ปกิณกะกฎหมาย

ข้อสังเกตบางประการต่อประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเกี่ยวกับสแปมประกอบพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

*ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล**

ภูมิหลังของการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือที่มักถูกเรียกติดปากว่า พ.ร.บ. คอมพิวเตอร์ฯ ฉบับแรก นั้นผ่านมรสุมคำวิพากษ์วิจารณ์มาตลอดระยะเวลาสิบปีของการบังคับใช้ ทั้งในแง่ของถ้อยคำในข้อบทที่ไม่ชัดเจนหรือไม่ครอบคลุมประเด็นปัญหาจริงในโลกยุคดิจิทัล เช่น มาตรา 11 ที่มุ่งควบคุมเรื่องสแปมแต่กลับไม่สามารถบังคับใช้ได้ตามวัตถุประสงค์เนื่องจากกำหนดลักษณะของสแปมไว้แคบเกินไป[1] ไปจนถึงการตีความให้ทับซ้อนกับความผิดในกฎหมายอาญาเดิมแต่มีบทลงโทษรุนแรงกว่าและไม่สามารถยอมความได้ จนทำให้การฟ้องร้องตาม

---

* LLB (Kyoto University), LLM in Law, Development and Governance (SOAS, University of London), LLM International Law Program (GSICS, Kobe University), อาจารย์ประจำคณะนิติศาสตร์ ธรรมศาสตร์

[1]คณาธิป ทองวีรวงศ์, “มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว : ศึกษากรณีการรบกวนสิทธิในความเป็นอยู่ส่วนตัวโดยธุรกิจขายตรง”, 2553, http://www.stjohn.ac.th/sju/research/pdf/re11-5-54_3.pdf (เข้าถึงล่าสุด 1 กันยายน 2560).

พ.ร.บ. คอมพิวเตอร์ฯ ถูกใช้เสมือนเป็นเป็นเครื่องมือในการกลั่นแกล้ง ดังเช่นที่พบเห็นในสถิติของการฟ้องร้องตามมาตรา 14 และมาตรา 15[2] ประกอบกับกิจกรรมในโลกยุคดิจิทัลมีความซับซ้อนมากขึ้นเรื่อย ๆ จึงมีความพยายามแก้ไขเนื้อหาของ พ.ร.บ. คอมพิวเตอร์ฯ ตลอดหลายปีที่ผ่านมา โดยเฉพาะในประเด็นการนำมาตรา 14 ไปใช้กับการฟ้องความผิดฐานหมิ่นประมาทตามกฎหมายอาญา[3] จนกระทั่งความพยายามนี้เกิดเป็นรูปธรรมขึ้นในช่วงต้นปี พ.ศ. 2558 ในสมัยของรัฐบาลทหาร โดยร่างแก้ไข พ.ร.บ. คอมพิวเตอร์ฯ เป็นส่วนหนึ่งของชุดกฎหมายเศรษฐกิจดิจิทัลอันมีวัตถุประสงค์เพื่อสร้างสภาวะแวดล้อมที่เหมาะสมต่อการพัฒนาเศรษฐกิจดิจิทัล[4]

ร่างแก้ไขนี้เผชิญกับคำวิพากษ์วิจารณ์จากสังคมอีกระลอก เนื่องจากเมื่ออ่านร่วมกับร่างพระราชบัญญัติอื่น ๆ เช่น ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงไซเบอร์ แล้วสามารถเข้าใจได้ว่ากฎหมายชุดนี้อาจเปิดช่องให้อำนาจเจ้าหน้าที่รัฐเข้าสอดส่องข้อมูลของประชาชนได้มากขึ้น หลังจากนั้นร่างแก้ไข พ.ร.บ. คอมพิวเตอร์ฯ ก็ได้รับการแก้ไขและนำเข้าสู่การรับฟังความคิดเห็นจากผู้มีส่วนได้เสียแบบวงปิดหลายครั้ง จนกระทั่งมีการเปิดเผยร่างและเปิดรับฟังความคิดเห็นอย่างเป็นการทั่วไปก่อนจะนำเข้าสู่สภานิติบัญญัติประมาณสามสัปดาห์ ซึ่งในช่วงครึ่งปีหลังของปี พ.ศ. 2559 นั้นเกิดความตื่นตัวเกี่ยวกับเนื้อหาของร่างแก้ไข พ.ร.บ. คอมพิวเตอร์ฯ โดยเริ่มจากสื่อใหม่บนอินเทอร์เน็ตและสื่อสังคมรายงานข่าว จนขยายวงกว้างไปสู่การอภิปรายถกเถียงในสื่อกระแสหลักเช่นรายการโทรทัศน์ ทั้งยังมีองค์กรเอกชนระหว่างประเทศที่ทำงานเกี่ยวกับสิทธิมนุษยชนร่วมแสดงความเห็น[5] นำไปสู่การลงชื่อทางอินเทอร์เน็ตเพื่อคัดค้านร่างแก้ไข พ.ร.บ. คอมพิวเตอร์ฯ นี้อย่างกว้างขวาง[6]

---

[2]ดูเพิ่มเติม สาวตรี สุขศรีและคณะ, “อาชญากรรมคอมพิวเตอร์? : งานวิจัยหัวข้อ “ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น” (โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw) ในมูลนิธิอาสาสมัครเพื่อสังคม, 2555), https://ilaw.or.th/sites/default/files/ComputerCrimeResearch.pdf (เข้าถึงล่าสุด 1 กันยายน 2560); ilaw, “ตารางคดี “ปิดปาก” นักเคลื่อนไหวด้วย พ.ร.บ. คอมพิวเตอร์ฯ มาตรา 14(1)”, 31 ธันวาคม 2559, https://freedom.ilaw.or.th/blog/ตารางคดี-ปิดปาก-นักเคลื่อนไหว-ด้วย พ.ร.บ. คอมพิวเตอร์ฯ-มาตรา-141 (เข้าถึงล่าสุด 1 กันยายน 2560).

[3]ilaw, “รวมความเห็นคนร่าง #พรบคอม ย้ำ ไม่ให้ใช้ฟ้องหมิ่นประมาทแล้ว”, 29 พ.ค. 2560, https://ilaw.or.th/node/4513 (เข้าถึงล่าสุด 1 กันยายน 2560).

[4]ดูเพิ่มเติม ETDA, “ร่างกฎหมายเศรษฐกิจดิจิทัล”, https://ictlawcenter.etda.or.th/de_laws (เข้าถึงล่าสุด 1 กันยายน 2560)

[5]ilaw, “เนื้อหาเดิม พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14(1) กลับมาแล้ว ซ้ำซ้อนกฎหมายหมิ่นประมาทแต่โทษหนักกว่า”, https://ilaw.or.th/node/4319 (เข้าถึงล่าสุด 1 กันยายน 2560); ดูเพิ่มเติม Amnesty International, “URGENT ACTION GRAVE CONCERN OVER THAI COMPUTER CRIMES ACT” (UA: 225/16 Index: ASA 39/4944/2016 Thailand), 7 October 2016, https://www.amnesty.org/download/Documents/ASA3949442016ENGLISH.pdf (เข้าถึงล่าสุด 1 กันยายน 2560).

[6]Change.org, “แคมเปญรณรงค์เข้าชื่อหยุด #พรบคอม หยุดกฎหมายล้วงข้อมูลส่วนบุคคล”, https://www.change.org/p/หยุด-พรบคอม-หยุดกฎหมายล้วงข้อมูลส่วนบุคคล (เข้าถึงล่าสุด 1 กันยายน 2560)

หลังจากที่สภานิติบัญญัติแห่งชาติมีมติให้ผ่านร่างแก้ไข พ.ร.บ. คอมพิวเตอร์ฯ อย่างล้นหลาม โดยแทบไม่มีการแก้ไขเปลี่ยนแปลง[7] กลายเป็น พ.ร.บ. คอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ในภาคประชาสังคมและสื่อก็ยังมีอภิปรายถกเถียงอย่างต่อเนื่องถึงผลกระทบของ พ.ร.บ.คอมพิวเตอร์ฯ ฉบับใหม่ และจับตาดูประกาศกระทรวงฯ ที่จะต้องออกประกอบมาตราต่าง ๆ โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้จัดรับฟังความเห็นของประชาชนทั้งหมด 5 ครั้งในแต่ละภูมิภาค ซึ่งนับว่าเป็นการจัดรับฟังความคิดเห็นอย่างกว้างขวางกว่าตอนจัดทำกฎหมายหลัก จนออกมาเป็นประกาศกระทรวงฯ 5 ฉบับ[8]

ในบทความนี้ ผู้เขียนขอตั้งประเด็นข้อสังเกตเกี่ยวกับปัญหาสำคัญในการใช้และการตีความประกาศที่ออกตามอำนาจในมาตรา 11 วรรคสาม เรื่อง ลักษณะวิธีการส่ง ลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ (ต่อไปนี้เรียกว่า “ประกาศกระทรวงฯ เรื่องสแปม”) ซึ่งประเด็นของสแปมนี้สะท้อนปัญหาใหญ่เกี่ยวกับการร่างกฎหมายที่เกี่ยวข้องเศรษฐกิจดิจิทัล กล่าวคือ การสร้างสมดุลระหว่างภาคส่วนต่าง ๆ ที่มีส่วนเกี่ยวข้องกับธุรกรรมบนโลกดิจิทัล เพื่อไม่ให้การกำกับดูแลในประเด็นที่จำเป็นโดยกฎหมายสร้างภาระให้แก่ผู้ประกอบการหรือผู้บริโภคมากจนเกินไป[9]

เนื้อหาของประกาศกระทรวงฯ เรื่องสแปม

มาตรา 11 ใน พ.ร.บ.คอมพิวเตอร์ฯ ฉบับที่ 1 มีปัญหาว่าการตีความถ้อยคำที่เขียนไว้ในกฎหมายไม่สามารถนำไปสู่การบรรลุเจตนารมณ์ของกฎหมายที่ต้องการลดปริมาณข้อความที่สร้างความเดือดร้อนรำคาญได้ (สแปม) เนื่องจากกำหนดให้หมายรวมถึงเฉพาะการส่งข้อความแบบที่ปกปิดตัวตนของผู้ส่ง แต่ลักษณะการส่งสแปมในประเทศไทยนั้นมักเป็นการส่งโดยไม่ปกปิดตัวตนของผู้ส่ง จึงทำให้ไม่สามารถบังคับใช้มาตรา 11 กับกรณีของสแปมส่วนใหญ่ได้ ใน พ.ร.บ. คอมพิวเตอร์ฯ ฉบับที่ 2 จึงพยายามแก้ไขปัญหานี้โดยเพิ่มขอบเขตการบังคับใช้ในวรรคสองให้ครอบคลุมไปถึงการส่งข้อความในลักษณะสแปม “โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย” นอกจากนี้ในวรรคสาม ยังกำหนดให้ต้องออกประกาศกระทรวงเกี่ยวกับสองประเด็น

---

[7]สำนักข่าวอิศรา, “สนช.ผ่านฉลุย พ.ร.บ.คอมพ์ฯ เพิ่ม กก. กลั่นกรอง 9 คน-กมธ.ยันไม่ละเมิดสิทธิชัวร์”, 16 ธันวาคม 2559, https://www.isranews.org/isranews-news/52601-snch-52147.html (เข้าถึงล่าสุด 1 กันยายน 2560).

[8]1) ประกาศออกตามอำนาจในมาตรา 11 วรรคสาม เรื่อง ลักษณะวิธีการส่ง ลักษณะและปริมาณของข้อมูล ความที่และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ

2) ประกาศออกตามอำนาจในมาตรา 15 วรรคสอง เรื่อง ขั้นตอนการแจ้งเตือน การระงับทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์

3) ประกาศออกตามอำนาจในมาตรา 17/1 เรื่อง แต่งตั้งคณะกรรมการเปรียบเทียบ

4) ประกาศออกตามอำนาจในมาตรา 20 วรรคสาม เรื่อง แต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์

5) ประกาศออกตามอำนาจในมาตรา 20 วรรคสี่ เรื่อง หลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือผู้ให้บริการ

[9]ในเสวนาเกี่ยวกับการรับฟังความเห็นและในการให้สัมภาษณ์กับสื่อหลายครั้ง ตัวแทนจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้เน้นย้ำหลายครั้งเรื่องการสร้างสมดุล ไม่ใช่เป็นการออกกฎหมายเพื่อควบคุมหรือเพิ่มอำนาจรัฐ

ใหญ่คือ หนึ่ง ลักษณะและวิธีการส่งที่ไม่ถือเป็นสแปม และ สอง ลักษณะ “การบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย” หรืออาจเรียกได้ว่า “easy opt-out”

ข้อ 4 ของประกาศนี้กำหนดข้อยกเว้นไว้เป็นรายการของลักษณะการส่งข้อมูลแบบที่จะไม่เข้าข่ายสแปมเอาไว้ค่อนข้างละเอียด คือ เพื่อติดต่อเป็นหลักฐานในการทำนิติกรรมสัญญา (transactional) หรือแสดงนิติสัมพันธ์ระหว่างกัน (relationship) เพื่อการแจ้งข้อมูลโดยหน่วยงานรัฐ เป็นการส่งโดยสถาบันการศึกษา หรือหน่วยงานองค์กรการกุศล หรือการส่งอื่น ๆ ที่ไม่มีวัตถุประสงค์เชิงพาณิชย์ แต่ในเนื้อหาประกาศไม่มีการนิยามคำว่า “วัตถุประสงค์เชิงพาณิชย์” จึงอาจเกิดปัญหาการตีความในอนาคตได้[10] รวมถึงเปิดช่องให้ผู้ส่งข้อมูลอาศัยความคลุมเครือนี้แอบซ่อนลักษณะทางพาณิชย์ของข้อมูล เช่นที่เรามักพบเห็นในบทความเชิงโฆษณา (advertorial) ซึ่งหากข้อมูลที่ส่งไม่เข้าตามลักษณะข้อยกเว้นตามข้อ 4 ก็จะต้องได้รับ “ความยินยอมจากผู้รับข้อมูล” ก่อนส่ง ดังที่ข้อ 5 ของประกาศกระทรวงฯ กำหนดไว้ ซึ่งสอดคล้องกับกฎหมายหลาย ๆ ประเทศเช่น แคนาดา ออสเตรเลีย และประเทศในสหภาพยุโรป[11] แม้ข้อ 5 มิได้กำหนดว่าความยินยอมนั้นต้องให้ในลักษณะใด จึงอาจตีความรวมถึงความยินยอมโดยปริยายได้[12] โดยในทางปฏิบัติภาคธุรกิจต่าง ๆ ก็ควรเก็บบันทึกการได้รับความยินยอมจากผู้รับข้อมูลไว้เป็นหลักฐานด้วย

นอกจากนี้ข้อ 5 ยังกำหนดต่อไปอีกว่า แม้ในกรณีที่ผู้รับข้อมูลให้ความยินยอมในการรับข้อมูลไว้แล้ว ผู้ส่งข้อมูลก็ยังมีหน้าที่ต้องเปิดโอกาสให้ผู้รับยกเลิกการรับข้อมูลได้โดยง่ายด้วย ทว่า ปัญหาใหญ่ของประกาศกระทรวงฯ ฉบับนี้คือวิธีการยกเลิกการรับข้อมูล “ในกรณีที่ผู้รับข้อมูลคำสั่งบอกเลิกยกเลิกหรือปฏิเสธการรับข้อมูลไปยังผู้ส่งข้อมูลแล้วปรากฏว่าผู้ส่งข้อมูลยังฝ่าฝืนและส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์เพิ่มเติมอีก” ที่ระบุไว้ในข้อ 5(4) นั้นในชั้นการรับฟังความเห็นกระทรวงผู้ร่างได้สอบถามผู้มีส่วนได้เสียว่า ควรจะกำหนดให้ผู้ส่งข้อมูลมีความผิดทันที หรือต้องให้ผู้รับข้อมูลที่ต้องการยกเลิกแจ้งซ้ำ หลังจากรับฟังความเห็นแล้ว ผู้ร่างตัดสินใจใช้ทางเลือกที่สองคือกำหนดให้ผู้รับข้อมูลแจ้งคำสั่งยกเลิกซ้ำอีกครั้งโดยส่งที่อีเมล์และไปรษณีย์ลงทะเบียนตอบรับ หรือ

---

[10]ตัวอย่างนิยามของประเทศสหรัฐอเมริกา CAN-SPAM Act 2003, Section 3 (2) (A) “(2) COMNfERCIAL ELECTRONIC MAIL MESSAGE.— (A) IN GENERAL.--The term **"commercial electronic mail message"** means **any electronic mail message the primary propose of which is the commercial advertisement or promotion of a commercial product or service** (including content on an Internet website operated for a commercial purpose)”; สำหรับนิยามที่มีความละเอียดมากกว่านี้ ดูเพิ่มเติมกฎหมายของประเทศออสเตรเลีย Spam Act 2003, Part 1, Section 6.

[11]ประเทศที่มิได้กำหนดให้ต้องมีความยินยอมในการส่งข้อมูลคือสหรัฐอเมริกา ดูเพิ่มเติม litmus, “The Guide to International Email Spam Laws”, https://litmus.com/blog/the-ultimate-guide-to-international-email-law-infographic (เข้าถึงล่าสุด 1 กันยายน 2560).

[12]ตัวอย่างประเทศออสเตรเลีย ตีความว่าความยินยอมโดยปริยาย (inferred consent) สามารถเกิดขึ้นได้ในกรณีที่มีความสัมพันธ์กันในแบบที่คาดหมายได้ว่าจะได้รับข้อความเชิงพาณิชย์จากอีกฝ่าย หรือการเปิดเผยอีเมล์ธุรกิจต่อสาธารณะในลักษณะที่ไม่ได้มีประสงค์ห้ามการส่งข้อความเชิงพาณิชย์และเนื้อหาของข้อความนั้นมีความเชื่อมโยงกับตำแหน่งหน้าที่การงานของบุคคลนั้น ๆ ดู ACMA, “Spam consent”, https://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/spam-consent-ensuring-you-dont-spam-i-acma (เข้าถึงล่าสุด 1 กันยายน 2560).

วิธีการอื่นที่ยืนยันได้ว่าผู้ส่งข้อมูลได้รับคำสั่งดังกล่าวแล้ว หากผ่านขั้นตอนนี้ไปแล้วผู้ส่งข้อมูลยังฝ่าฝืนและส่งข้อมูลอีกจึงจะมีความผิดและต้องระวางโทษปรับ

ประเด็นปัญหาของประกาศกระทรวงฯ เรื่องสแปม

ในสภาพความเป็นจริง ขั้นตอนดังกล่าวข้างต้นนั้นจะทำให้เกิดความยุ่งยากต่อผู้รับข้อมูลที่ไม่ต้องการได้รับข้อมูลนั้นอีก ทั้งยังทำให้เป็นภาระของผู้รับข้อมูลที่จะต้องหาทางยืนยันให้ผู้ส่งข้อมูลได้รับคำสั่งยกเลิกการรับข้อมูลด้วยตนเอง จึงไม่สอดคล้องกับหลักการ “easy opt-out” ดังที่เขียนไว้ในกฎหมายหลัก อีกทั้งหากพิจารณากฎหมายของประเทศอื่น ๆ ที่มีมักกำหนดให้วิธีการยกเลิกรับนั้นกระทำได้โดยง่าย ซึ่งผู้รับข้อมูลไม่จำเป็นต้องให้ข้อมูลอื่นเพิ่มเติม หรือไม่จำเป็นต้องดำเนินการใด ๆ ที่ซับซ้อนยุ่งยากมากไปกว่าการเข้าไปหน้าลิงก์เว็บเพจที่จะกดยกเลิกการรับข้อมูลและไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม[13] เช่น กฎหมายของสหรัฐอเมริกากำหนดให้การยกเลิกต้องเป็นการสื่อสารผ่านอินเทอร์เน็ต (internet-based communication) เท่านั้น[14] ส่วนกฎหมายออสเตรเลียก็กำหนดให้เป็นข้อความอิเล็กทรอนิกส์ (electronic message)[15] รวมถึงในทางปฏิบัติผู้ให้บริการที่ส่งข้อมูลประเภทนี้หลายรายก็ทำให้สามารถคลิกที่ลิงก์ท้ายอีเมล์ (เช่น ลิงก์ที่เขียนว่า “unsubscribe”) เพียงครั้งเดียว[16] ก็สามารถยกเลิกรับข้อความดังกล่าวได้แล้วโดยไม่ต้องมีการล็อกอินเข้าไปยืนยันตัวตน หรือเขียนอีเมล์ไปอธิบายเหตุผลของการไม่ต้องการรับข้อความดังกล่าวแต่อย่างใด โดยประเทศญี่ปุ่นกรมคุ้มครองผู้บริโภค (Consumer Affairs Agency) ได้ออกไกด์ไลน์แนะนำว่าหากในบริษัทเดียวมีการส่งข้อความหลายประเภทก็อาจให้ผู้รับข้อมูลเลือกได้ในหน้าเว็บเพจที่ดำเนินการ unsubscribe ว่าจะเลือกเลิกรับข้อความลักษณะใดบ้าง[17]

วิธีการ easy opt-out ดังกล่าวสามารถกระทำได้โดยง่าย มิได้เพิ่มภาระให้กับภาคธุรกิจมากจนเกินไปดังจะได้ว่าภาคธุรกิจในหลายประเทศก็ใช้วิธีการเพิ่มลิงก์ unsubscribe ไว้ท้ายข้อความเช่นนี้มาเป็นเวลานานกว่าสิบปีแล้วนอกจากนี้เมื่อพิจารณาว่าในปัจจุบันมีวิธีการทางเทคนิคอื่น ๆ ที่ผู้รับ

---

[13]Derek Bambauer et al., “A Comparative Analysis of Spam Laws: The Quest for a Model Law”, presented at ITU WSIS THEMATIC MEETING ON CYBERSECURITY (2005), p. 34.

[14]CAN-SPAM Act 2003, Section 5 (a) (3) and (5), https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf (เข้าถึงล่าสุด 1 กันยายน 2560).

[15]Spam Act 2003, Part 2, Section 18 (8), https://www.legislation.gov.au/Details/C2005C00382 (เข้าถึงล่าสุด 1 กันยายน 2560).

[16]เมื่อศึกษาเอกสารแนะนำการปฏิบัติตามกฎหมาย (compliance quideline) ที่จัดทำโดยหน่วยงานทั้งภาครัฐและเอกชนจะพบว่าส่วนใหญ่แนะนำให้บริษัทต่าง ๆ โดยเฉพาะบริษัทที่ส่งอีเมล์ข้ามประเทศหรือส่งหาลูกค้าที่เป็นชาวต่างชาตินั้นปฏิบัติตามหลักการ easy-opt out คือ ไม่คิดค่าใช้จ่ายเพิ่ม ไม่ต้องมีกระบวนการล็อกอิน ไม่ขอข้อมูลอื่นนอกจากที่อยู่อีเมล์และไม่ต้องให้ผู้รับข้อมูลต้องเข้าสู่เว็บไซต์มากกว่าหนึ่งหน้า

[17]Consumer Affairs Agency, “特定電子メールの送信等に関するガイドライン (ไกด์ไลน์เกี่ยวกับการส่งอีเมล์ทางพาณิชย์)”, สิงหาคม 2011, หน้า 22, http://www.caa.go.jp/trade/pdf/110831kouhyou_2.pdf (เข้าถึงล่าสุด 1 กันยายน 2560).

ข้อมูลจะสามารถปฏิเสธการรับข้อมูลได้ เช่น การบล็อกข้อความอัตโนมัติ หรือแจ้งไปยังเซิร์ฟเวอร์ของอีเมล์ว่าข้อความนั้น ๆ เป็นอีเมล์ขยะ การที่ภาคธุรกิจจะปฏิบัติตามคำสั่งยกเลิกของผู้รับข้อมูลโดยตรงย่อมเป็นประโยชน์กับภาคธุรกิจเองมากกว่า กล่าวคือ ยังสามารถรักษาความสัมพันธ์ที่ดีกับลูกค้า (หรือว่าที่ลูกค้าในอนาคต) และทำให้อีเมล์ของบริษัทไม่ถูกจัดอยู่ในรายชื่ออีเมล์ขยะ นอกจากนี้แล้วการปฏิเสธข้อความด้วยวิธีการทางเทคนิคนั้นยังเป็นภาระแก่ผู้ให้บริการอินเทอร์เน็ตและเครือข่ายโดยรวมอีกด้วย[18]

ดังอภิปรายข้างต้น แนวโน้มของกฎหมายทั่วโลกจึงมุ่งสร้างแรงจูงใจให้ภาคธุรกิจปรับปรุงการส่งข้อความหาลูกค้าหรือผู้บริโภคในรูปแบบที่ไม่สร้างความเดือดร้อนรำคาญ คือเป็นการสื่อสารเชิงพาณิชย์อย่างตรงไปตรงมา ชัดเจนว่าใครเป็นผู้ส่ง เคารพความยินยอมของผู้รับข้อมูล โดยเฉพาะเปิดโอกาสให้สามารถยกเลิกการรับข้อความได้โดยไม่สร้างภาระให้กับผู้รับ ในภาพกว้าง แนวโน้มเช่นนี้สะท้อนกระแสการคุ้มครองความเป็นส่วนตัวบนโลกออนไลน์ด้วยเช่นกัน ทำให้ในทางปฏิบัติทั่วโลกนั้นภาคธุรกิจจะต้องปรับตัวปฏิบัติตามกฎหมายเกี่ยวกับสแปมใหม่ ๆ โดยเริ่มจากการจัดการฐานข้อมูลลูกค้า โดยเฉพาะบันทึกเกี่ยวกับความยินยอมของลูกค้าให้ชัดเจนมากขึ้น ซึ่งจะนำไปสู่การแบ่งประเภทข้อมูลตามลักษณะความเป็นส่วนตัวด้วย

การที่กฎหมายไทยสวนกระแสโลกโดยไม่ยึดหลักการของ easy opt-out และผลักภาระไปให้ผู้รับข้อมูลเช่นนี้ อาจทำให้กฎหมายมาตรานี้ไม่สามารถบังคับใช้ได้ตามวัตถุประสงค์ ส่งผลให้ภาคธุรกิจไทยไม่ยอมปรับตัว ยังคงใช้วิธีการเดิม ๆ ในการติดต่อสื่อสารกับลูกค้าจนเกิดความเดือดร้อนรำคาญ ไม่ปฏิบัติต่อข้อมูลที่อยู่อีเมล์ของลูกค้าในฐานะข้อมูลส่วนบุคคล และนำไปสู่สภาวะที่ไม่มีความเชื่อใจ (trust) ระหว่างภาคธุรกิจกับผู้บริโภค ซึ่งแน่นอนว่าเป็นสภาวะอันไม่พึงประสงค์ต่อการขับเคลื่อนสังคมไปสู่ดิจิทัลตามยุทธศาสตร์ชาติ อีกทั้งผิดไปจากมาตรฐานโลกทั้งที่โลกดิจิทัลในยุคต่อไปจะต้องมีกิจกรรมข้ามพรมแดนมากขึ้น และอาจทำให้ธุรกิจไทยที่ต้องทำงานติดต่อสื่อสารกับลูกค้าชาวต่างชาติกระทำผิดกฎหมายลักษณะเดียวกันของต่างรัฐอื่นด้วย

ในภาพใหญ่ ประเด็นปัญหาของการร่างพระราชบัญญัติและประกาศฉบับนี้สะท้อนปัญหาของการหาจุดสมดุลระหว่างการไหลเวียนอย่างเสรีของข้อมูล สิทธิเสรีภาพของประชาชนที่เกี่ยวข้องการปฏิบัติงานของเจ้าหน้าที่รัฐ และภาระของภาคธุรกิจ ซึ่งอาจเกิดจากความไม่เข้าใจว่าผลการแทรกแซงของรัฐเพื่อกำกับดูแลการส่งอีเมล์เชิงพาณิชย์นั้นไม่ได้เป็นไปเพื่อประโยชน์ของผู้บริโภคเพียงอย่างเดียว แต่ยังเป็นประโยชน์ต่อภาคธุรกิจเองในระยะยาวและต่อเครือข่ายอินเทอร์เน็ตโดยรวมอีกด้วย ทำให้ในท้ายที่สุดกฎหมายถูกเขียนมาในลักษณะที่มุ่งหวังจะลดภาระของภาคธุรกิจมากเกินจนเพิ่มภาระให้กับผู้บริโภค และเปิดช่องให้ภาคธุรกิจยังคงดำเนินการตามแนวทางเดิมไม่ปรับตัวให้สอดคล้องกับทางปฏิบัติของสังคมนานาชาติ

---

[18]Meyer Potashman, International Spam Regulation & Enforcement: Recommendations Following the World Summit on the Information Society, 29 Boston College International and Comparative Law Review 323 (2006), p.325-326. อนึ่ง นอกจากทำให้เกิดสภาพแวดล้อมอันไม่พึงประสงค์ของการใช้เครือข่ายสแปมยังเป็นปัญหาเกี่ยวโยงกับการพัฒนาโครงสร้างอินเทอร์เน็ตพื้นฐานในประเทศกำลังพัฒนาด้วย จึงทำให้สแปมเป็นประเด็นหลักแรก ๆ ของการอภิบาลอินเทอร์เน็ตในระดับระหว่างประเทศช่วงทศวรรษปี 2000s