิงพาณิชย์ให้แก่ผู้ประกอบการ เพื่อให้เกิดจริยธรรมในการโฆษณา และสามารถใช้อีเมลเชิงพาณิชย์เพื่อทาการตลาดได้อย่างถูกต้องตามกฎหมาย

1.4 ขอบเขตการศึกษา

เอกัตศึกษาฉบับนี้มุ่งศึกษาเฉพาะกรณีปัญหาเรื่องผลกระทบต่อการดาเนินกิจกรรมทางการตลาดในรูปแบบการส่งอีเมลเชิงพาณิชย์ของภาคเอกชนตามพระราชบัญญัติว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มาตรา 4 ที่บัญญัติถึงการส่งข้อมูลผ่านระบบอิเล็กทรอนิกส์ที่มีลักษณะเป็นการก่อให้เกิดความเดือดร้อนราคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรืออีเมล โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ซึ่งหมายถึงการส่งอีเมลสแปม (spam) ในเชิงพาณิชย์ โดยศึกษาจากหนังสือและบทความ คาพิพากษาของศาล โดยในเนื้อหาของเอกัตศึกษาฉบับนี้จะกล่าวถึง กฎหมายที่เกี่ยวข้องกับการกระทา

ความผิดเกี่ยวกับคอมพิวเตอร์ ปัญหาและอุปสรรค รวมทั้งข้อสังเกตต่างๆ โดยศึกษาเปรียบเทียบกับกฎหมายต่างประเทศอันได้แก่ สหรัฐอเมริกา และสหภาพยุโรป

1.5 วิธีการศึกษาวิจัย

การศึกษานี้จะใช้การวิจัยเชิงเอกสาร (Documentary Research) เป็นหลัก โดยจะศึกษาค้นคว้าและวิเคราะห์ข้อมูลจากตัวบทกฎหมาย ข้อเท็จจริง และผลการวิเคราะห์จากสานักต่างๆที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ รวมถึงบทความและข้อมูลจากเว็บไซต์ต่างๆ เพื่อพิจารณาเสนอแนวทางที่จะท าให้เกิดประโยชน์สูงสุดต่อทั้งภาครัฐและธุรกิจ

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ท าให้ทราบแนวคิดและทฤษฎีที่เกี่ยวข้องกับกระท าความผิดเกี่ยวกับสแปม และการใช้มาตรการทางกฎหมายเพื่อป้องกันการกระท าผิดดังกล่าว

1.6.2 ท าให้ทราบถึงกฎหมายและมาตรการทางกฎหมายในการต่อต้านการกระท าความผิดเกี่ยวกับสแปมของต่างประเทศ อันได้แก่ สหรัฐอเมริกา และสหภาพยุโรป

1.6.3 ท าให้ทราบถึงความแตกต่างของหลักเกณฑ์ที่ใช้ในการก าหนดมาตรการทางกฎหมายเกี่ยวกับการต่อต้านการกระท าความผิดเกี่ยวกับสแปม (หลัก Opt-in และ Opt-out)

1.6.4 ท าให้ทราบถึงหลักเกณฑ์และขอบเขตในการส่งอีเมลเชิงพาณิชย์ที่ไม่ก่อให้เกิดความเดือดร้อนร าคาญใจแก่ผู้รับ

1.6.5 ท าให้ทราบถึงผลกระทบจากพระราชบัญญัติว่าด้วยการกระท าผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 ที่มีต่อการส่งอีเมลเชิงพาณิชย์ในปัจจุบัน

1.6.6 ท าให้ทราบถึงแนวทางการใช้อีเมลเชิงพาณิชย์เพื่อท าการตลาดที่ก่อให้เกิดประสิทธิภาพสูงสุด และไม่ขัดต่อพระราชบัญญัติว่าด้วยการกระท าผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560

1.6.7 ท าให้ทราบถึงแนวทางที่เหมาะสมในการนากฎหมายต่างประเทศมาปรับใช้กับบริบทในประเทศไทย โดยการเพิ่มเติมกฎหมายเพื่อให้สามารถตอบสนองต่อสภาวะทางธุรกิจปัจจุบัน และช่วยให้ผู้ประกอบการสามารถส่งอีเมลเชิงพาณิชย์ได้อย่างมีประสิทธิภาพ ในขณะที่ยังคงคุ้มครองสิทธิในความเป็นอยู่ส่วนบุคคล (Rights of privacy) ของผู้บริโภค

บทที่ 2
การกระทาความผิดฐานส่งอีเมลเชิงพาณิชย์ในลักษณะสแปม (spam)

“สแปม”(spam) หรือที่รู้จักในนามของ “จดหมายขยะ” โดยทั่วไปเป็นการส่งอีเมลที่มีเนื้อหา (content) เชิงพาณิชย์ไปยังผู้รับจานวนมากโดยที่ผู้รับเองไม่ได้ต้องการหรือไม่เคยมีความสัมพันธ์ใดๆกับผู้ส่งนั้นมาก่อน การทาสแปมเริ่มมามีบทบาทมากในช่วงยุคศตวรรษที่ 20 เพราะเป็นยุคที่การใช้อินเทอร์เน็ตได้รับความนิยมและเข้ามาเป็นส่วนหนึ่งในชีวิตประจาวันของคนทั่วไป ทาให้ผู้ประกอบการจานวนมากเริ่มเล็งเห็นโอกาสในการใช้อีเมลเป็นช่องทางในการโฆษณาประชาสัมพันธ์สินค้าหรือบริการ หรือส่งต่อข้อมูลทางการตลาดต่างๆให้แก่ผู้บริโภคโดยตรง (e-mail marketing) อย่างไรก็ตาม หากผู้ประกอบการหลายรายส่งอีเมลจานวนมากออกมาพร้อมๆกัน จานวนอีเมลที่มากมายมหาศาลนั้น ย่อมส่งผลกระทบต่อระบบอินเทอร์เน็ต พื้นที่ในกล่องข้อความของผู้รับและเกิดภาระในการบริหารจัดการของผู้ให้บริการที่เกี่ยวข้องกับการส่งอีเมล

หากการทาสแปมจากัดอยู่แค่จุดประสงค์เพื่อการโฆษณาเชิงพาณิชย์ มาตรการทางแพ่งก็คงจะเพียงพอที่จะใช้จัดการปัญหาที่เกิดขึ้นได้ แต่ในระยะหลัง การกระทารูปแบบนี้เริ่มลุกลามไปถึงการก่ออาชญากรรมทางคอมพิวเตอร์ โดยผู้ทาสแปม (spammer) หลายรายใช้การส่งอีเมลเป็นเครื่องมือในการกระจายไวรัส มัลแวร์ หรือใช้เนื้อหาเพื่อเชิญชวนให้ผู้รับกดลิงก์เชื่อมโยง (Hyperlink) ไปยังหน้าเว็ปปลอมที่สร้างเอาไว้หลอกลวงผู้บริโภคหรือที่สร้างไว้เพื่อใช้ขโมยข้อมูลส่วนบุคคลของผู้บริโภค (phishing) การกระทาดังกล่าวจึงถือเป็นความผิดที่รัฐควรเข้ามามีบทบาทในการปราบปรามและควบคุมดูแลเพื่อให้เกิดความสงบสุขในสังคม โดยในบทนี้จะอธิบายถึง 2.1 ที่มาของการกระทาผิดเกี่ยวกับสแปม 2.2 แนวความคิดที่เกี่ยวกับการกระทาความผิดในลักษณะสแปม 2.3 ปัญหาอันเกิดจากการกระทาความผิดเกี่ยวกับสแปม 2.4 บทบาทของภาครัฐในการหามาตรการควบคุมกระทาความผิดฐานส่งข้อมูลหรืออีเมลในลักษณะสแปม (spam)และ 2.5 การใช้อีเมลในลักษณะสแปมเพื่อจุดประสงค์เชิงพาณิชย์ในปัจจุบัน เพื่อให้ผู้อ่านมีความเข้าใจเกี่ยวกับการกระทาความผิดเกี่ยวกับสแปมมากขึ้น

2.1 ที่มาของการกระท ผิดเกี่ยวกับสแปม (spam)

สแปมเป็นการกระทาความผิดรูปแบบหนึ่งที่เกิดขึ้นช่วงปลายศตวรรษที่ 19 ซึ่งเป็นยุคที่ 6 (Sixth Generation) ของการพัฒนาคอมพิวเตอร์[1] เพราะเป็นช่วงที่คอมพิวเตอร์มีวิวัฒนาการแบบก้าวกระโดดจนสามารถลดขนาดตัวเครื่องให้เล็กลงพอที่จะนามาวางในบ้านหรือสานักงานทั่วไปได้ ประกอบกับราคาที่ลดลง ธุรกิจทั่วไปที่ไม่ใช่บริษัทยักษ์ใหญ่หรือประชาชนธรรมดาจึงสามารถซื้อหาคอมพิวเตอร์มาใช้เพื่อการสื่อสาร หรือนามาใช้ได้ทั่วไปในวิถีชีวิตประจาวันได้ ความรุ่งโรจน์ของยุคอินเทอร์เน็ต ทาให้ทั้งภาครัฐ ภาคธุรกิจ และภาคครัวเรือนต่างก็หันมาการใช้งานระบบเครือข่ายและอาศัยข้อดีของอินเทอร์เน็ตในการอานวยความสะดวกในชีวิตประจาวัน ผู้ประกอบการหลายรายเล็งเห็นโอกาสในการดาเนินกิจกรรมทางการตลาดผ่านทางช่องทางที่แสนสะดวกสบายนี้ จนท าให้การ

[1] สถาบันนวัตกรรมและพัฒนากระบวนการเรียนรู้มหาวิทยาลัยมหิดล. ยุคของคอมพิวเตอร์ [ออนไลน์]. 2017. แหล่งที่มา: http://www.il.mahidol.ac.th/e-media/computer/evolution/6thGeneration.html [6 กุมภาพันธ์ 2018]

ส่งอีเมลโฆษณาเข้าหากลุ่มลูกค้าโดยตรงเกิดขึ้นเป็นจานวนมาก จนในที่สุดกลายเป็นปัญหาที่สร้างความเดือดร้อนราคาญให้แก่ผู้รับ และส่งผลกระทบต่อผู้ให้บริการเครื่อข่ายอินเทอร์เน็ต (Internet Service Provider : ISPs) ในด้านต่างๆมากมาย

2.1.1 ความหมายของสแปม (spam)

สแปม (spam) หมายถึง “ข้อความที่ไม่ได้ถูกร้องขอให้ส่ง” (unsolicited message) ผ่านสื่ออิเล็กทรอนิกส์ในรูปแบบต่างๆ ไม่ว่าจะเป็น อีเมล การบริการส่งข้อความสั้นผ่านทางโทรศัพท์ (SMS) ข้อความทางโทรสาร (Fax) การส่งผ่าน Bluetooth เข้าหาโทรศัพท์หรือเครื่องช่วยงานส่วนบุคคลแบบดิจิทัล (PDA) หรือเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยตรง หรือแม้กระทั้งการโพสต์ผ่านสื่อสังคมออนไลน์ (Social Media) ต่างๆ โดยที่ผู้ส่งข้อมูลไม่ได้รับการยินยอมจากผู้รับล่วงหน้า หรือเป็นข้อความอันมีลักษณะที่ก่อให้เกิดความเดือดร้อนหรือร าคาญใจ และไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ทั้งนี้ อาจเป็นการส่งถึงผู้รับทั้งแบบเจาะจงและไม่เจาะจง ซึ่งถือเป็นการละเมิดสิทธิความเป็นอยู่ส่วนบุคคลของผู้ที่ใช้งานระบบบริการการสื่อสารแบบอิเล็กทรอนิกส์ (Electronic Communication Service)[2] โดยพระราชบัญญัติว่าด้วยการกระทาความผิดทางคอมพิวเตอร์ของประเทศไทย ได้ให้ความหมายและกาหนดโทษของความผิดฐานส่งสแปมไว้ในมาตรา 11[3] ว่า สแปมคืออีเมลที่ถูกส่งมาโดยที่ผู้ส่งปกปิดตัวตน (Anonymous remailer) หรือปลอมแปลงตัวตน (Spoofing) ซึ่งท ให้ผู้รับเกิดความเดือดร้อนราคาญ หรือเป็นการรบกวนระบบของคอมพิวเตอร์ของผู้รับหรือผู้ให้บริการเครือข่าย อินเทอร์เน็ต รวมทั้งเป็นอีเมลที่ไม่มีช่องทางให้ผู้รับสามารถบอกเลิก (Opt-out) หรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับ (unsubscribe) ได้

---

[2] Eleni Kosta; Peggy Valcke; David Stevens. Spam, Spam, Spam, Spam Lovely Spam: Whyis Bluespam Different. 23 Int'l Rev. L. Computers&Tech. 89 (2009).

[3] พระราชบัญญัติว่าด้วยการกระทาความผิดทางคอมพิวเตอร์ พ.ศ. 2560 มาตรา 11 “ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนร าคญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกินสองแสนบาท

ให้รัฐมนตรีออกประกาศก หนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนร าคญแก่ผู้รับและลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย”

2.1.2 จุดกำเนิดของสแปม (spam)

เดิมทีคำว่า “SPAM” เป็นเพียงเครื่องหมายการค้าของเนื้อสัตว์บรรจุกระป๋องยี่ห้อหนึ่งที่ได้รับความนิยมมากในช่วงสงครามโลกครั้งที่สอง ผลิตโดยบริษัท Hormel Foods Corporation ซึ่งใช้ตัวอักษรนี้เป็นเครื่องหมายการค้ามาตั้งแต่ปี 1930 ต่อมาในปี 1970 รายการตลกชื่อดังของอังกฤษรายการหนึ่งชื่อ Monty Python ใช้คำว่า SPAM เป็นวลีหลักในบทละครตลกที่มีเรื่องราวเกิดขึ้นในร้านอาหาร ตัวเอกคือลูกค้าคู่หนุ่มสาวที่เข้าไปสั่งอาหารในร้านอาหารนั้น แล้วพบว่าในเมนูมีแต่คำว่า SPAM อยู่เต็มไปหมด จนลูกค้าคนอื่นๆในร้านต่างก็ร้องออกมาเป็นเพลงว่า “Spam, Spam, Spam, Spammity Spam, Wonderful Spam” วนไปวนมา และบทละครทั้งเรื่องมีแต่คำว่า SPAM จานวนมาก ไม่ว่าตัวละครตัวไหนต่างๆก็ร้องแต่คำว่า SPAM ซ้าไปซ้ามาจนฟังดูน่าราคาญ นับแต่นั้นเป็นต้นมา คนส่วนใหญ่จึงติดภาพว่า SPAM หมายถึงสิ่งที่กวนใจ สิ่งน่าราคาญ อย่างไรก็ตาม ผู้จัดทารายการทีวีรายการนั้นไม่ได้มีการขออนุญาต หรือถามความเห็นจากจากบริษัท Hormel Foods Corporation ก่อนที่จะนาคาๆนี้มาใช้ หลังจากที่รายการนี้ออกอากาศได้พักใหญ่ บริษัท Hormel ดาเนินการฟ้องร้องผู้จัดรายการในฐานละเมิดลิขสิทธิเครื่องหมายการค้าและเป็นการดูหมิ่นเครื่องหมายการค้าท าให้เกิดความเสื่อมเสียชื่อเสียง[4]

ต่อมาเมื่อถึงยุคที่อินเทอร์เน็ตแพร่หลาย และคาว่า spam ถูกใช้ในการอธิบายถึง “อีเมลที่ส่งโดยไม่ได้ถูกร้องขอ” ทางบริษัท Hormel Foods ถึงขั้นต้องสร้างเวปไซด์ขึ้นมาเพื่อออกประกาศทาความเข้าใจแก่บุคคลทั่วไปว่า “SPAM” ที่เป็นตัวอักษรพิมพ์ใหญ่นี้นั้น เป็นเครื่องหมายการค้าของบริษัทตน และขอความร่วมมือเพื่อสงวนคานี้ไว้ และยินยอมให้ใช้คาว่า “spam” ที่เป็นตัวอักษรพิมพ์เล็กในฐานะค าแสลงเพื่ออธิบายถึงอีเมลที่ส่งโดยไม่ได้ถูกร้องขอให้ส่งนี้[5]

การกระทาความผิดในรูปแบบสแปมเมลเกิดขึ้นตั้งแต่เมื่อ 40 ปีก่อน โดยมีการค้นพบหลักฐานเกี่ยวกับการกระทาความผิดด้านสแปมเมลครั้งแรกเมื่อวันที่ 3 พฤษภาคม 1978 โดยพนักงานขายชื่อ Gary Thuerk ใช้คอมพิวเตอร์ของเขาส่งอีเมลที่มีเนื้อหาโฆษณาเมนเฟรมคอมพิวเตอร์ (Mainframe) รูปแบบใหม่ของบริษัท Hewlett-Packard Co.,Ltd ไปยังทุกๆบัญชีอีเมลในเขต West Coast ของสหรัฐอเมริกา ที่มีประวัติเชื่อมต่ออยู่ใน ARPANET (ระบบเครือข่ายหลักก่อนที่จะเปลี่ยนมาเป็น “อินเทอร์เน็ต” ในปัจจุบัน) ซึ่งมีจานวนมากถึง 593 อีเมล ในคราวเดียว แม้ว่าการส่งครั้งนั้นจะมีกระแสตอบรับจากผู้บริโภคทั้งดีและไม่ดี แต่เนื่องจากอีเมลของเขามีขนาดใหญ่เกินไปจนกินพื้นที่ในกล่องข้อความ (Mail Boxe) ของผู้ที่ได้รับอีเมล จนส่งผลต่อระบบการทางานของคอมพิวเตอร์ของผู้ใช้บางส่วน ทางผู้ดูแลระบบของ ARPANET จึงต้องแก้ปัญหาโดยส่งจดหมายไปยังผู้จัดการของ Thuerk ว่าการใช้เครือข่ายด้วยจุดประสงค์เชิงพาณิชย์นั้นขัดต่อนโยบายการใช้งานของเครือข่าย และร้องขอให้ Gary Thuerk หยุดทาการโฆษณาด้วยวิธีดังกล่าว

---

[4] Cori Phelan, Hormel Foods Corp. v. Jim Henson Productions, Inc., 73 F.3d 497 (2d Cir. 1996), 6 DePaul J. Art, Tech. & Intell. Prop. L. 313 (1996)

[5] นางสาวศศิมา ศรีพจน์ธรรม. มาตรการทางกฎหมายเพื่อการจัดการจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงประสงค์ (Spam Mail). ปริญญาตรี, คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2548, หน้า 14.

ถึงแม้ว่าโดยส่วนตัวแล้วเขาจะรู้สึกว่านี่เป็นวิธีที่มีประสิทธิภาพมากในการโฆษณาด้วยต้นทุนต่ำ[6] แต่เขาก็ยอมหยุดการกระทำดังกล่าวไปในที่สุด

16 ปีถัดมา มีการพบหลักฐานการเกิดสแปมอีกครั้งในวันที่ 12 เมษายน 1994 โดยนาย Laurence Canter และนาง Martha Siegel สองทนายชาว Arizona ทำการโฆษณางานบริการด้านการให้คำปรึกษาเกี่ยวกับการย้ายถิ่นที่อยู่ โดยการส่งข้อความภายใต้หัวข้อ "Green Card Lottery - Final One?" เข้ากลุ่มสนทนาใน USENET กว่า 5,500 กลุ่มพร้อมๆกัน ซึ่งถือว่าเป็นปริมาณที่เยอะมากในขณะนั้น ทำให้ผู้ใช้งานได้รับข้อความแบบเดียวกันนี้ซ้ำๆผ่านจากทุกๆกลุ่ม ซึ่งในขณะนั้นยังไม่มีมาตรการทางแพ่งออกมารองรับอย่างเป็นทางการ และทางตำรวจหรือผู้ที่เกี่ยวข้องก็ยังไม่ได้ให้ความสนใจปัญหานี้มากเท่าไรนัก ทำให้ผู้ให้บริการเครือข่ายอินเทอร์เน็ต (ISPs) ทั้งหลายเริ่มมีการเจรจาเกี่ยวกับเรื่องมาตรการเพื่อรวบรวมรายชื่อผู้ที่มีส่วนเกี่ยวข้องกับการทำสแปม (Anti-Spam Blacklists) กันเอง แม้ว่าจะไม่ได้มีการบังคับใช้อย่างเป็นทางการ แต่ก็เริ่มมีบทลงโทษที่ไม่เป็นทางการออกมาให้เห็น โดยหลังจากที่ฝ่าย ISPs ของระบบที่ทนายทั้งสองคนใช้งานได้รับการร้องเรียนจากผู้ใช้เป็นจำนวนมาก ผู้ดูแลระบบจึงทำการตรวจค้นเมลเซิร์ฟเวอร์ (mail server) ของพวกเขา แล้วสองวันหลังจากนั้นก็มีการออกประกาศเพื่อขอระงับการบริการทันที ทำให้ทนายทั้งสองเกิดความไม่พอใจแต่ยังไม่หยุดการกระทำ หลังจากนั้นยังมีการโพสต์โฆษณาตัวอื่นไปยังกลุ่มกว่า 1,000 newsgroups อีกครั้ง ในเดือนมิถุนายน 1994 แต่ครั้งนี้ Arnt Gulbrandsen ได้สร้างซอฟต์แวร์ “cancelbot” ออกมาแก้ไขปัญหานี้ได้อย่างทันท่วงที โดย ซอฟต์แวร์ ตัวนี้จะทำการหว่านหาข้อความโฆษณาของ Canter กับ Siegel บนระบบแล้วทำลายทิ้งในทันที ทำให้การทำสแปมของทนายทั้งสองต้องยุติลงนับแต่นั้นเป็นต้นมา โดยต่อมาพวกเขาได้ออกมาให้สัมภาษณ์กับสื่อในเดือนธันวาคม 1994 ว่าการโฆษณาครั้งนั้นทำให้เขาทั้งสองได้ลูกค้าใหม่มากว่า 1,000 คน และสร้างกำไรได้ถึง 100,000 ดอลลาร์[7] จากค่าใช้จ่ายที่เขาใช้ไปในการโฆษณาไปเพียงแค่ 1 เพนนีเท่านั้น

เนื่องจากในระยะแรกโลกอินเทอร์เน็ตยังไม่มีกฎหมายเข้ามาควบคุมการกระทำผิดประเภทนี้ จึงทำให้ผู้ใช้คิดไปว่าอินเทอร์เน็ตเปรียบเสมือนโลกในอุดมคติที่จะแสวงหาประโยชน์ได้อย่างอิสระ ต่างจากโลกความจริงที่มีกฎหมายควบคุมอย่างเคร่งครัด ภาระการควบคุมจึงตกไปอยู่กับผู้ดูแลระบบเครือข่ายต่างๆ ที่ต้องทำหน้าที่ตรวจจับและพิทักษ์ระบบของพวกเขาเอง เช่น สร้างข้อสัญญาและขั้นตอนที่จำเป็นในการสื่อสารผ่านทางเครือข่าย หรือสร้างซอฟต์แวร์ขึ้นมาป้องกันเอง จนกลายเป็นว่าการพิพากษาพฤติกรรมที่เกี่ยวเนื่องกับสแปมเป็นการลงโทษกันเองโดยภาคเอกชน ไม่ได้ผ่านกระบวนการยุติธรรมของภาครัฐ หรือไม่สามารถนำมาดำเนินคดีในศาลได้ ทำให้นอกจากนักการตลาดแล้ว ยังมีเหล่าผู้ไม่ประสงค์ดีเข้ามากอบโกยผลประโยชน์จากช่องโหว่ตรงจุดนี้เป็นจำนวนมาก

---

[6] Templeton Brad. Reflections on the 25th Anniversary of Spam [Online]. 2008. Available from: http://www.templetons.com/brad/spamreact.html [7 Febuary 2018.]

[7] SANDBERG, J. Phoenix Lawyers Irk Internet Users Again by Broadcasting Ad [Online]. 1994. Available from: https://web.archive.org/web/20081204122549/http://www.l-ware.com/wall_stree_journal__june_22_1994.htm [13 February 2018.]

2.1.3 ลักษณะและประเภทของสแปม (spam)

หลังจากที่สแปมเริ่มเป็นที่รู้จักในวงกว้าง ไม่เพียงแต่นักการตลาดเท่านั้นที่ให้ความสนใจกับการใช้สแปมเป็นเครื่องมือในการทาการตลาดผ่านอีเมล (e-mail Marketing) แต่ยังมีมิจฉาชีพแอบแฝงที่คอยอาศัยช่องทางการส่งอีเมลเพื่อล่อลวงผู้บริโภค หรือใช้ช่องทางนี้ในการก่อให้เกิดความปั่นป่วนในสังคม หรือสร้างข้อความเท็จใส่ร้ายท ให้เกิดความเสียหายต่อตัวบุคคลด้วยเช่นกัน รูปแบบการท สแปมที่มีความหลากหลายมากขึ้นเป็นตัวสะท้อนถึงความแตกต่างด้านทัศนคติของผู้ทาสแปม (spammer) สแปมบางประเภทเป็นเพียงเรื่องเกี่ยวกับสิทธิและอุดมการณ์ที่มีจุดประสงค์เพียงเพื่อกระจายสิ่งที่ตนอยากจะสื่อออกไปเท่านั้น แต่ก็บางจาพวกก็มุ่งหวังที่จะแสวงหาผลประโยชน์จากการหลอกลวงผู้รับ เช่น การโฆษณาหลอกขายสินค้า บริการ ซอฟต์แวร์เถื่อน หรือสินค้าลามกอนาจารที่ไม่สามารถหาซื้อโดยเปิดเผยได้ ซึ่งหากผู้รับหลงเชื่อโอนเงินไปซื้อ สุดท้ายอาจจะไม่ได้รับสินค้า หรือได้รับสินค้าที่ด้อยคุณภาพไม่ตรงกับที่พรรณนาสรรพคุณไว้แต่แรก สแปมบางประเภทก็มีจุดประสงค์เพื่อหลอกดึงข้อมูลส่วนตัว ไม่ว่าจะเป็นข้อมูลธนาคาร เลขที่บัญชี ประวัติการศึกษา ฯลฯ เพื่อนาข้อมูลส่วนบุคคลที่อยู่ในคอมพิวเตอร์นั้นๆไปก่ออาชญากรรมต่อไป ทาให้โลกอินเทอร์เน็ตในยุคหนึ่งเปรียบเสมือนเป็นสังคมอิสระที่ไร้กฎเกณฑ์ ที่ไม่ว่าใครจะเข้ามาทาอะไร พูดอย่างไร แสวงหาประโยชน์อย่างไรก็ได้ ไม่มีฝ่ายไหนสามารถเข้ามาจัดระเบียบหรือกาหนดกฎเกณฑ์เพื่อป้องปรามผู้ใช้งานเครือข่ายในทางที่ผิดได้อย่างจริงจัง เพราะถึงแม้ผู้ให้บริการเครือข่ายอินเทอร์เน็ตหรือผู้ดูแลระบบบนเว็บไซต์ต่างๆ จะมีการสร้างเงื่อนไขในการให้บริการหรือการสมัครสมาชิกไว้ก็ตาม แต่กลับไม่มีประสิทธิภาพในการบังคับใช้ และไม่ได้มีบทลงโทษที่รุนแรงพอที่จะก่อให้เกิดความเกรงกลัวจนไม่กล้ากระทาความผิดนั้นอีก อัตราการเกิดของสแปมจึงเพิ่มขึ้นอย่างรวดเร็วจนยากจะควบคุม

2.1.3.1 ลักษณะโดยทั่วไปของสแปมเมล (spam mail)

การส่งอีเมลที่ไม่ได้ถูกร้องขอ หรืออีเมลไม่พึงประสงค์ หรือสแปมเมลนั้น มีหลายลักษณะขึ้นอยู่กับจุดประสงค์ในการส่งนั้นๆ โดยสามารถจ าแนกลักษณะร่วมทั่วไป ได้ดังนี้

1) เป็นจดหมายอิเล็กทรอนิกส์ที่ส่งได้ถึงทั่วทุกพื้นที่ที่สามารถเชื่อมต่อเครือข่ายอินเทอร์เน็ตได้ และยังสามารถส่งออกได้ครั้งละเป็นจานวนมากอย่างต่อเนื่อง ไม่จากัดกลุ่มเป้าหมาย แม้ว่าผู้รับจะไม่เคยให้ความยินยอมต่อการส่งจดหมายเหล่านั้นมาก่อนเลยก็ตาม โดยผู้ส่งสแปมบางรายอาจพัฒนาโปรแกรมค้นหารายชื่ออัตโนมัติที่เรียกว่า “harvester” หรือ “spiders” ขึ้นมาเพื่อกวาดหาที่อยู่อีเมลและรวบรวมข้อมูลที่ถูกทาการเชื่อมโยงลิงก์ (mailto) ของผู้ใช้งานอินเทอร์เน็ต หรืออาจซื้อที่อยู่อีเมลต่อมาจากเว็บไซต์อื่นที่มีคนเข้าไปลงทะเบียนไว้อีกทอดหนึ่ง เว็บไซต์บางแห่งในสหรัฐอเมริกาขายที่อยู่อีเมล 1 ล้านรายชื่อเพื่อเงินเพียง 59.95 ดอลลาร์ หรือขายซีดีที่มีรายชื่ออีเมล 15 ล้านชื่อเพียงเพื่อเงินแค่ 120 ดอลลาร์เท่านั้น[8] อย่างไรก็ตามผู้ส่งสแปมยังสามารถคัดกรอง

[8] Colorpack Creations Co., L. Admin, H. สแปม (Spam) คืออะไร มารู้จักกับ Spam และวิธีป้องกัน [ออนไลน์]. แหล่งที่มา: https://colorpack.net/host-articles/904-cms-web-tip/33-what-is-apam.html [1 มีนาคม 2561

กลุ่มเป้าหมายได้ละเอียดมากขึ้น โดยการซื้อประวัติการใช้งาน (Cookies History) จากเว็บไซต์ต่างๆ ที่มีการบันทึกประวัติการเยี่ยมชม พฤติกรรมการใช้งานของผู้ที่เข้ามาใช้งานเพื่อนามาวิเคราะห์ความชอบ และความสนใจของของผู้ใช้งานรายนั้นๆ เพื่อนามาวิเคราะห์หากลุ่มลูกค้าที่ต้องการติดต่อด้วยจริงๆได้เช่นกัน

2) มีเนื้อหาหลากหลายและมีวัตถุประสงค์ในการส่งที่แตกต่างกัน แต่ก่อให้เกิดปัญหาทางใดทางหนึ่งไม่ว่าจะต่อตัวผู้รับเองหรือต่อสังคมส่วนรวม เช่น

1. สแปมที่มีเนื้อหาเชิงพาณิชย์ทั่วไป มีจุดประสงค์ในการส่งเพียงเพื่อนาเสนอสินค้าหรือบริการที่ถูกกฎหมาย ซึ่งแม้ว่าเนื้อหาในการโฆษณาจะไม่ขัดต่อกฎหมายใดๆเลยก็ตาม แต่การส่งที่มากไป หรือส่งแล้วก่อให้เกิดภาระต่อผู้รับ ตลอดจนผู้ให้บริการเครือข่ายอินเทอร์เน็ตก็นับว่าเป็นปัญหาที่ก่อให้เกิดความเดือดร้อน

2. สแปมเชิงพาณิชย์ที่มีเนื้อหาขัดต่อกฎหมายโดยชัดเจน อาทิเช่น จดหมายลูกโซ่, การหลอกลวงขายสินค้าที่คุณภาพไม่ตรงกับที่ระบุในโฆษณา, โฆษณาขายสินค้าผิดกฎหมายหรือสินค้าละเมิดลิขสิทธิ์ เช่น ยาไวอะกร้า ซอฟต์แวร์เถื่อน การส่งข้อมูลที่มีเนื้อหาลามกอนาจาร การเชิญชวนให้เล่นพนัน การปล่อยข่าวเท็จเพื่อให้เกิดความโกลาหล เช่น “Pump and dump” เป็นต้น

3. สแปมที่ไม่มีจุดประสงค์ในเชิงพาณิชย์ แต่มุ่งหวังจะล้วงข้อมูลความลับส่วนบุคคลของผู้รับเพื่อนาไปใช้ประโยชน์ในทางอาชญากรรม โดยหลอกให้ผู้รับคลิกเข้าไปยังเว็ปช์ปลอม หรือจงใจปล่อยไวรัส หรือมัลแวร์ เพื่อให้ระบบป้องกันตัวของคอมพิวเตอร์ของผู้รับนั้นเสียหาย

3) เขียนการหัวเรื่องด้วยข้อความเชิญชวนที่น่าสนใจจนทาให้ผู้รับเกิดความรู้สึกอยากเปิดอ่าน เกิดความรู้สึกสงสัย หรือคล้อยตามได้ง่าย โดยชื่อหัวข้อเรื่องเหล่านั้น อาจจะมีหรือไม่มีความสอดคล้องกับเนื้อหาที่อยู่ด้านในเลยแม้แต่น้อย เช่น “ขอบคุณสาหรับการตอบคาถาม” หรือ “คุณได้รับอนุมัติบัตรเครดิตแล้ว” หรือ “คุณคือผู้โชคดีจากการจับฉลาก” ฯลฯ และมันมีการใช้เครื่องหมายหรือสัญลักษณ์ที่กระตุ้นความสนใจ เช่นเครื่องหมายอุทาน (Exclamation mark (!))

4) เป็นการโฆษณาประชาสัมพันธ์ที่มีต้นทุนต่ามากเมื่อเทียบกับวิธีการอื่นๆ ไม่ว่าจะเป็นการแจกใบปลิว, การลงโฆษณาโทรทัศน์-วิทยุ, การส่งทางไปรษณีย์ ฯลฯ อีกทั้งยังสามารถส่งออกได้คราวละมากๆและเข้าถึงผู้บริโภคได้โดยตรงแบบไม่จากัดกลุ่มเป้าหมายและไม่จากัดจานวน ทาให้การทาสแปมจึงกลายเป็นที่นิยมในหมู่นักการตลาดช่วงต้นยุคศตวรรษที่ 20 เป็นอย่างมาก

5) มักไม่ระบุตัวตนของผู้ส่ง (Anonymous remailer) หรือปลอมแปลงตัวตนของผู้ส่ง (Spoofing) ทาให้ผู้รับไม่สามารถสืบหาที่มาของอีเมลฉบับนั้นๆได้ เนื่องจากผู้ส่งเองก็ต้องการป้องกันตัวเองจากการโดนทาสแปมกลับ หรือโดนโต้กลับโดยการใช้ Mail Bomb (การส่งอีเมลจานวนมากให้กับผู้ใช้งานคนเดียว เพื่อให้ระบบการประมวลผลของคอมพิวเตอร์เกิดขัดข้องจนถึงขั้นเครื่องแฮงค์) เช่นกัน ยิ่งไปกว่านั้น ยังเพื่อหลีกเลี่ยงการโดนฟ้องร้อง หรือเลี่ยงการตรวจจับจากผู้ให้บริการ

เครือข่ายอินเทอร์เน็ต (ISPs)[9] เพราะ ISPs มีการกาหนดเงื่อนไขการให้บริการที่เคร่งครัดอยู่แล้ว หากมีผู้ใช้งานที่ละเมิดข้อก าหนดเหล่านั้นก็อาจถึงขั้นโดนสั่งปิดเว็บไซต์ได้เลยทีเดียว

6) ยากที่ผู้รับจะบอกปฏิเสธ เนื่องจากไม่มีช่องทางในการตอบกลับ หรือหาตัวตนที่แท้จริงของผู้ส่งสแปมไม่พบ

2.1.3.2 ประเภทของสแปม (spam)

การส่งสแปมไม่เพียงแต่ก่อให้เกิดความร าคาญแก่ผู้รับเท่านั้น ยังก่อให้เกิดผลกระทบต่อสิทธิสิทธิในความเป็นอยู่ส่วนบุคคล (Rights of Privacy) ซึ่งระยะหลัง การส่งสแปมไม่ได้หยุดอยู่แค่การโฆษณาเชิงพาณิชย์เท่านั้น ยังก่อให้เกิดความเสียหายในด้านอื่นๆ อาทิ การหลอกลวงฉ้อโกงผู้บริโภค การเผยแพร่สื่อลามกอนาจาร หรือมีเนื้อหาเกี่ยวกับของละเมิดลิขสิทธิ์ และเป็นภัยคุกคามด้านความปลอดภัยบนโลกอินเทอร์เน็ตเนื่องจากมีการแฝงไวรัสเข้ามาก่อกวนระบบคอมพิวเตอร์เพื่อสร้างช่องทางให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลส่วนบุคคลของผู้รับรายนั้นๆ ไม่ว่าจะเป็นเลขบัญชีธนาคาร เลขที่บัตรประจาตัวประชาชน เบอร์โทรศัพท์ ที่อยู่อีเมล ฯลฯ หรืออาจแฮกเข้ามาควบคุมคอมพิวเตอร์ของผู้รับเมลให้กลายเป็นเครื่องซอมบี้เพื่อกระจายสแปมเมลหรือไวรัสนั้นๆต่อไปยังเครื่องอื่นๆอีกทอดหนึ่ง (Zombie PC) โดยกองศูนย์อินเทอร์เนตของการไฟฟ้าฝ่ายผลิตได้แบ่งประเภทของสแปมเมลไว้ตามจุดประสงค์ในการส่ง ดังต่อไปนี้[10]

1) สแปมโฆษณา (spamvertise) ได้แก่ อีเมลเชิงพาณิชย์ที่มุ่งเน้นการเผยแพร่ประชาสัมพันธ์ตัวสินค้าหรือบริการ ซึ่งจะส่งถึงผู้รับโดยทั่วไปโดยไม่สนใจว่าผู้รับต้องการหรือไม่หรือไม่รอให้เกิดการยินยอมตอบรับจากผู้รับ บ้างก็เป็นการหลอกขายสินค้า หรือโฆษณาแอบแฝง จนอาจก่อให้เกิดความร าคาญและเป็นการรบกวนผู้รับได้

2) สแปมที่ไม่มีเนื้อความ (blank spam) ได้แก่ การส่งข้อความที่มีจุดประสงค์หลักเพื่อก่อก่วนระบบอีเมล หรือจงใจให้ระบบของปลายทางติดขัดลงจนเกิดปัญหาต่อการใช้งาน โดยจะเป็นอีเมลที่ไม่มีเนื้อหาด้านในแต่ใช้การส่งเป็นจานวนมากจนทาให้ระบบล่ม เพราะระบบของผู้รับปลายทางจะพยายามบล็อกและกาจัดอีเมลไม่พึงประสงค์เหล่านี้ หรืออาจเป็นอีเมลที่ทาให้ดูเหมือนเป็นอีเมลเปล่าแต่ที่จริงมีการแฝงไวรัส อาทิเช่น มัลแวร์ เวิร์ม เข้าไปกระจายในระบบของผู้รับปลายทางเพื่อให้ไวรัสเหล่านั้นแพร่กระจายตัวเองผ่านทางข้อความที่ไม่มีบรรทัดหัวเรื่อง

3) ฟิชชิ่ง (phishing) และ ฟาร์มมิ่ง (pharming) ได้แก่ อีเมลที่มีจุดประสงค์เพื่อล่อลวงให้ผู้รับเปิดเผยข้อมูลความลับส่วนบุคคลหรือข้อมูลที่ไม่ควรเปิดเผยสู่สาธารณะ โดยเบื้องหลังจะมีการสร้างเว็บไซต์ปลอมเพื่อหลอกให้ผู้รับกรอกข้อมูลลงไป เช่น หน้าเว็บไซต์ปลอมที่เหมือนกับเว็บไซต์ของธนาคาร หรือเว็บไซต์เลียนแบบโซเชียลเน็ตเวิร์ค หรืออาจใช้เนื้อหาในอีเมลหลอกล่อให้ผู้รับตอบกลับ อาทิ หลอกถามข้อมูลพาสเวิร์ด (password) อีเมล หมายเลขบัตรเครดิตหมายเลขบัตร

---

[9] นางสาวศศิมา ศรีพจน์ธรรม. มาตรการทางกฎหมายเพื่อการจัดการจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงประสงค์, หน้า 15.

[10] EGAT Mail Admin. รู้จักกับ SPAM [ออนไลน์]. แหล่งที่มา: https://mail.egat.co.th/owapage/km/spam.html [เข้าถึงเมื่อ 27 กุมภาพันธ์ 2561]

ประชาชน ซึ่งหากผู้รับไม่รู้เท่าทันแล้วตอบกลับไป อาจถูกดักข้อมูลและบันทึกไว้เพื่อหาผลประโยชน์ในอนาคต

4) สแปมรูปภาพ (Image spam) เป็นอีเมลโฆษณาที่ใช้ “รูปภาพ”แทนที่จะเป็นข้อมูลตัวอักษรเพื่อ เลี่ยงการตรวจจับจากระบบดักจับสแปมต่างๆ เช่น Spam Assasin, RadicalSpam, Bogofilter, SpamBayes โดยรูปภาพเหล่านี้จะสามารถเปิดตัวเองได้ทันทีเมื่อคลิ๊กเปิดอีเมล อาจมีจุดประสงค์แค่เพื่อโฆษณา หรือจงใจก่อกวนระบบการทางานของคอมพิวเตอร์ของผู้รับ

5) แบคสแกตเตอร์ สแปม (Backscatter spam) ได้แก่ อีเมลไม่พึงประสงค์ที่แนบไฟล์ไวรัส (Virus) หรือโทรจัน (Trojan) ไว้แล้วใช้เนื้อหาในอีเมลหลอกล่อให้ผู้รับกดใช้งาน (run) ไฟล์ดังกล่าว เพื่อให้ไวรัสนั้นๆทางาน ซึ่งอาจสร้างความเสียหายแก่ข้อมูลหรือทรัพย์สินของเหยื่อ หรือใช้ไวรัสเพื่อทาให้เครื่องคอมพิวเตอร์ของเหยื่อกลายเป็น Zombie PC ที่เป็นตัวกลางในการกระจายสแปมต่อออกไปยังผู้ใช้ต่างๆที่เครื่องคอมพิวเตอร์นั้นมีประวัติข้อมูลอยู่

ทฤษฎีวิวัฒนาการของชาร์ลส์ ดาร์วิน เรื่อง Survival of Fittest (การอยู่รอดของผู้ที่แข็งแกร่งที่สุด)[11] สามารถนามาอธิบายถึงวิวัฒนาการของผู้ทาสแปมได้เช่นกัน โดยยิ่งมาตรการป้องปรามด้านเทคโนโลยีหรือมาตรการทางกฎหมายในเรื่องนี้ มีประสิทธิภาพและมีความรวดเร็วมากเท่าใด เหล่าผู้ที่ทาสแปมก็จะยิ่งต้องเร่งพัฒนาเทคนิคของตนให้มากขึ้นเพื่อให้ตนอยู่รอด แน่นอนว่าเหล่าคนที่ไม่เก่งพอก็จะค่อยๆถูกกาจัดออกไป ในขณะเดียวกันคนที่อยู่รอดได้ จะยิ่งมีความแข็งแกร่งและมีความอันตรายมากขึ้นอย่างยากที่จะหยุดยั้ง แม้ปัจจุบันจะคาดการณ์ได้ว่ามีคนท าสแปมอยู่เพียง 150 กลุ่มทั่วโลกเท่านั้น ถึงจานวนที่ไม่มากนักแต่หนึ่งในนั้นก็มีศักยภาพมากพอที่จะสามารถสร้างผลกระทบต่อผู้ให้บริการเครือข่ายอินเทอร์เน็ต (“ISPs”) ทั่วโลกได้เลยทีเดียว[12]

2.2 แนวความคิดที่เกี่ยวกับกระท าความผิดในลักษณะสแปม (spam)

ในช่วงปลายยุคศตวรรษที่ 19 เทคโนโลยีเริ่มเข้ามามีบทบาทในชีวิตประจาวันของผู้คนมากขึ้น การส่งข้อมูลข่าวสารทางไปรษณีย์ปกติเริ่มถูกแทนที่ด้วยการใช้งานอีเมล เพราะนอกจากจะทาให้การส่งข้อมูลเกิดความสะดวกรวดเร็วแล้ว ยังช่วยประหยัดค่าใช้จ่ายได้ดีอีกด้วย ท าให้ทั้งภาคครัวเรือนและภาคธุรกิจต่างก็หันมาใช้อีเมลในการติดต่อสื่อสารกันมากขึ้น เพราะนอกจากจะช่วยลดภาระค่าใช้จ่ายในด้านต่างๆ ยังสามารถเก็บข้อมูลไว้เป็นหลักฐานในการปฏิบัติงานได้เป็นระยะเวลานานโดยไม่สิ้นเปลืองพื้นที่ ผู้ประกอบการจานวนมากประยุกต์ใช้ช่องทางนี้เข้ามาแทนที่วิธีการโฆษณาแบบเก่าๆ เช่น กลยุทธ์การขายตรง การแจกใบปลิว การใช้คอลเซ็นเตอร์ ฯลฯ โดยในระยะแรกการส่ง

[11] Magazine, S. ชัยวัฒน์ คุประตกุล. คลื่นวิทย์-เทคโนฯ : ทฤษฎีวิวัฒนาการกับการฆ่าล้างเผ่าพันธุ์ [ออนไลน์]. 2012. แหล่งที่มา: https://www.sarakadee.com/2012/07/04/social-darwinism/ [1 มีนาคม 2561]

[12] Hedley, S. A Brief History of Spam. Information & Communication Technology Law 15, 3 (2006): 223.

อีเมลไม่ได้สร้างปัญหาอะไรให้แก่ผู้รับมากนัก ทาให้ผู้ใช้งานไม่ตระหนักถึงภาระหรือผลกระทบจากการส่งอีเมล จนแต่ละวันมีอีเมลกว่าพันล้านฉบับส่งผ่านอยู่บนโลกอินเทอร์เน็ต

แต่ต่อมา เมื่อผู้ทาสแปมมีจานวนมากขึ้นทุกวัน จานวนสแปมเมลที่ถูกส่งออกจึงเพิ่มมากขึ้นในระยะเวลาอันรวดเร็ว แน่นอนว่าการส่งอีเมลเป็นจานวนมากๆย่อมก่อให้เกิดค่าใช้จ่ายต่างๆทั้งต่อผู้รับและผู้ดูแลระบบ แม้สิ่งเหล่านี้จะดูเหมือนว่าเป็นปัญหาสาหรับผู้ที่มีหน้าที่กลั่นกรองและควบคุมความปลอดภัยบนระบบ (เช่น ผู้ให้บริการเครือข่ายอินเทอร์เน็ตและผู้ดูแลระบบ) มากกว่าเป็นปัญหากับผู้ใช้งานทั่วไปก็ตาม แต่ก็ยังมีผู้ใช้งานจานวนมากที่เรียกร้องให้มีมาตรการในการลดจานวนสแปมเพราะการที่ผู้รับต้องคอยมานั่งลบสแปมเมลจานวนมากๆออกจากกล่องข้อความ (Mailbox) ของตนทุกวัน ก็เป็นภาระที่น่าเบื่อ ซึ่งถ้าไม่คอยลบออก พื้นที่ในกล่องข้อความ (Mailbox) ของตนก็อาจจะเต็มจนไม่สามารถรับอีเมลอื่นที่มีความจาเป็นจริงๆเข้ามาได้ จึงกล่าวได้ว่าการใช้สแปมเมลในเชิงพาณิชย์ส่งผลกระทบต่อสิทธิในความเป็นอยู่ส่วนบุคคล (Rights of Privacy) ของผู้รับ และเป็นการผลักภาระค่าใช้จ่ายในการทาโฆษณามาที่ผู้ใช้บริการและผู้ดูแลระบบ เพราะผู้รับต้องเสียพื้นที่ในกล่องข้อความ (Mailbox) ของตน เสียค่าบริการอินเทอร์เน็ตในการเปิดอ่าน ส่วนทางผู้ให้บริการเครือข่ายอินเทอร์เน็ตเองก็ต้องเสียพื้นที่บนเซิร์ฟเวอร์ รวมทั้งเสียค่าใช้จ่ายในการพัฒนาระบบป้องกันและกลั่นกรองสแปมเมลออกจากอีเมลปกติ

แม้ว่าการส่งสแปมเมลเชิงพาณิชย์จะเป็นเครื่องมือที่ช่วยสนับสนุนให้เกิดการขับเคลื่อนในภาคธุรกิจก็ตาม แต่สแปมเมลก็เป็นเครื่องมือในการทาอาชญากรรมบางประเภทเช่นกัน อาทิ การขโมยข้อมูลส่วนบุคคล การล่อลวงขายสินค้า การปลอมแปลงหรือส่งต่อข้อมูลเท็จที่ทาให้เกิดความปั่นป่วนในสังคม หรือใช้เป็นเครื่องมือในการกระจายไวรัสหรือมัลแวร์ จึงกล่าวได้ว่าการทาสแปมส่งผลกระทบต่อสังคมและประชาชนส่วนมาก รัฐจึงต้องเข้ามาก หนดโทษเพื่อป้องกันและควบคุมการกระทารูปแบบนี้ให้ได้สัดส่วนที่พอเหมาะพอควรกับสภาพเศรษฐกิจของประเทศ และไม่กระทบต่อสิทธิของประชาชน

2.3 ปัญหาอันเกิดจากการกระท าความผิดเกี่ยวกับสแปม (spam)

สาเหตุที่ทาให้สแปมกลายมาเป็นปัญหาเร่งด่วน จนทั้งภาครัฐและภาคเอกชนหันมาตื่นตัวที่จะจัดหามาตรการป้องกันทั้งด้านเทคโนโลยีและด้านกฎหมาย ก็สืบเนื่องมาจากสแปมก่อให้เกิดผลกระทบในมิติต่างๆ ดังต่อไปนี้

2.3.1 การละเมิดสิทธิในความเป็นอยู่ส่วนบุคคล (Rights of Privacy)

รัฐธรรมนูญแห่งราชอาณาจักรไทย ฉบับปี 2560 หมวด 3 ได้บัญญัติเกี่ยวกับเรื่องสิทธิเสรีภาพของประชาชนเอาไว้ โดยมีเป้าหมายเพื่อให้ความคุ้มครองด้านสิทธิเสรีภาพของบุคคล

และป้องกันไม่ให้บุคคลใดๆโดนละเมิดสิทธิเสรีภาพนั้นด้วย โดยมาตรา 32[13] และมาตรา 36[14] ได้กำหนดนิยามเกี่ยวกับสิทธิความเป็นส่วนตัวของบุคคล และระบุป้องกันมิให้ข้อมูลส่วนบุคคลถูกเผยแพร่หรือถูกนำไปใช้ประโยชน์โดยมิชอบ หรือโดยไม่ได้รับความยินยอม ซึ่งแน่นอนว่าบุคคลทุกคนย่อมมีอิสระในการสื่อสาร การพูด การออกความคิดเห็น การโฆษณา ฯลฯ แต่อิสระนั้นย่อมต้องอยู่บนขอบเขตของการใช้สิทธิที่ไม่กระทบกับความสงบเรียบร้อยและประโยชน์สาธารณะ (Public interest) ของสังคม ดังนั้น รัฐธรรมนูญในมาตรา 34[15] จึงได้ระบุให้สิทธิเสรีภาพในการกระทำดังกล่าวสามารถถูกจำกัดได้ด้วยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะ เพียง “เท่าที่จำเป็น” เท่านั้น เพื่อให้การออกกฎหมายเฉพาะนั้นอยู่บนหลักความได้สัดส่วน (Principle of Proportionality) และคุ้มค่ากับสิทธิเสรีภาพของมหาชนที่ถูกริดรอนไป

สิทธิความเป็นอยู่ส่วนบุคคลยังได้รับการรับรองให้เป็นสิทธิพื้นฐานประการหนึ่งที่ทุกคนควรได้รับการคุ้มครอง ตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1984 ข้อ 12 (Universal Declaration of Human Right 1984 Article 12)[16] ซึ่งบัญญัติไว้ว่า

“บุคคลจะถูกแทรกสอดในความเป็นอยู่ส่วนตัว ในครอบครัว ในเคหสถาน หรือการติดต่อสื่อสาร หรือไม่อาจโดนลบหลู่ในเกียรติยศ และชื่อเสียง ทั้งนี้ บุคคลทุกคนย่อมมีสิทธิที่จะได้รับการปกป้องคุ้มครองโดยกฎหมายอันเนื่องจากการก้าวล่วงในสิทธิเช่นที่ว่านั้น”

ดังนั้นเมื่อพิจารณาถึงปัญหาที่เกี่ยวข้องกับสแปมเมลแล้ว จะเห็นได้ว่า การถูกใช้ที่อยู่อีเมล (e-mail address) ซึ่งเปรียบเสมือนเป็นกล่องจดหมายส่วนตัวของบุคคล ไปใช้งานโดยที่ไม่ได้รับความยินยอมจากเจ้าของ หรือโดยที่เจ้าตัวไม่ต้องการ ย่อมถือว่าเป็นการถูกละเมิดต่อสิทธิในความเป็นอยู่ส่วนตัวของบุคคลนั้นๆ เสมือนเช่นการที่เจ้าของบ้านถูกบุคคลภายนอกที่ตนไม่รู้จัก ล่วงรู้ถึงข้อมูลที่อยู่ จนทำให้มีจดหมายที่ไม่ต้องการจำนวนมากถูกส่งเข้ามาในกล่องไปรษณีย์หน้าบ้านตน ก่อให้เกิดภาระในการคัดแยก จัดเก็บ หรือสร้างความรำคาญ ย่อมเป็นการกระทำที่กระทบสิทธิความเป็นอยู่ส่วนตัวของเจ้าของบ้าน เพราะแท้ที่จริงแล้วผู้ส่งกระทำไปเพียงเพื่อประโยชน์ส่วนตนหรือผลประโยชน์ของธุรกิจตนเท่านั้น ไม่ได้มีส่วนสนับสนุนให้เกิดประโยชน์ต่อสาธารณะ หรือไม่ได้มีส่วนช่วยให้เกิดความเรียบร้อยของประชาชนในสังคม

---

[13] รัฐธรรมนูญแห่งราชอาณาจักรไทย ฉบับปี 2560 หมวด 3 มาตรา 32 “บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ”

[14] รัฐธรรมนูญแห่งราชอาณาจักรไทย ฉบับปี 2560 หมวด 3 มาตรา 36 “บุคคลย่อมมีเสรีภาพในการติดต่อสื่อสารถึงกันไม่ว่าในทางใด ๆ การตรวจ การกัก หรือการเปิดเผยข้อมูลที่บุคคลสื่อสารถึงกัน รวมทั้งการกระทำด้วยประการใด ๆ เพื่อให้ล่วงรู้หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันจะกระทำมิได้ เว้นแต่มีคำสั่งหรือหมายของศาลหรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ”

[15] รัฐธรรมนูญแห่งราชอาณาจักรไทย ฉบับปี 2560 หมวด 3 มาตรา 34 “บุคคลย่อมมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น การจำกัดเสรีภาพดังกล่าวจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเฉพาะเพื่อรักษาความมั่นคงของรัฐ เพื่อคุ้มครองสิทธิหรือเสรีภาพของบุคคลอื่น เพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเพื่อป้องกันสุขภาพของประชาชนเสรีภาพทางวิชาการย่อมได้รับความคุ้มครอง แต่การใช้เสรีภาพนั้นต้องไม่ขัดต่อหน้าที่ของปวงชนชาวไทย ศีลธรรมอันดีของประชาชน ต้องเคารพและไม่ปิดกั้นความเห็นต่างของบุคคลอื่น”

[16] Universal Declaration of Human Right 1984, 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.”

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ให้นิยามของคาว่า “ข้อมูลข่าวสารส่วนบุคคล” ไว้ว่า “*ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทางาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทาให้รู้ตัวผู้นั้นได้เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียง ของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย*” ดังนั้น ไม่ว่าจะเป็นอีเมล เบอร์โทรศัพท์ ที่อยู่ หรือแม้กระทั่งข้อมูลลักษณะนิสัยในการใช้งานอินเทอร์เน็ตที่สามารถบ่งบอกความเป็นตัวตนของบุคคลนั้นๆ (cookies) ก็สามารถนับรวมว่าเป็นข้อมูลส่วนบุคคลด้วยเช่นกัน อย่างไรก็ตามเจ้าของข้อมูลควรมีสิทธิ์เลือกได้ว่าจะตนอยากเปิดเผยข้อมูลส่วนบุคคลของตนหรือไม่ ตามพื้นฐานทั่วไปแล้วหากผู้รับไม่ยินยอมที่จะแจ้งข้อมูลส่วนบุคคลของตนให้ผู้ส่งทราบ การส่งข้อมูลย่อมเกิดขึ้นไม่ได้ และถึงแม้หน้าที่ในการปกป้องข้อมูลของตนเองให้เป็นความลับอยู่เสมอก็เป็นความรับผิดชอบของตัวผู้ใช้งานอินเทอร์เน็ตเองด้วยก็ตาม แต่บางครั้งที่ผู้ใช้งานเผลอทาการเชื่อมโยง (hyperlink) โดยไม่ได้ตั้งใจ หรือข้อมูลอีเมลและข้อมูลการใช้งานที่ถูกเก็บไว้ในเว็บเซิร์ฟเวอร์ (cookies) ของเว็บไซต์ที่เข้าไปใช้งานโดยไม่รู้ตัว การที่ผู้ทาสแปมใช้วิธีไม่โปร่งใสในการรวบรวมที่อยู่อีเมล เช่น ซื้อรายชื่อที่อยู่อีเมลจากเว็บไซต์ที่เราไปสมัครเป็นสมาชิกไว้โดยที่เราไม่ให้ให้ความยินยอม หรือใช้วิธีเจาะระบบในการหาอีเมลของผู้ใช้งานจากเซิร์ฟเวอร์โดยพลการ (Directory Harvest Attacks: DHA) ย่อมเป็นการกระทาที่ละเมิดสิทธิส่วนบุคคลของเจ้าของอีเมลเช่นกัน ผู้บริโภคควรมีสิทธิ์เลือกที่จะรับรู้เฉพาะสิ่งที่ตนต้องการ หรือปฏิเสธในสิ่งที่ตนไม่ต้องการได้[17] แต่การที่มีสแปมส่งเข้ามาในกล่องข้อความ (Mail Box) เป็นจานวนมากโดยที่ผู้รับไม่เคยสมัครรับ อีกทั้งยังไม่มีสิทธิที่จะบอกปฏิเสธได้เลย จึงเป็นการคุกคามความเป็นอยู่ส่วนตัวอย่างยิ่ง และการที่พื้นที่ในกล่องข้อความส่วนตัว (Mail box) มีแต่ของที่ไม่ต้องการ ยังทาให้สิ้นเปลืองพื้นที่เก็บข้อมูลโดยใช่เหตุ ทาให้ต้องเสียเวลาในการคัดแยกข้อความไม่พึงประสงค์ออกไป เพื่อไม่ให้เกิดความสูญเสียทางโอกาสจากการที่อีเมลสาคัญอื่นๆจะส่งเข้ามาไม่ได้เพราะพื้นที่รับเต็ม และยังสิ้นเปลืองค่าธรรมเนียมการใช้อินเทอร์เน็ตไปโดยไร้ประโยชน์อีกด้วย[18]

แต่การแก้ปัญหาโดยใช้หลัก “การละเมิดสิทธิส่วนบุคคล” นั้นมีข้อจากัดอยู่เช่นกัน เพราะการส่ง สแปมเมลมักจะเป็นการส่งที่กระจายออกไปเป็นวงกว้าง จนยากจะระบุขอบเขตของพื้นที่ที่เกิดผลกระทบ และยากที่จะประเมินความเสียหายออกมาเป็นมูลค่าทางเศรษฐกิจ เหยื่อหลายรายมักคิดว่าการฟ้องร้องทางแพ่งเป็นเรื่องที่ได้ไม่คุ้มเสีย เพราะการตอบโต้หรือฟ้องร้องจากเหยื่อเพียงรายเดียวคงไม่มีพลังมาพอที่จะต่อกรกับผู้ทาสแปม และตัวเหยื่อเองก็ไม่สามารถรวมกลุ่มกันได้เพราะไม่สามารถสืบรู้ได้เองว่าใครโดนเรื่องเดียวกันบ้าง ทั้งนี้ ผลกระทบที่เกิดขึ้นกับเหยื่อเพียงรายเดียวก็อาจจะไม่มีความรุนแรงมากพอที่จะทาให้สังคมรู้สึกต่อต้านจนผลักดันให้เกิดมาตรการรองรับ

---

[17] นางสาวศศิมา ศรีพจน์ธรรม. มาตรการทางกฎหมายเพื่อการจัดการจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงประสงค์, หน้า 28.

[18] เรื่องเดียวกัน. หน้า 26-27.

และที่สาคัญที่สุดคือ เป็นเรื่องยากที่เหยื่อจะมีความสามารถพอที่จะสืบหาตัวตนของผู้ท สแปมเพื่อนา ตัวมาด าเนินคดีได้ด้วยตัวเอง[19]

2.3.2 ต้นทุนในการด าเนินธุรกิจของผู้ประกอบการ

การส่งอีเมลในแต่ละครั้งจะต้องอาศัยแบนด์วิดท์ (Bandwidth) บนเมลเซิร์ฟเวอร์ เป็นเส้นทางในการน ส่งข้อมูลอิเล็กทรอนิกส์ เปรียบได้ว่าแบนด์วิดท์เป็นเสมือนถนน[20] และอีเมลเป็น เหมือนรถที่ใช้ในการขนส่งข้อมูล ซึ่งแน่นอนว่าถนนแต่ละแห่งย่อมมีความกว้างและเลนที่จ ากัด หากมี รถขนส่งที่วิ่งเข้ามามากเกินไป การจราจรก็จะเกิดความติดขัดและทาให้การขนส่งเกิดความล่าช้าเป็น ธรรมดา ดังนั้นหากมีสแปมเมลส่งเข้ามามากเกินไป ก็จะส่งผลกระทบต่อการส่งอีเมลปกติอื่นๆทาให้ ต้องเลื่อนเวลาในการนาส่งออกไป ซึ่งตามปกติหากเซิร์ฟเวอร์ที่เป็นตัวแทนถ่ายโอนข้อความ (Mail Transfer Agent: MTA) ไม่สามารถส่งต่อเมลนั้นๆไปถึงปลายทางได้ ระบบก็จะพยายามมทาการส่ง ใหม่ทุกๆ 4 ชั่วโมง และถ้าภายใน 3 วัน (หรือตามเงื่อนไขที่กาหนดไว้ใน MTA) ยังไม่สามารถส่งได้ เมลฉบับนั้นๆก็จะถูกส่งคืนไปยังผู้ส่ง ดังนั้นการที่การจราจร (Traffic) บนแบนด์วิดท์เต็มอาจส่งผลให้ ได้รับเมลช้าลงหรือถึงขั้นไม่ได้รับเลยในที่สุด ดังนั้นผู้ให้บริการเครือข่ายอินเทอร์เน็ต (ISPs) จึงต้อง แก้ไขปัญหานี้ด้วยการเสียค่าใช้จ่ายเพื่อขยายแบนด์วิดท์ หรือต้องเสียค่าใช้จ่ายเพื่อจ้างพนักงานมาคัด แยกสแปมเมลออกจากระบบเพิ่มขึ้น เพื่อให้สามารถรักษาระดับความเร็วในการส่งข้อมูลให้ตอบสนอง ทันต่อความต้องการของผู้ใช้บริการ

หลายบริษัทนิยมใช้เมลเซิร์ฟเวอร์ (Mail Server) เป็นฮาร์ดดิส (Hard disk) ในการ จัดเก็บข้อมูลอีเมลต่างๆ เพื่อช่วยขยายพื้นที่กล่องข้อความ (Mail Box) ของผู้ใช้งาน และเพื่อบริหาร จัดการด้านความปลอดภัยของข้อมูลในองค์กรด้วยตนเอง โดยเมลเซิร์ฟเวอร์ (Mail Server) ก็ เปรียบเสมือนตู้จดหมายของบริษัท หากในตู้จดหมายเต็มไปด้วยจดหมายที่ไม่พึงประสงค์จนทาให้ไม่ สามารถใส่จดหมายที่มีความจาเป็นลงไปได้ บริษัทก็ต้องเสียค่าใช้จ่ายในการขยายขนาดของตู้ ไปรษณีย์โดยไม่จาเป็น ซึ่งถือเป็นต้นทุนในการดาเนินธุรกิจเพิ่มขึ้นเช่นกัน และปัญหาที่ร้ายแรงกว่า นั้น คือการที่สแปมเมอร์เจาะเข้าเมลเซิร์ฟเวอร์ (Mail Server) ของบริษัทผ่านทางการคลิกเปิดสแปม เมล แล้วแปลงเซิร์ฟเวอร์บริษัทให้กลายเป็นตัวกลางในการทารีเลย์ (Relay server)[21] เพื่อเป็น ตัวกลางในการกระจายส่งสแปมเมลต่อไปยังผู้รับจานวนมาก ซึ่งการที่เมลเซิร์ฟเวอร์ของบริษัทถูกใช้ เป็นตัวกลางในการส่งต่อสแปมเมล ย่อมส่งผลกระทบต่อประสิทธิภาพการทางาน (Performance) ของเซิร์ฟเวอร์ และอาจส่งผลกระทบต่อชื่อเสียงและภาพลักษณ์ของบริษัท เพราะหากผู้รับตรวจสอบ เจอที่มาของ สแปมเมลว่า ผู้ส่ง (Sender) คือตัวบริษัท ก็อาจทาให้เกิดความรู้สึกไม่ดีต่อบริษัท แม้ว่า ที่จริงแล้วบริษัทไม่ได้มีส่วนเกี่ยวข้องอะไรกับสแปมเมอร์ก็ตาม

---

[19] Hedley, S. A Brief History of Spam.

[20] ชินณปพัชร เอกวิพัทธ์พล. Bandwidth (แบนด์วิดท์) คืออะไร [ออนไลน์]. 28 กรกฎาคม 2560. แหล่งที่มา: http://www.8webz.com/bandwidth-แบนด์วิดท์-คืออะไร/ [เข้าถึงเมื่อ 17 พฤษภาคม 2561]

[21] นางสาวศศิมา ศรีพจน์ธรรม. มาตรการทางกฎหมายเพื่อการจัดการจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงประสงค์, หน้า 21.

จากปัญหาที่กล่าวไปในข้างต้น ผู้ให้บริการเครือข่ายอินเทอร์เน็ตและบริษัทที่โดนผลกระทบจานวนมากยอมที่จะจ่ายเงินไปเพื่อซื้อซอฟต์แวร์มาป้องกันสแปมเมลมากกว่า โดยรายการการวิจัยของ Ferris Research ในสหรัฐอเมริกา สารวจพบว่าในช่วงปี 2003 ปัญหาสแปมทาให้เกิดต้นทุนต่อภาคธุรกิจในสหรัฐอเมริการวมทั้งหมดถึงราว 10,000 ล้านเหรียญสหรัฐ ซึ่งคิดเป็นค่าเฉลี่ยที่ 14 ดอลลาร์สหรัฐต่อผู้ใช้งานหนึ่งคน[22] ถึงแม้จะเป็นค่าใช้จ่ายที่สูง แต่หากเทียบกับความเสี่ยงที่อาจจะเกิดขึ้นทั้งด้านชื่อเสียง ภาพลักษณ์ ประสิทธิภาพการทางานของเซิร์ฟเวอร์ ฯลฯ ก็ถือว่าเป็นการลงทุนที่คุ้มค่า เพราะระดับความรุนแรง และความซับซ้อนในการทาสแปมเมลนั้นพัฒนามากขึ้นทุกวัน ซึ่งผู้รับ หรือตัวผู้ให้บริการไม่สามารถพัฒนาระบบมาป้องกันตัวเองได้ตลอดไป การที่มีบริษัทผู้เชี่ยวชาญเฉพาะด้านมาช่วยพัฒนาซอฟต์แวร์ เข้ามาช่วยดูแล ตรวจจับ กลั่นกรอง รวมถึงวิเคราะห์พฤติกรรม (Heuristic) ของสแปมเมอร์ จึงเป็นวิธีการที่ปลอดภัย มีประสิทธิภาพ และสามารถป้องกันได้แบบทันท่วงทีมากกว่า

2.3.3 ความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน

คาว่า “ศีลธรรมอันดีและความสงบเรียบร้อยในสังคม” (be contrary to public order or good morals) ไม่ได้มีกฎหมายฉบับใดฉบับหนึ่งให้คานิยามเอาไว้โดยเฉพาะ แต่กฎหมายหลายฉบับกลับมีบทบัญญัติที่เกี่ยวข้องกับคาๆนี้ไว้ เช่น ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 150 ที่บัญญัติว่า “การใดมีวัตถุประสงค์เป็นการต้องห้ามชัดแจ้งโดยกฎหมายเป็นการพ้นวิสัย หรือเป็นการขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน การนั้นเป็นโมฆะ” หรือพระราชบัญญัติว่าด้วยข้อสัญญาที่ไม่เป็นธรรม พ.ศ.2540 มาตรา9 ที่บัญญัติว่า “ความตกลงหรือความยินยอมของผู้เสียหายสาหรับการกระทาที่ต้องห้ามชัดแจ้งโดยกฎหมาย หรือขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน จะนามาอ้างเป็นเหตุยกเว้นหรือจากัดความรับผิดเพื่อละเมิดมิได้” ที่เป็นเช่นนี้ก็เพื่อให้ศาลได้มีอานาจในการวินิจฉัยและพิจารณาความผิดตามบรรทัดฐานและจารีตประเพณีของสังคมในยุคสมัยนั้นๆได้อย่างเหมาะสม อาจกล่าวโดยรวมได้ว่าคาๆนี้หมายถึงการกระทาทั้งทางตรงหรือทางอ้อมที่ส่งผลกระทบต่อมหาชนหรือชีวิตความเป็นอยู่โดยปกติสุขทั่วไปของประชาชน ณ ขณะนั้น หรือเป็นการกระทาที่สังคมในยุคสมัยนั้นมองว่าเป็นเรื่องผิดแบบแผน (Norm) หรือผิดไปจากประเพณีปฏิบัติ ณ ขณะนั้น ด้วยเหตุนี้ หลายกฎหมายจึงนิยมบัญญัติประเด็นนี้ลงไปเพื่อเปิดช่องให้การพิพากษาสามารถกระท าได้ตามความเปลี่ยนแปลงและค่านิยมของยุคสมัย[23]

เมื่อพิจารณาถึงเรื่องการทาสแปม แม้ในอดีตการกระทานี้จะยังไม่มีกฎหมายฉบับใดออกมากากับ แต่เนื่องจากการกระทาความผิดรูปแบบสแปมไม่เพียงแต่ส่งผลกระทบต่อต้นทุนในการดาเนินธุรกิจ หรือกระทบต่อสิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภคเท่านั้น เนื้อหาของสแปมเม

---

[22] Paul wood, “MessageLabs white paper, A spammer in the works: Everything you need to know,” [Online]. 2006. Available from: http://www.messagelabs.com/Threat_Watch/white_Papers [18 March 2018.]

[23] ธานินทร์ กรัยวิเชียร. ความส าคัญของการตีความในวิชาชีพกฎหมาย. ใน 100ปี ชาตกาล ศาสตราจารย์จิตติ ติงศภัทิย์. มหาวิทยาลัยธรรมศาสตร์: 2551., หน้า 14.

ลบางประเภทก็ขัดต่อศีลธรรมอันดีและความสงบเรียบร้อยในสังคมด้วยเช่นกัน อาทิ การโฆษณาหลอกขายสินค้าหรือบริการที่เกี่ยวข้องกับเรื่องเพศ การส่งรูปภาพอนาจาร เพราะการส่งข้อมูลอีเมลไม่สามารถจากัดอายุผู้รับได้ สื่อเหล่านี้จึงอาจถึงมือเด็กที่ยังไม่บรรลุนิติภาวะที่ยังไม่มีวิจารณญานพอจะแยกแยะผิดถูก หรืออาจเป็นจนหมายลูกโซ่ที่มีเนื้อหาปลุกปั่นให้เกิดความขัดแย้งในสังคม ทาให้ประชาชนเกิดความตื่นตระหนก หรือส่งผลต่อความมั่นคงของประเทศ หรือใช้เพื่อเป็นเครื่องมือทางการเมืองในการปล่อยข่าวลือให้ประชาชนเกิดความขัดแย้ง หรือเป็นเครื่องมือในการปล่อยข่าวลือเพื่อท าลายชื่อของบริษัทคู่แข่ง เช่น กรณีการโพสต์ภาพตึกเอียงบริเวณแยกเพลินจิตเมื่อวันที่ 15 สิงหาคม พ.ศ. 2560 ที่ผ่านมา ซึ่งเป็นที่ฮือฮาและมีการส่งต่อภาพนั้นต่อๆกันไปในวงกว้างในระยะเวลาสั้นๆ จนทาให้พนักงานที่ทางานอยู่ตึกใกล้เคียงบริเวณนั้นเกิดความตื่นตระหนกเข้าใจไปว่าตึกกาลังจะถล่ม แม้กระทั่งพนักงานก่อสร้างที่อยู่ในตึกนั้นเองหรือบริเวณใกล้เคียงต่างทยอยตัวพากันออกจากพื้นที่ทางาน จนเกิดความโกลาหลและหลายบริษัทก็ไม่สามารถทางานได้ ทั้งที่จริงการเอียงของตึกเป็นไปตามดีไซน์ที่ออกแบบไว้แต่แรก ไม่ได้มีความผิดปกติแต่อย่างใด[24]

ภาพที่ 1 ข่าวตึกทรุดขณะก่อสร้างจากหนังสือพิมพ์ผู้จัดการออนไลน์[25]

[24] MGR Online. อย่าแตกตื่น! อาคารเอียงแค่ดีไซน์ โรงแรมของ "เอม-พินทองทา" ลูกสาวทักษิณ, [ออนไลน์]. 2560. แหล่งที่มา: https://mgronline.com/onlinesection/detail/9600000083254 [1 มีนาคม 2561]

[25] เรื่องเดียวกัน

2.3.4 ความรับผิดทางอาญา

รัฐธรรมนูญแห่งราชอาณาจักรไทยได้บัญญัติเกณฑ์ในการก าหนดโทษทางอาญาไว้ว่า “ต้องเป็นความผิดร้ายแรง”[26] ดังนั้นโดยเนื้อแท้แล้วการกระทาผิดในรูปแบบสแปมเชิงพาณิชย์แต่เดิมจึงควรเอาผิดแค่ทางแพ่งเท่านั้นไม่ควรมีความผิดฐานอาญาได้ เนื่องจากเป็นเรื่องระหว่างเอกชนด้วยกันเอง เปรียบเสมือนเป็นเพียงการเสนอที่ไม่ได้เกิดจากการยินยอมจากผู้รับก่อนล่วงหน้าเท่านั้น แต่เนื่องจากในระยะหลังๆการทาสแปมเริ่มทวีความรุนแรง ผลกระทบไม่ได้มีเพียงแค่ด้านเศรษฐกิจ แต่เป็นการกระทาที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีในสังคม และยังยากที่จะใช้มาตรการอื่นเพื่อให้มีประสิทธิภาพเพียงพอที่จะทาให้ผู้กระทาผิดยาเกรงต่อกฎหมาย ทาให้รัฐต้องเข้ามาด าเนินการป้องกันและปราบปรามมิให้เกิดมีการกระทาผิดนั้นอีก ยิ่งในยุคปัจจุบันที่สื่อสังคมออนไลน์ (Social media) เข้ามามีอิทธิพลในชีวิตของผู้คนมากขึ้น ช่องทางในการกระทาผิด หรือช่องทางในการค้นหาที่อยู่อีเมลของผู้บริโภคก็ทาได้ง่ายมากขึ้น หากปัญหาสแปมยังคงเป็นเพียงภาระของเหล่าผู้ให้บริการเครือข่ายอินเทอร์เน็ต หรือผู้ดูแลระบบที่ต้องเป็นคนกาหนดเงื่อนไขการใช้งาน หรือกาหนดนโยบายป้องกันขึ้นเอง ก็คงจะเป็นภาระที่หนักเกินไปและไม่สามารถทาให้เหล่าสแปมเมอร์ยาเกรงได้ เพราะยากที่ผู้ให้บริการเครือข่ายอินเทอร์เน็ตจะมีความสามารถในการกลั่นกรองข้อความสนทนาของผู้ใช้จานวนมากทั้งหมด ดังนั้นภาครัฐจึงต้องเข้ามามีบทบาทในการกาหนดมาตรการทางกฎหมายเพื่อปราบปรามเหล่าผู้ท าสแปม ยิ่งไปกว่านั้นหากการกระทารูปแบบนี้จ ากัดโทษอยู่เพียงความผิดทางแพ่ง หน้าที่ในการร้องต่อศาลหรือระบุตัวหาผู้กระทาความผิดจะเป็นของผู้ฟ้องเอง กว่าคดีความจะจบก็ใช้เวลานาน ค่าเสียหายที่ได้ก็อาจจะไม่คุ้มกับค่าใช้จ่ายและเวลาที่เสียไปกับการฟ้องร้องต่อศาลก็เป็นได้ หลายประเทศจึงมีการระบุโทษทางอาญาลงไปในกฎหมายที่เกี่ยวกับเรื่องนี้ด้วย เพราะในกฎหมายเอกชนมีหลักว่า “เมื่อไม่มีกฎหมายห้าม ทาได้” (Nullum crimen, nulla poena sine lege) การกาหนดความผิดอาญาให้กับการกระทานี้ จึงสามารถช่วยดึงรัฐเข้ามาเป็นตัวกลางในการสืบสวนเพื่อก าหนดโทษให้แน่ชัด[27] เพื่อป้องกันไม่ให้เกิดการกระท าความผิดซ้ า

ในประเทศไทยเอง เดิมทีการกระทาผิดที่เกี่ยวกับคอมพิวเตอร์ยังไม่สามารถเอาผิดทางอาญาได้ครอบคลุมมากนัก เนื่องจากข้อมูลดิจิทัลถือเป็นวัตถุที่ไร้รูปร่าง จึงไม่เข้าข่ายเป็น “ทรัพย์”[28] หรือ “ทรัพย์สิน”[29] (อ้างอิงคาพิพากษาที่ 5161/2547 ที่ตัดสินว่าการที่จาเลยนาแผ่นดิสมาคัดลอกข้อมูลดิจิทัลที่อยู่ในแผ่นดิสก์ของโจทก์ไป ไม่ถือเป็นความผิดฐานลักทรัพย์[30]) ดังนั้นการกระทาความผิดในหลายรูปแบบ เช่น การขโมยข้อมูลดิจิทัลจึงไม่สามารถเอาผิดโทษอาญาฐานลัก

---

[26] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 77 “รัฐพึงใช้ระบบอนุญาตและระบบคณะกรรมการในกฎหมายเฉพาะกรณีที่จ าเป็น พึงก าหนดหลักเกณฑ์ การใช้ดุลพินิจของเจ้าหน้าที่ของรัฐและระยะเวลาในการดาเนินการตามขั้นตอนต่าง ๆ ที่บัญญัติไว้ในกฎหมายให้ชัดเจน และพึงก าหนดโทษอาญาเฉพาะความผิดร้ายแรง”

[27] มานิตย์ จุมปา. ความรู้พื้นฐานเกี่ยวกับกฎหมาย. พิมพ์ครั้งที่ 14. ส านักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2559. หน้า123-125.

[28] ประมวลกฎหมายแพ่งและพาณิชย์ หมวด 3 มาตรา 137 “ทรัพย์ หมายความว่า วัตถุมีรูปร่าง”

[29] ประมวลกฎหมายแพ่งและพาณิชย์ หมวด 3 มาตรา 138 “ทรัพย์สิน หมายความ รวมทั้ง ทรัพย์ และ วัตถุไม่มีรูปร่าง ซึ่ง อาจมีราคา และ อาจถือเอาได้”

[30] ค าพิพากษาฎีกาที่ 5161/2547. เนติบัณฑิตยสภา. หน้า 940.

ทรัพย์ตาม มาตรา 334[31] ได้ หรือการปลอมแปลงข้อมูลดิจิทัลใส่ลงไปในระบบคอมพิวเตอร์ ก็ไม่สามารถเอาผิดอาญาฐานปลอมแปลงเอกสารตามมาตรา 264[32] ได้เช่นกัน

Herbert L. Packer ให้หลักการพิจารณาความผิดทางอาญาไว้ 6 ประการ ดังต่อไปนี้[33]

1) การกระทานั้นเป็นที่เห็นได้ชัดในหมู่ชนส่วนมากว่าเป็นการกระทาที่กระทบกระเทือนต่อสังคม และหมู่ชนส่วนมากมิได้ให้อภัยแก่การกระท าเช่นนั้น

2) ถ้าการกระทาดังกล่าวเป็นความผิดทางอาญาแล้ว จะไม่ขัดแย้งกับวัตถุประสงค์ของการลงโทษประการต่างๆ

3) การปรามปรามการกระทาเช่นนั้น หรือการถือว่าการกระทาเช่นนั้นเป็นความผิดทางอาญาจะไม่มีผลในการลดการกระท าอื่นที่สังคมเห็นว่าถูกต้องให้น้อยลง

4) หากเป็นความผิดทางอาญาแล้ว จะมีการบังคับใช้กฎหมายอย่างเสมอภาคและเท่าเทียมกัน

5) การใช้กระบวนการยุติธรรมทางอาญากับการกระทาดังกล่าวจะไม่มีผลให้เกิดการใช้กระบวนการนั้นอย่างเกินความสามารถทั้งด้านคุณภาพและปริมาณ

6) ไม่มีมาตรการควบคุมอย่างสมเหตุสมผลอื่นแล้วนอกจากการใช้กฎหมายอาญากับกรณีที่เกิดขึ้น

หลักการข้างต้นของ Packer มีขึ้นเพื่อเป็นหลักเกณฑ์การกาหนดความผิดทางอาญา ซึ่งหากพิจารณาแต่ละข้อแล้ว จะเห็นว่าผลกระทบที่เกิดขึ้นจากการกระทาความผิดในรูปแบบของสแปมนั้นเข้าข่ายว่าเป็นการกระทาที่ส่งผลกระทบต่อมหาชนและเป็นการกระทาผิดที่มีความซับซ้อนเกินกว่าที่ประชาชนทั่วไปจะเป็นผู้พิสูจน์ หรือสืบหาผู้กระทาความผิดด้วยตนเอง จึงเป็นเหตุอันสมควรที่ภาครัฐจะกาหนดกฎหมายเฉพาะขึ้นมารองรับ และมีบทกาหนดโทษทางอาญาเพื่อให้ป้องปรามเหล่าสแปมเมอร์ และคุ้มครองสิทธิในการใช้ชีวิตส่วนตัวของประชาชนทั่วไปที่เป็นผู้บริโภคอย่างเคร่งครัด แต่ในขณะเดียวกันก็ต้องยึดหลักศุภนิติกระบวนในการใช้อานาจรัฐเพื่อดักจับผู้ที่เกี่ยวข้องกับการกระทาความผิด เพื่อคุ้มครองสิทธิเสรีภาพในการประกอบอาชีพของผู้ให้บริการเครือข่ายอินเทอร์เน็ต เจ้าของเว็บไซต์ หรือเจ้าของกิจการที่ทาการโฆษณาด้วยช่องทางการส่งอีเมลที่อาจตกเป็นจ าเลยในคดีด้วยเช่นกัน

---

[31] ประมวลกฎหมายอาญา หมวด 1 มาตรา 334 “ผู้ใดเอาทรัพย์ของผู้อื่น หรือที่ผู้อื่นเป็นเจ้าของรวม อยู่ด้วยไปโดยทุจริต ผู้นั้นกระท าความผิดฐานลักทรัพย์ ต้องระวาง โทษจ าคุกไม่เกินสามปี และปรับไม่เกินหกพันบาท”

[32] ประมวลกฎหมายอาญา หมวด 3 มาตรา 264 “ผู้ใดท าเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด เติมหรือตัดทอนข้อความหรือแก้ไขด้วยประการใดๆ ในเอกสารที่แท้จริง หรือประทับตราปลอมหรือลงลายมือชื่อปลอมในเอกสาร โดยประการที่น่าจะเกิด ความเสียหายแก่ผู้อื่นหรือประชาชน ถ้าได้กระท าเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง ผู้นั้นกระท าความผิดฐานปลอมเอกสาร ต้องระวางโทษจาคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจ าทั้งปรับ”

[33] เกียรติขจร วัจนะสวัสดิ์, ค าอธิบายกฎหมายอาญา ภาค1 (หจก. จิรรัชการพิมพ์, 2549), หน้า 2-10.

2.4 บทบาทของภาครัฐในการหามาตรการควบคุมการกระทาความผิดฐานส่งข้อมูลหรืออีเมลในลักษณะ สแปม (spam)

เดิมทีจุดประสงค์หลักในการส่งสแปมมักใช้เพื่อทาการตลาดทางตรง (Direct Marketing) ไม่ว่าจะเป็นการโฆษณาแนะนาสินค้า การเชิญชวนหรือนาเสนอโปรโมชั่น เนื่องจากผู้ส่งเสียค่าใช้จ่ายที่น้อยมากในการส่งแต่ละครั้งเมื่อเทียบกับการโฆษณาประชาสัมพันธ์สินค้าและบริการด้วยวิธีอื่น และยังสามารถส่งออกได้ครั้งละหลายๆคน หรือหลายที่อยู่อีเมล ซึ่งยังท ให้เข้าถึงกลุ่มเป้าหมายได้มากขึ้นในระยะเวลาสั้นๆ ดังนั้นการส่งสแปมจึงไม่ใช่เรื่องที่ยอมรับกันไม่ได้เสียทีเดียว เทียบได้กับการโฆษณาโดยทั่วไป เช่น การแจกใบปลิว การเดินขายสินค้าตามบ้าน การส่งแฟกซ์ตามที่บริษัททั่วไปทาเพียงแต่ต้องมีเนื้อหาสอดคล้องกับมาตรา 22 ของพระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2522 ดังนี้

1) ไม่มีลักษณะอันเป็นเท็จ หรือท าให้เข้าใจผิดในสาระส าคัญของสินค้า-บริการ

2) ไม่มีเนื้อหาเกี่ยวกับการกระทาความผิดทางกฎหมาย หรือขัดต่อศีลธรรมอันดีน าไปสู่ความเสื่อมเสียในวัฒนธรรมของชาติ

3) ไม่ก่อให้เกิดความแตกแยกหรือเสื่อมความสามัคคีในหมู่ประชาชน

หากการทาสแปมเป็นการส่งออกไปอย่างถูกต้องตามกฎหมาย และมีวิธีการให้ผู้รับสามารถบอกยกเลิกบริการได้ตามความสมัครใจ ภาครัฐคงไม่จาเป็นต้องเข้ามาแทรกแซงกิจกรรมเหล่านี้ แต่เนื่องจากการกระทาที่เกินกว่าเหตุจนกระทบต่อสิทธิของผู้บริโภค และเกิดปัญหาขึ้นอีกมากมายตามที่กล่าวไปข้างต้น ภาครัฐจ าเป็นต้องสร้างมาตรการทางกฎหมายออกมาเพื่อควบคุมและคุ้มครองให้เกิดความสงบสุขในสังคม และเพื่อให้สามารถกาหนดหลักเกณฑ์ในการพิจารณาการกระทาความผิดทางคอมพิวเตอร์ได้อย่างเคร่งครัด

2.4.1 ลักษณะของหลักเกณฑ์ Opt-in และ Opt-out

หลักเกณฑ์ที่นามาใช้พิจารณาความผิดเกี่ยวกับการส่งสแปมเมลที่ทั่วโลกนิยมน ามาใช้มี2 รูปแบบ ได้แก่ หลัก Opt-in และหลัก Opt-out[34]

Opt-in หมายถึง การส่งข้อความไปยังผู้รับหรือผู้บริโภคจะเกิดขึ้นได้เมื่อผู้รับนั้นเป็นคนให้อนุญาตให้ส่ง กล่าวคือ ผู้รับจะต้องเป็นคนลงทะเบียนบอกรับโฆษณาหรือข้อมูลนั้นๆด้วยตนเองก่อน ผู้ส่งไม่สามารถส่งอีเมลไปหาโดยพลการได้ แม้ว่าผู้ส่งจะมีรายการที่อยู่นั้นๆอยู่ในมือก็ตาม ซึ่งวิธีนี้อาจทาให้ดูเหมือนเป็นการจ ากัดสิทธิเสรีภาพในการท าการพาณิชย์ของผู้ประกอบการก็ตาม แต่ก็ถือว่าเป็นวิธีการส่งเมลที่ปลอดภัยจากการโดนกดรายงาน (report) สะท้อนให้เกิดภาพลักษณ์ที่ดีต่อบริษัท และเป็นวิธีที่สามารถปกป้องสิทธิในความเป็นส่วนตัวของผู้บริโภคได้มากที่สุดเช่นกัน[35]

Opt-out หมายถึง การส่งข้อความถึงผู้รับด้วยที่อยู่ใดๆก็ได้โดยเสรี ไม่จาเป็นต้องได้รับค ายินยอม หรือการตอบรับจากผู้รับก่อนล่วงหน้า ซึ่งวิธีการนี้ได้รับความนิยมในการท าการตลาดเป็นจานวนมาก เพราะเพียงแค่สามารถหาที่อยู่ของผู้รับมาได้ไม่ว่าจะด้วยวิธีใดก็ตาม ก็จะสามารถ

---

[34] นาวิก น าสียง. การตลาดแบบ Opt-in หรือ Opt-out ดี? [ออนไลน์]. 2558. แหล่งที่มา: https://www.ecampaign101.com/email/การตลาดแบบ-opt-in-หรือ-opt-out-ดี/ [เข้าถึงเมื่อ 20 มิถุนายน 2561]

[35] เรื่องเดียวกัน

สื่อสารไปยังผู้บริโภคได้โดยตรงเลย แน่นอนว่าข้อดีของวิธีนี้คือทาให้สามารถเข้าถึงปลายทางผู้รับได้อย่างเสรี และไม่จากัดจานวน แต่ก็มีข้อเสียตรงที่อาจโดนผู้รับกดรายงาน (report) ว่าเป็นสแปมจนทาให้ติดบัญชีดา (Blacklist) หรือโดนซอฟต์แวร์ป้องกันสแปมดักจับจนอีเมลถูกโยนเข้าไปในกล่องอีเมลขยะ (Junk mail folder) ได้ง่าย สุดท้ายผู้รับก็จะไม่ได้เปิดอ่านเมลนั้นอยู่ดี และอาจทาให้ผู้รับเกิดความราคาญ จนส่งผลเสียต่อภาพลักษณ์ของบริษัทได้ ดังนั้นในอีเมลโฆษณาที่ใช้หลักการ Opt-out นี้ จึงควรเปิดช่องทางให้ผู้รับสามารถบอกเลิก (unsubscribe) ไว้ด้วย[36]

ทั้งสองวิธีที่กล่าวถึงในข้างต้น ต่างก็มีทั้งข้อดีและข้อเสียแตกต่างกันไป ดังนั้นจึงขึ้นอยู่เจตจานงของประเทศผู้ตรากฎหมายว่าจะชั่งน้าหนักให้การปกป้องอยู่ที่ด้านไหนมากกว่ากันเท่านั้น

2.4.2 จุดประสงค์ที่ภาครัฐจาเป็นต้องเข้ามาแทรกแซงการส่งข้อมูลหรืออีเมลในลักษณะสแปม (spam)

หลังจากยุคเฟื่องฟูของอินเทอร์เน็ตในช่วงต้นศตวรรษที่ 20 ปัญหาการใช้สแปมเริ่มเข้ามารบกวนความเป็นปกติสุขของคนหมู่มากตามที่ได้กล่าวไปข้างต้น ภาครัฐจึงจาเป็นต้องเข้ามาก หนดกฎเกณฑ์เพื่อให้เกิดความเป็นธรรมทั้งในฝั่งของผู้รับและผู้ส่ง ในช่วงแรกที่สแปมส่วนมากเป็นเพียงสิ่งมุ่งหาผลประโยชน์เชิงพาณิชย์ ภาครัฐอาจทาหน้าที่เพียงช่วยดูแลให้เกิดเสรีภาพต่อทั้งด้านผู้ประกอบการและผู้บริโภคทั้งสองฝ่ายผ่านบทกฎหมายที่ใกล้เคียง เช่น ใช้ประมวลแพ่งและพาณิชย์ในการปกป้องสิทธิในความเป็นส่วนตัวของผู้รับ และใช้กฎหมายที่เกี่ยวข้องกับการโฆษณามาปรับใช้เพื่อให้ทางฝั่งผู้ประกอบการที่เป็นคนส่ง ได้รับเสรีภาพทางการค้าและสามารถใช้ประโยชน์จากช่องทางอิเล็กทรอนิกส์ในการสื่อสาร หรือโปรโมทตัวสินค้าได้อย่างเต็มที่ แต่อย่างไรก็ตาม แม้ว่าสิทธิในการประกอบอาชีพ หรือสิทธิในการส่งอีเมลเพื่อสื่อสารหรือแสดงความคิดเห็นนี้จะเป็นสิทธิขั้นพื้นฐานตามกฎหมายที่พึงมี แต่หากใช้มากเกินไปจนก่อให้เกิดความเสียหายแก่ผู้อื่นย่อมเป็นเรื่องที่ไม่สมควร เมื่อพิจารณาถึงข้อจากัดในการใช้สิทธิตามจุดประสงค์ต่างๆ การกระทาความผิดในรูปแบบของสแปมเมลเกี่ยวข้องกับข้อจ ากัดในการใช้สิทธิดังต่อไปนี้

1) การใช้สิทธิที่เกินส่วนจนท าให้ผู้อื่นเกิดความเสียหาย (abuse of rights) อันได้แก่ การใช้อภิสิทธิ์เพื่อให้ตนได้รับผลประโยชน์เกินขอบเขตจนไปกระทบต่อสิทธิของผู้อื่น โดยในประมวลแพ่งและพาณิชย์ได้กล่าวถึงเรื่องนี้ไว้ในมาตรา 421 ที่บัญญัติว่า “การใช้สิทธิซึ่งมีแต่จะให้เกิดเสียหายแก่บุคคลอื่นนั้น ท่านว่าเป็นการอันมิชอบด้วยกฎหมาย” แต่แนวคาพิพากษาของประเทศไทยมีการวางหลักในเรื่องนี้ไว้ว่า “การใช้สิทธิเกินส่วนนี้จะต้องเป็นการแกล้งโดยผู้กระทามุ่งต่อผลที่จะให้เกิดความเสียหายแก่ผู้อื่นฝ่ายเดียว แต่ถ้าเป็นการกระทาโดยประสงค์ต่อผลอันเป็นธรรมดาแห่งสิทธินั้น แม้จาเลยผู้กระทาจะเห็นว่าผู้อื่นได้รับความเสียหายบ้าง ก็ไม่เป็นการละเมิด”[37] เพราะฉะนั้น การกระทาที่จะถือได้ว่าเป็นการใช้สิทธิเกินส่วนจึงต้องเป็นการกระทาที่ไม่มีวัตถุประสงค์อื่นเลยนอกจากเพื่อให้ผู้อื่นเสียหาย เมื่อนาแนวทางนี้มาพิจารณาถึงเรื่องการส่งสแปมเมล จึงเป็นเรื่องยากที่จะนา

---

[36] เรื่องเดียวกัน

[37] มานิตย์ จุมปา. ความรู้พื้นฐานเกี่ยวกับกฎหมาย. หน้า 282-283.

ความผิดฐานละเมิดมาปรับใช้กับการส่งสแปมเชิงพาณิชย์ เพราะจุดประสงค์ในการส่งสแปมประเภทนี้คือการทาเพื่อโฆษณาเท่านั้น ไม่ได้ทาไปเพื่อก่อความเสียหายให้ฝ่ายผู้รับ แม้ว่าฝ่ายผู้รับและหลายฝ่ายที่เกี่ยวข้องจะได้รับความเสียหายมากมายก็ตาม

2) การใช้สิทธิโดยไม่สุจริต โดยทั่วไปคาว่าสุจริตหมายถึง “การไม่รู้ข้อเท็จจริงที่เกิดขึ้นของคู่กรณีหรือเหตุการณ์อื่นๆที่เกี่ยวข้อง”[38] แต่ในทางกฎหมายยังไม่มีการกาหนดบทนิยามหรือองค์ประกอบในการพิจารณาความผิดของหลักนี้ไว้ตายตัว แม้ว่ากฎหมายหลายฉบับจะใช้หลักสุจริตในการพิจารณาก็ตาม ดังนั้นการพิจารณาจึงต้องใช้ดุลพินิจของผู้พิพากษา โดยหน้าที่ในการนาสืบว่าจาเลยเป็นผู้ที่กระทาโดยไม่สุจริตก็เป็นหน้าที่ของผู้ที่ฟ้อง ตัวอย่างเช่น **คาพิพากษาฎีกาที่ 751/2571** “นิติกรรมใดที่คู่กรณีได้ทาไป ท่านให้สันนิษฐานไว้ก่อนว่า นิติกรรมนั้นได้กระท าโดยสุจริต เมื่อผู้ใดคัดค้าน ผู้นั้นต้องนาสืบหักล้างข้อสันนิษฐานฯ” ซึ่งการที่ผู้รับสแปมเมลจะต้องรับภาระในการพิสูจน์เจตนาของผู้ท าสแปม ถือว่าเป็นภาระที่หนักมากเพราะต้องใช้ผู้ที่มีความสามารถเฉพาะทางและเทคโนโลยีเฉพาะทางในการหาหลักฐาน

3) การใช้สิทธิโดยขัดต่อความสงบเรียบร้อยและศีลธรรมอันดี จากที่ได้กล่าวไปในข้างต้นว่า “ความสงบเรียบร้อยและศีลธรรมอันดี” ไม่ได้มีกฎหมายฉบับใดให้ค านิยามไว้โดยตรง จึงไม่สามารถระบุหลักเกณฑ์หรือองค์ประกอบของความผิดที่ต้องนามาใช้พิจารณาได้ ซึ่งถ้าหากเป็นการกระทาที่ขัดต่อขนบธรรมเนียมและจารีตประเพณีอย่างชัดเจน เช่น การส่งข้อมูลลามกอนาจาร หรือการหมิ่นสถาบันพระมหากษัตริย์ คงไม่ยากที่จะใช้สามัญสานึกพื้นฐานมาพิจารณา แต่เนื่องจากการกระทาความผิดรูปแบบสแปมมีความซับซ้อน และมีรูปแบบที่เปลี่ยนแปลงไปตลอด การใช้หลักการนี้จึงอาจเกิดความคลุมเครือได้

4) การใช้สิทธิโดยทุจริตฉ้อโกง เช่นการปดปิดแหล่งที่มาของอีเมลเพื่อไม่ให้ผู้รับสามารถติดต่อไปยังผู้ส่งต้นทาง หรือการใช้ข้อความอันเป็นเท็จเพื่อปกปิดความจริงซึ่งควรบอกให้แจ้งแก่ผู้รับ หรือการใช้หัวเรื่องเท็จที่ทาให้ผู้รับเข้าใจผิดในสาระส าคัญของเนื้อหาในอีเมล เพื่อลวงให้ผู้รับเปิดอีเมลซึ่งมีการแฝงไวรัส มัลแวร์ หรือโปรแกรมอัตโนมัติต่างๆ ที่สามารถฝังตัวเข้ามาในระบบของผู้ใช้งานได้ ทาให้ผู้รับมีโอกาสเสี่ยงที่จะถูกขโมยข้อมูลส่วนบุคคลหรือถูกใช้งานระบบคอมพิวเตอร์ของตนเพื่อจุดประสงค์อันมิชอบ

จากประเด็นดังกล่าว แม้ว่าจะสามารถปรับใช้บทกฎหมายที่ใกล้เคียงอย่างยิ่งหลายบทหลายมาตรามาต่อสู้กับเหล่าสแปมเมอร์ได้ แต่ถ้าหากไม่มีการกาหนดโทษทางอาญาที่ชัดเจนหรือไม่มีกฎหมายเฉพาะเข้ามาควบคุม การพิพากษาหรือตีความเอาจากบทบัญญัติกฎหมายอื่นที่มีความหมายค่อนข้างกว้างนั้น ไม่อาจควบคุมอาชญากรรมและไม่อาจทาให้เกิดความชอบธรรมในกระบวนการยุติธรรมได้เพียงพอ กล่าวคือ การที่โจทก์ผู้ฟ้องต้องมีภาระในการพิสูจน์ให้เห็นถึงความเสียหายที่เกิดขึ้นจากการกระท าดังกล่าวให้เห็นเป็นรูปธรรมชัดเจนด้วยตัวเองเป็นเรื่องยาก ต้องอาศัย

[38] เรื่องเดียวกัน. หน้า 283-285

ผู้เชี่ยวชาญเฉพาะด้านในการตีค่าความให้ความเสียหายนั้นกลายเป็นรูปธรรม อีกทั้งการกระทาความผิดในรูปแบบสแปมยังก่อให้เกิดผลเสียหายหรือเกิดความเดือดร้อนกับบุคคลในวงกว้างจนไม่สามารถจากัดขอบเขตพื้นที่ที่เกิดความเสียหายได้ และไม่ได้ส่งผลกระทบต่อผู้ใดผู้หนึ่งเพียงคนเดียว การพิสูจน์ถึงระดับความเดือดร้อนเสียหายที่มีมากพอสมควรแก่โทษเมื่อเทียบจากมาตรฐานของวิญญูชน (objective) จึงเป็นเรื่องยากสาหรับใครคนใดคนหนึ่ง และยากที่ผู้เสียหายจะสามารถรวมตัวกันเพื่อพิสูจน์ความเสียหายที่เกิดขึ้นนั้นให้ชัดเจน อีกทั้งค่าใช้จ่ายหรือเวลาที่ต้องเสียไปเพื่อการพิสูจน์หาหลักฐานอาจไม่คุ้มค่าสาหรับผู้เสียหาย รัฐจึงควรเข้ามาแทรกแซงการกระทารูปแบบนี้เพื่อปกป้องผลประโยชน์และสิทธิของประชาชนในชาติ โดยเฉพาะอย่างยิ่ง เมื่อการทาสแปมมีวิวัฒนาการจนไปถึงขั้นที่มีการหลอกลวง ฉ้อโกง จนความเสียหายที่เกิดขึ้นกระทบกระเทือนไปถึงด้านเศรษฐกิจ สังคม และความมั่นคงของรัฐ ภาครัฐจึงไม่สามารถปล่อยให้ปัญหานี้ลุกลามได้อีกต่อไป ด้วยเหตุผลนี้ จึงจาเป็นต้องตรากฎหมายเฉพาะออกมาเพื่อรองรับการกระทาความผิดที่มีรูปแบบพิเศษเฉพาะตัวนี้ เพื่อกาหนดลักษณะการกระทาที่เป็นความผิดไว้ให้ชัดเจน ลดภาระการพิสูจน์ของผู้เสียหาย รวมถึงเพื่อควบคุมการเพิ่มจานวนของสแปม ควบคุมความเหมาะสมของเนื้อหาในอีเมล ปราบปรามการกระท าความผิดของสแปมเมอร์ และให้ท าให้เกิดกระบวนการยุติธรรมที่ชอบด้วยกฎหมาย

2.5 การใช้อีเมลในลักษณะสแปมเพื่อจุดประสงค์เชิงพาณิชย์ในปัจจุบัน

คาว่า Email Marketing หรือก็คือ “วิธีทาการตลาดด้วยอีเมล” กลายเป็นคาคุ้นหูสาหรับสังคมในปัจจุบัน ไม่ว่าจะเป็นทั้งด้านผู้ประกอบการหรือผู้บริโภค เพราะปัจจุบันเทคโนโลยีเข้ามามีบทบาททั้งในภาคเศรษฐกิจและสังคมเป็นอย่างมาก ผู้ประกอบการสามารถเจาะจงกลุ่มเป้าหมายที่ต้องการและเข้าถึงผู้บริโภคได้อย่างรวดเร็วเพียงเสี้ยววินาที แต่เมื่อทุกอย่างสะดวกสบายขึ้น แน่นอนว่าการแข่งขันในตลาดก็ย่อมจะรุนแรงมากขึ้นเช่นกัน นักการตลาดต่างพยายามหาคอนเทนท์ (content) ที่น่าสนใจออกมาเพื่อจูงใจผู้บริโภค และหาช่องทางการสื่อสารที่สามารถเข้าถึงผู้บริโภคได้รวดเร็ว ลดเวลาการทาธุรกิจ และทาให้ผู้บริโภคสามารถติดต่อได้อย่างสะดวกไม่ว่าจะเป็นทั้งแบบออฟไลน์ หรือออนไลน์ จึงเป็นสาเหตุให้การส่งอีเมลเชิงพาณิชย์กลายเป็นวิธีที่ตอบโจทก์กับความต้องการและสภาพสังคมในปัจจุบันได้มากที่สุดด้วยเหตุผลดังต่อไปนี้[39]

1) เป็นช่องทางที่ช่วยให้เกิดปฏิสัมพันธ์ การตอบโต้ระหว่างผู้ประกอบการและผู้บริโภคได้อย่างรวดเร็ว (Quick Response) เพื่อลดความล่าช้าและต้นทุนในกิจกรรมดูแลลูกค้า (Customer Service)

2) เป็นช่องทางการประชาสัมพันธ์แบบไม่จากัดเวลา ไม่มีข้อจากัดเรื่องเขตเวลา (Time Zone) จึงท าให้สามารถสื่อสารได้ทั่วทุกมุมโลกตลอดเวลา

[39] Supansa. การตลาดอิเล็กทรอนิกส์ (e-Marketing) หมายถึง [ออนไลน์]. 2561. แหล่งที่มา: https://www.wynnsoft-solution.com/การตลาดอิเล็กทรอนิกส์_(e-Marketing)_หมายถึง [เข้าถึงเมื่อ 17 พฤษภาคม 2561]

3) สามารถกระจายไปยังกลุ่มผู้บริโภคได้โดยตรงแบบตัวต่อตัว และสามารถจากัดกลุ่มเป้าหมายได้ชัดเจน

4) สามารถเกิดการสื่อสารสองทาง (Two Way Communication) ระหว่างผู้ประกอบการและผู้บริโภค และมีส่วนส่งเสริมให้การบริหารความสัมพันธ์ลูกค้า (Customer Relationship Management) มีประสิทธิภาพมากยิ่งขึ้น

5) เป็นวิธีการประชาสัมพันธ์ที่ใช้ต้นทุนต่ าแต่เกิดประสิทธิภาพสูง

นอกจากนี้การโฆษณาโดยใช้อีเมลเชิงพาณิชย์ ยังเป็นส่วนหนึ่งของการทาการตลาดอิเล็กทรอนิกส์ (Electronics Marketing) ซึ่งเป็นเครื่องมือสาคัญในการประชาสัมพันธ์บนตลาดพาณิชย์อิเล็กทรอนิกส์ (e-commerce) ที่ก าลังได้รับความนิยมมากในปัจจุบัน

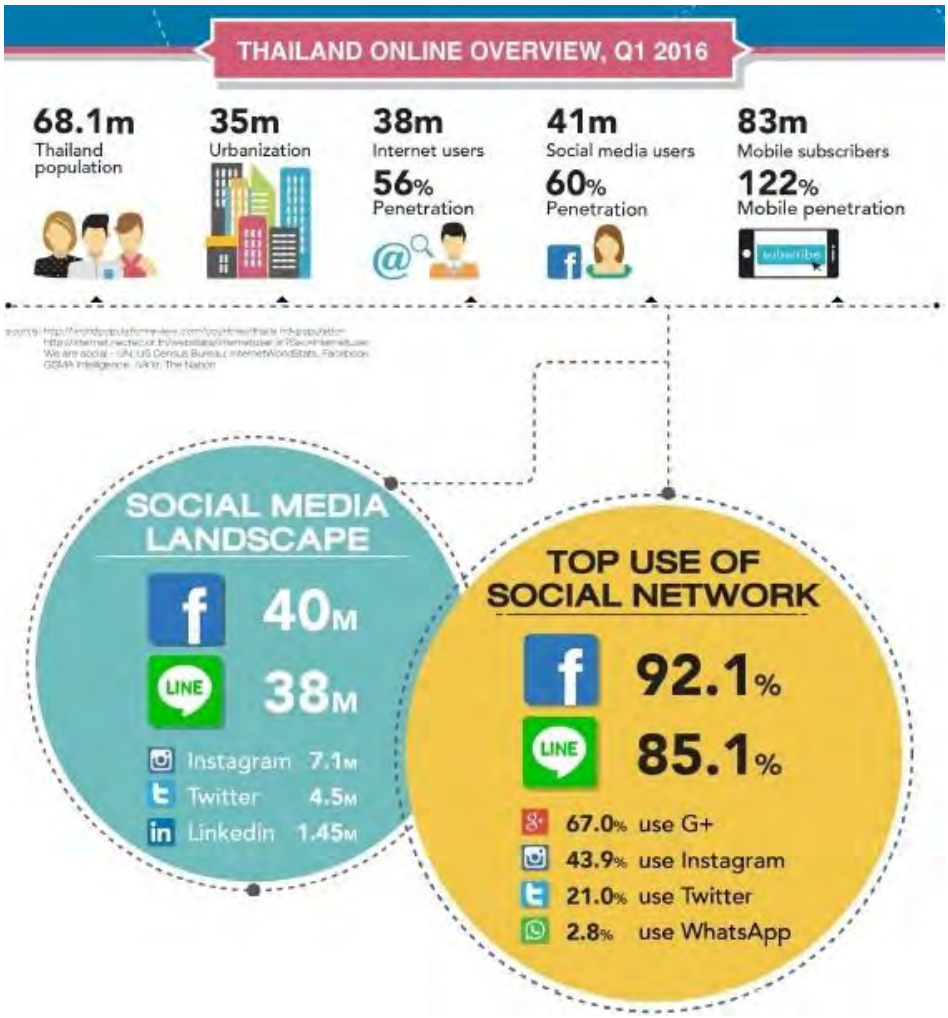
2.5.1 สถานการณ์การตลาด e-commerce ในปัจจุบัน

จานวนผู้ใช้งานอินเทอร์เน็ตมีเพิ่มมากขึ้นโดยตลอด ผลสารวจของสมาคมโฆษณาดิจิทัล (ประเทศไทย) พบว่าในไตรมาสที่ 1 ปี 2559 ประเทศไทยมีผู้ใช้งานอินเทอร์เน็ตรวมทั้งสิ้น 38 ล้านคน จากประชากรรวมทั้งประเทศ 68.1 ล้านคน ซึ่งคิดเป็น 56% ของจานวนประชากรทั้งหมด[40] (อ้างอิงภาพที่2) สาเหตุหนึ่งที่ทาให้การเติบโตเพิ่มมากขึ้นอย่างต่อเนื่องทุกปีก็เพราะเทคโนโลยีของเครือข่ายอินเทอร์เน็ตทั้ง 3G 4G Boardbrand ถูกพัฒนาให้มีความเร็วสูงและสามารถครอบคลุมได้ทั่วถึงทุกพื้นที่ อีกทั้งเครื่องมือในการเข้าถึงเครือข่ายอินเทอร์เน็ตไม่ว่าจะเป็น สมาร์ทโฟน แท็ปเล็ต โน๊ตบุ๊ก ก็ถูกพัฒนาให้มีประสิทธิภาพสูง ราคาย่อมเยา และมีขนาดเล็กลงสามารถพกพาได้สะดวก จนไม่ว่าใครอายุเท่าไหร่ก็สามารถซื้อหามาใช้งานได้โดยง่าย จนอุปกรณ์เหล่านี้แทบจะกลายเป็นปัจจัยที่ห้าในการด ำเนินชีวิตปัจจุบันไปแล้ว เมื่อผู้คนสามารถเข้าถึงเครือข่ายอินเทอร์เน็ตได้ตลอดเวลา ความนิยมในการใช้อีเมลเพื่อติดต่อสื่อสาร หรือการสื่อสารกันผ่านสังคมออนไลน์ (Social media) ต่างๆ ไม่ว่าจะเป็นเฟสบุ๊ก อินสตาแกรม ทวิตเตอร์ ไลน์ ฯลฯ จึงเพิ่มสูงขึ้นอย่างต่อเนื่อง ทาให้ภาคธุรกิจไม่ว่าจะเป็นขนาดใหญ่หรือขนาดเล็กอย่าง Startup ต่างก็ต้องเร่งพัฒนาตนเองให้ก้าวตามทันกระแสและยุคสมัยที่ทุกสิ่งสามารถเกิดขึ้นบนเครือข่ายออนไลน์ มิเช่นนั้นธุรกิจก็อาจอยู่รอดในสภาพการณ์เช่นนี้ได้ยาก อันจะเห็นได้จากผลสารวจของสานักงานสถิติแห่งชาติที่ระบุว่าในปี 2557 ธุรกิจที่เข้ามาจดทะเบียนพาณิชย์อิเล็กทรอนิกส์สามารถจาแนกสัดส่วนตามขนาดของธุรกิจได้เป็น ธุรกิจขนาดเล็ก (1-5 คน) ร้อยละ 70.3 ธุรกิจขนาดกลาง (6-50 คน) ร้อยละ 22.9 ธุรกิจขนาดใหญ่ (≥50 คน) ร้อยละ 6.8[41] (อ้างอิงภาพที่ 3)

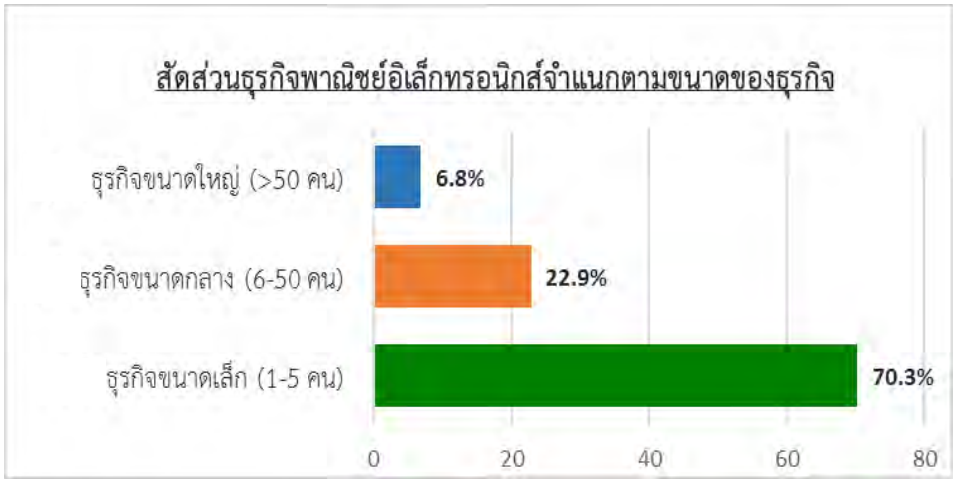
---

[40] สมาคมโฆษณาดิจิทัล (ประเทศไทย). DAAT เผยข้อมูลผู้ใช้อินเทอร์เน็ตของไทย ไตรมาส 1 ประจาปี 2559 [ออนไลน์]. 2559. แหล่งที่มา http://www.daat.in.th/index.php/daat-internet/ [27 กุมภาพันธ์ 2561]

[41] ส านักงานสถิติแห่งชาติ, การส ารวจสถานภาพการพาณิชย์อิเล็กทรอนิกส์ของประเทศไทย พ.ศ. 2557



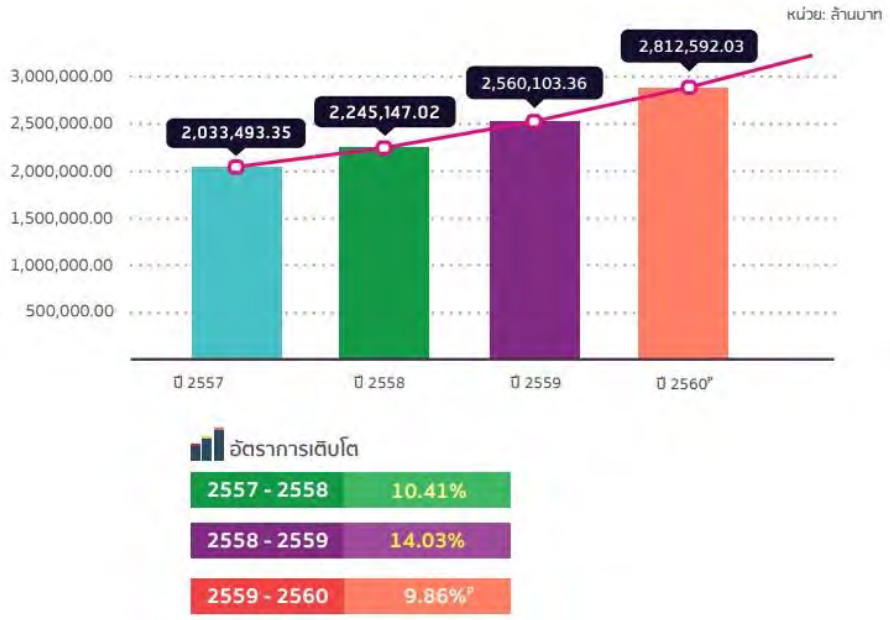
ภาพที่ 2 ผลส ชวจจ านวผู้ใช้อินเทอร์เน็ตในประเทศไทยประจ ไตรมาสแรกปี 2559[42]



ภาพที่ 3 สัดส่วนธุรกิจพาณิชย์อิเล็กทรอนิกส์จ าแนกตมขนาดของธุรกิจประจ าปี2557[43]

[42] สมาคมโฆษณาดิจิทัล (ประเทศไทย), DAAT เผยข้อมูลผู้ใช้อินเทอร์เน็ตของไทย ไตรมาส 1 ประจาปี 2559 [ออนไลน์].
[43] เรื่องเดียวกัน

ข้อมูลของสานักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ระบุว่าในช่วงปี 2560 ที่ผ่านมาตลาด e-commerce ในประเทศไทยมีมูลค่าสูงถึง 2,812 ล้านบาท ซึ่งเติบโตเพิ่มขึ้นจากปี 2558 ถึง 14.03%[44] (อ้างอิงภาพที่ 2.4) ธุรกิจใหม่ๆที่หันมาเพิ่มช่องทางการจาหน่ายหรือช่องทางการเข้าถึงลูกค้าผ่านระบบ e-commerce ก็เพิ่มมากขึ้นจนท าให้อัตราการแข่งขันสูงขึ้นทุกปี



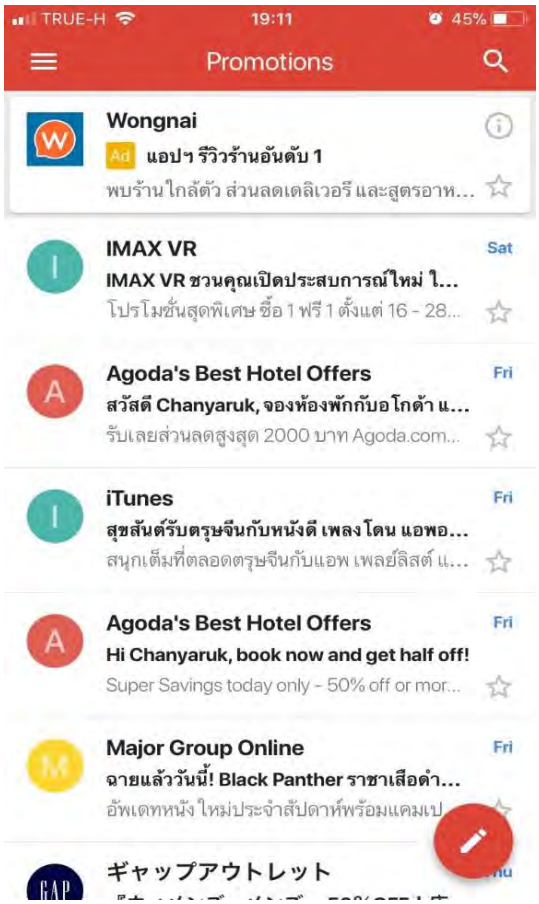
ภาพที่ 4 มูลค่า e-commerce ในประเทศไทยปี 2557-2560[45]

ไม่เพียงแค่การทาธุรกิจผ่านทางเว็บไซต์เท่านั้น ปัจจุบันหลายบริษัทเริ่มหันมาพัฒนาแอปพลิเคชันควบคู่กันไปด้วย เช่น Lazada Pomelo Central Online Agoda ฯลฯ เพราะนอกจากจะท ให้ผู้บริโภคสามารถเข้าถึงได้ง่ายแล้ว ยังเป็นอีกช่องทางที่ให้ผู้ประกอบการสามารถสร้างฐานข้อมูล (Database) ของลูกค้าได้ด้วยเช่นกัน เพราะลูกค้าที่โหลดแอปพลิเคชันเข้ามาใช้งานมักถูกบังคับให้ลงทะเบียนเพื่อเริ่มใช้งานเสมอ ดังนั้น ข้อมูลส่วนตัวไม่ว่าจะเป็นเพศ ชื่อ นามสกุล อีเมล เบอร์โทรศัพท์ หรือกระทั่งที่อยู่ก็ตกไปอยู่ในมือของผู้ประกอบการโดยปริยายแม้ว่าจะยังไม่เกิดการซื้อขายขึ้นเลยก็ตาม แน่นอนว่าผู้ประกอบการมีหน้าที่จะต้องจัดทาเงื่อนไข (Term&condition) ในการลงทะเบียนหรือใช้ข้อมูลส่วนของลูกค้าอยู่แล้ว แต่ก็มีลูกค้าน้อยคนที่จะอ่านเงื่อนไขเหล่านั้นจนจบ หรือบางทีก็มีการทาเครื่องหมายคาไว้ที่ช่องยินยอมรับข่าวสาร (Subscribe) โดยอัตโนมัติ ท ให้ลูกค้าบางคนที่ไม่ทันระวังมองข้ามไป หลังจากที่การลงทะเบียนเสร็จสิ้นจึงมีเมลโฆษณาเข้ามาตลอดเวลาโดยไม่รู้ตัว ยิ่งหากเป็นคนที่มีอีเมลหลายอีเมล หรือเป็นคนที่ไม่ค่อยได้เปิดเข้าไปเช็คในโฟลเดอร์ Promotion ของอีเมล ก็อาจจะเผอเรอจนไม่ทราบว่ามีอีเมลโฆษณาจานวนมากค้างอยู่ในกล่องข้อความ (Mail Box) ก็เป็นได้

---

[44] ส นักยุทธศาสตร์. รายงานผลการส าจจมูลค่าพาณิชย์อิเล็กทรอนิกส์ในประเทศไทยปี 2560. พิมพ์ครั้งที่ 1. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, กันยายน 2560.

[45] เรื่องเดียวกัน



ภาพที่ 5 ตัวอย่างโฟลเดอร์ Promotion ในอีเมล

เมื่อข้อมูลส่วนตัวไม่เป็นความลับอีกต่อไป การทาโฆษณารูปแบบของการส่งข้อความที่แทบจะไม่เสียค่าใช้จ่าย หรือไม่สามารถคิดค่าบริการโดยตรง เช่น นับตามจานวนข้อความหรือน้าหนักของจดหมายได้อย่างอีเมล จึงเป็นทางเลือกที่สะดวก ง่ายดาย และประหยัดต้นทุนสาหรับผู้ประกอบการ โดยผู้ที่เกี่ยวข้องกับการด าเนินธุรกิจทางอีเมลแบ่งได้ 2 กลุ่มใหญ่ๆ ดังนี้

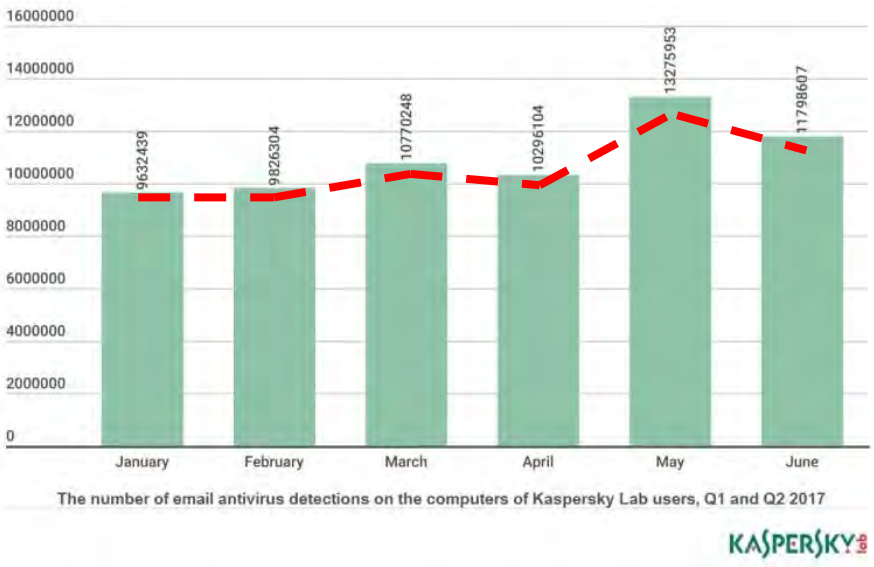
1) ผู้ให้บริการอีเมล (E-mail service provider) ที่คิดค่าบริการจากการเช่าใช้ที่อยู่สาหรับส่งอีเมลเป็นหลัก แต่ในช่วงหลังมีผู้ให้บริการอีเมลฟรีเกิดขึ้นเป็นจานวนมาก เช่น Hotmail Yahoo หรือ Gmail แม้ว่าจะไม่ได้คิดค่าบริการสาหรับการเช่าที่อยู่อีเมลโดยตรง แต่มักหารายได้จากการขายพื้นที่โฆษณาแทน

2) ผู้ทาการตลาดผ่านอีเมล (E-mail marketer) หมายถึง บริษัทผู้บริหารแพลตฟอร์มการตลาดผ่านออนไลน์แบบเบ็ดเสร็จ เช่น Mailchimp, Benchmark, Email, Drip ActiveCampaign GetResponse เป็นต้น ซึ่งบริษัทเหล่านี้จะช่วยเข้ามาบริหารจัดการตั้งแต่ขั้นตอนการรวบรวมอีเมลลูกค้าเพื่อสร้างฐานข้อมูล (Database) สร้างแบบฟอร์มในการลงทะเบียน (Signup form) เพื่อนาฐานข้อมูล (Database) เหล่านั้นมาแบ่งกลุ่ม (Segment) เพื่อจาแนกประเภทของลูกค้าแล้วนาข้อมูลเหล่านั้นมาเชื่อมต่อกับระบบการบริหารลูกค้าสัมพันธ์ (Customer Relationship

Management : CRM) เพื่อสร้างอีเมลโฆษณาให้มีเนื้อหา (content) ตรงตามความต้องการและสามารถดึงดูดลูกค้าได้มากที่สุด แต่การทาโฆษณาโดยส่งอีเมลผ่านบริษัทเหล่านี้ก็มีความเสี่ยงที่จะติดนโยบายการใช้งาน (Policy) ของผู้ให้บริการเครือข่ายอินเทอร์เน็ต (ISPs) ทาให้อีเมลนั้นโดนดักจับว่าเป็นสแปม ทาให้โดนโยนอีเมลเข้าไปยังกล่องข้อความขยะ (Junk Box) แทน เนื่องจากอีเมลของผู้ส่งเป็นอีเมลที่ไม่เคยมีปฏิสัมพันธ์กับเจ้าของอีเมลมาก่อน ยิ่งไปกว่านั้น ก็มีความเสี่ยงที่จะโดนลูกค้ากดรายงาน (report) เพราะเป็นอีเมลที่ส่งเข้ามาโดยผู้ใช้ไม่เคยร้องขอ

2.5.2 สถิติการท สแปมเมลและฟิชชิ่ง (spam mail & phishing)

การเกิดขึ้นของสแปมไม่ได้เป็นแค่ช่องทางที่ใช้ในการโฆษณาสินค้าหรือบริการเท่านั้น ยังมีเหล่ามิจฉาชีพที่อาศัยช่องทางนี้ในการล่อลวงผู้บริโภคอยู่ด้วยเช่นกัน ไม่ว่าจะเป็นการเชิญชวนหรือหลอกล่อให้ผู้ใช้สมัครใช้บริการอื่นแบบเสียเงิน การปลอมแปลงชื่อผู้ส่งเป็นหน่วยงานหรือบุคคลที่มีชื่อเสียง ฯลฯ จากผลสารวจสถิติภัยคุกคามจากสแปมเมลและการทาฟิชชิ่ง (Phishing) ของบริษัท Kaspersky ในปี 2560 ไตรมาสที่สอง ทาให้พบว่าสแปมเมลมีอัตราเติบโตจากไตรมาสที่หนึ่งเพิ่มขึ้นถึง 17%[46] (อ้างอิงภาพที่ 6)



ภาพที่ 6 จ านวนอีเมลที่โปรแกรม Antivirus ดักจับว่าเป็นสแปม ไตรมาสที่ 1-2 ปี2560[47]

ประเภทของสแปมที่ที่พบมากได้แก่ การส่งมัลแวร์โดยแนบไฟล์ .ZIP เข้ามาทางอีเมลที่ปลอมแปลงเนื้อหาหรือปลอมแปลงหัวเรื่องว่า “การส่งของคุณล้มเหลว” ทาให้ผู้รับเกิดความรู้สึกสงสัยว่าส่งตนเองเคยส่งอะไรไปหาใคร เมื่อคลิ๊กที่ลิงก์ในเนื้อเมล หรือคลิ๊กเปิดไฟล์แนบเหล่านั้น ตัวมัลแวร์ก็จะท ขานทันที (อ้างอิงภาพที่ 7) หรือใช้เนื้อหาเมลที่แจ้งว่ามีวิธีป้องกันมัลแวร์ หรือมีบริการแก้ไขเครื่อง

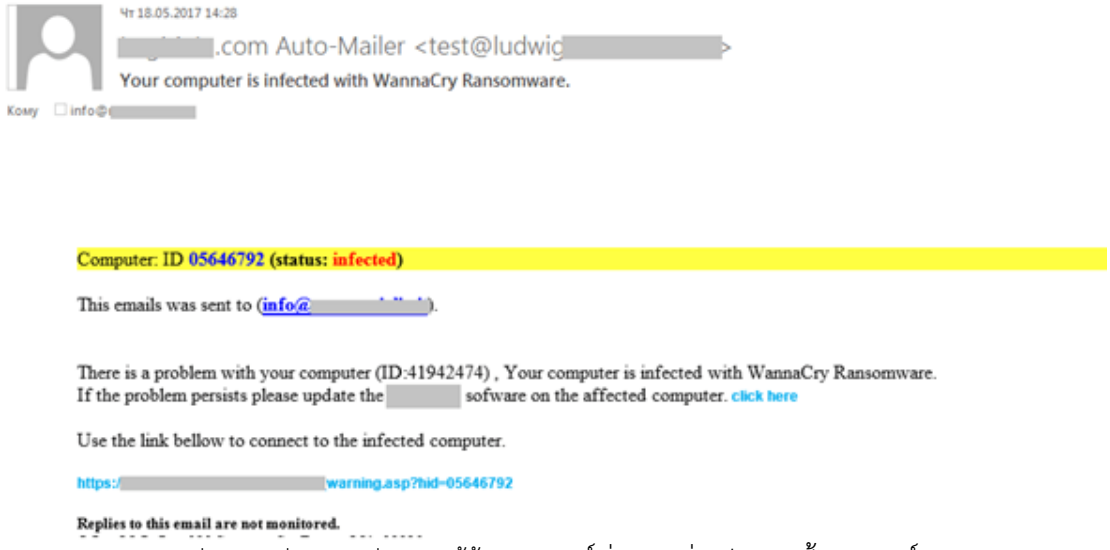
---

[46] Darya Gudkova, M. V., Tatyana Shcherbakova, Nadezhda Demidova [Online]. 2017. Available from: https://securelist.com/spam-and-phishing-in-q2-2017/81537/ [14 March 2018.]

[47] เรื่องเดียวกัน

ที่ติดมัลแวร์ เพื่อหลอกให้ผู้รับคลิกลิงก์เข้าไปยังหน้าเว็บไซต์ที่แพร่กระจายมัลแวร์อีกทอดหนึ่ง (อ้างอิงภาพที่ 8)

ภาพที่ 7 ตัวอย่างอีเมลที่แผงมัลแวร์เข้ามาในไฟล์แนบ[48]

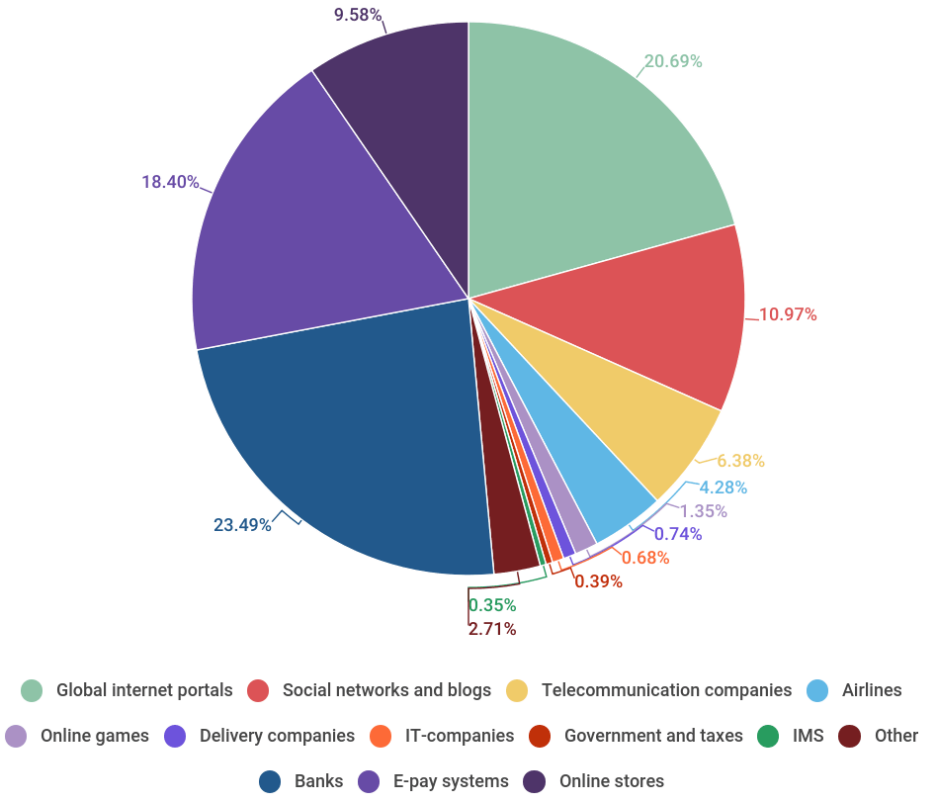


ภาพที่ 8 ตัวอย่างอีเมลที่หลอกให้ผู้รับคลิกลิงก์ที่หลอกว่าเป็นวิธีแก้ไขมัลแวร์[49]

[48] เรื่องเดียวกัน

[49] เรื่องเดียวกัน

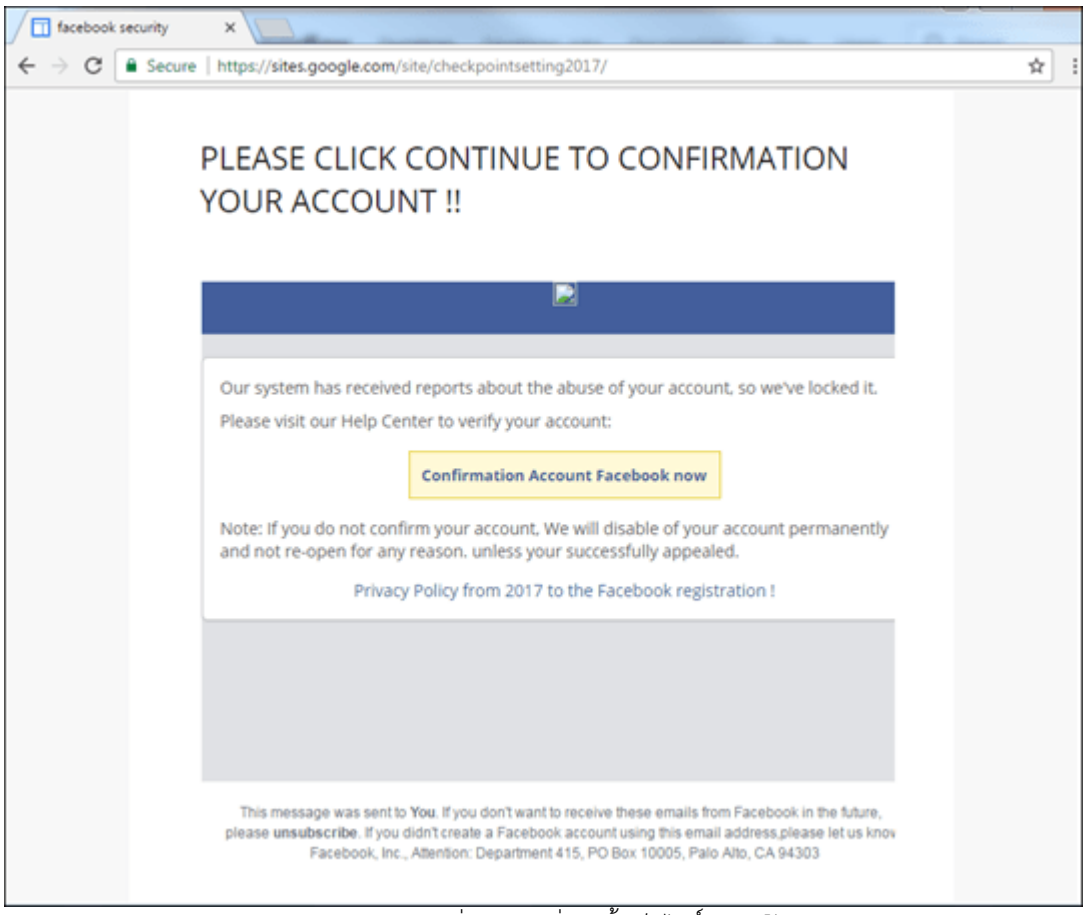
นอกจากนี้ Kaspersky ยังพบว่าในไตรมาสที่สองของปี 2560 นี้ ระบบ Anti-Phishing สามารถปกป้องผู้ใช้งานที่โดนหลอกเข้าไปใน phishing pages ได้ถึง 46,557,343 คน และยังมีผู้ใช้งานที่โดนทา Phishing มากถึง 8.26% จากจ นวนผู้ใช้งาน Kaspersky ทั่วโลก โดยประเภทของอีเมล Phishing ที่พบมากที่สุดคือบริการด้านการเงิน เช่น ธนาคาร 23.49% ระบบชาระค่าบริการ 8.40% และร้านขายสินค้าออนไลน์ 9.58% ตามล ดับ (อ้างอิงภาพที่ 9)



ภาพที่ 9 ประเภทของอีเมล Phishing ที่สามารถตรวจจับได้ในไตรมาสที่สอง ปี2560[50]

โดยองค์กรหรือเพจที่โดนโจมตีจากการทาฟิชชิ่ง (Phishing) มากที่สุดคือ Facebook รองลงมาคือ Microsoft Corporation และ Yahoo! ตามลาดับ โดยล่อให้ผู้รับคลิ๊กลิงก์แคมเปญโปรโมทต่างๆ เช่น แจกตั๋วโดยสารเครื่องบิน เพื่อให้ผู้ใช้เข้ามากรอกข้อมูลส่วนบุคคลในเว็บไซต์ปลอมที่สร้างขึ้น หรือท าURL เลียนแบบเพื่อลวงให้ผู้ที่คลิ๊กลิงก์เข้าใจผิด (อ้างอิงภาพที่10)

[50] เรื่องเดียวกัน



ภาพที่ 10 ตัวอย่างหน้าเว็บไซต์ปลอม[51]

จากรายละเอียดที่กล่าวมาทั้งหมดท ให้ทราบได้ว่า การใช้อีเมลมีทั้งข้อดีและข้อเสียขึ้นอยู่กับผู้ที่ใช้งานว่าจะใช้ไปในทางใดและมีวิธีการใช้อย่างไร ปัจจุบันการหลอกลวงผ่านสแปมเมลไม่ใช่เรื่องไกลตัวอีกต่อไป ผู้บริโภคจึงควรศึกษาทาความเข้าใจให้ทันกับวิวัฒนาการของสแปมเพื่อที่จะได้สามารถปกป้องตนเองให้ปลอดภัย แต่ในขณะเดียวกันภาครัฐก็ควรเข้ามามีส่วนช่วยกาหนดมาตรการป้องปรามที่เป็นธรรมและไม่เข้มงวดจนเกิดผลกระทบกับผู้ประกอบการมากเกินไปเพื่อให้เกิดความสมดุลทั้งด้านเศรษฐกิจและสังคม ส่วนตัวผู้ประกอบการเองก็มีความจาเป็นอย่างยิ่งที่จะต้องทาความเข้าใจในกฎเกณฑ์ที่เกี่ยวข้อง เพื่อให้สามารถพัฒนาธุรกิจของตนให้ประสบความสาเร็จในยุคดิจิทัลอย่างถูกกฎหมาย และเกิดภาพลักษณ์ที่ดี

[51] เรื่องเดียวกัน

บทที่ 3
กฎหมายเกี่ยวกับการกระท ผิดในรูปแบบสแปม (spam) ของประเทศไทย

ในยุคปัจจุบัน อินเทอร์เน็ตกลายเป็นเครื่องมืออานวยความสะดวกที่ช่วยลดอุปสรรคด้านระยะทางหรือความต่างของช่วงเวลาที่ใช้ในการติดต่อสื่อสาร จึงทาให้การใช้จดหมายอิเล็กทรอนิกส์ การหาข้อมูลความรู้บนอินเทอร์เน็ต การเชื่อมต่อระบบขององค์กรต่างๆสามารถดาเนินการได้จากทุกที่ในระยะเวลาอันสั้น ยิ่งไปกว่านั้น ปัจจุบันเครือข่ายโซเชียลเน็ตเวิร์ค (Social Network) เองก็เข้ามามีบทบาททั้งทางด้านสังคมทั่วไปและในด้านการดาเนินธุรกิจมากขึ้น แน่นอนว่าอินเทอร์เน็ตคือวิวัฒนาการที่ก่อให้เกิดประโยชน์ต่อมนุษย์มากมาย แต่ในขณะเดียวกันก็มีผู้ไม่ประสงค์ดีที่คอยแสวงหาผลประโยชน์จากความสะดวกสบายนี้เช่นกัน การใช้อินเทอร์เน็ตผิดวัตถุประสงค์ และอาชญากรรมทางคอมพิวเตอร์ประเภทต่างๆเกิดขึ้นตามมาอีกมากมาย อาทิเช่น การแสดงความคิดเห็นเชิงหมิ่นประมาทบนอินเทอร์เน็ต การแฮกข้อมูลส่วนบุคคลหรือเว็บไซต์สาคัญๆ การเผยแพร่ข่าวปลอม การสร้างข้อมูลเท็จเพื่อหลอกลวงผู้บริโภค ฯลฯ

สแปมถือเป็น “ภัยคุกคามทางอินเทอร์เน็ต” รูปแบบหนึ่งเช่นกัน เพราะเป็นการกระทาที่ก่อให้เกิดความเดือดร้อนราคาญทั้งต่อตัวผู้รับที่เป็นบุคคลธรรมดาตลอดจนที่เป็นผู้ประกอบการ อีกทั้งยังสร้างภาระผลเสียให้แก่ผู้ให้บริการเครือข่าย ทั้งนี้ แม้ว่าภาคเอกชนจะพยายามหามาตรการต่างๆขึ้นมาป้องกันและรับมือกับปัญหาเหล่านี้กันแล้วก็ตาม แต่การป้องกันปัญหาที่ปลายเหตุ ไม่ได้ช่วยแก้ปัญหาได้อย่างแท้จริง ดังนั้นจึงต้องอาศัยการออกกฎหมายจากภาครัฐเข้ามาช่วยแก้ปัญหาและปราบปรามให้ผู้ที่คิดจะกระทา เกิดความยาเกรงต่อโทษจากผลของการกระทานั้นๆ เพื่อป้องกันไม่ให้มีการกระทาความผิดดังกล่าว โดยในบทนี้จะอธิบายถึงที่มา จุดประสงค์ และสาระสาคัญของพระราชบัญญัติว่าด้วยการกระท ผิดเกี่ยวกับคอมพิวเตอร์ พร้อมทั้งเปรียบเทียบพระราชบัญญัติฯเดิมกับพระราชบัญญัติฯใหม่ที่มีผลบังคับใช้ตั้งแต่ พ.ศ. 2560 เพื่อสะท้อนให้เห็นถึงภาพรวมของบทบัญญัติทางกฎหมายของประเทศไทยที่เกี่ยวข้องกับความผิดฐานสแปม (spam)

3.1 พระราชบัญญัติว่าด้วยการกระท ผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

อาชญากรรมทางคอมพิวเตอร์มีความรุนแรงและมีเทคโนโลยีที่ซับซ้อนมากขึ้นทุกวัน การอาศัยเพียงแค่กฎหมายอาญาแบบเดิมมาใช้ในการพิพากษาจึงยากต่อการนาตัวผู้กระทาความผิดมาลงโทษได้ อีกทั้งการสืบหาหลักฐานเกี่ยวกับการกระท ผิดรูปแบบนี้ก็เป็นเรื่องยากเนื่องจากข้อมูลเป็นสิ่งที่ไร้รูปร่าง เกิดการเปลี่ยนแปลงง่าย ถูกท าลายง่าย สูญหายง่าย ต้องอาศัยผู้ที่มีความช านาญเฉพาะทางในการสืบค้น หลังจากที่ทั่วโลกประสบความเสียหายจากภัยคุกคามในระบบสารสนเทศ ประเทศไทยก็เริ่มตื่นตัวที่จะหามาตรการทางกฎหมายออกมาป้องกันและปราบปรามการกระทาความผิดลักษณะนี้ด้วยเช่นกัน โดยคณะรัฐมนตรีลงมติให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ (กทสช.) เป็นผู้รับผิดชอบโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ ตามข้อเสนอของ

กระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อม ในวันที่ 15 ธันวาคม พ.ศ. 2541 ต่อมาจึงมีการจัดตั้ง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ICT) เมื่อวันที่ 3 ตุลาคม พ.ศ. 2545 เพื่อรับหน้าที่วางแผน ส่งเสริม พัฒนา ดาเนินกิจการที่เกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสาร และแต่งตั้งคณะกรรมการกลั่นกรองและพิจารณาความผิดเกี่ยวกับคอมพิวเตอร์ จนกลายมาเป็นร่างพระราชบัญญัติที่เกี่ยวข้องกับการกระทาความผิดบนระบบคอมพิวเตอร์ พ.ศ. .... เพื่อส่งเสนอให้สภานิติบัญญัติแห่งชาติพิจารณา หลังจากที่ร่างพระราชบัญญัติฯฉบับนี้ได้รับการลงมติเห็นชอบให้ประกาศใช้เป็นกฎหมายในการประชุมสภานิติบัญญัติแห่งชาติครั้งที่ 24/2550 ณ วันที่ 9 พฤษภาคม พ.ศ. 2550 หลังจากนั้นประเทศไทยจึงมีพระราชบัญญัติว่าด้วยการกระทาผิดเกี่ยวกับคอมพิวเตอร์เป็นครั้งแรกในปี พ.ศ. 2550 ซึ่งประกาศลงราชกิจจานุเบกษาเล่มที่ 124 ตอน 27ก ในวันที่ 18 มิถุนายน พ.ศ. 2550 และมีผลบังคับใช้ตั้งแต่ วันที่ 18 กรกฎาคม พ.ศ. 2550 เป็นต้นมา

หลังจากที่พระราชบัญญัติฯฉบับนี้ประกาศใช้ได้ไม่นาน ก็เกิดเสียงวิพากษ์วิจารณ์เกี่ยวกับการบังคับใช้ในหลายแง่มุม ไม่ว่าจะเป็นด้านการให้อานาจแก่พนักงานเจ้าหน้าที่มากเกินไป หรือบทบัญญัติบางประการที่ยังคลุมเครือ เช่น การตีความคาว่า “ข้อมูลอันไม่เหมาะสม” ซึ่งมีผลกระทบต่อสิทธิเสรีภาพในการแสดงความคิดเห็นของประชาชน คดีตัวอย่างในการสะท้อนความไม่พอใจกับการบังคับใช้พระราชบัญญัติฯนี้ คือ คดีเว็บไซต์ของกระทรวง ICT โดนแฮกเกอร์โจมตี เปลี่ยนหน้าเว็บไซต์ของกระทรวงให้กลายเป็นรูปภาพของอดีตนายกรัฐมนตรี พ.ต.ท. ทักษิณ ชินวัตร แทน[1] และหลังจากนั้นเว็บไซต์ของหน่วยงานรัฐบาลอีกหลายแห่งก็โดนแฮกเกอร์โจมตีอย่างต่อเนื่องเรื่อยมา

เนื่องจากในระยะแรกยังไม่ได้มีการกาหนดผู้รับผิดชอบหลักในการดาเนินคดี ทาให้ไม่มีการประสานงานระหว่างหน่วยงาน กระบวนการในการดาเนินคดีเองก็ไม่มีความชัดเจน พนักงานเจ้าหน้าที่ที่มีความเชี่ยวชาญเฉพาะด้านมักจะโดนเรียกตัวมาช่วยท าคดีเพียงครั้งคราว ท ให้การสืบหาหลักฐาน ไม่เกิดความต่อเนื่อง จากปัญหาดังกล่าวทาให้ภาครัฐพยายามพิจารณาปรับปรุงตัวบทให้สอดคล้องกับสถานการณ์ ทันต่อวิวัฒนาการทางเทคโนโลยี และความซับซ้อนด้านเทคนิคในการกระท าความผิด จนเมื่อวันที่ 16 ธันวาคม พ.ศ. 2559 ที่ผ่านมา ร่างพระราชบัญญัติว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับใหม่ ได้ผ่านการเห็นชอบจากสภานิติบัญญัติแห่งชาติ และประกาศลงราชกิจจานุเบกษา ในชื่อ “พระราชบัญญัติ ว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560” โดยมีผลบังคับใช้ตั้งแต่วันที่ 31 พฤษภาคม พ.ศ. 2560 เป็นต้นมา

3.1.1 วัตถุประสงค์ของพระราชบัญญัติว่าด้วยการกระท ิดเกี่ยวกับคอมพิวเตอร์

เนื่องจากปัญหาภัยคุกคามในระบบสารสนเทศที่เกิดจาก ไวรัส การแฮกข้อมูล การส่งอีเมล หรือการเผยแพร่รูปภาพ ข้อความที่มีลักษณะไม่เหมาะสมซึ่งขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีในสังคม จนส่งผลเสียต่อความมั่นคงทางเศรษฐกิจ สังคม และการเมืองการปกครองของ

[1] สายสืบภาคประชาชน. บ่วน ! เว็บไอซีที “แฮ็กเกอร์” ลุ้นคุก 15 ปี - ปรับ 3 แสน !? [ออนไลน์]. แหล่งที่มา: http://oknation.nationtv.tv/blog/Anti-Corruption/2007/07/20/entry-1 [1 มีนาคม, 2018]

ประเทศ ภาครัฐจึงจาเป็นต้องใช้กรอบกฎหมายในการกาหนดฐานความผิดและบทลงโทษส หรับการกระท าความผิดทางคอมพิวเตอร์ในรูปแบบใหม่ที่กฎหมายปัจจุบันยังไม่สามารถรองรับหรือครอบคลุมถึง เพื่อให้สามารถคุ้มครองสิทธิของประชาชนผู้บริสุทธิ์ และเป็นการกาหนดบทบัญญัติเกี่ยวกับอานาจหน้าที่ของพนักงานเจ้าหน้าที่ที่มีความรู้ความชานาญพิเศษทางด้านคอมพิวเตอร์อย่างชัดเจน อีกทั้งยังเป็นการกาหนดหน้าที่ของผู้ให้บริการไม่ว่าจะแก่ตนเองหรือแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต

3.2 การก หนดความผิดและบทลงโทษของความผิดแต่ละประเภทของผู้ใช้งานคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทาความผิดทางคอมพิวเตอร์ พ.ศ. 2550 กาหนดเกี่ยวกับความผิดและบทลงโทษของความผิดแต่ละประเภทของผู้ใช้งานคอมพิวเตอร์ไว้ดังต่อไปนี้

1) การเข้าถึง (access) ระบบคอมพิวเตอร์ (system) หรือข้อมูลคอมพิวเตอร์ (information resources) โดยมิชอบ ได้แก่ การกาหนดโทษให้บุคคลที่ลักลอบแฮกเข้าคอมพิวเตอร์หรือเข้าระบบของผู้อื่นโดยไม่ได้รับอนุญาต (Unauthorized Access) เพื่อขโมยข้อมูลที่อยู่ในเครื่องหรือในระบบนั้นๆไปใช้เพื่อประโยชน์ในทางที่ทาให้เจ้าของข้อมูลได้รับความเสียหาย หรือทาประโยชน์อื่นใดที่เจ้าของข้อมูลไม่เห็นชอบ โดยมีมาตราที่เกี่ยวข้องกับฐานความผิดนี้ คือ

“***มาตรา 5*** *ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สาหรับตน ต้องระวางโทษจาคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจ าทั้งปรับ*”

“***มาตรา 7*** *ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ซึ่งมีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สาหรับตน ต้องระวางโทษจาคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้ง จ าทั้งปรับ*”

อย่างไรก็ตาม การกระทาในฐานความผิดนี้จะต้องมีองค์ประกอบทางความผิดครบจึงจะเอาผิดได้ ซึ่งก็หมายความว่าระบบหรือคอมพิวเตอร์นั้นๆจะต้องมีการกาหนดมาตรการป้องกันการเข้าถึง อาทิเช่น รหัสผ่าน (password) การสแกนลายนิ้วมือ (fingerprint authentication) หรือมีการเข้ารหัสข้อมูล (encryption) เอาไว้ เพื่อป้องกันมิให้บุคคลภายนอกเข้าถึงได้โดยง่ายเพื่อแสดงเจตนาของเจ้าของข้อมูลว่าข้อมูลนั้นๆเป็นสิ่งสาคัญที่ตนไม่ต้องการให้ตกไปอยู่ในมือของผู้อื่นจริงๆ มิเช่นนั้นจะไม่สามารถเอาผิดตามมาตราดังกล่าวได้ โดยผู้เสียหายอาจต้องใช้กฎหมายอื่น อย่างเช่น ประมวลกฎหมายแพ่งและพาณิชย์ในเรื่องละเมิดเพื่อด าเนินคดีฟ้องร้องแทน

2) การเปิดเผยมาตรการป้องกันการเข้าถึง ได้แก่ การก หนดโทษให้บุคคลที่นารหัสซึ่งตนล่วงรู้ไปเปิดเผยแก่ผู้อื่นโดยที่เจ้าของระบบหรือเจ้าของคอมพิวเตอร์นั้นๆไม่ได้ให้อนุญาต ซึ่งอาจท าให้เข้ามูลนั้นๆรั่วไหลออกไปได้ ให้ถือเป็นการกระท าที่ความผิดตามมาตราดังต่อไปนี้

"***มาตรา 6*** *ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทาขึ้นเป็นการเฉพาะ ถ้า น ามาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษ จ าคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจ าทั้งปรับ*"

3) การดักข้อมูลคอมพิวเตอร์โดยมิชอบ ได้แก่ การกาหนดโทษให้บุคคลที่ทาการดักรับข้อมูลทางคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ไม่ว่าจะการดักข้อมูลที่อยู่ระหว่างการส่งผ่าน (sniffer) หรือเป็นการใช้ไฟล์ Keylogger เพื่อเก็บ History ของแป้นพิมพ์สาหรับนาไปแฮก ID และ Password ของผู้ใช้งาน หรือการทา CSRF (Cross-site Request Forgery) เพื่อดัก Login Cookies ในเว็บบราวเซอร์ แล้วจัดเก็บข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานนั้น โดยการกระทาเหล่านี้จะให้ถือเป็นความผิดตามมาตราดังต่อไปนี้

"***มาตรา 8*** *ผู้ใดกระทาด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่ง ข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มี ไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจาคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจ าทั้งปรับ*"

4) การรบกวนระบบคอมพิวเตอร์ (system) หรือข้อมูลคอมพิวเตอร์ (information resources) โดยมิชอบ ได้แก่ การกาหนดโทษให้บุคคลที่ลักลอบเข้าไปแก้ไข เปลี่ยนแปลง ทาลายข้อมูลของผู้อื่น อาทิ รหัสผ่าน ไฟล์ข้อมูล ภาพถ่าย โปรแกรม ฯลฯ โดยที่ไม่ได้รับอนุญาตจากเจ้าของข้อมูลนั้น รวมถึงการก่อกวนการทางานของระบบหรือคอมพิวเตอร์จนทาให้เกิดปัญหาในการใช้งานตามปกติ เช่น DDos (Distributed Denial-of-Service) ซึ่งมีมาตราที่เกี่ยวข้องกับฐานความผิดนี้ คือ

"***มาตรา 9*** *ผู้ใดทาให้เสียหาย ท าลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ไม่ว่าทั้งหมดหรือบางส่วนซึ่ง ข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางจาคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจ าทั้งปรับ*"

"***มาตรา 10*** *ผู้ใดกระทาด้วยประการใดโดยมิชอบเพื่อให้การทางานของระบบคอมพิวเตอร์ของผู้อื่น ถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทางานตามปกติได้ ต้องระวางโทษจาคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจ าทั้งปรับ*"

5) สแปมเมล (spam Mail) ได้แก่ การกาหนดโทษให้แก่บุคคลที่ส่งอีเมลโดยปกปิดที่อยู่รวมถึงชื่อของผู้ส่ง ให้ถือเป็นการกระท าที่ความผิดตามมาตราดังต่อไปนี้

"***มาตรา 11*** *ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ แก่บุคคลอื่นโดยปกปิด หรือปลอม แปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น โดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท*"

6) การกระทาซึ่งก่อให้เกิดผลกระทบต่อความความสงบเรียบร้อยและความมั่นคงของชาติ ได้แก่ การกาหนดโทษเพิ่มเติมจากฐานความผิดเดิมตามมาตราที่ 9 และมาตราที่ 10 ใน

กรณีที่ความผิดนั้น น มาซึ่งผลกระทบระดับมหาชนหรือส่งผลต่อความมั่นคงของชาติ เพื่อให้โทษนั้นมีความสอดคล้องกับระดับความเสียหายที่เกิดขึ้น โดยมีมาตราที่เกี่ยวข้องกับฐานความผิดนี้ คือ

"***มาตรา 12*** *ถ้าการกระท าความผิดตามมาตรา 9 หรือ มาตรา 10*

(1) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจาคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(2) เป็นการกระทาโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทาต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจาคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทาความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจาคุก ตั้งแต่สิบปีถึงยี่สิบปี"

7) การจาหน่ายอุปกรณ์หรือเผยแพร่ชุดคาสั่งเพื่อใช้กระทาความผิด ได้แก่ การกาหนดโทษให้แก่บุคคลที่มีส่วนในการสนับสนุนให้เกิดการกระทาความผิดทางคอมพิวเตอร์ โดยการจาหน่ายจ่ายแจกฮาร์ดแวร์ (Hardware) หรือซอฟต์แวร์ (Software) ที่สามารถนาไปใช้เพื่อกระทาความผิดหรือเป็นส่วนช่วยอานวยความสะดวกให้เกิดการกระทาผิด เช่น Trojan, Horse, Bombs, Rabbit, Sniffer ฯลฯ ให้ถือเป็นการกระท าที่มีความผิดตามมาตราดังต่อไปนี้

"***มาตรา 13*** *ผู้ใดจาหน่ายหรือเผยแพร่ชุดคาสั่งที่จัดทาขึ้นโดยเฉพาะเพื่อนาไปใช้เป็นเครื่องมือในการกระทาความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือ มาตรา 11 ต้องระวางโทษจ าคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจ าทั้งปรับ*"

8) การนาเข้า ปลอมแปลง เผยแพร่เนื้อหาอันไม่เหมาะสม ได้แก่ การกาหนดโทษให้บุคคลที่สร้างหรือเผยแพร่ข้อมูลที่มีเนื้อหาในเชิงลามกอนาจาร ปลุกปั่นให้เกิดความตื่นตระหนก ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร ข้อมูลที่หมิ่นประมาทหรือแสดงความอาฆาตมาดร้ายต่อสถาบันพระมหากษัตริย์ ข้อมูลเท็จที่ก่อให้เกิดความเสียหายกับบุคคลอื่น โดยส่งต่อออกไปในวงกว้างหรือเป็นการกระจายข้อมูลสู่สาธารณะ ต้องมีโทษทั้งทางแพ่งและอาญาตามมาตราดังต่อไปนี้

"***มาตรา 14*** *ผู้ใดกระทาความผิดที่ระบุไว้ ดังต่อไปนี้ ต้องระวางโทษจาคุกไม่เกินห้าปี หรือ หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจ าทั้งปรับ*

(1) นาเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นาเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดย โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นาเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นาเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)"

ดังนั้น การเผยแพร่ข้อมูลปลอมหรือข้อมูลเท็จบนเครือข่ายสังคมออนไลน์ (Social media) หรือการส่งต่ออีเมล (Forward) ที่มีข้อมูลอันเป็นความผิดดังกล่าว โดยไม่ได้มีการศึกษาตรึกตรองให้ดีเสียก่อนว่าข้อมูลนั้นๆเป็นความจริง หรือเป็นข้อมูลที่มีเนื้อหาเหมาะสมหรือไม่ ก็อาจท ให้มีความผิดตามมาตรา 14 นี้ได้เช่นกัน

9) การเผยแพร่ภาพที่ถูกสร้างขึ้นโดยการตัดต่อ-ดัดแปลงโดยมิชอบ ได้แก่ การกาหนดโทษให้บุคคลที่ทาการตัดต่อ หรือเผยแพร่ภาพที่ถูกตัดต่อ-ดัดแปลงนั้น ไปยังระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้จนทาให้ผู้นั้นได้รับความเสียหาย ถูกดูหมิ่น ถูกเกลียดชัง เสื่อมเสียชื่อเสียง ไม่ว่าจะเป็นเพียงแค่การกลั่นแกล้งให้อับอาย การหมิ่นประมาท หรือการตัดต่อเพื่อน าภาพไปใช้เชิงพาณิชย์โดยที่บุคคลในภาพไม่ยินยอม จะต้องได้รับโทษตามมาตราดังต่อไปนี้

"***มาตรา 16*** *ผู้ใดนาเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดทั้งนี้โดยประการที่น่าจะทาให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่นถูกเกลียดชังหรือได้รับความอับอายต้องระวางโทษจ าคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาทหรือทั้งจ าทั้งปรับ"*

3.3 การก หนดอ นาจหน้าที่ของพนักงานเจ้าหน้าที่

มาตรา 28 ก หนดให้รัฐมนตรีมีอานาจในการแต่งตั้งผู้ที่มีความรู้ ความช นาญเกี่ยวกับระบบคอมพิวเตอร์ โดยมีกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เป็นหน่วยงานในการกากับดูแล และจัดตั้งหน่วยงาน "สานักกากับการใช้เทคโนโลยีสารสนเทศ" ขึ้นเพื่อเตรียมความพร้อมทั้งด้านทรัพยากรณ์บุคคลและด้านอุปกรณ์ต่างๆในการปฏิบัติงานสืบสวนสอบสวนอาชญากรรมทางคอมพิวเตอร์ โดยมีมาตรา 18 เป็นตัวกาหนดอานาจของพนักงานเจ้าหน้าที่ โดยแบ่งขอบเขตอานาจในการด าเนินการได้ดังต่อไปนี้

3.3.1 อ นาจที่ด ินการได้เลยโดยไม่ต้องขออ นาจศาล (มาตรา 18) ได้แก่

1) การออกจดหมายเพื่อสอบถามหรือให้เรียกบุคคลที่เกี่ยวข้องกับการกระทาความผิด ส่งค าชี้แจงเป็นหนังสือ เอกสาร หรือข้อมูลหลักฐานในรูปแบบต่างๆที่ต้องการ

2) การขอเรียกดูข้อมูลจราจรทางคอมพิวเตอร์ (Log File) จาก ISPs หรือจากบุคคลที่เกี่ยวข้องเพื่อน ามาพิจารณาคดี

3) สั่งให้ ISPs ส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการตามมาตรา 26 ที่อยู่ในความครอบครอง ให้แก่พนักงานเจ้าหน้าที่

3.3.2 อานาจที่ต้องขออานาจจากศาล (มาตรา 19) โดยจะต้องส่งสาเนารายละเอียดในการด าเนินการตามอานาจหน้าที่ที่ได้รับมอบหมายภายใน 48 ชั่วโมงนับตั้งแต่เริ่มลงมือด าเนินการ

1) สั่งทาสาเนาข้อมูลคอมพิวเตอร์ หรือข้อมูลการจราจรทางคอมพิวเตอร์ (Log File) จากระบบคอมพิวเตอร์ที่ต้องสงสัย โดยจะต้องไม่เป็นอุปสรรคในการดาเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลนั้นเกินความจ าเป็น

2) สั่งให้บุคคลที่ครอบครองข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการเก็บข้อมูลคอมพิวเตอร์ ส่งมอบของดังกล่าวให้แก่พนักงานเจ้าหน้าที่

3) เข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ (Log File) หรืออุปกรณ์คอมพิวเตอร์ ที่เป็นหลักฐานเกี่ยวโยงกับการกระทาความผิด โดยจุดประสงค์เพื่อสืบสวนหาตัวผู้กระท าผิด

4) ถอดรหัสเพื่อเข้าถึงข้อมูล หรือสั่งให้บุคคลที่เกี่ยวข้องให้ความร่วมมือหรือท าการถอดรหัสให้

5) ยึดอายัดระบบคอมพิวเตอร์เท่าที่จาเป็นเพื่อประโยชน์ในการสืบสวนสอบสวนหาตัวผู้กระทาผิดได้เป็นเวลา 30 วัน หากจาเป็นต้องยึดอายัดไว้นานกว่านั้น จะต้องยื่นคาร้องต่อศาลเพื่อขอขยายเวลาการยึดอายัดอีกกี่ครั้งก็ได้ แต่รวมแล้วจะต้องไม่มีการขยายเวลาเกิน 60 วัน

6) ระงับ หรือสั่งระงับการเผยแพร่ข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการก่อการร้าย ซึ่งก่อให้เกิดผลกระทบต่อความมั่นคงแห่งราชอาณาจักร หรือขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน

7) สั่งห้ามจาหน่าย ห้ามเผยแพร่ ระงับการใช้งาน ทาลาย แก้ไข กาหนดเงื่อนไขการใช้งานชุดค าสั่งที่มีลักษณะไม่พึงประสงค์

3.3.3 หน้าที่และความรับผิดชอบในการรักษาข้อมูลให้เป็นความลับของพนักงานเจ้าหน้าที่ โดยหากกระทาโดยประมาทจนท าให้ผู้อื่นล่วงรู้ข้อมูลนั้นๆ จะต้องระวางโทษจาคุกตามมาตรา 23 โดยผู้ที่ล่วงรู้ข้อมูลความลับนั้น ก็มีโทษตามมาตรา 24 ด้วยเช่นกัน

3.3.4 หน้าที่ในการใช้ข้อมูล (มาตรา 25) โดยน ข้อมูลที่สืบค้นได้ตามพระราชบัญญัติฉบับนี้มาใช้เพื่ออ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความ

อาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยาน ซึ่งจะต้องเป็นหลักฐานที่ไม่ได้เกิดขึ้นจากการจูงใจ การให้ค ามั่นสัญญา การขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

3.3.5 หน้าที่เพื่อการดาเนินคดีโดยทั่วไป (มาตรา 29) ได้แก่ รับคาร้องทุกข์กล่าวโทษ สืบสวน จับกุม ควบคุม ค้นหาหลักฐาน และประสานงานกับเจ้าหน้าที่ฝ่ายต่างๆที่เกี่ยวข้องเพื่อก าหนดระเบียบแนวทาง และวิธีปฏิบัติในการด าเนินคดี

3.4 ก หนดหน้าที่ของผู้ให้บริการ

มาตรา 26 กาหนดให้ผู้ให้บริการมีหน้าที่ต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวข้องไว้ไม่น้อยกว่า 90 วัน นับตั้งแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ และมีหน้าที่ต้องเก็บข้อมูลของผู้ใช้บริการที่สามารถระบุตัวตนของผู้ใช้ได้เท่าที่จ าเป็น นับตั้งแต่เริ่มใช้บริการจนถึง 90 วันหลังจากที่หยุดใช้บริการ เพื่อให้สามารถนามาใช้เป็นหลักฐานส าคัญต่อการน าผู้กระท าความผิดมาลงโทษ โดยผู้ให้บริการตามพระราชบัญญัติฯฉบับนี้ หมายถึง

3.4.1 ผู้ให้บริการ หมายถึง ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น โดยศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่โจ้ ได้จ าแนกประเภทของผู้ให้บริการออกมาดังนี้[2]

1) ผู้ประกอบกิจการโทรคมนาคม (Telecommunication Carrier) ได้แก่ ผู้ให้บริการ เครือข่ายโทรศัพท์มือถือ ผู้ให้บริการวงจรสื่อสาร ผู้ให้บริการดาวเทียม

2) ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) รวมถึง ผู้ให้บริการอินเทอร์เน็ต (ISPs) ผู้ประกอบการที่ให้บริการในห้องพัก ห้องเช่า โรงแรม ร้านอาหาร องค์กรธุรกิจ หน่วยงานภาครัฐ สถาบันการศึกษา ฯลฯ ที่มีบริการอินเทอร์เน็ต

3) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ เช่น ผู้ให้บริการเช่า Web hosting เว็บเซิร์ฟเวอร์ ศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต (Host Service Provider)

4) ผู้ให้บริการร้านอินเทอร์เน็ต อินเทอร์เน็ตคาเฟ่ และร้านเกมออนไลน์

3.4.2 ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์ เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอปพลิเคชันต่างๆ (Content Service Provider) เกี่ยวกับธุรกรรมทางธนาคารอิเล็กทรอนิกส์ (Internet Banking) การชาระเงินผ่านระบบอิเล็กทรอนิกส์ (e-payment) การพาณิชย์อิเล็กทรอนิกส์ (e-commerce) หรือผู้ให้บริการเว็บบอร์ด Blog ต่างๆ

---

[2] Information Technology Center : Maejo University. บทที่ 10 ความปลอดภัยในการท างานระบบเครือข่าย, 10.6 สรุปรายละเอียด พรบ. ที่เกี่ยวข้องกับผู้ให้บริการ [ออนไลน์]. แหล่งที่มา: http://csmju.jowave.com/cs100_v2/lesson10-5.html [12 มีนาคม 2561]

โดยข้อมูลจราจรทางคอมพิวเตอร์ที่จ าเป็นต้องเก็บ คือข้อมูลจราจรที่สามารถระบุตัวผู้ใช้บริการเป็นรายบุคคลได้ อาทิเช่น ชื่อ-นามสกุล หมายเลขบัตรประชาชน IP Address วันเวลาที่ใช้งาน เป็นต้น แต่จะต้องเป็นข้อมูลเฉพาะในส่วนที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น และหากผู้ให้บริการมีเจตนายินยอมหรือสนับสนุนให้เกิดการกระทาความผิด จะต้องระวางโทษเช่นเดียวกับผู้กระท าความผิดตามมาตรา 14 เพื่อให้ผู้ให้บริการ อาทิ เจ้าของเว็บไซต์มีหน้าที่ต้องคอยตรวจสอบและพิจารณาเนื้อหาที่อยู่ในระบบของตนว่าไม่เหมาะสมหรือไม่ (มาตรา 26)

3.5 สาระสาคัญของพระราชบัญญัติว่าด้วยการกระทาความผิดทางคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

พระราชบัญญัติว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 (“พระราชบัญญัติ ปี2560”) มีโครงสร้างส่วนใหญ่เหมือนกับพระราชบัญญัติฯ ปี2550 เพียงแต่มีการปรับปรุงตัวบทและเพิ่มเติมเนื้อหาในบางส่วน เพื่อให้เกิดความชัดเจนในการบังคับใช้ โดยสามารถสรุปความแตกต่างได้ตามตารางดังต่อไปนี้

ตารางที่ 1 เปรียบเทียบความแตกต่างของพระราชบัญญัติฯปี 2550 กับปี 2560

หัวข้อ	พระราชบัญญัติฯ ปี 2550	พระราชบัญญัติฯ ปี2560
กระทรวงที่ก ากับดูแล	**มาตรา 4** ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอ านาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้	**มาตรา 3** ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอ านาจแต่งตั้งพนักงานเจ้าหน้าที่กับออกกฎกระทรวงและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้
การส่งสแปมโดยปกปิดแหล่งที่มา	**มาตรา 11** การส่งสแปมโดยปลอมแปลงแหล่งที่มาของการส่ง ต้องระวางโทษปรับไม่เกิน 100,000 บาท	**มาตรา 4** เพิ่มโทษปรับเป็น 200,000 บาท ในกรณีที่ไม่เปิดช่องทางให้ผู้รับบอกเลิกได้ อีกทั้ง ยังให้รัฐมนตรีออกประกาศกาหนดลักษณะ วิธีการส่ง และปริมาณของสแปม
ความผิดที่ก่อให้ เกิดความเสียหายต่อประชาชนหรือความมั่นคงของประเทศ	**มาตรา 12** การรบกวนระบบหรือข้อมูลคอมพิวเตอร์ โดยมิชอบ จนท าให้ 1) หากเกิดความเสียหายต่อประชาชนต้องระวางโทษจ าคุกไม่เกิน 10 ปี และปรับไม่เกิน 200,000 บาท 2) หากท าให้ข้อมูลคอมพิวเตอร์	**มาตรา 5** เพิ่มเติมฐานความผิดจากมาตรา12 เดิม ได้แก่ การเข้าถึงหรือการเปิดเผยมาตรการป้องกันการเข้าถึงของระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ รวมทั้งการดักข้อมูลคอมพิวเตอร์โดยมิชอบ การส่งสแปมเมลที่ก่อให้เกิดความเสียหายต่อประชาชน หรือความมั่นคงของประเทศ ต้องระวางโทษจ าคุกตั้งแต่ 1-7 ปี และปรับตั้งแต่

	หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อสาธารณะ หรือกระทบต่อความมั่นคงของประเทศต้องระวางโทษจ าคุกไม่เกิน 3-5 ปี และปรับ 60,000-300,000 บาท แต่ถ้าท าให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจ าคุก10-20 ปี	20,000-140,000 บาท โดยหากท าให้ข้อมูลหรือระบบนั้นๆเกิดความเสียหายด้วย จะต้องระวางโทษจ าคุกตั้งแต่ 1-10ปี และปรับตั้งแต่ 20,000-200,000 บาท **มาตรา 6** เพิ่มมาตรา 12/1 ว่า หากความผิดตามมาตรา 12 เดิมเป็นเหตุให้เกิดอันตรายต่อแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่นต้องระวางโทษจ าคุกไม่เกิน 10 ปี และปรับไม่เกิน 200,000 บาท หากเป็นท าให้ผู้อื่นถึงแก่ความตายต้องระวางโทษจ าคุกตั้งแต่ 5-20 ปี และปรับตั้งแต่ 100,000-400,000 บาท
การจ าหน่ายอุปกรณ์หรือเผยแพร่ชุดค าสั่งเพื่อใช้กระท าความผิด	**มาตรา 13** ต้องระวางโทษจ าคุกไม่เกิน 1ปี หรือปรับไม่เกิน 20,000 บาท หรือทั้งจ าทั้งปรับ	**มาตรา 7** เพิ่มโทษเป็นต้องระวางโทษจ าคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000บาท หรือทั้งจ าทั้งปรับ และหากท าให้เกิดผลกระทบต่อความมั่นคงของประเทศ หรือเป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ซึ่งตนเล็งเห็นเหตุอยู่ก่อนแล้วจะต้องรับผิดทางอาญาตามความผิดที่มีก าหนดโทษสูงขึ้นด้วย
การหมิ่นประมาทออนไลน์	**มาตรา 14** (1) การน าเข้าข้อมูลเท็จไม่ว่าทั้งหมดหรือบางส่วน ที่ท าให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจ าคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจ าทั้งปรับ	**มาตรา 8** เพิ่มบทบัญญัติในมาตรา14 (1)เดิมได้แก่ การน าเข้าข้อมูลเท็จไม่ว่าทั้งหมดหรือบางส่วน ที่ท าให้เกิดความเสียหายแก่ผู้อื่น อันมิใช่การกระท าความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา ต้องระวางโทษจ าคุกไม่เกิน 5 ปี หรือปรับไม่เกิน100,000 บาท หรือทั้งจ าทั้งปรับ
การน าเข้าข้อมูลเท็จที่มีผลต่อความมั่นคงของประเทศ	**มาตรา 14 (2)** การน าเข้าข้อมูลเท็จที่น่าจะก่อให้เกิด - ความเสียหายต่อความมั่นคงของประเทศ - ความตื่นตระหนกแก่ประชาชน	**มาตรา 8** เพิ่มนิยามของมาตรา14 (2) การน าเข้าข้อมูลเท็จที่น่าจะก่อให้เกิด - ความเสียหายต่อความมั่นคงปลอดภัยของประเทศ - ความปลอดภัยสาธารณะ - ความมั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ - ความตื่นตระหนกแก่ประชาชน

การเผยแพร่ข้อมูลเท็จที่ส่งผลกระทบต่อบุคคล	**มาตรา 14 (5)** การเผยแพร่หรือส่งต่อข้อมูลเท็จตาม (1) (2) (3) ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ	**มาตรา 8 วรรคสอง** เพิ่มบทบัญญัติจากมาตรา 14 (5) เดิม ว่า หากการกระทำความผิดตามมาตรา 14 (1) เป็นการกระทำผิดแค่ต่อบุคคลใดบุคคลหนึ่งโดยเฉพาะ ผู้กระทำผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลดังกล่าว จะต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้
ขอบเขตการรับโทษของผู้ให้บริการ	**มาตรา 15** ให้ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา14	**มาตรา 9** เพิ่มบทบัญญัติในมาตรา15 เดิม ว่า ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการแพร่ข้อมูล และการนำข้อมูลนั้นออกจากระบบคอมพิวเตอร์ เว้นแต่ผู้ให้บริการจะพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสองแล้วจึงจะไม่ต้องรับโทษ
การเผยแพร่ภาพที่ถูกสร้างขึ้นโดยการตัดต่อ/ดัดแปลง โดยมิชอบ	**มาตรา 16** การเผยแพร่ภาพตัดต่อจนทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ	**มาตรา 10** เพิ่มโทษจากมาตรา16เดิม เป็น ระวางโทษจำคุกไม่เกิน 3ปี หรือปรับไม่เกิน 200,000 บาท และเพิ่มความครอบคลุมไปถึงภาพผู้เสียชีวิตที่ทำให้เกิดผลกระทบต่อญาติที่ยังมีชีวิตด้วย โดยญาติติดตัวของผู้ตายสามารถร้องทุกข์แทนได้
การสั่งให้ทำลายภาพตัดต่อ	ไม่มีบทบัญญัติ	**มาตรา 11** เพิ่มมาตรา 16/1 ได้แก่ หากพิพากษาแล้วว่าจำเลยมีความผิดจริง สามารถสั่งให้ - จำเลยทำลายข้อมูลภาพดังกล่าว - เผยแพร่คำพิพากษานั้นไปยังสื่อต่างๆ โดยให้จำเลยเป็นผู้ออกค่าใช้จ่าย - ศาลพิจารณาการดำเนินการอื่นๆเพื่อบรรเทาความเสียหาย เพิ่มมาตรา 16/2 ให้ผู้อื่นที่มีข้อมูลนั้นๆในครอบครอง ทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษในมาตรา14 หรือมาตรา 16 แล้วแต่กรณี
การรับโทษ	**มาตรา 17** ต้องรับโทษในประเทศไทยแม้ว่าจะกระทำความผิดจะเกิดนอกประเทศไทย ถ้า (1) ผู้กระทำผิดเป็นคนไทย และรัฐบาลของประเทศที่เกิดความผิด	**มาตรา 12** ให้เพิ่มมาตรา 17/1 เพื่อให้รัฐมนตรีสามารถแต่งตั้งคณะกรรมการเปรียบเทียบ โดยแต่ละคณะจะต้องมีกรรมการจำนวน 9 คน และสามในเก้าจะต้องมาจากผู้แทนภาคเอกชนที่เกี่ยวข้อง ดังนั้นจึง

	ร้องขอให้ลงโทษ (2) ผู้กระท าผิดเป็นคนต่างด้าว แต่รัฐบาลไทยหรือคนไทยเป็นผู้เสียหาย	สามารถแบ่งคณะกรรมการออกเป็นสองชุด - คณะกรรมการที่ท าหน้าที่ปรียบเทียบปรับส าหรับความผิดที่มีแต่โทษปรับหรือโทษจ าคุกไม่เกิน 2 ปี - คณะกรรมการกลั่นกรองข้อมูลที่ไม่ผิดกฎหมายแต่สั่งระงับได้
อ านาจเจ้าหน้าที่	**มาตรา 18** เจ้าหน้าที่มีอ านาจ -ออกจดหมายเพื่อสอบถามหรือให้เรียกบุคคลที่เกี่ยวข้องกับการกระท าความผิดส่งค าชี้แจง - การเรียกดูLog File จาก ผู้ให้บริการหรือบุคคลที่เกี่ยวข้อง - สั่งให้ส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่อยู่ในความครอบครอง - ขออนุญาตศาลเพื่อสั่งท าสเนาข้อมูลคอมพิวเตอร์ Log file จากระบบคอมพิวเตอร์ที่ต้องสงสัย - ขออนุญาตศาลเพื่อสั่งให้ส่งมอบอุปกรณ์เก็บข้อมูล หรือข้อมูลคอมพิวเตอร์ - ขออนุญาตศาลเพื่อเข้าถึงข้อมูล - ขออนุญาตศาลเพื่อถอดรหัสข้อมูล - ขออนุญาตศาลเพื่ออายัดระบบที่ต้องสงสัย	**มาตรา 13** เพิ่มวรรคสองของมาตรา18 ว่า ให้พนักงานสืบสวนตามกฎหมายอื่น สามารถร้องขอให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ด าเนินการตามวรรคหนึ่ง เพื่อเป็นประโยชน์ต่อการสืบคดี โดยพนักงานเจ้าหน้าที่จะต้องด าเนินการภายใน 7วัน หรือไม่เกิน 15 วัน ตามแต่เหตุสมควร
เนื้อหาที่ถูกจ ากัดการเผยแพร่	**มาตรา 20** พนักงานเจ้าหน้าที่สามารถขอความเห็นชอบจากรัฐมนตรีเพื่อระงับการเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีเนื้อหาขัดต่อความสงบเรียบร้อยตามประมวลกฎหมายอาญาในภาคสอง ลักษณะ 1 หรือลักษณะ 1/1	**มาตรา 14** ขยายความมาตรา 20 เดิม โดยเพิ่มประเภทข้อมูลที่สามารถสั่งระงับหรือลบท าลายดังต่อไปนี้ - ข้อมูลที่เป็นความผิดตามพระราชบัญญัติฯ ฉบับนี้ - ข้อมูลที่มีเนื้อหาขัดต่อความสงบเรียบร้อยตามประมวลกฎหมายอาญาในภาคสอง ลักษณะ1 หรือลักษณะ 1/1 - ข้อมูลที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญาหรือกฎหมายอื่นซึ่งข้อมูลที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และเจ้าหน้าที่ตามกฎหมายนั้นหรือพนักงานสอบสวนตาม

		ประมวลกฎหมายวิธีพิจารณาความอาญาได้ ร้องขอ
ชุดค าสั่งไม่พึงประสงค์	**มาตรา 21** พนักงานเจ้าหน้าที่สามารถยื่นค าร้องต่อศาลเพื่อให้มีค าสั่งห้ามจ าหน่าย เผยแพร่ หรือสั่งระงับ แก้ไข ก าหนดเงื่อนไขการใช้ข้อมูลคอมพิวเตอร์ที่มีชุดคาสั่งไม่พึงประสงค์นั้นรวมอยู่ ชุดค าสั่งไม่พึงประสงค์ หมายถึง ชุดค าสั่งที่มีผลท าให้ข้อมูล หรือระบบคอมพิวเตอร์หรือชุดค าสั่งอื่นเกิดความเสียหาย ถูกท าลายถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามค าสั่งที่ก าหนดไว้ หรือโดยประการอื่นตามที่ก าหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดค าสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดค าสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา	**มาตรา 15** เปลี่ยนแปลงความหมายของชุดค าสั่งไม่พึงประสงค์ ดังนี้ “ชุดค าสั่งไม่พึงประสงค์หมายถึงชุดค าสั่งที่มีผลท าให้ข้อมูลหรือระบบคอมพิวเตอร์หรือชุดค าสั่งอื่นเกิดความเสียหาย ถูกท าลายถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามค าสั่งหรือโดยประการอื่นตามที่ก าหนดในกฎกระทรวง เว้นแต่เป็นชุดค าสั่งไม่พึงประสงค์ที่อาจน ามาใช้เพื่อป้องกันหรือแก้ไขชุดค าสั่งดังกล่าวข้างต้น <u>ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษา ก าหนดรายชื่อ ลักษณะ หรือรายละเอียดของชุดค าสั่งไม่พึงประสงค์ ซึ่งอาจน ามาใช้เพื่อป้องกันหรือแก้ไขชุดค าสั่งไม่พึงประสงค์ก็ได้</u>”
หน้าที่ในการรักษาข้อมูลที่ได้มาให้เป็นความลับ	**มาตรา 23** พนักงานเจ้าหน้าที่ที่ประมาทจนท าให้ข้อมูลที่ได้มาตามมาตร18 รั่วไหล ต้องระวางโทษจ าคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000บาท หรือทั้งจ าทั้งปรับ **มาตรา 24** ผู้ใดที่น าข้อมูลที่ล่วงรู้จากเจ้าหน้าที่ ไปเปิดเผยต่อผู้อื่น ต้องระวางโทษจ าคุกไม่เกิน 2 ปี หรือปรับไม่เกิน40,000บาท หรือทั้งจ าทั้งปรับ	**มาตรา 16** เพิ่มเติมให้พนักงานสอบสวนตามมาตรา18 วรรคสองมีหน้าที่ต้องรักษาความลับตามมาตรา23 และมาตรา24 เช่นเดียวกับพนักงานเจ้าหน้าที่
หน้าที่ในการรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้	**มาตรา 26** ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบ แต่หากจ าเป็นพนักงานเจ้าหน้าที่สามารถสั่งให้	**มาตรา 17** ขยายเวลาในการเก็บข้อมูลจราจรตามวรรคหนึ่งของมาตรา26 เป็น “ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า90วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบ แต่ในกรณี

ให้บริการ	เก็บไว้เกิน90วันแต่ไม่เกิน1ปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จ าเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า90วันนับตั้งแต่การใช้บริการสิ้นสุดลง	จ าเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการเก็บรักษาไว้เกิน90วันแต่ไม่เกิน 2ปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้”
พนักงานเจ้าหน้าที่และค่าตอบแทน	**มาตรา 28** การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความช านาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีก าหนด	**มาตรา 18** เพิ่มวรรคสองของมาตรา28 ดังนี้ “ผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ อาจได้รับค่าตอบแทนพิเศษ ตามที่รัฐมนตรีก าหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง ในการก าหนดให้ได้รับค่าตอบแทนพิเศษต้องค านึงถึงภาระหน้าที่ ความรู้ความเชี่ยวชาญ ความขาดแคลนในการหาผู้มาปฏิบัติหน้าที่หรือคุณภาพของงาน และการด ารงตนอยู่ในความยุติธรรมโดยเปรียบเทียบค่าตอบแทนของผู้ปฏิบัติงานอื่นในกระบวนการยุติธรรมด้วย
วิธีการเบิกค่าใช้จ่าย	ไม่ระบุ	**มาตรา 19** เพิ่มมาตรา31 ค่าใช้จ่ายในเรื่องดังต่อไปนี้ รวมทั้งวิธีการเบิกจ่ายให้เป็นไปตามระเบียบที่รัฐมนตรีก าหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง - การสืบสวน การหาข้อมูล และรวบรวมพยานหลักฐานในคดีความผิดตามพระราชบัญญัตินี้ - การด าเนินการตามมาตรา18 วรรคหนึ่ง (4) (5) (6) (7) และ (7) และมาตรา20 - การด าเนินการอื่นใดอันจ าเป็นแก่การป้องกันและปราบปรามการกระท าความผิดตามพระราชบัญญัตินี้

3.6 สรุปสาระสาคัญของพระราชบัญญัติว่าด้วยการกระท าความผิดทางคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

พระราชบัญญัติฯนี้ถูกปรับปรุงเพื่อให้สอดคล้องกับสถานการณ์และความซับซ้อนด้านเทคโนโลยีที่ใช้กระทาความผิดในปัจจุบัน รวมทั้งแก้ไขปัญหาในการใช้พระราชบัญญัติฯผิดจุดประสงค์เพื่อให้สามารถบรรเทาความเสียหายที่เกิดขึ้นได้อย่างรวดเร็วมากขึ้น สาระสาคัญประเด็นหลักๆที่อยู่ในพระราชบัญญัติฯ สามารถสรุปใจความได้ดังต่อไปนี้

3.6.1 ขอบเขตในการส่งสแปมเมล (spam mail)

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ออกประกาศเรื่อง เรื่อง ลักษณะ และวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่ และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนราคาญแก่ผู้รับ เพื่อขยายความของมาตรา 11 ให้มีความชัดเจนมากขึ้น โดยมุ่งที่จะดูแลสิทธิความเป็นอยู่ส่วนบุคคล (Rights of Privacy) จากการเพิ่มเติมกฎเกณฑ์ให้ ผู้ส่งต้องเปิดช่องทางให้ผู้รับบอกเลิกได้โดยง่าย และให้รัฐมนตรีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมออกประกาศเรื่องลักษณะวิธีการส่ง ปริมาณข้อมูล ความถี่ และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนราคาญแก่ผู้รับ โดยมีเนื้อหาดังต่อไปนี้

1) ผู้ส่งข้อมูล หมายถึง บุคคลที่มีเจตนาส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์เพื่อประโยชน์ทางการค้า ซึ่งรวมไปถึงผู้ให้บริการเว็บไซต์หรือผู้ให้บริการแอปพลิเคชัน (Application) หรือผู้ให้บริการประเภทสื่อสังคมออนไลน์ (Social Media) ที่โฆษณาหรือสนับสนุนการส่งข้อมูลหรือจดหมายอิเล็กทรอนิกส์ดังกล่าว แต่ไม่รวมถึงผู้ให้บริการโทรคมนาคมที่เป็นสื่อกลาง ส าหรับการส่งผ่านข้อมูล

2) ลักษณะข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ที่ส่งได้โดยไม่ถือว่าเป็นการก่อให้เกิดความเดือดร้อน ได้แก่

1. ข้อมูลที่ใช้ติดต่อหรือเป็นหลักฐานในการเข้าทานิติกรรมสัญญา (Transaction) ที่คู่สัญญาได้เคยมีการตกลงกันไว้เรียบร้อยแล้ว เช่น ใบเสร็จยืนยันการชาระหนี้ ใบแจ้งหนี้ (invoice) ใบรับประกัน (warrantee) ใบเคลมสินค้า ข้อมูลหลักประกันตัวสินค้าหรือบริการ (security) ข้อมูลแจ้งการเปลี่ยนหรือเพิ่มเติมเงื่อนไขการซื้อขายหรือการบริการสมาชิกเดิม สัญญาจ้างแรงงาน การส่งมอบข้อมูลหรือบริการที่ผู้รับและผู้ส่งตกลงกันไว้ก่อนแล้ว (membership)

2. ข้อมูลที่ไม่ได้มีวัตถุประสงค์เพื่อแสวงหากาไรทางธุรกิจ ที่ส่งโดยองค์กรของรัฐ หรือสถาบันการศึกษา หรือหน่วยงานการกุศล

3. ข้อมูลที่ไม่มีลักษณะผิดกฎหมาย ไม่ละเมิดสิทธิส่วนบุคคล และไม่มีวัตถุประสงค์เชิงพาณิชย์

3) ลักษณะของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์เชิงพาณิชย์ที่สามารถส่งได้ เมื่อได้รับความยินยอมจากผู้รับและไม่ก่อให้เกิดความเดือดร้อนราคาญแก่ผู้รับ โดยมีเงื่อนไขดังต่อไปนี้

1. ข้อมูลที่ต้องระบุเวลาส่ง ได้แก่ วิธีการบอกเลิกหรือแจ้งความประสงค์ในการปฏิเสธเพื่อรับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์นั้น (Opt-out) ที่ทาได้โดยง่าย เช่น ต้องระบุที่อยู่อีเมล หมายเลขโทรศัทพ์ หมายเลขโทรสาร หรือที่อยู่ของไฟล์หรือเว็บไซต์บนอินเทอร์เน็ต (URL) เพื่อเข้าไปท าการยกเลิกการเป็นสมาชิก (unsubscribe)

2. ผู้ส่งต้องรีบดาเนินการเพื่อยกเลิกการส่งภายในระยะเวลา 7 วันหลังจากที่ได้รับค าสั่งยกเลิกจากผู้รับข้อมูล

3. ห้ามเรียกร้องเงินหรือค่าตอบแทนใดๆในการบอกเลิก

4. ห้ามเรียกร้องข้อมูลของผู้รับเพิ่มเติมเพื่อทาการบอกเลิก

5. ห้ามกระท าการใดๆที่มีวัตถุประสงค์เชิงพาณิชย์เพิ่มเติม เช่น การให้คลิกลิงก์เข้าไปยังเว็บไซต์เพื่อซื้อสินค้า

โดยข้อบังคับข้างต้น ให้บังคับใช้กับผู้ให้บริการเว็บไซต์ ผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการประเภทสื่อสังคมออนไลน์ที่ทาการโฆษณาหรือสนับสนุนการส่งข้อมูลหรือจดหมายอิเล็กทรอนิกส์ด้วยเช่นกัน หากละเมิดไม่ปฏิบัติตามเงื่อนไขข้างต้นให้ถือว่าผู้ส่งข้อมูลมีความผิดตามมาตรา 11 วรรคสอง ต้องระวางโทษปรับไม่เกิน 200,000 บาท

3.6.2 การดูแลและป้องกันข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์

มาตรา12 ที่เกี่ยวโยงกับการป้องกันการรบกวนหรือการสร้างความเสียหายต่อระบบและข้อมูลคอมพิวเตอร์ ถูกเพิ่มเติมให้ครอบคลุมถึงการดักข้อมูลคอมพิวเตอร์โดยมิชอบ การส่งสแปมเมลที่กระทบต่อความเสียหายของประชาชน หรือต่อความมั่นคงของรัฐ ซึ่งรวมไปถึงระบบโครงสร้างพื้นฐานที่ส าคัญของประเทศ ซึ่งอาจส่งผลกระทบต่อประชาชนในวงกว้าง อาทิเช่น ระบบการชาระเงินอิเล็กทรอนิกส์ (e-payment) ระบบพลังงาน ระบบไฟฟ้า ระบบประปา ระบบสาธารณสุข โดยได้ระบุแจกแจงโทษตามความเหมาะสมของระดับการกระทาความผิดไว้ละเอียดมากขึ้น เช่นขยายระยะเวลาในการจ าคุกจาก 3-5 ปี เป็น 1-7 ปี และขยายช่วงของอัตราโทษปรับจากเดิม 60,000-300,000 บาท เป็น 20,000-140,000 บาท เพื่อให้ศาลสามารถใช้ดุลพิจในการพิจารณาระดับผลกระทบที่เกิดขึ้นจากการกระทาความผิดนั้นได้อย่างยืดหยุ่นมากขึ้น และมีการเพิ่มโทษในการจาหน่ายอุปกรณ์หรือเผยแพร่ชุดคาสั่งเพื่อใช้กระทาความผิด (มาตรา13) ลดโทษให้การเผยแพร่ข้อมูลเท็จที่ส่งผลกระทบต่อบุคคลธรรมดาเฉพาะบุคคลไม่ได้มีผลต่อส่วนรวม (มาตรา14(5)) เป็นต้น

3.6.3 การกระท ขันเป็นความผิดฐานหมิ่นประมาท

มาตรา14(1) ระบุให้แยกความผิดฐานหมิ่นประมาทตามพระราชบัญญัติฯนี้ ออกจากการหมิ่นประมาททางอาญาตามปกติอย่างชัดเจน เนื่องจากตั้งแต่มีการบังคับใช้พระราชบัญญัติฯ ในปี 2550 เป็นต้นมา คดีที่ฟ้องร้องโดยใช้พระราชบัญญัติการกระทาผิดทางคอมพิวเตอร์มากที่สุดกลับเป็นคดีตามมาตรา 14(1) ซึ่งเป็นเรื่องเกี่ยวกับความผิดฐานหมิ่นประมาท ฉ้อโกง เป็นหลัก ซึ่งขัดกับจุดประสงค์ที่แท้จริงในการบังคับใช้กฎหมายที่ต้องการให้มาตรการนี้เป็นเครื่องมือในการป้องกันและปราบปรามการปลอมแปลงข้อมูลคอมพิวเตอร์ เช่น Phishing เท่านั้น ซึ่งอาจเป็นเพราะอัตราโทษตามมาตรา 14(1) ได้แก่ โทษจาคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท นั้นเป็นโทษที่มากกว่าความผิดฐานหมิ่นประมาทในทางอาญาที่อัตราโทษเพียงจาคุกไม่เกิน 1 ปี ปรับไม่เกิน 20,000 บาท ดังนั้นพระราชบัญญัติฯ ปี 2560 จึงเพิ่มเติมบทบัญญัติว่า “*ความผิดนั้นจะต้องไม่ใช่การกระท าตามผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา*” และเพิ่มหลักสุจริตในมาตรา14 วรรคสอง ว่าการหมิ่นประมาทที่กระทาไปโดยการติชมด้วยความสุจริต หรือการวิพากษ์วิจารณ์ที่เป็นประโยชน์สาธารณะ ถือเป็นความผิดที่ยอมความได้

3.6.4 ผู้ให้บริการ

เปิดช่องให้ผู้รับบริการสามารถหลุดพ้นจากการรับโทษ หากพิสูจน์ได้ว่าตนได้กระทาตามขั้นตอนที่กฎหมายกาหนดแล้ว โดยมาตรา 15 ได้ระบุให้รัฐมนตรีออกประกาศกระทรวงเพื่อก าหนดแนวทางในการรับมือเมื่อผู้ให้บริการพบกับข้อมูลที่ขัดต่อกฎหมายฉบับนี้อย่างชัดเจน โดยหากผู้ให้บริการได้มีการดาเนินการตามขั้นตอนนั้นๆแล้ว ก็จะไม่ถือว่ามีความผิดตามกฎหมาย ทาให้ผู้ให้บริการได้รับความคุ้มครองอย่างเป็นธรรม และมีแนวปฏิบัติในการให้บริการที่ชัดเจนขึ้น และมาตรา 16 ได้ระบุให้ขยายเวลาในการเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อใช้เป็นหลักฐานในการสืบสวนสอบสวน

3.6.5 การคุ้มครองความเสียหายต่อบุคคลธรรมดา

มาตรา16 มีการระบุเพิ่มเติมความคุ้มครองในเรื่องการเผยแพร่ภาพตัดต่อที่ทาให้เกิดความเสียหายของตัวบุคคล ให้ขยายขอบเขตรวมไปถึงบุคคลที่เสียชีวิตแล้วด้วยเช่นกัน โดยญาติที่ยังมีชีวิต สามารถเข้าทาการฟ้องร้องดาเนินคดีแทนบุคคลผู้เสียชีวิตไปแล้วได้ และเพิ่มอัตราเพดานโทษปรับสาหรับการเผยแพร่ภาพตัดต่อที่ขัดต่อกฎหมายนี้ จากเดิม 60,000 บาท เป็น 200,000 บาท เพื่อให้ศาลสามารถพิจารณาลงโทษได้เหมาะสมกับระดับความเสียหายที่เกิดต่อตัวผู้เสียหาย หรือต่อความสงบสุขเรียบร้อยของสังคม อีกทั้งยังเพิ่มมาตรการบรรเทาความเสียหายจากเนื้อหา (content) ที่ศาลพิพากษาว่าผิด โดยศาลสามารถสั่งให้ทาลาย หรือให้จาเลยเผยแพร่คาพิพากษาเพื่อล้างมลทินให้แก่โจทก์ หรือสั่งให้ผู้ที่มีครอบครองท าลายข้อมูลนั้นเสียก็ได้ (มารา16/2 และมาตรา16/2)

3.6.6 การลงโทษผู้กระท ความผิด

มาตรา 17/1 ได้เพิ่มมาตรการส าหรับเปรียบเทียบปรับ โดยความผิดที่มีโทษจ ุกไม่เกิน 2 ปี สามารถใช้อัตราเปรียบเทียบปรับแทนได้ และได้เพิ่มการแต่งตั้งคณะกรรมการที่จะเป็นผู้พิจารณาอัตราในการเปรียบเทียบปรับ เพื่อลดภาระในการดาเนินคดีที่ชั้นศาล ย่นเวลาและลดค่าใช้จ่ายในการบรรเทาความเสียหายให้ผู้เสียหาย

3.6.7 การเชื่อมโยงความร่วมมือของพนักงานเจ้าหน้าที่ในทุกภาคส่วน

มาตรา 18 ถูกเพิ่มเติมให้พนักงานสืบสวนตามกฎหมายอื่นๆสามารถขอความร่วมมือในการหาหลักฐานเชิงเทคนิคจากพนักงานเจ้าหน้าที่ตามกฎหมายนี้เพื่อประโยชน์ในการสืบสวนสอบสวนคดี และยังกาหนดระยะเวลาในการดาเนินการไว้ชัดเจน เพื่อให้พนักงานเจ้าหน้าที่ตามกฎหมายฉบับนี้ด าเนินการช่วยเหลืออย่างไม่ผัดผ่อน

3.6.8 พนักงานเจ้าหน้าที่

มาตรา 20 ก าหนดให้มีการแต่งตั้งคณะกรรมการอีกชุดเพื่อกลั่นกรองข้อมูลที่ถือเป็นความผิดตามพระราชบัญญัติฯนี้ โดยเปิดโอกาสตัวแทนจากภาคเอกชนที่มีความรู้ความเชี่ยวชาญในแต่ละด้าน เช่น ด้านสิทธิมนุษยชน ด้านสื่อสารมวลชน ด้านเทคโนโลยีสารสนเทศ เข้ามาร่วมเป็นคณะกรรมการชุดนี้ เพื่อให้การตัดสินมีความเป็นธรรมต่อทุกฝ่ายมากที่สุด และยังเพิ่มค่าจ้างให้พนักงานเจ้าหน้าที่เพื่อให้เทียบเท่ากับราคาตลาด เพื่อแก้ปัญหาการขาดแคลนทรัพยากรบุคคล และจูงใจคนมีความสามารถเข้ามาร่วมงาน

บทที่ 4
กฎหมายเกี่ยวกับการกระท ิดในรูปแบบสแปม (spam) ในต่างประเทศ

ปัญหาที่เกี่ยวข้องกับสแปมเมลเป็นปัญหาทั้งต่อผู้รับและผู้ให้บริการ อีกทั้งยังเป็นภาระต่อภาคเอกชนที่ต้องหมั่นปรับปรุงมาตรการทางเทคโนโลยีให้ทันสมัยอยู่เสมอเพื่อดักจับและป้องกันสแปมเมล ถึงกระนั้นความพยายามจากภาคเอกชนเพียงฝ่ายเดียวยังไม่สามารถรองรับปัญหานี้ได้ทั้งหมด และความเสียหายที่เกิดขึ้นยังไม่ได้รับการเยียวยาอย่างเหมาะสม เพราะเป็นเรื่องยากที่จะประเมินมูลค่าความเสียหายออกมาเป็นตัวเลข หรือยากที่จะสืบหาตัวตนที่แท้จริงของผู้ทาสแปมมาดาเนินคดี ดังนั้น ในหลายประเทศจึงได้สร้างมาตรการทางกฎหมายเฉพาะออกมาปรามปราม วางหลักเกณฑ์การพิจารณาความผิดเชิงเทคนิค และหาเจ้าหน้าที่ที่มีความสามารถเฉพาะทางเพื่อมาสืบสวนและดูแลการกระทารูปแบบนี้ โดยแต่ละประเทศมีการให้คาจากัดความของสแปม และมีหลักการในการพิจารณาพิพากษาคดีที่แต่งต่างกันออกไป ดังที่จะมีการอธิบายในข้อ 4.1 ความหมายของการกระทาความผิดในลักษณะสแปม (spam) ข้อ 4.2 กฎหมายต่อต้านการกระทาความผิดเกี่ยวกับสแปม (spam) ในประเทศสหรัฐอเมริกา ข้อ 4.3 กฎหมายต่อต้านการกระทาความผิดเกี่ยวกับสแปมในสหภาพยุโรป และสรุปความแตกต่างของหลักเกณฑ์ในการบังคับใช้กฎหมายต่อต้านการกระท าความผิดเกี่ยวกับสแปมในสหรัฐอเมริกาและสหภาพยุโรปในข้อ 4.4

4.1 ความหมายของการกระทาความผิดในลักษณะสแปม (spam)

ปัจจุบัน หลายประเทศทั่วโลกได้ให้ความสนใจกับปัญหานี้ โดยมีความพยายามในการออกกฎหมายเพื่อเข้ามาช่วยลดจานวนสแปมเมลลง แม้ว่าเจตนารมณ์ในการบัญญัติจะมีความคล้ายคลึงกัน แต่จุดประสงค์และมาตรการทางกฎหมายที่ถูกสร้างขึ้นมานั้นย่อมมีความแตกต่างกันไปในแต่ละประเทศ บริษัทที่กาลังขยายตัวออกไปสู่ระดับสากลจึงควรศึกษาและทาความเข้าใจเกี่ยวกับกฎหมายป้องกันสแปมทั้งจากประเทศที่เป็นต้นทางผู้ส่งและประเทศปลายทางที่เป็นผู้รับให้ลึกซึ้ง เพื่อไม่ให้เกิดผลกระทบต่อการดาเนินธุรกิจ และป้องกันความเสี่ยงจากการโดนฟ้องร้อง เพราะสแปมไม่ได้เป็นเพียงแค่ “อีเมลที่ไม่ต้องการ” (unwanted mail) เท่านั้น ในหลายประเทศให้คานิยามของสแปมว่า “ข้อความหลอกลวงทางอิเล็กทรอนิกส์ที่ไม่พึงประสงค์” (unsolicited misleading electronic messages) โดยนิยามของการกระทาความผิดฐานส่งข้อมูลหรือจดหมายอิเล็กทรอนิกส์ในลักษณะสแปมในแต่ละประเทศมีความแตกต่างกันแล้วแต่แนวนโยบายการบริหารประเทศ

ประเทศสหรัฐอเมริกามีกฎหมายควบคุมการโจมตีทางการตลาดและสื่อลามกอันไม่พึงประสงค์ หรือ Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM Act 2003) ได้ให้คานิยามว่าสแปมเมลคือ “การส่งอีเมลเชิงพาณิชย์ที่ไม่ได้ถูกร้องขอ” (Unsolicited Commercial e-mail: UCE) และ “การส่งอีเมลที่ไม่ได้ถูกร้องขอเป็นจานวนมากในคราวเดียว” (Unsolicited Bulk e-mail: UBE) โดยกฎหมายฉบับนี้มีเจตนาจะป้องกันไม่ให้นักการ

ตลาดส่งอีเมลที่ไม่เป็นที่ต้องการหรืออีเมลที่มีเนื้อหาไม่เหมาะสมให้แก่ผู้รับ และเปิดโอกาสให้ผู้รับสามารถเลือกที่จะปฏิเสธรับ (Opt-Out) อีเมลนั้นได้ ซึ่งกาหนดโทษปรับสูงสุดไว้ถึง 16,000 ดอลลาร์ต่ออีเมลหนึ่งฉบับ[1]

สาหรับ Canada Anti-Spam Legislation (CASL) 2014 ของประเทศแคนาดา ให้นิยามว่าสแปมคือ“ข้อความโฆษณาอิเล็กทรอนิกส์เชิงพาณิชย์ที่ไม่ได้ร้องขอ” (Unsolicited commercial electronic messages: CEMs) ซึ่งตีความครอบคลุมถึงการโฆษณาผ่านสื่ออิเล็กโทรนิกส์ทุกช่องทาง ไม่ว่าจะเป็น อีเมล การบริการส่งข้อความสั้น (SMS) และระบบส่งข้อความทันที (IM) โดยจุดประสงค์ของกฎหมายฉบับนี้ คือ การจัดการกับข้อความโฆษณาที่ส่งไปโดยไม่ได้รับการยินยอม (permission) จากผู้รับ เพื่อป้องกันประชาชนชาวแคนาดาจากอันตรายที่มาจากไวรัล มัลแวร์ สปายแวร์ หรือการโดนเก็บเกี่ยวข้อมูลที่อยู่อีเมลบนอินเทอร์เน็ตโดยมิชอบ (address harvesting) และสร้างความวางใจให้แก่ธุรกิจว่าจะสามารถท าการแข่งขันบนตลาดโลกได้อย่างเป็นธรรม[2]

ในทานองเดียวกัน สหภาพยุโรปมีกฎหมายที่บังคับใช้ร่วมกันในกลุ่ม ได้แก่ ระเบียบว่าด้วยสิทธิส่วนบุคคลและการสื่อสารทางอิเล็กทรอนิกส์ หรือ Privacy and Electronic Communications Directive 2002/58/EC (E-privacy Directive) ให้คานิยามไว้ว่า “การสื่อสารเชิงพาณิชย์ที่ไม่พึงประสงค์” (Unsolicited Commercial Communication: UCC) เพื่อสื่อความหมายถึง การสื่อสารเชิงพาณิชย์ผ่านระบบอัตโนมัติที่ไม่ได้รับความยินยอมจากผู้รับล่วงหน้า[3] โดยในบทบัญญัติของกฎหมายฉบับนี้ จะครอบคลุมถึงการสื่อสารเชิงพาณิชย์ในทุกช่องทาง ไม่ว่าจะเป็นการทาการตลาดทางโทรศัพท์ สื่ออิเล็กทรอนิกส์ โทรสาร ระบบสื่อสารของอุปกรณ์อิเล็กทรอนิกส์แบบสองทางด้วยคลื่นวิทยุระยะสั้น (Bluetooth) อีเมล ฯลฯ ซึ่งสร้างขึ้นเพื่อเป็นเครื่องมือสาคัญในการปกป้องสิทธิความเป็นอยู่ส่วนบุคคล รวมถึงเป็นการป้องกันข้อมูลที่อยู่บนระบบเครือข่ายอิเล็กทรอนิกส์สาธารณะ และให้ความชัดเจนในเรื่องของความยินยอม (Consent) และการละเมิดสิทธิความเป็นอยู่ส่วนบุคคลจากการเข้าถึงข้อมูลของผู้ใช้บริการโดยยึดหลัก Opt-in สาหรับการส่งอีเมลเชิงพาณิชย์

ส่วนประเทศญี่ปุ่นมีกฎหมายที่เกี่ยวข้องคือ The Act on Regulation of Transmission of Specific Electronic Mail โดยกาหนดนิยามของ “จดหมายอิเล็กทรอนิกส์ (e-mail)” และ “จดหมายอิเล็กทรอนิกส์เฉพาะเรื่อง (Specified Electronic Mail)” โดยมีวัตถุประสงค์เพื่อป้องกันไม่ให้เกิดอุปสรรคในการรับส่งอีเมลทั้งในประเทศและระหว่างประเทศ โดยกาหนดให้ผู้ส่งยึดหลัก Opt-in และมีการกาหนดมาตรการต่างๆในการส่งจดหมายอิเล็กทรอนิกส์เฉพาะเรื่อง เช่น การกาหนดรายละเอียดที่ต้องระบุในจดหมายอิเล็กทรอนิกส์เฉพาะเรื่อง กาหนดห้ามไม่ให้ส่งไปยังบุคคล

---

[1] MCKERNAN. K. Anti-SPAM Laws Around the World [Online]. 2016. Available from: https://pierryinc.com/2016/07/18/anti-spam-laws-around-world/ [8 April 2018]

[2] Canada's Anti-Spam Legislation. Canada's Law on Spam and Other Electronic Threats. [Online]. 2017. แหล่งที่มา: http://fightspam.gc.ca/eic/site/030.nsf/eng/home [13 June 2017.]

[3] Ibd.

หรือประเทศที่เลือกใช้ระบบ Opt-out เท่านั้น กาหนดไม่ให้ส่งอีเมลโดยใช้ที่อยู่ปลอม และยังมีมาตรการที่เกี่ยวข้องกับหน้าที่ของผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail Service Provider) ว่าต้องจัดหามาตรการป้องกันการรบกวนที่อาจเกิดขึ้นจากการโอนจดหมายอิเล็กทรอนิกส์เฉพาะเรื่อง[4]

จากตัวอย่างในข้างต้น จะเห็นได้ว่าแต่ละประเทศต่างมีเกณฑ์ในการพิจารณาความผิดและจุดประสงค์ในการบัญญัติกฎหมายที่แตกต่างกันไป ตามแนวคิดในการบังคับใช้ สถานการณ์การใช้งานอินเทอร์เน็ต ระดับความรุนแรง ลักษณะการกระท าความผิดที่เกิดขึ้นในประเทศของตน

นอกจากนี้รายงานจากการสารวจของ Kaspersky ในไตรมาสแรกของปี 2017 พบว่าประเทศที่เป็นจุดกาเนิดของสแปมมากที่สุดคือสหรัฐอเมริกา (18.75%) และต่อมาได้แก่ ประเทศเวียดนาม (7.86%) และสาธารณรัฐประชาชนจีน (7.77%)[5] ตามลาดับ โดยมาตรการทางกฎหมายเกี่ยวกับสแปมเมลที่น่าสนใจและถูกนาไปเป็นแบบอย่างให้หลายประเทศปรับใช้ ได้แก่ “กฎหมายควบคุมการโจมตีทางการตลาดและสื่อลามกอันไม่พึงประสงค์” หรือ Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) ของสหรัฐอเมริกา และ “ระเบียบว่าด้วยสิทธิส่วนบุคคลและการสื่อสารทางอิเล็กทรอนิกส์” หรือ Privacy and Electronic Communications Directive (E-privacy Directive) ของสหภาพยุโรป ผู้ศึกษาจึงขอหยิบยกตัวบทกฎหมายของสองประเทศดังกล่าว เพื่อนามาเป็นแนวทางในการศึกษาและนามาพิจารณาหาแนวทางการใช้งานที่เหมาะสมในประเทศไทย

4.2 กฎหมายต่อต้านการกระท าความผิดเกี่ยวกับสแปม (spam) ในประเทศสหรัฐอเมริกา

“กฎหมายควบคุมการโจมตีทางการตลาดและสื่อลามกอันไม่พึงประสงค์” (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003: CAN-SPAM Act) หรือที่ถูกเรียกกันทั่วไปว่า CAN-SPAM ถูกร่างขึ้นโดยคณะกรรมการการค้าสหรัฐ (the Federal Trade Commission: FTC) ที่เป็นหน่วยงานในการคุ้มครองผู้บริโภคแห่งชาติของสหรัฐอเมริกา และสภาครองเกรสได้อนุมัติร่างกฎหมายนี้ให้มีผลบังคับใช้ในฐานะเป็นกฎหมายระดับสหรัฐ (Federal Law) ตั้งแต่วันที่ 1 มกราคม 2004 เป็นต้นมา โดยมีเนื้อหาหลัก 3 ประการ ได้แก่ ประการที่หนึ่ง การวางหลักเกณฑ์และคานิยามของวัตถุประสงค์หลัก (the primary purpose) ในการส่งอีเมลเชิงพาณิชย์ ประการที่สอง เพื่อคุ้มครองผู้รับให้มีสิทธิในการบอกปฏิเสธไม่รับอีเมลจากแหล่งที่มาที่ตนไม่ต้องการ (Opt-out) และประการที่สาม วางมาตรการที่เกี่ยวข้องกับการแสดงฉลาก (Label) เพื่อบ่งชี้อีเมลที่มีเนื้อหาเกี่ยวกับเรื่องเพศ ต่อมาในปี 2008 คณะกรรมการการค้าแห่งสหรัฐ (Federal Trade Commission: FTA) ได้อนุมัติกฎเกณฑ์ของ CAN-SPAM ใหม่อีกครั้งเพื่อให้เกิดการตีความที่ชัดเจนต่อบทบัญญัติที่เกี่ยวข้อง

---

[4] Ibd.

[5] Darya Gudkova, M. V., Tatyana Shcherbakova, Nadezhda Demidova [Online]. 2017. Available from: https://securelist.com/spam-and-phishing-in-q1-2017/78221/ [10 April 2018.]

4.2.1 ที่มาของ CAN-SPAM

ประเทศสหรัฐอเมริกาเป็นประเทศลาดับต้นๆที่ประสบปัญหาการคุกคามจาก “อีเมลเชิงพาณิชย์ที่ไม่ได้ถูกร้องขอ” (Unsolicited Commercial e-mail: UCE) จากในปี 2001 ที่มีจานวน UCE เพียง 7% แต่ในปี 2003 กลับมีจานวน UCE ในแต่ละวันเพิ่มมากกว่าครึ่งของจานวนอีเมลทั้งหมดที่วิ่งอยู่บนเครือข่ายอินเทอร์เน็ต[6] และยังมีทีท่าว่าจะเพิ่มขึ้นอย่างต่อเนื่องไม่สิ้นสุด โดยเนื้อความใน UCE ส่วนใหญ่มักเป็นเนื้อหาเกี่ยวกับการหลอกลวง ฉ้อโกง และฝ่ายผู้รับไม่สามารถทาการบอกปฏิเสธอีเมลเหล่านั้นได้ จึงทาให้ต้องเผชิญกับต้นทุนในด้านต่างๆ ไม่ว่าจะเป็นด้านพื้นที่ในการจัดเก็บ ด้านเวลาที่ต้องเสียไปกับการบริหารจัดการเพื่อคัดแยกอีเมล อีกทั้งผู้รับที่ได้รับอีเมลเหล่านี้เป็นจานวนมากๆยังประสบกับความเสี่ยงในการสูญเสียโอกาสรับ หรือพลาดโอกาสในการตรวจสอบอีเมลที่มีความสาคัญ หรืออาจท ให้อีเมลที่มีความส คัญจริงๆถูกมองข้ามไป อันเป็นสาเหตุที่ทาให้คุณประโยชน์และความน่าเชื่อถือในการใช้งานอีเมลลดลง ทางด้านภาคธุรกิจ หน่วยงานการศึกษา องค์กรไม่แสวงผลกาไร หรือตัวผู้ให้บริการเครือข่ายอินเทอร์เน็ต (Internet Service Provider: ISPs) ฯลฯ ต่างก็ต้องแบกรับต้นทุนด้านการประกอบการที่เพิ่มขึ้นจากการลงทุนเพื่อโครงสร้างพื้นฐานในการดักจับและป้องกัน UCE

เนื่องจากในอดีตไม่ได้มีกฎหมายระดับสหรัฐออกมากากับดูแลปัญหาเหล่านี้โดยเฉพาะ จึงไม่มีระเบียบแบบแผนใดมาควบคุมวิธีการส่งอีเมลเชิงพาณิชย์มากนัก ผู้ส่งบางรายอาจทาทีเหมือนเปิดช่องทางในการปฏิเสธรับ (opt-out) เพื่อสร้างความน่าเชื่อถือให้อีเมลของตน แต่สุดท้ายก็ไม่ปฏิบัติตามคาร้องขอปฏิเสธของผู้รับ หรือบางรายอาจไม่เปิดช่องทางให้ผู้รับสามารถส่งคาปฏิเสธได้เลย ผู้ส่งบางรายอาจใช้โปรแกรมอัตโนมัติ (Bot) ในการหารายชื่อที่อยู่อีเมลจานวนมากจากหน้าเว็บไซต์หรือบริการออนไลน์ต่างๆที่เคยมีคนมาลงทะเบียนหรือโพสต์ที่อยู่อีเมลเอาไว้ (Harvesting) เพื่อทาการส่งอีเมลโฆษณาครั้งละจานวนมากๆ (Bulk e-mail) ทาให้ปัญหาเหล่านี้ยิ่งทวีความรุนแรงเพิ่มขึ้นเรื่อยๆ

ปัญหาอีกประการหนึ่งคือการที่แต่ละรัฐมีมาตรการทางกฎหมายที่ไม่สอดคล้องกัน หลายรัฐมีการออกกฎหมายมาเพื่อควบคุมและลดจานวน UCE ภายในรัฐของตน จึงทาให้มาตรฐานของแต่ละรัฐมีความแตกต่างกัน อีกทั้งการส่งอีเมลยังเป็นสิ่งที่ไม่สามารถใช้หลักการจากัดถิ่นที่อยู่มาจากัดขอบเขตพฤติกรรมได้ เนื่องจากการกระทารูปแบบนี้มักไม่ได้เกิดขึ้นเพียงแค่พื้นที่ใดพื้นที่พื้นที่หนึ่ง ทาให้ผู้ที่ต้องการส่งอีเมลเชิงพาณิชย์โดยสุจริตอาจเกิดความสับสนในการอ้างอิงตัวบทกฎหมายเพื่อปฏิบัติให้ถูกต้อง และยังมีปัญหาเกี่ยวกับเรื่องความขัดแย้งในขอบเขตอานาจศาลระหว่างประเทศในการดาเนินคดีความ ตัวอย่างเช่นข้อพิพาทเรื่องการแสดงงานฝีมือของ Nazi ที่ถูกนาไปประมูล

[6] CAN-SPAM Act, section 2 (2)

ออนไลน์บนเว็บไซต์ Yahoo! โดยคดีนี้บริษัท Ligue contre le racisme et L'Antisemitisme เป็นผู้ฟ้องบริษัท Yahoo! ฐานละเมิด แม้ศาลสูง ณ กรุงปารีส (High Court of Paris) จะมีคำพิพากษา[7] ให้บริษัท Yahoo! มีความผิดฐานละเมิดตามมาตรา R645-1[8] ของประมวลกฎหมายอาญาประเทศฝรั่งเศสจริง ต้องรับโทษปรับ 100,000 ยูโร[9] และต้องลบผลงานของ Nazi ออกจากไดเรกทอรีบราวเซอร์ (browser directory) ที่สาธารณรัฐฝรั่งเศสสามารถเข้าถึงได้ Yahoo! อีกด้วย

แต่เนื่องจากการประมูลนี้ถูกจัดขึ้นภายใต้ขอบเขตอานาจศาลของสหรัฐอเมริกา เพราะเซิร์ฟเวอร์ของเว็บไซต์ที่ใช้ในการประมูลตั้งอยู่ในสหรัฐ และถึงแม้ว่าจะไม่ได้มีการจากัดสิทธิการเข้าถึงของผู้เข้าร่วมประมูลที่อยู่ในประเทศฝรั่งเศสก็ตาม แต่เป็นประมูลที่ถูกจัดขึ้นโดยมีเป้าหมายลูกค้าหลักเป็นคนที่อยู่ในสหรัฐอเมริกาอยู่แล้ว หลังจากได้รับคาพิพากษาดังกล่าว ทางบริษัท Yahoo! จึงได้ส่งคาอุทธรณ์ไปยัง ศาลเขตในแคลิฟอเนีย (United States District Court for the Northern District of California) และศาลได้กลับคาพิพากษาว่าคาสั่งของศาลฝรั่งเศสถือเป็นการละเมิดต่ออิสรภาพในการแสดงออกภายใต้บทบัญญัติของ First Amendment ตามรัฐธรรมนูญที่บัญญัติว่า

"*สภาคองเกรซควรจะทาให้ไม่มีกฎหมายที่พาดพิงถึงการก่อตั้งศาสนา หรือห้ามการใช้สิทธิอย่างอิสระเช่นนั้น หรือริดรอนเสรีภาพในการพูด (Freedom of speech) หรือการเสนอข่าวสาร หรือสิทธิของประชาชนที่จะประชุม/ชุมนุมกันโดยสงบ และยื่นคาร้องต่อรัฐบาลเพื่อแก้ไขข้อข้องใจนั้น*"

แม้ว่าท้ายที่สุดบริษัท Yahoo! เลือกที่จะนาผลงานของ Nazi ออกจากเว็บไซต์ของตนเพื่อเป็นการยุติปัญหาดังกล่าว แต่การอ้างถึง First Amendment เพื่อเป็นเครื่องมือในการขออิสระทางการสื่อสารออนไลน์โดยปราศจากการแทรกแซงของรัฐ เป็นตัวจุดประกายให้สื่อต่างๆ ออกมาวิพากษ์วิจารณ์ และเกิดประเด็นถกเถียงกันอย่างกว้างขวางในสหรัฐอเมริกา หลายฝ่ายมองว่าเป็นการใช้อานาจของกฎหมายต่างประเทศมาควบคุมพฤติกรรมของธุรกิจระหว่างประเทศ แต่

---

[7] UJEF et LICRA v. Yahoo! Inc. et Yahoo France, Tribunal de Grande Instance de Paris, No RG:00/0538, May 22, 2000 and November 22, 2000

[8] Article R645-1 of the French Criminal Code prohibits to "wear or exhibit" in public uniforms, insignias and emblems which "recall those used" by

An organisation declared illegal in application of Art. 9 of the Nuremberg Charter, or by

A person found guilty of crimes against humanity as defined by Arts. L211-1 to L212-3 or by the Law № 64-1326 of 1964-12-26. Display is allowed for the purposes of films, theatrical productions and historical exhibitions.The penalty is a fifth class fine (up to 1,500 EUR), to which can be added one or more complementary penalties among:

Withdrawal of the right to possess or hold any regulated weapon for up to three years;

Confiscation of one or more regulated weapon either possessed by the convict or to which he has a free access; Confiscation of the objects concerned; From 20 to 120 hours of community service.

[9] Martin Samson. Yahoo, Inc. V. La Ligue Contre Le Racisme Et L'antisemitisme, Et Al, 145 F. Supp. 2d 1168, Case No. C-00-21275jf (N.D. Ca., September 24, 2001) [Online]. Available from: http://www.internetlibrary.com/cases/lib_case17.cfm [8 April 2018.]

ประเด็นที่สาคัญที่สังเกตุได้จากคดีนี้คือ อุปสรรค์ในการบังคับใช้คาพิพากษาของศาลต่างประเทศในกรณีที่ไม่มีกฎหมายระดับสหรัฐเข้ามาดูแลปัญหาเฉพาะทาง[10]

อย่างไรก็ตาม การเพิ่มขึ้นอย่างรวดเร็วของปัญหาและการใช้สแปมเมลในทางที่ผิด คงไม่สามารถแก้ไขได้ด้วยการบังคับใช้กฎหมายเพียงอย่างเดียว แต่ยังต้องอาศัยการประสานความร่วมมือเพื่อให้เกิดการบังคับใช้ที่สอดคล้องกัน และยังต้องอาศัยมาตรการทางเทคโนโลยีเข้ามารับมือด้วย

4.2.2 จุดประสงค์ของกฎหมาย CAN-SPAM

จุดประสงค์หลักในการบัญญัติกฎหมาย CAN-SPAM ตามมาตรา 2(b) มี 3 ประการ

1) เพื่อควบคุมและลดจานวนอีเมลเชิงพาณิชย์ที่ไม่ได้ถูกร้องขอ (UCE) และอีเมลเกี่ยวกับเรื่องเพศที่ไม่ได้ถูกร้องขอ(unsolicited pornography)

2) กาหนดห้ามไม่ให้ผู้ที่ส่ง (Sender) ทาการส่งอีเมลเหล่านี้โดยปลอมแปลงแหล่งที่มาในการส่ง หรือใช้หัวเรื่อง (Header) ที่บิดเบือนจากเนื้อหาที่อยู่ข้างในเพื่อลวงให้ผู้รับเกิดความเข้าใจผิด

3) เปิดโอกาสให้ผู้รับสามารถเลือกที่จะหยุดรับ (Opt-Out) อีเมลเชิงพาณิชย์ที่ไม่ได้ถูกร้องขอจากแหล่งที่มาเดิม

4.2.3 การนิยามของค ศัพท์ที่เกี่ยวข้อง

กฎหมายฉบับนี้ได้ก าหนดนิยามของค ศัพท์ที่เกี่ยวข้องกับสแปมเมลเอาไว้ ดังนี้[11]

1) การให้และยืนยันความยินยอม (Affirmative Consent)[12] หมายถึง

1. มีการให้ความยินยอมเพื่อรับอีเมลเชิงพาณิชย์นั้นอย่างชัดเจน หรือมีการแสดงออกเพื่อร้องขอให้ส่งอย่างชัดเจนจากทางฝั่งตัวผู้รับและ

2. หากอีเมลเชิงพาณิชย์นั้นจะถูกส่งโดยบุคคลอื่น (other party) ที่ไม่ใช่บุคคลเดียวกับที่ผู้รับเคยให้คายินยอมเอาไว้ จะต้องมีการแจ้งให้ผู้รับรู้ล่วงหน้าอย่างชัดเจน ณ เวลาที่ผู้รับให้คายินยอม ว่าที่อยู่อีเมลของผู้รับนั้นจะถูกส่งต่อไปยังบุคคลอื่นเพื่อจุดประสงค์ในการส่งอีเมลเชิงพาณิชย์นั้นๆ

2) หน่วยงานผู้รับผิดชอบ (Commission) หมายถึง คณะกรรมการการค้าสหรัฐ (FTC)[13]

3) ชื่อโดเมน (Domain name) หมายถึง ชื่อที่เป็นอักขระอักษรเลขที่ถูกลงทะเบียนหรือถูกกาหนดโดยองค์กรที่มีหน้าที่เป็นตัวแทนในการจดชื่อโดเมนในระบบสากล (Registrar) หรือ

---

[10] นางสาวศศิมา ศรีพจน์ธรรม. มาตรการทางกฎหมายเพื่อการจัดการจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงประสงค์ (Spam Mail). ปริญญาตรี, คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2548, หน้า 66-69.

[11] CAN-SPAM Act, section 3

[12] CAN-SPAM Act, section 3 (1)

[13] CAN-SPAM Act, section 3 (3)

องค์กรที่เป็นเจ้าของชื่อโดเมนระดับสูงสุด (Registry) หรือผู้ที่มือ นาจกระทาการจดทะเบียนโดเมนที่เป็นส่วนหนึ่งของที่อยู่อิเล็กทรอนิกส์บนอินเทอร์เน็ต[14]

4) ที่อยู่อีเมล (Electronic mail address) หมายถึง จุดหมายปลายทาง หรือชุดตัวอักขระ (string of characters) หรือชื่อผู้ใช้งานที่เป็นเอกลักษณ์ หรือกล่องข้อความ (โดยทั่วไปจะถูกอ้างอิงถึง Local part ที่เป็นชื่อหน้า เช่น Chanyaruk@xxx.xxx) หรือสิ่งที่อ้างอิงถึงอินเทอร์เน็ตโดเมน (โดยทั่วไปจะหมายถึงชื่อโดเมน (Domain part) ที่อยู่หลังเครื่องหมาย @ เช่น xxxx@example.com) ที่สามารถส่งข้อความอิเล็กทรอนิกส์ไปถึงได้[15]

5) ข้อความในอีเมล (Electronic mail message) หมายถึง ข้อความที่ส่งไปยัง “ที่อยู่อีเมล” แบบเฉพาะเจาะจง[16]

6) ข้อมูลหัวจดหมาย (Header Information) หมายถึง สิ่งบ่งชี้แหล่งข้อมูลจุดหมายปลายทาง และข้อมูลเครือข่าย (routing information) ที่แนบกับข้อความอีเมล รวมไปถึงชื่อโดเมนต้นทาง (originating domain name) และที่อยู่อีเมลต้นทาง (originating electronic mail address) และข้อมูลอื่นๆที่ปรากฏอยู่บนแถบระบุตัวตน (identifying line) หรือการแสดงเจตนาเพื่อระบุบุคคลที่เป็นผู้ก่อการของข้อความดังกล่าว[17]

7) ผู้ก่อการ (Initiate) หมายถึง บุคคลที่เป็นผู้เริ่มในการสร้าง หรือส่งต่อ หรือจัดหาอีเมลฉบับนั้นๆ แต่ไม่รวมถึงการกระทาเพื่อส่งต่อที่ทาอยู่เป็นประจาอยู่แล้ว ดังนั้น ผู้ก่อการในบริบทนี้จึงมีได้มากกว่าหนึ่งคน[18]

8) การจัดหา (Procure) ในบริบทนี้หมายถึง การจงใจจ่ายหรือเสนอความคิดเพื่อให้เกิดอีเมลนั้น รวมไปถึงบุคคลอื่นใดที่เป็นตัวแทนในการริเริ่มสร้างข้อความนั้นๆด้วย[19]

9) ผู้รับ (recipient) หมายถึง ที่อยู่อีเมลของผู้ใช้งานที่ได้รับสิทธิ (authorize) ให้สามารถส่งข้อความไปถึงได้ ถ้าผู้รับมีที่อยู่อีเมลที่สามารถส่งข้อความอีเมลเชิงพาณิชย์ไปถึงได้มากกว่า 1 ที่อยู่ แต่ละที่อยู่ควรถูกปฏิบัติเยี่ยงผู้รับที่เป็นคนละคนกัน โดยแต่ละที่อยู่อีแมลจะถูกนับเป็นหนึ่งผู้รับ และหากที่อยู่อีเมลถูกมอบให้ (reassign) ผู้ใช้งานคนใหม่ ผู้ใช้งานคนใหม่จะไม่ถูกปฏิบัติด้วยเช่นเดียวกับผู้รับอีเมลเชิงพาณิชย์เดิมก่อนถูกส่งมอบ[20]

10) ผู้ส่ง (Sender) หมายถึง บุคคลที่เป็นผู้ก่อการในการทาข้อความโฆษณาหรือโปรโมทสินค้า ผลิตภัณฑ์ บริการ หรืออินเทอร์เน็ตเว็บไซด์[21]

---

[14] CAN-SPAM Act, section 3 (4)

[15] CAN-SPAM Act, section 3 (5)

[16] CAN-SPAM Act, section 3 (6)

[17] CAN-SPAM Act, section 3 (8)

[18] CAN-SPAM Act, section 3 (9)

[19] CAN-SPAM Act, section 3 (12)

[20] CAN-SPAM Act, section 3 (14)

[21] CAN-SPAM Act, section 3 (16)

4.2.4 ลักษณะของอีเมลที่ถูกควบคุมการส่งโดย CAN-SPAM

กฎหมายฉบับนี้จัดทาขึ้นเพื่อจากัดจานวนและควบคุมการดาเนินการเพื่อส่งอีเมลโฆษณาที่ไม่ได้รับการร้องขอจากผู้รับ โดยแบ่งออกเป็น 2 ประเภท ได้แก่

1) อีเมลเชิงพาณิชย์ (Commercial electronic mail message) หมายถึง จดหมายอิเล็กทรอนิกส์ที่มีวัตถุประสงค์หลัก (the primary purpose) ในการโฆษณาเชิงพาณิชย์หรือเพื่อประชาสัมพันธ์ สินค้าหรือบริการ (รวมถึงเนื้อหาบนเว็บไซต์ที่ถูกจัดทาขึ้นเพื่อจุดประสงค์ทางการค้าด้วย) โดย FTC ได้ออกมาตรการเพิ่มเติมเพื่อกาหนดนิยามของข้อกาหนดเรื่องวัตถุประสงค์หลัก (the primary purpose) ดังต่อไปนี้[22]

1. วัตถุประสงค์หลักของอีเมลที่จะถูกพิจารณาว่าเป็นเชิงข้อความพาณิชย์ ได้แก่ อีเมลที่มีเนื้อหาเกี่ยวกับการโฆษณา ประชาสัมพันธ์สินค้าหรือบริการเชิงพาณิชย์เท่านั้น

2. แม้จะมีทั้งเนื้อหาเชิงพาณิชย์และเนื้อหาเชิงความสัมพันธ์หรือธุรกรรม แต่ผู้รับมีเหตุผลพอที่จะสามารถตีความได้จากชื่อเรื่องของอีเมล (Subject) ว่าเนื้อความด้านในเป็นเนื้อหาเชิงพาณิชย์ หรือเป็นเนื้อหาเชิงความสัมพันธ์หรือธุรกรรมที่ไม่ได้แสดงสาระสาคัญของสัญญาหรือข้อความในสัญญาทั้งหมดในอีเมล

3. ชื่อหัวเรื่อง (Subject) ของอีเมลที่แสดงได้ว่าเนื้อหาด้านในเป็นเนื้อหาเชิงพาณิชย์ หรือเนื้อความในตัวอีเมลจะต้องมีวัตถุประสงค์หลักเชิงพาณิชย์

4. การอ้างอิงถึงธุรกิจ (Business) หรือลิงก์ (link) เพื่อเชื่อมโยงไปยังเว็บไซต์เชิงพาณิชย์ ซึ่งมีวัตถุประสงค์อื่นมากกว่าการโฆษณาหรือส่งเสริมการจาหน่ายสินค้าและบริการ จะไม่นับว่าเป็นอีเมลเชิงพาณิชย์

2) ข้อความเชิงความสัมพันธ์หรือธุรกรรม(Transactional or relationship message) หมายความถึง ข้อความที่เกิดจากการที่ผู้ส่งและผู้รับได้มีการก่อนิติกรรมกันมาก่อนล่วงหน้าอยู่แล้ว และที่มีวัตถุประสงค์หลัก (the primary purpose) ดังต่อไปนี้

1. เพื่ออานวยความสะดวก หรือเพื่อความสมบูรณ์ หรือเพื่อยืนยันธุรกรรมที่ผู้รับได้ตกลงกันไว้ผู้ส่งมาก่อนล่วงหน้า

2. เพื่อส่งมอบข้อมูลการรับประกัน (warranty information) หรือการเรียกสินค้าคืน (Product Recall) หรือข้อมูลความปลอดภัย (safety information) หรือข้อมูลการรักษาความปลอดภัย (security information) หรือข้อมูลเพื่อแจ้งการเปลี่ยนเปลงข้อกาหนดการใช้งานเกี่ยวกับผลิตภัณฑ์หรือบริการ ที่ผู้รับซื้อหรือใช้งานอยู่[23]

3. เพื่อส่งประกาศแจ้งเกี่ยวกับการเปลี่ยนแปลงคุณสมบัติ เงื่อนไข หรือการแจ้งเกี่ยวกับการเปลี่ยนแปลงสถานะหรือตาแหน่งของผู้รับ หรือการประกาศแจ้งข้อมูลตามช่วงระยะเวลาที่มีการกาหนดไว้ เช่น ข้อมูลยอดเงินในบัญชี (account balance) หรือข้อมูลแจ้ง

---

[22] CAN-SPAM Act, section 3 (2)

[23] CAN-SPAM Act, section 3 (17)

สถานะการเดินบัญชี (account statement) ที่เกี่ยวข้องกับการบอกรับเป็นสมาชิก การเป็นสมาชิก การกู้เงิน หรือความสัมพันธ์ที่เทียบเคียงได้กับการพาณิชย์ที่ยังดาเนินอยู่ รวมไปถึงการซื้อหรือใช้ผลิตภัณฑ์หรือบริการโดยผู้รับที่ผู้ส่งเป็นคนน าเสนอ

4. เพื่อส่งข้อมูลที่เกี่ยวกับการจ้างงาน หรือสวัสดิการ ที่ผู้รับมีความเกี่ยวข้อง เข้าร่วม หรือขึ้นทะเบียนอยู่โดยตรง ณ ขณะที่ท าการส่ง

5. เพื่อส่งมอบสินค้าหรือบริการ รวมถึงการแจ้งข้อมูลล่าสุด (Update) และการเพิ่มประสิทธิภาพ (Upgrade) สินค้าหรือบริการ ที่ผู้รับมีสิทธิที่จะได้รับตามเงื่อนไขในการทาธุรกรรมที่ผู้รับได้ตกลงกระท าไว้กับผู้ส่งมาก่อนแล้ว

4.2.5 สาระสาคัญของกฎหมาย CAN-SPAM

เนื่องจากกฎหมายฉบับนี้เป็นกฎหมายระดับสหรัฐ (Federal Law) จึงทาให้ทุกมลรัฐในสหรัฐอเมริกาต้องยึดหลักเกณฑ์มาตรฐานดังต่อไปนี้ในการส่งอีเมลเชิงพาณิชย์

1) ห้ามมิให้ส่งอีเมลเชิงพาณิชย์โดยแสดงข้อมูลการส่งเท็จ หรือแสดงข้อมูลที่ก่อให้เกิดการเข้าใจผิด (misleading transmission)[24] อันได้แก่

1. การปลอมแปลงหรือใช้ข้อมูลหัวจดหมาย (Header) ที่ก่อให้เกิดความเข้าใจผิดในสาระสาคัญ (Materially) ของอีเมล หรือการสร้างที่อยู่อีเมล (an originating e-mail address) หรือชื่อโดเมน (domain name) หรือทะเบียนที่อยู่ในไอพีแอดเดรส (Internet Protocol) เพื่อจุดประสงค์ในการฉ้อโกง บิดเบือน หรือจงใจท าให้เกิดความเข้าใจผิด

2. การแสดงแถบผู้ส่ง (form line) ที่ไม่สามารถระบุตัวตนของผู้ก่อการได้

3. การแสดงตัวตนที่ไม่แน่ชัดหรือทาให้เกิดความเข้าใจผิดในคอมพิวเตอร์ที่ใช้เป็นตัวก่อการในการส่งข้อความ เนื่องจากผู้ก่อการใช้คอมพิวเตอร์เครื่องอื่นในการสร้างข้อความและจงใจใช้เครื่องแม่ข่ายอื่นในการส่ง (Relay) หรือส่งต่อข้อมูล (retransmit) ที่มีวัตถุประสงค์เพื่อปลอมแปลงแหล่งที่มา

2) ห้ามใช้ชื่อหัวเรื่อง (Subject) เท็จ กล่าวคือ ผู้ใดที่ส่งอีเมลเชิงพาณิชย์โดยรู้หรือตีความจากพฤติการณ์ได้ว่ารู้ ว่าชื่อหัวเรื่องที่ใช้กับอีเมลเชิงพาณิชย์นั้นจะก่อให้ผู้รับเกิดความเข้าใจผิดในเนื้อหาที่แท้จริงของข้อความ (deceptive subject headings) ทั้งที่มีการกระทาอันมีเหตุให้เชื่อได้ว่าผู้ส่งรู้ถึงสาระสาคัญที่แท้จริงของเนื้อความหรือหัวข้อของข้อความอีเมลนั้นอยู่แล้ว ถือว่าเป็นการกระท าที่ผิดกฎหมาย[25]

3) ผู้ส่งต้องมีที่อยู่อีเมลที่สามารถติดต่อได้หรือมาตรการในการตอบรับทางอินเทอร์เน็ตอื่นๆ เพื่อให้ผู้รับสามารถใช้ส่งข้อความ หรือตอบกลับ หรือสื่อสารผ่านทางมาตรการต่างๆ บนอินเทอร์เน็ตที่ผู้ส่งจัดเตรียมไว้ ในการส่งคาร้องขอที่จะปฏิเสธไม่รับอีเมลเหล่านั้นอีกในอนาคต[26]

---

[24] CAN-SPAM Act, section 5 (a)(1)

[25] CAN-SPAM Act, section 5 (a)(2)

[26] CAN-SPAM Act, section 5 (a)(3)

หากผู้ใดส่งอีเมลเชิงพาณิชย์โดยไม่ระบุที่อยู่อีเมลที่สามารถติดต่อได้ หรือไม่ระบุมาตรการในการตอบรับทางอินเทอร์เน็ตอื่นๆที่ชัดเจนและเห็นได้ชัด จะถือว่าเป็นการกระทาที่ขัดต่อกฎหมาย โดยที่อยู่ในการรับข้อความหรือมาตรการในสื่อสารใดๆที่ระบุไว้นั้น จะต้องยังใช้งานได้ไม่น้อยกว่า 30 วันหลังจากที่อีเมลต้นก าเนิดถูกส่งออกไป

4) ห้ามส่งอีเมลเชิงพาณิชย์หลังจากที่ได้รับการบอกปฏิเสธไม่รับตามมาตรา 5 (a)(3) หากผู้รับได้ส่งคาขอเพื่อปฏิเสธการรับตามมาตรการที่จัดไว้ตามที่ระบุด้านบนแล้ว ผู้รับจะต้องไม่ได้รับอีเมลเชิงพาณิชย์ใดๆจากผู้ส่งอีก[27] ตามเงื่อนไขดังต่อไปนี้

1. ผู้ส่ง ผู้ที่มีอานาจกระทาการแทนตัวผู้ส่ง หรือผู้ที่มีส่วนช่วยในการส่ง เช่น ทาการจัดหาหรือคัดเลือกที่อยู่อีเมลสาหรับจัดส่ง ฯลฯ จะต้องทาการยกเลิกส่งอีเมลเชิงพาณิชย์นั้นภายใน 10 วันทาการ หลังจากที่ได้รับหรือมีพฤติการณ์อันสันนิษฐานได้ว่ารับรู้ “คาร้องขอเพื่อปฏิเสธการรับอีเมลเชิงพาณิชย์” (Opt-out notification) จากผู้รับ และห้ามทาการช่วยเหลือผู้อื่นเพื่อส่งอีเมลไปยังผู้รับนั้น หรือใช้สิทธิของผู้อื่นในการส่งอีเมลในนามของตนไปยังอยู่อีเมลของผู้รับนั้นอีก และห้ามทาการขาย ให้เช่า หรือแลกเปลี่ยนข้อมูลที่อยู่อีเมลของผู้รับที่มีการส่งค ขอปฏิเสธไม่รับอีเมลแล้ว เพื่อจุดประสงค์อื่นใด

2. ข้อห้ามตามวรรคหนึ่งของมาตรานี้จะตกไป หากได้รับคายินยอมโดยชัดแจ้งจากผู้รับตามมาภายหลังจากที่มีการส่งค ขอปฏิเสธรับ

5) ผู้ส่งจะต้องระบุตัวตน ช่องทางการบอกปฏิเสธรับ (Opt-out) และที่อยู่ทางไปรษณีย์ของผู้ส่งในอีเมลเชิงพาณิชย์[28]ด้วยรายละเอียดขั้นต่ าดังต่อไปนี้

1. ผู้ส่งต้องมีสิ่งบ่งชี้ที่ชัดเจนและเห็นได้ชัด (clear and conspicuous) ว่าอีเมลนั้นเป็นข้อความการโฆษณาหรือการเชิญชวน

2. มีคาเตือนเกียวกับโอกาสในการปฏิเสธไม่รับอีเมลเชิงพาณิชย์เพิ่มเติมจากตัวผู้ส่ง (Opt-out notice)

3. มีการระบุที่อยู่ทางไปรษณีย์ที่ถูกต้องของผู้ส่ง (a valid physical postal address of the sender) ในเนื้อความอีเมล

เว้นแต่ หากผู้รับได้มีการให้ได้มีการให้ความยินยอมล่วงหน้าโดยชัดแจ้ง (prior affirmative consent) ในการรับไว้อยู่แล้ว ไม่จาเป็นต้องมีสิ่งบ่งชี้ที่ชัดเจนและเห็นได้ชัดว่าว่าอีเมลนั้นเป็นข้อความการโฆษณาหรือการเชิญชวน

6) ผู้ส่งต้องแสดงสาระสาคัญของอีเมลในหัวจดหมาย โดย “สาระสาคัญ” (Materially) ในบริบทของข้อมูลหัวจดหมายเท็จหรือก่อให้เกิดความเข้าใจผิด หมายถึง การปลอมแปลงแก้ไขหรือปกปิดข้อมูลหัวจดหมาย จนท าให้ผู้รับ ผู้ให้บริการอินเทอร์เน็ต ผู้ที่มีสิทธิร้องเรียนการ

---

[27] CAN-SPAM Act, section 5 (a)(4)

[28] CAN-SPAM Act, section 5 (a)(5)

กระท าความผิดตามมาตรานี้ หรือหน่วยงานตามกฎหมายฉบับนี้ ต้องสูญเสียความสามารถในการบ่งชี้หรือตอบโต้กับผู้ส่ง หรือสูญเสียความสามารถในการสืบสวนการกระท าความผิดนี้

7) ข้อห้ามที่ถือเป็นความผิดร้ายแรงในการกระทาความผิดที่เกี่ยวเนื่องกับการส่งอีเมลเชิงพาณิชย์[29] ได้แก่

1. การรวบรวมที่อยู่อีเมลด้วยวิธีอัตโนมัติจากเว็บไซต์หรือบริการออนไลน์ใดๆที่ดาเนินการโดยบุคคลอื่น (address harvesting) ซึ่ง ณ ขณะที่ผู้ใช้งานลงทะเบียน มีการประกาศแจ้ง (notice) ว่าเว็บไซต์หรือบริการออนไลน์เหล่านั้นจะไม่ขาย โอน แจกจ่าย ที่อยู่อีเมลที่ปรากฏบนเว็บไซต์หรือบริการออนไลน์ ให้แก่บุคคลอื่นใด เพื่อประโยชน์ในการส่งหรือสนับสนุนให้บุคคลอื่นส่งอีเมลไปยังที่อยู่เหล่านี้

2. การใช้วิธีการสุ่มที่อยู่อีเมลของผู้รับโดยเรียงลาดับตามตัวอักษรอัตโนมัติ (randomly generating e-mail address) ซึ่งอาศัยความน่าจะเป็นจากการผสมตัวอักษรกับตัวเลข aa@gmail.com ab@gmail.com ac@gmail.com เป็นต้น

3. การขโมยที่อยู่อีเมลของผู้ใช้งานทั่วไปที่ลงทะเบียนไว้เพื่อการส่งแบบจานวนทวีคูณ (Multiple) หรือใช้ที่อยู่ของผู้ใช้งานออนไลน์อื่นในการส่งผ่าน หรือให้สิทธิในการส่งผ่านอีเมลเชิงพาณิชย์ที่ผิดกฎหมายในลักษณะนี้ โดยจ าเพาะทวีคูณ (Multiple)[30]

4. การใช้คอมพิวเตอร์หรือคอมพิวเตอร์แม่ข่ายของผู้อื่นในการส่งผ่านหรือส่งต่อ (Relay mail) โดยรู้ว่าเป็นอีเมลเชิงพาณิชย์ที่ผิดกฎหมายตามมาตรา 5 (a)

8) ผู้ส่งต้องแสดงฉลากค าเตือน (Warning Labels) บนอีเมลที่มีเนื้อหาเกี่ยวกับเรื่องเพศ[31] ตามหลักเกณฑ์ดังต่อไปนี้

1. อีเมลเชิงพาณิชย์ที่มีเนื้อหาเกี่ยวกับเรื่องเพศหรือสื่อลามกอนาจาร (sexually oriented material) จะต้องแสดงฉลากคาเตือน (Warning Labels) ที่แถบหัวเรื่อง (Subject line) และในตัวเนื้อความของอีเมล (message body) โดยใส่เครื่องหมาย (Mark) หรือคาบอกกล่าว (Notice) ตามที่คณะกรรมการการค้าสหรัฐเป็นผู้กาหนด หรือต้องระบุในข้อความอีเมลว่าผู้รับจะสามารถรับชมได้ต่อเมื่อเปิดจดหมายเท่านั้น เพื่อเปิดช่องให้ผู้รับสามารถเลือกได้เองว่าจะงดเว้นการกระทาหรือไม่ รวมไปถึงต้องแสดงวิธีการบอกปฏิเสธรับ (opt-out) และที่อยู่ทางไปรษณีย์ของผู้ส่ง และวิธีการเข้าถึงเนื้อหาทางเพศที่อยู่ในอีเมลฉบับนั้น

2. หากผู้รับได้ให้และยืนยันความยินยอม (affirmative consent) ไว้ล่วงหน้าแล้ว ไม่จาเป็นต้องแสดงฉลากคาเตือน (Warning Labels) ที่แถบหัวเรื่อง (Subject line) ตามที่ระบุในข้อ1) ก็ได้

---

[29] CAN-SPAM Act, section 5 (b)

[30] CAN-SPAM Act, section 4 (d)(3) MULTIPLE. The term 'multiple' means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period

[31] CAN-SPAM Act, section 5 (d)

3. การแสดงเครื่องหมาย (Mark) และคาบอกกล่าว (Notice) ในอีเมลที่มีเนื้อหาทางเพศจะต้องกระทาภายใน 120 วัน นับตั้งแต่วันที่ 16 ธันวาคม 2003 เพื่อผู้รับสามารถทาการคัดกรอง (filter) จดหมายประเภทนี้ได้

บุคคลที่ฝ่าฝืนบทบัญญัติดังกล่าว จะมีโทษจาคุกไม่เกิน 5 ปี หรือปรับตามเรื่องที่ 18 แห่งประมวลกฎหมายแห่งสหรัฐอเมริกา (Title 18 of United State Code) หรือทั้งจ าทั้งปรับ

9) กาหนดให้มีการจัดตั้งหน่วยงานในการจัดทารายชื่อผู้ปฏิเสธไม่รับอีเมลเชิงพาณิชย์ (Do-Not-E-Mail registry)[32] ภายใน 6 เดือนหลังจากที่กฎหมายฉบับนี้มีผลบังคับใช้ คณะกรรมการจะต้องจัดส่ง “แผนการและกาหนดการในการก่อตั้งแผนกทะเบียนรายชื่อผู้ปฏิเสธไม่รับอีเมลเชิงพาณิชย์” “คาอธิบายถึงแนวทางในการปฏิบัติ มาตรการด้านเทคนิค ความปลอดภัย สิทธิความเป็นอยู่ส่วนบุคคล การบังคับใช้ หรือแนวทางอื่นๆที่เกี่ยวข้องในการขึ้นทะเบียน” และ “คาอธิบายแนวทางการนารายชื่อที่ลงทะเบียนไว้ปรับใช้กับที่อยู่อีเมลที่เป็นของเด็ก” ให้แก่วุฒิสภาที่เป็นคณะกรรมาธิการด้านพาณิชย์ วิทยาศาสตร์ และการคมนาคม และสภาผู้แทนราษฎรที่เป็นคณะกรรมาธิการด้านพลังงานและการพาณิชย์ ทั้งนี้ คณะกรรมการจะสามารถเพิ่มเติมแผนงานได้ภายใน 9 เดือนหลังจากที่ประกาศใช้กฎหมายฉบับนี้

4.2.6 หน้าที่ของภาคธุรกิจในใช้อีเมลเชิงพาณิชย์เพื่อโฆษณาประชาสัมพันธ์

มาตรา 6 บัญญัติให้บุคคลหรือธุรกิจมีหน้าที่ในการป้องกันไม่ให้เกิดการส่งอีเมลเชิงพาณิชย์ที่เป็นความผิด และมีหน้าที่ในการหามาตรการเพื่อตรวจจับและรายงานการส่งอีเมลเชิงพาณิชย์ที่เป็นความผิดให้แก่คณะกรรมการที่กากับดูแล โดยบุคคลใดที่ทาการสนับสนุนหรือยอมให้มีการประชาสัมพันธ์ในการค้า ธุรกิจ สินค้า ผลิตภัณฑ์ ทรัพย์สิน การให้บริการใดๆของตน เพื่อจุดประสงค์ทางการขาย การเช่า การเสนอให้เช่า หรือแม้แต่การกระทาอื่นใดที่เกี่ยวกับการค้าหรือธุรกิจนั้น ด้วยการใช้อีเมลเชิงพาณิชย์ที่ขัดต่อมาตรา 5(a)(1) โดยรู้หรือควรจะรู้ถึงการกระทาเช่นนั้น และได้รับหรือคาดว่าจะได้รับผลประโยชน์ทางการค้าจากการสนับสนุนให้มีการกระทาเช่นนั้น โดยปราศจากการป้องกันอย่างสมเหตุสมผล หรือไม่รายงานต่อคณะกรรมการที่กากับดูแลจะถือว่าเป็นผู้ร่วมกระท าความผิด

ส าหรับบุคคลที่สามที่เป็นผู้จัดหาสินค้า ผลิตภัณฑ์ ทรัพย์สิน การบริการ แก่บุคคลที่กระท าความผิดตามบทบัญญัติข้างต้นจะไม่ถือว่าเป็นผู้ที่มีส่วนสนับสนุนในการกระท าความผิด ยกเว้นกรณีที่บุคคลที่สามนั้น

1. เป็นผู้ที่มีผลประโยชน์ทางธุรกิจ หรือมีกรรมสิทธิ์ หรือมีความเป็นเจ้าของมากกว่า 50% ในการค้าหรือธุรกิจที่มีการกระท าผิด

2. เป็นผู้ที่มีความรู้ความเชี่ยวชาญในตัวสินค้า ผลิตภัณฑ์ ทรัพย์สิน การบริการ ที่ถูกน าไปใช้ประชาสัมพันธ์ทางอีเมลที่ผิดกฎหมายตามมาตรา 5(a)(1)

3. เป็นผู้ที่ได้รับหรือคาดว่าจะได้รับผลประโยชน์ทางการค้าจากการส่งเสริมให้ใช้อีเมลเชิงพาณิชย์นั้น

---

[32] CAN-SPAM Act, section 9

4.2.7 การกระทำที่เป็นความผิดตามกฎหมาย CAN-SPAM

มาตรา 4 (a) กำหนดให้ผู้กระทำ (Whoever) และผู้ร่วมกระทำความผิด (Conspires to do so) ที่มีการดำเนินการเพื่อใช้อีเมลเชิงพาณิชย์โดยมิชอบ ด้วยวิธีการดังต่อไปนี้

1) การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต และใช้ระบบคอมพิวเตอร์นั้นเพื่อการส่งผ่านอีเมลเชิงพาณิชย์จำนวนมาก (Multiple)

2) การใช้ระบบคอมพิวเตอร์แม่ข่ายของผู้อื่นในการส่ง (Relay) หรือส่งต่อข้อมูล (retransmit) อีเมลเชิงพาณิชย์จำนวนมาก (Multiple) ซึ่งมีจุดประสงค์เพื่อหลอกลวงหรือทำให้ผู้รับหรือผู้ให้บริการอินเทอร์เน็ตเข้าใจผิดในที่มาของอีเมลนั้น

3) การปลอมแปลงหรือบิดเบือนสาระสำคัญของหัวเรื่อง (Header) ของอีเมลเชิงพาณิชย์ และการจงใจส่งอีเมลที่มีการปลอมแปลงหัวเรื่องดังกล่าว

4) การใช้ข้อมูลระบุตัวตนที่เป็นเท็จเพื่อลงทะเบียนใช้งานอีเมล (e-mail account) หรือเปิดใช้บัญชีผู้ให้บริการออนไลน์ (Online user account) มากกว่า 5บัญชีขึ้นไป หรือเพื่อลงทะเบียนเปิดใช้ชื่อโดเมน (Domain Name) มากกว่า 2 ชื่อขึ้นไป และจงใจส่งอีเมลเชิงพาณิชย์โดยอีเมลหรือโดเมนดังกล่าวนั้น

5) การแอบอ้างเป็นผู้ลงทะเบียนหรือเป็นผู้รับสิทธิโดยชอบจากผู้ลงทะเบียนเลขที่อยู่ไอพี (Internet Protocol addresses: IP address) จำนวนมากกว่า 5 ที่อยู่ขึ้นไป และจงใจส่งอีเมลเชิงพาณิชย์โดยใช้งานเลขที่อยู่ไอพีดังกล่าว

4.2.8 บทลงโทษของการกระทำความผิดตามกฎมาย CAN-SPAM

มาตรา 4 (b) ได้บัญญัติถึงบทลงโทษของการกระทำความผิดไว้ดังต่อไปนี้

1) โทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับในกรณีที่

1. มีการกระทำผิด หรือมีส่วนร่วมในการดำเนินการใดๆที่เป็นการกระทำผิดตามกฎหมายอาญาของประเทศสหรัฐอเมริกาหรือของรัฐใด ๆ

2. จำเลยที่ถูกพิพากษาว่ามีความผิดตามมาตรา 1030 หรือภายใต้กฎหมายของรัฐใดๆ เกี่ยวกับการส่งอีเมลเชิงพาณิชย์หรือการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

2) โทษปรับหรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับในกรณีที่

1. การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต และใช้ระบบคอมพิวเตอร์นั้นเพื่อการส่งผ่านอีเมลเชิงพาณิชย์จำนวนมาก (Multiple)

2. การใช้ข้อมูลระบุตัวตนที่เป็นเท็จเพื่อลงทะเบียนใช้งานอีเมล (e-mail account) หรือเปิดใช้บัญชีผู้ให้บริการออนไลน์ (Online user account) มากกว่า 20 บัญชีขึ้นไป หรือเพื่อลงทะเบียนเปิดใช้ชื่อโดเมน (Domain Name) มากกว่า 10 ชื่อขึ้นไป

3. การส่งอีเมลเชิงพาณิชย์ที่เป็นความผิดตามกฎหมายนี้ จำนวนมากกว่า 2,500 ฉบับภายในเวลา 24 ชั่วโมง หรือมากกว่า 25,000 ฉบับ ในเวลา 30 วัน หรือมากกว่า 250,000 ฉบับ ในเวลา 1 ปี

4. การกระทาความผิดนั้นเป็นเหตุให้ผู้อื่นเกิดความเสียหายที่สามารถตีเป็นมูลค่าความเสียหายภายในระยะเวลา 1 ปีนั้นได้ ตั้งแต่ 5,000 เหรียญดอลลาร์สหรัฐขึ้นไป

5. ผู้กระทาผิดที่ได้รับผลประโยชน์จากการกระทาความผิดนั้นเป็นมูลค่ามากกว่า 5,000 เหรียญดอลลาร์สหรัฐขึ้นไปภายในระยะเวลา 1 ปี

6. จ าเลยที่เป็นผู้ก่อการ โดยมีผู้ร่วมกระท าความผิดตั้งแต่3 คนขึ้นไป

3) โทษปรับหรือจ าคุกไม่เกิน 1 ปี หรือทั้งจ าทั้งปรับในกรณีอื่นที่เหลือ

อย่างไรก็ตาม ศาลมีอ านาจในการริบทรัพย์ของจ าเลยที่ถูกพิพากษาว่ามีความผิด ทั้งสังหาริมทรัพย์และอสังหาริมทรัพย์ใดๆที่ตรวจสอบย้อนกลับได้ว่าได้มาจากการกระทาผิดดังกล่าว รวมไปถึงอุปกรณ์ เทคโนโลยี โปรแกรมคอมพิวเตอร์ที่ใช้หรือมีไว้เพื่อสนับสนุนให้เกิดการกระทาผิดด้วย อีกทั้ง คณะกรรมการด้านการกาหนดโทษของสหรัฐอเมริกา (United States Sentencing Commission: U.S.S.C) มีอ านาจในการพิจารณาทบทวนหลักเกณฑ์การพิจารณาและนโยบายเพื่อให้บทลงโทษที่เหมาะสมต่อการกระท าผิด2 ฐาน ดังต่อไปนี้

1. การรวบรวมหรือได้มาซึ่งที่อยู่อีเมลของผู้รับโดยมิชอบ ได้แก่ การรวบรวมที่อยู่อีเมลด้วยวิธีอัตโนมัติจากเว็บไซต์หรือบริการออนไลน์ใดๆที่ดาเนินการโดยบุคคลอื่น (address harvesting) และ การสุ่มที่อยู่อีเมลของผู้รับโดยเรียงลาดับตามตัวอักษรอัตโนมัติ (randomly generating e-mail address)

2. ผู้กระทาผิดทราบอยู่แล้วว่าอีเมลเชิงพาณิชย์นั้นมีเนื้อหาที่ขัดต่อกฎหมาย หรือมีการโฆษณาโดเมนที่ถูกจดขึ้นมาด้วยข้อมูลเท็จ

4.3 กฎหมายต่อต้านการกระท าความผิดเกี่ยวกับสแปมในสหภาพยุโรป

ระบบกฎหมายในสหภาพยุโรปมีลักษณะที่แตกต่างไปจากประเทศอื่นเล็กน้อย เนื่องจากสหภาพยุโรปเกิดจากการรวมตัวกันของประเทศสมาชิกจานวน 27 ประเทศ ดังนั้นแต่ละประเทศจึงมีกฎหมายภายในเป็นของตนเองกันอยู่ก่อนแล้ว และมีหลักเกณฑ์ร่วมแห่งสหภาพเข้ามาเป็นกรอบในการก าหนดทิศทางการบังคับใช้กฎหมายทั้งภายในประเทศและระหว่างประเทศสมาชิกอีกขั้นนึง โดยหลักเกณฑ์ที่ว่านี้จะแบ่งออกเป็น “กฎ” (Regulation) และ “ระเบียบ” (Directive) โดย “กฎ” จะมีอานาจบังคับใช้เช่นเดียวกับกฎหมาย ซึ่งจะมีผลผูกพันธ์กับทุกประเทศสมาชิกทันทีที่มีการบังคับใช้ แต่ “ระเบียบ” จะมีผลผูกพันธ์กับประเทศสมาชิกก็ต่อเมื่อประเทศสมาชิกนั้นยินยอมที่จะนาเข้ามาใช้[33]

สหภาพยุโรปได้บัญญัติกฎหมายต่อต้านกระทาความผิดเกี่ยวกับสแปมในรูปแบบของ “ระเบียบ”(Directives) โดยประเทศสมาชิกสามารถตัดสินใจเพื่อเลือกนามาบังคับใช้ในประเทศของตนได้ ซึ่งระเบียบที่สามารถนามาปรับใช้กับการกระทาความผิดในรูปแบบสแปมเมลได้มี 4 ระเบียบ

[33] สราวุธ ปิติยาศักดิ์. กฎหมายเทคโนโลยีสารสนเทศ. ส านักพิมพ์นิติธรรม, 2555. หน้า 323.

ได้แก่ ระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Directive 95/46/EC) ระเบียบว่าด้วยสิทธิส่วนบุคคลในระบบโทรคมนาคม (Telecommunications Privacy Directives 97/66/EC) ระเบียบว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ (E-Commerce Directive 2000/31/EC) และระเบียบว่าด้วยความเป็นส่วนตัวทางอิเล็กทรอนิกส์ (E-Privacy Directive 2002/58/EC)

4.3.1 ระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Directive 95/46/EC)

ระเบียบฉบับนี้ออกมาในวันที่ 24 ตุลาคม 1995 โดยมีจุดประสงค์เพื่อกาหนดหลักเกณฑ์ในการใช้งานข้อมูลส่วนบุคคล และเสริมสร้างให้เกิดความอิสระทางการเคลื่อนไหวของข้อมูล และป้องกันการรวบรวมข้อมูลเพื่อนาไปใช้ในทางมิชอบ เพื่อก่อให้เกิดความสัมพันธ์อันดีระหว่างประชาชนในแต่ละประเทศสมาชิก ขจัดอุปสรรคที่เป็นกาแพงระหว่างประเทศสมาชิก พร้อมทั้งคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานของประชาชน[34] โดยมาตรา 2 ได้มีการก าหนดนิยามของ “ข้อมูลส่วนบุคคล” (Personal Data) หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาที่ระบุหรือสามารถระบุตัวตนของเจ้าของได้ ทั้งทางตรงและทางอ้อมโดยเฉพาะโดยอ้างถึง หมายเลขประจาตัว ปัจจัยที่เฉพาะเจาะจงไม่ว่าจะเป็นทางร่างกาย จิตใจ สรีระ สถานะทางเศรษฐกิจ วัฒนธรรม หรืออัตลักษณ์ทางสังคม กล่าวคือ ชื่อ ที่อยู่ เบอร์โทรศัพท์ที่อยู่อีเมล เชื้อชาติ ศาสนา วันเกิด ตาแหน่งงาน สถานที่ทางาน เลขที่บัญชีธนาคาร ฯลฯ ต่างก็ถูกคุ้มครองในฐานะข้อมูลส่วนบุคคลทั้งสิ้น และมีการกาหนดหลักปฏิบัติในการใช้งานข้อมูลส่วนบุคคล (Principles Relating to Data Quality)[35] ไว้ในมาตรา 6 ดังต่อไปนี้

1) ต้องมีการประมวลผล (processing) ข้อมูลอย่างเป็นธรรมและชอบด้วยกฎหมาย

2) การรวบรวมข้อมูลจะต้องทาโดยจุดประสงค์ที่ชอบด้วยกฎหมาย ชัดเจนและเป็นการเฉพาะเจาะจง และไม่นาข้อมูลที่ได้มานั้นไปใช้ประมวลผลเพื่อจุดประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่กาหนดไว้ เว้นแต่จะเป็นการประมวลผลด้วยวัตถุประสงค์ทางวิทยศาสตร์ สถิติ หรือประวัติศาสตร์ในประเทศสมาชิกที่มีมาตรการปกป้องข้อมูลที่เหมาะสมแล้ว

3) มีมาตรการการจัดการข้อมูลเพียงพอ และไม่มีการใช้งานเกินขอบเขตวัตถุประสงค์ในการเก็บรวบรวมหรือการประมวลผล

4) ข้อมูลมีความถูกต้องและต้องมีการอัพเดทในกรณีที่จาเป็น และมีมาตรการที่เหมาะสมในการลบหรือแก้ไขข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์ เพื่อประโยชน์ในการเก็บรวมรวมข้อมูลหรือการประมวลผลเพิ่มเติม

5) จัดเก็บด้วยรูปแบบที่ยังสามารถแยกแยะระบุตัวเจ้าของข้อมูลได้ตามระยะเวลาที่จาเป็นซึ่งสอดคล้องกับจุดประสงค์ในการเก็บรวบรวม และประเทศสมาชิกจะต้องจัดหามาตรการที่

---

[34] Directive 95/46/Ec of the European Parliament and of the Council of 24 October 1995. [Online]. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [6 April 20118.]

[35] Data Protection Directive 95/46/EC, section I, article 6

เหมาะสมในการปกป้องข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้นั้นให้นานขึ้นหากเพื่อเป็นประโยชน์ด้านวิทยาศาสตร์ สถิติ หรือประวัติศาสตร์

อย่างไรก็ตาม เจ้าของข้อมูลต้องทราบถึงวัตถุประสงค์ในการจัดเก็บหรือการประมวลผลข้อมูล และการประมวลผลจะต้องทาเพียงเท่าที่จาเป็นตามวัตถุประสงค์ในสัญญาที่ทาไว้กับเจ้าของข้อมูล หรือเป็นการปฏิบัติหน้าที่ตามที่กฎหมายในฐานะผู้ครอบครองข้อมูล หรือเพื่อปกป้องผลประโยชน์ของเจ้าของข้อมูลเท่านั้น และเจ้าของข้อมูลมีสิทธิ์คัดค้านในการนาข้อมูลของตนไปใช้เพื่อวัตถุประสงค์ด้านการตลาดแบบตรง หรือปฏิเสธการถูกเปิดเผยข้อมูลผู้ต่อบุคคลที่สามด้วยจุดประงสงค์ในการท าการตลาดแบบตรงได้

ดังนั้น จึงสรุปได้ว่าระเบียบฉบับนี้เป็นการคุ้มครองตั้งแต่ต้นน้า เนื่องจากกาหนดให้ต้องขอความยินยอมตั้งแต่ขั้นกระบวนการเก็บรวมรวมข้อมูล ตลอดจนไปถึงต้องได้รับความยินยอมจากผู้รับก่อนทาการส่งอีเมลเชิงพาณิชย์ (Opt-in) โดยผู้ส่งมีสิทธิเพียงเป็นฝ่ายเริ่มส่งคาร้องขอในการขอเก็บรวบรวมข้อมูล หรือขออนุญาตส่งอีเมลเชิงพาณิชย์ให้ผู้รับได้พิจารณาให้ความยินยอมเท่านั้น จึงจะไม่ถือว่าเป็นการละเมิดสิทธิของผู้รับ ซึ่งการให้ความคุ้มครองในสิทธิของข้อมูลส่วนบุคคลนี้ ทาให้กลุ่มประเทศในสหภาพยุโรปสามารถปกป้องประชาชนจากการรุกรานของสแปมเมลได้อย่างมีประสิทธิภาพ

4.3.2 ระเบียบว่าด้วยสิทธิส่วนบุคคลในระบบโทรคมนาคม (Telecommunications Privacy Directives 97/66/EC)

ระเบียบฉบับนี้ออกมาในวันที่ 15 ธันวาคม 1997 โดยมีสาระสาคัญที่เกี่ยวข้องกับการปกป้องสิทธิของผู้บริโภคในมาตรา 12 ที่กาหนดหลักเกณฑ์การใช้โทรศัพท์อันไม่พึงประสงค์ (Unsolicited calls) โดยวัตถุประสงค์เพื่อท าการตลาดแบบตรง (Direct Marketing) ไว้ดังนี้

1) การใช้ระบบโทรศัพท์ตอบรับอัตโนมัติ (automatic calling machines) หรือเครื่องโทรสาร (fax) เพื่อวัตถุประสงค์ในการทาตลาดทางตรงจะต้องได้รับความยินยอมจากผู้รับก่อนล่วงหน้าเท่านั้น

2) ประเทศสมาชิกจะต้องมีมาตรการที่เหมาะสมเพื่อให้มั่นใจได้ว่า ผู้บริโภคจะไม่เกิดภาระค่าใช้จ่ายจากการรับโทรศัพท์ที่มีวัตถุประสงค์เพื่อการตลาดแบบตรง และการสื่อสารทางโทรศัพท์รูปแบบนี้จะไม่เกิดขึ้นโดยปราศจากความยินยอมจากผู้ใช้บริการที่เกี่ยวข้อง หรือความไม่ยินยอมจากผู้รับบริการที่ไม่ต้องการรับสายเหล่านี้ โดยให้แต่ละประเทศเลือกใช้หลักเกณฑ์จากสองตัวเลือกนี้เอง

3) สิทธิดังกล่าวสามารถใช้บังคับแก่ผู้บริโภคที่เป็นบุคคลธรรมดา ประเทศสมาชิกจะต้องรับรองได้ว่าในกฎหมายที่บังคับใช้ในประเทศของตนมีความสอดคล้องกับระเบียบปฏิบัติแห่งชาตินี้ เพื่อให้บุคคลได้รับการปกป้องจากโทรศัพท์ไม่พึงประสงค์อย่างชอบธรรมตามกฎหมาย

กล่าวได้ว่า ระเบียบปฏิบัติฉบับนี้เป็นอีกหนึ่งมาตราฐานที่สะท้อนให้เห็นว่าประเทศในกลุ่มสหภาพยุโรปให้ความสาคัญกับสิทธิขั้นพื้นฐานของผู้บริโภคมากกว่าการอานวยความสะดวก

ด้านการโฆษณาของภาคธุรกิจ เพราะหลัก Opt-in ยังคงถูกนามาใช้กับการสื่อสารทางโทรศัพท์ด้วยเช่นกัน

4.3.3 ระเบียบว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ (E-Commerce Directive 2000/31/EC)

ระเบียบฉบับนี้ออกมาในวันที่ 8 มิถุนายน 2000 เพื่อกาหนดหลักเกณฑ์ทางกฎหมายด้านการพาณิชย์อิเล็กทรอนิกส์ เพื่อสนับสนุนการตลาดภายในประเทศสมาชิกและเสริมสร้างความมั่นใจในเสรีภาพของการแลกเปลี่ยนข้อมูลจากการบริการในสังคมสารสนเทศ โดยมาตราที่เกี่ยวข้องกับปัญหาสแปมเมลคือมาตรา 7 ว่าด้วยเรื่อง “การสื่อสารเชิงพาณิชย์อันไม่พึงประสงค์” (Unsolicited Commercial Communication) โดยอนุญาตให้แต่ละประเทศสมาชิกสามารถอนุญาตให้มีการใช้อีเมลในการสื่อสารเชิงพาณิชย์อันไม่พึงประสงค์ได้ เพียงแต่ต้องมีมาตรการในการตรวจสอบให้แน่ใจว่าผู้ให้บริการการสื่อสารในประเทศของตนทาการสื่อสารเชิงพาณิชย์ดังกล่าว ด้วยวิธีการที่ถูกต้องตามกฎหมาย ซึ่ง ณ ขณะที่อีเมลนั้นไปถึงผู้รับ ผู้รับจะสามารถระบุตัวตนของผู้ส่งได้ชัดเจน ไม่คลุมเครือ อีกทั้งประเทศที่อนุญาตให้มีการส่งอีเมลเชิงพาณิชย์อันไม่พึงประสงค์นี้ ยังต้องมีมาตรการบังคับให้ผู้ให้บริการมีหน้าที่ให้คาปรึกษาและจัดหาวิธีลงทะเบียนปฏิเสธไม่รับอีเมล (Opt-out registers) ให้แก่ผู้รับด้วยเช่นกัน

นับเป็นครั้งแรกที่สหภาพยุโรปนามาตรการ Opt-out เข้ามาปรับใช้กับระเบียบด้านการบริการข้อมูลออนไลน์ เนื่องจากในยุคนั้นอีเมลเริ่มเข้ามามีบทบาทในฐานะเครื่องมือสาคัญในการท าการตลาด ระเบียบฉบับนี้จึงเป็นการเปิดโอกาสให้ประเทศสมาชิกที่ต้องการใช้ประโยชน์จากการส่งอีเมลรูปแบบนี้มีเสรีในดาเนินการได้มากขึ้น เพียงแต่ต้องมีวัตถุประสงค์ในการส่งและการระบุตัวตนของผู้ส่งที่ชัดเจนเพื่อให้ผู้รับสามารถเลือกปฏิเสธรับได้

4.3.4 ระเบียบว่าด้วยความเป็นส่วนตัวทางอิเล็กทรอนิกส์ (E-Privacy Directive 2002/58/EC)

ระเบียบฉบับนี้ออกมาในวันที่ 12 กรกฎาคม 2002 โดยเป็นระเบียบที่มีความเกี่ยวข้องกับปัญหาสแปมเมลมากที่สุด สาระสาคัญของระเบียบฉบับนี้กล่าวถึงเรื่องการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้งาน (Internet User) ที่ถูกนาไปใช้บนเครือข่ายอิเล็กทรอนิกส์โดยตรง เนื่องจากการขยายตัวอย่างรวดเร็วของการตลาดบนอินเทอร์เน็ตส่งผลกระทบมากมายต่อตัวผู้บริโภค สหภาพยุโรปจึงต้องออกระเบียบฉบับนี้ขึ้นมาเพื่อขยายขอบเขตการคุ้มครองจากมาตรา 12 ของระเบียบว่าด้วยสิทธิส่วนบุคคลในระบบโทรคมนาคม (Telecommunications Privacy Directives) ให้ครอบคลุมถึงการสื่อสารทางอิเล็กทรอนิกส์ทุกประเภท และให้มีความสอดคล้องกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 2 ของระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Directive)

มาตรา 13 ของระเบียบฉบับนี้ ได้ระบุหลักเกณฑ์เกี่ยวกับ “การสื่อสารที่ไม่พึงประสงค์” (Unsolicited communications) ไว้ดังนี้

1) การใช้ระบบโทรศัพท์แบบอัตโนมัติโดย (automatic calling machines) เครื่องโทรสาร (fax) หรือจดหมายอิเล็กทรอนิกส์ (e-mail) เพื่อจุดประสงค์ในการทาการตลาดแบบตรงจะต้องได้รับการยินยอมจากผู้ใช้บริการก่อนล่วงหน้าเท่านั้น

2) กรณีที่บุคคลธรรมดาหรือนิติบุคคลได้รับข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์ของผู้บริโภคมา ณ เวลาที่มีการซื้อขายสินค้าหรือบริการตามที่กาหนดไว้ในระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Directive) บุคคลนั้นสามารถนาข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์ดังกล่าวไปใช้ทาการตลาดแบบตรงของสินค้าหรือบริการที่มีลักษณะคล้ายคลึงกับของเดิมได้ เพียงแต่ต้องมีการระบุมาตรการในการบอกปฏิเสธรับ (Opt-out) ไว้อย่างชัดเจน ปฏิบัติตามได้ง่าย และปราศจากค่าใช้จ่ายเพิ่มเติม

3) ประเทศสมาชิกจะต้องมีมาตรการที่เหมาะสมเพื่อให้มั่นใจได้ว่า ผู้บริโภคจะไม่เกิดภาระค่าใช้จ่ายจากการสื่อสารที่ไม่พึงประสงค์เพื่อการตลาดแบบตรงนี้ และการสื่อสารรูปแบบนี้จะไม่เกิดขึ้นโดยปราศจากความยินยอมจากผู้ใช้บริการที่เกี่ยวข้อง หรือความไม่ยินยอมจากผู้รับบริการที่ไม่ต้องการบอกรับ โดยให้แต่ละประเทศเลือกใช้หลักเกณฑ์จากสองตัวเลือกนี้เอง

4) ห้ามส่งอีเมลเพื่อจุดประสงค์ในการทาการตลาดแบบตรง โดยปลอมแปลงหรือปิดบังข้อมูลในการระบุตัวตนของผู้ส่ง หรือโดยไม่มีการระบุที่อยู่ที่ถูกต้องเพื่อให้ผู้รับสามารถติดต่อกลับได้

5) วรรค 1 และ 3 ให้ใช้บังคับกับบุคคลธรรมดา โดยประเทศสมาชิกจะต้องตรวจสอบกฎหมายภายในของประเทศตน ว่ามีการคุ้มครองผลประโยชน์อันชอบด้วยกฎหมายของบุคคลธรรมดานั้นว่าครอบคลุมถึงการป้องกัน “การสื่อสารอันไม่พึงประสงค์” (Unsolicited communications) อย่างเพียงพอหรือไม่

จะเห็นได้ว่ามาตรานี้กาหนดห้ามไม่ให้มีการใช้อีเมลเพื่อจุดประสงค์ทางการตลาดแบบตรงเว้นแต่จะได้คายินยอมล่วงหน้าจากผู้รับเสียก่อน ซึ่งถือเป็นการย้าจุดยืนในการปกป้องสิทธิส่วนบุคคลของผู้บริโภคด้วยหลักการ Opt-in อีกครั้ง ยิ่งไปกว่านั้น ถึงภาคธุรกิจจะมีสิทธิในการเก็บรวมรวมที่อยู่ทางอิเล็กทรอนิกส์ของผู้บริโภคเพื่อประโยชน์ในการทาการตลาด แต่ก็จะสามารถ น าไปใช้ได้กับลูกค้าที่ไม่บอกปฏิเสธเท่านั้น

4.4 สรุปความแตกต่างของหลักเกณฑ์ในการบังคับใช้มาตรการต่อต้านการกระทาความผิดเกี่ยวกับสแปมในสหรัฐอเมริกาและสหภาพยุโรป

ทั้งในสหรัฐอเมริกาและสหภาพยุโรปต่างก็ตระหนักถึงความสาคัญในการหามาตรการทางกฎหมายเข้ามารองรับปัญหาสแปมเมล แต่เนื่องจากแนวนโยบายในการบริหารประเทศที่แตกต่างกันทาให้กฎหมายที่เกี่ยวกับการควบคุมและปราบปรามสแปมเมลของทั้งสองประเทศจึงมีหลักเกณฑ์ที่แตกต่างกัน ดังที่จะสรุปในตารางต่อไปนี้

ตารางที่ 2 สรุปความแตกต่างของหลักเกณฑ์ในการบังคับใช้กฎหมายต่อต้านการกระทาความผิดเกี่ยวกับสแปมเมลในสหรัฐอเมริกาและสหภาพยุโรป

หัวข้อ	สหรัฐอเมริกา	สหภาพยุโรป
ประเภทของสแปม	CAN-SPAM จะใช้บังคับกับอีเมลเชิงพาณิชย์ที่มีวัตถุประสงค์หลักเพื่อโฆษณาหรือประชาสัมพันธ์สินค้าหรือบริการเชิงพาณิชย์เท่านั้น	E-Privacy Directive จะใช้บังคับกับอีเมลที่มีจุดประสงค์ในการท าการตลาดแบบตรง รวมถึงข้อความที่เกี่ยวกับการกุศลและการเมืองด้วย[36]
ค านิยามของสแปม	อีเมลเชิงพาณิชย์ที่ไม่ได้ถูกร้องขอ (Unsolicited Commercial e-mail)	การสื่อสารที่ไม่พึงประสงค์เพื่อจุดประสงค์ในการท าการตลาดแบบตรง (Unsolicited communications for the purposes of direct marketing)[37]
ขอบเขตการคุ้มครอง	การสื่อสารทางอีเมลในทุกระดับ	การสื่อสารบนระบบอิเล็กทรอนิกส์ทั้งหมด ไม่ว่าจะเป็น ระบบโทรศัพท์แบบอัตโนมัติ เครื่องโทรสาร หรืออีเมล ฯลฯ ที่เป็นระดับธุรกิจต่อบุคคลธรรมดา (Business-to-Consumer: B2C) ไม่ครอบคลุมถึงระดับธุรกิจต่อธุรกิจ (Business-to-Business: B2B)
สิทธิในการฟ้องร้องทางแพ่ง	ไม่มีระบุ	บุคคลธรรมดาที่เป็นผู้เสียหายสามารถท าการฟ้องร้องได้เองโดยอิสระ[38]
การระบุที่อยู่ทางไปรษณีย์ของผู้ส่ง	ต้องระบุที่อยู่ทางไปรษณีย์ที่สามารถติดต่อได้จริง	ต้องระบุที่อยู่ทางไปรษณีย์ที่สามารถติดต่อได้จริง และหากผู้ส่งเป็นภาคธุรกิจจะต้องระบุชื่อบริษัท ประเภทของ

[36] สราวุธ ปิติยาศักดิ์. กฎหมายเทคโนโลยีสารสนเทศ. หน้า 328-329.

[37] E-Privacy Directive 2002/58/EC, Article 13

[38] E-Privacy Directive 2002/58/EC, Article 15 (2) the provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

Data Protection Directive 95/46/EC, Article 22 without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

		กิจการ เลขที่จดทะเบียน และเลขภาษีมูลค่าเพิ่ม[39]
หลักเกณฑ์ในการส่งสแปมเมล	- ผู้ส่งต้องระบุช่องทางเพื่อการปฏิเสธรับ (Opt-out) อย่างชัดเจน และต้องยุติการส่ง หลังจากที่ได้รับคำร้องขอเพื่อปฏิเสธการรับ(Opt-out notification) ภายใน 10 วันทำการ - ต้องมีการแสดงฉลากคำเตือน (Warning Labels) ที่แถบหัวเรื่องในกรณีที่มีเนื้อหาลามกอนาจาร - ห้ามใช้หัวเรื่องเท็จหรือทำให้เข้าใจผิดในสาระสำคัญของอีเมล - ต้องสามารถระบุแหล่งที่มา เช่น โดเมนต้นทาง ที่อยู่อีเมลของผู้ส่งต้นทาง ฯลฯ ที่สามารถบ่งชี้ถึงตัวตนของผู้ส่งที่แท้จริงได้ - ห้ามใช้ระบบคอมพิวเตอร์แม่ข่ายของผู้อื่นในการส่ง (Relay) หรือส่งต่อข้อมูล (retransmit) - ห้ามเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาตเพื่อทำการส่งอีเมลเชิงพาณิชย์จำนวนมาก (Multiple) - ห้ามเปิดใช้ชื่อโดเมนมากกว่า 2 ชื่อขึ้นไปเพื่อจงใจส่งอีเมลเชิงพาณิชย์ - ห้ามเปิดใช้บัญชีผู้ให้บริการออนไลน์ (Online user account) มากกว่า 5 บัญชีขึ้นไป เพื่อการส่งอีเมลเชิงพาณิชย์	- ผู้ส่งต้องได้รับความยินยอมล่วงหน้าจากผู้รับ (Opt-in) - ต้องมีการระบุช่องทางเพื่อการปฏิเสธรับ (Opt-out) และที่อยู่ทางไปรษณีย์ที่ติดต่อได้ของผู้ส่งในอีเมลที่มีเนื้อหาเกี่ยวกับการตลาดแบบตรง - ห้ามปลอมแปลงหรือปกปิดตัวตนของผู้ส่ง

[39] E-Commerce Directive 2000/31/EC, Article 5 (d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register.

หลักเกณฑ์ในการนำที่อยู่อีเมลของผู้บริโภคไปใช้งานเพื่อจุดประสงค์อื่น	กระทำได้หากอีเมลถูกส่งโดยชอบด้วยกฎหมายฉบับนี้	นำไปใช้ได้เฉพาะภายในขอบเขตตามวัตถุประสงค์ที่ระบุไว้แต่แรกเท่านั้น เว้นแต่จะนำข้อมูลที่อยู่อีเมลของผู้รับที่ได้มาจากการทำธุรกรรมซื้อขายไปใช้เพื่อส่งอีเมลโฆษณาสินค้าลักษณะเดียวกัน และระบุสิทธิและช่องทางในการปฏิเสธรับ (Opt-out) ในอีเมลให้ชัดเจน[40]

ตารางเปรียบเทียบขั้นต้นทำให้เห็นได้ชัดเจนว่าแนวนโยบายในการบริหารของรัฐทั้งสองประเทศมีความแตกต่างกัน โดยในสหรัฐอเมริกาเน้นให้ความสำคัญกับ “สังคมประชาธิปไตย” และอิสรภาพในการแสดงออกภายใต้บทบัญญัติของ First Amendment ตามที่บัญญัติในรัฐธรรมนูญ แต่สหภาพยุโรปให้ความสำคัญกับการปกป้องสิทธิในความเป็นส่วนตัว (Private life) ของประชาชนมตามบทบัญญัติในอนุสัญญาว่าด้วยสิทธิมนุษยชนยุโรปมาตรา 8 ว่าด้วยเรื่องของสิทธิเกี่ยวกับชีวิตส่วนบุคคลและครอบครัว (The European Convention on Human Rights Article 8)[41] มากกว่า ดังนั้นกฎหมายที่เกี่ยวกับการควบคุมและปราบปรามสแปมเมลของทั้งสองประเทศจึงมีหลักเกณฑ์ที่แตกต่างกันอย่างชัดเจน

เมื่อพิจารณาถึงกฎหมายที่บังคับใช้ในประเทศไทย พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ได้นำเอาหลัก Opt-out เข้ามาใช้เป็นหลักเกณฑ์เพื่อควบคุมการทำการตลาดด้วยวิธีการส่งอีเมลเช่นเดียวกับประเทศสหรัฐอเมริกา และมีการปรับปรุงบทบัญญัติให้ครอบคลุมถึงการส่งข้อมูลโฆษณาบนสื่อสังคมออนไลน์ (Social Media) หรือบริการแอปพลิเคชัน (Application) ต่างๆด้วย แต่หลักเกณฑ์ดังกล่าวจะมีประสิทธิภาพเพียงพอในการลดปริมาณข้อความโฆษณาอันไม่พึงประสงค์ที่อยู่บนระบบสารสนเทศในประเทศไทยได้หรือไม่ ในบทถัดไปจะทำการวิเคราะห์การบังคับใช้พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ในประเทศไทยต่อไป

[40] สราวุธ ปิติยาศักดิ์. กฎหมายเทคโนโลยีสารสนเทศ. หน้า 330.

[41] The European Convention on Human Rights Article 8 Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

บทที่ 5
วิเคราะห์มาตรการในการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ในประเทศไทย

ประเทศไทยเป็นประเทศที่มีระบบเศรษฐกิจแบบทุนนิยม ภาครัฐจึงมีหน้าที่ในการสร้างนโยบายเพื่อสนับสนุนให้เกิดตลาดการแข่งขันเสรี ไม่ว่าจะเป็นตลาดในประเทศหรือระหว่างประเทศ โดยเฉพาะในยุคปัจจุบันที่เทคโนโลยีถูกพัฒนาขึ้นมาในหลายรูปแบบเพื่อตอบสนองต่อวิถีการใช้ชีวิตของผู้คนในสังคมให้เกิดความสะดวกสบาย จนปฏิเสธไม่ได้ว่าเทคโนโลยีกลายเป็นส่วนหนึ่งในชีวิตประจำวันของทุกคนไปแล้ว แต่ในทางกลับกันการใช้เพื่อติดต่อสื่อสารข้อมูลให้สะดวกรวดเร็วมากขึ้นเท่าไหร่ วิจารณญาณในการกลั่นกรอง ทบทวน ข้อมูลเหล่านั้นยิ่งมีน้อยลง ผู้บริโภคมีแนวโน้มว่าจะรับเอาข้อมูลเท็จและเชื่อโดยไม่ตรวจสอบให้แน่ชัดมากขึ้น เทคโนโลยีที่ซับซ้อนทำให้การหลอกลวงบนอินเทอร์เน็ตเกิดขึ้นได้อย่างแนบเนียนและน่าเชื่อถือ อีกทั้งการเข้าถึงข้อมูลส่วนบุคคลของผู้บริโภคทำได้ง่ายขึ้น จนมีความเสี่ยงที่สิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภคจะถูกรบกวนเกินขอบเขตที่เหมาะสม ผู้บริโภคจำนวนมากถูกนักการตลาดรบกวนโดยการส่งอีเมลโฆษณาเข้ามาหาโดยที่ตนไม่ได้มีความต้องการ หรือมิจฉาชีพจำนวนมากใช้ช่องทางอีเมลในการส่งข้อมูลไปหลอกลวงผู้บริโภค ดังนั้น ปัญหาการเกี่ยวกับการส่งสแปม จึงกลายเป็นปัญหาสำคัญที่ภาครัฐทั่วโลกต้องเข้ามากำกับดูแล เพื่อให้เกิดประสิทธิภาพในการใช้ทรัพยากรสารสนเทศบนอินเทอร์เน็ต (Internet Resource) ปกป้องคุ้มครองสิทธิความเป็นอยู่ส่วนบุคคลของประชาชนในประเทศ (Rights of Privacy) รักษาความสงบเรียบร้อยและศีลธรรมอันดีในสังคม ผลักดันให้เกิดความเสมอภาคและเสรีในการดำเนินกิจกรรมทางเศรษฐกิจ โดยในบทนี้จะบรรยายถึงหลักเกณฑ์ในการพิจารณาการกระทำผิดเกี่ยวกับสแปมในประเทศไทยเปรียบเทียบกับกฎหมายต่างประเทศตามหัวข้อที่ 5.1 และข้อที่นักการตลาดพึงระวังในการใช้อีเมลเชิงพาณิชย์เพื่อทำการตลาดในหัวข้อ 5.2 และการคุ้มครองสิทธิความเป็นอยู่ส่วนบุคคล (Rights of privacy) ของผู้บริโภคในหัวข้อ 5.3

5.1 หลักเกณฑ์พิจารณาการกระทำความผิดเกี่ยวกับสแปม (spam)

การกระทำความผิดฐานส่งอีเมลที่เป็นการรบกวนผู้อื่น (spam mail) โดยทั่วไปสามารถแบ่งได้เป็น 2 ลักษณะ ได้แก่ อีเมลเชิงพาณิชย์เพื่อการโฆษณา (commercial spam) ที่ก่อให้เกิดความเดือดร้อนราคาญต่อผู้รับ และอีเมลที่ใช้เป็นเครื่องมือในการก่ออาชญากรรม[1] โดยประเทศไทยมีบทบัญญัติทางกฎหมายที่เกี่ยวข้องกับเรื่องนี้มีระบุใน พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ มาตรา 11 ซึ่งได้จำแนกองค์ประกอบความผิดไว้โดยแบ่งเป็น องค์ประกอบภายนอก ได้แก่ “การปกปิดแหล่งที่มาในการส่งข้อมูล” และ “อันเป็นการรบกวนการใช้งานระบบคอมพิวเตอร์

[1] มานิตย์ จุมปา. คำอธิบายกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์. พิมพ์ครั้งที่ 2. ศูนย์หนังสือกฎหมายวิญญูชน, 2554. หน้า 82-84.

ของบุคคลอื่นโดยปกติสุข” และ“การไม่เปิดโอกาสให้ผู้รับบอกเลิกได้โดยง่าย” และองค์ประกอบภายในได้แก่ “เจตนา” หากขาดองค์ประกอบใดองค์ประกอบหนึ่งไปจะไม่สามารถเอาโทษได้

องค์ประกอบประการแรก “การปกปิดแหล่งที่มาในการส่งข้อมูล” ในประเทศไทยหมายถึง การปลอมแปลงหรือปกปิดเลขที่อยู่ไอพี (Internet Protocol address : IP Address) เพื่อป้องกันไม่ให้สามารถตรวจสอบข้อมูลการจราจรทางคอมพิวเตอร์ (Traffic) ย้อนไปถึงที่อยู่ของผู้ส่งได้[2] นั้น ซึ่งหากมองจากมุมของปุถุชนทั่วไป ผู้รับมักจะดูเพียงรายละเอียดเบื้องต้น เช่น ที่อยู่อีเมล ชื่อบริษัท หรือรายละเอียดอื่นๆที่สามารถมองเห็นได้โดยง่ายมากกว่า น้อยคนที่จะตรวจสอบลึกไปถึง IP Address ของผู้ส่งเพื่อดูว่าเป็นของปลอมหรือไม่ บทบัญญัตินี้จึงมีประโยชน์เฉพาะกับเวลาสืบสวนหลังจากที่เกิดการร้องเรียนจากผู้เสียหายแล้วเท่านั้น ไม่ได้เป็นการป้องกันตั้งแต่ต้นน้ำที่จะไม่ให้ผู้รับเปิดอ่าน และไม่สามารถคุ้มครองสิทธิผู้บริโภคในการรับรู้ข้อมูลที่เป็นสาระสำคัญของตัวผู้ส่งที่ควรกระทำได้โดยง่าย เพราะหากเป็นสินค้าทั่วไปผู้บริโภคจะได้รับการคุ้มครองสิทธิในการรับรู้ข้อมูลโดยพระราชบัญญัติคุ้มครองผู้บริโภค ที่ควบคุมให้ผู้ผลิตต้องแสดงฉลาก ที่ระบุทั้งรายละเอียดของตัวผลิตภัณฑ์และรายละเอียดของผู้ผลิตอย่างเช่น ชื่อบริษัท ที่อยู่ เบอร์โทรศัพท์ เพื่อให้ผู้รับสามารถติดต่อได้โดยง่าย[3] ผู้รับอีเมลจึงควรมีสิทธิในการรับรู้ข้อมูลเบื้องต้นเพื่อตัดสินใจเปิดรับเท่าเทียมกับผู้บริโภคที่ได้รับข้อมูลก่อนทำการตัดสินใจซื้อสินค้าเช่นกัน มาตรฐานในการแสดงฉลากจึงไม่ควรจำกัดอยู่แค่บนสินค้าปกติ การส่งอีเมลเชิงพาณิชย์ที่เป็นส่วนหนึ่งของการโฆษณาก็ควรมีบทบัญญัติเข้ามาควบคุมด้านฉลากหรือหัวจดหมาย (Heading) ให้มีการแสดงชื่อเรื่อง (subject) ที่สื่อถึงเนื้อหาที่เป็นสาระสำคัญของอีเมลนั้น และมีการแสดงตัวตนของผู้ส่งที่แถบผู้ส่ง (from line) อย่างชัดเจน เพื่อให้ผู้รับสามารถพิจารณาได้แต่แรกเห็นว่าตนต้องการจะเปิดอีเมลนั้นหรือไม่

เมื่อศึกษาเปรียบเทียบกับกฎหมายในสหรัฐอเมริกา CAN-SPAM มีบทบัญญัติเรื่องใช้ข้อมูลหัวจดหมาย (Header) เท็จหรือก่อให้เกิดความเข้าใจผิดในสาระสำคัญ (Materially) ของอีเมล[4] ที่ครอบคลุมการปลอมแปลงข้อมูลเกี่ยวกับที่มา (source) บริเวณแถบผู้ส่ง (from line) หรือที่อยู่ไอพีต้นทาง (IP address) หรือชื่อโดเมน (Domain name) ทั้งหมดที่เป็นข้อมูลเบื้องต้นที่บุคคลทั่วไปสามารถรับรู้ได้โดยง่าย และยังมีบทบัญญัติเกี่ยวกับการใช้ชื่อหัวเรื่อง (subject) ที่ต้องมีความชัดเจน

---

[2] สราวุธ ปิติยาศักดิ์. กฎหมายเทคโนโลยีสารสนเทศ. สำนักพิมพ์นิติธรรม, 2555. หน้า 293-294.

[3] พระราชบัญญัติคุ้มครองผู้บริโภค (ฉบับที่ 2) พ.ศ. 2541 มาตรา 11 ให้ยกเลิกความในมาตรา 31 แห่งพระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2522และให้ใช้ความต่อไปนี้แทน “มาตรา 31 ฉลากของสินค้าที่ควบคุมฉลาก จะต้องมีลักษณะดังต่อไปนี้

(1) ใช้ข้อความที่ตรงต่อความจริงและไม่มีข้อความที่อาจก่อให้เกิดความเข้าใจผิดในสาระสำคัญเกี่ยวกับสินค้า

(2) ต้องระบุข้อความดังต่อไปนี้

(ก) ชื่อหรือเครื่องหมายการค้าของผู้ผลิตหรือของผู้นำเข้าเพื่อขายแล้วแต่กรณี

(ข) สถานที่ผลิตหรือสถานที่ประกอบธุรกิจนำเข้า แล้วแต่กรณี

(ค) ระบุข้อความที่แสดงให้เข้าใจได้ว่าสินค้านั้นคืออะไร ในกรณีที่เป็นสินค้านำเข้าให้ระบุชื่อประเทศที่ผลิตด้วย

(3) ต้องระบุข้อความอันจำเป็น ได้แก่ ราคา ปริมาณ วิธีใช้ ข้อแนะนำ คำเตือน วัน เดือน ปีที่หมดอายุในกรณีเป็นสินค้าที่หมดอายุได้ หรือกรณีอื่น เพื่อคุ้มครองสิทธิของผู้บริโภค ทั้งนี้ ตามหลักเกณฑ์และเงื่อนไขที่คณะกรรมการว่าด้วยฉลากกำหนดโดยประกาศในราชกิจจานุเบกษา”

[4] CAN-SPAM Act, section 5 (a)(1)

และสื่อถึงเนื้อหาที่เป็นสาระสาคัญในอีเมล[5] รวมทั้งยังบัญญัติให้ผู้ส่งต้องระบุที่อยู่ทางไปรษณีย์ในเนื้อความของอีเมลเพื่อให้ผู้รับสามารถติดต่อได้อย่างสะดวก[6]อีกด้วย บทบัญญัตินี้ไม่เพียงแต่จะปกป้องสิทธิในการรับรู้ข้อมูลแหล่งที่มาเท่านั้น แต่ยังสามารถเป็นตัวกรองไวรัส มัลแวร์ หรือโทรจัน ที่จะแพร่เชื้อจากการเปิดอีเมลได้ขั้นหนึ่งอีกด้วย ดังนั้น การที่กฎหมายในประเทศไทยยังระบุโทษเพียง “ปกปิดหรือปลอมแปลงแหล่งที่มาในการส่งข้อมูล” จึงอาจยังไม่เพียงพอที่จะปกป้องผู้รับจากอันตรายที่อาจเกิดจากการเปิดอีเมล หรือยังไม่ช่วยให้ผู้รับได้ทราบข้อมูลเบื้องต้นเพียงพอก่อนทาการตัดสินใจเปิด

องค์ประกอบประการที่สอง “อันเป็นการรบกวนการใช้งานระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข” การตีความของคาว่า “โดยปกติสุข” ต้องอาศัยวิจารณญาณของวิญญูชนเป็นเครื่องวัดและเป็นการพิจารณาแบบภาววิสัย (Objective) ไม่ใช่การพิจารณาตามหลักความเป็นจริงแบบอัตวิสัย (Subject)[7] ดังนั้น เกณฑ์ที่จะวัดว่าการรบกวนนั้นมีลักษณะรุนแรงมากพอจะนับเป็นความผิดได้หรือไม่ จึงไม่ได้มีระบุแบบเป็นตัวเลขชัดเจน อีกทั้งการกระทาความผิดในรูปแบบนี้เป็นเรื่องทางเทคนิคเฉพาะ ยากที่วิญญูชนทั่วไปที่ไม่ใช่ผู้เชี่ยวชาญจะพิสูจน์หรือจินตนาการถึงระดับความเสียหายที่แท้จริงด้วยตนเอง และประชาชนทั่วไปก็ไม่อาจทราบถึงผลกระทบอื่นที่เกิดขึ้นนอกจากในประเด็นที่ตนเกิดความรู้สึกราคาญหรือโดนรบกวนพื้นที่ในกล่องจดหมาย (mail box) ได้ ทาให้ไม่ค่อยมีผู้เสียหายที่เป็นผู้รับปลายทาง (end user) ทาการฟ้องร้องในคดีนี้มากนัก ทั้งๆที่มีจานวนสแปม-เมลวิ่งอยู่บนระบบอินเทอร์เน็ตมากมาย กล่าวกันว่าแค่ปี 2011 ปีเดียวก็มีการส่งสแปมเมลกว่า 7 ล้านล้านรายการแล้ว[8] จากที่กล่าวไปในบทที่ 2 ว่าสแปมไม่ได้เป็นปัญหาของผู้รับแต่เพียงอย่างเดียว การที่ผู้ประกอบการใช้เสรีภาพในการโฆษณาจนเกิดส่วน ก่อให้เกิดผลกระทบแอบแฝงต่อหลายภาคส่วน เพียงแต่ไม่มีใครออกมาพิสูจน์ร้องทุกข์ ภาระในการป้องกันสแปมจึงกลายเป็นของภาคเอกชน เช่น ผู้ให้บริการอินเทอร์เน็ต (ISPs) หรือผู้ให้บริการอีเมล (ESP) หรือผู้ดูแลระบบเพียงเท่านั้น ประเด็นนี้จึงยังคงเป็นสิ่งที่ยากจะพิสูจน์และยากที่คนทั่วไปจะเห็นภาพ

เมื่อพิจารณาเปรียบเทียบกับ CAN-SPAM จะเห็นว่ากฎหมายมีการกาหนดจานวนอีเมลเชิงทวีคูณ (multiple) ที่ผู้ส่งสามารถทาการส่งได้ต่อชั่วโมง/ต่อวัน/ต่อปี[9] อย่างชัดเจน อีกทั้งยังกาหนดว่ามูลค่าความเสียหายที่เกิดขึ้นเท่าไหร่จึงจะถือเป็นความผิด[10] และกาหนดโทษเพิ่มเติมตามมูลค่าผลตอบแทนที่ได้จากการส่งอีเมลเชิงพาณิชย์ที่ขัดต่อกฎหมายนั้น[11] ท าให้ไม่ว่าใครก็สามารถเข้าใจใน

---

[5] CAN-SPAM Act, section 5 (a)(2)

[6] CAN-SPAM Act, section 5 (a)(3)

[7] พรเพชร วิชิตชลชัย. ค าอธิบายพระราชบัญญัติว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. ส านักงานศาลยุติธรรม, 2550.

[8] สุพิศ ปราณีตพลกรัง. กฎหมายว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์. ส านักพิมพ์นิติธรรม, กันยายน 2560. หน้า 22.

[9] CAN-SPAM Act, section 4 (a)(1) แก้ไขเพิ่มเติม s 1037 (b) (2) (C)

[10] CAN-SPAM Act, section 4 (a)(1) แก้ไขเพิ่มเติม s 1037 (b) (2) (D)

[11] CAN-SPAM Act, section 4 (a)(1) แก้ไขเพิ่มเติม s 1037 (b) (2) (E)

มาตรฐานเกณฑ์ขั้นต่ำ หรือมีข้อมูลเชิงเปรียบเทียบแบบเป็นรูปธรรม ด้านผู้ประกอบการก็มีตัวเลขให้อ้างอิงเพื่อที่จะดำเนินกิจกรรมทางการตลาดนั้นได้อย่างถูกต้องตามกฎหมาย ดังนั้นในคณะกรรมการของประเทศไทย ควรจะทำการศึกษาเพื่อหาหลักเกณฑ์ที่เป็นรูปธรรมเช่นนี้ เพื่ออำนวยความสะดวกให้นักการตลาดสามารถ กำหนดนโยบายของตนให้สอดคล้อง และเหมาะสมกับสภาพตลาดในปัจจุบัน

องค์ประกอบประการที่สาม “การไม่เปิดโอกาสให้ผู้รับบอกเลิกได้โดยง่าย” ในเรื่องนี้ พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2560 มาตรา 4 ได้หยิบยกเอาหลัก Opt-out เข้ามาเป็นเกณฑ์เพิ่มเติมในการส่งอีเมลเชิงพาณิชย์ จากเดิมที่มาตรา 11 ในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 กำหนดโทษไว้เพียงกรณีปลอมแปลงแหล่งที่มาของการส่งอีเมล แต่กฎหมายฉบับใหม่ได้เพิ่มโทษปรับในกรณีที่ผู้ส่งไม่ได้จัดหาช่องทางการปฏิเสธรับ (opt-out) ให้ผู้รับไว้ด้วย แต่อย่างไรก็ตาม แม้ว่าหลัก Opt-out จะช่วยให้ภาคธุรกิจเกิดความคล่องตัวและมีเสรีภาพในการโฆษณาสอดคล้องตามสิทธิขั้นพื้นฐานของประชาชนตามมาตรา 34 ในรัฐธรรมนูญ พ.ศ. 2560[12] แต่ยังคงมีประเด็นปัญหาที่น่ากังขาในเรื่องการรักษาสิทธิความเป็นอยู่ส่วนบุคคล (Rights of Privacy) เนื่องจากการส่งโฆษณาที่ก่อให้เกิดความเดือดร้อนราคาญแก่ผู้รับที่ทำให้เกิดภาระในการดำเนินการเพื่อขอปฏิเสธรับ ทั้งที่ตนเองไม่ได้ให้ความยินยอมในการบอกรับมาก่อน และยังก่อให้เกิดภาระการจัดการเพื่อบริหารทรัพยากรสารสนเทศทางฝั่งผู้รับเอง อาจถือเป็นการทำ “ละเมิด” ต่อสิทธิและเสรีภาพของปวงชนชาวไทยตามที่บัญญัติไว้ในรัฐธรรมนูญ พ.ศ. 2560 หมวด 3 สิทธิและเสรีภาพของปวงชนชาวไทย มาตรา 32 ที่บัญญัติไว้ว่า *“บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ”*

ยิ่งไปกว่านั้น การดำเนินกิจกรรมโฆษณาโดยไม่เปิดอิสระให้ผู้รับบอกรับบริการโดยสมัครใจยังเป็นการขัดต่อสิทธิ 5 ประการของผู้บริโภคที่จะได้รับความคุ้มครองตามพระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2522 (ฉบับที่ 2) พ.ศ. 2541[13] ต่อมา กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ออก

---

[12] รัฐธรรมนูญ พ.ศ. 2560 หมวด 3 สิทธิและเสรีภาพของปวงชนชาวไทย มาตรา 34 บุคคลย่อมมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อ ความหมายโดยวิธีอื่น การจ ำกัดเสรีภาพดังกล่าวจะกระทำมิได้ เว้นแต่โดยอาศัย อ ำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเฉพาะเพื่อรักษาความมั่นคงของรัฐ เพื่อคุ้มครองสิทธิหรือเสรีภาพของบุคคลอื่น เพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเพื่อป้องกันสุขภาพของประชาชน เสรีภาพทางวิชาการย่อมได้รับความคุ้มครอง แต่การใช้เสรีภาพนั้นต้องไม่ขัดต่อหน้าที่ของปวงชนชาวไทยหรือศีลธรรมอันดีของประชาชน และต้องเคารพและไม่ปิดกั้นความเห็นต่างของบุคคลอื่น

[13] พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2522 (ฉบับที่ 2) พ.ศ. 2541 สิทธิของผู้บริโภค 5 ประการ

(1) สิทธิที่จะได้รับข่าวสารรวมทั้งค ำพรรณนาคุณภาพที่ถูกต้องและเพียงพอเกี่ยวกับสินค้าหรือบริการ ได้แก่ สิทธิที่จะได้รับการโฆษณาหรือการแสดงฉลากตามความเป็นจริงและปราศจากพิษภัยแก่ผู้บริโภครวมตลอดถึงสิทธิที่จะได้รับทราบข้อมูลเกี่ยวกับสินค้าหรือบริการอย่างถูกต้องและเพียงพอที่จะไม่หลงผิดในการซื้อสินค้าหรือรับบริการโดยไม่เป็นธรรม

(2) สิทธิที่จะมีอิสระในการเลือกหาสินค้าหรือบริการ ได้แก่ สิทธิที่จะเลือกซื้อสินค้าหรือรับบริการโดยความสมัครใจของผู้บริโภคและปราศจากการชักจูงใจอันไม่เป็นธรรม

ประกาศเรื่อง ลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนราคาญแก่ผู้รับ ในวันที่ 21 กรกฎาคม พ.ศ. 2560 โดยในข้อที่ 5 ได้บัญญัติให้ผู้ประกอบการที่ต้องการส่งอีเมลเชิงพาณิชย์ ต้องได้รับความยินยอมจากผู้รับก่อนจึงจะสามารถส่งได้โดยไม่ถือเป็นการก่อให้เกิดความเดือดร้อนราคาญ (Opt-in)[14] ยิ่งไปกว่านั้นยังต้องระบุช่องทางในการบอกปฏิเสธรับ (Opt-out) ไว้ในอีเมลเชิงพาณิชย์นั้นด้วย[15]

เมื่อเปรียบเทียบกับกฎหมายในต่างประเทศ มาตรการของไทยมีความคล้ายคลึงกับมาตรการของสหภาพยุโรปที่ระบุให้ผู้ส่งต้องได้รับความยินยอมจากผู้รับ (opt-in) และต้องชี้แจงช่องทางในการปฏิเสธรับ (Opt-out) ให้ผู้รับเข้าใจได้ง่ายและปราศจากค่าใช้จ่ายเพิ่มเติม แต่มาตรการของสหภาพยุโรปมีความยืดหยุ่นมากกว่าตรงที่ยินยอมให้ผู้ประกอบการนารายชื่อที่อยู่อีเมลที่ตนเองถือครองอยู่ไม่ว่าที่ได้มาจากการทาธุรกรรมซื้อขายหรือได้มาจากการสมัครลงทะเบียนรับข่าวสาร ไปใช้ในการส่งอีเมลโฆษณาสินค้าที่มีลักษณะเดียวกันได้เพียงแต่ต้องระบุสิทธิในการปฏิเสธรับ (Opt-out) ในอีเมลให้ชัดเจนด้วย

แนวทางดังกล่าวมีลักษณะตรงกับหลัก inferred consent ซึ่งหมายถึง ความยินยอมที่อ้างอิงจากความประพฤติและความสัมพันธ์ทางธุรกิจของผู้รับที่มีความเกี่ยวข้องกับผู้ส่งกันก่อนอยู่แล้ว และเป็นที่คาดหมายได้ว่าอีกฝ่ายควรได้รับการส่งข้อความ[16] ซึ่งประเด็นนี้ช่วยเพิ่มอิสระในการโฆษณาให้แก่ผู้ประกอบการ

แม้ในปัจจุบันประเทศไทยยังไม่ได้มีหลักเกณฑ์เกี่ยวกับจุดประสงค์ในการนาข้อมูลส่วนบุคคลของผู้บริโภคไปใช้งาน แต่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่กาลังจะประกาศใช้ในอีกไม่นานนี้ มาตรา 18 ระบุว่า “*ผู้ใดควบคุมข้อมูลส่วนบุคคลต้องทาการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้ก่อนหรือขณะเก็บรวบรวม การเก็บรวมรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ตามวรรคหนึ่งจะกระทามิได้ เว้นแต่ (1) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว (2) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระท าได้*”

กล่าวคือ หากพระราชบัญญัติฯนี้มีผลบังคับให้ผู้ประกอบการไม่สามารถนาข้อมูลส่วนบุคคลของลูกค้าไปใช้งานเพื่อจุดประสงค์อื่นนอกเหนือจากที่ได้แจ้งไว้เมื่อตอนขอข้อมูลได้ ดังนั้น หากในอนาคตมีสินค้าตัวใหม่ที่เป็นสินค้าประเภทเดียวกัน หรือมีโปรโมชั่นของสินค้าอื่นที่เกี่ยวข้อง ก็จะไม่สามารถส่งให้ลูกค้าได้ทันที ซึ่งการจากัดสิทธิที่มากเกินไปก็ไม่ทาให้เกิดความคล่องตัวในการประกอบ

---

(3) สิทธิที่จะได้รับความปลอดภัยจากการใช้สินค้าหรือบริการ ได้แก่ สิทธิที่จะได้รับสินค้าหรือบริการที่ปลอดภัยมีสภาพและคุณภาพได้มาตรฐานเหมาะสมแก่การใช้ ไม่ก่อให้เกิดอันตรายต่อชีวิตร่างกายหรือทรัพย์สิน ในกรณีใช้ตามค าแนะน าหรือระมัดระวังตามสภาพของสินค้าหรือบริการนั้นแล้ว

(4) สิทธิที่จะได้รับความเป็นธรรมในการท าสัญญา ได้แก่ สิทธิที่จะได้รับข้อสัญญาโดยไม่ถูกเอารัดเอาเปรียบจากผู้ประกอบธุรกิจ

(5) สิทธิที่จะได้รับการพิจารณาและชดเชยความเสียหาย ได้แก่ สิทธิที่จะได้รับการคุ้มครองและชดใช้ค่าเสียหายเมื่อมีการละเมิดสิทธิของผู้บริโภคตามข้อ 1, 2, 3 และ 4 ดังกล่าว

[14] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนร าคาญแก่ผู้รับ พ.ศ. 2560 ข้อ 5

[15] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนร าคาญแก่ผู้รับ พ.ศ. 2560 ข้อ 5 (1)(d)

[16] The Department of Internal Affairs of Te Tari Taiwhenua. Three Steps to Ensure You Are Not Spamming [Online]. . Available from: https://www.dia.govt.nz/Spam-Three-Steps#in [2 June 2018.]

ธุรกิจหลัก inferred consent จึงเป็นอีกหนึ่งทางเลือกที่เหมาะสมในการปกป้องสิทธิของผู้รับแต่พอดีในขณะที่ก็ช่วยสนับสนุนให้เกิดกิจกรรมทางการตลาดได้

เมื่อพิจารณาจากองค์ประกอบทางความผิดที่เกี่ยวกับความผิดฐานสแปมเมล์ในแต่ละประเทศ จะสามารถสรุปได้ดังตารางต่อไปนี้

ตารางที่ 3 องค์ประกอบทางความผิดฐานส่งสแปมเมล

	ประเทศไทย	สหรัฐอเมริกา	สหภาพยุโรป
องค์ประกอบทางความผิด	1. ปกปิดหรือปลอมแปลงแหล่งที่มาในการส่งข้อมูล 2. เป็นการรบกวนการใช้งานระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข 3. ไม่เปิดโอกาสให้ผู้รับบอกเลิกได้โดยง่าย (opt-out) 4. โดยเจตนา	1.ปกปิดหรือปลอมแปลงหรือทาให้เข้าใจผิดในสาระสาคัญของข้อมูลหัวจดหมาย (Header) ได้แก่ - ข้อมูลเกี่ยวกับที่มา (source) บริเวณแถบผู้ส่ง (from line) หรือ - ที่อยู่ไอพีต้นทาง (IP-address) หรือ - ชื่อโดเมน (Domain name) หรือ - หัวจดหมาย (subject) 2. ใช้หัวจดหมาย (subject heading) ที่ทาให้เข้าใจผิดในสาระสาคัญหรือข้อเท็จจริงของเนื้อหาในอีเมล 3. ไม่เปิดโอกาสให้ผู้รับบอกเลิกได้โดยง่าย (opt-out) 4. โดยเจตนา	1. โดยไม่ได้รับความยินยอมจากผู้รับ (opt-in) และ 2. ไม่เปิดโอกาสให้ผู้รับบอกเลิกได้โดยง่าย (opt-out) 3. ปลอมแปลงหรือปิดบังข้อมูลในการระบุตัวตนของผู้ส่ง หรือโดยไม่มีการระบุที่อยู่ที่ถูกต้องเพื่อให้ผู้รับสามารถติดต่อกลับได้ 4. โดยเจตนา

5.1.1 วิเคราะห์ข้อดีและข้อเสียของหลักเกณฑ์ Opt-in และ Opt-out

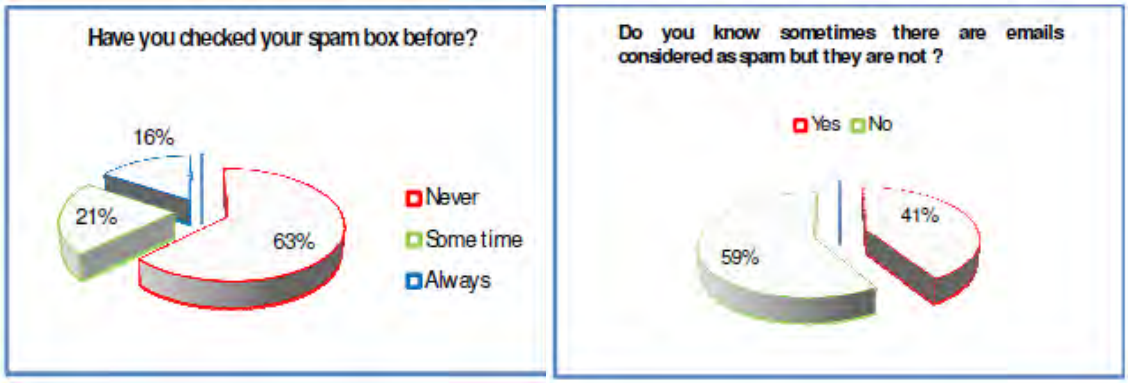
จากบทวิเคราะห์ข้างต้นที่สะท้อนให้เห็นถึงองค์ประกอบทางความผิด และหลักการที่แต่ละประเทศนามาใช้เป็นหลักเกณฑ์ในการส่งอีเมลเชิงพาณิชย์ แน่นอนว่าการกาหนดมาตรการทางกฎหมายเป็นหน้าที่ของภาครัฐที่จะพิจารณาถึงสถานการณ์ของปัญหา สภาพสังคม สิทธิพื้นฐานของประชาชน ตลอดจนภาวะความจาเป็นทางเศรษฐกิจและความสะดวกในการดาเนินกิจกรรมทางการค้าของแต่ละประเทศ แล้วจึงเลือกหลักการที่เหมาะสมมาปรับใช้เพื่อให้เกิดประสิทธิภาพสูงสุด เนื่องจากหลักการทั้งสองต่างมีข้อดี-ข้อเสียต่างกัน เบื้องต้นผู้เขียนจะขออธิบายถึงข้อดีและข้อเสียของหลักการทั้งสอง ดังตารางต่อไปนี้

ตารางที่ 4 เปรียบเทียบลักษณะของหลักเกณฑ์ Opt-in และ Opt-out

หัวข้อ	Opt-out	Opt-in
ความอิสระทางการค้า	ผู้ประกอบการมีอิสระในการส่งอีเมลเชิงพาณิชย์ที่มีเนื้อหาเหมาะสมตามกฎหมายให้ผู้รับที่ตนมีรายชื่อที่อยู่อีเมลอยู่โดยตรง	ผู้ประกอบการจะสามารถส่งอีเมลเชิงพาณิชย์ให้ผู้รับได้ก็ต่อเมื่อผู้รับได้ให้ความยินยอมในการรับ (Consent) ล่วงหน้า
โอกาสในการเข้าถึงผู้บริโภค	สามารถเข้าถึงลูกค้าได้จานวนมากแบบไม่จ ากัดกลุ่ม	สามารถเข้าถึงลูกค้ากลุ่มเป้าหมาย (Target Customer) ได้ตรงจุด
ความเสี่ยงในการติดบัญชีด า (Blacklist)	มีความเสี่ยงที่ผู้รับจะกดรายงาน (report) และมีความเสี่ยงที่อีเมลจะถูกโอนไปยังกล่องอีเมลขยะ (Spam Box) โดยอัตโนมัติ เนื่องจากติดนโยบายของผู้ให้บริการอีเมล (ISPs Policy) ดักไว้เพราะ IP หรือที่อยู่ในการส่งนั้นเป็นที่อยู่ที่ไม่เคยมีความสัมพันธ์กับผู้รับมาก่อน จึงมีความเสี่ยงที่ผู้รับจะไม่ได้เปิดอ่านและสูญเสียโอกาสในการโฆษณา	ปลอดภัยจากการโดนรายงาน (report) และไม่มีความเสี่ยงที่จะถูกโอนไปยังกล่องอีเมลขยะ (Spam Box) เนื่องจากผู้รับเคยให้ความยินยอมไว้ก่อนอยู่แล้ว และมีแนวโน้มที่ผู้รับจะเปิดอ่านอีเมลมากกว่า
ภาพลักษณ์ของผู้ประกอบการ	ผลกระทบต่อภาพลักษณ์อันดี อาจเกิดจากการส่งอีเมลจานวนมากเกินไปจนทาให้ผู้รับรู้สึกร าคาญใจหรือการที่บริษัทติด Blacklist อาจบั่นทอนภาพลักษณ์ที่ดีของผู้ประกอบการ	เกิดภาพลักษณ์ที่ดีว่าผู้ประกอบการเคารพในสิทธิความเป็นอยู่ส่วนบุคคลของผู้รับ ซึ่งจะก่อให้เกิดความเชื่อใจและรักษาความสัมพันธ์ที่ดีกับผู้บริโภคได้ในระยะยาว
ภาระค่าใช้จ่าย	ต้นทุนในการโฆษณาต่า แต่มีต้นทุนในการหา mail server และต้นทุนด้านการจ้างงานผู้เชี่ยวชาญเฉพาะด้าน เพื่อวางระบบที่สามารถส่งข้อความคราวละมากๆ	มีขั้นตอนในการโฆษณามากขึ้น เนื่องจากต้องขอความยินยอมจากลูกค้าก่อน แต่ประหยัดต้นทุนด้านค่าใช้จ่ายและด้านเวลามากกว่าการส่งอีเมลแบบไม่จ ากัดกลุ่ม

แม้ว่าการทาการตลาดด้วยอีเมลเชิงพาณิชย์จะเป็นวิธีการโฆษณาทางออนไลน์ที่ดี สะดวก และประหยัดค่าใช้จ่าย แต่ผู้ประกอบการต้องไม่ลืมว่าการสื่อสารกับผู้บริโภคอย่างมีประสิทธิภาพต่างหากที่เป็นสิ่งที่สาคัญที่สุดในการทาการตลาด หากข้อความที่ส่งไปไม่ถูกเปิดอ่าน

หรือที่อยู่อีเมลของผู้ประกอบการโดนนโยบายตัวกรองของผู้ให้บริการอินเทอร์เน็ตดักจับว่าเป็นที่อยู่ของสแปมเมอร์ หรือ IP address ของผู้ประกอบการโดนดักเพราะทาการส่งอีเมลจานวนมากในวันเดียว การทาการตลาดนั้นย่อมไร้ความหมายเพราะไม่สามารถสื่อสารไปถึงตัวผู้บริโภค จากผลสารวจของ University of Malaya และ Multimedia University เกี่ยวกับภาพลักษณ์ของสแปมกับผู้บริโภคจานวน 70 คนในประเทศมาเลเซีย พบว่า 63% ของกลุ่มสารวจไม่เคยตรวจสอบหรือเปิดโฟลเดอร์สแปมเมลในกล่องข้อความของเขามาก่อนเลย และ 59% ของกลุ่มสารวจไม่เคยทราบว่าอีเมลบางฉบับมีโอกาสที่จะถูกนโยบายของผู้ให้บริการอีเมลดักจับว่าเป็นสแปมเมล[17] (อ้างอิงภาพที่11)



ภาพที่ 11 ผลลัพธ์จากการวิจัยโดยใช้แบบสอบถามเรื่องการท าการตลาดผ่านอีเมล (e-mail marketing) กับประชากรชาวมาเลเซีย 70 คน โดยมหาวิทยาลัย University of Malaya และ Multimedia University[18]

ผลการส ารวจเกี่ยวกับรูปแบบการโฆษณาที่ได้รับความเชื่อถือจากผู้บริโภค “Global Trust in Advertising 2015” โดยบริษัทนีลเส็น (Nielsen) ประเทศไทย ที่ทาการสารวจผู้บริโภคจ านวน 30,000 คนใน 60 ประเทศทั่วโลก ชี้ให้เห็นว่าคนส่วนใหญ่ให้ความเชื่อถือในค าแนะน าจากคนรู้จักมากที่สุด (83%) รองลงมาคือเว็บไซต์ของผลิตภัณฑ์เอง (70%) บทความโฆษณาในหนังสือต่างๆ (66%) ความคิดเห็นที่โพสต์ในออนไลน์ (66%) และอีเมลที่ตนสมัครไว้ (56%) ตามลาดับ[19] (อ้างอิงภาพที่ 12) จึงเป็นเครื่องพิสูจน์ว่าความน่าเชื่อถือของข้อมูลเป็นสิ่งสาคัญที่จะนามาซึ่งการตัดสินใจซื้อของผู้บริโภค โดยเฉพาะข้อมูลที่อยู่บนอินเทอร์เน็ต หากไม่ใช่สิ่งที่ผู้บริโภคมีความต้องการที่จะเข้าถึง (access) ด้วยตนเองก่อนแล้ว ถึงแม้ข้อความนั้นจะผ่านเข้าไปถึงกล่องอีเมล (mail box) ของผู้บริโภคได้ ก็มีโอกาสน้อยที่ผู้บริโภคจะเปิดเข้าไปอ่านหรืออ่านอย่างสนใจจนเกิดความต้องการที่จะซื้อ ดังนั้นการทาการตลาดด้วยหลัก Opt-out จึงเป็นการสื่อสารที่ไม่อาจก่อให้เกิดประสิทธิภาพและประสิทธิผลเท่าที่ควร นักการตลาดที่ดีจึงควรสร้างช่องทางที่ทาให้ผู้บริโภคเกิดความเชื่อถือได้เพื่อสร้างความไว้วางใจในเนื้อหาการโฆษณามากกว่า จึงจะทาให้กิจกรรมทางการตลาดนั้นเกิดประสิทธิภาพ และส่งผลท าให้องค์กรเกิดภาพลักษณ์เชิงบวก

---

[17] Mostafa Raad, N. M. Y., Gazi Mahabubul Alam, B. B. Zaidan, A. A. Zaidan. Impact of Spam Advertisement through E-Mail: A Study to Assess the Influence of the Anti-Spam on the E-Mail Marketing. African Journal of Business Management Vol. 4(11) (4 September 2010): 2362-2367.

[18] Ibid., p. 5

[19] Brand Buffet. Zn-UP. 10 รูปแบบโฆษณาที่ผู้บริโภคเชื่อถือมากที่สุด 2015 [ออนไลน์]. 2015. แหล่งที่มา: https://www.brandbuffet.in.th/2015/10/nielsen-consumer-trust-in-ad-type/ [10 เมษายน 2561]

ภาพที่ 12 Infographic แสดงผลการสำรวจเกี่ยวกับรูปแบบการโฆษณาที่ได้รับความเชื่อถือจากผู้บริโภคประเทศไทย[20] “Global Trust in Advertising 2015” โดยบริษัทนีลเส็น (Nielsen)

จากผลรายงานเรื่องสแปมและฟิชชิ่ง (Spam and Phishing Reports) ประจำปี 2017 โดยบริษัท Kasperskylab ที่เป็นบริษัทชั้นนำด้านการพัฒนาซอฟต์แวร์ป้องกันไวรัส พบว่าสัดส่วนของสแปมที่อยู่ในระบบการจราจรสำหรับแลกเปลี่ยนอีเมล (mail traffic) ในปี 2017 อยู่ที่ 56.63% จากอีเมลทั้งหมดในระบบ ถึงแม้จะมีอัตราลดลงจากปี 2016 ที่ 1.68% แต่แนวโน้มของสแปมยังคงมีจำนวนมากกว่าครึ่งหนึ่งของอีเมลปกติเช่นเดิม โดยประเทศที่เป็นแหล่งกำเนิดสแปมมากที่สุดในโลกได้แก่ สหรัฐอเมริกา มีสัดส่วนอยู่ที่ 13.21% รองลงมาคือสาธารณรัฐประชาชนจีน (11.25%) และเวียดนาม (9.85%) ตามลำดับ[21] จึงสามารถสรุปได้ว่า ถึงแม้สหรัฐอเมริกาจะเป็นประเทศลำดับแรกๆในโลกที่มีการออกกฎหมายเพื่อจำกัดและปราบปรามสแปมเมล แต่กฎหมายที่ใช้ในปัจจุบันยังไม่สามารถแก้ไขปัญหานี้ได้มากนัก เพราะสัดส่วนของการทำสแปมเมลยังคงสูงที่สุดในโลกอย่างไม่เปลี่ยนแปลงมาตั้งแต่อดีตจนถึงปัจจุบัน ผลการรายงานนี้ช่วยย้ำให้เห็นอีกครั้งว่า หลัก Opt-out เพียงอย่างเดียว อาจมีประสิทธิภาพไม่เพียงพอที่จะปราบปรามการกระทำความผิดในรูปแบบนี้ได้

สำหรับประเทศไทยที่เพิ่งเริ่มนำหลักการ Opt-in มาใช้เมื่อเดือนกรกฎาคม พ.ศ. 2560 ที่ผ่านมา ตามแบบอย่างในสหภาพยุโรป ถือเป็นสัญญาณดีว่ารัฐเริ่มหันมาให้ความสำคัญกับ

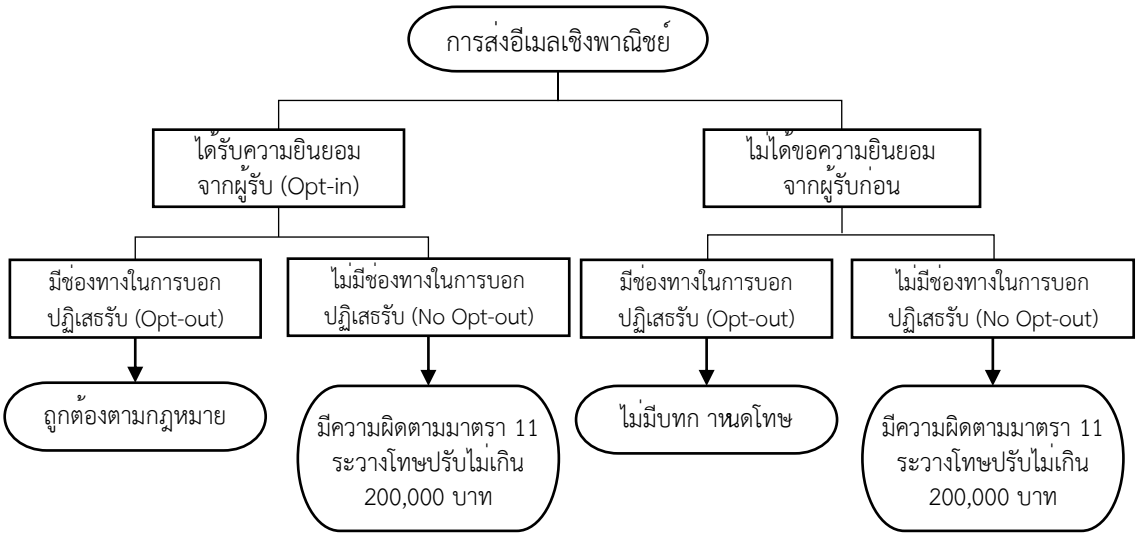
---

[20] เรื่องเดียวกัน

[21] Darya Gudkova, M. V., Tatyana Shcherbakova, Nadezhda Demidova. Spam and Phishing in 2017 [Online]. 2018. Available from: https://securelist.com/spam-and-phishing-in-2017/83833/ [20 April 2018]

สิทธิด้านข้อมูลส่วนบุคคลของประชาชนมากขึ้นแล้ว หากในอนาคตอันใกล้สามารถยกร่างพระราชบัญญัติคุ้มครองผู้บริโภคได้สาเร็จ การนาข้อมูลส่วนบุคคลของผู้บริโภคไปใช้งานผิดจุดประสงค์จะต้องระวางโทษปรับไม่เกิน 300,000 บาท และหากการใช้งานนั้นนามาซึ่งประโยชน์อันมิควรได้หรือก่อให้เกิดความเสียหายแก่ผู้อื่น จะต้องระวางโทษจาคุกไม่เกิน 6 เดือนหรือปรับไม่เกิน 500,000 บาท หรือทั้งจาทั้งปรับ[22] ดังนั้น ในอนาคตผู้ประกอบการหรือนักการตลาดจะมีข้อจากัดในการดาเนินกิจกรรมทางการตลาดมากขึ้นอย่างแน่นอน จากเดิมที่สามารถนาข้อมูลลูกค้ามาสร้างเป็นฐานข้อมูล (database) เพื่อการดาเนินกิจกรรมทางการตลาด หรือเพื่อนามาวิเคราะห์ วิจัย พัฒนาผลิตภัณฑ์ใหม่ๆ ต่อไปอาจกระทาได้ยากขึ้น รัฐจึงควรกลับมาทบทวนประเด็นการเพิ่มหลัก inferred consent เข้าไปปรับใช้กับมาตรการ Opt-in

อย่างไรก็ตาม บทบัญญัติทางกฎหมายไทยในปัจจุบันยังไม่สามารถเอาโทษแก่การส่งอีเมลเชิงพาณิชย์ที่มีช่องทางการปฏิเสธรับระบุไว้ แม้ว่าจะไม่ได้รับความยินยอมจากผู้รับก่อนก็ตาม เนื่องจาก “การไม่เปิดโอกาสให้แจ้งความประสงค์เพื่อบอกเลิก” กลายเป็นองค์ประกอบทางความผิดของความผิดฐานนี้ไปแล้ว หากผู้กระทาไม่มีความผิดครบองค์ประกอบ (อ้างอิงภาพที่ 3) กล่าวคือ หากผู้รับได้รับอีเมลเชิงพาณิชย์โดยที่ตนไม่เคยให้คายินยอมไว้ แต่ในอีเมลนั้นมีช่องทางการแจ้งบอกเลิกและผู้รับนั้นไม่สามารถหาหลักฐานมาพิสูจน์ถึงการรบกวนการใช้งานระบบคอมพิวเตอร์โดยปกติสุขของตนได้ ก็ไม่สามารถฟ้องได้ การเพิ่มมาตรการ opt-in เข้าไปจึงไม่สามารถปกป้องสิทธิความเป็นอยู่ส่วนบุคคล (Rights of Privacy) ของผู้รับได้อย่างแท้จริง ดังนั้น จึงควรที่จะผลักดันให้พระราชบัญญัติคุ้มครองผู้บริโภคมีผลบังคับใช้ในเร็ววัน



ภาพที่ 13 แผนภาพสรุปการพิจารณาความผิดฐานท สแปมเมลในประเทศไทย

5.1.2 โทษและอัตราโทษ

[22] ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... หมวด7 มาตรา 44

โทษและอัตราโทษที่เกี่ยวข้องกับการทาสแปมในประเทศไทยกาหนดโทษปรับไว้ที่ 200,000 บาท และไม่มีโทษจาคุก แม้ว่าในขณะที่ร่างกฎหมายคณะกรรมการจะอ้างอิงองค์ประกอบทางความผิดฐานบุกรุกตามประมวลกฎหมายอาญา มาตรา 362[23] มาใช้ในการกาหนดองค์ประกอบความผิดเรื่อง “การรบกวนการใช้คอมพิวเตอร์ของผู้อื่นโดยปกติสุข” ของพระราชบัญญัติฯนี้ก็ตาม[24] หากเทียบกันแล้วการมีเพียงโทษปรับดูจะเป็นโทษที่ค่อนข้างเบา ทั้งที่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้ระวางโทษปรับในการนาข้อมูลส่วนบุคคลของผู้บริโภคไปใช้งานผิดจุดประสงค์ไว้ถึง 300,000 บาท และเพิ่มเพดานโทษปรับและเพิ่มโทษจาคุกหากการนั้นก่อความเสียหายให้ผู้อื่นหรือท าให้ได้มาซึ่งประโยชน์อันมิควรได้

การกระทาความผิดอีกอย่างหนึ่งที่เกี่ยวข้องกับการส่งสแปมเมลคือ “การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ เพื่อทาให้ระบบนั้นเป็นตัวกลางในการส่งผ่านอีเมลเป็นจานวนมาก (relay and transmit)” เนื่องจากการจะส่งอีเมลจานวนมากจาเป็นต้องใช้เซิร์ฟเวอร์ที่มีขนาด (capacity) ใหญ่ สแปมเมอร์ที่เป็นมิจฉาชีพจึงนิยมใช้ไวรัสหรือมัลแวร์แฝงเข้าไปยังเซิร์ฟเวอร์ของบริษัทหรือองค์กรต่างๆ เพื่อแปลงสภาพให้เซิร์ฟเวอร์นั้นกลางเป็นตัวกระจายเมลให้แก่ตน ในประเด็นนี้ พระราชบัญญัติว่าด้วยการกระทาผิดทางคอมพิวเตอร์ มาตรา 10 ได้ระวางโทษไว้ที่ ปรับไม่เกิน 100,000 บาท หรือจาคุกไม่เกิน 5 ปี หรือทั้งจาทั้งปรับ ทั้งที่การถูกลักลอบใช้ทรัพยากรของบริษัทไปเพื่อการส่งสแปมย่อมเป็นการรบกวนสิทธิในการใช้ประโยชน์จากทรัพย์นั้น อีกทั้งยังท าให้เสื่อมเสียถึงชื่อเสียงของบริษัท และมีความเสี่ยงที่ IP address ของบริษัทจะติดบัญชีดา (black list) อีกด้วย ซึ่งหากเทียบฐานความผิดกับบทบัญญัติทั่วไปในประมวลแพ่งและพาณิชย์ การกระทาผิดรูปแบบนี้จะมีความคล้ายคลึงกับความผิดฐานละเมิด มาตรา 420[25] และเรื่องสิทธิในการใช้สอยทรัพย์ส่วนบุคคล มาตรา 1336[26] และเรื่องสิทธิในการครอบครองมาตรา 1374[27] ซึ่งสามารถเยียวยาความเสียหายที่เกิดขึ้นโดยการให้ค่าสินไหมทดแทน รวมกับค่าเสียหายที่เกิดจากการละเมิดนั้น แต่ก็เป็นเรื่องยากที่ผู้เสียหายจะต้องท าการพิสูจน์ให้เห็นถึงมูลค่าความเสียหายที่เกิดขึ้นจากการละเมิดนั้นด้วยตนเอง

---

[23] ประมวลกฎหมายอาญามาตรา 362 ผู้ใดเข้าไปในอสังหาริมทรัพย์ของผู้อื่นเพื่อถือการครอบครองอสังหาริมทรัพย์นั้นทั้งหมดหรือแต่บางส่วน หรือเข้าไปกระท าการใดๆ อันเป็นการรบกวนการครอบครองอสังหาริมทรัพย์ของเขาโดยปกติสุข ต้องระวางโทษจ าคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 2,000 บาท หรือทั้งจ าทั้งปรับ

[24] มานิตย์ จุมปา. ค าอธิบายกฎหมายว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์. ศูนย์หนังสือกฎหมายวิญญูชน, 2554. หน้า 82-84.

[25] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 ผู้ใดจงใจหรือประมาทเลินเล่อ ท าต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทาละเมิดจ าต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น

[26] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 1336 ภายใต้บังคับแห่งกฎหมาย เจ้าของทรัพย์สินมีสิทธิใช้สอยและจ าหน่ายทรัพย์สินของตนและได้ซึ่งดอกผลแห่งทรัพย์สินนั้น กับทั้งมีสิทธิติดตามและเอาคืนซึ่งทรัพย์สินของตนจากบุคคลผู้ไม่มีสิทธิจะยึดถือไว้ และมีสิทธิขัดขวางมิให้ผู้อื่นสอดเข้าเกี่ยวข้องกับทรัพย์สินนั้นโดยมิชอบด้วยกฎหมาย

[27] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 1374 ถ้าผู้ครอบครองถูกรบกวนในการครอบครองทรัพย์สิน เพราะมีผู้สอดเข้าเกี่ยวข้องโดยมิชอบด้วยกฎหมายไซร้ ท่านว่าผู้ครอบครองมีสิทธิจะให้ปลดเปลื้องการรบกวนนั้นได้ ถ้าเป็นที่น่าวิตกว่าจะยังมีการรบกวนอีก ผู้ครอบครองจะขอต่อศาลให้สั่งห้ามก็ได้ การฟ้องคดีเพื่อปลดเปลื้องการรบกวนนั้น ท่านว่าต้องฟ้องภายในปีหนึ่งนับแต่เวลาถูกรบกวน

เมื่อเปรียบเทียบกับสหรัฐอเมริกา แม้ว่า CAN-SPAM จะไม่ได้นำเอาหลัก opt-in มาใช้งาน แต่ก็มีการจำแนกโทษตามระดับความรุนแรงของผลกระทบที่เกิดจากการทำสแปมเมลไว้อย่างชัดเจน ดังต่อไปนี้[28]

1) โทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับในกรณีกระทำหรือมีส่วนร่วมในการกระทำที่มีความผิดทางอาญา

2) โทษปรับหรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับในกรณี

2.1) เข้าถึงระบบคอมพิวเตอร์ของผู้อื่นเพื่อส่งผ่านอีเมลเชิงทวีคูณ

2.2) ใช้ข้อมูลระบุตัวตนที่เป็นเท็จเพื่อลงทะเบียนใช้งานอีเมลหรือเปิดใช้บัญชีผู้ให้บริการออนไลน์มากกว่า 20 บัญชีขึ้นไป หรือเพื่อลงทะเบียนเปิดใช้ชื่อโดเมนมากกว่า 10 ชื่อขึ้นไป

2.3) ส่งอีเมลเชิงพาณิชย์มากกว่า 2,500 ฉบับภายในเวลา 24 ชั่วโมง หรือมากกว่า 25,000 ฉบับในเวลา 30 วัน หรือมากกว่า 250,000 ฉบับในเวลา 1 ปี

2.4) เป็นเหตุให้ผู้อื่นเกิดความเสียหายซึ่งตีเป็นมูลค่าภายในระยะเวลา 1 ปี ได้ตั้งแต่ 5,000 เหรียญดอลลาร์สหรัฐขึ้นไป

2.5) ได้รับผลประโยชน์จากการส่งอีเมลนั้นเป็นมูลค่ามากกว่า 5,000 เหรียญดอลลาร์สหรัฐขึ้นไปภายในระยะเวลา 1 ปี

2.6) เป็นผู้ก่อการที่มีผู้ร่วมกระทำความผิดตั้งแต่3 คนขึ้นไป

3) โทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ ในกรณีอื่นที่เหลือ

จึงส่งผลให้รัฐสามารถใช้อำนาจเพื่อปกป้องและเยียวยาผู้ที่ได้รับผลกระทบได้อย่างเป็นธรรม เนื่องจากผลกระทบที่เกิดจากการทำสแปมเป็นภัยแฝงที่สร้างความเสียหายให้กับผู้ใช้งานในระบบเป็นวงกว้าง และยากจะทำการพิสูจน์ความเสียหายโดยผู้เสียหายรายใดรายหนึ่งเพียงคนเดียว การจำแนกโทษตามระดับความรุนแรงของผลกระทบที่เกิดขึ้น เช่นเดียวกับสหรัฐอเมริกาจึงเป็นแนวทางที่ควรนำมาปรับใช้กับประเทศไทยด้วยเช่นกัน

5.1.3 สถานการณ์ในการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในประเทศไทย

ปัจจุบัน กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้มีการควบคุมให้ผู้ประกอบการที่ใช้ข้อความหรืออีเมลเชิงพาณิชย์เพื่อทำการตลาด ต้องขอความยินยอมจากผู้รับก่อนจึงจะสามารถทำการสิ่งอีเมลได้ และเพิ่มคำนิยามของ “ผู้ส่ง” ให้ครอบคลุมตั้งแต่ผู้ส่งอีเมล ตลอดจนถึงผู้ส่งข้อมูลอิเล็กทรอนิกส์ ผู้ให้บริการเว็บไซต์ ผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการประเภทสื่อสังคมออนไลน์ (Social Media) และเพิ่มคำนิยามของ “ข้อมูลคอมพิวเตอร์” ให้ครอบคลุมตั้งแต่ ข้อความคำสั่งใดๆก็ตามที่คอมพิวเตอร์ประมวลผลได้ ไปจนถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วย

[28] CAN-SPAM Act, section 4(b)

ธุรกรรมทางอิเล็กทรอนิกส์[29] ดังนั้นไม่ว่าจะเป็นข้อความโฆษณาบนสื่อสังคมออนไลน์ (Social Media) หรือบริการแอปพลิเคชัน (Application) ต่างๆ จึงถือเป็นสิ่งที่ต้องถูกควบคุมตามบทบัญญัตินี้ด้วย การฝากร้านในอินสตาแกรมดาราที่ธุรกิจรายย่อยนิยมทาจนสร้างความเดือดร้อนราคาญให้กับดาราหลายท่านในช่วงปี 2014 ถึง 2017 กลายเป็นการกระท ที่มีความผิดตามพระราชบัญญัติว่าด้วยการกระท าความผิดทางคอมพิวเตอร์ มาตรา11 ซึ่งมีโทษปรับสูงสุดถึง 200,000 บาท

สาหรับประเด็นดังกล่าว ต่างประเทศเองก็ยังไม่มีบทบัญญัติเฉพาะออกมารองรับเช่นกัน อาจเป็นเพราะวัฒนธรรมในการใช้สังคมออนไลน์ (Social Network) และจิตสานึกด้านสิทธิของพื้นที่ส่วนบุคคลแตกต่างกัน และส่วนใหญ่สามารถปรับใช้กฎหมายเกี่ยวกับการคุ้มครองสิทธิความเป็นอยู่ส่วนบุคคลเข้ามาใช้ได้ มาตรการในการแก้ไขส่วนใหญ่จึงมาจากนโยบายของผู้ให้บริการสื่อสังคมออนไลน์เอง เพราะหากผู้โพสต์โดนกดรายงาน (report) บ่อยๆ สุดท้ายแอคเคาท์ (account) นั้นก็จะติดบัญชีดา (black list) ทาให้ไม่สามารถใช้งานต่อไปได้ ผู้ประกอบการรายใหญ่หรือเจ้าของร้านที่ต้องการรักษาภาพลักษณ์ของตนจึงไม่เลือกใช้วิธีนี้ จะมีก็เพียงแต่ผู้ค้ารายย่อยที่ไม่สนใจภาพลักษณ์ หรือไม่ได้หวังจะใช้งานแอคเคาท์นั้นเพื่อทาธุรกิจในระยะยาวเท่านั้นที่เลือกใช้วิธีนี้ ดังนั้นแม้จะมีกฎหมายเข้ามารองรับในประเด็นนี้ แต่โอกาสที่กฎหมายจะถูกนามาใช้งานยังมีไม่มากนัก อีกทั้งระดับความรุนแรงของปัญหายังไม่ทาให้เกิดผลกระทบต่อสังคมส่วนรวม การปล่อยให้ภาคเอกชนเป็นผู้จัดการกับปัญหาเองอาจทาให้เกิดประสิทธิภาพมากกว่า เช่น ให้ผู้ให้บริการสื่อสังคมออนไลน์เพิ่มเติมนโยบายความเป็นส่วนตัว หรือหลักเกณฑ์พื้นฐานของบัญชีด า(black list)[30]

จากการขยายตัวและสภาวะการแข่งขันที่ดุเดือดของตลาดออนไลน์ ผู้ประกอบการรายใหญ่เริ่มหันมาพัฒนาแอปพลิเคชันบนมือถือ เพื่อให้สามารถสื่อสารถึงกลุ่มลูกค้าเป้าหมายได้รวดเร็วและมีจานวนมากขึ้น ในปี 2014 ตลาดแอปพลิเคชันในประเทศไทยใหญ่เป็นอันดับที่ 20 ของโลก โดยมีมูลค่าในตลาดสูงถึง 93.5 ล้านดอลลาร์สหรัฐ[31] ประโยชน์ในการสร้างแอปพลิเคชันสาหรับผู้ประกอบการอย่างหนึ่งก็คือ การได้มาซึ่งข้อมูลส่วนบุคคล (personal data) ของลูกค้าที่เป็นกลุ่มเป้าหมายที่แท้จริง เนื่องจากเมื่อผู้บริโภคมีการดาวน์โหลดแอปพลิเคชันเหล่านี้มาใช้ ระบบมักจะบังคับให้กรอกข้อมูลอาทิ ชื่อ นามสกุล ที่อยู่อีเมล เบอร์โทรศัพท์ ฯลฯ เพื่อทาการลงทะเบียน ผู้ประกอบการจึงสามารถนาข้อมูลเหล่านี้มาสร้างฐานข้อมูล (Database) เพื่อใช้ในการวิเคราะห์พฤติกรรมของผู้บริโภค เพื่อนามาปรับปรุงรูปแบบการทาการตลาด หรือนามาวิเคราะห์เพื่อพัฒนาสินค้าของตน ยิ่งไปกว่านั้นยังสามารถนาฐานข้อมูลเหล่านี้มาใช้ในการติดต่อสื่อสารกับผู้บริโภคได้โดยตรง แต่หลังจากที่ประกาศเรื่องลักษณะและวิธีการส่ง และลักษณะและปริมาณของ

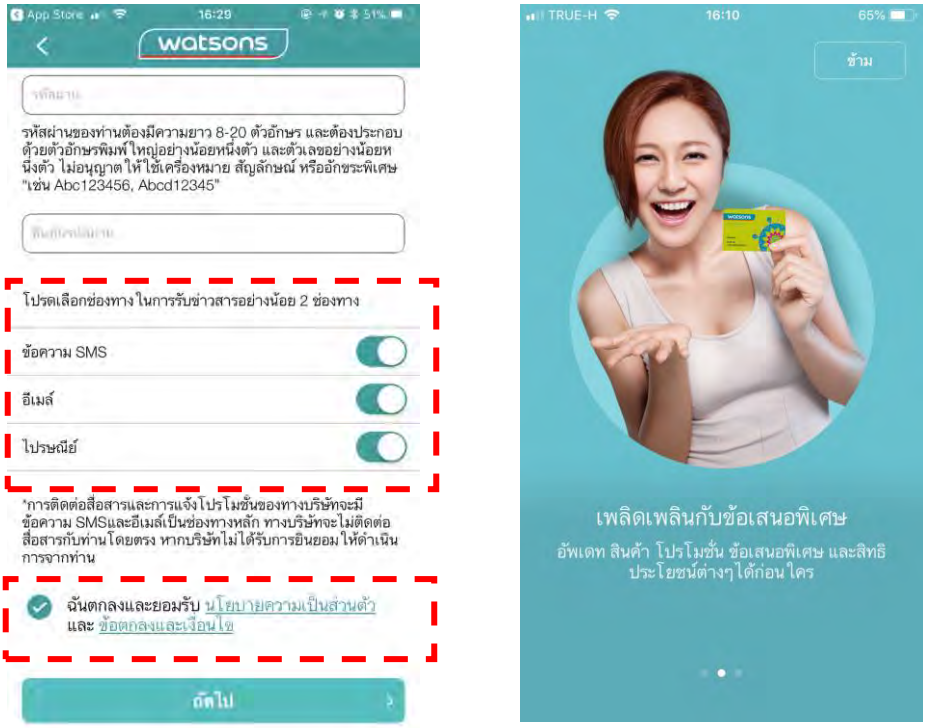
---

[29] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส พ.ศ. 2544, “ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

[30] Sunny Smile. โพสต์ฝากร้านค้าออนไลน์ กับเรื่องเข้าใจผิดในการโปรโมท Fanpage [ออนไลน์]. 2556. แหล่งที่มา: https://blog.lnw.co.th/2013/07/25/โพสฝากร้านค้าออนไลน์/ [20 มิถุนายน 2561]

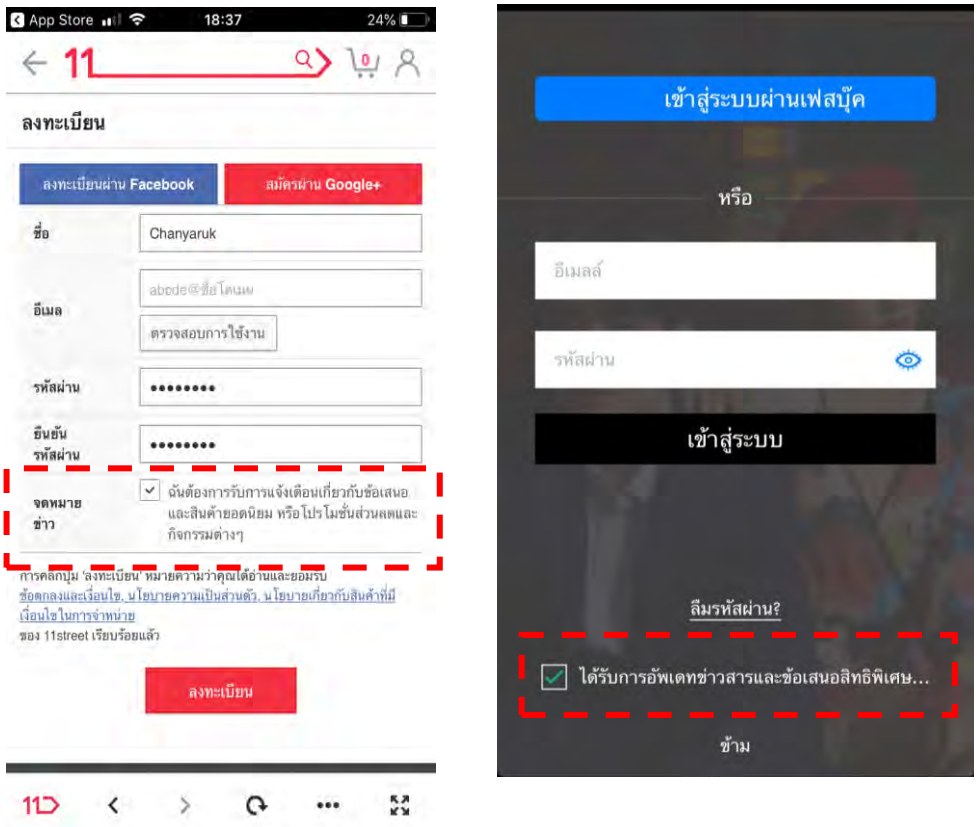
[31] Admin ITGenius. เทรนด์แอปพลิเคชั่นโลก [ออนไลน์]. 2016. แหล่งที่มา: https://www.itgenius.co.th/article/เทรนด์แอปพลิเคชั่นโลก [13 เมษยน 2561]

ข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนราคาญแก่ผู้รับ มีผลบังคับใช้ ผู้ประกอบการเริ่มหันมาใส่ใจในการขอความยินยอมจากผู้บริโภคก่อนที่จะทาการส่งข้อมูลโฆษณา โดยที่ด้านล่างของหน้าจอการลงทะเบียนมักจะแสดงข้อความเพื่อให้คายินยอมรับจดหมายข่าว และใส่เครื่องหมายแสดงความยินยอมค้างไว้ที่ข้อความนั้น ซึ่งผู้บริโภคจานวนมากมักเผอเรอมองข้ามจุดนี้ไป หรือบางแอปพลิเคชันอาจบังคับให้ทาการยินยอมเพื่อรับข้อมูลข่าวสาร ไม่เช่นนั้นจะไม่สามารถทาการลงทะเบียนได้เลย ดังนั้น การกระทาแบบนี้จึงยังเป็นจุดที่คลุมเครืออยู่ว่าการบังคับให้ยินยอมสามารถยึดถือเป็นคาให้และยืนยันในการยินยอม (affirmative consent)[32] ได้หรือไม่



ภาพที่ 14 ตัวอย่างจากแอปพลิเคชันของ Watsons
ที่ระบุให้ผู้ลงทะเบียนต้องท าการยินยอมในการรับข่าวสารอย่างน้อย 2 ช่องทาง

[32]CAN-SPAM Act, section 3 (1)



ภาพที่ 15 ตัวอย่างแอปพลิเคชัน 11 street และ Pomelo ที่ใส่เครื่องหมายในช่องยินยอม
เพื่อรับข้อมูลข่าวสารเอาไว้ล่วงหน้า

เมื่อผู้บริโภคได้มีการให้ความยินยอมรับข้อมูลข่าวสารด้วยวิธีดังกล่าวข้างต้นแล้ว ผู้ประกอบการมีสิทธิที่จะส่งอีเมลเชิงพาณิชย์มายังที่อยู่อีเมลที่ผู้บริโภคได้ให้ไว้ เมื่อไหร่ มากเท่าไหร่ ย่อมได้ เพราะปัจจุบันประเทศไทยยังไม่มีกฎหมายออกมากากับปริมาณหรือความถี่ในการส่งข้อมูล อีกทั้งผู้ประกอบการยังสามารถ ขอที่อยู่อีเมลนี้ไปใช้เพื่อส่งข่าวสารหรือประชาสัมพันธ์ในเรื่องอื่นๆ ได้อย่างอิสระตราบเท่าที่ข้อมูลนั้นมีความเกี่ยวเนื่องกับบริษัทของตน จนกว่าผู้บริโภคจะเข้าไป ดำเนินการเพื่อปฏิเสธรับเอง

สาหรับปัญหาเรื่องนี้มาตรา 3(1) ของ CAN-SPAM มีการกาหนดลักษณะของคายินยอมไว้อย่างชัดเจน โดย “การให้และยืนยันในการยินยอม” (affirmative consent) หมายถึง การที่ผู้รับให้ยินยอมอย่างชัดแจ้งที่จะได้รับข้อความไม่ว่าจะเป็นการตอบสนองต่อคาร้องที่จากผู้ส่ง หรือเป็นความต้องการที่เริ่มจากเจ้าตัวเอง ส่วนในสหภาพยุโรปก็กาลังร่างกฎหมายให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคฉบับใหม่ที่จะมีผลบังคับใช้ในปี 2018 ได้แก่ General Data Protection Regulation (GDPR) และระบุเรื่อง “ความยินยอม” (consent) ไว้ในพันธกรณีทั่วไป (General Obligations) ว่าเมื่อมีการประมวลผลข้อมูลจะต้องได้รับความยินยอมอย่างชัดแจ้ง (clear and affirmative consent) จากเจ้าของข้อมูล ซึ่งคาขอความยินยอมต้องอ่านแล้วเข้าใจง่าย ใช้ภาษาที่

รวบรัดชัดเจน และการถอนความยินยอมก็ต้องทาได้โดยง่ายเช่นกัน[33] และเพื่อควบคุมพฤติกรรมของบุคคลที่ใช้งานข้อมูลส่วนบุคคลของคนอื่นให้ครอบคลุมมายิ่งขึ้น จึงมีค าอธิบายเพิ่มเติมของระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Directive 95/46/EC) Article 7 ว่าบุคคลที่เป็นเจ้าของข้อมูล จะต้องให้ความยินยอมอย่างชัดเจน (clear and affirmative consent) ในการประมวลผลข้อมูลส่วนบุคคลของตน โดยการให้ความยินยอมนั้นจะต้องเป็นขั้นตอนที่เกิดโดยบุคคลแต่ละคน อาจหมายถึงการให้ทาเครื่องหมายที่ช่องยินยอมเมื่อเข้าสู่เว็บไซต์บนอินเทอร์เน็ต หรือการทาเครื่องหมายบริเวณคาแถลงที่ระบุว่ายอมรับการประมวลผลข้อมูลส่วนบุคคลที่เสนอไว้ แต่การทาเครื่องหมายที่ช่องเหล่านั้นไว้ล่วงหน้า (pre-ticked) จะไม่ถือว่าเป็นความยินยอม และต้องมีการเปิดช่องให้ถอนค ายินยอมได้โดยง่ายด้วย[34]

เมื่อพิจารณาจากบทบัญญัติของทั้งสองประเทศข้างต้น กฎหมายไทยควรจะเริ่มพิจารณาเรื่อง “ความยินยอม” ในบริบทของการบอกรับโฆษณาจากผู้ประกอบการให้ชัดเจน เพื่อป้องกันไม่ให้ผู้ประกอบการใช้การบังคับทางอ้อมว่าจะต้องเลือกช่องทางรับข่าวโฆษณาก่อนจึงจะสามารถสมัครใช้งานแอปพลิเคชันได้ แต่อาจให้ใช้วิธีทาเครื่องหมายคาไว้บริเวณช่องบอกรับเสมือนเป็นค าเชิญชวนแทน เพราะหากผู้บริโภคไม่ต้องการจริงๆเจ้าตัวก็ยังมีสิทธิ์กดเครื่องหมายนั้นออก

ปัญหาอีกประการเกี่ยวกับการใช้ข้อความเพื่อโฆษณาบนสื่อออนไลน์ได้แก่ “คลิกเบต” (Clickbait) หรือการใช้พาดหัวข่าวเพื่อเชิญชวนหรือกระตุ้นความสนใจจนทาให้ผู้บริโภคอยากคลิกลิงก์เชื่อมโยงเข้าไปยังเว็บไซต์เป้าหมาย ทั้งที่ความจริงเนื้อหาภายในเว็บไซต์นั้นจะไม่ได้มีเรื่องน่าสนใจเหมือนดังพาดหัวข่าวนั้นเลย การกระทารูปแบบนี้ยังคงเป็นสิ่งคลุมเครือที่กฎหมายยังไม่มีบทบัญญัติครอบคลุมถึง เนื่องจากผู้ที่สร้างเนื้อหาเหล่านี้ไม่ได้ใช้ข้อมูลเท็จ เพียงแต่ตั้งชื่อหัวเรื่องให้น่าสนใจเพื่อดึงดูดให้ผู้บริโภคคลิกเข้าไปเพิ่มยอดผู้เข้าชม (view) ให้แก่เว็บไซต์ เพื่อนามาซึ่งรายได้จากการขายพื้นที่โฆษณาต่ออีกทอดหนึ่งเท่านั้น ผู้ทาจึงไม่มีความผิดตามมาตรา 14 ว่าด้วยเรื่องการน าเข้าข้อมูลเท็จ ถึงแม้ว่าจะดูเหมือนเป็นการกระทาผิดที่ไม่รุนแรง แต่กล่าวได้ว่าเป็นการกระท าที่ขุ่นใจผู้บริโภคอย่างไม่เป็นธรรมได้เช่นกัน อีกทั้งผู้บริโภคยังต้องสิ้นเปลืองข้อมูลอินเทอร์เน็ต (internet data) ในการเปิดเข้าไปดูอีกด้วย

บทบัญญัติของกฎหมายต่างประเทศที่สามารถนาปรับมาใช้กับปัญหานี้ได้คือ CAN-SPAM ที่มีบทบัญญัติห้ามมิให้ใช้หัวเรื่องที่ทาให้เข้าใจผิดในสาระสาคัญของเนื้อหา (deceptive subject headings)[35] โดยเจตนา เพราะหากสามารถกาหนดมาตรฐานการใช้หัวเรื่อง (header) ได้เหมาะสม ย่อมต้องเป็นประโยชน์ต่อผู้บริโภคตามที่กล่าวไปในข้อ 5.1 เรื่ององค์ประกอบทางความผิด

---

[33] blogone. sunnywalker. รู้จัก GDPR กฎใหม่คุ้มครองข้อมูลยุโรป ข้อมูลเก็บที่ไหน กฎหมายตามไปคุ้มครองที่นั่น [ออนไลน์]. 2018. แหล่งที่มา: https://www.blognone.com/node/100324 [13 เมษยน 2561]

[34] Rikke ULDALL. "Q&A: New Eu Rules on Data Protection Put the Citizen Back in the Driving Seat." edited by GUILLOT, J. D.: The European Parliament, June 1, 2016.

[35] CAN-SPAM Act, section 5 (a)(2)

ภาพที่ 16 ตัวอย่างลักษณะการพาดหัวข่าวเพื่อจุดประสงค์ในการคลิกเบต[36]

แม้ปัจจุบันจะยังไม่มีคดีความที่เกี่ยวกับการส่งสแปมเมลในประเทศไทยออกมาให้เห็นมากเท่าไรนัก แต่ก็ปฏิเสธไม่ได้ว่าความเดือดร้อนที่เกิดขึ้นจากปัญหานี้มีอยู่ทั่วไปและใกล้ตัวกับทุกคนในสังคม หลายคนอาจมองว่าเป็นเพียงปัญหาเล็กน้อยที่ท าให้เกิดความหงุดหงิดกวนใจเพียงเท่านั้น ผลกระทบที่เกิดขึ้นกับผู้บริโภคแต่ละรายจึงไม่รุนแรง และยังไม่มีกระแสต่อต้านที่รุนแรงในสังคม ท าให้ไม่มีผู้เสียหายรายใดออกมาด าเนินคดีให้เสียเวลาหรือค่าใช้จ่าย แต่หากเรามองถึงภาพใหญ่ภาระที่เกิดขึ้นกับผู้ให้บริการเครือข่าย หรือองค์กรต่างๆที่ต้องคอยหามาตรการที่ทันสมัยอยู่เสมอเข้ามาดักจับสแปมเมลเพื่อไม่ให้การจราจรบนระบบอินเทอร์เน็ต (Internet Traffic) เกิดความขัดข้อง รวมถึงปัญหาด้านสิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภคที่ถูกนาข้อมูลส่วนบุคคลไปใช้โดยที่เจ้าตัวไม่ได้ตั้งใจให้ค ายินยอม ย่อมเป็นปัญหาส าคัญที่ไม่อาจเมินเฉยอยู่ได้

5.2 ข้อที่นักการตลาดพึงระวังในการใช้อีเมลเชิงพาณิชย์เพื่อทาการตลาด

จากการขยายตัวของตลาดพาณิชย์อิเล็กทรอนิกส์ (e-commerce) และการเปลี่ยนแปลงพฤติกรรมการซื้อของผู้บริโภคทั้งในและนอกประเทศ วิถีชีวิตที่เร่งรีบทาให้ผู้บริโภคหันมาซื้อของผ่านระบบออนไลน์กันมากกว่าจับจ่ายทางหน้าร้านเช่นเดิม ผู้ประกอบการหลายรายจึงต้องผันตัวเองจากที่เคยอยู่แต่ในตลาดออฟไลน์เข้ามาอยู่ในตลาดออนไลน์เพื่อความอยู่รอด บางธุรกิจอาจใช้ช่องทางออนไลน์เป็นเสมือนสาขาของหน้าร้านหลักที่ช่วยอานวยความสะดวกให้ลูกค้าสามารถเข้าไปชมสินค้าได้จากทุกแห่งทุกเวลา หรือบางธุรกิจอาจใช้ช่องทางออนไลน์เป็นเครื่องมือในการสื่อสารทางตรงกับตัวผู้บริโภคและเพื่อศึกษาพฤติกรรมของกลุ่มลูกค้า แม้กระทั่งห้างสรรพสินค้าหรือแบรนด์เสื้อผ้ารายใหญ่ๆที่เคยจาหน่ายเพียงที่หน้าร้าน (shop) ยังต้องหันมาสร้างเว็บไซต์หรือพัฒนาแอปพลิเคชันของตนเองขึ้นมาเพื่อเพิ่มโอกาสในการจ าหน่ายสินค้า

[36] ปานระพี. In เตือนคนไทย ระวังคลิกเบท clickbait: บทความไอที 24 ชั่วโมง, 1 พฤศจิกายน 2016.

แม้ว่าการเข้ามาในตลาดออนไลน์จะมีส่วนทาให้ผู้ประกอบการต้องเพิ่มการลงทุนด้านเทคโนโลยีและการจ้างงานผู้เชี่ยวชาญเพื่อพัฒนาระบบ ซึ่งอาจส่งผลทาให้ต้นทุนทางการค้าเพิ่มสูงขึ้น แต่หากมองในระยะยาว การลงทุนรูปแบบนี้ย่อมส่งผลดีในแง่การเพิ่มช่องทางกระจายสินค้า (Channel) ขยายโอกาสในการขาย (Lead) การโฆษณาประชาสัมพันธ์ (Advertise) และการชิงส่วนแบ่งทางการตลาด (Market Shares) ยิ่งไปกว่านั้น ศูนย์วิจัยกสิกรไทยยังชี้ให้เห็นว่าตลาดการพาณิชย์อิเล็กทรอนิกส์จะยังคงมีแนวโน้มขยายตัวมากขึ้น 17% ต่อปี โดยในปี 2565 อาจมีมูลค่าถึง 8.2% จากมูลค่าในตลาดค้าปลีกทั้งหมด[37] จากแนวโน้มดังกล่าว ภาครัฐจึงควรเตรียมพร้อมรับมือให้ทันต่อสถานการณ์ของตลาด ไม่ว่าจะเป็นด้านกฎหมายที่รองรับเกี่ยวกับความปลอดภัยในการด าเนินกิจการและคุ้มครองสิทธิของผู้บริโภค มาตรการเพื่อส่งเสริมและอานวยความสะดวกให้ผู้ประกอบการสามารถแข่งขันในตลาดได้อย่างเป็นธรรม ส่วนทางด้านผู้ประกอบการเอง หากตัดสินใจจะใช้อีเมลในการโฆษณาประชาสัมพันธ์ ก็ควรจะต้องศึกษาแนวทางที่มีประสิทธิภาพในการสร้างผลกาไรและสามารถตอบสนองต่อความต้องการของผู้บริโภคได้ รวมไปถึงต้องศึกษากฎหมายที่เกี่ยวข้องเพื่อให้ตนเองสามารถด าเนินกิจกรรมทางการตลาดได้อย่างปลอดภัย

5.2.1 การศึกษากลุ่มลูกค้าเป้าหมายเพื่อให้เกิดประสิทธิภาพในการสื่อสาร

การที่จะทาให้การโฆษณาทางอีเมลประสบผลสาเสร็จ นักการตลาดจะต้องกาหนดลูกค้าเป้าหมายและแบ่งกลุ่ม (segment) ของลูกค้านั้นให้ชัดเจนก่อนเป็นอันดับแรก เพื่อแยกกลุ่มลูกค้าที่ต้องการติดต่อ เนื่องจากลูกค้าในแต่เพศแต่ละช่วงวัยมีพฤติกรรมและความสนใจที่แตกต่างกัน ประวัติการใช้บริการ หรือการมีส่วนร่วมกับอีเมล (e-mail engagement) เป็นตัวช่วยให้นักการตลาดสามารถวิเคราะห์เพื่อหาแนวทางในการสร้างเนื้อหา (content) ที่เหมาะสมกับลูกค้าแต่ละกลุ่มได้ เช่น กลุ่มลูกค้าที่เคยใช้บริการหรือมีอัตราการมีส่วนร่วมสูง ควรเน้นที่การส่งอีเมลประชาสัมพันธ์ข่าว-สารหรือส่วนลดราคา (promotional e-mails) หากเป็นลูกค้าที่ใช้บริการครั้งแรก ควรเน้นไปที่เนื้อหาเกี่ยวกับการแนะนาผลิตภัณฑ์ หรือเป็นเนื้อหาแสดงความขอบคุณสาหรับการ เลือกใช้ผลิตภัณฑ์ของบริษัท เพื่อให้ลูกค้าเกิดความประทับใจ (impression) และการจดจาในตัวผลิตภัณฑ์ (awareness) ประเด็นเหล่านี้มีส่วนช่วยให้ผู้รับไม่เกิดความราคาญใจเวลารับอีเมลจนกดรายงาน (report) อีเมลนั้นไปยังผู้ใช้บริการอีเมล

การโดนกดรายงาน (report) นามาซึ่งปัญหาให้กับผู้ประกอบการมากมาย ไม่ว่าจะเป็นด้านภาพลักษณ์ชื่อเสียงของบริษัท หรือเสียเวลาที่จะต้องยื่นเรื่องไปยังผู้ให้บริการอินเทอร์เน็ตเพื่อขอปลดรายชื่อตนเองออกจากบัญชีดา (blacklist) วิธีการป้องกันไม่ให้โดนผู้รับกดรายงาน (report) วิธีหนึ่งก็คือ การใช้หลัก opt-in ในการส่งอีเมล เพราะถ้าเป็นสิ่งที่ผู้รับเคยให้ความยินยอมเอาไว้เอง แนวโน้มที่จะมีทัศนคติเชิงลบกับบริการอีเมลเหล่านั้นจะมีน้อยลง ตามประกาศกระทรวงดิจิทัลเพื่อ

---

[37] ศูนย์วิจัยกสิกรไทย. ปรับธุรกิจให้ทัน รับกระแส E-Commerce โต [ออนไลน์]. 14 กรกฎาคม 2560. แหล่งที่มา: https://www.kasikornbank.com/th/business/sme/KSMEKnowledge/article/KSMEAnalysis/Pages/E-Commerce_E-MarketPlace.aspx]

เศรษฐกิจและสังคมได้ออกประกาศเรื่อง ลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ข้อ 5 กาหนดให้การส่งอีเมลเชิงพาณิชย์ต้องได้รับความยินยอมจากผู้รับก่อนเช่นเดียวกับระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Directive 95/46/EC) ในสหภาพยุโรป ดังนั้นผู้ประกอบการที่ต้องการรวบรวมรายชื่อลูกค้าเพื่อส่งอีเมล ควรจะมีการสร้างช่องให้ระบุความยินยอมรับข่าวสารไว้ที่ใบสมัครใช้บริการ ใบลงทะเบียนรับประกันสินค้า หรือบนระบบลงทะเบียนแอปพลิเคชันที่ผู้บริโภคโหลดมาใช้งาน

ยิ่งไปกว่านั้น นักการตลาดผู้สร้างอีเมลเชิงพาณิชย์จะต้องไม่ลืมเตรียมช่องทางสาหรับการบอกปฏิเสธรับ (opt-out) ที่เห็นได้ชัดและเข้าใจได้ง่ายไว้ในอีเมลนั้นๆ เพื่อให้สอดคล้องกับบทบัญญัติข้อ 5(1) ในประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้เรื่อง ลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ นอกจากนี้ผู้ประกอบการควรมีการเตรียมการเพื่อจัดทารายชื่อผู้ปฏิเสธไม่รับอีเมลเชิงพาณิชย์ (opt-out list) เพราะแม้ว่ากฎหมายในประเทศไทยจะยังไม่มีบทบัญญัติเกี่ยวกับเรื่องนี้เหมือนสหรัฐอเมริกา[38] แต่ผู้ประกอบการควรตระหนักในจุดนี้ เพื่อป้องกันไม่ให้เกิดการส่งอีเมลเข้าไปหารายชื่อเหล่านี้ซ้า และเก็บไว้เป็นฐานข้อมูลเพื่อประเมินพฤติกรรมผู้บริโภค

5.2.2 การสร้างเนื้อหาที่เหมาะสมและเกิดประสิทธิภาพในการจูงใจผู้บริโภค

ปัจจัยสาคัญที่จะทาให้การโฆษณาหรือการส่งข้อมูลถึงผู้บริโภคเกิดขึ้นอย่างมีประสิทธิภาพและประสิทธิผล คือ ลักษณะของเนื้อหา (content) และวิธีการนาเสนอเนื้อหานั้นๆ (presentation) ผู้ประกอบการจานวนมากที่ใช้วิธีทาการตลาดผ่านอีเมล แต่ไม่ได้รับผลตอบแทนกลับมาอย่างที่คาดหวัง เนื่องจากนักการตลาดที่เป็นคนสร้างอีเมลไม่ได้ศึกษาถึงความสนใจและพฤติกรรมของลูกค้าที่เป็นกลุ่มเป้าหมายมากพอและไม่เคยศึกษาถึงหลักเกณฑ์ในการส่งอีเมล ระบบการส่งผ่านข้อมูลบนอินเทอร์เน็ต ระบบป้องกันความปลอดภัย หรือนโยบายด้านความปลอดภัยที่เกี่ยวข้องกับการส่งอีเมลเลย ดังนั้นถึงแม้จะสามารถสร้างเนื้อหา (content) ได้ดี แต่ถ้าไม่ได้ใช้หัวจดหมาย (subject) ที่น่าสนใจมากพอ โอกาสที่ผู้รับจะเปิดอ่านย่อมน้อยลง หรือถ้าเนื้อหาในอีเมลขัดกับนโยบายของระบบที่เกี่ยวข้องกับการส่งผ่านอีเมล แน่นอนว่าอีเมลเหล่านั้นย่อมส่งไปไม่ถึงผู้บริโภค หรืออาจถูกโอนเข้าไปยังกล่องจดหมายขยะ (spam box) ทาให้ผู้รับไม่ได้ใส่ใจที่จะเปิดเข้าไปอ่าน

การสร้างเนื้อหา (content) ที่สามารถจูงใจผู้บริโภค อันดับแรกจะต้องเข้าใจว่าใครคือกลุ่มเป้าหมาย และกลุ่มเป้าหมายนั้นมีพฤติกรรมการรับสื่อ (media) อย่างไร ถึงจะสามารถ

---

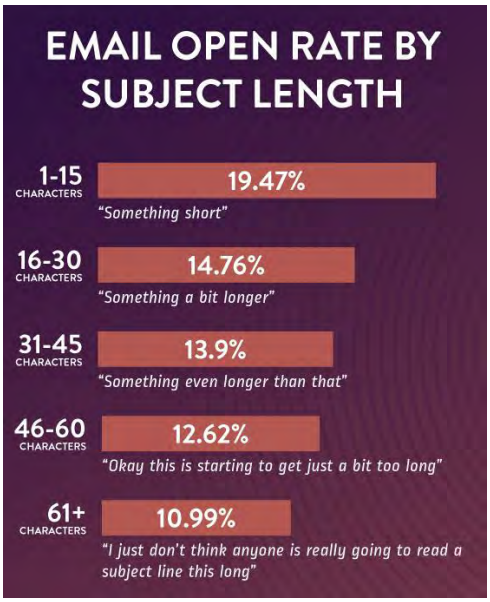
[38] CAN-SPAM Act, section 9 (a) IN GENEP~.--Not later than 6 months after the date of enactment of this Act, the Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce a report that--

(1) sets forth a plan and timetable for establishing a nationwide marketing **Do-Not-E-Mail registry**;

(2) includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a registry; and

(3) includes an explanation of how the registry would be applied with respect to children with e-mail accounts.

วิเคราะห์ได้ว่าอีเมลแบบไหนถึงจะสามารถเพิ่มโอกาสในการเปิดอ่านได้ การตั้งชื่อหัวเรื่องที่ดี ควรใช้ภาษาที่เข้าใจง่าย ชัดเจน กระชับ อาจตั้งชื่อด้วยประโยคคาถามหรือใช้เครื่องหมายอัศเจรีย์ (!) เพื่อกระตุ้นให้ผู้รับเกิดความอยากรู้ร่วมด้วยก็ได้ จากการส ำรวจของ Graphly ที่เป็นบริษัทผู้ให้บริการด้านการวางระบบและการทาการตลาดออนไลน์ พบว่าความยาวของหัวเรื่อง (subject) เป็นปัจจัยสาคัญอย่างหนึ่งในการช่วยกระตุ้นให้ผู้บริโภคเปิดอ่านอีเมล ชื่อหัวเรื่องที่ยาวเกินไปจะท าให้โอกาสในการถูกเปิดมีน้อยลง โดยหัวเรื่องที่มีตัวอักษรมากกว่า 61 ตัวอักษรมีอัตราการถูกเปิดอ่านเพียง 10.99% ในขณะที่อีเมลที่มีหัวเรื่องสั้นๆราว 1-15 ตัวอักษรมีอัตราการถูกเปิดอ่านถึง 19.47%[39] (อ้างอิงภาพที่ 11) สาเหตุประการหนึ่งที่ทาให้อีเมลที่มีชื่อหัวเรื่องสั้นได้รับความสนใจมากกว่าคือ พฤติกรรมการรับสื่อของผู้บริโภคที่เปลี่ยนแปลงไป โดยปัจจุบันคนหันมาใช้โทรศัพท์มือถือในการสื่อสาร หรือตรวจสอบอีเมลมากกว่าการใช้คอมพิวเตอร์หรือโน้ตบุ๊กเหมือนสมัยก่อน ดังนั้นเมื่ออุปกรณ์ (device) ที่ใช้งานมีขนาดเล็กลง สัดส่วนในการแสดงผลของหน้าจอจึงแคบลงตามไปด้วย การใช้หัวเรื่องที่กระชับ ได้ใจความ อ่านเข้าใจได้ง่าย จึงมีส่วนให้ผู้รับเกิดความสนใจที่จะเปิดดูเนื้อหาที่อยู่ด้านในมากกว่า



ภาพที่ 17 ผลการส ำรวจความยาวของหัวเรื่อง (subject) อีเมลที่ส่งผลต่ออัตราการเปิดอ่านโดยผู้รับ[40]

ปัจจุบันพระราชบัญญัติว่าด้วยการกระทาผิดทางคอมพิวเตอร์บัญญัติไว้เพียงห้ามปกปิดหรือปลอมแปลงแหล่งที่มาในการส่งข้อมูล ไม่ได้ระบุถึงเรื่องหัวจดหมาย (Header) แต่ผู้ประกอบการควรคานึงถึงกฎหมายที่เกี่ยวข้องทั้งในประเทศของผู้จัดทาและประเทศปลายทางผู้รับ รวมไปถึงนโยบายความปลอดภัยของระบบที่เกี่ยวข้องกับการส่งอีเมล หากผู้ประกอบการรู้ว่าปลายทางผู้รับมีถิ่นฐานอยู่ในสหรัฐอเมริกา ควรต้องใช้ชื่อหัวเรื่องที่ชัดเจนเพื่อให้ผู้รับสามารถตีความในสาระสาคัญหรือบริบทของเนื้อหาที่อยู่ในอีเมลนั้นได้ในทันที อีกทั้งยังต้องให้ความระวังเกี่ยวกับ

[39] Jarrod Morris. Why Do People Open Emails? [Online]. 2016. Available from: https://graphly.io/why-do-people-open-emails/ [24 April 2018]

[40] Ibid.

รายละเอียดที่ต้องแสดงในแถบผู้ส่ง (from line) ว่าต้องละเอียดมากพอที่ผู้รับจะสามารถระบุตัวตนของผู้จัดทาได้ และหากเป็นอีเมลที่มีเนื้อหาเกี่ยวกับเรื่องเพศ จะต้องมีการแสดงฉลากคาเตือน (warning label) ให้สอดคล้องตามที่ CAN-SPAM บัญญัติไว้ มิเช่นนั้นอีเมลเหล่านั้นอาจโดนดักโดยระบบป้องกันความปลอดภัยจนไม่สามารถส่งถึงผู้รับได้

นอกจากการตั้งชื่อหัวเรื่องที่น่าสนใจและสอดคล้องกับบทบัญญัติของกฎหมายที่เกี่ยวข้องแล้ว เนื้อหาด้านในของอีเมลก็มีความสาคัญไม่แพ้กัน การตั้งชื่อหัวเรื่องที่ดีอาจมีส่วนช่วยในการเพิ่มอัตราการคลิกผ่าน (Click through Rate: CTR) ได้ก็จริง แต่ไม่สามารถยืนยันได้ว่าผู้รับมีความสนใจในเนื้อหานั้นจริงหรือไม่ การออกแบบเนื้อหา (content) ด้านในให้น่าสนใจ ชัดเจน เข้าใจง่าย และตรงกับความต้องการของผู้รับแต่ละกลุ่ม เป็นส่วนสาคัญที่จะทาให้เกิดประสิทธิภาพในการสื่อสาร ปัจจุบันการประยุกต์ใช้ Infographic (Information Graphic) เป็นอีกหนึ่งทางเลือกที่นักการตลาดนิยมมากในปัจจุบัน เนื่องจากการอธิบายด้วยรูปภาพจะท าให้ผู้รับเข้าใจประเด็นที่ต้องการจะสื่อได้ง่ายและเร็วมากขึ้น แต่ข้อจากัดบางประการของฝั่งผู้รับอาจทาให้ไม่สามารถแสดงผลรูปภาพเหล่านั้นได้ทันที นักการตลาดจึงควรผสมผสานระหว่างการใช้รูปภาพและตัวอักษร (text) ให้สมดุลกัน โดยที่ใต้รูปภาพควรจะมี คาอธิบายใต้ภาพ (Alternate Text : Alt Text) เพื่อเป็นตัวช่วยในการอธิบายรูปภาพในกรณีอุปกรณ์ (device) ของผู้รับไม่สามารถแสดงผลรูปภาพนั้นได้ และการใช้คาศัพท์ที่เหมาะสมเพื่อกระตุ้นทาให้ผู้บริโภครู้สึกอยากมีส่วนร่วม รวมถึงเลือกใช้ตัวอักษรที่มีความโดดเด่น เช่น ตัวหนา หรือตัวอักษรที่มีสีสันตัดกันเพื่อดึงดูดความสนใจ ก็เป็นอีกตัวช่วยที่จะท ให้ผู้รับเกิดความจดจ าในเนื้อหานั้น[41]

5.2.3 ขนาดจานวนอีเมลเชิงพาณิชย์ที่เหมาะสมสาหรับการส่งออกในแต่ละครั้ง

ผู้ประกอบการที่ต้องการทาการตลาดโดยใช้อีเมลเป็นเครื่องมือในการส่งข้อความถึงผู้บริโภค ควรทาความเข้าใจเกี่ยวกับนโยบาย (Policy) รักษาความปลอดภัยของผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider: ISPs) และผู้ให้บริการอีเมล (Email Server Provider: ESP) แต่ละเจ้าให้ดีด้วย เนื่องจากกว่าที่อีเมลจะผ่านเข้าไปถึงกล่องจดหมาย (Primary inbox) ของผู้บริโภคได้ จะต้องผ่านระบบและกระบวนการคัดกรองของทั้งจาก ISPs และ ESP หลายขั้นตอน หากเป็นอีเมลที่มีเนื้อหาขัดกับนโยบาย (Policy) หรือเป็นอีเมลจากที่อยู่ที่น่าสงสัยหรือติดบัญชีดา (Blacklist) ของระบบอยู่ อีเมลเหล่านั้นจะถูกตีกลับไปยังผู้ส่ง หรือโดนโอนไปยังกล่องข้อความขยะ (spam box) ทันที ซึ่งอีเมลที่ค้างอยู่ในข้อความขยะ (spam box) จะถูกระบบลบออกไปโดยอัตโนมัติหากผู้รับไม่ได้เข้ามาเปิดอ่านภายใน 30 วันหลังจากที่รับอีเมลเข้ามา[42]

---

[41] Jason Chainey. "12 Tips to Achieve Success with Email Marketing." In Marketing Tips: How to Plan for Success. Market Location Inc., 11 December 2017.

[42] Google. นโยบายโปรแกรม [ออนไลน์]. 2018. แหล่งที่มา: https://support.google.com/mail/answer/7015314?hl=th&co=GENIE.Platform=iOS [เข้าถึงเมื่อ 17 พฤษภาคม 2561]

ถึงแม้จะเป็นอีเมลจากบริษัทรายใหญ่ที่เป็นที่รู้จักทั่วโลก เช่น สายการบินไลอ้อนแอร์ หรือ Apple Inc. ก็มีโอกาสที่จะโดนระบบป้องกันของผู้ให้บริการอีเมลดักจับว่าเป็นสแปม หากข้อความที่ผู้ประกอบการพยายามส่งมาถึงผู้บริโภคถูกโอนไปไว้ในกล่องจดหมายขยะ (spam box) ก็จะทาให้สูญเสียโอกาสในการถูกเปิดอ่านไปในที่สุด สาเหตุส่วนหนึ่งก็เพราะหลักเกณฑ์ในการคัดกรองสแปมเมลยังคงมีความแตกต่างกันแล้วแต่นโยบายของผู้ให้บริการแต่ละราย บางรายอาจไม่ได้พิจารณาเพียงแค่ความสัมพันธ์ (relation) ระหว่างผู้ส่งกับผู้รับเท่านั้น แต่ยังพิจารณาจากปริมาณการส่งแต่ละครั้งที่จ่ายออกมาจากที่อยู่ไอพี (IP address) ของผู้ส่งด้วย ซึ่งในประเทศไทยยังไม่มีกฎหมายใดบัญญัติเกี่ยวกับความถี่ ระยะห่าง ปริมาณ และขนาดในการส่งอีเมลที่เข้าข่ายว่าเป็นสแปมเอาไว้ ผู้ให้บริการจึงสามารถกาหนดนโยบายของตนเองได้โดยอิสระ ตัวอย่างเช่น Microsoft 360 จากัดข้อความอีเมลที่ส่งจากบัญชีอีเมล Cloud-Based หนึ่งบัญชีในช่วงระยะเวลา 24 ชั่วโมง ผู้รับสาหรับ Exchange Online อยู่ที่ 1,500 คนต่อวัน[43] ผู้ประกอบการจึงควรพึงระวังด้วยตนเองว่ายิ่งจานวนอีเมลที่ส่งในแต่ละครั้งมีมากเท่าไหร่ ความเสี่ยงที่อีเมลเหล่านั้นจะถูกโอนไปยังกล่องจดหมายขยะ (spam box) ก็มีมากขึ้นเท่านั้น

เมื่อเปรียบเทียบกับสหรัฐอเมริกาที่มีการกาหนดจานวนการส่งเชิงทวีคูณ (Multiple) ที่เข้าข่ายเป็นการทาสแปมที่ขัดต่อกฎหมายไว้อย่างชัดเจนใน CAN-SPAM มาตรา 4(b)(C)[44] ทาให้ผู้ให้บริการที่อยู่ในประเทศสามารถอ้างอิงมาตรฐานเดียวกันในการกาหนดนโยบายการใช้งานของตน ด้านผู้ประกอบการก็สามารถยึดเป็นแนวทางในการดาเนินกิจกรรมทางการตลาดของตนได้

ปัญหาอีกประการที่สาคัญคือ “ขนาดของอีเมล” (email size) โดยเฉพาะอย่างยิ่งผู้ส่งที่ใช้รูปภาพหรือคลิปวิดีโอแนบท้ายบริเวณ signature ของผู้ส่ง เนื่องจากการส่งไฟล์ขนาดใหญ่จ นวนมากในเวลาเดียวกัน จะทาให้การจราจรบนแบนด์วิดท์ (bandwidth) ของระบบรับส่ง (Data-Transfer) เกิดปัญหาคอขวด ทาให้การส่งผ่านข้อมูลหยุดชะงักได้ ข้อมูลจากบริษัท ลอยด์ แห่งลอนดอน (Lloyd’s London) ระบุว่าในปี 2542 ที่ผ่านมา มีบริษัทพาณิชย์อิเล็กทรอนิกส์ (e-commerce) สูญเสียรายได้ราว 20 พันล้านดอลลาร์สหรัฐเนื่องจากการหยุดชะงักของระบบคอมพิวเตอร์ เช่น อีเบย์สูญเสียรายได้จากการจาหน่ายราว 5 ล้านดอลลาร์สหรัฐ[45] อีกทั้งการกระทาดังกล่าวอาจกลายเป็นความตามผิดมาตรา 10 ว่าด้วยการกระทาเพื่อให้การทางานของระบบคอมพิวเตอร์ไม่สามารถทางานได้ตามปกติ ดังนั้นผู้ส่งจึงควรคานวณขนาดของอีเมลให้ดีก่อนส่งออก

อย่างไรก็ตามการส่งอีเมลเป็นพฤติกรรมที่ยากจะกาหนดขอบเขตพื้นที่ แนวทางที่จะ

---

[43] Microsoft. อีเมลจ นวนมากและขีดจากัดอัตราผู้รับรายวัน. [ออนไลน์]. 2012. แหล่งที่มา: https://msdn.microsoft.com/th-th/library/ff381292(v=exchsrvcs.149).aspx [14 เมษายน 2561]

[44] CAN-SPAM Act, section 4 (b)(C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period;

[45] ชวลิต อัตถศาสตร์, ไพบูลย์ อมรภิญโญเกียรติ, พัชรินทร์ ฉัตรวชิระกุล, อิทธินันท์ สุวรรณจูฑะ. กฎหมายไซเบอร์. บริษัท เนชั่น มัลติมีเดีย กรุ๊ป จากัด (มหาชน): บริษัท ซีเอ็ดยูเคชั่น จ ากัด (มหาชน), ตุลาคม 2545. หน้า 37

ช่วยให้เกิดความเสมอภาคได้มากที่สุดคือการที่องค์กรด้านอาชญากรรมคอมพิวเตอร์ หรือเหล่าผู้ให้บริการรายใหญ่ทั่วโลกหันมาร่วมมือกันเพื่อกาหนดแนวนโยบายที่เป็นบรรทัดฐานสากล แม้ปัจจุบันจะมีบางประเทศมีบทบัญญัติเกี่ยวกับจานวน ความถี่ หรือปริมาณในการส่งอีเมลแล้วก็ตาม แต่หากทาให้ทั่วโลกมีมาตรฐานเดียวกันได้ ย่อมเป็นการสนับสนุนให้เกิดการทากิจกรรมทางการตลาดที่โปร่งใส และเป็นการปกป้องสิทธิของผู้รับได้อย่างเท่าเทียมกัน

5.3 การคุ้มครองสิทธิความเป็นอยู่ส่วนบุคคล (Rights of privacy) ของผู้บริโภค

จากการที่ผู้ประกอบการสามารถเข้าถึงข้อมูลส่วนบุคคล (Personal Data) ของผู้บริโภคได้ด้วยวิธีการดังที่กล่าวไปข้างต้น ที่อยู่อีเมลจึงถูกกระทาเหมือนไม่ใช่ข้อมูลส่วนบุคคลอีกต่อไป ผู้ประกอบการบางรายที่ไร้จรรยาบรรณอาจทาการซื้อขายหรือแลกเปลี่ยนข้อมูลของผู้บริโภคที่ตนถือครองอยู่ แม้ปัจจุบันกฎหมายเกี่ยวกับการคุ้มครองสิทธิความเป็นอยู่ส่วนบุคคลด้านข้อมูลส่วนบุคคลในประเทศไทยมีบัญญัติอยู่ในหลายพระราชบัญญัติ แต่ยังไม่มีการบูรณาการเพื่อรวบรวมบทบัญญัติทั้งหมดที่มีให้ครอบคลุมถึงข้อมูลส่วนบุคคลทุกประเภท และให้คุ้มครองจากการใช้งานโดยบุคคลหรือธุรกิจทุกรูปแบบ อาทิเช่น ข้อมูลเบอร์โทรศัพท์ได้รับการคุ้มครองโดยพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มาตรา 50[46] ส่วนข้อมูลเครดิตหรือข้อมูลทางด้านการเงินของผู้บริโภคได้รับความคุ้มครองโดยพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 มาตรา 51[47] เพียงแต่คุ้มครองเฉพาะในขอบเขตการใช้งานโดยสถาบันการเงิน หรือบริษัทข้อมูลเครดิตเพียงเท่านั้น ไม่ได้กล่าวถึงการใช้งานโดยผู้ประกอบการประเภทอื่นๆ ส่วนข้อมูลที่อยู่อีเมลนั้น ยังไม่มีกฎหมายฉบับใดออกมาคุ้มครองการซื้อขาย หรือการถูกน ไปใช้งานด้วยจุดประสงค์อื่นนอกเหนือจากที่แจ้งความประสงค์ไว้ตอนส่งมอบข้อมูลโดยเฉพาะ

ยิ่งไปกว่านั้น ข้อมูลพฤติกรรมของผู้บริโภคส่วนหนึ่งมักถูกเก็บรวมรวมไว้บนเว็บไซต์ที่ถูกเข้าใช้งานโดยไม่รู้ตัว หรือที่เรียกกันว่า “คุกกี้” (cookies) เว็บไซต์อีคอมเมิร์ซรายใหญ่ๆมักมีการฝังโปรแกรมคุกกี้เข้าไปที่หน้าเว็บ เพื่อทาให้เครื่องคอมพิวเตอร์ของลูกค้าจดจาประวัติการเข้าถึงเพื่อย่นระยะเวลาในการเปิดใช้งานในคราวถัดไป หรือทาให้สามารถประมวลผลเพื่อแสดงโฆษณาสินค้าที่ลูกค้าให้ความสนใจออกมาให้เห็น ซึ่งลูกค้าที่เข้าใช้งานเว็บไซต์นั้นๆอาจไม่รู้ตัวเลยว่าประวัติการเข้าชมเว็บไซต์ ประวัติการทาธุรกรรม ชื่อ นามสกุล เบอร์โทร ที่อยู่อีเมล ได้ถูกเก็บรวมรวมไว้เป็นคุกกี้แล้ว กล่าวได้ว่า การถูกเก็บข้อมูลเช่นนี้ก็เป็นการละเมิดสิทธิเสรีภาพส่วนบุคคลได้เช่นกัน

---

[46] พระราชบัญญัติประกอบกิจการโทรคมนาคม พ.ศ 2544 มาตรา 50 ให้คณะกรรมการก หนดมาตรการเพื่อคุ้มครองผู้ใช้บริการเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม ให้ผู้รับใบอนุญาตมีหน้าที่ปฏิบัติตามมาตรการที่คณะกรรมการกาหนดตามวรรคหนึ่ง เมื่อพบว่ามีบุคคลใดกระท การละเมิดสิทธิของผู้ใช้บริการตามวรรคหนึ่ง ให้ผู้รับใบอนุญาตหรือคณะกรรมการดาเนินการเพื่อระงับการกระท ดังกล่าว และแจ้งให้ผู้ใช้บริการทราบโดยเร็ว

[47] พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 มาตรา 51 บริษัทข้อมูลเครดิตใดหรือผู้ประมวลผลข้อมูลผู้ใดเปิดเผยหรือให้ข้อมูลแก่สมาชิกของตนหรือผู้ใช้บริการเพื่อประโยชน์อย่างอื่นหรือเปิดเผยหรือให้ข้อมูลแก่ผู้อื่นนอกเหนือจากที่กาหนดในมาตรา 20 ต้องระวางโทษจ คุกไม่เกินห้าปี หรือปรับไม่เกินห้าแสนบาท หรือทั้งจ ทั้งปรับ

ในยุคที่การซื้อขายสินค้าออนไลน์กลายเป็นกิจกรรมที่เกิดขึ้นเป็นปกติทั่วไป จานวนธุรกรรม (Transaction) ที่เกิดขึ้นในแต่ละวันมีมูลค่ามหาศาล จึงเป็นธรรมดาที่ผู้ประกอบการทั้งรายใหญ่รายย่อยจะมีข้อมูลส่วนบุคคลของผู้บริโภคถือครองอยู่ในมือเป็นจานวนมาก เพราะอย่างน้อยการซื้อขายแต่ละครั้งผู้ซื้อต้องแจ้งข้อมูล อาทิ ชื่อ ที่อยู่ เบอร์โทรศัพท์ หรืออีเมลให้แก่ผู้ประกอบการ เพื่อทาการยืนยันการส่งสินค้าหรือยืนยันการชาระเงิน นี่จึงเป็นอีกหนึ่งช่องทางที่ทาให้ข้อมูลของผู้บริโภคหลุดรอดออกไปสู่สาธารณะได้โดยง่าย หากผู้ประกอบการรายนั้นๆไม่ได้จัดหามาตรการในการใช้งานหรือมาตรการในการรักษาความลับของข้อมูลลูกค้าที่ดีเพียงพอ สภาพในปัจจุบันบุคคลทั่วไปมักมีประสบการณ์ในการรับอีเมลโฆษณาขายสินค้าจากแหล่งที่ตนไม่เคยรู้จัก หรือรับโทรศัพท์จากผู้ที่ต้องการเสนอโปรโมชั่นบัตรเครดิต หรือได้รับจดหมายเชิญชวนให้ร่วมเป็นสมาชิกในกิจกรรมพิเศษฯลฯ ทั้งที่ในความจริงการกระทาดังกล่าวเปรียบเสมือนการรุกรานสิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภค และหากข้อมูลเหล่านี้หลุดรอดไปถึงมือของมิจฉาชีพ อาจนามาซึ่งการถูกหลอกลวงหรือคดีความต่างๆต่อไป

ตัวอย่างเกี่ยวกับการใช้งานข้อมูลผู้บริโภคโดยไม่มีมาตรการทางความปลอดภัยที่เพียงพออีกหนึ่งกรณีคือ การที่นาย Niall Merrigan นักวิจัยด้านความมั่นคงปลอดภัยของ Microsoft ASP.NET ได้เขียนลงบล็อกของตนเองในวันที่ 13 เมษายน 2018 กรณีที่เขาตรวจพบว่าบริษัท ทรู คอร์ปอเรชั่น จากัด (มหาชน) ที่เป็นผู้ให้บริการเครือข่ายโทรศัพท์มือถือรายใหญ่ในประเทศไทย มีการตั้งค่าเซิร์ฟเวอร์สาหรับจัดเก็บข้อมูลลูกค้า (AWS S3 Bucket) ไม่รัดกุม จนทาให้ข้อมูลสาเนาบัตรประชาชนของลูกค้าผู้มาลงทะเบียนซิมการ์ดในช่วงปี 2016-2018 ที่สแกนเก็บไว้กว่า 46,000 รายหลุดสู่สาธารณะในช่วงเดือนมกราคม 2018 ที่ผ่านมา[48] การเผยแพร่ข่าวในครั้งนี้ส่งผลกระทบต่อความน่าเชื่อถือในระบบบริหารจัดการข้อมูลส่วนบุคคลในประเทศไทยเป็นอย่างมาก อีกทั้ง ยังไม่มีบทบัญญัติของกฎหมายฉบับใดเข้ามารองรับความเดือดร้อนที่อาจเกิดขึ้นกับผู้บริโภคจากการที่ข้อมูลของตนหลุดออกสู่สาธารณะเช่นนี้ เพราะปัจจุบันมีเพียงพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 เท่านั้นที่สามารถนาบทบัญญัติมาปรับใช้ได้ ผู้บริโภคมีหน้าที่จะต้องส่งหนังสือร้องเรียนความเสียหายที่ระบุข้อเท็จจริงอย่างชัดแจ้ง พร้อมทั้งต้องเป็นผู้หาหลักฐานไปยื่นต่อคณะกรรมการกิจการโทรคมนาคมแห่งชาติด้วยตนเอง[49] จึงเท่ากับว่าต้องรอให้มีความเสียหายเกิดขึ้นจริงและผู้เสียหายต้องรู้ตัวก่อนถึงจะทาการร้องเรียนได้ ในความเป็นจริงกว่าผู้เสียหายจะรู้ว่าข้อมูลของตนถูกนาไปใช้ในทางมิชอบก็อาจสายเกินไป และการประเมินความเสียหายจากการกระทาเหล่านี้ก็เป็นเรื่องทางเทคนิคเฉพาะ ไม่ใช่เรื่องง่ายที่ประชาชนธรรมดาจะสามารถพิสูจน์ด้วยตัวเอง ยิ่งไปกว่า

---

[48] Niall Merrigan. Another Telco Is Failing at Security [Online]. 2018. Available from: https://www.certsandprogs.com/2018/04/another-telco-is-failing-at-security.html#axzz5CXkf6GxS [13 April 2018.]

[49] พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มาตรา 45 ผู้ใดได้รับความเดือดร้อนเสียหายอันเนื่องมาแต่การให้บริการโทรคมนาคมของผู้รับใบอนุญาต ผู้นั้นมีสิทธิร้องเรียนต่อคณะกรรมการได้ โดยท าเป็นหนังสือยื่นต่อสานักงาน หนังสือร้องเรียนตามวรรคหนึ่งต้องระบุข้อเท็จจริงที่แจ้งชัด และถ้ามีเอกสารหลักฐานที่เกี่ยวข้องกับกรณีดังกล่าวก็ให้ส่งไปพร้อมหนังสือนั้นด้วย ในระหว่างการพิจารณาค ร้องเรียนของคณะกรรมการ ถ้าผู้ร้องเรียนขอให้คณะกรรมการมีอ านาจพิจารณาก หนดให้ผู้รับใบอนุญาตด นินการใดเพื่อแก้ไขเยียวยาความเสียหายให้แก่ผู้ร้องเรียนเป็นการชั่วคราวได้

นั้น พระราชบัญญัติฯนี้ยังมีเพียงโทษทางปกครอง[50] ไม่ได้มีโทษทางแพ่งหรือโทษทางอาญาที่รุนแรงพอจะท าควบคุมให้ผู้ประกอบการเกิดวินัยด้านการใช้งานข้อมูลส่วนตัวของผู้บริโภค

เมื่อเปรียบเทียบกับสหภาพยุโรป ระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Directive 95/46/EC) ที่ให้คานิยามของคาว่า “ข้อมูลส่วนบุคคล” ไว้อย่างครอบคลุมทั้งหมด ไม่ว่าจะเป็นที่อยู่ ที่อยู่อีเมล เบอร์โทรศัพท์ วันเดือนปีเกิด เชื้อชาติ ศาสนา ฯลฯ และมีการจากัดหลักเกณฑ์ในการนาข้อมูลของผู้บริโภคให้สามารถนาไปใช้งานได้เพียงเท่าที่จาเป็นตามวัตถุประสงค์ที่ได้แจ้งไว้แต่แรกเท่านั้น เว้นแต่เป็นการทาโฆษณาสาหรับสินค้าที่มีลักษณะใกล้เคียง (like product) กับของเดิมที่ผู้รับให้คายินยอมไว้ จึงจะสามารถใช้หลัก inferred consent ได้ อีกทั้งการใช้โปรแกรมคุกกี้ยังถือเป็นการละเมิดสิทธิเสรีภาพส่วนบุคคล แต่เพื่ออานวยความสะดวกในการประกอบการของธุรกิจอีคอมเมิร์ซ คณะกรรมาธิการจึงมีนโยบายกาหนดให้ผู้ประกอบการสามารถใช้โปรแกรมคุกกี้ได้ เพียงแต่ต้องมีระบบแจ้งเตือน เช่น หน้าต่างอัตโนมัติ (Pop-up windows) ให้ผู้เข้าใช้งานทราบว่าเว็บไซต์ของตนมีการใช้โปรแกรมคุกกี้ และระบุรายละเอียดเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล พร้อมทั้งชี้แจงให้ทราบถึงโปรแกรมที่จะสกัดกั้นการทางานของคุกกี้ด้วย[51]

ดังนั้น การที่ประเทศไทยยังไม่มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะออกมาบังคับใช้ จึงเป็นช่องว่างให้ผู้ประกอบการที่ไม่ใช่ภาครัฐ หรือธุรกิจเฉพาะที่มีบทบัญญัติเฉพาะทางควบคุม สามารถน าข้อมูลของผู้บริโภคที่ตนได้มาจากการทาธุรกรรม ไปใช้เพื่อประโยชน์อย่างอื่นนอกเหนือจากจุดประสงค์ ณ เวลาที่ผู้บริโภคส่งมอบข้อมูลแต่แรก อีกทั้งยังไม่มีหลักเกณฑ์มาตรฐานให้ผู้ประกอบการใช้อ้างอิงเพื่อบริหาร จัดเก็บ ใช้งานข้อมูลเหล่านั้นๆ อย่างเหมาะสมและปลอดภัยต่อตัวผู้บริโภค ดังนั้นประเทศไทยจึงควรนาบทบัญญัติของสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในแง่ของนิยามคาว่า “ข้อมูลส่วนบุคคล” หรือการวางมาตรการเพื่อให้ผู้ประกอบการสามารถเก็บรวบรวม ใช้งาน ประมวลผล ข้อมูลผู้บริโภคได้ตามความสมควรที่พอเหมาะพอดี มาปรับใช้เพื่ออ้างอิงในการยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และผลักดันให้ร่างพระราชบัญญัติฯนี้มีผลบังคับใช้ในเร็ววัน

จากการวิเคราะห์เปรียบเทียบในครั้งนี้ จึงท าให้เห็นว่ากฎหมายในประเทศไทยที่เกี่ยวข้องกับการกระท าความผิดในรูปแบบสแปมยังมีจุดที่ควรปรับปรุงเพิ่มเติม และเห็นถึงแนวทางที่เหมาะสมในการนาเอาบทบัญญัติของกฎหมายต่างประเทศเข้ามาปรับใช้ในบริบทของสังคมไทย อันจะนาไปสู่บทสรุปและข้อเสนอแนะของการปรับปรุงแนวทางการทาการตลาดด้วยอีเมลเชิงพาณิชย์ของผู้ประกอบการ และแนวทางการพิจารณาเพิ่มเติมกฎหมายที่เกี่ยวข้องในบทถัดไป

---

[50] พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มาตรา 66 ในกรณีที่ผู้รับใบอนุญาตไม่ปฏิบัติตามค าสั่งของเลขาธิการตามมาตรา 64 และพ้นกาหนดระยะเวลาอุทธรณ์ตามมาตรา 65 หรือคณะกรรมการวินิจฉัยยืนตามค าสั่งเลขาธิการ เมื่อเลขาธิการได้มีหนังสือเตือนแล้วยังไม่มีการปฏิบัติตามค าสั่งนั้น ให้เลขาธิการพิจารณาก าหนดค่าปรับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง ซึ่งต้องไม่ต่ ากว่าสองหมื่นบาทต่อวัน

[51] ชวลิต อัตถศาสตร์, ไพบูลย์ อมรภิญโญเกียรติ, พัชรินทร์ ฉัตรวชิระกุล, อิทธินันท์ สุวรรณจูฑะ. กฎหมายไซเบอร์. หน้า 48-51

บทที่ 6
บทสรุปและข้อเสนอแนะ

ความก้าวหน้าทางเทคโนโลยีสารสนเทศส่งผลทั้งต่อระบบเศรษฐกิจและพฤติกรรมของผู้บริโภคในยุคปัจจุบัน แม้ว่าเทคโนโลยีสารสนเทศเป็นฟันเฟืองสาคัญในการขับเคลื่อนกิจกรรมของธุรกิจให้สามารถด าเนินได้อย่างสะดวก รวดเร็ว ประหยัดต้นทุนและทรัพยากร ซึ่งเป็นผลดีต่อภาพรวมของระบบเศรษฐกิจทั้งในและระหว่างประเทศ แต่ด้านผู้บริโภคเองก็สามารถใช้ประโยชน์จากเทคโนโลยีในการเข้าถึงข้อมูลข่าวสารต่างๆ และท าให้การด าเนินชีวิตในแต่ละวันง่ายและสะดวกสบายมากขึ้น อย่างไรก็ตามเทคโนโลยีเปรียบเสมือนดาบสองคมขึ้นอยู่กับจุดประสงค์ของผู้ใช้งานว่าจะน าไปใช้ในทางสุจริตหรือไม่ การฉ้อโกง ปล่อยข่าวลวง ขโมยข้อมูล ฯลฯ กลายเป็นปัญหาสาคัญที่หลายประเทศทั่วโลกตื่นตัว และบัญญัติกฎหมายออกมาเพื่อจากัดปราบปรามผู้ที่น าเทคโนโลยีไปใช้ในทางมิชอบ ด้านภาคธุรกิจเองก็มีการน าเทคโนโลยีมาประยุกต์ใช้เพื่อเป็นช่องทางในการสื่อการกับผู้บริโภคทางตรงเช่นกัน แต่ยิ่งการติดต่อสื่อสารท าได้ง่ายขึ้นเท่าไหร่ กาแพงกั้นที่กั้นความเป็นส่วนตัวของผู้บริโภคก็ยิ่งบางลงเท่านั้น ดังนั้นจึงควรมีการก าหนดกรอบหรือระเบียบที่เหมาะสมให้แก่ภาคธุรกิจ เพื่อคุ้มครองสิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภค แต่ยังคงรักษาประสิทธิภาพในการสื่อสารจากภาคธุรกิจไว้ได้ โดยในบทนี้จะบรรยายถึงบทสรุปเกี่ยวกับการบังคับใช้พระราชบัญญัติว่าด้วยความรับผิดเกี่ยวกับคอมพิวเตอร์ที่มีผลกระทบต่อการใช้อีเมลเชิงพาณิชย์ในข้อ 6.1 และเสนอแนะมาตรการทางกฎหมายเพื่อเป็นแนวทางในการส่งเสริมให้เกิดสภาพคล่องทางการประกอบธุรกิจในขณะที่ยังคงสามารถคุ้มครองสิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภคในประเทศไทยตามประเด็นต่างๆที่ได้ศึกษาเปรียบเทียบกับกฎหมายของต่างประเทศ ให้สอดคล้องกับบริบทของสังคมไทยในหัวข้อ 6.2

6.1 บทสรุป

ปัจจุบัน การใช้สแปมเมลมีจุดมุ่งหมายหลายรูปแบบ ทั้งในเชิงพาณิชย์และในการประกอบอาชญากรรม กล่าวได้ว่าเทคโนโลยีรูปแบบนี้ก่อให้เกิดทั้งผลดีและผลเสียต่อตัวผู้รับและต่อภาคธุรกิจในคราวเดียวกัน หากรัฐยังคงปล่อยให้การกระทารูปแบบนี้เกิดขึ้นได้โดยอิสระ ภาระค่าใช้จ่ายและผลกระทบด้านต่างๆจะตกอยู่ที่ตัวผู้รับหรือตกอยู่ที่ผู้ให้บริการที่เกี่ยวข้องกับการส่งเท่านั้น รัฐจึงมีความจาเป็นที่จะต้องเข้ามากาหนดขอบเขตของการกระทาเพื่อป้องกันสิทธิด้านต่างๆของผู้ที่ได้รับผลกระทบ และบทบัญญัติโทษสาหรับการกระทาความผิดให้ชัดเจน เพื่อป้องปรามไม่ให้เกิดการกระท าความผิดที่ส่งผลกระทบร้ายแรงต่อประชาชน

ประเทศแรกที่มีกฎหมายเกี่ยวกับการกระทาความผิดทางคอมพิวเตอร์บังคับใช้ได้แก่ สหรัฐอเมริกา โดยออกเป็นพระราชบัญญัติว่าด้วยการฉ้อโกงและการละเมิดคอมพิวเตอร์ (Computer fraud and abuse act : CFAA) ในปี 1986 มีจุดประสงค์เพื่อดูแลป้องกันและรักษาผลประโยชน์

ของรัฐในส่วนที่เกี่ยวข้องกับคอมพิวเตอร์ของรัฐบาลกลาง ระบบธนาคาร และระบบการค้า[1] และต่อมาเมื่อการกระทาผิดรูปแบบนี้เริ่มมีความซับซ้อนมากขึ้นเรื่อยๆ การกระทาหลายรูปแบบยากจะตีค่าความเสียหายออกมาเป็นมูลค่า หรือยากที่จะคาดเดาผลที่เกิดจากการกระท าหลายประเทศจึงเริ่มหันมาให้ความส าคัญด้านการปกป้องสิทธิความเป็นอยู่ส่วนบุคคล (Rights of Privacy) ของประชาชนทั่วไปที่ได้รับผลกระทบด้านลบจากการพัฒนาของเทคโนโลยี ตัวอย่างเช่นในสหภาพยุโรปที่มีการบังคับใช้ระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Directive 95/46/EC) ในปี 1995 จึงกล่าวได้ว่ายิ่งเทคโนโลยีสารสนเทศล่วงล้าเข้ามาในวิถีชีวิตของประชาชนมากขึ้นเท่าไหร่ กฎหมายที่นามาใช้ควบคุมยิ่งต้องมีบทบัญญัติที่ละเอียดอ่อน และครอบคลุมกับทุกแง่มุมมากขึ้นเท่านั้น

แม้ว่าการบัญญัติกฎหมายจะเป็นเครื่องมือเพื่อช่วยจากัดการกระทาความผิดและคุ้มครองสิทธิของประชาชน แต่ในขณะเดียวกันกฎหมายก็เป็นสิ่งจ ากัดเสรีภาพหรือความสะดวกในการด าเนินกิจกรรมทางธุรกิจด้วยเช่นกัน กฎหมายที่เข้มงวดมากเกินไปอาจกลายเป็นสิ่งขัดขวางการไหลเวียนในระบบเศรษฐกิจได้ ดังนั้น รัฐจึงต้องคานึงถึงสมดุลระหว่างตราชั่งทั้งสองฝั่งให้ดีเพื่อให้เกิดประโยชน์สูงสุดกับทุกภาคส่วนในสังคม ยิ่งในปัจจุบันที่ตลาดการพาณิชย์อิเล็กทรอนิกส์ (e-commerce) มีอัตราการเติบโตสูง พฤติกรรมการซื้อของผู้บริโภคที่เปลี่ยนแปลงไปทาให้ผู้ประกอบการหลายรายต้องผันตัวเข้าสู่ตลาดออนไลน์เพื่อความอยู่รอด และท่ามกลางความดุเดือดของการแข่งขันในตลาดออนไลน์นี้เอง นักการตลาดจึงควรหาช่องทางที่มีประสิทธิภาพในการติดต่อสื่อสารเพื่อโฆษณาประชาสัมพันธ์ (advertise) ให้ผู้ประกอบการเกิดความสัมพันธ์ที่ดีกับลูกค้าจนนาไปสู่การขยายโอกาสในการซื้อ (Lead) แม้ว่าปัจจุบันประเทศไทยจะมีกฎหมายที่เกี่ยวข้องกับการกระท าผิดดังกล่าวแต่ยังคงไม่สามารถคุ้มครองสิทธิส่วนบุคคลของประชาชนได้อย่างมีประสิทธิภาพ และยังมีประเด็นที่ไม่ชัดเจนทาให้ผู้ประกอบการยากที่จะปฏิบัติให้สอดคล้อง ดังนั้นผู้เขียนจึงได้ศึกษามาตรการทางกฎหมายของสหรัฐอเมริกาและสหภาพยุโรป เพื่อนามาวิเคราะห์เปรียบเทียบตามข้อพิจารณาต่างๆ อันสามารถสรุปโดยแบ่งเป็นข้อพิจารณาเกี่ยวกับการกาหนดฐานความผิดและข้อพิจารณาเกี่ยวกับการเพิ่มเติมหลักเกณฑ์เพื่อให้ผู้ประกอบการหรือผู้ให้บริการอินเทอร์เน็ตมีมาตรฐานร่วมกัน และส่งผลให้เกิดความมีประสิทธิภาพในการท าการตลาดผ่านอีเมล ดังต่อไปนี้

ข้อพิจารณาเกี่ยวกับการกาหนดฐานความผิด การใช้อีเมลเชิงพาณิชย์เพื่อโฆษณาประชาสัมพันธ์เป็นสิ่งที่สะดวกและประหยัดต้นทุนให้แก่ผู้ประกอบการ แต่การโฆษณาที่ก่อให้เกิดความราคาญหรือกระทบต่อสิทธิของผู้รับมากไป ย่อมก่อให้เกิดผลเสียทั้งต่อตัวผู้ส่งและผู้รับ ซึ่งการกระทาความผิดฐานส่งข้อความโฆษณาที่เข้าข่ายเป็นการรบกวนผู้รับ (spam) โดยปกปิดแหล่งที่มาและไม่เปิดโอกาสให้ผู้รับบอกเลิกได้โดยง่าย ปัจจุบันมีความผิดตามมาตรา 11 ของพระราชบัญญัติว่าด้วยการกระทาความผิดทางคอมพิวเตอร์ มีโทษปรับไม่เกิน 200,000 บาท เพียงเท่านั้น ทั้งที่เดิมทีคณะกรรมาธิการยกร่างพิจารณาโทษของการกระทาผิดรูปแบบนี้โดยเทียบเคียงคาว่า “การรบกวน

[1] สุพิศ ปราณีตพลกรัง. กฎหมายว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์. สานักพิมพ์นิติธรรม, กันยายน 2560. หน้า 1-9.

การครอบครองทรัพย์ของผู้อื่นโดยปกติสุข ”กับองค์ประกอบทางความผิดฐานบุกรุกตามประมวลกฎหมายอาญา มาตรา 362[2] ที่มีทั้งโทษปรับและโทษจ าคุก[3] เนื่องจากการส่งอีเมลที่ไม่ได้ถูกร้องขอเป็นจานวนมากย่อมส่งผลกระทบต่อประสิทธิภาพการประมวลผลของคอมพิวเตอร์ และยังสิ้นเปลืองพื้นที่ในกล่องข้อความของผู้รับโดยที่ผู้รับไม่อนุญาต จึงเปรียบเสมือนเป็นการขัดขวางไม่ให้ผู้รับสามารถใช้ประโยชน์จากคอมพิวเตอร์หรือกล่องข้อความอีเมลของตนได้อย่างปกติตามที่ควรจะเป็น อีกทั้งการกระทาความผิดในรูปแบบสแปมยังก่อให้เกิดผลเสียหายหรือเกิดความเดือดร้อนกับบุคคลในวงกว้าง ซึ่งไม่ได้กระทบต่อผู้ใดผู้หนึ่งเพียงคนเดียว การพิสูจน์ถึงระดับความเดือดร้อนเสียหายที่มีมากพอสมควรแก่โทษเมื่อเทียบจากมาตรฐานของวิญญูชน (objective) ยังคงเป็นเรื่องที่ยากสาหรับคนทั่วไป เนื่องจากการกระทารูปแบบนี้เรื่องทางเทคนิคเฉพาะและยากที่จะจากัดขอบเขตพื้นที่ที่เกิดความเสียหาย ทาให้ยากที่ผู้เสียหายจะสามารถรวมตัวกันเพื่อพิสูจน์ความเสียหายให้ชัดเจน และค่าใช้จ่ายหรือเวลาที่ต้องเสียไปเพื่อการพิสูจน์หาหลักฐานอาจไม่คุ้มค่าส าหรับผู้เสียหาย

จากการศึกษากฎหมายต่างประเทศเกี่ยวกับประเด็นนี้ พบว่าบทบัญญัติของ CAN-SPAM ของสหรัฐอเมริกามีการระบุจาแนกโทษและอัตราโทษตามระดับความผิดที่กาหนดไว้อย่างชัดเจน จึงทาให้ภาระในการพิสูจน์ของผู้เสียหายลดลงได้ในระดับหนึ่ง และทาให้ศาลสามารถพิจารณาโทษปรับตามผลกระทบที่เกิดขึ้นจริงเพื่อลงโทษผู้กระท าความผิดได้อย่างเหมาะสมมากกว่า

สาหรับประเทศไทยความผิดฐานนี้ถูกกาหนดเพดานโทษปรับไว้ที่ 200,000 บาท อาจไม่สามารถป้องปรามไม่ให้เกิดการกระทาผิดได้มากนัก เพราะธุรกิจรายใหญ่ย่อมกาลังมากพอที่จะจ่ายค่าปรับ อีกทั้งค่าใช้จ่ายในการผลิตสื่อโฆษณารูปแบบอื่นๆไม่ว่าจะเป็นป้ายโฆษณา หรือการสร้างวีดีโอโฆษณาก็มีต้นทุนสูง และค่าใช้จ่ายในการลงสื่อโฆษณาเหล่านั้นตามช่องทางอื่นๆก็มีราคาแพง เช่น การลงโฆษณาในยูทูปมีราคาไม่ต่ ากว่า 20,000 บาทต่อเดือน การซื้อพื้นที่ลงป้ายโฆษณาตามท้องถนนมีราคาเฉลี่ยไม่ต่ากว่า 40,000 บาทต่อเดือน (ราคาเฉลี่ยจากบริษัท คิว แอดเวอร์ไทซิ่ง จากัด ณ เดือนมีนาคม 2561) ดังนั้น การสร้างและการส่งอีเมลโฆษณาจึงเป็นช่องทางโฆษณาที่ใช้ต้นทุนต่าและสามารถเข้าถึงลูกค้าจานวนมากได้ ซึ่งแม้จะนาต้นทุนที่ใช้ในการสร้างอีเมลนั้นมารวมกับค่าปรับ ก็ยังเป็นรายจ่ายที่น้อยกว่าการโฆษณาด้วยช่องทางอื่นอยู่ดี ดังนั้น หากรัฐต้องการปรามปรามการกระทารูปแบบนี้ และลดภาระการพิสูจน์ของผู้เสียหาย รัฐควรที่จะบัญญัติโทษทางอาญาแยกตามระดับความเสียหายที่เกิดจากการกระท าความผิดฐานสแปมเมลให้ชัดเจน

ข้อพิจารณาเกี่ยวกับการเพิ่มเติมหลักเกณฑ์ เพื่อให้ผู้ประกอบการหรือผู้ให้บริการอินเทอร์เน็ตมีมาตรฐานร่วมกัน และส่งผลให้เกิดความมีประสิทธิภาพในการทาการตลาดผ่านอีเมล เนื่องจากปัจจุบันการทาการตลาดออนไลน์เป็นเรื่องจาเป็นสาหรับสาหรับผู้ประกอบการ เนื่องจาก

---

[2] ประมวลกฎหมายอาญา มาตรา 362 ผู้ใดเข้าไปในอสังหาริมทรัพย์ของผู้อื่น เพื่อถือการครอบครองอสังหาริมทรัพย์นั้นทั้งหมดหรือแต่บางส่วน หรือเข้าไปกระทาการใด ๆ อันเป็นการรบกวนการครอบครองอสังหาริมทรัพย์ของเขาโดยปกติสุข ต้องระวางโทษจ าคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจ าทั้งปรับ

[3] มานิตย์ จุมปา. ค าอธิบายกฎหมายว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์. พิมพ์ครั้งที่ 2. ศูนย์หนังสือกฎหมายวิญญูชน. 2554. หน้า 83-85

ผู้บริโภคหันมาใช้สื่อออนไลน์กันมากขึ้น การทาการตลาดที่ดีย่อมต้องคานึงถึงทุกปัจจัยไม่ว่าจะเป็นด้านเนื้อหาที่ใช้ ช่องทางโฆษณาที่เป็นมิตรกับผู้รับ และกฎหมายที่เกี่ยวข้อง เพื่อสร้างภาพลักษณ์ที่ดีและก่อให้เกิดประสิทธิภาพสูงสุดจากการโฆษณานั้น

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ออกประกาศเรื่องลักษณะ และวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนร าคาญแก่ผู้รับ เมื่อเดือนกรกฎาคม ปี 2560 ที่ผ่านมา โดยใจความหลักของประกาศคือการเพิ่มนิยามของ “ผู้ส่ง” ให้ครอบคลุมถึงผู้ให้บริการประเภทสื่อสังคมออนไลน์ (Social Media) หรือผู้ให้บริการแอปพลิเคชัน (Application) และเพิ่มเติมข้อกาหนดให้การส่งข้อมูลคอมพิวเตอร์หรืออีเมลเชิงพาณิชย์ต้องมีการขอความยินยอมจากผู้รับก่อน (Opt-in) ซึ่งประเด็นดังกล่าวมีส่วนช่วยปกป้องไม่ให้มีการส่งโฆษณาที่เป็นการรบกวนสิทธิความเป็นอยู่ส่วนบุคคลของผู้รับได้ครอบคลุมมากขึ้น แต่ยังไม่ได้ช่วยสนับสนุนให้ผู้ประกอบการสามารถทาการตลาดได้อย่างมีประสิทธิภาพ เพราะถึงแม้ผู้ประกอบการจะได้รับความยินยอมจากผู้รับแล้ว โอกาสที่อีเมลโฆษณาเชิงพาณิชย์นั้นจะถูกโอนไปยังกล่องข้อความขยะ (spam box) หรือโดนดักโดยผู้ให้บริการระบบก็ยังคงอยู่ เพราะผู้ให้บริการอีเมล หรือผู้ให้บริการเครือข่ายแต่ละเจ้า มีนโยบายความปลอดภัยของระบบที่แตกต่างกัน ผู้ประกอบการที่ส่งอีเมลผ่านทางที่อยู่ไอพี (IP address) เดียวเป็นจ านวนมาก อาจไปติดเงื่อนไขของระบบใดระบบหนึ่งได้

หากพิจารณาเทียบกับ CAN-SPAM ของสหรัฐอเมริกาที่มีการกาหนดจานวนการส่งเชิงทวีคูณ (Multiple) และกาหนดจานวนที่อยู่ไอพี (IP address) และที่อยู่โดเมน (Domain Name) ที่สามารถใช้ส่งได้โดยไม่ผิดกฎหมายไว้ชัดเจน ทาให้ไม่ว่าจะเป็นผู้ให้บริการหรือผู้ประกอบการก็สามารถกาหนดนโยบายความปลอดภัย หรือวิธีการทาการตลาดของตนได้โดยใช้มาตรฐานเดียวกัน ผู้ประกอบการจึงมั่นใจได้ว่าถ้าตนปฏิบัติตามหลักเกณฑ์ดังกล่าว ข้อความที่ตนสร้างสรรค์มานั้นจะสื่อสารไปถึงผู้บริโภคอย่างแน่นอน

อย่างไรก็ตาม ยังคงมีประเด็นเรื่องการใช้สิทธิจนเกินส่วนของผู้ประกอบการ เนื่องจากกฎหมายในประเทศไทยยังไม่ได้ก าหนดปริมาณและความถี่ที่เหมาะสมในการส่งอีเมลโฆษณาที่เหมาะกับอัตราการส่งถ่ายข้อมูลระบบเครือข่ายอินเทอร์เน็ตในปัจจุบันเอาไว้ ท าให้ผู้ประกอบการสามารถส่งอีเมลโฆษณาได้อย่างไม่จากัด ซึ่งอาจก่อให้เกิดปัญหาต่อการใช้งานตามปกติของผู้ใช้งานคนอื่นๆ เนื่องจากการที่มีอีเมลจานวนมากวิ่งอยู่บนระบบ จะทาให้เกิดความล่าช้าในการประมวลผล จนอาจส่งผลให้ระบบหยุดชะงักได้ อีกทั้งยังก่อให้เกิดภาระค่าใช้จ่ายต่อผู้ให้บริการอินเทอร์เน็ต (ISPs) หรือผู้ดูแลระบบที่ต้องขยายแบนด์วิดท์ (Bandwidth) หรือเซิร์ฟเวอร์ (server) เพื่อรองรับกับอีเมลจ านวนมากนั้น และยังต้องคอยพัฒนา จัดหามาตรการในการป้องกันสแปมเมลที่ทันสมัยอยู่เสมอ

อีกประเด็นที่ต้องคานึงถึงคือ การให้และยืนยันความยินยอม (affirmative consent) เนื่องจากประกาศฉบับนี้ก าหนดให้ต้องมีการขอความยินยอมจากผู้รับก่อนจึงจะท าการส่งข้อมูลโดยไม่ถือเป็นการก่อให้เกิดความเดือดร้อนราคาญ ซึ่งอาจเป็นการจากัดสิทธิในการโฆษณาของผู้ประกอบการมากเกินไป หากเปรียบเทียบกับสหภาพยุโรปที่แม้จะให้ความสาคัญด้านสิทธิความ

เป็นอยู่ส่วนบุคคลอย่างเคร่งครัด แต่ก็ยังไม่ลืมที่จะส่งเสริมการดาเนินกิจกรรมทางการตลาดของผู้ประกอบการ โดยยินยอมให้ใช้ inferred consent ได้ในกรณีที่ทาการโฆษณาสินค้าอื่นที่มีลักษณะใกล้เคียงกับสินค้าเดิมที่ผู้รับให้คายินยอมไว้[4] หากเปิดช่องทางให้ผู้รับนั้นสามารถบอกปฏิเสธรับได้โดยง่าย ดังนั้นประเทศไทยก็ควรพิจารณาถึงบริบทข้อนี้เพื่อเพิ่มอิสระให้แก่ผู้ประกอบการ

ข้อพิจารณาเกี่ยวกับการคุ้มครองสิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภค โดยการส่งข้อมูลโฆษณาโดยบิดเบือนหัวเรื่องหรือทาให้ไม่ทราบถึงสาระส าคัญที่แท้จริงของเนื้อความในนั้น เป็นการขัดต่อสิทธิของผู้บริโภคในการรับรู้คาพรรณนาที่ถูกต้องและเพียงพอตามพระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2522 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2541 ซึ่งในปัจจุบันยังไม่มีบทบัญญัติเกี่ยวกับเรื่องนี้ในกฎหมายเกี่ยวกับการกระทาความผิดทางคอมพิวเตอร์ ทาให้ผู้บริโภคมีความเสี่ยงที่จะติดไวรัส หรือการโดนขโมยข้อมูลจากมัลแวร์ที่แฝงเข้ามาหลังจากที่เปิดรับอีเมล เนื่องจากหัวเรื่องที่ถูกบิดเบือนทาให้วิจารณญานของผู้รับบกพร่องจนไม่สามารถพิจารณาว่าควรเปิดอีเมลนั้นหรือไม่ เมื่อเทียบกับ CAN-SPAM ของสหรัฐอเมริกาที่มีบทบัญญัติเรื่องการแสดงชื่อหัวเรื่อง (Subject Heading) ให้กับอีเมลเชิงพาณิชย์อย่างชัดเจน ว่าต้องเป็นชื่อที่ผู้รับสามารถตีความถึงสาระสาคัญ (Materially)[5] ของอีเมลได้ และกาหนดให้อีเมลเชิงพาณิชย์ที่มีเนื้อหาเกี่ยวกับเรื่องเพศหรือสื่อลามกอนาจารต้องแสดงฉลาก (Label) ตามมาตรฐานที่กาหนด จึงมีส่วนช่วยให้ผู้บริโภคสามารถตัดสินใจรับข้อมูลเหล่านั้นได้อย่างเป็นธรรมมากกว่า

การถูกรบกวนด้วยอีเมลโฆษณาหรือข้อความโฆษณาเป็นจานวนมาก ย่อมกระทบต่อสิทธิความเป็นอยู่ส่วนบุคคล (Rights of Privacy) ของผู้บริโภค ยิ่งถ้าข้อมูลนั้นมีขนาดใหญ่มากๆ เช่น ไฟล์วีดีโอ หรือภาพถ่ายที่มีความละเอียดสูง พื้นที่ในการรับของผู้บริโภคยิ่งถูกใช้ไปโดยสิ้นเปลือง อีกทั้งยังส่งผลให้การจราจรบนระบบอินเทอร์เน็ต (internet traffic) เกิดการติดขัด จนเกิดปัญหากับการส่งข้อมูลอื่นๆตามปกติไปด้วย

แม้ว่าประเทศไทยจะพยายามจ ากัดการกระท าผิดกล่าวด้วยการนาหลัก Opt-in เข้ามาใช้แล้วก็ตาม แต่ในประกาศของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ออกประกาศเรื่องลักษณะ และวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนราคาญแก่ผู้รับ พ.ศ. 2560 ยังไม่ได้มีการระบุถึงขนาด หรือความถี่ที่เหมาะสมในการส่งข้อมูลเอาไว้ ดังนั้น เพื่อให้เกิดความเป็นธรรมทั้งฝ่ายผู้ส่งและผู้รับ จึงควรมีหลักเกณฑ์ที่เป็นบรรทัดฐานให้ผู้ส่งสามารถอ้างอิงขนาดและจ านวนในการส่งที่ท าไม่ก่อให้เกิดผลกระทบต่อตัวผู้รับ

---

[4] E-Privacy Directive 2002/58/EC Article 13 (2) Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

[5] CAN-SPAM,section 5 (a)(6)

การใช้งานอินเทอร์เน็ตมีส่วนทาให้ข้อมูลส่วนบุคคลรั่วไหลไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ การโพสต์ความคิดเห็น หรือสมัครรับข่าวสารจากที่ใดที่หนึ่งย่อมหลงเหลือ “ข้อมูลจราจรคอมพิวเตอร์” (Log file) หรือคุกกี้ (Cookies) ทิ้งไว้บนเซิร์ฟเวอร์หรือเว็บโฮสติ้ง (Web Hosting) และบางครั้งเวลาพิมพ์ที่อยู่อีเมลลงไปในหน้าเว็บต่างๆ ระบบของเว็บไซต์นั้นๆจะทาไฮเปอร์ลิงก์ (hyperlink) ให้แก่ที่อยู่อีเมลนั้นโดยอัตโนมัติ จึงทาให้มิจฉาชีพสามารถเข้ามาขโมยข้อมูลได้อย่างง่ายดาย หากเจ้าของระบบหรือเจ้าของเว็บไซต์ไม่มีมาตรการป้องกันที่ดีเพียงพอ

ปัจจุบันพระราชบัญญัติว่าด้วยการกระทาความผิดทางคอมพิวเตอร์ยังคงก หนดหน้าที่ของผู้ให้บริการไว้เพียงแค่การเก็บรักษาข้อมูลการจราจร (Log file) ไว้เพื่อให้สามารถสืบถึงตัวผู้ใช้บริการได้ ซึ่งเป็นประโยชน์ในการสืบหาตัวผู้กระทาความผิด แต่ไม่ได้ช่วยคุ้มครองด้านการโจรกรรมข้อมูล เนื่องจากไม่ได้ระบุให้ผู้ให้บริการมีหน้าที่จัดหามาตรการป้องกันการรวบรวมที่อยู่อีเมลด้วยวิธีอัตโนมัติ (address harvesting) จากบุคคลภายนอก จึงเป็นช่องว่างให้เกิดการรวมรวมรายชื่อที่อยู่อีเมลหรือการรวบรวมประวัติการใช้งาน (Cookies History) เพื่อนาไปขาย ซึ่งในสหรัฐอเมริกากาหนดให้การกระทาแบบนี้เป็นความผิดร้ายแรงที่ต้องรับโทษสูงกว่าความผิดฐานสแปมโดยทั่วไป[6]ดังนั้น เมื่อพิจารณาจากสภาพตลาดออนไลน์ในประเทศไทยและผลกระทบจากการที่ข้อมูลส่วนตัวอาจถูกขโมยเพื่อนาไปใช้ในทางมิชอบ ประเทศไทยจึงควรมีบทบัญญัติเรื่องหน้าที่ในการป้องกันการเข้าถึงข้อมูลของผู้ใช้งานเพิ่มเติมเช่นกัน

จากการศึกษา วิเคราะห์ในประเด็นต่างๆข้างต้น พบว่ากฎหมายและมาตรการที่มีอยู่ในปัจจุบันของประเทศไทยไม่อาจปกป้องสิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภค และไม่สามารถส่งเสริมให้ภาคธุรกิจสามารถดาเนินกิจกรรมทางการตลาดอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพ ดังนั้นเพื่อเป็นการแก้ไขปัญหาดังกล่าว จึงจ าเป็นต้องมีบทบัญญัติเพิ่มเติมเกี่ยวกับ ลักษณะ วิธีการ ความถี่ ปริมาณ และการแสดงชื่อหัวเรื่องในการส่งข้อมูลเหล่านั้น รวมทั้งพิจารณาเพื่อปรับใช้หลัก inferred consent เพื่อช่วยอานวยความสะดวกและส่งเสริมการทากิจกรรมทางการตลาดของภาคธุรกิจ โดยผู้เขียนจะนาเสนอแนวทางในการกาหนดมาตรการทางกฎหมายและแนวทางการทาการตลาดออนไลน์ที่สอดคล้องกับกฎหมายและก่อให้เกิดประสิทธิภาพสูงสุดในหัวข้อถัดไป

6.2 ข้อเสนอแนะ

การศึกษาถึงกฎหมายของประเทศไทยในปัจจุบันและการศึกษาวิเคราะห์เปรียบเทียบกับกฎหมายต่างประเทศที่เกี่ยวข้องกับการกระทาความผิดฐานสแปม ผู้เขียนพบแนวทางที่เหมาะสมกับประเทศไทย เพื่อส่งเสริมการทาการตลาดด้วยอีเมลเชิงพาณิชย์ให้เกิดประสิทธิภาพ ในขณะที่ยังคงคุ้มครองสิทธิในความเป็นอยู่ส่วนบุคคลของผู้รับได้อย่างเหมาะสม ผู้เขียนจึงจะขอนาเสนอแนวทางสาหรับการเพิ่มเติมบทบัญญัติทางกฎหมายและแนวทางที่เหมาะสมสาหรับการทาการตลาดโดยใช้อีเมลเชิงพาณิชย์ ดังต่อไปนี้

[6] CAN-SPAM Act, section 5 (b)

แนวทางสาหรับการเพิ่มเติมบทบัญญัติทางกฎหมาย โดยบทบัญญัติเกี่ยวกับการให้ข้อมูลผู้บริโภคที่เพียงพอ การปกป้องคุ้มครองข้อมูลส่วนบุคคล และหลักเกณฑ์ที่ชัดเจนในการกาหนดมาตรฐานการส่งข้อความโฆษณาเชิงพาณิชย์ ควรพิจารณาเพิ่มเติมบทบัญญัติดังต่อไปนี้

1) ควรพิจารณาแยกโทษและอัตราโทษตามระดับความรุนแรงของความเสียหายที่เกิดขึ้นให้ชัดเจน เพื่อให้ผู้เสียหายได้รับการเยียวยาที่เหมาะสมและเป็นธรรม

2) ควรออกประกาศเกี่ยวกับลักษณะการกาหนดชื่อหัวเรื่อง (Subject) แถบผู้ส่ง (from line) และฉลากค าเตือน (label) ให้ชัดเจน เพื่อให้ผู้รับสามารถใช้วิจารณญาณในการพิจารณาก่อนเปิดอ่านได้อย่างถูกต้อง

3) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมควรพิจารณากาหนดความถี่และขนาดของข้อมูลโฆษณาที่เป็นการก่อให้เกิดความเดือดร้อนแก่ผู้รับ และออกเป็นประกาศให้ชัดเจน เพื่อให้ทั้งผู้ประกอบการและผู้บริการเครือข่ายสามารถนาไปอ้างอิงในการกาหนดนโยบายของตนได้เป็นมาตรฐานเดียวกัน

4) พิจารณาเพิ่มเติมบทบัญญัติเรื่อง inferred consent มาปรับใช้กับการส่งข้อความโฆษณาเชิงพาณิชย์ที่ไม่ขัดต่อกฎหมาย เพื่อส่งเสริมเสรีภาพในการทาโฆษณาของผู้ประกอบการ

5) เพิ่มเติมหน้าที่ให้เจ้าของเว็บโฮสติ้ง (Web Hosting) ให้ต้องจัดหามาตรการป้องกันการรวบรวมข้อมูลผู้ใช้งานโดยโปรแกรมอัตโนมัติ (Harvesting) หรือการเก็บรวบรวมประวัติการใช้งานของผู้รับ (Cookies) เพื่อป้องกันไม่ให้มิจฉาชีพเข้ามาขโมยข้อมูลของผู้ใช้งานได้โดยง่าย

6) ผลักดันให้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้ในเร็ววัน เพื่อคุ้มครองไม่ให้ข้อมูลส่วนบุคคล เช่น ที่อยู่อีเมล หรือประวัติการใช้งาน ที่อยู่ ชื่อ ฯลฯ ถูกเปิดเผยหรือนาไปใช้วัตถุประสงค์อื่นนอกจากวัตถุประสงค์ที่ได้แจ้งไว้แต่แรก[7] และเพื่อให้ผู้ที่มีหน้าที่ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอานาจ หรือโดยมิชอบ[8] เพื่อป้องกันไม่ให้เกิดการซื้อขายข้อมูลส่วนบุคคล และเพื่อกาหนดโทษให้การได้มาซึ่งข้อมูลส่วนบุคคลโดยมิชอบ[9]

แนวทางที่เหมาะสมส หรับผู้ประกอบการในการท าการตลาดด้วยอีเมลเชิงพาณิชย์

เทคโนโลยีมีส่วนช่วยทาให้การติดต่อสื่อสารกับผู้บริโภค การโฆษณาสินค้าหรือบริการ การสร้างการรับรู้และจดจ ในตัวตราสินค้า (Brand) การวิเคราะห์พฤติกรรมของผู้บริโภคทาได้สะดวกรวดเร็วมากขึ้น แต่การทาการตลาดผ่านอีเมลหรือระบบออนไลน์ให้ได้ผลดี ไม่ควรใช้วิธีหว่านแหส่งโฆษณาอะไรที่เราอยากจะส่งไปหาใครก็ได้ เพราะนอกจากจะสร้างความราคาญให้แก่ผู้รับจนเกิดความรู้สึกไม่ดีต่อ

---

[7] ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... ฉบับที่สคก. ตรวจพิจารณาแล้ว เรื่องเสร็จที่ 1135/2559 มาตรา 24

[8] ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... ฉบับที่สคก. ตรวจพิจารณาแล้ว เรื่องเสร็จที่ 1135/2559 มาตรา 29

[9] ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... ฉบับที่สคก. ตรวจพิจารณาแล้ว เรื่องเสร็จที่ 1135/2559 มาตรา 42

ตราสินค้า (Brand) และถ้าข้อความโฆษณานั้นก่อให้เกิดความเดือดร้อนร าคาญแก่ผู้รับ ยังเข้าข่ายเป็นการกระทาที่ขัดต่อกฎหมายด้วย ดังนั้น การส่งข้อมูลโดยได้รับความสมัครใจจากผู้รับ จึงก่อให้เกิดผลดีแก่ผู้ประกอบการมากกว่า เพราะนอกจากจะสามารถสร้างฐานข้อมูลลูกค้าที่แท้จริง (customer database) ได้แล้ว ยังทาให้สามารถสื่อสารกับลูกค้าเป้าหมายได้ตรงกลุ่ม และสามารถบริหารความสัมพันธ์อันดีระหว่างธุรกิจและลูกค้า (Customer Relationship Management: CRM)[10] ได้อย่างยั่งยืน

ภาพที่ 18 ข้อดีของการท าตลาดออนไลน์[11]

การทาการตลาดด้วยอีเมลในยุคปัจจุบันมีการพัฒนารูปแบบไปมาก ไม่ว่าจะเป็นด้านเนื้อหาการนาเสนอ การประยุกต์ใช้อินโฟกราฟิก (infographic) การแบ่งกลุ่ม (segment) ลูกค้าเพื่อสร้างเนื้อหาที่เหมาะสมกับแต่ละกลุ่มเป็นอีกหนึ่งแนวทางสาคัญเพื่อเชิญชวนให้กลุ่มเป้าหมายแสดงพฤติกรรมตอบสนองบางอย่าง (Call to Action) เช่น การมอบคูปองส่วนลดในการลงทะเบียนเพื่อรับข่าวสาร การเล่นเกมส์หรือร่วมกิจกรรมบนโลกออนไลน์ สามารถกระตุ้นให้ผู้บริโภคเกิดความจดจาในตราสินค้า (Brand Awareness) จูงใจให้เกิดการซื้อต่อเนื่อง (Cross Selling) และก่อให้เกิดความรู้สึกจงรักภักดีต่อสินค้า (Royalty) กล่าวได้ว่า การตลาดเป็นฟันเฟืองสาคัญตัวหนึ่งที่ช่วยขับเคลื่อนธุรกิจไปสู่ผลก าไรสูงสุด

อย่างไรก็ตาม ทุกประเทศย่อมมีกฎหมายเข้ามาควบคุมการดาเนินกิจกรรมทางการตลาดเพื่อจุดประสงค์ในการคุ้มครองผู้บริโภค ยิ่งกับสื่อการตลาดออนไลน์ที่กาหนดขอบเขตการแพร่กระจายได้ยาก ผู้ประกอบการยิ่งต้องศึกษาบทบัญญัติที่แตกต่างกันของกฎหมายที่เกี่ยวข้องในแต่ละประเทศให้ดี และปฏิบัติตามอย่างเคร่งครัด

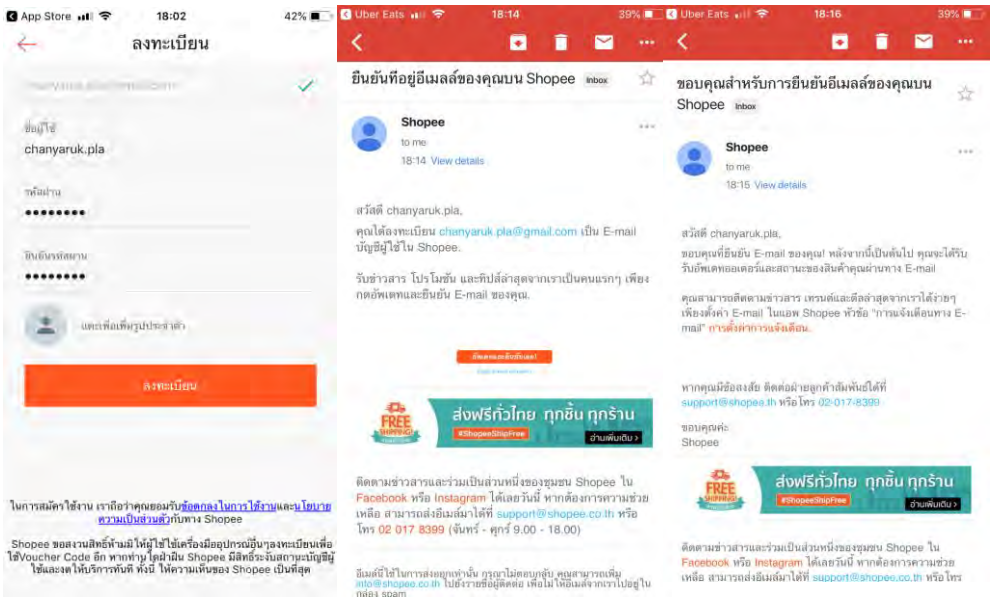
---

[10] ณัฐพล ใยไพโรจน์. Digital Marketing Concept&Case Study 3rd Edition. นนทบุรี: ไอดีซี, 2559. หน้า 159

[11] เรื่องเดียวกัน. หน้า 158

บริบทในประเทศไทยปัจจุบัน มีการกำหนดให้ต้องได้รับความยินยอมจากผู้รับก่อนส่งข้อความโฆษณาไปหาเจ้าตัวโดยตรงแล้ว มิเช่นนั้นจะถือว่าเป็นสิ่งที่ก่อให้เกิดความเดือดร้อนร าคญ ต้องระวางโทษปรับไม่เกิน 200,000 บาทตามมาตรา 11 ของพระราชบัญญัติว่าด้วยความรับผิดเกี่ยวกับคอมพิวเตอร์ ดังนั้นการทาการตลาดรูปแบบนี้จะต้องมีขั้นตอนการขอรับความยินยอมเพิ่มขึ้นมาจากเมื่อก่อนด้วย จากการศึกษาวิเคราะห์กฎหมายตามที่น าเสนอไปในเอกัตศึกษาฉบับนี้ ผู้เขียนจึงสามารถสรุปแนวทางข้อเสนอแนะสาหรับการทาการตลาดด้วยอีเมลเชิงพาณิชย์ เพื่อให้ผู้ประกอบการสามารถด าเนินกิจกรรมได้ถูกต้องตามกฎหมายและเกิดประสิทธิภาพสูงสุด ดังต่อไปนี้

1) จัดให้มีช่องทาง Opt-in ก่อนเสมอเพื่อให้สอดคล้องกับบทบัญญัติทางกฎหมายและเพื่อเพิ่มประสิทธิภาพในการสื่อสารข้อมูลโฆษณาประชาสัมพันธ์ หรือเพื่อกลั่นกรองกลุ่มลูกค้าเป้าหมายที่แท้จริง ควรใช้การบอกรับรูปแบบ Double Opt-in โดยสร้างคอลัมน์ที่มีข้อความยินยอมรับข่าวสาร เช่น "หากต้องการเรียนรู้เพิ่มเติม" หรือ "ลงทะเบียนเพื่อรับข่าวสารและโปรโมชั่นเด็ดจากเราก่อนใคร" ไว้ที่ด้านล่างของหน้าต่างป๊อปอัพ (Pop-up windows) ที่จะปรากฏขึ้นมาเวลาที่ลูกค้าเปิดเข้าเว็บไซต์หรือสมัครสมาชิกเพื่อซื้อสินค้า แล้วหลังจากที่ลูกค้ากรอกข้อมูลเสร็จ จะมีอีเมลส่งไปยืนยันตัวตนของลูกค้าอีกครั้งก่อน เมื่อลูกค้าคลิกยินยอมจึงจะสามารถเริ่มการส่งอีเมลโฆษณาเชิงพาณิชย์จริง (อ้างอิงภาพที่ 27) ซึ่งรูปแบบนี้จะช่วยกรองลูกค้าที่เป็นลูกค้าคุณภาพจริงๆได้ และเมื่อเกิดความสัมพันธ์ในระบบอีเมลแล้ว อีเมลที่เราส่งไปหลังจากนั้นจะไม่มีทางถูกระบบอีเมลหรือระบบอินเทอร์เน็ตดักจับว่าเป็นสแปมเมลแน่นอน



ภาพที่ 19 ตัวอย่างจากแอปพลิเคชัน Shopee ที่ใช้รูปแบบ Double Opt-in ในการลงทะเบียนและ Subscribe

การยินยอมแบบ Single Opt-in หรือการขอความยินยอมทางเดียว อาจช่วยให้ยอดติดตาม (Subscribe) หรือรายชื่อผู้ที่ยินยอมเติบโตอย่างรวดเร็ว แต่อัตราการเปิดอ่านจริงกลับมีจานวนน้อย จากผลการสารวจในปี 2011 ของ Mailchimp ที่เป็นแพลตฟอร์มที่ได้รับความนิยมมากที่สุดในแวดวงการทาการตลาดผ่านอีเมล พบว่าการใช้รูปแบบ Double Opt-in ทาให้อัตราการเปิด

อ่านอีเมลโฆษณาสูงกว่ารูปแบบ Single Opt-in ถึง 144% และยอดการขอปฏิเสธรับข่าวสาร (Unsubscribe) ยังต่ำกว่าการใช้รูปแบบ Single Opt-in ถึง 7%[12] อีกทั้งการใช้รูปแบบ Single Opt-in ยังมีโอกาสเสี่ยงที่ระบบอีเมลจะดักจับว่าเป็นสแปม เพราะบัญชีอีเมล (e-mail account) ของผู้ประกอบการที่ใช้ในการส่งไม่เคยมีความสัมพันธ์กับผู้รับมาก่อนเลย

นอกจากนี้ รูปแบบ Double Opt-in ยังแสดงให้เห็นถึงการเคารพสิทธิความเป็นอยู่ส่วนบุคคลของผู้รับ ซึ่งส่งผลดีต่อภาพลักษณ์ที่ดีของธุรกิจ และสอดคล้องกับบทบัญญัติทางกฎหมายในปัจจุบันด้วย

2) จัดทำบัญชีรายชื่อผู้ที่แจ้งปฏิเสธรับข้อมูลข่าวสาร (Opt-out List) เพื่อป้องกันไม่ให้มีการส่งข้อมูลไปหากลุ่มลูกค้าที่ไม่ต้องการอีก และเพื่อเก็บรายชื่อเหล่านั้นไว้เป็นฐานข้อมูลในการวิเคราะห์พฤติกรรมของลูกค้า

3) สร้างเทมเพลตที่ส่งเสริมการใช้งานบนโทรศัพท์มือถือและแท็บเล็ต เพื่อให้ผู้รับสามารถอ่านข้อความได้อย่างชัดเจนโดยไม่ต้องเลื่อนหน้าจอมากนัก โดยใช้ชื่อหัวข้อ (Subject) ที่กระชับได้ใจความ ออกแบบเนื้อหาด้านในให้เรียบง่าย สะอาดตา ตรงประเด็น ดึงดูดใจผู้อ่าน และติดตั้งปุ่ม Call to Action ให้โดดเด่น สังเกตเห็นได้ง่ายตั้งแต่เปิดอีเมล ที่สำคัญที่สุดคือ ขนาดของไฟล์รูปภาพหรือข้อมูลต้องไม่ใหญ่จนเกินไปจนทำให้เกิดความล่าช้าในการดาวน์โหลด

4) จัดให้มีมาตรการในการเก็บรักษาข้อมูลของลูกค้าให้ปลอดภัย เพื่อหลีกเลี่ยงการถูกนำไปใช้ผิดวัตถุประสงค์

ผู้เขียนเห็นว่าปัญหาในการทำการตลาดด้วยอีเมลเชิงพาณิชย์ และปัญหาเรื่องสิทธิความเป็นอยู่ส่วนบุคคล (Privacy of life) ในประเทศไทยยังคงมีอยู่ จากการศึกษาถึงสาเหตุของปัญหาดังกล่าว แนวความคิดทางทฤษฎีและกฎหมายที่เกี่ยวข้อง พร้อมทั้งศึกษาเปรียบเทียบและวิเคราะห์จากกฎหมายของต่างประเทศ ทั้งสหรัฐอเมริกาและสหภาพยุโรป พบว่าแนวทางของต่างประเทศบางประการสามารถนำมาปรับใช้ให้เหมาะสมกับบริบทของประเทศไทยได้

แม้ว่าบริบททางสังคมในประเทศไทยกับต่างประเทศจะมีความแตกต่างกัน แต่การทำธุรกิจในปัจจุบันนั้นไร้ขอบเขต ตลาดการค้าอิเล็กทรอนิกส์ (e-Marketplace) ทำให้กำแพงที่กั้นระหว่างประเทศหลายลง ทั้งภาครัฐและภาคธุรกิจจึงจำเป็นอย่างยิ่งที่จะต้องศึกษาสถานการณ์ในตลาดและกฎหมายที่เกี่ยวข้องของทุกประเทศ เพื่อกำหนดนโยบายให้สอดคล้อง พร้อมทั้งนำมาตรการบางประการมาปรับใช้เพื่อช่วยอำนวยความสะดวกและส่งเสริมการทำกิจกรรมทางการตลาดของภาคธุรกิจ และเพื่อปกป้องสิทธิความเป็นอยู่ส่วนบุคคลของผู้บริโภคได้อย่างเป็นธรรม ตามสมมติฐานของการศึกษาที่ได้กำหนดไว้แล้วตอนต้น

---

[12] Ariel in Resources. The Importance and Benefit of Double Opt-in Email Marketing [Online]. 2015. Available from: https://www.elegantthemes.com/blog/resources/the-importance-and-benefit-of-double-opt-in-email-marketing [5 June 2018.]

บรรณานุกรม

Law

Article R645-1 of the French Criminal Code

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

Data Protection Directive 95/46/EC

E-Privacy Directive 2002/58/EC

The European Convention on Human Rights. Article 8

Universal Declaration of Human Right 1984. Article 12

Judgment

UJEF et LICRA v. Yahoo! Inc. et Yahoo France, Tribunal de Grande Instance de Paris, No RG:00/0538, May 22, 2000 and November 22, 2000

Article

Eleni Kosta; Peggy Valcke; David Stevens. Spam, Spam, Spam, Spam Lovely Spam: Whyis Bluespam Different. 23 Int'l Rev. L. Computers&Tech. 89 (2009).

Hedley, S. A Brief History of Spam. Information & Communication Technology Law 15, 3 (2006): 223.

Mostafa Raad, N. M. Y., Gazi Mahabubul Alam, B. B. Zaidan, A. A. Zaidan. Impact of Spam Advertisement through E-Mail: A Study to Assess the Influence of the Anti-Spam on the E-Mail Marketing. African Journal of Business Management Vol. 4(11) (4 September 2010): 2362-2367.

Press Release

Rikke ULDALL. "Q&A: New Eu Rules on Data Protection Put the Citizen Back in the Driving Seat." edited by GUILLOT, J. D.: The European Parliament, June 1, 2016.

Website

Ariel in Resources. The Importance and Benefit of Double Opt-in Email Marketing [Online]. 2015. Available from: https://www.elegantthemes.com/blog/resources/the-importance-and-benefit-of-double-opt-in-email-marketing [5 June 2018.]

Canada's Anti-Spam Legislation. Canada's Law on Spam and Other Electronic Threats. [Online]. 2017. Available from: http://fightspam.gc.ca/eic/site/030.nsf/eng/home[13 June 2017.]

Darya Gudkova, M. V., Tatyana Shcherbakova, Nadezhda Demidova [Online]. 2017. Available from: https://securelist.com/spam-and-phishing-in-q1-2017/78221/ [10 April 2018.]

Darya Gudkova, M. V., Tatyana Shcherbakova, Nadezhda Demidova [Online]. 2017. Available from: https://securelist.com/spam-and-phishing-in-q2-2017/81537/ [14 March 2018.]

Darya Gudkova, M. V., Tatyana Shcherbakova, Nadezhda Demidova. Spam and Phishing in 2017 [Online]. 2018. Available from: https://securelist.com/spam-and-phishing-in-2017/83833/ [20 April 2018]

Jarrod Morris. Why Do People Open Emails? [Online]. 2016. Available from: https://graphly.io/why-do-people-open-emails/ [24 April 2018]

Martin Samson. Yahoo, Inc. V. La Ligue Contre Le Racisme Et L'antisemitisme, Et Al, 145 F. Supp. 2d 1168, Case No. C-00-21275jf (N.D. Ca., September 24, 2001) [Online]. Available from: http://www.internetlibrary.com/cases/lib_case17.cfm [8 April 2018.]

MCKERNAN. K. Anti-SPAM Laws Around the World [Online]. 2016. Available from: https://pierryinc.com/2016/07/18/anti-spam-laws-around-world/ [8 April 2018]

Niall Merrigan. Another Telco Is Failing at Security [Online]. 2018. Available from: https://www.certsandprogs.com/2018/04/another-telco-is-failing-at-security.html#axzz5CXkf6GxS [13 April 2018.]

Paul wood, “MessageLabs white paper, A spammer in the works: Everything you need to know,” [Online]. 2006. Available from: http://www.messagelabs.com/Threat_Watch/white_Papers [18 March 2018.]

SANDBERG, J. Phoenix Lawyers Irk Internet Users Again by Broadcasting Ad [Online]. 1994. Available from: https://web.archive.org/web/20081204122549/http://www.l-ware.com/wall_stree_journal__june_22_1994.htm [13 February 2018.]

Templeton Brad. Reflections on the 25th Anniversary of Spam [Online]. 2008. Available from: http://www.templetons.com/brad/spamreact.html [7 Febuary 2018.]

The Department of Internal Affairs of Te Tari Taiwhenua. Three Steps to Ensure You Are Not Spamming [Online]. . Available from: https://www.dia.govt.nz/Spam-Three-Steps#in [2 June 2018.]

กฎหมาย

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนร าคญแก่ผู้รับ พ.ศ. 2560

ประมวลกฎหมายแพ่งและพาณิชย์

ประมวลกฎหมายอาญา

พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2522 (ฉบับที่ 2) พ.ศ. 2541

พระราชบัญญัติว่าด้วยการกระท าความผิดทางคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560

รัฐธรรมนูญแห่งราชอาณาจักรไทย ฉบับปี 2560 หมวด 3

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

หนังสือ

เกียรติขจร วัจนะสวัสดิ์. ค าอธิบายกฎหมายอาญา ภาค1 (หจก. จิรรัชการพิมพ์, 2549).

ชวลิต อัตถศาสตร์, ไพบูลย์ อมรภิญโญเกียรติ, พัชรินทร์ ฉัตรวชิระกุล, อิทธินันท์ สุวรรณจูฑะ. กฎหมายไซเบอร์. บริษัท เนชั่น มัลติมีเดีย กรุ๊ป จ ากัด (มหาชน): บริษัท ซีเอ็ดยูเคชั่น จากัด (มหาชน), 2545.

ณัฐพล ใยไพโรจน์. Digital Marketing Concept & Case Study 3rd Edition. นนทบุรี: ไอดีซีฯ, 2559.

ธานินทร์ กรัยวิเชียร. ความสาคัญของการตีความในวิชาชีพกฎหมาย. ใน 100ปี ชาตกาล ศาสตราจารย์จิตติ ติงศภัทิย์. มหาวิทยาลัยธรรมศาสตร์: 2551.

พรเพชร วิชิตชลชัย. คาอธิบายพระราชบัญญัติว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. ส านักงานศาลยุติธรรม, 2550.

มานิตย์ จุมปา. ความรู้พื้นฐานเกี่ยวกับกฎหมาย. พิมพ์ครั้งที่ 14. สานักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2559.

มานิตย์ จุมปา. คาอธิบายกฎหมายว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์. พิมพ์ครั้งที่ 2. ศูนย์หนังสือกฎหมายวิญญูชน. 2554.

สราวุธ ปิติยาศักดิ์. กฎหมายเทคโนโลยีสารสนเทศ. พิมพ์ครั้งที่ 1. ส านักพิมพ์นิติธรรม, 2555.

สุพิศ ปราณีตพลกรัง. กฎหมายว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์. สานักพิมพ์นิติธรรม. 2560.

รายงานสถิติ

ส านักงานสถิติแห่งชาติ, การส ารวจสถานภาพการพาณิชย์อิเล็กทรอนิกส์ของประเทศไทย พ.ศ. 2557

ส านักยุทธศาสตร์. รายงานผลการสารวจมูลค่าพาณิชย์อิเล็กทรอนิกส์ในประเทศไทยปี 2560. พิมพ์ครั้งที่ 1. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2560.

วิทยานิพนธ์

นางสาวศศิมา ศรีพจน์ธรรม. มาตรการทางกฎหมายเพื่อการจัดการจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงประสงค์ (Spam Mail). ปริญญาตรี, คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2548.

เว็บไซต์

Admin ITGenius. เทรนด์แอปพลิเคชันโลก [ออนไลน์]. 2016. แหล่งที่มา: https://www.itgenius.co.th/article/เทรนด์แอปพลิเคชันโลก [13 เมษยน 2561]

blogone. sunnywalker. รู้จัก GDPR กฎใหม่คุ้มครองข้อมูลยุโรป ข้อมูลเก็บที่ไหน กฎหมายตามไปคุ้มครองที่นั่น [ออนไลน์]. 2018. แหล่งที่มา: https://www.blognone.com/node/100324 [13 เมษยน 2561]

Brand Buffet. PP. [ออนไลน์]. 2017. แหล่งที่มา: https://www.brandbuffet.in.th/2017/06/mba-chula-digital-marketing-tool/ [10 มีนาคม 2561]

Brand Buffet. Zn-UP. 10 รูปแบบโฆษณาที่ผู้บริโภคเชื่อถือมากที่สุด 2015 [ออนไลน์]. 2015. แหล่งที่มา: https://www.brandbuffet.in.th/2015/10/nielsen-consumer-trust-in-ad-type/ [10 เมษายน 2561]

Colorpack Creations Co., L. Admin, H. สแปม (Spam) คืออะไร มารู้จักกับ Spam และวิธีป้องกัน [ออนไลน์]. แหล่งที่มา: https://colorpack.net/host-articles/904-cms-web-tip/33-what-is-apam.html [1 มีนาคม 2561]

EGAT Mail Admin. รู้จักกับ SPAM [ออนไลน์]. แหล่งที่มา: https://mail.egat.co.th/owapage/km/spam.html [เข้าถึงเมื่อ 27 กุมภาพันธ์ 2561]

Google. นโยบายโปรแกรม [ออนไลน์]. 2018. แหล่งที่มา: https://support.google.com/mail/answer/7015314?hl=th&co=GENIE.Platform=iOS [เข้าถึงเมื่อ 17 พฤษภาคม 2561]

Information Technology Center : Maejo University. บทที่ 10 ความปลอดภัยในการท ขานบนระบบเครือข่าย, 10.6 สรุปรายละเอียด พรบ. ที่เกี่ยวข้องกับผู้ให้บริการ [ออนไลน์]. แหล่งที่มา: http://csmju.jowave.com/cs100_v2/lesson10-5.html [12 มีนาคม 2561]

Magazine, S. ชัยวัฒน์ คุประตกุล. คลื่นวิทย์-เทคโนฯ : ทฤษฎีวิวัฒนาการกับการฆ่าล้างเผ่าพันธุ์ [ออนไลน์]. 2012. แหล่งที่มา: https://www.sarakadee.com/2012/07/04/social-darwinism/ [1 มีนาคม 2561]

MGR Online. อย่าแตกตื่น! อาคารเอียงแค่ดีไซน์ โรงแรมของ "เอม-พินทองทา" ลูกสาวทักษิณ, [ออนไลน์]. 2560. แหล่งที่มา: https://mgronline.com/onlinesection/detail/9600000083254 [1 มีนาคม 2561]

Microsoft. อีเมลจ านนมากและขีดจ ากัดอัตราผู้รับรายวัน. [ออนไลน์]. 2012. แหล่งที่มา: https://msdn.microsoft.com/th-th/library/ff381292(v=exchsrvcs.149).aspx [14 เมษายน 2561]

WorkpointNews. เตือนภัยกลโกง ! แก๊งคอลเซ็นเตอร์ระบาดหนัก แฉฐานปฏิบัติการตั้งอยู่นอกประเทศ [ออนไลน์]. 2017. แหล่งที่มา: https://workpointnews.com/2017/12/06/เตือนภัยกลโกง-แก๊งคอล/ [14 เมษายน 2561]

Sunny Smile. โพสต์ฝากร้านค้าออนไลน์ กับเรื่องเข้าใจผิดในการโปรโมท Fanpage [ออนไลน์]. 2556. แหล่งที่มา: https://blog.lnw.co.th/2013/07/25/โพสฝากร้านค้าออนไลน์/ [20 มิถุนายน 2561]

ชินณปพัชร เอกวิพัทธ์พล. Bandwidth (แบนด์วิดท์) คืออะไร [ออนไลน์]. 28 กรกฎาคม 2560. แหล่งที่มา: http://www.8webz.com/bandwidth-แบนด์วิดท์-คืออะไร/ [เข้าถึงเมื่อ 17 พฤษภาคม 2561]

นาวิก น าเสนอ. การตลาดแบบ Opt-in หรือ Opt-out ดี? [ออนไลน์]. 2558. แหล่งที่มา: https://www.ecampaign101.com/email/การตลาดแบบ-opt-in-หรือ-opt-out-ดี/ [20 มิถุนายน 2561]

ศูนย์วิจัยกสิกรไทย. ปรับธุรกิจให้ทัน รับกระแส E-Commerce โต [ออนไลน์]. 2560. แหล่งที่มา: https://www.kasikornbank.com/th/business/sme/KSMEKnowledge/article/KSMEAnalysis/Pages/E-Commerce_E-MarketPlace.aspx [14 เมษายน 2561]

สถาบันนวัตกรรมและพัฒนากระบวนการเรียนรู้มหาวิทยาลัยมหิดล. ยุคของคอมพิวเตอร์ [ออนไลน์]. 2017. แหล่งที่มา: http://www.il.mahidol.ac.th/e-media/computer/evolution/6thGeneration.html [6 กุมภาพันธ์ 2018]

สมาคมโฆษณาดิจิทัล (ประเทศไทย). DAAT เผยข้อมูลผู้ใช้อินเทอร์เน็ตของไทย ไตรมาส 1 ประจ าปี 2559 [ออนไลน์]. 2559. แหล่งที่มา http://www.daat.in.th/index.php/daat-internet/ [27 กุมภาพันธ์ 2561]

สายสืบภาคประชาชน. ป่วน ! เว็บไอซีที “แฮ็กเกอร์” ลุ้นคุก 15 ปี - ปรับ 3 แสน !? [ออนไลน์]. แหล่งที่มา: http://oknation.nationtv.tv/blog/Anti-Corruption/2007/07/20/entry-1 [1 มีนาคม, 2018]

[ออนไลน์]. แหล่งที่มา: http://www.central.co.th/ [2 มิถุนายน 2561]

[ออนไลน์]. แหล่งที่มา: https://www.nike.com/th/ [2 มิถุนายน 2561]