Sawatree Suksri, สาวตรี สุขศรี
Siriphon Kusonsinwut, ศิริพล กุศลสินวุฒิ
Orapin Yingyongpathana อรพิณ ยิ่งยงพัฒนา

Research on the Impact of the Computer-related Crimes Act 2007 and State Policies on the Right to Freedom of Expression

COM-PUTER CRIME?

อาชญากรรมคอมพิวเตอร์?

งานวิจัยหัวข้อ ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น

Computer Crime?

Research title:

Impact of the Computer-related Crime Act 2007 and State Policies on the Right to Freedom of Expression

Sawatree Suksri
Siriphon Kusonsinwut
Orapin Yingyongpathana

อาชญากรรมคอมพิวเตอร์?

งานวิจัยหัวข้อ

ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิด
เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น

สาวตรี สุขศรี
ศิริพล กุศลศิลป์วุฒิ
อรพิณ ยิ่งยงพัฒนา

อาชญากรรมคอมพิวเตอร์?

งานวิจัยหัวข้อ "ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิด
เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น"

คณะวิจัย

สาวตรี สุขศรี (หัวหน้าโครงการ)
ศิริพล กุศลศิลป์วุฒิ
อรพิณ ยิ่งยงพัฒนา

ผู้ช่วยคณะวิจัย

ดนุช วัลลิกุล ทิวสน สีอุ่น พาขวัญ ชื่นสุวรรณกุล อัชฌา สงฆ์เจริญ

กองบรรณาธิการ

พรพิมพ์ แซ่ลิ้ม ยิ่งชีพ อัชฌานนท์ ธนกฤต เปี่ยมมงคล อาจินต์ ทองอยู่คง

บรรณาธิการต้นฉบับภาษาอังกฤษ

อเล็ก แบมฟอร์ด

ผู้แปล

กัปตัน จึงธีรพานิช ปกป้อง เลาวัณย์ศิริ พงษ์เลิศ พงษ์วนานต์
พิภพ อุดมอิทธิพงศ์ สุลักษณ์ หลำอุบล อธิป จิตตฤกษ์

ที่ปรึกษา

รุจน์ โกมลบุตร ธีระ สุธีวรางกูร

ออกแบบปกและรูปเล่ม

กรมัยพล สิริมงคลรุจิกุล

พิสูจน์อักษร

จิรนันท์ หาญธำรงวิทย์ กษมาพร แสงสุระธรรม ณภัค เสรีรักษ์ พีระเดช ตันเรืองพร

จัดทำโดย

ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพ
โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw)
http://freedom.ilaw.or.th

พิมพ์ที่

โรงพิมพ์ภาพพิมพ์

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataoging in Publication Data

สาวตรี สุขศรี.

อาชญากรรมคอมพิวเตอร์? : งานวิจัยหัวข้อ “ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น”.-- กรงเทพฯ : โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw) ในมูลนิธิอาสาสมัครเพื่อสังคม, 2555.

720 หน้า.

1. คอมพิวเตอร์--กฎหมายและระเบียบข้อบังคับ. I. ศิริพล กุศลศิลป์วุฒิ, ผู้แต่งร่วม. II. อรพิณ ยิ่งยงพัฒนา, ผู้แต่งร่วม. III. ชื่อเรื่อง.

343.0994
ISBN 978-616-91463-0-8

สนับสนุนโดย

HEINRICH BÖLL STIFTUNG SOUTHEAST ASIA

มูลนิธิไฮน์ริค เบิลล์ เอเชียตะวันออกเฉียงใต้

Computer Crime?

Research title : Impact of the Computer-related Crime Act 2007 and State Policies on the Right to Freedom of Expression

Research Team

Sawatree Suksri (Director)

Siriphon Kusonsinwut

Orapin Yingyongpathana

Research Assistants

Danuch Wallikul, Tewson Seeoun, Pakwan Chuensuwankul and Atcha Songcharoen

Editorial Team

Pornpim Saelim, Yingcheep Atchanont, Thanakrit Piammongkol and Arjin Thongyuukong

Editor (English version)

Alec Bamford

Translators

Kaptan Jungteerapanich, Pokpong Lawansiri, Pipob Udomittipong, Ponglert Pongwanan, Suluck Lamubol and Athip Jittarerk

Advisors

Ruj Komonbutr and Theera Sutheewarangkul

Cover Design and Layout

Kornmaipol Sirimongkolrujikul

Proof Reader

Jiranan Hanthamrongwit, Napak Serirak, Kasamaponn Saengsuratham and Peeradej Tanruangporn

Production Editor

iLaw FREEDOM

Freedom of Expression Documentation Centre, iLaw

http://freedom.ilaw.or.th

Printing House

Parbpim Ltd., Part.

Supported by

HEINRICH
BÖLL
STIFTUNG
SOUTHEAST
ASIA

Heinrich Böll Foundation Southeast Asia

สารบัญ

ผลการศึกษาภาคที่ 2

Table of Content

บทสรุปย่อ

งานวิจัยหัวข้อ “ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิและเสรีภาพในการแสดงความคิดเห็น” ฉบับนี้ ศึกษาผลกระทบจากการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ตั้งแต่เริ่มประกาศใช้เมื่อเดือนกรกฎาคม 2550 ถึงเดือนธันวาคม 2554 แนวนโยบายของรัฐไทย รวมทั้งปฏิกิริยาของประชาชนที่มีต่อกฎหมายและการบังคับใช้ โดยเปรียบเทียบประเด็นต่างๆ ดังกล่าวกับต่างประเทศ

ผลการศึกษาการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

ผลการศึกษาพบว่า ตลอดช่วงระยะเวลา 4 ปี 6 เดือน ที่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีผลใช้บังคับ มีสถิติการระงับการเผยแพร่เนื้อหา หรือการปิดเว็บไซต์โดยอาศัยมาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ผ่านคำสั่งศาลจำนวน 156 ฉบับ จำนวนทั้งสิ้น 81,213 ยูอาร์แอล ทั้งนี้ เนื้อหาที่ถูกปิดกั้นเป็นอันดับหนึ่ง คือ เนื้อหาและภาพดูหมิ่น หมิ่นประมาท พระมหากษัตริย์ พระราชินี และรัชทายาท ซึ่งมีคำสั่งศาล 90 ฉบับ ให้ระงับการเข้าถึง

60,790 ยูอาร์แอล หรือคิดเป็นร้อยละ 75 ของจำนวนยูอาร์แอลที่ถูกปิดกั้นทั้งหมด อันดับสอง คือ เนื้อหาและภาพลามกอนาจาร มีคำสั่งศาล 52 ฉบับ ให้ระงับการเข้าถึง 19,395 ยูอาร์แอล หรือคิดเป็นร้อยละ 24 ของจำนวนยูอาร์แอลที่ถูกปิดกั้นทั้งหมด ที่เหลืออีกร้อยละ 1 เป็นเนื้อหาเกี่ยวกับยาและการทำแท้งด้วยตนเอง เนื้อหายุยงให้เล่นการพนัน ดูหมิ่นศาสนา เว็บไซต์ปลอมเพื่อหลอกเอาข้อมูลอิเล็กทรอนิกส์ (Pharming) และเว็บไซต์ที่มีเนื้อหาที่อาจทำให้ประชาชนเข้าใจผิดเกี่ยวกับเหตุการณ์การควบคุมและสลายการชุมนุม ซึ่งอาจก่อให้เกิดความปั่นป่วน หรือกระด้างกระเดื่องในหมู่ประชาชน

ปี 2552 เป็นปีที่มี “จำนวนคำสั่งศาล” ให้ปิดกั้นเว็บไซต์ตามคำขอของกระทรวงเทคโนโลยีสารสนเทศ (ไอซีที) สูงที่สุด คือ 64 ฉบับ ยังผลให้ปิดกั้น 28,705 ยูอาร์แอล ในขณะที่ปี 2553 เป็นปีที่มี “จำนวนเว็บไซต์” ถูกปิดกั้นสูงที่สุด คือ 45,357 ยูอาร์แอล โดยคำสั่งศาล 45 ฉบับ แม้กฎหมายจะกำหนดกลไกการตรวจสอบถ่วงดุลอำนาจ โดยให้ศาลเป็นองค์กรผู้กลั่นกรองคำร้องให้ปิดกั้นเว็บไซต์ แต่ในทางปฏิบัติ ด้วยปัญหาหลายประการ ทั้งในแง่ของความเร่งด่วน จำนวนยูอาร์แอลที่ถูกร้องขอ รวมทั้งภารกิจส่วนอื่นๆ ของศาล พบว่าศาลไม่สามารถใช้เวลาได้มากนักในการกลั่นกรองคำร้องดังกล่าว เช่น ในปี 2552 และ 2553 จำนวนยูอาร์แอลที่ถูกยื่นขอต่อศาลมีจำนวนมาก เมื่อคำนวณออกมาแล้วพบว่าศาลต้องใช้เวลาพิจารณาและสั่งปิดกั้นโดยเฉลี่ยถึง 326 ยูอาร์แอลต่อวันในปี 2552 และ 986 ยูอาร์แอลต่อวันในปี 2553 ซึ่งข้อมูลชี้ว่า จากคำสั่งศาลทั้งสิ้น 156 ฉบับ มีถึง 142 ฉบับที่ศาลออกคำสั่งในวันเดียวกันกับที่กระทรวงไอซีทียื่นคำร้อง

ปัจจัยหนึ่งที่มีอิทธิพลต่อการปิดกั้นเว็บไซต์ในประเทศไทย ส่วนหนึ่งมาจากสถานการณ์ความขัดแย้งทางการเมือง ซึ่งส่งผลต่ออัตราการแสดงออกในเรื่องการเมืองของประชาชนผ่านสื่อออนไลน์ อย่างไรก็ดี การปิดกั้นเว็บไซต์ตามมาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550 เป็นเพียงหลักการที่ใช้เฉพาะในสถานการณ์ปกติเท่านั้น สำหรับในสถานการณ์ที่รัฐไทยเห็นว่ามีความพิเศษหรือไม่ปกติ ยังมีกฎหมายและมาตรการอื่นๆ ที่ใช้จำกัดการแสดงความคิดเห็นของประชาชน อาทิ การประกาศสถานการณ์

ฉุกเฉิน และใช้ พ.ร.ก.การบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 หรือการขอความร่วมมืออย่างไม่เป็นทางการไปยังผู้ให้บริการอินเทอร์เน็ต เพื่อให้ปิดกั้นเว็บไซต์ เป็นต้น

ด้านสถิติคดีความตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 พบว่า ตลอดระยะเวลาที่มีผลใช้บังคับ มีคดีความตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 จำนวนทั้งสิ้น 325 คดี แม้วัตถุประสงค์แรกเริ่มของการตราพระราชบัญญัติฉบับนี้จะเป็นไปเพื่ออุดช่องว่างของกฎหมาย และป้องปรามอาชญากรรมคอมพิวเตอร์โดยแท้ก็ตาม แต่เมื่อพิจารณาจากจำนวนคดีที่ขึ้นสู่ศาลแล้วกลับพบว่าคดีความผิดอันเกิดจากการเผยแพร่เนื้อหาตามมาตรา 14-16 มีสัดส่วนสูงถึงร้อยละ 66.15 ในขณะที่คดีที่กระทำต่อตัวระบบหรือข้อมูลคอมพิวเตอร์ (อาชญากรรมคอมพิวเตอร์โดยแท้) ตามมาตรา 5-13 มีเพียงร้อยละ 19 เท่านั้น ทั้งนี้ หากพิเคราะห์ในรายละเอียดของคดีความทั้งหมดสามารถจำแนกประเภทความผิดได้ดังนี้ อันดับหนึ่ง หมิ่นประมาทบุคคลอื่น จำนวน 100 คดี อันดับสอง อาชญากรรมคอมพิวเตอร์โดยแท้ 47 คดี อันดับสาม ดูหมิ่นกษัตริย์ฯ 40 คดี อันดับสี่ ความผิดฐานฉ้อโกงหรือหลอกลวงทางอินเทอร์เน็ต 31 คดี อันดับห้า เผยแพร่ภาพลามก 31 คดี อันดับหก เผยแพร่โปรแกรมที่เข้าข่ายผิดกฎหมาย 12 คดี อันดับเจ็ด เนื้อหาเกี่ยวกับความมั่นคง 6 คดี และเนื้อหาอื่นๆ ที่ไม่สามารถระบุได้อีก 58 คดี สำหรับลักษณะของผู้ถูกกล่าวหา พบว่าจากคดีความ 325 คดี บุคคลทั่วไปถูกตั้งข้อหา 220 คดี และตัวกลางผู้ให้บริการถูกตั้งข้อหาอีก 26 คดี ที่เหลือเป็นคดีที่คณะผู้วิจัยไม่สามารถระบุลักษณะของผู้กระทำความผิดได้ว่าอยู่ในกลุ่มใด

จากการสัมภาษณ์และสัมมนากลุ่มย่อยเพื่อแลกเปลี่ยน และแสดงความคิดเห็นเกี่ยวกับประสบการณ์ และผลที่เกิดจากการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งแหล่งข้อมูล และผู้เข้าร่วมเป็นบุคลากรภาครัฐ ตัวแทนผู้ประกอบการอินเทอร์เน็ต และตัวแทนกลุ่มเว็บมาสเตอร์ พบว่าจุดเด่นของกฎหมายฉบับนี้ คือ ทำให้การปิดกั้นเว็บไซต์ การขอและการส่งมอบข้อมูลจราจรคอมพิวเตอร์ มีความชัดเจนขึ้น อยู่ในขอบเขต และเป็น

ไปตามขั้นตอนของกฎหมาย แต่แม้กระนั้นก็ตาม ในทางปฏิบัติ การ “ขอความร่วมมือ” อย่างไม่เป็นทางการจากฝ่ายรัฐ ก็ยังปรากฏอยู่ด้วยข้ออ้างเรื่องเหตุจำเป็นเร่งด่วน

ประเด็นที่หลายฝ่ายเห็นว่าเป็นปัญหาร่วมกัน คือ ความไม่มั่นใจในการใช้การตีความกฎหมายของเจ้าหน้าที่รัฐ และผู้รับผิดชอบการบังคับใช้ เช่น การตีความมาตรา 14 (1) หรือความหมายของคำว่า “จงใจสนับสนุนหรือยินยอม” ของตัวกลางตามมาตรา 15 เป็นต้น นอกจากนี้ยังพบปัญหาในเรื่องบุคลากรในกระบวนการยุติธรรมยังขาดความรู้ความเข้าใจในองค์ประกอบความผิดและการใช้กฎหมายฉบับนี้ ความเห็นหนึ่งจากบุคลากรภาครัฐเห็นว่า ประเทศไทยควรจัดตั้งศาลชำนัญพิเศษซึ่งมีผู้พิพากษาสมทบที่มีความรู้ความเชี่ยวชาญเกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศเป็นองค์คณะพิจารณาคดีด้วย

สำหรับกลุ่มผู้ดูแลจัดการเว็บไซต์ แอดมิน หรือเว็บมาสเตอร์ เห็นว่า พ.ร.บ.คอมพิวเตอร์ฯ 2550 สร้างความเสี่ยงในความรับผิดทางอาญาแก่ตัวกลางผู้ให้บริการมากเกินไป ทำให้ผู้ให้บริการมีหน้าที่กลั่นกรองเนื้อหาของผู้ใช้บริการก่อน เว็บไซต์บางแห่งต้องปรับโครงสร้างเว็บไซต์ใหม่ เช่น กำหนดให้ผู้ใช้บริการต้องสมัครสมาชิกก่อนโพสต์เนื้อหา กฎหมายฉบับนี้จึงมีแนวโน้มละเมิดเสรีภาพมากกว่าการคุ้มครองเสรีภาพ ด้านกลุ่มผู้ประกอบการอินเทอร์เน็ตเห็นว่า กฎหมายควรแบ่งระดับความรับผิดชอบของผู้ให้บริการให้ชัดเจนกว่านี้ รวมทั้งควรมีแนวปฏิบัติที่ชัดเจนเกี่ยวกับการแจ้งให้ดำเนินการกับข้อความ หรือเนื้อหาที่ผิดกฎหมาย (takedown procedure) และรัฐควรหันมาใช้นโยบายให้ผู้ให้บริการกำกับดูแลกันเองแทนการกำหนดความรับผิดแก่ตัวกลาง นอกจากนี้ยังเห็นว่า เมื่อมีกฎหมายที่ออกมาเพื่อป้องกันการกระทำความผิดแล้ว ก็ควรให้ความสำคัญกับกลไกที่จะใช้คุ้มครองผู้ใช้บริการอินเทอร์เน็ตด้วย เช่น การคุ้มครองข้อมูลส่วนบุคคล เป็นต้น อย่างไรก็ตาม กลุ่มผู้ประกอบการอินเทอร์เน็ตเห็นว่า การปิดกั้นเว็บไซต์ ยังเป็นมาตรการที่มีความจำเป็นอยู่ แต่รัฐไม่ควรใช้อย่างพร่ำเพรื่อ และควรเข้าใจด้วยว่าการปิดกั้นเว็บไซต์ไม่ใช่หนทางการแก้

ปัญหาที่ได้ผล หรือตรงจุด หากแต่ต้องมุ่งแก้ปัญหาที่ต้นเหตุมากกว่า เช่น การพยายามสืบหาตัว และดำเนินคดีกับผู้กระทำความผิดที่แท้จริง เป็นต้น ในขณะที่ กลุ่มเว็บมาสเตอร์เห็นว่า ประเทศไทยควรมีคณะกรรมการร่วมหลายฝ่ายเพื่อทำหน้าที่ในการกลั่นกรองคำร้องปิดกั้นเว็บไซต์แทนศาล

ผลการวิเคราะห์ปัญหาที่เกี่ยวกับบทบัญญัติใน พ.ร.บ.คอมพิวเตอร์ฯ 2550

ผลการศึกษากฎหมาย และแนวนโยบายแห่งรัฐไทยพบว่า พ.ร.บ.คอมพิวเตอร์ฯ 2550 เป็นกฎหมายที่มีผลโดยตรงต่อเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นในสื่อออนไลน์ ซึ่งในงานวิจัยพบปัญหาของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ดังนี้

ปัญหาการนิยามศัพท์ เช่น คำว่า “ผู้ให้บริการ” ตามมาตรา 4 วรรคสาม ที่กำหนดนิยามและแยกประเภทของ “ผู้ให้บริการ” ไว้ไม่ชัดเจนและไม่สอดคล้องกับความจริงหรือความเข้าใจในทางเทคโนโลยี อีกทั้งยังกำหนดให้ผู้ให้บริการทุกประเภทมีหน้าที่ทั้งเก็บข้อมูลจราจรคอมพิวเตอร์ และมีความรับผิดต่อการเผยแพร่เนื้อหาของผู้อื่นโดยไม่แยกแยะ ทำให้ผู้ให้บริการบางประเภท โดยเฉพาะอย่างยิ่งที่ไม่ได้ปฏิบัติงาน หรือมีส่วนที่เกี่ยวข้องกับเนื้อหาข้อมูลดังกล่าวต้องเข้ามาร่วมรับผิดด้วย

ปัญหาในการบัญญัติฐานความผิด ซึ่งปรากฏความคลุมเครือของบทบัญญัติทั้งใน มาตรา 14 มาตรา 15 และ มาตรา 20 แห่ง พ.ร.บ.คอมพิวเตอร์ฯ 2550 ทั้งนี้ แม้เจตนารมณ์แรกเริ่มของพระราชบัญญัติฉบับนี้ คือ มุ่งเน้นแก้ปัญหาอาชญากรรมคอมพิวเตอร์โดยแท้ ที่ไม่สามารถอาศัยบทบัญญัติในประมวลกฎหมายอาญามาบังคับใช้ได้เนื่องจากมีองค์ประกอบความผิดแตกต่างกัน แต่ในท้ายที่สุดกลับพบว่า พระราชบัญญัติฉบับนี้ถูกนำมาใช้จัดการเนื้อหาที่เผยแพร่ในสื่ออินเทอร์เน็ตมากกว่า ซึ่งย่อมส่งผลกระทบโดยตรงต่อเสรีภาพของประชาชน

มาตรา 14 (1) มุ่งใช้กับข้อมูลคอมพิวเตอร์ปลอมหรือเท็จ เพื่อ

อุดช่องว่างของกฎหมายอาญาว่าด้วยการปลอมแปลงเอกสาร แต่ในทางปฏิบัติกลับพบว่ามาตรานี้มักถูกนำมาใช้ฟ้องร้องเรื่องหมิ่นประมาทเป็นจำนวนมาก ทั้งที่ความผิดฐานหมิ่นประมาทถูกกำหนดเอาไว้ในกฎหมายแพ่งและอาญาอยู่แล้ว การตั้งข้อหาหมิ่นประมาทด้วย พ.ร.บ.คอมพิวเตอร์ฯ 2550 ส่งผลทำให้ความผิดที่ว่าด้วยการหมิ่นประมาทกลายเป็น “อาญาแผ่นดิน” ที่นอกจากคู่กรณีจะตกลงยอมความกันไม่ได้แล้ว ยังทำให้บุคคลใดก็ได้สามารถเป็นผู้กล่าวโทษกับเจ้าพนักงาน นอกจากนี้ ในแง่ของการตีความยังอาจก่อให้เกิดคำถามได้อีกว่า ผู้ถูกกล่าวหาสามารถพิสูจน์เหตุยกเว้นความผิดหรือเหตุยกเว้นโทษตามประมวลกฎหมายอาญาได้หรือไม่ การตีความมาตรา 14 (1) เช่นนี้ ย่อมก่อให้เกิดความสับสนในการใช้การตีความกฎหมาย รวมทั้งส่งผลให้การหมิ่นประมาทตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีระดับความรุนแรงยิ่งกว่าที่กำหนดไว้ในประมวลกฎหมายอาญา

มาตรา 14 (2) มักถูกใช้ตั้งข้อหาควบคู่กับคดีความมั่นคง โดยมาตรา 14 (2) เป็นมาตราหนึ่งในกฎหมายฉบับนี้ที่มีปัญหาในเรื่องขอบเขตการบังคับใช้มากที่สุด และถูกวิพากษ์วิจารณ์ว่าถูกฝ่ายรัฐใช้เป็นเครื่องมือในการลิดรอนเสรีภาพในการแสดงความคิดเห็นของประชาชน เนื่องจากมีถ้อยคำกำกวมไม่ชัดเจนอย่าง “ความเสียหายต่อความมั่นคง” และ “ก่อให้เกิดความตื่นตระหนกแก่ประชาชน” ซึ่งขัดกับ “หลักความชอบด้วยกฎหมาย” หรือ ”หลักประกันทางกฎหมายอาญา” ในส่วนที่ว่า “กฎหมายต้องบัญญัติให้ชัดเจนแน่นอน” แต่มาตรานี้ ประชาชนโดยทั่วไปไม่สามารถเข้าใจได้ว่าข้อมูลที่มีเนื้อหาอย่างใดจึงจะเข้าข่ายเป็นความผิดดังกล่าว ขึ้นอยู่กับดุลพินิจของเจ้าพนักงานรัฐเป็นสำคัญ ซึ่งย่อมสุ่มเสี่ยงต่อการตีความเกินเลยหรือตามอำเภอใจ ท้ายที่สุดมาตรานี้จึงอาจถูกนำไปใช้เป็นเครื่องมือเล่นงานกันทางการเมือง

มาตรา 14 (3) บัญญัติถึงความผิดว่าด้วยการเผยแพร่เนื้อหาที่เกี่ยวกับความมั่นคงไว้เช่นกัน แต่มีความชัดเจนในเรื่ององค์ประกอบความผิดมากกว่ามาตรา 14 (2) เนื่องจากเชื่อมโยงไปยังฐานความผิดในประมวลกฎหมายอาญา จนเกิดคำถามขึ้นว่าเหตุใดจึงต้องมีทั้งมาตรา 14 (2) และ

(3) อยู่ในกฎหมายฉบับเดียวกัน

สถิติคดีชี้ว่าคดีตามมาตรา 14 (2) และ (3) ส่วนใหญ่เป็นการบังคับใช้ร่วมกับประมวลกฎหมายอาญา มาตรา 112 ความผิดฐานหมิ่นประมาทพระมหากษัตริย์ พระราชินี และรัชทายาท ซึ่งหากจะกล่าวถึงปัญหาของบทบัญญัติ รวมทั้งการบังคับใช้ พ.ร.บ. คอมพิวเตอร์ฯ 2550 ที่ส่งผลกระทบต่อเสรีภาพของประชาชนในสื่อออนไลน์ให้ครบถ้วนแล้ว ก็มิอาจหลีกเลี่ยงการกล่าวถึงปัญหาในเนื้อหา ปัญหาการบังคับใช้ไปจนถึงปัญหาอุดมการณ์ในการใช้การตีความมาตรา 112 แห่งประมวลกฎหมายอาญาไปได้ ซึ่งอาจสรุปสาระสำคัญของปัญหาดังกล่าวได้ว่า มาตรา 112 มีลักษณะเป็นอัตวิสัยอยู่มาก และมีสถานะเป็นอาญาแผ่นดิน ที่ยังผลให้บุคคลใด ๆ ก็ได้ กล่าวโทษหรือแจ้งความกับเจ้าหน้าที่รัฐเพื่อให้ดำเนินคดีกับบุคคลอื่น ด้วยลักษณะเช่นนี้เอง จึงเปิดโอกาสให้เกิดการกลั่นแกล้งฟ้องกัน อีกทั้งยังกำหนดอัตราโทษไว้สูงมาก ไม่เป็นไปตามหลักความได้สัดส่วน คือ จำคุกตั้งแต่ 3 ถึง 15 ปี โดยไม่มีบทกำหนดเหตุยกเว้นความผิด ไม่มีเหตุยกเว้นโทษ ปิดโอกาสไม่ให้ผู้กระทำความผิดได้พิสูจน์ความจริงของถ้อยคำที่ตนกล่าว

ปัญหาอีกปัญหาหนึ่งที่พบจาก พ.ร.บ. คอมพิวเตอร์ฯ 2550 ก็คือความซ้ำซ้อนกันของกฎหมาย กล่าวคือ มาตรา 14 (1) ว่าด้วยการเผยแพร่ข้อมูลเท็จซึ่งทำให้ผู้อื่นได้รับความเสียหาย ที่ในทางปฏิบัติมักถูกนำมาใช้ฟ้องคดีซ้ำซ้อนกับความผิดฐานหมิ่นประมาท มาตรา 14 (3) ว่าด้วยความผิดเกี่ยวกับความมั่นคงซ้ำซ้อนกันเองกับมาตรา 14 (2) และมาตรา 14 (4) ว่าด้วยความผิดเกี่ยวกับการเผยแพร่ข้อมูลลามก ก็มีลักษณะซ้ำซ้อนกับมาตรา 287 แห่งประมวลกฎหมายอาญา และในทางปฏิบัติพบว่ามาตราดังกล่าวมักถูกใช้ไปเพื่อการขอคำสั่งปิดกั้นเว็บไซต์มากกว่าที่จะนำมาใช้ดำเนินคดีกับผู้กระทำความผิด

มาตรา 15 ซึ่งกำหนดความรับผิดแก่ผู้ให้บริการนั้น นอกจากจะมีปัญหาในแง่ของความชัดเจนของนิยามคำว่า “ผู้ให้บริการ” ดังกล่าวไปแล้ว มาตรานี้ยังกำหนดโทษแก่ผู้ให้บริการไว้ให้เท่ากับผู้กระทำความผิดหรือตัวการอีกด้วย ซึ่งไม่น่าจะสมเหตุสมผลหรือได้สัดส่วนระหว่างความผิดที่

เกิดขึ้นกับหน้าที่ความรับผิดชอบ เพราะหลายกรณีผู้ให้บริการมีสถานะเป็นเพียง “ตัวกลาง” ผู้ส่งผ่านข้อมูลในระบบคอมพิวเตอร์เท่านั้น ในขณะที่หากพิจารณาตามกฎหมายอาญาแล้ว การกระทำของผู้ให้บริการอาจเข้าข่ายเป็นเพียง “ผู้สนับสนุน” และด้วยผลของมาตรา 15 นี้เอง ที่ทำให้ผู้ให้บริการจำนวนไม่น้อยตัดสินใจ “เซ็นเซอร์ตัวเอง” ซึ่งย่อมกระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชนด้วย และนอกจากปัญหาในตัว พ.ร.บ. คอมพิวเตอร์ฯ 2550 เองแล้ว ยังมีปัญหาว่าประเทศไทยยังไม่มีหลักเกณฑ์เกี่ยวกับมาตรการการกำกับเนื้อหาบนอินเทอร์เน็ต ที่ผู้ดูแลรักษาข้อมูลยอมรับที่จะลบข้อมูลในส่วนที่มีการบอกแจ้งให้ทราบออกจากพื้นที่การให้บริการของตน โดยไม่ต้องตรวจสอบความผิดกฎหมายโดยศาลก่อน (Notice and Takedown) ทำให้รัฐขาดแนวทางปฏิบัติที่ชัดเจนว่าใครบ้างที่ควรเป็นผู้มีอำนาจบอกแจ้งเนื้อหาที่อาจเป็นความผิดนั้นแก่ผู้ให้บริการ ไม่มีระเบียบที่แน่ชัดเกี่ยวกับวิธีการบอกแจ้ง (อย่างเป็นทางการ) รายละเอียดที่จำเป็นในการบอกแจ้ง มาตรการที่ยืนยันเบื้องต้นว่าข้อความนั้นเข้าข่ายเป็นความผิดอย่างไร รวมทั้งระยะเวลาอันสมควรที่รัฐกำหนดให้ผู้ให้บริการดำเนินการกับเนื้อหาภายหลังได้รับแจ้ง เป็นผลทำให้ในช่วงระยะที่ผ่านมา การบังคับใช้กฎหมายในหลายๆ กรณีไม่มีมาตรฐาน ขึ้นอยู่กับดุลพินิจของเจ้าพนักงานแต่ละราย กระทั่งเป็นเพียงการบังคับให้ร่วมมืออย่างไม่เป็นทางการ

มาตรา 20 ว่าด้วยการระงับการเผยแพร่เนื้อหา หรือการปิดเว็บไซต์ ถือได้ว่าเป็นมาตรการเร่งด่วนที่รัฐใช้เป็นเครื่องมือปราบปรามการกระทำความผิด แต่กลับปรากฏว่าใช้ถ้อยคำที่คลุมเครือไม่ชัดเจนว่าเนื้อหาประเภทใดที่อาจถูกปิดกั้นได้ ซึ่งโดยหลักการแล้วมาตรการเช่นนี้ต้องบัญญัติเงื่อนไขและหลักเกณฑ์ให้ชัดเจน วางอยู่บนหลักพื้นฐานว่าด้วยการคุ้มครองเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็น การปิดกั้นเว็บไซต์ควรเป็นมาตรการขั้นสุดท้าย ใช้เท่าที่จำเป็น และอย่างจำกัดเสมือนหนึ่งเป็นเพียง “ข้อยกเว้น” เนื่องจากกระทบสิทธิของประชาชนค่อนข้างมาก เพราะให้อำนาจกับฝ่ายบริหารโดยยังไม่ผ่านการพิจารณา “ความผิด” ในกระบวนการยุติธรรมเสียก่อน แต่ความเป็นจริงที่เกิดขึ้นก็

คือ ที่ผ่านมา มาตรา ๒๐ กลายเป็นบทบัญญัติที่ถูกนำมาใช้เป็น “หลัก” ดังที่แสดงให้เห็นแล้วจากผลการศึกษาในส่วนของสถิติการปิดกั้นเว็บไซต์กับการดำเนินคดีกับผู้กระทำความผิด

การศึกษาเปรียบเทียบกฎหมายควบคุมสื่อออนไลน์และแนวนโยบายรัฐกับต่างประเทศ

หากเปรียบเทียบสถานการณ์กฎหมายกับสื่อออนไลน์ในต่างประเทศ ในที่นี้คือ ประเทศสหพันธรัฐเยอรมนี มาเลเซีย สหรัฐอเมริกา และจีนแล้ว พบว่าทุกประเทศต่างรับรองเสรีภาพในการแสดงความคิดเห็นและการรับรู้ข้อมูลข่าวสารเอาไว้ในรัฐธรรมนูญเหมือนกัน แต่มี “ข้อยกเว้น” หรือ “ข้อจำกัดเสรีภาพ” ลักษณะนี้ที่แตกต่างกันออกไป เช่น เยอรมนีมีข้อยกเว้นไม่ให้ความคุ้มครองเนื้อหาต่างๆ ที่เป็นอันตรายต่อเด็กและเยาวชน ต่อสันติภาพของประชาชน การดูถูกศักดิ์ศรีความเป็นมนุษย์ เหยียดหยามเชื้อชาติอื่น รวมทั้งการเผยแพร่ชาตินิยมเยอรมัน (ลัทธินาซี) สหรัฐอเมริกามีข้อยกเว้นกรณีเนื้อหาที่เป็นอันตรายต่อเด็กและเยาวชน จีนมีข้อยกเว้นในกรณีเนื้อหาที่เกี่ยวกับความมั่นคงของชาติและเสถียรภาพของรัฐบาล ส่วนมาเลเซียมีข้อยกเว้นในกรณีเนื้อหาที่เกี่ยวกับความมั่นคง ขัดต่อหลักความเชื่อในศาสนาอิสลาม ลามกอนาจารและหยาบคาย และเนื้อหาที่เป็นอันตรายต่อเด็กและเยาวชน อย่างไรก็ตาม ไม่ปรากฏว่ามีประเทศใดข้างต้นที่บัญญัติความผิดเกี่ยวกับการเผยแพร่เนื้อหาไว้ในกฎหมายที่ว่าด้วยอาชญากรรมคอมพิวเตอร์ รวมทั้งไม่มีประเทศใดที่กำหนดความผิดและโทษสำหรับผู้ให้บริการอินเทอร์เน็ตหรือตัวกลางไว้ “เท่ากับ” ผู้เผยแพร่เนื้อหาที่เป็นความผิดนั้นเอง ในขณะที่ประเทศจีนและมาเลเซียพยายามกำกับดูแลเนื้อหาในอินเทอร์เน็ต โดยกำหนดเป็น “ภาระหน้าที่” ในการช่วยสอดส่องสื่อออนไลน์แก่ผู้ให้บริการ

เมื่อศึกษาเปรียบเทียบกันแล้วพบว่า การปิดกั้นเว็บไซต์เกิดขึ้นในทุกประเทศ แต่ทั้งความถี่ของการใช้อำนาจปิดกั้น (เท่าที่สืบค้นได้ และ

เป็นข่าว) และลักษณะของการใช้อำนาจรัฐมีความแตกต่างกัน กรณีของเยอรมนีมีคดีหรือกรณีปิดกั้นเว็บไซต์ค่อนข้างน้อย และในกรณีที่เกิดการปิดกั้นจะเป็นไปตามขอบเขตแห่งกฎหมายที่ชัดเจน กระทำภายใต้หลักแห่งความได้สัดส่วน และส่วนใหญ่ถูกโต้แย้งคัดค้าน จนถึงกระทั่งการกระทำเช่นนั้นของรัฐถูกประชาชนยื่นฟ้องต่อศาล กรณีของสหรัฐอเมริกาจำนวนหนึ่งมีลักษณะปิดกั้นเว็บไซต์อย่างไม่เป็นทางการ โดยใช้อำนาจลับที่รัฐสั่งการไปยังผู้ให้บริการ และมีหน่วยพิเศษตรวจสอบปิดกั้นโดยเฉพาะ สำหรับจีนและไทย มีอัตราการใช้มาตรการปิดกั้นเว็บไซต์ค่อนข้างมาก และมีปัญหาในเรื่องที่บทบัญญัติให้อำนาจยังมีความคลุมเครือ ไม่มีการบอกแจ้งผู้ได้รับผลกระทบ และหลายกรณีเกิดขึ้นอย่างไม่เป็นทางการ ในขณะที่มาเลเซียไม่ค่อยปรากฏการปิดกั้นเว็บไซต์ เนื่องจากมีกฎหมายรับรองคุ้มครองไม่ให้ใช้มาตรการนี้ แต่รัฐมักอาศัยช่องทางอื่นในการควบคุมเนื้อหา เช่น การคุกคามสื่อพลเมือง หรือการดำเนินคดีความมั่นคงกับสำนักข่าวออนไลน์ เป็นต้น ทั้งนี้มีข้อที่ควรสังเกตด้วยว่า รัฐไทยอาจถือเป็นประเทศที่มีมุมมองต่อการปิดกั้นเว็บไซต์ที่มีลักษณะเฉพาะตัว เพราะในขณะที่ประเทศอื่น รวมทั้งประเทศจีนใช้มาตรการเหล่านี้อย่างปิดลับหรือไม่ประสงค์ให้เป็นข่าว แต่จำนวนเว็บไซต์ที่ถูกปิดกั้นในประเทศไทยกลับถือเป็นผลงานการบริหารของกระทรวงไอซีที ในรูปของการ “แถลงผลงาน” ในทุก ๆ รัฐบาลที่ผ่านมา

ด้านสถานการณ์การคุกคามประชาชน หรือพลเมืองอินเทอร์เน็ตนั้น ประเทศจีนและมาเลเซียมีความถี่ในการคุกคามจับกุมผู้ใช้อินเทอร์เน็ตอย่างสม่ำเสมอโดยอาศัยกฎหมายความมั่นคงฉบับต่าง ๆ ที่ใช้บังคับอยู่ ซึ่งหากเปรียบเทียบกับประเทศไทยแล้วพบว่า ความถี่ในการจับกุมหรือความพยายามในการคุกคามผู้ใช้อินเทอร์เน็ตในประเทศไทยไม่ได้เกิดขึ้นอย่างสม่ำเสมอ แต่เกิดขึ้นในช่วงที่มีสถานการณ์ความขัดแย้งทางการเมือง จากการศึกษาพบว่า สถิติคดีเรื่องนี้พุ่งสูงขึ้นอย่างก้าวกระโดดในช่วงการชุมนุมเรียกร้องทางการเมืองของประชาชนกลุ่มต่าง ๆ โดยเฉพาะอย่างยิ่งภายหลังการทำรัฐประหาร 19 กันยายน 2549 นอกจากนี้ ไม่ค่อยพบการดำเนินคดีกับ “ผู้ให้บริการ” เพียงเพราะเขาเป็นผู้ให้บริการ (ไม่ใช่ผู้

เผยแพร่เนื้อหานั้นด้วยตนเอง) ในประเทศอื่นๆ ซึ่งแตกต่างจากกรณีของประเทศไทยที่มุ่งเน้นให้ผู้ให้บริการต้องรับผิดในการกระทำของผู้อื่น

ในส่วนของการเคลื่อนไหว และปฏิกิริยาของประชาชนต่อกฎหมายและนโยบายของรัฐ พบว่าประชาชนในประเทศตะวันตกอย่างเยอรมนีและอเมริกา มีลักษณะหลากหลายช่องทางมากกว่าในประเทศตะวันออก ไม่ว่าจะเป็นการเดินขบวน การรณรงค์ต่อต้าน การจัดสัมมนาให้ความรู้กับสังคมโดยรวม การทำจดหมายเปิดผนึก โดยเฉพาะอย่างยิ่งการนำคดีขึ้นสู่ศาลสูง ในขณะที่รูปแบบการเคลื่อนไหวในจีน มาเลเซีย รวมทั้งไทย มักจำกัดอยู่ในเรื่องของการประท้วงเรียกร้องเชิงนโยบายและสังคมเท่านั้น ไม่ค่อยพบการตอบโต้เรียกร้องให้เกิดผลบังคับทางกฎหมายอย่างในประเทศตะวันตก

ข้อเสนอในงานวิจัย

จากผลการวิจัย คณะผู้วิจัยมีข้อเสนอแนะ ดังนี้

ข้อเสนอแนะทางกฎหมาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ควรเป็นกฎหมายอาญาที่กำหนดความผิดและโทษสำหรับอาชญากรรมคอมพิวเตอร์โดยแท้ หรืออาชญากรรมที่กระทำต่อตัวระบบหรือข้อมูลคอมพิวเตอร์โดยตรงเท่านั้น เช่น การเข้าถึงระบบโดยปราศจากอำนาจ การรบกวนข้อมูล การโจรกรรมข้อมูล เพื่ออุดช่องว่างทางกฎหมายและแก้ปัญหาเรื่องความซ้ำซ้อนของกฎหมาย แต่หากรัฐยืนยันว่าจำเป็นต้องบัญญัติบทลงโทษเกี่ยวกับการเผยแพร่เนื้อหาซึ่งเป็นความผิดบนสื่อออนไลน์ด้วย บทบัญญัติดังกล่าวก็ต้องมีความชัดเจนไม่คลุมเครือ รวมทั้งต้องสอดคล้องกับเจตนารมณ์ของกฎหมายอื่นที่กำหนดความผิดลักษณะเดียวกันนั้นไว้อยู่ก่อน ซึ่งอันที่จริงแล้วรัฐสามารถใช้วิธีแก้ไขเพิ่มเติมความผิดเหล่านั้นไว้ในหมวดความผิดพื้นฐานในเรื่องเดียวกันในประมวลกฎหมายอาญาได้

ควรกำหนดนิยามคำว่า “ผู้ให้บริการ” ให้สอดคล้องกับลักษณะการ

ประกอบกิจการ ภาระหน้าที่ และควรหมายเฉพาะผู้ให้บริการที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์เท่านั้น ไม่ควรขยายความไปถึงผู้ประกอบการด้านโทรคมนาคมประเภทอื่นๆ ที่ห่างไกลจากเนื้อหา หรือไม่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์

การกำหนดความรับผิดและโทษแก่ผู้ให้บริการเกี่ยวกับการเผยแพร่เนื้อหา ผู้บัญญัติกฎหมายควรจำแนกระดับของความรับผิดตามลักษณะ และประเภทของผู้ให้บริการอินเทอร์เน็ต โดยคำนึงถึงความเกี่ยวข้องเชื่อมโยงกับเนื้อหา เช่น ผู้ให้บริการเนื้อหาควรมีความรับผิดต่อเนื้อหา ในขณะที่ผู้ให้บริการทางเทคนิคโดยแท้ไม่ควรมีความรับผิดต่อเนื้อหาใดๆ เลย เว้นแต่เข้าเงื่อนไขบางประการ เช่น พิสูจน์ได้ว่าเขาเป็นผู้คัดเลือก ปรับปรุง หรือเปลี่ยนแปลงข้อมูลที่เผยแพร่นั้น ฯลฯ และหากผู้บัญญัติกฎหมายประสงค์ให้ผู้ให้บริการร่วมรับผิดชอบต่อการกระทำของผู้ใช้บริการอินเทอร์เน็ต หรือลูกค้าของตน กฎหมายก็ไม่ควรกำหนดโทษไว้ “เท่ากับ” ผู้กระทำความผิดที่แท้จริง แต่ควรใช้อัตราที่เหมาะสม ได้สัดส่วน รวมทั้งสอดคล้องกับหลักการในเรื่องผู้กระทำความผิดหลายคน

ในส่วนของมาตรการการระงับการเผยแพร่เนื้อหา หรือปิดกั้นเว็บไซต์ ต้องแก้ไขมาตรา 20 ให้มีความชัดเจน ไม่คลุมเครือ และไม่ทำให้ตีความหมายได้หลายอย่าง อยู่บนหลักที่ว่าหากไม่รีบปิดกั้นโดยเร็วก็จะก่อให้เกิดความเสียหายอย่างมาก หรือไม่มีวิธีการใดที่จะช่วยแก้ไขผลของเนื้อหาที่เผยแพร่นั้นได้อีกแล้ว กฎหมายจะต้องกำหนดวิธีการ กระบวนการ และเงื่อนไขการใช้อำนาจปิดกั้นนี้ไว้อย่างชัดเจนเป็นลายลักษณ์อักษร ซึ่งต้องมีหลักเกณฑ์ที่แน่ชัดในการบอกแจ้งให้ผู้ให้บริการอินเทอร์เน็ตทราบเนื้อหานั้น เมื่อปิดกั้นเว็บไซต์แล้ว ต้องมีกระบวนการต่อเนื่องเพื่อฟ้องร้องและดำเนินคดีกับบุคคลผู้เผยแพร่ข้อมูลอันเป็นเหตุให้ต้องปิดกั้นเว็บไซต์ และหากในท้ายที่สุดพบว่าเนื้อหานั้นไม่ได้เป็นความผิด ศาลจะต้องยกเลิกคำสั่งปิดกั้น และมีมาตรการเยียวยาความเสียหายแก่ผู้ถูกสั่งด้วย นอกจากนี้ ควรมีองค์กรผู้มีอำนาจออกคำสั่งที่มีความรู้ความสามารถ เป็นผู้แทนจากหลายฝ่าย และควรกำหนดกระบวนการพิจารณา รวมทั้งการโต้แย้งคัดค้าน

คำสั่งไว้ในกฎหมายด้วย

ข้อเสนอแนะทางนโยบาย รัฐควรหามาตรการเพื่อกำกับดูแลเนื้อหาบนสื่อออนไลน์ที่ได้ดุลยภาพกับการคุ้มครองเสรีภาพของประชาชน แทนการใช้มาตรการปิดกั้นช่องทางการเข้าถึงเว็บไซต์ เช่น การส่งเสริมกระบวนการหรือกลไกตรวจสอบกันเองระหว่างผู้ใช้และผู้ให้บริการอินเทอร์เน็ต นอกจากนี้ ต้องเร่งพัฒนาความรู้ความสามารถด้านเทคโนโลยีคอมพิวเตอร์ของเจ้าหน้าที่รัฐให้ดีขึ้น รัฐควรต้องส่งเสริมให้มีศาลชำนัญพิเศษเพื่อพิจารณาคดีที่เกี่ยวข้องกับคอมพิวเตอร์โดยเฉพาะ และจัดทำคู่มือปฏิบัติงาน หรืออธิบายกฎหมายและกฎระเบียบต่างๆ ที่เกี่ยวข้อง นอกจากนี้ยังควรสนับสนุนให้ผู้ประกอบการทำประมวลจริยธรรม (Code of Conduct) ในการให้บริการสื่อออนไลน์ รวมทั้งใช้นโยบาย หรือแสวงหามาตรการประเภทอื่น เพื่อสร้างแรงจูงใจในการกำกับดูแลให้แก่ผู้ประกอบการแทนนโยบายปราบปรามหรือลงโทษเพียงอย่างเดียว เช่น มาตรการทางภาษี เป็นต้น

ข้อเสนอแนะต่อประชาชนและผู้ให้บริการสื่อออนไลน์ ประชาชน องค์กรเอกชนที่ทำงานด้านนี้ ฯลฯ ควรให้ความสำคัญกับสิทธิในข้อมูลส่วนบุคคล เสรีภาพในการรับรู้ข่าวสารและเสรีภาพในการแสดงความคิดเห็น และควรตื่นตัว ตรวจสอบการออกกฎหมาย กฎระเบียบต่างๆ รวมทั้งนโยบายของรัฐ ที่อาจส่งผลกระทบต่อเสรีภาพในการรับรู้ข่าวสารและการแสดงความคิดเห็นอย่างสม่ำเสมอ เพื่อไม่ให้รัฐใช้อำนาจเกินขอบเขตและไม่ชอบธรรม นอกจากนี้ ผู้ให้บริการอินเทอร์เน็ตอาจรวมตัวกัน หรือจัดตั้งเป็นกลุ่มผู้ประกอบการอย่างเข้มแข็งเพื่อเฝ้าระวังไม่ให้รัฐกำหนดภาระหน้าที่อันไม่เป็นธรรมและเกินสมควรแก่ผู้ให้บริการ อันจะส่งผลกระทบต่อสิทธิและเสรีภาพของประชาชนด้วย และที่สำคัญ ควรพัฒนาวิธีการและแนวทางการคัดค้านโต้แย้งกฎหมาย นโยบายที่ไม่ชอบธรรม การออกคำสั่งตามอำเภอใจ หรือเรียกร้องสิทธิให้หลากหลายยิ่งขึ้น จากที่เคยจำกัดอยู่ที่การเรียกร้องเชิงนโยบายและสังคมเท่านั้น ก็ก้าวไปสู่การเรียกร้องที่เป็นรูปธรรมและให้ผลทางกฎหมาย อย่างการนำคดีขึ้นสู่ศาลที่เกี่ยวข้อง เป็นต้น

Executive Summary

The Impacts of the Computer-related Crime Act 2007 (CCA) and State Policies on the Right to Freedom of Expression aims to explore implications of the enforcement of CCA since it came into force in July 2007 until December 2011 vis-à-vis state policies as well as public reaction toward the law and its enforcement in comparison to the situation abroad.

Findings on the enforcement of the CCA

It was found that during the entire period of four years and six months when the CCA has been in force, 156 orders have been issued by the courts invoking Section 20 of the CCA to ban access to content or the entire website of a total of 81,213 URLs. The most frequently blocked content concerns information and images deemed to insult and defame the King,

Queen, Heir-apparent, or Regent, for which 90 court orders have been issued to block access to 60,790 URLs, or approximately 75% of the total. This is followed by the blocking of access to pornographic content and images with 52 court orders blocking 19,395 URLs, or 24% of the total. The remain 1% concern content involving abortion medication or self-abortion methods, gambling or blasphemy, bogus and Pharming websites, and websites which might cause misunderstanding about the containment and suppression of demonstrations and which could lead to public commotion or stir up people's resistance.

2009 saw the highest number of court orders issued to block website requested by the Ministry of Information Communication and Technology (MICT); 64 orders suppressed access to 28,705 URLs. 2010 saw the biggest number of websites blocked, 45,357 URLs, by 45 court orders. Though checks and balance mechanisms are built into the law requiring the courts to review and use their discretion prior to issuing orders, in reality, because problems of urgency, the number of URLs involved and the other responsibilities of the courts, it was found that the judiciary could not have spent much time reviewing the requests. For example, in 2009 and 2010, an enormous number of URLs were the subject of requests to the court. On average, the court issued orders to block access to 326 URLs per day in 2009 and 986 in 2010. The data shows that of 156 orders, 142 were issued on the same day the requests were submitted by the MICT.

One dominant factor contributing to the blocking of access to websites in Thailand is the intense political conflicts that have led to a surge of the use of social media to express political views. Nevertheless, Section 20 of the CCA to block access is enforced in normal situations; during emergencies, the

Thai state has other legal provisions to which they can resort to restrict expression of views, i.e., a declaration of emergency and enforcement of the Emergency Decree, or informal requests for cooperation from internet service providers (ISPs) to block certain websites, etc.

It was found that throughout the period the CCA was in force, 325 legal cases were filed. Though one of the basic aims of enacting the CCA was to fill a legal loophole and crack down on conventional computer-related crime, it was found that 66.15% of prosecutions related to the dissemination of allegedly offensive information under Sections 14-16, and only 19% of the cases directly involved offences concerning infringement of computer systems or data (conventional computer-related crime). Prosecutions involved: (1) libel (100 cases), (2) conventional computer related crime (47), (3) lèse majesté (40), (4) electronic fraud or cheating (31), (5) dissemination of pornographic material (31), (6) illegal distribution of software (12), (7) information regarding national security (six); 58 cases were unclassified. Most of those accused and prosecuted were men (153 cases), followed by women (67) and intermediaries or ISPs (26), with the remainder unclassified.

Based on interviews and group discussions eliciting opinions regarding enforcement of the CCA with informants from state agencies, ISPs and webmasters, it was found that one unique feature of the law is it provides clearer definitions and procedures for blocking websites, requests and submission of computer traffic information. However, despite these procedures, informal requests for "cooperation" from the authorities claimed urgency still persist.

One problem shared by various informants is a lack of

confidence in the interpretation by law by state officials and law enforcement officials of Section 14 (1) or the definition of the phrase "intentionally supporting or consenting to" in Section 15 with respect to intermediaries. A lack of knowledge and understanding regarding elements of the crime and enforcement of the law was also found among personnel in the judicial process. One state official opined that a special court should be established to try the cases with help from associate judges who are knowledgeable in computer science and technology.

Webmasters or website administrators tended to the view that the CCA seems to impose disproportionate liability on intermediaries or service providers, forcing them to filter content posted by users. Some websites had to overhaul their structure by requiring prior registration of users for posting messages. Thus, the law tends to infringe, rather than protect freedom. ISPs wanted the levels of liability to be clearly spelled out in law and clear procedures on how to proceed with any information or content deemed illegal (takedown procedures). The state should adopt a policy to encourage ISPs to monitor themselves, instead of imposing penalties on intermediaries. As the law exists to prevent the commission of offences, they also thought it is important to develop mechanisms to protect the personal information of internet users. It was agreed among ISPs that blocking websites is still a necessary measure, but not one that should be used by the state too often. The state should also acknowledge that website blocking is not an effective or direct solution. More effort should be put into solving problems at their root causes, by identifying and prosecuting the real perpetrators. Most webmasters thought a multilateral committee should be established to review blocking requests, in place of the courts.

Analysis of problems regarding provisions in the CCA

The analysis of legal provisions and state policies found the CCA has a direct impact on the right to freedom of information and opinion online. Problems found during the study include:

Definition issues. For example, the term "service provider" in Section 4 fails to clearly define and classify types of "service provider", showing a lack of understanding of reality and the technology. It requires all kinds of service providers to keep computer traffic logs and be indiscriminately held responsible for the dissemination of content uploaded by others. Certain service providers who are not involved with illegal information have consequently been held liable.

Criminality issues concerning provisions in Sections 14, 15 and 20 of the CCA. One fundamental aim of the CCA is to address conventional computer-related crime which cannot be dealt with under the Criminal Code as the elements of the crimes are different. But it was found the CCA has been used mainly to suppress internet content and thus has direct implications for the rights and freedoms of the people.

Section 14 (1) was intended to address bogus or fraudulent computer data, to close a loophole regarding document counterfeiting. It was found that in reality this Section has been used mainly for libel prosecutions, even though libel offences are already actionable under either the Civil or Criminal Code. When a charge of libel is brought to the Court under the CCA, the offence becomes non-compoundable, preventing any mediation between the conflicting parties. It also allows any persons to make accusations. Other problems in interpretation make it

difficult to decide if the accused should be allowed to prove the truth of a statement in order to be exempt from prosecution or penalty. The current interpretation of Section 14 (1) may cause confusion and simply ensures that libel charges under the CCA carry more severe penalties than this under the Criminal Code.

Section 14 (2) is also often used in conjunction with charges concerning national security. In terms of the extent of enforcement, Section 14 (2) is one of the most controversial legal provisions. Its use by the state has been criticized as infringing on the people's right to freedom of expression. It contains vague and ambiguous phrases such as "damage to security" and "causing public panic", which are in breach of the "legality principle" or criminal law safeguards concerning the "certainty of law". The Section fails to establish clearly for ordinary people what kind of information is an offence against the law. State officials are allowed broad discretion in interpreting the law, creating a danger that the law becomes subject to excessive or arbitrary interpretation and eventually a tool of political suppression.

Section 14 (3) also deals with offences regarding the dissemination of security information. However, the elements of crime are spelled out more clearly than in Section 14 (2) since it is linked to offences in the Criminal Code. The question has thus arisen as to why both Section 14 (2) and Section 14 (3) are part of the same law.

Many prosecutions under Section 14 (2) and (3) are made in conjunction with the use of Section 112 of the Criminal Code regarding lèse majesté. A comprehensive examination of the provisions and enforcement of the CCA and infringement of the people's freedoms in the virtual world cannot avoid discussion of the content, enforcement and ideology underlying interpreta-

tion of Section 112 of the Criminal Code. Essentially, Section 112 can be considered as subject to individual discretion. The law allows anyone to report a case. As a result, the law has been used as a tool against others. And because it carries heavy and disproportionate penalties, including imprisonment of three to fifteen years, and provides no grounds for exemption from either liability and penalty, it allows no opportunity for the accused to prove the truth of what is said.

Another problem stemming from the CCA is legal redundancy. Section 14 (1) on the dissemination of false information causing damage to another party has in practice been used for legal actions for defamation. Section 14 (3) also overlaps with Section 14 (2).regarding national security offences and Section 14 (4) regarding dissemination of pornographic materials is similar to Section 287 of the Criminal Code. In practice, it was found that this Section has been used merely to request court orders to block websites, rather than for prosecutions.

Section 15 provides for liability of service providers. Apart from the lack of a clear definition of the term "service provider" already mentioned, this Section sets a rate of penalties for service providers as the same as that for perpetrators. This is unreasonable and disproportionate. In many instances, service providers simply act as an "intermediary" transmitting online data. According to the Criminal Code, service providers should be held responsible only as "supporters" rather than "principals". As a result, a number of service providers have decided to "self-censor", leading to an infringement on the people's right to freedom of expression. Apart from problems with the CCA, Thailand has no internet content monitoring procedures by which service providers can decide to take down

certain information from their servers without having to wait for a court order (Notice and Takedown). The state has no clear procedure to identify the persons mandated to advise service providers on which data could be actionable. There are no clear notification procedures, no details of the information required to be submitted to the state to establish the existence of an offence and no clear guidelines on a grace period for service providers to delete data after being notified. As a result, enforcement of the law has failed to follow any standard pattern, and has been subject mainly to the discretion of individual officials relying on informal cooperation.

Section 20 deals with suppression of information dissemination and website closure, considered urgent measures by the state to prevent commission of an offence. But the Section contains vague definitions of offensive content. Restriction on access to information should be based on clear definitions with clear conditions and procedures, based on the principle for upholding freedom of information and expression. Blocking websites should be used as a last resort, only when necessary under "exceptional" circumstances because of the extensive impact on the rights of the people. This Section allows the state to operate without having to go through any prior judicial oversight. The findings of the study on website blocking and prosecutions show that in reality, Section 20 has been used as a "primary" tool.

Comparative study of online control laws and state policies in other countries

Germany, Malaysia, the USA and China all pledge to

uphold the rights to freedom of expression and information as prescribed in their constitutions. Exceptions or restrictions on freedoms do exist and vary from country to country. For example, Germany does not protect any content harmful to children and youth and to peace, content that offends human dignity, racism and dissemination of German nationalism (Nazism). USA has only one restriction imposed on content deemed harmful to children and youth. China restricts content regarding national security and government stability. Malaysia does not protect content affecting national security, blasphemy, pornography and obscenity, and content harmful to children and youth. However, none of these countries have computer-related laws on the dissemination of such information. In addition, they have no law that imposes the same tariff of penalties on both the service providers as intermediaries and the principals who disseminate the information. Both China and Malaysia try to monitor internet content by making it a "duty" of ISPs.

Websites are blocked in all countries, though frequency (as far as it has been reported and identified) and the way this authority is used seem to differ. In Germany, quite a few website are blocked through orders derived from clearly defined laws and under the principle of proportionality. Despite this, orders usually meet strong opposition. The state is often taken to Court to fight closure orders. In the US, a few websites have been blocked informally based on the exercise of state power through ISPs and there is a special agency to monitor and issue blocking orders. China and Thailand seem to rely heavily on blocking websites and tend to have vaguely defined legal provisions. Those affected by state orders are often not informed in advance and many cases happen informally. Websites are

rarely blocked in Malaysia, since such orders are not feasible due to other protective laws; the state often uses other ways to control content such as by clamping down on civil rights, or prosecuting online news networks on security-related charges. It should be noted that the underlying perspectives that prompt the Thai authorities to clamp down on websites are quite unique. While other countries, including China, normally use measures discreetly and avoid media publicity, every government in Thailand has proudly presented in press conferences the number of websites blocked.

With regard to intimidation of people or netizens, China and Malaysia frequently arrest netizens under a number of national security laws in force. In Thailand, arrests and attempts to threaten netizens have not been regular, mostly coinciding with political conflict. The study shows the numbers rose significantly during street protests against the government, particularly after the 19 September 2006 coup. In addition, while in other countries, service providers are often spared (since they merely provided a service, but were not involved with disseminating content), in Thailand, the authorities force ISPs to take responsibility for acts committed by others.

In terms of movements and reactions of the people toward the law and state policies, people in Germany and the US have more channels through which they can express themselves than in the East. People there can demonstrate, launch opposition campaigns, organize seminars to educate society, write open letters and appeal cases to higher courts, while movements in China, Malaysia and Thailand are often restricted to calls for social justice and policy. There are few demands for effective law enforcement as in the West.

Recommendations

Legal recommendations. The CCA should be a criminal law specifying offences and penalties for conventional computer related crime or any criminal action directly against the system or data, i.e., unauthorized access, data interference, data theft, etc., in order to fill out the legal loophole and to address legal redundancies. Should the state insist on applying it with any illegal data disseminated online, then the provisions have to be made clearly and unambiguous and it should serve the purpose of existing offences in other relevant laws. In fact, it could be easier if the state simply amend the exist Criminal Code and add new computer related criminal offences in there.

The definition of "service provider" should be spelled out to correctly describe the functionalities and duties and should just refer to service providers of computer system or network only. It should not be expanded to also cover other telecommunication operators who are quit irrelevant to the content and not involved with the computer related crime.

In terms of liability and penalty rate of the service providers concerned with the dissemination of illegal content, the law drafters should classify levels of liability and types of ISPs in light of the content. For example, the ISPs might be held liable for the content, but technical service providers should not be held liable for any content at all. An exception can happen, for example, if it could be proven that the technicians are also involved with recruiting, revising or modifying the data. If the law drafters insist on holding the service providers liable for the offence committed by their users or by their clients, then the law should not impose the same penalties on both the service

providers and the perpetrators. But they should be imposed proportionately and fit the principle of multiple culprits.

As for measures to suppress content or to block websites, Section 20 should be amended to make it clear and not prone to be subjected to individual discretions. It should rest on the principle that if the suppression does not take place soon enough, massive damage could have happened. Or if the impact of such dissemination of information is irreversible, the law should provide for clear and written methods, process and conditions for the exercise of suppression power. And the ISPs should be informed of such procedures. After the website is blocked, other process should commence including prosecution against the person who has disseminate the data that has led to the blockade of website. If in the end, it was found that the content is not illegal, the order has to be rescinded by the court and remedies should be provided for the damage parties. In addition, there should be a body of knowledgeable persons who are representatives from various parties and are able to develop the review process as well as to oppose the order.

Policy recommendation. The state should develop measures to monitor online content while striking the balance with the protection of people's freedom. Instead of website blockade, other measures such as the promotion of self-monitoring among users and ISPs should be encouraged. In addition, an effort should be made to increase knowledge in computer technology among state officials. The state should endeavor to establish a special court to try computer related offences and to develop handbooks, guidelines, or commentaries of concerned laws and regulations. In addition, a code of conduct should be developed by the operators. The policy and measures should be geared

toward creating incentives among the operators, instead of stressing the suppression or punishment such as tax incentives.

Recommendation for people and ISPs. Individuals and NGOs working on the issue should place an importance on the right to information and freedom of expression, stay alert and constantly monitor any attempt by the state to issue a law or regulation or policy which might infringe on the right to information and freedom of expression. This should ensure that the state does not exercise its power beyond the limits and unfairly. In addition, the ISPs might get together or form as a network of entrepreneurs to monitor and prevent the government from imposing disproportionate penalty rates on ISPs which also affect people's rights and freedom. Most importantly, a method should be developed to oppose the unfair law and policy, to contain any arbitrary use of power, or to demand more rights and freedom. From advocating policy options, one can transcend them and keep developing clear advocacies by using law as our leverage including litigation.

บทนำ

ผลกระทบจาก พ.ร.บ. ว่าด้วยการกระทำความผิด
เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐ
กับสิทธิเสรีภาพในการแสดงความคิดเห็น

1. โครงการ

มาตรา 45[1] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 กำหนดให้รัฐต้องคุ้มครองสิทธิและเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นของประชาชนไม่ว่าโดยวิธีการใดๆ และกระทำผ่านสื่อประเภทใดไว้อย่างชัดเจน อย่างไรก็ดี ภายใต้ระบบการปกครองโดยกฎหมาย (นิติรัฐ-ประชาธิปไตย) การใช้สิทธิและเสรีภาพของบุคคลใดบุคคลหนึ่ง โดยเฉพาะอย่างยิ่งสิทธิและเสรีภาพประเภทที่ต้องมีการแสดงออกมาภายนอก จำเป็นต้องอยู่ภายในขอบเขตตามที่กฎหมายกำหนดเสมอ เพื่อป้องกันไม่ให้การใช้สิทธิและเสรีภาพเช่นว่านั้นส่งผลกระทบหรือล่วงละเมิดสิทธิและเสรีภาพของบุคคลอื่นได้

ในกรณีของเสรีภาพในการแสดงความคิดเห็นนี้ รัฐธรรมนูญมาตรา 45 วรรคสอง จึงบัญญัติ “ข้อยกเว้น” ของการคุ้มครอง และให้อำนาจแก่รัฐในอันที่จะกำหนด “มาตรการทางกฎหมาย” เพื่อจำกัดหรือควบคุมการใช้สิทธิและเสรีภาพดังกล่าวไว้ ทั้งนี้ ด้วยเหตุผลสำคัญ 4 ประการ คือ

เพื่อความมั่นคงแห่งรัฐ เพื่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน เพื่อคุ้มครองสิทธิส่วนบุคคลหรือชื่อเสียงของบุคคลอื่น และเพื่อป้องกันหรือระงับความเสื่อมทรามทางจิตใจหรือสุขภาพของประชาชน

อนึ่ง แม้ในฐานะของ “ผู้ใช้อำนาจปกครอง” รัฐจะสามารถตรากฎหมาย หรือใช้มาตรการอื่นใดเพื่อจัดการ ดูแล รวมทั้งกลั่นกรองหรือควบคุมสิทธิและเสรีภาพของประชาชนได้ แต่การตรากฎหมายหรือการใช้มาตรการเหล่านั้นก็จำต้องมีขอบเขตเช่นกัน เพื่อเป็นหลักประกันแก่ประชาชนว่าจะไม่ถูกฝ่ายผู้ปกครองรัฐใช้อำนาจตามอำเภอใจ หรือล่วงละเมิดเสรีภาพจนเกินสมควร รัฐธรรมนูญมาตรา 29 จึงกำหนดกรอบการตรากฎหมายเพื่อจำกัดสิทธิและเสรีภาพของประชาชนไว้ให้แก่รัฐเช่นกัน ว่า ต้องเป็นไปเพียงเท่าที่จำเป็น และกฎหมายนั้นจะกระทบกับสาระสำคัญแห่งสิทธิและเสรีภาพนั้นมิได้ รวมทั้งต้องใช้บังคับอย่างเสมอหน้าเท่าเทียมไม่เลือกปฏิบัติ[2]

อย่างไรก็ตาม แม้รัฐธรรมนูญจะกำหนดให้ความคุ้มครองประชาชนและวางกรอบในการบัญญัติกฎหมายไว้เช่นนั้นแล้ว แต่ในช่วงเวลาหลายปีที่ผ่านมา การณ์กลับปรากฏว่า รัฐไทยโดยหน่วยงานผู้รับผิดชอบกลับตรากฎหมายและใช้มาตรการในเชิงควบคุม จำกัดสิทธิ กระทั่งแทรกแซงเสรีภาพการเสนอข้อมูลข่าวสารของสื่อ รวมทั้งการแสดงความคิดเห็นของประชาชนไทยอย่างมาก จนมีคำถามเกิดขึ้นว่าเป็นการใช้อำนาจเกินเลยไปหรือไม่ อาทิเช่น การประกาศใช้ พ.ร.ก.การบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 ซึ่งมุ่งเน้นควบคุมการเสนอข่าวเกี่ยวกับสถานการณ์การเมืองของสื่อประเภทต่าง ๆ ไม่ว่าจะเป็นโทรทัศน์ วิทยุชุมชน และเว็บไซต์ หรือการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ต่อไปจะใช้คำว่า “พ.ร.บ.คอมพิวเตอร์ฯ 2550”) ที่ใช้ถ้อยคำคลุมเครือไม่ชัดเจน ทั้งยังให้อำนาจรัฐระงับการเผยแพร่ข้อมูล หรือปิดกั้นเว็บไซต์ได้โดยปรากฏข้อเท็จจริงด้วยว่า ในการใช้อำนาจดังกล่าวหลายกรณีรัฐไม่ได้ให้เหตุผลที่ชัดเจนเพียงพอต่อเจ้าของเว็บไซต์ที่ถูกปิดกั้น หรือการเซ็นเซอร์เว็บไซต์ในหลาย ๆ ครั้งก็มิได้เป็นไปตามกระบวนการที่กฎหมายกำหนดไว้

(ขอคำสั่งศาลตามมาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550[3]) แต่รัฐกลับใช้มาตรการ “ขอความร่วมมือ” หรือใช้อำนาจอย่างไม่เป็นทางการขอให้ผู้ให้บริการอินเทอร์เน็ตระงับการเผยแพร่เนื้อหา หรือปิดกั้นช่องทางการเข้าถึงเว็บไซต์บางแห่งที่รัฐเห็นว่า “ไม่เหมาะสม” แต่อาจไม่เข้าข่ายผิดกฎหมาย

มีสถิติตัวเลข (ดังจะได้แสดงในรายงานวิจัยฉบับนี้ต่อไป) อันน่ากังวลอย่างยิ่งว่า ยิ่งสถานการณ์ความขัดแย้งในสังคมไทยรุนแรงขึ้นเท่าไร สถานการณ์การควบคุมและแทรกแซงสื่อ โดยเฉพาะอย่างยิ่งสื่อออนไลน์หรืออินเทอร์เน็ต (ซึ่งอยู่ในขอบเขตงานวิจัยฉบับนี้) ก็ยิ่งรุนแรงมากขึ้นเท่านั้น ทั้งนี้ โดยอาศัยอำนาจดังกล่าวตาม พ.ร.ก.การบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548[4] ทั้งๆ ที่ในช่วงที่เกิดวิกฤตการณ์การเมืองหรือมีสถานการณ์ความขัดแย้งใดๆ ขึ้น รัฐยิ่งควรเป็นหลักที่มั่นคงในการให้ความคุ้มครองสิทธิและเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นของประชาชน เพราะเป็นช่วงเวลาที่จำเป็นอย่างยิ่งที่ประชาชนควรได้รับข้อมูลข่าวสารอย่างครบถ้วนรอบด้าน เพื่อใช้ประกอบการตัดสินใจหรือแสดงเจตนารมณ์ และมีส่วนร่วมทางการเมือง

นอกจากนี้ ยังมีเหตุการณ์ที่ทำให้เชื่อได้อีกว่า รัฐบังคับใช้กฎหมายและมาตรการต่างๆ อย่างเลือกปฏิบัติและไม่เสมอภาคเท่าเทียมกัน เพราะในขณะที่มีสื่อหลายสำนักเสนอเนื้อหาและภาพข่าวที่มีระดับความรุนแรงแบบเดียวกัน แต่รัฐกลับเลือกควบคุมเฉพาะสื่อบางสำนัก หรือบางกลุ่มที่นำเสนอข้อมูลด้านที่รัฐเห็นว่าไม่เป็นมิตร หรืออยู่คนละฝ่ายการเมืองกับตนเท่านั้น เช่น การปิดวิทยุชุมชนจำนวนมากโดยรัฐบาลประชาธิปัตย์ในปี 2553[5] หรือโดยรัฐบาลเพื่อไทยในปี 2554[6] ซึ่งกรณีต่างๆ เหล่านี้นอกจากจะนำมาซึ่งคำถามว่ารัฐกระทำการขัดหรือแย้งต่อบทบัญญัติของรัฐธรรมนูญหรือไม่แล้ว ยังสะท้อนให้เห็นทัศนคติของรัฐไทยที่มีต่อสิทธิและเสรีภาพในเรื่องนี้ของประชาชนอีกด้วย แม้ที่ผ่านมาจะมีความพยายามจากหลายฝ่ายเสนอข้อร้องเรียนต่อสาธารณะ รวมทั้งนำคดีขึ้นสู่ศาลเพื่อขอให้ตรวจสอบความชอบด้วยกฎหมายของการใช้อำนาจรัฐ แต่ก็ยังไม่ได้รับการตอบสนองเท่าที่ควร อีกทั้งยังมีบางกรณีที่ศาลปฏิเสธไม่ตรวจสอบการใช้อำนาจของรัฐ

ในลักษณะดังกล่าวด้วย เช่น ศาลยุติธรรมชั้นต้นยกฟ้องเว็บไซต์ประชาไท ซึ่งเป็นโจทก์ฟ้องหน่วยงาน ศอฉ. ในสมัยรัฐบาลนายอภิสิทธิ์ เวชชาชีวะ ว่าใช้อำนาจตาม พ.ร.ก.ฉุกเฉินฯ สั่งปิดกั้นเว็บไซต์ประชาไท โดยไม่ชอบ[7] เป็นต้น

อนึ่ง นอกจากสื่อและเว็บไซต์จะโดนควบคุมอย่างเข้มข้นในช่วงที่ผ่านมาแล้ว ยังมีข้อที่ต้องตั้งเป็นข้อสังเกตด้วยว่า คดีความที่เกิดขึ้นโดยอาศัยข้อหาตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ส่วนใหญ่เป็นคดีที่เกี่ยวกับการเผยแพร่เนื้อหาในอินเทอร์เน็ต หาใช่อาชญากรรมโดยแท้ไม่ อีกทั้งผู้ต้องหาจำนวนไม่น้อยคือผู้ให้บริการที่ไม่ได้เป็นผู้ลงมือโพสต์ข้อมูลด้วยตัวเอง สถานการณ์เช่นนี้จึงย่อมไม่อาจปฏิเสธได้เลยว่า พ.ร.บ.คอมพิวเตอร์ฯ 2550 กลายเป็นตัวแปร หรือเข้ามามีบทบาทอย่างสำคัญกับการจำกัดเสรีภาพในสื่อออนไลน์

ด้วยข้อเท็จจริงต่างๆ ดังกล่าวมา จึงน่าจะเป็นประโยชน์อย่างยิ่งหากมีการรวบรวมสถิติและตัวอย่างคดีความ เก็บสถิติจำนวนสื่อออนไลน์ที่ถูกปิดกั้น ประมวลลักษณะการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ของรัฐ รวมทั้งสำรวจแนวนโยบายและทัศนคติของผู้มีอำนาจปกครองและเจ้าหน้าที่รัฐที่มีต่อสิทธิและเสรีภาพของประชาชนในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็น เพื่อนำมาศึกษาวิเคราะห์ให้เห็นถึงเหตุผลที่แท้จริง และสถานการณ์การควบคุมสื่ออินเทอร์เน็ตที่เกิดขึ้นอย่างมากในประเทศไทย อย่างไรก็ตาม การศึกษาวิจัยนี้คงมิอาจครบถ้วนสมบูรณ์ได้เลยหากไม่ได้มีการศึกษาสถานการณ์ในเรื่องเดียวกันที่เกิดขึ้นในต่างประเทศ และนำมาวิเคราะห์เปรียบเทียบ เพื่อนำไปสู่ข้อเสนอแนะสุดท้ายสำหรับการสร้างสมดุลระหว่างการป้องกันและปราบปรามการกระทำความผิดในสื่อออนไลน์กับการคุ้มครองสิทธิและเสรีภาพของประชาชนต่อไป ทั้งนี้ บนพื้นฐานที่คณะผู้วิจัยเห็นว่า การให้ความสำคัญกับเสรีภาพในการแสดงความคิดเห็นของประชาชนนั้นมีความสำคัญ และจำเป็นอย่างยิ่งในการสร้างประชาธิปไตยที่แท้จริงให้เกิดขึ้นได้ในสังคมไทย

2. ลักษณะกิจกรรม

งานวิจัยเชิงปริมาณและคุณภาพ เกี่ยวกับ “ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550”

3. กรอบเวลาที่ศึกษา

เดือนกรกฎาคม 2550 – ธันวาคม 2554

4. เป้าหมายของโครงการ

1) รวบรวมสถิติทางคดีตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 และการดำเนินนโยบายต่าง ๆ ของรัฐที่เกี่ยวกับเสรีภาพของประชาชนในสื่อออนไลน์ (อินเทอร์เน็ต)

2) รวบรวมข้อมูลและความคิดเห็น รวมทั้งแนวทางการแก้ปัญหาที่เกิดขึ้นจากการปิดกั้น/ควบคุมเนื้อหาในสื่อออนไลน์ ทั้งจากผู้วางนโยบายและมาตรการควบคุมสื่อ หน่วยงานและเจ้าหน้าที่ผู้บังคับใช้กฎหมาย รวมทั้งผู้ได้รับผลกระทบจากการบังคับใช้มาตรการเหล่านั้น

3) ศึกษาปัญหาที่เกิดขึ้นจากตัวบทกฎหมาย และการบังคับใช้กฎหมายที่เกี่ยวกับเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชนในสื่อออนไลน์ โดยเฉพาะอย่างยิ่งปัญหาที่เกิดจาก พ.ร.บ.คอมพิวเตอร์ฯ 2550

4) สำรวจกฎหมาย และแนวนโยบายที่เกี่ยวกับเสรีภาพของประชาชนในสื่อออนไลน์ของต่างประเทศ เพื่อศึกษาเปรียบเทียบกับกรณีที่เกิดขึ้นในประเทศไทย

5) วิเคราะห์และประเมินผลดีผลเสีย (โดยเปรียบเทียบกับต่างประเทศด้วย) ระหว่าง การใช้กฎหมายและนโยบายที่เน้นการควบคุม/กลั่นกรองเนื้อหาในสื่อออนไลน์ กับ การใช้กฎหมายและนโยบายที่ให้ความ

สำคัญกับสิทธิและเสรีภาพของประชาชน โดยจัดทำเป็นบทสรุป และข้อเสนอแนะแนวทางที่เหมาะสม เพื่อสร้างสมดุลย์ระหว่างการป้องกันและปราบปรามการกระทำความผิดกับการคุ้มครองเสรีภาพของประชาชนต่อไป

นิยามศัพท์ที่เกี่ยวข้อง

admin แอดมิน

มาจากคำว่า administrator โดยทั่วไปหมายถึงผู้ดูแลเว็บไซต์ ทั้งนี้อาจหมายถึงผู้ที่ดูแลด้านเทคนิค ด้านเนื้อหา หรือภาพรวมหน้าตาเว็บอย่างใดอย่างหนึ่งหรือทั้งหมดก็ได้ ทั้งนี้ภาระความรับผิดชอบขึ้นอยู่กับแต่ละเว็บไซต์กำหนด (ความหมายคล้าย webmaster)

BitTorrent บิททอร์เรนท์

ดู Torrent

blog บล็อก

ย่อมาจาก web log แปลตรงตัวคือบันทึกบนเว็บ ปัจจุบันใช้เรียกเว็บไซต์ที่มีการเขียนเนื้อหาเพิ่มเติมเรื่อยๆ

comment คอมเมนต์

(น.) ความเห็น เนื้อหาในอินเทอร์เน็ตที่เกิดจากการสนทนาต่อเนื่องจากข่าวหรือกระทู้

(ก.) เขียนข้อความแสดงความเห็น

domain name โดเมนเนม

ชื่อของเว็บไซต์ เช่น naksit.org มีไว้เพื่อใช้เรียกที่อยู่เว็บไซต์ต่างๆ แทนการใช้ชุดตัวเลขไอพีแอดเดรส

file ไฟล์

แฟ้มบันทึกข้อมูลในระบบคอมพิวเตอร์ โดยส่วนใหญ่จะจัดเก็บไว้ในฮาร์ดดิสก์ หรือบนอินเทอร์เน็ต

FTP เอฟทีพี

วิธีการส่งข้อมูลแบบหนึ่งในอินเทอร์เน็ต ออกแบบมาเพื่อการส่งไฟล์แบบไม่มีการเข้ารหัสข้อมูลระหว่างส่ง ส่วนแบบที่มีการเข้ารหัสนั้นชื่อว่า SFTP

Google กูเกิล

ชื่อทางการค้า หมายถึง 1) บริษัทผู้ให้บริการอินเทอร์เน็ต 2) ใช้เรียกแทน เพื่อหมายถึง เสิร์ชเอนจิน หรือเครื่องมือสำหรับค้นหาสิ่งต่างๆ บนอินเทอร์เน็ต

hacker แฮกเกอร์

บุคคลผู้มีความเชี่ยวชาญในเรื่องหนึ่งๆ และมีกลเม็ดสามารถแก้ไขปรับปรุงสิ่งที่ตนมีความเชี่ยวชาญ แต่มักถูกหมายความถึง computer hacker หรือผู้เชี่ยวชาญด้านคอมพิวเตอร์โดยรวม เช่น ผู้พัฒนาซอฟต์แวร์ ผู้ตรวจสอบความปลอดภัยระบบ (ค้นหาช่องโหว่แล้วแก้ไข) ไม่จำเป็นต้องเป็นผู้ประสงค์ร้าย อย่างไรก็ตาม ในภาษาพูด ในสื่อกระแสหลัก คำว่า hacker มักถูกใช้สื่อความถึงผู้ค้นหาและใช้ช่องโหว่ของระบบรักษาความปลอดภัยเพื่อทำลายหรือขโมยข้อมูล ทั้งที่คำที่ถูกต้องตรงตามความหมายดังกล่าวจริงๆ แล้วคือ คำว่า cracker

ดังนั้น อาจพอสรุปได้ว่า hacker มีสองประเภท สีขาว (white hat hacker) คือพวกประสงค์ดี และสีดำ (black hat hacker) คือ cracker

hosting โฮสติ้ง

ผู้ให้บริการพื้นที่สำหรับเว็บไซต์ เป็นผู้ครอบครองคอมพิวเตอร์

(อาจจะจำนวนมาก) หรือคอมพิวเตอร์ขนาดใหญ่ซึ่งมีพื้นที่มากๆ ที่เชื่อมต่อกับอินเทอร์เน็ต แล้วแบ่งพื้นที่ให้คนอื่นเช่าสำหรับเก็บรักษาเว็บไซต์

Internet อินเทอร์เน็ต

การเชื่อมต่อระหว่างเครือข่ายคอมพิวเตอร์ไร้พรมแดน ทำให้เข้าถึงข้อมูลข่าวสารและการบริการ ผ่านการเข้าถึงลิงก์ข้อมูล ระบบอีเมล และอื่นๆ

IP address ไอพี แอดเดรส

หมายเลขประจำเครื่องคอมพิวเตอร์ชุดหนึ่ง เมื่อต่ออินเทอร์เน็ต ผู้เชื่อมต่อจะได้รับหมายเลขที่อยู่ ณ ช่วงเวลานั้นๆ จากผู้ให้บริการอินเทอร์เน็ต หมายเลขนี้เปลี่ยนไปทุกครั้งเมื่อเชื่อมต่ออินเทอร์เน็ตใหม่ เลขไอพียังสามารถระบุได้ว่าการเชื่อมต่อนั้นมาจากจังหวัดใด ประเทศใด ปัจจุบันเลขหมายไอพีเป็นเบาะแสสำคัญที่นิยมใช้เพื่อหาตัวผู้กระทำความผิด แต่มีข้อบกพร่องเพราะผู้ใช้สัญญาณอินเทอร์เน็ตไม่จำเป็นต้องเป็นคนเดียวกับผู้จดทะเบียนขอใช้บริการอินเทอร์เน็ต นอกจากนี้ ไอพียังสามารถปลอมแปลงได้

ISP ไอเอสพี

ย่อมาจากคำว่า Internet Service Provider หมายถึง ผู้ให้บริการอินเทอร์เน็ต เช่น บริษัททรู บริษัท 3BB ฯลฯ

link ลิงก์

เรียกอีกอย่างว่า Hyperlink หมายถึง การอ้างอิงข้อมูลที่ช่วยให้ผู้ใช้สามารถกดเพื่อเข้าถึงข้อมูลในโลกออนไลน์ได้อัตโนมัติ

log file ล็อกไฟล์

ข้อความที่ระบบปฏิบัติการคอมพิวเตอร์บันทึกเอาไว้เพื่อทราบว่า

ผู้ใช้ทำกิจกรรมอะไร ในช่วงเวลาใด บนคอมพิวเตอร์เครื่องนั้นบ้าง

log in ล็อกอิน

การเข้าสู่ระบบ โดยกรอกชื่อบัญชี (username) และรหัสผ่าน (password)

meta data เมตาดาตา

ข้อมูลที่อธิบายข้อมูล เช่น กล้องดิจิตอลรุ่นใหม่เมื่อถ่ายภาพแล้วมักมีข้อมูลอธิบายไว้ด้วยว่า ภาพดังกล่าวถ่ายจากกล้องรุ่นใด ถ่ายเมื่อใด

modem โมเด็ม

อุปกรณ์ที่ทำให้สามารถส่งข้อมูลผ่านสายโทรศัพท์ได้

moderator โมเดอเรเตอร์

ผู้อำนวยการการสนทนาในเว็บบอร์ด ห้องแชต หรือในเกมออนไลน์ บางครั้งสามารถปิดกั้นผู้ใช้หรือลบกระทู้ได้ moderator อาจจะเป็นทีมงานของเว็บไซต์หรือเป็นอาสาสมัครที่เลือกขึ้นมาจากผู้ใช้ก็ได้ แล้วแต่นโยบายของเว็บ

pharming ฟาร์มมิง

การทำเว็บไซต์ปลอม หรือเชื่อมต่อให้คนทั่วไปเข้าถึงเว็บไซต์ปลอม เพื่อให้คนหลงเชื่อ แล้วเผลอให้ข้อมูลส่วนบุคคล เช่น ทำเว็บไซต์หน้าตาเหมือนเว็บไซต์ธนาคารจริง จนคนหลงเชื่อและกรอกรหัส

phising ฟิชชิง

การส่งข้อความที่น่าเชื่อถือ เพื่อให้หลงเชื่อ และยอมให้ข้อมูลส่วนบุคคล

provider โพรไวเดอร์

ผู้ให้บริการ

proxy พร็อกซี

ระบบบริการการเข้าถึงอินเทอร์เน็ตที่ให้ผู้ใช้เข้าสู่อินเทอร์เน็ตด้วยทางเดินอ้อม มักถูกนำมาใช้เพื่อเข้าเว็บไซต์ที่ถูกปิดกั้น เหมือนเวลาถนนเส้นหนึ่งถูกปิด ผู้สัญจรก็เลือกเดินเส้นทางอื่นเพื่อไปถึงปลายทางแทน

search engine เสิร์ชเอนจิน

เครื่องมือค้นหาเว็บไซต์ มีหลายยี่ห้อ เช่น Google, Yahoo, Bing

server เซิร์ฟเวอร์

คอมพิวเตอร์ที่มีโปรแกรมบางอย่างที่ยอมให้คอมพิวเตอร์เครื่องอื่น (อาจจะเครื่องใดก็ได้บนอินเทอร์เน็ต หรือแค่ในองค์กร) เรียกใช้ เช่น คอมพิวเตอร์ที่เก็บเว็บไซต์ (และยอมให้คอมพิวเตอร์เครื่องอื่นเปิดเว็บไซต์นั้นดูได้) ก็เรียกว่า web server หรือคอมพิวเตอร์ที่เชื่อมกับ printer แล้วยอมให้เครื่องอื่นใช้ printer นั้นด้วยก็เรียกว่า print server

Spam สแปม

จดหมายที่ถูกส่งมาโดยผู้รับไม่พึงประสงค์

Torrent ทอร์เรนท์

โปรแกรมสำหรับแบ่งปันไฟล์ที่ผู้ใช้สามารถค้นหาและดาวน์โหลดข้อมูลผ่านอินเทอร์เน็ตจากคอมพิวเตอร์ของผู้อื่นที่ร่วมใช้โปรแกรมเดียวกันได้ ผลิตภัณฑ์ที่เป็นที่รู้จัก เช่น BitTorrent

URL ยูอาร์แอล

ชื่อที่อ้างอิงถึงตำแหน่งที่ใช้เก็บแฟ้มข้อมูลบนระบบอินเทอร์เน็ต

โดยทั่วไป จะประกอบไปด้วยสองส่วน คือ ชื่อเครื่องคอมพิวเตอร์ที่ใช้เก็บข้อมูลนั้น และตำแหน่งของแฟ้มข้อมูลในเครื่องคอมพิวเตอร์นั้น

virus ไวรัส

โปรแกรมคอมพิวเตอร์ที่สามารถขยายพันธุ์ได้ด้วยตัวเอง และสามารถแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นได้ ผ่านการติดต่อทางอินเทอร์เน็ตหรือ Thumbdrive

webmaster เว็บมาสเตอร์

ผู้ดูแลเว็บไซต์ ซึ่งแต่เดิม มีบุคคลคนเดียวที่ทำทุกอย่างในเว็บ ทั้งสร้างเว็บ ออกแบบ และดูแลเนื้อหา เรียกรวมๆ ว่า “เว็บมาสเตอร์” แต่ปัจจุบันความหมายของคำนี้เปลี่ยนไปตามแต่ละเว็บไซต์ โดยทั่วไปมักหมายถึงคนดูแลเว็บที่รู้รายละเอียดทางเทคนิค (คล้ายคำว่า admin)

website เว็บไซต์

สื่อซึ่งบรรจุเนื้อหา โดยอาจเป็นข้อความ ภาพ วิดีโอ หรือเสียง สามารถเข้าถึงได้ผ่านทางออนไลน์ โดยเชื่อมต่อด้วยยูอาร์แอลของเว็บไซต์นั้นๆ ในหนึ่งเว็บไซต์ สามารถมีได้หลายหน้าเว็บ

web page เว็บเพจ

หน้าเว็บ

YouTube ยูทูบ

(เครื่องหมายการค้า) เว็บไซต์วิดีโอยอดนิยม เปิดให้คนทั่วไปเลือกชมและแบ่งปันคลิปวิดีโอของตนเอง

บทที่

ผลการศึกษาภาคที่ 1

ศึกษาสถิติที่เกี่ยวกับการบังคับใช้
พ.ร.บ.คอมพิวเตอร์ฯ 2550 และสำรวจความคิดเห็น
ที่มีต่อการบังคับใช้กฎหมายดังกล่าวจากมุมมองเจ้าหน้าที่รัฐ
และผู้ให้บริการหรือดูแลสื่อออนไลน์

การวิจัยเรื่อง **"ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น"** ภายใต้สังคมข้อมูลข่าวสารแบบใหม่ (สื่อออนไลน์) ในส่วนที่หนึ่งนี้ มุ่งศึกษาผลการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ต่อไปจะเรียกว่า "พ.ร.บ.คอมพิวเตอร์ฯ 2550") นับตั้งแต่เดือนกรกฎาคม ปี 2550 ซึ่ง พ.ร.บ. คอมพิวเตอร์ฯ 2550 มีผลบังคับใช้ จนถึงเดือนธันวาคม ปี 2554 รวมระยะเวลาราว 3 ปี 6 เดือน โดยแบ่งลักษณะการศึกษาในภาคนี้ออกเป็นสองส่วน คือ

• ศึกษาผลกระทบเชิงปริมาณ: รวบรวมสถิติการระงับการเผยแพร่เนื้อหา หรือปิดกั้นช่องทางการเข้าถึงเว็บไซต์ และสถิติการดำเนินคดีตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550

• ศึกษาผลกระทบเชิงคุณภาพ: การสัมภาษณ์ และจัดสัมมนากลุ่มย่อย เพื่อเก็บข้อมูลจากบุคคลต่างๆ ที่เกี่ยวข้องกับการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

1. การศึกษาผลกระทบเชิงปริมาณ

ในส่วนของการศึกษาเชิงปริมาณ รายงานฉบับนี้มุ่งวิเคราะห์ผลพวงจากการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ตลอดระยะเวลา 4 ปี 6 เดือน โดยเลือกศึกษาผลกระทบที่เกิดจากการบังคับใช้กฎหมายในสองลักษณะ คือ การระงับการเผยแพร่เนื้อหา หรือปิดกั้นช่องทางการเข้าถึงเว็บไซต์ และการดำเนินคดีกับประชาชนด้วยข้อหาต่าง ๆ ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550

วิธีศึกษา

รวบรวมสถิติการปิดกั้นช่องทางการเข้าถึงเว็บไซต์[1] โดยอาศัยแหล่งข้อมูลหลักจากฐานข้อมูลศาลอาญา[2] ประกอบกับการขอข้อมูลเพิ่มเติมจากผู้เกี่ยวข้อง โดยเฉพาะอย่างยิ่งจากบริษัทผู้ให้บริการอินเทอร์เน็ตรายใหญ่หนึ่งราย (ขอสงวนนาม)

รวบรวมสถิติการดำเนินคดี โดยใช้แหล่งข้อมูลจากหน่วยงานต่าง ๆ ของภาครัฐที่มีหน้าที่เกี่ยวข้องโดยตรงกับการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ประกอบด้วย

- กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที)
- กองบังคับการปราบปรามอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.)
- กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี (บก.ปอท.)
- กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม (ดีเอสไอ)
- กองบังคับการปราบปราม สำนักงานตำรวจแห่งชาติ
- ศาลอาญา

ข้อจำกัดงานวิจัย

ตัวเลขสถิติการดำเนินคดีที่ปรากฏในรายงานวิจัยฉบับนี้ เป็นเพียงส่วนที่คณะผู้วิจัยสืบทราบ และสามารถรวบรวมได้เท่านั้น ดังนั้น จึงมิอาจ

สรุปได้ว่า ตัวเลขดังกล่าวคือจำนวนคดีความทั้งหมดที่เกิดขึ้นในประเทศไทย ยังคงมีคดีอีกจำนวนหนึ่งที่ยังอยู่ในระหว่างการสืบสวนสอบสวนของเจ้าพนักงานตามสถานีตำรวจทั่วประเทศ ซึ่งมีข้อจำกัดในการที่หน่วยงานเหล่านั้นจะเปิดเผยหรือให้ข้อมูลได้ โดยเฉพาะอย่างยิ่งข้อมูลเกี่ยวกับคดีที่ยังพิจารณาไม่เสร็จสิ้น เพราะอาจส่งผลกระทบต่อรูปคดี และสิทธิส่วนบุคคลของผู้ต้องหา นอกจากนี้ คณะผู้วิจัยไม่สามารถเข้าถึงฐานข้อมูลของศาลในต่างจังหวัดได้ครบทุกแห่ง เนื่องจากมีระบบการจัดเก็บข้อมูลที่ไม่อาจเข้าถึงได้ และด้วยข้อจำกัดประการต่าง ๆ ดังกล่าวมา สถิติคดีความที่ปรากฏในรายงานวิจัยฉบับนี้จึงเป็นเพียงส่วนหนึ่งของข้อมูลทั้งหมด ซึ่งคณะผู้วิจัยรวบรวมได้และคัดเลือกมานำเสนอโดยพิจารณาแล้วว่ามีความน่าเชื่อถือทั้งมีแหล่งที่มาที่ชัดเจน สามารถตรวจสอบได้

ผลการศึกษา

1.1 ผลการศึกษาสถิติการระงับการเผยแพร่ หรือปิดกั้นช่องทางการเข้าถึงเว็บไซต์

นับแต่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีผลใช้บังคับ รัฐไทยโดยปฏิบัติการผ่านรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) สามารถใช้มาตรการปิดกั้น หรือระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่ “อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรฯ หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน” ได้ โดยอาศัยอำนาจตามมาตรา 20 ของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งกำหนดว่า

“ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือ

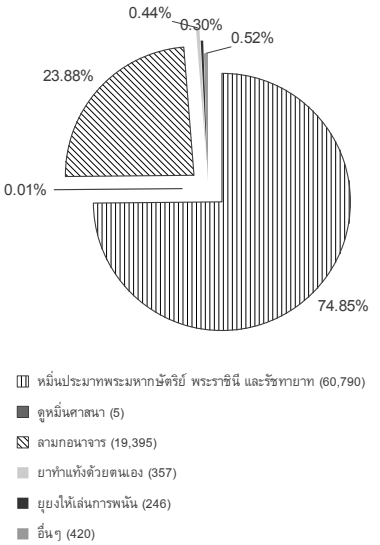
เนื้อหา	2550		2551		2552		2553		2554		Total	
	Court order	URL	Court order	URL	Court order	URL	Court order	URL	Court order	URL	Court order	URL
หมิ่นประมาทพระมหากษัตริย์ พระราชินี และรัชทายาท	0	0	7	1,937	30	16,525	27	39,115	26	3,213	**90**	**60,790**
ลามกอนาจาร	0	0	4	96	27	11,609	15	6,105	6	1,585	**52**	**19,395**
ขายยาทำแท้ง	0	0	1	37	3	320	0	0			**4**	**357**
พนันออนไลน์	0	0	0	0	2	246	0	0			**2**	**246**
ดูหมิ่นหรือลบหลู่ศาสนา	1	2	1	1	1	2	0	0			**3**	**5**
อื่นๆ	0	0	0	0	1	3	3	137	1	280	**5**	**420**
Total	**1**	**2**	**13**	**2,071**	**64**	**28,705**	**45**	**45,357**	**33**	**5,078**	**156**	**81,213**

แผนภาพที่ 1 : จำนวนคำสั่งศาลและจำนวนยูอาร์แอลที่ถูกระงับ จำแนกตามประเภทเนื้อหา

ศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้"

โดยตั้งแต่ประกาศใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 เป็นต้นมา คณะผู้วิจัยพบว่า เคยมีคำสั่งศาลให้ระงับการเข้าถึงเว็บไซต์ต่าง ๆ จำนวนทั้งสิ้น 156 ฉบับ โดยในปี 2550 ศาลมีคำสั่งให้ปิดกั้นการเข้าถึงเว็บไซต์จำนวน 2 ยูอาร์แอล ปี 2551 จำนวน 2,071 ยูอาร์แอล ปี 2552 จำนวน 28,705 ยูอาร์แอล และปี 2553 จำนวน 45,357 ยูอาร์แอล รวมจำนวนหน้าเว็บเพจที่ถูกระงับการเผยแพร่โดยมีคำสั่งศาลทั้งสิ้น 81,213 ยูอาร์แอล

จากตารางแสดงสถิติจะเห็นได้ว่า ยูอาร์แอลที่ถูกระงับการเผยแพร่ ตามคำสั่งศาลเหล่านี้ มีเหตุผลประกอบ (ที่ปรากฏในคำร้องขอให้ระงับการเข้าถึงเว็บไซต์ ที่พนักงานเจ้าหน้าที่โดยความเห็นชอบของกระทรวงไอซีที) ซึ่งสามารถจำแนกเนื้อหาออกได้เป็น อันดับหนึ่ง เนื้อหาและภาพซึ่งดูหมิ่น หมิ่นประมาทพระมหากษัตริย์ พระราชินี และรัชทายาท มีคำสั่งศาลจำนวน 90 ฉบับ เพื่อระงับการเข้าถึง 60,790 ยูอาร์แอล อันดับสอง เนื้อหา



แผนภาพที่ 2 : สัดส่วนประเภทเนื้อหาที่กระทรวงไอซีทียื่นคำร้องต่อศาลให้มีคำสั่งระงับการเข้าถึงเว็บไซต์

และภาพลามกอนาจาร มีคำสั่งศาล 52 ฉบับ ให้ระงับการเข้าถึง 19,395 ยูอาร์แอล อันดับสาม เนื้อหาเกี่ยวกับยาและการทำแท้งด้วยตนเอง โดยคำสั่งศาล 4 ฉบับ ให้ระงับการเข้าถึง 357 ยูอาร์แอล อันดับสี่ เนื้อหายุยงให้เล่นการพนัน มีคำสั่งศาล 2 ฉบับ ให้ระงับการเข้าถึง 246 ยูอาร์แอล อันดับห้า เนื้อหาดูหมิ่นศาสนา มีคำสั่งศาล 3 ฉบับ ให้ระงับการเข้าถึง 5 ยูอาร์แอล และ อันดับหก เป็นเนื้อหาประเภทอื่นๆ อาทิ เว็บไซต์ที่ทำปลอมขึ้นโดยมีเป้าหมายหลอกลวงเอาข้อมูลอิเล็กทรอนิกส์ โดยเฉพาะอย่างยิ่งข้อมูลด้านการเงินการธนาคารจากเหยื่อ (Pharming) เว็บไซต์หลอกลวงผู้บริโภค รวมทั้งเว็บไซต์ที่มีเนื้อหาที่อาจทำให้ประชาชนเข้าใจรัฐบาลผิดเกี่ยวกับเหตุการณ์การควบคุมการชุมนุมจนอาจก่อให้เกิดความปั่นป่วนหรือกระด้างกระเดื่องในหมู่ประชาชน รวมจำนวนคำสั่งศาลทั้งสิ้น 5 ฉบับ ให้ระงับการเข้าถึง 420 ยูอาร์แอล ซึ่งสามารถจำแนกให้เห็นเป็นสัดส่วนประเภทเนื้อหาที่ถูกคำสั่งศาลปิดกั้นได้ ดังแผนภาพที่ 2

อนึ่ง ในฐานข้อมูลศาลอาญา ยังระบุจำนวนยูอาร์แอลที่ถูกระงับการเผยแพร่ โดยจำแนกตามประเภทเนื้อหาให้ละเอียดลงไปตามแต่ละเดือน

Timing	หมิ่นประมาทกษัตริย์ ราชินี รัชทายาท		ลามกอนาจาร		ยาทำแท้ง		พนันออนไลน์		ดูหมิ่นหรือลบหลู่ศาสนา		อื่น ๆ		รวม	
	จำนวนคำสั่งศาล	URL	จำนวนคำสั่งศาล	URL	จำนวนคำสั่งศาล	URL	จำนวนคำสั่งศาล	URL	จำนวนคำสั่งศาล	URL	จำนวนคำสั่งศาล	URL	จำนวนคำสั่งศาล	URL
ต.ค.50									1	2			1	2
ม.ค.51									1	1			1	1
ก.พ.51			1	7									1	7
พ.ค.51			1	1									1	1
มิ.ย.51	1	9	1	2									2	11
ก.ค.51													0	0
ส.ค.51	2	407											2	407
ก.ย.51	1	630	1	86									2	716
ต.ค.51	1	491											1	491
พ.ย.51													0	0
ธ.ค.51	2	400			1	37							3	437
ม.ค.52	3	808											3	808
ก.พ.52	4	1,400	1	305	1	14							6	1,719
มี.ค.52	4	765	3	825					1	2			8	1,592
เม.ย.52	2	887	4	936									6	1,823
พ.ค.52	3	713	4	2,213			1	72					8	2,998
มิ.ย.52	3	770	3	1,948									6	2,718
ก.ค.52	2	469	3	875									5	1,344
ส.ค.52	1	843	1	132							1	3	3	978
ก.ย.52	2	1,985	2	879	1	61	1	174					6	3,099
ต.ค.52	3	3,737	3	1,430									6	5,167
พ.ย.52	2	3,007	1	741									3	3,748
ธ.ค.52	1	1,141	2	1,325	1	245							4	2,711
ม.ค.53	2	4,119											2	4,119
ก.พ.53	4	6,731	2	1,127							1	3	7	7,861
มี.ค.53	6	9,672	1	373									7	10,045
เม.ย.53	2	2,277	1	21									3	2,298
พ.ค.53													0	0
มิ.ย.53	3	4,513											3	4,513
ก.ค.53													0	0
ส.ค.53	5	9,289	3	1,322							1	2	9	10,613
ก.ย.53	3	2,267	2	944									5	3,211
ต.ค.53			2	998									2	998
พ.ย.53	1	2	1	250									2	252
ธ.ค.53	1	245	3	1,070							1	132	5	1,447
ม.ค.54	3	1,618	1	277									4	1,895
ก.พ.54			1	303									1	303
มี.ค.54	4	194	1	307									5	501
เม.ย.54	1	135	1	315									2	450
พ.ค.54	2	351	2	383									4	734
มิ.ย.54	2	2											2	2
ก.ค.54	2	125											2	125
ส.ค.54	1	52											1	52
ก.ย.54	2	14									1	280	3	294
ต.ค.54	1	1											1	1
พ.ย.54	1	300											1	300
ธ.ค.54	7	421											7	421
Total	90	60,790	52	19,395	4	357	2	246	3	5	5	420	156	81,213

แผนภาพที่ 3: เว็บเพจประเภทต่างๆ ที่มีหมายศาลให้ระงับการเข้าถึง จำแนกตามประเภท เดือนและปี

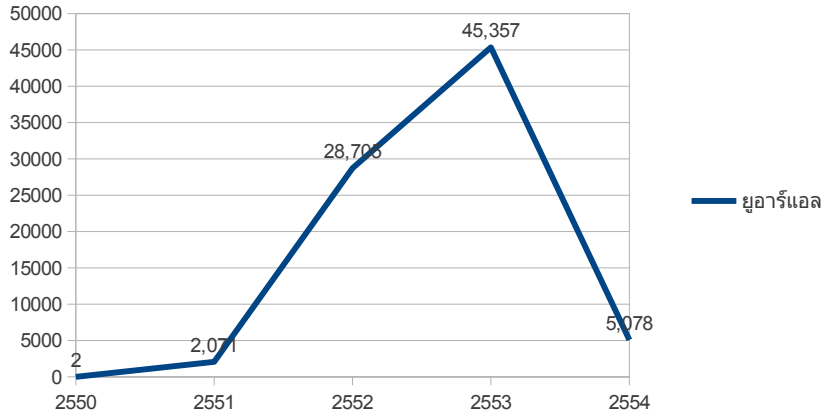
อีกด้วย ซึ่งคณะผู้วิจัยเห็นว่า การจำแนกรายละเอียดของข้อมูลการปิดกั้นเว็บไซต์ในแต่ละเดือนดังกล่าว น่าจะเป็นประโยชน์ต่อการวิเคราะห์ "ปัจจัย" ที่มีผลต่อการบังคับใช้กฎหมายในเรื่องนี้ในแต่ละช่วงเวลา จึงได้นำมาแสดงไว้ด้วย ดังแผนภาพที่ 3

<u>บทวิเคราะห์ และข้อสังเกตต่อสถิติการระงับการเผยแพร่ หรือปิดกั้นช่องทางการเข้าถึงเว็บไซต์</u>

1) อัตราการระงับการเผยแพร่ข้อมูล หรือปิดกั้นช่องทางการเข้าถึงเว็บไซต์ แปรผันตามสถานการณ์ และการแสดงออกทางการเมือง

เป็นที่น่าสังเกตว่า เมื่อพิจารณาจากแผนภาพที่ 1 และ 3 การระงับการเข้าถึงเว็บไซต์ในช่วงปี 2550 และ 2551 ยังเกิดขึ้นไม่มากนักเมื่อเทียบกับระยะเวลาต่อมาซึ่งพบว่าสถิติตัวเลขค่อยๆ สูงขึ้นเรื่อยๆ โดยเฉพาะอย่างยิ่งตั้งแต่ช่วงปี 2552 ถึงปี 2553 จนทำให้ปี 2553 เป็นปีที่มีการปิดกั้นการเข้าถึงเว็บไซต์มากที่สุด และหลังจากนั้นอัตราการปิดกั้นจึงค่อยๆ ลดลงในปี 2554

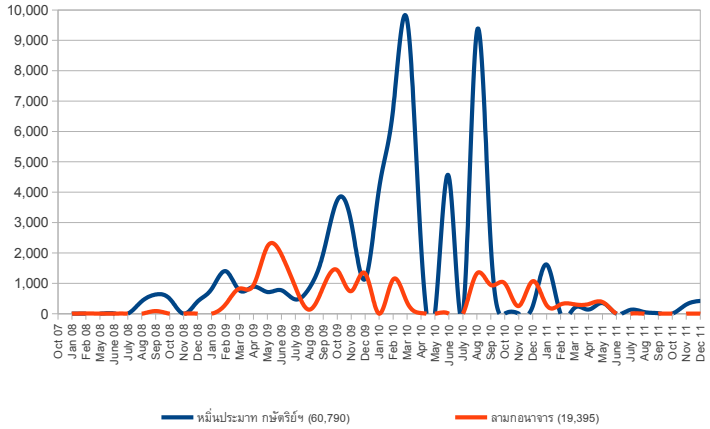
หากพิจารณาจากสถิติ อาจกล่าวได้ว่า สาเหตุหนึ่งที่ช่วงปี 2550 - 2551 ยังมีคำสั่งศาลระงับการเข้าถึงเว็บไซต์ไม่มากนักเมื่อเทียบกับปีอื่นๆ น่าจะเป็นเพราะ พ.ร.บ.คอมพิวเตอร์ฯ 2550 เพิ่งมีผลใช้บังคับได้เพียงระยะเวลาสั้นๆ เท่านั้น กล่าวคือ วันที่ 18 กรกฎาคม 2550 ทั้งหน่วยงานที่เกี่ยวข้องก็ยังไม่มีเจ้าพนักงานผู้รับผิดชอบปฏิบัติการตามกฎหมายในส่วนนี้โดยเฉพาะ ในขณะที่ส่วนราชการที่มีหน้าที่กำกับดูแลการปิดกั้นเว็บไซต์โดยตรงอย่าง "สำนักกำกับดูแลการใช้เทคโนโลยีสารสนเทศ"[3] ของกระทรวงไอซีที ก็เพิ่งถูกตั้งขึ้นเมื่อปี 2552 นอกจากนี้ ในส่วนงานที่เกี่ยวข้องกับศาลเอง ก็อาจยังไม่ได้มีการเตรียมความพร้อมสำหรับการตรวจสอบเว็บไซต์ รวมถึงออกคำสั่งตามมาตรา 20 อนึ่ง แม้กระทรวงไอซีทีจะเคยใช้อำนาจตามประกาศของคณะปฏิรูปการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข (คปค.) ฉบับที่ 5[4] เพื่อปิดกั้นเว็บไซต์



แผนภาพที่ 4: สถิติการปิดกั้นการเข้าถึงเว็บไซต์ จำแนกตามปี

มาแล้วจำนวนไม่น้อย ก่อนหน้าที่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 จะมีผลใช้บังคับ แต่ก็เป็นการปิดกั้นด้วยวิธีการสั่งไปยังผู้ให้บริการอินเทอร์เน็ตโดยตรง ไม่ต้องมีกระบวนการและขั้นตอนตามกฎหมาย รวมทั้งไม่ต้องรวบรวมพยานหลักฐาน เพื่อแสดงเหตุอันสมควร และทำคำร้องไปยังศาล

อย่างไรก็ตาม ภายหลังปี 2551 เป็นต้นมา สถิติการปิดกั้นเว็บไซต์ก็เริ่มสูงขึ้นเรื่อยๆ โดยได้กล่าวไปแล้วว่า เนื้อหาของเว็บไซต์ที่ถูกปิดกั้นในช่วงปี 2550-2554 สองอันดับแรก คือ หนึ่ง เนื้อหาและภาพดูหมิ่น หมิ่นประมาทพระมหากษัตริย์ พระราชินี และรัชทายาท ซึ่งมีจำนวนรวม 60,790 ยูอาร์แอล และสอง เนื้อหาและภาพลามกอนาจาร ซึ่งมีจำนวนรวม 19,395 ยูอาร์แอล (ดูแผนภาพที่ 5) ซึ่งหากพิจารณาจำนวนการปิดกั้นเว็บไซต์ด้วยเหตุผลว่ามีเนื้อหาหมิ่นประมาทพระมหากษัตริย์ พระราชินี และรัชทายาท ประกอบกับบริบททางสังคมและสถานการณ์ทางการเมือง (ดูแผนภาพที่ 6) แล้ว มีข้อที่ควรสังเกตว่า ช่วงที่สถิติการปิดกั้นเว็บไซต์หมิ่นฯ เกิดขึ้นสูง



แผนภาพที่ 5: สถิติการปิดกั้นการเข้าถึงเว็บไซต์ จำแนกตามเหตุผลที่เกี่ยวกับเนื้อหาดูหมิ่นหรือหมิ่นประมาทกษัตริย์ฯ และเรื่องลามกอนาจาร

มาก คือ สมัยที่ ร.ต.หญิง ระนองรักษ์ สุวรรณฉวี และนายจุติ ไกรฤกษ์ เป็นรัฐมนตรีว่าการกระทรวงไอซีที ภายใต้รัฐบาลของนายอภิสิทธิ์ เวชชาชีวะ

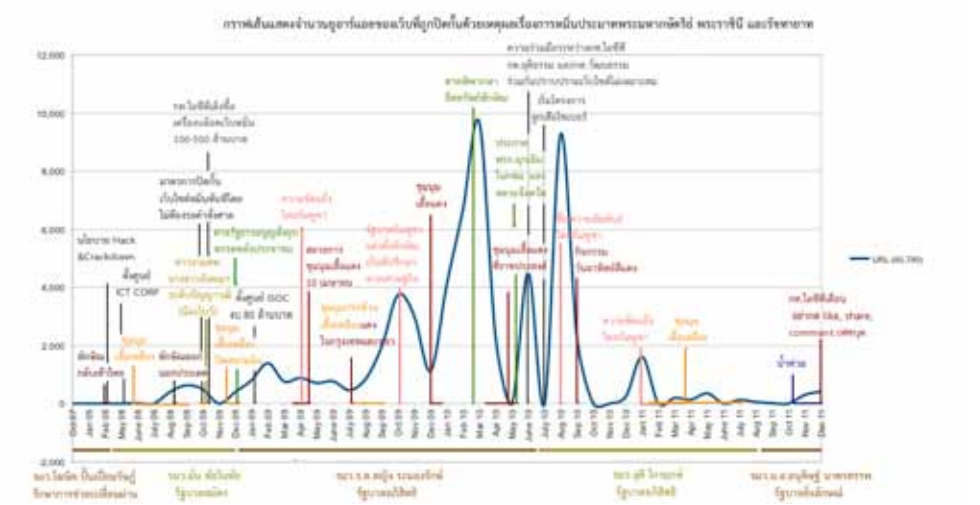
ทั้งนี้ เมื่อพิจารณาย่อยลงไป จะพบว่าช่วงเดือนที่มีการปิดเว็บไซต์หมิ่นประมาทกษัตริย์ฯ สูงสุดสามอันดับแรก คือ เดือนมีนาคม 2553 จำนวน 9,672 ยูอาร์แอล เดือนสิงหาคม 2553 จำนวน 9,289 ยูอาร์แอล และเดือนกุมภาพันธ์ 2553 ปิดกั้นทั้งสิ้น 6,731 ยูอาร์แอล ซึ่งทั้งสามเดือนดังกล่าวล้วนเป็นช่วงที่ความขัดแย้งระหว่างประชาชนกับรัฐบาล และระหว่างประชาชนด้วยกันเองที่สังกัดกลุ่มต่างๆ ปรากฏขึ้นอย่างเด่นชัด กล่าวคือ เดือนกุมภาพันธ์ 2553 เป็นช่วงที่มีการเคลื่อนไหวและกลุ่มคนเสื้อแดงประกาศว่าจะมีการชุมนุมใหญ่ และมีนาคม 2553 เป็นช่วงการชุมนุมใหญ่ต่อเนื่องของ นปช.และคนเสื้อแดงที่บริเวณสะพานผ่านฟ้า ก่อนจะขยายไปชุมนุมที่สี่แยกราชประสงค์ ส่วนเดือนสิงหาคม 2553 เป็นเดือนที่กลุ่มคนเสื้อแดงกลับมาเคลื่อนไหวกันอย่างคึกคักภายหลังจากเหตุการณ์การ

สลายการชุมนุมในเดือนพฤษภาคม และมีการใช้สื่อออนไลน์ชักชวนให้คนเสื้อแดงด้วยกันกลับมารวมตัวเพื่อทำกิจกรรมอีกครั้งหนึ่งในนาม “กิจกรรมวันอาทิตย์สีแดง”[5] ในวันที่ 19 กันยายน 2553 ซึ่งเป็นวันครบสี่ปีของการรัฐประหาร 19 กันยายน 2549

แม้ไม่มีข้อมูลยืนยันเป็นที่ประจักษ์ว่าเว็บเพจต่างๆ ที่ถูกปิดไปมีเนื้อหาอย่างไรบ้าง หรือมีเนื้อหาเข้าข่ายดูหมิ่น หมิ่นประมาทกษัตริย์ฯ จริงหรือไม่ แต่ข้อเท็จจริงก็ปรากฏว่า การปิดกั้นเว็บไซต์จำนวนมากภายใต้รัฐบาลอภิสิทธิ์ด้วยข้อหาหมิ่นประมาทกษัตริย์ฯ สอดคล้องกับกรณีที่ผู้ชุมนุมเรียกร้องทางการเมืองจำนวนมากถูกกล่าวหาจากรัฐบาล (ผ่านทาง ศอฉ.) ว่าเป็นกลุ่ม “ล้มเจ้า” ด้วยเหตุนี้เอง จึงอาจเกิดคำถามได้ว่า สถิติการปิดกั้นเว็บไซต์จำนวนมากที่อ้างว่ามีการดูหมิ่น หรือหมิ่นประมาทกษัตริย์ฯ นั้น แท้ที่จริงแล้วเป็นเพราะมีการดูหมิ่น หรือหมิ่นประมาทกษัตริย์ฯ เพิ่มขึ้นจริงๆ หรือเป็นเพราะคู่ขัดแย้งทางการเมืองต้องการอาศัยเหตุผลในเรื่องสถาบันกษัตริย์ฯ เพื่อจัดการกับการแสดงความคิดเห็นของฝ่ายการเมืองตรงข้ามกันแน่

เช่นเดียวกัน เมื่อพิเคราะห์ช่วงเดือนที่สถิติการปิดเว็บหมิ่นฯ มีจำนวนลดลงนั้น จะพบว่าเป็นช่วงท้ายๆ ของการดำรงตำแหน่งรัฐมนตรีว่าการกระทรวงไอซีทีของนายจุติ ไกรฤกษ์ ภายใต้รัฐบาลอภิสิทธิ์ เวชชาชีวะ และในสมัยของรมว.อนุดิษฐ์ นาครทรรพ ภายใต้รัฐบาลยิ่งลักษณ์ ชินวัตร จำนวนการปิดเว็บที่ลดลงนี้ อาจตีความหมายได้หลายประการ เช่น เพราะนโยบายเกี่ยวกับการปราบปรามเว็บหมิ่นฯ ที่เกิดขึ้นก่อนหน้านี้ได้ผลจริงในการช่วยลดจำนวนเว็บหมิ่นฯ ลง หรืออาจมองได้เช่นกันว่าการประกาศยุบสภาการเลือกตั้งและการได้รัฐบาลใหม่ นำไปสู่นโยบายการจัดการเว็บไซต์ที่มีเนื้อหาเข้าข่ายผิดกฎหมายที่แตกต่างกัน

อาจกล่าวได้ว่านอกจากประเด็นความขัดแย้งทางการเมืองแล้ว นโยบายรัฐอาจเป็นอีกหนึ่งสาเหตุสำคัญที่ส่งผลให้เกิดความตื่นตัวเรื่องการปิดเว็บไซต์ เช่น ในช่วงเดือนมิถุนายน และกรกฎาคม 2553 ภายหลังเกิดความร่วมมือระหว่างกระทรวงไอซีที กระทรวงยุติธรรม และกระทรวง



แผนภาพที่ 6: กราฟเส้นแสดงจำนวนยูอาร์แอลที่ถูกปิดกั้นด้วยสาเหตุเรื่องการหมิ่นประมาทพระมหากษัตริย์ พระราชินี และรัชทายาท ในแต่ละเดือนตั้งแต่ปี 2550 ถึง 2554

วัฒนธรรม และการริเริ่มโครงการลูกเสือไซเบอร์ พบว่าสถิติการปิดกั้นเว็บไซต์ในเดือนสิงหาคมมีจำนวนสูงมาก แต่ก็เป็นเพียงระยะเวลาสั้นๆ หลังจากการประกาศนโยบาย เมื่อกระแสเริ่มเบาบางลง สถิติการปิดเว็บไซต์ก็มีจำนวนลดลงอย่างเห็นได้ชัด

อย่างไรก็ดี มาตรา 20 ของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ไม่ได้เป็นเพียงเครื่องมือเดียวที่รัฐใช้จำกัดการเข้าถึงข้อมูลข่าวสาร หากพิจารณาแผนภาพที่ 6 ย่อมเห็นได้ถึงความผันผวนอย่างมีนัยยะสำคัญของจำนวนเว็บไซต์ที่ถูกปิดกั้น กล่าวคือ บางช่วงสถิติการปิดกั้นเว็บไซต์สูงมากถึงหลักหมื่นยูอาร์แอล ในขณะที่บางช่วงซึ่งห่างกันไม่นาน จำนวนยูอาร์แอลที่ถูกระงับการเผยแพร่อยู่ในหลักสิบ หรือกระทั่งไม่มีคำสั่งศาลเลย ซึ่งผลจากการศึกษาพบว่า ในช่วงเวลาที่สถิติการปิดกั้นเว็บไซต์อย่างเป็นทางการตามคำสั่งศาลมีจำนวนเพียงเล็กน้อยนั้น ในความเป็นจริงจำนวนเว็บไซต์ที่ถูกปิดกั้นหาได้ลดน้อยลงไม่ ยูอาร์แอลจำนวนมากยังคงถูกปิดกั้น เพียงแต่

มิได้เป็นไปตามคำสั่งศาล หากแต่เป็นผลมาจากการใช้อำนาจอื่น โดยเฉพาะอย่างยิ่งอำนาจตาม พ.ร.ก.การบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 เช่น ในเดือนพฤษภาคม ปี 2553 ที่ไม่ปรากฏคำสั่งศาลเลยนั้น เป็นช่วงเวลาที่นายอภิสิทธิ์ เวชชาชีวะ นายกรัฐมนตรี ประกาศให้หลายพื้นที่ใช้ พ.ร.ก.การบริหารราชการในสถานการณ์ฉุกเฉินฯ ตั้งแต่เดือนเมษายน 2553 ถึงเดือนธันวาคม 2553[6] โดยตั้งศูนย์อำนวยการแก้ไขสถานการณ์ฉุกเฉิน (ศอฉ.) ให้ปฏิบัติการตามกฎหมาย แหล่งข้อมูลจากผู้ให้บริการอินเทอร์เน็ตรายใหญ่จากภาคเอกชนรายหนึ่งระบุว่า เว็บไซต์ที่มีคำสั่งจาก ศอฉ. ให้ปิดกั้นมีจำนวนเป็นตัวเลขในหลัก “หลายหมื่น” โดยมีรูปแบบการปิดกั้นแตกต่างไปจากการปิดกั้นโดยกระทรวงไอซีทีด้วย เพราะในขณะที่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 มาตรา 20 กระทรวงไอซีทีปิดกั้นเว็บไซต์ได้เพียงเฉพาะส่วนที่ขัดกฎหมายและตามคำสั่งศาลเท่านั้น แต่ศอฉ. สามารถสั่งปิดกั้นมากน้อยอย่างไรก็ได้โดยไม่ต้องขอคำสั่งศาล ทั้งนี้โดยอาศัยมาตรา 9 (3) พ.ร.ก.การบริหารราชการในสถานการณ์ฉุกเฉินฯ[7] จากข้อมูลเบื้องต้นที่คณะผู้วิจัยเข้าถึงได้ พบว่าการปิดกั้นเว็บไซต์โดยศอฉ. ทั้งแบบที่ปรากฏเป็นข่าวและไม่เป็นข่าวเป็นการปิดกั้นแบบเหมารวม โดยไม่สนใจผลกระทบที่เกิดขึ้นกับเว็บไซต์รายอื่นที่ให้บริการเนื้อหาทั่วไป ทั้งนี้เพราะ ไม่เพียงแต่เว็บไซต์ที่ถูกพิจารณาว่ามีเนื้อหาฝ่าฝืนมาตรา 9 (3) พ.ร.ก.ฉุกเฉินฯ เท่านั้นที่ถูกปิดกั้น แต่เว็บไซต์ที่มีเนื้อหาไม่เข้าข่ายผิดกฎหมายอีกจำนวนมากก็ถูกปิดกั้นไปด้วย[8] หากพิจารณาจากเอกสารคำสั่งของศอฉ. อย่างน้อย 3 ฉบับ จะพบว่า ศอฉ.สั่งปิดกั้นเว็บไซต์/ยูอาร์แอล/หมายเลขไอพี/เบอร์โทรศัพท์กว่า 600 รายการ โดยไม่ได้ใช้วิธีระบุเจาะจงชื่อเว็บไซต์หรือยูอาร์แอลเป้าหมาย แต่ใช้วิธีระบุเป็น “ช่วงตัวเลข” ของหมายเลขไอพี เช่น ให้ปิดกั้นเว็บไซต์ที่มีหมายเลขไอพีอยู่ในช่วงตั้งแต่ XXX.XXX.XXX.0 ถึง XXX.XXX.XXX.255 สาเหตุเพราะในช่วงหมายเลขไอพีดังกล่าวนี้เป็นชื่อที่อยู่ของเว็บไซต์ที่ศอฉ. มองว่าเข้าข่าย พ.ร.ก.ฉุกเฉินฯ ปรากฏอยู่ แต่ปัญหาก็คือ ในความเป็นจริงแล้วช่วงหมายเลขไอพี หรือแม้แต่หมายเลขไอพีหนึ่งๆ นั้นมักไม่ใช่ที่อยู่ของเว็บไซต์ใดเว็บไซต์หนึ่งเพียงเว็บไซต์เดียว

แต่เป็นที่อยู่ของกลุ่มเครื่องคอมพิวเตอร์แม่ข่าย (server) ที่อาจถูกจัดแบ่งพื้นที่ให้เช่าใช้โดยเว็บไซต์อื่นๆ อีกจำนวนมาก คำสั่งศอฉ. ที่สั่งปิดเป็นช่วงหมายเลขจึงย่อมส่งผลกระทบต่อเว็บไซต์อื่นๆ ที่ไม่เกี่ยวข้อง หรือไม่ได้ละเมิด พ.ร.ก.ฉุกเฉินฯ แต่อย่างใด

การปิดกั้นเว็บไซต์โดยใช้อำนาจตาม พ.ร.ก.ฉุกเฉินฯ แม้เป็นการกระทำที่ไม่ผิดกฎหมายก็ตาม แต่ด้วยวิธีการนี้ย่อมทำให้ศอฉ. สามารถสั่งการไปยังผู้ให้บริการได้โดยตรงโดยไม่มีกระบวนการกลั่นกรองและถ่วงดุลจากองค์กรภายนอก ทั้งในทางปฏิบัติยังพบว่า กระบวนการปิดเว็บด้วย พ.ร.ก.ฉุกเฉินฯ ที่ผ่านมาขาดความโปร่งใส เพราะไม่มีการทำบันทึกหลักฐานในการใช้อำนาจทุกครั้ง และไม่มีเอกสารแสดงรายละเอียดที่ชัดเจนว่าด้วยการปฏิบัติการตามกฎหมาย หรือเคยสั่งการให้ดำเนินการอย่างไรกับเว็บไซต์ใดไปบ้าง จึงเป็นเรื่องยากที่ประชาชนผู้ได้รับผลกระทบทั้งโดยตรงและโดยอ้อมจะตรวจสอบได้ว่า เว็บไซต์ที่ถูกสั่งปิดไปมีเนื้อหาที่เข้าข่ายผิดกฎหมายจริงหรือไม่ ศอฉ.ใช้อำนาจโดยถูกต้องชอบธรรมหรือไม่ หรือสาเหตุที่ถูกปิดไปก็เพียงเพราะมีการแสดงความคิดเห็นทางการเมืองที่ขัดต่อแนวทางของรัฐเท่านั้น นอกจากนี้ แม้ พ.ร.ก.ฉุกเฉินฯ จะถูกประกาศใช้เฉพาะในเขตกรุงเทพมหานครและบางจังหวัดเท่านั้น แต่เมื่อการปิดเว็บไซต์ที่โดยปกติแล้วประชาชนสามารถเข้าถึงได้ทั่วประเทศ จึงย่อมส่งผลกระทบไปทั่วประเทศด้วย มิใช่เฉพาะแต่จังหวัดที่อยู่ภายใต้ พ.ร.ก.ฉุกเฉินฯ เท่านั้น และประเด็นปัญหาที่น่าสนใจอีกประเด็นหนึ่งก็คือ แม้ในท้ายที่สุดรัฐบาลได้ยกเลิกการประกาศสถานการณ์ฉุกเฉินไปแล้วก็ตาม แต่ในทางปฏิบัติ ไม่มีผู้ให้บริการรายใดที่ปลดบล็อคยูอาร์แอลจำนวนหลายหมื่นให้กลับมาเข้าถึงได้ดังเดิมเลย ส่งผลให้เว็บไซต์จำนวนหนึ่งที่เคยถูกปิดกั้นยังคงถูกปิดกั้นอยู่ต่อไป[9]

อนึ่ง นอกจากการใช้อำนาจตามกฎหมายฉบับต่างๆ แล้ว จากการศึกษา คณะผู้วิจัยยังพบว่า รัฐบาลยังคงใช้วิธีการ “ขอความร่วมมือ” ไปยังผู้ให้บริการระดับต่างๆ เพื่อให้ปิดกั้นช่องทางการเข้าถึงเว็บไซต์ โดยไม่มีคำสั่งศาลด้วย ซึ่งโดยหลักการปกครองแบบ “นิติรัฐ-ประชาธิปไตย” แล้ว การ

ใช้อำนาจรัฐในลักษณะกึ่งบังคับกึ่งตักเตือนเช่นการขอความร่วมมือนี้ถือเป็นกลไกที่ขาดความถูกต้องโปร่งใส เพราะประชาชนไม่สามารถตรวจสอบได้

จากข้อมูลสถิติการปิดกั้นเว็บไซต์ จะเห็นได้ว่าปี 2553 เป็นปีที่รัฐปิดกั้นเว็บไซต์จำนวนสูงที่สุด จากนั้นก็ค่อยๆ ลดลงเรื่อยมาเป็นลำดับ ซึ่งทั้งหมดนี้อยู่ในช่วงที่สถานการณ์การเมืองไทยเริ่มเปลี่ยนแปลงอีกครั้ง เพราะเป็นช่วงที่มีการเลือกตั้งทั่วไป และได้นางสาวยิ่งลักษณ์ ชินวัตร จากพรรคเพื่อไทย เป็นนายกรัฐมนตรี อย่างไรก็ดี คณะผู้วิจัยเห็นพ้องต้องกันว่าการลดลงของจำนวนเว็บไซต์ที่ถูกปิดกั้นนี้ยังไม่สามารถสะท้อน หรือสรุปได้ว่าสถานการณ์ด้านเสรีภาพในการแสดงความคิดเห็นในประเทศไทยมีแนวโน้มในทางที่ดีขึ้น ดังจะเห็นได้ว่า ด้วยระยะเวลาเพียงสามเดือนที่ น.อ. อนุดิษฐ์ นาครทรรพ เข้าดำรงตำแหน่งเป็นรัฐมนตรีว่าการกระทรวงไอซีทีคนแรกในสมัยของนางสาวยิ่งลักษณ์ กระทรวงไอซีทีใช้วิธีการ “ขอความร่วมมือ” ไปยังผู้ให้บริการเฟซบุค (Facebook) ให้ปิดกั้นเนื้อหาไปกว่า 10,000 ยูอาร์แอล[10] (ซึ่งตัวเลขนี้ไม่ได้รวมอยู่ในสถิติของรายงานฉบับนี้ เนื่องจากไม่ได้ปิดกั้นโดยคำสั่งศาลตามมาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550) นอกจากนี้ ร.ต.อ.เฉลิม อยู่บำรุง รองนายกรัฐมนตรี ยังประกาศผ่านสื่อสาธารณะว่าจะปิดกั้นเว็บไซต์ที่เข้าข่ายหมิ่นสถาบันกษัตริย์ฯ ต่อไป โดยใช้งบประมาณจำนวนกว่า 400 ล้านบาท[11] อีกทั้งกระทรวงไอซีทียังเคยออกมาเปิดเผยด้วยว่ากระทรวงได้ส่งตัวแทนไปเจรจากับผู้ให้บริการรายใหญ่ระดับโลกเพื่อ “ขอความร่วมมือ” ในการระงับการเข้าถึงเว็บไซต์จากผู้ชมในประเทศไทยด้วย[12] [13]

โดยสรุปจะเห็นได้ว่า อัตราการปิดกั้นเว็บไซต์ในประเทศไทยภายหลัง พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีผลใช้บังคับเป็นต้นมา แปรผันไปมาโดยมีปัจจัยสำคัญ หรือได้รับอิทธิพลส่วนหนึ่งมาจากสถานการณ์ความขัดแย้งทางการเมือง และอัตราการแสดงออกในเรื่องที่เกี่ยวกับการเมืองของประชาชนในพื้นที่สื่อออนไลน์ อย่างไรก็ดี ในที่สุดแล้ว สถิติและตัวเลขเว็บไซต์ที่ถูกปิดกั้นที่เป็นข้อมูลอย่างเป็นทางการผ่านการเก็บบันทึกคำสั่งศาลอาจไม่ใช่ตัวชี้วัดหรือเป็นข้อสรุปแนวโน้มหรือสถานการณ์เสรีภาพในการ

แสดงความคิดเห็นของประชาชนได้ทั้งหมด เพราะแม้ประเทศไทยจะมีมาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ที่กำหนดหลักเกณฑ์การปิดกั้นเว็บไซต์ที่ต้องขอคำสั่งศาลแล้วก็ตาม แต่นั่นก็เป็นเพียงหลักการที่ใช้เฉพาะในสถานการณ์ปกติเท่านั้น สำหรับรัฐไทยแล้ว ที่ผ่านมายังปรากฏวิธีการจำกัดการแสดงความคิดเห็นของประชาชนอีกหลายวิธี เช่น รัฐสามารถอ้างสถานการณ์พิเศษบางอย่างที่ทำให้รัฐต้องใช้มาตรการเร่งด่วนควบคุมการแสดงออกของประชาชนและสื่อ (ประกาศสถานการณ์ฉุกเฉิน และใช้กฎหมายพิเศษ) ขอความร่วมมือไปยังผู้ให้บริการอินเทอร์เน็ต เพื่อให้ปิดกั้นช่องทางการเข้าถึงเว็บไซต์อย่างลับๆ โดยไม่มีการบันทึกเป็นลายลักษณ์อักษร ทั้งไม่มีกฎหมายฉบับใดให้อำนาจ เป็นต้น

2) กลไกตรวจสอบถ่วงดุลการใช้อำนาจของกระทรวงไอซีที ด้วยการกลั่นกรองคำร้องโดยศาล

การปิดกั้นเว็บไซต์เป็นเรื่องที่ถูกต่อต้านจากประชาชนส่วนหนึ่งมาอย่างต่อเนื่อง เพราะถือเป็นการแทรกแซงสื่อ และปิดกั้นการเข้าถึงข้อมูลข่าวสาร ทั้งไม่สอดคล้องกับอุดมการณ์นิติรัฐ-ประชาธิปไตย ดังนั้น ในการร่าง พ.ร.บ.คอมพิวเตอร์ฯ 2550 จึงมีความพยายามในการสร้างกลไกตรวจสอบถ่วงดุลการใช้อำนาจของเจ้าพนักงานรัฐ และกระทรวงไอซีทีในลักษณะที่อาจกระทบต่อสิทธิและเสรีภาพของประชาชนได้ ซึ่งกลไกสำคัญหนึ่งที่ปรากฏอยู่ใน พ.ร.บ.คอมพิวเตอร์ฯ 2550 ก็คือ กำหนดให้องค์กรตุลาการเป็นผู้กลั่นกรองคำร้องของเจ้าพนักงานรัฐ และทำคำสั่งให้ระงับการเผยแพร่เว็บไซต์ ดังที่ระบุไว้ในมาตรา 20

อย่างไรก็ตาม จากการพิจารณาคำสั่งศาลพบว่าในทางปฏิบัติแล้ว ศาลไม่ได้ใช้เวลามากนักในการกลั่นกรองคำร้องของกระทรวงไอซีทีเพื่อออกคำสั่งระงับการเผยแพร่เว็บไซต์ โดยจากสถิติคำสั่งปิดกั้นของศาล ปรากฏข้อเท็จจริงว่า นับแต่ประกาศใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 เป็นต้นมา มีคำสั่งศาลให้ระงับการเข้าถึงเว็บไซต์ทั้งสิ้น 156 ฉบับ ในจำนวนนี้ มีคำสั่งศาลถึง 142 ฉบับที่ออกในวันเดียวกับวันที่กระทรวงไอซีที

ปี	รวมวันที่ศาลใช้พิจารณาคำร้อง	จำนวน URL	จำนวน URL เฉลี่ยต่อวัน
2550	2	2	1
2551	35	2,071	59
2552	88	28,705	326
2553	46	45,357	986
2554	36	5,078	141
Total	**207**	**81,213**	**392**

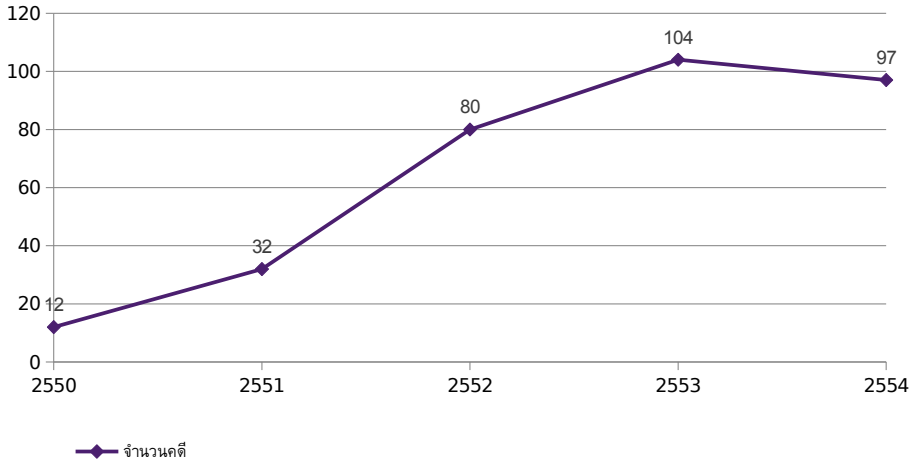
แผนภาพที่ 7: ตารางแสดงจำนวนวันและจำนวนเว็บเพจที่ศาลใช้พิจารณา จำแนกรายปี

ยื่นคำร้องขอ และมีผลเป็นการปิดกั้นเว็บเพจจำนวน 78,192 ยูอาร์แอล จึงเท่ากับว่าโดยเฉลี่ยแล้ว ในช่วงปี 2550-2551 เมื่อกระทรวงไอซีทียื่นคำร้องต่อศาล ศาลจะใช้เวลาราว 2-6 วันในการพิจารณาว่าควรออกคำสั่งปิดกั้นการเข้าถึงยูอาร์แอลที่ถูกร้องขึ้นมาหรือไม่ แต่หลังจากนั้นในปี 2552-2553 เนื่องจากยูอาร์แอลที่ถูกยื่นไปยังศาลมีจำนวนเพิ่มขึ้นอย่างมาก ซึ่งหากพิจารณาจากจำนวนคำสั่งศาลที่ออก ประกอบกับจำนวนยูอาร์แอลที่ถูกปิดกั้นจะพบว่า เฉลี่ยแล้วศาลใช้เวลาพิจารณาและสั่งปิดกั้น 326 ยูอาร์แอลต่อวันในปี 2552 และ 986 ยูอาร์แอลต่อวันในปี 2553 (ดูแผนภาพที่ 7)

ประเด็นในเรื่องระยะเวลาที่ใช้กลั่นกรองเนื้อหาของเว็บเพจที่ถูกยื่นขอเข้ามาเพื่อมีคำสั่งระงับการเผยแพร่นี้ นับเป็นเรื่องสำคัญอย่างยิ่ง แม้มาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550 จะไม่ใช่บทบัญญัติที่มีโทษทางอาญาในตัวเองก็ตาม แต่มาตรการที่ใช้ กล่าวคือ “การปิดกั้น” ไม่ให้ผู้ใช้บริการอินเทอร์เน็ตคนอื่นๆ เข้าถึงเนื้อหาได้ ย่อมส่งผลกระทบต่อเสรีภาพในการ

แสดงความคิดเห็นของเจ้าของเว็บไซต์นั้นโดยตรง ซึ่งเป็นเสรีภาพที่ได้รับการรับรองไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย ดังนั้น การลิดรอนหรือจำกัดเสรีภาพจึงควรเป็นไปอย่างรอบคอบ มีเหตุผล และพอสมควรแก่เหตุ ในความเป็นจริงก็คือ การตรวจสอบเนื้อหาในหน้าเว็บเพจจำนวนหลักร้อยยูอาร์แอลอย่างละเอียดรอบคอบ เพื่อพิจารณาออกคำสั่งให้ระงับการเผยแพร่เว็บเพจเหล่านั้นในวันเดียว โดยผู้พิพากษาเพียงท่านเดียว (หรือแม้กฎหมายกำหนดให้เป็นองค์คณะก็ตาม) เป็นเรื่องที่ทำได้ยากลำบาก ยิ่งหากพิจารณาภารกิจหลักของศาลในการพิจารณาพิพากษาอรรถคดีต่างๆ จำนวนมากอยู่แล้วในแต่ละวันประกอบด้วย จึงยิ่งเป็นเรื่องที่แทบเป็นไปไม่ได้เลยที่ศาลจะใช้เวลาเพียงสั้นๆ เพื่อตรวจสอบเว็บเพจที่ถูกร้องขอเข้ามาโดยละเอียด หรือมิเช่นนั้น ศาลคงจำเป็นต้องมีคณะทำงานขนาดใหญ่ที่ทำหน้าที่เป็นฝ่ายตรวจสอบเนื้อหาของเว็บเพจเหล่านั้นซึ่งต้องทำงานได้อย่างรวดเร็วมาก อย่างไรก็ตาม ผลจากศึกษาวิจัยไม่พบข้อเท็จจริงใดที่แสดงให้เห็นว่าในช่วงเวลาที่ผ่านมามีคณะทำงานในลักษณะดังกล่าวเพื่อช่วยเหลือศาลทำคำสั่งปิดกั้นเว็บไซต์หรือไม่ ด้วยเหตุนี้เอง จึงอาจเกิดคำถามจากสังคม รวมทั้งผู้ได้รับผลกระทบโดยตรงได้ว่า ในที่สุดแล้วศาลได้ตรวจพิจารณากลั่นกรองเนื้อหาในเว็บเพจเหล่านั้น เพื่อถ่วงดุลและตรวจสอบการทำงานของฝ่ายบริหารตามเจตนารมณ์ของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ได้จริงหรือไม่

สำหรับขั้นตอนการระงับการเผยแพร่เว็บไซต์ตามมาตรา 20 นั้น ภายหลังศาลมีคำสั่ง สำเนาคำสั่งจะถูกส่งต่อไปยังผู้ให้บริการอินเทอร์เน็ตหลายรายเพื่อระงับการเข้าถึง อันมีผลให้ผู้ใช้อินเทอร์เน็ตในประเทศไทยไม่สามารถเข้าถึงได้ด้วยวิธีการและช่องทางปกติ

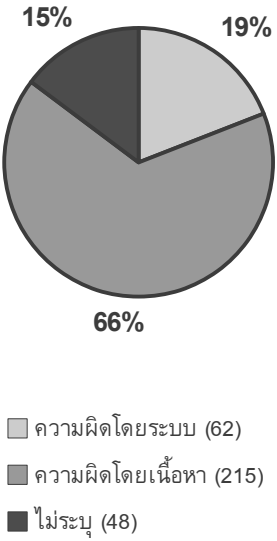


แผนภาพที่ 8: จำนวนคดีตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ตั้งแต่ปี 2550 - 2554

1.2 ผลการศึกษาสถิติการดำเนินคดีตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550

จากการรวบรวมข้อมูลตั้งแต่เดือนกรกฎาคม 2550 ถึงเดือนธันวาคม 2554 พบว่ามีคดีความตาม พ.ร.บ.คอมพิวเตอร์ทั้งสิ้น 325 คดี เป็นคดีที่เริ่มต้นในปี 2550 จำนวน 12 คดี ปี 2551 จำนวน 32 คดี ปี 2552 จำนวน 80 คดี ปี 2553 อีกจำนวน 104 คดี และปี 2554 จำนวน 97 คดี (ดูแผนภาพที่ 8)

สำหรับประเภทความผิดที่ถูกตั้งข้อหาตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 นั้น สามารถจำแนกออกได้เป็น 2 ลักษณะด้วยกัน คือ 1) อาชญากรรมคอมพิวเตอร์โดยแท้ หรือการกระทำความผิดต่อ “ข้อมูล หรือระบบคอมพิวเตอร์” ตามมาตรา 5 ถึงมาตรา 13[14] อาทิ การเข้าถึงระบบโดยมิชอบด้วยกฎหมาย การดักข้อมูล หรือการก่อวินาศกรรมคอมพิวเตอร์ด้วยการเผยแพร่โปรแกรมทำลาย ฯลฯ และ 2) ความผิดที่ว่าด้วยการเผยแพร่

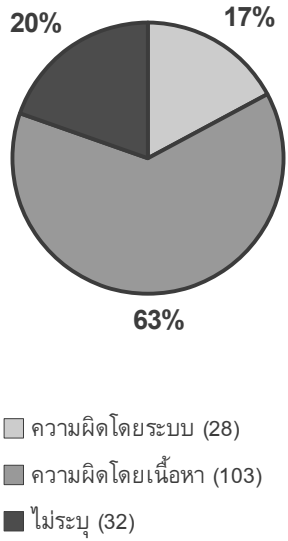


แผนภาพที่ 9: คดีที่ฟ้องร้องตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ทั้งหมด

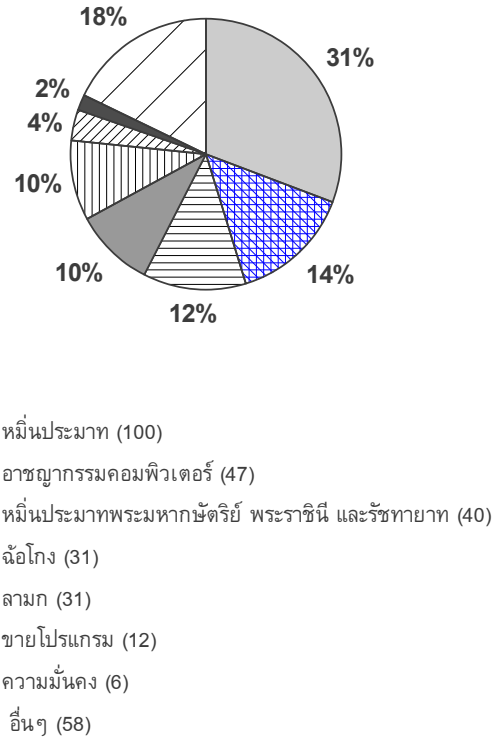
"เนื้อหา" ในระบบคอมพิวเตอร์ซึ่งบัญญัติไว้ตั้งแต่มาตรา 14 ถึงมาตรา 16[15] เช่น การเผยแพร่ภาพลามกอนาจาร การเผยแพร่ข้อมูลที่ขัดต่อความมั่นคง หรือการหมิ่นประมาทด้วยการตัดต่อภาพ เป็นต้น

จากการเก็บสถิติคดีในช่วง 4 ปี 6 เดือน หลัง พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีผลใช้บังคับ หากพิจารณาสัดส่วนของคดีต่างๆ ที่ศาลพิจารณาพิพากษาแล้ว จะพบว่าเป็นคดีที่เป็นความผิดต่อข้อมูล หรือระบบคอมพิวเตอร์ (อาชญากรรมคอมพิวเตอร์โดยแท้) จำนวน 28 คดี คิดเป็นร้อยละ 17.18 ของคดีทั้งหมด ในขณะที่คดีที่เป็นความผิดที่ว่าด้วยการเผยแพร่เนื้อหา มีจำนวน 103 คดี หรือคิดเป็นร้อยละ 63.19 ของคดีทั้งหมด นอกนั้นเป็นส่วนที่ยังมีข้อมูลไม่ชัดเจนอีก 32 คดี หรือร้อยละ 19.63 (ดูแผนภาพที่ 9-10)

โดยในบรรดาคดีต่างๆ เหล่านี้สามารถจำแนกตามประเภทของความผิดออกได้ 7 ประเภทด้วยกัน โดยเรียงตามลำดับความมากน้อยของ



แผนภาพที่ 10: คดีทั้งหมดที่ศาลชั้นต้นพิพากษาแล้ว จำแนกตามประเภทความผิด



แผนภาพที่ 11: จำนวนคดีจำแนกตามประเภทเนื้อหาความผิด

จำนวนคดี ดังนี้ อันดับหนึ่ง หมิ่นประมาทบุคคลอื่น จำนวน 100 คดี อันดับสอง อาชญากรรมคอมพิวเตอร์โดยแท้ 47 คดี อันดับสาม ดูหมิ่นกษัตริย์ฯ 40 คดี อันดับสี่ ความผิดฐานฉ้อโกงหรือหลอกลวงทางอินเทอร์เน็ต 31 คดี อันดับห้า เผยแพร่ภาพลามก 31 คดี อันดับหก การขายโปรแกรมที่เข้าข่ายผิดกฎหมาย 12 คดี อันดับเจ็ด เนื้อหาที่เป็นความผิดเกี่ยวกับความมั่นคง 6 คดี นอกนั้นเป็นเนื้อหาอื่นๆ และที่ไม่สามารถระบุได้อีก 58 คดี (ดูแผนภาพที่ 11)

จากสถิติคดีความข้างต้น หากจำแนกคดีตาม “สถานะของคดี” และ “ผลของคดี” สามารถแยกออกได้ดังนี้ 1) คดีที่อยู่ในชั้นพนักงานสอบสวน หรือเจ้าหน้าที่ตำรวจ 89 คดี 2) คดีที่พนักงานอัยการสั่งฟ้อง 70 คดี 3) คดีที่พนักงานอัยการสั่งไม่ฟ้อง 1 คดี 4) คดีที่มีการไกล่เกลี่ย/จำหน่ายคดี 20 คดี 6) คดีที่ศาลพิพากษายกฟ้องโจทก์ 13 คดี 7) คดีที่ศาลพิพากษาว่าจำเลยมีความผิด 73 คดี 8) คดีที่พนักงานสอบสวนตั้งข้อหาตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 แต่อัยการไม่ได้สั่งฟ้องตามข้อหาดังกล่าว หรือศาลไม่ได้พิพากษาว่าเป็นความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 อีก 2 คดี นอกนั้นเป็นคดีที่ศาลพิพากษาแล้ว แต่เป็นคดีที่เกิดขึ้นในศาลต่างจังหวัด ซึ่งฐานข้อมูลที่จัดเก็บข้อมูลคดีบอกเพียงหมายเลขคดีและข้อกล่าวหา แต่ไม่ได้ระบุลงไปถึงรายละเอียดการกระทำผิดและผลของคดี ซึ่งมีจำนวนทั้งสิ้น 57 คดี (ดูแผนภาพที่ 12)

สำหรับแผนภาพที่ 13 จะเห็นได้ว่าความผิดฐานหมิ่นประมาทนั้น นอกจากเป็นความผิดประเภทที่ถูกฟ้องเป็นคดีความตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 เป็นจำนวนมากแล้ว ยังถือเป็นคดีที่มีการไกล่เกลี่ยจำหน่ายคดีสูงที่สุด ทั้งยังเป็นคดีที่ศาลพิพากษายกฟ้องสูงที่สุดอีกด้วย ต่างจากคดีประเภทอื่นๆ อย่าง อาชญากรรมคอมพิวเตอร์ หมิ่นประมาทกษัตริย์ฯ หรือการเผยแพร่เนื้อหาและภาพลามก ซึ่งมีจำนวนคดีที่ถูกฟ้องเป็นอันดับรองลงมาตามลำดับ แต่เมื่อคดีขึ้นสู่ศาลแล้ว ผลของคดีส่วนใหญ่ศาลจะพิพากษาลงโทษจำเลย ดังนี้ คดีอาชญากรรมคอมพิวเตอร์ที่ศาลชั้นต้นพิจารณาแล้ว ร้อยละ 66.67 พิพากษาว่าจำเลยมีความผิด คดีหมิ่นประมาท

ประเภทความผิด	สถานะคดี								รวม
	สืบสวน สอบสวน	อัยการ		ศาล					
		สั่งฟ้อง	ไม่สั่งฟ้อง	ไม่ตั้งข้อหา พ.ร.บ.คอมฯ	ไกล่เกลี่ย จำหน่ายคดี	ยกฟ้อง	ต้องโทษ	ตัดสินแล้ว แต่เข้าไม่ถึงข้อมูล	
ความผิดต่อระบบ (มาตรา 5-13)	24	10	0	0	4	1	18	5	**62**
ความผิดด้วยเนื้อหา (มาตรา 14-16)	62	48	1	1	15	12	54	22	**215**
ไม่สามารถระบุได้	3	12	0	1	1	0	1	30	**48**
รวม	**89**	**70**	**1**	**2**	**20**	**13**	**73**	**57**	**325**

แผนภาพที่ 12: ตารางแสดงจำนวนคดีจำแนกตามขั้นตอนสถานะคดีและประเภทความผิด

คดี พ.ร.บ.คอมพิวเตอร์	ความมั่นคง	หมิ่นประมาท	หมิ่นสถาบัน	ลามก	ฉ้อโกง	อาชญากรรมคอมพิวเตอร์	ขายโปรแกรม	อื่นๆ	รวม
คดีที่อยู่ระหว่างการสืบสวนสอบสวน	1	15	28	1	11	14	10	9	**89**
คดีที่อัยการสั่งฟ้องแล้ว	2	32	4	3	8	9	0	12	**70**
คดีที่อัยการไม่สั่งฟ้อง	1	0	0	0	0	0	0	0	**1**
คดีที่อัยการ/ศาลไม่ได้ตั้งข้อหาพ.ร.บ./ไม่ตัดสินว่าผิดตามพ.ร.บ.คอมพิวเตอร์*	0	1	0	0	1	0	0	0	**2**
คดีที่มีการไกล่เกลี่ย จำหน่ายคดี	0	14	0	0	1	4	0	1	**20**
คดีที่ศาลยกฟ้อง	1	10	1	0	0	1	0	0	**13**
คดีที่ศาลพิพากษาแล้วว่ามีความผิด	1	17	7	23	5	16	0	4	**73**
คดีที่ศาลตัดสินแล้ว แต่ไม่รู้ผล**	0	11	0	4	5	3	2	32	**57**
รวม	**6**	**100**	**40**	**31**	**31**	**47**	**12**	**58**	**325**

แผนภาพที่ 13: สถานะความคืบหน้าคดี แจกแจงตามลักษณะของประเภทเนื้อหาความผิด

กษัตริย์ฯ ที่ศาลชั้นต้นพิจารณาแล้ว ร้อยละ 87.5 พิพากษาว่าจำเลยมีความผิด และคดีเกี่ยวกับภาพหรือข้อความลามกที่ศาลชั้นต้นพิจารณาแล้ว พบว่าร้อยละ 85.19 พิพากษาว่าจำเลยมีความผิด

จากคดีที่ศาลพิพากษาว่าจำเลยมีความผิดทั้งหมด 73 คดี (ดูแผนภาพที่ 14) ยังสามารถจำแนกออกได้เป็นคดีที่จำเลยรับสารภาพ 62 คดี และคดีที่จำเลยต่อสู้คดี 11 คดี ในกรณีที่จำเลยรับสารภาพ หากเป็นคดีประเภทหมิ่นประมาทและเผยแพร่ภาพหรือข้อความลามก ศาลมีแนวโน้มให้รอลงอาญา โดยส่วนใหญ่ให้เหตุผลว่า จำเลยให้การรับสารภาพ ไม่เคยต้องโทษจำคุก และความประพฤติโดยรวมไม่เสียหาย เห็นควรให้โอกาสกลับตัวเป็นพลเมืองดีจึงให้รอการลงโทษ บางคดีศาลสั่งว่าระหว่างรอลงอาญาให้จำเลยทำกิจกรรมบริการสังคมหรือสาธารณประโยชน์ หรือเข้าร่วมกิจกรรมอบรมธรรมะเพื่อใช้หลักธรรมทางศาสนากล่อมเกลาจิตใจ ทั้งนี้ ลักษณะคำพิพากษาของคดีประเภทดังกล่าว ยังมีความแตกต่างกับคดีอาชญากรรมคอมพิวเตอร์ คดีฉ้อโกง และคดีหมิ่นประมาทกษัตริย์ฯ ที่พบว่าศาลมักสั่งจำคุกโดยไม่รอลงอาญา เช่น ตัวอย่างคำพิพากษาคดีหนึ่ง เป็นคดีหมายเลขแดงที่ ด.1945/2553 ศาลอาญากรุงเทพฯ ใต้ คดีนี้จำเลยลักลอบเข้าสู่ระบบคอมพิวเตอร์ของบริษัทโฮสติ้งแห่งหนึ่ง จากนั้นได้ทำการลบข้อมูลของสมาชิกรายหนึ่ง ศาลพิพากษาให้จำเลยมีความผิด ลงโทษจำคุกโดยไม่รอลงอาญา ระบุเหตุผลว่า “ในสภาพปัจจุบันมีการใช้คอมพิวเตอร์กันแพร่หลาย ในทางด้านเศรษฐกิจ และในการค้นหาข้อมูลในการศึกษาและอื่นๆ โดยทั่วไป การที่จำเลยได้กระทำความผิดดังกล่าวย่อมเป็นการกระทบต่อความเชื่อมั่นเกี่ยวกับการใช้งานทางคอมพิวเตอร์และสังคมโดยรวม นับว่าเป็นเรื่องร้ายแรง จึงไม่มีเหตุให้รอการลงโทษแก่จำเลย”

จากข้อมูลคดีความที่รวบรวมได้ หากจำแนกตามหมวดหมู่ผู้ร้องทุกข์กล่าวโทษจะพบว่า อันดับหนึ่งของจำนวนผู้ร้องทุกข์หรือกล่าวโทษเป็นบุคคลทั่วไปเพศหญิง 66 คดี อันดับสอง นิติบุคคล 56 คดี อันดับสาม บุคคลทั่วไปเพศชาย 44 คดี อันดับสี่ กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี (ปอท.) 19 คดี อันดับห้า กระทรวงไอซีที 17 คดี อันดับหก

ข้อหา	ศาลตัดสินว่ามีความผิด (73)				ยกฟ้อง	ไกล่เกลี่ยจำหน่ายคดี	เข้าไม่ถึงผลการพิจารณา		รวม
	รับสารภาพ (62)		สู้คดี (11)				รับสารภาพ	สู้คดี	
	ต้องโทษจำคุก	รอลงอาญา	ต้องโทษจำคุก	รอลงอาญา					
ความมั่นคง	0	1	0	0	1	0	0	0	**2**
หมิ่นประมาท	1	16	0	0	10	14	2	9	**52**
หมิ่นสถาบัน	4	1	2	0	1	0	0	0	**8**
ลามก	2	19	2	0	0	0	3	1	**27**
ฉ้อโกง	5	0	0	0	0	1	0	5	**11**
อาชญากรรมคอมพิวเตอร์	9	2	5	0	1	4	0	3	**24**
ขายโปรแกรม	0	0	0	0	0	0	2	0	**2**
อื่นๆ	0	2	2	0	0	1	19	13	**37**
รวม	**21**	**41**	**11**	**0**	**13**	**20**	**26**	**31**	**163**

แผนภาพที่ 14: รายละเอียดคดีที่ศาลชั้นต้นพิจารณาเสร็จสิ้นแล้ว

กรมสอบสวนคดีพิเศษหรือดีเอสไอ 13 คดี อันดับเจ็ด กองบังคับการปราบปราม 12 คดี อันดับแปด หน่วยงานรัฐอื่นๆ 12 คดี อันดับเก้า ตำรวจท้องที่ 6 คดี อันดับสิบ คือ กองบังคับการปราบปรามอาชญากรรมต่อเด็กและสตรี (ปคส.) 4 คดี อันดับสิบเอ็ด กองบังคับการปราบปรามอาชญากรรมทางเศรษฐกิจ (ปอศ.) 3 คดี และเป็นคดีที่ไม่ปรากฏชัดว่าเริ่มต้นโดยใคร 73 คดี อย่างไรก็ตาม แม้ในรายงานวิจัยฉบับนี้จะมีข้อมูลอย่างเป็นทางการว่ากระทรวงไอซีทีเป็นผู้กล่าวโทษเพียง 17 คดี แต่ในจำนวน 17 คดีดังกล่าว พบว่ามี 1 คดีที่กระทรวงไอซีทีแจ้งความไว้กับตำรวจกองบังคับการปราบปราม โดยใช้วิธีการ “ยื่นบัญชีรายชื่อยูอาร์แอลหรือเว็บเพจ” ที่อ้างว่ามีเนื้อหาเข้าข่ายดูหมิ่น หรือหมิ่นประมาทกษัตริย์ฯ ตามประมวลกฎหมายอาญามาตรา 112 ทั้งสิ้น 1,037 ยูอาร์แอล ปัจจุบันคดีนี้ยังอยู่ในระหว่างการสอบสวนของเจ้าหน้าที่ตำรวจ แต่เมื่อพิจารณาจากสำนวนการสอบสวนดังกล่าวของเจ้าหน้าที่ตำรวจจะพบว่า จากยูอาร์แอลทั้งหมดที่กระทรวงไอซีที

ยื่นแจ้งความมาเพียงครั้งเดียวนั้น อาจก่อให้เกิดคดีความที่จะนำส่งต่อไปยังชั้นพนักงานอัยการ หรืออาจขึ้นสู่ศาลได้อีกถึง 997 คดี

สำหรับรายละเอียดผู้ต้องหาและจำเลยตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 นั้น พบว่าบุคคลทั่วไปเพศชายถูกตั้งข้อหาและดำเนินคดีมากที่สุด จำนวน 153 คดี รองลงมาคือบุคคลทั่วไปเพศหญิง 67 คดี นอกจากนี้ยังมีผู้ให้บริการอินเทอร์เน็ต ที่จัดอยู่ในกลุ่มของการให้บริการเนื้อหา (Content Provider) หรือเป็นตัวกลางในการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ต อาทิ เจ้าของเว็บไซต์ ผู้ให้บริการพื้นที่แลกเปลี่ยนในกระดานข่าว ผู้ดูแลเว็บไซต์ (Webmaster) หรือผู้ดูแลระบบ (Admin) ของเว็บไซต์ ถูกดำเนินคดีด้วยจำนวนทั้งสิ้น 24 คดี นอกเหนือจากนี้เป็นคดีที่ยังไม่สามารถระบุลักษณะของผู้กระทำความผิดได้ว่าอยู่ในกลุ่มใด

<u>บทวิเคราะห์ และข้อสังเกตต่อคดีความที่เกี่ยวกับการเผยแพร่เนื้อหาในสื่อออนไลน์</u>

จากสถิติคดีความทั้งหมดที่คณะผู้วิจัยสามารถเข้าถึงและรวบรวมได้ จะเห็นได้ว่าข้อหาความผิดอันเกิดจากการเผยแพร่เนื้อหาตามมาตรา 14 ถึงมาตรา 16 พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีสัดส่วนสูงมาก เมื่อเปรียบเทียบกับความผิดที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์โดยแท้ หรืออาชญากรรมที่กระทำต่อตัวข้อมูลหรือระบบคอมพิวเตอร์โดยตรง ตามมาตรา 5 ถึงมาตรา 13 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ทั้งนี้ มีทั้งคดีที่ตั้งข้อหาโดยอาศัยบทบัญญัติใน พ.ร.บ.คอมพิวเตอร์ฯ 2550 เพียงฉบับเดียว และคดีที่ใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ประกอบกับความผิดตามกฎหมายฉบับอื่น เช่น ประมวลกฎหมายอาญา

1) การใช้มาตรา 14 (1) กับกรณีหมิ่นประมาท และความเท็จจริงของเนื้อหา

ผู้ร้องทุกข์	ความมั่นคง	หมิ่นประมาท	หมิ่นสถาบัน	ลามก	ฉ้อโกง	อาชญากรรมคอมพิวเตอร์	ขายโปรแกรม	อื่นๆ	รวม
เจ้าทุกข์ ชาย	0	24	1	1	5	9	0	4	**44**
เจ้าทุกข์ หญิง	0	39	0	12	9	2	0	4	**66**
นิติบุคคลเอกชน	0	19	0	0	5	**25**	0	7	**56**
ปอศ	0	0	0	0	1	2	0	0	**3**
ปอท	1	0	3	0	2	2	10	1	**19**
ปตส ต้ามนุษย์	0	0	0	4	0	0	0	0	**4**
กองปราบ	2	1	8	0	0	0	0	1	**12**
ดีเอสไอ	1	0	9	0	0	3	0	0	**13**
ไอซีที	0	0	**16**	0	0	0	0	1	**17**
หน่วยงานรัฐ	1	1	2	4	1	2	0	1	**12**
ตำรวจท้องที่	0	1	1	2	0	0	0	2	**6**
ไม่ปรากฏ	1	15	0	8	8	2	2	37	**73**
รวม	**6**	**100**	**40**	**31**	**31**	**47**	**12**	**58**	**325**

แผนภาพที่ 15: จำแนกประเภทคดีตามบุคคล/หน่วยงานที่ร้องทุกข์กล่าวโทษ

ผู้ต้องหา		ความมั่นคง	หมิ่นประมาท	หมิ่นสถาบัน	ลามก	ฉ้อโกง	อาชญากรรมคอมพิวเตอร์	ขายโปรแกรม	อื่นๆ	รวม
บุคคลทั่วไป	เพศชาย	3	42	15	21	18	26	9	19	**153**
	เพศหญิง	1	23	4	3	8	9	1	18	**67**
	นิติบุคคลเอกชน	0	6	0	0	1	**1**	0	1	**9**
	ยังไม่รู้ตัวผู้กระทำผิด	0	6	14	0	1	**6**	0	3	**30**
	ไม่มีข้อมูล	1	7	3	2	3	5	2	17	**40**
ผู้ให้บริการ	ผู้ให้บริการ	1	15	3	5	0	0	0	0	**24**
	อื่นๆ	0	1	1	0	0	0	0	0	**2**
รวม		**6**	**100**	**40**	**31**	**31**	**47**	***12***	**58**	**325**

แผนภาพที่ 16: จำแนกประเภทผู้ถูกตั้งข้อหา/ดำเนินคดีตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 แจกแจงตามประเภทความผิด

"มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน"

เนื่องจากการติดต่อสื่อสารในอินเทอร์เน็ตนั้น ผู้รับ-ส่งสาร สามารถปิดบังตัวตนที่แท้จริงได้ การสืบย้อนรอยเพื่อหาตัวผู้กระทำความผิดอาจทำได้ก็จริงอยู่ แต่ไม่ใช่เรื่องง่ายเหมือนเช่นในสังคมจริง ๆ ผู้เล่นอินเทอร์เน็ตจึงสามารถต่อว่าด่าทอ กล่าวหากัน กระทั่งนำภาพหรือเรื่องส่วนตัวของบุคคลอื่นมาเผยแพร่จนนำมาซึ่งความเสียหายต่อชื่อเสียง เกียรติยศ โดยไม่ต้องเกรงว่าตนจะถูกจับได้ จนน่าจะเป็นเหตุให้มีสถิติการนำคดีหมิ่นประมาทขึ้นสู่ศาลมากกว่าในสมัยก่อน ทั้งนี้ ไม่ว่าคดีเหล่านั้นโจทก์จะรู้ตัวผู้กระทำหรือไม่ก็ตาม นอกจากนี้ ในช่วงหลายปีที่ผ่านมายังปรากฏข้อเท็จจริงว่า คดีหมิ่นประมาทจำนวนไม่น้อยถูกใช้เป็นเครื่องมือทางการเมือง เช่น นักการเมืองฟ้องร้องซึ่งกันและกัน หรือการฟ้องร้องสื่อมวลชน อย่างไรก็ดี มีข้อที่ต้องสังเกตด้วยว่า โดยการใช้การตีความกฎหมายแล้ว ความผิดที่ว่าด้วยการหมิ่นประมาทนั้นแม้จะเกิดขึ้นในสื่อออนไลน์ก็ตาม ย่อมสามารถใช้ มาตรา 423[16] แห่งประมวลกฎหมายแพ่งพาณิชย์ หรือมาตรา 326[17] ประกอบมาตรา 328[18] แห่งประมวลกฎหมายอาญา มาบังคับได้อยู่แล้ว โดยไม่จำเป็นต้องอาศัยตัวบทใน พ.ร.บ.คอมพิวเตอร์ฯ 2550 อีก แต่ในความเป็นจริงกลับพบว่า การหมิ่นประมาทที่เกิดขึ้นในอินเทอร์เน็ตจำนวนมากถูกฟ้องในฐานะคดีอาชญากรรมคอมพิวเตอร์ด้วย โดยผู้เกี่ยวข้องใช้วิธีตั้งข้อหาตามประมวลกฎหมายแพ่งฯ หรือกฎหมายอาญา ประกอบกับ มาตรา 14 (1) พ.ร.บ.คอมพิวเตอร์ฯ 2550 ทั้ง ๆ ที่หากตีความตามเจตนารมณ์ของผู้ร่างกฎหมายประกอบกับถ้อยคำในมาตรา 14 (1) พ.ร.บ.คอมพิวเตอร์ฯ 2550 แล้ว จะพบว่าการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลเท็จ จนอาจทำให้ผู้อื่นได้รับความเสียหายนั้น หาได้ใช้ในความหมายแบบเดียวกับการ

หมิ่นประมาทไม่

เป้าหมายของมาตรา 14 (1) ผู้บัญญัติต้องการอุดช่องว่างของกฎหมายอาญาที่ว่าด้วยการ “ปลอมแปลงเอกสาร” หรือการทำ “เอกสารเท็จ” ซึ่งตามกฎหมายในสมัยเดิมบัญญัติให้คำว่า “เอกสาร” หมายเฉพาะแต่ “กระดาษหรือวัตถุอื่นใดที่มีรูปร่างและจับต้องได้” เท่านั้น[19] จึงทำให้ไม่สามารถตีความกฎหมายเหล่านั้นให้ครอบคลุมถึงการปลอมแปลงข้อมูลอิเล็กทรอนิกส์ได้[20] ก่อให้เกิดช่องว่างของกฎหมาย ฉะนั้น ความหมายของมาตรา 14 (1) จึงมิได้หมายถึงการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลที่มีเนื้อหา (ไม่ว่าจะเป็นความจริงหรือความเท็จก็ตาม) ที่อาจทำให้บุคคลอื่นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง อันเป็นองค์ประกอบความผิดทำนองเดียวกับความผิดในฐาน “หมิ่นประมาท” ตามประมวลกฎหมายแพ่งฯ หรือประมวลกฎหมายอาญา หากแต่คือ “การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ไม่แท้จริง (ข้อมูลคอมพิวเตอร์ปลอม) ที่ถูกทำขึ้นโดยผู้ไม่มีอำนาจตามกฎหมายที่จะทำข้อมูลนั้นขึ้นมาได้” หรือมิเช่นนั้นก็คือ “การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง ข้อมูลคอมพิวเตอร์ที่แท้จริง (ผู้มีอำนาจตามกฎหมายเคยทำข้อมูลฯ ดังกล่าวขึ้นแล้วโดยชอบด้วยกฎหมาย) แต่ต่อมาถูกผู้กระทำความผิดแก้ไข เปลี่ยนแปลง หรือทำให้ข้อมูลนั้นผิดความหมาย หรือเปลี่ยนแปลงไปจากเดิม” อันเป็นความหมายแบบเดียวกับความผิดในฐาน “ปลอมแปลงเอกสาร” ตามประมวลกฎหมายอาญา

การตีความมาตรา 14 (1) ให้กลายเป็นมาตราเพื่อจัดการกับความผิดฐานหมิ่นประมาทเช่นนี้ นอกจากก่อให้เกิดผลที่ผิดพลาดคลาดเคลื่อนในทางกฎหมาย รวมทั้งเกิดความซ้ำซ้อนในการใช้กฎหมายแล้ว ย่อมก่อให้เกิดความสับสนทั้งกับผู้ถูกฟ้อง และประชาชนทั่วไปด้วย[21]

2) การใช้มาตรา 14 (2) และ (3) กับเหตุผลด้านความมั่นคง

“มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ...

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จโดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา"

ดูเหมือนว่า พ.ร.บ.คอมพิวเตอร์ฯ 2550 ฉบับนี้ ผู้ร่างกฎหมายให้ความสำคัญกับการรักษาความมั่นคงของประเทศเป็นอย่างมาก โดยกำหนดความผิดเกี่ยวกับเรื่องนี้ไว้ทั้งในมาตรา 14 (2) และ (3) อย่างไรก็ตาม มาตรา 14 (2) เป็นมาตราหนึ่งในกฎหมายฉบับนี้ที่มีปัญหาในเรื่องขอบเขตการบังคับใช้มากที่สุด และถูกวิพากษ์วิจารณ์ว่าถูกฝ่ายรัฐใช้เป็นเครื่องมือในการลิดรอนเสรีภาพในการแสดงความคิดเห็นของประชาชน เพราะใช้ถ้อยคำที่กำกวมไม่ชัดเจนอย่าง "ความเสียหายต่อความมั่นคง" และ "ก่อให้เกิดความตื่นตระหนกแก่ประชาชน" เพราะประชาชนโดยทั่วไปไม่สามารถเข้าใจได้ว่าข้อมูลที่มีเนื้อหาอย่างใดจึงจะเข้าข่ายเป็นความผิดดังกล่าว ขึ้นอยู่กับดุลพินิจของเจ้าพนักงานรัฐเป็นสำคัญ ซึ่งย่อมแปรเปลี่ยนได้ตามยุคสมัยและทัศนคติของผู้บังคับใช้กฎหมาย ในท้ายที่สุดมาตรานี้จึงอาจถูกนำไปใช้เป็นเครื่องมือเล่นงานกันทางการเมือง ยิ่งหากมีการฟ้องคดีแล้วจำเลยไม่ต่อสู้คดี ความคลุมเครือในการกระทำตามฟ้องก็คงยังไม่ได้รับการพิสูจน์ หรือตีความให้ชัดเจนขึ้นมาได้ ตัวอย่างเช่น คดีความมั่นคงคดีหนึ่งที่ศาลพิพากษาลงโทษผู้เขียนข้อความและนำภาพถ่ายนายคิม จอง อิล ประธานาธิบดีประเทศเกาหลีเหนือ ในลักษณะที่อาจทำให้ประชาชนเกิดความสับสนแตกแยกความสามัคคี และอาจมีผลกระทบต่อความสัมพันธ์ระหว่างประเทศไทยกับประเทศเกาหลีเหนือ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ คดีดังกล่าวปรากฏว่าจำเลยรับสารภาพ ศาลจึงตัดสินว่ามีความผิดเลย โดยไม่มีการพิสูจน์ว่าการพูดถึงประธานาธิบดีเกาหลีเหนือเช่นนั้นมีผลกระทบต่อความมั่นคงระหว่าง

ประเทศอย่างไร

จากสถิติคดีชี้ให้เห็นว่า คดีความมั่นคงซึ่งเป็นการตั้งข้อหาร่วมกับมาตรา 14 (2) (หรือ (3) แล้วแต่กรณี ส่วนใหญ่เป็นความผิดในฐานหมิ่นประมาทพระมหากษัตริย์ พระราชินี และรัชทายาท ตามประมวลกฎหมายอาญามาตรา 112 (จำนวน 40 คดี) นอกเหนือจากนี้เป็นเนื้อหาที่กระทบต่อความมั่นคงในลักษณะอื่นๆ หรือขัดต่อศีลธรรมอันดีของประชาชน (จำนวน 6 คดี) ซึ่งเมื่อพิจารณาจากบริบททางสังคมในช่วงสองสามปีที่ผ่านมาแล้ว จะพบว่าหากมีการฟ้องร้องคดี โดยเฉพาะอย่างยิ่งฐานหมิ่นประมาทกษัตริย์ฯ ผู้ต้องหาจำนวนมากที่ถูกจับกุมจะไม่ได้รับอนุญาตให้ประกันตัว นอกจากนี้ยังมีความพยายามของบุคลากรในกระบวนการยุติธรรมจูงใจให้ผู้ต้องหาหรือจำเลยรับสารภาพ หรือสนับสนุนให้ขอพระราชทานอภัยโทษแทนการสู้คดี ประกอบกับหาทนายความแก้ต่างคดีให้ได้ยาก เป็นผลให้ผู้ต้องหาส่วนใหญ่เลือกที่จะรับสารภาพ ดังนั้น แม้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 จะใช้บังคับมาแล้วกว่า 4 ปี ก็ยังไม่มีตัวอย่างคดีที่จะนำมาศึกษาวิเคราะห์ได้ว่าความหมายของคำว่า “ความมั่นคง” ตามที่นิยามไว้ในมาตรานี้กว้างขวางเพียงใด ปัจจุบันมีคดีความมั่นคงเพียงสองคดีเท่านั้นที่ศาลยกฟ้อง แต่เหตุที่ยกฟ้องไม่ได้พูดถึงเนื้อหาใจความว่า ข้อความที่เผยแพร่บนเครือข่ายอินเทอร์เน็ตนั้นส่งผลกระทบต่อความมั่นคงได้อย่างไร แต่เกิดจากสาเหตุว่าไม่อาจพิสูจน์ได้จริงว่าจำเลยเป็นผู้เขียนข้อความ

<u>ตัวอย่างคดี มาตรา 14 (3)</u> ในบรรดาคดีความมั่นคงที่ฟ้องตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 นั้น มีตัวอย่างคดี 2 คดีที่น่าสนใจ ซึ่งจำเลยเป็นผู้ให้บริการ ถูกฟ้องในฐานะตัวกลางที่จงใจสนับสนุน หรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 (3) และมาตรา 15 พ.ร.บ. คอมพิวเตอร์ฯ 2550 โดยทั้งสองคดีศาลพิพากษาลงโทษจำเลย กล่าวคือ คดีแดงที่ อ.1226/2554 ของศาลอาญา โดยมีนายธันย์ฐวุฒิ ท. ผู้ออกแบบเว็บไซต์ นปช.ยูเอสเอ เป็นจำเลย ซึ่งถูกกล่าวหาว่าเป็นผู้เขียนข้อความหมิ่นประมาทกษัตริย์ฯ ด้วยตนเอง 2 ข้อความ และยินยอมปล่อยให้เผยแพร่บทความหมิ่นประมาทกษัตริย์ฯ อีก 1 บทความ จำเลยให้การปฏิเสธทุกข้อกล่าวหา

และสู้คดีว่า ตนรู้จักเว็บไซต์นี้จริง ล็อกอินเข้าระบบจริงเพราะรับจ้างออกแบบเว็บไซต์ในส่วนงานออกแบบให้ แต่ไม่ใช่ผู้โพสต์ข้อความทั้งสอง และไม่ใช่ผู้มีอำนาจหน้าที่ควบคุมดูแลเนื้อหาของเว็บไซต์ คดีนี้มีหลักฐานเป็นข้อมูลจราจรคอมพิวเตอร์ที่แสดงว่า จำเลยล็อกอินเข้าระบบของเว็บไซต์ผ่านโปรแกรมส่งไฟล์ FTP (File Transfer Protocal) ด้วยชื่อ “noporch“ ซึ่งเจ้าหน้าที่ตำรวจเห็นว่าโปรแกรมดังกล่าวต้องใช้งานโดยผู้มีความรู้ความสามารถ จึงตีความว่าจำเลยน่าจะเป็นผู้ดูแลระบบซึ่งเป็นผู้ให้บริการตามกฎหมาย อีกทั้งข้อความทั้งสองข้อความที่ปรากฏตามฟ้องนั้น ปรากฏหลักฐานว่าผู้โพสต์ลงทะเบียนด้วยชื่อ “admin“ (ไม่ใช่ชื่อ “noporch” ที่จำเลยใช้) คำว่า admin มีความหมายเป็นที่เข้าใจทั่วไปว่าหมายถึง ผู้ดูแลระบบ ตำรวจจึงตั้งข้อหาจำเลย ซึ่งใช้โปรแกรม FTP ด้วยชื่อ noporch ว่าน่าจะเป็นคนเดียวกับผู้ที่โพสต์ด้วยชื่อ admin ดังนั้น จำเลยจึงน่าจะเป็นทั้งผู้เขียนข้อความและเป็นผู้ให้บริการตามกฎหมาย ผลของคดีนี้ศาลพิพากษาจำคุกจำเลย 13 ปี

อีกคดีหนึ่ง คดีแดงที่ อ.2091/2555 จำเลยเป็นผู้อำนวยการเว็บไซต์หนังสือพิมพ์ประชาไท ซึ่งเป็นเว็บข่าวที่มีกองบรรณาธิการรับผิดชอบเนื้อหาชัดเจน และมีพื้นที่เว็บบอร์ดที่เปิดให้คนทั่วไปตั้งกระทู้แสดงความคิดเห็นได้ ซึ่งการฟ้องร้องดังกล่าวเป็นผลมาจาก “ข้อความของผู้อื่น” ซึ่งเข้ามาเขียนไว้ในพื้นที่เว็บไซต์ประชาไท โดยศาลพิพากษาให้จำเลย คือ นางสาวจีรนุช เปรมชัยพร ผู้อำนวยการประชาไท มีความผิดตามมาตรา 14 (3) และ 15 พ.ร.บ. คอมพิวเตอร์ฯ 2550 ให้จำคุก 1 ปี ปรับ 30,000 บาท แต่เนื่องจำเลยให้การเป็นประโยชน์จึงลดโทษ 1 ใน 3 เหลือจำคุก 8 เดือน ปรับ 20,000 บาท และจำเลยไม่เคยกระทำความผิดจึงให้รอลงอาญา 1 ปี โดยศาลให้เหตุผลว่า จำเลยปล่อยให้มีการนำเข้าข้อมูลที่เป็นความผิดเกี่ยวกับความมั่นคงของประเทศอยู่ในเว็บบอร์ดที่ตนดูแล แม้ข้อความส่วนใหญ่ปรากฏอยู่นาน 1-10วัน แต่มีข้อความหนึ่งปรากฏอยู่นานถึง 20 วัน ศาลจึงถือว่าเป็นเวลาที่จำเลยควรจะรู้ และลบข้อความที่เป็นปัญหานั้นได้ แต่ไม่ลบ จึงถือเป็นการการงดเว้นไม่ปฏิบัติหน้าที่ตามเวลาอันสมควร ถือเป็น “การยินยอม

โดยปริยาย” ให้มีการนำเข้าข้อมูลที่มีความผิดเข้าสู่ระบบคอมพิวเตอร์ซึ่งเป็นความผิดตามมาตรา 15 ประกอบ 14 พ.ร.บ. คอมพิวเตอร์ ฯ 2550 จริง[22]

อย่างไรก็ตาม คดีดังกล่าวคณะผู้วิจัยเห็นว่ามีความน่าสนใจยิ่งอย่างน้อยสองประเด็น ประเด็นแรก คือ แม้ศาลในคดีนี้จะยอมรับว่าปัจจุบันประเทศไทยยังไม่มีข้อกำหนดที่ชัดเจนเป็นลายลักษณ์อักษรในเรื่อง “ระยะเวลา” ที่ผู้ให้บริการต้องดำเนินการลบข้อความเมื่อได้รับแจ้ง (Notice & Takedown) ซึ่งแตกต่างจากประเทศอื่นหลายประเทศ และแม้ข้อเท็จจริงจะปรากฏว่ามีเพียงข้อความเดียวเท่านั้นที่ปรากฏอยู่ 20 วัน แล้วจำเลยจึงลบ (ข้อความอื่นๆ จำเลยลบภายในระยะเวลา 1-3 วัน หรืออย่างมาก 10 วัน) ศาลก็ยังใช้ดุลพินิจพิพากษา “ในทางที่เป็นโทษ” แก่จำเลยว่าเป็นระยะเวลาที่ “นานเกินสมควร” ส่วนอีกประเด็นหนึ่งที่สืบเนื่องกันก็คือ ศาลใช้ระยะเวลา 20 วันดังกล่าวมาเป็นเหตุผลสำคัญเพื่อถือ “โดยปริยาย” ว่าจำเลย “ยินยอม” ให้มีการนำเข้าสู่ข้อความที่เป็นความผิด เช่นนี้จึงเท่ากับว่าแม้โจทก์ไม่สามารถพิสูจน์ให้ศาลเห็นได้อย่างชัดเจน “จนสิ้นสงสัย” ว่าจำเลย “จงใจ” สนับสนุนหรือยินยอมให้ผู้อื่นกระทำความผิดจริง แต่ศาลก็ยังพิพากษาลงโทษจำเลย ดังนั้น ด้วยประเด็นทั้งสองนี้เอง จึงอาจก่อให้เกิดคำถามได้เช่นกันว่า คำพิพากษาคดีนี้มีความชอบธรรม หรือเป็นไปตาม “หลักประกันในทางกฎหมายอาญา” หรือไม่ อย่างไร

3) การบังคับใช้มาตรา 14 (4) กับความผิดที่เกี่ยวกับการเผยแพร่ข้อมูลอันลามก

“มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ...

(4) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้”

ความสามารถในการปิดบังตัวตน ประกอบกับความสามารถของ

เทคโนโลยีการสื่อสารทางอินเทอร์เน็ตที่รวดเร็วและเข้าถึงง่าย เป็นปัจจัยที่เอื้อให้อินเทอร์เน็ตกลายเป็นแหล่งสำคัญในการเผยแพร่ภาพวาบหวิวโป๊เปลือย ซึ่งอาจถูกตีความว่าผิดกฎหมายว่าด้วยการแพร่ภาพลามกอนาจาร แต่ฐานความผิดว่าด้วยการเผยแพร่ภาพลามกปรากฏอยู่ในประมวลกฎหมายอาญามาตรา 287[23] อยู่แล้ว แต่ฝ่ายผู้ร่างกฎหมายเห็นว่า ควรนำเรื่องนี้มากำหนดไว้ให้ชัดเจนในกฎหมายคอมพิวเตอร์ด้วย เพื่อป้องกันปัญหาการใช้การตีความจึงปรากฏเป็นมาตรา 14 (4) พ.ร.บ.คอมพิวเตอร์ฯ 2550 อย่างไรก็ตาม ที่ผ่านมา มาตรานี้ถูกใช้ไปเพื่อการขอคำสั่งศาลปิดกั้นเว็บไซต์มากกว่า สำหรับการดำเนินคดีนั้น พบว่ามีคดีตามมาตรา 14 (4) ทั้งสิ้นเพียง 22 คดี โดยเป็นคดีที่ศาลพิพากษาแล้ว 18 คดี ซึ่งพบว่า นอกจากหนึ่งคดีที่คณะผู้วิจัยไม่สามารถเข้าถึงผลการพิจารณาได้ 17 คดีที่เหลือล้วนเป็นคดีที่จำเลยรับสารภาพทั้งสิ้น ที่มาของคดีความเหล่านี้ มีทั้งคดีที่ฟ้องร้องโดยเจ้าหน้าที่รัฐ และโดยผู้เสียหายเองซึ่งถูกนำภาพของตนไปเผยแพร่ โดยในกรณีหลังมีจำนวนมากกว่า ทั้งนี้การตั้งข้อหามักใช้มาตรา 14 (4) ควบคู่ไปกับการใช้มาตรา 287 ประมวลกฎหมายอาญา นอกจากนี้ หลายคดียังใช้มาตรา 326 และ 328 ประมวลกฎหมายอาญา หรือความผิดฐานหมิ่นประมาทร่วมกันไปด้วย

<u>ตัวอย่างคดีตามมาตรา 14 (4)</u> คดีที่ตั้งข้อหาตามมาตรา 14 (4) จากทั้งหมด 22 คดีนั้น พบว่ามี 5 คดีที่เป็นการดำเนินคดีกับ “ผู้ให้บริการ” ซึ่ง “ทุกคดี” ผู้ให้บริการรับสารภาพ ส่งผลให้ศาลพิพากษาจำคุกโดยรอลงอาญาไว้ก่อน และทำนองเดียวกันกับกรณีคดีของผู้อำนวยการเว็บไซต์ประชาไท เพราะไม่ปรากฏข้อมูลที่ชี้ชัดว่า หลังจากผู้เสียหายดำเนินคดีกับผู้ให้บริการจนศาลพิพากษาตัดสินลงโทษแล้ว ทางฝ่ายรัฐได้มีความพยายามในการดำเนินคดีกับผู้ใช้บริการซึ่งเป็นตัวการ หรือเป็นผู้นำภาพลามกอนาจารดังกล่าวเข้าสู่ระบบคอมพิวเตอร์ด้วยหรือไม่ ตัวอย่างคดีหนึ่ง คือ จำเลยเป็นผู้ให้บริการฟรีเว็บบอร์ดชื่อ 212cafe ซึ่งเปิดให้คนทั่วไปสร้างเว็บบอร์ดของตัวเองได้ ปรากฏว่ามีผู้นำภาพเปลือยของผู้เสียหายไปเผยแพร่บนเว็บบอร์ดใน 212cafe ผู้เสียหายจึงแจ้งความร้องทุกข์กับเจ้าหน้าที่ตำรวจ

เจ้าหน้าที่ตำรวจได้ทำการประสานไปยังเจ้าของเว็บ 212cafe ในฐานะผู้ให้บริการเพื่อแจ้งให้นำภาพเหล่านั้นออกจากเว็บบอร์ด แต่เนื่องจากช่วงเวลาที่เจ้าหน้าที่ตำรวจประสานงานไปนั้น จำเลยไม่อยู่บ้าน เจ้าหน้าที่จึงไม่สามารถติดต่อผู้ให้บริการได้ ในที่สุดตำรวจจึงนำกำลังเข้าจับกุมผู้ให้บริการที่บ้าน โดยตั้งข้อหาว่า "จงใจสนับสนุนหรือยินยอม" ให้มีการนำเข้าข้อความหรือภาพลามกสู่ระบบคอมพิวเตอร์ (มาตรา 14 (4) ประกอบ 15 พ.ร.บ. คอมพิวเตอร์ฯ 2550) คดีนี้มีความน่าสนใจตรงที่ว่า การที่เจ้าหน้าที่รัฐไม่สามารถติดต่อผู้ให้บริการได้ (ไม่ว่าด้วยเหตุผลใดๆ) ผู้ให้บริการนั้นก็อาจถูกฟ้องคดีให้ต้องรับผิดแล้วตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550

อนึ่ง ยังมิพักต้องกล่าวว่าในที่สุดแล้วศาลจะมีคำพิพากษาคดีลักษณะนี้ว่าอย่างไร แต่เมื่อถูกดำเนินคดีซึ่งเป็นผลพวงมาจากการกระทำของผู้อื่น ผู้ให้บริการดังกล่าวย่อมได้รับความเดือดร้อนจากการต้องต่อสู้คดีแล้ว ข้อที่ต้องพิจารณาก็คือ เมื่อพิจารณาจากขนาดของการประกอบกิจการ เจ้าของเว็บไซต์ 212cafe เป็นเพียงผู้ประกอบการรายเล็กที่เขียนระบบเว็บบอร์ดเพื่อให้บริการฟรีแก่บุคคลทั่วไป (ซึ่งปัจจุบันมีผู้ให้บริการลักษณะนี้จำนวนมาก) ดังนั้น ความสามารถทั้งในแง่ของงบประมาณ และบุคลากรในการตรวจตราดูแลเนื้อหาในบริการของตน จึงย่อมมีไม่เท่ากับผู้ให้บริการรายใหญ่ การสร้างภาระความรับผิดให้แก่ผู้ให้บริการทุกๆ ประเภท ซึ่งเป็นเพียงตัวกลางส่งผ่านข้อมูลในสื่อออนไลน์ จึงย่อมส่งผลกระทบต่อแรงจูงใจในการประกอบการ รวมทั้งสร้างบรรยากาศแห่งความกลัวให้เกิดขึ้นในหมู่ผู้ประกอบการ โดยเฉพาะอย่างยิ่งผู้ประกอบการรายย่อย และเงื่อนไขต่างๆ เหล่านี้เองที่จะทำให้โอกาสในการสื่อสารอย่างมีเสรีภาพในสื่อออนไลน์ต้องลดน้อยลง

สรุปผลการศึกษาผลกระทบเชิงปริมาณ

กล่าวได้ว่าระยะเวลาตั้งแต่เดือนกรกฎาคม 2550 ถึงธันวาคม 2554 รวม 4 ปี 6 เดือนนั้น พ.ร.บ.คอมพิวเตอร์ฯ 2550 ถูกใช้ไปกับการจัด

ระเบียบ “เนื้อหา” ในสื่อออนไลน์มากกว่าการใช้เพื่อแก้ปัญหาอาชญากรรมคอมพิวเตอร์โดยแท้ หรืออาชญากรรมที่กระทำต่อตัวข้อมูลหรือระบบคอมพิวเตอร์โดยตรง ตามมาตรา 5 ถึงมาตรา 13 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งเป็นเจตนารมณ์แรกเริ่มของกฎหมายฉบับนี้

พ.ร.บ.คอมพิวเตอร์ฯ 2550 ถูกใช้เพื่อปิดกั้นการเข้าถึงเว็บไซต์รวม 81,213 ยูอาร์แอล โดยส่วนใหญ่มีสาเหตุมาจากมีเนื้อหาหมิ่นประมาทพระมหากษัตริย์ พระราชินี และรัชทายาท ภาพลามกอนาจาร และเหตุผลอื่นๆ ตามลำดับ โดยมีข้อสังเกตว่าสถิติการปิดเว็บไซต์มีลักษณะแปรผันตามสถานการณ์ความขัดแย้งทางการเมือง

หากพิจารณามาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งเป็นบทให้อำนาจรัฐในการปิดกั้นเว็บไซต์ จะเห็นได้ว่า แม้มาตรานี้จะยังมีปัญหาความคลุมเครือไม่ชัดเจนของตัวบทบัญญัติเองปรากฏอยู่ แต่โดยกระบวนการการใช้อำนาจแล้ว มาตรา 20 ถูกออกแบบโดยมีระบบป้องกันการใช้อำนาจของเจ้าหน้าที่รัฐโดยพลการ เนื่องจากทุกครั้ง ก่อนปิดกั้นเว็บไซต์พนักงานเจ้าหน้าที่จะต้องร้องขอไปยังศาลเพื่อให้ศาลช่วยพิจารณาเนื้อหาและออกคำสั่ง อย่างไรก็ตาม จากสถิติการปิดเว็บไซต์ตามคำสั่งศาลในช่วงเวลาไม่กี่ปีของการบังคับใช้กฎหมายฉบับนี้ ย่อมทำให้กลไกการตรวจสอบกลั่นกรองโดยองค์กรตุลาการหรือศาลดังกล่าวถูกตั้งคำถามได้ว่า มีประสิทธิภาพ และมีความยุติธรรมกับเจ้าของเว็บไซต์ผู้ได้รับผลกระทบ และกับประชาชนผู้บริโภคสื่อออนไลน์เพียงพอหรือไม่ เพราะในช่วงเวลาที่ผ่านมา เว็บไซต์ที่รัฐบาลต้องการปิดกั้นมีจำนวนมากเฉลี่ยถึงวันละ 392 ยูอาร์แอล คงต้องถือเป็นเรื่องยากลำบากอย่างยิ่ง หรือแทบเป็นไปไม่ได้เลยที่องค์คณะผู้พิพากษาจะมีเวลาวินิจฉัยเนื้อหาของเว็บไซต์เหล่านั้นอย่างละเอียดรอบคอบ เพื่อออกคำสั่งอนุญาตปิดกั้นได้ภายในวันเดียว

นอกจากนี้ จากผลการวิจัยย่อมเห็นได้ว่า แม้ในที่สุดแล้วประเทศไทยจะไม่มี พ.ร.บ.คอมพิวเตอร์ฯ 2550 แต่รัฐก็ยังคงมีมาตรการอื่นๆ สำหรับใช้ปิดกั้นการเข้าถึงเว็บไซต์ได้ ทั้งนี้ไม่ว่าจะเป็นการใช้อำนาจตาม พ.ร.ก.การบริหารราชการในสถานการณ์ฉุกเฉินและตามกฎหมายว่า

ด้วยความมั่นคงฉบับอื่น หรือการขอความร่วมมือจากผู้ให้บริการ ซึ่งทั้งสองวิธีดังกล่าวเป็นกรณีที่รัฐโดยเจ้าหน้าที่รัฐผู้บังคับใช้กฎหมายสามารถสั่งการไปยังผู้ให้บริการได้โดยตรงโดยไม่จำเป็นต้องผ่านกระบวนการตรวจสอบการใช้อำนาจจากศาลก่อน และ ปัจจุบันประเทศไทยก็ยังไม่มีกฎเกณฑ์หรือแนวปฏิบัติที่ชัดเจนในเรื่อง “ระยะเวลา” ของการแจ้งเตือนเนื้อหาที่อาจเข้าข่ายผิดกฎหมายเพื่อให้ผู้ให้บริการดำเนินการกับเนื้อหาเหล่านั้น รวมทั้ง “ระยะเวลา” ในการปิดกั้นเว็บไซต์ ไม่มีการบันทึกหลักฐานการใช้อำนาจกระทั่งไม่มีบทบังคับให้เจ้าหน้าที่รัฐต้องแสดงเหตุผลของการใช้อำนาจเหล่านั้นต่อผู้ได้รับผลกระทบโดยตรง

ในแง่ของการใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 เพื่อดำเนินคดีกับบุคคลนั้น พบว่า ตลอดระยะเวลากว่า 4 ปีของการใช้กฎหมาย คดีความมากกว่าครึ่งหนึ่งเป็นเรื่องของการเผยแพร่เนื้อหาในสื่อออนไลน์ กล่าวคือ ร้อยละ 66.15 ขณะที่การดำเนินคดีอาชญากรรมคอมพิวเตอร์โดยแท้ที่มีเพียงร้อยละ 19 ของจำนวนคดีทั้งหมดเท่านั้น

ประเภทของคดีที่พบมากที่สุดสามอันดับแรก คือ คดีหมิ่นประมาท คดีอาชญากรรมคอมพิวเตอร์โดยแท้ และคดีหมิ่นประมาทกษัตริย์ฯ โดยมีข้อควรสังเกตว่า ทั้งคดีหมิ่นประมาท และคดีอาชญากรรมคอมพิวเตอร์ เป็นคดีที่ร้องทุกข์กล่าวโทษโดยประชาชนหรือเอกชน ในขณะที่คดีหมิ่นประมาทกษัตริย์ฯ เป็นการร้องทุกข์โดยรัฐ คือ กระทรวงไอซีที ดีเอสไอ และกองบังคับการปราบปราม

ดังที่กล่าวไปแล้วว่า เจตนารมณ์เริ่มแรกของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 คือ มุ่งแก้ปัญหาอาชญากรรมคอมพิวเตอร์โดยแท้ ซึ่งไม่สามารถอาศัยการตีความบทบัญญัติในประมวลกฎหมายอาญามาบังคับใช้ได้เพราะมีองค์ประกอบความผิดแตกต่างกัน แต่ในทางปฏิบัติพระราชบัญญัติฉบับนี้กลับถูกนำมาใช้จัดการเนื้อหาที่เผยแพร่ในสื่ออินเทอร์เน็ต ซึ่งย่อมส่งผลกระทบโดยตรงต่อสิทธิและเสรีภาพของประชาชน มาตราที่ถูกนำมาใช้ฟ้องร้องอย่างมากคือ มาตรา 14 ที่ในทางการนิติบัญญัติ หรือการบัญญัติกฎหมายแล้วถือว่ามีเนื้อหาสาระทับซ้อนกับความผิดตามที่กำหนดไว้ใน

ประมวลกฎหมายอาญา จะแตกต่างกันก็เพียงแต่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 กำหนดโทษไว้รุนแรงกว่า ส่งผลให้ทั้งความผิดฐานหมิ่นประมาท การเผยแพร่ข้อความหรือภาพลามก เป็นความผิดที่มีโทษสูงกว่าที่กำหนดไว้ในประมวลกฎหมายอาญา หรือทำให้การกระทำความผิดบางอย่าง โดยเฉพาะอย่างยิ่งความผิดในฐานหมิ่นประมาทบุคคลอื่น กลายเป็นความผิดอาญาแผ่นดิน ที่ใครก็ได้สามารถกล่าวโทษกับเจ้าพนักงานได้ การบัญญัติกฎหมายที่ซ้ำซ้อนเช่นนี้ อย่างน้อยที่สุดย่อมทำให้เกิดความสับสนต่อทั้งประชาชน และเจ้าหน้าที่ผู้บังคับใช้กฎหมาย จนส่งผลให้การใช้การตีความผิดพลาดคลาดเคลื่อนไปจากเจตนารมณ์ของกฎหมายได้

นอกจากมาตรา 14 แล้ว พ.ร.บ.คอมพิวเตอร์ฯ 2550 ยังมีบทบัญญัติอื่นๆ ที่ส่งผลกับเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นของประชาชนด้วย โดยเฉพาะอย่างยิ่งมาตรา 15 ที่รัฐมุ่งเอาผิดกับตัวกลางผู้ให้บริการ โดยไม่พยายามทำความเข้าใจลักษณะ จำนวน และธรรมชาติของการไหลเวียนข้อมูลในสื่อออนไลน์ ที่ผู้ให้บริการไม่สามารถตรวจสอบข้อมูลเหล่านั้นได้ทั้งหมด ก่อให้เกิดสภาวการณ์ที่เรียกว่า “สื่อเซ็นเซอร์ตัวเอง” ไม่กล้านำเสนอข่าวสาร ไม่ยอมให้ผู้ใช้บริการแสดงความคิดเห็นต่อสถานการณ์ใดสถานการณ์หนึ่งได้โดยอิสระ กระทั่งบางครั้งมีการตัดทอนหรือบิดเบือนข่าวสารเพื่อไม่ให้หมิ่นเหม่ หรือทำให้ตนต้องเกิดความรับผิด นอกจากนี้ คณะผู้วิจัยยังพบปัญหาสำคัญอีกประการหนึ่งว่า หลายคดีที่ผู้ให้บริการเป็นจำเลย เป็นกรณีที่เจ้าพนักงานรัฐไม่สามารถสืบหาหรือไม่พยายามสืบหาตัวผู้กระทำผิดที่แท้จริงมาลงโทษให้ได้เสียก่อน (ซึ่งเป็นเรื่องที่อาจต้องใช้เวลา ความสามารถทางเทคนิค และมีความซับซ้อนยุ่งยากกว่า) แต่กลับมุ่งเป้าหมายมาดำเนินคดีกับเจ้าของเว็บไซต์ หรือผู้ให้บริการอินเทอร์เน็ตแทน ซึ่งย่อมไม่เป็นไปตามเจตนารมณ์ของกฎหมายฉบับนี้เช่นกัน

2. การศึกษาผลกระทบเชิงคุณภาพ

นอกจากผลการศึกษาและบทวิเคราะห์ที่พิจารณาจากสถิติการปิดกั้นเว็บไซต์ และจำนวนคดีความที่เกิดขึ้นในรอบ 4 ปี 6 เดือน ซึ่งเป็นการวิจัยเชิงปริมาณแล้ว เพื่อให้งานวิจัยฉบับนี้มีความสมบูรณ์ และครบถ้วนรอบด้าน คณะผู้วิจัยจึงได้ทำการเก็บข้อมูลความคิดเห็นจากบุคลากรในองค์กรต่างๆ ที่เกี่ยวข้องกับการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ด้วย โดยใช้วิธีการสัมภาษณ์เชิงลึก (In-depth interview) และการจัดสนทนากลุ่มย่อย (Focus Group)

ผลการศึกษาที่ได้จากการเก็บรวบรวมข้อมูล แบ่งออกเป็น 3 ส่วนคือ

2.1 บทบาทของหน่วยงานภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายและนโยบาย ที่กระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชน

2.2 บทบาทการดำเนินงานของผู้ประกอบการอินเทอร์เน็ต ภายใต้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่กระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชน

2.3 บทบาทของเว็บมาสเตอร์และผู้ดูแลเว็บบอร์ดต่างๆ ภายใต้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่กระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชน

2.1 บทบาทของหน่วยงานภาครัฐ ที่เกี่ยวข้องกับการบังคับใช้กฎหมายและนโยบาย ที่กระทบต่อสิทธิเสรีภาพในการแสดงความคิดเห็นของประชาชน

วิธีศึกษา

การศึกษาส่วนนี้ใช้วิธีการสัมภาษณ์เชิงลึกเจ้าหน้าที่รัฐที่มี

ประสบการณ์ และเป็นผู้บังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 โดยใช้วิธีสุ่มตัวอย่าง และเพื่อให้ได้บุคลากรที่สามารถให้ข้อมูลได้จริง คณะผู้วิจัยยังได้ขอคำแนะนำจากบุคคลอื่นๆ เพื่อติดต่อขอสัมภาษณ์บุคลากรในหน่วยงาน รวมทั้งสิ้น 7 คน ได้แก่

1. เจ้าหน้าที่ (ขอสงวนนาม) สำนักกำกับการใช้เทคโลยีและสารสนเทศ (ปัจจุบันเปลี่ยนชื่อเป็น สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

2. พนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 (ขอสงวนนาม) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

3. เจ้าหน้าที่ตำรวจระดับสูง (ขอสงวนนาม) กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี (ปอท.)

4. พ.ต.อ.ศิริพงษ์ ติมุลา รองผู้บัญชาการ กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี (ปอท.)

5. นายเกริกไชย ศรีศุกร์เจริญ พนักงานสอบสวนคดีพิเศษชำนาญการพิเศษ สำนักคดีเทคโนโลยีสารสนเทศ กรมสอบสวนคดีพิเศษ (ดีเอสไอ)

6. พ.ต.อ.อนุชิต บุญญะปฏิภาค กลุ่มงานตรวจพิสูจน์หลักฐานอาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง

7. เจ้าหน้าที่ตำรวจผู้เชี่ยวชาญเทคโนโลยี (ขอสงวนนาม) สำนักงานตำรวจแห่งชาติ

สัมภาษณ์โดย นางสาวสาวตรี สุขศรี และนางสาวอรพิณ ยิ่งยงพัฒนา นักวิจัย นายดนุช วัลลิกุล นายยิ่งชีพ อัชฌานนท์ นายธนกฤต เปี่ยมมงคล และนางสาวอัชฌา สงฆ์เจริญ คณะผู้ช่วยนักวิจัย การสัมภาษณ์เริ่มต้นจากการนัดหมายทางโทรศัพท์เพื่อขอนัดพบ ส่งจดหมายเพื่อขอสัมภาษณ์ เก็บข้อมูลขณะสัมภาษณ์ด้วยการบันทึกเสียงและจดบันทึก อย่างไรก็ตาม การบันทึกเสียงจะใช้เฉพาะกรณีที่ได้รับความยินยอมจากแหล่งข้อมูลเท่านั้น ก่อนการสัมภาษณ์ได้ตกลงเงื่อนไขการระบุชื่อ และเอกลักษณ์ของแหล่งข้อมูล แหล่งข้อมูลมีอิสระตลอดการสัมภาษณ์ในการขอให้คณะผู้วิจัย

ปกปิดเอกลักษณ์เพียงบางส่วนหรือตลอดการสัมภาษณ์ได้ การสัมภาษณ์จะใช้วิธีสนทนาแลกเปลี่ยน และสลับกับการถามคำถาม ซึ่งคำถามและแนวทางการสัมภาษณ์เป็นไปตามวัตถุประสงค์ของงานวิจัย มีโครงสร้างการสัมภาษณ์ดังนี้

1) แนะนำตัว

คณะวิจัยแนะนำตัว แนะนำโครงการ วัตถุประสงค์ และวัตถุประสงค์ของการสัมภาษณ์

2) สอบถามรายละเอียดเบื้องต้น

ชื่อ สกุล ตำแหน่งงาน อายุงาน อำนาจหน้าที่ และหน้าที่ในส่วนที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ฯ 2550

3) คำถาม

ข้อมูลทั่วไป

• วัตถุประสงค์ อำนาจหน้าที่ของหน่วยงาน ในส่วนที่เกี่ยวกับการติดต่อสื่อสารในสื่อออนไลน์

• ความเกี่ยวข้องของงานของผู้ให้สัมภาษณ์ตามวัตถุประสงค์ของหน่วยงาน กับ พ.ร.บ.คอมพิวเตอร์ฯ 2550

ประสบการณ์การบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

• ขั้นตอนและกระบวนการรับแจ้งหรือรับเรื่อง เมื่อมีข้อเท็จจริงที่เกิดการกระทำที่ (น่าจะ) เป็นความผิด

• ลักษณะการกระทำความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ที่พบส่วนใหญ่

• รายละเอียดการทำงานในขอบเขตงานอื่นๆ ที่นอกเหนือจากการรับเรื่องร้องเรียน และการสอบสวนคดี เช่น คำสั่งหรือปฏิบัติการอื่นใดอย่างการปิดกั้นเว็บไซต์ การตรวจตราเนื้อหาบนอินเทอร์เน็ต การขอความร่วมมือจากผู้ให้บริการอินเทอร์เน็ต ฯลฯ

• ขั้นตอนการทำงานในการแสวงหาและรวบรวมพยานหลักฐาน

อำนาจหน้าที่ที่ใช้ และอุปสรรคที่พบทั้งในตัวบทกฎหมาย ทางเทคนิค วิธีการ หรือข้อเท็จจริงอื่นๆ

ปัญหาอุปสรรค ต่อการทำงานภายใต้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

• ความสะดวกในการใช้อำนาจภายใต้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

• ความรัดกุมและการตีความบทบัญญัติมาตราต่างๆ ใน พ.ร.บ.คอมพิวเตอร์ฯ 2550

• แรงกดดันจากปัญหาทางการเมือง/หน่วยงานอื่นๆ ที่กระทบต่อเสรีภาพของประชาชน

ความคิดเห็น และข้อเสนอแนะต่อ พ.ร.บ.คอมพิวเตอร์ฯ 2550

• ความเหมาะสม สอดคล้อง ระหว่าง หลักการและเหตุผล รวมทั้งมาตรการและบทบัญญัติต่างๆ ใน พ.ร.บ.คอมพิวเตอร์ฯ 2550 กับยุคสมัยเทคโนโลยีสารสนเทศ

• ข้อเสนอเพิ่มเติมเพื่อแก้ไข พ.ร.บ.คอมพิวเตอร์ฯ 2550

• จุดสมดุลในการทำงานระหว่าง “การป้องกันและปราบปรามการกระทำความผิด” กับ “การคุ้มครองเสรีภาพในการแสดงความคิดเห็น และการรับรู้ข้อมูลข่าวสารของประชาชน”

• ทัศนคติของเจ้าหน้าที่รัฐต่อการเกิดขึ้นของสื่อใหม่/สื่อพลเมือง หรือพื้นที่ใหม่ในการแสดงความคิดเห็นที่หลากหลาย

•ข้อเสนอแนะเพิ่มเติม ทั้งในส่วนของกฎหมาย (พ.ร.บ.คอมพิวเตอร์ฯ 2550 หรือกฎหมายอื่นๆ) นโยบายที่เกี่ยวกับ “สื่อออนไลน์” ของฝ่ายรัฐ รวมทั้งข้อเสนอแนะต่อประชาชนผู้ใช้บริการสื่อสารออนไลน์

ผลการศึกษา

จากการสัมภาษณ์แหล่งข้อมูลทั้ง 7 คน สามารถประมวลผลโดย

แบ่งหมวดหมู่ดังนี้

1. อำนาจหน้าที่ และขั้นตอนการทำงานของเจ้าหน้าที่รัฐในส่วนที่เกี่ยวข้องกับการใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

2. ปัญหาที่เกิดขึ้นจากตัวบทบัญญัติ และการบังคับใช้ พ.ร.บ. คอมพิวเตอร์ฯ 2550 ในส่วนที่เกี่ยวกับเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นของประชาชน

3. ความคิดเห็นและข้อเสนอแนะเพิ่มเติมเกี่ยวกับการแก้ไขและการใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

1) อำนาจหน้าที่ และขั้นตอนการทำงานของเจ้าหน้าที่รัฐ ในส่วนที่เกี่ยวข้องกับการใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

(1) อำนาจหน้าที่ และขั้นตอนการทำงานที่เกี่ยวกับ พ.ร.บ. คอมพิวเตอร์ฯ 2550

ปัจจุบันมีหน่วยงานภาครัฐที่รับผิดชอบงานที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์เป็นหลัก สามหน่วยงานด้วยกัน คือ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) สำนักงานตำรวจแห่งชาติ และกรมสอบสวนคดีพิเศษ (ดีเอสไอ)

“กระทรวงไอซีที” เป็นหน่วยงานที่มีอำนาจโดยตรงในการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 โดยภายในกระทรวงมีส่วนราชการชื่อว่า “สำนักกำกับดูแลการใช้เทคโนโลยีสารสนเทศและการสื่อสาร” ทำหน้าที่เป็นหน่วยสนับสนุน และทำงานร่วมกับเจ้าหน้าที่สืบสวนสอบสวน เช่น การปิดเว็บไซต์ การขอข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้ กระทรวงไอซีทีจะเป็นผู้รับเรื่องร้องเรียนจากประชาชน นอกจากนี้ ก็ให้การสนับสนุนหน่วยงานต่างๆ ด้านความรู้ในการดำเนินคดีเกี่ยวกับเทคโนโลยีและอินเทอร์เน็ต รวมถึงช่วยสืบหาตัวผู้กระทำความผิดก่อนมีการดำเนินคดี จากนั้นจึงส่งเรื่องไปให้เจ้าหน้าที่ตำรวจ (พนักงานเจ้าหน้าที่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 (ขอสงวนนาม), 2553)

นอกจากนี้ กระทรวงไอซีทียังจัดอบรมพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 เพื่อให้ความรู้เรื่อง พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งพนักงานเจ้าหน้าที่จะถูกส่งตัวไปทำงานร่วมกับเจ้าหน้าที่ตำรวจเพื่อเรียนรู้เทคนิคการสืบสวนสอบสวน และเรียนรู้บทบาทหน้าที่ตามอำนาจของพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 (พนักงานเจ้าหน้าที่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 (ขอสงวนนาม), 2553)

"สำนักงานตำรวจแห่งชาติ" มีทั้งส่วนงานปราบปราม งานสนับสนุน และกองพิสูจน์หลักฐาน ด้วยลักษณะเฉพาะของคดีที่ต้องการความสามารถเฉพาะทาง ทำให้ช่วง 1-2 ปีแรกของการประกาศใช้กฎหมายคดี พ.ร.บ.คอมพิวเตอร์ฯ 2550 จำนวนหนึ่งจึงอยู่ในความรับผิดชอบของราชการส่วนกลาง คือ กองบังคับการปราบปราม แต่ในช่วงแรกไม่ได้มีแผนกที่ตั้งขึ้นเพื่อดูแลคดีอาชญากรรมคอมพิวเตอร์โดยเฉพาะ แต่คดีจะถูกจัดให้อยู่ในความรับผิดชอบของกองบังคับการปราบปรามการกระทำผิดต่อเด็กและสตรี (บก.ปดส.) และกองบังคับการปราบปรามอาชญากรรมทางเศรษฐกิจและเทคโนโลยี (บก.ปศท.)[24] นอกจากนี้ ยังมีการจัดแฟ้มคดีหมิ่นประมาทกษัตริย์ฯ แยกเป็นคดีสำคัญในความดูแลของกองบังคับการปราบปรามด้วย ซึ่งส่วนหนึ่งเป็นคดีที่ฟ้องด้วย พ.ร.บ.คอมพิวเตอร์ฯ 2550

สำหรับส่วนงานสนับสนุน สำนักงานตำรวจแห่งชาติมีศูนย์ตรวจสอบและวิเคราะห์การกระทำผิดทางเทคโนโลยี (ศตท.) เป็นทีมงานขนาดเล็กที่มีเจ้าหน้าที่ 2-3 นายทำงานเชิงวิชาการ เพื่อให้ความรู้ประสานงานตรวจพิสูจน์หลักฐาน รวมถึงเบิกความในชั้นศาล แต่ไม่ได้ทำงานภาคปฏิบัติอย่างการจับกุมและปราบปรามการกระทำความผิด ทั้งนี้ หน่วยงานดังกล่าวปรับเปลี่ยนชื่อหลายครั้ง ชื่อเดิม คือ **"ศูนย์ตรวจสอบและวิเคราะห์การกระทำผิดทางเทคโนโลยี ภายใต้สำนักงานตำรวจแห่งชาติ"** จนเมื่อปี 2546-2547 สถานการณ์อาชญากรรมคอมพิวเตอร์รุนแรงขึ้น สถานทูตสหรัฐอเมริกาได้ให้การสนับสนุนทั้งอุปกรณ์และงบประมาณให้ตำรวจตั้งศูนย์เฉพาะกิจเพื่อปราบปรามอาชญากรรมทางเทคโนโลยี จึงได้ตั้งหน่วย คือ **"กองบังคับการศูนย์ตรวจสอบและวิเคราะห์การกระ**

ทำผิดทางเทคโนโลยี" หรือ ศตท. อยู่ในโครงสร้างของสำนักงานตำรวจแห่งชาติ แต่สังกัดสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร ของส่วนกลางสำนักงานตำรวจแห่งชาติ ศตท. มีอำนาจสืบสวนและวิเคราะห์ข้อมูลเกี่ยวกับอาชญากรรมคอมพิวเตอร์ สนับสนุนหน่วยปฏิบัติ อย่างไรก็ดี ศูนย์นี้ไม่มีอำนาจสอบสวน จึงทำให้การทำงานไม่จบในหน่วยงานเดียวทำให้ล่าช้า สุดท้ายจึงมีการปรับโครงสร้างให้เกิดหน่วยงานที่มีอำนาจสอบสวนโดยตรงด้วย

เดือนกันยายน ปี 2552 เกิด **"กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี (ปอท.)"** สังกัดกองบัญชาการตำรวจสอบสวนกลางโดยมีพระราชกฤษฎีกาแบ่งส่วนราชการ และกฎกระทรวงให้อำนาจไว้[25] ออกตามความในพระราชกฤษฎีกาเพื่อแบ่งอำนาจหน้าที่ในการทำงาน ซึ่งออกแบบให้มีอำนาจหน้าที่ต่างกัน เช่น กองกำกับการ 1 มีอำนาจหน้าที่เกี่ยวกับคดีที่มีคอมพิวเตอร์เป็นเป้าหมาย กองกำกับการ 2 สืบสวนคดีที่คนร้ายใช้คอมพิวเตอร์เป็นเครื่องมือ กองกำกับการ 3 คดีตามที่มีการนำข้อมูลอันเลวร้ายเข้าสู่คอมพิวเตอร์ กลุ่มงานสนับสนุนคดีเทคโนโลยีก็จะเป็นส่วนงานนิติคอมพิวเตอร์ เป็นหน่วยเทคนิคสนับสนุนกอง 1, 2, 3 ทำหน้าที่ตรวจพิสูจน์ ตรวจสถานที่เกิดเหตุ สืบสวนสอบสวนทางเทคนิค หลังจากตั้ง ปอท. เจ้าหน้าที่ส่วนใหญ่ของ ศตท. จึงย้ายมาสังกัดที่ ปอท. อย่างไรก็ดี ศตท.ยังคงดำเนินงานอยู่จนถึงปัจจุบัน เพียงแต่ลดภารกิจเป็นงานสนับสนุน ทำงานเชิงวิชาการ อบรมให้ความรู้ โดยมีสถานะในระดับกองกำกับการ (พ.ต.อ.ศิริพงษ์ ติมุลา รอง ผบก.ปอท., 2554)

กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี (ปอท.) จำแนกหมวดหมู่ของคดีไว้สามหมวดใหญ่ คือ หนึ่ง ฉ้อโกง สอง แฮกเกอร์ และสาม Black Content ซึ่งได้แก่ เว็บโป๊ เว็บพนัน และเว็บหมิ่นสถาบันฯ (เจ้าหน้าที่ตำรวจระดับสูง (ขอสงวนนาม) ปอท., 2554)

แม้จะมีหน่วยงานที่ตั้งขึ้นโดยมีหน้าที่และความเชี่ยวชาญเฉพาะทางเกี่ยวกับคดีทางเทคโนโลยี แต่กฎหมายไม่ได้ห้ามหน่วยงานอื่นทำคดีเทคโนโลยี ดังนั้น ตำรวจนครบาล ตำรวจกองบังคับการปราบปราม

สามารถทำคดีได้เอง

อีกหน่วยงานหนึ่งที่มีความสำคัญคือ **"กองพิสูจน์หลักฐาน"** ทั้งนี้คดีที่เกี่ยวกับเทคโนโลยีที่กองพิสูจน์หลักฐานต้องทำหน้าที่ตรวจพยานหลักฐานมีมาตั้งแต่ก่อนประกาศใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 แล้ว จนกระทั่งหลังประกาศใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 จึงได้ตั้ง **"กลุ่มงานตรวจพิสูจน์หลักฐานอาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง"** ขึ้นเมื่อวันที่ 7 กันยายน 2552 ทำหน้าที่ตรวจพิสูจน์หลักฐาน รวมถึงให้การในชั้นศาล หน่วยงานนี้ถูกจัดตั้งขึ้นเพื่อให้ทำงานสอดคล้องกับหน่วยงานอื่นๆ เช่น ปอท. โดยกองพิสูจน์หลักฐานจะทำหน้าที่ตรวจพิสูจน์ในขั้นตอนสุดท้าย (พ.ต.อ.อนุชิต บุญญะปฏิภาค กลุ่มงานตรวจพิสูจน์หลักฐานอาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง, 2554)

สำหรับ **"กรมสอบสวนคดีพิเศษ"** นั้นมีสำนักคดีเทคโนโลยีและสารสนเทศที่รับผิดชอบคดีที่มีเทคโนโลยีเข้ามาเกี่ยวข้องโดยเฉพาะภายในสำนักฯ มีเจ้าหน้าที่สืบสวนสอบสวนราว 20 คน โดยดีเอสไอจะรับคดีจากสำนักข่าวกรองที่ส่งเรื่องเข้ามา รวมทั้งที่มาจากการร้องเรียนของประชาชน และมีทั้งคดีที่ดีเอสไอตรวจพบเองด้วย ทางดีเอสไอจะเป็นผู้วินิจฉัยว่าคดีใดที่จะให้ตำรวจรับผิดชอบ และคดีใดที่เข้าเงื่อนไขให้ดีเอสไอรับผิดชอบ นอกจากนี้ เนื่องจากดีเอสไอมีอำนาจสอบสวนพิเศษตาม พ.ร.บ.การสอบสวนคดีพิเศษ[26] จึงทำให้เจ้าหน้าที่ดีเอสไอมีอำนาจมากกว่าเจ้าหน้าที่ตำรวจซึ่งใช้อำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา (เกริกไชย ศรีศุกร์เจริญ พนักงานสอบสวนคดีพิเศษชำนาญการพิเศษ สำนักคดีเทคโนโลยีสารสนเทศ กรมสอบสวนคดีพิเศษ (ดีเอสไอ), 2554)

ลักษณะคดีที่เข้ามาในสำนักเทคโนโลยีสารสนเทศแบ่งออกเป็น 5 หมวด ได้แก่ คดีความมั่นคง ค้ามนุษย์ ฉ้อโกง การพนันออนไลน์ และคดีเกี่ยวกับการต่อเติมตัดแต่งรูปภาพข้อมูล ทั้งนี้ ความผิดฐานหมิ่นประมาทกษัตริย์ฯ จัดอยู่ในหมวดคดีความมั่นคง และเป็นประเภทคดีที่ถูกส่งมาดีเอสไอมากที่สุด เพราะรัฐบาลมอบหมายให้เป็นคดีพิเศษในความดูแลของดีเอสไอ ขณะที่คดีประเภทอื่นๆ เช่น คดีพนันออนไลน์ จะเลือกทำเป็นคดี

ยุทธศาสตร์เพียงเพื่อให้เกิดการศึกษาวิธีการและขั้นตอนในการดำเนินคดี (นายเกริกไชย ศรีศุกร์เจริญ พนักงานสอบสวนคดีพิเศษชำนาญการพิเศษ สำนักคดีเทคโนโลยีสารสนเทศ กรมสอบสวนคดีพิเศษ (ดีเอสไอ), 2554)

เมื่อวันที่ 19 ธันวาคม 2554 คณะรัฐมนตรีมีมติเห็นชอบให้เพิ่มประเภทคดีตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ให้เป็นคดีที่อยู่ในความรับผิดชอบของดีเอสไอ โดยให้กำหนดไว้เป็นคดีประเภทใหม่ในกฎกระทรวงว่าด้วยการกำหนดคดีพิเศษ และประกาศในราชกิจจานุเบกษาวันที่ 20 เมษายน 2555[27]

(2) การใช้มาตรการปิดกั้นเว็บไซต์

เจ้าหน้าที่กระทรวงไอซีที กล่าวว่า หน้าที่ที่ต้องทำในแต่ละวันมีสองอย่างคือ หนึ่ง ทำหน้าที่หาตัวผู้กระทำผิดในคดีต่างๆ ด้วยการตามหาไอพี และสอง ปิดกั้นเว็บไซต์ ซึ่งเมื่อมี พ.ร.บ.คอมพิวเตอร์ฯ 2550 แล้วทำให้การทำงานทั้งในส่วนของการปิดกั้นเว็บไซต์ และการดำเนินคดีมีความชัดเจนในอำนาจหน้าที่ยิ่งขึ้น อย่างไรก็ดี พบว่า แม้จะมีการปิดกั้นเว็บไซต์ด้วยเหตุผลที่มีเนื้อหาขัดต่อกฎหมาย แต่กลับไม่ค่อยมีการดำเนินคดีกับเว็บไซต์ที่ถูกปิดกั้นจริง

“ทางกระทรวงมีกลไกรับแจ้งเว็บไซต์ที่ไม่เหมาะสม ทั้งช่องทาง 1212 สายด่วนฮอตไลน์ 1111 คอลเซ็นเตอร์ ผ่านระบบอีเมล และแจ้งผ่านหน้าเว็บกระทรวง นอกจากนี้ยังมีหนังสือราชการจากหน่วยงานอื่นๆ ที่ส่งเข้ามาว่าพบเว็บไซต์ที่ไม่เหมาะสม และขอให้กระทรวงไอซีทีดำเนินการตามหน้าที่ก่อนมี พ.ร.บ.คอมพิวเตอร์ฯ 2550 หน่วยงานราชการที่ประสานงานให้พิจารณาปิดเว็บไซต์บ่อยที่สุด คือ กระทรวงวัฒนธรรม ซึ่งบางครั้งแจ้งให้พิจารณาเว็บไซต์ต่อครั้งเป็นจำนวนมากราว 3,000 ยูอาร์แอล อย่างนี้ไอซีทีก็ตาย หรืออยากจะบ้า ให้พิจารณาแล้วจะพิจารณาอะไร บรรทัดฐานแต่ละคนไม่เท่ากัน คือ ถ้าเราเล่นบ่อยๆ เราจะรู้สึกธรรมดา ช่วงนั้นกระทรวงไอซีทีจะโดนกระทรวงวัฒนธรรมต่อว่าตลอดว่า ส่งไปแล้วไม่เห็นทำอะไรเลย ทำไมจึงละเว้นไม่ปฏิบัติหน้าที่ ซึ่งเขาไม่เข้าใจว่าเรื่องแบบนี้ไม่ได้ทำกัน

ง่ายๆ ก่อนมี พ.ร.บ.คอมพิวเตอร์ฯ 2550 การปิดเว็บไซต์เกิดขึ้นได้ยากมาก ต้องให้ไอเอสพี (ISP หรือ Internet Service Provider หมายถึงผู้ให้บริการอินเทอร์เน็ต) เซ็คลิสต์ด้วย เพราะว่าช่วงนั้นมันไม่มีกฎหมาย เราได้แต่ขอความร่วมมือ"

"ก่อนมีกฎหมาย มันค่อนข้างลักลั่นว่ามีอำนาจหน้าที่หรือไม่ ใช้อำนาจตรงไหน ช่วงหนึ่ง กระทรวงวัฒนธรรมส่งหนังสือมาให้ปิดเว็บไซต์เกี่ยวกับรักร่วมเพศแห่งหนึ่ง บอกว่าขัดต่อศีลธรรมอันดีของประชาชน เราก็ส่งไปให้ไอเอสพีปิด พอปิดแล้ว ปรากฏว่า เจ้าของเว็บรวมตัวกันมาประท้วงที่หน้ากระทรวง เพราะเว็บของเขาไม่ได้โป๊ พอเขามาร้องเรียน ก็ต้องบอกไปว่า เราไม่ได้คิดเอง กระทรวงวัฒนธรรมส่งเรื่องมา พอบอกไปแบบนั้น กระทรวงวัฒนธรรมก็เดือดอีกว่า ทำไมคุณต้องอ้างแหล่งที่มาด้วย เราก็ว่าก็คุณพิจารณามาอย่างนี้ผมก็บอกสิว่าผมไม่ได้พิจารณาเอง เราจะรู้ไหมล่ะว่ามันขัดต่อประเพณีหรือศีลธรรมอันดีของประชาชนอย่างไร"

"พอมี พ.ร.บ. แล้วง่ายหน่อย เพราะเจ้าหน้าที่ไม่ต้องใช้ดุลยพินิจกันเอง แต่หน่วยงานต่างๆ ต้องนำเรื่องเสนอรัฐมนตรีไอซีทีก่อน เมื่อรัฐมนตรีอนุมัติแล้ว เจ้าหน้าที่ก็ไปยื่นที่ศาลอาญา เพราะไอซีทีไม่ได้มีหน้าที่พิจารณาเนื้อหา เรามีหน้าที่อธิบายว่าเนื้อหานั้นๆ อาจจะขัดกับมาตรา 20 อย่างไร ฝ่ายศาลจะเห็นด้วยหรือไม่เห็นด้วยก็ตาม ท่านจะไม่เห็นด้วยก็ได้ ซึ่งมีหลายกรณีที่ศาลเห็นว่าไม่ต้องบล็อค อย่างกรณีหนึ่ง เรื่องยาลดความอ้วนที่ อย.ร้องมา ศาลตัดสินว่าไม่ต้องบล็อก จะไปบล็อคทำไม เพราะ อย. มีหน้าที่ต้องไปอธิบายกับผู้บริโภคว่า มันไม่ดีตรงไหน อย่างไร"

"พอเราได้คำสั่งศาลมา เราก็ส่งให้ไอเอสพี ไอเอสพีจะใช้อำนาจอะไรก็เรื่องของไอเอสพี เราไม่ได้ไปบังคับเขา เพียงแต่เราสำเนาคำสั่งศาลส่งให้"

"ขั้นตอนการปิดเว็บตามกฎหมายคือมาตรา 20 เจ้าหน้าที่ยื่นรัฐมนตรี รัฐมนตรีอนุมัติ ไปยื่นต่อศาล ศาลอนุมัติ ซึ่งขั้นตอนการดำเนินงานของศาลไม่นาน ถ้าเป็นคดีที่ละเอียดอ่อนมากๆ ศาลเร็ว แต่พอมีอำนาจพิเศษใช้ พ.ร.ก.ฉุกเฉินฯ ก็ใช้กันเต็มที่เลย จนตอนนี้เรายังแยกไม่ได้เลยว่า

มีการใช้อำนาจตาม พ.ร.ก.ฉุกเฉินฯ ขอให้ไอเอสพีปิดไปเท่าไหร่ ซึ่งผมว่าปิดไปหลายหมื่น เพราะว่าช่วง พ.ร.ก.ฉุกเฉินฯ มีเจ้าหน้าที่ไปยื่นคำร้องขอศาลว่าขอระงับการเข้าถึงเว็บไซต์น้อยลงมาก เพราะว่าใช้ พ.ร.ก. มันเร็วกว่า ที่น่าสนใจคือ มันจะเป็นบรรทัดฐานต่อไปในอนาคต ไม่ว่ารัฐบาลไหนๆ ขึ้นมา พอมีปัญหา สมมติเรื่องเหลืองทะเลาะกับแดงประท้วง รัฐบาลก็จะประกาศ พ.ร.ก.ฉุกเฉิน"

"ในส่วนของกระบวนการการดำเนินคดีกับเว็บที่ถูกปิดนั้น มีไม่มากเท่าไร เพราะคนเน้นเอาง่ายๆ เอาเร็วๆ ปิดเร็วที่สุด ไม่ต้องรับผิดชอบสั่งปิดมันอย่างเดียว ซึ่งจริงๆ แล้ว ถ้าเขาทำความผิดจริง รัฐก็ต้องสืบหาผู้กระทำความผิด ยิ่งถ้าเป็นเว็บภาษาไทย หรือมีคนไทยทำ มันควรจะหาตัวผู้กระทำผิดได้ แต่นี่ปิดแล้วก็ลืมไปเลย นี่เป็นลักษณะของการใช้อำนาจที่พอถึงจุดหนึ่งมันจะเปลี่ยนไม่ได้ เพราะมันชินแล้ว"

"กรณีการหมิ่นประมาทกัน ด่ากันบนเน็ต คนที่เข้ามาแจ้งหรือร้องเรียน เขาไม่ได้อยากดำเนินคดี เขาแค่อยากรู้ว่าใคร พอรู้แล้วก็ไม่อยากขึ้นศาลให้ยุ่งยาก เว้นแต่เป็นกรณีที่เสียหายกับทรัพย์สิน"

(เจ้าหน้าที่ (ขอสงวนนาม) กระทรวงไอซีที, 2553)

(3) การดำเนินคดีผู้กระทำผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550

จากการศึกษาและรวบรวมข้อมูล คณะผู้วิจัยพบว่า ที่มาของคดีตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ส่วนใหญ่ มีทั้งจากการร้องเรียนของประชาชน จากหน่วยงานราชการต่างๆ และยังมาจากการตระเวนตรวจสอบในสื่อออนไลน์ของเจ้าหน้าที่ตำรวจเอง

"ที่มาของคดีที่เข้ามาสู่ ปอท. มีทั้งส่วนที่มาจากประชาชนแจ้งโดยตรง ส่งมาจากโรงพัก หน่วยราชการเป็นผู้เสียหาย หรือทำเป็นหนังสือร้องขอให้ทำการสืบสวน หรือผู้บัญชาการทำหนังสือให้ทำการสืบสวน ส่วนใหญ่จะแจ้งเองและก็ทำหนังสือมา"

"นอกจากนี้ การทำงานของ ปอท.เองก็มีหน่วยลาดตระเวน ที่มีภารกิจหลักในการตรวจตราเรื่องการหมิ่นสถาบันฯ เว็บโป๊ เว็บขาย

ของฉ้อโกง โดยวิธีการทำงานของหน่วยลาดตระเวนนั้น ใช้วิธีค้นหาจากกูเกิลดู เช่น กรณีเว็บพนันบอลซึ่งมีหลายเว็บก็ต้องดูว่าเว็บใดคนเข้าเยอะสุดอาจจะเข้าข่ายได้ มีคำสำหรับตรวจค้นหา ดังนั้นจะมีระดับที่ต้องดูว่าเรื่องใด เว็บใดที่ต้องทำโดยเร่งด่วน"

(พ.ต.อ.ศิริพงษ์ ติมุลา รองผบก. ปอท., 2554)

พ.ต.อ.ศิริพงษ์ ติมุลา รองผบก. ปอท. กล่าวว่า ก่อนประกาศใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 การทำงานสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์จะใช้อำนาจตามประมวลกฎหมายอาญา ซึ่งก็สามารถใช้ได้แต่ไม่ตรง ดังนั้น พ.ร.บ.คอมพิวเตอร์ฯ 2550 จึงทำให้การทำงานง่ายขึ้น เพราะมีบทบัญญัติโดยเฉพาะ สามารถตีความได้ง่าย

"ข้อดีตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 คือ หนึ่ง มีฐานความผิดบัญญัติเป็นการเฉพาะ ทำให้ผู้ปฏิบัติงานตีความง่ายขึ้น ไม่สับสน มีความชัดเจนในการตีความ สอง ให้อำนาจพนักงานเจ้าหน้าที่ในการสอบสวนเก็บพยานหลักฐานเป็นการเฉพาะตามมาตรา 18[28] ในคดีที่เป็นความผิดมูลฐานอยู่ในคดีอาชญากรรมคอมพิวเตอร์ พนักงานเจ้าหน้าที่จะมีอำนาจพิเศษมากกว่าคดีธรรมดา คือ สามารถเข้าถึงตรวจสอบระบบ การอายัด การยึด แต่กฎหมายก็มีการตรวจสอบถ่วงดุล เช่น ต้องขออนุญาตศาล การรายงานศาล การทำงานต้องคำนึงถึงผลกระทบต่อเสรีภาพของประชาชน สาม ทำให้ทุกภาคส่วนตื่นตัว โดยเฉพาะผู้ให้บริการต้องระมัดระวังระบบข้อมูลของตัวเอง ต้องเก็บข้อมูลจราจรเพื่อให้เจ้าหน้าที่ติดตามร่องรอยคนร้ายได้ ก่อนหน้านั้นไม่มี บางบริษัทก็ไม่เก็บข้อมูล"

(พ.ต.อ.ศิริพงษ์ ติมุลา รองผบก. ปอท., 2554)

ทั้งนี้ แม้จะมีการประกาศใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 เพื่อปราบปรามอาชญากรรมคอมพิวเตอร์ แต่กลับพบว่า คดีความที่พบมาก หรือคดีที่หน่วยงานรัฐให้ความสำคัญ มักเป็นการเผยแพร่เนื้อหาในสื่อออนไลน์ที่เกี่ยวข้องกับความมั่นคง โดยเป็นคดีหมิ่นประมาทกษัตริย์ฯ ที่ฟ้องคู่กับ

มาตรา 112 ประมวลกฎหมายอาญา

“ถ้าจัดลำดับอาชญากรรมคอมพิวเตอร์ในประเทศไทย คดีที่มากอันดับหนึ่งคือ 1. คดีหมิ่นประมาทออนไลน์ ตามมาตรา 14 (3) พ.ร.บ.คอมพิวเตอร์ฯ 2550 และจะเกี่ยวเนื่องกับมาตรา 112 ส่วนใหญ่มาจากไอซีทีและกองปราบ 2. หมิ่นประมาทออนไลน์ ตามกฎหมายอาญา 3. ฉ้อโกงออนไลน์ ตามกฎหมายอาญา 4. การพนันออนไลน์ ตาม พ.ร.บ.การพนัน 5. เผยแพร่ภาพลามก มาตรา 14 (4) มาตรา 287 อาญา 6. อาชญากรรมคอมพิวเตอร์ตาม มาตรา 5-7 ส่วนเรื่องการละเมิดลิขสิทธิ์ออนไลน์จะมีกองบังคับการปราบปรามอาชญากรรมทางเศรษฐกิจ (ปอศ.) อยู่แล้ว”

“สาเหตุที่จำนวนคดีตามมาตรา 5-13 ซึ่งเป็นกรณีอาชญากรรมคอมพิวเตอร์โดยแท้ มีจำนวนน้อย ทั้งๆ ที่ในความเป็นจริง อาชญากรรมลักษณะนี้เกิดขึ้นเยอะ เป็นเพราะไม่ค่อยมีคนมาแจ้งความ เนื่องจากเขาจะต่อสู้กันเองกับผู้กระทำผิด และต้องการรักษาภาพลักษณ์ของบริษัท คล้ายๆ กับความผิดฐานข่มขืน คือ ถ้าไม่จำเป็นผู้เสียหายก็ไม่อยากมาแจ้งความ เช่น ล่าสุดมีการ Hack เว็บไซต์ของพรรคการเมือง ก็ไม่มีการมาแจ้งความ เนื่องจากเป็นเรื่องของภาพลักษณ์”

(พ.ต.อ.ศิริพงษ์ ติมุลา รองผบก. ปอท., 2554)

“ความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ที่พบมากในสมัยแรกๆ เป็นเรื่องภาพตัดต่อ ส่วนใหญ่เป็นคดีดารา ต่อมาเป็นคดีทางการเมือง คดีความมั่นคงซึ่งก็เป็นไปตามยุคสมัย ต่อมาก็เป็นเรื่องการรับส่งอีเมล ส่วนระยะหลังๆ คดีที่พบเยอะมักจะเป็นคดีที่ต้องตรวจหลักฐานบนโซเชียลเน็ตเวิร์ค เป็นเรื่องการส่งข้อความที่กระทบต่อความมั่นคงซึ่งมีเยอะพอสมควร”

(พ.ต.อ.อนุชิต บุญญะปฏิภาค กลุ่มงานตรวจพิสูจน์หลักฐานอาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง, 2554)

นายเกริกไชย ศรีศุกร์เจริญ พนักงานสอบสวนคดีพิเศษชำนาญการพิเศษ สำนักคดีเทคโนโลยีสารสนเทศ กรมสอบสวนคดีพิเศษ (ดีเอสไอ) กล่าวว่า ความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 เป็นเหมือนเครื่องมือของกฎหมายทุกฉบับ เป็นพื้นฐานเริ่มต้นของการกระทำความผิดอื่นๆ เช่น การเข้าถึงข้อมูลโดยมิชอบ การเข้าถึงระบบคอมพิวเตอร์เพื่อไปทำความผิดตามบทกฎหมายอื่น

"สถานการณ์ทางการเมืองก็มีผลต่อการทำงานบ้าง หลังจาก 10 เมษายน 2554 เริ่มมีคดีเข้ามาเยอะ ส่วนคดีจะมากน้อยอย่างไรก็ต้องประเมินสถานการณ์ทางการเมืองด้วย เพราะอาจมีการดึงสถาบันพระมหากษัตริย์เข้ามาเกี่ยวข้องกับการเมือง เมื่อก่อนไม่ค่อยมีคดีมาตรา 112 ซึ่งนอกจากสำนักเทคโนโลยีนี้แล้ว ยังมีสำนักคดีความมั่นคงที่รับผิดชอบ อาจต้องประสานงานกันหากมีคดีเกี่ยวกับคอมฯ และเกี่ยวกับความมั่นคง"

"ดีเอสไอจะทำงานร่วมกับหน่วยงานอื่น ประสานงานกันตั้งเป็นคณะกรรมการพิจารณาเฉพาะคดีความมั่นคง คณะกรรมการนี้ตั้งขึ้นหลายปีแล้ว เป็นความลับ ทำหน้าที่พิจารณาประเภทคดีและความยากง่ายของคดี แต่ทุกคดีจะมีอัยการเข้ามาร่วมด้วยตามมาตรา 32" [29]

(นายเกริกไชย ศรีศุกร์เจริญ กรมสอบสวนคดีพิเศษ (ดีเอสไอ), 2554)

อย่างไรก็ดี แม้หน่วยงานอย่างกระทรวงไอซีที และกองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยีจะเห็นว่า การเกิดขึ้นของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ทำให้การทำงานมีขอบเขตที่ชัดเจนขึ้น และเจ้าหน้าที่มีอำนาจหน้าที่ตามกฎหมาย แต่สำหรับกรมสอบสวนคดีพิเศษแล้ว พ.ร.บ.คอมพิวเตอร์ฯ 2550 ไม่ได้มีความจำเป็นมากนัก เพราะมีอำนาจที่ให้ไว้แล้วตาม พ.ร.บ.การสอบสวนคดีพิเศษ

"เมื่อต้องดำเนินคดี ทางดีเอสไอไม่ค่อยใช้มาตรา 18 ของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 เพราะมีหลายอย่างติดขัด เช่น เรื่องระยะเวลาตามที่กฎหมายกำหนด เมื่อมาตรา 18 ใช้งานไม่ได้ ดีเอสไอก็จะหันไปใช้

มาตรา 25[30] ของ พ.ร.บ.การสอบสวนคดีพิเศษแทน ซึ่งเป็นกฎหมายที่เกิดก่อน พ.ร.บ.คอมพิวเตอร์ฯ 2550 การใช้มาตรา 25 ในการรวบรวมพยานหลักฐานต้องมีเหตุผลที่เพียงพอและมีขั้นตอนเฉพาะ และต้องผ่านความเห็นของกรมฯ และส่งไปยังอธิบดีศาลอาญาเท่านั้นที่จะอนุมัติแล้วจึงจะมีอำนาจ เนื่องจากเป็นคดีพิเศษ จึงไม่อาจขออำนาจจากศาลทั่วไปได้ และมาตรา 25 เป็นกฎหมายที่ค่อนข้างกระทบสิทธิบุคคลภายนอกซึ่งมีกฎหมายอื่นคุ้มครองอยู่ ส่วนการจะเป็นคดีพิเศษหรือไม่ ต้องเข้าเงื่อนไขตามมาตรา 21 ก่อน เมื่อเป็นคดีพิเศษซึ่งเป็นคดีที่ค่อนข้างยุ่งยากซับซ้อนในการรวบรวมพยานหลักฐานจึงจะใช้อำนาจตามกฎหมายฉบับนี้ได้"

"ปัจจุบัน หากเกิดคดีขึ้นดีเอสไอก็มักจะใช้มาตรา 25 พ.ร.บ. สอบสวนคดีพิเศษ ก่อน เนื่องจากเป็นกฎหมายที่เกิดก่อน ต่อมาเมื่อมีมาตรา 18 พ.ร.บ. คอมพิวเตอร์ฯ 2550 จึงอาจมีคำถามได้ว่าทำไมดีเอสไอถึงไม่ใช้มาตรา 18 พ.ร.บ. คอมพิวเตอร์ฯ 2550 แต่ทางดีเอสไอเห็นว่า หากใช้มาตรา 18 ซึ่งต้องมีกระบวนการขั้นตอน ทั้งต้องมีการแจ้งเกี่ยวกับข้อมูลที่ถูกรื้อไปแล้ว (มาตรา 25 ไม่ต้องแจ้งก่อน) ซึ่งในมุมของประชาชนอาจจะมองว่าเป็นการละเมิดสิทธิ กฎหมายจึงกำหนดให้อธิบดีศาลอาญาอนุมัติเท่านั้น ซึ่งต้องมีการพิจารณาแล้วว่าเป็นเรื่องที่สำคัญจริงๆ จึงจะอนุมัติ"

"มาตรา 25 จะมีกำหนดวิธีการในกฎ ระเบียบ ข้อบังคับ ซึ่งเป็นกฎหมายลูก เช่น ขั้นตอนการดักฟังโทรศัพท์ ระยะเวลาในการเก็บข้อมูล เป็นต้น ซึ่งข้อมูลที่ได้จะสามารถเอามาเป็นพยานหลักฐานได้เนื่องจากศาลให้อำนาจในการเข้าถึงข้อมูล ซึ่งต่างจากพยานหลักฐานของคดีตำรวจถ้าได้มาโดยไม่ชอบโดยไม่มีอำนาจก็ไม่สามารถรับฟังเป็นพยานหลักฐานได้"

(นายเกริกไชย ศรีศุกร์เจริญ กรมสอบสวนคดีพิเศษ (ดีเอสไอ), 2554)

(4) การยึด อายัด ตรวจพยานหลักฐานทางอิเล็กทรอนิกส์

ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ พยานหลักฐานทางอิเล็กทรอนิกส์ถือเป็นสิ่งสำคัญมากในคดี ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550

นั้น ทั้งมาตรา 18 อำนาจพนักงานเจ้าหน้าที่ มาตรา 26[31] การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ ประกาศกระทรวงฯ เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวน และดำเนินคดีกับผู้กระทำความผิด รวมถึงกฎกระทรวงกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ ล้วนเป็นสิ่งที่ถูกกำหนดขึ้นเพื่อใช้รวบรวมพยานหลักฐานในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ทั้งสิ้น

"กฎหมายวิธีพิจารณาความอาญาซึ่งก็สามารถใช้ได้แต่ไม่ตรงเสียทีเดียว ถ้ามองในเชิงคุณค่าของพยานหลักฐานจะไม่มีหลักประกันอะไรที่จะบอกว่า การได้มาซึ่งพยานหลักฐานนั้นมีความน่าเชื่อถือ ไม่ถูกปนเปื้อน เนื่องจากข้อมูลคอมพิวเตอร์เป็นพยานหลักฐานทางอิเล็กทรอนิกส์ มีคุณลักษณะไม่เหมือนพยานหลักฐานในแบบทั่วไป เช่น พยานเอกสาร พยานวัตถุ เป็นต้น สิ่งที่แตกต่างคือ 1. เป็นข้อมูลที่อาจจะระเหยได้ หายง่าย เช่น เก็บไว้ในหน่วยความจำคอมพิวเตอร์ พอปิดเครื่องข้อมูลอาจจะหายไปได้ 2. สามารถถูกเปลี่ยนแปลงได้ง่าย เช่น หากคลิกเปิดไฟล์ ข้อมูลบางอย่างที่อยู่ใน metadata ของไฟล์ถูกเปลี่ยนแปลงไป ดังนั้น จึงต้องมีหลักประกันว่าพยานหลักฐานจะไม่เปลี่ยนแปลง หรือหากเปลี่ยนแปลงต้องมีคนรับผิดชอบ ซึ่งหลักประกันนี้จะแฝงอยู่ในแนวทางการปฏิบัติงานของเจ้าหน้าที่ เช่น มีการเซ็นรับ การถ่ายรูป หรือการตรวจพิสูจน์ฮาร์ดดิสก์ต้องมีโปรแกรมการพิสูจน์ที่ถูกต้องซึ่งโปรแกรมเหล่านี้จะมีหลักประกันนี้ฝังอยู่กับตัวโปรแกรม ดังนั้น พนักงานเจ้าหน้าที่ก็ต้องมีองค์ความรู้พวกนี้ด้วย"

(พ.ต.อ.ศิริพงษ์ ติมุลา รองผบก. ปอท., 2554)

"ขั้นตอนการทำงานและหาพยานหลักฐานต่าง ๆ ขึ้นอยู่กับมูลเหตุของแต่ละคดี บางคดีเพียงแค่หาข้อมูลจราจรคอมพิวเตอร์ที่ชี้ไปยังต้นตอ หากผู้ต้องหายอมรับสารภาพก็จบ บางคดีต้องยึด อายัดวัตถุพยานคอมพิวเตอร์ เพื่อทำ computer forensic คือ ตรวจสอบว่าในฮาร์ดดิสก์มีข้อมูลอะไรอยู่บ้าง และมีการลบ เปลี่ยนแปลง แก้ไขข้อมูลหรือไม่"

"ตลอดการทำงานจะมีการถ่ายวิดีโอ คือ เรามีวัตถุก้อนหนึ่ง พอเรามาตรวจสอบ ขณะที่เรากำลังทำอะไรอยู่กับวัตถุต้องสงสัยก้อนนั้น เราจะถ่ายวิดีโอ ส่วนมากขั้นแรกก็คือ จะมีการห่อ (wrap) หลักฐานเหล่านั้นด้วยถุงดำ แล้วก็ดูขั้นตอนการแกะ พอแกะเรียบร้อย ทำการโคลนเรียบร้อย เราก็ใส่กลับคืน ดูว่าไม่มีอะไรแตกหัก แล้วก็ปิด จากนั้นจึงเซ็นชื่อเพื่อรับรอง"

"บางกรณี ความจุของฮาร์ดดิสก์มีความซับซ้อน เช่น มีการเข้ารหัสข้อมูล เราอาจจะต้องทำการแกะรหัส หรือบางทีข้อมูลก็อาจเป็นเรื่องของการโอนเงินที่มันซับซ้อนมากกว่าที่จะเป็นคำแค่คำเดียว ความซับซ้อนของแต่ละคดีก็ขึ้นอยู่กับลักษณะของคดีที่เกิดขึ้น ถ้าโพสต์ด่ากันแป๊บเดียวก็เจอแล้ว เช่นด่าว่าคุณ "โง่" ก็ค้นหาในฮาร์ดดิสก์คำว่าโง่ ถ้าเป็นเรื่องประหลาดมากกว่านี้ เช่นไปเรื่องการฉ้อโกง โอนเงินทับซ้อน เราก็ต้องมาตรวจอีกระดับหนึ่งว่ามันมีการทำอะไรบ้าง"

(พนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 (ขอสงวนนาม) กระทรวงไอซีที, 2553)

สำหรับหลักฐานทางอิเล็กทรอนิกส์ที่ยึดได้แล้ว จะถูกส่งไปยังกลุ่มงานตรวจพิสูจน์หลักฐานอาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง ทั้งนี้ กองพิสูจน์หลักฐานไม่ได้ทำหน้าที่ตรวจสอบว่าพยานหลักฐานหนึ่งๆ ได้มาจากที่ไหน และอย่างไร แต่ตรวจสอบจากพยานหลักฐานที่ได้มาแล้วเท่านั้น เช่น พบอะไรในเครื่องต้องสงสัย โดยปกติกองพิสูจน์หลักฐานต้องรับคดีทั้งหมดที่เป็นเรื่องดิจิตอลจากทั่วประเทศ ซึ่งนอกจากความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 แล้ว ยังรวมถึง พ.ร.บ.ลิขสิทธิ์ พ.ร.บ.ผลิตภัณฑ์ซีดี พ.ร.บ.ธุรกรรมอิเล็กทรอนิกส์ บัตรอิเล็คทรอนิกส์ รวมทั้งสิ้นราว 300 คดีต่อปี ซึ่งมีเจ้าหน้าที่ทั้งหมดแค่เพียง 3 คน (พ.ต.อ. อนุชิต บุญญะปฏิภาค กองพิสูจน์หลักฐานกลาง, 2554)

2) ปัญหาที่เกิดขึ้นจากตัวบทบัญญัติ และการบังคับใช้ พ.ร.บ. คอมพิวเตอร์ฯ 2550 ในส่วนที่เกี่ยวกับเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นของประชาชน

นับแต่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีผลบังคับใช้ เป็นเวลากว่า 4 ปี ในมุมมองของเจ้าหน้าที่รัฐที่เกี่ยวข้อง พบปัญหาสี่เรื่องหลัก คือ

(1) ปัญหาการตีความ ซึ่งหลายมาตราในกฎหมายฉบับนี้ต้องอาศัยดุลพินิจในการตีความอย่างมาก

(2) คดีส่วนใหญ่ถูกให้น้ำหนักไปที่เรื่องที่เกี่ยวกับความมั่นคง ในขณะที่การบังคับใช้กฎหมายเพื่อปราบปรามอาชญากรรมคอมพิวเตอร์โดยแท้ และการคุ้มครองประชาชนโดยรวมยังมีไม่มากนัก

(3) พบปัญหาในเรื่องความรู้ความเข้าใจของบุคลากรที่มีต่อคดี พ.ร.บ.คอมพิวเตอร์ฯ 2550 และ

(4) มีปัญหาการประสานงานระหว่างเจ้าหน้าที่รัฐกับผู้ให้บริการ

(1) การตีความกฎหมาย

เนื้อหาบางมาตราของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ต้องอาศัยดุลพินิจของเจ้าพนักงานที่ต้องบังคับใช้กฎหมายฉบับนี้มากเกินไป เช่น มาตรา 14 (1) ซึ่งมีความคลุมเครือ และยากที่จะพิสูจน์ให้เห็นถึง “ความเท็จ” ซึ่งเจ้าหน้าที่ตำรวจต้องใช้ดุลพินิจว่าจะดำเนินการเพื่อส่งให้อัยการ เพื่อทำคำสั่งฟ้องหรือไม่ จากนั้นก็ขึ้นอยู่กับศาลว่าจะพิจารณาอย่างไร อย่างไรก็ดี ในมุมมองของเจ้าพนักงานยังเห็นว่า ปัญหาลักษณะนี้เป็นเรื่องของการบังคับใช้ ไม่ใช่ปัญหาในตัวบทกฎหมาย เช่น การบัญญัติให้มาตรา 14 (1) มีองค์ประกอบความผิดในเรื่องความแท้จริงของข้อมูล ย่อมเป็นผลทำให้พนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งได้รับการแต่งตั้งให้มาปฏิบัติงานเพราะเป็นผู้เชี่ยวชาญด้านเทคโนโลยี ต้องเข้ามาร่วมวิเคราะห์ความแท้จริงของข้อมูลด้วย ซึ่งเป็นเรื่องยากที่จะพิสูจน์

“มาตรา 14 (1) การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลปลอม

ทั้งหมดหรือบางส่วน หรือข้อมูลอันเป็นเท็จ เราจะบอกได้อย่างไรว่าข้อมูลนั้นเป็นจริงหรือเป็นเท็จ ถ้าเราบอกว่า 1 บวก 1 เท่ากับ 3 อย่างนี้มันชัดว่าข้อมูลมันเป็นเท็จ แต่ถ้าเราหยิบสีขึ้นมาสักสีหนึ่ง ซึ่งมันออกส้มๆ แดงๆ คนหนึ่งอาจบอกสีส้ม ในขณะที่อีกคนบอกสีแดง ถามว่ามันจริงหรือเท็จ ตอบยากมาก ต้องมาตีความพิสูจน์ แล้วใครจะเป็นคนรับรองว่าจริงหรือเท็จ หรือว่ามันเป็นแค่การหมิ่นประมาทธรรมดาไม่ได้เกี่ยวว่าต้องเป็นความเท็จหรือความจริง ทั้งหมดนี้มันขึ้นอยู่กับการตีความ ถัดจากนั้นก็เป็นดุลพินิจของการส่งฟ้อง และศาลพิจารณา เรามีหน้าที่ที่จะต้องดำเนินตามกฎหมายอาญา ไม่เช่นนั้นเราก็จะละเลยการปฏิบัติหน้าที่ หรือละเว้นการปฏิบัติหน้าที่"

(พนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 (ขอสงวนนาม) กระทรวงไอซีที, 2553)

นอกจากมีการนำมาตรา 14 (1) มาใช้ทั้งกับความผิดฐานนำเข้าข้อมูลเท็จ และการหมิ่นประมาทแล้ว บางครั้งบทบัญญัติข้อนี้ยังถูกนำไปใช้กับการหลอกลวงฉ้อโกงผ่านโลกออนไลน์ด้วย โดยตั้งข้อหาว่าเป็นการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จแบบหนึ่ง

"มีปัญหาบ้างเรื่องการตีความ ซึ่งใช้วิธีพูดคุยกันในระดับผู้ปฏิบัติงาน เช่น การฉ้อโกงออนไลน์ มีผู้โพสต์ในเว็บไซต์ว่ามี iPad จะขาย แต่จริงๆ เป็นความเท็จ แล้วจะผิดมาตรา 14 (1) หรือไม่ ซึ่งผู้โพสต์ไม่ได้มีเจตนาจะนำเข้าซึ่งข้อมูลอันเป็นเท็จหรอก เขาต้องการหลอกขายนั่นเอง ดังนั้น ต้องดูเจตนาเขา แต่เรื่องนี้เข้าฉ้อโกงแน่ๆ"

(พ.ต.อ.ศิริพงษ์ ติมุลา รองผบก. ปอท., 2554)

สำหรับตัวอย่างกรณีการหลอกขายของบนเว็บบอร์ดต่างๆ นั้น ในความเห็นของเจ้าหน้าที่ตำรวจระดับสูง (ขอสงวนนาม) ปอท. เห็นว่าเข้าข่ายฉ้อโกงตามประมวลกฎหมายอาญา มากกว่าที่จะเป็นความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 แต่ในทางปฏิบัติเจ้าหน้าที่ก็ต้องสั่งฟ้องไปตาม

พ.ร.บ.คอมพิวเตอร์ฯ 2550 ด้วย เพราะมีขั้นตอนสืบหาตัวผู้กระทำผิดที่ต้องอาศัยหลักฐานทางคอมพิวเตอร์ และเพื่อจะทำให้เจ้าหน้าที่มีอำนาจขอข้อมูลจราจรจากผู้ให้บริการ รวมถึงการยึดและอายัดคอมพิวเตอร์ ก็จึงจำเป็นต้องฟ้องคดีตาม พ.ร.บ.คอมพิวเตอร์ควบคู่ไปด้วย

นอกจากมาตรา 14 (1) ที่ต้องอาศัยดุลพินิจในการพิจารณาความแท้จริงของข้อมูลแล้ว ปัญหาที่เกี่ยวเนื่องกับการสื่อสารในโลกออนไลน์มักมีประเด็นใหม่ๆ ที่ทำให้เจ้าหน้าที่ต้องพิเคราะห์ด้วยว่า ประเด็นนั้นๆ เข้าองค์ประกอบความผิดของกฎหมายที่มีอยู่หรือไม่ เช่น ภาพเปลือยที่มาจากการสร้างขึ้นโดยโปรแกรมคอมพิวเตอร์จะจัดเป็นข้อมูลอันลามกได้หรือไม่ หรือ Item ในเกมออนไลน์ จะสามารถนิยามเป็น “ทรัพย์” ประเภทหนึ่งได้หรือไม่ เป็นต้น

“คำถามคือ ภาพเปลือย แต่ไม่มีภาพคนจริงๆ เป็นภาพแอนิเมชันหรือสร้างขึ้นจากซีจี จะถือว่าเป็นภาพลามกได้หรือไม่ หรือข้าวของที่อยู่ในคอมพิวเตอร์ถือเป็นทรัพย์หรือไม่ ถ้ามีคนมาแจ้งความว่า เล่นเกมส์แล้วซื้อของในเกมผ่านเครดิตการ์ด เช่น ซื้อรถ ซื้อบ้าน แล้วรถกับบ้านหายไป คนเล่นเสียหายเพราะต้องใช้เงินซื้อ แต่จะนับเอาทรัพย์สินตรงไหน จะจับด้วยกฎหมายข้อไหน กฎหมายอาญาก็ไม่ลง แต่เป็นการทำแบบแฮกเกอร์เพราะลักลอบเข้าไปในที่ที่เขาไม่อนุญาตให้เข้า กฎหมายมันจึงต้องไปอีกพอสมควร ผมใช้คำว่า คอมพิวเตอร์มันคืออีกโลกหนึ่ง มันมีอยู่จริง ปฏิเสธไม่ได้ รับรู้เซนส์ทุกอย่างได้ แต่กฎหมายมันตามไม่ทัน”

“อีกประเด็นคือ เมื่อกระทำผิดจากเมืองนอกแล้วมาเมืองไทยผิดหรือไม่ ตัวอย่างที่ง่ายสุด คือ ภาพโป๊เด็ก ที่ต่างประเทศเขาบอกชัดว่าตราบที่อายุเกิน 18 แล้วก็ไม่ผิดกฎหมาย แต่ของไทยเรามันผิดหมด หากเป็นการทำจากเมืองนอก เมื่อคอมพิวเตอร์มันเผยแพร่ข้ามประเทศได้ แบบนี้เราจะถือว่าผิดกฎหมายเราหรือไม่”

(พ.ต.อ. อนุชิต บุญญะปฏิภาค กองพิสูจน์หลักฐานกลาง, 2554)

นอกจากนี้ เจ้าหน้าที่ตำรวจระดับสูง (ขอสงวนนาม) ปอท. ยังเห็น

ว่า มีคดีจำนวนมากที่ไม่เป็นธรรมกับผู้ต้องหา เพราะมีการตีความกฎหมายอาญาแบบขยายความในทางที่เป็นโทษกับบุคคล โดยเฉพาะอย่างยิ่งกับคดีดูหมิ่น หรือหมิ่นประมาทกษัตริย์ฯ

"การเป็นข้าราชการมันยากนะ ถ้าคดี (หมิ่นประมาทกษัตริย์ฯ) เกิดขึ้นมาแล้ว เราจะทำความเห็นว่าควรสั่งฟ้องหรือไม่ฟ้อง ก็ต้องคิดแล้วคิดอีกเดี๋ยวจะโดนหาว่าไม่จงรักภักดีได้ถ้าเราสั่งไม่ฟ้อง ในขณะที่อัยการกับศาลเขาอาจจะง่ายกว่า ถ้าตำรวจเห็นว่าเรื่องนี้ไม่เข้าองค์ประกอบความผิดแล้วทำความเห็นสั่งไม่ฟ้องไป คนที่ไม่ชอบใจเรามันก็มี ถ้าโดนข้อหานี้ก็... ทั้งที่เราเองก็จงรักภักดี แต่ไม่มีใครฟังหรอก"

(เจ้าหน้าที่ตำรวจระดับสูง (ขอสงวนนาม) ปอท., 2554)

(2) การใช้กฎหมายเพื่อคุ้มครองสิทธิและเสรีภาพของประชาชน

ปัญหาหนึ่งที่พบบ่อยก็คือ เมื่อมีผู้เสียหายจากอาชญากรรมคอมพิวเตอร์ไปแจ้งความกับตำรวจ แต่ตำรวจไม่ยอมรับแจ้ง โดยให้เหตุผลว่าไม่ได้อยู่ในเขตอำนาจตามท้องที่ที่กระทำผิด หรือไม่สามารถทำคดีได้ เพราะไม่มีอำนาจหน้าที่แบบเจ้าพนักงานตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 สถานีตำรวจย่อยในพื้นที่ต่างๆ เหล่านั้นก็มักแนะนำให้ผู้เสียหายไปแจ้งความที่กรุงเทพฯ แต่เมื่อมาถึงที่กรุงเทพฯ หน่วยงาน อาทิ กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี และกรมสอบสวนคดีพิเศษก็มีข้อจำกัดกันอีก เนื่องจากเน้นการรับแจ้งเฉพาะคดียุทธศาสตร์ ลักษณะดังกล่าวนี้ย่อมทำให้ประชาชนทั่วไปที่ได้รับความเดือดร้อนรู้สึกว่าตนไม่สามารถพึ่งพาเจ้าหน้าที่ตำรวจได้

"ในกรณีที่แต่ละหน่วยงานมั่นใจว่าหน่วยของตัวเองมีศักยภาพ เขาก็อาจจะแข่งกันทำงาน กรณีใหญ่ทำ กรณีเล็กไม่ทำ คือถ้าเป็นอาชญากรรมคอมพิวเตอร์โดยแท้ (pure cyber crime) มันก็มีไม่กี่หน่วยที่อยากจะทำ เพราะมันเป็นคดีที่มีเรื่องเทคนิคมากและพิสูจน์ยาก ส่วนใหญ่มีปัญหามากกับเจ้าหน้าที่ตำรวจของสถานีตำรวจที่อยู่ทั่วประเทศ เพราะเขาไม่มีความรู้ไม่รู้ว่าจะรับเรื่องแล้วทำอะไรต่อ"

(เจ้าหน้าที่ (ขอสงวนนาม) กระทรวงไอซีที, 2553)

"ผมก็รู้สึกไม่ดีนะเวลาที่ประชาชนมาแจ้งตำรวจแล้วบอกว่าตำรวจไม่รู้เรื่อง เจ้าหน้าที่ที่รับแจ้งความจำเป็นต้องมีความรู้เบื้องต้นว่าจะตอบสนองอย่างไร เพราะถ้าเจ้าหน้าที่ตำรวจไม่รู้ว่าจะตอบสนองอย่างไรก็จะใช้วิธีเดิมๆ คือ ไม่รับเรื่องเสียเลย ซึ่งจะทำให้พยานหลักฐานสูญหายไปตามเวลา ความรู้สึกของผู้เสียหายที่เดินทางจากเชียงรายมากรุงเทพฯ แล้วได้รับการปฏิเสธว่าไม่อยู่ในเขตอำนาจ เจ้าหน้าที่ไม่มีอำนาจตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ก็จะเสียความรู้สึก แต่ปัญหาก็คือ ตำรวจลืมไปแล้วหรือเปล่าว่า อาชญากรรมคอมพิวเตอร์มันไร้พรมแดน"

(เจ้าหน้าที่ตำรวจผู้เชี่ยวชาญเทคโนโลยี (ขอสงวนนาม) สำนักงานตำรวจแห่งชาติ, 2554)

เหตุผลที่ตำรวจระบุว่าไม่สามารถรับเรื่องร้องทุกข์กล่าวโทษได้เพราะไม่ได้อยู่ในเขตอำนาจตามท้องที่ที่กระทำผิดนั้น แต่ในความเป็นจริงคดีที่เกี่ยวข้องกับสื่อออนไลน์เป็นคดีที่ยากที่จะระบุเขตแดนด้วยวิธีเดิมๆ เพราะอินเทอร์เน็ตไม่มีพรมแดน การกระทำผิดหรือผลกระทบของการกระทำจึงอาจจะเกิดขึ้นในท้องที่ใดก็ได้ แต่ในขณะเดียวกันเงื่อนไขนี้ก็เปิดช่องให้เกิดการกลั่นแกล้งฟ้องกันขึ้นได้ ซึ่งที่ผ่านมาพบว่ามีหลายคดีที่โจทก์ฟ้องคดีจำเลยด้วยมูลเหตุอย่างเดียวกันในพื้นที่หลายจังหวัด

(3) ความรู้ความเข้าใจใน พ.ร.บ.คอมพิวเตอร์ฯ 2550

ดังกล่าวไปแล้วว่า ปัญหาของการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งสำคัญมากปัญหาหนึ่งก็คือ บุคลากรในกระบวนการยุติธรรมยังมีความรู้เกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ไม่เพียงพอ กล่าวคือ ในระดับเจ้าหน้าที่สืบสวนสอบสวนนั้น แม้ตามกฎหมายจะกำหนดให้มีพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 แต่จนถึงปัจจุบันก็ยังขาดแคลนคนที่มีความรู้ความสามารถในเรื่องเทคโนโลยีถึงระดับที่

สามารถทำงานสืบสวนสอบสวนคดีในลักษณะนี้ได้ ในขณะที่การจัดอบรมเพื่อพัฒนาบุคลากรก็ยังเกิดขึ้นอย่างจำกัด อีกทั้งด้วยวัฒนธรรมของระบบราชการเองที่แม้มีการพัฒนาบุคลากรจนสามารถทำงานได้แล้ว แต่เมื่อถึงเวลาหนึ่งก็มักมีการโยกย้ายให้ไปทำงานในส่วนราชการอื่นแทน ทั้งนี้ บุคคลที่จะได้รับการแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ต้องมีคุณสมบัติตามที่กำหนดไว้ในประกาศกระทรวง[32] เช่น มีความรู้ความชำนาญเกี่ยวกับระบบคอมพิวเตอร์ สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีด้านวิศวกรรมศาสตร์ วิทยาศาสตร์วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์ และผ่านการอบรมด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (information security)

อนึ่ง แม้จะมีประกาศหลักเกณฑ์คุณสมบัติพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ไว้แล้ว แต่ในตัวประกาศเองก็เปิดช่องให้การแต่งตั้งนี้เป็นดุลพินิจของรัฐมนตรีว่าการกระทรวงไอซีทีด้วย[33] ซึ่งย่อมหมายความว่า แม้จะไม่มีคุณสมบัติใดๆ เข้าหลักเกณฑ์ตามที่กฎหมายกำหนดไว้ แต่หากรัฐมนตรีฯ เห็นสมควร ก็สามารถแต่งตั้งบุคคลดังกล่าวเป็นพนักงานเจ้าหน้าที่ตามกฎหมายฉบับนี้ได้ ซึ่งปัจจุบัน มีพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 จำนวนมากขึ้น และกระจายไปสังกัดอยู่ตามหน่วยต่างๆ ทั้งที่เกี่ยวกับงานไอซีทีโดยตรง และกระทรวงอื่นๆ เช่น กระทรวงวัฒนธรรม กระทรวงกลาโหม ฯลฯ (พนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 (ขอสงวนนาม) กระทรวงไอซีที, 2553)

“ด้วยปัจจัยต่างๆ ทำให้เราสามารถจัดอบรมได้เพียง 2-3 รุ่นในแต่ละปี รุ่นละประมาณ 20-30 คนเท่านั้น เราจะเน้นที่การสร้างหัวหน้าทีมเพื่อจะไปฝึกลูกทีมและสร้างเครือข่าย การจะแก้ปัญหาทั้งหมดก็สามารถทำได้โดยการกระจายความรู้เท่านั้น”

(เจ้าหน้าที่ตำรวจผู้เชี่ยวชาญเทคโนโลยี (ขอสงวนนาม) สำนักงานตำรวจแห่งชาติ, 2554)

"ที่ผ่านมามีการแต่งตั้งพนักงานเจ้าหน้าที่ พ.ร.บ.คอมพิวเตอร์ ประจำ ปอท. 14 คน แต่แต่งตั้งแล้วก็โยกย้ายไป ปัจจุบันเหลือพนักงานเจ้าหน้าที่เพียง 8 คน ซึ่งต้องดูแลคดีเป็นพัน เพราะทั้งคดีหมิ่นสถาบันฯ และคดีเผยแพร่ภาพลามก ล้วนก็อยู่ในความรับผิดชอบของ ปอท."

(เจ้าหน้าที่ตำรวจระดับสูง (ขอสงวนนาม) ปอท., 2554)

"ในส่วนตำรวจเรา มีเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 อยู่ประมาณ 100 คน แต่ก็มีเจ้าหน้าที่กระจัดกระจายอยู่ตามหน่วยงานต่าง ๆ ด้วย ซึ่งเจ้าหน้าที่มาจากหลายทาง บางคนมีความรู้มาก่อนแล้ว และก็ผ่านการอบรมอีกที แต่อย่างไรก็ตาม ก็ไม่มีการประเมินว่าเมื่ออบรมแล้วจะมีความรู้มากน้อยเพียงใด เพียงแต่สันนิษฐานว่าเมื่อผ่านการอบรมแล้วก็น่าจะมีความรู้เพียงพอแล้ว"

(พ.ต.อ.ศิริพงษ์ ติมุลา รองผบก. ปอท., 2554)

ทั้งนี้ แนวทางการสร้างพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ยังมีปัญหาอยู่มาก กล่าวคือ ด้วยความเข้าใจผิดที่ว่า พนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 เท่านั้นที่จะมีอำนาจขอข้อมูลจากผู้ให้บริการตามที่กำหนดไว้ในมาตรา 18 ได้ จึงทำให้มีการแต่งตั้งพนักงานเจ้าหน้าที่จำนวนมากโดยที่ไม่ได้เป็นผู้มีคุณสมบัติตามหลักเกณฑ์ในกฎหมาย เช่น พบว่ามีพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 กระจายอยู่ในหน่วยงานทหาร และกระทรวงวัฒนธรรม ลักษณะเช่นนี้ส่งผลกระทบต่อความน่าเชื่อถือของเจ้าหน้าที่รัฐ และในที่สุดฝ่ายรัฐก็จะถูกมองว่าเน้นการใช้อำนาจเพื่อควบคุมตรวจสอบประชาชนมากกว่าการคุ้มครอง

"การจะฝึกคนที่มีความเชี่ยวชาญจริง ๆ ขึ้นมาหนึ่งคนไม่ใช่เรื่องง่าย ใช้ทั้งเงินและเวลา แต่ยิ่งพนักงานเจ้าหน้าที่มีมากขึ้นเท่าไรก็ยิ่งลำบาก ยิ่งตอนนี้มีจำนวนเป็นร้อย โอกาสที่จะเรียนรู้และทดลองทำจริงยิ่งน้อยลงไปอีก ทุกวันนี้จะเห็นเลยว่าพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ไม่ได้รับการยอมรับ เพราะคนที่ได้รับแต่งตั้งไปไม่มีความรู้ความสามารถ

ในด้านนี้ ปัญหาหนึ่งมาจากการอยากได้อำนาจ ให้มีอำนาจขอข้อมูลได้ก็จบ ซึ่งการทำแบบนี้มันลดมาตรฐานตัวเอง ทั้งๆ ที่ตามเจตนารมณ์ของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 คือ ต้องการสร้างผู้เชี่ยวชาญพิเศษเพื่อปฏิบัติงาน การตั้งพนักงานเจ้าหน้าที่จะไม่มีประโยชน์เลยถ้าไม่มีความรู้จริง และหากให้คนเหล่านี้มีอำนาจโดยไม่มีความรู้ที่จะทำงาน หรือไม่รู้แม้กระทั่งขอบเขตอำนาจของตัวเอง ในอนาคตจะยิ่งสร้างปัญหาด้านไอซีที"

(เจ้าหน้าที่ตำรวจผู้เชี่ยวชาญเทคโนโลยี (ขอสงวนนาม) สำนักงานตำรวจแห่งชาติ, 2554)

"การมีพนักงานเจ้าหน้าที่จำนวนมากขึ้นย่อมไม่สำคัญเท่ากับการมีเจ้าหน้าที่ที่มีคุณภาพ เพราะเคยคุยกันแล้วกลัวว่า พนักงานเจ้าหน้าที่ยิ่งเยอะยิ่งมั่ว เพราะต่างหน่วยงานต่างขอแต่งตั้งเจ้าหน้าที่ แล้วเวลาเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ในหน่วยงานต่างๆ ขอข้อมูลไปที่ไอเอสพี เขาไม่ต้องรายงานเลย ไปออกเป็นหนังสือเซ็นออกไปได้เลย ตอนนี้เราก็ไม่รู้ว่าพนักงานเจ้าหน้าที่หน่วยอื่นขอข้อมูลอะไรไปจากไอเอสพีบ้าง ก็เคยมีแนวคิดกับส่วนที่เกี่ยวข้องว่า หากใครขออะไรก็ทำสำเนามาหน่อยได้ไหม เดี๋ยวมีปัญหาใช้อำนาจเกินขอบเขต"

(เจ้าหน้าที่ (ขอสงวนนาม) กระทรวงไอซีที, 2553)

"ความเข้าใจคอมพิวเตอร์ของเจ้าหน้าที่หลายระดับหลายส่วนงานยังมีปัญหา เช่น จะให้อธิบายคำศัพท์เทคนิคอย่างไรในศาล เช่น คำว่าโดเมนจะอธิบายว่าอย่างไร ในการสอบสวนงานพนักงานอัยการต้องจับกฎหมาย ซึ่งบางเรื่องมันเป็นเทคโนโลยีที่มีความเคลือบแคลงสงสัยขึ้นและเป็นประโยชน์กับผู้ต้องหา เป็นสิ่งที่เจอในศาลบ่อยๆ เช่น แฮกเกอร์คืออะไร เว็บเพจหมายถึงอะไร การเข้าถึงโดยไม่ถูกต้องหมายถึงอะไร"

(พ.ต.อ. อนุชิต บุญญะปฏิภาค กองพิสูจน์หลักฐานกลาง, 2554)

(4) ขอบเขตของอำนาจเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550

มาตรา 26 ของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 กำหนดหน้าที่แก่ผู้ให้บริการว่าต้องเก็บข้อมูลจราจรคอมพิวเตอร์เอาไว้ไม่น้อยกว่าเก้าสิบวัน และมาตรา 18 กำหนดอำนาจของพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในการสอบถาม เรียกดูข้อมูล ทำสำเนาข้อมูลคอมพิวเตอร์ ฯลฯ ทั้งนี้ ในมุมมองเจ้าหน้าที่รัฐมองว่าที่ผ่านมาพบอุปสรรคการทำงานในขั้นตอนนี้ เพราะในขณะที่กฎหมายเขียนให้อำนาจไว้ ก็สามารถถูกตีความได้ด้วยเช่นกันว่า เป็นการตัดอำนาจเจ้าหน้าที่สืบสวนสอบสวนคนอื่นๆ ที่ไม่ได้เป็นเจ้าพนักงานตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550

“กฎหมายมันบิดเบี้ยวเพราะการตีความ มันถูกตีความว่าตำรวจทั่วไปไม่สามารถใช้อำนาจตามมาตรา 18 ได้ ซึ่งอำนาจตามมาตรา 18 มีสองส่วน คือ ส่วนที่ต้องใช้อำนาจศาลและส่วนที่ไม่ต้องใช้ ส่วนที่ไม่ต้องใช้อำนาจ คือ อำนาจของพนักงานสอบสวนในการเรียกข้อมูล ฯลฯ แต่ส่วนที่ต้องใช้อำนาจศาล พนักงานสอบสวนก็ต้องขอศาลเหมือนกัน เราจึงต้องแก้ความเข้าใจของคน ไม่ว่าจะเป็นพนักงานสอบสวน หรือไอเอสพี ไม่อย่างนั้นคุณต้องตั้งพนักงานเจ้าหน้าที่กี่คนเพื่อรองรับคดีที่เกี่ยวกับคอมพิวเตอร์และการทำคดีก็ต้องใช้ความรู้”

(เจ้าหน้าที่ตำรวจผู้เชี่ยวชาญเทคโนโลยี (ขอสงวนนาม) สำนักงานตำรวจแห่งชาติ, 2554)

เจ้าหน้าที่จากกระทรวงไอซีทีและเจ้าหน้าที่ตำรวจผู้เชี่ยวชาญด้านเทคโนโลยีจากสำนักงานตำรวจแห่งชาติกล่าวว่า ทุกวันนี้เมื่อมีคดีต้องติดตามหาตัวผู้กระทำผิด ผู้ให้บริการจะยอมให้ข้อมูลแก่ผู้ที่ได้รับแต่งตั้งเป็นพนักงานเจ้าหน้าที่เท่านั้น ซึ่งโดยส่วนตัวเขากลับเห็นว่าพนักงานสอบสวนทั่วไปก็ควรมีอำนาจในการขอข้อมูลจากผู้ให้บริการด้วย เช่น การขอไอพีแอดเดรส ซึ่งเป็นข้อมูลพื้นฐานในการทำคดีประเภทอื่นๆ อำนาจนี้ไม่ควรจำกัดเฉพาะผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 เท่านั้น เพราะจะทำให้เรื่องทุกเรื่องมากระจุกตัว

อยู่ที่ศูนย์กลาง ทั้งที่ในความเป็นจริงอาชญากรรมต่างๆ สมัยนี้ ไม่ว่าจะเป็นค้ายาเสพติด ค้ามนุษย์ ฯลฯ แม้ไม่ได้มีลักษณะที่เข้าว่าเป็นอาชญากรรมคอมพิวเตอร์ แต่ก็มักมีพยานหลักฐานอิเล็กทรอนิกส์เข้ามาเกี่ยวข้องด้วย

"การขอข้อมูลจากผู้ให้บริการมีขั้นตอนยากเกินความจำเป็น อีกทั้งยังมีเรื่องความรับผิดของเจ้าหน้าที่ เช่น เมื่อไปขอไอพีแอดเดรสมาแล้ว ก็ต้องมีความชัดเจนว่าจะเอาข้อมูลนั้นไปใช้ทำอะไร หากขอข้อมูลไปโดยเหตุที่ไม่จำเป็นก็ต้องรับผิดชอบ อย่างไรก็ตาม ต้องให้อำนาจส่วนนี้แก่เจ้าหน้าที่อื่นๆ ด้วย เพราะบางเรื่องมีความจำเป็นและต้องทำโดยเร็ว เกี่ยวกับความเป็นความตาย ข้อมูลส่วนนี้เป็นเพียงเศษเสี้ยวของพยานหลักฐานเท่านั้น แต่หากการขอข้อมูลส่วนนี้เป็นไปด้วยความยากลำบาก ส่วนที่เหลือก็ไม่ต้องพูดถึง"

(เจ้าหน้าที่ตำรวจผู้เชี่ยวชาญเทคโนโลยี (ขอสงวนนาม) สำนักงานตำรวจแห่งชาติ, 2554)

"สืบเนื่องจากกระแสที่ไม่ไว้วางใจตำรวจ เนื้อหาของร่างกฎหมายจึงถูกปรับแก้โดยถอดเอาอำนาจตำรวจออกเยอะมาก กฎหมายนี้เลยเขียนปัดความรับผิดชอบทั้งหมดไปให้คนกลุ่มใหม่ที่เรียกว่า พนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งตอนนั้นจะมีภาพร่างที่จินตนาการกันว่าจะต้องมี "พนักงานพันธุ์ใหม่" ที่เหมือนซุปเปอร์แมนมาใช้บังคับกฎหมายฉบับนี้ ในขณะที่ภาครัฐเองก็ไม่ได้มีความเข้าใจเรื่องอาชญากรรมคอมพิวเตอร์กันดีพอ เรียกได้ว่าเหตุการณ์ใดที่มีคอมพิวเตอร์เข้ามาเกี่ยวข้อง ก็จะปัดมาให้พนักงานเจ้าหน้าที่ตามกฎหมายนี้เลย"

"มันยังก้ำกึ่งระหว่างกฎหมายอาญา กับ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ว่าพนักงานสอบสวนใช้อำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญาเพื่อยึดอายัดคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ได้หรือไม่ สมมติว่ามันไม่ใช่คดีที่เป็นอาชญากรรมคอมพิวเตอร์โดยแท้ (pure cyber crime) เช่น คดีค้ายาเสพติดในระบบอินเทอร์เน็ต เราก็ต้องกลับมาคิดแล้วนะว่า ปปส. ยังจะใช้อำนาจของเขาได้ไหม ตรงนี้อำนาจมันยังไม่ชัด สมมติ ปปส.

พบคนขายยาในเน็ต จะขอไอพีจากผู้ให้บริการเลยโดยไม่ต้องมาผ่านไอซีทีเลยได้หรือไม่ ซึ่งผมยังเชื่อว่าตาม ป.วิ อาญา น่าจะขอได้ แต่ถ้าผู้ให้บริการเขาบอกว่าขอเขาได้แต่เฉพาะพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์เท่านั้น ทุกหน่วยก็จะดิ้นรนอยากเป็นพนักงานเจ้าหน้าที่กัน"

(เจ้าหน้าที่ (ขอสงวนนาม) กระทรวงไอซีที, 2553)

"ถ้าพนักงานตำรวจทั่ว ๆ ไปมีอำนาจตรวจสอบข้อมูลได้ เช่น ทำเรื่องการเงินก็ตรวจสอบเรื่องการเงินได้ ทำเรื่องไซเบอร์ก็ตรวจสอบเรื่องไซเบอร์ได้ การแต่งตั้งพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ก็จะลดลง"

(เจ้าหน้าที่ตำรวจผู้เชี่ยวชาญเทคโนโลยี (ขอสงวนนาม) สำนักงานตำรวจแห่งชาติ, 2554)

3) ความคิดเห็น และข้อเสนอแนะเพิ่มเติมเกี่ยวกับการแก้ไข และการใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

จากการสอบถามมุมมองและทัศนคติของบุคลากรภาครัฐที่มีต่อการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 และนโยบายที่เกี่ยวข้องนั้น พบว่าในประเด็นที่เกี่ยวกับมาตรการระงับการเผยแพร่เนื้อหาหรือปิดกั้นเว็บไซต์นั้น เจ้าหน้าที่ภาครัฐส่วนใหญ่เห็นว่ายังเป็นมาตรการที่จำเป็นอยู่ เพราะช่วยบรรเทาปัญหาได้ ส่วนการดำเนินคดีที่เกี่ยวกับคอมพิวเตอร์ บุคลากรภาครัฐเสนอให้เพิ่มอำนาจแก่พนักงานเจ้าหน้าที่สอบสวนทั่วไป ให้สามารถใช้อำนาจในการขอดู ขอทำสำเนา และยึดอายัดพยานหลักฐานอิเล็กทรอนิกส์ได้ โดยมีพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งแต่งตั้งโดยรัฐมนตรีกระทรวงไอซีทีทำหน้าที่เป็นหน่วยสนับสนุนหรือให้ความช่วยเหลือเฉพาะทางแก่เจ้าหน้าที่อื่นๆ เหล่านั้น นอกจากนี้ยังมีความเห็นจากแหล่งข้อมูลส่วนหนึ่งว่า ควรมีการตั้งศาลชำนัญพิเศษเพื่อพิจารณาคดีตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 หรือมีผู้พิพากษาสมทบที่มีความรู้ความเชี่ยวชาญด้านคอมพิวเตอร์ร่วมพิจารณาคดีที่เกี่ยวข้องกับคอมพิวเตอร์กับ

ผู้พิพากษาอาชีพ

(1) ทัศนะต่อมาตรการปิดกั้นเว็บไซต์

สำหรับทัศนคติของภาครัฐที่มีต่อการปิดกั้นเว็บไซต์นั้น คณะผู้วิจัยพบว่าเจ้าหน้าที่รัฐยังเห็นว่า กลไกนี้มีความจำเป็น ถึงแม้จะไม่สามารถแก้ปัญหาได้ตรงจุด แต่ก็ช่วยบรรเทาปัญหาให้ลดน้อยลงได้

"การวิพากษ์วิจารณ์ อย่างคลิปต่างๆ ซึ่งอาจจะก่อให้เกิดความไม่สงบในบ้านเมืองนั้นเราไม่ได้ปิดกั้น เราเรียกว่าระงับ คือชะลอ บรรเทา เหมือนกับเราเกิดอุบัติเหตุเรื่องไหน เกิดแผลตรงไหน เราก็ต้องเอานิ้วกดแผลไว้เพื่อเลือดจะได้ไหลน้อยลง โดยขออำนาจศาลให้ระงับการเข้าถึง"

(พนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 (ขอสงวนนาม) กระทรวงไอซีที, 2553)

"การปิดเว็บดีกว่าไม่ได้ทำอะไรเลย เพราะอย่างน้อยก็เป็นการปิดกั้นช่องทาง เป็นการบรรเทาผลร้าย ส่งผลดีในแง่จิตวิทยาสังคม แม้กฎหมายจะบัญญัติไว้กว้าง แต่ขึ้นอยู่กับผู้ใช้ผู้ตีความกฎหมายมากกว่า เพราะในประเทศที่เจริญแล้วไม่มีกฎหมายลายลักษณ์อักษรก็ยังไม่มีปัญหา และกระบวนการไม่ได้จบที่กระทรวงไอซีที แต่ยังมีศาลที่มีอำนาจพิจารณาอีกชั้น"

(พ.ต.อ. ศิริพงษ์ ติมุลา รองผบก.ปอท., 2554)

"เห็นว่าไม่ควรปิด เพราะยิ่งปิดก็ยิ่งเปิด เนื่องจากเป็นธรรมชาติของมนุษย์ เช่น เว็บโป๊ ยิ่งปิดก็ยิ่งมีคนอยากรู้ อีกทั้งหากมีการกระทำความผิด การจับผู้กระทำความผิดมาลงโทษน่าจะง่ายและแก้ปัญหาได้มากกว่า นอกจากนี้ มาตรา 20[34] พ.ร.บ.คอมพิวเตอร์ฯ 2550 ก็ใช้ถ้อยคำกว้างๆ ขึ้นอยู่กับดุลพินิจของผู้ใช้"

(นายเกริกไชย ศรีศุกร์เจริญ กรมสอบสวนคดีพิเศษ (ดีเอสไอ), 2554)

(2) วัตถุประสงค์ หรือหน้าที่ของ พ.ร.บ.คอมพิวเตอร์ฯ 2550

สำหรับประเด็นด้านความเหมาะสมของฐานความผิดที่กำหนดไว้ใน พ.ร.บ.คอมพิวเตอร์ฯ 2550 นั้น นายเกริกชัย ศรีศุกร์เจริญ กรมสอบสวนคดีพิเศษ มีความเห็นว่า หากในอนาคตจะมีการแก้ไขปรับปรุง พ.ร.บ.คอมพิวเตอร์ฯ 2550 ก็ควรเน้นความผิดต่อระบบคอมพิวเตอร์เท่านั้น โดยตัดความผิดในส่วนของการเผยแพร่เนื้อหาในเครือข่ายคอมพิวเตอร์ออก เนื่องจากซ้ำซ้อนกับกฎหมายอื่นๆ ที่มีอยู่แล้ว วัตถุประสงค์หลักของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ควรมีขึ้นเพื่อแก้ปัญหาอาชญากรรมคอมพิวเตอร์โดยแท้

"ในแง่ของความรับผิด มีการใช้มาตรา 14 (2) กันเยอะ และมีปัญหามาก ซึ่งร่างเดิมไม่มีมาตรานี้ แต่พอเกิดเหตุการณ์ความวุ่นวายทางการเมืองเข้ามา ก็จึงเพิ่มเข้าไป เห็นว่าถ้าตัดมาตรา 14 ไปก็ไม่มีปัญหาอะไร ส่วนมาตรา 16 ก็สามารถใช้ความผิดฐานหมิ่นประมาท (ตามประมวลกฎหมายอาญา) ได้อยู่แล้ว จริงๆ แล้ว พ.ร.บ.คอมพิวเตอร์ฯ 2550 ควรบัญญัติเฉพาะความผิดเกี่ยวกับเรื่องทางเทคนิคล้วนๆ"

(นายเกริกไชย ศรีศุกร์เจริญ กรมสอบสวนคดีพิเศษ (ดีเอสไอ), 2554)

(3) ตั้งศาลชำนาญพิเศษ

พ.ต.อ. ศิริพงษ์ติมุลา รองผบก. ปอท. และนายเกริกไชย ศรีศุกร์เจริญ กรมสอบสวนคดีพิเศษ มีความเห็นว่า ควรมีการจัดตั้งศาลชำนัญพิเศษเฉพาะทางเพื่อพิจารณาพิพากษาคดีความผิดที่เกี่ยวกับคอมพิวเตอร์

"เห็นด้วยกับการมีศาลชำนัญพิเศษเรื่องคอมพิวเตอร์ เป็นเรื่องจำเป็น"

(พ.ต.อ. ศิริพงษ์ ติมุลา รองผบก.ปอท., 2554)

"ต่อไปเราอาจต้องมีการจัดตั้งศาลคอมพิวเตอร์ขึ้นมาเป็นศาลชำนาญการ เพราะคดีลักษณะนี้จำเป็นอย่างยิ่งที่ศาล อัยการ ต้องมีความรู้

เรื่องคอมฯ หรือมิเช่นนั้นก็ควรมีผู้พิพากษาสมทบซึ่งเป็นผู้เชี่ยวชาญด้านนี้"

(นายเกริกไชย ศรีศุกร์เจริญ กรมสอบสวนคดีพิเศษ (ดีเอสไอ), 2554)

2.2 บทบาทของผู้ประกอบการอินเทอร์เน็ต ภายใต้ พ.ร.บ. คอมพิวเตอร์ฯ 2550 ในส่วนที่กระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชน

วิธีศึกษา

การศึกษาส่วนนี้ คณะผู้วิจัยใช้วิธีศึกษาด้วยการจัดสัมมนากลุ่มย่อย (focus group) เพื่อรวบรวมข้อมูลจาก "ผู้ให้บริการ" ซึ่งเป็นผู้ประกอบการอินเทอร์เน็ต ไม่ว่าจะเป็น กลุ่มผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต ผู้ประกอบการเว็บโฮสติ้ง (ผู้ให้บริการให้เช่าใช้พื้นที่ในเครื่องคอมพิวเตอร์) และดาตาเซ็นเตอร์ หรือผู้ให้บริการพื้นที่จัดเก็บเนื้อหา ซึ่งแม้แหล่งข้อมูลจะมาจากหน่วยงานที่แตกต่างกัน แต่ปรากฏว่าล้วนมีประสบการณ์เกี่ยวกับ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ที่คล้ายคลึงกัน

คณะผู้วิจัยได้ทำจดหมายไปยังบริษัทกลุ่มผู้ประกอบการ และอาศัยเครือข่ายเพื่อขอคำแนะนำบุคคลต่างๆ เพื่อให้ได้บุคลากรที่สามารถให้ข้อมูลได้จริง และเชิญเข้าร่วมการสัมมนากลุ่มย่อย แหล่งข้อมูลที่เข้าร่วมมีทั้งสิ้น 14 คน จาก 8 หน่วยงาน โดยมีกลุ่มผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต ประกอบด้วยฝ่ายนิติกรจากบริษัท กสท โทรคมนาคม จำกัด (มหาชน) จำนวน 2 คน ผู้ชำนาญการฝ่ายกฎหมาย บริษัท แอดวานซ์ อินโฟ เซอร์วิส จำกัด (มหาชน) จำนวน 1 คน สายงานรัฐกิจสัมพันธ์ บมจ.โทเทิ่ล แอ็คเซ็ส คอมมูนิเคชั่น จำนวน 3 คน ฝ่ายกฎหมาย บริษัท ทีทีแอนด์ที จำกัด (มหาชน) จำนวน 2 คน ตัวแทนจากบริษัท ทรู คอร์ปอร์เรชั่น จำกัด (มหาชน) จำนวน 1 คน กลุ่มผู้ประกอบการเว็บโฮสติ้ง ได้แก่ ตัวแทนจากบริษัท เอเน็ต จำกัด จำนวน 3 คน ตัวแทนจากชมรมผู้ประกอบการธุรกิจโฮสติ้ง จำนวน

1 คน และตัวแทนจากบริษัท โปรอิมเมจ เอ็นจิเนียริ่ง แอนด์ คอมมูนิเคชั่น จำกัด จำนวน 1 คนซึ่งเป็นทั้งผู้ประกอบการเว็บโฮสติ้งและดาตาเซ็นเตอร์

ก่อนเริ่มสัมมนามีการทำความตกลงร่วมกันว่าจะเก็บข้อมูลด้วยการบันทึกเสียงและจดบันทึก และกำหนดเงื่อนไขอื่นๆ ในการระบุชื่อและเอกลักษณ์ของแหล่งข้อมูล ทั้งนี้ ในข้อตกลงดังกล่าว ผู้เข้าร่วมไม่สะดวกที่จะให้เปิดเผยเอกลักษณ์ของตนเอง ดังนั้น ในงานวิจัยฉบับนี้จึงไม่เปิดเผยชื่อ และตำแหน่ง แต่จะใช้วิธีกำกับตัวผู้ให้บริการแต่ละคนด้วยหมายเลขแทน

แนวคำถามสำหรับผู้ให้บริการ

• ภารกิจและหน้าที่ของหน่วยงานในส่วนที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ฯ 2550

• ลักษณะงานและความรับผิดชอบขององค์กรที่ต้องปรับเปลี่ยนภายหลังประกาศใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

• รูปแบบการกระทำความผิดที่พบจากการใช้งานของผู้ใช้บริการและช่องทางการรับแจ้งการกระทำความผิด

• ความสะดวก หรืออุปสรรคที่เกิดขึ้นจาก พ.ร.บ.คอมพิวเตอร์ 2550

• แรงกดดันจากปัญหาทางการเมืองที่ส่งผลต่อการทำงานขององค์กร

• ขั้นตอน รูปแบบ และปัญหาที่พบจากการประสานความร่วมมือระหว่างผู้ให้บริการกับเจ้าหน้าที่รัฐ

• หลักเกณฑ์ แนวปฏิบัติ หรือคู่มือการปฏิบัติงานขององค์กรเพื่อกำกับดูแลเนื้อหาในพื้นที่บริหาร และการประสานงานกับภาครัฐ

• ข้อตกลง และการประสานความร่วมมือในระหว่างกลุ่มผู้ให้บริการเพื่อเฝ้าระวังเนื้อหา

• ความเห็นต่อมาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550 หรือมาตรการระงับการเผยแพร่เนื้อหา หรือปิดกั้นเว็บไซต์ ทั้งในประเด็นความ

ชัดเจนของเงื่อนไข และขั้นตอนในการสั่งปิดกั้นเว็บไซต์

• ลักษณะของเนื้อหา กระบวนการปิดกั้น และปริมาณเว็บไซต์ที่ปิดกั้นเปรียบเทียบก่อน และหลังการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

• นโยบายในการแจ้งเหตุผลของการปิดกั้นไปยังผู้ใช้บริการ

• ผลกระทบของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ต่อเสรีภาพในการเข้าถึงข้อมูล และการแสดงความคิดเห็นของประชาชน รวมทั้งเสรีภาพของผู้ให้บริการ

• ความเห็นต่อมาตรา 15 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ที่เกี่ยวกับความรับผิดของตัวกลาง ทั้งในประเด็นความชัดเจนของคำนิยามผู้ให้บริการ ภาระหน้าที่ และอัตราโทษ

• ความเหมาะสมของภาระหน้าที่ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ และระยะเวลาในการจัดเก็บข้อมูลดังกล่าว

• ข้อเสนอแนะเกี่ยวกับ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ทั้งในแง่เจตนารมณ์ บทบัญญัติ อัตราโทษ ประสิทธิภาพ ฯลฯ

• ทัศนคติต่อสื่อใหม่/สื่อพลเมือง และข้อเสนอแนะเพิ่มเติมเกี่ยวกับนโยบาย "สื่อออนไลน์" รวมทั้งข้อเสนอแนะต่อประชาชนผู้ใช้บริการสื่อออนไลน์

ผลการศึกษา

จากการประมวลผลข้อมูลที่ได้จากการจัดสัมมนา สามารถแบ่งประเด็นการศึกษาได้ดังนี้

1) ลักษณะการทำงานของผู้ให้บริการภายใต้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่เกี่ยวกับเสรีภาพในการเข้าถึงข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน

2) ปัญหาที่พบจากการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่เกี่ยวกับเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน

3) ความคิดเห็นและข้อเสนอแนะต่อกฎหมาย และแนวนโยบายของรัฐ

1) ลักษณะการทำงานของผู้ให้บริการภายใต้ พ.ร.บ. คอมพิวเตอร์ฯ 2550 ในส่วนที่เกี่ยวกับเสรีภาพในการเข้าถึงข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน

อาจกล่าวได้ว่า ที่ผ่านมาภาระหน้าที่หลักของผู้ให้บริการอินเทอร์เน็ตนั้น นอกจากการให้บริการแก่ลูกค้าของตนแล้ว ยังต้องคอยให้ความร่วมมือกับเจ้าหน้าที่รัฐในเรื่องต่างๆ ด้วย โดยเฉพาะอย่างยิ่งการปิดกั้นเว็บไซต์ อย่างไรก็ตาม ภายหลังประเทศไทยมี พ.ร.บ. คอมพิวเตอร์ฯ 2550 วิธีการรวมทั้งรูปแบบในส่วนการทำงานประสานกับเจ้าหน้าที่รัฐของผู้ให้บริการก็เปลี่ยนแปลงไปมาก โดยผู้ให้บริการส่วนใหญ่ให้ข้อมูลตรงกันว่า ก่อนมี พ.ร.บ.คอมพิวเตอร์ฯ 2550 การขอความร่วมมือจากรัฐให้ปิดเว็บไซต์เป็นไปอย่างไม่เป็นทางการและไร้แบบแผนที่ชัดเจน หลายกรณีพบว่าลักษณะความผิดของเนื้อหาของเว็บไซต์ที่รัฐต้องการให้ปิดกั้นนั้นขาดความชัดเจน หรือเป็นเนื้อหาที่ไม่มีลักษณะที่ควรถูกปิดกั้นเลย แต่ผู้ให้บริการก็ถูกขอความร่วมมือให้ปิดกั้น แต่หลังจาก พ.ร.บ.คอมพิวเตอร์ฯ 2550 ใช้บังคับ กระบวนการและขั้นตอนในการปิดเว็บไซต์ก็ชัดเจนมากขึ้น ทั้งยังเป็นไปตามกฎหมาย โดยปัจจุบัน ผู้ให้บริการส่วนใหญ่ยึดหลักว่าจะปิดกั้นตามคำสั่งศาลเท่านั้น

“ก่อนที่จะมี พ.ร.บ.คอมพิวเตอร์ฯ 2550 การปิดกั้นเว็บไซต์เป็นไปอย่างไม่มีแบบแผนเปิดกว้างมาก หนังสือที่รัฐส่งมาเป็นหนังสือขอความร่วมมือ ซึ่งผู้ประกอบการจะไม่ให้ความร่วมมือก็ไม่ได้ เวลาปิดก็ปิดทีละสิบยี่สิบยูอาร์แอล และอย่างที่เรารู้ ในโลกไซเบอร์ ปิดที่หนึ่งเนื้อหานั้นก็จะไปปรากฏอีกที่หนึ่งอยู่ดี ทั้งหมดนี้เป็นความหนักใจของผู้ประกอบการ แต่พอมีกฎหมายนี้ขึ้นมา ต่อไปนี้ถ้าจะปิดกั้นเว็บไซต์ต้องมีคำสั่งศาล เป็นผลทำให้จำนวนการปิดกั้นลดลง อย่างไรก็ตาม การปิดยังคงเป็นไปอย่างสะเปะ

สะปะในแง่ของเนื้อหา ดังนั้น ข้อดีของการมีกฎหมายก็คือ ทำให้การปิดกั้นชัดเจนมากขึ้น ต้องมีคำสั่งศาล หรืออย่างน้อยก็มีขั้นตอนการกลั่นกรอง"

"ตอนที่ยังไม่มีหมายศาล ก็เคยปฏิเสธ เพราะเท่าที่ทราบมาการปฏิเสธก็ไม่มีผลอะไร เพราะการขอความร่วมมือมันก็เป็นเรื่องเทาๆ บางครั้งก็มีการสอดไส้ เช่น บอกว่าเป็นเรื่องประเภทหนึ่ง แต่จริงๆ แล้วไม่ใช่"

(ผู้ประกอบการหมายเลข 3, 2554)

"ช่วงที่มีปัญหาหนัก คือช่วงรัฐประหาร ซึ่งมีการบล็อคเว็บโดยแจ้งกันทางโทรศัพท์ มีทั้งสั่งให้ปิดกั้น และสั่งให้ลบ ซึ่งบางเว็บก็เป็นเว็บธรรมดาไม่น่าจะผิดกฎหมายอะไร ซึ่งทางเราจะบอกให้แฟกซ์มาเป็นเอกสาร หรือทำเป็นหนังสือมา บางครั้งคนที่โทรมาก็บอกว่า ไม่เป็นไร ถ้าคุณไม่ทำผมจัดการเอง แต่พอมี พ.ร.บ.คอมพิวเตอร์ฯ 2550 แล้ว ก็เป็นไปตามคำสั่งศาล พอมีคำสั่งศาลแล้ว หากมีเรื่องอะไรทางเราก็สามารถอ้างคำสั่งศาลได้"

(ผู้ประกอบการหมายเลข 1, 2554)

"การสั่งให้ปิดกั้น บางครั้งจะมีการสอดไส้มาด้วย โดยผู้สั่งจะให้มาเป็นเลขยูอาร์แอล ซึ่งปรกติฝ่ายกฎหมายของเราจะกรองก่อน หากพบว่าเป็นเนื้อหาที่สอดไส้มา (ไม่ได้มีเนื้อหาตามที่แจ้ง – คณะผู้วิจัย) ทางเราก็จะแจ้งไปทางเจ้าหน้าที่ นอกจากนี้ ก็มีปัญหาการขอผิดประเภท เช่น จะบล็อกเฟซบุครายบุคคล แต่ให้ยูอาร์แอลมาผิด เป็นต้น ทำให้ลูกค้าหลายคนเข้าเฟซบุคตัวเองไม่ได้ ที่ผ่านมามีความผิดพลาดพวกนี้เยอะ นี่ยังไม่นับว่ามีกรณีพิมพ์ผิด พิมพ์ตกหล่นด้วย"

"เรื่องจำนวนการปิดเว็บ ผมเข้าใจว่าตอนนี้ไม่ใช่หลักหมื่นนะ ต้องเป็นแสนแล้ว เพราะมันไม่มีการยกเลิกการปิดกั้นเลย มันมีแต่ให้ปิดกั้นเพิ่มขึ้น"

(ผู้ประกอบการหมายเลข 4, 2554)

นอกจากการปิดกั้นเว็บไซต์แล้ว ปัจจุบันผู้ให้บริการยังมีหน้าที่ตามกฎหมายต้องเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันด้วย ทั้งนี้ เพื่อให้ข้อมูลแก่พนักงานเจ้าหน้าที่ ในกรณีที่จะมีการดำเนินคดีกับผู้กระทำความผิด อย่างไรก็ตาม ก่อนหน้าที่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 จะมีผลใช้บังคับก็มีกรณีที่เจ้าหน้าที่รัฐขอข้อมูลการใช้บริการลักษณะนี้จากผู้ให้บริการเช่นกัน แต่ในขณะนั้นผู้ให้บริการสามารถปฏิเสธไม่ให้ข้อมูลได้โดยอ้างเหตุผลเรื่อง “ข้อมูลส่วนบุคคล” ของลูกค้า แต่เมื่อ พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีผลใช้บังคับแล้ว กฎหมายกำหนดให้เป็นหน้าที่ และหากไม่ปฏิบัติตามก็มีความผิดและโทษ อย่างไรก็ตาม ยังมีความไม่ชัดเจนในหมู่ผู้ให้บริการว่า การส่งมอบข้อมูลให้กับภาครัฐนั้น ผู้ให้บริการมีหน้าที่ต้องมอบให้เฉพาะกับเจ้าพนักงานตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 เท่านั้น หรือต้องมอบให้เจ้าหน้าที่ตำรวจหรือพนักงานสอบสวนในคดีอื่นๆ ด้วย

“ถ้าเป็นสมัยก่อนที่จะมี พ.ร.บ.คอมพิวเตอร์ฯ 2550 ผมเข้าใจว่าทางบริษัทเราไม่ให้ข้อมูลเลย มันให้ไม่ได้ เพราะเป็นข้อมูลลูกค้า เป็นข้อมูลส่วนตัว แต่หลังประกาศใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ถ้าคนที่มาขอข้อมูลจราจรคอมพิวเตอร์เป็นเจ้าพนักงานตามกฎหมายฉบับนี้ เราก็สบายใจที่จะให้เพราะเขามีอำนาจ แต่ถ้าเป็นตำรวจจากสถานีตำรวจเราก็มักปฏิเสธ เนื่องจากไม่มีหน้าที่ต้องให้ โดยเราจะตรวจสอบด้วยว่าเป็นเจ้าพนักงานจริงหรือไม่”

(ผู้ประกอบการหมายเลข 4, 2554)

“ผมว่า เจ้าหน้าที่ตำรวจมีอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญาที่จะขอข้อมูลได้นะ”

(ผู้ประกอบการหมายเลข 5, 2554)

2) ปัญหาที่พบจากการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่เกี่ยวกับเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน

เนื่องจากมาตรา 15 พ.ร.บ.คอมพิวเตอร์ฯ 2550 กำหนดว่าผู้ให้บริการที่ “จงใจสนับสนุน หรือยินยอม” ให้มีการเผยแพร่ข้อความที่เป็นความผิด (ตามมาตรา 14 พ.ร.บ.คอมพิวเตอร์ฯ 2550) มีความผิดและต้องรับโทษเท่ากับผู้ที่โพสต์หรือเผยแพร่ข้อความ แต่ปัญหาสำคัญในประเด็นนี้ก็คือ ของคำว่า จงใจสนับสนุนและยินยอมตามมาตรานี้มีความหมายอย่างไร อีกทั้งยังมีปัญหาในประเด็น “ระยะเวลา” ในการดำเนินการกับเนื้อหาที่อาจเข้าข่ายเป็นความผิดด้วย เนื่องจากจนถึงปัจจุบันก็ยังเป็นที่สงสัยว่าผู้ให้บริการจะต้องดำเนินการรวดเร็วเพียงใดกับเนื้อหาเหล่านั้นจึงจะหลุดพ้นจากการ “จงใจสนับสนุนหรือยินยอม” ให้มีการเผยแพร่ข้อความที่เข้าข่ายผิดกฎหมาย อย่างไรก็ตาม แม้ผู้ให้บริการจะต้องการให้ความร่วมมือ หรือมีความพยายามในการเร่งดำเนินการเพียงใด แต่บางครั้งข้อมูลที่ภาครัฐแจ้งให้ปิดกั้นก็อาจมีความผิดพลาดในเรื่องแหล่งที่อยู่ออนไลน์ หรือเป็นข้อมูลที่ไม่อยู่ในสภาพที่ผู้ให้บริการจะดำเนินการโดยรวดเร็วได้ มาตรานี้จึงเป็นปัญหาอย่างยิ่งกับผู้ให้บริการในประเทศไทย

“ผมคิดว่าในคำสั่งศาลน่าจะระบุระยะเวลาให้ดำเนินการด้วย ซึ่งก็ไม่น่าจะมีกรณีที่มีหมายศาลมาแล้วผู้ประกอบการจะไม่ทำตาม”

(ผู้ประกอบการหมายเลข 5, 2554)

“ในทางปฏิบัติ เรื่องเนื้อหา เราก็ต้องเอาออกก่อน แล้วค่อยตรวจสอบข้อความอีกครั้ง ทางไอเอสพีเองผมว่าถ้าซีเรียส โดยเฉพาะอย่างยิ่งประเด็นหมิ่นสถาบันฯ ทุกเจ้าลบได้ทันทีภายใน 24 ชั่วโมง ส่วนกรณีอื่นภายใน 48 ชั่วโมงก็สามารถเอาลงได้หมด”

(ผู้ประกอบการหมายเลข 3, 2554)

“จริงๆ แล้วเรื่องทางเทคนิคใช้เวลาไม่นานครับ ถ้าระบุมาเป็นยูอาร์แอลเลย ส่วนใหญ่การบล็อคก็จะใช้เวลาไม่เกิน 24 ชั่วโมง แต่มันอาจมีรายละเอียดว่าบางเว็บเราเองก็บล็อคไม่ได้ เพราะอุปกรณ์ที่มีอยู่บล็อคไม่ได้จริงๆ หรือหากบางกรณีถ้าเป็นเนื้อหาในประเทศ เราก็จะคุยกันว่าน่าจะไป

คุยกับต้นตอตรงๆ ก่อน ไอเอสพีไม่น่าจะต้องคอยปิดกั้นไปหมด เพราะถ้าปิดเยอะๆ เข้า โดยเฉพาะอย่างยิ่ง การปิดกั้นเว็บไซต์ในประเทศ มันก็ลำบากในเรื่องอุปกรณ์ อันนี้เป็นเทคนิคลึกๆ ที่ผมไม่แน่ใจว่าทางเจ้าหน้าที่เข้าใจหรือเปล่า แต่เข้าใจว่าระหว่างฝ่ายกฎหมาย กับเจ้าหน้าที่มีการประสานกันอยู่ตลอดว่าอะไรทำได้หรืออะไรทำไม่ได้"

(ผู้ประกอบการหมายเลข 4, 2554)

ปัญหาหนึ่งที่มาจากการปิดกั้นเว็บไซต์ก็คือ คนทั่วไปจะไม่มีโอกาสทราบว่าเหตุใดจึงไม่สามารถเข้าเว็บไซต์นั้นได้ เพราะเมื่อมีคำสั่งปิดกั้น ผู้ใช้บริการทั่วไปก็จะเข้าดูเว็บไซต์นั้นไม่ได้ แต่ไม่รู้ว่าเป็นเพราะความผิดพลาดทางเทคนิค หรือเป็นเพราะถูกปิดกั้นตามคำสั่งศาล ซึ่งปัจจุบันยังไม่มีแนวปฏิบัติที่ชัดเจนร่วมกันระหว่างกระทรวงไอซีทีและผู้ให้บริการว่าจะใช้รูปแบบการแสดงเหตุผลหรือไม่ อย่างไร นอกจากนี้ ก็มักเกิดปัญหาการบังคับใช้กฎหมายไม่ทั่วถึง คือหลังจากมีคำสั่งศาลแล้ว กระทรวงไอซีทีมักใช้วิธีส่งคำสั่งนั้นไปยังผู้ให้บริการอินเทอร์เน็ต ซึ่งข้อเท็จจริงปรากฏว่าผู้ให้บริการบางรายได้รับคำสั่ง แต่บางรายก็ไม่ได้รับ ดังนั้น ในขณะที่บางรายปิดตามคำสั่ง แต่บางรายก็ไม่ได้ปิด ส่งผลให้ผู้ใช้บริการมีความรู้สึกว่าผู้ให้บริการแต่ละรายให้เสรีภาพกับผู้ใช้บริการในระดับที่แตกต่างกัน ซึ่งย่อมส่งผลต่อการประกอบธุรกิจโดยตรง ในท้ายที่สุด ฝ่ายผู้ให้บริการจึงมักตกเป็นจำเลย หรือต้องแบกรับคำถาม คำร้องเรียน และต้องอธิบายชี้แจงเองว่าปิดกั้นด้วยสาเหตุใด ทั้งนี้ เพราะในขณะที่ผู้ให้บริการจำเป็นต้องให้ความร่วมมือกับภาครัฐ แต่อีกด้านหนึ่งก็ต้องสนองความต้องการของผู้ใช้บริการซึ่งเป็นลูกค้าของตนด้วย

"กระทรวงไอซีทีมักไม่ยอมแสดงให้ชัดเจนว่าไอซีทีเป็นคนสั่งให้ปิดกั้น แต่สั่งแค่ให้ทำให้เว็บไซต์เข้าไม่ได้เฉยๆ โดยไม่ต้องบอกเหตุผลกับผู้ใช้บริการ ซึ่งมันเป็นเรื่องที่เป็นไปไม่ได้สำหรับผู้ให้บริการ เพราะถ้าเว็บไหนหายไปเฉยๆ ทุกคนต้องเข้าใจว่าการให้บริการมีปัญหา ลูกค้าก็จะโทรมาถามและต่อว่าว่าเรามีสิทธิอะไรที่จะไม่ให้เขาเข้าเว็บไซต์นั้น หรือหาก

ไอซีทีควบคุมไม่ทั่วถึง ก็จะมีผู้ให้บริการรายเล็กๆ ที่ยังเปิดให้เข้าถึงเว็บไซต์นั้นได้อยู่ ดังนั้น พอเราปิด และบอกว่าทางราชการขอความร่วมมือในการปิดแล้ว ลูกค้าก็จะถามว่าแล้วทำไมคนอื่นๆ เขายังเข้าเว็บนั้นได้ อันนี้เป็นปัญหาของการบังคับใช้ เราจึงมักโดนข้อกล่าวหาว่าปิดกันเอง โดยเฉพาะช่วงที่มีปัญหาทางการเมืองรุนแรง"

(ผู้ประกอบการหมายเลข 4, 2554)

อนึ่ง แม้ปัจจุบันจะมี พ.ร.บ.คอมพิวเตอร์ฯ 2550 และมาตรา 20 แล้วก็ตาม แต่รูปแบบการ "ขอความร่วมมือ" จากฝ่ายรัฐ ก็ยังมีมาอย่างต่อเนื่อง โดยส่วนใหญ่อ้างเหตุผลในแง่ความจำเป็นเร่งด่วน ต้องรีบปิดกั้น โดยขอให้ปิดกั้นไปก่อนแล้วจะส่งคำสั่งศาลตามมาภายหลัง ซึ่งบางครั้งก็ไม่ได้ส่งมาตามที่บอก และการขอความร่วมมือให้ปิดกั้นเรื่องบางเรื่อง ผู้ให้บริการก็ไม่กล้าปฏิเสธ หรือไม่ให้ความร่วมมือ อย่างเรื่องที่เกี่ยวกับสถาบันพระมหากษัตริย์ เป็นต้น

"ถ้ามีคำสั่งศาลมาก็ไม่มีปัญหา เราปิดกั้นให้ แต่ที่มีปัญหา คือขอให้ปิดไปก่อน แล้วคำสั่งศาลจะตามมา แต่สุดท้ายก็ไม่มา โดยเจ้าหน้าที่ที่รับผิดชอบมักอ้างว่าขอไม่ได้ ทุกวันนี้เรื่องก็ยังคาอยู่กับผู้ประกอบการ และผู้ประกอบการก็ไม่กล้าปลดการปิดกั้นนั้นออก จึงอยากขอให้ไอซีทีกำหนดระยะเวลาปิดกั้น หรือมีเงื่อนไขว่าหากเวลาผ่านไปหนึ่งหรือสองเดือนแล้วยังไม่มีคำสั่งศาลก็ให้ปลดออกได้ นอกจากนี้ ไอซีทีสามารถประกาศได้หรือไม่ว่าตนเป็นผู้สั่งปิดเอง และเนื้อหานั้นเป็นความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในฐานใด ส่วนเราผู้ประกอบการก็ได้แต่ทำตามกฎหมายทุกฉบับ แม้ว่ามันอาจจะซ้ำซ้อนกันก็ตาม"

(ผู้ประกอบการหมายเลข 6, 2554)

"ปัญหาอันดับแรกคือ หากบริษัทไม่ให้ความร่วมมือ (แม้ไม่มีคำสั่งศาล - คณะผู้วิจัย) บริษัทจะโดนมองว่า กำลังคิดอะไรอยู่ เช่น รัฐขอความร่วมมือในเรื่องเว็บหมิ่นสถาบันฯ ซึ่งเป็นเรื่องที่ไม่มีใครปฏิเสธได้ ก็จะไม่มี

ใครกล้าไม่ให้ความร่วมมือ แต่ถ้าเป็นเรื่องอื่น เช่น เว็บโป๊ ยังพออ้างได้ ว่าบางคนบอกว่าอันนี้โป๊ บางคนบอกไม่โป๊ แต่ถ้าเป็นเรื่องหมิ่นสถาบันฯ ถ้าไม่ให้ความร่วมมือมันก็ส่อให้เห็นแล้วว่าคุณสนับสนุนหรือเปล่า เอาล่ะ ในทางกฎหมายอาจทำอะไรเราไม่ได้ แต่คงมีการขึ้นแบล็คลิสต์ไว้ในใจแล้ว ว่าเวลาขอความร่วมมือไปแล้วเจ้านี้ไม่ให้"

(ผู้ประกอบการหมายเลข 7, 2554)

"สำหรับโฮสติ้งจะมีการเก็บข้อมูลของผู้เช่าใช้พื้นที่ ใครที่เช่าเพื่อไปทำเรื่องผิดกฎหมายเราก็จะไม่รับอยู่แล้ว เช่น เรื่องการพนัน เรื่องโป๊ โดยเขาก็จะใช้วิธีไปเช่าต่างประเทศ หรือหนีไปอยู่ใต้ดินแทน ถามว่าไม่รู้หรือว่าเขาขอเช่าไปทำเรื่องอะไร ก็ต้องตอบว่า บางทีเราก็ไม่รู้จริง ๆ เพราะมีแค่สาย ไม่รู้จะเข้าเครื่องเขาอย่างไร หรือบางคนให้ข้อมูลมา ให้บัตรประชาชนปลอมมา เราก็ไม่รู้จะไปพิสูจน์อย่างไร นอกจากนี้ ก็มีปัญหาว่า ตอนขอเช่าแจ้งเพื่อวัตถุประสงค์หนึ่ง แต่พอจริง ๆ กลับเอาไปทำเรื่องอื่น ซึ่งเกินความสามารถของผู้ประกอบการที่จะไปตามตรวจสอบได้ เราห้ามผู้ใช้บริการไม่ได้ว่าคุณอย่าอัพโหลด หรือโพสต์อะไรที่ผิดกฎหมาย สิ่งที่เราทำได้ คือ ถ้ามีคนแจ้งมา เราก็จะลบให้ ถ้าไม่มีคนแจ้งเราก็ไม่มีทางรู้ แต่สิ่งที่เกิดขึ้นในช่วงหลัง ๆ ก็คือ ภาครัฐพยายามผลักให้ผู้ให้บริการต้องทำหน้าที่ตรวจตราเนื้อหา ซึ่งเราทำไม่ไหว กลายเป็นว่าเพื่อนบางคนก็ถึงขนาดต้องปิดกิจการไป เพราะไม่อยากแบกรับภาระตรงนี้ มันได้ไม่คุ้มเสีย พอรัฐจับใครไม่ได้ก็จะหันมาจับผู้ให้บริการ"

(ผู้ประกอบการหมายเลข 1, 2554)

3) ความคิดเห็นและข้อเสนอแนะต่อกฎหมาย และแนวนโยบายของรัฐ

ผลการศึกษาในส่วนนี้ รวบรวมความคิดเห็นและข้อเสนอแนะจากผู้ให้บริการอินเทอร์เน็ต ซึ่งคณะผู้วิจัยพบว่า ผู้ให้บริการส่วนใหญ่ยัง

ให้ความสำคัญกับการปิดกั้น หรือระงับการเข้าถึงเว็บไซต์อยู่ โดยมองว่ามีความจำเป็นเพราะมีคนเสียหายจากการแสดงความคิดเห็นในบางเรื่อง อย่างไรก็ตาม รัฐไม่ควรนำมาตรการนี้มาใช้เป็นเครื่องมืออย่างพร่ำเพรื่อในการปิดกั้นสื่อหรือปิดปากประชาชน โดยเฉพาะอย่างยิ่ง ไม่ควรนำเรื่องการเมืองมาเป็นเหตุผลในการปิดกั้น หากเรื่องเหล่านั้นไม่ได้ผิดกฎหมาย

"ถ้าไม่มีการปิดกั้นเลย ผลเสียก็จะตกอยู่กับฝ่ายผู้เสียหาย โดยส่วนตัวผมคิดว่าต้องมี แต่ควรมีการทบทวนว่าอย่าเอามาใช้ในการปิดสื่อ เช่น ในเรื่องทางการเมือง คือตอนนี้กลายเป็นว่า ใครมีอำนาจก็ปิดฝ่ายตรงข้าม และอีกข้อคือ วิธีการอะไรที่เรารู้ว่าทำแล้วไม่ได้ผลก็ต้องปรับเปลี่ยนไปจัดการในลักษณะอื่นที่เหมาะสมแทน เพราะไม่อย่างนั้นจะกลายเป็นว่าเมื่อคนกระทำความผิดแล้วถูกบล็อค เขาก็จะย้ายโดเมนหนี อีกทั้งการปิดกั้นนี้ ผู้ประกอบการต้องใช้อุปกรณ์มากขึ้น มีต้นทุนสูงขึ้น ในที่สุดแล้วก็ต้องผลักภาระไปที่ผู้บริโภค"

(ผู้ประกอบการหมายเลข 3, 2554)

"ผมคิดว่าการปิดกั้นเว็บไซต์ เป็นการบรรเทาความเสียหายในเบื้องต้น ผมเชื่อว่าถ้ามีนโยบายว่าให้ดำเนินการ และเจ้าหน้าที่มีความรู้ความสามารถพอ ผมเชื่อว่าเจ้าหน้าที่ก็จะดำเนินการ"

(ผู้ประกอบการหมายเลข 8, 2554)

"คิดว่ายังต้องมีการปิดเว็บอยู่ เพราะขณะนี้มีการกระทำผิดเยอะ แต่จะต้องไม่เอาไปใช้เพื่อสนองนาย เพื่อการเมือง เพื่อความเกลียดชัง ปัญหาตอนนี้คือ เอาอำนาจไปใช้ในทางผิด และในสังคมเราพ่อแม่ไม่ค่อยให้ความสนใจ พอมีอะไรเกิดขึ้นก็เอาแต่ขอให้มีการเซ็นเซอร์ ทั้งที่จริงเรื่องเหล่านี้ควรเป็นหน้าที่ของครอบครัว จริงๆ มันต้องจัดการเรื่องของตัวเอง ไม่ใช่สั่งให้ทุกคนต้องเห็นเหมือนกันหมด ซึ่งมันเป็นไปไม่ได้"

(ผู้ประกอบการหมายเลข 1, 2554)

“ถ้าดูตามตัวบทแล้ว การจะปิดเว็บจะต้องมีคำสั่งศาล และต้องเป็นเรื่องความมั่นคงและความสงบของรัฐ และศีลธรรมอันดี อันนี้ผมว่าก็ไม่น่าจะมีปัญหา หากไม่ปิดกั้น แล้วเราจะปล่อยมันเอาไว้เฉยๆ อย่างนี้หรือ”

(ผู้ประกอบการหมายเลข 7, 2554)

ผู้ประกอบการบางส่วนเห็นว่า การปิดกั้นเว็บไซต์ที่ให้อำนาจผ่านหน่วยงานศาลเป็นเรื่องเหมาะสมแล้ว แต่น่าจะมีกลไกอื่นๆ เพื่อช่วยแก้ไขปัญหา กรณีที่คำสั่งศาลนั้นไม่ชอบด้วยกฎหมายด้วย ในขณะที่มีผู้ให้บริการบางคนเห็นว่า หากมีกรณีที่ศาลใช้ดุลพินิจออกคำสั่งแล้วส่งผลให้เกิดความเสียหายขึ้น ผู้เสียหายก็คงต้องการร้องเรียนหรือฟ้องกลับ แต่ก็เชื่อว่า หากผู้เสียหายจากการปิดกั้นนั้นรู้ดีอยู่แก่ใจว่าตนทำผิดจริงๆ ก็จะไม่ฟ้องร้อง เพราะต้องเสี่ยงเปิดเผยตัวตน และอาจทำให้ได้รับโทษทางกฎหมายด้วย

“ผมสนับสนุนให้เป็นดุลพินิจของศาลนะครับ แต่สมมติว่าถ้าคำสั่งศาลไม่ชอบขึ้นมาไม่ว่าจะด้วยเหตุผลใดก็ตาม ผมว่ามันต้องมีกลไกแก้ไขด้วย”

(ผู้ประกอบการหมายเลข 3, 2554)

“ผมคิดว่าการให้ดุลพินิจแก่ศาลซึ่งไม่มีส่วนได้เสียเลยเป็นผู้ตัดสินเป็นสิ่งที่ถูกต้องแล้ว ผู้ประกอบการเองคงไม่มีเวลาไปนั่งตรวจสอบ และถ้าให้ผู้ประกอบการมีดุลยพินิจคัดค้าน ก็จะมีปัญหาว่าทุกวันนี้ศรีธนญชัยก็เยอะอยู่แล้ว และผมเชื่อว่าถ้ามีความเสียหายเกิดขึ้น ผู้เสียหายเขาจะร้องเอง การที่เขาไม่ร้องเรียนหรือไม่คัดค้าน ก็คงเป็นเพราะเขารู้ดีแก่ใจว่าตัวเองทำผิด เพราะของอย่างนี้มันใช้วิจารณญาณง่ายๆ ก็เห็นแล้วว่าผิดหรือไม่ผิด”

(ผู้ประกอบการหมายเลข 7, 2554)

อย่างไรก็ดี ปัจจุบันการระงับการเข้าถึงเว็บไซต์ก็ยังมีช่องโหว่ในตัวเอง เพราะทำได้เพียงบรรเทาปัญหา เนื่องจากธรรมชาติของสื่ออินเทอร์เน็ตไม่ใช่สื่อที่ควบคุมได้ง่าย ผู้ให้บริการจึงเสนอข้อควรระวังไว้

ด้วยว่า ที่ผ่านมา พ.ร.บ.คอมพิวเตอร์ฯ 2550 ถูกใช้เป็นเครื่องมือของรัฐมากกว่าที่จะแก้ไขปัญหาให้กับประชาชนที่ได้รับความเดือดร้อน ทั้งเสนอว่ารัฐบาลและศาลไม่ควรใช้การปิดเว็บไซต์กับเรื่องที่ไม่ชัดว่าเป็นความผิดตามกฎหมายหรือไม่ สำหรับกรณีที่มีเว็บไซต์ที่กระทำความผิดจริง และรัฐมีพยานหลักฐานชัดเจน แทนที่รัฐจะใช้วิธีปิดกั้นเว็บไซต์ ซึ่งอาจแก้ปัญหาไม่ได้ เนื่องจากผู้กระทำความผิดยังสามารถไปกระทำความผิดที่อื่นได้ รัฐควรเลือกใช้วิธีแก้ปัญหาที่ต้นเหตุ เช่น ดำเนินคดีกับผู้กระทำความผิดมากกว่า

"ผมคิดว่าการปิดกั้นเป็นมาตรการชั่วคราวและสามารถมีได้ แต่ผมไม่ทราบว่ามีการดำเนินคดีจริงๆ เป็นจำนวนเท่าไร ในความเห็นผม การปิดกั้นมักถูกใช้เป็นเครื่องมือสำหรับความผิดที่เทาๆ คือ รัฐเองก็ไม่แน่ใจว่าจะจับเขาไปดำเนินคดีได้หรือเปล่า แต่อย่างน้อยมันก็เป็นการบรรเทาความเสียหายบางอย่าง คือมันมีช่องทางนี้ที่ใช้ได้ก็ใช้แต่ต้องไม่ลืมว่า การสร้างเว็บนั้นเป็นเรื่องง่ายมาก ถ้าผมสร้างเว็บขึ้นมาแล้วถูกปิด ผมก็ไปสร้างเว็บใหม่ได้ และเราก็เข้าใจว่าตำรวจคงไม่มาจับ ดังนั้น ถ้ามีอะไรที่มันเป็นความผิดจริงๆ ก็ควรหามาตรการที่แก้ปัญหาได้จริงมากกว่า"

"การคุมอินเทอร์เน็ตเป็นเรื่องยากมานานแล้ว ขอบเขตของประเทศทำให้การควบคุมเป็นไปได้ยาก แค่เขาหนีไปต่างประเทศ รัฐก็ทำอะไรไม่ได้แล้ว การบล็อคก็ไม่สามารถป้องกันได้ในระยะยาว เพราะยูอาร์แอลมันเปิดทุกวัน วันละเป็นล้าน ปิดยูอาร์แอลนี้ก็ไปโผล่ที่ยูอาร์แอลอื่น และผมรู้สึกว่าต่อไปคงจะปิดไม่ได้อีกแล้ว พอเริ่มมีเฟซบุค เริ่มมีเว็บ 2.0[35] ซึ่งมีความซับซ้อนขึ้น ต่อไปในทางเทคนิคคงจะปิดด้วยยูอาร์แอลได้ยาก"

(ผู้ประกอบการหมายเลข 4, 2554)

ผู้ให้บริการยังมีข้อเสนอแนะอื่นๆ เกี่ยวกับ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ด้วย เช่น หากต้องการให้ผู้ให้บริการมีส่วนรับผิดชอบต่อเนื้อหาในสื่อออนไลน์ด้วย กฎหมายต้องแบ่งระดับความรับผิดชอบของผู้ให้บริการเสียใหม่ และมีแนวปฏิบัติเกี่ยวกับการบอกแจ้งเพื่อให้ปิดกั้นข้อความ (take-down procedure) ที่ชัดเจน อย่างไรก็ดี อยากให้กฎหมายเข้าใจด้วยว่า

ผู้ให้บริการมีสถานะเป็นเพียง “ตัวกลาง” และการจะกำหนดให้ผู้ให้บริการมีหน้าที่ต้องตรวจตราเนื้อหาในอินเทอร์เน็ตซึ่งมีจำนวนมหาศาล เป็นเรื่องที่ไม่ควรทำอย่างยิ่ง

“น่าจะมีมาตรการเรื่อง takedown procedure เพื่อแสดงให้เห็นว่าผู้ประกอบการไม่ได้เจตนาที่จะสนับสนุน ถ้ามีกระบวนการพวกนี้อยู่ในกฎหมายก็จะทำให้ชัดเจนขึ้น”

(ผู้ประกอบการหมายเลข 4, 2554)

“มีเจ้าหน้าที่บางท่านเอาไอเอสพีไปเทียบกับหนังสือพิมพ์ว่าให้ไอเอสพีดูแลกันเอง ผมก็บอกว่ามันไม่เหมือนกันโดยสิ้นเชิง เพราะไอเอสพีไม่ใช่คนพิมพ์ข้อความลงไป อย่างโฮสติ้งอาจจะมีกึ่งๆ บ้าง เพราะเป็นผู้ให้เช่าที่ให้เขามาแปะเนื้อหา แต่ไอเอสพียิ่งหนักเลยครับเพราะเราเป็นเพียงแค่เจ้าของท่อ การจะให้เราต้องตรวจสอบเนื้อหามันคงเป็นไปไม่ได้ แค่การบล็อคก็เป็นเรื่องที่ยากแล้ว”

(ผู้ประกอบการหมายเลข 4, 2554)

กรณีที่หากจะมีการแก้ไขกฎหมาย ผู้ให้บริการซึ่งมีภาระในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log file) เสนอว่า กฎหมายควรคำนึงถึงการเปลี่ยนแปลงของโลกเทคโนโลยีด้วย ซึ่งในหมู่ผู้ให้บริการมีความกังวลว่าในอนาคตการเก็บบันทึกส่วนนี้จะทำได้ยากขึ้น โดยเฉพาะอย่างยิ่ง กรณีที่โลกอินเทอร์เน็ตกำลังอยู่ในช่วงเปลี่ยนผ่าน จาก internet protocol จากยุค IPV4 ไปสู่ IPV6[36] เพราะในช่วงของการเปลี่ยนผ่านจากรุ่นหนึ่งไปสู่อีกรุ่นหนึ่งนั้น ปกติแล้วจะต้องมีการแปลงไฟล์ข้อมูล เป็นผลให้ข้อมูลมีจำนวนเพิ่มมากขึ้น และย่อมส่งผลกระทบโดยตรงต่อข้อบังคับที่ให้ผู้ให้บริการมีหน้าที่เก็บข้อมูลจราจรคอมพิวเตอร์นานถึงเก้าสิบวัน และจะเป็นภาระมากสำหรับผู้ให้บริการ นอกจากนี้กฎหมายควรจำแนกแยกแยะระดับผู้ให้บริการที่ต้องจัดเก็บข้อมูลจราจรคอมพิวเตอร์ให้ชัดเจนด้วย

“ตอนนี้ IP เป็นเวอร์ชั่น 4 แต่คงเคยได้ยินกันมาบ้างว่าถ้า IPV4

หมดแล้ว เรากำลังจะเปลี่ยนเป็น IPV6 ซึ่งจะทำให้หน้าตาของ IP address ที่เราเข้าใจเปลี่ยนแปลงไป ซึ่งการเปลี่ยนจาก 4 ไป 6 นี้ จะทำให้ 4 กับ 6 คุยกันไม่รู้เรื่องเลย แต่พอ 4 หมดจะต้องขึ้น 6 ไปทีละนิด เนื่องจากอินเทอร์เน็ตใหญ่มากจึงไม่มีทางที่จะเปลี่ยนทีเดียววันเดียวได้ และไม่มีใครบอกได้ว่าต้องใช้เวลาเท่าไรในการเปลี่ยน

ปัญหาคือระหว่างเปลี่ยน จะต้องมีการแปลงจากเวอร์ชั่น 4 ไปเวอร์ชั่น 6 สมมติว่าผมมีเวอร์ชั่น 6 จะคุยกับเวอร์ชั่น 4 ซึ่งเว็บไซต์ทั่วไป 99.99% เป็นเวอร์ชั่น 4 ผมต้องไปแปลงเป็นเวอร์ชั่น 4 ก่อน แล้วแปลงเป็น 6 อีกที ขั้นตอนนี้จะค่อยๆ มีไปเรื่อยๆ ในอนาคตจนกว่าทุกคนจะเป็น 6 หมด และช่วงที่มีการเปลี่ยนผ่านนี้เอง จะยุ่งยากสำหรับผู้ให้บริการ เพราะเมื่อก่อนเรามี IP เวอร์ชั่นเดียว คือ เวอร์ชั่น 4 เราเก็บทีเดียวจบ แต่วันนี้เรามีสองเวอร์ชั่นการแปลงจาก 4 ไป 6 จาก 6 ไป 4 ทำให้เรามีภาระในการเก็บข้อมูลเยอะขึ้นมาก ข้อมูลที่เก็บจะมากขึ้นอย่างมหาศาล ซึ่งแทบจะเป็นไปไม่ได้เลยที่จะเก็บ หากจะมีการปรับปรุงกฎหมายในอนาคต เรื่องนี้จะเป็นประเด็นสำคัญและจะเป็นภาระมากสำหรับผู้ให้บริการ"

(ผู้ประกอบการหมายเลข 4, 2554)

"ผู้ที่ประสบปัญหาจริงๆ น่าจะเป็นผู้ให้บริการรายย่อย คือ ถ้ามีการขยับให้ลดจำนวนวัน หรือรูปแบบการเก็บก็น่าจะดี แต่ปัญหาคือ กฎหมายกำหนดไว้เก้าสิบวัน แต่เวลามาขอจริงๆ มีการขอเกิน 90 วัน อันนี้บังคับกันให้ได้ก่อนดีกว่า แค่นี้ก็แย่แล้ว"

(ผู้ประกอบการหมายเลข 3, 2554)

2.3 บทบาทของเว็บมาสเตอร์ และผู้ดูแลเว็บบอร์ดต่าง ๆ ภายใต้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่กระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชน

วิธีศึกษา

การศึกษาส่วนนี้ คณะผู้วิจัยใช้วิธีจัดสนทนากลุ่มย่อยในกลุ่มเว็บมาสเตอร์และเจ้าของหรือผู้ดูแลเว็บไซต์ต่างๆ ที่มีหน้าที่กำกับดูแลเนื้อหาภายในเว็บไซต์ของตน โดยคัดเลือกแหล่งข้อมูลจากความหลากหลายของเนื้อหา ได้แก่ เว็บไซต์ข่าวการเมือง เว็บไซต์ข่าวเทคโนโลยี เว็บข่าววาไรตี้ สมาคมวิชาชีพ เว็บบล็อก เว็บบอร์ด และผู้ประกอบการอินเทอร์เน็ต ประกอบด้วย

เว็บไซต์ข่าวการเมือง:

1. ชูวัส ฤกษ์ศิริสุข บรรณาธิการเว็บไซต์ประชาไท (http://prachatai.com)

2. วริษฐ์ ลิ้มทองกุล ผู้สื่อข่าวและคอลัมน์นิสต์ เอเอสทีวีผู้จัดการ (http://www.manager.co.th)

เว็บไซต์ข่าวเทคโนโลยี:

3. อิสริยะ ไพรีพ่ายฤทธิ์ ผู้ก่อตั้งและเว็บมาสเตอร์บล็อกนัน (http://blognone.com)

เว็บไซต์ข่าววาไรตี้:

4. สมพร ศึกษามั่น เว็บมาสเตอร์เอ็มไทย (http://mthai.com)

5. สิทธิโชค สุภาภรณ์ เว็บมาสเตอร์เอ็มไทย

เว็บบอร์ด:

6. ธรรมาภรณ์ สีขาว ฝ่ายกฎหมาย เว็บไซต์พันทิป (http://www.pantip.com)

เว็บบล็อก:

7. ปฏิญญา เสงี่ยมจิตร์ ผู้ก่อตั้งและเว็บมาสเตอร์เอ็กซ์ทีน (http://exteen.com)

สมาคมวิชาชีพ:

8. อศินา พรวศิน ประธานชมรมนักข่าวสายเทคโนโลยีสารสนเทศและผู้สื่อข่าวสายไอทีหนังสือพิมพ์เดอะเนชั่น

ประเด็นในการสัมมนากลุ่มย่อย

การสนทนากลุ่มย่อยนี้ นำสนทนาโดยคณะผู้วิจัย คือ นางสาวสาวตรี สุขศรี และนางสาวอรพิณ ยิ่งยงพัฒนา ก่อนการสัมมนาได้ตกลงว่าแหล่งข้อมูลมีอิสระตลอดการสัมภาษณ์ที่จะขอให้คณะผู้วิจัยปกปิดเอกลักษณ์เพียงแค่ส่วนใดส่วนหนึ่ง หรือตลอดการสัมภาษณ์ได้ โดยประเด็นการพูดคุยเป็นไปตามวัตถุประสงค์ของงานวิจัย ในการสนทนามีทั้งสนทนาแลกเปลี่ยน และถามคำถาม ทั้งนี้ โครงสร้างการคุยใช้แนวคำถามเดียวกันกับการสัมมนากลุ่มย่อยในกลุ่มผู้ประกอบการอินเทอร์เน็ต

ผลการศึกษา

ผลจากการสนทนากลุ่มย่อย แบ่งเป็นหมวดหมู่ดังนี้

1) ลักษณะการทำงานของผู้เว็บมาสเตอร์ และผู้ดูแลเว็บบอร์ดต่างๆ ภายใต้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่เกี่ยวกับเสรีภาพในการเข้าถึงข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน

2) ปัญหาที่พบจากการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่เกี่ยวกับเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน

3) ความคิดเห็นและข้อเสนอแนะต่อกฎหมาย และแนวนโยบายของรัฐ

1) ลักษณะการทำงานของเว็บมาสเตอร์ และผู้ดูแลเว็บบอร์ดต่างๆ ภายใต้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่เกี่ยวกับเสรีภาพในการเข้าถึงข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน

เว็บไซต์ต่างๆ ที่คณะผู้วิจัยเลือกศึกษาในงานวิจัยฉบับนี้ล้วนแล้วแต่เปิดให้บริการมาก่อนที่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 จะมีผลใช้บังคับ

และโดยผลของกฎหมายฉบับนี้ก็ทำให้ผู้ก่อตั้งและดูแลเว็บไซต์เหล่านี้มีสถานะเป็น "ผู้ให้บริการ" ประเภท ผู้ให้บริการเนื้อหาในอินเทอร์เน็ต ซึ่งต้องมีภาระหน้าที่และความรับผิดตามกฎหมาย ด้วยเหตุนี้เอง ผู้ประกอบการเว็บไซต์แต่ละรายจึงจำเป็นต้องปรับเปลี่ยนนโยบายเพื่อไม่ให้ต้องเกิดความรับผิดชอบกับเนื้อหาที่เกิดขึ้นในพื้นที่ให้บริการของตน ทั้งนี้ ลักษณะการปรับเปลี่ยนที่เกิดขึ้นจะมีทั้งการพยายามกลั่นกรองเนื้อหาของผู้ใช้บริการก่อนที่ข้อความจะถูกเผยแพร่ การกำหนดให้ผู้ใช้บริการต้องสมัครสมาชิกก่อนที่จะเผยแพร่เนื้อหาหรือแสดงความคิดเห็นใดๆ การเพิ่มบุคลากร และเครื่องมือเพื่อคอยตรวจตราข้อความ หรือกระทั่งการเพิ่มฝ่ายกฎหมายเพื่อคอยตรวจสอบข้อกฎหมายต่างๆ ที่เกี่ยวข้อง ประสานความร่วมมือเจ้าหน้าที่รัฐ หรือเพื่อต่อสู้คดี

เว็บไซต์ MThai คือ เว็บไซต์ข่าววาไรตี้ที่ได้รับความนิยมจากผู้ใช้บริการอินเทอร์เน็ต เป็นแหล่งรวมข่าวหลากหลายประเภท และท้ายข่าวแต่ละเรื่องมีพื้นที่ให้บุคคลทั่วไปแสดงความคิดเห็น นอกจากนี้ยังเปิดให้บริการกระดานสนทนาหรือเว็บบอร์ดด้วย และภายหลัง พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีผลบังคับใช้ MThai ได้ตั้งฝ่ายกฎหมายเพิ่มขึ้นเพื่อคอยประสานงานกับกระทรวงไอซีทีโดยเฉพาะ และกำหนดกติกาเพิ่มเติมสำหรับการใช้บริการเว็บไซต์ โดยอนุญาตให้เฉพาะผู้สมัครสมาชิกเท่านั้นตั้งกระทู้ในเว็บบอร์ดได้ และใช้ระบบการกลั่นกรองเนื้อหาก่อนให้กระทู้ที่ถูกตั้งนั้นเผยแพร่ต่อสาธารณะ แต่สำหรับในส่วนของการแสดงความคิดเห็นจะใช้วิธีการตรวจสอบภายหลังเนื่องจากมีข้อมูลจำนวนมากจึงไม่สามารถกลั่นกรองได้ ทั้งนี้ ทางเว็บไซต์ได้เพิ่มทีมงานที่ทำหน้าที่ตรวจตราเนื้อหาในเว็บอีกราว 10 คน เพื่อดำเนินการต่างๆ ดังกล่าว (สมพร ศึกษามั่น MThai, 2554)

"ปัจจุบันนี้หลายเว็บไซต์มีความพยายามที่จะเปิดให้มีการแสดงความคิดเห็นเฉพาะคนที่เป็นสมาชิกเท่านั้น ถ้าเป็นเมื่อก่อนใครจะแสดงความเห็นก็ได้ ทำให้เราไม่สามารถรู้ได้ว่าใครเป็นคนแสดงความคิดเห็นเพื่อจะกลั่นแกล้งคนอื่น แต่ปัจจุบันนี้มีการเก็บล็อกไฟล์ (log file) เก็บไอพี

ก็ทำให้สามารถตามตัวได้”

“เราอนุญาตให้เฉพาะสมาชิกสามารถตั้งกระทู้ได้ และมีคนตรวจ (moderator) ก่อนจึงขึ้นกระทู้ได้ แต่ในส่วนความคิดเห็นนั้นเราเปิดกว้าง... เราใช้วิธีให้ความเห็นขึ้นไปก่อนแล้วจึงให้เว็บมาสเตอร์คอยตรวจเช็คอีกทีหนึ่ง เพื่อกรองความเห็นที่ไม่เหมาะสม เช่น คำที่หมิ่นประมาท หรือที่จะทำให้เกิดความเสื่อมเสียออก ... การที่เราให้สมาชิกเท่านั้นตั้งกระทู้ได้ คือ การสร้างนโยบายว่าสมาชิกจะต้องรับผิดชอบข้อความที่โพสต์ นี่เป็นขั้นตอนเบื้องต้นในการจัดการ ... อย่างไรก็ดี หรือบางเรื่องที่อาจก่อให้เกิดการแตกแยกเราก็จะไม่ปล่อยให้ขึ้นเลย แต่นี่ก็เป็นมาตรการขั้นสุดท้ายที่เราจะใช้ ส่วนกระบวนการแจ้งข้อความไม่เหมาะสม เราแจ้งไว้ที่หน้าเว็บว่าถ้ามีปัญหาให้แจ้งมาที่เว็บมาสเตอร์ ในกรณีเร่งด่วนสามารถโทรได้ ส่วนใหญ่ที่แจ้งมา คือ ผู้ที่ถูกหมิ่นประมาท เราก็จะถามว่าจะให้ลบอย่างเดียว หรือว่าต้องการแจ้งความด้วย”

(สมพร ศึกษามั่น MThai, 2554)

“เชื่อว่า ทุกเว็บน่าจะมีความกังวลในเรื่องของการหมิ่นสถาบันฯ โดยเฉพาะช่วงสองปีนี้ จึงมักใช้วิธีป้องกันไว้ก่อน โดยถ้าพบเห็นก็ปิดไปก่อนเลย ก่อนหน้านี้ที่เว็บเคยมีปัญหาว่าในช่วงวันเสาร์อาทิตย์หรือเวลาดึกๆ มักมีความเห็นหมิ่นสถาบันฯ หลุดเข้ามา ซึ่งเป็นช่วงเวลาที่ไม่มีใครดูแล และเมื่อเจ้าหน้าที่ติดต่อมาก็จะไม่มีใครรับเรื่องไว้ ปัจจุบัน ก็ยังคงมีปัญหานี้อยู่แม้ว่าเราจะใช้วิธีการบล็อคถ้อยคำแล้วก็ตาม ซึ่งที่จริงแล้วมันเป็นวิธีแก้ปัญหาที่ปลายเหตุ เพราะคนที่กระทำก็จะมีวิธีแก้ปัญหาของเขา เช่น ใช้คำย่อ เคาะวรรค ผมว่าถ้า พ.ร.บ.คอมพิวเตอร์ฯ 2550 ตั้งใจจะเอาผิดผู้ให้บริการเว็บจริงๆ มันก็น่าจะลำบาก และเกิดปัญหามากๆ สำหรับคนดูแล”

(สิทธิโชค สุภาภรณ์ Mthai, 2554)

ด้านเว็บไซต์พันทิปซึ่งเป็นชุมชนเว็บบอร์ดแห่งแรก และมีขนาดใหญ่ที่สุดของเมืองไทยซึ่งประกอบไปด้วยเว็บบอร์ดสังคมการเมือง

ภาพยนตร์ ศิลปวัฒนธรรม วรรณกรรม วิทยาศาสตร์ ฯลฯ นั้น ได้มีการปรับเพิ่มมาตรการในการดูแลเนื้อหาในเว็บเช่นกัน ทั้งนี้ พันทิปกำหนดให้ผู้ใช้ต้องสมัครสมาชิก โดยกรอกรหัสประจำตัวประชาชนสิบสามหลัก ผู้เป็นสมาชิกแล้วจะสามารถตั้งกระทู้ได้ เติมรูปภาพ และแก้ไขข้อความได้ ทั้งนี้ พันทิปใช้ระบบการกลั่นกรองเนื้อหาภายหลังการโพสต์

"พันทิปจะกลั่นกรองเนื้อหาหลังความเห็นออกไปแล้ว เช่น ถ้าขัดต่อศีลธรรมอย่างชัดแจ้งก็จะเอาออกไปเลย แต่ถ้าเป็นการติชมตามธรรมดาก็จะคงไว้ ขั้นแรกต้องดูว่าขัดกับสำนึกทั่วไปหรือไม่ ขั้นที่สองถ้าเป็นการติชมทั่วไปเราก็จะพยายามดำเนินการอย่างอื่นๆ ก่อนที่จะไปลบความคิดเห็นของเขาออก เช่น ตัวอย่างที่เคยเกิดขึ้นคือ มีการติชมอุปกรณ์ไฟฟ้าชนิดหนึ่ง จากนั้นมีหนังสือจากกระทรวงไอซีทีมาขอไอพีแอดเดรสของคนที่ติชมนั้น ทางพันทิปก็ไม่ให้ไป และตอบกลับกระทรวงไปว่า ตรงนี้เป็นพื้นที่สาธารณะที่ให้มาแสดงความคิดเห็น และคิดว่าความเห็นดังกล่าวไม่ใช่การหมิ่นประมาท จึงขออนุญาตไม่ให้ไอพีแอดเดรส ถ้าทางเจ้าหน้าที่มีความเห็นอย่างไรให้ส่งหนังสือมาอีกครั้งหนึ่ง"

(ธรรมาภรณ์ สีขาว Pantip, 2554)

เว็บไซต์ประชาไท ก่อตั้งปี 2547 เป็นเว็บไซต์หนังสือพิมพ์ออนไลน์ ซึ่งเน้นการนำเสนอข่าวกระแสรอง ข่าวที่ไม่เป็นข่าว และสะท้อนเสียงของคนชายขอบ โดยในยุคเริ่มแรกของการก่อตั้งประชาไทมีทั้งส่วนงานข่าว บทความ และกระดานสนทนาซึ่งไม่เกิดปัญหาใดเกี่ยวกับการเปิดให้ผู้ใช้อินเทอร์เน็ตเข้ามาแสดงความคิดเห็น แต่จากวิกฤตการณ์การเมืองนับแต่การรัฐประหาร 19 กันยายน 2549 เป็นต้นมา พบว่าจำนวนผู้เล่นเว็บบอร์ดมีจำนวนสูงขึ้นอย่างมากจนเว็บบอร์ดประชาไทกลายเป็นชุมชนขนาดใหญ่และเป็นที่รวมตัวกันของผู้สนใจการเมืองเฉพาะกลุ่ม โดยเฉพาะฝ่ายที่ต่อต้านการรัฐประหาร

ปี 2552 ผู้อำนวยการเว็บไซต์ประชาไทถูกดำเนินคดี โดยมีกระทรวงไอซีทีเป็นโจทก์ ในฐานเป็นผู้ให้บริการที่จงใจสนับสนุนหรือยินยอม

ให้มีการเผยแพร่ความเห็นจำนวนสิบความเห็นที่กระทบต่อความมั่นคงของประเทศตามมาตรา 14 (3) และมาตรา 15 ต่อมาในปี 2553 ประชาไทถูกฟ้องอีกคดีหนึ่งในฐานะผู้ให้บริการด้วยข้อหาหมิ่นสถาบันฯ และในช่วงที่มีการประกาศ พ.ร.ก.การบริหารราชการในสถานการณ์ฉุกเฉินเมื่อเดือนเมษายนปี 2553 ศูนย์อำนวยการสถานการณ์ฉุกเฉิน (ศอฉ.) มีคำสั่งปิดเว็บไซต์ประชาไทและเว็บไซต์การเมืองจำนวนมาก ส่งผลให้ประชาไทต้องเปิดโดเมนใหม่อีกอย่างน้อยสามครั้ง ต่อมา ในเดือนกรกฎาคมปีเดียวกัน ประชาไทตัดสินใจปิดเว็บบอร์ด เพื่อลดแรงเสียดทานทางการเมือง และนอกจากนั้นก็ยังฟ้องรัฐบาลนายอภิสิทธิ์ เวชชาชีวะ และศอฉ. ต่อศาลแพ่งเพื่อเรียกร้องค่าเสียหายที่เกิดจากการถูกระงับการเผยแพร่ด้วยเหตุผลว่าใช้อำนาจหน้าที่โดยมิชอบ ศาลชั้นต้นยกฟ้อง ปัจจุบันคดีนี้อยู่ในชั้นศาลอุทธรณ์ ทั้งนี้ การทำงานของประชาไทจำแนกออกเป็นทีมข่าว และทีมติดตามตรวจสอบเนื้อหาซึ่งมีเว็บมาสเตอร์เป็นผู้ดูแล และใช้ระบบสมาชิกดูแลกันเอง

“เราต้องระวังในสามเรื่องด้วยกัน คือ เรื่องการหมิ่นเชื้อชาติ หมิ่นศาสนา และการหมิ่นสถาบันกษัตริย์ โดยในเวลาที่ยังไม่มี พ.ร.บ. คอมพิวเตอร์ฯ 2550 ปัญหาที่ทีมงานต้องถกเถียงกันบ่อยๆ ในกองบรรณาธิการและฝ่ายตรวจสอบเนื้อหา คือ แค่ไหนคือการหมิ่น อะไรควรเซ็นเซอร์ อะไรไม่ควร เพราะบ้านเราถูกตีความให้เพียงการวิพากษ์วิจารณ์เป็นหมิ่นหมดเลย ...ในขณะที่ฝ่ายหนึ่งเสนอว่าควรพยายามเปิดเสรีเต็มที่ให้กับเนื้อหาข่าว อีกฝ่ายก็พยายามป้องกันไว้ก่อนเพื่อความปลอดภัยขององค์กร เราจึงต้องทำให้ตรงนี้มันสมดุลกัน เรียกว่าตอนนั้นการพิจารณาเรื่องควรเสนออะไรหรือไม่ เป็นภารกิจหลักเลยก็ว่าได้...แต่พอมี พ.ร.บ.คอมพิวเตอร์ฯ 2550 เกิดขึ้น ก็จบเลย เพราะตอนนี้ อะไรๆ ก็เสนอไม่ได้ ที่สุดแล้วเราก็จำเป็นต้องเซ็นเซอร์ในระดับที่หนักสุด คือ ปิดเว็บบอร์ด ซึ่งนี่เป็นกระบวนการ อันเป็นผลกระทบจาก พ.ร.บ.คอมพิวเตอร์ฯ 2550 แน่นอน”

“การปิดเว็บบอร์ดของเรายังอาจยังถือว่าไม่เท่าไร แต่ถ้าเว็บบอร์ด

ขนาดใหญ่อย่างพันทิป ก็คิดว่าเขาคงมีปัญหามากกว่า เพราะเป็นเวทีขนาดใหญ่ เป็นความรู้ที่ประเมินค่าไม่ได้ พันทิปก่อให้เกิดประโยชน์แก่สังคมแค่ไหนในช่วง 10-20 ปีที่ผ่านมาหลายคนคงทราบ แต่ในกรณีประชาไทนั้นบังเอิญว่าเป็นเว็บบอร์ดขนาดเล็ก และโดนคดีเราเลยต้องปิด"

(ชูวัส ฤกษ์ศิริสุข ประชาไท, 2554)

เว็บไซต์เอเอสทีวีผู้จัดการ ถือเป็นเว็บไซต์ข่าวที่เกิดขึ้นเป็นลำดับแรกๆ ของประเทศไทย ดำเนินงานโดยเครือหนังสือพิมพ์ผู้จัดการ ซึ่งมีทั้งหนังสือพิมพ์รายวันและรายสัปดาห์ ก่อนจะเพิ่มช่องทางการเผยแพร่ในสื่อออนไลน์ และเครือผู้จัดการก็จัดได้ว่าเป็นสื่อที่มีการเคลื่อนไหวทางการเมืองสูงมาก ทั้งเป็นจุดริเริ่มและเติบโตของเครือข่ายพันธมิตรประชาชนเพื่อประชาธิปไตยด้วย ถือเป็นเว็บไซต์ข่าวที่มีบทบาทอย่างมากในการระดมมวลชนเพื่อเรียกร้องให้เกิดการต่อต้านอดีตนายกรัฐมนตรี พ.ต.ท.ทักษิณ ชินวัตร โดยมีรูปแบบการชุมนุมสาธารณะขนาดใหญ่ ทั้งนี้ เว็บไซต์ผู้จัดการเป็นเว็บข่าวที่ได้รับความนิยมเป็นอันดับหนึ่งมาอย่างต่อเนื่อง และยาวนาน ระบบการทำงานของเว็บไซต์ผู้จัดการจะใช้วิธีกลั่นกรองเนื้อหาภายหลัง จนเมื่อมีการประกาศใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ภายในองค์กรก็มีแนวปฏิบัติว่า จะลบกระทู้ภายในสามวันหลังได้รับแจ้งจากเจ้าหน้าที่

"ทางผู้จัดการค่อนข้างจะเสรีมากครับ ไม่ต้องมีการลงทะเบียน ไม่ต้องให้บัตรประชาชน แต่ก็มีการคัดกรองคำโดยระบบคอมพิวเตอร์ ซึ่งเราทำมาตั้งนานแล้วเป็นสิบปีแต่ก็ไม่ได้ผล เพราะผู้ใช้มีวิธีพลิกแพลงต่างๆ นานา จึงต้องเปลี่ยนมาเป็นการใช้คนกรองคอมเมนต์ก่อน ไม่ได้ขึ้นทันที ซึ่งบางทีดึกๆ คนกรองก็เหนื่อยเพราะความเห็นมีเป็นหมื่นๆ ต้องใช้กำลังคนเยอะมาก ลงทุนค่อนข้างสูง"

"หลังมี พ.ร.บ.คอมพิวเตอร์ฯ 2550 ก็ยังใช้ระบบเดิมอยู่ แต่เราได้คำแนะนำจากอาจารย์ไพบูลย์ อมรภิญโญเกียรติ (นักวิชาการด้านกฎหมายผู้เชี่ยวชาญคดี พ.ร.บ.คอมพิวเตอร์ฯ 2550 ว่าควรมี Policy and Disclaimer คือ มีวิธีปฏิบัติที่จะแจ้งให้ผู้ที่แสดงความเห็น และผู้เสียหายทราบ ซึ่ง

สอดคล้องกับมาตรา 15 ที่ถ้าเรามี Policy and Disclaimer โดยที่เราจะมีการลบภายในสามวันถ้ามีการแจ้งเข้ามา ซึ่งน่าจะใช้กล่าวอ้างกับศาลได้"

(วริษฐ์ ลิ้มทองกุล เอเอสทีวีผู้จัดการ, 2554)

สำหรับประเด็นรูปแบบการประสานงานเพื่อขอความร่วมมือในการปิดกั้นเว็บไซต์นั้น พบว่ามีทั้งลักษณะที่เป็นทางการ คือ ส่งหนังสือราชการและส่งเป็นจดหมายอิเล็กทรอนิกส์ (email) โดยภายในจดหมายจะระบุยูอาร์แอลที่ต้องการให้ลบ แต่มักไม่ระบุข้อความที่มีปัญหา

"มีบางกรณีที่เจ้าหน้าที่ติดต่อมาแบบไม่เป็นทางการให้ช่วยมอนิเตอร์ เช่น บอกว่ากระทู้นี้มีข้อความหมิ่นสถาบันฯ แต่อีกกรณี คือ มีจดหมายมาเป็นทางการเพื่อขอไอพีแอดเดรส...เขาจะให้ URL มา และจะระบุว่าให้ลบลิงก์ไหน แต่จะไม่ได้ระบุว่ามีข้อความอะไร โดยแต่ละครั้งจะส่งมาหลายลิงก์...ก่อนที่จะมีกฎหมายเราไม่รู้ว่าจะให้ได้ยังไงเพราะมันเป็นข้อมูลส่วนบุคคล เราจึงไม่เคยให้เลย สิ่งที่ตามมาคือ เดิมเราเก็บมันไว้เป็นปีไม่เคยลบ แต่หลังจากมีกฎหมาย กฎหมายกำหนดว่าเราต้องเก็บข้อมูลจราจรไว้ 90 วัน พอกฎหมายกำหนดไว้ 90 วันเราก็ลบเลย"

(ชูวัส ฤกษ์ศิริสุข ประชาไท, 2554)

"ทาง MThai จะมีมาทั้งสองรูปแบบ คือ ขอความร่วมมือในเรื่องการหมิ่นประมาท การโฆษณาขายยาต่างๆ ที่ไม่ถูกกฎหมาย เจ้าหน้าที่จะขอว่าถ้าเกิดกรณีอย่างนี้ขึ้นก็ขอให้แจ้งไปทางทีมงานของเขา และขอให้ติดต่อโดยตรงเพื่อดำเนินการในขั้นตอนต่อไป ซึ่งอาจจะเป็นการสืบหาคนโพสต์ข้อความ อีกกรณีก็จะเป็นการแจ้งความของเจ้าทุกข์โดยเจ้าหน้าที่รัฐจะแฟกซ์บันทึกประจำวันที่ผู้เสียหายไปแจ้งความไว้กับเจ้าหน้าที่ตำรวจมาให้ รวมทั้งระบุยูอาร์แอลมาให้ด้วย ซึ่งทางเราก็จะตรวจสอบไอพีแอดเดรสและส่งให้กับเจ้าหน้าที่เพื่อดำเนินการต่อ"

(สมพร ศึกษามั่น MThai, 2554)

2) ปัญหาที่พบจากการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่เกี่ยวกับเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน

ในมุมมองของผู้ให้บริการเนื้อหานั้น นอกจากการต้องปรับเปลี่ยนแนวนโยบายและวิธีปฏิบัติขององค์กรเพื่อให้สอดคล้องกับภาระหน้าที่ตามที่กำหนดไว้ใน พ.ร.บ.คอมพิวเตอร์ฯ 2550 แล้ว หน่วยงานผู้ให้บริการยังพบปัญหาที่เกิดขึ้นจาก พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในประเด็นอื่นๆ ด้วย อาทิ เช่น การเน้นการกำหนดโทษให้ตัวกลางเพื่อหาคนรับผิดชอบให้ได้ มากกว่าการพยายามสืบหาผู้กระทำความผิดตัวจริง ความคลุมเครือของถ้อยคำในกฎหมายและปล่อยให้เป็นดุลพินิจของพนักงานเจ้าหน้าที่ตีความบทบัญญัติมากเกินไป เช่น เรื่องข้อมูลปลอมหรือเท็จตามที่กำหนดในมาตรา 14 (1) ที่ในทางปฏิบัติมักใช้กับกรณีการหมิ่นประมาทบุคคล ซึ่งมีความความลักลั่นกับประมวลกฎหมายอาญา

ฝ่ายกฎหมายของเว็บบอร์ดพันทิปเล่าประสบการณ์ว่า เมื่อมีกรณีการหมิ่นประมาทเกิดขึ้น พ.ร.บ.คอมพิวเตอร์ฯ 2550 มาตรา 14 มักถูกนำมาใช้โดยระบุว่า เป็นการนำเข้าสู่ข้อมูลคอมพิวเตอร์อันเป็นเท็จ ซึ่งเรื่องนี้มีความลักลั่นกับประมวลกฎหมายอาญา มาตรา 326 และ 328 ว่าด้วยความผิดฐานหมิ่นประมาท ที่เน้นคำนึงที่ผลกระทบของผู้เสียหายว่าถูกหมิ่นประมาทหรือไม่ มากกว่าเรื่องความเท็จของข้อมูลซึ่งมิได้อยู่ในองค์ประกอบความผิด อีกทั้งยังมีข้อยกเว้นเรื่องการติชม และปัญหาจะเกิดขึ้นทันทีหากกรณีนั้นๆ ถูกฟ้องทั้งประมวลกฎหมายอาญาและ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ที่ทำให้ต้องเกิดการตีความกฎหมาย นอกจากนี้ยังเห็นได้ว่า การใช้กฎหมายนี้เป็นไปในลักษณะที่ต้องการหาคนมารับผิดโดยอ้างมาตรา 15 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ว่าด้วยความรับผิดของตัวกลางผู้ให้บริการมากกว่าจะหาตัวผู้กระทำความผิดที่แท้จริงมาลงโทษ (ธรรมภรณ์ สีขาว เว็บไซต์พันทิป, 2554)

นอกจากนี้ ยังมีผู้ให้บริการสะท้อนปัญหาด้วยว่า ผู้บังคับใช้

กฎหมายไม่ได้ใช้กฎหมายอย่างตรงไปตรงมา ยังขาดความเข้าใจและใช้กฎหมายผิดวัตถุประสงค์ ตัวแทนจากเว็บไซต์ข่าวการเมืองอย่างเอเอสทีวีผู้จัดการเล่าว่า กรณีของเอเอสทีวีผู้จัดการนั้น มีนโยบายว่า ถ้าตำรวจทั่วไปแจ้งขอข้อมูลมาก็จะไม่ให้ แต่ทราบมาว่าตอนนี้เจ้าหน้าที่ภาครัฐหลายหน่วยงานอยากเป็นเจ้าพนักงานตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ทั้งที่ไม่ได้มีความรู้ความเข้าใจในเทคโนโลยีด้านนี้เพียงพอ และทั้งไม่ได้มีส่วนงานเกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ฯ 2550 เลย เช่น กรมสรรพากร หรือกระทรวงการคลัง ซึ่งกฎหมายฉบับนี้ไม่น่าจะอยากให้อำนาจนี้ใช้กันโดยกว้างขวางขนาดนั้น จึงไม่ได้ระบุเปิดช่องไว้ เช่น เรื่องการตรวจภาษี ซึ่งผมว่ามันเป็นการใช้ พ.ร.บ.อย่างผิดวัตถุประสงค์" (วริษฐ์ ลิ้มทองกุล เอเอสทีวีผู้จัดการ, 2554)

อย่างไรก็ตาม ในมุมของผู้ให้บริการด้านเนื้อหา ก็มีทัศนคติต่อบทบาทและภาระความรับผิดชอบที่ผู้ให้บริการพึงแบกรับแตกต่างกัน ด้านหนึ่งเห็นว่าผู้ให้บริการจำเป็นต้องลงทุนบางอย่างเพื่อรับผิดชอบกับผลกระทบจากการใช้สื่ออินเทอร์เน็ตด้วย แต่ขณะเดียวกัน ก็มีมุมมองที่เห็นว่า พ.ร.บ.คอมพิวเตอร์ฯ 2550 ไม่ได้ถูกออกแบบมารองรับเสรีภาพในการนำเสนอข่าวเลย กลับยิ่งทำให้ผู้ให้บริการเว็บไซต์ต้องแบกรับทั้งงบประมาณและความเสี่ยงที่จะต้องมีความรับผิด ความเสี่ยงนี้มีมาทั้งจากฝ่ายรัฐ ฝ่ายผู้เสียหาย ผู้ใช้บริการอินเทอร์เน็ต และภาคประชาสังคมด้วย ที่จำนวนหนึ่งพยายามเรียกร้องให้ผู้ให้บริการต้องรับผิดชอบในเนื้อหา ทั้งต้องลงทุนลงแรงอย่างเต็มที่หากต้องการประกอบธุรกิจ

"ในวันนี้ ผู้ให้บริการถือว่าเป็นสื่อ คุณเป็นคนหยิบไมโครโฟนให้คนอื่นพูดได้ดังๆ ดังนั้นคุณก็ต้องรับผิดชอบ เสรีภาพกับความรับผิดชอบนั้นจะต้องมาด้วยกัน แต่เสรีภาพนั้นแค่ไหน เราก็ต้องกำหนดกติกาว่าอะไรผิดไม่ผิด การที่จะพูดอะไรก็ต้องมีความรับผิดชอบ"

"เรื่องที่บอกว่าต้นทุนเพิ่ม การที่ต้องเก็บ log file แน่นอนว่าก็ต้องมีต้นทุนที่เพิ่มขึ้น แต่ถ้าคุณมองว่าคุณทำธุรกิจ มันก็ต้องมีการลงทุน เรื่องคนที่จะมามอนิเตอร์ก็ต้องมีการลงทุน รวมทั้งจะต้องมีการสร้าง

ความรู้ ความเข้าใจด้วย"

(อศินา พรวศิน ประธานชมรมนักข่าวสายเทคโนโลยีสารสนเทศ, 2554)

แม้เรื่องความเสี่ยงต่อการถูกฟ้องคดี จะไม่เป็นอุปสรรคสำหรับสื่อขนาดใหญ่ แต่สิ่งนี้เป็นอุปสรรคสำคัญสำหรับเว็บไซต์ประเภทที่ผู้ใช้เป็นผู้สร้างเนื้อหา (user-generated content) และเว็บไซต์ขนาดเล็กที่อาจไม่ได้ริเริ่มขึ้นในแบบผู้ประกอบการที่หวังผลกำไรทางออนไลน์อย่างจริงจัง ตัวอย่างเช่น เว็บไซต์ Exteen ซึ่งเริ่มต้นมาจากกลุ่มนักศึกษาด้านวิศวกรรมศาสตร์ที่สร้างพื้นชุมชนบล็อกเกอร์ โดยเว็บไซต์ Exteen เป็นเว็บบล็อกของไทยที่อนุญาตให้คนทั่วไปเป็นเจ้าของบล็อกได้ ด้วยลักษณะกฎหมายแบบ พ.ร.บ.คอมพิวเตอร์ฯ 2550 จึงส่งผลให้ผู้ให้บริการกลุ่มนี้ต้องแบกรับภาระสูงขึ้น และส่งผลให้เกิดการเซ็นเซอร์ตัวเองยิ่งขึ้น หรือมิเช่นนั้นก็ต้องใช้วิธีการอื่นใดเพื่อหลบเลี่ยงกฎหมาย เช่น การย้ายเซิร์ฟเวอร์ไปต่างประเทศ ซึ่งย่อมส่งผลกระทบต่อธุรกิจเทคโนโลยีสารสนเทศในภาพรวม เพราะแรงจูงใจที่อยากประกอบการในประเทศไทยมีน้อยลง

"เรื่องการฟ้องร้องเป็นเรื่องธรรมดาของคนเป็นสื่อ ถ้าคุณรับความเสี่ยงไม่ได้ก็ไม่ต้องให้มีคอมเมนต์"

(วริษฐ์ ลิ้มทองกุล เอเอสทีวีผู้จัดการ, 2554)

"ที่ว่าถ้าไม่อยากรับความเสี่ยงก็ไม่ต้องมีคอมเมนต์ แต่เว็บของผมส่วนที่เป็นหลักคือเนื้อหาที่ผู้ใช้เป็นคนเขียน เมื่อผมต้องรับผิดชอบเนื้อหาเหล่านั้น ผมต้องรับภาระนั้น ซึ่งก็อาจโดนฟ้องได้"

(ปฏิญญา เสงี่ยมจิตร์ Exteen, 2554)

"โดยตัวอินเทอร์เน็ตเองมันเป็นสิ่งที่ยากต่อการควบคุม ในส่วนที่เกี่ยวกับการให้บริการ ผมคิดว่าเว็บใหญ่ๆ จะมีภาระเพิ่มขึ้นมา แต่การหมิ่นต่างๆ ไม่ได้ลดลง ที่ชัดที่สุดคงเป็นพันทิปซึ่งปิดห้องราชดำเนินใน

เหตุการณ์ทางการเมืองหลายครั้ง ทำให้คนในห้องราชดำเนินไหลออกไปตั้งเว็บใหม่ คนที่ทำความผิดก็ยังคงทำอยู่ เพียงแค่เปลี่ยนที่เท่านั้นเอง ซึ่งถ้ามองในมุมของรัฐก็อาจไม่ได้ช่วยอะไร แต่ถ้ามองในมุมของเว็บใหญ่ๆ เขาต้องเหนื่อยขึ้นเยอะ เพราะต้องมีทีมมอนิเตอร์ตลอดเวลา หรืออย่างในกรณีของประชาไทก็ต้องปิดเว็บไปเลย อีกกรณีคือ พอเซิร์ฟเวอร์อยู่ในเมืองไทย อยู่ในขอบเขตของกฎหมายไทย มันไม่มีอิสระ คนก็จะหนีไปใช้บริการในต่างประเทศกันหมด"

(อิสริยะ ไพรีพ่ายฤทธิ์ Blognone, 2554)

"หน่วยงานของผมเป็นหน่วยเล็กๆ ที่ไม่มีฝ่ายกฎหมาย พอมีอะไรเกิดขึ้นก็จะกลัวไว้ก่อน ผมว่าสิ่งเหล่านี้มันก็จะก่อให้เกิดความกังวลในผู้ประกอบการรายใหม่ๆ และทำให้ความสามารถในการเข้ามาเป็นผู้ให้บริการมันน้อยลง"

(สมพร ศึกษามั่น MThai, 2554)

"มาตรา 14 และ 15 ทำให้ทุกคนที่เข้าถึงอินเทอร์เน็ตหรือใช้คอมพิวเตอร์สามารถเป็นอาชญากรได้ทุกเมื่อ และความผิดและโทษของตัวกลางก็เท่ากับผู้ใช้ มันจึงเป็นภาระในการมอนิเตอร์ สำคัญกว่านั้นมันได้สร้างโครงสร้างของการเซ็นเซอร์ตัวเอง โดยการไม่อนุญาตให้แสดงความคิดเห็น"

(ชูวัส ฤกษ์ศิริสุข ประชาไท, 2554)

3) ความคิดเห็น และข้อเสนอแนะต่อกฎหมายและแนวนโยบายของรัฐ

ในมุมมองของกลุ่มผู้ให้บริการเนื้อหา (content provider) และผู้ดูแลเว็บไซต์นั้น ยังคงเห็นว่า พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีความจำเป็นอยู่ เพื่อป้องกันการกระทำความผิด แต่ก็ควรให้ความสำคัญกับกลไกที่

จะนำมาใช้ในการปกป้องคุ้มครองผู้ใช้อินเทอร์เน็ตด้วย แต่เมื่อพิจารณา พ.ร.บ.คอมพิวเตอร์ฯ 2550 ฉบับปัจจุบันแล้วกลับพบว่า มีหลายเรื่องที่ผู้ใช้อินเทอร์เน็ตยังไม่ได้รับการคุ้มครอง เช่น เรื่องข้อมูลส่วนบุคคล ในขณะที่กำหนดภาระหน้าที่ และความรับผิดมากเกินสมควรให้กับผู้ให้บริการ

"การเกิดขึ้นของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 เป็นพัฒนาการปกติของทุกวงการ พอมันเริ่มโตขึ้นก็ต้องมีกฎหมายควบคุม อยากให้มองว่ามันเข้ามาเป็นกลไกที่จะปกป้องคุ้มครองผู้ใช้อินเทอร์เน็ตทุกคน เช่น เรื่องการเจาะระบบโดยไม่มีอำนาจ แต่ก็ยังมีเรื่องอื่นๆ ที่ยังไม่ได้รับความคุ้มครอง เช่น ข้อมูลส่วนบุคคล เราก็ต้องยอมรับนะครับว่า พ.ร.บ.คอมพิวเตอร์ฯ 2550 นั้นเกิดขึ้นมาด้วยเงื่อนไขพิเศษ ถ้าหากว่าไม่มีรัฐบาล คมช. ก็คงไม่ถูกดันออกมาเร็วขนาดนี้"

(อิสริยะ ไพรีพ่ายฤทธิ์ Blognone, 2554)

ด้านตัวแทนจากเว็บไซต์ข่าววาไรตี้ MThai เห็นว่า พ.ร.บ.คอมพิวเตอร์ฯ 2550 เน้นหนักไปในทางควบคุมพฤติกรรมประชาชนมาก จึงอยากให้กฎหมายหันมาสนใจ หรือเน้นด้านการคุ้มครองสิทธิและเสรีภาพของประชาชนให้มากขึ้น เช่น กำหนดด้วยว่าผู้ใช้บริการจะได้รับความคุ้มครองอย่างไรบ้าง (สิทธิโชค สุภาภรณ์ MThai, 2554)

อีกข้อเรียกร้องสำคัญคือ การกำหนดขอบเขตความรับผิดชอบของผู้ให้บริการให้ชัดเจนว่าผู้ให้บริการมีกี่ระดับ และจะชี้วัดอย่างไรว่าเมื่อไรที่เข้าข่าย "จงใจสนับสนุนหรือยินยอม" ให้มีการเผยแพร่หรือนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อความที่เป็นความผิดต่อกฎหมาย (สิทธิโชค สุภาภรณ์ MThai, 2554) นอกจากนี้ ก็ไม่ควรกำหนดโทษของตัวกลางเอาไว้สูงเท่ากับผู้กระทำผิดซึ่งถือว่าแรงเกินไป

"ผมคิดว่ากฎหมายอาจบัญญัติแรงเกินไป คือ ให้ผู้ให้บริการรับความผิดเท่ากับผู้กระทำผิด แต่ถูกต้องล่ะ ว่ามันต้องมีบทลงโทษผู้ให้บริการด้วยระดับหนึ่ง เพื่อรักษาความรับผิดชอบเอาไว้"

(วริษฐ์ ลิ้มทองกุล เอเอสทีวีผู้จัดการ, 2554)

"อยากให้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีความชัดเจนว่า จะมีความผิดเรื่องหมิ่นประมาทไหม เพราะลักลั่นกับความผิดฐานหมิ่นประมาทในประมวลกฎหมายอาญา พอเอา พ.ร.บ.คอมพิวเตอร์ฯ 2550 มาโยงผู้ประกอบการก็มีส่วนผิดด้วย และหากจะมีความผิดเรื่องการหมิ่นประมาทแล้ว ข้อยกเว้นตามมาตรา 329 ในประมวลกฎหมายอาญา (การติชมโดยสุจริต) ต้องนำมาใช้หรือไม่ และถ้าเอามาใช้ เรื่องการปลอมจะเป็นการปลอมในส่วนเนื้อหา หรือว่าปลอมจากต้นฉบับ"

(ธรรมภรณ์ สีขาว Pantip, 2554)

ประเด็นสำคัญอีกเรื่องหนึ่งที่สังคมออนไลน์ควรให้ความสนใจ คือ ความเชื่อมั่น และความรู้ความเข้าใจของทุกๆ ฝ่ายที่จำเป็นต้องเข้ามาเกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งนอกจากความน่าเชื่อถือของภาครัฐ ผู้บังคับใช้กฎหมายควรใช้กฎหมายอย่างตรงไปตรงมา ไม่ใช้เป็นเครื่องมือทางการเมืองแล้ว ยังมีเรื่องความน่าเชื่อถือของผู้ให้บริการด้วย ในฐานะองค์ประกอบสำคัญหนึ่งที่เป็นผู้ดูแลจัดเก็บข้อมูลของผู้ใช้บริการ ในขณะที่ในส่วนของบทบัญญัติเอง กฎหมายควรต้องปรับให้สอดคล้องกับลักษณะของการสื่อสารออนไลน์ ซึ่งมีการเปลี่ยนรูปแบบอยู่เสมอ และรัฐก็ควรมีมาตรการในการให้ความรู้เกี่ยวกับ พ.ร.บ.คอมพิวเตอร์ฯ 2550 กับประชาชนทั่วไป ให้มากกว่านี้

"ในเรื่องการเก็บ log file เราจะเชื่อได้หรือไม่ว่าการเก็บข้อมูลของแต่ละที่น่าเชื่อถือจริง เช่น ถ้ามีคนเข้ามาเขียนข้อความดูหมิ่นใน Exteen แล้วผมก็สร้าง log file หลอกๆ ขึ้นมาเพื่อโยนความผิด จะมีอะไรที่จะสร้างความมั่นใจได้ว่า log file ที่เป็นแค่ข้อความธรรมดาๆ นั้นเชื่อถือได้ เพราะ พ.ร.บ.ก็ไม่ได้กำหนดตรงนี้ไว้"

(ปฏิญญา เสงี่ยมจิตร์ Exteen, 2554)

"เนื้อหาในเว็บไม่ได้มาจากเซิร์ฟเวอร์ของเราหมด บางทีมันก็มาจากที่อื่นได้ด้วย เช่น เดี๋ยวนี้มีบางเว็บไซต์ที่สร้างเพจในเฟซบุค (Facebook) ไว้ และเชื่อมโยงให้การเขียน หรือการแสดงความคิดเห็นบนนั้นมาแสดงในหน้าเว็บไซต์หลักของเราได้ด้วย ซึ่งโดยปกติแล้วเราคงรับผิดชอบเฉพาะเนื้อหาในเว็บเรา แต่เมื่อคอมเมนต์ทุกอย่างมันเกิดขึ้นในเฟซบุค มันก็จะเกิดปัญหาขึ้นมาทันทีว่า ถ้ามีคนมาคอมเมนต์อะไรที่ไม่ดี ใครจะเป็นคนรับผิดชอบเราซึ่งเป็นเจ้าของเว็บหลักหรือเฟซบุค ซึ่งถ้ามองหน้าเว็บคนที่ต้องรับผิดชอบก็คือเจ้าของเว็บ แต่ถ้าเราเข้าใจระบบการทำงาน เราก็จะรู้ว่าระบบคอมเมนต์มันไม่ได้อยู่กับเราแต่มันไปอยู่ที่เซิร์ฟเวอร์ของเฟซบุคเขา"

(อิสริยะ ไพรีพ่ายฤทธิ์ Blognone, 2554)

"ภาครัฐมีงบประมาณไม่น้อยในการเผยแพร่กฎหมายฉบับนี้ แต่ก็ใช้เงินจำนวนไม่น้อยไปในการอบรม ซึ่งค่อนข้างเปล่าประโยชน์ และไม่ได้ประสิทธิผลอย่างแท้จริงเมื่อเทียบกับกฎหมายฉบับอื่นที่รัฐบาลมีเงินให้ แต่ถ้านำเงินไปใช้อย่างอื่น เช่น การวิจัย อาจได้ประโยชน์มากกว่า ผมว่ามันเป็นเรื่องการใช้เงินด้วยที่ไม่ถูกต้อง ชมรมผู้สื่อข่าวออนไลน์เองก็เคยคุยกันว่าทุกเว็บไซต์ควรมีการเผยแพร่ว่าปัจจุบัน ประเทศไทยมี พ.ร.บ.ฉบับนี้อยู่"

(วริษฐ์ ลิ้มทองกุล เอเอสทีวีผู้จัดการ, 2554)

"ประเด็นที่หลายคนไม่เข้าใจรวมถึงผมด้วย คือ กระบวนการทำงานของฝ่ายรัฐ เจ้าหน้าที่ก็จะมาจากหลายหน่วยงานทำให้เกิดความสับสนว่าใครคือผู้มีอำนาจกันแน่ อีกประเด็น คือ คนจะไม่เชื่อว่าเจ้าหน้าที่มีความรู้ความสามารถเพียงพอจริงๆ ผมคิดว่าพนักงานเจ้าหน้าที่ควรได้รับการรับรองว่าสามารถปฏิบัติหน้าที่ได้จริงๆ"

(อิสริยะ ไพรีพ่ายฤทธิ์ Blognone, 2554)

"ปัญหาอยู่ที่กฎหมาย หรืออยู่ที่การบังคับใช้กฎหมาย ไม่ได้อยากให้มองว่าตัวกฎหมายเป็นปัญหาแต่การใช้กฎหมายต่างหากที่เป็นปัญหา"

(อศินา พรวศิน ประธานชมรมนักข่าวสายเทคโนโลยีสารสนเทศ, 2554)

"ผมคิดว่าปัญหาเรื่องการบังคับใช้มีในกฎหมายทุกฉบับ แต่กฎหมายที่ดีต้องทำให้การบังคับใช้ที่มีปัญหาเกิดขึ้นไม่ได้ เราจะยอมให้กฎหมายเป็นเครื่องมือของผู้มีอำนาจอย่างนั้นหรือ เสรีภาพของเราเป็นเสรีภาพที่ล้มความไม่เป็นธรรมได้ เราต้องไม่ยอมให้มีการตีความและเลือกใช้กฎหมายเพื่อผู้มีอำนาจ"

(ชูวัส ฤกษ์ศิริสุข ประชาไท, 2554)

ข้อเสนอแนะจากมุมของผู้ให้บริการเว็บไซต์และผู้ดูแลเว็บบอร์ด คือ ควรให้ความเคารพประชาชน โดยแทนที่จะใช้การบังคับกฎหมาย และกำหนดแต่ภาระความรับผิดอย่างเดียว ก็ควรหันมาใช้นโยบายให้ผู้ให้บริการมีแนวทางการกำกับดูแลกันเอง รวมถึงให้มีคณะกรรมการกลั่นกรองเรื่องการปิดกั้นเว็บไซต์ ซึ่งเรื่องนี้ ทางชมรมผู้ผลิตข่าวออนไลน์เคยยื่นเรื่องให้กับรัฐมนตรีกระทรวงไอซีที เสนอให้ตั้งคณะกรรมการกลั่นกรองการปิดเว็บไซต์ แต่ก็ไม่ได้รับการตอบสนอง (วริษฐ์ ลิ้มทองกุล เอเอสทีวีผู้จัดการ, 2554)

"สิ่งที่สังคมไทยควรทำ คือ การปฏิบัติกับประชาชนแบบเป็นผู้ใหญ่ ซึ่งเป็นสิ่งที่สังคมไทยไม่เคยทำ เราเคยลองใช้วิธีการควบคุมคนแล้ว ปรากฏว่า วัฒนธรรมการเคารพซึ่งกันและกันในความเป็นมนุษย์ก็ไม่เคยเกิดขึ้นเลย สิ่งที่เราไม่เคยลองเลยในประวัติศาสตร์ คือ การให้สิทธิเสรีภาพ ทุกสังคมที่มีเสรีภาพผู้คนจะใช้สิทธิอย่างเคารพกัน และรับผิดชอบ ความรับผิดชอบเกิดจากการใช้สิทธิเสรีภาพโดยการตระหนักว่าเมื่อเรามีสิทธิคนอื่นก็มีสิทธิเช่นกัน ความรับผิดชอบจึงเกิด ผมคิดว่าควรมองเรื่องสิทธิเป็นเรื่องการให้การศึกษาผู้คน และเอาหลักนั้นมาออกแบบกฎหมาย และมันจะทำให้เกิดกลไกในการควบคุมกันเอง"

(ชูวัส ฤกษ์ศิริสุข ประชาไท, 2554)

สรุปการศึกษาผลกระทบเชิงคุณภาพ

ผลจากการเก็บข้อมูลและความคิดเห็นจาก “บุคลากรภาครัฐ” โดยใช้วิธีการสัมภาษณ์เชิงลึก (in-depth interview) และจาก “ผู้ให้บริการ” ทั้งกลุ่มผู้ประกอบการอินเทอร์เน็ต กลุ่มเว็บมาสเตอร์และผู้ดูแลเว็บบอร์ด โดยใช้วิธีการจัดสนทนากลุ่มย่อย (focus group) สามารถประมวลผลสรุปได้ดังต่อไปนี้

1. ประสบการณ์การที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ฯ 2550

กลุ่มภาครัฐ: พ.ร.บ.คอมพิวเตอร์ฯ 2550 ช่วยทำให้เจ้าหน้าที่มีอำนาจหน้าที่ชัดเจนในการปิดกั้นเว็บไซต์ แต่แม้เว็บไซต์ต่างๆ จะถูกปิดกั้นด้วยเหตุผลที่มีเนื้อหาขัดกฎหมาย แต่กลับไม่ค่อยพบการดำเนินคดีกับเว็บไซต์ที่ถูกปิดกั้นจริง

พ.ร.บ.คอมพิวเตอร์ฯ 2550 ให้อำนาจหน้าที่พนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ ให้สามารถทำงานได้ และกำหนดหน้าที่ให้ผู้ให้บริการต้องเก็บข้อมูลจราจรคอมพิวเตอร์ด้วย ซึ่งเป็นประโยชน์ในการทำงานสืบสวนสอบสวน แต่พบว่าคดีที่เป็นเรื่องอาชญากรรมคอมพิวเตอร์โดยแท้กลับมีไม่มากนัก ตรงกันข้าม ความขัดแย้งและการเปลี่ยนแปลงทางการเมือง ส่งผลให้อัตราการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 กับคดีด้านความมั่นคงเพิ่มสูงขึ้น

อย่างไรก็ดี แม้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 จะให้อำนาจแก่พนักงานเจ้าหน้าที่ แต่เรื่องนี้ไม่เป็นผลใดๆ ต่อการทำงานของกรมสอบสวนคดีพิเศษ เนื่องจากมีอำนาจที่ให้ไว้แล้วตาม พ.ร.บ.การสอบสวนคดีพิเศษในที่สุดแล้ว พ.ร.บ.คอมพิวเตอร์ฯ จึงไม่ได้มีความจำเป็นกับดีเอสไอมากนัก

กลุ่มผู้ประกอบการอินเทอร์เน็ต: พ.ร.บ.คอมพิวเตอร์ฯ 2550 ทำให้การประสานความร่วมมือกับภาครัฐในการปิดกั้นเว็บไซต์มีความชัดเจนขึ้น ทำให้การปิดเว็บไซต์เป็นไปตามขั้นตอนกฎหมาย โดยผู้ให้บริการใช้หลัก

เกณฑ์ว่าจะปิดกั้นตามหมายศาลเท่านั้น นอกจากนี้ กฎหมายนี้ยังส่งผลให้แนวปฏิบัติในการให้ข้อมูลจราจรคอมพิวเตอร์แก่ภาครัฐเปลี่ยนแปลงไป จากเดิมที่ผู้ให้บริการอาจปฏิเสธโดยอ้างเหตุผลเรื่อง “ข้อมูลส่วนบุคคล” ของลูกค้าได้ แต่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 กำหนดให้เป็นหน้าที่ของผู้ให้บริการที่ต้องให้ข้อมูลกับพนักงานเจ้าหน้าที่ หากไม่ปฏิบัติตามก็มีความผิดและโทษ

กลุ่มเว็บมาสเตอร์ และผู้ดูแลเว็บบอร์ด: พ.ร.บ.คอมพิวเตอร์ฯ 2550 ส่งผลให้ผู้ให้บริการต้องปรับเปลี่ยนแนวปฏิบัติภายในองค์กร เช่น มีการกลั่นกรองเนื้อหาของผู้ใช้บริการก่อนที่ข้อความจะถูกเผยแพร่ออกไป กำหนดให้ผู้ใช้บริการต้องสมัครสมาชิกก่อนที่จะโพสต์เนื้อหา หรือแสดงความคิดเห็นใดๆ เพิ่มบุคลากรและเครื่องมือเพื่อตรวจตราข้อความ หรือกระทั่งเพิ่มฝ่ายดูแลด้านกฎหมายเพื่อตรวจสอบข้อกฎหมายต่างๆ ที่เกี่ยวข้อง และคอยประสานความร่วมมือกับเจ้าหน้าที่รัฐ

2. ปัญหาจาก พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่เกี่ยวกับเสรีภาพในการแสดงความคิดเห็นของประชาชน

กลุ่มภาครัฐ: พบปัญหาในสี่เรื่องหลัก คือ

1) ปัญหาการตีความ หลายมาตราในกฎหมายขึ้นอยู่กับดุลพินิจในการตีความของเจ้าหน้าที่รัฐมากเกินไป เช่น เรื่องข้อมูลปลอมหรือเท็จ (forged or false computer data) ที่มีความคลุมเครือและยากที่จะพิสูจน์ให้เห็นถึง “ความเท็จ” นอกจากนี้ การสื่อสารในโลกออนไลน์มักมีประเด็นใหม่ๆ ที่ทำให้เจ้าหน้าที่ต้องพิเคราะห์ว่าประเด็นนั้นๆ เข้าองค์ประกอบของกฎหมายที่มีอยู่หรือไม่

2) การบังคับใช้กฎหมายเพื่อปราบปรามอาชญากรรมคอมพิวเตอร์และการคุ้มครองประชาชนโดยรวมยังไม่ปรากฏชัด เช่น มีผู้เสียหายจากอาชญากรรมคอมพิวเตอร์ไปแจ้งความแล้วตำรวจไม่รับแจ้ง โดยให้เหตุผลว่าไม่ได้อยู่ในเขตอำนาจตามท้องที่ที่กระทำผิด หรือบอกว่าไม่สามารถทำ

คดีได้ เพราะไม่มีอำนาจหน้าที่แบบเจ้าพนักงานตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 เป็นต้น

3) พบปัญหาขาดบุคลากรที่มีความรู้ความเข้าใจที่เพียงพอในคดีความตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 กล่าวคือ ด้วยระบบราชการที่แม้มีการพัฒนาคน จนสามารถทำงานได้แล้ว แต่ก็มักถูกโยกย้ายไปทำงานในส่วนราชการอื่นแทน ส่วนการแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 นั้น มีหลายกรณีที่ไม่ได้แต่งตั้งจากผู้มีคุณสมบัติเป็นไปตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมาย แต่เป็นการแต่งตั้งตามดุลพินิจของรัฐมนตรีกระทรวงไอซีที หรือแต่งตั้งเจ้าพนักงานที่ไม่ได้มีความรู้ความเชี่ยวชาญด้านนี้ เพียงเพื่อให้เจ้าหน้าที่นั้นมีอำนาจในการขอข้อมูลจากผู้ให้บริการตาม พ.ร.บ. คอมพิวเตอร์ฯ 2550 เท่านั้น ซึ่งเหล่านี้ย่อมส่งผลกระทบโดยตรงต่อความน่าเชื่อถือของเจ้าหน้าที่รัฐ

4) เนื่องจากกฎหมายให้อำนาจแก่พนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในการสอบถาม เรียกขอดูข้อมูล ทำสำเนาข้อมูลคอมพิวเตอร์ ในอีกด้านหนึ่งก็ทำให้ถูกตีความได้ว่า เจ้าหน้าที่สืบสวนสอบสวนคนอื่นๆ ไม่มีอำนาจเหล่านั้น ส่งผลให้ความผิดบางลักษณะ เช่น การฉ้อโกงที่ใช้วิธีหลอกลวงผ่านทางเว็บไซต์ ซึ่งเข้าองค์ประกอบความผิดในฐานฉ้อโกงตามประมวลกฎหมายอาญาอยู่แล้ว เพียงแต่ใช้คอมพิวเตอร์เพื่ออำนวยความสะดวกในการกระทำความผิดนั้น ในทางปฏิบัติเจ้าหน้าที่ต้องสั่งฟ้องตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ด้วย เพื่อให้เจ้าหน้าที่มีอำนาจขอข้อมูลจากผู้ให้บริการ จึงทำให้คดีทั้งหมดที่มีคอมพิวเตอร์เข้าไปเกี่ยวข้องกระจุกตัวอยู่ที่ศูนย์กลาง

<u>กลุ่มผู้ประกอบการอินเทอร์เน็ต</u>: พบปัญหาหลักสามประเด็นคือ

1) การตีความมาตรา 15 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งกำหนดว่าผู้ให้บริการที่ “จงใจสนับสนุน หรือยินยอม” ให้มีการเผยแพร่ข้อความที่เป็นความผิด (ตามมาตรา 14) ต้องรับโทษเท่ากับผู้โพสต์ข้อความนั้น ทำให้ฝ่ายผู้ให้บริการมีความกังวลใจ เพราะไม่มั่นใจว่ารัฐให้ความหมาย หรือใช้

ตัวชี้วัดใดในการที่จะพิสูจน์ว่าผู้ให้บริการ “จงใจสนับสนุนหรือยินยอม” ให้เผยแพร่สิ่งผิดกฎหมายหรือไม่

2) พบปัญหาการให้ความร่วมมือกับภาครัฐกรณีการปิดกั้นเว็บไซต์ เพราะแม้ผู้ให้บริการจะพยายามเร่งดำเนินการแล้ว แต่บางครั้งข้อมูลที่ภาครัฐแจ้งให้ระงับการเข้าถึงขาดความชัดเจน มีข้อผิดพลาด หรือไม่ได้อยู่ในสภาพที่ผู้ให้บริการจะดำเนินการอย่างรวดเร็วได้ เช่น พิมพ์คำสั่งลงบนกระดาษแทนที่จะให้ข้อมูลเป็นไฟล์ ทำให้ผู้ให้บริการถูกฟ้องร้องดำเนินคดี นอกจากนี้ ปัจจุบัน ประเทศไทยยังไม่มีแนวปฏิบัติที่ชัดเจนระหว่างกระทรวงไอซีทีกับผู้ให้บริการว่าจะแสดงเหตุผลในการปิดกั้นเว็บไซต์แก่ประชาชนอย่างไร อีกทั้งยังพบปัญหาการบังคับใช้กฎหมายไม่ทั่วถึง กล่าวคือ ผู้ให้บริการบางรายได้รับคำสั่งปิดกั้น แต่บางรายไม่ได้รับ ส่งผลให้เกิดความไม่พอใจผู้ให้บริการในกลุ่มลูกค้าผู้ใช้บริการ

3) แม้มี พ.ร.บ. คอมพิวเตอร์ฯ 2550 แล้วก็ตาม แต่รูปแบบการ “ขอความร่วมมือ” จากฝ่ายรัฐ ยังคงปรากฏอยู่ โดยส่วนใหญ่อ้างเหตุผลในแง่ความจำเป็นเร่งด่วนขอให้ปิดกั้นไปก่อน แล้วจะส่งคำสั่งศาลตามมาภายหลัง ซึ่งบางครั้งไม่ได้ส่งมาตามที่บอก

<u>กลุ่มเว็บมาสเตอร์</u>: พบปัญหาสี่ประเด็นหลัก ดังนี้

1) เมื่อ พ.ร.บ.คอมพิวเตอร์ฯ 2550 กำหนดโทษให้ตัวกลาง ทำให้เจ้าหน้าที่รัฐเน้นการฟ้องคดีผู้ให้บริการเพื่อหาคนมารับผิดชอบเนื้อหาให้ได้มากกว่าการสืบหาผู้กระทำความผิดตัวจริง

2) ถ้อยคำในกฎหมายยังคลุมเครือ ปล่อยให้เป็นดุลพินิจของเจ้าหน้าที่รัฐมากเกินไป เช่น เรื่องข้อมูลปลอมหรือเท็จตามมาตรา 14 (1) ซึ่งในทางปฏิบัติมักถูกใช้ไปกับกรณีหมิ่นประมาทบุคคล ทำให้เกิดความลักลั่นกับประมวลกฎหมายอาญา

3) พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีแนวโน้มถูกนำไปใช้ในทางละเมิดเสรีภาพมากกว่าการคุ้มครอง ผู้ให้บริการเว็บไซต์เห็นว่ากฎหมายไม่ได้ถูกออกแบบมารองรับเรื่องเสรีภาพในการนำเสนอข่าว และพบว่าผู้บังคับใช้

กฎหมายไม่ได้ใช้กฎหมายอย่างตรงไปตรงมา ยังขาดความเข้าใจและใช้กฎหมายผิดวัตถุประสงค์ ผลเสียคือทำให้กฎหมายนี้ถูกใช้เป็นเครื่องมือทำลายคนที่มีความคิดเห็นแตกต่างกัน

4) กฎหมายนี้ทำให้ผู้ประสงค์จะประกอบธุรกิจด้านนี้ต้องแบกรับภาระมากเกินไป ทั้งในแง่งบประมาณ บุคลากร รวมทั้งความเสี่ยงที่จะต้องมีความรับผิด ซึ่งเรื่องเหล่านี้อาจจะไม่เป็นอุปสรรคสำหรับสื่อขนาดใหญ่ แต่เป็นอุปสรรคสำคัญสำหรับเว็บไซต์ประเภทที่ผู้ใช้เป็นผู้สร้างเนื้อหา (user-generated content) และเว็บไซต์ขนาดเล็ก ผลกระทบที่เกิดขึ้น คือ ทำให้เกิดการเซ็นเซอร์ตัวเองยิ่งขึ้น หรือมิเช่นนั้นก็ต้องใช้วิธีการอื่นใดเพื่อหลบเลี่ยงกฎหมาย เช่น ย้ายเซิร์ฟเวอร์ไปต่างประเทศ ซึ่งย่อมกระทบต่อธุรกิจด้านนี้ในภาพรวม

3. ความคิดเห็นและข้อเสนอแนะเพิ่มเติมเกี่ยวกับ พ.ร.บ. คอมพิวเตอร์ฯ 2550 และนโยบายรัฐ

กลุ่มภาครัฐ: ยังมีความจำเป็นต้องมีกลไก หรือมาตรการระงับการเข้าถึงเว็บไซต์อยู่ เพราะช่วยบรรเทาปัญหาได้ ส่วนการดำเนินคดีที่เกี่ยวกับคอมพิวเตอร์นั้น ควรเพิ่มอำนาจแก่พนักงานเจ้าหน้าที่สอบสวนทั่วๆ ไปให้สามารถใช้อำนาจในการขอดู ขอทำสำเนา และยึดอายัดพยานหลักฐานอิเล็กทรอนิกส์ได้ ในขณะที่พนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งแต่งตั้งโดยรัฐมนตรีกระทรวงไอซีทีสามารถทำหน้าที่ในเชิงสนับสนุน หรือให้ความช่วยเหลือเฉพาะทาง และยังมีความเห็นจากแหล่งข้อมูลส่วนหนึ่งว่า ควรจัดตั้งศาลชำนัญพิเศษเรื่อง พ.ร.บ.คอมพิวเตอร์ฯ 2550 หรือมีผู้พิพากษาสมทบร่วมพิจารณาคดีที่เกี่ยวกับคอมพิวเตอร์

กลุ่มผู้ประกอบการอินเทอร์เน็ต: ผู้ให้บริการส่วนใหญ่เห็นว่าการระงับการเข้าถึงเว็บไซต์ยังมีความจำเป็นอยู่ แต่รัฐไม่ควรนำมาตรการนี้มา

ใช้เป็นเครื่องมืออย่างพร่ำเพรื่อในการปิดกั้นสื่อ หรือปิดปากประชาชน โดยเฉพาะอย่างยิ่งไม่ควรนำปัญหาทางการเมืองมาเป็นเหตุผลในการปิดกั้น ในขณะที่กลไกการกลั่นกรองการปิดกั้นโดยศาลเป็นเรื่องเหมาะสมแล้ว แต่ก็ควรมีกลไกอื่นเพื่อไว้แก้ปัญหากรณีที่คำสั่งศาลนั้นไม่ชอบด้วยกฎหมายด้วย อย่างไรก็ดี ผู้ให้บริการส่วนหนึ่งเห็นว่าที่ผ่านมา พ.ร.บ.คอมพิวเตอร์ฯ 2550 ถูกใช้เป็นเครื่องมือของรัฐมากกว่าใช้แก้ไขปัญหาให้ประชาชนที่ได้รับความเดือดร้อน จึงเสนอว่ากรณีที่มีเว็บไซต์กระทำความผิดจริง และรัฐมีพยานหลักฐานชัดเจน แทนที่รัฐจะใช้วิธีปิดกั้นเว็บไซต์ซึ่งอาจแก้ปัญหาไม่ได้ รัฐควรเลือกใช้วิธีแก้ปัญหาที่ต้นเหตุ เช่น ดำเนินคดีกับผู้กระทำความผิดแทน

ข้อเสนออื่นๆ ที่เกี่ยวกับ พ.ร.บ.คอมพิวเตอร์ฯ 2550 เช่น หากรัฐต้องการให้ผู้ให้บริการมีส่วนรับผิดชอบต่อเนื้อหาด้วย กฎหมายต้องแบ่งระดับความรับผิดชอบของผู้ให้บริการให้ชัดเจนกว่าที่เป็นอยู่ และมีแนวปฏิบัติเกี่ยวกับการแจ้งให้ดำเนินการกับข้อความ (takedown procedure) อย่างไรก็ดี รัฐควรออกกฎหมายบนพื้นฐานความเข้าใจที่ว่า ผู้ให้บริการบางประเภทมีสถานะเป็นเพียง “ตัวกลาง” ในการส่งผ่านเนื้อหา ไม่ได้มีหน้าที่ในการตรวจสอบดูแลเนื้อหาโดยตรง ดังนั้น การกำหนดให้ผู้ให้บริการประเภทดังกล่าวมีหน้าที่ตรวจตราเนื้อหาในอินเทอร์เน็ต (ซึ่งมีจำนวนมหาศาล) ด้วย จึงไม่เหมาะสมอย่างยิ่ง และหากในอนาคตจะมีการปรับปรุงแก้ไขกฎหมาย ผู้มีอำนาจหน้าที่เกี่ยวข้องก็ควรคำนึงถึงการเปลี่ยนแปลงของโลกเทคโนโลยีด้วย

<u>กลุ่มเว็บมาสเตอร์</u>: กลุ่มผู้ให้บริการเนื้อหา (content provider) และผู้ดูแลเว็บไซต์ยังคงเห็นว่า พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีความจำเป็นเพื่อป้องกันการกระทำความผิด แต่ก็ควรให้ความสำคัญกับกลไกที่จะนำมาใช้ในการปกป้องคุ้มครองผู้ใช้บริการอินเทอร์เน็ตด้วย ในขณะที่ปัจจุบันยังคงมีอีกหลายเรื่องที่ผู้ใช้อินเทอร์เน็ตไม่ได้รับการคุ้มครอง เช่น ข้อมูลส่วนบุคคล ในขณะที่กฎหมายกำหนดภาระหน้าที่และความรับผิดมากเกินสมควรให้กับผู้ให้บริการ ซึ่งย่อมส่งผลกระทบต่อการใช้บริการได้ในที่สุด จึงเสนอว่า

กฎหมายต้องปรับตัวให้สอดคล้องกับลักษณะของการสื่อสารออนไลน์ ซึ่งมีการเปลี่ยนรูปแบบอยู่เสมอ และรัฐควรมีมาตรการในการให้ความรู้เกี่ยวกับ พ.ร.บ.คอมพิวเตอร์ ฯ 2550 กับประชาชนมากกว่านี้ นอกจากนี้ รัฐควรให้ความเคารพประชาชน โดยแทนที่จะใช้การบังคับกฎหมาย และกำหนดภาระความรับผิดอย่างเดียว ควรหันมาใช้นโยบายให้ผู้ให้บริการกำกับดูแลกันเอง รวมถึงให้มีคณะกรรมการกลั่นกรองเรื่องการปิดกั้นเว็บไซต์ด้วย

บทที่

ผลการศึกษาภาคที่ 2

การศึกษากฎหมาย แนวนโยบายแห่งรัฐ
ปฏิกิริยาภาคประชาชนต่อกรณีเสรีภาพ
ในการแสดงความคิดเห็นในสื่อออนไลน์
เปรียบเทียบไทยกับต่างประเทศ:
กฎหมายไทย กับสิทธิและเสรีภาพในสื่อออนไลน์

กฎหมายไทย กับสิทธิและเสรีภาพในสื่อออนไลน์

1. หลักการคุ้มครองเสรีภาพในการแสดงความคิดเห็นตามรัฐธรรมนูญแห่งราชอาณาจักรไทย

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 บัญญัติรับรองสิทธิและเสรีภาพของชนชาวไทยไว้ในหมวด 3 มาตรา 26 ถึงมาตรา 69 อย่างไรก็ดี ประเทศไทยเริ่มเห็นความสำคัญของสิทธิและเสรีภาพของประชาชนและบัญญัติรับรองอย่างเป็นลายลักษณ์อักษรมาตั้งแต่รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 โดยนอกจากมีเป้าหมายในการให้ความคุ้มครองสิทธิและเสรีภาพเหล่านั้น และไม่ให้บุคคลละเมิดสิทธิเสรีภาพซึ่งกันและกันแล้ว ยังเป็นไปเพื่อป้องกันไม่ให้องค์กรต่าง ๆ ของรัฐใช้อำนาจละเมิดสิทธิและเสรีภาพของประชาชนตามอำเภอใจด้วย[1] ซึ่งถือเป็นการยืนยัน “หลักนิติรัฐ” (Rechtstaatsprincip) ซึ่งมีความสัมพันธ์ใกล้ชิดกับการปกครองในระบอบประชาธิปไตย สำหรับบทบัญญัติคุ้มครองเสรีภาพในการแสดงความคิดเห็นของประชาชน (รวมทั้งสื่อมวลชน ซึ่งย่อมหมายถึงการ

รับรองสิทธิในการรับรู้ข้อมูลข่าวสารด้วย) นั้น บัญญัติทั้งในรัฐธรรมนูญแห่งราชอาณาจักรไทยปี พ.ศ. 2540 และสืบเนื่องต่อมาในรัฐธรรมนูญปี 2550 **มาตรา 45** ความว่า

"บุคคลย่อมมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น

การจำกัดเสรีภาพตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เฉพาะเพื่อรักษาความมั่นคงของรัฐ เพื่อคุ้มครองสิทธิ เสรีภาพ เกียรติยศ ชื่อเสียง สิทธิในครอบครัวหรือความเป็นอยู่ส่วนตัวของบุคคลอื่น เพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดี ของประชาชน หรือเพื่อป้องกันหรือระงับความเสื่อมทรามทางจิตใจหรือสุขภาพของประชาชน

การสั่งปิดกิจการหนังสือพิมพ์ หรือสื่อมวลชนอื่นเพื่อลิดรอนเสรีภาพตามมาตรานี้ จะกระทำมิได้

การห้ามหนังสือพิมพ์หรือสื่อมวลชนอื่นเสนอข่าวสารหรือแสดงความคิดเห็น ทั้งหมด หรือบางส่วน หรือการแทรกแซงด้วยวิธีการใดๆ เพื่อลิดรอนเสรีภาพตามมาตรานี้ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายซึ่งได้ตราขึ้นตามวรรคสอง

การให้นำข่าวหรือบทความไปให้เจ้าหน้าที่ตรวจก่อนนำไปโฆษณาในหนังสือพิมพ์ หรือสื่อมวลชนอื่น จะกระทำมิได้ เว้นแต่จะกระทำในระหว่างเวลาที่ประเทศอยู่ในภาวะสงคราม แต่ทั้งนี้จะต้องกระทำโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายซึ่งได้ตราขึ้น ตามวรรคสอง

เจ้าของกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่นต้องเป็นบุคคลสัญชาติไทย

การให้เงินหรือทรัพย์สินอื่นเพื่ออุดหนุนกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่นของเอกชน รัฐจะกระทำมิได้"

เมื่อพิจารณาจากบทบัญญัติดังกล่าวจะเห็นได้ว่า แม้ในรัฐธรรมนูญซึ่งเป็นกฎหมายสูงสุดของประเทศเอง ก็หาได้กำหนดให้การใช้เสรีภาพของบุคคลในเรื่องนี้ เป็นไปอย่างไม่มีขอบเขต หรือข้อจำกัดใดๆ ไม่ แต่คง

ยืนยันในหลักการที่ว่า “รัฐ” ในฐานะตัวแทนผู้ใช้อำนาจปกครองย่อมกำหนดมาตรการทางกฎหมาย เพื่อจำกัด หรือควบคุมการใช้เสรีภาพของประชาชน และ/หรือสื่อมวลชนได้เช่นกัน ทั้งนี้ภายใต้เหตุผลหลัก 4 ประการ คือ 1) เพื่อความมั่นคงของรัฐ 2) เพื่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน 3) เพื่อคุ้มครองสิทธิส่วนบุคคลหรือชื่อเสียงเกียรติยศของบุคคลอื่น และ 4) เพื่อป้องกันหรือระงับความเสื่อมทรามทางจิตใจหรือสุขภาพของประชาชน (มาตรา 45 วรรค 2) แต่ทั้งนี้ ฝ่ายรัฐเองคงต้องไม่ลืมด้วยว่า รัฐธรรมนูญยังมีบทบัญญัติเพื่อกำกับควบคุม “การใช้อำนาจควบคุมหรือจำกัดสิทธิและเสรีภาพของประชาชน” โดยรัฐไว้ด้วยอีกชั้นหนึ่ง เพื่อป้องกันไม่ให้การใช้อำนาจนั้นเกินขอบเขต หรือล่วงละเมิดประชาชนจนเกินไป ดังปรากฏอยู่ใน **มาตรา 29** แห่งรัฐธรรมนูญ

“การจำกัดสิทธิและเสรีภาพของบุคคลที่รัฐธรรมนูญรับรองไว้จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อการที่รัฐธรรมนูญนี้กำหนดไว้ และเท่าที่จำเป็น และจะกระทบกระเทือนสาระสำคัญแห่งสิทธิและเสรีภาพนั้นมิได้...”

จากบทบัญญัติมาตรานี้จะเห็นได้ว่า เพื่อคุ้มครองสิทธิเสรีภาพของบุคคล ในขณะเดียวกันก็เพื่อป้องกันการใช้อำนาจตามอำเภอใจโดยองค์กรของรัฐ แม้รัฐจะมีอำนาจจำกัดสิทธิเสรีภาพของบุคคลตามที่รัฐธรรมนูญรับรองไว้ได้ แต่ก็ต้องอยู่ภายใต้หลักเกณฑ์สำคัญอย่างน้อย 4 ประการ คือ

1) การจำกัดสิทธิและเสรีภาพต้องอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะ

2) การจำกัดสิทธิและเสรีภาพต้องเป็นไปเพื่อการที่รัฐธรรมนูญกำหนด กล่าวคือ ต้องทำไปเพื่อคุ้มครอง “ประโยชน์สาธารณะ” (public interest) ซึ่งเป็นความมุ่งหมาย หรือวัตถุประสงค์ของการดำเนินการของรัฐเพื่อตอบสนองความต้องการของคนส่วนใหญ่ในสังคม[2] ในกรณีของเสรีภาพในการแสดงความคิดเห็นก็คือ ต้องอยู่ภายในกรอบของเหตุผลสี่ประการตามมาตรา 45 วรรคสอง (ดังกล่าวมาแล้ว) เท่านั้น

3) จะต้องกระทำเพียง “เท่าที่จำเป็น” หรือกล่าวอีกอย่างก็คือ

การจำกัดสิทธิและเสรีภาพของบุคคลนั้นต้องเป็นไปตาม “หลักแห่งความได้สัดส่วน” (Principle of Proportionality) ซึ่งเป็นหลักสากลที่ถูกคิดค้นขึ้นเพื่อควบคุมการใช้อำนาจตามอำเภอใจของฝ่ายรัฐ ซึ่งประกอบด้วยหลักเกณฑ์ย่อยสามประการคือ (1) “หลักแห่งความสัมฤทธิ์ผล” คือ หลักที่รัฐต้องเลือกใช้มาตรการที่สามารถดำเนินการให้บรรลุตามเจตนารมณ์ หรือสิ่งที่รัฐธรรมนูญประสงค์จะให้เกิดขึ้น เท่านั้น (2) “หลักแห่งความจำเป็น” ถ้ารัฐมีมาตรการในการจำกัดเสรีภาพของบุคคลหลายมาตรการ รัฐต้องเลือกใช้มาตรการที่กระทบต่อเสรีภาพนั้นให้น้อยที่สุดเท่าที่สามารถบรรลุเจตนารมณ์ของรัฐธรรมนูญได้ และ (3) “หลักแห่งความเหมาะสม” ถ้าการใช้มาตรการในการจำกัดเสรีภาพก่อให้เกิดประโยชน์แก่มหาชนน้อย และไม่คุ้มค่ากับความเสียหายที่จะเกิดแก่เสรีภาพของปัจเจกชน รัฐต้องละเว้นไม่ใช้มาตรการนั้น[3]

4) การจำกัดสิทธิและเสรีภาพจะต้องไม่กระทบกับสาระสำคัญแห่งสิทธิและเสรีภาพนั้น ซึ่งมีความหมายอีกนัยหนึ่งว่า เมื่อรัฐธรรมนูญรับรองคุ้มครองสิทธิและเสรีภาพในเรื่องใดเรื่องหนึ่งไว้แล้ว รัฐย่อมมีอำนาจกระทำได้ก็เฉพาะแต่เพียงการ “จำกัด” ขอบเขตของการใช้สิทธิและเสรีภาพของบุคคลในเรื่องนั้นๆ เท่านั้น จะกระทำการใดๆ ที่ส่งผลถึงขนาดเป็นการ “กำจัด” หรือ “เพิกถอน” สิทธิและเสรีภาพเหล่านั้นไปเลยมิได้[4] หากบทบัญญัติแห่งกฎหมายฉบับใดให้ผลถึงขนาดนั้น ย่อมใช้บังคับมิได้ ทั้งนี้โดยผลแห่งมาตรา 6 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550[5] เนื่องจากเป็นกฎหมายที่ขัดหรือแย้งกับรัฐธรรมนูญ

กล่าวโดยสรุป แม้สิทธิและเสรีภาพตามที่รัฐธรรมนูญคุ้มครองจะเป็นเรื่องที่ต้องมีขอบเขต และแม้รัฐ คือ ผู้มีอำนาจในการกำหนดขอบเขตจำกัด หรือควบคุมการใช้สิทธิและเสรีภาพเช่นว่านั้น โดยอาศัยการออกกฎหมาย และบังคับการต่างๆ ไปตามอำนาจที่กำหนดไว้ในกฎหมายที่ออก แต่ก็หาได้หมายความว่า รัฐจะสามารถออกกฎหมายที่ไม่ยุติธรรม หรือใช้อำนาจตามกฎหมายนั้นอย่างไม่เป็นธรรม ตามอำเภอใจ หรือขัดต่อสิทธิและเสรีภาพของประชาชนอย่างเกินสมควรแก่เหตุได้

2. ความเป็นมา และปัญหาในภาพรวมของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ปัจจุบัน กฎหมายไทยฉบับหลักที่มีผลโดยตรงต่อเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นในสื่อออนไลน์ ซึ่งอยู่ในขอบเขตของงานวิจัยฉบับนี้ คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยกฎหมายฉบับนี้มีเป้าหมายในการกำหนดความผิดและโทษสำหรับการกระทำที่เกี่ยวข้องกับระบบหรือข้อมูลคอมพิวเตอร์ ทั้งในแง่ของการใช้ระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด และในแง่ของการลงมือกระทำความผิดต่อตัวระบบหรือข้อมูลคอมพิวเตอร์เอง พ.ร.บ.คอมพิวเตอร์ฯ 2550 เป็นกฎหมายหนึ่งในกฎหมาย 6 ฉบับ[6] ที่ต้องศึกษาพัฒนาและบัญญัติให้แล้วเสร็จเพื่อประกาศใช้ให้ได้ตาม “โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ” ซึ่งริเริ่มและดำเนินการโดยกระทรวงวิทยาศาสตร์และเทคโนโลยีสิ่งแวดล้อมมาตั้งแต่ปี พ.ศ. 2541 อย่างไรก็ดี จนถึงปัจจุบันคงมีกฎหมายในโครงการดังกล่าวเพียงสองฉบับเท่านั้นที่มีผลบังคับใช้แล้ว คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544[7] ทั้งนี้ ยังไม่มีความชัดเจนใดๆ ว่าร่างกฎหมายฉบับอื่นๆ ในโครงการเดียวกันจะถูกผลักดันให้เป็นกฎหมายได้เมื่อใด

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ต่อไปจะเรียกว่า “พ.ร.บ.คอมพิวเตอร์ฯ 2550”) บัญญัติเสร็จสิ้น และมีผลบังคับใช้ภายหลังพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์บังคับใช้ไปแล้วราว 6 ปี โดยถูกแก้ไขปรับปรุงเรื่อยมาจากร่างกฎหมาย 4 ฉบับ[8] เป็นที่น่าสังเกตว่าหลักการและเหตุผลแรกเริ่มของการบัญญัติกฎหมายฉบับนี้ ซึ่งขณะนั้นใช้ชื่อว่า “พระราชบัญญัติอาชญากรรมคอมพิวเตอร์” ถูกประกาศในโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศใจความว่า *“โดยมีวัตถุประสงค์เพื่อกำหนดมาตรการทางอาญาในการลงโทษ*

ผู้กระทำผิดต่อระบบการทำงานของคอมพิวเตอร์ ระบบข้อมูล และระบบเครือข่าย ซึ่งในปัจจุบันยังไม่มีบทบัญญัติของกฎหมายฉบับใดกำหนดว่าเป็นความผิด ทั้งนี้ เพื่อเป็นหลักประกันสิทธิเสรีภาพและการคุ้มครองการอยู่ร่วมกันของสังคม" [9] แต่เมื่อมีการปรับปรุงแก้ไขร่างกฎหมายหลายครั้ง จนผ่านออกมาเป็นกฎหมายโดยการพิจารณาของคณะกรรมการวิสามัญของสภานิติบัญญัติแห่งชาติ (สนช.) ที่ได้รับการแต่งตั้งขึ้นภายหลังรัฐประหาร ปี พ.ศ. 2549[10] พบว่า นอกจากประเด็นในเรื่อง "หลักประกันสิทธิเสรีภาพ" จะสูญหายไปจาก "หลักการและเหตุผล" ของกฎหมายฉบับนี้แล้ว ยังปรากฏฐานความผิดเกี่ยวกับการเผยแพร่เนื้อหาในอินเทอร์เน็ตในมาตรา 14 ซึ่งใช้ถ้อยคำคลุมเครือ มีมาตรา 15 กำหนดความผิดและโทษสำหรับผู้ให้บริการไว้ให้เท่ากับตัวการผู้กระทำความผิด อีกทั้งมีบทจำแนกประเภทผู้ให้บริการในลักษณะที่ไม่สอดคล้องกับความเข้าใจในวงการเทคโนโลยีสารสนเทศ (มาตรา 3) โดยเฉพาะอย่างยิ่ง มีมาตรา 20 ให้อำนาจรัฐในการระงับการเผยแพร่ข้อมูลต่าง ๆ ในระบบคอมพิวเตอร์ ในฐานะมาตรการเร่งด่วน ซึ่งมีเงื่อนไขครอบคลุมเนื้อหากว้างขวาง จนส่งผลให้เกิดปัญหาในแง่ของการใช้การตีความในเวลาต่อมา ในระยะเวลากว่า 4 ปี ของการมีผลบังคับใช้ จึงเกิดเสียงวิพากษ์วิจารณ์มาโดยตลอดว่า พ.ร.บ.คอมพิวเตอร์ฯ 2550 ถูกสร้างขึ้นเพื่อให้ฝ่ายรัฐใช้เป็นเครื่องมือควบคุม และปิดกั้นการแสดงความคิดเห็นของประชาชนได้โดยชอบด้วยกฎหมาย

3. ปัญหาของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในประเด็นเสรีภาพในการแสดงความคิดเห็นของประชาชน

หากกล่าวถึงสถานการณ์สิทธิและเสรีภาพในการรับรู้ข้อมูลข่าวสารและแสดงออกซึ่งความคิดเห็นของประชาชนไทยกันอย่างจริงจังแล้ว อาจเห็นได้ว่าช่วงหลายปีที่ผ่านมาสถานการณ์ดังกล่าวอยู่ในระดับที่น่าเป็นห่วง เพราะนับเนื่องจากกลางสมัยรัฐบาล พ.ต.ท. ทักษิณ ชินวัตร รัฐบาลรัฐประหาร รัฐบาลสมัคร-สมชาย รัฐบาลนายอภิสิทธิ์ เวชชาชีวะ ช่วงของการ

ประกาศสถานการณ์ฉุกเฉินในเหตุการณ์ความขัดแย้งทางการเมืองเดือนเมษายน-พฤษภาคม 2553 กระทั่งช่วงต้นของรัฐบาลที่มีนางสาวยิ่งลักษณ์ ชินวัตร เป็นนายกรัฐมนตรี สื่อมวลชน โดยเฉพาะอย่างยิ่งสื่อกระแสรองอย่างเว็บไซต์ กระดานข่าว และช่องทางการติดต่อสื่อสารส่วนบุคคล หรือกลุ่มคนรูปแบบต่างๆ ไม่ว่าจะเป็นโทรศัพท์ SMS จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายสังคม (social network) อย่างเฟซบุค (Facebook) หรือทวิตเตอร์ (Twitter) ล้วนแล้วแต่ถูกสอดส่องและกำกับควบคุมโดยภาครัฐมาแล้วทั้งสิ้น

อย่างไรก็ตาม ควรต้องเข้าใจด้วยว่า เพียงการเฝ้าระวังหรือสอดส่องเนื้อหาที่เผยแพร่ในพื้นที่สาธารณะโดยภาครัฐก็ดี หรือโดยภาคเอกชนก็ดี เพื่อป้องกันการกระทำความผิดที่อาจเกิดขึ้นในโลกออนไลน์นั้น ย่อมเป็นสิ่งที่กระทำได้ เสมือนหนึ่งการลาดตระเวนเพื่อตรวจตราความสงบเรียบร้อยในเขตท้องที่ต่างๆ ของตำรวจในโลกแห่งความเป็นจริง เพียงแค่ดำเนินการไปเช่นนั้นคงมิอาจถือได้ว่ารัฐล่วงละเมิดสิทธิและเสรีภาพของประชาชนแล้ว แต่หากสิ่งที่เกิดขึ้นนั้นมิใช่เพียงแค่ลาดตระเวนเพื่อตรวจตราความเรียบร้อย กลับเลยไปถึงขั้นคุกคาม แทรกแซง ลบทิ้ง ปิดกั้นช่องทางเข้าถึงหรือควบคุมการแสดงออกไม่ว่าด้วยวิธีใดๆ โดยไม่มีกระบวนการพิสูจน์ความผิดหรือการพิจารณาคดี กรณีดังกล่าวมานี้ก็จำเป็นต้องถูกตรวจสอบได้โดยฝ่ายประชาชนผู้ได้รับผลกระทบ

ในช่วงที่ผ่านมาประโยคที่ว่า “ปัญหาไม่ได้อยู่ที่ตัวกฎหมาย แต่อยู่ที่ผู้บังคับใช้กฎหมาย” คือประโยคที่หลายฝ่ายใช้กล่าวถึงปัญหาของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งอันที่จริง “ความจริง” ข้อนี้หาได้จำกัดไว้แต่เฉพาะกับ พ.ร.บ.คอมพิวเตอร์ฯ 2550 เท่านั้นไม่ แต่เป็น “ปัญหาร่วมกัน” ของกฎหมายไทยส่วนใหญ่เลยทีเดียว อย่างไรก็ตาม การกล่าวประโยคนี้แล้วมองข้าม “ปัญหาอื่นๆ” ของกฎหมายฉบับนั้นไป หรือกล่าวประโยคนี้ขึ้นโดยผู้กล่าวมีเจตนาเพื่อหลีกเลี่ยงที่จะไม่พิจารณาว่าแท้ที่จริงแล้ว “ตัวบทบัญญัติ” ของกฎหมายเองก็มีปัญหาที่จำเป็นต้องได้รับการปรับปรุงแก้ไขเช่นเดียวกัน ย่อมไม่ใช่เรื่องที่ถูกต้อง หากพิจารณาบทบัญญัติต่างๆ ของ

พ.ร.บ.คอมพิวเตอร์ฯ 2550 ที่เกี่ยวข้องกับสิทธิและเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นสื่อออนไลน์ ประกอบกับสถิติตัวเลขต่างๆ สถานการณ์การใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 รวมทั้งความคิดเห็นที่สะท้อนมาจากเจ้าหน้าที่รัฐ และผู้ประกอบการอินเทอร์เน็ต ซึ่งปรากฏอยู่ในผลการวิจัยภาคที่ 1 ย่อมพบว่าแท้ที่จริงแล้วปัญหาของกฎหมายฉบับนี้ไม่ได้อยู่ที่ผู้บังคับใช้กฎหมายแต่เพียงอย่างเดียวเท่านั้น หากแต่ถ้อยคำในกฎหมายฉบับนี้เองได้สร้างความสับสน ทั้งยังเปิดช่องหรือเอื้อให้สิทธิและเสรีภาพของประชาชนถูกล่วงละเมิดจากฝ่ายรัฐได้โดยง่ายด้วย และด้วยเหตุนี้เอง คณะผู้วิจัยจึงได้ศึกษาวิเคราะห์และเสนอไว้ในรายงานวิจัยฉบับนี้เพื่อชี้ให้เห็นปัญหาของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในส่วนที่อยู่นอกเหนือจาก “ปัญหาการบังคับใช้” ว่ามีอย่างไรบ้าง ดังนี้

3.1 บทนิยามคำศัพท์

มาตรา 4 *“ผู้ให้บริการ” หมายความว่า*

(1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

คำนิยามที่น่าจะเป็นปัญหาที่สุดต่อการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ พ.ศ. 2550 โดยเฉพาะอย่างยิ่งในประเด็นเสรีภาพในการรับรู้ข้อมูลข่าวสาร คือคำว่า “ผู้ให้บริการ” ซึ่งมักถูกวิพากษ์วิจารณ์ในเรื่องของความไม่ชัดเจน ทั้งการแบ่งประเภทก็ไม่สอดคล้องกับความเข้าใจในทางเทคโนโลยีสารสนเทศ[11] เป็นที่น่าสังเกตว่า นอกจากความไม่ชัดเจนของถ้อยคำใน พ.ร.บ.คอมพิวเตอร์ฯ 2550 เองแล้ว รายละเอียดที่กำหนดไว้ใน “ประกาศ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550" [12] ก็ยังมีปัญหาในประเด็นการจำแนกประเภทผู้ให้บริการแบบข้ามหมวดหมู่ไม่สอดคล้องกับคำนิยามจริงอีกด้วย อาทิเช่น แทนที่ผู้ให้บริการคอมพิวเตอร์เซิร์ฟเวอร์ (host service provider) ซึ่งเป็นการบริการให้เช่าใช้พื้นที่เพื่อเก็บรักษาข้อมูลของบุคคลอื่นจะอยู่ในหมวดหมู่ของ "ผู้ให้บริการเก็บรักษาข้อมูลฯ" ตาม (2) กลับอยู่ในหมวดของผู้ให้บริการเข้าสู่อินเทอร์เน็ต หรือติดต่อสื่อสารด้วยวิธีอื่นซึ่งอยู่ใน (1) เป็นต้น

นอกจากนี้ ยังเป็นที่น่าสงสัยว่าด้วยเหตุผลใด พ.ร.บ.คอมพิวเตอร์ฯ 2550 จึงเป็นกฎหมายที่กำหนดภาระหน้าที่และความรับผิดชอบให้แก่ "ผู้ให้บริการโทรคมนาคม" ด้วย ทั้งที่ผู้ให้บริการโทรคมนาคมบางประเภทไม่ได้ทำงาน หรือให้บริการที่เกี่ยวข้องกับฐานความผิดตามพระราชบัญญัติฉบับนี้โดยตรง เช่น ผู้ให้บริการดาวเทียม หรือผู้ให้บริการเอทีเอ็ม เป็นต้น ทั้งนี้ตามบันทึกของสำนักงานคณะกรรมการกฤษฎีกาเคยให้เหตุผลในเรื่องนี้ไว้ว่า *"ผู้ให้บริการ ตาม (1) พ.ร.บ.คอมพิวเตอร์ฯ 2550 ให้หมายรวมถึงบุคคลที่รับจ้างบุคคลอื่นในการสร้างโปรแกรมเพื่อให้ มีการเข้าสู่ระบบคอมพิวเตอร์และผู้ให้บริการโทรศัพท์และโทรคมนาคมด้วย เพราะในการสืบหาตัวผู้กระทำความผิดนั้นจำเป็นต้องขอข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการโทรศัพท์ และโทรคมนาคม เพื่อทราบเส้นทางการติดต่อสื่อสารที่ชัดเจน..."* [13] อย่างไรก็ตาม การกำหนดนิยามคำว่า "ผู้ให้บริการ" ไว้อย่างกว้างขวางทั้งยังรวมเอาผู้ให้บริการโทรคมนาคมและอื่นๆ ไว้เช่นนี้ คณะผู้วิจัยเห็นว่า เป็นการบัญญัติที่ไม่ได้พิจารณากฎหมายในภาพรวมอย่างเพียงพอ ดังจะเห็นได้ว่าใน พ.ร.บ. คอมพิวเตอร์ฯ 2550 นั้น "ผู้ให้บริการ" ไม่ได้มีเฉพาะภาระหน้าที่ในการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ หรือ log file แต่เพียงอย่างเดียว แต่เขาอาจต้องรับผิดต่อการเผยแพร่เนื้อหาของผู้อื่นตามมาตรา 15 ประกอบมาตรา 14 พ.ร.บ. คอมพิวเตอร์ฯ 2550 ด้วย ดังนั้น เมื่อมาตรา 15 ใช้ถ้อยคำกว้างๆ ว่า "ผู้ให้บริการ" ต้องรับผิด โดยไม่ได้มีการเจาะจงว่า หมายถึง ผู้ให้บริการประเภทใด หรือผู้ให้บริการที่เกี่ยวข้อง

กับเนื้อหาของข้อมูลในระดับใด ที่จะตกอยู่ภายใต้บทบัญญัตินี้ ย่อมทำให้ “ผู้ให้บริการทุกประเภท” (ที่แม้โดยลักษณะการทำงาน หรือบริการของเขาจะไม่ได้เกี่ยวข้องกับการแสดงเนื้อหาของข้อมูลโดยตรง เป็นแต่เพียงให้บริการทางเทคนิค เชื่อมโยงคอมพิวเตอร์ จัดการดูแลระบบ ฯลฯ) อาจต้องเข้ามาร่วมรับผิดกับผู้กระทำความผิดที่แท้จริงด้วย เพราะอยู่ในความหมายของ “บทนิยาม” ของคำว่า “ผู้ให้บริการ”

ประเด็นเรื่องความไม่ชัดเจน ทั้งยังครอบคลุมใช้บังคับกับผู้ให้บริการประเภทต่างๆ อย่างกว้างขวาง ไม่ได้จำกัดขอบเขตอยู่เฉพาะแต่ผู้ให้บริการที่เกี่ยวข้องใกล้ชิดกับการ “เผยแพร่ หรือแสดง” เนื้อหาในสื่อออนไลน์ เป็นประเด็นที่ถูกวิพากษ์วิจารณ์มาโดยตลอด แต่ที่ผ่านมาผู้บัญญัติกฎหมายมักให้เหตุผลโต้แย้งว่า ในที่สุดแล้วก็ต้องมีกระบวนการในการพิสูจน์ “เจตนา” ของผู้ให้บริการก่อนที่ศาลจะตัดสินอยู่ดี ดังนั้น หากผู้ให้บริการรายใดไม่รู้เห็น หรือเกี่ยวข้องกับการกระทำความผิด เขาย่อมไม่ต้องมีความรับผิด แต่คำถามสำหรับคำอธิบายดังกล่าวก็คือ เหตุใดทั้ง “รัฐ” เองและ “ผู้ให้บริการ” จึงต้องเสียเวลาหรือต้นทุนอื่นๆ ในการฟ้องร้องและต่อสู้คดีเพื่อผลลัพธ์สุดท้ายที่ว่า บุคคลเหล่านั้นไม่ได้จงใจสนับสนุนหรือยินยอม เพราะเหตุที่ลักษณะการให้บริการของเขาเองไม่มีความเกี่ยวพันกับเนื้อหาที่ถูกเผยแพร่มาตั้งแต่แรกด้วย ทั้งที่ในความเป็นจริงฝ่ายนิติบัญญัติน่าจะสามารถบัญญัติกฎหมายที่วางขอบเขตคำว่า “ผู้ให้บริการ” ให้ชัดเจนกว่านี้ได้ การบัญญัติให้ครอบคลุมกว้างขวางเช่นนี้จึงรังแต่จะสร้างบรรยากาศแห่งความกลัว และเป็นผลให้เกิดการเซ็นเซอร์ตัวเองในหมู่ผู้ให้บริการ ซึ่งย่อมส่งผลกระทบโดยตรงต่อเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นของประชาชนทั่วไป ทั้งยังน่าจะส่งผลไม่โดยตรงก็โดยอ้อมต่อพัฒนาการ และแรงจูงใจในการประกอบกิจการเพื่อให้บริการด้านเทคโนโลยีสารสนเทศ อีกด้วย

3.2 ฐานความผิดใน พ.ร.บ.คอมพิวเตอร์ฯ 2550 ที่กระทบต่อเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นในสื่อออนไลน์

มาตรา 14 *"ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ*

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิด ความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

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

1) มาตรา 14 (1): นับเป็นเรื่องที่น่าสนใจว่า เหตุใดภายหลัง พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีผลบังคับใช้ มาตรา 14 (1) จึงถูกทั้งบุคคลทั่วไปและพนักงานเจ้าหน้าที่นำไปฟ้องร้องผู้กระทำความผิดในลักษณะของการ "หมิ่นประมาท" บุคคลอื่นบนอินเทอร์เน็ต ทั้งที่เป้าหมายของมาตรา 14 (1) มิได้กำหนดองค์ประกอบไว้สำหรับความผิดในฐานนี้ ดังที่ปรากฏในผลการศึกษาสถิติคดีความในรายงานวิจัยฉบับนี้ (ภาค 1) ว่า คดีส่วนใหญ่ที่ฟ้องโดยอาศัยข้อหาตามมาตรา 14 (1) เป็นคดี "หมิ่นประมาท" ซึ่งโจทก์มุ่งเอาผิดกับการใช้ข้อมูลเท็จเพื่อใส่ความหรือกล่าวหากันทางอินเทอร์เน็ต

หรือการนำภาพหรือเรื่องส่วนตัวมาเผยแพร่จนเกิดความเสียหายต่อชื่อเสียง เกียรติยศ หรือถูกดูถูกเกลียดชัง ซึ่งคดีลักษณะนี้เป็นประเภทคดีตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ที่มีจำนวนมากที่สุดด้วย[14]

เจตนารมณ์แรกเริ่มของมาตรา 14 (1) ผู้บัญญัติต้องการอุดช่องว่างของกฎหมายอาญาที่ว่าด้วยการ “ปลอมแปลงเอกสาร” หรือการทำ “เอกสารเท็จ” ซึ่งตามกฎหมายในสมัยเดิมบัญญัติให้คำว่า “เอกสาร” หมายเฉพาะแต่ “กระดาษหรือวัตถุอื่นใดที่มีรูปร่างและจับต้องได้” เท่านั้น[15] จึงทำให้ไม่สามารถตีความกฎหมายเหล่านั้นให้ครอบคลุมถึงการปลอมแปลงข้อมูลอิเล็กทรอนิกส์ได้[16] ก่อให้เกิดช่องว่างของกฎหมาย ฉะนั้น ความหมายของ มาตรา 14 (1) จึงมิได้หมายถึง การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลที่มีเนื้อหา (ไม่ว่าจะเป็นความจริงหรือความเท็จก็ตาม) ที่อาจทำให้บุคคลอื่นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง อันเป็นองค์ประกอบความผิดทำนองเดียวกับความผิดในฐาน “หมิ่นประมาท” ตามประมวลกฎหมายแพ่งฯ หรือประมวลกฎหมายอาญา หากแต่คือ “การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง ข้อมูลคอมพิวเตอร์ไม่แท้จริง (ข้อมูลคอมพิวเตอร์ปลอม) ที่ถูกทำขึ้นโดยผู้ไม่มีอำนาจตามกฎหมายที่จะทำข้อมูลนั้นขึ้นมาได้” หรือมิเช่นนั้นก็คือ “การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่แท้จริง (ผู้มีอำนาจตามกฎหมายเคยทำข้อมูลฯ ดังกล่าวขึ้นแล้วโดยชอบด้วยกฎหมาย) แต่ต่อมาถูกผู้กระทำความผิดแก้ไข เปลี่ยนแปลง หรือทำให้ข้อมูลนั้นผิดความหมาย หรือเปลี่ยนแปลงไปจากเดิม” อันเป็นความหมายแบบเดียวกับความผิดในฐาน “ปลอมแปลงเอกสาร” ตามประมวลกฎหมายอาญา กล่าวคือ ผู้ไม่มีอำนาจตามกฎหมายที่จะทำเอกสารนั้นได้ ได้จัดทำ “เอกสารอันไม่แท้จริง” ขึ้นทั้งฉบับ (โดยจะมี “เอกสารแท้จริง” อยู่ก่อนหรือไม่ ไม่ใช่สาระสำคัญ) หรือแก้ไขเปลี่ยนแปลง “เอกสารที่แท้จริง” เพียงบางส่วนให้เปลี่ยนความหมายไปจากเดิม หรือผิดไปจากของจริง ทั้งนี้ เพื่อให้บุคคลอื่นหลงเชื่อว่าเอกสารนั้นเป็น “เอกสารที่แท้จริง”[17] ยกตัวอย่างเช่น บุคคลที่ไม่ใช่เจ้าหน้าที่รัฐหรืออาจเป็นเจ้าหน้าที่รัฐแต่ไม่ได้อยู่ส่วนงานหรือไม่มีอำนาจหน้าที่ในการออกหนังสือเดินทาง ได้ทำการออกหนังสือเดินทาง

ให้บุคคลอื่นไป เช่นนี้ แม้ข้อมูลในหนังสือเดินทางนั้นจะเป็นความจริงทุกอย่าง เช่น ชื่อนามสกุล ที่อยู่ของเจ้าของหนังสือเดินทางนั้นถูกต้องแท้จริง แต่หนังสือเดินทางดังกล่าวย่อมเป็น “หนังสือเดินทางปลอม” หรือในอีกกรณีหนึ่ง คือ นำเอาหนังสือเดินทางของจริงของ นาย ก. มาลบ ตัดทอน หรือแก้ไขเพิ่มเติมเนื้อความเพื่อให้กลายเป็นหนังสือเดินทางของนาย ข. แทน เป็นต้น ซึ่งทั้งสองกรณีดังกล่าวถือได้ว่าผู้กระทำมีความผิดฐานปลอมเอกสารตามประมวลกฎหมายอาญาแล้ว โดยสรุปก็คือ หากจะต้องมีการตีความมาตรา 14 (1) เพื่อบังคับใช้ จะต้องเป็นการตีความเทียบเคียงลักษณะความผิดกับการปลอมหรือแปลงเอกสารดังกล่าวเท่านั้น ไม่ใช่การหมิ่นประมาทบุคคลอื่น

สำหรับการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง “ข้อมูลคอมพิวเตอร์อันเป็นเท็จ” นั้น ที่ถูกต้องแล้วก็ควรจะใช้วิธีการตีความบนหลักการเดียวกันกับการทำ “เอกสารเท็จ” ตามประมวลกฎหมายอาญาในหมวด “ความผิดเกี่ยวกับเอกสาร” เช่นกัน คือ เป็นกรณีที่บุคคลผู้มีอำนาจทำเอกสาร (หรือข้อมูลคอมพิวเตอร์) ได้ตามกฎหมาย แต่ผู้นั้นได้บิดเบือน “เนื้อหา” ในเอกสาร (หรือข้อมูล) นั้น ให้ผิดเพี้ยนไปจากความจริง กรณีนี้แม้เอกสารหรือข้อมูลที่ออกมาจะเรียกว่าเป็น “เอกสารหรือข้อมูลที่แท้จริง” (ไม่ใช่ของทำปลอม) แต่ผู้กระทำเช่นนี้ก็มีความผิดได้ เพราะตนได้ผลิตเอกสารหรือข้อมูลที่มีเนื้อหา “อันเป็นเท็จ” หรือที่เรียกว่าความผิดฐานทำเอกสารเท็จ (หรือนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่เป็นเท็จ) นั่นเอง โดยสรุปย่อมเห็นได้ว่า สิ่งที่กฎหมายในเรื่องนี้มุ่งประสงค์จะคุ้มครอง คือ “ความเชื่อถือได้ และความมั่นคงของเอกสาร (หรือข้อมูล)” ในการนำไปใช้เป็นพยานหลักฐานหรือใช้อ้างอิงในเรื่องต่าง ๆ มาตรา 14 (1) จึงหาได้มุ่งคุ้มครองชื่อเสียง เกียรติยศของบุคคล ซึ่งเป็นความผิดในเรื่องหมิ่นประมาทที่อยู่ในอีกหมวดความผิดหนึ่งไม่

จากเป้าหมายที่แท้จริงของ มาตรา 14 (1) ดังกล่าวมา จึงอาจกล่าวได้ว่า ด้วยปัญหาความไม่ชัดเจนของถ้อยคำในตัวบทบัญญัติเอง และรวมทั้งการไม่มีความรู้ความเข้าใจที่เพียงพอในเจตนารมณ์ เป้าหมาย

หรือความหมายของมาตรานี้ของพนักงานเจ้าหน้าที่ มาตรา 14 (1) จึงถูกเข้าใจผิด หรือถูกนำมาใช้ผิดหน้าที่มาโดยตลอด มักเกิดคำถามขึ้นอยู่เสมอว่า เหตุใดเมื่อเกิดการ “ใส่ความ” กันขึ้นในอินเทอร์เน็ต จึงต้องฟ้องร้องโดยอาศัย มาตรา 14 (1) พ.ร.บ.คอมพิวเตอร์ฯ 2550 ประกอบกับกฎหมายแพ่งฯ หรือกฎหมายอาญาด้วย จนก่อให้เกิดความสับสนแก่ผู้ถูกฟ้องร้อง รวมทั้งประชาชนทั่วไป การนำ มาตรา 14 (1) พ.ร.บ.คอมพิวเตอร์ฯ 2550 มาฟ้องร้องกันในเรื่องหมิ่นประมาท ยังมีผลทำให้ความผิดที่ว่าด้วยการหมิ่นประมาทต้องกลายเป็น “อาญาแผ่นดิน” ที่นอกจากคู่กรณีจะตกลงยอมความกันไม่ได้แล้ว ยังทำให้ใครๆ ก็ตามสามารถเป็นผู้กล่าวโทษกับเจ้าพนักงานให้ดำเนินคดีกับใครก็ได้ (ซึ่งต่างจาก “อาญาส่วนตัว”) ก่อให้เกิดผลประหลาด และไม่สอดคล้องกับบทบัญญัติหลักที่ว่าด้วยการหมิ่นประมาทตามกฎหมายอาญา นอกจากนี้ ยังอาจเกิดคำถามในแง่การใช้การตีความได้อีกว่า ผู้ถูกกล่าวหาว่ากระทำความผิดตามมาตรานี้สามารถพิสูจน์เหตุยกเว้นความผิด (มาตรา 329[18]) หรือเหตุยกเว้นโทษ (มาตรา 330) ตามที่บัญญัติไว้ในประมวลกฎหมายอาญาได้หรือไม่ กล่าวให้ถึงที่สุด การใช้การตีความมาตรา 14 (1) ให้กลายเป็นมาตราเพื่อจัดการกับความผิดฐานหมิ่นประมาทเช่นนี้ ได้ส่งผลให้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 กลายเป็นกฎหมายที่ทำให้การหมิ่นประมาทมีระดับความรุนแรงยิ่งกว่าที่กำหนดไว้ในประมวลกฎหมายอาญาเสียอีก ทั้งนี้ ทั้งในแง่ของอัตราโทษจำคุกและโทษปรับที่สูงขึ้น ผู้ถูกกล่าวหาอาจไม่สามารถพิสูจน์เหตุยกเว้นความผิดหรือยกเว้นโทษได้ และเป็นความผิดที่ไม่สามารถยอมความได้ ซึ่งไม่น่าจะสอดคล้องกับเจตนารมณ์ของกฎหมายในเรื่องนี้

อนึ่ง ความสับสนในการบังคับใช้บทบัญญัติข้อนี้ อาจเกิดมาจากปัญหาเรื่องการจัดวาง หรือตำแหน่งแห่งที่ของมาตรา 14 (1) ด้วย ทั้งนี้เพราะโดยหลักการแล้ว ความผิดที่ว่าด้วยการ “ปลอมแปลง” หรือ “ทำให้เป็นเท็จ” ดังอธิบายมาข้างต้น ไม่ใช่ความผิดประเภทเดียวกันกับความผิดที่ว่าด้วยการ “เผยแพร่” ข้อมูลที่มี “เนื้อหาผิดกฎหมาย” เนื่องจากการกระทำผิดเพราะทำข้อมูลปลอม หรือข้อมูลเท็จเป็นความผิดที่เกิดจาก

ตัว “การกระทำ” (ทำปลอม ทำแปลง ทำให้เป็นเท็จ) ซึ่งไม่เหมือนกับการเผยแพร่ข้อมูลที่เป็นความผิดเพราะ “เนื้อหานั้นผิดในตัวของมันเอง” (ภาพลามกอนาจาร ข้อความหมิ่นประมาทหรือใส่ความบุคคลอื่น ยั่วยุให้ล้มล้างรัฐบาล หรือทำการก่อการร้าย) ดังนั้น เมื่อเจตนารมณ์ของ (1) ไม่เหมือนกับวงเล็บอื่นๆ แต่ถูกนำมาบัญญัติรวมไว้ด้วยกัน ประกอบกับลักษณะการใช้คำใน (1) ที่ว่า “น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน” ซึ่งตีความได้กว้างมากไม่ได้จำเพาะว่าต้องกระทบหรือเสียหายในแง่ของ “ความเชื่อถือได้ และความมั่นคงของข้อมูล” เท่านั้น ทำให้ผู้บังคับใช้เกิดความสับสนและเข้าใจไปได้ว่าถ้าเสียหายต่อชื่อเสียง เกียรติยศ ก็เป็นความผิดตาม (1) ได้เหมือนกัน โดยไม่ทันได้คิดว่าถ้าตีความไปเช่นนั้น จะทำให้ (1) ไปซ้ำซ้อนกับความผิดฐานหมิ่นประมาท และก่อให้เกิดผลประหลาดทางกฎหมายต่างๆ ดังกล่าวแล้ว

คดีตามมาตรา 14 (1) คดีหนึ่งที่มีรายละเอียดน่าสนใจ คือ คดีแดงที่ อ.4465/2552 คดีดังกล่าว ผู้เสียหายฟ้องนายวันฉัตร ผดุงรัตน์ เจ้าของเว็บไซต์พันทิปซึ่งเป็นผู้ให้บริการชุมชนเว็บบอร์ดรายใหญ่ของประเทศเป็นจำเลย โดยโจทก์แจ้งว่ามีผู้เขียนข้อความกล่าวหาโจทก์ว่าโกงเงินขององค์กร โดยข้อความเหล่านั้นเป็นเอกสารภาพที่ปรากฏอยู่ในฟรีเว็บบอร์ดของ Pantown ซึ่งเป็นบริการหนึ่งของเว็บไซต์พันทิป มีวัตถุประสงค์ให้ผู้ใช้บริการสร้างพื้นที่ชุมชนเว็บบอร์ดของตนเองได้ โจทก์ฟ้องจำเลยในฐานะเจ้าของเว็บไซต์ว่ามีหน้าที่ควบคุมดูแล กำกับ ติดตาม ตรวจสอบเนื้อหาในเว็บไซต์ แต่ยินยอมให้มีการนำข้อความเท็จขึ้นเว็บไซต์ของตน ทั้งเพิกเฉยไม่นำข้อความที่ “ใส่ความ” (ซึ่งเป็นองค์ประกอบสำคัญของความผิดฐานหมิ่นประมาท - คณะผู้วิจัย) โจทก์ออกจากเว็บไซต์ คดีนี้ศาลชั้นต้นพิพากษายกฟ้อง เนื่องจากไม่เข้าองค์ประกอบความผิดตามมาตรา 14 (1) โดยมีพยานปากสำคัญ คือ ตัวแทนจากคณะกรรมการกฤษฎีกาที่ให้การเรื่องการตีความหมาย มาตรา 14 (1) ว่า คำว่า “ข้อมูลปลอมหรือเท็จ” นั้น หากเป็นการนำเอกสารที่มีอยู่แล้วมาลงเว็บไซต์โดยไม่ได้แก้ไข จะเรียกว่าเป็นข้อมูลเท็จไม่ได้ หากโจทก์เห็นว่าข้อความในเอกสารดังกล่าวเป็นข้อมูลเท็จ

ก็เป็นเรื่องที่โจทก์ต้องไปว่ากล่าวกับผู้ทำเอกสาร ซึ่งโจทก์ยังไม่สามารถพิสูจน์ว่าข้อความในเอกสารเป็นเท็จหรือไม่ และแน่นอนว่า ศาลกำหนดว่าภาระการพิสูจน์ความเท็จจริงนั้นเป็นของโจทก์ ไม่ใช่ของจำเลย

จากคดีความดังกล่าว จะเห็นได้ว่า ลักษณะของการตีความหมายมาตรา 14 (1) ของตัวแทนคณะกรรมการกฤษฎีกา ได้นำไปสู่ประเด็นในเรื่องที่เกี่ยวกับ “ภาระการพิสูจน์ของโจทก์” ที่ต้องพิสูจน์ “ความแท้จริง” ของข้อมูลที่เอามาเผยแพร่ ซึ่งเป็นประเด็นเช่นเดียวกันกับการพิสูจน์ “ความแท้จริง” ของเอกสาร ในความผิดฐานปลอมหรือแปลงเอกสาร หรือเอกสารเท็จ ตามประมวลกฎหมายอาญา หาใช่เรื่องที่เกี่ยวกับการ “ใส่ความ” ในความผิดฐานหมิ่นประมาทไม่ เพราะความเป็นการใส่ความจริง กฎหมายจะไม่สนใจเลยว่าเรื่องที่ใส่ความกันนั้นเป็นความจริงหรือเป็นความเท็จ ดังนั้น โดยปกติแล้ว โจทก์ในคดีหมิ่นประมาทจึงไม่มีภาระหน้าที่ที่จะต้องพิสูจน์ให้ศาลเห็นว่าข้อมูลหรือข้อความที่นำมาเผยแพร่นั้นเป็นความเท็จหรือความจริง เช่นนี้จึงย่อมเท่ากับว่า แม้แต่กรรมการกฤษฎีกาเอง ก็มิได้เห็นว่า มาตรา 14 (1) พ.ร.บ. คอมพิวเตอร์ เป็นมาตราที่จะนำมาใช้กับความผิดในฐานหมิ่นประมาทได้

2) มาตรา 14 (2): กล่าวได้ว่า มาตรา 14 (2) เป็นมาตราหนึ่งในกฎหมายฉบับนี้ที่มีปัญหาในเรื่องขอบเขตการบังคับใช้มากที่สุด และถูกวิพากษ์วิจารณ์ว่าถูกฝ่ายรัฐใช้เป็นเครื่องมือในการลิดรอนเสรีภาพของประชาชนในการแสดงความคิดเห็น คณะผู้วิจัยเห็นว่า ด้วยถ้อยคำต่างๆ ที่อยู่ในอนุมาตรานี้ ไม่ว่าจะเป็น “เกิดความเสียหายต่อความมั่นคง” ก็ดี หรือ “ก่อให้เกิดความตื่นตระหนกแก่ประชาชน” ก็ดี ในทางกฎหมายแล้วมีลักษณะที่ขัดหรือแย้งต่อ “หลักประกันทางกฎหมายอาญา”[19] (ไม่มีความผิดไม่มีโทษ โดยไม่มีกฎหมาย) ในส่วนที่ว่า “กฎหมายอาญาต้องบัญญัติให้ชัดเจนแน่นอน” (nullum crimen sine lege certa)[20] เนื่องจากถ้อยคำดังกล่าว ประชาชนทั่วไปอ่านแล้วไม่สามารถเข้าใจได้ทันทีว่า ข้อมูลที่มีเนื้อหาเช่นใดจึงจะถือว่าก่อความเสียหายต่อความมั่นคงแล้ว หรือแค่ไหนเพียงใดจึงเข้าข่ายเป็นการสร้างความตื่นตระหนกแก่ประชาชน มาตรา 14

(2) เป็นบทบัญญัติที่เปิดช่องให้เจ้าพนักงานใช้ดุลพินิจได้อย่างเต็มที่ในการพิจารณาว่าเนื้อหาหนึ่งๆ เป็นความผิดหรือไม่ ซึ่งย่อมสุ่มเสี่ยงต่อการตีความที่เกินเลยไป เพราะมีความหมายไม่แน่นอน ทั้งอาจแปรเปลี่ยนได้ตามยุคสมัยและทัศนคติของผู้มีอำนาจปกครอง ในขณะที่ความผิดฐานนี้มีโทษจำคุกสูงถึงห้าปี ประเด็นในเรื่องการบัญญัติที่ขัดต่อหลักประกันทางกฎหมายอาญานี้ สะท้อนให้เห็นได้อย่างชัดเจนว่า ปัญหาของพระราชบัญญัติฉบับนี้ไม่ได้อยู่ที่มุมมองหรือทัศนคติของผู้บังคับใช้กฎหมายแต่เพียงอย่างเดียวเท่านั้น หากแต่เป็นการบัญญัติกฎหมายที่อิงแอบอยู่กับเรื่องทางการเมืองและเปิดช่องว่างของกฎหมายเสียเองด้วยการเลือกใช้ถ้อยคำที่ไม่อาจกำหนดนิยามที่ชัดเจนได้

อนึ่ง เรื่องที่ควรตั้งเป็นข้อสังเกต ก็คือ มาตรา 14 (3) พ.ร.บ. คอมพิวเตอร์ฯ 2550 ก็เป็นบทคุ้มครองความมั่นคงเช่นเดียวกัน เพราะกำหนดโทษไว้สำหรับการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลใดๆ ที่เป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา[21] แต่มาตรา 14 (3) แตกต่างจากมาตรา 14 (2) อย่างมีนัยยะสำคัญ เพราะความผิดตาม (3) มีความชัดเจนในเรื่อง “องค์ประกอบความผิด” มากกว่า เนื่องจากเชื่อมโยงไปยังฐานความผิดในประมวลกฎหมายอาญา ทั้งกฎหมายอาญายังไม่สนใจด้วยว่าเนื้อหาที่เข้าข่ายเป็นความผิดเหล่านั้นจะเป็นความเท็จหรือว่าความจริง หากครบองค์ประกอบผู้กระทำย่อมมีความผิด จึงย่อมครอบคลุมการกระทำความผิดที่ “ขัดต่อความมั่นคง” ได้มากกว่ามาตรา 14 (2) ซึ่งหมายเฉพาะการนำเข้าสู่ข้อมูลอันเป็นเท็จ ดังนั้น จึงย่อมเกิดคำถามได้ว่า ด้วยเหตุผลใด พ.ร.บ. คอมพิวเตอร์ฯ 2550 จึงต้องบัญญัติ มาตรา 14 (2) ที่ใช้ถ้อยคำคลุมเครือเพื่อคุ้มครองความมั่นคงไว้อีกวงเล็บหนึ่ง จนในท้ายที่สุดมาตรานี้อาจถูกใช้เป็นเครื่องมือเล่นงานกันทางการเมืองได้

3) มาตรา 14 (3): แม้มาตรา 14 (3) เป็นบทบัญญัติที่มีความชัดเจนกว่ามาตรา 14 (2) ดังกล่าวไปแล้ว เนื่องจากมีการเชื่อมโยงกลับไปยังประมวลกฎหมายอาญา ซึ่งกำหนดฐานความผิดที่ระบุองค์ประกอบ

ความผิดไว้แน่ชัดกว่าการใช้ถ้อยคำลอยๆ ประเภท “ขัดต่อความมั่นคง” หรือ “ทำให้ประชาชนตื่นตระหนก” หากแต่ความแตกต่างนี้ก็หาได้หมายความว่าด้วยการใช้มาตรา 14 (3) ประกอบกับความผิดตามมาตราต่างๆ ที่บัญญัติไว้ในหมวดความมั่นคง และความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญานั้น จะนำความชัดเจนมาสู่ประชาชน หรือทำให้ประชาชนคาดหมายได้ว่าสิ่งที่ตนกระทำ หรือแสดงความคิดเห็นไปไม่ว่าจะในสื่อทั่วไปหรือสื่อออนไลน์นั้น จะเป็นความผิดต่อกฎหมายหรือไม่ เพราะปรากฏว่าบางมาตราในประมวลกฎหมายอาญาหมวดความมั่นคงแห่งรัฐเอง ก็ก่อให้เกิดปัญหาต่อเสรีภาพในการแสดงความคิดเห็นของประชาชนได้เช่นกัน

หากพิจารณาจากสถิติการดำเนินคดีในรายงานวิจัยฉบับนี้ จะพบว่ากรณีที่ถูกอ้างว่าเป็นความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 โดยอาศัยมาตรา 14 (3) รวมทั้ง 14 (2) ด้วย ส่วนใหญ่เป็นการใช้บังคับร่วมกับประมวลกฎหมายอาญา มาตรา 112 หรือความผิดฐานหมิ่นประมาท ดูหมิ่น หรืออาฆาตมาดร้ายพระมหากษัตริย์ พระราชินี รัชทายาท หรือผู้สำเร็จราชการแทนพระองค์ฯ[22] (จำนวน 40 คดี) ซึ่งในช่วงสองปีที่ผ่านมา มาตรา 112 ดังกล่าว ก็ถูกวิพากษ์วิจารณ์มาโดยตลอดว่ามีปัญหาขัดต่อระบอบการปกครองในระบอบประชาธิปไตย ทั้งนี้ ทั้งปัญหาในส่วนเนื้อหาของบทบัญญัติเอง ปัญหาการบังคับใช้ไปจนถึงปัญหาในเรื่องของอุดมการณ์ในการตีความ โดยอาจพอสรุปสาระสำคัญแห่งปัญหาได้ 4 ประเด็นใหญ่ๆ คือ

• เนื่องจาก มาตรา 112 นั้น มีลักษณะเป็น “อัตวิสัย” อยู่มาก กล่าวคือ ตามปกติแล้วบุคคลผู้จะพิจารณาว่าถ้อยคำหรือการกระทำใดการกระทำหนึ่งที่กระทำต่อตนมีความร้ายแรง หรือถึงเป็นการหมิ่นประมาทหรือดูหมิ่นตนเองหรือไม่ ก็ควรเป็นบุคคลคนนั้นเอง ไม่ควรเป็นบุคคลอื่นใดที่ไม่ได้ถูกหมิ่นประมาท หรือดูหมิ่น (ไม่ต่างจากลักษณะของมาตรา 326 หมิ่นประมาทบุคคลธรรมดา[23]) ดังนั้น ผู้มีอำนาจในการฟ้องร้อง หรือร้องทุกข์เพื่อมอบอำนาจให้เจ้าหน้าที่รัฐดำเนินคดีกับผู้กระทำความผิด ก็ควรหมายเฉพาะบุคคลผู้ถูกหมิ่นประมาทหรือดูหมิ่นนั้นเท่านั้น ซึ่งในทางกฎหมายเรียกว่า “อาญาส่วนตัว” แต่กลับปรากฏว่า มาตรา 112 มีสถานะ

เป็น “อาญาแผ่นดิน” ยังผลให้บุคคลใดๆ ก็ได้ กล่าวโทษหรือแจ้งความกับเจ้าหน้าที่รัฐเพื่อให้ดำเนินคดีกับบุคคลอื่น ด้วยลักษณะเช่นนี้เอง จึงเปิดโอกาสให้เกิดการกลั่นแกล้งฟ้องกัน

• มาตรา 112 กำหนดอัตราโทษไว้สูงเกินไป คือ จำคุกตั้งแต่ 3 ถึง 15 ปี ซึ่งน่าจะขัดกับหลักความได้สัดส่วน กล่าวคือ ความเสียหายที่ผู้ถูกกระทำได้รับกับโทษที่ผู้กระทำต้องรับนั้นไม่ได้สัดส่วนกัน

• มาตรา 112 ไม่มีบทกำหนดเหตุยกเว้นความผิด (การกระทำแม้ครบองค์ประกอบความผิด แต่ผู้กระทำไม่มีความผิด) เพื่อเปิดโอกาสให้ผู้ถูกกล่าวหาว่ากระทำความผิดแก้ต่างได้ว่าตนกล่าวถ้อยคำหรือกระทำการใดๆ ไป “โดยสุจริต” หรือเป็นเพียงการ “วิพากษ์วิจารณ์” ที่อยู่ในกรอบของระบอบประชาธิปไตย (แตกต่างจากการหมิ่นประมาทบุคคลธรรมดามาตรา 326 ที่มีมาตรา 329[24] เป็นเหตุยกเว้นความผิดได้) และ

• มาตรา 112 ไม่มีเหตุยกเว้นโทษ (การกระทำครบองค์ประกอบความผิด เป็นความผิดกฎหมาย แต่ผู้กระทำไม่ต้องรับโทษ) จึงปิดโอกาสไม่ให้ผู้กระทำความผิดได้พิสูจน์ “ความจริง” ของถ้อยคำที่ตนกล่าว ดังนั้น แม้ถ้อยคำนั้นจะเป็นความจริง ทั้งเป็นประโยชน์กับประชาชน และไม่ได้เป็นเรื่องส่วนตัวของผู้ถูกหมิ่นประมาท ผู้กล่าวถ้อยคำก็ยังต้องมีความผิด และรับโทษอยู่ดี (แตกต่างจากการหมิ่นประมาทบุคคลธรรมดามาตรา 326 ที่มีมาตรา 330[25] เป็นเหตุยกเว้นโทษได้)[26]

จะเห็นได้ว่า ด้วยลักษณะต่างๆ ดังกล่าวมาของมาตรา 112 ประมวลกฎหมายอาญา รวมทั้งการบังคับใช้ ส่งผลโดยตรงต่อเสรีภาพในการแสดงความคิดเห็นของบุคคล “โดยสุจริต” และปิดกั้นไม่ให้สังคมไทยได้รับรู้ “ความจริง” ซึ่งอาจเกิดขึ้นผ่านการวิพากษ์วิจารณ์สถาบัน หรือองค์กรที่เป็นส่วนหนึ่งของระบอบประชาธิปไตย และอยู่ภายใต้รัฐธรรมนูญ

โดยสรุป หากจะกล่าวถึงปัญหาของบทบัญญัติ รวมทั้งการบังคับใช้ พ.ร.บ. คอมพิวเตอร์ฯ 2550 ที่ส่งผลกระทบต่อเสรีภาพของประชาชนในสื่อออนไลน์ให้ครบถ้วนแล้ว หลายกรณีเรามิอาจหลีกเลี่ยงการกล่าวถึงปัญหาของบทบัญญัติแห่งกฎหมายฉบับอื่นที่นำมาใช้ประกอบหรือใช้ร่วม

กับ พ.ร.บ. คอมพิวเตอร์ฯ 2550 ได้ อย่างไรก็ดี ข้อค้นพบในส่วนนี้ ไม่ควรเป็นบทสรุปว่า “การดำรงอยู่ หรือการมีกฎหมายสารบัญญัติอย่างที่เป็นอยู่ในปัจจุบันของ พ.ร.บ. คอมพิวเตอร์ฯ 2550 (โดยเฉพาะอย่างยิ่งมาตรา 14) ไม่ได้ส่งผลกระทบโดยตรงต่อเสรีภาพในการแสดงความคิดเห็นในสื่อออนไลน์ จึงไม่จำเป็นต้องปรับปรุงแก้ไข” เพราะหลายครั้ง ที่การละเมิดเสรีภาพของประชาชนมีแนวโน้มกว้างขวางและรุนแรงขึ้น ก็เพราะมีกฎหมายหลายฉบับช่วยเสริมช่องทางการใช้อำนาจ หรือใช้ดุลพินิจให้กับฝ่ายรัฐมากเกินไป

4) มาตรา 15 *“ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตาม มาตรา 14”*

มาตรา 15 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ถูกวิพากษ์วิจารณ์มาโดยตลอดเช่นกันนับตั้งแต่กฎหมายมีผลบังคับใช้ ในเรื่องความไม่ชัดเจน และความไม่สมเหตุสมผลของการกำหนดความรับผิดแก่ผู้ให้บริการ ซึ่งเป็นเพียง “ตัวกลาง” ในการเผยแพร่ข้อมูลในระบบคอมพิวเตอร์ โดยมีประเด็นที่ควรพิจารณา ดังนี้

ประเด็นแรก มาตรา 15 กำหนดโทษแก่ผู้ให้บริการไว้เท่ากับผู้กระทำความผิด หรือตัวการ (ในที่นี้ย่อมหมายถึง ผู้ผลิต หรือโพสต์เผยแพร่ข้อความที่อาจเป็นความผิดตามมาตรา 14) ทั้งๆ ที่ผู้ให้บริการไม่ใช่ผู้นำข้อมูลที่มีเนื้อหาเป็นความผิดเข้าสู่ระบบคอมพิวเตอร์ด้วยตนเอง อย่างไรก็ตาม หากพิจารณาลักษณะของการให้บริการจะพบว่า ในบางกรณีหากอาศัยหลักทั่วไปในกฎหมายอาญามาอธิบายความผิดแล้ว การกระทำของผู้ให้บริการอาจเข้าข่ายเพียง “ผู้สนับสนุน[27]” ซึ่งมีโทษน้อยกว่าตัวการ เท่านั้น เช่น ผู้ให้บริการที่เกี่ยวข้องเห็นข้อความที่มีเนื้อหาหมิ่นประมาทบุคคลอื่นอย่างชัดเจนแล้ว แต่ยังนิ่งเฉยไม่ดำเนินการใดๆ หรือปล่อยให้มีการเผยแพร่อยู่ต่อไป การกำหนดโทษสถานหนักแก่ผู้ให้บริการเช่นนี้ นอกจากจะส่งผลกระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชน (ผู้ใช้บริการ)

โดยอ้อมแล้ว เพราะทำให้ผู้ให้บริการต้องคอยเซ็นเซอร์เนื้อหาข้อมูลที่อยู่ในพื้นที่ให้บริการของตนก่อนที่ตนเองจะถูกดำเนินคดี (self censorship) ยังกระทบต่อแรงจูงใจในการประกอบกิจการให้บริการอินเทอร์เน็ต ซึ่งย่อมกระทบต่อพัฒนาการทางเทคโนโลยีสารสนเทศโดยรวมอีกด้วย นอกจากนี้ ในทางปฏิบัติที่เกี่ยวกับการดำเนินคดีเกี่ยวกับคอมพิวเตอร์ในช่วงเวลากว่า 4 ปี ของการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ที่ผ่านมา ยังมีเหตุผลอันควรเชื่อด้วยว่า เมื่อเกิดการกระทำความผิดในระบบคอมพิวเตอร์ขึ้น เจ้าพนักงานที่เกี่ยวข้องมักมุ่งเน้นดำเนินคดีกับผู้ให้บริการก่อน เนื่องจากสืบหาตัวได้ง่ายกว่า จนละเลยหรือไม่พยายามแสวงหาตัวผู้กระทำความผิด (ที่นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลนั้น) มาลงโทษ ซึ่งไม่น่าจะถูกต้องตามเจตนารมณ์ของกฎหมาย

ประเด็นที่สอง ประเทศไทยยังไม่มีหลักเกณฑ์ที่ชัดเจนเกี่ยวกับ “มาตรการในการควบคุมเนื้อหาด้วยตนเอง” เพื่อการกำกับเนื้อหาบนอินเทอร์เน็ต ซึ่งเป็นมาตรการที่ผู้ดูแลรักษาข้อมูลยอมรับที่จะลบข้อมูลในส่วนที่มีการบอกแจ้งให้ทราบออกจากพื้นที่การให้บริการของตน โดยไม่ต้องตรวจสอบความผิดกฎหมายโดยศาลก่อน (notice and takedown) ทำให้ในปัจจุบัน ทั้งฝ่ายพนักงานเจ้าหน้าที่ของรัฐเอง และฝ่ายผู้ให้บริการไม่มีแนวทางในการปฏิบัติที่ชัดเจนเกี่ยวกับเรื่องนี้ โดยเฉพาะอย่างยิ่งในปัญหาที่ว่า

- ใครบ้างที่ควรเป็นผู้มีอำนาจในการบอกแจ้งเนื้อหาที่อาจเป็นความผิด แก่ผู้ให้บริการ
- วิธีการในการบอกแจ้ง
- รายละเอียดที่จำเป็นต้องมีในการบอกแจ้ง อาทิ ข้อความที่เข้าข่ายเป็นความผิด มาตราที่ยืนยันเบื้องต้นว่าข้อความนั้นเข้าข่ายเป็นความผิด แหล่งที่อยู่ออนไลน์ หรือยูอาร์แอลของข้อความนั้น เป็นต้น
- ระยะเวลาที่กำหนดให้ผู้ให้บริการดำเนินการกับเนื้อหาที่เข้าข่ายเป็นความผิด ภายหลังได้รับแจ้ง รวมทั้ง
- ลักษณะของการดำเนินการกับเนื้อหาที่ได้รับแจ้งนั้น ควรเป็น

อย่างไร กล่าวคือ ลบทั้งหมด หรือว่าลบเพียงบางส่วน

ในขณะที่ในหลายประเทศมีระเบียบหลักการเหล่านี้ใช้บังคับแล้ว อาทิเช่น ประเทศสหรัฐอเมริกา อังกฤษ ญี่ปุ่น หรือมาเลเซีย ทั้งที่อยู่ในรูปของกฎหมายอย่าง “Act on the Limitation of Liability for Damaged of Specified Telecommunications Service Providers 2001” ของประเทศญี่ปุ่น หรือในรูปแบบของ Code of Conduct ในสหรัฐอเมริกา หรืออังกฤษ เป็นต้น การไม่มีหลักเกณฑ์หรือแนวทางปฏิบัติการให้เป็นไปตามกฎหมายที่ชัดเจนในส่วนนี้ อาจเป็นผลให้ผู้ให้บริการบางรายถูกเจ้าหน้าที่รัฐฟ้องคดีได้ แม้ว่าผู้ให้บริการนั้นได้ใช้ความพยายามอย่างที่สุดแล้วเพื่อดำเนินการกับข้อมูลที่ได้รับแจ้ง เพียงแต่ไม่รวดเร็วอย่างที่เจ้าพนักงานต้องการเท่านั้น

ประเด็นที่สาม มีเหตุผลอันควรเชื่อว่า มีผู้พยายามตีความเจตนารมณ์ของมาตรา 15 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ว่าผู้ร่างกฎหมายต้องการกำหนดหน้าที่ในการตรวจสอบเนื้อหาในอินเทอร์เน็ตเป็นการทั่วไปให้แก่ผู้ให้บริการ กล่าวคือ แม้ไม่มีการบอกแจ้งใดๆ จากเจ้าหน้าที่รัฐหรือผู้เสียหายเลยก็ตาม ผู้ให้บริการก็ต้องมีหน้าที่ตรวจตราและดำเนินการกับเนื้อหาในพื้นที่ให้บริการของตนเอง และหากเมื่อใดพบว่ามีการกระทำความผิดเกิดขึ้น ผู้ให้บริการต้องมีความรับผิดด้วยถ้าไม่ดำเนินการกับข้อมูลนั้นตั้งแต่พบเห็น คณะผู้วิจัยเห็นว่า การตีความเช่นนี้ไม่น่าจะถูกต้อง ทั้งไม่สอดคล้องกับธรรมชาติและลักษณะของการเผยแพร่ข้อมูลบนเครือข่ายอินเทอร์เน็ต ที่มีข้อมูลจำนวนมหาศาลส่งผ่านไปมาระหว่างกันอย่างรวดเร็ว จึงย่อมไม่ใช่เรื่องง่ายในการที่จะติดตามตรวจสอบ หรือสืบทราบได้ว่าเนื้อหาที่ส่งเข้ามาในแต่ละนาทีนั้นเป็นเนื้อหาที่อาจเข้าข่ายผิดกฎหมายหรือไม่ อย่างไรก็ตาม จากการศึกษา คณะผู้วิจัยพบรายงานการประชุมคณะกรรมาธิการวิสามัญ (เพื่อพิจารณาร่าง พ.ร.บ.คอมพิวเตอร์ฯ) ครั้งที่ 9/2550 ลงวันที่ 10 กุมภาพันธ์ พ.ศ. 2550 ที่มีเนื้อหาแสดงถึงการอภิปรายของคณะกรรมาธิการฯ เป็นเชิงยอมรับว่า มาตรา 15 ไม่ควรเป็นมาตราที่กำหนดหน้าที่ในการตรวจสอบเนื้อหาโดยทั่วไปแก่ผู้ให้บริการหรือตัวกลาง เพราะจะเป็นการเพิ่มภาระแก่ผู้ให้บริการเกินสมควร

5) มาตรา 20 *"ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่ง ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่ กำหนดไว้ในภาคสองลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้อง พร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้ ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้"*

มาตรา 20 ซึ่งได้รับการบัญญัติเพิ่มเข้ามาในร่างกฎหมายฉบับสุดท้ายโดยคณะกรรมาธิการวิสามัญของสภานิติบัญญัติแห่งชาติ ก่อนที่จะมีผลบังคับใช้เป็นกฎหมายในปี 2550 เป็นบทบัญญัติที่มีปัญหาในการบังคับใช้ และถูกวิพากษ์วิจารณ์มากที่สุดอีกบทหนึ่ง เนื่องจากเป็นมาตรการเร่งด่วนที่รัฐสามารถสั่งระงับการเผยแพร่ข้อมูลของประชาชนได้ทันทีโดยยังไม่ต้องมีคำพิพากษาของศาลว่าข้อมูลเหล่านั้นมีเนื้อหาเป็นความผิดตามกฎหมายจริงหรือไม่

ก่อนหน้าที่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 จะมีผลบังคับใช้ ผู้วิจัย (สาวตรี สุขศรี)แสดงความคิดเห็นต่อเรื่องนี้ไว้ว่า ในที่สุดแล้ว ประเทศไทยอาจจำเป็นต้องมีมาตรการ "เร่งด่วน" ในทำนองนี้ หรือที่เรียกว่าการ "เซ็นเซอร์ในภายหลัง (การเผยแพร่)" กับเนื้อหาบางประเภทที่ผิดกฎหมายอย่างชัดเจนเช่นกัน ทั้งนี้เพื่อเป็นเครื่องมือในการปราบปรามการกระทำความผิด รวมทั้งระงับยับยั้งความเสียหายที่จะเกิดขึ้นต่อไปในวงกว้าง เพราะแม้แต่กฎหมายของประเทศประชาธิปไตยหลายๆ ประเทศ ก็กำหนดมาตรการดังกล่าวไว้สำหรับเนื้อหาบางประเภทที่รัฐไม่อาจยอมให้เผยแพร่ต่อสาธารณะได้ เช่น เนื้อหาหรือภาพลามกอนาจารเด็ก ภาพการใช้ความรุนแรงหรือการทำทารุณกรรมอันผิดลักษณะมนุษย์ หรือภาพหรือเนื้อหาในเชิงดูถูกเหยียดหยามเผ่าพันธุ์อื่น เป็นต้น อย่างไรก็ตาม มาตรการ

ดังกล่าวจะต้องบัญญัติเงื่อนไขและหลักเกณฑ์การใช้ให้ชัดเจน ทั้งต้องวางอยู่บนหลักพื้นฐานว่าด้วยการคุ้มครองเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นของประชาชน ข้อบัญญัติจึงควรมีลักษณะเป็น “ข้อยกเว้น” อย่างยิ่ง หรือมีเหตุผลที่มิอาจก้าวล่วงได้จริงๆ รัฐจึงจะใช้อำนาจปิดกั้นเนื้อหาได้ ซึ่งต้องมีกฎหมายเป็นลายลักษณ์อักษรบัญญัติโดยแจ้งชัดด้วยว่าเนื้อหาในลักษณะใดบ้างที่อาจถูกปิดกั้น

อย่างไรก็ตาม ปรากฏว่ามาตรา 20 พ.ร.บ. คอมพิวเตอร์ฯ 2550 เป็นไปในทิศทางตรงกันข้าม กล่าวคือ ใช้ถ้อยคำคลุมเครือไม่ชัดเจนว่าเนื้อหาประเภทใดที่อาจถูกปิดกั้นได้ กฎหมายเขียนให้อำนาจรัฐเพื่อปิดกั้นเป็น “หลัก” ไม่ใช่ “ข้อยกเว้น” ที่ต้องตีความโดยเคร่งครัดรัดกุม ทั้งให้หน่วยงานรัฐใช้ดุลพินิจพิจารณากันเอง แม้มาตรา 20 กำหนดเงื่อนไขให้ต้องผ่านการกลั่นกรองการใช้ดุลพินิจของพนักงานเจ้าหน้าที่จากศาลก่อนก็ตาม แต่ที่ผ่านมาก็ยังมีประเด็นปัญหา และข้อถกเถียงเกี่ยวกับข้อจำกัดของศาลในการทำภารกิจนี้ในประการต่างๆ เช่น ศาลมีภาระงานหลักในการพิจารณาอรรถคดีและออกหมายอื่นๆ ซึ่งมีจำนวนมากอยู่แล้ว จึงอาจทำให้ไม่สามารถให้เวลากับการพิจารณาเนื้อหาในเว็บไซต์ (ซึ่งต้องทำโดยรวดเร็ว) ได้อย่างรอบคอบเพียงพอ โดยเฉพาะอย่างยิ่งเมื่อข้อมูลที่ถูกส่งไปยังศาลเพื่อขอคำสั่งมีปริมาณมาก[28] รวมทั้งมุมมองและทัศนคติของศาลเองที่มีต่อสิทธิเสรีภาพในการเผยแพร่เนื้อหาในระบบคอมพิวเตอร์ จากการเก็บรวบรวมข้อมูลสถิติซึ่งเป็นผลการวิจัยในภาคที่ 1 คณะผู้วิจัยพบว่าช่วงเวลากว่าสี่ปีของการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ปรากฏคำสั่งศาลตามมาตรานี้กว่าร้อยฉบับที่อนุญาตให้พนักงานเจ้าหน้าที่ระงับการเผยแพร่หน้าเว็บเพจจำนวนกว่า 80,000 ยูอาร์แอล[29] ทั้งยังพบข้อเท็จจริงด้วยว่า คำสั่งศาลดังกล่าวได้รับการพิจารณาและดำเนินการโดยรวดเร็ว จนหลายๆ กรณีถูกตั้งคำถามว่า หากพิจารณาประกอบกับระยะเวลาที่ศาลใช้ การตรวจพิจารณาเนื้อหาดังกล่าวมีความละเอียดครบถ้วนจริงหรือไม่ ซึ่งเหตุต่างๆ เหล่านี้เองย่อมก่อให้เกิดความไม่มั่นคงในหมู่ประชาชน

ปัญหาอีกประการหนึ่งที่อาจยังไม่ค่อยถูกเรียกร้องเพื่อทำให้เกิด

ความชัดเจนก็คือ แท้ที่จริงแล้วคำว่า “ระงับการเผยแพร่” ตามมาตรานี้มีความหมายและขอบเขตอย่างไร ศาลสามารถสั่งระงับการเผยแพร่ได้ทั้งเว็บไซต์ หรือควรต้องระงับเฉพาะส่วนที่มีข้อมูลที่อาจเข้าข่ายเป็นความผิดปรากฏอยู่เท่านั้น เพราะที่ผ่านมามักมีกรณีที่พบว่า แม้จะสามารถระบุหรือเจาะจงได้ว่า “เนื้อหา” ส่วนใดบ้างในเว็บไซต์ที่อาจเข้าข่ายเป็นความผิด แต่เว็บไซต์นั้นกลับถูกระงับการเผยแพร่ทั้งหมด ทั้งที่พื้นที่ส่วนใหญ่ถูกใช้เพื่อการเผยแพร่ข่าวสารทั่วไปที่ไม่เป็นความผิด เช่น กรณีของการปิดกั้นเว็บข่าวประชาไท เป็นต้น ซึ่งเหล่านี้ย่อมมีลักษณะขัดต่อสิทธิและเสรีภาพในการรับรู้ข้อมูลข่าวสารของประชาชน และเป็นการกระทำที่เกินกว่าเหตุ หรือเกินกว่ากรณีที่จำต้องกระทำเพื่อระงับยับยั้งความเสียหายตามเจตนารมณ์ของกฎหมาย

3.3 ปัญหาในภาพรวมของความผิดที่ว่าด้วยการเผยแพร่เนื้อหาบนสื่อออนไลน์

กล่าวได้ว่า สำหรับ พ.ร.บ.คอมพิวเตอร์ฯ 2550 แล้ว บทบัญญัติในส่วนที่มีปัญหาในแง่ของการใช้การตีความมากที่สุด แต่กลับถูกหยิบยกขึ้นบังคับใช้มากที่สุด ก็คือ บทที่ว่าด้วยความผิดเกี่ยวกับการเผยแพร่เนื้อหา ทั้งที่เป้าหมายแรกของพระราชบัญญัติฉบับนี้ต้องการขจัดช่องว่างของกฎหมาย เนื่องจากกฎหมายที่มีอยู่เดิมไม่สามารถตีความให้ครอบคลุมการกระทำความผิดรูปแบบใหม่ซึ่งมีองค์ประกอบความผิดแตกต่างจากความผิดพื้นฐานอื่นๆ เช่น ความผิดฐานลักทรัพย์หรือทำให้เสียทรัพย์ไม่สามารถนำมาใช้ได้ถนัดนักกับการโจรกรรมข้อมูล การดักรับข้อมูล และการทำให้ข้อมูลหรือระบบคอมพิวเตอร์เสียหาย ทำนองเดียวกันกับที่ไม่สามารถนำความผิดฐานบุกรุก มาใช้กับการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นได้ เป็นต้น ซึ่งความผิดดังกล่าวล้วนมีประเด็นทางเทคโนโลยีใหม่ๆ ที่กฎหมายเก่าไปไม่ถึง ในขณะที่ความผิดเกี่ยวกับการเผยแพร่เนื้อหานั้น สามารถนำกฎหมายฉบับต่างๆ ที่มีอยู่เดิมมาปรับใช้ได้อยู่แล้ว โดยเฉพาะอย่างยิ่งประมวลกฎหมาย

อาญา เพราะเป็นการกระทำที่ไม่ได้มีลักษณะหรือองค์ประกอบความผิดใหม่ มีก็แต่เพียง “พื้นที่” ที่ใช้กระทำผิดเท่านั้นที่อาจเปลี่ยนแปลงไป การเผยแพร่ภาพลามกอนาจารแม้ทำในเครือข่ายคอมพิวเตอร์ ก็ยังคงใช้มาตรา 287[30] ประมวลกฎหมายอาญาได้ ทำนองเดียวกับการหมิ่นประมาทที่ปรับได้กับมาตรา 326 และ 328 กระทั่งเนื้อหาขัดต่อความมั่นคงก็ใช้มาตรา 112 หรือ 116 ได้ ซึ่งความผิดในส่วนนี้กฎหมายของหลายประเทศ[31] ก็หาได้นำมาบัญญัติรวมไว้ในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ไม่ อย่างมากก็ใช้วิธีแก้ไขเพิ่มเติมให้ชัดเจนขึ้นในหมวดความผิดที่เกี่ยวข้องกันของประมวลกฎหมายอาญาหรือกฎหมายอื่นๆ ปัจจุบันหลายฝ่าย ไม่ว่าจะเป็น ฝ่ายผู้บังคับใช้กฎหมายเอง ผู้ประกอบการอินเทอร์เน็ต รวมทั้งผู้ใช้บริการจำนวนหนึ่ง จึงเห็นว่าเพื่อไม่ให้เกิดปัญหาความซ้ำซ้อนของกฎหมาย ทั้งไม่มีปัญหาเรื่องการตีความ พ.ร.บ. คอมพิวเตอร์ ควรเป็นกฎหมายที่กำหนดความผิดและโทษสำหรับการกระทำทางเทคนิคโดยแท้ อย่างการเข้าถึงระบบโดยมิชอบ การรบกวนข้อมูล การโจรกรรมข้อมูล การฉ้อโกงคอมพิวเตอร์ หรือการก่อวินาศกรรมคอมพิวเตอร์ เท่านั้น

3.4 บทสรุป

ปฏิเสธไม่ได้ว่า ในยุคปัจจุบันคอมพิวเตอร์และอินเทอร์เน็ตเป็น “สื่อใหม่” ที่มีอิทธิพลต่อแนวคิดของประชาชนจำนวนไม่น้อย และเป็นพื้นที่ที่เปิดโอกาสให้มีการแลกเปลี่ยนและแสดงออกทางความคิดได้อย่างเสรี ด้วยศักยภาพดังกล่าวประกอบกับความสะดวกรวดเร็ว และข้อมูลจำนวนมหาศาลที่ไหลเวียน จึงมักปรากฏข้อเท็จจริงว่าฝ่าย “รัฐ” หรือผู้กุมอำนาจทางการเมืองการปกครองหรือทางธุรกิจในหลายประเทศมองอินเทอร์เน็ตอย่างที่เป็นได้ทั้งมิตรและศัตรู อินเทอร์เน็ตย่อมมีประโยชน์อย่างยิ่งหากรัฐสามารถใช้เป็นเครื่องมือในการสื่อสารกับประชาชนได้อย่างมีประสิทธิภาพ แต่ในขณะเดียวกัน หากรัฐไม่สามารถตรวจสอบหรือกำกับควบคุมให้การติดต่อสื่อสารทางอินเทอร์เน็ต รวมทั้งการเผยแพร่ข้อมูลข่าวสารต่างๆ

อยู่ภายในขอบเขตของสิ่งที่รัฐประสงค์ให้ประชาชนรู้ อินเทอร์เน็ตก็อาจกลายเป็นสื่อที่เป็นภัยในสายตาของรัฐ และนับแต่เดือนกรกฎาคม ปี 2550 เป็นต้นมา พ.ร.บ.คอมพิวเตอร์ฯ 2550 ก็กลายเป็นกฎหมายฉบับหนึ่งที่เข้ามามีบทบาทอย่างสำคัญในการ "จัดระเบียบ" การสื่อสารในอินเทอร์เน็ต

จากผลการศึกษาวิจัยภาค 1 ในส่วนของการเก็บรวมรวมสถิติต่างๆ อันเป็นผลพวงมาจาก พ.ร.บ.คอมพิวเตอร์ฯ 2550 จะพบว่าสถิติจำนวนเว็บไซต์ที่ถูกปิดกั้นกว่า 80,000 ยูอาร์แอล มีสัดส่วนแตกต่างกันอย่างมหาศาลกับสถิติคดีความที่อยู่ในกระบวนการยุติธรรม (ชั้นตำรวจ อัยการ และศาล) ซึ่งมีอยู่เพียงหลักร้อย เรื่องนี้นอกจากอาจถูกตั้งคำถามถึงข้อจำกัดต่างๆ ความรวดเร็ว กระทั่งความสามารถของเจ้าหน้าที่รัฐในการทำคดีแล้ว ยังสะท้อนให้เห็นด้วยว่าหน่วยงานรัฐที่เกี่ยวข้องเลือกที่จะใช้ "มาตรการเร่งด่วน" มากกว่าพยายามเสาะแสวงหาตัวการผู้กระทำและต้นตอของความผิด ในขณะเดียวกัน คดีความที่เกิดขึ้นแล้วจำนวนหนึ่งก็ถูกตั้งคำถามถึงความถูกต้องแห่งการ "ตั้งข้อหา" รวมทั้งความสับสน และซ้ำซ้อนกับกฎหมายฉบับอื่นที่มีอยู่ก่อน ซึ่งเหล่านี้ย่อมส่งผลกระทบโดยตรงต่อสิทธิและเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน อย่างไรก็ตาม คณะผู้วิจัยพบว่า คำถามและปัญหาต่างๆ ดังกล่าวมาไม่ได้มาจาก "การบังคับใช้" หรือ "ทัศนคติของผู้บังคับใช้" แต่เพียงอย่างเดียว หากแต่ยังเป็นผลมาจาก "บทบัญญัติ" ของพระราชบัญญัตินี้เองด้วย เพราะใช้ถ้อยคำที่กว้างขวาง สับสน ซ้ำซ้อน และไม่มีหลักการที่ชัดเจนแน่นอน ทั้งนี้ ตั้งแต่การให้คำนิยาม โดยเฉพาะอย่างยิ่ง คำว่า "ผู้ให้บริการ" ที่ไม่สอดคล้องกับความเข้าใจในวงการผู้ประกอบการและเทคโนโลยีสารสนเทศ มีความหมายกว้างกินความไปถึง "ผู้ให้บริการโทรคมนาคม" อื่นๆ ที่อาจไม่เกี่ยวข้องกับระบบหรือข้อมูลคอมพิวเตอร์อันเป็น "วัตถุ" แห่งกฎหมายตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 เลย ทำให้อาจต้องเสียเวลาทั้งผู้ฟ้องและผู้ถูกฟ้องเมื่อพบในท้ายที่สุดว่า ผู้ถูกฟ้องนั้นไม่มีคุณสมบัติหรือลักษณะที่จะเข้ามารับผิดชอบกับการกระทำความผิดที่เกิดขึ้นได้

มาตราที่กำหนดฐานความผิดบัญญัติไว้อย่างคลุมเครือ ในที่นี้

หมายเฉพาะ มาตรา 14 ซึ่งอยู่ในขอบเขตและเกี่ยวข้องกับหัวข้องานวิจัยเท่านั้น นับปัญหาตั้งแต่ความผิดตาม (1) ของมาตรา 14 ซึ่งอันที่จริงแล้วเป็นบทบัญญัติที่ว่าด้วยการ “ปลอมแปลง” หรือ “ทำให้เป็นเท็จ” ไม่ใช่ความผิดที่ว่าด้วยการ “เผยแพร่” ข้อมูลที่มี “เนื้อหาผิดกฎหมาย” แต่ถูกนำมาบัญญัติรวมไว้กับวงเล็บอื่นๆ ทำให้เกิดความสับสนกับผู้ใช้ มีการตีความไปถึงความผิดฐานหมิ่นประมาทจนก่อให้เกิดผลประหลาดต่างๆ นานา ความผิดใน (2) “ขัดต่อความมั่นคง” หรือ “ทำให้ประชาชนตื่นตระหนก” ก็ใช้ถ้อยคำคลุมเครือเปิดช่องให้อยู่ในดุลพินิจของเจ้าหน้าที่รัฐมากเกินไป ทั้งความหมายยังแปรเปลี่ยนไปตามยุคสมัยและทัศนคติของผู้ใช้อำนาจปกครอง ก่อให้เกิด “ความไม่มั่นคง” กับประชาชน ด้วยไม่รู้ว่าตนจะถูกดำเนินคดีอาญาเมื่อไร ทั้ง (2) ก็เป็นเรื่องซ้ำซ้อนกันเองกับ (3) ซึ่งกำหนดให้การเผยแพร่เนื้อหาที่ขัดต่อความมั่นคง หรือก่อการร้ายเป็นความผิดอยู่แล้ว ในขณะที่ มาตรา 15 พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีปัญหาในแง่ของหลักการ โดยเฉพาะอย่างยิ่งการกำหนดโทษไว้รุนแรง พิจารณาแล้วไม่เหมาะสมกับสภาพความผิด และโดยไม่คำนึงถึงลักษณะข้อมูลในอินเทอร์เน็ต ผู้ให้บริการซึ่งไม่ใช่ผู้กระทำความผิดด้วยตัวเองต้องเสี่ยงกับการรับโทษเท่าตัวการ จนก่อให้เกิดบรรยากาศแห่งความกลัว และสถานการณ์ “เซ็นเซอร์ตัวเอง” และโดยเฉพาะอย่างยิ่ง มาตรา 20 ซึ่งมีปัญหาในแง่ของการบัญญัติมากที่สุดมาตราหนึ่งในกฎหมายฉบับนี้ เพราะให้อำนาจเจ้าหน้าที่รัฐปิดกั้นเว็บไซต์ได้ภายใต้เงื่อนไขที่คลุมเครือว่า “ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน” ยังผลให้มีสถิติการปิดกั้นเว็บไซต์จำนวนมาก แต่ไม่สอดคล้องกับสถิติการฟ้องคดีเพื่อให้พิสูจน์ว่า ในที่สุดแล้ว “เนื้อหา” ที่รัฐปิดกั้นไปก่อนนั้น เป็นความผิดในฐานใด หรือกระทั่งเป็นความผิดจริงหรือไม่

แม้การป้องกันและปราบปรามการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์เป็นเรื่องที่มีความสำคัญเร่งด่วนในยุคข้อมูลข่าวสาร แต่ในประเทศที่อ้างตัวว่าปกครองในระบอบนิติรัฐ-ประชาธิปไตย การให้หลักประกันสิทธิเสรีภาพในการรับรู้ข้อมูล

ข่าวสาร และการแสดงความคิดเห็น รวมทั้งการให้ความเคารพต่อความคิด ความเชื่อ และการใช้วิจารณญาณของประชาชน ย่อมเป็นเรื่องที่รัฐต้องให้ความสำคัญ และพยายามอย่างถึงที่สุดเพื่อแสวงหาจุดร่วมที่สมดุลกับการป้องกันและปราบปรามการกระทำความผิดดังกล่าวด้วย

4. แนวนโยบายแห่งรัฐที่เกี่ยวกับเสรีภาพในการแสดงความคิดเห็นในสื่อออนไลน์

รายงานส่วนนี้จะได้กล่าวถึง แนวนโยบายและแนวปฏิบัติของภาครัฐที่เกี่ยวกับสื่อออนไลน์ ซึ่งหลายกรณีสามารถสะท้อนให้เห็นทัศนคติของผู้ใช้อำนาจรัฐ และเจ้าหน้าที่ผู้ปฏิบัติงานในระดับต่าง ๆ ที่มีต่อสิทธิเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นของประชาชน และเพื่อความสะดวกในการลำดับเหตุการณ์ ทั้งเพื่อง่ายต่อการทำความเข้าใจพัฒนาการและความเปลี่ยนแปลงของแนวนโยบาย คณะผู้วิจัยจึงได้รวบรวมและแบ่งการนำเสนอข้อมูลตามวาระการดำรงตำแหน่งของรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ซึ่งเป็นหน่วยงานรัฐผู้รับผิดชอบ และบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 โดยตรง

นับจากวันที่ 18 กรกฎาคม พ.ศ. 2550 ซึ่งเป็นวันที่ พ.ร.บ. คอมพิวเตอร์ฯ 2550 มีผลบังคับใช้ จนถึงปัจจุบัน (รัฐบาลนางสาวยิ่งลักษณ์ ชินวัตร พ.ศ. 2555) ข้อมูลการบังคับใช้กฎหมาย ปัญหาจากการบังคับใช้กฎหมาย รวมทั้งแนวนโยบายของรัฐที่ส่งผลกระทบอย่างหนึ่งอย่างใดต่อสิทธิและเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน อาจแบ่งได้อย่างน้อย 6 ช่วงเวลาตามวาระการดำรงตำแหน่งรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารดังนี้

1) นายสิทธิชัย โภไคยอุดม (9 ตุลาคม พ.ศ. 2549 ถึง 30 กันยายน พ.ศ. 2550)

2) นายโฆสิต ปั้นเปี่ยมรัษฎ์ (รักษาราชการแทน 1 ตุลาคม พ.ศ. 2550 ถึง 6 กุมภาพันธ์ พ.ศ. 2551)

3) นายมั่น พัธโนทัย (6 กุมภาพันธ์ พ.ศ. 2551 ถึง 2 ธันวาคม พ.ศ. 2551)

4) ร.ต.หญิง ระนองรักษ์ สุวรรณฉวี (20 ธันวาคม พ.ศ. 2551 ถึง 6 มิถุนายน พ.ศ. 2553)

5) นายจุติ ไกรฤกษ์ (6 มิถุนายน พ.ศ. 2553 ถึง 3 กรกฎาคม พ.ศ. 2554)

6) น.อ. อนุดิษฐ์ นาครทรรพ (9 สิงหาคม พ.ศ. 2554 จนถึงปัจจุบัน)

4.1. นโยบายรัฐในช่วงที่ นายสิทธิชัย โภไคยอุดม เป็นรัฐมนตรีว่าการกระทรวงไอซีที (9 ตุลาคม พ.ศ. 2549 ถึง 30 กันยายน พ.ศ. 2550)

4.1.1 ข้อมูลเบื้องต้น

นายสิทธิชัย โภไคยอุดม เป็นรัฐมนตรีว่าการกระทรวงไอซีที ในรัฐบาลพลเอก สุรยุทธ์ จุลานนท์ สำเร็จการศึกษาด้านวิศวกรรม เคยรับราชการเป็นอาจารย์ที่สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ประเด็นหลักของกระทรวงไอซีทีในขณะนั้น คือ การแปรสัมปทานโทรศัพท์เคลื่อนที่ในระบบ 3 จี และการแก้ไขปัญหาข้อพิพาทเรื่องดาวเทียมไทยคมกับกลุ่มเทมาเส็คของประเทศสิงคโปร์ อย่างไรก็ตาม ผลงานชิ้นแรกของนายสิทธิชัยในฐานะรัฐมนตรีว่าการกระทรวง ก็คือ การผลักดันร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.... เข้าสู่การพิจารณาของสภานิติบัญญัติแห่งชาติ โดยนายสิทธิชัยกล่าวถึงเหตุผลในการผลักดันว่า

"...เนื่องจากยังไม่มีกฎหมายที่สามารถควบคุมการกระทำความผิดได้ ทั้งการป้องกันแฮกเกอร์ การลงข้อความที่เสื่อมเสีย ลามก อนาจาร ข้อความที่หมิ่นพระบรมเดชานุภาพ และการหมิ่นประมาทส่วนบุคคล โดยจะมีการปรับปรุงการใช้อำนาจ และดุลพินิจของเจ้าหน้าที่ให้เหมาะสม แต่จะไม่ให้กฎหมายฉบับนี้ห้าม หรือปกปิดข้อมูลทางวิชาการ และการแสดง

ความเห็นทางการเมือง ...” [32]

ปลายเดือนพฤศจิกายน 2549 ภายหลังดำรงตำแหน่งได้สองเดือน กระทรวงไอซีทีจัดแถลงผลงานต่อสื่อมวลชนโดยมุ่งเน้นผลงานด้านการแก้ปัญหาการใช้เทคโนโลยีการสื่อสารไปในทางที่ผิด ซึ่งกระทรวงไอซีทีได้ทำการปิดกั้นช่องทางการเข้าถึงเว็บไซต์ที่ไม่เหมาะสมไปกว่า 3,100 เว็บไซต์ ทั้งยังมีข้อมูลจากการรับแจ้งเว็บไซต์ไม่เหมาะสมประมาณวันละ 15,000 ครั้ง อย่างไรก็ตาม ในการแถลงผลงานดังกล่าวไม่มีการให้ข้อมูลรายละเอียดใดๆ เกี่ยวกับเว็บไซต์ที่ถูกปิดกั้นหรือถูกแจ้งเข้ามาว่าส่วนใหญ่แล้วมีเนื้อหาเกี่ยวกับเรื่องอะไรหรือไม่เหมาะสมอย่างไร ทั้งนี้การปิดกั้นเว็บไซต์ในช่วงเวลาดังกล่าวกระทรวงไอซีทีน่าจะสั่งให้ปิดกั้นเองโดยลำพังไม่ได้ร้องขอคำสั่งศาลแต่อย่างใด ซึ่งเป็นการใช้อำนาจตามประกาศคณะปฏิรูปการปกครอง (คปค.) ฉบับที่ 5 ที่ออกโดยคณะปฏิรูปการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขภายหลังการทำรัฐประหารวันที่ 19 กันยายน 2549[33] ไม่ใช่การใช้อำนาจตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งในขณะนั้นยังไม่มีผลใช้บังคับ อย่างไรก็ตาม มีข้อควรสังเกตว่าในการแถลงผลงานครั้งนั้น กระทรวงไอซีทีเองหาได้อ้างอิงประกาศ คปค. ฉบับที่ 5 ในการปฏิบัติงานไม่ จึงเป็นผลให้เกิดกระแสวิพากษ์วิจารณ์ในสังคมและแวดวงไอทีว่ากระทรวงไอซีทีใช้อำนาจตามกฎหมายฉบับใดสั่งปิดกั้นเว็บไซต์ของประชาชน

4.1.2 กรณีโปรแกรม “แคมฟรอก” (Camfrog)

ปลายเดือนธันวาคม 2549 เกิดกระแสข่าววัยรุ่นไทยใช้โปรแกรม “แคมฟรอก” (Camfrog) ติดต่อสื่อสารผ่านกล้องเว็บแคมโดยมีการโชว์ลามกอนาจาร เป็นผลให้กระทรวงวัฒนธรรมโดยปลัดกระทรวงในขณะนั้นเข้าหารือกับนายสิทธิชัยเกี่ยวกับความเป็นไปได้ในการปิดกั้นการใช้งาน นำไปสู่การสั่งการให้บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ปิดกั้นการเชื่อมต่อระหว่างประเทศของโปรแกรมดังกล่าว นายสิทธิชัยกล่าวถึงกรณีดังกล่าวว่า

“...ถึงแม้วิธีนี้จะเป็นการแก้ปัญหาที่ปลายเหตุ แต่ก็เชื่อว่าจะ

สามารถแก้ปัญหาได้ โดยอยากขอโทษคนที่ได้รับความเสียหาย เพราะแคมฟรอกไม่ได้สร้างความเสียหายเพียงอย่างเดียว แต่ยังสามารถสร้างประโยชน์ เพราะที่ผ่านมาได้มีผู้พิการทางสายตาสามารถรับฟังทางเสียงได้..." [34]

กรณีนี้ยังนำไปสู่การจัดตั้งหน่วยงานเฉพาะกิจของตำรวจเพื่อปราบปรามอาชญากรรมคอมพิวเตอร์ โดยหน่วยงานแรกที่ตั้งขึ้น คือ "กองบังคับการปราบปรามการกระทำผิดต่อเด็ก เยาวชน และสตรี" (ปคส.) ซึ่งต่อมาเปลี่ยนเป็น "กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับการค้ามนุษย์" (ปคม.) นอกจากนี้ ในเวลาใกล้เคียงกัน เกิดกรณีใช้พระพุทธรูปเป็นตราสัญลักษณ์ของเว็บไซต์ลามกอนาจาร เกิดการวิพากษ์วิจารณ์อย่างกว้างขวาง นายสิทธิชัย จึงมอบหมายให้ปลัดกระทรวงไอซีที ประสานงานกับบริษัท กสท โทรคมนาคม จำกัด (มหาชน) และผู้ให้บริการอินเทอร์เน็ตให้ปิดกั้นเว็บไซต์ที่เผยแพร่ภาพลามกอนาจาร โดยหน่วยงานที่มีบทบาทสำคัญในช่วงเวลาดังกล่าว คือ ศูนย์เฝ้าระวังทางวัฒนธรรม ของกระทรวงวัฒนธรรม และศูนย์พิทักษ์พระพุทธศาสนาแห่งประเทศไทย ซึ่งทำหน้าที่สอดส่องดูแลเว็บไซต์ไม่เหมาะสมต่างๆ เพื่อแจ้งกระทรวงไอซีทีให้ทำการปิดกั้น ราวต้นเดือนมกราคม 2550 ปรากฏว่ากระทรวงไอซีทีสั่งปิดกั้นเว็บไซต์ลามกอนาจารไปจำนวนกว่า 15,000 เว็บไซต์[35] ซึ่งการปิดกั้นเว็บไซต์ในช่วงเวลานี้ คงเป็นการใช้อำนาจตามประกาศ คปค. ฉบับที่ 5 เช่นกัน เนื่องจาก พ.ร.บ.คอมพิวเตอร์ฯ 2550 ยังไม่มีผลใช้บังคับ

4.1.3 กรณีเว็บไซต์ Youtube.com และ Pantip.com ห้องราชดำเนิน

เหตุการณ์เกี่ยวกับเสรีภาพในการเข้าถึงข้อมูลข่าวสารทางอินเทอร์เน็ตที่นำไปสู่การวิพากษ์วิจารณ์ถึงบทบาทและการใช้อำนาจของนายสิทธิชัยในวงกว้างก็คือ กรณีสั่งปิดกั้นเว็บไซต์ Youtube.com ราวเดือนเมษายน 2550 เมื่อมีผู้เผยแพร่เนื้อหาที่อาจเข้าข่ายเป็นความผิดตาม

ประมวลกฎหมายอาญา มาตรา 112 ดูหมิ่น หมิ่นประมาท หรือแสดงความอาฆาตมาดร้ายพระมหากษัตริย์ฯ ลงในเว็บไซต์ดังกล่าว นายสิทธิชัยชี้แจงต่อกรณีนี้ว่า

"...เบื้องต้นได้พยายามปิดยูอาร์แอลเพราะเห็นว่าเป็นเว็บไซต์ที่มีประโยชน์เช่นกัน แต่ก็ไม่สามารถกั้นการเข้าถึงข้อมูลดังกล่าวได้ จึงต้องปิดกั้นทั้งเว็บไซต์ โดยจากนี้ต้องรอดูว่าเนื้อหาดังกล่าวยังมีการเผยแพร่อยู่หรือไม่ ถ้าไม่มีแล้วก็อาจจะยกเลิกการปิดกั้น..." [36]

หลังปิดกั้นเว็บไซต์ YouTube เพียงไม่กี่วัน กระทรวงไอซีทีสั่งปิดกระดานข่าวห้องราชดำเนินที่ให้บริการอยู่บนเว็บไซต์ Pantip.com ด้วยเหตุผลว่า มีข้อความกระทบต่อความมั่นคงเป็นจำนวนมาก แต่หลังจากผู้ดูแลเว็บไซต์แสดงให้กระทรวงไอซีทีเชื่อมั่นว่าจะทำการตรวจสอบอย่างเคร่งครัดเพื่อไม่ให้มีการแสดงความคิดเห็นในลักษณะดูหมิ่นพระมหากษัตริย์ ดูหมิ่นพลเอก เปรม ติณสูลานนท์ ประธานองคมนตรี รวมทั้งหมิ่นประมาทบุคคลอื่นๆ อีก จึงได้รับอนุญาตให้เปิดใช้งานใหม่ ส่วนกรณี YouTube นั้น หลังจากรัฐบาลไทยส่งเรื่องไปยังผู้ดูแลระบบในประเทศสหรัฐอเมริกา และเกิดข้อโต้แย้งเกี่ยวกับหน้าที่ของผู้ให้บริการ จึงได้ข้อยุติร่วมกันว่า เว็บไซต์ยินยอมลบเนื้อหาที่อาจเข้าข่ายหมิ่นประมาทกษัตริย์ฯ ออก กระทรวงไอซีทีจึงยกเลิกการปิดกั้น ทั้งสองกรณีได้นำไปสู่การจัดระเบียบและกำชับผู้ให้บริการอินเทอร์เน็ตทุกรายว่าต้องคอยสอดส่องดูแล รวมทั้งปิดกั้นเว็บไซต์ที่มีเนื้อหาหมิ่นพระบรมเดชานุภาพ และถือเป็นครั้งแรกที่กระทรวงไอซีทีอ้างถึงประกาศ คปค. ฉบับที่ 5 ว่าเป็นกฎหมายที่ให้อำนาจกระทรวงไอซีทีในการปิดกั้นเว็บไซต์

4.1.4 กรณีเว็บไซต์ PTV และกลุ่มแนวร่วมประชาธิปไตยไม่เอาเผด็จการ

ปลายเดือนพฤษภาคม 2550 มีการชุมนุมประท้วงรัฐบาลโดยกลุ่มแนวร่วมประชาธิปไตยไม่เอาเผด็จการ (นปก.) ซึ่งนอกจากการชุมนุม

แล้ว ยังมีการแจ้งข่าวสารต่างๆ และถ่ายทอดภาพการชุมนุมผ่านเว็บไซต์ ซึ่งต่อมาถูกปิดกั้นการเข้าถึงโดยกระทรวงไอซีที นายสิทธิชัยให้เหตุผลว่าเป็นเว็บไซต์ที่มีเนื้อหา “ขัดต่อความมั่นคง” เพราะปลุกปั่นให้ประชาชนออกมาชุมนุม

เดือนกรกฎาคม 2550 กระทรวงไอซีทีแถลงต่อคณะรัฐมนตรีว่าได้ดำเนินการปิดกั้นเว็บไซต์ที่มีเนื้อหายั่วยุหรือก่อความวุ่นวายไปกว่า 20 เว็บไซต์ โดยมีการกล่าวเปรียบเทียบการปิดกั้นอินเทอร์เน็ตกับนโยบายฆ่าตัดตอนในสมัยรัฐบาลทักษิณ ชินวัตร ในประเด็นการละเมิดสิทธิมนุษยชนว่า การปิดกั้นการเข้าถึงเว็บไซต์ถือว่าละเมิดสิทธิประชาชนเล็กน้อยมากเมื่อเทียบกับการฆ่าตัดตอน[37]

4.1.5 บทสรุป และวิเคราะห์

จะเห็นได้ว่านโยบายและแนวปฏิบัติของกระทรวงไอซีทีในสมัยของนายสิทธิชัย โภไคยอุดม มีลักษณะค่อนข้างเคร่งครัดเข้มงวด กระทั่งหมิ่นเหม่ต่อการละเมิดเสรีภาพในการเข้าถึงข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชนซึ่งได้รับการรับรองไว้ในรัฐธรรมนูญด้วย โดยเป็นที่น่าสังเกตว่าการปิดกั้นเว็บไซต์ในสมัยของนายสิทธิชัยนั้น จำนวนมากไม่ชัดเจนว่าเป็นการใช้อำนาจตามกฎหมายฉบับใด เนื่องจากเป็นเวลาที่ พ.ร.บ. คอมพิวเตอร์ฯ 2550 ยังไม่ประกาศใช้ ทั้งกระทรวงไอซีทีเองก็ไม่เคยให้เหตุผล หรืออ้างอิงกฎหมายที่ชัดเจนด้วย จนในเดือนเมษายน 2550 จึงเริ่มมีการอ้างถึงประกาศ คปค. ฉบับที่ 5 ในกรณีของการปิดเว็บไซต์ YouTube หลังจากกรณีปิดกั้นเว็บไซต์ของกลุ่มแนวร่วมประชาธิปไตยไม่เอาเผด็จการ พ.ร.บ. คอมพิวเตอร์ฯ 2550 ก็มีผลใช้บังคับ และประกาศ คปค. ฉบับที่ 5 ก็ถูกยกเลิกไป[38] อย่างไรก็ดี ภายหลัง พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีผลใช้บังคับได้ไม่นานนายสิทธิชัยก็ลาออกจากตำแหน่งรัฐมนตรีว่าการกระทรวงไอซีที

อนึ่ง ในยุคของนายสิทธิชัยนี้เอง ที่ถือเป็นจุดเริ่มของหน่วยงานใหม่ๆ หลายหน่วยงานที่มีหน้าที่เฉพาะในการตรวจตราเนื้อหาที่เผยแพร่

ในสื่อออนไลน์ และหลายแห่งยังคงปฏิบัติหน้าที่ในลักษณะดังกล่าวอยู่ต่อมาจนถึงปัจจุบัน

4.2. นโยบายรัฐในช่วงที่ นายโฆสิต ปั้นเปี่ยมรัษฎ์ เป็นรัฐมนตรีว่าการกระทรวงไอซีที (รักษาราชการแทน 1 ตุลาคม พ.ศ. 2550 ถึง6 กุมภาพันธ์ พ.ศ. 2551)

4.2.1 ข้อมูลเบื้องต้น

เนื่องจากนายโฆษิต ปั้นเปี่ยมรัษฎ์ เป็นเพียงผู้รักษาราชการแทนรัฐมนตรีว่าการที่ลาออกไป ในขณะเดียวกันก็ดำรงตำแหน่งรองนายกรัฐมนตรีด้านเศรษฐกิจด้วย ประกอบกับเป็นช่วงของการเตรียมการเลือกตั้งผู้แทนราษฎรซึ่งจะเกิดขึ้นในวันที่ 23 ธันวาคม 2550 จึงไม่ได้มีการดำเนินนโยบายใดๆ เพิ่มเติม นโยบายและแนวปฏิบัติของกระทรวงไอซีทีในสมัยของนายโฆสิตในภาพรวมจึงยังเป็นลักษณะเดียวกันกับสมัยของนายสิทธิชัย คือ เน้นการตรวจสอบเนื้อหาในสื่อออนไลน์ และปิดกั้นเว็บไซต์ที่มีเนื้อหาไม่เหมาะสมโดยอาศัยความร่วมมือระหว่างสามหน่วยงานหลัก คือ กระทรวงไอซีที กระทรวงวัฒนธรรม และสำนักงานตำรวจแห่งชาติ ทั้งนี้เว็บไซต์ส่วนใหญ่ที่ถูกปิดกั้นในช่วงดังกล่าวคือเว็บไซต์ลามกอนาจาร และดูหมิ่นพุทธศาสนา[39]

4.2.2 บทสรุป และวิเคราะห์

นโยบายและแนวปฏิบัติเกี่ยวกับเว็บไซต์ที่เผยแพร่ภาพลามกอนาจารยังคงเป็นเช่นเดิม โดยกระทรวงวัฒนธรรมจัดตั้งศูนย์เฝ้าระวังทางวัฒนธรรมขึ้นเพื่อสอดส่องดูแลโดยเฉพาะ และในช่วงเวลานั้นก็แทบไม่มีปัญหาหรือกรณีใดๆ ที่เกี่ยวข้องกับการเมืองเกิดขึ้นเลย ซึ่งอาจเป็นเพราะใกล้ช่วงเวลาเลือกตั้งทั่วไป ทำให้สถานการณ์ทางการเมืองสงบลง

4.3 นโยบายรัฐในช่วงที่ นายมั่น พัธโนทัย เป็นรัฐมนตรีว่าการกระทรวงไอซีที (6 กุมภาพันธ์ พ.ศ. 2551 ถึง 2 ธันวาคม พ.ศ. 2551)

4.3.1 ข้อมูลเบื้องต้น

นายมั่น พัธโนทัย เป็นรัฐมนตรีว่าการกระทรวงไอซีทีในรัฐบาลนายสมัคร สุนทรเวช และนายสมชาย วงศ์สวัสดิ์ สำเร็จการศึกษาจากคณะนิติศาสตร์ โดยเขายอมรับว่าไม่มีความรู้ด้านเทคโนโลยีสารสนเทศเลย ทั้งไม่ได้เตรียมตัวมาดำรงตำแหน่งรัฐมนตรีว่าการกระทรวงไอซีทีอีกด้วย ทั้งนี้ อาจกล่าวได้ว่า ประเด็นที่กระทรวงไอซีทีในสมัยของนายมั่นให้ความสำคัญ และถูกจับตามองจากสังคม คือ การร่างพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์และกิจการโทรคมนาคม พ.ศ. ...

สำหรับการดำเนินนโยบายที่มีผลต่อเสรีภาพของประชาชนในสื่อออนไลน์นั้น เป็นไปในเชิงรุกมากขึ้น มีการริเริ่มโครงการและตั้งหน่วยงานสอดส่องเนื้อหาบนเว็บไซต์เพิ่มเติม ซึ่งอาจเป็นผลมาจากการที่เครือข่ายสังคมออนไลน์ (social network) เริ่มได้รับความนิยมมากขึ้นซึ่งมีการเผยแพร่ภาพลามกอนาจาร หรือการล่อลวงผ่านทางเครื่องมือดังกล่าว ทั้งยังเป็นช่วงที่มีเว็บไซต์พนันฟุตบอลเกิดขึ้นจำนวนมาก นอกจากนี้ ในช่วงระยะเวลาดังกล่าวยังได้มีการพูดถึงแนวทางในการแก้ไขเปลี่ยนแปลงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ พ.ศ. 2550 ด้วย เพื่อแก้ปัญหาการบังคับใช้ และเพิ่มประสิทธิภาพในการควบคุมเว็บไซต์ที่มีเนื้อหาหมิ่นประมาทพระมหากษัตริย์ให้เข้มงวดยิ่งขึ้น

4.3.2 โครงการ Hack and Crack

หลังจากนายมั่นเข้ารับตำแหน่งได้หนึ่งเดือน กระทรวงไอซีทีก็ริเริ่มโครงการชื่อว่า Hack and Crack มีวัตถุประสงค์เพื่อแก้ปัญหาและลดช่องว่างในทางปฏิบัติที่รัฐไม่สามารถสั่งปิดกั้นการเข้าถึงเว็บไซต์ที่มีเนื้อหาหมิ่นพระบรมเดชานุภาพ หรือหมิ่นศาสนาพุทธได้โดยสมบูรณ์ เนื่องจากหลาย

กรณีเป็นเว็บไซต์ของต่างประเทศ กระทรวงจึงต้องการตั้งเจ้าหน้าที่พิเศษในการเจาะระบบคอมพิวเตอร์ของผู้อื่นเพื่อเข้าไปลบข้อมูลในระบบหรือในเว็บไซต์เหล่านั้น นายมั่นกล่าวถึงโครงการฯ ดังกล่าวว่า

"การกระทำลักษณะนี้ อาจเข้าข่ายผิดกฎหมายอยู่บ้าง แต่บางครั้งก็ต้องยอมแลก ถ้าเป็นสิ่งที่ยอมรับไม่ได้จริงๆ" [40]

อย่างไรก็ตาม โครงการนี้ถูกต่อต้านทั้งจากนักกฎหมาย และนักคอมพิวเตอร์จำนวนไม่น้อย ซึ่งนอกจากเหตุผลเรื่องรัฐบาลไม่ควรทำผิดกฎหมายเสียเองแล้ว (ในเวลานั้น การเข้าถึงระบบหรือข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่มีอำนาจ หรือการเจาะระบบเป็นความผิดตามกฎหมายของประเทศส่วนใหญ่แล้ว) ยังมีประเด็นวิพากษ์วิจารณ์ในเรื่องการไม่ประเมินศักยภาพของหน่วยงาน รวมทั้งความสามารถของเจ้าหน้าที่ไทยเองด้วยซึ่งปฏิเสธไม่ได้ว่าอาจยังด้อยกว่ากลุ่มประเทศตะวันตก อย่างไรก็ตาม โครงการดังกล่าวถูกล้มเลิกไปในท้ายที่สุด

4.3.3 ตั้งศูนย์ประสานความร่วมมือปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศและการสื่อสาร (ICT CORP) และตั้งงบประมาณเพื่อการปิดกั้นเว็บไซต์

เดือนพฤษภาคม 2551 กระทรวงไอซีทีตั้งศูนย์ประสานความร่วมมือปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศและการสื่อสาร หรือ ICT CORP ขึ้น ซึ่งเกิดจากความร่วมมือระหว่างหลายหน่วยงาน เช่น กองปราบปราม สำนักข่าวกรองแห่งชาติ และกรมสอบสวนคดีพิเศษ (DSI) เป็นต้น มีภารกิจสืบสวนร่องรอยการก่ออาชญากรรมคอมพิวเตอร์และอาชญากรรมประเภทอื่นๆ ที่กระทำผ่านคอมพิวเตอร์ ซึ่งส่วนมากเป็นคดีฉ้อโกงผ่านอินเทอร์เน็ต หมิ่นประมาท และเผยแพร่ภาพลามกอนาจาร และนอกเหนือจากหน้าที่ในการสืบหาตัวผู้กระทำความผิดแล้ว หน่วยงานดังกล่าวยังมีหน้าที่ตรวจจับและเฝ้าระวังเว็บไซต์ที่มีเนื้อหาหมิ่นพระบรมเดชานุภาพด้วย นายมั่นให้สัมภาษณ์กรณีนี้ไว้ว่า

"...ทางกระทรวงมีหน่วยไอซีทีคอร์ปคอยตรวจจับ หรือเฝ้าระวังเว็บไซต์กว่า 200 เว็บไซต์ ตลอด 24 ชั่วโมง ซึ่งมีเจ้าหน้าที่เพียง 10 คน ที่ผ่านมา ผู้ให้บริการอินเทอร์เน็ตกว่า 200 แห่ง ก็ให้ความร่วมมืออย่างดี มีการประชุมร่วมกันหลายครั้ง..." [41]

จากนั้นในเดือนกรกฎาคมปีเดียวกัน นายมั่นเปิดเผยว่าตรวจพบเว็บไซต์ที่มีเนื้อหาไม่เหมาะสมกว่า 1,200 เว็บไซต์ ในจำนวนนี้มีกว่า 700 เว็บไซต์ที่มีเนื้อหาหมิ่นพระบรมเดชานุภาพ โดยศาลมีคำสั่งให้ปิดกั้นแล้ว 416 เว็บไซต์[42]

อนึ่ง นอกจากการตั้งศูนย์ประสานความร่วมมือแล้ว ในยุคของนายมั่นนี้เองที่กระทรวงไอซีทีได้เตรียมจัดงบประมาณเฉพาะเพื่อซื้ออุปกรณ์และเครื่องมือจากต่างประเทศสำหรับภารกิจปิดกั้นเว็บไซต์ไม่เหมาะสม โดยเฉพาะอย่างยิ่งที่มีเนื้อหาเป็นการจาบจ้วงสถาบันฯ ทั้งนี้ อุปกรณ์ดังกล่าวมีราคาเครื่องละ 100-500 ล้านบาท ซึ่งนายมั่นกล่าวถึงกรณีนี้ว่า

"จะมีการหารือเพื่อขอซื้อเครื่องที่บล็อกเว็บไม่เหมาะสม ราคาเครื่องละ 100-500 ลบ. จะช่วยบล็อกเว็บไม่เหมาะสมได้รวมถึงเว็บก่อการร้าย เว็บโป๊ก็สามารถทำได้" [43]

4.3.4 การแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

การแก้ไข พ.ร.บ.คอมพิวเตอร์ฯ 2550 ถูกกล่าวถึงเป็นครั้งแรกในเดือนสิงหาคม 2551 โดยเฉพาะอย่างยิ่งในประเด็นปัญหาการบังคับใช้ บทบัญญัติที่ไม่สอดคล้องกับสภาพสังคมออนไลน์และพัฒนาการด้านเทคโนโลยี รวมทั้งภาระหน้าที่ของผู้ให้บริการที่ต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ 90 วัน ซึ่งมีค่าใช้จ่ายในการดำเนินการสูง อย่างไรก็ตาม ในท้ายที่สุดยังไม่มีข้อเสนอใดๆ ที่เป็นรูปธรรมเพื่อการแก้ไขดังกล่าว กระทั่งเดือนตุลาคม 2551 ซึ่งมีรายงานว่าเว็บไซต์หมิ่นประมาทพระมหากษัตริย์เพิ่มจำนวนขึ้น ที่ประชุมไอซีทีจึงออกข้อเสนอแก้ไขเพิ่ม

เติม พ.ร.บ.คอมพิวเตอร์ฯ 2550 เพื่อเพิ่มอำนาจแก่เจ้าพนักงานให้สามารถปิดกั้นเว็บไซต์ที่มีเนื้อหาหมิ่นพระมหากษัตริย์ได้ทันทีที่ตรวจพบโดยไม่ต้องขอคำสั่งศาล เพื่อให้เกิดความรวดเร็วก่อนที่เว็บไซต์เหล่านั้นจะปิดตัวและย้ายเซิร์ฟเวอร์หนีไปที่อื่น นอกจากนี้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ยังเสนอให้จัดซื้ออุปกรณ์เพิ่มประสิทธิภาพแบบเดียวกับกระทรวงกลาโหมของสหรัฐ เพื่อใช้สำหรับตรวจสอบเนื้อหาและปิดกั้นเว็บไซต์ได้ทันที โดยนายมั่นกล่าวว่า

"มั่นใจว่า ถ้ามีการปิดกั้นเว็บไซต์หมิ่นเบื้องสูง จะไม่มีการฟ้องร้อง เพราะไอซีทีเตรียมเก็บหลักฐานก่อนมีการปิดกั้น ถ้ากล้ามาฟ้องร้องจริง ก็เท่ากับเปิดเผยว่าเป็นผู้ดูแลเว็บไซต์ที่ปล่อยให้มีเนื้อหาหมิ่นเบื้องสูง"

4.3.5 แนวปฏิบัติอื่นๆ

เดือนพฤศจิกายน 2551 กระทรวงไอซีทีออกมาตรการ 5 ข้อในการดำเนินการกับเว็บไซต์ที่มีเนื้อหาเข้าข่ายหมิ่นประมาทพระมหากษัตริย์[44] ดังนี้

1) ให้ผู้ให้บริการร่วมมือปิดกั้นเว็บไซต์หมิ่นพระบรมเดชานุภาพทันทีที่พบเห็น

2) ให้ผู้ให้บริการสืบค้นหาตัวผู้กระทำผิดทุกครั้งก่อนการปิดกั้นเว็บไซต์

3) กระทรวงไอซีทีจะดำเนินการพิสูจน์ทราบตัวผู้กระทำผิด และเสนอไปยังสำนักงานตำรวจแห่งชาติ เพื่อดำเนินคดีและขอความร่วมมือผู้ให้บริการนำเสนอรายชื่อผู้กระทำผิดขึ้นบัญชีและนำประกาศเผยแพร่ต่อไป

4) หากกระทรวงไอซีทีตรวจพบว่า ผู้ให้บริการไม่ดำเนินการปิดกั้นเว็บไซต์ที่ไม่เหมาะสม ตามกระทรวงไอซีทีมีหนังสือแจ้งไปเกิน 3 ครั้ง ก็จะดำเนินการขั้นเด็ดขาดส่งเรื่องไปยังคณะกรรมการกิจการโทรคมนาคมแห่งชาติ หรือ กทช. เพิกถอนใบอนุญาตทันที แต่การดำเนินการขั้นเด็ดขาดนั้น กระทรวงอาจจะไม่จำเป็นต้องส่งหนังสือแจ้งเตือนครบ 3 ครั้ง ถ้าเนื้อหามีความรุนแรงมากเกินไป โดยการดำเนินการเรื่องนี้ได้รับการตอบรับให้ความ

ร่วมมือจาก กทช. เป็นอย่างดี

5) สำหรับผู้ให้บริการที่อยู่ภายใต้การดูแลของบริษัท ทีโอที จำกัด (มหาชน) และ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้สั่งการให้มีการดำเนินการตามอย่างเคร่งครัด นอกจากนี้ ศูนย์เฝ้าระวังจะดำเนินการตลอด 24 ชั่วโมง และเปิดให้ประชาชนมีส่วนร่วมในการร้องเรียนหรือแจ้งข้อมูลเว็บไซต์ไม่เหมาะสม"

นอกจากกระทรวงไอซีทีแล้ว ในช่วงท้ายๆ ของการดำรงตำแหน่งของนายมั่น สำนักงานตำรวจแห่งชาติโดย พล.ต.อ. พัชรวาท วงษ์สุวรรณ ผู้บัญชาการตำรวจแห่งชาติ ยังได้แต่งตั้งคณะกรรมการตรวจสอบและพิจารณาข้อมูลข่าวสารที่อาจมีผลกระทบต่อสถาบันพระมหากษัตริย์ เพื่อทำหน้าที่สอดส่องและพิจารณาข้อมูลข่าวสารในเว็บไซต์ หรือวิทยุชุมชนที่อาจมีผลกระทบต่อสถาบันพระมหากษัตริย์ รวมทั้งรับแจ้งจากประชาชนและหน่วยงานต่างๆ เพื่อส่งให้หน่วยงานที่มีอำนาจหน้าที่สอบสวนดำเนินการตามกฎหมาย

4.3.6 บทสรุป และวิเคราะห์

ช่วงเดือนสุดท้ายของวาระการดำรงตำแหน่งของนายมั่นนั้น มีการชุมนุมของกลุ่มพันธมิตรประชาชนเพื่อประชาธิปไตย และมีคำพิพากษายุบพรรคพลังประชาชนโดยศาลรัฐธรรมนูญ จึงทำให้สถานการณ์ทางการเมืองไม่เสถียรภาพ และไม่อาจบริหารราชการได้โดยปกติ อย่างไรก็ตาม จากกรณีต่างๆ ตามที่กล่าวมาข้างต้น จะเห็นได้ว่านโยบายและแนวปฏิบัติของนายมั่นในฐานะรัฐมนตรีว่าการกระทรวงไอซีที รวมถึงทัศนคติของหน่วยงานภาครัฐอื่นๆ มีแนวโน้มที่จะเข้มงวดรุนแรงกับเนื้อหาในสื่อออนไลน์มากขึ้นกว่ารัฐบาลในสมัยของพลเอกสุรยุทธ์ จุลานนท์ ทั้งเป็นเรื่องที่รัฐพร้อมที่จะจัดสรรงบประมาณจำนวนมากเพื่อดำเนินการดังกล่าว และแม้นายมั่นจะถือได้ว่าเป็นรัฐมนตรีที่อยู่ในขั้วการเมืองตรงข้ามกับรัฐมนตรีว่าการกระทรวงไอซีทีสองคนแรก คือ นายสิทธิชัย และนายโฆษิต แต่นโยบายและแนว

ปฏิบัติก็ยังเป็นไปในทิศทางเดียวกัน คือ มุ่งเน้นการตรวจสอบเนื้อหา และการปิดกั้นเว็บไซต์ โดยเฉพาะอย่างยิ่ง เว็บไซต์ที่รัฐเห็นว่าเข้าข่ายเป็นความผิดฐานหมิ่นประมาทพระมหากษัตริย์ มีการตั้งหน่วยงานเฉพาะเพื่อลาดตระเวนตรวจสอบเนื้อหาในอินเทอร์เน็ตหลายหน่วยงานทั้งจากกระทรวงไอซีที ดีเอสไอ และสำนักงานตำรวจแห่งชาติ

อย่างไรก็ตาม เป็นเรื่องที่ควรตั้งข้อสังเกตไว้ด้วยว่า แม้ในยุคที่นายมั่นเป็นรัฐมนตรีกระทรวงไอซีทีนั้น พ.ร.บ.คอมพิวเตอร์ฯ 2550 จะมีผลใช้บังคับแล้ว แต่กระทรวงไอซีทีกลับออก “มาตรการ” เชิงบังคับ (ด้วยใบอนุญาตประกอบการ) หรือกระทำในลักษณะ “ขอความร่วมมือ” จากผู้ให้บริการให้ทำการปิดกั้นเว็บไซต์ทันทีที่พบเห็นแทนที่จะแจ้งเรื่องไปยังเจ้าพนักงานที่เกี่ยวข้อง เพื่อขอคำสั่งศาลตามกฎหมายต่อไป ซึ่งคณะผู้วิจัยเห็นว่าน่าจะเป็นคำสั่งหรือการใช้อำนาจรัฐในลักษณะที่ขัดต่อทั้ง พ.ร.บ.คอมพิวเตอร์ฯ 2550 และรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 45 เพราะเรื่องดังกล่าวย่อมกระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชนโดยตรง หากรัฐต้องการจำกัดการใช้เสรีภาพดังกล่าวรัฐธรรมนูญกำหนดให้ต้องบัญญัติเป็นกฎหมายเฉพาะเจาะจง มิใช่เพียงออกเป็นมติหรือมาตรการบังคับประเภทอื่นใดเท่านั้น นอกจากนี้ ในยุคของนายมั่นซึ่งเป็นรัฐมนตรีที่เป็นนักกฎหมาย ยังมีความพยายามที่จะเสนอโครงการหรือกระทำการใดๆ อันเป็นความผิดต่อกฎหมายเสียเอง อย่างโครงการ Hack and Crack เป็นต้น

4.4 นโยบายและแนวปฏิบัติในช่วงที่ ร.ต.หญิง ระนองรักษ์ สุวรรณฉวี เป็นรัฐมนตรีว่าการกระทรวงไอซีที (20 ธันวาคม พ.ศ. 2551 ถึง 6 มิถุนายน พ.ศ. 2553)

4.4.1 ข้อมูลเบื้องต้น

ร.ต.หญิง ระนองรักษ์ สุวรรณฉวี เป็นรัฐมนตรีว่าการกระทรวงไอซีที ในรัฐบาลนายอภิสิทธิ์ เวชชาชีวะ โดยวันแรกที่เข้ารับตำแหน่ง ร.ต.หญิง

ระนองรักษ์ กล่าวว่า

"ภารกิจแรกที่ต้องดำเนินการอย่างเร่งด่วนและต่อเนื่อง คือ จัดการกับเว็บไซต์ที่เข้าข่ายหมิ่นพระบรมเดชานุภาพและสถาบันเบื้องสูง เนื่องจากมองว่าเป็นเรื่องสำคัญมากที่สุด"

จึงกล่าวได้ว่า นอกเหนือจากประเด็นสัมปทานดาวเทียมไทยคมและเทคโนโลยี 3 จี ซึ่งเป็นภารกิจที่ต่อเนื่องมาจากรัฐมนตรีคนก่อน การปราบปรามเว็บไซต์ที่มีเนื้อหาหมิ่นพระบรมเดชานุภาพหรือกระทบต่อความมั่นคง เป็นสิ่งที่ ร.ต.หญิง ระนองรักษ์ ให้ความสำคัญที่สุด โดยนอกจากศูนย์ประสานงานความร่วมมือปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศและการสื่อสาร หรือ ICT CORP ที่ตั้งขึ้นสมัยนายมั่นแล้ว ร.ต.หญิง ระนองรักษ์ ยังจัดตั้งหน่วยงานเพิ่มเติม เพื่อดูแลสอดส่องเนื้อหาบนอินเทอร์เน็ตโดยเฉพาะอีกหน่วยหนึ่ง คือ ศูนย์ปฏิบัติการความปลอดภัยอินเทอร์เน็ต หรือ Internet Security Operation Center (ISOC)

ทั้งนี้ ในช่วงเวลาที่ ร.ต.หญิง ระนองรักษ์ดำรงตำแหน่ง ได้เกิดการชุมนุมทางการเมืองของกลุ่มคนเสื้อแดง 2 ครั้ง คือ ช่วงเดือนมีนาคมถึงเมษายน 2552 และเดือนเมษายนถึงพฤษภาคม 2553 ซึ่งมีการประกาศใช้ พ.ร.ก.การบริหารราชการในสถานการณ์ฉุกเฉิน 2548 ด้วย ทั้งรัฐบาลยังได้ตั้งศูนย์อำนวยการแก้ไขสถานการณ์ฉุกเฉิน (ศอฉ.) ขึ้น ซึ่งมีทั้งอำนาจในการควบคุมสถานการณ์ฉุกเฉินที่เกี่ยวกับการชุมนุม และควบคุมการสื่อสารประเภทต่างๆ

4.4.2 ศูนย์ปฏิบัติการความปลอดภัยอินเทอร์เน็ต หรือ Internet Security Operation Center (ISOC)

วันที่ 29 มกราคม 2552 นายอภิสิทธิ์ เวชชาชีวะ นายกรัฐมนตรีออกคำสั่งสำนักนายกรัฐมนตรีที่ 34/2552 แต่งตั้ง "คณะกรรมการอำนวยการกำหนดนโยบายในการป้องกันและปราบปรามการนำเสนอข้อมูลข่าวสารที่ผิดกฎหมายและ/หรือไม่เหมาะสมผ่านระบบเทคโนโลยีสารสนเทศและ

การสื่อสาร" โดยมี ร.ต.หญิง ระนองรักษ์ รัฐมนตรีว่าการกระทรวงไอซีที เป็นประธาน และภายหลังการประชุมคณะกรรมการอำนวยการฯ ครั้งที่ 1 ได้มีการจัดตั้ง "ศูนย์ปฏิบัติการความปลอดภัยอินเทอร์เน็ต" หรือ Internet Security Operation Center (ISOC)[45] (ต่อมาปรับรูปแบบเป็น Cyber Security Operation Center: CSOC หรือ "ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์" ในสมัยที่นาวาอากาศเอก อนุดิษฐ์ นาครทรรพ เป็นรัฐมนตรีกว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร) เพื่อคอยประสานการทำงานกับหน่วยงานทหารและตำรวจ โดยมีงบประมาณสำหรับโครงการดังกล่าว 80 ล้านบาท ภาระหน้าที่หลักของศูนย์นี้ คือ เฝ้าระวังภัยคุกคามจากเนื้อหาที่ไม่เหมาะสมบนอินเทอร์เน็ต รวมทั้งปฏิบัติการและสนับสนุนภารกิจอื่นที่เกี่ยวข้องกับนโยบายในการดำเนินคดีผู้กระทำความผิดคดีหมิ่นสถาบันพระมหากษัตริย์ตาม พ.ร.บ.คอมพิวเตอร์ฯ ซึ่งตลอดสมัยของ ร.ต.หญิง ระนองรักษ์ มีการแถลงผลงานของ ISOC เป็นระยะดังนี้

1) วันที่ 4 กุมภาพันธ์ 2552 ระงับการเข้าถึงเว็บไซต์ทั้งสิ้น 4,818 ยูอาร์แอล แบ่งเป็นเว็บไซต์หมิ่นพระบรมเดชานุภาพ 4,683 ยูอาร์แอล เว็บไซต์ลามกอนาจาร 98 ยูอาร์แอล และเว็บไซต์โฆษณาเท็จ 37 ยูอาร์แอล[46]

2) วันที่ 24 เมษายน 2552 ระงับการเข้าถึงเว็บไซต์ทั้งสิ้น 8,955 ยูอาร์แอล แบ่งเป็นเว็บไซต์ที่กระทบต่อความมั่นคง 6,218 ยูอาร์แอล เว็บไซต์ลามกอนาจาร 2,307 ยูอาร์แอล และเว็บไซต์การพนัน 430 ยูอาร์แอล[47]

3) วันที่ 29 กรกฎาคม 2552 ระงับการเข้าถึงเว็บไซต์ทั้งสิ้น 16,944 ยูอาร์แอล แบ่งเป็นเว็บไซต์ที่กระทบต่อความมั่นคง 11,000 ยูอาร์แอล เว็บไซต์ที่เผยแพร่ข้อมูลกระทบด้านสังคมและวัฒนธรรม 5,872 ยูอาร์แอล และเว็บไซต์ที่เผยแพร่ข้อมูลกระทบด้านเศรษฐกิจ 72 ยูอาร์แอล[48]

4) วันที่ 15 กันยายน 2552 ระงับการเข้าถึงเว็บไซต์ทั้งสิ้น 19,124 ยูอาร์แอล แบ่งเป็นเว็บไซต์ที่กระทบต่อความมั่นคง 10,578 ยูอาร์แอล เว็บไซต์ลามกอนาจาร 8,474 ยูอาร์แอล และเว็บไซต์การพนัน 72 ยูอาร์แอล[49]

อย่างไรก็ตาม หลังจากเดือนตุลาคม 2552 ก็ไม่มีการแถลง

ผลงานของ ISOC อย่างเป็นทางการอีกเลย มีเพียงการให้สัมภาษณ์ในเดือนพฤษภาคม 2553 โดย พ.ต.อ. สุชาติ วงศ์อนันต์ชัย ผู้ตรวจราชการกระทรวงไอซีทีเท่านั้นว่า ISOC ระงับการเข้าถึงเว็บไซต์ไปทั้งสิ้นราว 50,000 ยูอาร์แอล โดยไม่มีการแจ้งรายละเอียดใดๆ ว่าเว็บไซต์ที่ถูกปิดไปมีเนื้อหาประเภทใดบ้าง

4.4.3 ความคิดเห็นต่อการชุมนุมทางการเมืองของกลุ่มคนเสื้อแดง

ดังกล่าวไปแล้วว่า การชุมนุมทางการเมืองสองครั้งใหญ่เกิดขึ้นในช่วงที่ ร.ต.หญิง ระนองรักษ์ เป็นรัฐมนตรีว่าการกระทรวงไอซีที ซึ่งได้เกิดกรณีสำคัญๆ ที่เกี่ยวกับการควบคุมการสื่อสารสู่มวลชนหลายกรณี อาทิ ในเดือนเมษายน พ.ศ. 2552 รัฐบาลตัดสัญญาณการสื่อสารผ่านดาวเทียมที่ส่งสัญญาณการปราศรัยของ พ.ต.ท. ทักษิณ ชินวัตร อดีตนายกรัฐมนตรี โดยได้มีการหารือกับคณะกรรมการกิจการโทรคมนาคมแห่งชาติ หรือ กทช. เพื่อหาช่องทางทางกฎหมายในการดำเนินการ ซึ่ง ร.ต.หญิง ระนองรักษ์ กล่าวถึงกรณีนี้ว่า

"...ต้องดูว่ามีข้อกฎหมายใดเอามาบังคับใช้ได้ ถ้าการแพร่สัญญาณกระทบต่อความมั่นคง หรือทำให้เกิดความแตกแยกก็อาจใช้กฎหมายเข้ามากำกับดูแลได้ ส่วนถ้าจะมองว่าดีทีวีผิดหรือไม่ ต้องดูว่าเนื้อหาที่ส่งออกมาเกี่ยวกับความมั่นคงของชาติหรือมีเนื้อหาทำให้เกิดความแตกแยกหรือไม่..."

ภายหลังการสลายการชุมนุมเมื่อวันที่ 10 เมษายน 2552 ร.ต.หญิง ระนองรักษ์ กล่าวถึงการดำเนินการกับผู้เผยแพร่เนื้อหาที่ไม่เหมาะสม และเป็นภัยต่อความมั่นคงของชาติบนเว็บไซต์ว่า

"ผู้ที่เผยแพร่เนื้อหาที่ไม่เหมาะสมอันเป็นภัยต่อความมั่นคงของประเทศชาติบนเว็บไซต์ต่างๆ ทางอินเทอร์เน็ต ทั้งเผยแพร่เนื้อหา ภาพหรือข้อความที่มีลักษณะปลุกระดมอันเป็นเหตุให้เกิดความวุ่นวายหรือการจลาจล หรือเว็บไซต์ที่มีเนื้อหาหมิ่นประมาทบุคคลหรือสถาบันที่ส่งผล

กระทบต่อความมั่นคงของประเทศชาติ กระทรวงไอซีทีจะใช้กฎหมายบังคับอย่างจริงจังและเข้มงวด” [50]

สำหรับการชุมนุมในเดือนเมษายนถึงพฤษภาคม 2553 นั้น ก่อนมีการประกาศสถานการณ์ฉุกเฉิน รัฐบาลได้ตั้งศูนย์อำนวยการรักษาความสงบเรียบร้อย (ศอ.รส.) ให้มีอำนาจและสามารถออกคำสั่งให้กระทรวงไอซีทีปิดกั้นเว็บไซต์ที่เข้าข่ายยั่วยุและปลุกระดมให้เกิดความแตกแยกได้ทันที โดยไม่ต้องแสดงพยานหลักฐานเบื้องต้นใดๆ รวมทั้งไม่ต้องขอคำสั่งศาล[51] เมื่อมีการประกาศสถานการณ์ฉุกเฉินแล้ว ศูนย์อำนวยการแก้ไขสถานการณ์ฉุกเฉิน (ศอฉ.) ที่จัดตั้งขึ้นใหม่ก็กลายเป็นหน่วยงานที่มีอำนาจโดยตรงตาม พ.ร.ก.การบริหารราชการในสถานการณ์ฉุกเฉิน 2548 ในการปิดกั้นการเข้าถึงข้อมูลข่าวสารในสื่อประเภทต่างๆ ซึ่งหมายรวมถึงสื่อออนไลน์ด้วย โดย ศอ.รส. และ ศอฉ. แถลงตัวเลขเว็บไซต์ที่ถูกปิดกั้นเป็นระยะดังนี้

1) วันที่ 9 เมษายน 2553 ปิดกั้นเว็บไซต์ที่เข้าข่ายปลุกระดม 350 เว็บไซต์

2) วันที่ 30 เมษายน 2553 ปิดกั้นเว็บไซต์ที่เข้าข่ายปลุกระดม 420 เว็บไซต์

3) วันที่ 8 พฤษภาคม 2553 ปิดกั้นเว็บไซต์ที่เข้าข่ายปลุกระดม 612 เว็บไซต์

4) วันที่ 17 พฤษภาคม 2553 ปิดกั้นเว็บไซต์ที่เข้าข่ายปลุกระดม 770 เว็บไซต์

4.4.4 มีหน่วยงานภาครัฐหลายหน่วยงานที่ถูกตั้งขึ้นเพื่อตรวจสอบ และปิดกั้นเว็บไซต์

เดือนกันยายน 2553 มีการจัดสัมมนาเรื่อง “การบูรณาการการตรวจสอบ และดำเนินการปิดกั้นเว็บไซต์ที่ไม่เหมาะสม และผิดกฎหมาย” เพื่อสะท้อนปัญหาเกี่ยวกับการดำเนินการตรวจสอบและตามปิดกั้นการเข้า

ถึงเว็บไซต์ที่ไม่เหมาะสมของหน่วยงานที่เกี่ยวข้องทั้งหลาย ไม่ว่าจะเป็นกระทรวงไอซีที กรมสอบสวนคดีพิเศษ รวมทั้งสำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.) ซึ่งปัญหาหลักที่เกิดขึ้นคือ ขาดการประสานงานที่ดี ทั้งไม่มีการส่งข้อมูลการปิดกั้นเว็บไซต์ของกระทรวงไอซีทีให้หน่วยงานอื่น ยังผลให้การควบคุมเนื้อหาในสื่อออนไลน์ไม่เป็นไปอย่างบูรณาการ เช่น เมื่อ กทช. ไม่ได้รับการรายงานการปิดกั้นเว็บไซต์จากกระทรวงไอซีที ก็ไม่สามารถใช้อำนาจทางการปกครองเพื่อกำกับดูแลหรือลงโทษผู้ประกอบการด้วยการสั่งพัก สั่งถอน หรือไม่ต่อใบอนุญาตการให้บริการได้ เป็นต้น โดย ร.ต.หญิง ระนองรักษ์ แสดงทัศนะในงานว่า

"ลำพังไอซีทีทำงานปิดเว็บไซต์คนเดียวไม่ได้ เพราะต้องมีหลายหน่วยงานมาช่วยกัน โดยเฉพาะเว็บไซต์ที่ไม่เหมาะสมที่กระจายอยู่บนโลกอินเทอร์เน็ตอย่างรวดเร็ว รวมถึงเว็บไซต์ที่บ่อนทำลายความมั่นคงประเทศ ไม่ว่าจะเป็นชาติ ศาสน์ กษัตริย์ ดังนั้นทุกฝ่ายต้องช่วยกันอย่างเข้มข้น" [52]

จากปัญหาที่ถูกสะท้อนในงานสัมมนาดังกล่าว เป็นผลทำให้หน่วยงานความมั่นคงต่างๆ โดยเฉพาะอย่างยิ่ง ฝ่ายทหารและกองทัพเห็นความไม่มีประสิทธิภาพในการปราบปรามเว็บไซต์ที่มีเนื้อหาไม่เหมาะสมหรือเนื้อหาที่กระทบต่อความมั่นคงและหมิ่นพระบรมเดชานุภาพ วันที่ 25 กันยายน 2552 พล.อ. ประวิตร วงษ์สุวรรณ รัฐมนตรีว่าการกระทรวงกลาโหม จึงกล่าวถึงเรื่องนี้ในการประชุมสภากลาโหม และสั่งให้กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.) และเหล่าทัพร่วมมือกับกระทรวงไอซีทีในการกวาดล้างเว็บไซต์ที่มีเนื้อหาหมิ่นพระบรมเดชานุภาพ ในขณะที่หน่วยงานตำรวจมีฝ่ายที่รับผิดชอบโดยเฉพาะ คือ สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ (สทส.) ทำให้ในที่สุดแล้วในช่วงระยะเวลาการดำรงตำแหน่งของ ร.ต.หญิง ระนองรักษ์ เกิดหน่วยงานจำนวนมากทั้งจากกระทรวงไอซีที ทหาร ตำรวจเข้ามาทำหน้าที่เฝ้าระวัง ตรวจสอบ และร่วมกันดำเนินการปิดกั้นเนื้อหาบนสื่อออนไลน์

4.4.5 โครงการติดตั้งระบบดักจับข้อมูลบนเครือข่ายอินเทอร์เน็ต (sniffer) เพื่อป้องกันการละเมิดทรัพย์สินทางปัญญา

ในสมัยของ ร.ต.หญิง ระนองรักษ์ นอกจากภารกิจในการตรวจสอบปิดกั้นข้อมูลที่มีเนื้อหาเป็นความผิดตามกฎหมายอาญา และ พ.ร.บ.คอมพิวเตอร์ฯ 2550 แล้ว เนื่องจากในช่วงเวลานั้นประเทศต่างๆ ในซีกโลกตะวันตกกำลังให้ความสำคัญอย่างมากกับการป้องกันการละเมิดทรัพย์สินทางปัญญาที่กระทำบนเครือข่ายอินเทอร์เน็ตโดยอาศัยโปรแกรมแชร์ไฟล์ (file-sharing) เพื่อแสดงถึงความตื่นตัวต่อการแก้ไขปัญหาดังกล่าวเช่นกัน "คณะทำงานปราบคอนเทนท์เถื่อนบนอินเทอร์เน็ต" ในสังกัดกระทรวงไอซีที จึงมีมติเสนอให้ประเทศไทยใช้วิธีติดตั้งระบบดักจับข้อมูลบนเครือข่ายคอมพิวเตอร์ หรือ sniffer เพื่อประโยชน์ในการป้องกันการละเมิดทรัพย์สินทางปัญญา[53] โดยให้เหตุผลว่าประเทศสหรัฐอเมริกาก็ใช้วิธีการนี้ และทั้งผู้ให้บริการโทรคมนาคมก็ใช้เครื่องมือดังกล่าวเป็นปกติอยู่แล้ว จึงควรกำหนดเพิ่มหน้าที่แก่ผู้ให้บริการอินเทอร์เน็ตให้ติดตั้งเครื่องมือดังกล่าวไว้ที่เกตเวย์ เพื่อใช้ดักรับข้อมูลของผู้ใช้บริการอินเทอร์เน็ตทุกรายที่วิ่งไปมาอยู่บนระบบ (traffic) และตรวจสอบว่าลูกค้ารายใดบ้างที่ใช้ผลงานอันละเมิดลิขสิทธิ์

คณะทำงานฯ ดังกล่าวอ้างว่า การกำหนดมาตรการเช่นนี้ ถือเป็นการแก้ปัญหาที่ต้นเหตุ เพราะใช้วิธีเฝ้าระวังและป้องกันการกระทำความผิดไว้ก่อน แทนที่จะใช้เพียงมาตรการตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งจะนำมาใช้ได้ก็ต่อเมื่อเกิดการกระทำความผิดขึ้นแล้วเท่านั้น อันเป็นการแก้ปัญหาที่ปลายเหตุแล้ว อย่างไรก็ตาม ทันทีที่ข่าวนโยบายดังกล่าวแพร่กระจายออกไป ผู้ใช้บริการอินเทอร์เน็ตต่างแสดงความไม่เห็นด้วยและคัดค้านนโยบายนี้ เนื่องจากเห็นว่าเป็นวิธีการที่ละเมิดความเป็นส่วนตัวของประชาชนแบบเหมารวมและเกินกว่าเหตุ เพราะโดยปกติแล้วเครื่องมือ sniffer สามารถดักรับได้ทั้งข้อมูลจราจรคอมพิวเตอร์ หรือ log file และตัวเนื้อหา (content) ของข้อมูลนั้น อีกทั้งต้นทุนของผู้ประกอบการอาจสูงขึ้นจนมีการผลักภาระไปยังผู้บริโภคทำให้ต้องจ่ายค่าบริการแพงขึ้น นอกจากนี้

หากมีการนำข้อมูลที่ดักเก็บไว้ดังกล่าวไปใช้ในทางที่มิชอบ ย่อมเกิดผลเสียต่อผู้ใช้บริการอินเทอร์เน็ตได้ เช่น ข้อมูลส่วนบุคคลประเภทต่างๆ ถูกขายต่อให้ผู้ประกอบธุรกิจเพื่อดูพฤติกรรมการบริโภคและส่งจดหมายอิเล็กทรอนิกส์ไม่พึงประสงค์ (spam-mail) เพื่อโฆษณาสินค้า หรือกระทั่งอาจเกิดกรณีที่รัฐฉวยโอกาสใช้ข้อมูลเพื่อคอยติดตามตรวจสอบพฤติกรรมและสอดส่องความคิดเห็นของประชาชนในเรื่องอื่นๆ ที่ไม่เกี่ยวกับการละเมิดลิขสิทธิ์ โดยเฉพาะอย่างยิ่ง ความคิดเห็นในทางการเมืองการปกครอง เป็นต้น ซึ่งกรณีหลังนี้ได้เคยเกิดขึ้นไปบ้างแล้วในต่างประเทศ และจากข้อเท็จจริงที่ปรากฏ ก็ดูเหมือนว่า ในที่สุดแล้ว นโยบาย sniffer ของประเทศไทยก็หาได้มีเป้าหมายเพียงเพื่อป้องกันการละเมิดทรัพย์สินทางปัญญาแต่เพียงเท่านั้นไม่ แต่ยังมีเป้าหมายเพื่อการตรวจสอบข้อมูลที่อาจเข้าข่ายเป็นความผิดต่อความมั่นคงหรือในเรื่องอื่นๆ รวมทั้งเพื่อจับตาพฤติกรรมของผู้ใช้อินเทอร์เน็ตโดยรวมอีกด้วย ดังที่นายอาจิน จิรชีพพัฒนา ผู้อำนวยการสำนักส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเป็นผู้รับนโยบายดังกล่าวมาผลักดัน กล่าวถึงคนที่คัดค้านนโยบายนี้ว่า

“สำหรับกลุ่มผู้คัดค้านก็ต้องถามกลับไปถามว่า พวกเขาคัดค้านอะไร กรณีการดำเนินการของรัฐบาลครั้งนี้ต้องการสร้างความสงบสุขบนสังคมอินเทอร์เน็ต และเป็นเกราะป้องกันเยาวชนให้พ้นจากภัยที่มากับอินเทอร์เน็ต การทำหน้าที่ของรัฐครั้งนี้เปรียบเสมือนการทำงานของเจ้าหน้าที่ตรวจคนเข้าเมือง คนที่ผ่านไปมาต้องยอมเสียความเป็นส่วนตัวบ้างเพื่อความปลอดภัย ความสงบสุขของประเทศ และการเฝ้าระวังการใช้งานบนเครือข่ายนี้ก็ดูแลโดยรัฐ...” [54]

4.4.6 บทสรุป และวิเคราะห์

นโยบายและแนวปฏิบัติในสมัยของ ร.ต.หญิง ระนองรักษ์ ชัดเจนตั้งแต่แรกเข้ารับตำแหน่งแล้วว่าเน้นหนักที่การกวาดล้างเว็บไซต์ที่มีเนื้อหาไม่เหมาะสม ประกอบกับมีสถานการณ์การชุมนุมประท้วงทางการเมืองทำให้มีเว็บไซต์ถูกปิดกั้นในช่วงเวลาดังกล่าวเป็นจำนวนมากเมื่อเปรียบ

เทียบกับรัฐมนตรีคนก่อนหน้า โดยเว็บไซต์ส่วนใหญ่เป็นเว็บที่มีเนื้อหาเกี่ยวกับการเมือง หรือ “ไม่เหมาะสม” ด้วยประการอื่นใด หลายกรณีไม่แน่ชัดว่าผิดกฎหมายหรือไม่ อย่างไร (เนื่องจากไม่มีการฟ้องร้องดำเนินคดีกับผู้เป็นเจ้าของเว็บไซต์เหล่านั้น) ในขณะที่ภาครัฐเองก็ไม่สามารถให้ความหมายของคำว่า “กระทบต่อความมั่นคง” ตามความแห่ง พ.ร.บ.คอมพิวเตอร์ฯ 2550 ได้ชัดเจน ทำให้เกิดกระแสวิพากษ์วิจารณ์ถึงสถานการณ์การละเมิดสิทธิและเสรีภาพของประชาชนในการเข้าถึงข้อมูลข่าวสาร อย่างไรก็ตาม ต้องไม่ลืมว่าช่วงเวลาดังกล่าวอยู่ภายใต้การประกาศสถานการณ์ฉุกเฉินซึ่งทำให้รัฐมีอำนาจตามกฎหมายพิเศษ คือ พ.ร.ก. การบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 ทำให้การปิดกั้นการเข้าถึงเว็บไซต์โดยรัฐทำได้สะดวกและรวดเร็วกว่าช่วงเวลาปกติ เนื่องจากไม่จำเป็นต้องขอคำสั่งศาลเหมือนกับที่ระบุไว้ในมาตรา 20 พ.ร.บ. คอมพิวเตอร์ฯ 2550

ทิศทางของนโยบายและแนวปฏิบัติของฝ่ายรัฐที่มีต่อสิทธิการเข้าถึงข้อมูลข่าวสารและการแสดงความคิดเห็นบนสื่อออนไลน์นั้น มีแต่จะเข้มงวดมากขึ้นเรื่อยๆ โดยมีการทุ่มเทงบประมาณและบุคลากรจำนวนมากจากหลายหน่วยงานทั้งไอซีที ตำรวจ ตำรวจพิเศษ (ดีเอสไอ) ไปจนถึงทหาร เพื่อเฝ้าระวังและตรวจสอบเนื้อหาออนไลน์ รวมทั้งสอดส่องพฤติกรรมและแนวคิดของผู้ใช้บริการอินเทอร์เน็ต แม้ในหลายๆ กรณีจะหมิ่นเหม่ต่อการละเมิดสิทธิและเสรีภาพของประชาชนจนเกินกว่าเหตุ ก็กลับไม่พบข้อเท็จจริงใดๆ ที่แสดงให้เห็นว่าหน่วยงานรัฐได้คำนึงถึง หรือให้ความสำคัญในประเด็นดังกล่าวด้วย ทั้งนี้ เหตุผลหลักๆ ที่รัฐอ้างถึงเพื่อปิดกั้นเว็บไซต์ตั้งหน่วยงานเฉพาะ และทุ่มเทงบประมาณ ก็คือ ขัดต่อความมั่นคง และหมิ่นประมาทพระมหากษัตริย์

4.5 นโยบายและแนวปฏิบัติในช่วงที่ นายจุติ ไกรฤกษ์ เป็นรัฐมนตรีว่าการกระทรวงไอซีที (6 มิถุนายน พ.ศ. 2553 ถึง 9 สิงหาคม 2554)

4.5.1. ข้อมูลเบื้องต้น

นายจุติ ไกรฤกษ์ รับตำแหน่งรัฐมนตรีว่าการกระทรวงไอซีทีแทน ร.ต.หญิง ระนองรักษ์ สุวรรณฉวี ซึ่งถูกปรับออกจากคณะรัฐมนตรี โดยมีข้อสังเกตว่าในช่วงที่ ร.ต.หญิง ระนองรักษ์ ยังดำรงตำแหน่งอยู่ นายจุติในฐานะสมาชิกสภาผู้แทนราษฎร เคยยื่นกระทู้ถาม ร.ต.หญิง ระนองรักษ์ ต่อประธานสภาผู้แทนราษฎรว่ากระทรวงไอซีทีจะจัดการเด็ดขาดกับเว็บไซต์หมิ่นสถาบันพระมหากษัตริย์อย่างไร และใช้สิ่งใดเป็นตัวชี้วัดถึงผลสำเร็จของการดำเนินการ โดยเมื่อเข้ารับตำแหน่งนายจุติก็ได้ยืนยันเป้าหมายของการดำเนินการกับเว็บไซต์ดังกล่าวในงานแถลงการณ์ดำเนินงานว่า การเข้ารับตำแหน่งรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารครั้งนี้ นายกรัฐมนตรีได้ฝากให้นายจุติดูแลในสี่เรื่องด้วยกัน คือ 1) ความสุจริต 2) การผลักดันธุรกรรมทางอิเล็กทรอนิกส์ 3) การจัดการเว็บไซต์ที่กระทบต่อความมั่นคงและสถาบันฯ และ 4) ปัญหาสัญญาสัมปทานดาวเทียมไทยคม ทั้งกล่าวด้วยว่า จะดำเนินการจัดตั้งกลุ่มอาสาสมัครเยาวชนภายใต้ชื่อ “ลูกเสือบนเครือข่ายอินเทอร์เน็ต” (cyber scout) เพื่อเฝ้าระวังและสอดส่องดูแลข้อมูลข่าวสารที่เป็นภัยต่อสถาบันพระมหากษัตริย์และความมั่นคงของประเทศ[55]

หลังรับตำแหน่งเพียงหนึ่งสัปดาห์นายจุติ แสดงผลการทำงานด้วยการปิดกั้นเว็บไซต์พนันฟุตบอลไปกว่า 246 ยูอาร์แอล จากนั้นก็ปิดกั้นเว็บไซต์ที่อาจเข้าข่ายหมิ่นประมาทพระมหากษัตริย์ไปอีกราว 43,000 ยูอาร์แอล ภายในสัปดาห์ที่สอง[56] ซึ่งมากกว่าจำนวนเว็บไซต์ที่ถูกปิดกั้นไปตลอดระยะเวลาการดำรงตำแหน่งของ ร.ต.หญิง ระนองรักษ์ ถึงสองเท่า นอกจากนี้ยังมีการทำบันทึกข้อตกลงความร่วมมือ (MOU) ระหว่างสามกระทรวง คือ กระทรวงไอซีที กระทรวงยุติธรรม และกระทรวงวัฒนธรรม เพื่อป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศอีกด้วย[57]

4.5.2 โครงการสร้างลูกเสือบนเครือข่ายอินเทอร์เน็ต (cyber scout)

โครงการ cyber scout อยู่ในความรับผิดชอบของกระทรวงไอซีที แต่เป็นไปตามแผนพัฒนาลูกเสือไทยของกระทรวงศึกษาธิการ โดยเบื้องต้นวางเป้าหมายรับอาสาสมัคร Cyber Scout จำนวน 200 คน และจะขยายเป็น 1 แสนคนให้ได้ภายในสิ้นปี 2553 จากกลุ่มนักเรียน นิสิต นักศึกษา ครู อาจารย์ ตัวแทนภาครัฐ ภาคเอกชนที่มีความรู้ความสามารถใช้งานคอมพิวเตอร์และอินเทอร์เน็ตได้ดี ให้เข้าร่วมอบรมคุณธรรม จริยธรรม เทคนิค กฎหมายจากเจ้าหน้าที่และผู้เชี่ยวชาญ โดยหวังให้เยาวชนเป็นเครือข่ายเฝ้าระวังการกระทำความผิด และข้อมูลที่มีเนื้อหาไม่เหมาะสม หรือเป็นภัยต่อสถาบันฯ และความมั่นคงของประเทศ นายอภิสิทธิ์ เวชชาชีวะ นายกรัฐมนตรีในขณะนั้น กล่าวถึงโครงการดังกล่าวว่า

"...การจัดทำโครงการสร้างลูกเสือบนเครือข่ายอินเทอร์เน็ต หรือ cyber scout นี้ ถือเป็นก้าวแรกที่สำคัญ และเป็นจุดเริ่มต้นในการสร้างกลุ่มสังคมออนไลน์ที่มีจิตสำนึกในจริยธรรม คุณธรรม เพื่อให้เป็นแบบอย่างแก่เครือข่ายทางสังคมในการส่งเสริมการใช้งานอินเทอร์เน็ตอย่างเหมาะสม โดยร่วมกันช่วยสอดส่องดูแลภัยอันตรายและเฝ้าระวังข้อมูลข่าวสารที่เป็นภัยต่อสถาบัน.."

ในขณะที่ในงานเดียวกันนายจุติ กล่าวว่า

"เพื่อเป็นการสำนึกในพระมหากรุณาธิคุณ รวมทั้งถวายความจงรักภักดีแด่พระบาทสมเด็จพระเจ้าอยู่หัวภูมิพลอดุลยเดช กระทรวงฯ จึงได้จัดทำโครงการสร้างลูกเสือบนเครือข่ายอินเทอร์เน็ตนี้ขึ้น เพื่อสร้างอาสาสมัคร cyber scout ที่มีจิตสำนึกในด้านจริยธรรม คุณธรรม ให้เป็นเครือข่ายทางสังคมในการส่งเสริมการใช้งานอินเทอร์เน็ตอย่างปลอดภัย โดยอาสาสมัคร cyber scout เหล่านี้จะทำหน้าที่เฝ้าระวังข้อมูลหรือพฤติกรรมที่เป็นภัยต่อประเทศด้วยเทคโนโลยีสารสนเทศ...." [58]

จะเห็นได้ว่าโครงการดังกล่าวไม่ได้มีขึ้นเพื่อสร้างภูมิคุ้มกันและความรู้เท่าทันการบริโภคข้อมูลประเภทต่างๆ ในสื่อออนไลน์ให้กับเด็กและเยาวชน หรือประชาชนทั่วไปเท่านั้น แต่รัฐยังมีวัตถุประสงค์ตั้งโครงการนี้ขึ้นเพื่อช่วยอุดช่องว่างในการปฏิบัติงานของเจ้าหน้าที่รัฐด้วย ที่ปัจจุบันไม่สามารถป้องกันและปราบปรามเว็บไซต์ที่มีเนื้อหากระทบต่อความมั่นคง โดยเฉพาะอย่างยิ่งเว็บไซต์ที่ภาครัฐมองว่ามีเนื้อหาที่อาจเข้าข่ายหมิ่นสถาบันฯ ได้อย่างทั่วถึง วัตถุประสงค์ดังกล่าวสะท้อนออกมาจากคำกล่าวของทั้งนายอภิสิทธิ์ และนายจุติเอง ที่ต้องการให้มีหน่วยงานภาคประชาชน รวมทั้งเด็กและเยาวชนเข้ามาคอยสืบค้น และตรวจสอบเนื้อหา รวมทั้งประสานความร่วมมือกับภาครัฐในการปราบปรามเว็บไซต์เป้าหมาย

4.5.3 บันทึกข้อตกลงความร่วมมือ (MOU) ระหว่างกระทรวงไอซีที กระทรวงยุติธรรม และกระทรวงวัฒนธรรม

วันที่ 17 มิถุนายน 2553 กระทรวงไอซีทีโดยนายจุติ ลงนามบันทึกข้อตกลงความร่วมมือ กับกระทรวงยุติธรรมโดยนายพีระพันธุ์ สาลีรัฐวิภาค และกระทรวงวัฒนธรรมโดยนายนิพิฏฐ์ อินทรสมบัติ เพื่อป้องกันและปราบปรามการกระทำความผิดทางสื่อเทคโนโลยีสารสนเทศ โดยนอกจากความร่วมมือในการรักษาความปลอดภัยระบบข้อมูลของรัฐแล้ว ภารกิจสำคัญอีกประการหนึ่งก็คือ เร่งปราบปรามธุรกิจ หรือการกระทำที่ผิดกฎหมาย รวมทั้งตรวจสอบเว็บไซต์ที่ไม่เหมาะสมทั้งหมดโดยจะใช้งบประมาณดำเนินงานจากปี 2553 จำนวน 127 ล้านบาท นายพีระพันธุ์ สาลีรัฐวิภาค รัฐมนตรีว่าการกระทรวงยุติธรรม กล่าวถึงเรื่องนี้ว่า

“ภายใน 3 เดือน จะเร่งขอความร่วมมือไปยังหน่วยงานภาครัฐที่ให้บริการอินเทอร์เน็ตก่อน เพื่อให้ปิดกั้นเว็บไซต์ไม่เหมาะสม โดยเฉพาะเว็บไซต์หมิ่นสถาบันพระมหากษัตริย์ ที่จะต้องปิดกั้นทุกช่องทางไม่ให้เกิดขึ้น และหลังจากนั้นจะขอความร่วมมือไปยังผู้ให้บริการอินเทอร์เน็ตของเอกชน”

นอกจากการแต่งตั้งพนักงานเจ้าหน้าที่เฉพาะเพื่อปฏิบัติงานแล้ว การเซ็นสัญญาความร่วมมือครั้งนี้ ยังสนับสนุนให้รับอาสาสมัครเข้ามาช่วยคัดกรอง และรวบรวมข้อมูลเบื้องต้นที่เกี่ยวข้องกับเรื่องผิดกฎหมาย กระทบต่อสถาบันหลักของชาติ สื่อลามกอนาจาร การพนันออนไลน์ ยาเสพติด อาหาร ยา และอื่นๆ เพื่อส่งให้กระทรวงไอซีทีดำเนินการต่อไป

4.5.4 จัดระเบียบการหาเสียงผ่านเครือข่ายสังคมออนไลน์

ในขณะที่ประเทศสหรัฐอเมริกา ประเทศต่างๆ ในทวีปยุโรป รวมทั้งประเทศเพื่อนบ้านอย่างสิงคโปร์[59] ต่างให้เสรีภาพกับพรรคการเมืองและนักการเมืองในการใช้เทคโนโลยีสารสนเทศ หรือเครือข่ายสังคมออนไลน์ อย่างเฟซบุค หรือทวิตเตอร์ เป็นเครื่องมือในการหาเสียงเลือกตั้งและสื่อสารนโยบายกับประชาชน แต่สำหรับประเทศไทยแล้ว เรื่องดังกล่าวเป็นสิ่งที่รัฐจับตาอย่างเข้มงวด ถูกจัดระเบียบ หรือกระทั่งอาจถูกกลั่นกรองเนื้อหาก่อนเผยแพร่ต่อสาธารณชนได้ โดยก่อนมีการเลือกตั้งสมาชิกสภาผู้แทนราษฎรในวันที่ 3 กรกฎาคม 2554 กระทรวงไอซีทีและสำนักงานคณะกรรมการการเลือกตั้ง (กกต.) ได้หารือร่วมกันในประเด็นนี้ นางจีราวรรณ บุญเพิ่ม ปลัดกระทรวงไอซีทีในสมัยที่นายจุติเป็นรัฐมนตรี แสดงความคิดเห็นว่า

“ขณะนี้อยู่ระหว่างหารือกับ กกต. เพื่อเชิญเว็บมาสเตอร์เว็บโฮสติ้ง ผู้ให้บริการอินเทอร์เน็ต มาหารือเพื่อกำหนดแนวทางในการกลั่นกรองข้อมูลก่อนนำเสนอ เช่น มีการโพสต์แสดงความคิดเห็นในเว็บไซต์ต่างๆ อาจมีการคัดกรองก่อนนำเสนอ...” [60]

สำหรับการควบคุมดูแลการใช้เครือข่ายออนไลน์ของพรรคการเมือง หรือนักการเมืองในการหาเสียงนั้น กระทรวงไอซีทีจะใช้อำนาจต่างๆ ตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งแม้ว่าในท้ายที่สุดการหาเสียงผ่านเครือข่ายสังคมออนไลน์จะไม่ต้องห้ามตามกฎหมายฉบับใดเลยไม่ว่าจะเป็น พ.ร.บ.คอมพิวเตอร์ฯ 2550 หรือพ.ร.ฎ.เลือกตั้ง แต่ กกต. โดยคำ

แนะนำของกระทรวงไอซีที ก็ได้มอบนโยบายกับผู้สมัครและพรรคการเมืองว่า “ห้ามหาเสียงผ่านสื่ออิเล็กทรอนิกส์หลังเวลา 18.00 น. ก่อนวันเลือกตั้ง” โดยจะมีการตั้งทีมงานด้านเทคนิคเพื่อตรวจสอบการกระทำที่ฝ่าฝืนด้วย[61]

4.5.5 ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...

ผลงานชิ้นปิดท้ายก่อนลงจากตำแหน่งของนายจุติ ซึ่งถูกคนแวดวงไอทีวิพากษ์วิจารณ์ กระทั่งประท้วงคัดค้านมากที่สุดเรื่องหนึ่ง ก็คือ การพยายามผลักดันร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... ที่ออกมาเพื่อยกเลิก พ.ร.บ. คอมพิวเตอร์ฯ 2550 เข้าสู่การพิจารณาในสมัยรัฐบาลนายอภิสิทธิ์ เวชาชีวะ อย่างเร่งรีบ โดยขาดการมีส่วนร่วมของประชาชนอย่างกว้างขวางเพียงพอ[62] ทั้งๆ ที่ในร่างกฎหมายฉบับใหม่มีบทบัญญัติกำหนดฐานความผิดใหม่ และหน่วยงานใหม่เพิ่มขึ้นหลายมาตราซึ่งน่าจะส่งผลกระทบโดยตรงต่อสิทธิและเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน อาทิ การเพิ่มความรับผิดต่อเนื้อหาให้กับผู้ดูแลระบบ กำหนดให้เพียงแค่การทำสำเนาข้อมูลของผู้อื่นเป็นความผิด หรือการกำหนดให้มีคณะกรรมการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และให้อำนาจอย่างกว้างขวางแต่มีสัดส่วนกรรมการที่มาจากภาครัฐและหน่วยงานความมั่นคงเป็นส่วนใหญ่ เป็นต้น[63] อย่างไรก็ดี ด้วยเหตุผลหลายประการทำให้การเสนอร่างกฎหมายฉบับดังกล่าวเข้าสู่การพิจารณาของคณะรัฐมนตรีถูกชะลอออกไป[64]

4.5.6 บทสรุป และวิเคราะห์

กล่าวได้ว่า นโยบายรัฐที่เกี่ยวกับเสรีภาพในสื่อออนไลน์ในสมัยที่นายจุติ ไกรฤกษ์ เป็นรัฐมนตรีว่าการกระทรวงไอซีที ไม่ได้เปลี่ยนแปลงไปจากนโยบายของรัฐมนตรีคนก่อนๆ เลย โดยเฉพาะอย่างยิ่ง การขับเน้นการดำเนินการปิดกั้นเว็บไซต์ทั้งที่ผิดกฎหมายและแค่เพียงไม่เหมาะสม

ทั้งนี้ เป็นที่น่าสังเกตว่าแม้ในช่วงเวลาที่นายจุติดำรงตำแหน่งปัญหาความขัดแย้งทางการเมืองได้คลี่คลายลงบ้างแล้วและกำลังเข้าสู่ช่วงของการเลือกตั้งทั่วไป แต่ภายในระยะเวลาอันรวดเร็วภายหลังการเข้ารับตำแหน่งจำนวนเว็บไซต์ที่ถูกปิดกั้นกลับมีจำนวนมากกว่าสมัยของ ร.ต.หญิงระนองรักษ์ เสียอีก โดยเว็บไซต์ส่วนใหญ่มีเนื้อหาที่รัฐมองว่าเข้าข่ายเป็นการหมิ่นประมาทกษัตริย์ฯ อย่างไรก็ดี ข้อเท็จจริงปรากฏว่าจำนวนคดีความในชั้นศาลกลับมีไม่มากเท่ากับจำนวนเว็บไซต์ที่ถูกปิดกั้นไป[65] ปรากฏการณ์ดังกล่าวอาจตีความได้หลายนัย ในทางหนึ่งอาจเป็นปัญหาเรื่องข้อจำกัดของความผิดที่เกิดขึ้นในอินเทอร์เน็ต ซึ่งทำให้การสืบหาตัวผู้กระทำความผิดกระทำได้ยาก แต่ในอีกทางหนึ่งก็คือ รัฐสะดวกใจกับการเลือกใช้มาตรการปิดกั้นแบบเร่งด่วน มากกว่าจะพยายามค้นหาต้นตอเจ้าของเนื้อหาที่รัฐมองว่าเป็นความผิด แต่ไม่ว่าจะด้วยเหตุผลใดก็ตามย่อมก่อให้เกิดคำถามขึ้นในหมู่ประชาชนได้ว่า เว็บไซต์ที่ถูกปิดกั้นไปมีเนื้อหาเป็นความผิดตามกฎหมายฉบับใด หรือกระทั่งเป็นความผิดจริงหรือไม่

ในสมัยของนายจุตินี้ นอกจากงบประมาณจำนวนมหาศาล และบุคคลากรภาครัฐอีกจำนวนมากที่ใช้เพื่อการตรวจสอบ และปิดกั้นข้อมูลต่างๆ ในสื่อออนไลน์แล้ว ยังมีการแสวงหาความร่วมมือจากหน่วยงานอื่นๆ ของรัฐ (ทำข้อตกลงความร่วมมือสามกระทรวง) รวมทั้งจากภาคประชาชน (ลูกเสือไซเบอร์) อย่างชัดเจนและเป็นทางการ เพื่ออุดช่องว่างการปฏิบัติงานหรือช่วยแบ่งเบาภาระของเจ้าพนักงานรัฐอีกด้วย โดยแม้กระทรวงไอซีทีจะพยายามชูให้เห็นว่าความร่วมมือ และโครงการต่างๆ มีขึ้นเพื่อให้ความรู้และแนะนำการป้องกันตัวเองจากการบริโภคสื่อออนไลน์ รวมทั้งช่วยเฝ้าระวังข้อมูลที่มีเนื้อหาผิดกฎหมายทุกๆ เรื่อง แต่จากคำกล่าว และการแสดงความคิดเห็นของทั้งนายจุติเอง และนายอภิสิทธิ์ เวชชาชีวะ นายกรัฐมนตรีกลับสะท้อนว่ารัฐบาลในสมัยนั้นมุ่งเน้นไปที่การปิดกั้นและปราบปรามข้อมูลที่มีเนื้อหาเข้าข่ายหมิ่นสถาบันฯ หรือที่กระทบความมั่นคง ซึ่งย่อมทำให้เกิดคำถามในสังคมขึ้นได้ เพราะในขณะที่จนถึงปัจจุบัน ฝ่ายรัฐเองก็ยังไม่สามารถให้คำนิยามหรือเฉพาะเจาะจงได้ว่าเนื้อหาที่ขัดต่อความมั่นคง

หรือกระทั่งหมิ่นสถาบันฯ มีลักษณะอย่างไร เพียงการวิพากษ์วิจารณ์โดยทั่วไปจะถือเป็นการดูหมิ่น หรือหมิ่นประมาทได้หรือไม่ ซึ่งเหล่านี้ถือว่าเป็นเรื่องที่ยังมีความขัดแย้งทางความคิดในสังคม และการตีความทางกฎหมาย ฉะนั้น การดึงเด็กและเยาวชนเข้ามาทำหน้าที่สอดส่องค้นหา และรายงานให้รัฐดำเนินการปิดกั้นเว็บไซต์ที่มีเนื้อหาดังกล่าว ในท่ามกลางความขัดแย้งทางการเมืองระหว่างรัฐบาลกับประชาชนที่เห็นต่าง จะถือเป็นเรื่องที่เหมาะสมแล้วหรือไม่

และนอกจากนโยบายเร่งรัดการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ให้เข้มงวดยิ่งขึ้นแล้ว แนวคิดในการปรับแก้กฎหมายคอมพิวเตอร์ฉบับดังกล่าว เพื่อเพิ่มเติมผู้ที่ต้องเข้ามาร่วมรับผิดชอบกับเนื้อหา เพื่อเพิ่มอำนาจแก่เจ้าหน้าที่รัฐ หรือเพื่อให้มีกลไกในการปราบปรามการกระทำความผิดที่เกี่ยวกับการเผยแพร่เนื้อหาในเครือข่ายคอมพิวเตอร์ได้มากขึ้น ก็เกิดขึ้นในสมัยของนายจุติเช่นกัน

4.6 นโยบายและแนวปฏิบัติในช่วงที่ น.อ. อนุดิษฐ์ นาครทรรพเป็นรัฐมนตรีว่าการกระทรวงไอซีที (วันที่ 9 สิงหาคม 2554 จนถึงปัจจุบัน)

4.6.1 ข้อมูลเบื้องต้น

นาวาอากาศเอก อนุดิษฐ์ นาครทรรพ พรรคเพื่อไทย (พท.) เข้ารับตำแหน่งเป็นรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร หรือไอซีที ในรัฐบาลของนางสาวยิ่งลักษณ์ ชินวัตร เมื่อวันที่ 9 สิงหาคม 2554 จนถึงปัจจุบัน เคยเป็นเลขานุการ รมว.กลาโหม ที่ปรึกษา รมว.เกษตรและสหกรณ์ ทั้งอาจเป็นรัฐมนตรีว่าการกระทรวงไอซีทีคนแรกที่ใช้บริการต่างๆ ในเครือข่ายสังคมออนไลน์ เช่น เฟซบุค และทวิตเตอร์

สำหรับลักษณะงานในกระทรวงไอซีทีนี้ นอกเหนือจากภารกิจต่อเนื่องที่ น.อ. อนุดิษฐ์ ต้องเร่งสะสาง อาทิ ปัญหาการรักษาวงโคจร

ดาวเทียม สัญญาโทรคมนาคม การประมูลเพื่อติดตั้งโครงข่าย 3 จี ฯลฯ แล้ว การเฝ้าระวัง และคอยปิดกั้นเว็บไซต์ที่มีเนื้อหาเข้าข่ายหมิ่นประมาทกษัตริย์ฯ ยังคงเป็นภารกิจเร่งด่วนสำหรับรัฐบาลชุดนี้

4.6.2 สานต่องานเร่งปราบปรามเว็บหมิ่นประมาทกษัตริย์ฯ

น.อ. อนุดิษฐ์ แถลงนโยบายการดำเนินงานของกระทรวงไอซีทีเมื่อแรกเข้ารับตำแหน่งว่า

"จากนี้ไปจะมีการกำชับให้ข้าราชการ และเจ้าหน้าที่ของกระทรวงในทุกระดับ มีการเข้มงวดมากยิ่งขึ้น ในการกำกับดูแลปราบปรามการกระทำผิด พ.ร.บ.เกี่ยวกับคอมพิวเตอร์และการหมิ่นสถาบันผ่านเว็บไซต์ต่างๆ โดยจะดำเนินการบังคับใช้กฎหมายอย่างเด็ดขาด..." [66]

นอกจากนโยบายในการปิดกั้นเว็บไซต์อย่างเข้มงวดแล้ว ในสมัยนี้ยังมีแนวคิดในการดึงผู้ประกอบการร้านเกมคอมพิวเตอร์เข้ามาทำหน้าที่เฝ้าระวังเนื้อหาผิดกฎหมายอีกด้วย ดังที่ น.อ.อนุดิษฐ์ เคยให้สัมภาษณ์ไว้ครั้งหนึ่งว่า

"รัฐบาลชุดที่แล้วเข้มงวดในการปิดเว็บ หรือบล็อคเว็บหมิ่นต่อสถาบันมากเพียงใด รัฐบาลชุดนี้ไม่ได้ทำน้อยกว่าแน่นอน เพียงแต่ไม่อยากให้ข้อมูล เพราะการปกปิดก็เท่ากับว่าจะยิ่งทำให้คนสนใจเสาะหามาดูให้ได้ ที่ผ่านมาก็ได้เรียกผู้บริหารกระทรวงที่เกี่ยวข้องมาหารือ โดยจะปัดฝุ่นการจัดโครงการร้านเกมขึ้นมาใหม่ ทำงานประสานกับผู้ประกอบการร้านเกมเพื่อให้ช่วยเป็นหูเป็นตา" [67]

ในช่วงเวลาของการทำงานเพียงไม่กี่เดือนของรัฐบาลชุดนี้ ปรากฏว่ากระทรวงไอซีทีได้ขอความร่วมมือไปยังสำนักงานใหญ่เฟซบุค เพื่อให้ปิดหน้าเพจที่หมิ่นประมาทกษัตริย์ฯ ไปกว่า 10,000 ยูอาร์แอล[68] ทั้งยังมีการประกาศเตือนจากกระทรวงไอซีทีเกี่ยวกับการใช้เฟซบุคด้วยว่า ผู้พบเห็นการโพสต์ข้อมูล หรือข้อความที่น่าจะเข้าข่ายหมิ่นสถาบันฯ ไม่ควร กด

แบ่งปัน (Share) กดถูกใจ (Like) หรือแสดงความคิดเห็นต่อข้อความนั้น (Comment) เพราะอาจต้องมีความรับผิดด้วยตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550[69] เนื่องจากกระทรวงไอซีทีเห็นว่าเป็นการเผยแพร่ข้อมูลต่อในทางอ้อม การประกาศเตือนดังกล่าวได้ก่อให้เกิดข้อวิพากษ์วิจารณ์ขึ้นอย่างมากในสังคม ทั้งในแวดวงนักกฎหมาย และนักเทคโนโลยีสารสนเทศว่าเป็นการตีความกฎหมายที่เกินเลยไม่จากบทบัญญัติ ซึ่งย่อมขัดกับ “หลักประกันในทางกฎหมายอาญา” ด้วย

4.6.3 ทัศนะและความคิดเห็นต่อ พ.ร.บ.คอมพิวเตอร์ฯ 2550

น.อ. อนุดิษฐ์ นาครทรรพ ยังกล่าวไว้ว่า

“คงไม่ได้ทันสมัย เพราะว่าออกมาตั้งแต่ปี 2550 ฉะนั้นส่วนที่ยังเป็นช่องว่าง หรือส่วนที่ล้าหลังแล้วก็ควรจะต้องได้รับการปรับปรุงซึ่งกระทรวงทำอยู่ และก็จะเสนอ ครม.เพื่อปรับปรุงเพิ่มเติม”

แม้ น.อ. อนุดิษฐ์ ยืนยันว่าจะบังคับใช้กฎหมายคอมพิวเตอร์ด้วยมาตรฐานเดียวกันทั้งหมด รวมทั้งเห็นว่าการปิดกั้นเว็บไซต์ ไม่สามารถแก้ปัญหาการเผยแพร่ข้อมูลที่มีเนื้อหาผิดกฎหมายได้ เพราะปิดกั้นเท่าไรก็คงไม่หมด แต่สำหรับเว็บไซต์หมิ่นสถาบันฯ นั้น ในทัศนะของ น.อ. อนุดิษฐ์ แล้ว กระทรวงไอซีทีต้องดำเนินการอย่างเข้มงวด เด็ดขาด และควรพิจารณาปิดไปก่อนแบบเร่งด่วน ซึ่งแตกต่างกับการเผยแพร่เนื้อหาในเรื่องอื่นๆ ที่สามารถใช้เวลาพิจารณาเป็นกรณีๆ ไปได้ว่าผิดกฎหมายหรือไม่ เพื่อให้เกิดความถูกต้องชัดเจน นอกจากนี้ รัฐมนตรีว่าการกระทรวงไอซีทีคนปัจจุบัน ยังแสดงความเห็นเกี่ยวกับ เว็บไซต์ที่ถูกปิดกั้นโดยคำสั่งศาล (มาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550) ว่าน่าจะแตกต่างจากการถูกปิดกั้นตาม พ.ร.ก. บริหารราชการในสถานการณ์ฉุกเฉิน 2548 ด้วยว่า

“...ในหน่วยงานที่มาร่วมมือบูรณาการกัน เราเห็นตรงกันว่าการปราบปรามไม่ใช่วิธีที่สามารถแก้ปัญหาได้ คือ ปราบแล้วก็ไม่หมด...เรามีลำดับความสำคัญของแต่ละเรื่องอยู่แล้ว ถ้าเป็นเรื่องเว็บไซต์หมิ่นสถาบันฯ

เรื่องนี้ก็ต้องดำเนินการอย่างเข้มงวด เข้มข้น เด็ดขาด แต่ถ้าเป็นกรณีอื่น เราก็ต้องดูว่าสิ่งที่เกิดขึ้นผิดกฎหมายหรือเปล่า...สำหรับเว็บข่าวบางเว็บที่ถูกปิดกั้นโดย พ.ร.บ. (น่าจะหมายถึง พ.ร.ก. ฉุกเฉินฯ - คณะผู้วิจัย) เมื่อยกเลิก พ.ร.บ. นั้นแล้ว และเขาไม่ได้โดนคำสั่งศาลปิดอีก เขาก็มีสิทธิที่จะไปขอเปิด...เพราะเว็บที่ถูกปิดในช่วงนั้นมาจากการแสดงความเห็นต่างทางการเมือง ซึ่งต่างจากเว็บหมิ่นฯ เว็บหมิ่น ศาลจะเป็นผู้สั่งปิด ฉะนั้นอย่างไรก็เปิดอีกไม่ได้อยู่แล้ว...[70]"

จะเห็นได้ว่าความคิดเห็นในเรื่องนี้ของ น.อ.อนุดิษฐ์ อาจถูกตั้งคำถามได้ว่าถูกต้องเป็นธรรมหรือไม่ หรือกระทรวงไอซีทีมีนโยบาย และแนวทางในการปฏิบัติตามที่ น.อ. อนุดิษฐ์ กล่าวไว้จริงหรือ เพราะทางที่ถูกต้องแล้ว ไม่ว่าเนื้อหานั้นจะเข้าข่ายเป็นความผิดตามกฎหมายในเรื่องใด รัฐก็ควรพิจารณาให้รอบคอบและเท่าเทียมกันก่อนที่จะปิดกั้น

อย่างไรก็ตาม น.อ. อนุดิษฐ์ ยังไม่ได้กล่าวถึงปัญหาอื่นๆ ของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 โดยตรง ทั้งในแง่เนื้อหาและถ้อยคำที่อาจมีความคลุมเครือไม่ชัดเจน รวมทั้งปัญหาในการใช้การตีความ ทั้งไม่เคยกล่าวถึง "ร่าง พ.ร.บ.คอมพิวเตอร์ฯ พ.ศ. ..." ฉบับที่กระทรวงไอซีทีในสมัยของนายจุติพยายามผลักดันเข้าสู่การพิจารณาของคณะรัฐมนตรีในสมัยของนายอภิสิทธิ์ เวชชาชีวะ เมื่อราวเดือนมีนาคม 2554 ด้วย

4.6.4 นโยบายอื่นๆ ที่เกี่ยวกับเสรีภาพในการรับรู้ข้อมูลข่าวสารของประชาชน

อาจถือเป็นครั้งแรกที่กระทรวงไอซีทีมีนโยบายที่เป็นรูปธรรมในการพยายามกระจายโอกาสในการเข้าถึงอินเทอร์เน็ตของประชาชนไทยให้ทั่วถึงยิ่งขึ้น ไม่ว่าจะเป็นนโยบายฟรี wifi หรือการแจกอุปกรณ์เข้าถึงอินเทอร์เน็ตกับนักเรียน หรือการเชื่อมโยงกับ national information data center หรือศูนย์กลางข้อมูลของชาติ

แม้นโยบายเหล่านี้จะมีถกเถียงถึงประเด็นความเหมาะสมในเรื่อง

งบประมาณ และวัยของนักเรียน รวมทั้งเป็นนโยบายที่ไม่อาจทำให้เป็นจริงได้โดยง่าย หรือไม่แน่ว่าจะบรรลุวัตถุประสงค์การกระจายการเข้าถึงข่าวสารได้จริงหรือไม่ก็ตาม แต่ก็อาจเป็นเครื่องแสดงให้เห็นว่า กระทรวงไอซีทีให้ความสำคัญและคิดนโยบายในเชิงสนับสนุนสิทธิในการเข้าถึงข้อมูลของประชาชนด้วย มิใช่มุ่งแต่การควบคุมตรวจสอบ หรือปิดกั้นข้อมูลผิดกฎหมายหรือไม่เหมาะสมแต่เพียงอย่างเดียว ดังที่ น.อ. อนุดิษฐ์ เคยกล่าวว่า

"เรื่องของ free wi-fi ก็ต้องชัดเจน วันนี้เราบอกได้เลยว่าเราให้บริการ free wi-fi อย่างน้อย 20,000 จุด ก่อนสิ้นปีนี้แน่นอน โมเดลทำเสร็จแล้ว เหลือแต่ตัดสินใจเลือกว่าจะใช้โมเดลไหน เป็นเรื่องที่ทำได้ง่ายสุด เพราะแต่ละโอเปอเรเตอร์มีพื้นที่ให้บริการอยู่แล้ว โดยใช้กองทุน USO ของ กสทช. หรืองบประมาณรัฐ การขยายตรงนี้จะช่วยกระตุ้นอุตสาหกรรมคอนเทนต์ ทั้งสาระและบันเทิงผ่านรูปแบบต่างๆ จะสนับสนุนให้เกิดนักสร้างแอพพลิเคชั่น ช่วยสนับสนุนการให้บริการภาครัฐแก่ประชาชน..."[71]

4.6.5 บทสรุป และวิเคราะห์

แม้ น.อ. อนุดิษฐ์ จะเข้าดำรงตำแหน่งรัฐมนตรีว่าการกระทรวงไอซีทีในรัฐบาลที่มาจากการเลือกตั้งโดยถูกต้องตามระบอบประชาธิปไตย ซึ่งมีนางสาวยิ่งลักษณ์ ชินวัตร เป็นนายกรัฐมนตรี ทั้งเป็นช่วงที่ไม่มีสถานการณ์ความขัดแย้งทางการเมืองที่รุนแรง ซึ่งน่าจะทำให้นโยบายในลักษณะของการจำกัดเสรีภาพในการแสดงความผิดเห็นบนสื่อออนไลน์ลดน้อยลงกว่ายุคสมัยอื่นๆ แต่การณ์ก็ปรากฏว่าการปิดกั้นเว็บไซต์โดยกระทรวงไอซีทียังคงดำเนินอยู่ต่อไป ซึ่งนอกจากจะอาศัยอำนาจตามมาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550 และคำสั่งศาลเพื่อบังคับใช้กับผู้ให้บริการอินเทอร์เน็ตในประเทศไทยแล้ว ยังได้มีการขอความร่วมมือไปยังผู้ให้บริการอินเทอร์เน็ตในต่างประเทศ เพื่อให้ช่วยปิดกั้นเนื้อหาต่างๆ อีกด้วย

และเนื่องจาก น.อ. อนุดิษฐ์ เป็นรัฐมนตรีไอซีทีที่ใช้บริการรวมทั้งเฝ้ามองบทบาท และความสำคัญของบริการต่างๆ บนอินเทอร์เน็ต

โดยเฉพาะอย่างยิ่ง บทบาทของเครือข่ายสังคมออนไลน์ (แตกต่างจากสมัยของนายจุติ ไกรฤกษ์) ซึ่งได้รับความนิยม และมีอัตราการขยายตัวอย่างมากในหมู่ผู้เล่นชาวไทยจนน่าจะมีอิทธิพลต่อพฤติกรรมและแนวคิดของผู้เล่นในวงกว้าง จึงดูเหมือนว่าพื้นที่แสดงความคิดเห็นประเภทต่าง ๆ ในเครือข่ายสังคมออนไลน์ ไม่ว่าจะเป็นเฟซบุค (Facebook) กูเกิลพลัส (Google+) หรือทวิตเตอร์ (Twitter) กลายเป็นเป้าหมายที่กระทรวงไอซีทีในยุคของ น.อ. อนุดิษฐ์ ให้ความสำคัญ สอดส่องติดตาม รวมทั้งปิดกั้นเนื้อหาด้วย ความพยายามของกระทรวงไอซีทีในการสกัดกั้นเสรีภาพในการแสดงความคิดเห็นในเครือข่ายสังคมออนไลน์ที่เป็นที่วิพากษ์วิจารณ์อย่างมากก็คือ การห้ามผู้เล่นเฟซบุคแสดงความคิดเห็น หรือกดถูกใจ (Like) เนื้อหาของบุคคลอื่น หากเนื้อหานั้นเป็นเนื้อหาที่รัฐเห็นว่าเข้าข่ายหมิ่นประมาทกษัตริย์ฯ โดยให้เหตุผลเพียงว่าถือเป็นการ “เผยแพร่” เนื้อหานั้นทางอ้อม ซึ่งเป็นความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550

อย่างไรก็ตาม คณะผู้วิจัยเห็นว่า คำอธิบายเกี่ยวกับการห้ามแสดงความคิดเห็น หรือกดถูกใจดังกล่าวขาดความครบถ้วน และมีปัญหาในตัวเอง จนอาจมองได้ว่ารัฐกำลังพยายามใช้กฎหมายและโทษทางอาญามาสร้างบรรยากาศแห่งความกลัวให้เกิดขึ้นในหมู่ผู้ใช้บริการเครือข่ายสังคมออนไลน์ ด้วยวิธีการตัดทอนสาระสำคัญที่ว่า โดยหลักแล้ว การกระทำความผิดที่จะมีโทษทางอาญาได้นั้นผู้กระทำต้องกระทำโดย “เจตนา” เท่านั้น หากขาดเจตนาไป ย่อมมิอาจถือว่ากระทำความผิดใด ๆ ได้ การสันนิษฐานไว้ก่อนหรือให้ถือว่าผู้กระทำมี “เจตนา” กระทำความผิด มิอาจเกิดขึ้นได้ในทางอาญา สำหรับเรื่องนี้กรณีที่จะเป็นความผิด ก็คือ ผู้กระทำรู้ว่าเนื้อหาเหล่านั้นเป็นความผิด และประสงค์จะเผยแพร่ต่อไป คำถามก็คือ การแสดงความคิดเห็นหรือชื่นชอบต่อข้อเขียนหนึ่งที่ปรากฏในสื่อสังคมออนไลน์ ซึ่งกระทำกันเป็นปกติวิสัย จะถือโดยอัตโนมัติได้อย่างไรว่าผู้ที่กระทำไปเช่นนั้นในทุก ๆ กรณีมี “เจตนา” เผยแพร่เนื้อหาที่เป็นความผิดไม่ว่าจะโดยตรงหรือโดยอ้อม

ข้อเท็จจริงที่ควรนำมาพิจารณาประกอบการวิเคราะห์ลักษณะการดำเนินนโยบายในสมัยของ น.อ. อนุดิษฐ์ โดยเฉพาะอย่างยิ่งที่เกี่ยวกับการ

ปิดกั้นเว็บไซต์ ก็คือ นักการเมืองฝ่ายค้าน (พรรคประชาธิปัตย์) พยายามเรียกร้อง และกดดันให้กระทรวงไอซีทีจัดการขั้นเด็ดขาดกับเว็บไซต์ เครือข่ายสังคมออนไลน์ กระทั่งเว็บฝากไฟล์วิดีโออย่าง Youtube.com ที่มีเนื้อหาหมิ่นสถาบันฯ มิเช่นนั้นจะถือว่ารัฐบาลชุดนี้ไม่มีความจงรักภักดีหรือสนับสนุนให้ประชาชนหมิ่นสถาบันฯ เสียเอง[72] ข้อเรียกร้องเชิงกล่าวหาดังกล่าวจึงอาจเป็นปัจจัยหนึ่งที่ทำให้ในที่สุดแล้ว กระทรวงไอซีทีในยุคนี้ก็ไม่สามารถดำเนินนโยบายที่เกี่ยวกับการเผยแพร่เนื้อหาที่อาจหมิ่นประมาทกษัตริย์ฯ ในลักษณะอื่นใดได้ นอกจากปิดกั้นอย่างเข้มงวดและรวดเร็วยิ่งขึ้น

อนึ่ง งานวิจัยฉบับนี้คงไม่สามารถวิเคราะห์แนวนโยบายของกระทรวงไอซีทีในสมัยของ น.อ. อนุดิษฐ์ นาครทรรพ ได้ทั้งหมด เนื่องจากในเวลาที่ทำวิจัยยังไม่สิ้นสุดสมัยดังกล่าว

4.7 บทสรุป

จากลักษณะการดำเนินนโยบาย และแนวทางปฏิบัติของรัฐไทยตามที่กล่าวมาทั้งหมด คงเป็นเพียงส่วนหนึ่งเท่านั้นที่สะท้อนให้เห็นทัศนคติของบุคคลากรในภาครัฐที่เกี่ยวกับสิทธิและเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน ซึ่งอาจกล่าวได้ว่า การเฝ้าระวังติดตามตรวจสอบเนื้อหาในสื่อออนไลน์ และการปิดกั้นช่องทางการเข้าถึงข้อมูลเหล่านั้นไม่ว่าโดยวิธีการใดๆ โดยเฉพาะอย่างยิ่ง เนื้อหาที่ขัดต่อความมั่นคงของรัฐ เนื้อหาที่เข้าข่ายความผิดฐานหมิ่นประมาทกษัตริย์ฯ หรือกระทั่งที่มีลักษณะวิพากษ์วิจารณ์สถาบันพระมหากษัตริย์ ซึ่งรัฐมักเห็นว่าเข้าข่ายหมิ่นประมาทกษัตริย์ฯ แล้ว ถือเป็นภารกิจหลักของทุกๆ รัฐบาล โดยไม่สำคัญด้วยว่าประเทศไทยตกอยู่ภายใต้สถานการณ์การเมืองแบบใด ซึ่งบทบัญญัติหลักๆ ที่ใช้ดำเนินการในเรื่องนี้ ก็คือ มาตรา 14, 15 และ 20 พ.ร.บ. คอมพิวเตอร์ฯ 2550 ในสถานการณ์ปกติ และ พ.ร.ก. การบริหารราชการในสถานการณ์ฉุกเฉินฯ 2548 (รวมทั้ง พ.ร.บ.ความมั่นคงฯ และ

พ.ร.บ. กฎอัยการศึก ในพื้นที่สามจังหวัดชายแดนภาคใต้) ในกรณีที่รัฐบาลประกาศสถานการณ์ฉุกเฉิน ทั้งนี้ ในปัจจุบัน นอกจากการติดตามตรวจสอบพฤติกรรมและการแสดงความคิดเห็นของประชาชนในกระดานข่าว กระดานสนทนา และบริการทั่วๆ ไปในอินเทอร์เน็ตแล้ว ยังขยายไปถึงชุมชนต่างๆ ในเครือข่ายสังคมออนไลน์ (social network) กระทั่งมีความพยายามของรัฐที่จะตรวจสอบพื้นที่ส่วนบุคคลอย่างจดหมายอิเล็กทรอนิกส์ และช่องทางอื่นๆ ผ่านการใช้เครื่องมือดักรับข้อมูล (sniffer) ด้วย

เป็นข้อที่ควรต้องทราบด้วยว่า แท้ที่จริงแล้วการใช้มาตรการปิดกั้นการเข้าถึงสื่อออนไลน์โดยรัฐนั้นมีการดำเนินการมาตั้งแต่ก่อนที่ พ.ร.บ.คอมพิวเตอร์ฯ จะมีผลใช้บังคับเมื่อวันที่ 18 กรกฎาคม พ.ศ. 2550 ซึ่งหลายกรณีรัฐทำไปโดยไม่มีกฎหมายฉบับใดให้อำนาจ[73] บางกรณีอาศัยวิธี “ขอความร่วมมือ” จากผู้ให้บริการเป็นรายๆ ยังผลให้ผู้ใช้บริการเข้าเว็บไซต์ที่ต้องการไม่ได้เป็นครั้งๆ ไป ก่อให้เกิดความสงสัยแก่ประชาชนว่าเกิดปัญหาทางเทคนิคหรือว่าถูกใครปิดกั้น อาจกล่าวได้ว่า ประกาศคณะปฏิรูปการปกครองในระบอบประชาธิปไตยฯ (คปค.) ฉบับที่ 5 ที่ออกภายหลังรัฐประหาร 19 กันยายน 2549 คือกฎหมายฉบับแรกที่กำหนดให้อำนาจกระทรวงไอซีทีอย่างชัดเจนในการใช้ดุลพินิจปิดกั้นสื่อทุกประเภทโดยไม่สำคัญว่าประเทศจะตกอยู่ในสถานการณ์ฉุกเฉินหรือไม่ หากกระทรวงไอซีทีพิจารณาแล้วเห็นว่าเป็นข้อมูลหรือเนื้อหาที่ “อาจส่งผลกระทบต่อการปฏิรูปการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข” แม้ประกาศดังกล่าวจะมีอายุการใช้งานเพียงระยะเวลาสั้นๆ เท่านั้นก่อนประกาศใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 แต่กระทรวงไอซีทีซึ่งนายสิทธิชัย โภไคยอุดม เป็นรัฐมนตรีว่าการในขณะนั้น ก็ใช้อำนาจตามประกาศฉบับนี้ปิดกั้นเว็บไซต์อย่างเปิดเผยนับได้เกือบ 20,000 เว็บไซต์ คณะผู้วิจัยเห็นว่า การใช้อำนาจตามประกาศดังกล่าวเพื่อจำกัดเสรีภาพในการรับรู้ข้อมูลข่าวสารและแสดงความคิดเห็นของประชาชน นอกจากมีปัญหาในเรื่องความไม่ชัดเจนของถ้อยคำในตัวประกาศเองว่าการกระทำใดบ้างที่จะถือว่า “ส่งผลกระทบต่อการปฏิรูปการปกครอง” จนทำให้ขอบเขต

การใช้ดุลพินิจโดยหน่วยงานรัฐกว้างขวางมากเกินไปแล้ว ยังอาจถือได้ว่ารัฐอาศัยประกาศฉบับนี้ฉวยโอกาสกำหนด “เหตุผลใหม่” เพิ่มเติม “ข้อยกเว้น” สิทธิเสรีภาพของประชาชนตามที่บัญญัติไว้ในรัฐธรรมนูญด้วย

ในแง่ของเนื้อหาที่ถูกปิดกั้น พบว่าเว็บไซต์ที่ถูกปิดกั้นจำนวนมากรัฐไม่สามารถอธิบายได้โดยชัดเจนว่ามีเนื้อหาผิดกฎหมายฉบับใดและมาตราใด หรือกระทั่งเป็นความผิดจริงหรือไม่ เพราะภายหลังปิดกั้นไม่มีการนำคดีขึ้นสู่การพิจารณาของศาล ในขณะที่ประชาชนไม่สามารถตรวจสอบการใช้อำนาจของรัฐได้ เนื่องจากไม่สามารถเห็นเนื้อหาเหล่านั้นได้แล้ว ข้อสงสัยต่าง ๆ ที่เกิดขึ้นในหมู่ประชาชนผู้ใช้อินเทอร์เน็ตหลายกรณีจึงยังคงไม่มีคำตอบ อาทิ เนื้อหาที่ถูกปิดเป็นเรื่องที่ขัดต่อความมั่นคงหรือทำลายเสถียรภาพของรัฐจริงหรือไม่ หรือเป็นเพียงความคิดเห็นทางการเมืองที่อาจส่งผลกระทบต่อเสถียรภาพของรัฐบาลหรือผู้กุมอำนาจปกครอง เป็นเนื้อหาที่มีความรุนแรงถึงขนาดดูหมิ่น หมิ่นประมาท อาฆาตมาดร้ายพระมหากษัตริย์ฯ จริงหรือไม่ หรือเป็นแค่เพียงการวิพากษ์วิจารณ์โดยสุจริตอันเป็นเรื่องที่ทำได้ในระบอบนิติรัฐ-ประชาธิปไตย เป็นต้น

โดยสรุป หากพิจารณาทั้งจากสถิติการปิดกั้นเว็บไซต์ การจับกุมดำเนินคดีกับผู้ให้และผู้ใช้บริการอินเทอร์เน็ต ปัญหาความคลุมเครือไม่ชัดเจนของ พ.ร.บ. คอมพิวเตอร์ฯ 2550 ประกอบกับปัญหาการใช้การตีความ รวมทั้งแนวโนบายและทัศนคติของผู้ใช้บังคับกฎหมายแล้ว จึงมิควรต้องแปลกใจเลยว่าเหตุใดในปี 2554 ประเทศไทยจึงถูกองค์กร Freedom House[74] จัดอันดับให้อยู่ในกลุ่มประเทศที่ “ไม่มีเสรีภาพในอินเทอร์เน็ตเลย” (“Not Free”) ซึ่งเทียบได้กับประเทศจีน และประเทศพม่า[75]

5. ปฏิกิริยาและความเคลื่อนไหวของประชาชนและภาคสังคมที่มีต่อกฎหมาย และนโยบายแห่งรัฐที่กระทบเสรีภาพในสื่อออนไลน์

5.1 ปฏิกิริยาต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

5.1.1 ปฏิกิริยาต่อ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในชั้นพิจารณาเพื่อเสนอร่างกฎหมาย

ภายหลังการรัฐประหารวันที่ 19 กันยายน 2549 รัฐบาลซึ่งมีพลเอกสุรยุทธ์ จุลานนท์ เป็นนายกรัฐมนตรี ได้ตั้งสมาชิกสภานิติบัญญัติแห่งชาติ ("สนช.") ทำหน้าที่พิจารณาออกกฎหมายโดยมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... เป็นร่างกฎหมายฉบับแรกที่เข้าสู่การพิจารณาขององค์กรดังกล่าวเป็นวาระเร่งด่วนในวันที่ 15 พฤศจิกายน 2549 ในการนี้เองกลุ่มเอกชนภายใต้ชื่อ "กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย" (Freedom Against Censorship Thailand หรือ FACT) เป็นองค์กรแรกๆ ที่จัดทำข้อเสนอยื่นต่อ สนช. โดยเห็นว่า 1) ประเทศไทยไม่ควรออกกฎหมายฉบับนี้ด้วยความเร่งด่วน 2) มีความผิดหลายเรื่องในร่างกฎหมายที่สามารถนำกฎหมายอื่นมาปรับใช้ได้อยู่แล้ว จึงควรพิจารณาทบทวนให้รอบคอบ และ 3) รัฐบาลควรหลีกเลี่ยงการกำกับดูแลอินเทอร์เน็ตที่เข้มงวดเกินไป นอกจากนี้ ยังเรียกร้องให้กฎหมายที่ออกมาต้องมีความชัดเจนไม่คลุมเครืออย่าให้ดุลพินิจกับเจ้าหน้าที่รัฐในการตีความมากเกินไป เพราะอาจเป็นช่องทางให้เกิดการใช้กฎหมายเป็นเครื่องมือในการกดขี่การแสดงความเห็นทางการเมือง และปิดปากผู้ไม่เห็นด้วย

ในแง่ของการบังคับใช้กฎหมาย FCAT เสนอว่า 1) รัฐบาลควรต้องมีความรับผิด และมีความโปร่งใสในการค้นและยึดเครื่องคอมพิวเตอร์ 2) มีเจ้าหน้าที่รัฐอย่างน้อยหนึ่งคนเป็นผู้รับผิดชอบเต็มที่ และ 3) ข้อมูลเกี่ยวกับการใช้อินเทอร์เน็ตของผู้ใช้ทุกรายต้องถือเป็นสมบัติส่วนบุคคลโดยไม่ถูกยึด หรือจัดเก็บโดยรัฐหรือผู้ให้บริการโดยปราศจากหมายศาล เนื่องจากการรับรองว่าข้อมูลเกี่ยวกับการใช้อินเทอร์เน็ตทั้งหมดจะเป็นข้อมูลส่วนบุคคลเท่านั้น คือ เหตุผลหนึ่งที่ผู้ใช้คอมพิวเตอร์ยอมจ่ายค่าอินเทอร์เน็ตรายเดือนให้กับผู้ให้บริการ ทั้งนี้ FACT แสดงความไม่เห็นด้วยอย่างยิ่ง ที่ร่างกฎหมายว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ระบุโทษสำหรับความผิดบางประเภทถึงขั้นประหารชีวิต และจำคุกตลอดชีวิต[76]

5.1.2 ปฏิกิริยาต่อ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ภายหลังประกาศใช้

ภายหลัง พ.ร.บ. คอมพิวเตอร์ฯ 2550 ประกาศใช้ในวันที่ 18 กรกฎาคม 2550 ปรากฏว่ามีภาคประชาชนทั้งที่เห็นด้วย และไม่เห็นด้วยกับกฎหมายฉบับนี้ โดยมีเหตุผลสนับสนุนที่แตกต่างกัน ฝ่ายที่เห็นด้วยเห็นว่า พ.ร.บ.คอมพิวเตอร์ฯ 2550 ทำให้สิทธิส่วนบุคคลได้รับความคุ้มครองมากขึ้น เพราะมีฐานความผิดห้ามไม่ให้เข้าถึง หรือเจาะระบบคอมพิวเตอร์ของผู้อื่นโดยไม่มีอำนาจ หรือสามารถเอาผิดกับการแก้ไขเพิ่มเติมข้อมูลในคอมพิวเตอร์ของผู้อื่นโดยเจ้าของไม่ยินยอมได้ ซึ่งกฎหมายทั่วไปครอบคลุมไปไม่ถึง[77] ในขณะที่ฝ่ายไม่เห็นด้วย เกรงว่าจะเกิดผลกระทบต่อเสรีภาพในการแสดงความคิดเห็น และเสรีภาพในเรื่องอื่นๆ อันเป็นผลมาจากการใช้การตีความกฎหมายของเจ้าหน้าที่รัฐ เพราะถ้อยคำในกฎหมายหลายเรื่องยังคลุมเครือไม่ชัดเจน เช่น การห้ามส่งข้อมูลที่เป็นภาพลามกอนาจาร หรือภาพตัดต่อดัดแปลงที่ก่อให้เกิดความเสื่อมเสียให้กับผู้อื่น โดยเฉพาะอย่างยิ่ง มาตรา 14 ที่บัญญัติไว้ค่อนข้างกว้าง อย่างการห้ามนำเสนอข้อมูลที่กระทบต่อความมั่นคง ซึ่งไม่สามารถให้คำจำกัดความที่ชัดเจนได้ทำให้การตีความไปผูกโยงอยู่กับดุลพินิจ ทัศนคติของผู้ใช้อำนาจ และสถานการณ์การเมืองที่เปลี่ยนแปลงไป เปิดช่องให้เกิดการนำ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ไปใช้ในทางที่มิชอบ หรือเพื่อกลั่นแกล้งกันทางการเมือง[78] นอกจากนี้ ยังมีบทลงโทษหนักกับผู้ให้บริการตามมาตรา 15 ซึ่งส่งผลกระทบต่อพัฒนาการทางเทคโนโลยี และอุตสาหกรรมการให้บริการโทรคมนาคม[79]

ในขณะที่หน่วยงานผู้บังคับใช้กฎหมาย (พ.ต.อ. ศิริพงษ์ ติมุลา ผู้กำกับการศูนย์ตรวจสอบและวิเคราะห์การกระทำผิดทางคอมพิวเตอร์) แสดงความเห็นว่า แม้ประเทศไทยจะมีกฎหมายที่กำหนดฐานความผิดที่เกี่ยวกับคอมพิวเตอร์แล้ว แต่คาดว่าการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จะไม่ลดลง เมื่อเทียบกับเวลาก่อนที่กฎหมายฉบับนี้จะมีผลบังคับใช้ เนื่องจากความก้าวหน้าอย่างรวดเร็วของเทคโนโลยี ประกอบกับปัจจัยภายนอก เช่น ภาวะเศรษฐกิจที่ฝืดเคือง ดังนั้น ประชาชนจึงต้อง

ป้องกันตัวเองจากการกระทำความผิดก่อน โดยรัฐต้องเร่งให้ความรู้เกี่ยวกับกฎหมายฉบับนี้กับประชาชน[80]

5.1.3 ปฏิกิริยาต่อการบังคับใช้ และการดำเนินคดีกับบุคคลตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550

ถือเป็นเรื่องน่าสนใจอย่างยิ่ง เมื่อปรากฏว่าที่ผ่านมา พ.ร.บ. คอมพิวเตอร์ฯ 2550 ถูกนำมาปรับใช้บ่อยครั้งกับคดีเพียงไม่กี่ประเภทเท่านั้น มาตราหลักๆ ที่ถูกบังคับใช้คือ มาตรา 14 และ 15 ความผิดที่ว่าด้วยการเผยแพร่ข้อมูลที่มีเนื้อหาต้องห้ามในสื่อออนไลน์ และความรับผิดของผู้ให้บริหาร อนึ่ง ดังกล่าวไปแล้วว่า ประเด็นที่มักถูกตั้งคำถามและเป็นที่กังวลของฝ่ายประชาชนมาโดยตลอดก็คือ ความไม่ชัดเจนของถ้อยคำและองค์ประกอบความผิดของมาตราดังกล่าวที่เปิดโอกาสให้พนักงานเจ้าหน้าที่ใช้ดุลพินิจในการใช้การตีความได้อย่างกว้างขวาง หลายคดีที่เกิดขึ้นจึงมักถูกประท้วงคัดค้านโดยฝ่ายประชาชนและภาคสังคมอยู่เนืองๆ อาทิเช่น แถลงการณ์กรณีนายณัฐ สัตยาภรณ์พิสุทธิ์[81] และกรณีระหว่างวันที่ 13-15 ตุลาคม ปี 2552 เจ้าหน้าที่จับผู้ต้องหาสามราย คือ แพทย์หญิงทัศพร รัตนวงศา นายคทา ปาจริยพงศ์ และนางสาวธีรนันต์ วิภูชนิน จากกรณีปล่อยข่าวลือในตลาดหลักทรัพย์แห่งประเทศไทยทำให้นักลงทุนจำนวนมากตื่นตระหนกและพากันขายหุ้น[82] จากเหตุการณ์นี้มีกลุ่มประชาชนที่ไม่เห็นด้วย เช่น เครือข่ายพลเมืองเน็ต ซึ่งออกแถลงการณ์เพื่อร้องขอความชัดเจนกรณีใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 จับกุมผู้ใช้เน็ตในเดือนตุลาคม 2552[83] ชุมชนฟ้าเดียวกัน ออกแถลงการณ์ประณามการการจับแพะกรณีทุบหุ้น[84] สมัชชาสังคมก้าวหน้าคัดค้านการใช้กฎหมายฉบับนี้ว่าคุกคามการแสดงความเห็น และการรับรู้ข่าวสารกรณีข่าวทุบหุ้นเดือนตุลาคม 2552 ทั้งยังเรียกร้องผู้รักเสรีภาพให้ออกมาต้าน พ.ร.บ.คอมพิวเตอร์ฯ 2550[85] กระทั่งดีเจประจำคลื่นวิทยุชุมชนคนแท็กซี่ ก็วิพากษ์วิจารณ์ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ว่าเป็นกฎหมายที่สร้างความ

รุนแรงต่อโครงสร้างเสรีภาพและสิทธิทางการเมืองของประชาชน ซึ่งสวนทางกับการพัฒนาระบอบประชาธิปไตย[86]

นอกจากคดีความซึ่งมีผู้ใช้บริการสื่อออนไลน์เป็นจำเลยตามมาตรา 14 อนุมาตราต่าง ๆ ของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 แล้ว คดีความที่มีผู้ให้บริการเป็นจำเลยตามมาตรา 15 ก็ถูกจับตาเช่นเดียวกัน คดีสำคัญก็คือคดีที่มีนางสาวจีรนุช เปรมชัยพร ผู้อำนวยการเว็บไซต์ประชาไทเป็นจำเลย (ศาลมีคำพิพากษาไปแล้วเมื่อวันที่ 30 พฤษภาคม 2555 ให้จำคุก 8 เดือน และปรับ 20,000 บาท แต่ให้รอลงอาญา) ซึ่งมีประชาชน นักวิชาการ ภาคสังคมทั้งในและนอกประเทศหลายองค์กรตั้งคำถามถึงความเหมาะสมของกฎหมายมาตรานี้ ทั้งในส่วนของความผิดและอัตราโทษซึ่งส่งผลกระทบต่อสื่อสารมวลชน หรือผู้ทำหน้าที่เป็นเพียงตัวกลางส่งข่าวสารในสื่อออนไลน์เท่านั้น รวมทั้งมีการประท้วงกระบวนการดำเนินคดีในชั้นศาลด้วย อาทิ เครือข่ายนักกฎหมายสิทธิมนุษยชนออกแถลงการณ์คัดค้านการดำเนินคดีที่ไม่เป็นธรรม[87], เครือข่ายพลเมืองเน็ต ออกแถลงการณ์เรียกร้องให้ ส.ส. พิจารณาแก้ไข พ.ร.บ.คอมพิวเตอร์ฯ 2550 มาตรา 15[88], แอมเนสตี้ อินเตอร์เนชั่นแนล ประเทศไทย เรียกร้องให้ทางการไทยยกฟ้องจีรนุชในทุกข้อกล่าวหา[89], ผู้สื่อข่าวไร้พรมแดน (Reporters without Borders) แถลงเรียกร้องรัฐไทยถอนฟ้องกรณีจีรนุช[90], สมาชิกสภาผู้แทนราษฎรสหราชอาณาจักรจำนวน 11 คนจาก 3 พรรคการเมืองใหญ่ ลงชื่อสนับสนุนกระทู้สั้น (Early Day Motions) ที่เสนอโดย นายทอม วัตสัน (Tom Watson) ส.ส.พรรคแรงงานที่แสดงความเป็นห่วงการดำเนินคดีกับจีรนุชตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550[91], ชมรมนักข่าวเพื่อเสรีภาพประณามกรณีจับ ผอ. ประชาไท เสนอให้ถอนคดีโดยทันที พร้อมทั้งเรียกร้องให้สมาคมด้านสื่อและองค์กรด้านสิทธิมนุษยชน รวมทั้งสภาทนายความอย่าเพิกเฉยต่อกรณีนี้[92] เป็นต้น

นอกจากนี้ ยังมีการจัดสัมมนาพูดคุยในหลายเวทีเพื่อแสดงความคิดเห็นต่อการบังคับใช้กฎหมายและปัญหาของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ด้วย เช่น สมาคมนักข่าวนักหนังสือพิมพ์แห่งประเทศไทยร่วมกับ สถาบัน

อิศราจัดราชดำเนินเสวนาครั้งที่ 17/2551 เรื่อง " พ.ร.บ.คอมพิวเตอร์ปกป้องหรือคุกคาม"[93] และงานสัมมนา "3 ปี การบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 : หลักนิติรัฐกับความรับผิดชอบของภาครัฐ" ซึ่งจัดโดย เครือข่ายพลเมืองเน็ต คณะกรรมการรณรงค์เพื่อการปฏิรูปสื่อ (คปส.) และ Southeast Asia Press Alliance[94] เป็นต้น

5.1.4 ข้อเสนอต่อรัฐบาลเพื่อการแก้ไขปรับปรุงกฎหมาย และการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550

เนื่องจากปัญหาต่างๆ ที่เกิดขึ้นภายหลังประกาศใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งมีทั้งในส่วนถ้อยคำในกฎหมายเองและการใช้การตีความ เป็นผลให้กลุ่มประชาชนและองค์กรต่างๆ ทั้งที่เป็นผู้ได้รับผลกระทบโดยตรงและโดยอ้อม รวมทั้งหน่วยงานผู้บังคับใช้กฎหมายเสนอให้มีการทบทวนหลักการและเหตุผล กระทั่งเสนอแก้ไขปรับปรุงกฎหมายฉบับนี้ ทั้งนี้ เครือข่ายพลเมืองเน็ต เคยแถลงข้อเสนอต่อการใช้กฎหมายเกี่ยวกับคดีทางคอมพิวเตอร์ และอินเทอร์เน็ตในงานเสวนาเรื่อง "กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์: มุมมองจากสากลและหลักปฏิบัติ" มีสาระสำคัญสามประการ คือ 1) เจ้าหน้าที่ควรพยายามจับกุมผู้กระทำไม่ใช่ตัวกลาง 2) ผู้ต้องหาจำเป็นต้องได้รับการปฏิบัติในฐานะผู้บริสุทธิ์ตามสิทธิในรัฐธรรมนูญ และ 3) การกำกับดูแลสื่อออนไลน์ต้องตั้งอยู่บนความเป็นจริงที่เกิดขึ้น[95] นอกจากนี้ นายประสงค์ เลิศรัตนวิสุทธิ์ อดีตนายกสมาคมนักข่าวนักหนังสือพิมพ์แห่งประเทศไทย เคยแสดงความเห็นต่อกฎหมายคอมพิวเตอร์ในเวทีสัมมนา "3 ปี การบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ" ซึ่งจัดโดยเครือข่ายพลเมืองเน็ตว่า มาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ไม่ได้เขียนให้อำนาจศาลสั่งปิดเว็บไซต์ได้ ทำได้เพียงระงับการแสดงข้อมูลเฉพาะในส่วนที่ละเมิดกฎหมายเท่านั้น จึงเสนอว่าน่าจะมีการผลักดันหน่วยงาน เช่น ผู้ตรวจการแผ่นดินของรัฐสภา คณะกรรมการสิทธิมนุษยชน เพื่อฟ้องศาลรัฐธรรมนูญให้ตีความว่าขัดรัฐธรรมนูญหรือไม่[96] วันที่ 5 ตุลาคม 2554 องค์กรภาคประชาชนจัดเวที "บทสรุปการทบทวนสถานการณ์สิทธิ

มนุษยชนไทยในเวทีสหประชาชาติ: ประสบการณ์จากเจนีวา" ซึ่งเป็นงานที่สืบเนื่องมาจากการที่ประเทศไทยต้องจัดทำรายงานสิทธิมนุษยชนของประเทศไทยเพื่อเสนอต่อสภาสิทธิมนุษยชนแห่งสหประชาชาติ และปัญหาที่เกี่ยวกับละเมิดสิทธิโดยอาศัย พ.ร.บ.คอมพิวเตอร์ฯ 2550 ก็ถือเป็นประเด็นหนึ่งที่ได้รับความสนใจในเวทีดังกล่าว[97]

เป็นที่ทราบดีอยู่แล้วว่า อินเทอร์เน็ตเป็นเทคโนโลยีการสื่อสารที่ไร้พรมแดน และไม่เพียงแต่ข้อมูลข่าวสารโดยทั่วๆ ไปเท่านั้นที่ผู้คนจากทั่วโลกสามารถเข้าถึงและรับรู้ได้ แต่กฎเกณฑ์ต่างๆ ที่ถูกนำมาใช้กับสื่อประเภทนี้ โดยเฉพาะอย่างยิ่ง กฎเกณฑ์ที่เคร่งครัดเข้มงวด และมีแนวโน้มที่จะส่งผลกระทบต่อสิทธิเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็น ซึ่งเป็นสิทธิขั้นพื้นฐานที่นานาอารยะประเทศต่างให้ความคุ้มครอง ก็เป็นข้อมูลที่ใครๆ สามารถเข้าถึงได้เช่นกัน ทั้งยังมักถูกจับตามองและนำไปเป็นตัวชี้วัดระดับการให้ความคุ้มครองสิทธิพลเมืองของประเทศนั้นๆ อีกด้วย สำหรับในกรณีของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 นี้ ปรากฏว่าองค์กรผู้สื่อข่าวไร้พรมแดน (Reporters Without Borders) เคยเขียนจดหมายถวายพระบาทสมเด็จพระเจ้าอยู่หัวภูมิพลอดุลยเดช เนื่องในวโรกาสวันเฉลิมพระชนมพรรษาวันที่ 5 ธันวาคม 2552 เพื่อเรียกร้องให้พระราชทานอภัยโทษแก่ผู้ใช้อินเทอร์เน็ตที่กำลังถูกจำคุก หรือถูกดำเนินคดีในข้อหาที่เกี่ยวกับการแสดงความคิดเห็นที่แตกต่างบนอินเทอร์เน็ต[98] ในขณะที่ตัวแทนจากองค์กรฟอรัมเอเชีย เคยให้ข้อมูลแก่คณะมนตรีสิทธิมนุษยชนเรื่องการละเมิดเสรีภาพทางอินเทอร์เน็ตในประเทศไทยซึ่งเกิดจากมาตรการทางกฎหมายที่รุนแรงว่า มาตรา 112 ประมวลกฎหมายอาญา และมาตรา 14 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ถูกนำมาใช้มากขึ้นเพื่อคุกคามและจัดการผู้ใช้อินเทอร์เน็ต ซึ่งกฎหมายเหล่านี้นอกจากจะมีอัตราโทษสูงเกินไป คือ 3-15 ปี แล้ว ยังพบว่าผู้ต้องหาส่วนใหญ่ไม่ได้รับการประกันตัวด้วย และนอกจากการดำเนินคดีกับผู้ใช้และผู้ให้บริการอินเทอร์เน็ตแล้ว รัฐบาลไทยยังปิดกั้นการเข้าถึงเว็บไซต์จำนวนมากโดยไม่เปิดเผยรายชื่อยูอาร์แอล ทั้งไม่มีการแสดงเหตุผลสำหรับการปิดกั้น ข้อเรียกร้องสำคัญที่ตัวแทนฟอรัมเอเชีย

กล่าวไว้ ก็คือ “ตัวกลาง” (ผู้ให้บริการ) ไม่พึงถูกดำเนินคดีด้วยข้อความที่ตนไม่ได้เป็นผู้เขียน และไม่ควรถูกบังคับให้ต้องเซ็นเซอร์เนื้อหาในนามของรัฐ และประเทศไทยควรยกเลิกมาตรา 15 พ.ร.บ.คอมพิวเตอร์ฯ 2550 ซึ่งกำหนดให้ตัวกลางต้องรับผิด[99]

อนึ่ง ข้อเรียกร้องดังกล่าวสอดคล้องกับหลักเกณฑ์การควบคุมอินเทอร์เน็ตของภูมิภาคเอเชียแปซิฟิกด้วย ทั้งนี้ ที่ประชุมอินเทอร์เน็ตระดับภูมิภาคเอเชียแปซิฟิก ประจำปี 2011 (APrIGF: Asia-Pacific Regional Internet Governance Forum 2011) ซึ่งจัดขึ้นที่ประเทศสิงคโปร์ เน้นย้ำว่า การเซ็นเซอร์อินเทอร์เน็ตต้องเป็นไปตามข้อแนะนำของผู้รายงานพิเศษของสหประชาชาติที่เคยเสนอไว้ต่อคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ คือ

1) กฎหมายที่จะนำมาใช้ต้องชัดเจน โปร่งใส คาดเดาได้

2) มีเหตุผลชอบธรรมเพียงพอ และ

3) ต้องเป็นทางเลือกสุดท้าย ดำเนินการเฉพาะที่จำเป็น ไม่เกินสมควรแก่เหตุ/ตามสัดส่วน ทั้งต้องไม่ดำเนินคดีกับผู้ไม่เกี่ยวข้อง เช่น ตัวกลางที่เป็นเพียงทางผ่านของข้อมูล เป็นต้น และที่สำคัญก็คือ ไม่จำเป็นต้องทำให้การแสดงออกที่ชอบธรรมกลายเป็นความผิดทางอาญา[100]

นอกจากนี้ นายแฟรงค์ ลา รู (Frank La Rue) ผู้ตรวจการพิเศษด้านเสรีภาพการแสดงออกแห่งสหประชาชาติ เคยส่งแถลงการณ์จากเจนีวาเรียกร้องให้รัฐบาลไทยแก้ไขกฎหมายหมิ่นประมาทกษัตริย์ฯ และ พ.ร.บ.คอมพิวเตอร์ฯ 2550 พร้อมเสนอตัว ‘ร่วมมืออย่างสร้างสรรค์’ กับ ‘คณะกรรมการปฏิรูปกฎหมาย’ เพื่อแก้ไขกฎหมายดังกล่าวให้สอดคล้องกับหลักสิทธิมนุษยชนสากล[101] และนอกเหนือจากองค์กรด้านสิทธิแล้ว นักลงทุนและกลุ่มอุตสาหกรรมระดับโลกที่ดำเนินกิจการในประเทศไทย อาทิ กูเกิล ยาฮู อีเบย์ ฯลฯ ยังส่งสัญญาณความกังวล ต่อมาตรการควบคุมการจราจรทางอินเทอร์เน็ตในประเทศไทยว่า อาจส่งผลกระทบต่อศักยภาพการขยายตัวทางเศรษฐกิจของประเทศไทยได้[102]

5.1.5 ปฏิกิริยาต่อร่าง พ.ร.บ.คอมพิวเตอร์ฯ ฉบับใหม่

หลังจากมีข่าวการพยายามแก้ไขเพิ่มเติม พ.ร.บ.คอมพิวเตอร์ฯ 2550 มาหลายปีโดยไม่มีความคืบหน้าใดๆ เมื่อวันที่ 28 มีนาคม พ.ศ. 2554 คณะทำงานร่าง พ.ร.บ.คอมพิวเตอร์ฯ ได้จัดทำประชาพิจารณ์เกี่ยวกับร่างกฎหมายฉบับใหม่ ซึ่งร่างเสร็จเรียบร้อยแล้ว โดยเชิญเฉพาะผู้เชี่ยวชาญด้านคอมพิวเตอร์ และกฎหมายร่วมแสดงความคิดเห็น เหตุการณ์ดังกล่าวก่อให้เกิดกระแสวิพากษ์วิจารณ์ในวงกว้าง เนื่องจากมีกระบวนการร่างและการผลักดันร่างให้เป็นกฎหมายฉบับใหม่ที่ไม่โปร่งใสและเร่งรีบ ทั้งยังมีแนวโน้มว่ากฎหมายฉบับใหม่ ซึ่งมีผลเป็นการยกเลิก พ.ร.บ.คอมพิวเตอร์ฯ 2550 ทั้งฉบับ จะก่อให้เกิดปัญหาการละเมิดสิทธิและเสรีภาพของประชาชนมากกว่าเดิม[103] เป็นผลให้คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทยจัดเสวนาในหัวข้อ “เล่นเน็ตติดคุก: พ.ร.บ.คอมพิวเตอร์ใหม่คุ้มครองหรือคุกคาม” ขึ้น โดยเน้นประเด็นการทำสำเนาข้อมูลคอมพิวเตอร์ ตามมาตรา 16 ของร่างกฎหมายฉบับใหม่ ซึ่งพบปัญหาหลายประการ[104]

องค์กรสำคัญที่เป็นผู้จุดประกายให้เรื่องนี้ให้เป็นประเด็นสาธารณะ คือ โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน หรือ iLaw ซึ่งทำจดหมายเปิดผนึกถึงประชาชนและผู้ใช้อินเทอร์เน็ต เรียกร้องให้สังคมร่วมกันจับตาตรวจสอบร่างกฎหมายฉบับใหม่ เปิดช่องทางให้ร่วมลงนามทางอินเทอร์เน็ต เพื่อ “หยุด” การนำร่างกฎหมายฉบับดังกล่าวเข้าสู่การพิจารณาของคณะรัฐมนตรีโดยขาดการมีส่วนร่วมของประชาชน พร้อมทั้งชี้ให้เห็นว่าเนื้อหาของร่างกฎหมายฉบับใหม่นั้นนอกจากไม่ช่วยแก้ปัญหาเดิมแล้ว ยังอาจส่งผลกระทบต่อสิทธิเสรีภาพในสื่อออนไลน์มากขึ้นด้วย ซึ่งสวนทางกับการแก้ปัญหาอาชญากรรมคอมพิวเตอร์[105] ซึ่งมีประชาชนผู้ใช้อินเทอร์เน็ตจำนวนกว่า 560 คนร่วมลงชื่อ ทั้งนี้ iLaw ยังร่วมกับเครือข่ายพลเมืองเน็ต (Thai Netizen Network) เครือข่ายนักกฎหมายสิทธิมนุษยชน และกลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย (FACT) นำจดหมายเปิดผนึกดังกล่าวยื่นต่อนายอภิสิทธิ์ เวชชาชีวะ นายกรัฐมนตรีในขณะนั้น เพื่อเรียกร้องให้คณะรัฐมนตรียุติกระบวนการพิจารณาร่าง พ.ร.บ.คอมพิวเตอร์ฯ ที่

เสนอโดยกระทรวงไอซีที[106] จนในท้ายที่สุดเป็นผลให้การเสนอร่างกฎหมายฉบับดังกล่าวเข้าสู่การพิจารณาของคณะรัฐมนตรีถูกชะลอออกไป[107] และนับเป็นครั้งหนึ่งที่การเคลื่อนไหวของภาคประชาชนประสบผลสำเร็จ

5.1.6 ข้อเสนอภาคประชาชนและสังคมต่อร่าง พ.ร.บ. คอมพิวเตอร์ฯ ฉบับใหม่

ผลพวงจากการเสนอร่างกฎหมายฉบับใหม่ของภาครัฐ โดยมีลักษณะขาดการมีส่วนร่วมของประชาชนอย่างกว้างขวางเพียงพอ และกระแสต่อต้านคัดค้านของคนในแวดวงกฎหมาย และเทคโนโลยีสารสนเทศ ทำให้เกิดโครงการที่ใช้ชื่อว่า “My Computer Law”[108] ขึ้น โดยมีวัตถุประสงค์เพื่อรวบรวมความคิดเห็นของประชาชนทั้งผู้ให้และใช้บริการอินเทอร์เน็ต เกี่ยวกับกฎหมายคอมพิวเตอร์ และนำไปประมวลผลและพัฒนาเพื่อเสนอเป็นร่างกฎหมายฉบับประชาชน ทั้งนี้ โครงการฯ ประกอบด้วยกิจกรรมรณรงค์ให้ความรู้เกี่ยวกับอินเทอร์เน็ตและกฎหมายคอมพิวเตอร์, การจัดเวทีแลกเปลี่ยนความคิดเห็นในหมู่ประชาชน และหน่วยงานที่เกี่ยวข้อง, การร่าง พ.ร.บ.คอมพิวเตอร์ฯ ฉบับประชาชน, การเสนอร่างกฎหมายเข้าสู่สภา รวมทั้งการผลักดันร่างดังกล่าวในสภา นอกจากนี้ สถาบันวิจัยเพื่อการพัฒนาประเทศไทย (ทีดีอาร์ไอ) ยังจัดการประชุมระดมสมอง เรื่อง “ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...” เพื่อเผยแพร่บทวิเคราะห์ร่างกฎหมายคอมพิวเตอร์ฉบับใหม่ของกระทรวงไอซีที โดย อาจารย์สาวตรี สุขศรี คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ เพื่อชี้ให้เห็นข้อดี-ข้อเสีย รวมทั้งประเด็นปัญหาต่างๆ ของร่างกฎหมายฉบับใหม่เปรียบเทียบกับฉบับปัจจุบันโดยละเอียด เพื่อนำเสนอต่อหน่วยงานที่เกี่ยวข้องต่อไป[109]

5.2 ปฏิกิริยาต่อนโยบาย และแนวปฏิบัติของรัฐที่กระทบเสรีภาพในสื่อออนไลน์

5.2.1 ปฏิกิริยาต่อการระงับการเผยแพร่ข้อมูล และการปิดกั้นช่องทางการเข้าถึงเว็บไซต์ ทั้งนี้ ทั้งที่อาศัยอำนาจตามมาตรา 20 พ.ร.บ.คอมพิวเตอร์ฯ 2550 และตามกฎหมายฉบับอื่น

วันที่ 9 มีนาคม 2553 คณะรัฐมนตรีมีมติออกประกาศให้พื้นที่กรุงเทพมหานครและปริมณฑล อีก 7 จังหวัด 21 อำเภอ เป็นพื้นที่มีเหตุการณ์อันกระทบกับความมั่นคงภายในราชอาณาจักรตามพระราชบัญญัติการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. 2551 เริ่มตั้งแต่วันที่ 11 มีนาคม เป็นต้นไป ภายใต้การบริหารสถานการณ์โดยศูนย์อำนวยการรักษาความสงบเรียบร้อย (ศอ.รส.) ประกาศฉบับนี้เพิ่มการใช้อำนาจของฝ่ายบริหารตามกฎหมายฉบับต่างๆ 18 ฉบับ ซึ่งในจำนวนนี้มี พ.ร.บ. คอมพิวเตอร์ฯ 2550 รวมอยู่ด้วย โดยให้อำนาจกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) ควบคุมการจัดทำหรือเผยแพร่ข้อมูลทางอิเล็กทรอนิกส์ผ่านระบบอินเทอร์เน็ต และระบบสารสนเทศต่างๆ โดยสามารถสั่งยุติการเผยแพร่ หรือปิดกั้นสัญญาณ หากมีผู้ฝ่าฝืนให้ถือเป็นความผิดทางอาญาและดำเนินคดีได้ เป็นผลให้เครือข่ายพลเมืองเน็ต ออกแถลงการณ์คัดค้านการปิดกั้นการสื่อสารดังกล่าว และเรียกร้องให้รัฐบาลยกเลิกมาตรการทันที[110] นอกจากนี้ เครือข่ายพลเมืองเน็ตยังเคยออกจดหมายเปิดผนึก ขอให้รัฐบาลเปิดเผยรายชื่อเว็บไซต์ที่ถูกปิดกั้นโดยอาศัยคำสั่งตาม พ.ร.ก. บริหารราชการในสถานการณ์ฉุกเฉิน 2548 และให้ยกเลิกการประกาศสถานการณ์ฉุกเฉินดังกล่าว[111] รวมทั้งออกแถลงการณ์ เรื่อง “วิกฤตการเมืองและการปิดกั้นข้อมูลข่าวสาร” ด้วย[112]

สำหรับการปิดกั้นเว็บไซต์ในสถานการณ์ปกติซึ่งอาศัยอำนาจตาม พ.ร.บ.คอมพิวเตอร์ฯ 2550 (มาตรา 20) รวมทั้งการขอความร่วมมือไปยังผู้ให้บริการอินเทอร์เน็ตเป็นรายๆ ไปนั้น แม้ไม่ค่อยปรากฏการคัดค้านในลักษณะของการเขียนจดหมายเปิดผนึก หรือออกแถลงการณ์มากนัก (เท่าที่ค้นพบ ก็คือ แถลงการณ์คัดค้านการปิดกั้นชุมชนฟ้าเดียวกันเมื่อปี 2552 เนื่องจากกระทรวงไอซีทีไม่สามารถแสดงคำสั่งศาลให้กับผู้ให้บริการเว็บไซต์ที่ถูกปิดกั้นได้[113]) แต่ในส่วนของภาคประชาชนก็มีการจัด

งานสัมมนาวิชาการที่มีเนื้อหาเกี่ยวกับเสรีภาพในโลกออนไลน์กับปัญหาของ พ.ร.บ.คอมพิวเตอร์ฯ 2550 ทั้งนี้ ทั้งในระดับภายในประเทศ และระหว่างประเทศ เพื่อเสนอทางออกและแลกเปลี่ยนประสบการณ์ด้านการ Censorship[114] รวมทั้งการจัดกิจกรรมรณรงค์อื่นๆ เพื่อคัดค้านการปิดกั้นเว็บไซต์อยู่เนืองๆ อาทิเช่น กิจกรรมรณรงค์ “เซ็นเซอร์จัง” เพื่อต่อต้านการปิดเว็บแบบมั่ว[115] หรือแคมเปญ “ไทยแลนด์-แดนสวรรค์การเซ็นเซอร์” เมื่อปี 2554 โดยองค์กรผู้สื่อข่าวไร้พรมแดน เพื่อสะท้อนปัญหาเสรีภาพการแสดงออก และการปิดกั้นข้อมูลข่าวสารในประเทศไทย เวียดนาม และเม็กซิโก โดยเน้นเป้าหมายของการรณรงค์ไปที่กลุ่มนักท่องเที่ยว[116] เป็นต้น

นอกจากนี้ ดังกล่าวไปแล้วว่า ในทางความเป็นจริง รัฐบาลไทยดำเนินการระงับการเผยแพร่ข้อมูลในอินเทอร์เน็ต และปิดกั้นช่องทางการเข้าถึงเว็บไซต์มาแล้วก่อนที่ พ.ร.บ.คอมพิวเตอร์ฯ 2550 มีผลใช้บังคับ จนเมื่อปี 2549 “กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย” (FACT) ได้ทำหนังสือถึงคณะกรรมการสิทธิมนุษยชนแห่งชาติ[117] เพื่อร้องเรียนการใช้อำนาจดังกล่าวของรัฐโดยไม่มีกฎหมายฉบับใดให้อำนาจ ซึ่งถือเป็นการละเมิดเสรีภาพในการแสดงความคิดเห็นและขัดกับรัฐธรรมนูญ จากนั้นได้เปิดให้ผู้เห็นด้วยลงชื่อออนไลน์เพื่อสนับสนุนคำร้อง ซึ่งในท้ายที่สุดมีผู้ร่วมลงชื่อกว่า 1,200 คน[118]

5.2.2 ปฏิกิริยาต่อนโยบายด้านอื่นของรัฐที่น่าจะส่งผลกระทบต่อเสรีภาพในสื่อออนไลน์

จากข้อมูลในส่วนที่ว่าด้วยแนวนโยบายของรัฐที่เกี่ยวกับเสรีภาพในการแสดงความคิดเห็นในสื่อออนไลน์ จะเห็นได้ว่า มาตรการที่รัฐใช้เพื่อควบคุม หรือกำกับพฤติกรรม และการแสดงความคิดเห็นของประชาชนนั้นไม่ได้มีเพียงมาตรการระงับการเผยแพร่หรือปิดกั้นเว็บไซต์เท่านั้น หากแต่ยังมีโครงการลักษณะต่างๆ ความร่วมมือ รวมทั้งประกาศคำเตือน ซึ่งล้วนไม่เอื้อต่อเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็น อย่างไรก็ดี ทันทีที่นโยบาย หรือแนวทางปฏิบัติในลักษณะดังกล่าวเผยแพร่

สู่กลุ่มผู้ใช้อินเทอร์เน็ต ก็ปรากฏว่ามีกระแสวิพากษ์วิจารณ์ ถึงกระทั่งการประท้วงคัดค้านจนกระทรวงไอซีทีต้องยกเลิกโครงการบางอย่างไป อาทิเช่น กระแสต่อต้านแนวคิดในการติดตั้งระบบดักจับข้อมูล (sniffer) ของกระทรวงไอซีทีในยุครัฐมนตรีระนองรักษ์ โดยผู้ใช้และผู้ให้บริการอินเทอร์เน็ตซึ่งตั้งเป็นกลุ่ม "Thailand No Sniffer" บนทวิตเตอร์ และในเครือข่ายสังคมเฟซบุค[119] จนเป็นผลให้กระทรวงไอซีทียุติโครงการดังกล่าวไป[120] หรือปฏิกิริยาโต้ตอบการห้ามแสดงความคิดเห็นหรือกดถูกใจ (Like) ในเครือข่ายสังคมเฟซบุค ในยุคของรัฐมนตรีอนุดิษฐ์ ด้วยการออกแถลงการณ์ "กดไลค์ไม่ใช่อาชญากรรม" ของเครือข่ายพลเมืองเน็ต[121] รวมทั้งกระแสวิพากษ์วิจารณ์การที่กระทรวงไอซีทีดึงเอาเด็กและเยาวชนเข้ามายุ่งเกี่ยวกับความขัดแย้งทางการเมืองในโครงการสร้างลูกเสือไซเบอร์ (cyber scout) ในยุคของรัฐมนตรีจุติ ไกรฤกษ์ เป็นต้น

5.2.3 ปฏิกิริยาของภาคประชาชนในเชิงสนับสนุนการบังคับใช้กฎหมาย และแนวนโยบายแห่งรัฐเพื่อการปิดกั้นเสรีภาพในสื่อออนไลน์

สิ่งที่น่าสนใจสำหรับประเทศไทยก็คือ มีประชาชนไทยผู้ใช้อินเทอร์เน็ตจำนวนไม่น้อยที่เห็นด้วย และสนับสนุนให้รัฐใช้มาตรการในการตรวจสอบเนื้อหาในสื่อออนไลน์อย่างเคร่งครัด ปิดเว็บไซต์ต่างๆ ที่มีเนื้อหาลามกอนาจาร ขัดต่อความมั่นคง โดยเฉพาะอย่างยิ่ง เนื้อหาดูหมิ่นหมิ่นประมาท อาฆาตมาดร้าย หรือกระทั่งเพียงวิพากษ์วิจารณ์สถาบันพระมหากษัตริย์ฯ นอกจากนี้ยังมีการรวมกลุ่มกันเพื่อคอยตรวจตราเนื้อหาและรายงานไปยังเจ้าหน้าที่รัฐ ดังปรากฏว่ามีการตั้งกลุ่มหรือเพจต่างๆ ในเครือข่ายสังคมออนไลน์ (social network) อาทิ "สมาคม Report แห่งประเทศไทย" ซึ่งระบุคำอธิบายไว้ว่า

"เพจนี้ไม่มีนโยบายเผยแพร่การหมิ่นสถาบันให้เกิดความเสื่อมเสีย เราเผยแพร่เพื่อป้องกันภัยคุกคามทางโลกออนไลน์ และไม่มีนโยบายให้พูดในเรื่องการเมือง, พระมหากษัตริย์, หรือกล่าวอ้างบุคคลใด ร่วมกันป้องกันภัยคุมคามทาง Facebook..."

เพจดังกล่าวนี้ยังมีการรณรงค์ให้ผู้ใช้อินเทอร์เน็ต “หยุด Like” “หยุด Comment” “หยุด Share” และ “รายงาน ! ผู้ดูแล” รวมถึงมีปฏิบัติการ Bomb Report หรือนัดเวลากันเพื่อกดรายงานหน้าเพจหนึ่งๆ ไปยังผู้ดูแลระบบของเฟซบุ๊กเป็นระยะๆ ด้วย[122] นอกจากสมาคม Report แห่งประเทศไทยแล้ว ยังมีชมรมผู้รักสถาบันพระมหากษัตริย์ภายใต้ชื่อ “ชมรมนักรบไซเบอร์”[123] ซึ่งรวบรวมคนทุกสาขาอาชีพที่มีเวลาอยู่หน้าจอคอมพิวเตอร์ มาคอยติดตามตรวจสอบและรวบรวมเว็บไซต์ คลิปหมิ่นสถาบันฯ รวมทั้งเว็บไซต์ที่เกี่ยวกับความมั่นคง ยาเสพติด การพนัน และลามก เพื่อนำไปแจ้งแก่รัฐมนตรีว่าการกระทรวงไอซีทีให้ลงนามและส่งดำเนินการฟ้องร้องต่อศาลยุติธรรมต่อไป

นายอัครวุฒิ ตำราเรียง อุปนายกสมาคมผู้ดูแลเว็บไทย เคยให้ความเห็นในฐานะที่สมาคมฯ เป็นองค์กรวิชาชีพของผู้ดูแลเว็บไซต์ว่า การดำเนินการกับเว็บไซต์ที่มีเนื้อหาหมิ่นสถาบันพระมหากษัตริย์เป็นเรื่องที่ต้องทำโดยเร่งด่วนสูงสุด ทางสมาคมขอเสนอแนะให้ใช้มาตรการทางกฎหมายเป็นหลักในการดำเนินการกับเว็บไซต์ดังกล่าว ด้วยการขอความร่วมมือองค์กรภาคประชาสังคมและประชาชนทั่วไปในการแจ้งเบาะแส และเร่งรวบรวมหลักฐานเพื่อขออำนาจศาลในการสั่งปิดกั้นการเข้าถึง และดำเนินการกับเจ้าของเว็บไซต์ที่มีเจตนาทำลายสถาบันพระมหากษัตริย์[124]

นอกจากนี้เมื่อ วันที่ 18 สิงหาคม 2554 “เครือข่ายเฝ้าระวังพิทักษ์และปกป้องสถาบันพระมหากษัตริย์” และ “เครือข่ายพิทักษ์จักรีวงศ์” จำนวน 300 คน ได้ขอเข้าพบ น.อ. อนุดิษฐ์ นาครทรรพ รัฐมนตรีว่าการกระทรวงไอซีที เพื่อให้กำลังใจในการดำเนินการปิดเว็บไซต์ที่มีเนื้อหาหมิ่นสถาบันฯ ด้วย โดย นายฉัตรชัย ภู่โคกหวาย เลขานุการเครือข่าย กล่าวว่า “กลุ่มที่มีพฤติกรรมหมิ่นสถาบันส่วนใหญ่จะมีความสนิทสนมกับพรรคเพื่อไทย ดังนั้นจึงต้องการมาตอกย้ำ รมว.ไอซีที ซึ่งเป็นสมาชิกพรรคเพื่อไทยเช่นเดียวกันให้ดำเนินการอย่างเด็ดขาดในการปิดเว็บไซต์หมิ่นสถาบันพระมหากษัตริย์ทันทีที่เจอ”[125]

มีข้อสังเกตเพิ่มเติมด้วยว่า คดีความที่เกี่ยวกับการหมิ่นประมาท

กษัตริย์ฯ และ พ.ร.บ.คอมพิวเตอร์ฯ 2550 จำนวนหนึ่งมีส่วนเกี่ยวพันกับกลุ่มในเครือข่ายสังคมออนไลน์ (เฟซบุค) กลุ่มหนึ่งที่ใช้ชื่อว่า “ยุทธการลงทัณฑ์ทางสังคม” (Social Sanction) ซึ่งดำเนินการในลักษณะตรวจหาผู้เผยแพร่เนื้อหาวิพากษ์วิจารณ์สถาบันพระมหากษัตริย์ฯ แล้วนำรูปภาพของบุคคลดังกล่าวมาให้เพื่อนสมาชิกต่อว่าด่าทอในพื้นที่ออนไลน์ (เสียบประจาน) รวมทั้งค้นหาข้อมูลส่วนบุคคลของผู้ถูกเสียบประจานมาเผยแพร่เป็นการทั่วไป ซึ่งบางกรณีก็มีการส่งเรื่องให้กรมสอบสวนคดีพิเศษดำเนินคดีในเวลาต่อมา[126]

5.3 วิเคราะห์ปฏิกิริยา และความเคลื่อนไหวภาคประชาชน

จากปฏิกิริยาและความเคลื่อนไหวของภาคประชาชนตามที่กล่าวมา จะเห็นได้ว่า ในที่สุดแล้ว กลุ่มประชาชนที่ติดตามประเด็นเสรีภาพในสื่อออนไลน์ พ.ร.บ.คอมพิวเตอร์ฯ 2550 กับปัญหาการบังคับใช้ที่เกิดขึ้น รวมทั้งติดตามตรวจสอบแนวนโยบายของรัฐที่เกี่ยวกับการปิดกั้นเว็บไซต์ อย่างต่อเนื่องและจริงจัง ทั้งยังใช้สิทธิแสดงออก ประท้วง ออกแถลงการณ์ หรือโต้แย้งคัดค้านองค์กรหรือหน่วยงานรัฐต่อการดำเนินการที่น่าจะส่งผลกระทบต่อเสรีภาพของประชาชน มีอยู่เพียงไม่กี่กลุ่มเท่านั้น อาทิ กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย (FACT), เครือข่ายพลเมืองเน็ต (Thai Netizen Network) และโครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw) นอกเหนือจากองค์กรเหล่านี้ ก็มักเป็นกิจกรรมหรือความเคลื่อนไหวที่มาจากองค์กรที่รวมตัวเพื่อทำงานเฉพาะกิจอย่างกลุ่ม Thailand No Sniffer ที่รวมตัวกันเพื่อคัดค้านนโยบายการดักข้อมูลของกระทรวงไอซีที หรือมิเช่นนั้นก็เป็นกลุ่มที่รวมตัวอยู่แล้วเป็นปกติแต่จะเข้ามาทำกิจกรรมเกี่ยวกับเสรีภาพในการแสดงความคิดเห็นก็ต่อเมื่อเกิดเหตุที่กระทบกับกลุ่มนั้นเองโดยตรง หรือได้รับการบอกกล่าวและชักชวนเข้าร่วมกิจกรรม เช่น กลุ่มชุมชนฟ้าเดียวกัน หรือเครือข่ายนักกฎหมายสิทธิมนุษยชน เป็นต้น ทั้งนี้ ลักษณะของการเคลื่อนไหวยังคงอยู่ในรูปของการประท้วงเรียกร้องเชิงนโยบายและทาง

สังคมเท่านั้น ยังไม่ปรากฏการตอบโต้ หรือเรียกร้องเพื่อให้เกิดผลบังคับทางกฎหมายเหมือนในต่างประเทศอย่างการใช้สิทธิทางศาลฟ้องหน่วยงาน หรือเจ้าหน้าที่รัฐ เมื่อพบกรณีที่พนักงานเจ้าหน้าที่ หรือองค์กรที่เกี่ยวข้องนั้นใช้อำนาจในทางที่มิชอบ ละเมิดเสรีภาพของประชาชนอย่างเกินขอบเขต หรือกระทั่งร้องว่ากฎหมายบางเรื่องบางมาตราอาจขัดหรือแย้งกับรัฐธรรมนูญ

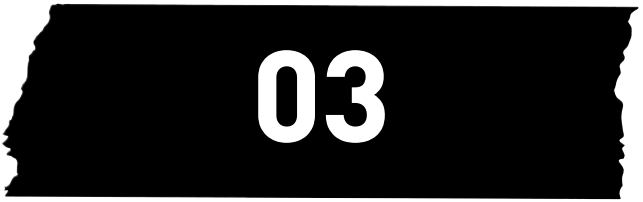
จากการศึกษาพบว่า เท่าที่รัฐใช้อำนาจปิดกั้นเว็บไซต์ในช่วงเวลาที่ผ่านมา มีกรณีที่ผู้ถูกคำสั่งปิดกั้นฟ้องรัฐเป็นจำเลยเพียงคดีเดียวเท่านั้น คือ คดีที่เว็บไซต์ข่าว “ประชาไท” (www.prachatai.com) ฟ้องนายกรัฐมนตรีและศูนย์อำนวยแก้ไขสถานการณ์ฉุกเฉิน (ศอฉ.) เป็นจำเลยในคดีแพ่งเพื่อโต้แย้งคัดค้านคำสั่งปิดกั้นเว็บไซต์ประชาไทซึ่งออกโดยอาศัยอำนาจตาม พ.ร.ก. การบริหารราชการในสถานการณ์ฉุกเฉิน 2548 รวมทั้งเรียกร้องให้รัฐชดใช้ค่าสินไหมทดแทน เนื่องจากเป็นการออกคำสั่งที่ไม่ชอบด้วยกฎหมาย เพราะไม่มีการให้เหตุผลหรืออธิบายว่าเนื้อหาส่วนใดของเว็บไซต์ที่เข้าข่ายต้องถูกปิดกั้น ทั้ง ศอฉ. ยังดำเนินการโดยขัดต่อหลัก “ความได้สัดส่วน” ด้วยการปิดกั้นทั้งเว็บไซต์ ทั้งที่ในความเป็นจริงพื้นที่ที่อาจมีเนื้อหาผิดกฎหมายอยู่ในส่วนบริการเว็บบอร์ด ซึ่งแยกต่างหากจากเว็บไซต์หลักที่นำเสนอข่าวสารตามปกติ คดีนี้ศาลชั้นต้นพิพากษายกฟ้องโจทก์ ด้วยเหตุผลว่า นายกรัฐมนตรี และ ศอฉ. ปิดกั้นเว็บไซต์โจทก์ได้ โดยอาศัยอำนาจตาม พ.ร.ก.ฉุกเฉินฯ 2548 และศาลจะไม่เข้าตรวจสอบหรือก้าวก่ายการใช้อำนาจของฝ่ายบริหารในลักษณะดังกล่าว ปัจจุบันคดีนี้อยู่ในชั้นอุทธรณ์[127]

สาเหตุของการไม่ตื่นตัวเท่าที่ควร หรือมีกลุ่มที่ให้ความสนใจต่อกรณีที่เสรีภาพของประชาชนถูกกระทบโดย พ.ร.บ.คอมพิวเตอร์ฯ 2550 จำนวนน้อยนั้น ส่วนหนึ่งน่าจะมาจากความที่กฎหมายในเรื่องเหล่านี้ยังไม่เป็นที่รู้จักกันในวงกว้าง กฎหมายเป็นเรื่องทางเทคนิคมากเกินไปทำให้ประชาชนทั่วไปขาดความสนใจ หรือมิเช่นนั้นก็ทำความเข้าใจได้ยาก รวมทั้งสาเหตุที่คนไทยยังไม่ค่อยให้ความสำคัญกับเสรีภาพในการติดต่อสื่อสาร การรับรู้ข้อมูลข่าวสาร และเสรีภาพในการแสดงความคิดเห็นมากพอ (ตราบใดที่ตนเองยังไม่ได้รับผลกระทบโดยตรง) ยิ่งไปกว่านั้น กลับมีคนไทยจำนวน

มากที่เห็นด้วยกับการปิดกั้นการแสดงความคิดเห็นของผู้อื่นสำหรับเรื่องบางเรื่องให้เคร่งครัด และเข้มงวดมากขึ้น

จากผลสำรวจของสวนดุสิตโพล ปี 2554 พบว่า ประชาชนไม่รู้จัก พ.ร.บ.คอมพิวเตอร์ฯ 2550 ในจำนวนเกือบครึ่งหนึ่งของผู้ตอบแบบสอบถาม โดยมีผู้รู้จักกฎหมายฉบับนี้ดีเพียงแค่ร้อยละ 0.98[128]เท่านั้น ในขณะที่ นายไพบูลย์ อมรภิญโญเกียรติ ที่ปรึกษากฎหมาย บริษัทที่ปรึกษากฎหมายไพบูลย์ จำกัด เคยกล่าวว่า หลังการประกาศใช้ พ.ร.บ. คอมพิวเตอร์ฯ 2550 มากว่า 3 ปี ผลสำรวจเบื้องต้นพบว่า มีผู้ไม่รู้ว่ามีกฎหมายดังกล่าวในจำนวนสูงถึงร้อยละ 70 ผู้ที่มีความรู้เกี่ยวกับกฎหมายฉบับนี้ในระดับปานกลางราวร้อยละ 10 มีความเข้าใจในระดับดีร้อยละ 7 และเข้าใจระดับดีมากเพียงร้อยละ 2-3 เท่านั้น ซึ่งสาเหตุส่วนหนึ่งเป็นเพราะศัพท์กฎหมายที่เข้าใจยาก ทั้งยังเกี่ยวพันกับความรู้ความเข้าใจในเทคโนโลยีคอมพิวเตอร์ ในส่วนของฝ่ายผู้บังคับใช้กฎหมายพบว่า เจ้าหน้าผู้ปฏิบัติการที่มีความรู้ความเข้าใจกฎหมายฉบับนี้ยังมีน้อย ปัจจุบันมีเจ้าหน้าที่ตำรวจที่เชี่ยวชาญด้านเทคโนโลยีอย่างแท้จริงเพียงไม่ถึง 10 คนเท่านั้น[129]

บทที่



กฎหมายเยอรมัน
กับสิทธิเสรีภาพในสื่อออนไลน์

กฎหมายเยอรมัน กับสิทธิเสรีภาพในสื่อออนไลน์

ความน่าสนใจต่อการศึกษากฎหมายในเรื่องนี้ของประเทศสหพันธรัฐเยอรมนีก็คือ นอกจากเป็นประเทศที่เคารพในหลักเสรีภาพในการแสดงความคิดเห็นและการคุ้มครองพื้นที่ส่วนบุคคลอย่างมากแล้ว ประเทศไทยยังได้รับอิทธิพลด้านนิติปรัชญา ระบบกฎหมาย และหลักการพื้นฐานในเรื่องสิทธิมนุษยชนมาจากประเทศเยอรมนีอีกด้วย จึงน่าจะเป็นประโยชน์หากได้ศึกษาเปรียบเทียบกฎหมาย แนวนโยบาย รวมทั้งการบังคับใช้กฎหมายที่เกี่ยวกับสิทธิเสรีภาพบนสื่อออนไลน์ระหว่างประเทศทั้งสอง อนึ่ง แม้ประเทศเยอรมนีจะเคารพในสิทธิเสรีภาพในการสื่อสารของประชาชน อีกทั้งมีกรณีที่รัฐดำเนินการปิดกั้นสื่อออนไลน์ไม่มากนักเมื่อเทียบกับประเทศอื่น แต่ในสังคมเยอรมันก็ยังมีประเด็นละเอียดอ่อนที่รัฐไม่อาจอนุญาตให้พลเมืองแสดงความคิดเห็นได้โดยเสรีเช่นกัน งานวิจัยชิ้นนี้จะพยายามชี้ให้เห็นที่มาแนวคิด เหตุผล รวมทั้งวิธีการจัดการกับประเด็นอ่อนไหวดังกล่าวของประเทศเยอรมนี โดยวิเคราะห์จากตัวบทกฎหมาย แนวนโยบายของรัฐ ความเคลื่อนไหวของประชาชน รวมทั้งคดีตัวอย่างการปิดกั้นเว็บไซต์ที่เกิดขึ้นแล้วในบางรัฐของประเทศเยอรมนี

1. หลักการคุ้มครองสิทธิเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็น

ประเทศสหพันธรัฐเยอรมนี ถือเป็นประเทศในลำดับต้นๆ ของโลกที่ให้ความสำคัญกับการคุ้มครองสิทธิและเสรีภาพของประชาชน รัฐธรรมนูญเยอรมัน (Grundgesetz) วางหลักการว่าด้วยการคุ้มครองสิทธิเสรีภาพส่วนบุคคลไว้ครอบคลุมว่า รัฐต้องให้ความคุ้มครองเสรีภาพทั้งหลายของทั้งผู้ให้บริการและผู้ใช้บริการการสื่อสารและโทรคมนาคมรูปแบบต่างๆ โดยเฉพาะอย่างยิ่งการคุ้มครองเสรีภาพนั้นจากการแทรกแซงโดยรัฐ หลายมาตราในรัฐธรรมนูญเยอรมันถูกตีความเพื่อใช้ในการคุ้มครองเนื้อหา รวมทั้งการแสดงความคิดเห็นของประชาชนในสื่อออนไลน์ หลักการเหล่านี้แม้ในขณะที่ประกาศใช้รัฐธรรมนูญจะยังไม่มีใครคิดถึงอินเทอร์เน็ตหรือสื่อออนไลน์มาก่อนก็ตาม แต่เมื่อข้อเท็จจริงในปัจจุบันปรากฏว่าอินเทอร์เน็ตเข้ามามีบทบาทในการดำเนินชีวิตมากขึ้น ข้อมูลข่าวสาร กิจกรรมต่างๆ เกิดขึ้นในเครือข่ายออนไลน์ การให้ความคุ้มครองสิทธิเสรีภาพจึงย่อมต้องถูกขยายความให้ครอบคลุมพื้นที่อิเล็กทรอนิกส์ด้วย

ปัจจุบัน บทบัญญัติหลักๆ ในรัฐธรรมนูญเยอรมัน ที่รับรองคุ้มครองสิทธิและเสรีภาพของประชาชน โดยเฉพาะอย่างยิ่งที่เกี่ยวกับเสรีภาพในการทำกิจกรรมต่างๆ ในสื่อออนไลน์ ประกอบด้วย

1.1 เสรีภาพในการแสดงความคิดเห็น ตามมาตรา 5[1] (1) ประโยคที่ 1 ส่วนที่ 1 รัฐธรรมนูญเยอรมัน (Art. 5 Abs. 1 Satz 1 Alt. 1 GG - Meinungsfreiheit[2])

ประเทศเยอรมนีให้ความสำคัญกับเสรีภาพในการแสดงความคิดเห็น โดยเฉพาะอย่างยิ่งในสื่อออนไลน์อย่างอินเทอร์เน็ตมาก จนศาลรัฐธรรมนูญเยอรมัน (Bundesverfassungsgericht (BVerfG)) เคยกล่าวไว้ในคดีหนึ่งว่า

"...สิทธิและเสรีภาพในการแสดงความคิดเห็นถือเป็นสิ่งสำคัญ

ของสิทธิมนุษยชน และยิ่งสำคัญมากสำหรับกระบวนการสร้างแนวคิดประชาธิปไตย หากปราศจากเสียแล้วซึ่งเสรีภาพในการแสดงความคิดเห็นโดยปัจเจกชน เจตจำนงทางการเมืองสาธารณะที่สมบูรณ์ครบถ้วนย่อมไม่อาจเกิดขึ้นได้ ทั้งนี้ สิทธิเสรีภาพในการแสดงความคิดเห็น ทั้งเจตจำนงร่วมทางการเมือง ซึ่งเกี่ยวพันอย่างแนบแน่นกับระบอบประชาธิปไตยนี้ ย่อมหมายรวมถึง เสรีภาพในการสื่อสารกันในอินเทอร์เน็ตด้วย...”

มาตรา 5 รัฐธรรมนูญเยอรมันบัญญัติให้ความคุ้มครอง การพูด การเขียน การวาด และการแสดงออกทุกรูปแบบ รวมทั้งการเผยแพร่ความคิดเห็นในสื่อประเภทต่าง ๆ จากการถูกปิดกั้น หรือถูกตรวจสอบ และแทรกแซงโดยรัฐ อย่างไรก็ตาม ในวรรค 2 ของมาตรา 5 เสรีภาพชนิดนี้อาจถูกจำกัดได้โดยการบัญญัติกฎหมาย โดยเฉพาะอย่างยิ่ง เพื่อเป้าหมายในการคุ้มครองเด็กและเยาวชน และเกียรติยศชื่อเสียงส่วนบุคคล

1.2 เสรีภาพในการรับรู้ข้อมูลข่าวสาร ตามมาตรา 5 (1) ประโยคที่ 1 ส่วนที่ 2 รัฐธรรมนูญเยอรมัน (Art. 5 Abs. 1 Satz 1 Alt. 2 GG – Informationsfreiheit[3])

เสรีภาพในการรับรู้ข้อมูลข่าวสารถือเป็นเสรีภาพที่มีความสำคัญเทียบเท่ากับเสรีภาพการแสดงความคิดเห็น (Meinungsfreiheit) และเสรีภาพในการพิมพ์ (Pressefreiheit) เนื่องจากเป็นส่วนสำคัญของกระบวนการสร้างความคิดเห็นสาธารณะ ทั้งนี้ หมายรวมถึงการรับรู้ข้อมูลข่าวสารจากแหล่งข่าวสารสาธารณะทุกประเภททั้งในระบบปิด (offline) และระบบเปิด (online) กล่าวได้ว่า การคุ้มครองเสรีภาพประเภทนี้ ก็คือ การให้ความคุ้มครองเสรีภาพในมิติทางฝ่าย “ผู้รับข้อมูลข่าวสาร” นอกเหนือจากมิติของ “ผู้ส่งข่าวสาร” ในรูปของเสรีภาพในการแสดงความคิดเห็น และมิติในการนำเสนอข่าวสารโดยสื่อสารมวลชน (เสรีภาพในการพิมพ์) เสรีภาพในการรับรู้ข้อมูลข่าวสาร ถือเป็นหลักประกันให้กับประชาชนในการ “เข้าถึง” ข้อมูลจากแหล่งต่าง ๆ ได้โดยอิสระ ดังนั้น โดยหลักแล้วการปิดกั้นหรือ

เซ็นเซอร์ช่องทางเข้าถึงข้อมูลสาธารณะใดๆ ไม่ว่าอุปกรณ์ในการส่งสารจะอยู่ในรูปแบบใด หรือมีเทคนิควิธีการอย่างไร ล้วนแล้วแต่กระทำมิได้[4]

1.3 เสรีภาพในการพิมพ์ และเสรีภาพในการออกอากาศ มาตรา 5 (1) ประโยคที่ 2 รัฐธรรมนูญเยอรมัน (Art. 5 Abs. 1 Satz 2 GG – Presse- und Rundfunkfreiheit[5])

สำหรับเสรีภาพในส่วนนี้ย่อมแตกต่างจากเสรีภาพในการแสดงความคิดเห็นธรรมดา เพราะนอกจากเป็นการคุ้มครองเสรีภาพในมิติของ “ผู้ส่งสาร” แล้ว ยังทำหน้าที่เป็นหลักประกันความเป็นอิสระของสถาบันหรือผู้ประกอบวิชาชีพสื่อ ในอันที่จะค้นหา ตระเตรียมข้อมูลข่าวสารตลอดกระบวนการ ไปจนถึงการนำข้อมูลข่าวสารนั้นเผยแพร่สู่ช่องทางการสื่อสารใดๆ[6] ไม่ว่าจะผ่านสิ่งพิมพ์ วิทยุกระจายเสียง หรือโทรทัศน์ โดยปราศจากการแทรกแซง หรือควบคุมโดยรัฐ หากไม่มีเสรีภาพในส่วนนี้เสียแล้ว ย่อมส่งผลกระทบต่อเสรีภาพสองเรื่องแรก ฉะนั้น หากต้องการให้การคุ้มครองเสรีภาพในเรื่องเหล่านี้เป็นไปอย่างครบถ้วนสมบูรณ์ จึงจำเป็นต้องให้ความคุ้มครองสถาบันและการทำงานของสื่อสารมวลชนด้วย

อย่างไรก็ตาม ในวงการกฎหมายเยอรมันยังคงมีความเห็นขัดแย้งกันอยู่ในประเด็นของคำนิยามและขอบเขตของเสรีภาพสองลักษณะตามมาตรานี้ ความเห็นหนึ่ง[7] มองว่าบทบัญญัตินี้ให้ความคุ้มครองเสรีภาพสื่อในความหมายโดยรวม หรือที่เรียกว่า “เสรีภาพสื่อสารมวลชน” (Medienfreiheit) ในขณะที่นักกฎหมายอีกกลุ่มหนึ่งเห็นว่า ด้วยลักษณะของถ้อยคำเอง เจตนารมณ์ของผู้ร่างรัฐธรรมนูญ รวมทั้งขอบเขตเสรีภาพทั้งสองประเภทดังกล่าวมีความแตกต่างกัน จึงไม่ควรนำมากล่าวไว้รวมกัน จึงเห็นว่า Pressefreiheit หรือเสรีภาพในการพิมพ์ มีขอบเขตกว้างกว่า ไม่จำกัดว่าต้องเป็นการนำเสนอข้อเท็จจริง หรือความคิดเห็นของบุคคลใดภายใต้เสรีภาพชนิดนี้ ผู้ส่งสารอาจเป็นบุคคลใดบุคคลหนึ่ง หรือคนกลุ่มใดกลุ่มหนึ่งก็ได้ โดยจะนำเสนอข้อเท็จจริง หรือแค่เพียงความคิดเห็น นำเสนอในรูปแบบใดๆ และจะถึงขั้นจัดตั้งเป็นองค์กรเพื่อให้บริการข้อมูลหรือไม่ก็ได้

ในขณะที่ Rundfunkfreiheit หรือเสรีภาพในการออกอากาศ มีลักษณะของการ “ให้บริการสาธารณะ” อยู่ด้วย ผู้มีใบอนุญาตเท่านั้นจึงเป็นผู้ส่งสารในช่องทางนี้ได้ ดังนั้น เสรีภาพในส่วนของการออกอากาศนี้โดยสภาพจึงมีขอบเขตจำกัดกว่าเสรีภาพในการพิมพ์[8]

ความเห็นต่างในประเด็นดังกล่าวมา มีผลต่อการคุ้มครองสื่อใหม่ (New Media) โดยเฉพาะอย่างยิ่งสื่ออินเทอร์เน็ต ว่าควรได้รับความคุ้มครองในขอบเขตความหมายของเสรีภาพประเภทใดกันแน่ นักกฎหมายส่วนหนึ่งเห็นว่าเนื่องจาก “ทุกคน” เป็นผู้ส่งสารในบริการออนไลน์ได้ เพียงแต่เปลี่ยนพื้นที่ในการนำเสนอจากเอกสารธรรมดาไปสู่เอกสารอิเล็กทรอนิกส์เท่านั้น ดังนั้น เสรีภาพในสื่อออนไลน์จึงควรมีความหมายและขอบเขตการคุ้มครองเช่นเดียวกับเสรีภาพการพิมพ์ หรือ Pressefreiheit[9] ในขณะที่นักกฎหมายอีกกลุ่มหนึ่งยึดความหมายของคำว่า Presse (เอกสารหรือสิ่งพิมพ์) ที่เรียกร้องให้การนำเสนอข้อมูลต้องเป็นเอกสารที่จับต้องได้เท่านั้น เสรีภาพในบริการสื่อออนไลน์ ซึ่งมีทั้งรูปแบบและเทคนิควิธีการในการนำเสนอข่าวสารที่แตกต่างไปจากสื่อสิ่งพิมพ์ จึงควรมีความหมายและขอบเขตเช่นเดียวกับเสรีภาพในการออกอากาศ หรือ Rundfunkfreiheit[10] อย่างไรก็ตาม ข้อถกเถียงเหล่านี้ยังไม่ยุติแต่ดูเหมือนว่าความเห็นที่สองที่สนับสนุนให้สื่อออนไลน์มีสถานภาพเช่นเดียวกันกับการออกอากาศ (Rundfunk) ได้รับการตอบรับมากกว่า เพราะก่อนหน้านี้ สื่อทางไกล (Telemedien) ในประเทศเยอรมนีก็ถูกถือว่าเป็นสื่อคนละประเภทกับ Presse เพราะติดที่นิยามว่าต้องมีเอกสารจับต้องได้เช่นกัน แต่ปัญหาก็คือ หากยึดถือตามแนวความเห็นนี้ย่อมหมายความว่าการเผยแพร่ข้อมูลในสื่อออนไลน์ โดยเฉพาะอย่างยิ่งบรรดาหนังสือพิมพ์ออนไลน์ (online erscheinenden Zeitungen) จะอยู่ภายใต้เงื่อนไข และข้อบังคับต่าง ๆ ตามที่กำหนดไว้ในกฎหมายว่าด้วยการกระจายเสียง หรือการออกอากาศ (Rundfunkstaatsvertrag – RStV) ไปด้วย

1.4 เสรีภาพในการประกอบอาชีพ ตามมาตรา 12 รัฐธรรมนูญเยอรมัน (Art. 12 Abs. 1 GG Berufsfreiheit)

ตราบใดที่การนำเสนอข้อมูลข่าวสารโดยผู้ให้บริการอินเทอร์เน็ต ไม่ว่าจะเป็น ผู้ให้บริการเนื้อหา ผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต หรือผู้ให้บริการพื้นที่เซิร์ฟเวอร์ เป็นเรื่องของการให้บริการข้อมูลหรือกิจกรรมต่างๆ แก่ประชาชน ย่อมต้องได้รับความคุ้มครองเสรีภาพในฐานะที่เป็นการประกอบอาชีพรูปแบบหนึ่งด้วย รัฐจึงมิอาจใช้มาตรการใดๆ ที่อาจกระทบต่อเสรีภาพและการตัดสินใจในการประกอบอาชีพได้ ในที่นี้ เช่น การสั่งให้ระงับการเผยแพร่ข้อมูลข่าวสาร หรือปิดกั้นช่องทางการเข้าถึง เป็นต้น

1.5 เสรีภาพด้านอื่นๆ ที่อาจเกี่ยวข้องกับเสรีภาพในสื่อออนไลน์

นอกเหนือจากเสรีภาพดังกล่าวมา การให้บริการข้อมูลข่าวสารหรือกิจกรรมต่างๆ ในสื่อออนไลน์ ยังอาจได้รับความคุ้มครองตามรัฐธรรมนูญเยอรมันในสถานะอื่นๆ ได้อีก ขึ้นอยู่กับเนื้อหา หรือลักษณะของกิจกรรมที่เกิดขึ้น อาทิ เสรีภาพในทางวิชาการ (Art. 5 Abs. 3 GG – Wissenschaftsfreiheit) เสรีภาพในทางความคิด ความเชื่อ หรือการนับถือศาสนา (Art. 4 GG - Die Freiheit des Glaubens, des Gewissens und die Freiheit des religiösen und weltanschaulichen Bekenntnisses) เสรีภาพในการก่อตั้งกลุ่มหรือสมาคม ซึ่งย่อมหมายรวมถึงกลุ่มในสื่อออนไลน์ด้วย (Art. 9 Abs. 1 Satz 1 GG Vereinigungsfreiheit) เสรีภาพในการประชุมหรือการร่วมชุมนุม (Art. 8 Abs. 1 GG – Versammlungsfreiheit) รวมทั้งเสรีภาพในศิลปะ (Art. 5 Abs. 3 GG – Kunstfreiheit) ซึ่งเคยมีการอ้างอิงและเกิดข้อถกเถียงถึงมาแล้ว กรณีเหตุการณ์เผยแพร่ภาพการ์ตูนล้อนบีมูฮัมหมัด (Mohammed-Karikaturen) ในประเทศเยอรมนี[11]

2. เนื้อหาต้องห้ามเผยแพร่ในสื่อสาธารณะ หรือการเผยแพร่นั้นเป็นความผิดตามกฎหมายเยอรมัน

จากบทบัญญัติต่างๆ ที่เกี่ยวกับการคุ้มครองสิทธิในการรับรู้ข้อมูลข่าวสาร เสรีภาพในการแสดงความคิดเห็น รวมทั้งเสรีภาพสื่อสารมวลชนแห่งรัฐธรรมนูญเยอรมัน แสดงให้เห็นว่าโดยหลักแล้วข้อมูลข่าวสารทุกประเภทย่อมได้รับความคุ้มครอง และรัฐจะปิดกั้นช่องทางหรือระงับการเผยแพร่เนื้อหาไม่ได้ ไม่ว่าจะเป็นการปิดกั้นก่อนเผยแพร่ (Vorzensur) หรือระงับการเผยแพร่ในภายหลัง (Nachzensur) อย่างไรก็ตาม แม้ประเทศเยอรมนีจะให้ความสำคัญกับสิทธิเสรีภาพในเรื่องต่างๆ ของประชาชนอย่างมาก แต่ “เสรีภาพ” เหล่านั้นอาจถูกจำกัดได้เช่นกัน ภายใต้ข้อยกเว้นที่มีเงื่อนไขชัดเจน การจำกัดเสรีภาพของประชาชนโดยรัฐจะเกิดขึ้นได้ก็ต่อเมื่อมีกฎหมายที่เป็นลายลักษณ์อักษรให้อำนาจไว้ และต้องเป็นไปตาม “หลักแห่งความได้สัดส่วน” (Principle of Proportionality หรือ Verhältnismäßigkeitsprinzip) ซึ่งประกอบด้วยหลักย่อยอีกสามหลัก[12] คือ

1) “หลักแห่งความสัมฤทธิ์ผล” (Geeignetheit) คือ ในบรรดามาตรการต่างๆ ที่รัฐธรรมนูญก็ดี หรือกฎหมายฉบับอื่นก็ดี เปิดช่องให้องค์กรของรัฐใช้อำนาจจำกัดสิทธิและเสรีภาพของบุคคลได้นั้น รัฐจะต้องเลือกใช้มาตรการที่สามารถดำเนินการให้บรรลุตามเจตนารมณ์ หรือสิ่งที่รัฐธรรมนูญหรือกฎหมายนั้นประสงค์จะให้เกิดขึ้นเท่านั้น กล่าวอีกอย่างก็คือ หลักแห่งความสัมฤทธิ์ผลนี้เรียกร้องให้ต้องมีการตรวจสอบดุลยภาพระหว่าง เหตุ (cause) และ ผล (effect)[13]

2) “หลักแห่งความจำเป็น” (Erforderlichkeit) กล่าวคือ หากมาตรการที่องค์กรของรัฐจะใช้เพื่อจำกัดสิทธิและเสรีภาพของบุคคลมีหลายมาตรการ องค์กรของรัฐต้องเลือกออก หรือเลือกใช้มาตรการที่กระทบกระเทือนต่อสิทธิและเสรีภาพนั้นน้อยที่สุด เพื่อให้บรรลุเจตนารมณ์ของรัฐธรรมนูญ และกฎหมายแล้วแต่กรณี

3) “หลักแห่งความเหมาะสม” (Angemessenheit) กล่าวคือ มาตรการหรือวิธีการที่จะองค์กรของรัฐจะใช้เพื่อจำกัดสิทธิและเสรีภาพตามกฎหมาย จะต้องชั่งน้ำหนักความได้สัดส่วนกัน หากปรากฏว่ามาตรการนั้นถ้าใช้แล้วจะก่อให้เกิดประโยชน์แก่มหาชนน้อยมาก ไม่คุ้มกับความเสียหาย

ที่จะเกิดแก่สิทธิและเสรีภาพของบุคคล เช่นนี้ องค์กรของรัฐต้องละเว้นไม่ใช้มาตรการเช่นว่านั้น[14]

แม้หลักแห่งความได้สัดส่วนนี้จะไม่ได้บัญญัติเป็นลายลักษณ์อักษร แต่ในประเทศเยอรมนีถือว่าเป็น “หลักทั่วไป” ตามกฎหมายมหาชน ที่สถาบันและองค์กรต่าง ๆ ของรัฐต้องยึดถือปฏิบัติ ทั้งนี้เพื่อให้สิทธิและเสรีภาพของประชาชนได้รับการคุ้มครองอย่างแท้จริง

สำหรับเนื้อหาที่ตกอยู่ภายใต้ข้อยกเว้น และไม่ได้รับความคุ้มครองตามกฎหมายแห่งประเทศเยอรมนี หรือกล่าวอีกนัยหนึ่งคือเนื้อหาที่หากเผยแพร่ต่อสาธารณะแล้วอาจเป็นความผิดตามกฎหมายได้ ส่วนใหญ่มีเหตุผลเบื้องหลังที่สำคัญ คือ เพื่อ “คุ้มครองเด็กและเยาวชน” (Jugendschutz) จากสิ่งซึ่งอาจเป็นภัยอันตราย หรือกระทบต่อพัฒนาการทางความคิดในเรื่องต่าง ๆ ไม่ว่าจะเป็นเรื่องในทางเพศ หรือความก้าวร้าวรุนแรง นอกเหนือจากนี้ก็เพื่อคุ้มครองเกียรติยศชื่อเสียงของบุคคล และเพื่อรักษาสันติภาพในการอยู่ร่วมกันของประชาชนในประเทศ อย่างไรก็ตาม ควรต้องทำความเข้าใจก่อนว่า การเผยแพร่เนื้อหาที่เป็นความผิดตามกฎหมายเยอรมันนี้ มิได้หมายความโดยอัตโนมัติว่ารัฐมีอำนาจปิดกั้นช่องทางการเข้าถึง หรือระงับการเผยแพร่ดังกล่าวได้ในทุกกรณี หากแต่มีเฉพาะบางกรณีที่เท่านั้นที่รัฐสามารถใช้มาตรการเร่งด่วนได้ ในขณะที่บางกรณีรัฐต้องฟ้องคดีผู้กระทำผิดเสียก่อน และบางกรณีรัฐคงทำได้แค่เพียงกำหนด “เงื่อนไขพิเศษ” เพื่อป้องกันไม่ให้มีการเผยแพร่กับเด็กและเยาวชนเท่านั้น ทำนองเดียวกับที่มาตรา 20 พ.ร.บ. คอมพิวเตอร์ฯ 2550 เองก็ไม่ได้ให้อำนาจรัฐไทยปิดกั้นเนื้อหาที่ผิดกฎหมายได้ทุกประเภท แต่หมายเฉพาะเนื้อหาที่มีความร้ายแรงถึงขนาดไม่อาจให้เผยแพร่ต่อไปได้เท่านั้น

โดยอาจจำแนกเนื้อหาต่าง ๆ ที่ต้องห้ามไม่ให้เผยแพร่ หรือการเผยแพร่จะเป็นความผิดตามกฎหมายฉบับต่าง ๆ ของเยอรมนีได้ ดังนี้

2.1 เนื้อหาที่มีลักษณะลามกอนาจาร (Pornographie)

ตามกฎหมายของประเทศเยอรมนี ภาพลามกอนาจารถูกจำแนก

ออกเป็น 2 ระดับ คือ ภาพลามกอนาจารธรรมดา (einfache Pornographie - § 184 StGB) และภาพลามกอนาจารที่ร้ายแรง (harte Pornographie - § 184a StGB) “ภาพลามกธรรมดา” (einfache Pornographie) หมายถึง ภาพต่างๆ ที่เข้าข่ายลามกอนาจาร เช่น ภาพแสดงการมีเพศสัมพันธ์ไม่ว่าด้วยวิธีการใดๆ หรือกิจกรรมในทางเพศอื่นๆ ซึ่งในภาพนั้นต้องไม่มีลักษณะของการใช้รุนแรงหรือกระทำทารุณกรรม (Gewaltätigkeit) ไม่มีภาพการร่วมเพศหรือทำกิจกรรมทางเพศระหว่างมนุษย์กับสัตว์ (sexuelle Handlungen mit Tieren) หรือการล่วงละเมิดทางเพศต่อเด็กและเยาวชน (sexuellen Missbrauch von Kindern – Kinderpornographie[15]) หากภาพลามกอนาจารมีลักษณะต้องห้ามต่างๆ ดังกล่าวปรากฏอยู่ ภาพจะถูกเพิ่มระดับให้กลายเป็นภาพลามกอนาจารในขั้นร้ายแรง (harte Pornographie) ทันที ทั้งนี้ ตามข้อตกลงระหว่างรัฐว่าด้วยการคุ้มครองเด็กและเยาวชนจากการนำเสนอสิ่งใดๆ ในสื่อ (Jugendmedienschutz-Staatsvertrag - JMStV) ยังระบุไว้อย่างชัดเจนด้วยว่า ภาพลามกอนาจารในระดับร้ายแรงให้หมายรวมถึงภาพที่สร้าง หรือจำลองขึ้น หรือที่ไม่ได้ใช้คนจริงๆ เป็นผู้แสดง (virtuellen Darstellungen) ด้วย ซึ่งแตกต่างจากประมวลกฎหมายอาญาที่ยังไม่ได้กำหนดถึงภาพลามกที่เกิดจากการจำลองหรือสร้างขึ้นดังกล่าว

ประมวลกฎหมายอาญามาตรา 184 (§ 184 StGB) ห้ามไม่ให้ผู้ใดเผยแพร่หรือเปิดช่องทางการเข้าถึงภาพลามกอนาจารทั้งสองระดับดังกล่าวให้แก่เด็กและเยาวชน[16] ซึ่งหมายรวมทั้งการเผยแพร่ในสื่อทุกชนิด และสื่อออนไลน์ด้วย ทำนองเดียวกับที่บัญญัติห้ามไว้ในมาตรา 4 (1) ข้อ 10[17] และมาตรา 4 (2) ข้อ 1[18] ตามข้อตกลงระหว่างรัฐว่าด้วยการคุ้มครองเด็กและเยาวชนจากการนำเสนอสิ่งใดๆ ในสื่อ (JMStV) หรือมาตรา 15 (2) ข้อ 1 แห่งพระราชบัญญัติคุ้มครองเด็กและเยาวชน (Jugendschutzgesetz - JuSchG) อย่างไรก็ตาม ภาพลามกอนาจารในระดับธรรมดา (einfache Pornographie) สามารถเผยแพร่แก่ผู้ใหญ่ได้โดยไม่เป็นความผิด[19] รวมทั้งอนุญาตให้มีไว้ในความครอบครองด้วย แต่สำหรับภาพลามกอนาจารระดับร้ายแรง (harte Pornographie) นั้น กฎหมายอาญาเยอรมันห้ามเผยแพร่ต่อสาธารณะโดย

เด็ดขาดไม่ว่าต่อเด็กและเยาวชน หรือต่อผู้ใหญ่ (§ 184a StGB) และใครก็ตามเพียงมีไว้ในครอบครองก็มีความผิดตามกฎหมายเยอรมัน ซึ่งกรณีที่อาจเกิดขึ้นได้บนสื่อออนไลน์ อาทิ การดาวน์โหลดภาพเหล่านั้นมาเก็บไว้ในคอมพิวเตอร์ส่วนตัว หรืออุปกรณ์เก็บบันทึกข้อมูลประเภทต่าง ๆ[20] เป็นต้น

นอกจากนี้ มาตรา 4 (1) ข้อ 9 JMStV และมาตรา 15 (2) ข้อ 4 JuSchG ยังกำหนดบทคุ้มครองเด็กและเยาวชนไว้กว้างกว่าประมวลกฎหมายอาญาอีกกรณีหนึ่งด้วย กล่าวคือ ห้ามมิให้ผู้ใดเผยแพร่ภาพเด็กและเยาวชนที่แม้เป็นเพียงการแสดงในลักษณะยั่วยุให้เกิดกำหนัด หรือเกิดกามารมณ์ (Erotographische Darstellungen) โดยไม่จำเป็นต้องแสดงการร่วมเพศ หรือขับเน้นกิจกรรมในทางเพศอย่างชัดเจน ที่เรียกว่า “Posing–Angebot” หรือ “Posendarstellungen von Minderjährigen” ด้วย

จะเห็นได้ว่า วัตถุประสงค์ในการห้ามมิให้เผยแพร่ภาพลามกอนาจารนั้นแท้จริงแล้ว มุ่งเน้นไปที่การคุ้มครองเด็กและเยาวชนเป็นสำคัญ ทั้งนี้โดยเป้าหมาย

1) เพื่อไม่ให้เด็กและเยาวชนเผชิญหน้ากับเรื่องราวที่เกี่ยวกับเพศก่อนวัยอันสมควร ซึ่งอาจส่งผลกระทบต่อทัศนคติ และพัฒนาการในทางเพศที่เหมาะสม และ

2) ไม่ให้เด็กและเยาวชนต้องตกเป็นเหยื่อในทางเพศของผู้ใหญ่ด้วยการเป็นผู้แสดง หรือมีส่วนร่วมกับฉากที่เกี่ยวกับเพศ รวมทั้งเหตุผลที่ว่ารัฐไม่ต้องการสนับสนุนให้เกิดกลุ่มบุคคลที่นิยมร่วมเพศกับเด็กและเยาวชน (Pedopien) ด้วย

2.2 เนื้อหาเผยแพร่แนวคิดลิทธิฝ่ายขวาหัวรุนแรง (Rechtsextremistische Angebot)

ข้อตกลงระหว่างรัฐว่าด้วยการคุ้มครองเด็กและเยาวชนจากการนำเสนอสิ่งใด ๆ ในสื่อ (Jugendmedienschutz-Staatsvertrag - JMStV) รวมทั้งลักษณะการดำเนินงานต่าง ๆ ของคณะกรรมการคุ้มครองเยาวชนจาก

สื่อสารมวลชน (Kommission für Jugendmedienschutz – KJM) ต่างก็ให้ความคุ้มครองเด็กและเยาวชนจากการเผยแพร่แนวคิดฝ่ายขวาหัวรุนแรงหรือลัทธิชาตินิยมเยอรมัน (Nationalsozialismus) โดยระบุไว้ในมาตรา 4 (1) ข้อ 1-4 JMStV[21] ว่าห้ามเผยแพร่เนื้อหาเหล่านี้ในช่องทางหรือสื่อใดๆ ที่เด็กและเยาวชนอาจเข้าถึงได้ ซึ่งย่อมหมายรวมถึงสื่อออนไลน์ด้วย อย่างไรก็ตาม นอกเหนือจากข้อตกลงที่คุ้มครองเด็กและเยาวชนเป็นพิเศษแล้ว สำหรับประเทศเยอรมนีนั้น การเผยแพร่แนวคิดลัทธิดังกล่าว รวมทั้งเนื้อหาอื่นๆ ในทำนองเดียวกันไม่ว่าด้วยวิธีการใดๆ ต่อประชาชนทั่วไป ก็ถือเป็นความผิดตามกฎหมายอาญาเยอรมันด้วย

สำหรับความหมายของลัทธิฝ่ายขวาหัวรุนแรง (Rechtsextremismus) นั้น มีความพยายามในการให้นิยามมาตั้งแต่ช่วงทศวรรษที่ 70 แต่ถึงปัจจุบันก็ไม่ชัดเจน และยังมีข้อถกเถียงกันว่าหมายถึงแนวคิดลักษณะใดบ้าง แต่ผลจากการศึกษาวิจัยโดยมูลนิธิฟรีดริค เอแบร์ท (Friedrich-Ebert-Stiftung) ในหัวข้อ “Vom Rand zur Mitte” ที่เผยแพร่ในปี 2006 ซึ่งพยายามค้นหาองค์ประกอบของอุดมการณ์ต่างๆ ดังกล่าวมาสรุปได้ว่าลัทธิฝ่ายขวาหัวรุนแรงน่าจะอยู่ในกลุ่มแนวคิดดังต่อไปนี้ 1) สนับสนุนเผด็จการนิยมฝ่ายขวา 2) ลัทธิคลั่งชาติ (Chauvinismus) 3) เกลียดชัง เลือกปฏิบัติ ต่อต้านคนต่างชาติ (Ausländerfeindlichkeit) 4) ลัทธิความเป็นอคติต่อชาวเซมิติค หรือลัทธิความเป็นอคติต่อชาวยิว (Antisemitism หรือ Judeophobia) ลัทธิสังคมแบบดาร์วิน (Sozialdarwinismus) หรือแนวคิดที่เกี่ยวกับการเลือกสรรแล้วโดยธรรมชาติ และความอยู่รอดของชนชาติที่เหมาะสมที่สุดของ ชาลส์ ดาร์วิน (Charles Darwin) นักวิทยาศาสตร์ชาวอังกฤษในคริสต์ศตวรรษที่ 19 ผู้เสนอ “ทฤษฎีวิวัฒนาการของสิ่งมีชีวิต” (Theory of Evolution[22]) รวมทั้งข้อมูลชวนเชื่อว่าลัทธิชาตินิยมนาซีเยอรมันเป็นลัทธิที่ไม่มีพิษภัย หรือเป็นลัทธิที่มีความสมเหตุสมผลดีแล้ว[23]

อนึ่ง เนื่องจากการบังคับใช้กฎหมายในประเทศเยอรมนีเป็นไปอย่างเคร่งครัด จึงปรากฏว่าการเผยแพร่เนื้อหาในลักษณะดังกล่าว โดยเฉพาะอย่างยิ่งการเผยแพร่ในสื่อออนไลน์ส่วนใหญ่ไม่ใช่เว็บไซต์ของ

ประเทศเยอรมนี หรือจากคอมพิวเตอร์เซิร์ฟเวอร์ที่อยู่ในประเทศเยอรมนีเอง แต่เป็นเว็บไซต์หรือเซิร์ฟเวอร์ที่ตั้งอยู่ในต่างประเทศ[24] เว็บไซต์แรกที่ถูกจับตามองในประเทศเยอรมนีชื่อว่า “Thule-Web” ซึ่งก่อนหน้านั้นระบบจดหมายเวียน (mailing list) ของ “Thule-Netz” ถูกใช้ในฐานะสื่อใหม่เพื่อแลกเปลี่ยนข้อมูลข่าวสารกันระหว่างกลุ่มชาตินิยมนาซีหลายกลุ่ม รวมทั้งหลายพรรคการเมืองของประเทศเยอรมนี (Republikaner, DVU, NPD) มาตั้งแต่ราวปี 1993 ต่อมาจึงเกิดเว็บไซต์ “Thule-Web” เพื่อนำเสนอข้อมูลข่าวสารที่มีเนื้อหาเกี่ยวกับแนวคิดลัทธิฝ่ายขวาหัวรุนแรง และการแบ่งแยกเชื้อชาติ

ความพยายามในการจัดการกับ Thule-Web ของประเทศเยอรมนีประสบความล้มเหลว เพราะชื่อโดเมนของเว็บไซต์นี้จดทะเบียนในนาม Max Mustermann กับเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ Dreamhaven ซึ่งตั้งอยู่ในประเทศสหรัฐอเมริกา[25] จนในปี 1995 ชาวอเมริกันที่ใช้ชื่อว่า Don Black ตั้งเว็บภายใต้ชื่อโดเมน www.stormfront.org เพื่อเผยแพร่ลัทธิฝ่ายขวาหัวรุนแรง การแบ่งแยกเชื้อชาติ และทฤษฎีการปฏิวัติ[26] ซึ่งในเว็บนี้มีห้องแลกเปลี่ยนภาษาเยอรมันโดยเฉพาะชื่อว่า Stormfront auf Deutsch ด้วย ก่อนที่เว็บไซต์ดังกล่าวจะถูกคำสั่งปิดกั้นโดยรัฐสภาเมืองดึสเซลดอร์ฟเมื่อเดือนมิถุนายน 2002 ปัจจุบัน เว็บไซต์นี้ไม่สามารถเข้าถึงได้แล้วในประเทศเยอรมนี เช่นเดียวกันกับ nazi-lauck-nsdapao.com ของ Gary Lauck[27] ซึ่งนำเสนอเนื้อหาลัทธิฝ่ายขวาเป็นภาษาต่างๆ ถึง 12 ภาษา ภาพการ์ตูนนาซีเยอรมัน เปิดให้ดาวน์โหลดหนังสือ “Mein Kampf” ของฮิตเลอร์ ฉากกิจกรรมของลัทธิฝ่ายขวาหัวรุนแรงเยอรมัน ช่องทางการสั่งซื้อเครื่องหมายสวัสดิกะ รวมทั้งข้อแนะนำการใช้อินเทอร์เน็ตเป็นอาวุธในการโฆษณาชวนเชื่อได้อย่างไร (“Wie Du das Internet als Propagandawaffe nutzen kannst”) หรือวิธีการเข้าถึงเว็บไซต์ที่ต้องห้ามหรือถูกปิดกั้น (“Wie man eine gesperrte/verbotene Netzseite aufrufen kann!”)

2.3 เนื้อหาสนับสนุนความรุนแรง หรือละเมิดศักดิ์ศรีความเป็นมนุษย์ (Gewaltverherrlichung und Verstöße gegen die Menschenwürde)

หลายปีที่ผ่านมา ประเทศเยอรมนีให้ความสำคัญกับการคุ้มครองเด็กและเยาวชนจากข้อมูลที่มีเนื้อหาเกี่ยวกับความรุนแรงในรูปแบบต่างๆ โดยเฉพาะอย่างยิ่งความรุนแรงที่ปรากฏอยู่ในรูปของเกมคอมพิวเตอร์ ผลพวงจากเหตุฆาตกรรมหมู่โดยนักเรียนอายุ 19 ปี ที่เมืองแอร์ฟูร์ท เมื่อปี 2002[28] ซึ่งภายหลังสืบสวนได้ความว่านักเรียนผู้ก่อเหตุ นอกจากมีปัญหากับเพื่อนและอาจารย์ที่โรงเรียนแล้ว ยังติดเกมคอมพิวเตอร์ที่มีเนื้อหารุนแรงด้วย ก่อให้เกิดประเด็นถกเถียงระดับชาติเกี่ยวกับระดับความรุนแรงของเกมคอมพิวเตอร์ ต้นเดือนเมษายน 2003 พระราชบัญญัติคุ้มครองเด็กและเยาวชนก็ถูกแก้ไขเพิ่มเติม และประกาศใช้อย่างรวดเร็ว เรื่องสำคัญที่ถูกบรรจุเพิ่มเติมในกฎหมายก็คือ เกมคอมพิวเตอร์ เป็นสื่อที่ต้องถูกจัดระดับความเหมาะสม (rate) และติดเครื่องหมายแสดงระดับอายุที่เหมาะสมของผู้เล่น เช่นเดียวกับสื่อทีวี ภาพยนตร์ หรือวิดีโอที่ทำไปแล้วก่อนหน้านี้

เนื้อหาที่จัดเป็นเรื่องต้องห้ามในหัวข้อนี้อีกลักษณะหนึ่งที่แพร่หลายอยู่ในอินเทอร์เน็ต ก็คือ เว็บไซต์รวมรูปภาพที่ไร้รสนิยมต่างๆ รู้จักกันในชื่อ “tasteless” (Geschmacklosigkeit) เว็บไซต์ที่เป็นที่รู้จักอย่างกว้างขวาง อาทิ Rotten.com ซึ่งนำเสนอภาพเหยื่ออาชญากรรม ผู้ได้รับบาดเจ็บจากอุบัติเหตุ ผู้ป่วยโรคร้ายแรง ภาพศพ รวมทั้งภาพการทรมานนักโทษในคุก Abu Ghraib ซึ่ง Rotten.com แสดงจุดยืนว่าเว็บไซต์จะเสนอภาพที่แม้ไม่เหมาะสม แต่ก็ไม่ผิดกฎหมาย อย่างไรก็ตาม เว็บไซต์ดังกล่าวขัดต่อข้อตกลงระหว่างรัฐที่คุ้มครองเยาวชนจากการนำเสนอสิ่งใดๆ ในสื่อ (§ 4 Abs. 1 Nr. 8 JMStV[29]) ในฐานะที่มีเนื้อหาละเมิดศักดิ์ศรีความเป็นมนุษย์ (Menschenwürdeverstoße) จึงเป็นเรื่องต้องห้ามไม่ให้เผยแพร่ โดยเฉพาะอย่างยิ่งกับเด็กและเยาวชน

2.4 เนื้อหาหมิ่นประมาทบุคคลอื่น (§ 185 ff. StGB)

ตามกฎหมายอาญาเยอรมัน ผู้ใดหมิ่นประมาทผู้อื่นในรูปแบบต่างๆ ตามที่กฎหมายกำหนดย่อมถือเป็นความผิดทั้งสิ้น ไม่ว่าจะได้กระทำผ่านสื่อประเภทใด หรือไม่ก็ตาม ดังนั้น แม้การกระทำเหล่านั้นจะเกิดขึ้นในระบบสื่อสารออนไลน์ อาทิ ส่งอีเมล หรือโดยผ่านบริการต่างๆ ทางเว็บไซต์ ผู้กระทำย่อมมีความผิดตามกฎหมายอาญาด้วย คดีหมิ่นประมาทบนอินเทอร์เน็ตคดีแรกที่เยอรมนี เกิดขึ้นเมื่อปี 1996 โดยศาลเมืองไรน์บาค (AG Rheinbach) ตัดสินว่า การใช้คำเรียกคู่สนทนาซึ่งเป็นผู้หญิง ในระหว่างการใช้บริการห้องสนทนาสาธารณะบนเครือข่ายอินเทอร์เน็ต (chat room หรือ ein öffenliches Diskussionsforum eines Onlinenetz) ว่า “Schlampe“ (“หญิงเลวๆ ที่มีความประพฤติไม่ดี”) ย่อมเป็นความผิดตามกฎหมายอาญา เพราะการใช้คำเรียกดังกล่าวสื่อไปในลักษณะเพื่อการหมิ่นประมาท[30]

จะเห็นได้ว่า โดยที่เยอรมนีไม่จำเป็นต้องบัญญัติกำหนดให้การหมิ่นประมาทบนเครือข่ายอินเทอร์เน็ต รวมทั้งบนการสื่อสารรูปแบบใหม่เป็นความผิดโดยเฉพาะเจาะจง หรือแยกบัญญัติเป็นกฎหมายเฉพาะใดๆ ศาลก็สามารถนำกฎหมายที่มีอยู่แล้วมาปรับใช้และตัดสินคดีความได้

2.5 เนื้อหาขัดต่อความสงบสันติและความเป็นระเบียบสาธารณะ[31]

นอกจากเนื้อหาที่เป็นความผิดในฐานหมิ่นประมาท หรือภาพลามกอนาจารแล้ว ประเทศเยอรมนียังกำหนดให้การเผยแพร่เนื้อหาข้อมูลที่ขัดต่อประโยชน์หรือความสงบสาธารณะ เป็นความผิดตามกฎหมายอาญาด้วย ซึ่งสามารถนำบทบัญญัติเหล่านั้นมาปรับใช้กับการกระทำที่เกิดขึ้นบนการสื่อสารออนไลน์ได้เช่นกัน อาทิ มาตรา 86 วรรค 1 และ 2 ของประมวลกฎหมายอาญา (StGB) การเปิดช่องทางให้เข้าถึงข้อมูลหรือโฆษณาชวนเชื่อให้กับองค์กรที่ขัดต่อกฎหมายรัฐธรรมนูญ (Propagandamittel in Datenspeichern öffentlich zugänglich zu machen) มาตรา 86a วรรค 1 (1) StGB การใช้สัญลักษณ์ขององค์กรที่ตั้งขึ้นโดยขัดต่อกฎหมายรัฐธรรมนูญ

(Verwendung von Kennzeichen verfassungswidriger Organisationen) เช่น แสดงสัญลักษณ์ขององค์กรนาซีในหน้าเว็บไซต์ การใช้ถ้อยคำเพื่อสร้างความแตกแยกในหมู่ประชาชน (Volksverhetzung - § 130 StGB) โดยการยั่วยุ ปลุกปั่นความรุนแรง ทำลายศักดิ์ศรีความเป็นมนุษย์โดยใช้ถ้อยคำเชิงปฏิปักษ์ที่ชัดเจน หรือโดยอาศัยความแตกต่างในเรื่องความเชื่อ เชื้อชาติ ศาสนา มากล่าวร้ายด่าทอคนกลุ่มใดกลุ่มหนึ่ง โดยมุ่งหมายสร้างความเกลียดชังให้เกิดขึ้นในหมู่ประชาชนหรือทำลายสันติภาพในสังคมโดยรวม

มาตรา 126 และ 130a ของประมวลกฎหมายอาญา ยังห้ามมิให้เผยแพร่ข้อมูลในที่ประชุมชุมนุมชนหรือผ่านสื่อเพื่อประกาศให้บุคคลกระทำความผิดตามกฎหมายอาญา ข่มขู่ด้วยวิธีการใดๆ (เช่น เผยแพร่คำขู่ประกาศเป็นการสาธารณะ ฯลฯ) เพื่อรบกวนสันติภาพสาธารณะ (der öffenliche Friede) ว่าจะกระทำความผิดที่ร้ายแรงต่างๆ อาทิ ฆาตกรรม (Mod - § 211 StGB) ฆ่าล้างเผ่าพันธุ์ (Völkermord - § 6 des Völkerstrafgesetzbuches) ก่อสงคราม (§§ 8, 9, 10, 11 oder 12 des Völkerstrafgesetzbuches) เป็นต้น

2.6 การพนันผิดกฎหมาย (§ 284 ff. StGB)

ประมวลกฎหมายอาญาเยอรมันบัญญัติห้ามมิให้ ให้บริการหรือจัดดำเนินการการพนันที่ไม่ได้รับอนุญาตจากรัฐ ไว้ตามมาตรา 284 วรรค 1 ซึ่งองค์ประกอบความผิดตามมาตราดังกล่าว สามารถนำมาปรับใช้กับการกระทำที่เกิดขึ้นในระบบสื่อสารออนไลน์ได้ หากเครื่องคอมพิวเตอร์เหล่านั้นดำเนินการหรือเปิดให้ผู้อื่นเล่นการพนันได้ เช่น เว็บไซต์การพนัน จำพวกคาสิโนออนไลน์ที่ไม่ได้รับอนุญาตจากรัฐ เป็นต้น ซึ่งนอกจากการบริการให้เล่นการพนันแล้ว ผู้โฆษณาแหล่งการพนันผิดกฎหมาย โดยเฉพาะอย่างยิ่งกรณีที่เจ้าของเว็บไซต์ทำไฮเปอร์ลิงก์ (hyperlink) จากหน้าเว็บไซต์ของตนไปยังเว็บไซต์การพนันผิดกฎหมาย ก็ถือเป็นความผิดเช่นกัน ตามความที่กำหนดไว้ในมาตรา 284 วรรค 4 และมาตรา 285 แห่งประมวลกฎหมายอาญา

ผู้เล่นการพนันกับแหล่งการพนันดังกล่าวย่อมมีความผิดด้วย

3. อาชญากรรมคอมพิวเตอร์ กับการเผยแพร่เนื้อหาผิดกฎหมายในสื่อออนไลน์

ประเทศสหพันธรัฐเยอรมนี ถือเป็นประเทศต้นๆ ในทวีปยุโรปที่ให้ความสำคัญกับปัญหาการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์และอินเทอร์เน็ต การถกเถียงในวงวิชาการเพื่อแสวงหามาตรการทางกฎหมาย รวมทั้งมาตรการอื่นๆ ที่เหมาะสมเพื่อป้องกันและปรามปรามการกระทำผิดเหล่านี้เกิดขึ้นตั้งแต่ก่อนปี 1986 ทั้งนี้เนื่องจากอัตราการกระทำความผิดในลักษณะดังกล่าวเพิ่มขึ้นอย่างต่อเนื่องไม่ว่าจะเป็น การฉ้อโกงทางคอมพิวเตอร์ (Computerbetrug) การปลอมแปลงข้อมูลคอมพิวเตอร์ (Datenveränderung) การเจาะระบบคอมพิวเตอร์ การจารกรรมข้อมูลส่วนบุคคลหรือข้อมูลทางการค้า (Computerspionage) การพนันผิดกฎหมายออนไลน์ รวมไปถึงการเผยแพร่ภาพลามกอนาจารเด็กและเยาวชน (Kinderpornographie) เคยมีรายงานการสำรวจการกระทำความผิดเหล่านี้ในยุคต้นๆ ในเยอรมนีพบว่าประมาณร้อยละ 1 ของเว็บไซต์ที่ให้บริการอยู่ในประเทศทั้งหมดเป็นเว็บไซต์ที่มีเนื้อหาผิดกฎหมาย[32] ปัญหาต่างๆ ที่เกิดขึ้น ส่งผลให้หน่วยงานผู้รับผิดชอบเร่งหาแนวทางในการป้องกันและปราบปรามที่มีประสิทธิภาพไม่ว่าจะเป็นการจัดตั้งหน่วยงานพิเศษเพื่อรับผิดชอบการกระทำความผิดด้านนี้เป็นการเฉพาะ ซึ่งในบางกรณีก็จำเป็นต้องกำหนด หรือใช้มาตรการบางประการที่ส่งผลกระทบทั้งต่อผู้ให้บริการและผู้ใช้บริการอินเทอร์เน็ตด้วย[33]

แม้อนุสัญญาว่าด้วยอาชญากรรมไซเบอร์ (Convention on Cybercrime)[34] ซึ่งออกโดยคณะมนตรียุโรป (Europarat) จะมีผลตั้งแต่วันที่ 1 กรกฎาคม 2004 ภายหลังมีประเทศลงนามให้สัตยาบันครบ 5 ประเทศ[35] ตามเงื่อนไขที่กำหนด แต่ประเทศเยอรมนีซึ่งลงนามในอนุสัญญาฉบับดังกล่าวตั้งแต่วันที่ 23 พฤศจิกายน 2001 กลับให้สัตยาบันและยัง

ผลให้ประเทศมีหน้าที่ต้องบัญญัติหรือปรับปรุงกฎหมายให้สอดคล้องกับอนุสัญญาฉบับนี้เมื่อวันที่ 9 มีนาคม 2009 สาเหตุที่เยอรมนีให้สัตยาบันรวมทั้งอนุวัติการตามอนุสัญญา (วันที่ 1 กรกฎาคม 2009)[36] ค่อนข้างล่าช้า เยอรมนีให้เหตุผลว่าข้อกำหนด และหลักเกณฑ์หลายข้อในอนุสัญญาดังกล่าวไม่สอดคล้องกับนโยบาย และมาตรการที่ประเทศเยอรมนีใช้บังคับอยู่แล้ว จึงต้องใช้เวลาในการศึกษาวิจัย และพิจารณาว่าจะสามารถปรับเปลี่ยนข้อกฎหมายภายในได้มากน้อยเพียงใด อย่างไรก็ตาม หากกล่าวถึงประวัติการบัญญัติ รวมทั้งการแก้ไขปรับปรุงกฎหมายเพื่อรองรับปัญหาการกระทำความผิดในรูปแบบใหม่เหล่านี้ ต้องนับว่าประเทศเยอรมนีตื่นตัวและดำเนินการมาเป็นระยะเวลานานแล้ว ตั้งแต่ปี 1986 ซึ่งมีการปฏิรูปกฎหมายหลายฉบับเพื่อป้องกันและปราบปรามอาชญากรรมทางเศรษฐกิจ (2. WiKG)[37] เยอรมนีเพิ่มเติมฐานความผิดหลักๆ ที่เกี่ยวกับคอมพิวเตอร์ไว้ในประมวลกฎหมายอาญาร่วมกับฐานความผิดดั้งเดิมในหมวดเดียวกัน ในขณะที่ฐานความผิดเฉพาะอื่นๆ อาทิ ความผิดเกี่ยวกับการละเมิดทรัพย์สินทางปัญญาบนอินเทอร์เน็ต[38] ข้อกำหนดเกี่ยวกับภาระหน้าที่รวมทั้งความรับผิดของผู้ให้บริการอินเทอร์เน็ตประเภทต่างๆ[39] จะถูกบัญญัติแยกไว้ในกฎหมายเฉพาะ สำหรับปัญหาในทางแพ่งและพาณิชย์ก็มีกฎหมายในเรื่องนั้นต่างหากเช่นกัน โดยเฉพาะอย่างยิ่ง เพื่อรองรับปฏิบัติการและธุรกรรมรูปแบบใหม่ๆ

ฝ่ายนิติบัญญัติประเทศเยอรมนีเห็นว่า มีการกระทำความผิดจำนวนมาก อาทิ ความผิดเกี่ยวกับทรัพย์ (เช่น การฉ้อโกง) การหมิ่นประมาท การเผยแพร่เนื้อหาที่เป็นภัยอันตรายต่อเด็กและเยาวชน หรือความผิดในลักษณะที่ทำให้เสียหายต่อสิทธิหรือพื้นที่ส่วนบุคคล ที่แม้อาศัยสื่อออนไลน์เป็นเครื่องมือ ก็ยังสามารถใช้กฎหมายอาญาทั่วไป รวมทั้งกฎหมายเฉพาะอื่นๆ ที่มีอยู่แล้ว ปรับใช้เพื่อลงโทษได้ เพราะความผิดเหล่านี้มีองค์ประกอบความผิดเช่นเดียวกับความผิดดั้งเดิม จึงไม่มีความจำเป็นที่รัฐต้องบัญญัติฐานความผิดขึ้นใหม่หรือแยกบัญญัติเป็นกฎหมายเฉพาะที่เกี่ยวกับคอมพิวเตอร์หรืออินเทอร์เน็ต ในขณะที่ความผิดบางประเภท เช่น การ

ฉ้อโกงคอมพิวเตอร์ การปลอมแปลง หรือโจรกรรมข้อมูลคอมพิวเตอร์ รวมทั้งการก่อวินาศกรรมคอมพิวเตอร์ นอกจากอาชญากรจะใช้เครื่องมือใหม่กระทำความผิดแล้ว องค์ประกอบความผิดยังเปลี่ยนแปลงไปด้วย แต่องค์ประกอบที่เปลี่ยนไปก็มีเพียงบางส่วน จึงยังสามารถบัญญัติมาตราเฉพาะเพิ่มเติมไว้ในหมวดความผิดเดียวกันในประมวลกฎหมายอาญาได้ เช่น เพิ่มความผิดฐานฉ้อโกงคอมพิวเตอร์ไว้ในหมวดความผิดฐานฉ้อโกง (ธรรมดา) เพิ่มความผิดฐานก่อวินาศกรรมคอมพิวเตอร์ไว้ในหมวดเดียวกับความผิดฐานทำให้เสียทรัพย์ เป็นต้น ด้วยเหตุนี้เอง ที่ผ่านมาประเทศเยอรมนีจึงรับมือกับอาชญากรรมเหล่านี้โดยอาศัยวิธีแก้ไขเพิ่มเติมไว้ในประมวลกฎหมายอาญาในหมวดหมู่ที่ใกล้เคียงเท่านั้น มิได้บัญญัติเป็นกฎหมายเฉพาะอย่างหลายๆ ประเทศ

สำหรับเครื่องมือทางกฎหมาย และมาตรการต่างๆ ที่ประเทศเยอรมนีใช้ดำเนินการกับเว็บไซต์หรือสื่อออนไลน์ที่เผยแพร่เนื้อหาผิดกฎหมายนั้น นอกจากบทบัญญัติที่กำหนดโทษสำหรับผู้เผยแพร่เนื้อหาที่เป็นความผิด ซึ่งต้องมีการนำคดีขึ้นสู่การพิจารณาของศาลตามกระบวนการปกติแล้ว ประเทศเยอรมนียังมีกฎหมายให้อำนาจรัฐใช้มาตรการเร่งด่วนเพื่อปิดกั้นช่องทางการเข้าถึงเว็บไซต์ หรือสื่อออนไลน์ที่มีเนื้อหาเป็นความผิดได้เช่นกัน โดยเฉพาะอย่างยิ่งมาตรการที่กำหนดไว้ในข้อตกลงระหว่างมลรัฐว่าด้วยสื่อบริการ (Der Mediendienstestaatsvertrag - MDStV) ซึ่งเป็นกฎหมายที่กำหนดลักษณะการให้บริการ ภาระหน้าที่และความรับผิดชอบของผู้ให้บริการสื่อเหล่านั้น ลักษณะเนื้อหาที่ต้องห้าม รวมทั้งสิ่งที่ผู้ให้บริการสื่อต้องดำเนินการเมื่อเกิดเนื้อหาที่เป็นความผิดขึ้น ทั้งนี้ ผู้ให้บริการสื่อออนไลน์บางประเภทมีหน้าที่โดยทั่วไป ในการต้องคอยดูแลเนื้อหาและบริการของตน รวมทั้งตรวจสอบการแสดงความคิดเห็นให้เสนอเฉพาะในสิ่งที่ชอบด้วยรัฐธรรมนูญ กฎหมายทั่วไป รวมทั้งกฎหมายที่คุ้มครองเกียรติยศชื่อเสียงของบุคคล ในขณะที่ผู้ให้บริการสื่อออนไลน์บางประเภท โดยเฉพาะอย่างยิ่งที่เกี่ยวกับการจำหน่ายสินค้าหรือให้บริการ ซึ่งตนเป็นเพียงตัวกลางรายงานข่าวสาร ต้องมีการตรวจสอบความเท็จจริงของข้อความ แยกข้อเท็จ

จริงกับความคิดเห็น รวมทั้งต้องแสดงตัวของผู้เขียน

ข้อตกลงระหว่างมลรัฐที่คุ้มครองเยาวชนจากการนำเสนอสิ่งใดๆ ในสื่อ (Jugendmedienschutz-Staatsvertrag – JMStV) จะต้องถูกนำมาใช้บังคับกับสื่อบริการประเภทต่างๆ ตามกฎหมายฉบับนี้ด้วย (§ 12 Unzulässige Mediendienste, Jugendschutz) โดยในมาตรา 22 ที่ว่าด้วย "การควบคุมดูแล" (Aufsicht) กำหนดให้แต่ละมลรัฐสามารถแต่งตั้งเจ้าพนักงานควบคุมดูแลการให้บริการในพื้นที่ของตน และหากพบการฝ่าฝืนหน้าที่ตามที่กำหนดไว้ ก็สามารถใช้มาตรการใดๆ ที่เหมาะสมและเพียงเท่าที่จำเป็นเพื่อบังคับการให้เป็นไปตามกฎหมายฉบับนี้ได้ โดยเฉพาะอย่างยิ่ง อาจสั่งห้ามมิให้ให้บริการ หรือกระทั่งปิดกั้นสื่อบริการเหล่านั้น[40] แต่มาตรการที่จะใช้ต้องเป็นไปตามเงื่อนไข และรายละเอียดตามที่กฎหมายกำหนด รวมทั้งต้องตกอยู่ภายใต้ "หลักแห่งความได้สัดส่วน" (Verhältnismäßigkeitsprinzip) ที่ประกอบด้วยหลักแห่งความสัมฤทธิ์ผล หลักแห่งความจำเป็น และหลักแห่งความเหมาะสม ตามที่เคยกล่าวถึงไปแล้ว ซึ่งกำหนดไว้ตอนท้ายของมาตรา 22 (2)[41]

4. แนวนโยบาย กฎหมาย และแนวทางปฏิบัติที่เกี่ยวกับสื่อออนไลน์

4.1 การควบคุมเนื้อหาความรุนแรงในเกมคอมพิวเตอร์

รัฐบาลเยอรมันมีนโยบายแข็งกร้าวเพื่อจัดระเบียบเกมคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งเกมออนไลน์ที่มีเนื้อหารุนแรงราวปี 2003 หลังเกิดเหตุสะเทือนขวัญที่เมืองแอร์ฟูร์ท ซึ่งมีนักเรียนใช้ปืนยิงเพื่อนนักเรียน อาจารย์ในโรงเรียน และฆ่าตัวตายตาม ภายหลังเหตุการณ์นี้ ได้เกิดการถกเถียงระดับชาติ จนต้นเดือนเมษายน 2003 กฎหมายคุ้มครองเด็กและเยาวชนก็ถูกแก้ไขเพิ่มเติมและประกาศใช้ ประเด็นหลักก็คือ กำหนดเพิ่มเติมให้เกมคอมพิวเตอร์ เป็นสื่อที่ต้องส่งเข้าสู่การพิจารณาเพื่อติดเครื่องหมายแสดงระดับอายุผู้เล่นที่เหมาะสม (ติดเรท) เหมือนกับสื่อทีวี ภาพยนตร์ หรือวิดีโอ ซึ่งเป็นสื่อควบคุมตามกฎหมายไปก่อนหน้าแล้ว นอกจากนี้ ยังกำหนดให้

องค์กรผู้ดูแลและคุ้มครองเด็กและเยาวชนแห่งรัฐต่าง ๆ มีหน้าที่คอยกำกับดูแลผู้ให้บริการสื่อสารทางไกล กำหนดมาตรการและกลไกตรวจสอบเพื่อควบคุมกันเอง รวมทั้งผลักดัน และสนับสนุนพ่อแม่หรือผู้ปกครองติดตั้งโปรแกรมกรองเนื้อหาที่เครื่องคอมพิวเตอร์เพื่อป้องกันการเข้าถึงภาพลามกหรือเนื้อหาที่อาจมีผลทำลายพัฒนาการ จากเด็กและเยาวชน

อย่างไรก็ตาม นักการเมืองบางพรรค เช่น พรรคคริสเตียนเดโมแครต (CDU) กลับเห็นว่า มาตรการเหล่านี้ก็ยังไม่เพียงพอ ทั้งเรียกร้องให้รัฐออกกฎหมายห้ามขายหรือจำหน่ายเกมอันตราย หรือเกมที่มีเนื้อหารุนแรงและเกี่ยวกับการฆ่า (Killerspielen) โดยเฉพาะอย่างยิ่งเกม Counter Strike ให้กับเด็กและเยาวชนโดยเด็ดขาด หากฝ่าฝืนก็ให้มีโทษถึงขั้นจำคุกหรือปรับในอัตราสูง ในขณะที่บางพรรค อย่างพรรคกรีน (Grün) เห็นว่าเป็นมาตรการที่รุนแรงเกินไป ทั้งกระทบต่อเสรีภาพในการรับรู้ข้อมูลข่าวสารและศิลปะวิทยาการตามที่รัฐธรรมนูญรับรอง เป็นผลให้เกิดการอภิปรายโต้เถียงกันยาวนานในสภา

4.2 การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และโทรคมนาคม

กระแสการก่อการร้ายสากล ที่ขยายวงความกังวลไปทั่วโลกยังผลให้หลายประเทศต่างพากันออกมาตรการทางกฎหมายกำหนดหน้าที่จัดเก็บข้อมูลจราจรคอมพิวเตอร์ และข้อมูลเกี่ยวกับเส้นทางการติดต่อสื่อสารต่าง ๆ แก่ผู้ให้บริการโทรคมนาคม ทั้งนี้ เพื่อประโยชน์ในการสืบหาตัวผู้กระทำความผิด ในกรณีของประเทศเยอรมนีนั้น วันที่ 9 พฤศจิกายน 2007 รัฐสภาเยอรมันผ่านกฎหมายแก้ไขเพิ่มเติมกฎหมายโทรคมนาคม[42] เพื่อควบคุมตรวจสอบการติดต่อสื่อสาร และเพื่อประโยชน์ต่อการสืบสวนการกระทำความผิด เรียกว่า Vorratsdatenspeicherung (telecommunication data retention) โดยผู้ให้บริการโทรคมนาคมต้องเก็บข้อมูลจราจร (traffic data) ของผู้ใช้บริการไว้ไม่น้อยกว่า 6 เดือน[43] บทบัญญัติดังกล่าวมีผลบังคับใช้ตั้งแต่วันที่ 1 มกราคม 2008 (เว้นแต่ผู้ให้บริการอินเทอร์เน็ตเท่านั้นที่

กฎหมายมีผลต้นปี 2009 เพื่อให้เวลาในการเตรียมการ)

อย่างไรก็ตาม ภายหลังการประท้วงคัดค้านจากประชาชนจำนวนมาก เนื่องจากมองว่ารัฐพยายามสอดส่องพฤติกรรมของประชาชนในประเทศแบบไม่เลือกหน้า จนมีการฟ้องคดีต่อศาลรัฐธรรมนูญว่าบทบัญญัติดังกล่าวขัดกับรัฐธรรมนูญ เพราะมีลักษณะละเมิดสิทธิความเป็นส่วนตัวจนเกินจำเป็น และในวันที่ 2 มีนาคม 2010 ศาลรัฐธรรมนูญเยอรมันตัดสินให้กฎหมายฉบับนี้เป็นโมฆะ รวมทั้งสั่งให้ผู้ให้บริการโทรคมนาคมที่จัดเก็บข้อมูลต่าง ๆ ของประชาชนไว้แล้วทำลายข้อมูลดังกล่าวเสีย[44]

4.3 มาตรการค้นออนไลน์

การค้นพยานหลักฐานออนไลน์ (Online-Durchsuchung) หมายถึง การเข้าถึงระบบข้อมูลสารสนเทศของผู้อื่น โดยฝ่ายเจ้าหน้าที่รัฐผ่านระบบโทรคมนาคม ทั้งนี้ หมายรวมทั้งการเข้าถึงแบบครั้งต่อครั้งเพื่อค้นหาข้อมูลที่ต้องการ (Online-Durchsicht) และการติดตั้งโปรแกรมบางประเภท เช่น โปรแกรมโทรจัน ไว้ในระบบข้อมูลเป้าหมาย เพื่อสอดแนมสังเกตการณ์ระยะยาว (Online-überwachung)

โดยเหตุที่กฎหมายเยอรมันยังไม่ได้บัญญัติกำหนดให้รัฐสามารถใช้วิธีการใด ๆ เพื่อให้ได้มาซึ่งข้อมูลของผู้ต้องสงสัย จึงเกิดแนวคิดว่า ควรกำหนดให้การค้นพยานหลักฐานออนไลน์เป็นวิธีที่รัฐสามารถทำได้ภายในกรอบของการดำเนินคดีอาญา หรือกระทั่งเพียงเพื่อป้องกันภยันตรายที่มีแนวโน้มว่าจะเกิดขึ้น โดยลักษณะของการค้นออนไลน์โดยรัฐนั้น ควรเป็นการทำแบบครั้งต่อครั้ง โดยมีหมายอนุญาตจากศาล และเฉพาะการค้นคอมพิวเตอร์ส่วนตัวของผู้ที่ถูกกล่าวหาว่ากระทำความผิดในคดีที่มีโทษร้ายแรงเท่านั้น เป้าหมายคือเพื่อให้ได้มาซึ่งพยานหลักฐานที่เกี่ยวกับการกระทำความผิด และด้วยวิธีการดังกล่าว ย่อมทำให้รัฐสามารถตรวจค้นเนื้อหาจากคอมพิวเตอร์ที่เกี่ยวพันกับการกระทำผิดได้โดยเจ้าหน้าที่รัฐไม่จำเป็นต้องเสียเวลาเดินทางไปที่คอมพิวเตอร์เป้าหมาย

อย่างไรก็ตาม แนวคิดดังกล่าวถูกตั้งคำถาม และมีประเด็นโต้

แย้งในวงการกฎหมายหลายประเด็น อาทิ การค้นออนไลน์ ถือเป็น “การค้น” ตามนัยของกฎหมายวิธีพิจารณาความหรือไม่ และส่วนต่างๆ ในคอมพิวเตอร์ โดยเฉพาะพื้นที่ที่ใช้สำหรับเก็บข้อมูลต่างๆ ของเจ้าของระบบน่าจะเปรียบเทียบได้กับบ้านพัก หรือที่รโหฐาน ซึ่งเป็นพื้นที่ส่วนบุคคล จึงควรได้รับความคุ้มครองโดยรัฐธรรมนูญในระดับที่ไม่แตกต่างกัน[45]

4.4 การกำหนดภาระหน้าที่แก่ผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต (access provider) ต้องปิดช่องทางการเข้าถึงเว็บไซต์ที่มีเนื้อหาลามกอนาจารเด็กและเยาวชน

การให้ความสำคัญอย่างมากกับการคุ้มครองเด็กและเยาวชนในเรื่องนี้ กอรปกับปัญหาในแง่ขอบเขตการบังคับใช้กฎหมายเยอรมันต่อข้อมูลที่มีต้นตอการเผยแพร่อยู่ในต่างประเทศ ปัญหาความร่วมมือระหว่างประเทศในการแสวงหาพยานหลักฐาน รวมทั้งความยุ่งยากในการส่งตัวผู้ต้องหามาดำเนินคดี เป็นเหตุผลสำคัญที่ทำให้ประเทศเยอรมนีต้องการจำกัดการเข้าถึงภาพลามกเด็กและเยาวชนให้เข้มงวดมากขึ้น จนในปี 2008 ได้มีความพยายามผลักดันร่างกฎหมายว่าด้วยการปิดกั้นช่องทางการเข้าถึงภาพลามกอนาจารเด็ก (Kinderpornografie) ในสื่ออินเทอร์เน็ต เข้าสู่สภา ทั้งนี้ เพื่อกำหนดภาระหน้าที่แก่ผู้ให้บริการประเภทเชื่อมต่ออินเทอร์เน็ต (access provider) ให้เป็นผู้ปิดกั้นช่องทางการเข้าถึงเว็บไซต์ตามบัญชีรายชื่อซึ่งจัดทำขึ้นโดยสำนักงานตำรวจแห่งชาติ

Joerg Ziercke ผู้บัญชาการสำนักงานตำรวจแห่งชาติ (der Präsident des deutschen Bundeskriminalamts) เคยกล่าวแสดงความเห็นด้วยและพร้อมให้ความร่วมมือกับนโยบายนี้ ทั้งยังเคยเข้าหารือเกี่ยวกับการบัญญัติกฎหมายด้วย นโยบายดังกล่าวส่วนหนึ่งเป็นผลมาจากมติที่ได้จากการประชุมสภาคองเกรสโลกครั้งที่ 3 ว่าด้วยการต่อต้านการล่วงละเมิดทางเพศต่อเด็กและเยาวชน (World Congress III against Sexual Exploitation of Children & Adolescents) ณ กรุงริโอ เดอจาเนโร ในเดือนพฤศจิกายน 2008 โดยประเทศสมาชิกในทวีปยุโรปควรร่วมกันหาทางพัฒนาแนวปฏิบัติ

เกี่ยวกับเรื่องนี้ รวมทั้งวางนโยบายเพื่อให้เกิดการประสานกันระหว่างผู้ให้บริการอินเทอร์เน็ต ศูนย์ข้อมูลแห่งชาติ พนักงานสอบสวน และองค์การตำรวจอาชญากรรมระหว่างประเทศ (Interpol)

รัฐบาลเยอรมันโดย Ursula von der Leyen รัฐมนตรีว่าการกระทรวงครอบครัว (Familienministerin) ซึ่งดูแลงานด้านครอบครัว เด็กและเยาวชน สังคมและวัฒนธรรม เริ่มดำเนินนโยบายนี้ก้าวแรกในเดือนเมษายน 2009 ด้วยการจัดให้ผู้ให้บริการอินเทอร์เน็ตรายใหญ่ลงนามทำข้อตกลงกับรัฐบาลว่าจะดำเนินการปิดกั้นช่องทางการเข้าถึงเนื้อหาเกี่ยวกับภาพลามกเด็กและเยาวชนในอินเทอร์เน็ตตามบัญชีรายชื่อเว็บไซต์ที่จะจัดทำขึ้นโดยสำนักงานตำรวจแห่งชาติ สัญญานี้สิ้นสุดในเดือนธันวาคม 2010[46] ทั้งนี้ สำนักงานตำรวจแห่งชาติจะไม่เปิดเผยรายชื่อเว็บไซต์ในบัญชี เป็นการทั่วไปด้วยเหตุผลด้านความปลอดภัยสาธารณะและเพื่อคุ้มครองทรัพย์สินทางปัญญา มีบริษัทผู้ให้บริการเชื่อมต่ออินเทอร์เน็ตรายใหญ่ร่วมทำสัญญาดังกล่าวจำนวน 5 ราย[47] ในขณะที่รายอื่นๆ ปฏิเสธไม่ทำสัญญาที่อยู่นอกเหนือกฎหมาย นอกจากนี้บางบริษัท (เช่น Manitu) ยังแจ้งแก่รัฐบาลด้วยว่าหากมีการบังคับใช้กฎหมายดังกล่าวกับผู้ให้บริการอินเทอร์เน็ตจริง ก็อาจฟ้องต่อศาลรัฐธรรมนูญ เนื่องจากน่าจะเป็นบทบัญญัติที่ขัดกับรัฐธรรมนูญมาตรา 5 ที่คุ้มครองเสรีภาพในการรับรู้ข้อมูลข่าวสาร

Das Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz – ZugErschwG[48]) คือ กฎหมายว่าด้วยการปิดกั้นช่องทางการเข้าถึงภาพลามกอนาจารเด็ก (Kinderpornograpie) ในสื่ออินเทอร์เน็ต ถูกประกาศและมีผลเป็นกฎหมาย (de jure) ตั้งแต่วันที่ 23 กุมภาพันธ์ 2010 (BGBl. I S. 78) แต่กำหนดให้เวลาแก่หน่วยงานรัฐที่เกี่ยวข้อง และผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต ซึ่งมีหน้าที่ปิดกั้นช่องทางตามกฎหมายฉบับนี้เตรียมความพร้อมในด้านต่างๆ เพื่อปฏิบัติตามกฎหมายอีกราว 2 ปี ดังนั้น กฎหมายจะมีผลบังคับใช้ในทางความเป็น

จริง (de facto) ในวันที่ 1 มกราคม 2013 อย่างไรก็ตาม ในท้ายที่สุด ZugErschwG ถูกยกเลิกเพิกถอนไปก่อนในปี 2011โดยรัฐบาลสมัยที่สองของนาง Angela Merkel ทั้งยังมีการเปลี่ยนแนวทางในการแก้ปัญหาเรื่องนี้จากการปิดกั้นช่องทางการเข้าถึง ซึ่งอาจส่งผลกระทบกับเนื้อหาประเภทอื่นๆ ด้วย ไปเป็นการลบเนื้อหาเฉพาะส่วนที่ผิดกฎหมายแทน[49]

ข้อกำหนดหลักๆ ของ Zugangserschwerungsgesetz ที่ถูกยกเลิกไปแล้ว คือ กำหนดให้สำนักงานตำรวจแห่งชาติ มีหน้าที่รวบรวม และจัดทำบัญชีรายชื่อโดเมน เลขหมายไอพี และยูอาร์แอลของเว็บไซต์ที่เผยแพร่หรือเชื่อมโยง ข้อมูลที่มีเนื้อหาเป็นภาพลามกเด็กและเยาวชน ซึ่งเป็นความผิดตามประมวลกฎหมายอาญามาตรา 184b ทั้งนี้ ทั้งที่เป็นเว็บไซต์ภายในประเทศและต่างประเทศ รายชื่อเหล่านี้จะถูกรวบรวมบันทึกไว้ในกรณีที่รัฐเยอรมันไม่สามารถดำเนินการลบข้อมูลนั้นได้เลย หรือไม่สามารถลบได้ในเวลาที่เหมาะสม โดยผู้ให้บริการเชื่อมต่ออินเทอร์เน็ตที่มีลูกค้าใช้บริการมากกว่าหนึ่งหมื่นคนขึ้นไป จะได้รับบัญชีรายชื่อเว็บไซต์ดังกล่าว และมีหน้าที่ต้องปิดกั้นช่องทางการเข้าถึงชื่อโดเมน รวมทั้งเปลี่ยนเส้นทางการเรียกดูข้อมูลจากเว็บไซต์ภาพลามกเด็กนั้นไปยังหน้าที่แสดงเครื่องหมาย “Stopp-Schild” ที่สำนักงานตำรวจแห่งชาติจัดทำขึ้นแทน

กฎหมายยังกำหนดให้สำนักงานตำรวจแห่งชาติ ต้องจัดทำเอกสารหลักฐานแสดงเหตุผลในการปิดกั้นช่องทางการเข้าถึงเว็บไซต์ต่างๆ และจะถูกตรวจสอบเป็นรายไตรมาส โดยวิธีการสุ่มตรวจสอบโดยคณะกรรมการผู้เชี่ยวชาญ ซึ่งได้รับการแต่งตั้งจากคณะกรรมการเพื่อการคุ้มครองข้อมูลแห่งชาติ (Bundesdatenschutzbeauftragt) อย่างไรก็ตาม ตั้งแต่เริ่มนโยบาย กระบวนการจัดทำร่างกฎหมาย ขั้นตอนการพิจารณา กระทั่งการลงมติในรัฐสภาเพื่อผ่านออกมาบังคับใช้ กฎหมายฉบับนี้ถูกประท้วงคัดค้านมาโดยตลอด ทั้งจากประชาชนทั่วไป สมาคมต่างๆ ที่เกี่ยวข้องกับการใช้และการให้บริการอินเทอร์เน็ตและคุ้มครองเสรีภาพในการรับรู้ข้อมูลข่าวสาร รวมทั้งพรรคการเมืองที่ไม่เห็นด้วยกับการใช้มาตรการปิดกั้นช่องทางสื่อสาร

5. การปิดกั้นช่องทางการเข้าถึงเว็บไซต์ และสื่อออนไลน์ในประเทศเยอรมนี

จากที่กล่าวมาทั้งหมด ย่อมเห็นได้ว่า แม้ในประเทศเยอรมนีซึ่งให้ความสำคัญกับการคุ้มครองสิทธิและเสรีภาพของประชาชนอย่างมากแล้ว ก็มีประเด็นต่าง ๆ ที่รัฐสามารถใช้เครื่องมือและมาตรการทางกฎหมายดำเนินการกับเนื้อหาที่ต้องห้ามมิให้นำเสนอหรือเผยแพร่ต่อสาธารณะได้ก่อนหน้าที่จะมีนโยบาย รวมทั้งความพยายามในการออกกฎหมายกำหนดหน้าที่แก่ผู้ให้บริการเชื่อมต่ออินเทอร์เน็ตให้คอยปิดกั้นการเข้าถึงเว็บไซต์ที่เสนอภาพลามกอนาจารเด็กและเยาวชน ประเทศเยอรมนีเคยมีกรณีที่รัฐสั่งปิดกั้นสื่อออนไลน์มาแล้วหลายครั้ง ที่สำคัญ ๆ ก็คือ

5.1 การปิดกระดานข่าวในปี 1991/1992

ซึ่งถือเป็นการ “ปิดกั้นอินเทอร์เน็ต” ครั้งแรกที่เกิดขึ้นในประเทศเยอรมนี[50] โดยเหตุการณ์นี้เริ่มต้นขึ้นจากการเสนอข่าวโดยนิตยสาร Emma ถึงการเผยแพร่ภาพลามกอนาจารในกระดานข่าว (Usenet) ซึ่งในสมัยนั้นกระดานข่าวเกือบทั้งหมดใช้คอมพิวเตอร์เซิร์ฟเวอร์ของมหาวิทยาลัย ทั้งกล่าวด้วยว่าบรรดานักวิชาการ อาจารย์ และนักศึกษาในมหาวิทยาลัยต่างพากันใช้เทคโนโลยีคอมพิวเตอร์เพื่อการเสพภาพลามกอนาจารที่มีทั้งประเภททารุณและซาดิสต์ ซึ่งการใช้ช่องทางจราจรข้อมูลและพื้นที่บันทึกของคอมพิวเตอร์ไปเพื่อการดังกล่าวย่อมส่งผลกระทบต่อภาษีของประชาชนที่สนับสนุนให้กับมหาวิทยาลัยอย่างมิอาจหลีกเลี่ยงได้ ทั้งยังทำให้เจ้าหน้าที่และนักศึกษาหญิงรู้สึกว่าถูกคุกคามทางเพศหากยังคงมีการบริโภคสื่อลามกในรั้วมหาวิทยาลัย ภายหลังจากการเสนอข่าวโดย Emma และมีสื่ออีกหลายสำนักตีแผ่ปัญหานี้ ผู้บริหารของหลายมหาวิทยาลัยในประเทศเยอรมนีต่างพากันปิด (Sperren) ห้องสนทนาจำนวนมาก และปรากฏว่าหลายกรณีที่โดนปิดไปไม่ใช่กระดานข่าวที่เผยแพร่ภาพลามก แต่เป็นพื้นที่สำหรับพูดคุยแลกเปลี่ยนระหว่างคนเพศทางเลือก

5.2 การปิดกั้นคอมพิวเตอร์เซิร์ฟเวอร์ www.xs4all.nl ในปี 1996/1997 เดือนเมษายนปี 1997 ประเทศเยอรมนี

โดยสถาบันวิจัยอินเทอร์เน็ตเยอรมัน (Das Deutsch Forschungs Netzt - DFN) ได้รับคำสั่งจากอัยการสูงสุด (Die Bundesanwaltschaft) ให้ปิดกั้นการเข้าถึงคอมพิวเตอร์เซิร์ฟเวอร์ XS4ALL ซึ่งเป็นของผู้ให้บริการชาวเนเธอร์แลนด์ การปิดโฮสต์ดังกล่าวเป็นเหตุให้ผู้ใช้บริการอินเทอร์เน็ตที่อยู่ในประเทศเยอรมนีเข้าถึงเว็บเพจไม่ได้ราว 3,100 ยูอาร์แอล ทั้งนี้ ด้วยเหตุผลเพราะในเซิร์ฟเวอร์ XS4ALL มีเว็บไซต์บางเว็บที่เผยแพร่เนื้อหาความรุนแรงที่เป็นความผิดตามกฎหมายอาญาของประเทศเยอรมนี[51] การปิดกั้นครั้งนั้น ยังผลให้เว็บไซต์สองแห่งของนาง Angela Marquardt[52] ซึ่งเป็นประชาชนเยอรมัน ถูกปิดกั้นไปด้วยเพียงเพราะเว็บไซต์ของเธอได้เชื่อมโยง ไปยังข้อมูลที่มีเนื้อหาเกี่ยวพันกับลัทธิฝ่ายซ้ายหัวรุนแรง[53] ก่อนที่จะถูกฟ้องต่อศาลแขวงเมืองเบอร์ลิน (Amtsgericht Berlin-Tiergarten) ซึ่งในท้ายที่สุดศาลพิพากษายกฟ้องโดยยกประโยชน์แห่งความสงสัยให้เธอ เนื่องจากพนักงานอัยการไม่สามารถพิสูจน์ให้เห็นได้ว่า Marquardt รู้ถึงเนื้อหาของเว็บไซต์ที่เธอเชื่อมโยงไปหรือไม่[54]

5.3 การปิดกั้นเว็บไซต์ ปี 2001/2002

ราวปลายปี 2001 Jürgen Büssow ผู้ว่าการเมืองดึสเซลดอร์ฟแห่งรัฐนอร์ดไรน์-เวสท์ฟาเลิน (Nordrhein-Westfalen) เป็นโจทก์ฟ้องผู้ให้บริการอินเทอร์เน็ตจำนวน 56 รายเป็นจำเลยฐานเผยแพร่เนื้อหาที่เป็นความผิดตามกฎหมายบนเครือข่ายอินเทอร์เน็ต รวมทั้งสั่งให้ปิดกั้นช่องทางการเข้าถึงเว็บไซต์สี่แห่ง ได้แก่ rotten.com, front14.org, nazi-lauck-nsdapao.com และ stormfront.org เพราะมีเนื้อหาเกี่ยวกับลัทธิฝ่ายขวาหัวรุนแรง (rechtsradikal) ละเมิดศักดิ์ศรีความเป็นมนุษย์ (Menschen-würde) สนับสนุนการทำสงคราม (kriegsverherrlichend) เป็นภัยต่อเด็กและเยาวชน (jugendgefährdend) รวมทั้งยุยงให้เกิดความเกลียดชังแตกแยกในหมู่ประชาชน (Volksverhetzung) ซึ่งล้วนแล้วแต่เป็นเรื่องต้อง

ห้ามตาม MDStV ขัดกับหลักการคุ้มครองสิทธิเสรีภาพในรัฐธรรมนูญ และเป็นความผิดตามกฎหมายอาญา ทั้งนี้โดยอาศัยข้อตกลงระหว่างรัฐว่าด้วยสื่อบริการ (Der Mediendienste-Staatsvertrag - MDStV) มาตรา 12 ว่าด้วย “สื่อบริการที่ต้องห้ามเผยแพร่” (§ 12 Unzulässige Mediendienste, Jugendschutz) และมาตรา 22 (2) ซึ่งให้อำนาจมลรัฐในการกำกับดูแลรวมทั้งกำหนด “มาตรการที่เหมาะสม” เพื่อดำเนินการกับสื่อนั้น (§ 22 Abs. 2 MDStV) พร้อมกันนั้น Büssow ยังพยายามเรียกร้องให้ประเทศเยอรมนีมีนโยบายควบคุมเนื้อหาในอินเทอร์เน็ตให้เข้มงวดยิ่งขึ้น

นอกจากนี้ ปี 2006 ช่วงของการแข่งขันฟุตบอลโลกที่ประเทศเยอรมนีเป็นเจ้าภาพ รัฐบาลยังปิดกั้นเว็บไซต์การพนันผิดกฎหมายที่ใช้ชื่อว่า Bwin[55] ด้วย

6. ปฏิกิริยาและความเคลื่อนไหวของประชาชนและภาคสังคมที่มีต่อกฎหมาย และนโยบายแห่งรัฐที่กระทบเสรีภาพในสื่อออนไลน์

ความเคลื่อนไหวภาคประชาชนในประเทศเยอรมนี โดยเฉพาะอย่างยิ่งที่เกี่ยวกับการออกกฎหมายและนโยบายรัฐ ที่อาจส่งผลกระทบต่อเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นในสื่อออนไลน์นั้นเกิดขึ้นบ่อยครั้ง หลากหลายรูปแบบ จากหลากหลายองค์กร ตั้งแต่การชุมนุมประท้วงคัดค้าน การทำคำโต้แย้งและเปิดให้ประชาชนทั่วไปร่วมลงชื่อออนไลน์ ทำความร่วมมือกับนักวิชาการ ผู้ประกอบวิชาชีพ เพื่อผลิตข้อเขียนหรือบทความเผยแพร่ให้ความรู้กับประชาชนผู้อาจได้รับผลกระทบ ที่สำคัญคือ การนำเรื่องขึ้นสู่ศาลไม่ว่าจะเป็นศาลปกครองหรือศาลรัฐธรรมนูญ ซึ่งผลลัพธ์ในท้ายที่สุดมีทั้งกรณีที่ศาลตัดสินยืนยันการใช้อำนาจของรัฐ และกรณีที่พิพากษายกเลิกคำสั่งหรือกฎหมาย ด้วยเหตุว่าขัดกับรัฐธรรมนูญ โดยมีกรณีสำคัญๆ ที่เคยเกิดขึ้น ดังนี้

6.1 ปฏิกิริยาต่อคำสั่งให้ปิดกั้นช่องทางการเข้าถึงเว็บไซต์

ปฏิกิริยาของภาคประชาชนที่ชัดเจนเกี่ยวกับกรณีที่รัฐใช้อำนาจปิดกั้นช่องทางการเข้าถึงเว็บไซต์ เกิดขึ้นกับการสั่งปิดกั้นเว็บไซต์สี่แห่งในปี 2001/2002 เกิดการประท้วง ล่ารายชื่อทางอินเทอร์เน็ตต่อต้านคำสั่งผู้ว่าการฯ[56] ทั้งมีการนำเรื่องฟ้องศาลปกครอง จัดแคมเปญต่อต้าน ออกจดหมายโต้แย้ง สัมมนาวิชาการ และจัดเวทีอภิปราย อย่างไรก็ตาม ปี 2005 ศาลปกครอง แห่งเมืองดึสเซลดอร์ฟ ตัดสินยืนยันว่าคำสั่งของ Jürgen Büssow ผู้ว่าการรัฐที่ให้ผู้ให้บริการอินเทอร์เน็ตปิดกั้นเว็บไซต์ดังกล่าวเป็นคำสั่งที่ชอบด้วยกฎหมาย[57] นอกจากนี้ ในเวลาต่อมาบรรดากลุ่มผู้ประท้วงบางส่วนยังถูกฟ้องศาลในฐานก่อให้เกิดความเกลียดชังแตกแยกในหมู่ประชาชน (Volkverhetzung) อีกด้วย ซึ่งจากเหตุการณ์ดังกล่าวจะเห็นได้ว่า ในที่สุดแล้วแม้ในประเทศเยอรมนี ซึ่งให้ความสำคัญกับการคุ้มครองเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงออกซึ่งความคิดเห็นอย่างมาก ก็เคยเกิดกรณีรัฐปิดกั้นการเข้าถึงเว็บไซต์ จนเกิดการประท้วงคัดค้านมาแล้ว แต่ประเด็นที่ควรตั้งเป็นข้อสังเกตก็คือ ประเภทเนื้อหาที่ถูกปิดกั้น รวมทั้งอำนาจในการสั่งการล้วนแต่ต้องมีตัวบทกฎหมายรับรองไว้โดยชัดเจน ฝ่ายประท้วงและผู้ไม่เห็นด้วยกับการปิดกั้นเองก็สามารถยกหลักในการคุ้มครองเสรีภาพในกฎหมายฉบับต่างๆ ขึ้นโต้แย้งกับฝ่ายรัฐในชั้นศาลได้ เพื่อนำไปสู่คำพิพากษาที่ยืนยัน “หลักการ” ตามกฎหมาย

6.2 ปฏิกิริยาต่อการแก้ไขกฎหมายโทรคมนาคม (Telekomunikationsgestez - TKG) กำหนดหน้าที่แก่ผู้ให้บริการโทรคมนาคมให้เก็บรักษาข้อมูลจราจรนาน 6 เดือน

วันที่ 9 พฤศจิกายน 2007 รัฐสภาเยอรมันผ่านกฎหมายแก้ไขเพิ่มเติมกฎหมายโทรคมนาคม[58] ฉบับหนึ่ง เพื่อควบคุมตรวจสอบการติดต่อสื่อสาร และเพื่อประโยชน์ต่อการสอบสวนการกระทำความผิดท่ามกลางเสียงประท้วงจากคนเยอรมันนับหมื่นคน เนื่องจากกฎหมายดังกล่าวมีบทบัญญัติที่อาจกระทบสิทธิความเป็นส่วนตัว รวมทั้งเสรีภาพ

ในการติดต่อสื่อสาร ซึ่งหมายรวมถึงการติดต่อสื่อสารทางอินเทอร์เน็ตด้วย เรียกว่า Vorratsdatenspeicherung (telecommunication data retention) โดยกำหนดหน้าที่แก่ผู้ให้บริการโทรคมนาคมต้องข้อมูลจราจร (traffic data) ของประชาชนผู้ใช้บริการทุกคนไว้เป็นระยะเวลา 6 เดือน[59] ด้วยเหตุผลว่า เพื่อประโยชน์ในการสืบสวนสอบสวนการกระทำความผิด บทบัญญัติดังกล่าวมีผลบังคับใช้ตั้งแต่วันที่ 1 มกราคม 2008 (เว้นแต่ผู้ให้บริการอินเทอร์เน็ตเท่านั้น ที่กฎหมายมีผลต้นปี 2009 เพื่อให้เวลาในการเตรียมการ) แม้บทบัญญัตินี้ไม่อนุญาตให้ผู้ให้บริการเก็บ “เนื้อหา” (content) ของการติดต่อสื่อสาร แต่การจัดเก็บข้อมูลที่ใช้สืบสาวหรือรู้ได้ว่าใครติดต่อทำอะไรกับใคร ที่ไหน เมื่อไร ของทุกๆ คนโดยปราศจากข้อกล่าวหา (เก็บของทุกคนไว้ก่อนมีข้อกล่าวหา) เป็นสิ่งที่คนเยอรมันมิอาจยอมรับได้

ภายใต้ข้อกำหนดนี้ เสรีภาพในการติดต่อสื่อสารและพื้นที่ความเป็นส่วนตัวจะถูกล่วงละเมิด การติดต่อสื่อสารที่ควรเป็นความลับในขอบเขตวิชาชีพต่างๆ โดยเฉพาะอย่างยิ่งการปรึกษาปัญหาทางการแพทย์ กฎหมาย ศาสนา รวมทั้งเสรีภาพในกิจกรรมทางการเมืองอาจถูกทำลายลง เพราะรัฐสามารถจับตาสอดแนม กล่าวให้ถึงที่สุดก็คือ “เสรีภาพในทางสังคม” จะได้รับความเสียหาย ก่อให้เกิดความหวาดระแวง หรือกลัวว่าข้อมูลของตนจะถูกนำไปใช้ในทางมิชอบอื่นใดนอกเหนือจากการสืบสวนดำเนินคดี ส่งผลให้ความเชื่อมั่นในการติดต่อสื่อสารของประชาชนลดน้อยลง และอาจส่งผลต่อพัฒนาการทางเทคโนโลยีสารสนเทศ ในขณะที่มีงานศึกษาวิจัยพบว่าการเก็บข้อมูลดังกล่าวไม่ได้ช่วยให้การสอบสวนอาชญากรรมทางอิเล็กทรอนิกส์หรือการป้องกันการก่อการร้ายมีประสิทธิภาพมากขึ้น หรือแตกต่างจากการสอบสวนโดยอาศัยข้อมูลที่ได้จากการร้องขอจากผู้ให้บริการที่จัดเก็บข้อมูลไว้ตามปกติธรรมดา (ไม่ได้เก็บล่วงหน้าก่อนเกิดเหตุ)

กระบวนการแก้ไขกฎหมายครั้งนั้นถูกประท้วง ทั้งจากประชาชนทั่วไป นักกฎหมาย กลุ่มไอที กลุ่มคุ้มครองข้อมูล และองค์กรทางเศรษฐกิจกว่า 40 องค์กร และภายหลังกฎหมายมีผลบังคับใช้ได้ไม่นาน (พฤศจิกายน 2007) บทบัญญัติในส่วนนี้ก็ถูกร้องเรียนต่อศาลรัฐธรรมนูญเยอรมัน

ที่เมืองคาร์ลสรูห์ ในวันที่ 31 ธันวาคม 2007 ซึ่งน่าสนใจว่าผู้ฟ้องศาลรัฐธรรมนูญในครั้งนี้มีจำนวนมากที่สุดในประวัติศาสตร์เยอรมัน[60] คือ มีโจทก์ร่วมกว่า 30,000 คน (มีเอกสารมอบอำนาจเป็นลายลักษณ์อักษร) พร้อมคำฟ้องอีกกว่า 150 หน้ากระดาษ[61] โดยมีกลุ่มทำงานเฉพาะกิจใช้ชื่อว่า German Working Group on Data Retention[62] เป็นผู้ขับเคลื่อนหลักในการให้ข้อมูลกับประชาชน จัดสัมมนา รวบรวมรายชื่อ ทำเอกสารมอบอำนาจเพื่อฟ้องร้อง ติดต่อประสานงานกับนักวิชาการ และกลุ่มองค์กรด้านสิทธิมนุษยชนและคุ้มครองข้อมูลข่าวสาร รวมทั้งทำโปสเตอร์รณรงค์ และจัดการประท้วงในรูปแบบต่างๆ และในท้ายที่สุดเมื่อวันที่ 2 มีนาคม 2010 ศาลรัฐธรรมนูญเยอรมันตัดสินให้กฎหมายฉบับนี้ตกเป็นโมฆะเพราะขัดกับรัฐธรรมนูญ ทั้งยังสั่งให้ผู้ให้บริการประเภทต่างๆ ที่ดำเนินการเก็บข้อมูลไปก่อนหน้านี้แล้วลบข้อมูลดังกล่าวทิ้งด้วย[63]

6.3 ปฏิกิริยาต่อกฎหมายปิดกั้นช่องทางการเข้าถึงภาพลามกอนาจารเด็กและเยาวชน (Zugangserschwerungsgesetz – ZugErschwG)

วันที่ 23 กุมภาพันธ์ 2010 Das Zugangserschwerungsgesetz หรือกฎหมายว่าด้วยการปิดกั้นช่องทางการเข้าถึงภาพลามกอนาจารเด็ก (Kinderpornografie) ในสื่ออินเทอร์เน็ต มีผลบังคับใช้เป็นกฎหมาย (de jure) แต่ให้เวลา 2 ปี แก่หน่วยงานรัฐที่เกี่ยวข้องและผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต ซึ่งเป็นผู้มีหน้าที่ปิดกั้นช่องทางตามกฎหมายฉบับนี้เตรียมความพร้อมในการปฏิบัติตามกฎหมาย วันที่ 1 มกราคม 2013 กฎหมายจะมีผลบังคับใช้ในความเป็นจริง (de facto) อย่างไรก็ตาม ปี 2011 กฎหมายฉบับนี้ถูกยกเลิกไป

ทั้งนี้ ตั้งแต่วันที่ 22 เมษายน 2009 Franziska Heine หญิงสาวเยอรมันอายุ 29 ปี จากเมืองเบอร์ลินได้เขียนคำร้องคัดค้านแผนการบัญญัติกฎหมายเพื่อการปิดกั้นเว็บไซต์ฉบับดังกล่าว และเปิดให้ประชาชนร่วมลงนามทางอินเทอร์เน็ต ตั้งแต่วันที่ 4 พฤษภาคม 2009[64] ปรากฏว่ามีผู้เข้าร่วม

ลงนามสนับสนุนคำร้องกว่า 134,000 คน[65] นอกจากการประท้วงคัดค้านที่หาแนวร่วมทางสื่อออนไลน์แล้ว องค์กรกลุ่มวิชาชีพและผู้ประกอบการซึ่งถูกตั้งขึ้นเฉพาะกิจเพื่อคัดค้านนโยบายปิดกั้นอินเทอร์เน็ตและการเซ็นเซอร์ (Arbeitskreises gegen Internetsperren und Zensur – AK Zensur)[66] เป็นอีกกลุ่มหนึ่งที่เกิดขึ้นในฐานะปฏิกิริยาต่อการบัญญัติกฎหมายฉบับนี้ โดยมีการศึกษาและพยายามชี้ให้เห็นว่ามาตรการปิดกั้นเว็บไซต์ไม่ใช่วิธีแก้ปัญหาที่ถูกต้อง รวมทั้งไม่ได้ทำให้การล่วงละเมิดทางเพศต่อเด็กและเยาวชนลดลงได้ เพราะแม้เว็บไซต์ตามบัญชีรายชื่อจะถูกปิดกั้นช่องทางการเข้าถึงไปแล้วก็ตาม แต่ในความเป็นจริงก็ยังสามารถเข้าถึงได้อยู่ดีด้วยเทคนิควิธีการพิเศษต่าง ๆ เนื่องจากภาพและเนื้อหาเหล่านั้นในที่สุดแล้วไม่ได้หายไปจากเครือข่ายอินเทอร์เน็ต

นอกจากนี้บรรดาคอลัมนิสต์ นักกฎหมาย สมาคมที่ตั้งขึ้นมาต่อต้านการปิดกั้นอินเทอร์เน็ต Missbrauchsopfern Gegen InternetSperren (MOGiS e.V.)[67] รวมทั้งองค์กรใหญ่ที่เฝ้าระวังและติดตามเรื่องราวเกี่ยวกับคอมพิวเตอร์ กฎหมายไอที สิทธิเสรีภาพกับสังคมออนไลน์มาโดยตลอดอย่าง Chaos Computer Club หรือ CCC[68] ต่างวิพากษ์วิจารณ์ว่ากฎหมายที่เกิดขึ้นโดยขาดการอภิปรายอย่างจริงจังฉบับนี้จะไม่สามารถจัดการกับปัญหาภาพลามกเด็กและเยาวชนได้ แต่เป็นการสร้างเครื่องมือในการตรวจสอบและเซ็นเซอร์ข้อมูลโดยทั่วไปเท่านั้น โดยข้อที่น่าสงสัยอย่างยิ่งในเจตนาของรัฐก็คือ การที่สำนักงานตำรวจแห่งชาติจะไม่เปิดเผยบัญชีรายชื่อเว็บไซต์ที่ถูกปิดกั้นเป็นการทั่วไป ซึ่งย่อมทำให้องค์กรอื่นไม่สามารถตรวจสอบการทำงานได้[69] ในขณะที่สมาคม Trotz Allem e.V. ซึ่งเป็นสมาคมคุ้มครองผู้หญิงจากการถูกล่วงละเมิดทางเพศ เขียนจดหมายเปิดผนึกถึงรัฐบาลระบุว่า การปิดกั้นเว็บไซต์ไม่ใช่การคุ้มครองเด็กและเยาวชนในโลกแห่งความเป็นจริง หากแต่เป็นการ “ปกป้องผู้กระทำความผิด (ที่เกี่ยวกับล่วงละเมิดเด็กและเยาวชน)” (Täterschutz)[70] ต่างหาก เนื่องจากวิธีการหนึ่งที่จะสามารถคุ้มครองเด็กจากการถูกล่วงละเมิดได้ก็คือ การค้นหาและนำตัวผู้กระทำกับเด็กมาลงโทษ แต่การชิงปิดกั้นเว็บไซต์จนทำให้ผู้ค้นหาภาพ

ลามกทางอินเทอร์เน็ตเข้าถึงไม่ได้ ย่อมทำให้ “กระทำความผิดไม่สำเร็จ” รวมทั้งไม่มีพยานหลักฐานเพื่อแสดงเจตนาของบุคคลนั้น[71] อย่างไรก็ดี ข้อคัดค้านที่สำคัญก็คือ กฎหมายฉบับนี้ส่งผลกระทบกับสิทธิและเสรีภาพที่รับรองไว้ในรัฐธรรมนูญอย่างน้อย 4 เรื่องด้วยกัน คือ เสรีภาพในการติดต่อสื่อสาร สิทธิในการเลือกบริโภคข้อมูลด้วยตนเอง เสรีภาพในการรับรู้ข้อมูลข่าวสาร และเสรีภาพในการประกอบอาชีพ (ของผู้ให้บริการอินเทอร์เน็ต)[72]

6.4 ปฏิกิริยาต่อการใช้มาตรการค้น (พยานหลักฐาน) ออนไลน์ (Online-Durchsicht, Online-Ueberwachung)

เมื่อครั้งที่ประเทศเยอรมนีต้องการนำมาตรการค้นออนไลน์มาใช้เพื่อการสืบสวนสอบสวนคดีอาญา ทั้งมีความพยายามตั้งแต่ปี 2007 ในการเสนอร่างกฎหมายว่าด้วยการค้นออนไลน์เพื่อการสืบสวนการกระทำความผิด (Gesetzentwurf zu Online-Durchsuchungen zu Strafverfolgungszwecken) นั้น ก็เกิดการประท้วงคัดค้านจากประชาชน และองค์กรหลายกลุ่มเช่นกัน โดยหากพิจารณาจากจำนวนผู้สนับสนุนแนวคิดให้อำนาจรัฐสามารถค้นออนไลน์ได้จากผลสำรวจประเด็นทางการเมือง (Politbarometer) พบว่าจำนวนผู้เห็นด้วยลดลงตามลำดับ จากที่เดือนกันยายนปี 2007 มีผู้สนับสนุนให้รัฐใช้มาตรการค้นออนไลน์ร้อยละ 65[73] แต่เมื่อสำรวจอีกครั้งในเดือนพฤศจิกายน ปี 2008 มีผู้สนับสนุนเหลือเพียงร้อยละ 57 เท่านั้น[74] การสำรวจเรื่องเดียวกันนี้ในเดือนตุลาคมปี 2011 ปรากฏว่ามีผู้ไม่เห็นด้วยกับการค้นออนไลน์ร้อยละ 52 ในขณะที่มีผู้เห็นด้วยเพียงร้อยละ 43[75] เดือนกุมภาพันธ์ ปี 2008 ศาลรัฐธรรมนูญเยอรมันมีคำตัดสินว่า ระเบียบว่าด้วยการค้นออนไลน์ ซึ่งใช้บังคับอยู่ในรัฐนอร์ดไรน์-เวสท์ฟาเลิน ขัดกับรัฐธรรมนูญ เพราะเป็นมาตรการที่ล่วงละเมิดและอาจส่งผลกระทบต่อสิทธิและพื้นที่ส่วนตัวซึ่งรัฐธรรมนูญรับรองคุ้มครองไว้

อย่างไรก็ตาม จากคำพิพากษานี้ ไม่ได้หมายความว่าการค้นออนไลน์ในทุกๆ กรณีขัดรัฐธรรมนูญและทำไม่ได้เลย หากเพื่อป้องกันภัยอันตรายที่จะเกิดขึ้น รัฐอาจใช้มาตรการค้นออนไลน์ได้ ถ้ามีการบัญญัติให้

อำนาจเป็นกฎหมายไว้โดยชัดแจ้ง ได้รับอนุญาตจากศาลภายใต้ข้อจำกัดที่เข้มงวดเพียงพอ[76] อนึ่ง แม้มีคำพิพากษาวางแนวในเรื่องนี้ไว้แล้ว แต่เดือนตุลาคม ปี 2011 องค์กร Chaos Computer Club หรือ CCC ออกมาเปิดเผยว่ายังมีหน่วยงานรัฐ และพนักงานสอบสวนใช้โปรแกรมสอดแนม (Spionagesoftware) ในสื่อต่างๆ ดังกล่าวอยู่ ซึ่งถือเป็นการปฏิบัติการที่ขัดต่อคำพิพากษาของศาลรัฐธรรมนูญ

7. บทสรุป

จากหลักการคุ้มครองเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นของประชาชนในรัฐธรรมนูญเยอรมัน ความชัดเจนของกฎหมายฉบับต่างๆ ที่กำหนดขึ้นเพื่อจำกัดสิทธิและเสรีภาพของประชาชนในเรื่องดังกล่าว แนวนโยบาย และวิธีปฏิบัติของรัฐ รวมทั้งปฏิกิริยาและความเคลื่อนไหวของภาคประชาชนตามที่กล่าวมา จะเห็นได้ว่าแม้ประเทศเยอรมนีจะให้ความสำคัญกับการคุ้มครองสิทธิและเสรีภาพของประชาชนอย่างมากแล้วก็ตาม แต่ในที่สุดก็ยังปรากฏกรณีที่รัฐใช้มาตรการเร่งด่วนเพื่อปิดกั้นเว็บไซต์ที่มีเนื้อหาบางอย่าง อย่างไรก็ดี มีข้อที่ควรสังเกตประการหนึ่งว่า การจำกัดการเข้าถึงเนื้อหาแบบเร่งด่วนก่อนที่ศาลจะพิพากษาว่าเนื้อหาเหล่านั้นเป็นความผิดจริงหรือไม่นั้น เยอรมนีจำกัดขอบเขตไว้ค่อนข้างเข้มงวดและชัดเจนในสองประเด็นหลักๆ คือ

1) เพื่อคุ้มครองเด็กและเยาวชน ซึ่งเยอรมนีถือว่าเป็นบุคคลที่รัฐจำเป็นต้องให้ความคุ้มครองเป็นพิเศษ โดยเฉพาะอย่างยิ่งในเรื่องที่เกี่ยวกับการใช้ความรุนแรง และลามกอนาจาร และ

2) เพื่อคุ้มครองสันติสุขและความสงบสุขของประชาชน (ไม่ใช่เพื่อความมั่นคงแห่งรัฐ ซึ่งเป็นเรื่องนามธรรม) ด้วยการไม่อนุญาตให้มีการเผยแพร่สิ่งยั่วยุ ปลุกปั่นโดยอาศัยความแตกต่างทางเชื้อชาติ ศาสนาเพื่อให้เกิดการดูถูกเหยียดหยามศักดิ์ศรีความเป็นมนุษย์ ก่อให้เกิดความรุนแรงและความแตกแยกในหมู่ประชาชน ซึ่งการเผยแพร่ลัทธิชาตินิยมนาซี

ทั้งลัทธิเก่าและใหม่ก็ล้วนแล้วแต่เกี่ยวพันกับประเด็นความรุนแรง และการแบ่งแยกดังกล่าว

อย่างไรก็ตาม หากพิจารณาจากกฎหมายฉบับต่างๆ ที่มีขึ้นเพื่อคุ้มครองเด็กและเยาวชนจากเนื้อหาอันเป็นภัยนั้น จะพบว่า การเผยแพร่แนวคิดชาตินิยมก็ดี การเลือกปฏิบัติก็ดี หรือการเหยียดหยามชนชาติอื่นก็ดี ล้วนแล้วแต่ถือเป็นสิ่งอันตรายต่อพัฒนาการด้านความคิดในเรื่องความเป็นมนุษย์ของเด็กและเยาวชนในสายตาของรัฐเยอรมันทั้งสิ้น ดังนั้น จึงอาจกล่าวได้ว่า สาระและเหตุผลสำคัญของการปิดกั้นข้อมูลในประเทศเยอรมนีก็คือ เพื่อวัตถุประสงค์ข้อ (1) นั่นเอง

สำหรับประเด็นความตื่นตัวต่อการคุ้มครองสิทธิและเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นนั้น พบว่าทั้งภาครัฐ และประชาชนต่างเห็นว่าสิทธิและเสรีภาพในเรื่องดังกล่าวมีความสำคัญอย่างยิ่งต่อกระบวนการสร้างประชาธิปไตย เพราะทำให้ประชาชนได้มีส่วนรวมในเรื่องการเมืองการปกครอง และสามารถแสดงเจตจำนงในเรื่องต่างๆ ได้อย่างอิสระ ในขณะที่องค์กรตุลาการ โดยเฉพาะอย่างยิ่ง ศาลรัฐธรรมนูญเยอรมันเคยพิพากษาว่ากฎหมายและมาตรการที่มีลักษณะล่วงละเมิดสิทธิและเสรีภาพของประชาชนเกินสมควรขัดรัฐธรรมนูญและให้สิ้นผลบังคับใช้ไปแล้วหลายต่อหลายกรณี ทางฝ่ายประชาชนและภาคสังคมเองก็ทำงานจับตาการใช้อำนาจของรัฐและปกป้องสิทธิและเสรีภาพของตนเองอย่างสม่ำเสมอ ดังจะเห็นได้ว่าในประเทศเยอรมนี มีกลุ่มประชาชน องค์กรต่างๆ ที่คอยติดตามประเด็นเสรีภาพในสื่อออนไลน์จำนวนมาก ทั้งยังสามารถแสดงออกเพื่อประท้วงคัดค้านองค์กรหรือหน่วยงานรัฐได้อย่างเข้มแข็ง โดยมีลักษณะของการเคลื่อนไหวที่หลากหลาย ไม่ว่าจะเป็นในรูปของการประท้วงเรียกร้องเชิงนโยบายและสังคม การรณรงค์ให้ความรู้ การเรียกร้องเพื่อให้เกิดผลบังคับทางกฎหมาย โดยเฉพาะอย่างยิ่ง ใช้สิทธิทางศาลเพื่อฟ้องร้องหน่วยงานหรือเจ้าหน้าที่รัฐเมื่อพบกรณีที่เจ้าหน้าที่หรือองค์กรที่เกี่ยวข้องนั้นใช้อำนาจในทางมิชอบ รวมทั้งการนำเรื่องขึ้นสู่ศาลเพื่อให้พิจารณาความชอบด้วยรัฐธรรมนูญของกฎหมายหรือมาตรการต่างๆ ของรัฐ เป็นต้น

บทสรุปสำคัญ สำหรับการศึกษากฎหมายและสถานการณ์สื่อออนไลน์ของประเทศเยอรมนีก็คือ ใช่ว่าการจำกัดควบคุมเสรีภาพในการรับรู้ข้อมูลข่าวสารหรือการแสดงความคิดเห็น กระทั่งการปิดกั้นเนื้อหาหรือเว็บไซต์จะเป็นสิ่งที่เกิดขึ้นไม่ได้ หรือยอมรับมิได้เลยในประเทศเสรีนิยมประชาธิปไตย (อย่างไรก็ตาม ประเทศเยอรมนีปกครองในระบอบสังคมนิยมประชาธิปไตย) ตรงกันข้าม สิ่งเหล่านั้นย่อมเกิดขึ้นได้ เพราะประเทศเหล่านี้ต่างก็ยอมรับหลักการปกครองโดยนิติรัฐ และการคุ้มครองสิทธิและเสรีภาพของบุคคลอย่างเท่าเทียม เมื่อเสรีภาพในการแสดงความคิดเห็นเป็นเสรีภาพประเภทที่ต้องมีการแสดงออกมาภายนอก หากบุคคลใดใช้อย่างเกินขอบเขตก็อาจล่วงละเมิดเสรีภาพของเอกชนคนอื่นหรือระเบียบของสังคมได้ ฉะนั้น เสรีภาพดังกล่าวจึงย่อมถูกจำกัดตัดทอนได้ อย่างไรก็ตาม การจำกัดตัดทอนนั้น จำเป็นต้องอยู่ภายใต้ขอบเขตของกฎหมายหรือมาตรการที่ยุติธรรมเพียงพอ กล่าวคือ ชัดเจนไม่คลุมเครือ ได้สัดส่วนหรือพอสมควรแก่เหตุ ใช้มาตรการนั้นเพียงเท่าที่จำเป็น มีกระบวนการขั้นตอนและวิธีการดำเนินการที่โปร่งใส ทั้งต้องมีกลไกเพื่อให้ประชาชนตรวจสอบความชอบด้วยกฎหมายของการใช้อำนาจโดยรัฐได้ หากรัฐสามารถทำได้ตามเงื่อนไขต่างๆ ดังที่กล่าวมา ดุลยภาพระหว่างการป้องกันและปราบปรามการกระทำความผิดกับการคุ้มครองสิทธิและเสรีภาพของประชาชนย่อมเป็นสิ่งที่เกิดขึ้นได้

บทที่

กฎหมายสหรัฐอเมริกา
กับสิทธิเสรีภาพในสื่อออนไลน์

กฎหมายสหรัฐอเมริกากับสิทธิเสรีภาพในสื่อออนไลน์

สหรัฐอเมริกา มีโครงการอาร์พาเน็ต (ARPANET - Advanced Research Project Agency Network) อันเป็นโครงการตั้งแต่ปี ค.ศ. 1969 ในสังกัดกระทรวงกลาโหม ที่มีขึ้นเพื่อพัฒนาระบบการสื่อสารของกองทัพ และพัฒนาต่อมาเป็นระบบที่เชื่อมโยงข้อมูลทั่วโลก หรืออินเทอร์เน็ตในปัจจุบัน[1] อินเทอร์เน็ตกลายเป็นเครื่องมือสำคัญในการเผยแพร่ความคิดเห็นและช่องทางการสืบค้นข้อมูลที่สะดวกรวดเร็ว ประหยัด และมีประสิทธิภาพสูงสุด โดยระบบนี้เอง ที่ทำให้การถ่ายทอดความคิดและเสรีภาพในการแสดงความคิดอย่างไร้พรมแดนเกิดขึ้นได้ สอดคล้องกับเจตนารมณ์ของผู้ร่างรัฐธรรมนูญสหรัฐฯ ที่อยากให้การคุ้มครองเสรีภาพดังกล่าวเป็นจริง ดังนั้น ในสายตาของสหรัฐอเมริกานั้น การพัฒนาระบบอินเทอร์เน็ต นอกจากเป็นการพัฒนาระบบเทคโนโลยีสารสนเทศให้ก้าวหน้าอย่างก้าวกระโดดแล้ว ยังถือเป็นเครื่องมือช่วยส่งเสริมเสรีภาพในการศึกษา รวมทั้งการแสดงความคิดเห็นของประชาชนอีกด้วย

นับตั้งแต่มีการตรารัฐธรรมนูญและแก้ไขเพิ่มเติมครั้งที่หนึ่ง (The First Amendment) ซึ่งถือเป็นหลักสิทธิเสรีภาพขั้นพื้นฐาน[2] โดยยึดถือหลักการมิให้รัฐตรากฎหมายใดๆ ขึ้นเพื่อจำกัดเสรีภาพในการแสดงความคิดเห็น[3] เพราะการแสดงความเห็นของประชาชนถือเป็นหัวใจสำคัญของการปกครองระบอบประชาธิปไตย พลเมืองในสหรัฐอเมริกาก็สามารถแลกเปลี่ยนข้อมูลข่าวสาร หรือโต้เถียงกันได้โดยเสรี ทั้งนี้สหรัฐอเมริกายังเชื่อมั่นในหลักตลาดแห่งความคิด เพราะด้วยหลักการนี้เท่านั้นที่จะสามารถทำให้ความจริงปรากฏขึ้นได้และเป็นประโยชน์สูงสุด นักวิชาการและศาลต่างเห็นพ้องต้องกันว่า กลไกของระบบตลาดและระบบควบคุมกันเองในการให้บริการอินเทอร์เน็ตเป็นมาตรการที่ดีที่สุดสำหรับสังคมประชาธิปไตย และการแสดงออกซึ่งความคิดเห็นผ่านสื่อออนไลน์ก็สมควรได้รับการคุ้มครองตามรัฐธรรมนูญอย่างสูงสุดเช่นเดียวกับการแสดงออกซึ่งความคิดเห็นผ่านสื่อรูปแบบอื่น[4] ดังนั้นโดยหลักแล้ว รัฐจึงไม่อาจแทรกแซงหรือปิดกั้นระบบสื่อสารใดๆ ได้ คงทำได้ก็แต่เข้าไปจัดการในเรื่องวิธีการ (manner) เวลา (time) หรือสถานที่ (place) ในการแสดงความคิดเห็นเท่านั้น อย่างไรก็ดี ตามกฎหมายสหรัฐอเมริกา การแทรกแซงหรือปิดกั้นช่องทางการเข้าถึงสื่ออาจเกิดขึ้นได้ภายใต้ข้อยกเว้น ซึ่งต้องพิสูจน์ให้ได้ว่ามีประโยชน์ของรัฐที่สำคัญยิ่งถึงขนาดที่รัฐจะต้องจำกัดสิทธิและเสรีภาพเช่นว่านั้น

1. หลักการคุ้มครองเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็น[5]

1.1 เสรีภาพในการแสดงความคิดเห็นของประชาชน

รัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่หนึ่ง กำหนดหลักประกันห้ามรัฐตรากฎหมาย หรือกระทำการอันเป็นการลิดรอนเสรีภาพในการแสดงความคิดเห็นของประชาชน ซึ่งต่อมาศาลสูงสุดแห่งสหรัฐ (Supreme Court of the United States) ได้วางบรรทัดฐานในการคุ้มครองการแสดง

ความคิดเห็นของประชาชนตามรัฐธรรมนูญข้างต้นไว้ด้วย โดยศาลยึดหลักการสำคัญที่ว่า

"แม้การแสดงความคิดเห็นนั้น อาจจะก่อให้เกิดลักษณะที่เป็นผลร้ายต่อบุคคลอื่น แต่ผลร้ายดังกล่าวก็อาจคลี่คลายได้ ด้วยการนำเสนอข้อมูลของอีกฝ่ายเพื่อหักล้างข้อเท็จจริงนั้น ฉะนั้น การสั่งห้ามการนำเสนอข้อมูลดังกล่าวโดยสิ้นเชิงโดยรัฐ จึงถือเป็นมาตรการที่เกินความจำเป็น และขัดต่อหลักรัฐธรรมนูญ"

ฉะนั้น จึงย่อมไม่ใช่หน้าที่ของรัฐที่จะห้ามการนำเสนอข้อมูลที่ไม่ตรงกับความจริง ในทางตรงกันข้าม รัฐควรส่งเสริมให้มีกระบวนการแลกเปลี่ยนข้อมูล หรือสนับสนุนให้มีการนำเสนอข้อมูลเพื่อหักล้างกัน หรือส่งเสริมให้เกิดตลาดแห่งความคิด เพื่อทำให้สังคมรับรู้ว่าข้อมูลใดเป็นจริงหรือเป็นเท็จ[6] เว้นแต่จะมีพยานหลักฐานที่ประจักษ์ชัดว่าภยันตรายร้ายแรงจะเกิดขึ้นอย่างแน่แท้ จนทำให้รัฐต้องจัดการแก้ปัญหาดังกล่าว อาทิ การแสดงความคิดเห็นที่เป็นภัยถึงขนาดยั่วยุให้ประชาชนละเมิดกฎหมายอย่างร้ายแรง เป็นภัยต่อสังคมอย่างแท้จริง หรือการเผยแพร่สิ่งลามกอนาจารที่จะเกิดความเสียหายต่อเด็กและเยาวชน เป็นต้น

ในคำพิพากษาดังกล่าว ศาลยังได้กำหนดประเภทของการแสดงความคิดเห็นที่ได้รับความคุ้มครอง และไม่ได้รับความคุ้มครองตามกฎหมายไว้อย่างชัดเจน นอกจากนี้ ศาลยังกำหนดลักษณะของกฎเกณฑ์ที่รัฐสามารถบัญญัติขึ้นเพื่อควบคุมการแสดงความคิดเห็น (ที่ไม่ได้รับความคุ้มครองตามรัฐธรรมนูญ) เอาไว้ด้วย โดยจำแนกออกเป็น 2 ลักษณะ คือ

1) กฎเกณฑ์ที่มีผลกระทบกับเนื้อหาหรือสารัตถะของความคิดเห็นนั้นโดยตรง (content-based regulation) และ

2) กฎเกณฑ์ที่ไม่มีผลกระทบโดยตรง เป็นแต่เพียงจัดระเบียบการแสดงความคิด (content-neutral regulation) เท่านั้น

ทั้งนี้ กฎเกณฑ์ดังกล่าวสามารถนำไปใช้เป็นเครื่องมือในการ

ตรวจสอบว่ากฎหมายควบคุมการแสดงความคิดเห็นที่ออกโดยรัฐฉบับใดขัดหรือแย้งต่อหลักการคุ้มครองเสรีภาพในการแสดงความคิดเห็นตามรัฐธรรมนูญ[7] กล่าวคือ เมื่อรัฐตรากฎหมายหรือข้อบังคับใดๆ ซึ่งระบุ "ข้อจำกัด" บางประการที่อาจส่งผลกระทบต่อเสรีภาพในการแสดงความคิดเห็นขึ้น กฎหมายหรือข้อบังคับนั้นๆ จะต้องถูกนำมาพิจารณาว่ามีวัตถุประสงค์เพื่อจำกัดเสรีภาพในการแสดงความคิดเห็นโดยตรงหรือไม่ (content-based on its face examination) หากโดยตัวเนื้อหาหรือข้อจำกัดในกฎหมายฉบับนั้นเองไม่ชัดแจ้งว่าต้องการห้ามการแสดงออกซึ่งความคิดเห็น ก็จะมีกระบวนการพิจารณาเพื่อตรวจสอบย้อนต่อไปถึง "เจตนารมณ์ที่แท้จริง" ของการกำหนด "ข้อจำกัด" นั้นว่ารัฐต้องการควบคุมสิ่งใดกันแน่ หากในท้ายที่สุดปรากฏว่า รัฐมีเจตนารมณ์ควบคุม "เนื้อหาในการแสดงความคิดเห็น" โดยตรง (content-based regulation) รัฐจะต้องแสดงให้ได้ว่ามีความจำเป็นอย่างยิ่งยวด และ "ข้อจำกัด" ที่กำหนดนั้นเป็นวิธีการอันร้ายแรงน้อยที่สุดแล้วเพื่อรักษาผลประโยชน์สาธารณะ หรือผลประโยชน์สูงสุดของรัฐ (compelling state interest)[8] ถ้ารัฐสามารถพิสูจน์ได้ กฎหมายหรือข้อบังคับที่บัญญัติขึ้นนั้นย่อมไม่ขัดกับรัฐธรรมนูญ

แต่หากกฎหมายหรือข้อบังคับที่บัญญัติขึ้นไม่ได้มีลักษณะเป็นการควบคุมจำกัดเนื้อหาหรือสาระสำคัญของความคิดเห็นโดยตรง เป็นแต่เพียงการจัดระเบียบการแสดงความคิดเห็น (content-neutral regulation) รัฐจะต้องแสดงให้เห็นว่า "วิธีการจัดการ" ดังกล่าวไม่มีผลเป็นการห้ามแสดงความคิดเห็นอย่างสิ้นเชิง ทั้งเป็นวิธีที่เหมาะสมแล้วอันจะนำไปสู่เป้าหมายของรัฐ (narrowly-tailored to serve a significant governmental interest) ซึ่งจะต้องไม่ใช่เพื่อความสะดวกของรัฐเท่านั้น ยกตัวอย่างเช่น การห้ามแจกจ่ายใบปลิวด้วยเหตุผล "เพื่อรักษาความสะอาดของบ้านเมือง" ย่อมส่งผลกระทบต่อเสรีภาพในการแสดงความคิดเห็นอย่างหลีกเลี่ยงไม่ได้ เมื่อพิจารณาข้อห้ามนี้แล้ว จะเห็นได้ว่า แม้เป็นเพียงการจัดระเบียบการแสดงความคิดเห็น ไม่ได้จำกัดเนื้อหาของการแสดงความคิดเห็นโดยตรงก็ตาม แต่วิธีการดังกล่าวคงไม่อาจถือเป็น

วิธีการที่ได้สัดส่วนหรือเหมาะสมแล้วที่จะนำไปสู่เป้าหมายของรัฐ (เพื่อความสะอาดของบ้านเมือง) ข้อกำหนดเช่นนี้ย่อมขัดต่อรัฐธรรมนูญ ในทางที่ถูกต้องแล้วรัฐต้องหาวิธีการอื่นใดเพื่อจัดการความสะอาดของบ้านเมืองมาใช้แทนการห้ามแจกจ่ายใบปลิวซึ่งเป็นการห้ามแสดงความคิดเห็น (โดยอ้อม)

ศาลสูงแห่งสหรัฐอเมริกายังยืนยันด้วยว่า รัฐไม่อาจบัญญัติกฎหมายที่มีโทษทางอาญาต่อการวิพากษ์วิจารณ์ที่เป็นไปเพื่อประโยชน์สาธารณะ โดยเฉพาะอย่างยิ่ง การวิพากษ์วิจารณ์การปฏิบัติงานของรัฐบาล รวมถึงการวิพากษ์วิจารณ์คำพิพากษาของศาล[9] เพราะการวิพากษ์วิจารณ์การทำงานของรัฐบาลย่อมเป็นประโยชน์ต่อสาธารณะ และต่อเจ้าพนักงานของรัฐ[10] ในขณะที่การวิพากษ์วิจารณ์คำพิพากษาหรือกระทั่งตัวผู้พิพากษาในการทำความเห็นทางคดีก็ไม่อาจก่อให้เกิดความเสียหายต่อกระบวนการยุติธรรมทั้งระบบได้[11] กลับจะก่อให้เกิดการพัฒนา หรือการปฏิรูประบบให้ดีขึ้น ดังนั้น รัฐหรือศาลจึงไม่อาจกำหนดกฎหมายห้ามวิพากษ์วิจารณ์หรือเผยแพร่ความลับของศาลได้ เพราะสิทธิรับรู้ข้อมูลข่าวสารใดๆ และเสรีภาพในการแสดงความคิดเห็นโดยอิสระ ย่อมอยู่เหนือกว่าผลประโยชน์ของรัฐในการคุ้มครองชื่อเสียงผู้พิพากษาเป็นการเฉพาะตัว[12]

1.2 เสรีภาพสื่อมวลชน

ในสหรัฐอเมริกา สื่อมวลชนได้รับความคุ้มครองตามรัฐธรรมนูญ โดยรัฐไม่อาจกำหนดข้อปฏิบัติใดๆ ที่ไม่มีความชอบธรรมต่อสื่อมวลชนได้[13] ทั้งนี้ การตรวจสอบเนื้อหาของสื่อก่อนการเผยแพร่ (prior restraints) เป็นสิ่งที่รัฐไม่อาจทำได้ทั้งยังขัดรัฐธรรมนูญ เพราะด้วยวิธีการดังกล่าว เสรีภาพในการแสดงความคิดเห็นของประชาชนจะถูกกระทบในระดับที่รุนแรงกว่าการถูกตรวจสอบหรือถูกฟ้องร้องดำเนินคดีภายหลังเผยแพร่ข้อมูลหรือความคิดเห็นนั้นออกไปแล้ว เนื่องจากผู้ที่ถูกตรวจสอบเนื้อหาหรือถูกดำเนินคดีเพราะเนื้อหาเหล่านั้นยังมีโอกาสได้ต่อสู้ว่าเนื้อหา หรือการบังคับใช้กฎหมายที่ใช้ลงโทษอันเนื่องจากการแสดงความคิดเห็นของเขา

นั้นไม่ชอบด้วยรัฐธรรมนูญอย่างไร ในขณะที่ผู้ถูกห้ามไม่ให้เผยแพร่ข้อมูลหรือแสดงความคิดเห็นใดๆ ออกสู่สาธารณะ ไม่มีสิทธิพิสูจน์หรือโต้แย้งการใช้กฎหมายในลักษณะดังกล่าวได้เลย[14]

2. เนื้อหาต้องห้ามเผยแพร่ในสื่อสาธารณะ ตามกฎหมายสหรัฐอเมริกา[15]

ดังกล่าวมาแล้วว่า สังคมอเมริกันยอมรับและให้ความสำคัญกับการใช้ประโยชน์จากคอมพิวเตอร์และอินเทอร์เน็ตต่อระบบการศึกษาและวิทยาการต่างๆ ซึ่งจะเป็นแหล่งข้อมูลแก่ประชาชนชาวอเมริกัน ทั้งจะนำความเปลี่ยนแปลงอย่างมหาศาลในอนาคตมาสู่ประเทศ อินเทอร์เน็ตไม่เพียงแต่มีบทบาทในเรื่องต่างๆ ในชีวิตประจำวันเท่านั้น หากแต่เป็นเครื่องมือสำคัญสำหรับประชาชนในการถกเถียง แลกเปลี่ยน และแสดงความคิดเห็นในเรื่องที่เกี่ยวกับการเมืองการปกครองด้วย นักวิชาการและนักการเมืองส่วนใหญ่เห็นว่า ไม่ควรมีกฎหมายหรือมาตรการใดๆ เพื่อควบคุมการแสดงความคิดเห็นในสื่อออนไลน์เป็นการเฉพาะหรือเป็นกรณีพิเศษ นอกจากนี้ รัฐบาลควรมีนโยบายสนับสนุนและส่งเสริมการเจริญเติบโตอย่างต่อเนื่องของอินเทอร์เน็ตและการให้บริการ เพื่อให้เกิดการแข่งขันในตลาดโดยอิสระ การใช้อำนาจรัฐควบคุม ปิดกั้น หรือตรวจสอบการเข้าถึงข้อมูลในสื่อออนไลน์จึงถูกต่อต้านจากประชาชน และศาลสูงสุดมาโดยตลอด

อย่างไรก็ตาม นับตั้งแต่ปี 1994 เป็นต้นมา รัฐบาลสหรัฐฯ มีความพยายามควบคุมการแสดงความคิดเห็นในสื่อออนไลน์มากขึ้นด้วยเหตุผลหลายประการ ที่สำคัญก็คือ เพื่อคุ้มครองสวัสดิภาพเด็กและเยาวชนมิให้ถูกล่อลวงหรือชักจูงไปในทางที่ผิด ทั้งยังประสงค์ที่จะปราบปรามการแสวงหาประโยชน์ทางเพศจากเด็กและเยาวชน[16] จึงห้ามการเผยแพร่ภาพลามกอนาจารเด็กและเยาวชน (child pornography)

ปัจจุบัน รัฐบาลสหรัฐฯ ตรากฎหมายพิเศษเพื่อควบคุม

การแสดงความคิดเห็นในสื่อออนไลน์ในหลายลักษณะ[17] แต่ก็มักถูกวิพากษ์วิจารณ์จากสังคมว่าเป็นกฎหมายที่ไม่จำเป็น และละเมิดสิทธิและเสรีภาพของประชาชนเกินสมควร ทั้งไม่มีการศึกษาวิจัยที่เพียงพอนำไปสู่การโต้แย้งในเรื่องความชอบด้วยรัฐธรรมนูญ ซึ่งปรากฏข้อเท็จจริงว่ากฎหมายจำนวนไม่น้อยถูกร้องต่อศาลว่ามีเนื้อหาขัดรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่หนึ่ง และถูกพิพากษาให้สิ้นผลบังคับใช้ไปหลายฉบับ ด้วยเหตุผลว่าเป็นการจำกัดเสรีภาพในการแสดงความคิดเห็น และกระทบต่อสารัตถะของการปกครองระบอบประชาธิปไตย[18]

เนื้อหาที่ไม่ได้รับความคุ้มครองตามรัฐธรรมนูญ และอาจเป็นความผิด ซึ่งรัฐสามารถออกกฎหมายจำกัดการเผยแพร่ หรือการแสดงออกได้ อาจจำแนกได้ดังนี้

2.1 ความคิดเห็นที่ส่งเสริมให้กระทำผิดกฎหมาย (advocacy of illegal conduct)

หากการแสดงความคิดเห็นใด ผู้แสดงความคิดเห็นนั้นมีเจตนารมณ์เพื่อปลุกเร้า หรือก่อให้เกิดการกระทำที่ผิดกฎหมาย หรือทำให้บ้านเมืองอยู่ในสภาวะไร้กฎหมาย อีกทั้งการกระทำดังกล่าวมีแนวโน้มหรือลักษณะที่อาจก่อให้เกิดภยันตรายอย่างร้ายแรงขึ้นในสังคม รัฐสามารถควบคุมหรือจำกัดเสรีภาพในการแสดงความคิดเห็นที่มีลักษณะดังกล่าวได้ โดยใช้มาตรการต่างๆ ที่เฉพาะเจาะจงบนพื้นฐานของการใช้ดุลพินิจอย่างระมัดระวัง ทั้งนี้ศาลเคยวางหลักเรื่องภยันตรายในปัจจุบันอย่างชัดแจ้ง หรือ The Clear and Present Danger Test ให้เป็นบรรทัดฐานถึงขอบเขตและลักษณะของการแสดงความคิดเห็นเชิงปลุกเร้าให้คนกระทำความผิดไว้ในคดี Brandenburg v. Ohio, 395 U.S. 444 (1969)[19] ว่า ถ้อยคำที่จะถือว่าผิดกฎหมาย และรัฐสามารถควบคุมได้นั้น จะต้องก่อให้เกิดภยันตรายในปัจจุบันอย่างชัดแจ้ง สำหรับในคดีนี้ซึ่งจำเลยคัดค้านการเกณฑ์ทหาร ยังไม่อาจถือได้อย่างชัดเจนว่าเป็นการไม่เชื่อฟัง แสดงความไม่จงรักภักดี หรือปฏิเสธการปฏิบัติหน้าที่ในกองทัพของสหรัฐอเมริกา ย่อมไม่อาจ

ถือได้ว่า จำเลยก่อให้เกิดภยันตรายได้อย่างแท้จริง สำหรับการแสดงความคิดเห็นโดยใช้ภาษาก้าวร้าว (offensive language) เช่น ไม่นับถือพระเจ้า ความเชื่อทางศาสนาหรือสิ่งศักดิ์สิทธิ์ หรือที่เกี่ยวข้องกับเชื้อชาตินั้น แม้จะมีลักษณะรุนแรงหรือลบหลู่ความเชื่อของผู้อื่น ก็ยังถือไม่ได้ว่าการกระทำนั้นก่อให้เกิดภยันตรายอย่างชัดแจ้ง จึงยังคงเป็นความคิดเห็นที่ได้รับความคุ้มครองตามรัฐธรรมนูญอยู่ ซึ่งรัฐไม่อาจบัญญัติกฎหมายหรือลงโทษเพื่อจำกัดการแสดงความคิดเห็นดังกล่าวได้

2.2 สิ่งลามกอนาจาร (obscenity)

รัฐธรรมนูญสหรัฐไม่คุ้มครองการเผยแพร่สิ่งลามกอนาจาร[20] ทั้งนี้ปัญหาว่าสิ่งใดถือเป็นสิ่งลามกอนาจารหรือไม่ ต้องพิจารณาตามหลักวิญญูชนทั่วไปในสังคมว่าเป็นสิ่งที่มีลักษณะกระตุ้นให้เกิดความต้องการทางเพศหรือไม่[21] โดยมีข้อที่ควรพิจารณาดังนี้[22]

1) วิญญูชนทั่วไปเห็นว่า สิ่งนั้นเป็นสิ่งยั่วยวนและเร่งเร้าความต้องการทางเพศ ความใคร่ ซึ่งสังคมหนึ่งอาจจะแตกต่างจากสังคมอื่นๆ

2) ภาพหรืองานดังกล่าวแสดงให้เห็นภาพหรือเรื่องราวที่ชัดแจ้งเกี่ยวกับเพศ เช่น ภาพแสดงการร่วมเพศ การสำเร็จความใคร่ หรือโชว์ให้เห็นอวัยวะเพศ ซึ่งมีกฎหมายบังคับใช้อย่างแจ้งชัด (fair notice) เป็นการล่วงหน้า

3) ภาพหรืองานดังกล่าว เมื่อพิจารณาในภาพรวมแล้ว ขาดคุณค่าทางวรรณกรรม ศิลปะ การเมือง หรือวิทยาศาสตร์

สำหรับกฎหมายที่เกี่ยวข้องกับการควบคุมการเผยแพร่สิ่งลามกอนาจารนั้น ประเทศสหรัฐอเมริกาตราขึ้นใช้บังคับหลายฉบับดังนี้

2.2.1 พระราชบัญญัติว่าด้วยความเหมาะสมในการสื่อสาร ค.ศ. 1994 (Communication Decency Act of 1994 – CDA หรือ ซีดีเอ)

ถือเป็นกฎหมายฉบับแรกที่บัญญัติขึ้นเพื่อควบคุมกิจกรรมใน

สื่อออนไลน์ในสมัยที่ซีดีเอมีผลบังคับใช้ก็เกิดกระแสวิพากษ์วิจารณ์ในสังคมว่า ถือเป็นช่วงที่เลวร้ายที่สุดในประวัติศาสตร์กฎหมายของสหรัฐอเมริกา ขณะที่อีกด้านหนึ่งก็มีเสียงสนับสนุนว่าซีดีเอมีเจตนารมณ์ที่ดีในการปกป้องผลประโยชน์ของเด็กและเยาวชน ทั้งนี้ซีดีเอถูกตราขึ้นเพื่อแก้ไขเพิ่มเติมพระราชบัญญัติโทรคมนาคม ค.ศ. 1934 (Telecommunication Act of 1934) และถูกจัดหมวดหมู่ไว้ในประมวลกฎหมายของสหรัฐ ในหมวด 47 มาตรา 223 (47 U.S.C.§ 223) ซึ่งแบ่งระดับความสำคัญ ดังนี้

- ความผิดสำหรับผู้ใช้บริการโทรคมนาคม หรืออินเทอร์เน็ตโดยทั่วไป

มาตรา 223 (1) (a) (1) (A) ห้ามมิให้บุคคลใดใช้เครื่องมือสื่อสารโดยรู้อยู่แล้วว่าจะก่อให้เกิด หรือชักชวน และดำเนินการส่งผ่านสิ่งใดๆ รวมถึงการกล่าวถึง เรียกร้อง แนะนำ เสนอภาพ หรือการสื่อสารใดๆ เกี่ยวกับภาพลามกอนาจาร หรือสิ่งไม่เหมาะสมในทางเพศ (obscene, lewd, lascivious, filthy, or indecent) โดยเจตนาที่จะรบกวน หรือกระทำการที่มิชอบ ข่มขู่ หรือติดตามรังควานบุคคลอื่น

มาตรา 223 (1) (a) (1) (B) ห้ามกระทำการในลักษณะเดียวกันกับมาตรา 223 (A) โดยรู้อยู่แล้วว่า ผู้รับข้อมูลอายุต่ำกว่า 18 ปี ไม่ว่าจะด้วยโทรศัพท์หรือวิธีการใดในการริเริ่มการสื่อสารนั้น

มาตรา 223 (1) (a) (1) (C) ห้ามโทรศัพท์หรือใช้เครื่องมือสื่อสารใดๆ เพื่อรบกวนบุคคลอื่นๆ โดยเฉพาะอย่างยิ่ง การโทรศัพท์โดยไม่เปิดเผยชื่อโดยมีเจตนาจะทำให้รำคาญหรือกระทำการไม่ชอบด้วยประการใดๆ ข่มขู่ หรือติดตามรังควานบุคคลใดๆ หรือบุคคลที่ได้รับการติดต่อดังกล่าว

มาตรา มาตรา 223 (1) (a) (1) (D) และ (E) กำหนดห้ามมิให้ติดตาม รบกวน รังควาน ผู้อื่น โดยใช้โทรศัพท์ หรือเครื่องมือสื่อสารในลักษณะเดียวกัน

บุคคลที่ฝ่าฝืนบทบัญญัติข้างต้นมีโทษปรับตามที่กำหนดไว้ใน

หมวด 18 แห่งประมวลกฎหมายสหรัฐอเมริกา และจำคุกไม่เกิน 2 ปี หรือทั้งจำทั้งปรับ

มาตรา 223 (2) (d) (1) (A) ห้ามใช้คอมพิวเตอร์ที่มีระบบบริการสื่อสาร (interactive computer service) ส่งข้อความ หรือภาพในลักษณะเดียวกันกับที่กล่าวไว้ข้างต้น ซึ่งมีลักษณะเป็นการบรรยายภาพหรือแสดงให้เห็นกิจกรรมทางเพศ หรืออวัยวะเพศ แก่บุคคลที่มีอายุต่ำกว่า 18 ปี ไม่ว่าบุคคลดังกล่าวจะเป็นผู้ริเริ่มใช้เครื่องมือสื่อสารด้วยตนเองหรือไม่ก็ตาม

ส่วนมาตรา 223 (2) (d) (1) (B) ห้ามมิให้ใช้บริการคอมพิวเตอร์ที่สามารถติดต่อสื่อสารได้ เพื่อแสดงภาพลามกอนาจาร หรือในลักษณะเดียวกันกับข้อ A เพื่อให้บริการแก่บุคคลที่มีอายุต่ำกว่า 18 ปี ผู้ฝ่าฝืนบทบัญญัติดังกล่าว ต้องระวางโทษปรับและจำคุกไม่เกิน 2 ปี

ข้อกำหนดในกฎหมายฉบับนี้ยังห้ามการโฆษณาสิ่งลามกอนาจารโดยใช้เครื่องมือสื่อสาร รวมถึงการอนุญาตให้บุคคลอื่นใช้เครื่องมือสื่อสารเพื่อการโฆษณาด้วย ทั้งยังห้ามมิให้ใช้เครื่องมือสื่อสารทำการสื่อสารเพื่อวัตถุประสงค์ทางการค้ากับเด็กอายุต่ำกว่า 18 ปี หรือบุคคลอื่นที่อายุไม่ต่ำกว่า 18 ปี แต่ปราศจากความยินยอม โดยบุคคลที่ยินยอมให้ใช้เครื่องมือสื่อสารกระทำการดังกล่าว ต้องระวางโทษ ปรับไม่เกิน 50,000 เหรียญ หรือจำคุกไม่เกิน 6 เดือน หรือทั้งจำทั้งปรับ ผู้ละเมิดโดยการใช้เครื่องมือโฆษณา ให้ถือว่าการกระทำผิดแต่ละวันเป็นการกระทำผิดต่างกรรมต่างวาระ

อนึ่ง มาตรา 507 เป็นบทอธิบายความหมายของการกระทำผิดที่เกี่ยวกับสิ่งลามกอนาจาร ที่กระทำผ่านหรือใช้เครื่องคอมพิวเตอร์ ให้การขนส่งหรือการนำเข้าภาพหรือสิ่งลามกอนาจารผ่านการเชื่อมต่อระบบคอมพิวเตอร์เป็นความผิดตามกฎหมายดังกล่าวด้วย[23] เนื่องจากกฎหมายเดิมกำหนดเฉพาะการนำเข้าหรือการขนส่งสิ่งลามกอนาจารผ่านระบบการขนส่งทางกายภาพเป็นหลัก[24]

- ความผิดของผู้ให้บริการอินเทอร์เน็ต

สำหรับในส่วนของผู้ให้บริการอินเทอร์เน็ต ประเทศสหรัฐอเมริกาค่อนข้างให้ความสำคัญ เพราะมีผลต่อการพัฒนาเทคโนโลยีและสิทธิในการเข้าถึงข้อมูลข่าวสารของประชาชน จึงบัญญัติบทคุ้มครองพิเศษสำหรับไว้โดยเฉพาะ เพื่อไม่ให้ต้องรับผิดในการกระทำของผู้ใช้บริการ เว้นแต่ลักษณะการให้บริการมีความเกี่ยวข้อง หรือเป็นผู้ควบคุมดูแลเนื้อหาที่เข้าข่ายเป็นความผิดนั้น หรือมีโอกาสได้รับรู้เนื้อหา รวมถึงเป็นผู้สมรู้ร่วมคิดในการเผยแพร่เนื้อหาเหล่านั้นด้วย ตามที่ปรากฏใน มาตรา 223 (2) (e) ของซีดีเอ ซึ่งมีรายละเอียดดังนี้

(1) บุคคลไม่ต้องรับผิดเพียงเพราะเป็นผู้ให้บริการการเข้าถึงระบบคอมพิวเตอร์ หรือการติดต่อสื่อสารให้กับหรือจากระบบ หรือเครือข่ายที่ไม่ได้ดำเนินการควบคุมโดยบุคคลนั้นเอง รวมถึงการส่งผ่าน หรือดาวน์โหลด หรือการเก็บข้อมูลโดยระบบโดยอัตโนมัติ หรือการเข้าถึงระบบซอฟท์แวร์ หรือระบบอื่นใดที่เกี่ยวข้อง ซึ่งเกิดขึ้นโดยระบบอันเนื่องมาจากการเชื่อมต่อ หากไม่ได้เป็นผู้จัดทำหรือก่อให้เกิดเนื้อหาหรือสิ่งลามกอนาจารนั้นเอง

(2) ข้อที่ไม่ต้องรับผิดตาม (1) ไม่อาจใช้อ้างยันในกรณีที่บุคคลนั้นเป็นผู้สมคบคิดโดยมีส่วนร่วมก่อให้เกิดหรือรู้อยู่แล้วว่าจะอาจจะก่อให้เกิดการแพร่หลายสิ่งดังกล่าวข้างต้น ซึ่งละเมิดต่อกฎหมายนี้ รวมถึงบุคคลที่โฆษณาให้ทราบว่า มีการให้บริการสิ่งลามกอนาจารดังกล่าว

(3) ข้อที่ไม่ต้องรับผิดตาม (1) ไม่อาจใช้อ้างยันในกรณีที่บุคคลนั้นเป็นผู้ให้บริการเข้าถึงหรือเชื่อมต่อระบบอินเทอร์เน็ตนั้น ซึ่งมีพฤติการณ์ละเมิดกฎหมายข้างต้น โดยบุคคลนั้นเป็นเจ้าของหรือควบคุมระบบดังกล่าวโดยตรง

(4) บุคคลผู้เป็นนายจ้างไม่ต้องรับผิดต่อการกระทำของลูกจ้างที่ละเมิดกฎหมายฉบับนี้ หากลูกจ้างได้กระทำการและอยู่ภายในขอบเขตตามทางการที่จ้าง เมื่อการละเมิดกฎหมายนั้น นายจ้างไม่ได้มีส่วนรู้เห็นอนุญาต หรือยินยอมให้กระทำการดังกล่าว หรือไม่ได้มีส่วนประมาทเลินเล่อ

และละเลยที่จะควบคุมระบบคอมพิวเตอร์ของตน อันอาจจะก่อให้เกิดการกระทำผิดดังกล่าวขึ้น

(5) ในกรณีนี้ให้ถือว่าบุคคลดังกล่าวสามารถอ้างเพื่อไม่ให้ตนถูกฟ้องร้องดำเนินคดีได้ หากได้ดำเนินมาตรการใดๆ ที่เหมาะสม และโดยสุจริต ภายในความก้าวหน้าทางเทคโนโลยีที่มีอยู่และเป็นไปได้ เพื่อห้ามปรามหรือป้องกันการเข้าถึงระบบคอมพิวเตอร์ดังกล่าวโดยผู้เยาว์ หรือการกำหนดให้มีระบบการเข้าถึงผ่านระบบตรวจสอบข้อมูลของบัตรเครดิต เดบิต หรือระบบรหัสเข้าถึงของผู้ใหญ่ (adult access code) หรือข้อมูลบัตรประจำตัวประชาชนที่แสดงว่าเป็นผู้ใหญ่แล้ว

(6) คณะกรรมการกลางกำกับดูแลกิจการสื่อสาร (Federal Communications Commission - FCC) อาจกำหนดมาตรฐานที่เหมาะสม มีประสิทธิภาพและมีเหตุผลอันสมควรในการจำกัดการเข้าถึง เพื่อห้ามมิให้มีการสื่อสารภายใตบทบัญญัติ ตามมาตรา 223 (2) (d) ของซีดีเอได้ แต่คณะกรรมการไม่มีอำนาจใดๆ ที่จะบังคับการให้เป็นไปตามกฎหมายด้วยตนเอง และกฎหมายนี้ก็ไม่มีเจตนารมณ์ที่จะให้อำนาจแก่คณะกรรมการ ที่จะยอมรับ กำหนดโทษ หรือให้ใบอนุญาตด้วยตนเอง และไม่มีอำนาจใดๆ ที่จะดำเนินการกับบุคคลที่ไม่ปฏิบัติตามมาตรการข้างต้นโดยตรง ทั้งไม่มีอำนาจที่จะให้การสนับสนุนผลิตภัณฑ์ที่เสนอเข้าไปเพื่อให้สอดคล้องกับมาตรการที่กำหนดโดยคณะกรรมการ แต่การปฏิบัติหรือไม่ปฏิบัติตามแนวทางที่คณะกรรมการกำหนดนั้น จะใช้เป็นพยานหลักฐานแสดงถึงเจตนาอันสุจริตเพื่อให้ได้มาซึ่งเหตุผลที่จะทำให้ไม่ต้องรับผิดตามกฎหมาย ตามข้อ (5) หากมีการฟ้องร้องตาม มาตรา 223 (2) (d) แห่งซีดีเอนี้

ส่วนข้ออ้างที่จะทำให้ไม่ต้องรับผิดนั้น คือกรณีที่เจ้าหน้าที่หรือบุคคลใดปฏิบัติตามกฎหมายแล้ว จะได้รับเอกสิทธิ์ที่จะไม่ถูกฟ้องร้องดำเนินคดีในศาล หรือในการดำเนินการทางปกครอง หากการกระทำดังกล่าวไม่เป็นการละเมิดกฎหมายอาญาหรือกฎหมายอื่นใด ทั้งบุคคลดังกล่าวมีเจตนาสุจริตที่จะปฏิบัติตามข้อกำหนดข้างต้น เพื่อจะได้รับ

ประโยชน์จากข้ออ้างที่จะไม่ถูกฟ้องร้องคดีในการจำกัดการเข้าถึง ป้องกันการส่งผ่านข้อมูล หรือห้ามการเข้าถึงระบบสื่อสารภายใต้มาตรานี้

อาจกล่าวสรุปในส่วนนี้ได้ว่า ซีดีเอเป็นบทบัญญัติที่ห้ามมิให้ปฏิบัติต่อผู้ให้บริการหรือผู้ให้บริการเชื่อมต่อของระบบคอมพิวเตอร์ในลักษณะเช่นเดียวกับผู้นำเสนอข้อมูล (publisher or speaker) ในสื่อดั้งเดิมประเภทอื่นๆ ตามกฎหมายฉบับนี้ ผู้ให้บริการเชื่อมต่ออินเทอร์เน็ตไม่ต้องรับผิดสำหรับเนื้อหาที่บุคคลอื่นเป็นผู้พิมพ์ผู้โฆษณา หากผู้ให้บริการนั้นไม่สามารถควบคุมระบบการแสดงเนื้อหานั้นได้ ทั้งนี้ มลรัฐหรือรัฐบาลท้องถิ่นต่างๆ จะออกกฎหมายเพื่อกำหนดความรับผิดใดๆ เพิ่มเติมแก่นิติบุคคลที่ประกอบการค้า บริการห้องสมุดที่ไม่แสวงหากำไร หรือสถาบันการศึกษามิได้ คงทำได้ก็แต่เพียงการคอยกำกับดูแลการดำเนินการดังกล่าวเท่านั้น

- การตรวจสอบควบคุม หรือเซ็นเซอร์เนื้อหา

สำหรับการตรวจสอบควบคุม หรือเซ็นเซอร์เนื้อหาที่เป็นความผิดกฎหมายในภาพรวม มีประเด็นที่น่าสนใจอย่างยิ่ง ก็คือ นอกจากซีดีเอจะมีบทบัญญัติที่กำหนดให้อำนาจบิดามารดาในการควบคุมการเข้าถึงสื่อออนไลน์กับบุตรหลานไว้อย่างชัดเจน (มาตรา 509 ของกฎหมายว่าด้วยอำนาจการจัดการการสื่อสารในโลกออนไลน์ของสมาชิกในครอบครัว หรือ Online Family Empowerment) แล้ว โดยแก้ไขเพิ่มเติม มาตรา 201 ของประมวลกฎหมาย 47 U.S.C. §201 และมาตราอื่นๆ เช่น มาตรา 230 กำหนดวิธีการป้องกันหรือการปิดกั้นสื่อลามกหรือไม่เหมาะสม (Protection for Private Blocking and Screening of Offensive Material) ซีดีเอยังมีบทคุ้มกันทางกฎหมายให้แก่ผู้ปิดกั้นช่องทางการเข้าถึง หรือตรวจสอบสื่อไม่เหมาะสมคนอื่นๆ ที่ไม่ใช่บิดามารดาด้วย โดยผู้ให้บริการไม่ต้องรับผิดในทางแพ่งหากดำเนินการปิดกั้นหรือจำกัดการเข้าถึงข้อมูล ภายหลังที่ตนพิจารณาแล้วว่าเป็นสื่อลามกอนาจาร ไม่เหมาะสม น่ารังเกียจ โดยไม่สำคัญว่าเนื้อหาเหล่านั้นจะได้รับความคุ้มครองตามรัฐธรรมนูญหรือไม่

นอกจากนี้ หากมีการกำหนดมาตรการใดที่จะปกป้องเด็กมิให้เข้าถึงระบบข้อมูลดังกล่าว โดยเป็นวิธีการที่มีเหตุผล มีประสิทธิภาพ และเหมาะสมแล้ว อาทิ การกำหนดรหัสผ่าน หรือใช้ระบบบัตรเครดิตเพื่อเข้าถึงระบบข้อมูล ผู้ให้บริการดังกล่าวย่อมได้รับความคุ้มกันตามกฎหมายมิให้ถูกฟ้องคดีแล้ว ซึ่งเรียกหลักการนี้ว่า “affirmative defense” อย่างไรก็ตาม ข้ออ้างนี้ไม่อาจใช้อ้างเพื่อให้หลุดพ้นความรับผิดได้ หากเป็นกรณีกระทำผิดตามกฎหมายอื่นด้วย[25] ทั้งซีดีเอก็หาได้มีผลเป็นการแก้ไข ขยาย หรือยับยั้งบทบัญญัติตามกฎหมายทรัพย์สินทางปัญญาแต่ประการใดไม่

- การมีผลใช้บังคับของซีดีเอ

ภายหลังซีดีเอมีผลใช้บังคับ ในปี 1997 สหภาพเสรีภาพพลเมืองอเมริกัน (American Civil Liberties Union) ยื่นฟ้องคดีต่อศาลว่า กฎหมายว่าด้วยความเหมาะสมในการสื่อสารซึ่งใช้ควบคุมการสื่อสารออนไลน์ดังกล่าวขัดรัฐธรรมนูญ เพราะมีลักษณะจำกัดสิทธิเสรีภาพของประชาชนมากเกินไป ท้ายที่สุด ศาลสูงสุดสหรัฐฯ พิพากษาว่ากฎหมายนี้ขัดรัฐธรรมนูญจริง เนื่องจากมีถ้อยคำที่มีความหมายกว้างขวาง คลุมเครือ ไม่ชัดเจน ทั้งไม่มีนิยามคำศัพท์เกี่ยวกับลักษณะที่ไม่เหมาะสมของเนื้อหาที่อาจถูกปิดกั้น หรือห้ามไม่ให้เผยแพร่ว่ามีลักษณะอย่างไร[26] โดยผลของคำตัดสินนี้เอง ในปี 2003 สภาคองเกรสจึงแก้ไขเพิ่มเติมกฎหมายในเรื่องนี้ให้ชัดเจนยิ่งขึ้นด้วยการเสนอกฎหมายเกี่ยวกับการคุ้มครองเด็ก (Prosecuting Remedies and Tools Against the Exploitation of Children Today Act of 2003 หรือ PROTECT Act) แก้ไขมาตรา 223 กำหนดว่า สิ่งต้องห้ามไม่ให้มีการสื่อสารนั้นจะต้องมีลักษณะลามกอนาจาร หรือเป็นภาพโป๊ของเด็ก (child pornography) นอกจากนี้ยังตัดถ้อยคำที่ไม่ชัดเจนอย่าง lewd, lascivious, filthy และ indecent *(มีความหมายทำนอง ลามก อนาจาร ความเสื่อมเสียทางเพศ ไม่เหมาะสม)* ออกไปด้วย ปัจจุบัน มาตรา 223 จึงครอบคลุมเฉพาะการกระทำที่มีลักษณะของการชักชวนและส่งผ่านซึ่งข้อความ ภาพ ฯลฯ ที่มีลักษณะลามกอนาจาร

หรือภาพโป๊เด็กไปยังบุคคลอื่น โดยมีเจตนาจะรบกวน กระทำไม่ชอบ ข่มขู่ ติดตามรังควาน หรือส่งสิ่งดังกล่าวไปยังเด็กที่มีอายุต่ำกว่า 18 ปี หรือการใช้เครื่องมือสื่อสารรบกวนรังควานบุคคลอื่นๆ เท่านั้น

2.2.2 พระราชบัญญัติป้องกันสื่อลามกเด็ก ค.ศ. 1996 (Child Pornography Prevention Act of 1996 หรือ CPPA)

กฎหมายนี้บัญญัติขึ้นเพื่อควบคุมสื่อและการกระทำในลักษณะต่างๆ ที่อาจกระทบต่อเด็กและเยาวชนให้เข้มงวดและชัดเจนขึ้น อาทิ มาตรา 2256 (8) (B) ห้ามมิให้กระทำด้วยวิธีการใดๆ เพื่อให้เกิดภาพเสมือนจริง (visual depiction) ในลักษณะเป็นการร่วมเพศหรือกระทำทางเพศของเด็กหรือผู้เยาว์ (engaging in sexually explicit conduct) มาตรา 2258 (2) ห้ามผลิตภาพยนตร์ที่ทำให้เห็นว่าเด็กหรือเยาวชนเป็นผู้แสดงเพื่อชักชวนหรือกระตุ้นความต้องการทางเพศ หรือร่วมเพศให้เกิดขึ้นแก่เด็กหรือเยาวชน มาตรา 2256 (8) (D) ห้ามการโฆษณาสิ่งลามกอนาจารโดยใช้ภาพเด็กในการโฆษณานั้น เป็นต้น

2.2.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนตัวออนไลน์ของเด็ก ค.ศ. 1998 (Children's Online Privacy Protection Act of 1998 หรือ COPPA)

เป็นกฎหมายที่กำหนดวิธีการเก็บข้อมูล และการเปิดเผยข้อมูลของผู้ประกอบการเว็บไซต์หรือผู้ให้บริการออนไลน์ที่เกี่ยวข้องกับบุคคลที่อายุต่ำกว่า 13 ปี รวมถึงข้อกำหนดของคณะกรรมการกลางกำกับดูแลกิจการสื่อสาร (FCC) ตาม 16 C.F.R. § 312 เพื่อให้เจ้าของเว็บไซต์หรือผู้ให้บริการออนไลน์ตรวจสอบอายุของผู้ที่จะเข้าถึงระบบข้อมูล การดาวน์โหลดข้อมูล และยังมีหน้าที่เปิดเผยข้อมูลต่อบิดามารดาของเด็กดังกล่าวด้วย

2.2.4 พระราชบัญญัติคุ้มครองเด็กบนสื่อออนไลน์ ค.ศ. 1998 (Children's Online Protection Act of 1998 หรือ COPA)

กฎหมายเฉพาะที่กำหนดโทษทางอาญาไว้สำหรับการเผยแพร่เนื้อหาไม่เหมาะสมหรือมีลักษณะละเมิด (offensive) เด็กผ่านสื่อออนไลน์ประเภทต่างๆ โดยเฉพาะอย่างยิ่งในเว็บไซต์ที่ทำขึ้นเพื่อการค้า กฎหมายนี้ห้ามผู้ให้บริการสื่อออนไลน์ จำหน่ายหรืออนุญาตให้เด็กเข้าถึงสิ่งที่อาจเป็นภยันตรายต่อเด็กได้ อาทิ ข้อมูลที่ไม่เหมาะสมในทางเพศ ซึ่งอาจเป็นกิจกรรมทางเพศ ภาพเปลือย รวมถึงภาพหญิงโชว์หน้าอกด้วย จึงทำให้กฎหมายนี้มีบทบัญญัติที่กว้างขวางกว่ากฎหมายควบคุมสิ่งลามกอนาจารฉบับอื่นๆ

อย่างไรก็ตาม กฎหมายฉบับนี้ถูกศาลสหรัฐพิพากษาว่าขัดต่อรัฐธรรมนูญ เนื่องจากมีถ้อยคำกว้างเกินไป และไม่มีนิยามคำว่า อันตรายต่อเด็ก (harmful to minor) ว่าหมายถึงการกระทำอย่างไรบ้าง[27]

2.2.5. พระราชบัญญัติป้องกันอินเทอร์เน็ตสำหรับเด็ก ค.ศ. 2000 (Children's Internet Protection Act of 2000 หรือ CIPA)

เป็นกฎหมายที่ใช้แรงจูงใจทางงบประมาณมาเป็นกลไกในการคุ้มครองเด็กและเยาวชน มีเนื้อหาเกี่ยวกับการจัดงบประมาณสนับสนุนสถานศึกษาหรือห้องสมุดที่ต้องการรับการสนับสนุนงบประมาณจากรัฐบาลกลาง ตามกฎหมายว่าด้วยการศึกษาระดับประถมและมัธยม (Elementary and Secondary Education Act of 1965) โดยกำหนดให้โรงเรียนและห้องสมุดที่ประสงค์จะรับเงินสนับสนุนจากรัฐบาลกลาง จะต้องใช้มาตรการในการป้องกันหรือตรวจสอบ (filters) มิให้มีการกระทำผิดเกี่ยวกับสื่อลามกอนาจารหรือไม่เหมาะสมต่อเด็ก

อย่างไรก็ดี ภายหลังมีผลใช้บังคับได้เพียง 1 ปี เท่านั้น ก็ถูกสหภาพเสรีภาพพลเมืองอเมริกันร้องต่อศาลว่ากฎหมายนี้มีเนื้อหาที่ขัดต่อรัฐธรรมนูญเช่นกัน ซึ่งแม้ศาลชั้นต้นเห็นว่า เนื้อหาในกฎหมายมีลักษณะจำกัดสิทธิของประชาชนในการเข้าถึงข้อมูลก็ตาม แต่ศาลสูงสุดสหรัฐฯ

ก็ไม่เห็นพ้องด้วยกับผู้ร้องที่ว่า รัฐมิอาจบัญญัติกฎหมายเช่นนี้ได้ จึงพิพากษาว่ากฎหมายฉบับนี้ไม่ขัดต่อรัฐธรรมนูญ ด้วยเหตุผลว่า บทบัญญัตินี้ใช้เฉพาะกับห้องสมุดหรือสถานศึกษาของรัฐเท่านั้น ซึ่งตามปกติแล้ว บรรณารักษ์จะต้องแสวงหาสื่อที่มีประโยชน์และมีคุณภาพสูงสุดมาให้บริการแก่นักเรียนนักศึกษาอยู่แล้ว อีกทั้งห้องสมุดก็มีการแลกเปลี่ยนความคิดเห็น การเข้าถึงข้อมูลและระบบอินเทอร์เน็ต ในลักษณะที่แตกต่างจากพื้นที่สาธารณะทั่วๆ ไป ดังนั้น กฎหมายที่กำหนดให้โรงเรียนหรือห้องสมุดสาธารณะต้องใช้มาตรการกลั่นกรองหรือปิดกั้นเว็บไซต์มิให้สามารถเข้าถึงภาพเคลื่อนไหว (visual depictions) ที่เป็นสิ่งลามกอนาจารและภาพโป๊ของเด็ก รวมทั้งสิ่งอื่นใดที่อาจเป็นอันตรายต่อเด็ก (harmful to minors) จึงเป็นสิ่งที่กระทำได้[28]

2.2.6 พระราชบัญญัติคุ้มครองเด็ก ค.ศ. 2003 (Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act of 2003 หรือ PROTECT Act)

กฎหมายฉบับนี้แก้ไขเพิ่มเติมจากกฎหมายเดิมหลายฉบับ โดยเฉพาะอย่างยิ่ง พระราชบัญญัติความจริงในชื่อโดเมน (Truth in Domain Names Act - TDNA of 2003) ซึ่งบัญญัติไว้ตาม 18 U.S.C. § 2252 (B) (b) รวมถึงแก้ไขปัญหาหลักการทางกฎหมายเดิมที่ว่า “สิ่งลามกอนาจาร” ไม่รวมถึงภาพที่ไม่ใช่มนุษย์ แต่เป็นการสร้างจากจินตนาการของมนุษย์ โดยกฎหมายฉบับนี้ มีข้อกำหนดห้ามไม่ให้ผู้ใดสร้างเว็บไซต์สาธารณะเพื่อหลอกลวงผู้ใช้บริการเกี่ยวกับชื่อเว็บไซต์ของตน และกำหนดให้ต้องมีความรับผิด หากมีการใช้ชื่อโดเมนเนมเพื่อหลอกลวงให้บุคคลอื่นเข้าไปในเว็บไซต์นั้นซึ่งมีภาพลามกอนาจาร หรือเป็นการหลอกลวงเด็กให้เข้าไปในเว็บไซต์ที่มีเนื้อหาเป็นอันตรายต่อเด็ก โทษสูงสุดสำหรับกรณีเหล่านี้สูงถึงขั้นจำคุกตลอดชีวิต อีกทั้งยังให้อำนาจเจ้าหน้าที่สามารถเข้าถึงข้อมูลและดักฟังการติดต่อสื่อสารของบุคคลได้สำหรับกรณีที่มีการล่วงละเมิดต่อเด็กและการลักพาตัวเด็ก นอกจากนี้ ยังมีข้อกำหนดห้ามมิให้ใช้คอมพิวเตอร์

สร้างภาพลามกเด็ก วาดภาพ สร้างรูปปั้น หรือภาพอื่นใดที่มีลักษณะอันลามกตามลักษณะ “Miller Test” (หลักที่ศาลสหรัฐฯ ใช้วินิจฉัยว่าการแสดงออกนั้นๆ เข้าข่ายลามกหรือไม่) ซึ่งก่อนหน้านี้กฎหมายไม่ได้หมายรวมให้กรณีดังกล่าวเป็นสิ่งลามกอนาจาร

อนึ่ง การครอบครองสิ่งลามกดังกล่าวมีความผิดเช่นกัน และต้องระวางโทษจำคุก 5 ปี หากนำไปจำหน่ายระวางโทษจำคุก 10 ปี สำหรับประชาชนชาวสหรัฐฯ ที่กระทำผิด แม้ได้กระทำนอกประเทศสหรัฐจะต้องรับโทษในประเทศ ซึ่งจำคุกไม่เกิน 30 ปี สำหรับการกระทำผิดทางเพศต่อเยาวชนในต่างประเทศ

2.2.7 พระราชบัญญัติความปลอดภัยและการปกป้องเด็ก อดัม วอร์ช ค.ศ. 2006 (Adam Walsh Child Protection and Safety Act of 2006)

เป็นกฎหมายที่ห้ามใช้ถ้อยคำหรือภาพดิจิตอล เพื่อหลอกลวงผู้อื่นให้ต้องเข้าสู่ภาพลามกลามกอนาจาร หรือหลอกลวงเด็กเพื่อเข้าไปดูวัตถุหรือสื่อที่เป็นอันตรายทางเพศต่อเด็ก

2.3 ถ้อยคำที่ก่อให้เกิดความรู้สึกโกรธเคือง หรือสร้างความขัดแย้ง (hostile audience and fighting words)

การแสดงความคิดเห็นที่สร้างความขัดแย้ง หรือ fighting words ที่อาจกระตุ้นให้ผู้ถูกกล่าวถึงกระทำรุนแรงต่อผู้กล่าวถ้อยคำนั้น ถ้อยคำที่ทำให้บุคคลธรรมดาทั่วไปสามารถรู้สึกโกรธแค้นได้ หรือมีความรุนแรงถึงขนาดที่จะต้องโต้ตอบทำร้ายกันไม่ได้รับความคุ้มครองตามรัฐธรรมนูญสหรัฐฯ โดยมีการยืนยันหลักการนี้ในหลายคดี เช่น คดี Feiner v. New York, 340 U.S. 315 (1951) ซึ่งจำเลยกล่าวว่า ประธานาธิบดีทรูแมนเป็นคนเกียจคร้าน (bum) ฯลฯ ทั้งยังเรียกร้องให้สมาชิกจับอาวุธขึ้นต่อสู้เพื่อสิทธิของตนตามกฎหมาย การใช้ถ้อยคำดังกล่าวเป็นผลให้ประชาชนที่ได้รับฟัง นำความไปแจ้งกับตำรวจและว่าถ้าตำรวจไม่จัดการไอ้ลูกโสเภณี

(son of the bitch) ที่กล่าวถ้อยคำดังกล่าวอยู่ พวกเขาจะไปจัดการกันเอง ตำรวจพยายามร้องขอให้จำเลยหยุดกล่าว แต่ก็ถูกปฏิเสธ ตำรวจจึงจับกุมจำเลยมาดำเนินคดี ศาลสูงสุดเห็นว่าการกล่าวถ้อยคำของจำเลยเป็นการยั่วยุให้เกิดความไม่สงบเรียบร้อยอย่างรุนแรงขึ้น การใช้ดุลพินิจของตำรวจและเข้าจับกุมเพื่อป้องกันภยันตรายที่อาจจะเกิดขึ้นได้ จึงเป็นเรื่องที่ชอบด้วยกฎหมาย[29] ไม่ใช่การกระทำที่ขัดต่อรัฐธรรมนูญ

2.4 ถ้อยคำหมิ่นประมาท หรือละเมิดเสรีภาพส่วนบุคคล (defamation and invasion of privacy)

ถ้อยคำที่มีลักษณะใส่ความหรือกล่าวให้ร้ายบุคคลอื่น (defamation) ไม่ได้รับความคุ้มครองตามรัฐธรรมนูญ ทั้งนี้ไม่ว่าจะเป็นการหมิ่นประมาทปัจเจกชนหรือกลุ่มบุคคลก็ตาม โดยการกระทำเช่นนี้ผู้กระทำอาจมีโทษทางอาญา อย่างไรก็ตาม การกำหนดความรับผิดทางอาญาสำหรับบุคคลที่กล่าววิพากษ์วิจารณ์การปฏิบัติงานของเจ้าหน้าที่รัฐนั้นมีข้อจำกัดบางประการดังเช่นที่ปรากฏในคดี New York Times Co. v. Sullivan, 376 U.S. 254 (1964) ศาลในคดีนี้พิพากษาว่า ในกรณีที่สื่อมวลชนวิพากษ์วิจารณ์การปฏิบัติหน้าที่ของเจ้าหน้าที่รัฐหรือบุคคลสาธารณะนั้น สื่อมวลชนจะต้องรับผิดทางอาญาก็ต่อเมื่อมีเจตนาที่จะแสดงข้อความอันเป็นเท็จ หรือมีเจตนาที่จะละเลยการแสวงหาความจริง หากสื่อมวลชนแสดงให้เห็นว่าความผิดพลาดในการเสนอข่าวสารนั้นเป็นความผิดพลาดโดยสุจริต (honest error) และเป็นการวิพากษ์วิจารณ์ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ (official conduct) เท่านั้น ไม่เกี่ยวกับเรื่องส่วนตัวของเจ้าหน้าที่รัฐ สื่อนั้นย่อมไม่มีความรับผิด

"ขอบเขตแห่งเสรีภาพของสื่อมวลชน ไม่ได้มีเพียงเสรีภาพในการเผยแพร่ข้อมูลข่าวสารเท่านั้น แต่ยังขยายความไปถึงเสรีภาพโดยปราศจากการลงโทษใดๆ เมื่อสื่อมวลชนนั้นนำเสนอข้อมูลที่เป็นเรื่องจริง ทั้งยังเกี่ยวข้องกับประโยชน์สาธารณะ"

ดังกล่าวมาแล้วว่า ประเทศสหรัฐอเมริกาให้ความสำคัญกับเสรีภาพในการแสดงความคิดเห็นอย่างมากในฐานะที่เป็นส่วนสำคัญของการปกครองในระบอบประชาธิปไตย การวิพากษ์วิจารณ์บุคคลสาธารณะโดยเฉพาะอย่างยิ่งการปฏิบัติหน้าที่โดยเจ้าพนักงานรัฐ กระทั่งการวิพากษ์วิจารณ์คำตัดสินของผู้พิพากษาก็ควรเป็นสิ่งที่ประชาชนกระทำได้โดยชอบ ดังนั้น แม้รัฐจะสามารถจำกัดเสรีภาพในการแสดงความคิด สำหรับกรณีที่ความคิดเห็นนั้นเข้าข่ายหมิ่นประมาทบุคคลอื่นได้ก็ตาม แต่รัฐจะกำหนดให้เป็นความรับผิดโดยเด็ดขาด (strict liability) สำหรับการหมิ่นประมาทบุคคลสาธารณะ (public figure) ไม่ได้ ซึ่งแตกต่างจากการหมิ่นประมาทบุคคลทั่วไปที่เป็น private figure

2.5 โฆษณาเพื่อประโยชน์ทางการค้า (commercial speech)

การโฆษณาเพื่อประโยชน์ทางการค้านั้น แม้เป็นเรื่องที่ได้รับความคุ้มครองตามรัฐธรรมนูญ แต่ก็ได้รับความคุ้มครองในระดับที่ต่ำกว่าการแสดงความเห็นในกรณีทั่วๆ ไป รัฐสามารถควบคุมการโฆษณาสินค้าให้มีความถูกต้องตรงกับความเป็นจริง (truthful speech) ได้ และหากการโฆษณาใดไม่ตรงกับความจริงหรือถึงขั้นหลอกลวงทำให้หลงผิด หรือมีลักษณะเป็นความผิดกฎหมาย (false, deception, or illegal) รัฐอาจจะจำกัดหรือห้ามการเผยแพร่การโฆษณานั้นๆ ได้ แต่การกำหนดให้เอกชนต้องส่งสื่อโฆษณาให้รัฐตรวจสอบ หรืออนุญาตก่อนการโฆษณาไม่อาจกระทำได้

3. แนวนโยบาย กฎหมาย และแนวทางปฏิบัติที่เกี่ยวกับสื่อออนไลน์

ในอดีต การตรวจสอบและควบคุมการนำเสนอข้อมูลผ่านระบบออนไลน์เป็นสิ่งไม่พึงปรารถนาของสังคมอเมริกัน และถูกต่อต้านตลอดมาทั้งฝ่ายนักวิชาการและองค์กรศาล แม้ฝ่ายรัฐบาลมีความประสงค์ที่จะออกฎหมายควบคุมการนำเสนอข่าวสารใดๆ แต่ก็ถูกวิพากษ์วิจารณ์และพิพากษาว่าขัดต่อรัฐธรรมนูญ ตามหลักสิทธิเสรีภาพขั้น

พื้นฐานของสหรัฐอเมริกาเสมอมา ในขณะที่ความพยายามในการควบคุมการแสดงความคิดเห็นโดยรัฐบาล ก็คุมได้เพียงบางประเด็นเท่านั้น และจะต้องผ่านการฟ้องร้องดำเนินคดี ไม่ใช่การปิดกั้น ทั้งนี้ ผู้ประกอบการอินเทอร์เน็ตในสหรัฐอเมริกาสามารถกำหนดมาตรการขึ้นเองได้เพื่อควบคุมเนื้อหาให้สอดคล้องกับหลักการเคารพเสรีภาพสื่อออนไลน์

รัฐบาลสหรัฐได้เริ่มควบคุมสื่อออนไลน์ ตั้งแต่ช่วงคริสตศตวรรษ 1990 เป็นต้นมา เพื่อแก้ไขปัญหาสื่อลามกที่แพร่หลายบนอินเทอร์เน็ต แต่กฎเกณฑ์ที่ออกมาก็ไม่สามารถแก้ไขปัญหาอย่างสมบูรณ์ได้ เนื่องจากถูกต่อต้านจากนักวิชาการและฝ่ายตุลาการ ทำให้กฎเกณฑ์ดังกล่าวถูกพิพากษาว่าขัดรัฐธรรมนูญ อย่างไรก็ตาม รัฐบาลเริ่มประสบความสำเร็จในการตรวจสอบและเฝ้าระวังสื่อออนไลน์มากขึ้น ด้วยการอ้างเหตุผลความมั่นคงของรัฐ (national security) ภายหลังเกิดเหตุการณ์การก่อการร้าย 11 กันยายน โดยรัฐบาลสามารถเข้าถึงข้อมูลออนไลน์ หรือ surveillance of digital communications ได้เพื่อตรวจสอบควบคุมและบัญญัติให้ผู้ประกอบการจัดเก็บข้อมูลออนไลน์ เพื่อให้เจ้าหน้าที่สามารถตรวจสอบและแกะรอยในภายหลังได้อย่างมีประสิทธิภาพ

อย่างไรก็ตาม เนื่องจากเป็นที่ยอมรับว่า เครือข่ายข้อมูลข่าวสารมีความสำคัญต่อสังคมและประชาคมระหว่างประเทศอย่างมาก โดยเฉพาะอย่างยิ่ง ในกรณีที่เกิดภัยพิบัติ แม้ในประเทศที่มีการปกครองแบบเผด็จการ ระบบเครือข่ายข้อมูลก็ทำให้รัฐบาลจะต้องตระหนักถึงความรับผิดชอบต่อประชาชนมากยิ่งขึ้น ยิ่งสังคมเปิดเสรีบนสื่อออนไลน์มากเท่าใด ก็จะยิ่งทำให้สังคมมีความเข้มแข็งและทำให้รัฐบาลมีความโปร่งใสและความรับผิดชอบต่อสังคมยิ่งขึ้น ในขณะเดียวกันก็กระตุ้นให้ปัจเจกชนมีความรู้สึกเป็นเจ้าของประเทศร่วมกัน ดังกล่าวมาแล้วว่า การแลกเปลี่ยนข้อมูลข่าวสารตามหลักการตลาดเสรีทางความคิดเป็นสิ่งสำคัญ ทั้งนี้ สหรัฐฯ ยอมรับหลักการนี้นับแต่ก่อตั้งประเทศ ทั้งยังผลักดันให้ได้รับรองไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human

Rights) ด้วย ซึ่งประชาชนสามารถวิพากษ์วิจารณ์รัฐบาลได้โดยเสรีและปราศจากความหวาดกลัว และสามารถเข้าถึงและสื่อสารผ่านเครือข่ายสังคมออนไลน์โดยปราศจากการตรวจสอบหรือปิดกั้นจากรัฐ

แม้เป็นที่ยอมรับว่า เสรีภาพในการแสดงความคิดเห็นก็มีข้อจำกัดในตัวเอง และสหรัฐฯ เองก็กำหนดเนื้อหาต้องห้ามไม่ให้เผยแพร่หลายลักษณะดังที่กล่าวไปแล้ว แต่เนื่องจากรัฐบาลสหรัฐฯ มีความเชื่อมั่นว่า ความมั่นคงของชาติและความเจริญงอกงามทางเศรษฐกิจสามารถพัฒนาไปพร้อมกันได้ภายใต้การใช้งานอินเทอร์เน็ต แม้ในด้านหนึ่งจะมีคนพยายามกระทำผิดบนสื่อออนไลน์ เช่น เข้าถึงข้อมูลเกี่ยวกับการเงินการธนาคารโดยไม่ได้รับอนุญาต เผยแพร่สื่อลามกทางเพศที่เกี่ยวกับเด็ก ค้าหญิงและเด็กออนไลน์ แต่ในอีกด้านหนึ่ง การติดต่อสื่อสารและการบริการข้อมูลที่รวดเร็วหลากหลายบนอินเทอร์เน็ตก็ช่วยทำให้ระบบต่างๆ ในประเทศพัฒนาไปได้อย่างรวดเร็วด้วย ดังนั้น ที่ผ่านมารัฐบาลสหรัฐฯ จึงดำเนินการทางการทูตสนับสนุนให้ประเทศต่างๆ ร่วมกันกำหนดนโยบายในการส่งเสริมเสรีภาพออนไลน์ เพื่อการส่งเสริมประชาธิปไตยและศักดิ์ศรีความเป็นมนุษย์ แต่ในขณะเดียวกันก็ร่วมกันปราบปรามอาชญากรรมบนเครือข่ายคอมพิวเตอร์ไปพร้อมกันด้วย

ปัจจุบัน รัฐบาลสหรัฐอเมริกามีแนวนโยบายที่เกี่ยวข้องกับการควบคุมสื่อออนไลน์ โดยสรุปได้ ดังนี้

3.1 นโยบายให้เอกชนมีส่วนร่วมในการพัฒนาซอฟต์แวร์เพื่อควบคุมเนื้อหาที่ไม่เหมาะสม

ในสหรัฐอเมริกา ผู้ให้บริการอินเทอร์เน็ตมีหน้าที่ต้องพัฒนาระบบซอฟต์แวร์เพื่อกลั่นกรองข้อมูล หรือเว็บไซต์ที่มีเนื้อหาเกี่ยวข้องกับภาพลามกอนาจารเด็ก โดยระบบเหล่านั้นจะต้องสามารถทำงานได้โดยอัตโนมัติ และไม่มีข้อผิดพลาดหรือมีน้อยที่สุดเพื่อไม่ให้การตรวจสอบกลั่นกรอง หรือการปิดกั้นนั้นไปกระทบกับเนื้อหาประเภทอื่นใดที่ไม่ใช่เนื้อหาที่ไม่เหมาะสม (false positives) นอกจากนี้ ยังมีบริษัท

เอกชนจำนวนหนึ่งพัฒนาซอฟต์แวร์เพื่อกลั่นกรองเนื้อหาจากปลายทางของผู้รับข้อมูลข่าวสารเหล่านั้นเอง เช่น บิดามารดา หรือนิติบุคคลนำไปใช้ในบ้าน หรือองค์กรของตนเพื่อกลั่นกรองเนื้อหาที่ไม่อยากให้บุตรหลาน หรือพนักงานเข้าถึงได้ เป็นต้น ซึ่งจะแตกต่างจากกรณีของการปิดกั้นโดยฝ่ายผู้ให้บริการอินเทอร์เน็ตอันเป็นการกลั่นกรองและปิดกั้นช่องทางมาตั้งแต่แหล่งกำเนิดข้อมูลดังกล่าว นอกจากนี้รัฐบาลยังกำหนดให้สถานศึกษา หรือห้องสมุดที่ได้รับเงินสนับสนุนจากรัฐต้องใช้ซอฟต์แวร์ปิดกั้นการเข้าถึงสื่อลามกอนาจารด้วย

3.2 การป้องกันมิให้ประชาชนเข้าถึงเนื้อหาที่เกี่ยวด้วยความมั่นคงของชาติ (national security)

แม้ประเทศสหรัฐอเมริกาจะให้สิทธิกับประชาชนในการเข้าถึงข้อมูลของฝ่ายรัฐในทุกๆ กรณี แต่สำหรับข้อมูลที่เกี่ยวข้องกับความมั่นคงของรัฐ หรือข่าวสารใดที่อาจจะสร้างความเสียหายต่อชื่อเสียงของรัฐบาลได้ ก็ปรากฏว่ามีการใช้อำนาจในทางบริหารภายในสั่งให้ปิดกั้นช่องทางเพื่อไม่ให้ประชาชนเข้าถึงข้อมูลเหล่านั้นได้ กรณีที่เคยเกิดขึ้นแล้ว เช่น สมัยประธานาธิบดีจอร์จ ดับเบิลยู บุช และ บารัค โอบามา รัฐบาลปิดกั้นการเข้าถึงเนื้อหาของบางเว็บไซต์ในสหรัฐอเมริกา โดยจากการตรวจสอบของภาคเอกชนซึ่งใช้วิธีการค้นหาข้อมูลที่เกี่ยวกับสงครามในปากีสถานหรืออิรักในเว็บไซต์กูเกิลจะไม่พบข้อมูล หรือบทความที่เขียนวิพากษ์วิจารณ์การทำสงครามดังกล่าวเลย ในขณะที่หากค้นหาข้อมูลแบบเดียวกันในประเทศอื่นๆ ในยุโรป จะพบข้อมูลเหล่านั้นปรากฏอยู่[30]

ในทางกฎหมายที่เป็นลายลักษณ์อักษรนั้น พบว่าการปิดกั้นข้อมูลข่าวสารที่เป็นความลับอันกระทบต่อความมั่นคงชาติ จะเป็นไปตามกฎหมายจารกรรม ค.ศ. 1917 (Espionage Act of 1917) ซึ่งกำหนดให้เป็นความผิดทางอาญาด้วย หากมีการเปิดเผยความลับทางการทหารตามนัย 18 U.S.C § 793 (d) และ (e)[31] แต่ประเด็นปัญหาที่เกิดขึ้นในความเป็นจริงก็คือ รัฐมักอ้างเหตุผลเดียวกันนี้เพื่อห้ามไม่ให้เปิดเผยข้อมูล

ข่าวสารของทางราชการประเภทอื่นๆ ด้วย จนในปี ค.ศ. 1966 สภาคองเกรสต้องตรากฎหมายเกี่ยวกับเสรีภาพในการเข้าถึงข้อมูลข่าวสารขึ้นฉบับหนึ่ง ชื่อว่า พระราชบัญญัติเสรีภาพในการเข้าถึงข้อมูลข่าวสาร ค.ศ. 1966 (Freedom of Information Act of 1966 - FOIA) แก้ไขเพิ่มเติมประมวลกฎหมายปกครอง (Administrative Procedure Act of 1946) เพื่อให้เป็นหลักประกันแก่ประชาชนว่าสามารถเข้าถึงข้อมูลของฝ่ายรัฐได้เสมอ เพราะถือเป็นสิทธิตามรัฐธรรมนูญ (public rights to know)[32] และหากรัฐประสงค์จะปิดกั้นการเข้าถึงข้อมูลดังกล่าวรัฐจะอ้างว่าเป็นข้อมูลที่เป็นความลับหรือกระทบต่อความมั่นคงของชาติลอยๆ ไม่ได้ แต่ต้องแสดงพยานหลักฐานที่หนักแน่นเพียงพอว่าการเปิดเผยนั้นจะเกิดภยันตรายอย่างแท้จริง (clear and present danger) ฯลฯ มิเช่นนั้นศาลจะสั่งให้รัฐเปิดเผยทุกกรณี[33] โดยผลของกฎหมายฉบับนี้ การปิดกั้นข้อมูลของทางราชการจึงเกิดขึ้นไม่ได้อีกต่อไป[34] เว้นแต่จะเข้าข้อยกเว้นที่กำหนดไว้อย่างชัดเจนเกี่ยวกับความมั่นคง เช่น การเปิดเผยข้อมูลจะกระทบต่อประโยชน์ของชาติในการป้องกันตนเองหรือนโยบายระหว่างประเทศ จะส่งผลกระทบต่อสิทธิและเสรีภาพในความเป็นส่วนตัวของปัจเจกชนอื่นจนเกินสมควร กระทบต่อประสิทธิภาพการปฏิบัติงานของรัฐอย่างร้ายแรง หรือการปิดกั้นนั้นไม่มีประโยชน์ และเป็นเพียงข้อมูล หรือกระบวนการการเสนอความเห็นภายในองค์กรเท่านั้น หรือด้วยเหตุผลว่าข้อมูลดังกล่าวอยู่ระหว่างกระบวนการสืบสวนสอบสวนและการดำเนินคดีทางอาญา เป็นต้น[35]

3.3 ความพยายามที่จะเข้าถึงข้อมูลของบุคคลอื่น ไม่ว่าจะเป็นองค์กร คนต่างชาติ หรือผู้ต้องสงสัยในคดีก่อการร้าย

ในอดีตที่ผ่านมา เป็นที่ยอมรับของศาลสูงสุดว่าฝ่ายบริหารมีอำนาจหน้าที่ตามรัฐธรรมนูญในการรักษาความมั่นคงของประเทศ หากสภาคองเกรสแสดงเจตจำนงอย่างชัดแจ้งว่า ให้เป็นดุลพินิจของฝ่ายบริหารที่จะดำเนินมาตรการใดๆ ในการป้องกันประเทศจากศัตรูแล้ว ศาลก็จะมีอำนาจอย่างจำกัดในอันที่จะตรวจสอบการใช้ดุลพินิจของฝ่ายบริหาร[36]

อย่างไรก็ตาม กรณีดังกล่าวก็หาใช่ว่าศาลจะไม่มีอำนาจในการตรวจสอบความถูกต้องของการกระทำต่างๆ โดยองค์กรบริหารตามหลักนิติรัฐเลย และย่อมถือว่าอันตรายต่อเสรีภาพของประชาชนอย่างยิ่งหากฝ่ายบริหารมีอำนาจอิสระในการเข้าถึงข้อมูล เพื่อดำเนินคดีกับประชาชนโดยไร้การตรวจสอบถ่วงดุลย์จากองค์กรตุลาการ ทั้งนี้ ที่ผ่านมาก็มักเกิดการใช้อำนาจโดยไม่ชอบด้วยกฎหมายของฝ่ายการเมืองอยู่เนืองๆ โดยไม่มีคำร้องขอต่อศาล หรือขอให้ออกหมายศาลเพื่อการตรวจสอบ[37] ในที่สุด สภาคองเกรสจึงตรากฎหมายการตรวจตราข่าวกรองต่างประเทศ (Foreign Intelligence Surveillance Act of 1978 - FISA) แก้ไขล่าสุดปี 1998 เพื่อแก้ปัญหาการตรวจค้นหรือการเข้าถึงข้อมูลโดยไม่มีหมายศาล ตามกฎหมายฉบับนี้ ฝ่ายบริหารต้องขออนุมัติศาลเพื่อการเข้าถึงข้อมูลทางอิเล็กทรอนิกส์ของปัจเจกชนที่เป็นคนในบังคับของชาติศัตรู โดยกระบวนการพิจารณาจะทำโดยศาลพิเศษ (Foreign Intelligence Surveillance Court) ซึ่งรัฐบาลต้องแสดงเหตุผลให้ศาลเห็นว่า มีความจำเป็นต้องเข้าถึงข้อมูลนั้นและไม่มีวิธีการอื่นใดที่จะได้มาซึ่งข้อมูลข่าวสารนั้นอีกแล้ว[38] ทั้งนี้ จะต้องดำเนินการภายในระยะเวลาจำกัด ไม่ว่าจะเป็นการดักฟังโทรศัพท์ การเฝ้าระวังทางระบบโทรคมนาคม และการสื่อสารในรูปแบบต่างๆ[39] อย่างไรก็ตาม กฎหมายฉบับนี้ยังมีข้อยกเว้นที่กำหนดให้อำนาจแก่ประธานาธิบดีสหรัฐอเมริกาผ่านรัฐมนตรียุติธรรม สามารถสั่งให้เจ้าหน้าที่ดักฟังและเข้าถึงข้อมูลอิเล็กทรอนิกส์ทุกรูปแบบโดยไม่ต้องขอหมายจากศาลเมื่อมีเหตุจำเป็นเร่งด่วน และสามารถปฏิบัติการได้เป็นระยะเวลาหนึ่งปี[40]

สำหรับการเข้าถึงข้อมูลส่วนบุคคลในระบบอิเล็กทรอนิกส์นั้น ตามปกติแล้ว เจ้าหน้าที่รัฐต้องปฏิบัติตามกฎหมายการควบคุมอาชญากรรม ค.ศ. 1968 (Omnibus Crime Control and Safe Street Act of 1968) ซึ่งถูกกำหนดไว้ในประมวลกฎหมายลำดับที่ 18 มาตรา 2510-2522 (18 U.S.C.§§ 2510-2522) ว่า การค้นและตรวจสอบข้อมูลคอมพิวเตอร์ รวมทั้งการดักฟังการสนทนา จะต้องได้รับอนุญาตจากศาลก่อน อนึ่ง กฎหมายฉบับนี้คุ้มครองเพียงข้อมูลที่ยังอยู่ใน “ระหว่างการส่ง” (transfer) เท่านั้น

ไม่คุ้มครองข้อมูลที่กระบวนการส่งสิ้นสุดลงแล้ว เนื่องจากกฎหมายมองว่าสิทธิในความเป็นส่วนตัวของ “ผู้ส่ง” หมดสิ้นไปเมื่อผู้รับได้รับข้อมูลนั้น เช่นนี้ หากเจ้าหน้าที่รัฐตรวจสอบคอมพิวเตอร์ของฝ่ายผู้รับ ย่อมไม่ถือเป็นการละเมิดสิทธิของผู้ส่ง ตามกฎหมายฉบับนี้[41]

กฎหมายความเป็นส่วนตัวในการสื่อสารอิเล็กทรอนิกส์ (Electronic Communication Privacy Act of 1986 - ECPA) เป็นกฎหมายอีกฉบับหนึ่งที่ห้ามมิให้รัฐตรวจสอบข้อมูลในระบบออนไลน์โดยไม่มีหมายศาล ตาม 18 U.S.C. §2703 (b) (A)-(B), (c) (1) (B) หากผู้เป็นเจ้าของคอมพิวเตอร์ตั้งรหัสผ่านไว้ สิทธิในความเป็นส่วนตัวย่อมได้รับความคุ้มครอง การตรวจค้นหรือเข้าถึงข้อมูลออนไลน์ทั่วไปโดยไม่มีหมายศาลไม่อาจกระทำได้[42] อย่างไรก็ตาม กรณีนี้ย่อมต่างจากการเข้าถึงคอมพิวเตอร์ที่เปิดให้บริการเป็นสาธารณะ และไม่มีสิทธิในความเป็นส่วนตัว[43] รวมถึงข้อมูลต่างๆ ที่จัดให้มีขึ้นและเผยแพร่บนอินเทอร์เน็ตด้วย[44] ซึ่งแม้กระทั่งได้ตั้งรหัสเข้าไว้ แต่หากทำให้ปรากฏ และบุคคลสามารถเข้าได้โดยอัตโนมัติ ก็แสดงให้เห็นว่าเจ้าของคอมพิวเตอร์ไม่ได้คาดหวังความเป็นส่วนตัว ดังนั้น การค้นและยึดคอมพิวเตอร์ในกรณีหลังนี้ย่อมไม่มีความจำเป็นต้องใช้หมายศาล

อย่างไรก็ดี ภายหลังการก่อการร้ายถล่มตึกเวิลด์เทรดเซ็นเตอร์เมื่อวันที่ 11 กันยายน 2001 รัฐบาลสหรัฐฯ ได้เพิ่มระดับความเข้มงวดในการจำกัดเสรีภาพในสื่ออนไลน์มากขึ้น ทั้งยังให้อำนาจรัฐในการเข้าถึงข้อมูลต่างๆ ทางสื่อออนไลน์ของประชาชนได้มากยิ่งขึ้นด้วยกฎหมายพิเศษที่สภาคองเกรสตราขึ้นภายหลังเกิดเหตุเพียง 45 วัน ได้แก่ กฎหมายการป้องกันและปราบปรามการก่อการร้ายสหรัฐอเมริกา (Uniting and Strengthening American by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism หรือ USA PATRIOT Act) บัญญัติขึ้นเพื่อแก้ไขเพิ่มเติมกฎหมายเดิม คือ กฎหมายโครงสร้างพื้นฐานสารสนเทศแห่งชาติ (National Information Infrastructure Protection Act of 1996[45] หรือ NIIPA) และกฎหมายฉบับอื่นๆ อย่าง กฎหมายการฉ้อโกงทางละเมิดและการทำละเมิด (Computer Fraud and Abuse Act of 1984, 1986 และ

1994[46]) และกฎหมายการตรวจตราข่าวกรองต่างประเทศ (FISA) โดยมีบทบัญญัติให้อำนาจแก่หน่วยงานความมั่นคงของรัฐ รวมถึงเอฟบีไออย่างกว้างขวาง อาทิ สามารถใช้เทคโนโลยีที่ชื่อ “คาร์นิวอร์” (Carnivore) เพื่อเข้าถึงข้อมูลทางอิเล็กทรอนิกส์ผ่านระบบออนไลน์ ดักฟัง (wiretap) และเฝ้าระวังระบบอีเมล หรือเข้าถึงข้อมูลของชาวต่างชาติ หรือองค์กรภายใต้การสนับสนุนของต่างชาติที่ต้องสงสัยว่าจะเป็นอันตรายต่อสหรัฐฯ อีกทั้งสามารถนำข้อมูลที่ได้มาไปใช้ประโยชน์ในการสืบสวนสอบสวน และเป็นพยานหลักฐานในชั้นศาลได้

สำหรับขั้นตอนในการเข้าถึงข้อมูลข้างต้น แม้จะอ้างเหตุผลเรื่อง “ความมั่นคง” แล้วก็ตาม รัฐก็จะต้องปฏิบัติตามขั้นตอนที่กำหนดไว้โดยรัฐมนตรีกระทรวงยุติธรรม ทั้งจะต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Privacy Protection Act of 1980 หรือ PPA 42 U.S.C. § 2000aa) ด้วย กล่าวคือ เจ้าหน้าที่จะต้องขอรับความเห็นชอบจากผู้ช่วยรัฐมนตรีกระทรวงยุติธรรม แผนกคดีอาญา และส่วนงานอาชญากรรมคอมพิวเตอร์และทรัพย์สินทางปัญญา (Computer Crime and Intellectual Property Section - CCIPS) ซึ่งเป็นฝ่ายวิเคราะห์และสนับสนุนข้อมูลที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของกระทรวงยุติธรรมก่อน[47] เมื่อได้รับอนุญาตแล้ว เจ้าหน้าที่ของรัฐจึงสามารถใช้หมายเรียกเพื่อขอพยานหลักฐานจากสำนักพิมพ์หรือบุคคลได้ และจะต้องละเว้นจากการค้นหากไม่จำเป็น แต่หลักการพื้นฐานเรื่องสิทธิเสรีภาพในการแสดงความคิดเห็นและการคุ้มครองข้อมูลส่วนบุคคลก็มีข้อยกเว้น เช่น กรณีการค้นหาสิ่งผิดกฎหมาย หรือสิ่งที่ได้มาจากการกระทำผิด กาiค้นเพื่อพบและจับผู้ต้องสงสัย รวมทั้งกรณีมีเหตุจำเป็นเร่งด่วนอย่างยิ่งที่จะต้องค้นทันทีเพื่อป้องกันการบาดเจ็บต่อร่างกายหรือความตาย (42 U.S.C. § 2000aa (a) (2)- 2000aa (b) (2)) ดังนั้น ปัจจุบัน เมื่อนำการคุ้มครองข้อมูลส่วนบุคคลมาใช้กับการกระทำผิดเกี่ยวกับคอมพิวเตอร์ จึงเกิดปัญหาการตีความพอสมควร เพราะเทคโนโลยีและวิทยาการได้เปลี่ยนแปลงไปจากปี 1980 แล้ว

อาจกล่าวสรุปได้ว่า ในกรณีที่รัฐอ้างเหตุผลเพื่อความมั่นคงของ

ชาติ เจ้าหน้าที่ของรัฐจะสามารถเข้าถึงข้อมูลข่าวสาร และสามารถตรวจค้น รวมทั้งยึดพยานหลักฐานในระบบคอมพิวเตอร์ได้เป็นกรณีพิเศษ แตกต่างจากกรณีปกติที่เจ้าหน้าที่ของรัฐไม่อาจกระทำการต่างๆ ดังกล่าวได้ แต่จะต้องปฏิบัติตามรัฐธรรมนูญสหรัฐอเมริกา[48] อย่างเคร่งครัด อย่างไรก็ตาม การดำเนินการต่างๆ ของรัฐบาลสหรัฐฯ ตามกฎหมายฉบับนี้ ก่อให้เกิดกระแสวิพากษ์วิจารณ์อย่างมากว่า เป็นการละเมิดสิทธิและเสรีภาพของผู้ใช้อินเทอร์เน็ตเกินสมควร โดยอ้างมาตรการเพื่อรักษาความมั่นคงของชาติ หรือสงครามต่อต้านการก่อการร้าย

3.4 ควบคุมสื่อออนไลน์ด้วยการกำหนดภาระหน้าที่ต่าง ๆ ให้กับผู้ให้บริการอินเทอร์เน็ต

กรณีที่เจ้าหน้าที่รัฐประสงค์จะตรวจสอบหรือเข้าถึงข้อมูลบางประเภท เช่น ข้อมูลเกี่ยวกับชื่อผู้สมัครใช้อีเมลและรายละเอียดอื่นๆ ของผู้ใช้อินเทอร์เน็ตจากผู้ให้บริการ เจ้าหน้าที่รัฐต้องอาศัยอำนาจตามกฎหมายว่าด้วยการจัดเก็บข้อมูลการสื่อสาร (Stored Communications Act - SCA) ซึ่งถูกนำมาจัดไว้ในประมวลกฎหมายลำดับที่ 18 มาตรา 2701–2712 (18 U.S.C.§§ 2701-2712) อันเป็นส่วนหนึ่งของกฎหมายความเป็นส่วนตัวในการสื่อสารอิเล็กทรอนิกส์ (Electronic Communication Privacy Act) วัตถุประสงค์เพื่อให้อำนาจเจ้าหน้าที่รัฐออกหมายเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการอินเทอร์เน็ตได้ หรือกล่าวอีกอย่างได้ว่า SCA คือกฎหมายที่กำหนดหน้าที่แก่ผู้ให้บริการอินเทอร์เน็ตต้องจัดเก็บข้อมูลต่างๆ เกี่ยวกับการใช้งานคอมพิวเตอร์ ชื่อบัญชี กระทั่งข้อมูลเกี่ยวกับตัวผู้ใช้บริการอินเทอร์เน็ต และมีหน้าที่ต้องส่งมอบแก่เจ้าหน้าที่เมื่อได้รับการร้องขอ

3.5 การแก้ปัญหาละเมิดลิขสิทธิ์ในออนไลน์

นอกเหนือจากสิ่งลามกอนาจารเด็กและเยาวชน ปัญหาความลับของหน่วยงาน และการก่อการร้ายแล้ว ในช่วงหลายปีที่ผ่านมา เนื้อหา

หรือกิจกรรมอีกประเภทหนึ่งที่ประเทศสหรัฐอเมริกาเข้มงวดกวดขัน และมีความพยายามที่จะออกกฎหมายเพื่อควบคุมอย่างเคร่งครัด จนบางกรณีอาจถูกมองว่าเกินขอบเขต หรือถึงขั้นละเมิดเสรีภาพของประชาชนในสื่อออนไลน์มากเกินไป ก็คือ การละเมิดทรัพย์สินทางปัญญา ดังจะเห็นได้จากกรณีการผลักดันร่างกฎหมายสองฉบับ คือ กฎหมายหยุดยั้งการละเมิดลิขสิทธิ์ออนไลน์ (Stop Online Piracy Act - SOPA) และกฎหมายป้องกันความเสี่ยงออนไลน์ต่อความสร้างสรรค์เชิงเศรษฐกิจและการโจรกรรมทรัพย์สินทางปัญญา (Preventing Real Online Threats to Economic Creativity and Theft to Intellectual Property Act of 2011 - Protect IP Act)

3.5.1 กฎหมายหยุดยั้งการละเมิดลิขสิทธิออนไลน์ (Stop Online Piracy Act - SOPA)

กฎหมายหยุดยั้งการละเมิดลิขสิทธิ์ออนไลน์ หรือ SOPA ในปัจจุบัน มีสถานะเป็นเพียงร่างกฎหมายซึ่งรัฐสภาให้ชะลอการพิจารณาไว้ก่อน จนกว่าจะมีความตกลงที่เป็นที่ยอมรับอย่างกว้างขวางต่อแนวทางแก้ปัญหาของร่างกฎหมายฉบับนี้ SOPA เป็นร่างกฎหมายที่ถูกนำเสนอโดยสภาผู้แทนราษฎร มีวัตถุประสงค์เพื่อจัดการการละเมิดทรัพย์สินทางปัญญาในสื่อออนไลน์ โดยเฉพาะอย่างยิ่งเว็บไซต์ต่างประเทศ ซึ่งอยู่นอกเหนือเขตอำนาจของสหรัฐอเมริกา ประกอบด้วยสาระสำคัญในสองส่วน คือ

1) การปราบปรามการละเมิดทรัพย์สินทางปัญญาออนไลน์ (Combating Online Piracy) ซึ่งเนื้อหาในส่วนนี้ จะกำหนดเครื่องมือสำหรับอัยการสูงสุด (Attorney General) และผู้ทรงสิทธิในทรัพย์สินทางปัญญา (rights holders) เพื่อป้องกันการละเมิดทรัพย์สินทางปัญญา กล่าวคือ

มาตรา 102 กำหนดให้เป็นอำนาจหน้าที่ของอัยการสูงสุดในการป้องกันเว็บไซต์ต่างประเทศที่ละเมิดทรัพย์สินทางปัญญา (foreign-infringing sites)[49] ทั้งนี้ โดยผ่านคำสั่งศาลที่ศาลมีต่อบุคคลที่เป็นตัวกลาง (intermediaries) ให้หยุดหรือเลิกกระทำการใดๆ อันเป็นการละเมิดในรูปแบบของคำสั่งงดเว้นกระทำการชั่วคราว (temporary restraining

order) คำสั่งห้ามในเบื้องต้น (preliminary injunction) หรือคำสั่งห้าม (injunction) ซึ่งจะใช้บังคับกับบุคคลดังต่อไปนี้

• ผู้ให้บริการอินเทอร์เน็ต (internet service provider) ผู้ให้บริการอินเทอร์เน็ตต้องมีมาตรการป้องกันจากการเข้าถึงเว็บไซต์ที่กระทำการละเมิด

• เว็บไซต์ผู้ให้บริการค้นหาข้อมูลทางอินเทอร์เน็ต (internet search engines) เว็บไซต์ผู้ให้บริการค้นหาข้อมูลทางอินเทอร์เน็ต ต้องมีมาตรการป้องกันไม่ให้มีลิงค์ของเว็บไซต์ที่กระทำละเมิดปรากฏในผลการค้นหาทางอินเทอร์เน็ต

• ผู้ให้บริการการชำระเงิน (payment network providers) บริษัทเหล่านี้ได้แก่บริษัทที่ดำเนินการเกี่ยวกับการชำระเงินทางอินเทอร์เน็ต เช่น PayPal, CCBill เป็นต้น มีหน้าที่ต้องป้องกัน ห้าม ระงับ บริการการทำธุรกรรมระหว่างเว็บไซต์ที่กระทำการละเมิดกับลูกค้าในสหรัฐอเมริกา

• ผู้ให้บริการโฆษณาทางอินเทอร์เน็ต (internet advertising services) บริษัทที่จัดหาพื้นที่การโฆษณาในเว็บไซต์โดยได้รับค่าตอบแทนจะต้องมีมาตรการในการหยุดให้บริการโฆษณาในเว็บไซต์ที่กระทำละเมิดหรือให้กับเว็บไซต์ที่กระทำละเมิด

ทั้งนี้ หากบุคคลเหล่านี้ไม่ปฏิบัติตามคำสั่งศาล หรือสร้างมาตรการแทรกแซงการคำสั่งศาล รัฐมนตรีกระทรวงยุติธรรมสามารถดำเนินคดีกับบุคคลเหล่านี้เพื่อให้ปฏิบัติตามคำสั่งได้

มาตรา 203 แห่งร่างกฎหมายฉบับนี้ กำหนดให้ผู้ทรงสิทธิในทรัพย์สินทางปัญญาสามารถกระทำการต่อเว็บไซต์ที่ขโมยทรัพย์สินของสหรัฐ (dedicated to theft of US property)[50] ทั้งที่เป็นเว็บไซต์ภายในและภายนอกสหรัฐอเมริกา โดยการส่งหนังสือบอกกล่าว (notice) ไปยังบุคคลที่เป็นตัวกลางสองประเภท คือ ผู้ให้บริการการชำระเงินและผู้ให้บริการโฆษณาทางอินเทอร์เน็ต โดยกำหนดให้บุคคลเหล่านี้หยุดการให้บริการกับเว็บไซต์นั้นภายใน 5 วัน โดยหากไม่ปฏิบัติตาม ผู้ให้บริการดังกล่าวอาจถูกฟ้องร้อง และมีความรับผิดต่อผู้ทรงสิทธิในทรัพย์สินทางปัญญาได้ และถ้า

ต่อมาศาลพิพากษาว่าเว็บไซต์ที่ถูกกล่าวหานั้นผิดจริง และถูกห้ามดำเนินการต่อไป ตัวกลางก็ต้องหยุดการทำธุรกิจใดๆ กับเว็บไซต์เหล่านั้นด้วย

2) เครื่องมือเพิ่มเติมเพื่อจัดการการละเมิดทรัพย์สินทางปัญญาออนไลน์ (Additional Enhancements to Combat Intellectual Property Theft) โดยร่างกฎหมายฉบับนี้ได้กำหนดบทลงโทษทางอาญาต่อการละเมิดทรัพย์สินทางปัญญาทางสื่ออิเล็กทรอนิกส์ เพิ่มโทษในการละเมิดทรัพย์สินทางปัญญาที่ทำให้เกิดการรั่วไหลของข้อมูลซึ่งทำให้รัฐบาลเสียหาย หรือกระทบต่อปฏิบัติการทางการทหาร นอกจากนี้ ก็ยังเพิ่มบทลงโทษทางอาญาทั้งโทษปรับและจำคุกต่อการสอดแนมทางเศรษฐกิจ (economic espionage) หรือการสอดแนมในความลับทางการค้า (trade secret)

SOPA ยังกำหนดให้มีตำแหน่งผู้แทนทางการทูตด้านทรัพย์สินทางปัญญา (Intellectual Property Attaché) ซึ่งจะได้รับมอบหมายให้ประจำอยู่ที่สถานทูตเพื่อทำให้หน้าปกป้อง พัฒนา และบังคับใช้สิทธิในทรัพย์สินทางปัญญาของสหรัฐอเมริกาตามกฎหมายทั่วโลก ทั้งต้องทำรายงานต่อผู้ประสานงานด้านการบังคับใช้ทรัพย์สินทางปัญญาของสหรัฐอเมริกา (US Intellectual Property Enforcement Coordinator) ด้วย

ผลกระทบของกฎหมาย SOPA ที่อาจมีต่อเสรีภาพในสื่อออนไลน์

ปัญหาของ SOPA ก็คือ ร่างกฎหมายฉบับนี้ กำหนดนิยามคำว่า “เว็บไซต์ที่กระทำละเมิด” ไว้อย่างกว้างขวาง กล่าวคือ เว็บไซต์ที่ให้การสนับสนุน (facilitate) ซึ่งครอบคลุมรวมไปถึงเว็บไซต์ที่ให้ผู้ใช้บริการเป็นผู้สร้างเนื้อหาด้วยตนเองด้วย (user-generated sites) เช่น เฟซบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) ยูทูบ (YouTube) และบล็อก (blog) โดยแม้มีเพียงแค่ส่วนหนึ่งของเนื้อหาที่เข้าข่ายละเมิดทรัพย์สินทางปัญญา เว็บไซต์นั้นไม่ว่าจะมีจำนวนหลายหน้าก็จะต้องถูกดำเนินการทั้งหมด

นอกจากนี้ ร่างกฎหมายยังกำหนดด้วยว่า ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการค้นหาข้อมูลทางอินเทอร์เน็ต ผู้ให้บริการการชำระเงิน ผู้ให้บริการ

โฆษณาทางอินเทอร์เน็ต สำนักทะเบียนหรือนายทะเบียนของชื่อโดเมนที่มีมาตรการเพื่อปิดกั้น ตรวจสอบ หรือตรวจตราเว็บไซต์ที่เชื่อได้ว่าละเมิดทรัพย์สินทางปัญญาของสหรัฐอเมริกา ผู้ให้บริการดังกล่าวจะได้รับการคุ้มกันจากการฟ้องร้องจากผู้ใช้บริการ ซึ่งการบัญญัติกฎหมายลักษณะนี้ย่อมก่อให้เกิดปัญหาเป็นอย่างมาก เพราะนอกจากจะทำให้ผู้ให้บริการหรือตัวกลางทำตัวเหมือนตำรวจและคอยสอดส่องเนื้อหา เพื่อให้ตนไม่ต้องมีความรับผิดแล้ว หากปรากฏว่าตัวกลางปิดกั้นเว็บไซต์นั้นโดยความผิดพลาดของตัวเอง ตัวกลางนั้นก็ยังได้รับความคุ้มกันจากการฟ้องร้องอยู่ดี ซึ่งย่อมส่งผลต่อเสรีภาพของผู้ใช้บริการอย่างมิอาจหลีกเลี่ยง

SOPA ยังให้อำนาจแก่ผู้ทรงสิทธิในทรัพย์สินทางปัญญาซึ่งเป็นเอกชน สามารถเรียกร้องให้ผู้ให้บริการที่กำหนดไว้ หยุดให้บริการกับเว็บไซต์ที่ละเมิดทรัพย์สินทางปัญญาได้อีกด้วย ซึ่งถือเป็นการกระทำที่นอกเหนือจากการควบคุมดูแลโดยอาศัยกระบวนการทางยุติธรรม และปัญหาก็คือ ปกติแล้วผู้ให้บริการประเภทต่างๆ มักมีแนวโน้มที่จะทำตามหนังสือบอกกล่าวของผู้ทรงสิทธิในทรัพย์สินทางปัญญาเสมอ เพื่อป้องกันไม่ให้ตนเองต้องมีความรับผิด[51] ซึ่งเหล่านี้เองย่อมส่งผลให้ “การปิดกั้นเว็บไซต์” เกิดขึ้นได้อย่างง่ายดาย ทั้งยังเป็นสิ่งที่ชอบธรรมตามกฎหมาย จนมีผู้กล่าวว่า ข้อกำหนดต่างๆ ในร่างกฎหมายฉบับนี้ละเมิดรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่หนึ่งของสหรัฐอเมริกา[52] เนื่องจากเปิดโอกาสให้เอกชนสามารถปิดกั้นการแสดงความคิดเห็น หรือระงับการให้บริการกับเว็บไซต์ที่เพียงถูกกล่าวหาว่าละเมิดทรัพย์สินทางปัญญาได้ โดยปราศจากหนังสือบอกกล่าวไปยังผู้ได้รับผลกระทบล่วงหน้า และการพิจารณาคดีตามกระบวนการทางยุติธรรม ทั้งที่ก่อนหน้านี้ศาลฎีกาสหรัฐอเมริกาเคยให้เหตุผลที่เกี่ยวกับการปิดกั้นการแสดงความคิดเห็นไว้ในหลายๆ คดีว่า “การปิดกั้นการแสดงความเห็นล่วงหน้า เป็นการละเมิดต่อสิทธิตามบทบัญญัติแก้ไขเพิ่มเติมครั้งที่หนึ่งของรัฐธรรมนูญสหรัฐอเมริกาอย่างร้ายแรง และไม่อาจให้มีการกระทำเช่นนี้ได้”[53] และ “มีเพียงกระบวนการพิจารณาทางยุติธรรมเท่านั้น

ที่เพียงพอ และสามารถยืนยันที่จะทำการปิดกั้นเสรีภาพในการแสดงความคิดเห็นอย่างสมเหตุสมผลและเป็นที่สุดได้"[54]

นอกจากนี้ ในด้านหนึ่ง แม้ SOPA จะมีบทบัญญัติป้องกันการฟ้องร้องผู้ให้บริการที่ปิดกั้นเว็บไซต์ไว้แล้ว ซึ่งย่อมส่งผลกระทบต่อฝ่ายผู้ให้บริการ แต่ในอีกด้านหนึ่ง SOPA ก็กลับสร้างความเสี่ยงให้กับผู้ให้บริการ ทำให้ต้องถูกดำเนินคดีได้ง่ายขึ้น ทั้งๆ ที่ปกติแล้ว "ตัวกลาง" เหล่านี้จะได้รับความคุ้มครองตามกฎหมายลิขสิทธิ์แห่งสหัสวรรษดิจิตอล (Digital Millennium Copyright Act[55]) โดยอาศัยบทบัญญัติที่คุ้มครองตามหลักการเรื่อง "safe harbor"[56]

3.5.2 กฎหมายป้องกันความเสี่ยงออนไลน์ต่อความสร้างสรรค์เชิงเศรษฐกิจและการโจรกรรมทรัพย์สินทางปัญญา (Preventing Real Online Threats to Economic Creativity and Theft to Intellectual Property Act of 2011 - Protect IP Act)

Protect IP Act เป็นร่างกฎหมายที่ถูกเสนอเข้าสู่วุฒิสภาสหรัฐเมื่อเดือนพฤษภาคม ปี 2011 ถือเป็นกฎหมายพี่น้องกันกับ SOPA ของสภาผู้แทนราษฎร โดยได้รับการสนับสนุนจากอุตสาหกรรมภาพยนตร์และเพลงของสหรัฐอเมริกา เช่น สภาหอการค้าสหรัฐอเมริกา (American Chamber of Commerce) สมาคมผู้สร้างภาพยนตร์แห่งสหรัฐอเมริกา (The Motion Picture Association of America) สหพันธ์นักดนตรีอเมริกัน (The American Federation of Musicians) ฯลฯ เป็นจำนวนเงินถึงกว่า 94 ล้านเหรียญสหรัฐ[57] สำหรับสถานะปัจจุบันของ Protect IP Act นั้น คงเป็นเช่นเดียวกับ SOPA ที่เกิดข้อถกเถียงอย่างมากเกี่ยวกับร่างกฎหมายจนทำให้กระบวนการพิจารณาร่างกฎหมายถูกชะลอออกไปโดยไม่มีกำหนด

เนื้อหาในร่างกฎหมาย มุ่งเน้นแก้ปัญหาเรื่องเขตอำนาจศาลสหรัฐอเมริกาและจัดการกับเว็บไซต์ทุจริต (rogue website) ที่ละเมิดทรัพย์สินทางปัญญา ซึ่งดำเนินกิจการในต่างประเทศ (non-domestic domain name)[58] โดยใช้วิธีจัดการผ่านตัวกลางซึ่งเป็นผู้ดูแลโดเมน

ด้วยการกำหนดให้บุคคลซึ่งเป็นตัวกลางซึ่งเป็นเจ้าของชื่อโดเมนที่จัดตั้งขึ้นในสหรัฐอเมริกา มีหน้าที่ต้องกระทำการอย่างหนึ่งอย่างใดเพื่อป้องกันการเข้าถึงเว็บไซต์เหล่านั้น หรือระงับการทำธุรกิจกับเว็บไซต์ที่ละเมิดทรัพย์สินทางปัญญาเหล่านั้น ทั้งนี้ Protect IP Act ให้อำนาจอัยการสูงสุด สามารถฟ้องร้องบุคคลดังต่อไปนี้ต่อศาลได้

1) เจ้าของชื่อโดเมนในประเทศ (domestic domain name) ที่ทำการที่เกี่ยวข้องกับกิจกรรมที่เป็นการละเมิดสิทธิและสามารถเข้าถึงได้ในสหรัฐอเมริกา

2) ผู้ให้บริการหรือเจ้าของเว็บไซต์ ที่กระทำการอันเกี่ยวข้องกับกิจกรรมอันเป็นการละเมิดสิทธิ์ซึ่งเข้าถึงผ่านชื่อโดเมนนอกประเทศสหรัฐอเมริกา

3) กรณีที่ไม่สามารถระบุตัวบุคคลใดบุคคลหนึ่งได้ สามารถดำเนินการอันเกี่ยวกับทรัพย์ (in rem) กับชื่อโดเมนนอกประเทศสหรัฐอเมริกาได้

โดยศาลอาจออกคำสั่งห้ามต่ออายุชื่อโดเมนที่ใช้ในสหรัฐอเมริกาและเว็บไซต์ที่ละเมิดสิทธิในทรัพย์สินทางปัญญาของสหรัฐอเมริกา เมื่อศาลมีคำสั่งแล้ว อัยการสูงสุดสามารถกระทำการอย่างใดอย่างหนึ่งโดยเฉพาะเจาะจง (specific actions) กับกลุ่มผู้ให้บริการดังต่อไปนี้ได้ โดยไม่ต้องขออนุญาตจากศาลอีก คือ

1) ผู้ให้บริการระบบโดเมนเซิร์ฟเวอร์ (operators of domain names system servers) อาจถูกสั่งให้ต้องสร้างมาตรการป้องกันการเข้าถึงโดเมนที่ถูกดำเนินการตามคำสั่งศาล นอกจากนี้หากเว็บไซต์ถูกถอนออกจากอินเทอร์เน็ตแล้ว ผู้ให้บริการระบบชื่อโดเมนเซิร์ฟเวอร์ดังกล่าว จะต้องแสดงข้อความชี้แจงว่าเว็บไซต์ดังกล่าวถูกถอนตามคำสั่งศาลที่ร้องขอโดยรัฐมนตรีกระทรวงยุติธรรม จึงอาจกล่าวได้ว่า บทบัญญัตินี้แท้ที่จริงแล้วก็คือ บทบัญญัติเพื่อการปิดกั้นชื่อโดเมนเซิร์ฟเวอร์ (DNS Blocking Provision) นั่นเอง

2) ผู้ให้บริการเกี่ยวกับการทำธุรกรรมทางการเงิน (financial transaction providers) ซึ่งหมายความถึงทุกๆ บริการที่ดำเนินการ

เกี่ยวกับธุรกรรมทางการเงิน ไม่ว่าจะเป็นธนาคาร ธุรกรรมกองทุน อิเล็กทรอนิกส์ และการชำระเงินประเภทต่างๆ ทางออนไลน์ มีหน้าที่ต้องปฏิบัติตามคำสั่งของศาลโดยใช้มาตรการที่สมเหตุสมผล และรวดเร็ว เพื่อป้องกัน ห้าม หรือยกเลิก การธุรกรรมการชำระเงินที่เกี่ยวข้องกับลูกค้าในสหรัฐอเมริกากับชื่อโดเมนที่กำหนดไว้ตามคำสั่งของศาล

3) ผู้ให้บริการโฆษณาทางอินเทอร์เน็ต (internet advertising services) เช่น ผลิตภัณฑ์การโฆษณาของบริษัทกูเกิลอย่าง Adwords, AdSense, AdBrite, AppNexus, Undertone Networks ฯลฯ ภายหลังศาลมีคำสั่งต่อชื่อโดเมนที่ถูกกล่าวหาละเมิดทรัพย์สินทางปัญญาแล้ว อัยการสูงสุดอาจสั่งให้ผู้ให้บริการที่ทำสัญญากับเว็บไซต์เหล่านั้นต้องมีมาตรการเพื่อ (ก) ป้องกันการให้บริการของตนจากการจัดโฆษณาในอินเทอร์เน็ตที่ข้องเกี่ยวกับชื่อโดเมนดังกล่าว หรือหยุดบริการโฆษณาในหน้าเว็บไซต์ที่ถูกกล่าวหา หรือ (ข) ยุติการให้บริการโฆษณาสำหรับเว็บไซต์นั้น หรือการให้การสนับสนุนผลการค้นหาหรือการเชื่อมโยง (ลิงก์)

4) ผู้ให้บริการเว็บไซต์ที่จัดหา “information location tools”[59] เช่น กูเกิล ยาฮู รวมถึงเว็บไซต์อย่างวิกิพีเดียและยูทูบ อาจถูกสั่งให้ต้อง (ก) เพิกถอนหรือทำให้เข้าถึงไม่ได้ซึ่งเว็บไซต์อันเกี่ยวข้องกับชื่อโดเมนที่กำหนดไว้ในคำสั่งศาล หรือ (ข) ไม่ให้บริการไฮเปอร์ลิงก์กับเว็บไซต์ดังกล่าว

และนอกจากอัยการสูงสุดแล้ว ผู้ทรงสิทธิในทรัพย์สินทางปัญญาก็สามารถฟ้องร้องบุคคลที่จดทะเบียนชื่อโดเมนที่ใช้ละเมิดทรัพย์สินทางปัญญาต่อศาลได้ ซึ่งถือเป็นสิทธิของเอกชนในการดำเนินการ (private right of action) และกรณีที่ศาลออกคำสั่งต่อชื่อโดเมนดังกล่าวแล้ว ผู้ทรงสิทธิสามารถนำคำสั่งนั้นไปให้ผู้ให้บริการธุรกรรมทางการเงิน และผู้ให้บริการโฆษณาทางอินเทอร์เน็ตปฏิบัติการอย่างใดอย่างหนึ่งโดยเฉพาะเจาะจงได้เช่นเดียวกับอัยการสูงสุด

ผลกระทบของกฎหมาย Protect IP Act ที่อาจมีต่อเสรีภาพในสื่อออนไลน์

การที่ร่างกฎหมายฉบับนี้กำหนดคำนิยามไว้อย่างกว้างขวางสำหรับเว็บไซต์ที่มี "กิจกรรมอันเป็นการละเมิด" จึงย่อมส่งผลเป็นการจำกัดเสรีภาพในการแสดงความคิดเห็น ซึ่งได้รับความคุ้มครองตามรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่หนึ่ง[60] Protect IP Act ยังให้อำนาจผู้ทรงสิทธิในทรัพย์สินทางปัญญามากเกินควร จนทำให้ผู้ทรงสิทธิในทรัพย์สินทางปัญญาซึ่งเป็นเอกชนมีอำนาจกว้างขวางที่จะจับผิด หรือร่วมปิดกั้นเว็บไซต์ได้ ทั้งกฎหมายฉบับนี้ยังพยายามเปลี่ยนแปลงธรรมชาติของอินเทอร์เน็ตให้มีลักษณะปิดมากกว่าเปิด[61] เช่น ผู้ให้บริการค้นหาข้อมูลอาจกลายเป็นผู้ละเมิดกฎหมายเพียงเพราะแสดงผลการค้นหาที่มีเว็บไซต์ที่ละเมิดลิขสิทธิ์รวมอยู่ด้วย[62] เป็นต้น อนึ่ง เป็นที่น่าสังเกตว่า แม้ Protect IP Act จะกำหนดให้มีการส่งหนังสือบอกกล่าวไปยังเจ้าของหรือผู้ให้บริการเว็บไซต์ที่ถูกกล่าวหาว่ากระทำละเมิดลิขสิทธิ์ แต่กฎหมายกลับไม่เปิดโอกาสให้ผู้ให้บริการเว็บไซต์เหล่านั้นได้โต้ตอบหรือคัดค้านก่อนที่จะถูกถอดออกจากอินเทอร์เน็ต ซึ่งแนวทางนี้อาจนำไปสู่การใช้อำนาจในทางมิชอบได้

กล่าวโดยสรุป โดยหลักการแล้ว หากเป็นการแสดงความคิดเห็นหรือวิพากษ์วิจารณ์นโยบายการบริหารราชการในสถานการณ์ปกติทั่วไป รัฐบาลสหรัฐอเมริกาไม่อาจกำหนดกฎเกณฑ์ใดๆ เพื่อปิดกั้นเว็บไซต์ที่แสดงความคิดเห็นที่แตกต่างจากรัฐบาลได้ เว้นแต่ข้อมูลเหล่านั้นมีเนื้อหาที่เกี่ยวกับสิ่งลามกอนาจารที่ต้องห้าม หรือมีลักษณะที่อาจก่อให้เกิดความรุนแรง ก็จะมีบทลงโทษทางอาญา และฟ้องร้องดำเนินคดีได้หากมีการเผยแพร่ข้อมูลดังกล่าว แต่ภายหลังจากมีภัยก่อการร้ายที่กระทบต่อความมั่นคงของรัฐ สภาคองเกรสได้ตรากฎหมายพิเศษ USA PATRIOT Act ขึ้นเพื่อให้อำนาจแก่เจ้าหน้าที่รัฐ รวมทั้งเอฟบีไอสามารถเข้าถึงข้อมูลออนไลน์ได้สะดวกรวดเร็ว แต่ก็ต้องได้รับความเห็นชอบจากกระทรวงยุติธรรมในการยื่นคำร้องต่อศาลก่อนเสมอ เช่นนี้จึงย่อมเห็นได้ว่า รัฐบาลสหรัฐอเมริกายึดมั่นในหลักการคุ้มครองเสรีภาพในการแสดง

ความคิดเห็นเสมอ แม้แต่ในกฎหมายที่เกี่ยวข้องกับความมั่นคง เช่น กฎหมายว่าด้วยความมั่นคงภายใน หรือ Domestic Security ที่กำหนดให้มีการจัดตั้ง Homeland Security Department ขึ้น และนิยามอำนาจหน้าที่ว่าเป็นการดำเนินการกับการก่อการร้ายที่ก่อภยันตรายอย่างร้ายแรงต่อประเทศขึ้นโดยบุคคลภายนอกหรือคนต่างชาติเท่านั้น[63] อย่างไรก็ตาม เป็นที่น่าตกใจว่า ประเทศเสรีประชาธิปไตยและยึดมั่นในระบบทุนนิยมอย่างสหรัฐอเมริกานั้น เสรีภาพในการรับรู้ข้อมูลข่าวสาร รวมทั้งเสรีภาพในการแสดงความคิด ก็อาจถูกฝ่ายรัฐและภาคอุตสาหกรรมพยายามจำกัดหรือบีบอัดให้เหลือน้อยลงได้ เพื่อประโยชน์ในการคุ้มครองทรัพย์สินทางปัญญา ซึ่งนับวันการคุ้มครองทรัพย์สินประเภทนี้จะขยายตัว และถูกตั้งคำถามมากขึ้นเรื่อยๆ ว่ายังสอดคล้องกับเจตนารมณ์แรกเริ่มของระบบกฎหมายที่ถูกสร้างขึ้นเพื่อคุ้มครองเจ้าของทรัพย์สินทางปัญญา ควบคู่ไปกับการให้ประโยชน์กับสาธารณชนอยู่อีกหรือไม่

4. ปฏิกิริยาและความเคลื่อนไหวฝ่ายประชาชน และสังคมที่มีต่อกฎหมายหรือนโยบายที่กระทบเสรีภาพในสื่อออนไลน์

4.1 ก่อนมีเหตุการณ์ก่อการร้าย 11 กันยายน

สังคมอเมริกันต่อต้านการตรวจสอบและปิดกั้นข้อมูลออนไลน์ในทุกรูปแบบโดยมีการฟ้องร้องคดีต่อศาลสูงสุด (U.S. Supreme Court) เพื่อให้พิพากษาว่ากฎหมายฉบับต่างๆ ที่มีบทบัญญัติละเมิดสิทธิและเสรีภาพของประชาชนในการเข้าถึงข้อมูล และแสดงออกซึ่งความคิดเห็นขัดต่อรัฐธรรมนูญ ตัวอย่างกฎหมายที่ถูกร้องให้ตรวจสอบความชอบด้วยรัฐธรรมนูญ ดังที่กล่าวถึงไปแล้ว ก็เช่น ซีดีเอ ซึ่งเป็นกฎหมายในระดับรัฐบาลกลาง และยังเป็นพื้นฐานให้มลรัฐอื่นๆ นำไปบัญญัติเป็นกฎหมายหมายระดับมลรัฐอีกหลายรัฐ ได้แก่ แคลิฟอร์เนีย อิลลินอยส์ แคนซัส เคนทักกี มิสซูรี นิวยอร์ก โอไฮโอ โรดไอแลนด์ เทนเนสซี และ เวอร์จีเนีย โดยองค์กรเอกชนเพื่อปกป้องสิทธิพลเมืองอเมริกันหรือ American Civil

Liberties Union (ACLU) ยื่นคำร้องต่อศาลสูงสุดอเมริกันให้พิพากษาว่า กฎหมายฉบับนี้ขัดต่อ The First Amendment ซึ่งในท้ายที่สุด ศาลสูงสุดสหรัฐพิพากษาว่า ซีดีเอในบางมาตราขัดต่อรัฐธรรมนูญจริง เนื่องจากมีถ้อยคำที่มีความหมายกว้างขวาง คลุมเครือ ไม่ชัดเจน[64]

4.2 ภายหลังเหตุการณ์ก่อการร้ายเมื่อวันที่ 11 กันยายน

รัฐบาลสหรัฐฯ พยายามผลักดันกฎหมายพิเศษและมาตรการอื่นๆ เพื่อแทรกแซงตรวจสอบข้อมูลของผู้ต้องสงสัยในทุกๆ รูปแบบ รวมถึงข้อมูลออนไลน์ การดำเนินการในลักษณะดังกล่าวส่งผลให้เกิดการวิพากษ์วิจารณ์และกระแสต่อต้านจากประชาชนชาวอเมริกันจำนวนไม่น้อยว่า ทั้งกฎหมายและการใช้อำนาจของเจ้าหน้าที่ของรัฐมีลักษณะฝ่าฝืนรัฐธรรมนูญที่ว่าด้วยการคุ้มครองเสรีภาพในการแสดงความคิดเห็นของประชาชน American Civil Liberties Union เอง ก็รณรงค์เพื่อต่อต้านการละเมิดสิทธิและเสรีภาพ รวมทั้งการบังคับใช้กฎหมายและการกระทำต่างๆ ที่ถูกผลักดันออกมาดังกล่าวอย่างต่อเนื่อง อย่างไรก็ตาม หลังเหตุการณ์ก่อการร้ายครั้งใหญ่ พบว่ามีประชาชนจำนวนไม่น้อยเช่นกันที่เริ่มสนับสนุนการออกฎหมายและการดำเนินนโยบายของรัฐบาลเพื่อต่อต้านการก่อการร้ายอย่างเข้มงวด ในที่นี้รวมทั้งกฎหมายที่ให้อำนาจเจ้าหน้าที่ตรวจสอบควบคุม และดักรับข้อมูลอิเล็กทรอนิกส์ต่างๆ ด้วย

4.3 ความเคลื่อนไหวต่อกฎหมายการป้องกันและปราบปรามการก่อการร้ายสหรัฐอเมริกา (USA PATRIOT Act)

USA PATRIOT Act เป็นกฎหมายที่ถูกตราขึ้นภายหลังเหตุการณ์ 11 กันยายน โดยรัฐบาลอ้างว่ามีเป้าหมายหลักเพื่อป้องกันการก่อการร้ายและเพื่อความปลอดภัยของประชาชน อย่างไรก็ตาม ด้วยเหตุที่กฎหมายดังกล่าวมีบทบัญญัติให้อำนาจรัฐอย่างกว้างขวางในการติดตามตรวจสอบการติดต่อสื่อสารทุกรูปแบบ และมีลักษณะของการละเมิดพื้นที่ส่วนบุคคลของประชาชนอย่างมาก จึงถูกต่อต้านจากประชาชนและองค์กรต่างๆ

จำนวนมาก ที่สำคัญ อาทิ

- สหภาพเสรีภาพพลเมืองอเมริกัน (American Civil Liberties Union - ACLU) โต้ตอบกฎหมายฉบับนี้ โดยการฟ้องร้องรัฐบาลสหรัฐอเมริกา เกี่ยวกับการดักฟังโทรศัพท์ของผู้อื่นและการมีคำสั่งศาลอย่างลับ ๆ เพื่อเรียกข้อมูลจากบริษัทผู้ให้บริการอินเทอร์เน็ต โดยสหภาพเสรีภาพฯ เห็นว่า การที่กฎหมายบัญญัติห้ามไม่ให้บริษัทอินเทอร์เน็ต หรือบริษัทอื่น ๆ ที่โดนหมายศาลเปิดเผยถึงการกระทำการต่าง ๆ ของรัฐ ทั้งไม่ได้กำหนดช่องทางใด ๆ ให้แก่ผู้ให้บริการหรือบริษัทเหล่านั้นที่จะสามารถคัดค้านหมายเรียกของศาลได้ ถือเป็นเรื่องที่ไม่ยุติธรรมอย่างยิ่ง

- ศูนย์ข้อมูลอิเล็กทรอนิกส์ส่วนบุคคล (Electronics Privacy Information Center - EPIC) ร่วมต่อต้านกฎหมายฉบับนี้เช่นกัน ด้วยการส่งคำร้องไปยังกระทรวงยุติธรรมสหรัฐอเมริกาให้เปิดเผยข้อมูลที่ได้มาจาก PATRIOT Act โดยอ้างสิทธิในข้อมูลข่าวสารของประชาชน อย่างไรก็ตาม กระทรวงยุติธรรมปฏิเสธการให้ข้อมูลตามคำร้องโดยอ้างว่าข้อมูลที่ร้องขอเข้าข้อยกเว้นที่รัฐไม่จำเป็นต้องเปิดเผยแก่สาธารณะชน เป็นผลให้ EPIC ฟ้องกระทรวงยุติธรรมต่อศาล ซึ่งในท้ายที่สุด ศาลมีคำสั่งให้รัฐบาลต้องเปิดเผยข้อมูลทั้งหมด นอกจากนี้ EPIC ยังร่วมกับองค์กรอื่น ๆ สร้างเว็บไซต์ขึ้นโดยเฉพาะ เพื่อรณรงค์ต่อต้านกฎหมายนี้ ในนาม “safe and free” อีกด้วย

- ศูนย์เพื่อประชาธิปไตยและเทคโนโลยี (Center for Democracy and Technology - CDT) เป็นอีกองค์กรหนึ่งที่แสดงความไม่เห็นด้วยและต่อต้านกฎหมายการป้องกันและปราบปรามการก่อการร้ายสหรัฐอเมริกา โดยเห็นว่าการละเมิดเสรีภาพออนไลน์ไม่สามารถซื้อความมั่นคงปลอดภัยได้ และมีเพียงการสื่อสารที่เสรีเท่านั้นที่จะเป็นแรงผลักดันทางบวกให้เกิดการต่อสู้กับการทำละเมิดในทุกรูปแบบ CDT ได้รณรงค์เรื่องอเมริกันที่ปลอดภัยและเสรี (American Safe and Free) และประกาศข้อกังวลต่อกฎหมายฉบับนี้หลายข้อ ไม่ว่าจะเป็น กรณีที่กฎหมายกำหนดให้อำนาจรัฐใช้เครื่องมือดักจับข้อมูลทางอินเทอร์เน็ตได้ทำให้รัฐบาลสามารถเก็บข้อมูลที่มิอาจบ่งชี้ได้จากการท่องเว็บไซต์ของประชาชนทุกคน หรืออันตรายที่เกิดจากการสืบค้น

อีเมลของประชาชน โดยปราศจากการกลั่นกรองตรวจสอบโดยกระบวนการยุติธรรม นอกจากนี้ ยังให้อำนาจรัฐสกัดกั้นการติดต่อสื่อสาร และอนุญาตให้ผู้ให้บริการอินเทอร์เน็ต และผู้จัดการเครือข่าย (network administrators) ตรวจตราสอดส่องผู้ใช้บริการได้เสมอโดยไม่ต้องมีคำสั่งศาล

- โครงการกฎหมายเพื่อมนุษยธรรม (The Humanitarian Law Project) ไม่เห็นด้วยกับกฎหมายนี้และฟ้องร้องต่อศาลสหรัฐอเมริกาว่า กฎหมายฉบับนี้ขัดกับรัฐธรรมนูญสหรัฐอเมริกา โดยเฉพาะอย่างยิ่งมาตรา 805 ที่อนุญาตให้รัฐบาลห้ามประชาชนไม่ให้จัดหาข้อมูลแก่องค์กรก่อการร้ายที่ถูกตั้งขึ้นมาโดยเฉพาะ (specially designated terrorist organization)[65] รวมถึงการเป็นที่ปรึกษาหรือเป็นผู้ช่วยองค์กรเหล่านั้น ซึ่งศาลสหรัฐอเมริกาเห็นด้วยตามที่ฟ้องและสั่งให้มาตรา 805 (a) (2) (B) เป็นโมฆะ เนื่องจากขัดกับบทบัญญัติแก้ไขเพิ่มเติมครั้งที่หนึ่งและห้าของรัฐธรรมนูญสหรัฐอเมริกา (First and Fifth Amendment) โครงการกฎหมายเพื่อมนุษยธรรมยังเห็นว่า PATRIOT Act ใช้ถ้อยคำที่คลุมเครือ เปิดช่องให้เจ้าหน้าที่รัฐสามารถกล่าวหาบุคคลใดๆ ว่า กระทำการละเมิดต่อกฎหมาย และดำเนินคดีในข้อหาที่บุคคลเหล่านั้นไม่สามารถทราบได้เลยว่า เป็นการกระทำที่เป็นความผิดความคลุมเครือยังก่อให้เกิดการเลือกปฏิบัติ (discrimination) หรือการปฏิบัติตามอำเภอใจ (arbitrary) ในการบังคับใช้กฎหมายดังกล่าวอีกด้วย

- มูลนิธิอิเล็กทรอนิกส์ฟรอนเทียร์ (Electronics Frontier Foundation - EFF) เห็นว่า มาตรา 215 ภายใต้กฎหมายฉบับนี้ ให้อำนาจอย่างกว้างขวางกับรัฐ ทั้งยังเห็นว่าแม้ขณะก็นี้ก็ยังไม่มีหลักฐานใดที่แสดงได้ชัดเจนว่าเสรีภาพทางออนไลน์จะเป็นกำแพงปิดกั้นความมีประสิทธิภาพของการติดตามและจับผู้ก่อการร้าย โดยรัฐได้อย่างไร[66] EFF ยังแสดงความกังวลว่า การตรวจตราและสอดส่อง โดยการดูบันทึกการใช้อินเทอร์เน็ตและสอดส่องข้อมูลเกี่ยวกับบุคคลที่เกี่ยวข้องกับการประท้วงที่ถูกต้องตามกฎหมาย ถือเป็นการปฏิบัติที่ต่ำกว่ามาตรฐานตามรัฐธรรมนูญซึ่งกำหนดว่า การสอดส่องข้อมูลของประชาชนโดยทั่วไปจะต้องผ่านกระบวนการ

สอบสวนโดยศาลเสียก่อน ทั้งเรื่องนี้ยังขัดกับหลักกฎหมายฉบับเก่าในปี 1970 ที่ห้ามรัฐไม่ให้สอดส่องประชาชนอเมริกันอย่างแพร่หลาย[67] และปัญหาที่สำคัญ ก็คือกฎหมายนี้มิได้จำกัดอยู่เพียงการก่อการร้ายเท่านั้น หากแต่หมายรวมถึงการกระทำความผิดอาญาที่ร้ายแรงด้วย เช่น รัฐสามารถดักรับหรือจารกรรมข้อมูลของแฮกเกอร์หรือบุคคลที่น่าสงสัยได้โดยไม่ต้องมีคำสั่งศาล และกฎหมายนี้ยังอนุญาตให้ใช้เครื่องดักฟังสำหรับการกระทำผิดใดๆ ที่อาจเข้าข่ายการละเมิดผ่านคอมพิวเตอร์ ซึ่งย่อมส่งผลให้เกิดการใช้อำนาจหน้าที่โดยมิชอบและเปิดโอกาสให้รัฐบาลสามารถจารกรรมข้อมูลของประชาชนได้

4.4 ปฏิกิริยาต่อร่างกฎหมายหยุดยั้งการละเมิดลิขสิทธิ์ออนไลน์ Stop Online Piracy Act (SOPA) และ กฎหมายป้องกันความเสี่ยงออนไลน์ต่อความสร้างสรรค์เชิงเศรษฐกิจและการโจรกรรมทรัพย์สินทางปัญญา (Protect IP Act - PIPA)

ในขณะที่รัฐบาลสหรัฐร่วมกับบริษัทอุตสาหกรรมขนาดใหญ่ โดยเฉพาะอุตสาหกรรมเพลงและภาพยนตร์ พยายามหามาตรการป้องกันการละเมิดลิขสิทธิ์ ด้วยการผลักดันร่างกฎหมายสองฉบับ คือ SOPA และ PIPAซึ่งมีบทบัญญัติเปิดช่องให้เกิดการแทรกแซงและจำกัดการเข้าถึงอินเทอร์เน็ตของประชาชนได้ ก็เกิดปฏิกิริยาต่อต้านร่างกฎหมายทั้งสองฉบับนี้เกิดขึ้นจำนวนมาก เช่น มีประชาชนจำนวนกว่า 50,000 ชื่อร่วมลงนามคัดค้านร่างกฎหมาย

- องค์กรฮิวแมนไรท์วอทช์ (Human Rights Watch - HRW) ร่วมกับองค์กรเกี่ยวกับเสรีภาพและสิทธิมนุษยชนอื่นๆ ส่งจดหมายเปิดผนึกไปยังรัฐสภา ระบุว่า หลายประเทศที่มีระบบการปกครองที่เข้มงวด ใช้วิธีการดังที่ปรากฏในร่างกฎหมายทั้งสองเพื่อปิดปากประชาชน หากสภาอเมริกันยอมให้กฎหมายทั้งสองฉบับนี้ออกมาใช้บังคับได้ จะทำให้ประเทศอื่นถือเป็นตัวอย่างและทำตามโดยออกกฎหมายที่มีเนื้อหาใกล้เคียงกัน ซึ่งจะทำให้เสรีภาพในการแสดงความคิดเห็นถดถอย ซึ่ง HRW เห็นว่าจะ

ดีกว่าหากมีแนวทางนโยบายที่สนับสนุนเสรีภาพออนไลน์ และหลีกเลี่ยงร่างกฎหมายที่บั่นทอนและยับยั้งประโยชน์ของอินเทอร์เน็ตที่เปิดโอกาสให้เกิดการโต้เถียงสนทนา และแลกเปลี่ยนข้อมูล[68]

- วิกิพีเดีย สารานุกรมออนไลน์ที่เปิดให้บริการทั่วโลก เป็นผู้ริเริ่มกิจกรรมจอมืด (blackout) หรือการทำหน้าจอเว็บไซต์ให้ดำเป็นเวลา 12 ชั่วโมงในวันที่ 18 มกราคม 2012 เพื่อต่อต้านและกดดันไม่ให้สภาผ่านกฎหมายทั้งสองฉบับนี้ ทั้งนี้ วิกิพีเดียเห็นว่า ร่างกฎหมายทั้งสองฉบับจะส่งผลกระทบอย่างยิ่งต่อวิถีการใช้อินเทอร์เน็ตของผู้คนทั่วโลก ไม่ว่าจะเป็นการอ่านบล็อก การหาข้อมูลลูกค้าในการทำธุรกิจ หรือการค้นหาข้อมูลในกูเกิล วิกิพีเดีย หรือการสื่อสารกับเพื่อนในเครือข่ายสังคมออนไลน์ทั้งนี้ ไม่ว่าเว็บไซต์เหล่านั้นจะอยู่ในสหรัฐอเมริกาหรือไม่ โดยเฉพาะอย่างยิ่งเว็บไซต์ต่างประเทศจะถูกกระทบจากร่างกฎหมายฉบับดังกล่าว ซึ่งบั่นทอนเสรีภาพในการพูด และอาจส่งผลกระทบต่อการสร้างนโยบายที่คล้ายกันในประเทศอื่นทั่วโลกอีกด้วย[69] นอกจากการทำหน้าจอดำแล้ว วิกิพีเดียยังสนับสนุนให้ประชาชนของสหรัฐอเมริกาบอกกล่าวให้สมาชิกวุฒิสภาทราบถึงการคัดค้านร่างกฎหมายสองฉบับนี้ และสนับสนุนให้ประชากรในโลกบอกกล่าวไปยังหน่วยงานรัฐของประเทศตน เพื่อยับยั้งการเกิดขึ้นของกฎหมายในลักษณะที่ใกล้เคียงกัน ปฏิบัติการจอมืดมีองค์กรและเว็บไซต์จำนวนมากเข้าร่วม อาทิ โกลบอลวอยซ์ (Global Voice) ซึ่งเป็นองค์กรส่งเสริมเสรีภาพออนไลน์, ไอเฟ็กซ์ (International Freedom of Expression Exchange Network - IFEX), ศูนย์เพื่อประชาธิปไตยและเทคโนโลยี (Center for Democracy and Technology – CDT), เอพีซี (Association for Progressive Communications - APC), เรดดิด (Reddit) ฯลฯ นอกจากนี้ยังมีการเผยแพร่ข้อมูลเชิงวิพากษ์เกี่ยวกับร่างกฎหมายดังกล่าวถึงกว่า 75,000 ข้อความสำหรับผู้อ่านกว่า 20 ภาษาทั่วโลกด้วย

- โกลบอลวอยซ์เห็นว่า ร่างกฎหมายสองฉบับนี้บังคับให้เว็บไซต์ที่ให้บริการเนื้อหาที่ผู้ใช้เป็นผู้สร้าง (user-generated content) ต้องทำหน้าที่ตรวจตราผู้ใช้บริการเพื่อป้องกันไม่ให้มีการเผยแพร่ข้อความ

หรือรูปภาพที่อาจจะละเมิดทรัพย์สินทางปัญญาได้ ซึ่งถือเป็นการเพิ่มภาระแก่ธุรกิจอินเทอร์เน็ตอย่างมาก นอกจากนี้ ยังเปิดช่องให้จำกัดเสรีภาพในการแสดงความเห็น และกลายเป็นการนำเหตุผลเรื่องปกป้องทรัพย์สินทางปัญญาไปใช้ในทางที่ผิด เพราะมาตรการตามร่างกฎหมายทั้งสองนำไปสู่การปิดกั้นการแสดงความคิดเห็นโดยพฤตินัย (de facto) หากร่างกฎหมายฉบับนี้ผ่าน ย่อมเป็นการส่งข้อความต่อโลกว่า รัฐบาลสหรัฐอเมริกาเชื่อว่าการสอดส่องตรวจตราประชาชนเป็นสิ่งที่ยอมรับได้

- สหภาพเสรีภาพพลเมืองอเมริกัน (American Civil Rights Union) เห็นว่า แม้ร่างกฎหมายทั้งสองฉบับมีจุดประสงค์ที่จะจัดการการละเมิดสิทธิในทรัพย์สินทางปัญญา แต่ในความเป็นจริงกฎหมายสองฉบับนี้อาจส่งผลกระทบกับเนื้อหาหรือเว็บไซต์ที่อาจไม่ได้เกี่ยวกับการละเมิดเลยด้วย อีกทั้งยังไม่มีข้อกำหนดให้ส่งหนังสือบอกแจ้งแก่เจ้าของเนื้อหา หรือผู้ผลิตเนื้อหาที่ถูกกฎหมายแต่อย่างใด ด้วยเหตุนี้จึงจำเป็นต้องประท้วงร่างกฎหมายทั้งสองฉบับ ซึ่งสหภาพเห็นสมควรให้หยุดการลงคะแนนเสียงต่อร่างกฎหมายทั้งสองฉบับไว้ก่อน

- มูลนิธิอิเล็กทรอนิกส์ฟรอนเทียร์ (Electronics Frontier Foundation - EFF) กังวลว่า ร่างกฎหมายนี้เขียนไว้อย่างคลุมเครือ กำหนดหน้าที่ให้เว็บไซต์ต้องทำตัวเป็นตำรวจ คอยตรวจตราเว็บไซต์ของตน (self police) ซึ่งเป็นการสร้างภาระทางการเงินให้แก่เว็บไซต์ต่างๆ อย่างมาก EFF ยังห่วงด้วยว่า หากร่างกฎหมายนี้ถูกบังคับใช้ อาจทำให้เครื่องมือที่ใช้หลีกเลี่ยงการปิดกั้นกลายเป็นสิ่งผิดกฎหมายไปด้วย ดังเช่นที่เป็นอยู่ในสาธารณรัฐประชาชนจีนและอิหร่าน ทั้งร่างกฎหมายนี้ ยังเปิดช่องให้รัฐบาลดำเนินการกับเว็บไซต์ที่เพียงแค่ช่วยจัดหาข้อมูลให้ผู้ใช้บริการเข้าถึงได้ด้วย ซึ่งนอกจากจะเป็นการปิดกั้นล่วงหน้า อันถือได้ว่าขัดหรือแย้ง หรือไม่เป็นไปตามทำนองคลองธรรมแห่งรัฐธรรมนูญสหรัฐอเมริกาแล้ว ยังทำลายนวัตกรรมทางออนไลน์อีกด้วย

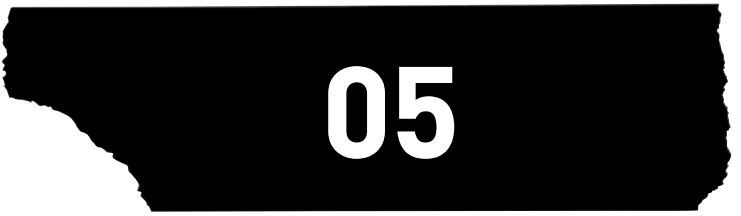
5. บทสรุป

อาจกล่าวโดยทั่วไปได้ว่า ระดับของความคุ้มครองเสรีภาพในการแสดงความคิดเห็นตามรัฐธรรมนูญอเมริกาอยู่ในระดับสูงกว่าหลายๆ ประเทศในโลกเสรี เพราะแม้กระทั่งถ้อยคำไม่พึงประสงค์ หรือสร้างความเกลียดชัง (hate speech) หากไม่ถึงกับก่อให้เกิดความโกรธแค้นและนำไปสู่การต่อสู้ทำร้ายกัน (fighting words)[70] ก็ยังสามารถกล่าวหรือแสดงความคิดเห็นได้ ในขณะที่ประเทศอื่น อย่างประเทศเยอรมนี และประเทศฝรั่งเศส ยังมีกฎหมายห้ามมิให้เผยแพร่ข้อมูลบางประเภท โดยเฉพาะอย่างยิ่ง การดูถูกเหยียดหยามเชื้อชาติ ศาสนา ชาตินิยม หรือโฆษณาชวนเชื่อเกี่ยวกับลัทธิการเมือง[71] ในสหรัฐอเมริกานั้น เฉพาะแต่การแสดงความคิดเห็นบางกรณีเท่านั้นที่ไม่ได้รับความคุ้มครองตามรัฐธรรมนูญ หรืออาจถูกรัฐจำกัดหรือควบคุมได้ เช่น การเผยแพร่สิ่งลามกอนาจาร (obscenity) การแสดงข้อความเพื่อหลอกลวงบุคคลอื่น (fraudulent misrepresentation) การใส่ความให้ร้าย (defamation) การสนับสนุนหรือยุยงให้มีการกระทำผิดกฎหมายอย่างร้ายแรง (advocacy of imminent lawless) หรือถ้อยคำยั่วยุให้มีการต่อสู้หรือทำร้ายกัน (fighting words)[72] เป็นต้น โดยเหตุผลของการจำกัดการแสดงความคิดเห็นในประเทศสหรัฐอเมริกาส่วนหนึ่งเป็นเช่นเดียวกับประเทศอื่นๆ ในยุโรป คือ ต้องการปกป้องคุ้มครองเด็กและเยาวชนจากการถูกล่วงละเมิดทางเพศ หรือจากการได้รับข้อมูลที่มีเนื้อหาที่อาจส่งผลกระทบต่อพัฒนาการในเรื่องต่างๆ ก่อนวัยอันควร นอกเหนือจากนี้ ก็คือ เพื่อป้องกันเหตุร้ายแรง หรือความเสียหายต่างๆ ที่จะมีมาแก่ระบบสังคม และเศรษฐกิจโดยรวม ทั้งนี้ หากรัฐประสงค์กำหนดระเบียบหรือกฎเกณฑ์เพื่อควบคุมเนื้อหาของการแสดงความคิดเห็นโดยตรง (content-base on its face examination) รัฐมีภาระต้องพิสูจน์ว่า มาตรการดังกล่าวนั้นจำเป็นต้องมีเพื่อรักษาผลประโยชน์อันจำเป็นอย่างยิ่งยวดของรัฐ (compelling government objective) แบบไม่อาจจะหลีกเลี่ยงได้ ทั้งเป็นวิธีการที่รุนแรงน้อยที่สุด และแคบที่สุด (narrowly as possible to achieve

that objective) ในขณะที่การควบคุมวิธีการแสดงความคิดเห็น เช่น เวลาหรือสถานที่ที่ไม่กระทบต่อเนื้อหาสาระโดยตรง (content-neutral) รัฐต้องพิสูจน์ว่า กฎเกณฑ์ดังกล่าวมีวัตถุประสงค์เพื่อคุ้มครองประโยชน์อันสำคัญของรัฐ (significant governmental interest) ที่รุนแรงน้อยที่สุด (narrowly tailored to serve that governmental interest) ทั้งไม่ตัดช่องทางเลือกในการแสดงความคิดเห็นของประชาชน (ศาลพิจารณาตามหลัก Rationale standard[73]) รวมทั้งกฎเกณฑ์การจัดระเบียบดังกล่าวไม่ขัดต่อรัฐธรรมนูญ

อย่างไรก็ตาม สถานการณ์เกี่ยวกับเสรีภาพการแสดงความคิดเห็น การเข้าถึงข้อมูลข่าวสาร และสิทธิความเป็นส่วนตัวในการติดต่อสื่อสารระหว่างกันในประเทศสหรัฐอเมริกาเริ่มถูกจำกัดหรือถูกรัฐตรวจสอบควบคุมเพิ่มขึ้นเรื่อยๆ ภายหลังเหตุการณ์ 11 กันยายน ด้วยเหตุผลสำคัญคือเพื่อป้องกันและต่อต้านการก่อการร้าย ทั้งในรูปแบบของการตรากฎหมายพิเศษและการใช้มาตรการในทางปฏิบัติอื่นๆ แต่แม้การจำกัดสิทธิและเสรีภาพดังกล่าวจะก่อให้เกิดความอึดอัดขัดข้องในการใช้เสรีภาพกับประชาชนจำนวนหนึ่ง แต่ขณะเดียวกันก็ทำให้ประชาชนอีกจำนวนหนึ่งเกิดความรู้สึกปลอดภัย ดังนั้น การประท้วงคัดค้านรัฐในเรื่องนี้จากกลุ่มประชาชนจึงไม่เป็นเอกภาพนัก ทว่า ข้อสังเกตสำคัญในกรณีของประเทศสหรัฐอเมริกาคือ ไม่ว่าการต่อสู้เพื่อเรียกร้องเสรีภาพการแสดงความคิดเห็นจะเกิดขึ้นกับกฎหมายฉบับใดหรือยุคสมัยใด กลไกการตรวจสอบความชอบด้วยรัฐธรรมนูญโดยยื่นคำร้องต่อศาลสูงสุดก็ยังเป็นวิธีการที่ภาคประชาชนเชื่อมั่นและดำเนินการควบคู่กับการประท้วงและรณรงค์ทางอื่นๆ อยู่เสมอ ทำให้การเรียกร้องมีพลังและมีเป้าหมายที่ชัดเจน ซึ่งไม่ค่อยพบในการเรียกร้องสิทธิของประชาชนในประเทศไทย รวมทั้งประเทศอื่นๆ ในแถบตะวันออก

บทที่



กฎหมายจีน
กับสิทธิเสรีภาพในสื่อออนไลน์

กฎหมายจีน กับสิทธิเสรีภาพในสื่อออนไลน์

ปี 2010 ประเทศจีนถูกจัดให้อยู่ในกลุ่มประเทศที่ไม่มีเสรีภาพ โดยจีนอยู่ในลำดับที่ 168 จาก 178 ประเทศ มีสื่อมวลชนถูกฆาตกรรมหนึ่งราย และถูกจำคุก 30 ราย แต่หากเริ่มนับตั้งแต่ปี 1999 มีนักเขียนในสื่อออนไลน์ถูกจำคุกรวม 76 ราย[1] การแสดงความคิดเห็นในทุกรูปแบบ ตั้งแต่การแจกจ่ายใบปลิว[2] ไปจนถึงการเผยแพร่ข้อมูลบนสื่อออนไลน์จะถูกตรวจสอบควบคุมและปิดกั้นอย่างเข้มงวด โดยเฉพาะอย่างยิ่งในประเด็นที่เกี่ยวข้องกับการเมือง เศรษฐกิจ สังคม และศาสนา ทั้งนี้ ในสายตาของรัฐบาลจีน การเรียกร้องให้ปฏิรูปการปกครองให้เป็นระบอบประชาธิปไตยถือเป็นการทำลายความมั่นคงของชาติและมีโทษร้ายแรง[3]

รัฐบาลจีนเห็นว่าข้อมูลข่าวสารเป็นเครื่องมือสร้างความชอบธรรมให้แก่รัฐบาลจีน ส่วนสื่อออนไลน์ก็มีไว้เพื่อสร้างความบันเทิงเท่านั้น ประชาชนจึงไม่ควรใช้เพื่อวิพากษ์วิจารณ์การทำงานของรัฐบาลหรือพรรคคอมมิวนิสต์ การแสดงความคิดเห็นใดๆ ต้องมีลักษณะของการแสดงความจงรักภักดีต่อรัฐบาลจีน และสิ่งนี้ก็ถือเป็นมาตรฐานทางวิชาชีพที่สำคัญสูงสุดของสื่อมวลชนในประเทศจีน[4] จึงเห็นได้ว่า ในระยะกว่าทศวรรษที่

ผ่านมา รัฐบาลจีนใช้เครื่องมือและมาตรการต่างๆ รวมถึงองค์กรตุลาการ เพื่อจำกัดเสรีภาพ ปิดกั้นสื่อกระแสหลัก ภาพยนตร์ต่างประเทศ รวมถึงสื่อทางเลือกอย่างเฟซบุคและทวิตเตอร์ กระทั่งเครื่องมือสืบค้นข้อมูลและเว็บไซต์ในอินเทอร์เน็ต (search engine) ด้วยการอ้างเหตุผลว่าเป็นไปเพื่อการรักษาความปลอดภัยของสังคม

การวิจัยในส่วนนี้ คณะผู้วิจัยจึงค้นหาหลักกฎหมายที่เกี่ยวข้องกับการติดต่อสื่อสารในสื่อออนไลน์ และชี้ให้เห็นปัญหา รวมทั้งลักษณะการจำกัดเสรีภาพการแสดงความคิดเห็นของประชาชนจีน โดยเฉพาะอย่างยิ่งแนวนโยบายแห่งรัฐ และความเคลื่อนไหวของภาคประชาชนต่อนโยบายดังกล่าว เพื่อนำมาเปรียบเทียบกับกรณีที่เกิดขึ้นในประเทศไทย ดังปรากฏในรายละเอียดต่อไปนี้

1. หลักการคุ้มครองเสรีภาพในการรับรู้ข้อมูลข่าวสารและแสดงความคิดเห็น

ประเทศจีนคุ้มครองเสรีภาพการแสดงความคิดเห็นของประชาชน โดยกำหนดไว้ในมาตรา 35 ของรัฐธรรมนูญแห่งสาธารณรัฐประชาชนจีน ค.ศ. 1982 โดยมีสาระสำคัญว่า ประชาชนแห่งสาธารณรัฐประชาชนจีน มีเสรีภาพในการแสดงความเห็น เสรีภาพในการตีพิมพ์งานวิชาการ เสรีภาพในการรวมตัวกันเป็นสมาคม เดินขบวน และการชุมนุม[5] ทั้งนี้ องค์กรของรัฐในทุกระดับจะต้องดำเนินมาตรการเพื่อให้การแสดงความเห็นเป็นไปโดยชอบด้วยกฎหมาย และไม่ละเมิดสิทธิของผู้อื่น ตลอดจนจะต้องไม่เป็นอันตรายต่อประโยชน์ของแผ่นดิน สังคม หรือส่วนรวม[6] อีกทั้งการใช้เสรีภาพเช่นว่านั้น จะต้องเคารพต่อกิจการของรัฐ (national affairs) และคำนึงถึงปัจจัยที่เกี่ยวข้องกับเศรษฐกิจ วัฒนธรรม และสังคมด้วย

สำหรับการเสนอผลงานวิจัยทางวิทยาศาสตร์ งานวรรณกรรม และวัฒนธรรม หากชอบด้วยกฎหมาย ตามนัยยะที่พรรคคอมมิวนิสต์กำหนดไว้ย่อมได้รับการปกป้องและไม่อาจจะถูกแทรกแซงได้ ทั้งไม่อาจทำให้ล่าช้า

หรือการขัดขวางการเสนอความคิดเห็นดังกล่าว[7]

จะเห็นได้ว่า แม้รัฐธรรมนูญจีนจะกำหนดหลักการที่ว่าด้วยเสรีภาพในการแสดงความคิดเห็นของประชาชนเอาไว้แล้วก็ตาม แต่ในความเป็นจริง ลักษณะของบทบัญญัติก็กำหนดกรอบของเสรีภาพไว้ค่อนข้างกว้างขวางและย่อมส่งผลต่อการคุ้มครองเสรีภาพ ซึ่งในท้ายที่สุดแล้วก็ปรากฏว่า การแสดงความคิดเห็นใดๆ จะได้รับความคุ้มครองตามรัฐธรรมนูญก็ต่อเมื่อสอดคล้องกับนโยบายของพรรคคอมมิวนิสต์ หากรัฐเห็นว่าการแสดงความคิดเห็นใดจะกระทบต่อผลประโยชน์ของชาติ รวมถึงวัฒนธรรม และขนบธรรมเนียมประเพณีของจีน (ที่พรรคคอมมิวนิสต์ได้กำหนดไว้) ก็จะถูกดำเนินคดีอย่างจริงจัง

นอกจากนี้ ประเทศจีนยังมีกฎหมายลำดับรองอีกจำนวนมากที่กำหนดขั้นตอนรายละเอียดการแสดงความคิดเห็นเอาไว้ อาทิ การกำหนดระบบใบอนุญาตสำหรับการให้บริการเชื่อมต่ออินเทอร์เน็ตกับต่างประเทศ ขั้นตอนการก่อตั้งสำนักพิมพ์หรือสำนักข่าว ขั้นตอนการเผยแพร่ข้อมูลซึ่งจะต้องผ่านการตรวจสอบเนื้อหาโดยรัฐเสียก่อน[8] หลักเกณฑ์สำหรับบริษัทที่ประกอบธุรกิจโทรคมนาคมที่ต้องถูกควบคุมโดยให้รัฐถือหุ้นในกิจการนั้นไม่น้อยกว่าร้อยละ 51 ฯลฯ และกระบวนการในลักษณะนี้ก็มีผลทำให้รัฐบาลจีนสามารถปิดกั้นการเชื่อมต่ออินเทอร์เน็ตจากทั่วโลกได้อย่างง่ายดาย[9] จึงทำให้เสรีภาพในการแสดงความคิดเห็นไม่เกิดขึ้นจริง

2. เนื้อหาต้องห้ามมิให้เผยแพร่ในสื่อสาธารณะตามกฎหมายจีน

2.1 เนื้อหาต้องห้ามตามกฎหมายว่าด้วยความลับ และความปลอดภัยของประเทศ

ตามกฎหมายอาญาว่าด้วยความมั่นคงแห่งชาติและความลับของรัฐ (National Security and State Secrets) และอรรถาธิบายประเด็นที่เกี่ยวข้องกับกฎหมายเฉพาะด้านที่ใช้ในการพิจารณาคดีว่าด้วยการขโมยหรือจารกรรมเพื่อการได้มาซึ่ง หรือการไขความลับ หรือการข่าวของรัฐโดย

ผิดกฎหมายแก่ชาวต่างชาติ (Explanation of Certain Issues Regarding the Specific Laws to be Used in Adjudicating Cases of Stealing or Spying to Obtain, or Illegally Supplying, State Secrets or Intelligence for Foreigners 2000) กำหนดห้ามเผยแพร่ข้อมูลข่าวสารเกี่ยวข้องกับความปลอดภัย และผลประโยชน์ของชาติ หากฝ่าฝืนมีความผิดฐานโจรกรรมข้อมูลอันเป็นความลับของชาติ ซึ่งเป็นความผิดตามประมวลกฎหมายอาญา มาตรา 111[10]

2.2 เนื้อหาที่ถือเป็นความผิดตามประมวลกฎหมายอาญา

ข้อมูลหรือข้อความใดที่ถูกเผยแพร่ต่อสาธารณะ หากรัฐบาลจีนพิจารณาแล้วเห็นว่าเป็นข้อความเท็จหรือเข้าข่ายเป็นความผิดทางอาญาฐานอื่นๆ ทั้งยังเกี่ยวข้องกับความปลอดภัยและผลประโยชน์ของชาติแล้ว จะถือเป็นความผิดตามประมวลกฎหมายอาญา ค.ศ. 1997 สำหรับผู้เผยแพร่ ไขข่าว หรือเปิดเผยความลับดังกล่าว ดังนี้

มาตรา 105 (2): การเผยแพร่ ไขข่าวลือ หรือการหมิ่นประมาทหรือวิธีการอื่น ที่เป็นการกระตุ้นให้เกิดการต่อต้านล้มล้างรัฐบาลระบอบสังคมนิยม ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือกักขัง อบรม หรือถูกตัดสิทธิในทางการเมืองได้ สำหรับผู้กระทำผิดที่เป็นผู้นำในการกระทำผิดหรือผู้ซึ่งได้กระทำผิดร้ายแรงยิ่งกว่า จะต้องถูกลงโทษจำคุกตั้งแต่ 5 ปีขึ้นไป

มาตรา 246: การใช้วิธีการรุนแรงหรือวิธีการอื่นๆ เพื่อทำให้เกิดความเสียหายหรืออับอายต่อบุคคลที่สาม หรือสร้างความเท็จเพื่อหมิ่นประมาทบุคคลที่สาม ในกรณีที่เกิดความเสียหายอย่างร้ายแรง ต้องระวางโทษจำคุกไม่เกิน 3 ปี โทษกักขังทางอาญา ต้องเข้ารับการศึกษา หรือถูกควบคุมดูแล รวมทั้งถูกตัดสิทธิทางการเมือง สำหรับความผิดทางอาญาข้างต้นจะถูกฟ้องร้องด้วย หากการฟ้องคดีมีความเหมาะสม และในกรณีที่ความสงบเรียบร้อยของสังคม และผลประโยชน์ของชาติถูกกระทบอย่างรุนแรง

มาตรา 283: การจัดทำหรือขายข้อมูลที่เป็นความลับที่ได้มา

จากการดักฟังโทรศัพท์โดยผิดกฎหมาย หรือได้มาจากการบันทึกภาพโดยกล้องขนาดเล็ก (micro-cameras) หรืออุปกรณ์อื่นใด รวมทั้งการได้มาโดยวิธีการอื่นซึ่งเป็นการโจรกรรม ต้องระวางโทษจำคุกไม่เกิน 3 ปี กักขัง หรือการต้องเข้ารับการศึกษาอบรม

2.3 เนื้อหาที่ถือว่าเป็นความผิดตามกฎหมายว่าด้วยความมั่นคงของรัฐ

ตามกฎหมายว่าด้วยความมั่นคงของรัฐ ค.ศ. 1993 (State Security Law 1993) มีข้อกำหนดอย่างกว้างขวางและคลุมเครือโดยห้ามมิให้องค์กรหรือปัจเจกชนก่อให้เกิดภยันตรายต่อความมั่นคงของประเทศจีน (มาตรา 4) เช่น การสมคบกันเพื่อล้มล้างรัฐบาลหรือแบ่งแยกรัฐ หรือการล้มล้างรัฐบาลสังคมนิยม การร่วมกับองค์กรจารกรรมข้อมูล หรือการยอมรับการกระทำขององค์กรจารกรรมข้อมูลหรือตัวแทนองค์กรดังกล่าว การขโมยข้อมูล หรือการสืบแสวงหาข้อมูลลับ หรือการซื้อข้อมูล หรือการให้ข้อมูลซึ่งเป็นความลับของรัฐ การกระตุ้น ยุยง หรือว่าจ้างเจ้าหน้าที่ของรัฐให้กระทำทรยศต่อชาติ และกระทำการใดๆ ซึ่งก่อให้เกิดความวุ่นวายอันเป็นอันตรายต่อความมั่นคงของรัฐ[11] ทั้งนี้ รัฐบาลจีนมักตีความให้ข้อมูลลับมีความเกี่ยวข้องกับการเผยแพร่ข่าวสารเสมอ โดยได้กำหนดระเบียบว่าด้วยการคุ้มครองความลับในการตีพิมพ์ข่าว (Regulations on the Protection of Secrets in News Publishing 1992) เพื่อปกป้องข้อมูลลับ โดยห้ามผู้ใดให้ข้อมูลข่าวสารลับแก่สำนักข่าวใดๆ เพื่อตีพิมพ์ หากข้อมูลที่จะเผยแพร่นั้นมีความไม่แน่ชัดว่าเกี่ยวข้องกับความลับของชาติหรือไม่ บุคคลดังกล่าวจะต้องขออนุมัติต่อองค์กรเพื่อตรวจสอบและให้ความเห็นชอบก่อน (มาตรา 14) โดยเฉพาะอย่างยิ่ง หากข่าวสารนั้นมีสาระซึ่งเกี่ยวข้องกับรัฐบาลจีน ระบบเศรษฐกิจ การทูต เทคโนโลยี หรือการทหาร (มาตรา 15) เป็นต้น

2.4 การห้ามการเผยแพร่ข้อมูลเกี่ยวกับกองทัพ และความมั่นคงอื่น ๆ ของประเทศ

กฎหมายว่าด้วยการคุ้มครองความลับของรัฐ ค.ศ. 1988 (Law on the Protection of State Secrets 1988) มาตรา 2 และมาตรา 8 กำหนดมิให้มีการเผยแพร่ข้อมูลอันเป็นความลับและผลประโยชน์ของประเทศ เช่น ข้อมูลสำคัญที่ใช้ในการตัดสินใจดำเนินการของรัฐ การป้องกันชาติและความแข็งแกร่งของกองทัพ กิจกรรมทางการทูตและการต่างประเทศ และหน้าที่อันเป็นความลับภายใต้การพิจารณาของประเทศ ประเด็นเกี่ยวกับเทคโนโลยีทางวิทยาศาสตร์ และการสืบสวนสอบสวนในคดีอาญา เป็นต้น นอกจากนี้ ยังมีการกำหนดมาตรการในการควบคุมการเผยแพร่ข้อมูลข่าวสารโดยกำหนดให้ข้อมูลเหล่านั้นเป็นข้อมูลความลับของชาติตามมาตรการดำเนินงานภายใต้กฎหมายการคุ้มครองความลับของรัฐ (Measures for the Implementation of the Law on the Protection of State Secrets 1990) และห้ามเผยแพร่ข้อมูลใดๆ ที่หากเปิดแล้วอาจเป็นอันตรายต่อความสามารถของรัฐบาลในการรักษาเสถียรภาพของรัฐและการป้องกันประเทศ หรือเป็นอันตรายต่อการเมืองและเศรษฐกิจของชาติ ทำให้ประสิทธิภาพหรือความเชื่อถือของมาตรการในการรักษาความปลอดภัยของรัฐลดลง หรือทำให้องค์กรของรัฐบาลสูญเสียซึ่งความสามารถในการใช้อำนาจตามกฎหมาย เป็นต้น

ในปี 1998 รัฐบาลจีนตรากฎหมายฉบับหนึ่ง กำหนดให้การตีพิมพ์เผยแพร่สิ่งใดๆ ที่อาจจะมีผลกระทบต่อความมั่นคงของชาติโดยไม่ได้รับอนุญาต ถือเป็นสิ่งที่ผิดกฎหมาย แม้ว่าเนื้อหาดังกล่าวจะไม่มีลักษณะที่ผิดกฎหมายเลยก็ตาม ซึ่งเป็นไปตามอรรถาธิบายประเด็นที่เกี่ยวข้องกับกฎหมายเฉพาะด้านที่ใช้ในการพิจารณาคดีอาญาการตีพิมพ์อันมิชอบด้วยกฎหมาย (Explanation Regarding Certain Questions About the Specific Laws to be used in Adjudicating Criminal Cases of Illegal Publication 1998) แม้เนื้อหานั้นอาจไม่ผิดกฎหมาย นอกจากนี้ การจำหน่ายข้อมูลใดๆ ที่อาจทำให้เกิดความเสียหายต่อความสงบเรียบร้อย หรือระบบ

เศรษฐกิจ หากมีความเสียหายอย่างร้ายแรงจะถูกลงโทษตามที่ได้กำหนดไว้ในประมวลกฎหมายอาญา มาตรา 225 และการกระทำผิดดังกล่าวบนสื่อออนไลน์อาจถูกลงโทษตาม “มาตรการชั่วคราวเกี่ยวกับการบริหารงานของวารสาร” ที่มีผลบังคับใช้ทางปกครองแล้ว (Administrative Sanction Implementation Measures for the Interim Measures on the Administration of Periodicals 1989) ซึ่งกำหนดโทษปรับไว้ ตั้งแต่ 0.5 – 1 เท่าของรายได้ที่ถือว่าผิดกฎหมาย รวมถึงการเพิกถอนการประกอบธุรกิจนั้นเป็นต้น

3. กฎหมายลำดับรอง และข้อกำหนดของรัฐเพื่อควบคุมการใช้เสรีภาพในการแสดงความคิดเห็น

3.1 ระบบการขอใบอนุญาตจากรัฐ

รัฐบาลจีนควบคุมการแสดงความคิดเห็นของประชาชนอย่างใกล้ชิดผ่านองค์กรของรัฐหลายองค์กร เช่น องค์กรบริหารจัดการสื่อและสิ่งพิมพ์ (General Administration of Press and Publication - GAPP) ซึ่งเป็นหน่วยงานพิจารณาให้ใบอนุญาตการประกอบกิจการพิมพ์ หรือองค์กรบริหารจัดการสื่อ วิทยุ ภาพยนตร์ และโทรทัศน์ แห่งรัฐ (The State Administration of Radio, Film, and Television) ที่มีหน้าที่พิจารณาใบอนุญาตประกอบกิจการวิทยุ ภาพยนตร์ และโทรทัศน์ โดยอยู่ภายใต้การบังคับบัญชาของกระทรวงอุตสาหกรรมข้อมูลข่าวสาร (Ministry for Information Industry)[12]

ผู้ประกอบกิจการสื่อทุกประเภทต้องได้รับใบอนุญาตให้ประกอบการจากรัฐบาลจีนภายใต้เงื่อนไขที่ยุ่งยากซับซ้อนอย่างมาก[13] ซึ่งปัจจุบันประเทศจีนมีผู้ประกอบการด้านอินเทอร์เน็ตรายใหญ่สี่ราย[14] ได้แก่ CSTNet, ChinaNet, CERNet และ CHINAGBN ไปจนถึงบริษัทผู้ให้บริการรายย่อยๆ อีกกว่า 3,000 บริษัททั่วประเทศ โดยใช้วิธีการให้บริษัทรายใหญ่ทำหน้าที่คอยควบคุมบริษัทเอกชนที่ให้บริการทางอินเทอร์เน็ต

รายย่อยที่ได้รับสัมปทานจากรัฐอีกทีหนึ่ง[15] รัฐบาลจีนสามารถจำกัดการเข้าถึง หรือปิดกั้นช่องทางการเข้าถึงเว็บไซต์ได้ทันทีตั้งแต่ระดับผู้ให้บริการการเข้าถึงอินเทอร์เน็ต

นอกจากต้องได้รับใบอนุญาตจากรัฐบาลจีนแล้ว ผู้ประกอบกิจการจะต้องปฏิบัติตามกฎหมายลำดับรองที่ควบคุมสื่อออนไลน์ฉบับต่างๆ อีกด้วย สำหรับบริษัทเอกชนของต่างประเทศที่เข้ามาประกอบธุรกิจให้บริการอินเทอร์เน็ตในประเทศจีน มีเงื่อนไขที่จะต้องขอรับใบอนุญาตจากทางการจีนเช่นกัน โดยเงื่อนไขดังกล่าวใช้บังคับทั้งกับกรณีการขอประกอบกิจการและทั้งการเผยแพร่ข่าวสาร หรือจัดทำกระดานสนทนาอิเล็กทรอนิกส์เพื่อแลกเปลี่ยนความคิดเห็นด้วย เงื่อนไขและกฎหมายฉบับต่างๆ ที่เกี่ยวข้องกับการเผยแพร่ข้อมูลในสื่อออนไลน์ ดังปรากฏต่อไปนี้

3.1.1 การเผยแพร่ข้อมูลบนสื่อออนไลน์

การเผยแพร่ข้อมูลใดๆ บนสื่อในประเทศจีนนั้น ผู้ประสงค์จะเผยแพร่ต้องได้รับอนุญาตตามบทบัญญัติว่าด้วยการจัดการสิ่งพิมพ์อิเล็กทรอนิกส์ ค.ศ. 1997 (Provisions on the Administration of Electronic Publications 1997) ก่อน มิเช่นนั้นอาจมีโทษทั้งทางอาญาและทางแพ่งได้[16] ส่วนวิธีการเผยแพร่ข้อมูลบนหนังสือพิมพ์อิเล็กทรอนิกส์ต้องได้รับอนุญาตตามข้อกำหนดเกี่ยวกับการตีพิมพ์เผยแพร่ ในข้อมาตรการที่ว่าด้วยการบันทึกสาระสำคัญของหนังสือ วารสาร สื่อเสียงและภาพ และสื่ออิเล็คทรอนิคส์ (Notice Regarding the Printing and Promulgation of the “Measures on the Recording of Important Topics of Books, Periodicals, Audio/Visual Productions and Electronic Publications” 1997) โดยเฉพาะอย่างยิ่ง หากสิ่งที่จะเผยแพร่นั้นเป็น “หัวข้อสำคัญ” ที่เกี่ยวข้องกับความมั่นคงของรัฐและสังคม นอกจากนี้หัวข้อที่เกี่ยวข้องกับรัฐบาล เศรษฐกิจ วัฒนธรรม และการทหาร ซึ่งรวมถึงวรรณกรรมที่เกี่ยวข้องกับพรรคคอมมิวนิสต์และประเทศชาติ อดีตและผู้นำในปัจจุบันของพรรคและชาติ และอัตชีวประวัติของบุคคลดังกล่าว ความลับของพรรคและชาติ

ความมั่นคงชาติหรือศาสนา ฯลฯ ตามที่ GAPP กำหนดไว้ ก็จะต้องได้รับความเห็นชอบจาก GAPP ก่อน และในกรณีที่รัฐเห็นว่าการเผยแพร่ใดไม่ถูกต้อง รัฐสามารถสั่งให้แก้ไขได้ตามข้อกำหนดในข้อกำหนดเกี่ยวกับการควบคุมการทำงานของอุตสาหกรรมวารสารให้อยู่ภายใต้การกำกับของรัฐ (Notice Regarding the Work of Bringing the Periodical Industry Under Control 1997) ไม่ว่าจะเป็นข้อมูลการเมืองที่ผิดพลาด[17] ชีวประวัติ หรือเอกสารบันทึกเชิงบรรยาย หรือพรรณนาถึงผู้นำพรรคคอมมิวนิสต์ที่คลาดเคลื่อนไป เป็นต้น

สำหรับผู้ประสงค์เผยแพร่งานเขียนบนสื่อออนไลน์ต้องได้รับอนุญาตจากรัฐตามข้อบัญญัติเฉพาะกาลเกี่ยวกับการบริหารงานสิ่งพิมพ์ออนไลน์ (Interim Provisions on the Administration of Internet Publishing 2002) มาตรา 6 เมื่อได้รับอนุมัติแล้ว ห้ามมิให้บุคคลใดๆ เข้าแทรกแซงหรือยับยั้ง ทำให้ล่าช้า หรือขัดขวางการตีพิมพ์บทความนั้นบนอินเทอร์เน็ต แต่เนื้อหาที่เผยแพร่ดังกล่าวจะต้องสอดคล้องกับ มาตรา 17 ด้วย กล่าวคือต้องไม่มีเนื้อหาที่เป็นอันตรายต่อเกียรติภูมิและประโยชน์ของรัฐ และห้ามมิให้มีการเผยแพร่ข่าวลือ กระทำการใดที่ก่อให้เกิดความไม่สงบ หรือสร้างความปั่นป่วนต่อเสถียรภาพของสังคม

3.1.2 การจัดทำกระดานข่าว หรือกระดานสนทนาอิเล็กทรอนิกส์

ตามข้อบัญญัติการบริหารงานการจัดทำกระดานข่าวหรือกระดานสนทนาอิเล็กทรอนิกส์ (Provisions on the Administration of Internet Electronic Bulletin Board Service 2000) มาตรา 5 ผู้ให้บริการข้อมูลทางอินเทอร์เน็ต (Operators of Internet Information Services) ซึ่งให้บริการกระดานแสดงความคิดเห็นทางอิเล็กทรอนิกส์นั้น ต้องยื่นขออนุญาตต่อหน่วยงานของรัฐในระดับต่างๆ หรือองค์กรบริหารกิจการโทรคมนาคมของเทศบาลที่เป็นอิสระ (Independent Municipality Telecommunications Administration Agency) หรือรัฐมนตรีกระทรวงอุตสาหกรรม

ข้อมูลข่าวสาร (Ministry of Information Industry) เพื่อขอใบอนุญาตประกอบการอินเทอร์เน็ตเพื่อการค้า (Commercial Internet Information Service License) สำหรับการขออนุญาตให้บริการทางอินเทอร์เน็ตที่ไม่ใช่การค้า ผู้ประกอบการก็ต้องแจ้งข้อมูลในขณะยื่นขอใบอนุญาตว่าจะจัดให้มีกระดานแสดงความคิดเห็นทางอิเล็กทรอนิกส์ด้วยหรือไม่

ทั้งนี้ ผู้ให้บริการจะต้องดำเนินการต่างๆ และเผยแพร่ข้อมูลที่มีเนื้อหาเป็นไปตามประเภทของเนื้อหา (category) ที่ตนแจ้งไว้ และได้รับอนุญาตแล้วเท่านั้น (มาตรา 11) หากผู้ประกอบการพบหรือได้รับแจ้งว่ามีข้อความแสดงความคิดเห็นที่ผิดกฎหมาย ก็ต้องดำเนินการลบข้อความดังกล่าวออกจากพื้นที่การให้บริการของตนทันที แต่ต้องเก็บข้อมูลดังกล่าวไว้เพื่อให้เจ้าหน้าที่ตรวจสอบ รวมถึงรายงานการกระทำดังกล่าวต่อหน่วยงานที่มีอำนาจหน้าที่รับผิดชอบด้วย (มาตรา 13)

3.1.3 การถ่ายทอดรายการวิทยุโทรทัศน์ผ่านดาวเทียมของต่างประเทศ

การถ่ายทอดรายการทางสถานีวิทยุโทรทัศน์ผ่านดาวเทียมของต่างประเทศในประเทศจีนนั้น สามารถทำได้ตามเงื่อนไขที่ปรากฏในมาตรการการบริหารการถ่ายทอดรายการวิทยุโทรทัศน์ผ่านดาวเทียมของต่างประเทศ (Measures on the Administration of Foreign Satellite Television Channel Reception 2004) ซึ่งผู้ประกอบการ หรือผู้ต้องการถ่ายทอดดังกล่าวต้องได้รับอนุญาตจากรัฐ และถ่ายทอดได้ในโรงแรมระดับสามดาวขึ้นไปเพื่อให้ลูกค้าชาวต่างประเทศในสถานที่ทำงาน หรือในอาคารให้เช่าเพื่อพักอาศัย หรือสถานที่อื่นๆ ที่จัดเตรียมไว้เพื่อการนี้เป็นการเฉพาะเท่านั้น[18] โดยสื่อดังกล่าวจะต้องมีทัศนคติที่ดีต่อประเทศจีน[19] ส่วนการขออนุญาตนั้น หากเป็นตัวแทนของรายการวิทยุของต่างประเทศที่ตั้งขึ้นในประเทศจีนจะได้รับอนุญาตให้ถ่ายทอดเฉพาะขอบเขตจำกัดเท่านั้น ในขณะที่รายการสถานีข่าวต่างประเทศไม่มีสิทธิได้รับอนุญาตเพื่อถ่ายทอดภายในประเทศจีนโดยเด็ดขาด[20]

สำหรับรายการวิทยุออนไลน์นั้น ตกอยู่ภายใต้มาตรการการบริหารการเผยแพร่เสียง/ภาพ ผ่านเครือข่ายอินเทอร์เน็ตหรือเครือข่ายข้อมูลอื่น (Measures on the Administration of Broadcasting Audio/Visual Program over the Internet or Other Information Network 2003) ซึ่งผู้ประกอบการต้องได้รับอนุญาตจากองค์กรบริหารจัดการวิทยุ ภาพยนตร์ และโทรทัศน์ แห่งรัฐ (State Administration of Radio, Film, and Television) ทั้งนี้ ผู้ขออนุญาตจะต้องประกอบกิจการในลักษณะเดียวกันในต่างประเทศมาแล้วอย่างน้อยสามปี (มาตรา 8) อีกทั้งจะต้องได้รับการรับรองจากหน่วยงานของรัฐบาลจีนด้วย (มาตรา 10)

3.2 กำหนดห้ามมิให้องค์กรเอกชนนำเสนอข่าวสารบางประเภท

มาตรา 5 ข้อบัญญัติชั่วคราวในการบริหารงานกลุ่มเว็บไซต์บนอินเทอร์เน็ตที่เกี่ยวข้องกับกิจการข่าว (Interim Provisions on the Administration of Internet Websites Engaged in News Posting Operations 2000) กำหนดให้องค์กรของรัฐเท่านั้นที่สามารถเสนอข่าวสารของรัฐบาลได้ เช่น หน่วยข่าวกลาง (central news units) จังหวัด ภูมิภาค หรือเทศบาลที่เป็นอิสระ สำหรับองค์กรอื่นๆ ไม่อาจจัดตั้งเป็นองค์กรข่าวได้ แต่สามารถสร้างเว็บเพจ และเสนอข่าวสารของหน่วยข่าวข้างต้นได้

สำหรับเว็บไซต์ซึ่งไม่มีวัตถุประสงค์ในการเสนอข่าว หากต่อมาประสงค์จะเสนอข่าวสารด้วย ต้องยื่นขออนุมัติและได้รับความเห็นชอบจากหน่วยงานด้านข่าวสารของรัฐบาล (The People's Government Information Office) ของจังหวัด หรือภูมิภาค หรือหน่วยงานบริหารเทศบาลที่เป็นอิสระเสียก่อน โดยหน่วยงานของรัฐดังกล่าวต้องรับรองก่อนที่จะเสนอไปยังคณะกรรมการกำกับดูแลข้อมูลข่าวสารแห่งรัฐ (State Council Information Agency) เพื่อเห็นชอบ (มาตรา 8)

3.3 ข้อกำหนดที่เกี่ยวกับการให้บริการอินเทอร์เน็ต

3.3.1 การควบคุมการจัดเก็บข้อมูลของผู้ให้บริการอินเทอร์เน็ต (อินเทอร์เน็ตคาเฟ่)

ตามมาตรการควบคุมการบริหารงานธุรกิจที่ให้บริการในการเข้าถึงอินเทอร์เน็ต (อินเทอร์เน็ตคาเฟ่) (Regulation on the Administration of Internet Access Service Business Establishments - Internet Cafes 2002) มาตรา 23 กำหนดให้ผู้ให้บริการอินเทอร์เน็ต ต้องตรวจสอบ จัดให้มีการลงทะเบียน และจัดเก็บข้อมูลเกี่ยวกับลูกค้าซึ่งมาใช้บริการในสถานบริการของตนเอง โดยจะต้องจัดเก็บข้อมูลต่าง ๆ ที่ลูกค้าใช้บริการ และข้อมูลของตัวผู้ใช้บริการไว้อย่างน้อย 60 วัน เพื่อให้หน่วยงานด้านวัฒนธรรมและความปลอดภัย (Cultural and Public Security Agency) ตรวจสอบว่ามีการกระทำใดที่ไม่ชอบด้วยกฎหมายหรือไม่

3.3.2 การควบคุมผู้ให้บริการข่าวสารทางอินเทอร์เน็ตเพื่อการค้า

ตามมาตรา 4 ของ มาตรการการบริหารการให้บริการข่าวสารทางอินเทอร์เน็ต (Measures for the Administration of Internet Information Services 2000) กำหนดให้ผู้ประสงค์จะให้บริการข่าวสารทางอินเทอร์เน็ต ซึ่งกระทำเพื่อการค้า (commercial internet information services) ต้องขอรับใบอนุญาต (licensing system) จากรัฐเท่านั้น ส่วนผู้บริหารข้อมูลทางอินเทอร์เน็ตที่ไม่ใช่ทางการค้า ต้องจดแจ้งเกี่ยวกับเว็บไซต์และลงทะเบียน (registration system) ต่อหน่วยงานของรัฐ หากไม่ปฏิบัติตามข้อกำหนดดังกล่าวจะไม่สามารถประกอบการเว็บไซต์ได้

นอกจากนี้ ในมาตรา 14 ยังกำหนดให้ผู้ให้บริการที่อยู่ในฐานะผู้เขียน (journalism) หรือตีพิมพ์เผยแพร่ข้อมูล และการให้บริการกระดานแสดงความคิดเห็น จะต้องจัดทำบันทึกข้อมูลการสื่อสารทั้งหมดไว้ด้วย เวลาที่เข้า-ออกอินเทอร์เน็ต ที่อยู่ทางอินเทอร์เน็ต ชื่อเมือง และบัญชีลูกค้าที่ใช้

บริการ รวมถึงเบอร์โทรศัพท์ ฯลฯ อีกทั้งผู้ให้บริการข้อมูลและผู้ให้บริการเชื่อมต่อทางอินเทอร์เน็ต (providers of internet information service and internet access providers) จะต้องเก็บรักษาข้อมูลไว้อย่างน้อย 60 วัน เพื่อให้เจ้าหน้าที่ผู้บังคับใช้กฎหมายที่เกี่ยวข้องตรวจสอบตามกฎหมายต่อไป

3.4 การใช้กฎหมายที่เกี่ยวกับการกระทำความผิดในระบบคอมพิวเตอร์

นอกจากระบบการขอใบอนุญาตจากรัฐ และการบังคับใช้กฎหมายที่ว่าด้วยการควบคุมสื่อประเภทดั้งเดิมแล้ว ในช่วงที่ผ่านมารัฐบาลจีนยังตรากฎหมายเฉพาะเพื่อปกป้องความลับสำหรับการติดต่อสื่อสารในระบบเครือข่ายคอมพิวเตอร์ด้วย ฉบับที่สำคัญก็คือ ข้อบัญญัติเกี่ยวกับการบริหารจัดการการปกป้องความลับข้อมูลในคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายนอกประเทศ (Provisions on the Administration of the Protection of Secrets on Internationally Networked Computer Information Systems 2000) โดยมีบทบัญญัติในลักษณะควบคุมการเผยแพร่ข้อมูลข่าวสารบนโลกออนไลน์โดยเฉพาะ ดังนี้

มาตรา 3: เอกชน นิติบุคคล หรือองค์กรใดๆ ผู้ซึ่งมีความประสงค์ที่จะเชื่อมต่อเครือข่ายระบบคอมพิวเตอร์ระหว่างประเทศในฐานะผู้ใช้ หรือในฐานะผู้ให้บริการอินเทอร์เน็ต หรือเพื่อการเชื่อมต่อระบบจะต้องปฏิบัติตามกฎหมายที่เกี่ยวข้อง

มาตรา 8: การควบคุมเพื่อการปกป้องข้อมูลความลับบนระบบออนไลน์ จะต้องยึดถือหลักการที่ว่า “ใครก็ตามที่เข้าสู่ระบบออนไลน์จะต้องเป็นผู้มีความรับผิดชอบ” ผู้ประสงค์ที่จะเป็นผู้ให้บริการ หรือเป็นผู้เผยแพร่ข้อมูลบนระบบเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อระหว่างประเทศจะต้องดำเนินการผ่านระบบการตรวจสอบ และปกป้องข้อมูลความลับ และได้รับความเห็นชอบจากหน่วยงานที่เกี่ยวข้องเสียก่อน ทั้งนี้ หน่วยงานซึ่งเป็นผู้ให้บริการในการตรวจสอบและให้ความเห็นชอบเกี่ยวกับการให้บริการ ต้องกำหนดมาตรการในการตรวจสอบและเห็นชอบของระบบ

ดังกล่าว ซึ่งต้องสอดคล้องกับกฎเกณฑ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูล และหน่วยงานซึ่งให้บริการข้อมูลต้องปฏิบัติตามกฎเกณฑ์ที่กำหนดขึ้น

มาตรา 9: บุคคลใดก็ตามซึ่งเป็นผู้รวบรวมข้อมูล โดยมีวัตถุประสงค์ในการให้บริการข้อมูลออนไลน์ ต้องขอความเห็นชอบจากหน่วยงานเสียก่อน เว้นแต่ข้อมูลนั้นเคยถูกเปิดเผยมาก่อนแล้วในสื่ออื่น บุคคลใดที่นำข้อมูลไปขยายความ หรือทำให้ข้อมูลออนไลน์เป็นปัจจุบัน ต้องดำเนินการตามมาตรการว่าด้วยการปกป้องความลับ และการตรวจสอบความถูกต้องของข้อมูลออนไลน์นั้นด้วย

มาตรา 10: หน่วยงานใดๆ หรือผู้ใช้บริการข้อมูลออนไลน์ซึ่งติดตั้งระบบกระดานข่าว ห้องสนทนา หรือระบบเครือข่ายข้อมูลของกลุ่มบุคคลใดๆ ต้องถูกตรวจสอบก่อน และได้รับการเห็นชอบจากองค์กรที่มีหน้าที่ปกป้องข้อมูลที่เป็นความลับ ซึ่งต้องถูกกำหนดให้มีหน้าที่ปกป้องความลับ และหน้าที่อื่นๆ ทั้งนี้ ห้ามมิให้องค์กรหรือปัจเจกชนกระจายข้อมูล บทสนทนา หรือส่งผ่านข้อมูลซึ่งเป็นความลับของชาติในระบบกระดานสนทนา ห้องสนทนา หรือเครือข่ายของกลุ่มบุคคล สำหรับบุคคลที่สร้างกระดานสนทนา ห้องสนทนาหรือระบบเครือข่ายข้อมูลของกลุ่ม และเปิดให้สาธารณะ หรือหน่วยงานระดับสูงขึ้นของบุคคลนั้นสามารถเข้าถึงได้ จะต้องใช้ความระมัดระวังอย่างยิ่งยวดในการรักษาความลับ ทำระบบตรวจสอบ และเฝ้าระมัดระวังตลอดเวลาอย่างจริงจัง สำหรับการเปิดข้อมูลใดๆ ซึ่งเกี่ยวข้องกับความลับ หรือมาตรการใดๆ บุคคลผู้มีความรับผิดชอบในระบบเครือข่ายข้างต้น หรือผู้ดูแลห้องสนทนา หรือ กระดานข่าวจะต้องกระทำในเวลาที่เหมาะสม และรายงานต่อพนักงานเจ้าหน้าที่ท้องถิ่นทันที

มาตรา 11: ผู้ใช้บริการอินเทอร์เน็ตในการติดต่อสื่อสาร หรือเพื่อการแลกเปลี่ยนข้อมูลข่าวสาร จะต้องปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับการปกป้องความลับของชาติ และจะต้องไม่แสวงหาประโยชน์จากการสื่อสารผ่านระบบออนไลน์เพื่อส่งผ่านข้อมูล หรือส่งต่อข้อมูลซึ่งเป็น

ความลับของชาติ องค์กรที่ให้บริการทางอินเทอร์เน็ต หรือการเข้าถึงอินเทอร์เน็ตต้องมีคำอธิบายอย่างชัดแจ้งเพื่อให้ผู้ใช้บริการทราบถึงข้อกำหนดเกี่ยวกับการปกป้องคุ้มครองความลับ และต้องมีระบบบริหารการติดต่อสื่อสารผ่านจดหมายอิเล็กทรอนิกส์ที่ตนให้บริการนั้นด้วย

มาตรา 12: ผู้ให้บริการอินเทอร์เน็ต และการเข้าถึงอินเทอร์เน็ตต้องจัดให้มีการเรียนรู้เกี่ยวกับการปกป้องความลับ ซึ่งเกี่ยวข้องกับการจัดระบบการเชื่อมต่อทางอินเทอร์เน็ตระหว่างประเทศ สำหรับสัญญาที่แสดงถึงการให้บริการระหว่างผู้ให้บริการกับผู้ใช้บริการ มีหน้าที่ต้องกำหนดเงื่อนไขการเคารพกฎหมายการคุ้มครองข้อมูลอันเป็นความลับและการเปิดเผยข้อมูลซึ่งเป็นความลับของประเทศว่าเป็นสิ่งที่ต้องห้าม

จะเห็นได้ว่ากฎหมายของประเทศจีนฉบับต่างๆ ดังกล่าวมาข้างต้น มีลักษณะของการบัญญัติที่กว้างขวาง และคลุมเครือ (overbroad and vague) ประชาชนอ่านแล้วอาจไม่สามารถเข้าใจได้ในทันทีว่าเนื้อหาแบบใดที่ต้องห้ามไม่ให้เผยแพร่ ไม่ว่าจะเป็นคำว่า “ประโยชน์ของชาติ” “การเผยแพร่ข่าวลือ” หรือการหมิ่นประมาทอันมีผลทำให้เป็นการล้มล้างระบอบการปกครองก็ไม่มีคำนิยาม

ตารางต่อไป แสดงให้เห็นบทบัญญัติของกฎหมายฉบับต่างๆ ที่เกี่ยวกับการควบคุมเนื้อหาในสื่อออนไลน์ (และสื่อดั้งเดิมประเภทอื่น)[21]

4. นโยบาย และแนวทางปฏิบัติที่เกี่ยวกับการควบคุมสื่อออนไลน์

รัฐบาลจีนตระหนักถึงอิทธิพลของสื่อออนไลน์เป็นอย่างยิ่ง นับแต่เริ่มเปิดประเทศในปี 1994 เป็นต้นมาจนถึงปัจจุบันมีประชาชนชาวจีนเข้าถึงอินเทอร์เน็ตได้ถึงเกือบ 400 ล้านคน[22] ดังนั้น นอกจากตัวบทกฎหมายในระดับต่างๆ แล้ว รัฐบาลจึงพยายามควบคุมการเผยแพร่ข้อมูลข่าวสารและการแสดงความคิดเห็นบนสื่อประเภทนี้อย่างเข้มข้น[23] โดยมีกลไก และนโยบายควบคุมต่างๆ ดังนี้

กฎหมาย	ผู้เสนอ	บทบัญญัติที่เกี่ยวข้อง
ข้อบัญญัติเฉพาะกาลเกี่ยวกับการบริหารงานสิ่งพิมพ์ออนไลน์ ปี 2545	MII GAPP	มาตรา17 : ข้อมูลที่เผยแพร่บนอินเทอร์เน็ตจะต้องไม่มีเนื้อหา ดังนี้... 3) สิ่งที่เป็นอันตรายต่อเกียรติภูมิ และประโยชน์ของรัฐ 6) การเผยแพร่ข่าวลือ หรือกระทำการใดๆ ที่ก่อให้เกิดความไม่สงบ และสร้างความปั่นป่วนต่อเสถียรภาพของสังคม
มาตรการเพื่อการบริหารใบอนุญาตการประกอบกิจการโทรคมนาคม ปี 2544	MII	Appendix 2 (III) (iv): ผู้ปฏิบัติ (Operators) หรือ ลูกจ้างต้องไม่ใช้เครือข่ายโทรคมนาคมในการผลิต ทำซ้ำ หรือ ก่อให้เกิด หรือ ส่งผ่านข้อมูลใดๆ ที่มีเนื้อหา ดังนี้.. 3) อันตรายต่อเกียรติภูมิ และ ประโยชน์ของรัฐ 6) การเผยแพร่ข่าวลือ กระทำการใดที่ก่อให้เกิดความไม่สงบ และสร้างความปั่นป่วนต่อเสถียรภาพของสังคม
ระเบียบการบริหารงานสื่อสิ่งพิมพ์ ปี 2544	SC	มาตรา 26: ห้ามตีพิมพ์ซึ่งบทความหรืองานเขียนที่มีเนื้อหา ดังต่อไปนี้... 3) อันตรายต่อเกียรติภูมิ และประโยชน์ของรัฐ 6) กระทำการใดที่ก่อให้เกิดความไม่สงบ และสร้างความปั่นป่วนต่อเสถียรภาพของสังคม
ประกาศว่าด้วยการเพิ่มความเข้มงวดในการจัดการวารสารที่เกี่ยวกับเหตุการณ์ปัจจุบัน การเมือง วิถีชีวิต และทฤษฎีวิทยาศาสตร์ ปี 2543	GAPP	2. ห้ามโดยเด็ดขาดในการตีพิมพ์เนื้อหาต่อไปนี้... 1) หักล้างแนวทางแบบมาร์กซิสม์ แนวคิดเหมาเจ๋อตุง และ ทฤษฎีเติ้งเสี่ยวผิง 3) ...ทำร้ายประโยชน์ของรัฐ 4)... มีอิทธิพลต่อเสถียรภาพของสังคม 5) ...สร้างความเชื่อเหนือธรรมชาติ หลอกลวง หรือ คำสอนที่ผิด 6) ขยายข่าวลือ ก่อและกระจายข่าวเท็จ ขัดขวางการปฏิบัติงานของพรรคและชาติ 7) ละเมิดความเชื่อของพรรค หรือ ละเมิดกฎเกณฑ์ซึ่งเกี่ยวข้องกับการพิมพ์
ประกาศว่าด้วยการเพิ่มความเข้มงวดในการคัดเลือกบทความสำหรับหนังสือพิมพ์และวารสาร ปี 2543	GAPP	1) ... [หนังสือพิมพ์และวารสาร] จะต้องไม่เลือกบทความซึ่งขัดแย้งกับนโยบายของพรรค หรือ ชาติ
บทบัญญัติว่าด้วยการจัดการกระดานสนทนาอิเล็กทรอนิกส์ทางอินเทอร์เน็ต ปี 2543	MII	มาตรา 9: ห้ามมิให้บุคคลใดๆ เผยแพร่ข้อมูลข่าวสาร ซึ่งมีเนื้อหาดังนี้ บนกระดานข่าวอิเล็กทรอนิกส์... (iii) อันตรายต่อเกียรติภูมิและประโยชน์ของรัฐ (vi) เผยแพร่ข่าวลือ, กระทำการใดที่ก่อให้เกิดความไม่สงบ และ สร้างความปั่นป่วนต่อเสถียรภาพของสังคม
ประกาศว่าด้วยการนำอุตสาหกรรมวารสารมาอยู่ในความควบคุม ปี 2540	GAPP	มาตรา 2 (6): ในสภาวการณ์ที่มีการเอามาตรการของรัฐไปใช้แล้ว และในกรณีที่มีการแนะนำให้แก้ไขการตีพิมพ์ แต่ไม่มีการกระทำให้ดีขึ้น จึงห้ามมิให้มีการตีพิมพ์เผยแพร่ต่อไป ดังนี้ : 1) บทความที่มีความผิดพลาดเกี่ยวกับการเมืองอย่างรุนแรง
บทบัญญัติว่าด้วยการจัดการสิ่งพิมพ์อิเล็กทรอนิกส์ ปี 2540	GAPP	มาตรา 6: ห้ามมิให้ตีพิมพ์เอกสารทางอิเล็กทรอนิกส์ ซึ่งมีข้อความดังนี้ : (iii) เป็นภัยต่อชาติ... เกียรติภูมิ และ ประโยชน์ของชาติ
มาตรการว่าด้วยการจัดการรักษาความปลอดภัยของเครือข่ายสารสนเทศระหว่างประเทศ ปี 2540	MPS	มาตรา 5: ห้ามมิให้หน่วยงานหรือเอกชน ใช้อินเทอร์เน็ตในการผลิต สำเนา หรือ ค้นหา หรือ การส่งต่อซึ่งข้อมูล ดังนี้ : (v) การเผยแพร่ข่าวลือ หรือ การทำให้เกิดความวุ่นวายต่อความสงบเรียบร้อยในสังคม ; (viii) เป็นอันตรายต่อความเชื่อถือของรัฐบาล

4.1 จัดตั้งองค์กรเพื่อควบคุมการแสดงความคิดเห็นอย่างเข้มงวด

รัฐบาลจีนจัดตั้งหน่วยงานจำนวนมากพร้อมๆ ไปกับการพัฒนาเทคโนโลยีสารสนเทศ โดยมีเป้าหมายเพื่อควบคุมตรวจสอบ และปิดกั้นการเข้าถึงสื่อออนไลน์ที่ผิดกฎหมาย หรือที่รัฐบาลเห็นว่าไม่เหมาะสมได้อย่างมีประสิทธิภาพ กระทั่งการใช้โปรแกรมเฉพาะเพื่อเข้าถึงข้อมูลของผู้อื่นโดยไม่ชอบ (hacking and cyber-espionage)[24] และสั่งให้ติดตั้งซอฟต์แวร์ที่เครื่องคอมพิวเตอร์ทุกเครื่องก่อนจำหน่ายไปยังท้องตลาด เพื่อป้องกันไม่ให้ประชาชนเข้าถึงข้อมูลอันไม่พึงประสงค์ (สำหรับรัฐบาล) โดยหน่วยงานรัฐที่เกี่ยวข้อง มีดังนี้

4.1.1 องค์กรบริหารจัดการสื่อ วิทยุ โทรทัศน์ และภาพยนตร์แห่งรัฐ The State Administration of Radio, Film, and Television (SARFT)

ได้แก่ หน่วยงานบริหารสถานีวิทยุ ภาพยนตร์ และโทรทัศน์ ซึ่งรัฐบาลกำหนดให้ผู้ประสงค์ให้บริการสิ่งต่างๆ เหล่านี้ผ่านทางระบบอินเทอร์เน็ตต้องได้รับอนุญาตจากหน่วยงานนี้ด้วย ทั้งนี้ หน่วยงาน SARFT องค์กรบริหารจัดการสื่อและสิ่งพิมพ์ (General Administration of Press and Publication - GAPP) และกรมประชาสัมพันธ์กลางของพรรค (Central Propaganda Department - CPD) ได้ร่วมกันออกระเบียบกำหนดให้สื่อมวลชน ฯลฯ ต้องสนับสนุนนโยบายของพรรคคอมมิวนิสต์ และถือเป็นจริยธรรม (ethics) ของสื่อที่จะต้องซื่อสัตย์และจงรักภักดีต่อนโยบายของพรรคคอมมิวนิสต์ ผู้บริหารสื่อจะต้องปฏิบัติตามบทบัญญัติชั่วคราวว่าด้วยการบริหารจัดการบุคคลผู้รับตำแหน่งผู้สื่อข่าวทางวิทยุและโทรทัศน์ และบุคคลผู้เข้ารับตำแหน่งบรรณาธิการ (Interim Implementation Rules for Administration of Those Employed as Radio and Television News Reporters and Editors) ด้วยการควบคุมลูกจ้างของตนให้ปฏิบัติตามนโยบายของพรรคคอมมิวนิสต์เช่นเดียวกัน

4.1.2 คณะกรรมการข้อมูลข่าวสารแห่งรัฐ (The State Council Information Office)

เป็นหน่วยงานกำหนดกฎเกณฑ์ที่เกี่ยวกับการแสดงความคิดเห็นบนสื่อทุกประเภท รวมถึงการจดทะเบียนเว็บไซต์ และการเผยแพร่ข่าวสารทางอินเทอร์เน็ตด้วย นอกจากนี้ยังมีหน้าที่ออกรายงานสมุดปกขาวเกี่ยวกับเสรีภาพในการแสดงความคิดเห็นของประชาชนจีน เนื่องจากจีนเป็นภาคีสมาชิกกติกาสากลว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง[25]

4.1.3 กระทรวงอุตสาหกรรมและเทคโนโลยีข้อมูลข่าวสาร (The Ministry of Industry and Information Technology - MIIT)

มีหน้าที่กำหนดกฎเกณฑ์เกี่ยวกับด้านอุตสาหกรรม ข้อมูลข่าวสารและเทคโนโลยี เช่น กำหนดให้คอมพิวเตอร์ทุกเครื่องในประเทศจีนต้องติดตั้งโปรแกรมตรวจสอบ (pre-installed) เพื่อปิดกั้นช่องทางการเข้าถึงข้อมูลที่ไม่พึงประสงค์ โปรแกรมเหล่านั้น เช่น โปรแกรมเขื่อนสีเขียว-ปกป้องเยาวชน (Green Dam-Youth Escort Internet Browsing Filtering Software) ซึ่งสามารถตรวจสอบข้อมูลที่ถือว่าเป็นภยันตรายต่อเด็ก (harmful information) หรือไม่พึงประสงค์อื่นได้อย่างมีประสิทธิภาพ

4.1.4 หน่วยงานกิจการทางอินเทอร์เน็ต แห่งคณะกรรมการข้อมูลข่าวสารของรัฐ (The Internet Affairs Bureau of the State Council Information Office)

มีหน้าที่ควบคุมการดำเนินกิจกรรมบนอินเทอร์เน็ตของประชาชนโดยเฉพาะ หน่วยงานนี้จะเฝ้าระวังและปิดกั้นการเข้าถึงเว็บไซต์ที่มีเนื้อหาเกี่ยวกับภาพลามกและการก่อการร้าย ซึ่งแต่เดิมมาหน่วยงานนี้มีทั้งอำนาจในการโฆษณาชวนเชื่อ (propaganda) และปิดกั้นข้อมูลที่เป็นปรปักษ์กับรัฐบาลจีน ตลอดจนการดำเนินคดีกับผู้ฝ่าฝืนบทบัญญัติแห่งกฎหมายด้านนี้ แต่ปัจจุบัน รัฐบาลจีนแยกหน่วยงานออกเป็นสำนักที่ห้า (The Bureau Five) และสำนักที่เก้า (The Bureau Nine - Internet news coordination bureau)

โดยหน่วยงานแรกเป็นหน่วยโฆษณาชวนเชื่อ ส่วนหน่วยงานที่สอง มีหน้าที่บังคับใช้กฎหมายตามที่รัฐบาลกำหนด รวมทั้งดำเนินคดีตามกฎหมายต่อไป

เหล่านี้ยังไม่ได้นับรวมองค์กรรัฐองค์กรอื่นๆ ที่มีหน้าที่ควบคุมตรวจสอบการนำเสนอข้อมูลข่าวสารเช่นเดียวกันเพียงแต่กระทำบนสื่อดั้งเดิมประเภทอื่น ไม่ว่าจะเป็น องค์กรบริหารจัดการสื่อและสิ่งพิมพ์ (GAPP) ซึ่งทำหน้าที่พิจารณาให้ใบอนุญาต ควบคุมสื่อสารมวลชนและอุตสาหกรรมการพิมพ์อย่างเบ็ดเสร็จ รวมถึงมีอำนาจตรวจสอบข้อมูลก่อนจัดพิมพ์และยกเลิกใบอนุญาตการพิมพ์ได้ หน่วยงานสร้างความเชื่อและความศรัทธาต่อนโยบายของรัฐบาลและพรรคคอมมิวนิสต์ (The Central Propaganda Department - CPD) มีหน้าที่ควบคุมการปฏิบัติงานของ GAPP ให้เป็นไปตามนโยบายดังกล่าวอย่างใกล้ชิด สำนักบริหารอุตสาหกรรมและพาณิชย์แห่งสาธารณรัฐประชาชนจีน (The State Administration of Industry and Commerce) ควบคุมและดำเนินคดีกับสิ่งตีพิมพ์ที่เกี่ยวข้องกับการเมือง ซึ่งถือว่าผิดกฎหมายด้วย หรือสำนักงานกลางโฆษณาการโพ้นทะเล (The Central Office for Overseas Publicity) ซึ่งเป็นหน่วยงานที่ตรวจสอบและควบคุมสื่อสิ่งพิมพ์ต่างประเทศ เป็นต้น

นอกจากองค์กรต่างๆ ดังกล่าวมา ประเทศจีนยังมีองค์กรอื่นๆ ที่ทำหน้าที่สำคัญเกี่ยวกับการควบคุมการแสดงความคิดเห็นของประชาชนรวมทั้งหมด 14 องค์กร อาทิ กระทรวงวัฒนธรรมและสำนักงานความลับแห่งรัฐ (State Secrecy Bureau) ที่มีหน้าที่กดดันการแสดงความคิดเห็น (chills freedom of expression) ด้วยการใช้กฎหมายว่าด้วยความลับของชาติ (State Secrets Laws) กระทรวงอุตสาหกรรมสารสนเทศ (Ministry of Information Industry - MII) มีหน้าที่ออกใบอนุญาตให้ผู้ประกอบการอินเทอร์เน็ต หรือกระทรวงตำรวจ (Ministry of Public Security) จะทำหน้าที่กลั่นกรอง (filtering) และเฝ้าระวัง (monitoring) ระบบอินเทอร์เน็ตด้วย[26]

อย่างไรก็ตาม องค์กรที่นับว่ามีความสำคัญที่สุดที่จะทำให้การปิดกั้นการแสดงความคิดเห็นของประชาชนจีนเกิดขึ้นจริงและคง

ความศักดิ์สิทธิ์ก็คือ องค์กรตุลาการหรือศาล ซึ่งปรากฏว่าศาลในประเทศจีนจะยึดถือนโยบายการเซ็นเซอร์ของรัฐบาลจีนอย่างเคร่งครัด ถึงขนาดที่เคยพิพากษาลงโทษการเผยแพร่ข้อมูลโดยไม่ได้รับอนุญาต โดยอาศัยประมวลกฎหมายอาญามาตรา 225 แม้เนื้อความนั้นจะไม่ผิดกฎหมายในตัวเองก็ตาม[27] โดยศาลจีนละเว้นที่จะพิจารณาว่ากฎหมายของรัฐบาลขัดรัฐธรรมนูญหรือไม่[28]

4.2 นโยบาย และมาตรการอื่น ๆ ของรัฐที่ใช้จำกัดเสรีภาพในการแสดงความคิดเห็นบนอินเทอร์เน็ต

ที่ผ่านมา รัฐบาลจีนใช้มาตรการที่เข้มงวดกับการแสดงความคิดเห็นหลายมาตรการ อาทิ การปิดกั้น (blocking) การกลั่นกรอง (filtering) และการเฝ้าระวังอย่างใกล้ชิด (monitoring) รวมทั้งการห้ามนำเข้าซึ่งเอกสารใดๆ ที่อาจกระทบต่อความมั่นคงและผลประโยชน์ของประเทศจีนด้วย[29] แม้ในปี 2002 ประเทศจีนจะถูกกดดันจากนานาชาติและองค์กรการค้าโลก (WTO) ให้พิจารณาทบทวนการใช้เทคโนโลยีที่เรียกว่า “เกรตไฟร์วอลล์” (The Great Firewall) เพราะขัดกับข้อกำหนดแห่งสนธิสัญญาดังกล่าว แต่ก็หาได้เกิดความเปลี่ยนแปลงใดๆ ในประเทศจีนไม่[30] สำหรับรูปแบบวิธีการที่รัฐบาลจีนใช้ในการจำกัดเสรีภาพในการแสดงความคิดเห็นต่างๆ ปรากฏดังนี้

4.2.1 การกลั่นกรองและการปิดกั้นเว็บไซต์โดยอัตโนมัติ

เนื่องจากรัฐบาลจีนมีทัศนคติว่ารัฐมีอำนาจเต็มที่ในการตรวจสอบ และบล็อกเว็บไซต์บางเว็บไซต์ได้เพื่อประโยชน์ของชาติ[31] ไม่ว่าจะเป็นการปิดกั้นเว็บไซต์ของสถานศึกษาในประเทศสหรัฐอเมริกา[32] เว็บไซต์ที่เกี่ยวข้องกับสิทธิมนุษยชน การศึกษา การเมือง และรวมทั้งเว็บไซต์ข่าว ทั้งนี้ โดยไม่ต้องมีการแจ้งเตือนผู้ให้บริการเว็บเหล่านั้นล่วงหน้า ทั้งผู้ถูกปิดกั้นดังกล่าวไม่มีโอกาสในการอุทธรณ์การปิดกั้นนั้น โดยรัฐบาลจีนอ้างว่าการพัฒนาเกรตไฟร์วอลล์นั้นก็เพื่อปิดกั้นเว็บไซต์ที่

เกี่ยวกับภาพลามกอนาจาร (obscenity) หรือจดหมายขยะ (junk mail) เท่านั้น แต่ในความเป็นจริงแล้วก็หาได้เป็นเช่นนั้นไม่ เพราะเว็บเพจทางการเมืองจำนวนไม่น้อยก็ถูกกลั่นกรองและไม่แสดงผลในเวลาต่อมา[33] โดยการปิดกั้นนั้นรัฐบาลจะแจ้งผู้ใช้บริการว่า “ข้อความที่ได้ลงไว้ต้องถูกลบทิ้งตามบทบัญญัติของกฎหมายและกฎระเบียบที่เกี่ยวข้อง” (The posting was deleted according to relative laws and regulations”)

อนึ่ง โปรแกรมเกรตไฟร์วอลล์ยังสามารถป้องกันการใช้เสิร์ชเอนจินเพื่อค้นหาเว็บไซต์ที่รัฐไม่พึงประสงค์ให้ประชาชนได้รับรู้อีกด้วย อาทิเช่น เว็บไซต์ข่าวบีบีซี หรือเว็บไซต์สำคัญและมีชื่อเสียงในด้านสิทธิมนุษยชนและวิพากษ์วิจารณ์รัฐบาลจีน เว็บไซต์ของแอมเนสตี้อินเตอร์เนชั่นแนล องค์กรฮิวแมนไรท์วอทช์ องค์กรแรงงานในประเทศจีน มูลนิธิ Dui Hua รวมทั้งองค์กรผู้สื่อข่าวไร้พรมแดน (Reporters Without Borders)[34] ผู้ให้คำปรึกษาด้านเทคโนโลยีคนหนึ่งเคยกล่าวว่า เขาไม่สามารถเข้าเว็บไซต์ตลาดหลักทรัพย์ฮ่องกงได้เลย หรือแม้กระทั่งเว็บไซต์ลิงก์อิน (LinkedIn) ก็ตาม เนื่องจากความเป็นกังวลของรัฐบาลจีนจนเกินเหตุต่อการรวมตัวกันประท้วงโดยอาศัยอินเทอร์เน็ตเป็นสื่อกลาง

ดังกล่าวมาแล้วว่าประเทศจีนนับเป็นประเทศในระดับต้นๆ ของโลกในเรื่องความสามารถในการพัฒนาเทคโนโลยีคอมพิวเตอร์เพื่อกลั่นกรองตรวจสอบเนื้อหาในระบบเครือข่ายอินเทอร์เน็ต นอกจากเกรตไฟร์วอลล์แล้ว จีนยังเคยใช้ซอฟต์แวร์ตรวจสอบเนื้อหาฟาหลุนกง (Falun Gong Content Examination System) ในปี 2004 ซึ่งเป็นโปรแกรมที่สามารถวิเคราะห์ และระบุได้ว่าเนื้อหาที่ตรวจสอบเป็นเนื้อหาที่สนับสนุนลัทธิฟาหลุนกง ซึ่งถูกเรียกว่าเป็นบทความสีดำหรือไม่ หากพบว่าใช่ก็จะถูกปิดกั้นทันที ซึ่งรัฐบาลจีนสั่งให้ติดตั้งระบบนี้ในคอมพิวเตอร์ส่วนตัวของประชาชน ระบบเซิร์ฟเวอร์รวมทั้งติดตั้งไว้ที่เกตเวย์ด้วยเพื่อคอยปิดกั้นการเข้าถึงจากผู้ใช้อินเทอร์เน็ตภายในประเทศ และหากมีผู้ใช้อินเทอร์เน็ตเข้าเว็บไซต์หรือเว็บเพจดังกล่าว ระบบก็จะทำการแจ้งไปยังเจ้าหน้าที่ผู้รับผิดชอบ

ในช่วงปี 2009 สืบเนื่องมาจากการประท้วงในประเทศอิหร่าน

และเหตุการณ์จลาจลของชนกลุ่มน้อยซึ่งได้คร่าชีวิตผู้คนไปกว่า 200 คน ในเขตปกครองตนเองซินเจียง (Xinjiang) ซึ่งเป็นภูมิภาคหนึ่งทางตะวันตกของประเทศจีน และประชากรส่วนใหญ่กล่าว 22 ล้านคนเป็นชาวมุสลิม ทำให้รัฐบาลจีนมองเห็นศักยภาพและปัญหาของอินเทอร์เน็ตที่เป็นตัวจุดชนวนการประท้วง และก่อให้เกิดการจลาจลทั้งในประเทศอิหร่านและในเขตปกครองตนเองซินเจียง ทำให้รัฐบาลจีนสั่งลบเนื้อหาจำนวนมากที่แสดงความไม่พอใจในการปกครองของเขตปกครองตนเองซินเจียง ในขณะที่เว็บไซต์หนึ่งซึ่งใช้ภาษาอุยกูร์ (Uighur) ซึ่งเป็นภาษาที่มีการพูดกันในเขตปกครองตนเองและเป็นเว็บไซต์ที่ได้รับความนิยมอย่างมากถูกปิดกั้น รัฐบาลจีนยังได้จับตัวผู้สร้างเนื้อหาในเว็บไซต์นั้นและสั่งให้จำคุก 3-10 ปี ในข้อหาการคุกคามความมั่นคงของรัฐ นอกจากนี้ ภายหลังเหตุจลาจลดังกล่าว รัฐบาลจีนยังดำเนินการปิดกั้นเครือข่ายสังคมออนไลน์อย่างเฟซบุคและทวิตเตอร์ โดยนักลงทุนด้านสื่อซึ่งมีความสัมพันธ์กับผู้ออกกฎหมายของจีนคนหนึ่งถึงกับกล่าวว่า “อิทธิพลของอินเทอร์เน็ตต่อเหตุการณ์อย่างในอิหร่านและซินเจียง ส่งผลกระทบต่อผู้นำของจีนดั่งแผ่นดินไหว”[35] ในขณะที่ Ilham Tohti นักวิชาการชาวอุยกูร์ในกรุงปักกิ่ง ซึ่งเว็บไซต์ของเขาได้ถูกปิดกั้นการเข้าถึงเช่นกัน กล่าวว่า “การจองจำ ได้ทำให้การแสดงความคิดเห็นหยุดนิ่ง และปิดกั้นการสนทนาระหว่างชาวอุยกูร์ ซึ่งคนจำนวนหนึ่งมีความสามารถจำกัดในการอ่านและเขียนภาษาจีน สำหรับชาวอุยกูร์ ไม่มีช่องทางมากมายนักในสื่อดั้งเดิม สื่อออนไลน์จึงเป็นช่องทางที่ทำให้สามารถแสดงความเห็นของตัวเองได้ แต่ในขณะนี้ เราก็ถูกปิดปาก”[36]

สำหรับระบบกระดานข่าว กระดานแสดงความคิดเห็น หรือ Internet bulletin board systems (BBSs) นั้น ปัจจุบัน ประเทศจีนได้จัดตั้งศูนย์กลางข้อมูลข่าวสารทางเครือข่ายของประเทศ (China Internet Network Information Center) ขึ้น และกำหนดว่า การใช้ระบบ BBSs ต้องได้รับใบอนุญาตจากหน่วยงานนี้ก่อน โดยบทความทั้งหมดในระบบกระดานข่าวจะถูกจับตาและเฝ้าระวัง และผู้ให้บริการระบบ BBSs มีหน้าที่ต้องจัด

เก็บข้อมูลไว้ไม่ว่าจะเป็นเนื้อหาที่มีการเผยแพร่ในระบบหรือในเว็บไซต์ เมื่อมีการแสดงความคิดเห็น รวมถึงที่อยู่ทางอินเทอร์เน็ต (IP address) ของผู้ใช้อินเทอร์เน็ตนั้น ทั้งนี้ นอกจากรัฐบาลจีนจะอาศัยซอฟต์แวร์เพื่อตรวจสอบกลั่นกรองจาก “คำต้องห้าม” และปิดกั้นการเข้าถึงระบบ BBSs แล้ว ยังกำหนดให้มีเจ้าหน้าที่รัฐคอยเฝ้าระวัง ปิดกั้น รวมทั้งลบข้อมูลหรือบทความประเภทที่รัฐบาลไม่อาจยอมรับให้มีการเผยแพร่ได้อีกด้วย[37]

4.2.2 กำหนดหน้าที่แก่ผู้ให้บริการอินเทอร์เน็ตให้ต้องช่วยกลั่นกรองเนื้อหาผิดกฎหมาย รวมทั้งจัดเก็บข้อมูลการใช้บริการ และข้อมูลของผู้ใช้บริการไว้ตามระยะเวลากำหนด

ภายใต้กฎหมายควบคุมอินเทอร์เน็ต หรือ Internet Measures[38] นั้น นอกจากผู้ให้บริการข้อมูลข่าวสารทางอินเทอร์เน็ต (internet information services) และผู้ให้บริการที่มีระบบ BBSs ต้องจัดเก็บข้อมูล เนื้อหาสาระที่มีการเผยแพร่ในเว็บไซต์ เวลาที่เผยแพร่ ที่อยู่ทางอินเทอร์เน็ตแล้ว ยังต้องเก็บข้อมูลที่เกี่ยวข้องกับระยะเวลาที่ลูกค้าแต่ละคนใช้บริการอินเทอร์เน็ต ข้อมูลบัญชีของลูกค้านั้น (customer’s account number) และเบอร์โทรศัพท์ของลูกค้าด้วย โดยเก็บเป็นเวลา 60 วัน เพื่อเตรียมพร้อมให้เจ้าหน้าที่เรียกข้อมูล หรือเข้ามาตรวจสอบได้ตลอดเวลา และหากผู้ให้บริการอินเทอร์เน็ตตรวจสอบเนื้อหาที่มีการเผยแพร่นั้นเอง แล้วพบว่าขัดต่อกฎหมาย จะต้องดำเนินการลบทันที แล้วรายงานให้เจ้าหน้าที่ที่มีอำนาจทราบ ในส่วนของอินเทอร์เน็ตคาเฟ่ นั้น ตามมาตรการควบคุมการบริหารงานธุรกิจที่ให้บริการในการเข้าถึงอินเตอร์เน็ต (Regulations on the Administration of Internet Cafes)[39]บังคับให้ลูกค้าร้านอินเทอร์เน็ตต้องแจ้งข้อมูลส่วนบุคคลและนำสำเนาบัตรประจำตัวประชาชนมามอบให้กับผู้ดำเนินการร้านค้า โดยผู้ให้บริการร้านค้าจะต้องเก็บรักษาข้อมูลดังกล่าวไว้เป็นเวลา 60 วัน และแจ้งข้อมูลดังกล่าวแก่เจ้าหน้าที่หรือหน่วยงานของกระทรวงวัฒนธรรมและตำรวจเพื่อตรวจสอบต่อไป[40] ทั้งนี้ นับตั้งแต่ปี 2002 เป็นต้นมา รัฐบาลจีนยังกำหนดให้ผู้ใช้บริการอินเทอร์เน็ตต้องซื้อบัตรเพื่อเข้าถึงระบบอินเทอร์เน็ต

เพราะบัตรนี้จะบันทึกชื่อ ที่อยู่ ข้อมูลอื่นๆ ที่จำเป็น รวมทั้งภาพของผู้ซื้อไว้ ซึ่งข้อมูลดังกล่าวจะถูกจัดเก็บในระบบฐานข้อมูลตำรวจทันทีเมื่อมีการนำบัตรไปใช้ในร้านอินเทอร์เน็ต ด้วยวิธีการนี้เองที่ทำให้เจ้าหน้าที่ตำรวจสามารถตรวจสอบการเข้าถึงเนื้อหาที่ผู้นั้นใช้บริการได้

4.2.3 ปฏิบัติการทางจิตวิทยา

รัฐบาลจีนยังกระทำการปฏิบัติการทางจิตวิทยา โดยจัดตั้งสมาคมอินเทอร์เน็ตแห่งประเทศจีนขึ้น (The Government-connected Internet Society) เพื่อรณรงค์ให้ผู้ให้บริการอินเทอร์เน็ตปิดกั้นเนื้อหาที่รัฐบาลจีนเห็นว่าไม่เหมาะสม ผู้เขียนหรือเผยแพร่เนื้อหาบนเว็บไซต์เองก็มีภาระหน้าที่ต้องตรวจสอบและละเว้นการเผยแพร่ข้อมูลดังกล่าวด้วยตนเอง รวมถึงมาตรการที่จะไม่อนุญาตให้ผู้ให้บริการอินเทอร์เน็ตจากต่างประเทศ ไม่ว่าจะเป็นกูเกิล (Google) ยาฮู (Yahoo) และไมโครซอฟท์ (Microsoft) ประกอบกิจการในประเทศจีนอีกต่อไป หากผู้ให้บริการเหล่านี้ไม่ปฏิบัติตามนโยบายข้างต้น[41] นอกจากนี้ รัฐบาลจีนยังว่าจ้างกลุ่มพลเมืองเน็ตที่ใช้ชื่อว่า “50 Cent Party” ให้โพสต์ข้อความสนับสนุนนโยบายและการบริหารประเทศของรัฐบาลจีนด้วย โดยได้รับค่าตอบแทนครั้งละ 50 Cent รวมถึงการจัดตั้ง Bureau Five และ Bureau Nine เพื่อติดตามความเคลื่อนไหวต่างๆ พร้อมกับดำเนินคดีอาญาอย่างจริงจัง เช่น เคยเกิดการฟ้องร้องคดีในความผิดฐานหมิ่นประมาท ตามประมวลกฎหมายอาญา มาตรา 246 เป็นจำนวนมาก[42] กรณีที่มีการเสนอความเห็นเกี่ยวกับการสลายการชุมนุมที่จตุรัสเทียนอันเหมิน[43] เป็นต้น

5. ปฏิกิริยาและความเคลื่อนไหวฝ่ายประชาชนและภาคสังคมที่มีต่อกฎหมาย หรือนโยบายที่กระทบเสรีภาพในสื่อออนไลน์[44]

ศาสตราจารย์แกรี่ คิง จากมหาวิทยาลัยฮาวาร์ดเคยกล่าวว่า “หากกล่าวถึงเสรีภาพในโลกออนไลน์แล้ว อาจดูเหมือนประชาชนจีนต่าง

คนต่างมีความเป็นอิสระ แต่ถ้ามองในภาพรวมทั้งหมดกลับถูกล่ามโซ่ตรวนเอาไว้"[45] โดยรัฐบาลจีนได้ตรวจสอบและจับผิดอย่างรุนแรง เว็บไซต์ศูนย์สิทธิมนุษยชนและการพัฒนาประชาธิปไตยนานาชาติ (International Center for Human Rights and Democracy Development) เคยแสดงความคิดเห็นว่า นโยบายการควบคุมสื่อออนไลน์ของประเทศจีนถือเป็นภัยคุกคามต่อการคุ้มครองสิทธิมนุษยชนโดยเฉพาะสิทธิความเป็นส่วนตัวและเสรีภาพซึ่งเป็นรากฐานสำคัญของประชาธิปไตย ดังเช่นเสรีภาพในการรวมกลุ่มและเสรีภาพในการแสดงความคิดเห็น รัฐบาลจีนบัญญัติกฎหมายจำนวนมากเพื่อใช้เป็นเครื่องมือในการจำกัดเสรีภาพการแสดงความคิดเห็นของประชาชนในสื่ออินเทอร์เน็ต ซึ่งนอกจากการดำเนินคดีและลงโทษทางอาญากับผู้สื่อข่าว นักเขียน และประชาชนที่ละเมิดกฎหมายเหล่านั้นอย่างต่อเนื่องแล้ว ยังปิดกั้นเว็บไซต์ที่รัฐบาลจีนพิจารณาแล้วเห็นว่าไม่เหมาะสมหรือกระทบต่อความมั่นคง กรณีที่สำคัญ อาทิ เว็บไซต์ที่เสนอข้อมูลความเคลื่อนไหวของดาไลลามะ (Dalai Lama) หรือเหตุการณ์สลายการชุมนุมนองเลือดที่จัตุรัสเทียนอันเหมิน เว็บไซต์ของลัทธิฟาหลุนกง การเคลื่อนไหวรณรงค์เกี่ยวกับความเชื่อทางศาสนา รวมทั้งสื่ออินเทอร์เน็ตอื่นๆ ที่รณรงค์เกี่ยวกับสิทธิมนุษยชน

อย่างไรก็ตาม แม้รัฐบาลจีนจะพยายามอย่างเข้มงวดในการบังคับใช้กฎหมายและมาตรการต่างๆ อย่างเต็มที่แล้ว แต่ก็มีประชาชนจีนหรือผู้ประกอบการสื่อที่ไม่เห็นด้วยกับการจำกัดเสรีภาพในการแสดงความคิดเห็นพยายามดื้อแพ่งหรือต่อต้าน และไม่ปฏิบัติตามกฎเกณฑ์หรือแนวนโยบายของรัฐบาลจีนเช่นกัน ทั้งนี้ มีปฏิกิริยาและการเคลื่อนไหวครั้งสำคัญๆ หรือที่น่าสนใจดังต่อไปนี้

5.1 ปฏิกิริยาเพื่อต่อต้านเกรตไฟร์วอลล์ (The great firewall)

ดังกล่าวไปแล้วว่า รัฐบาลจีนมีแนวคิดว่า รัฐเป็นผู้มีอำนาจเต็มในการกำกับตรวจสอบ รวมทั้งปิดกั้นการเข้าเข้าถึงเว็บไซต์บางเว็บไซต์ได้เพื่อประโยชน์ของชาติ[46] ทั้งนี้ โดยมิต้องมีการแจ้งเตือนผู้ให้

บริการเว็บไซต์เหล่านั้นล่วงหน้า จนมีการพัฒนาเครื่องมือตรวจสอบและปิดกั้นที่มีประสิทธิภาพสูง ภายใต้ชื่อเกรตไฟร์วอลล์ (Great Firewall) ซึ่งรัฐบาลจีนกล่าวแก่ประชาชนว่า เพื่อปิดกั้นเว็บไซต์ที่เกี่ยวกับภาพลามกอนาจาร (Obscenity) หรือจดหมายขยะ (Junk mail) เท่านั้น อย่างไรก็ตาม ด้วยศักยภาพของเครื่องมือดังกล่าว ประกอบกับทัศนคติของรัฐบาล ประชาชนจีนผู้ใช้บริการอินเทอร์เน็ตส่วนใหญ่จึงไม่เชื่อเช่นนั้น หนังสือพิมพ์นิวยอร์กไทม์สได้ตีพิมพ์บทสัมภาษณ์ Zhu Nan นักศึกษาจีนที่ให้ความสนใจการใช้และการควบคุมอินเทอร์เน็ตในประเทศจีน ซึ่งกล่าวว่า เขารู้สึกระแคะระคาย และอยากแสดงความเห็นเกี่ยวกับการใช้อำนาจอย่างกว้างขวางในการปิดกั้นเสรีภาพของสื่อออนไลน์ของรัฐบาลจีน จึงเขียนบล็อก และตั้งคำถามถึงเหตุผลในการปิดกั้นอินเทอร์เน็ตว่า

"เจ้าหน้าที่ในประเทศเราอ้างว่าการตรวจจับทางอินเทอร์เน็ตเป็นเรื่องที่ถูกต้องชอบธรรมตามกฎหมาย แต่เหตุใดจึงไม่ให้ประชาชนทราบรายละเอียดของกฎหมายดังกล่าว และเหตุใดจึงห้ามการวิจารณ์ หรือการตรวจสอบนโยบายทางกฎหมายนั้นในอินเทอร์เน็ต หากรัฐบาลตั้งใจจะตรวจสอบ และปิดกั้นเว็บไซต์โดยอ้างว่าถูกต้องชอบธรรมแล้ว รัฐบาลก็ต้องไม่กลัวการวิพากษ์วิจารณ์ที่เกิดขึ้น"[47]

นอกจาก Zhu Nan แล้ว ในประเทศจีนยังปรากฏผู้ใช้สื่อออนไลน์อีกจำนวนมาก ที่เห็นว่ารัฐบาลจีนใช้มาตรการเข้มงวดเกินไปกับอินเทอร์เน็ต เพราะกระทั่งเว็บไซต์ที่ไม่มีเนื้อความเกี่ยวข้องกับการเมืองเลยก็ถูกตรวจสอบหรือปิดกั้นไปด้วย การดำเนินนโยบายที่แข็งกร้าวในลักษณะนี้เองได้ก่อให้เกิดปฏิกิริยาตอบโต้จากประชาชนผู้ใช้อินเทอร์เน็ตอย่างรุนแรงและกว้างขวาง โดยเฉพาะอย่างยิ่งคนที่ไม่ได้สนใจในเรื่องการเมืองการปกครองเลย เพราะกลายเป็นแรงผลักให้เขาเหล่านั้นตื่นตัวและเริ่มหันมาต่อต้านการควบคุมโดยรัฐมากขึ้น

ปัจจุบัน มีประชาชนจีนจำนวนมากขึ้นเรื่อยๆ ที่รู้สึกไม่พอใจอย่างยิ่งต่อการที่รัฐบาลห้ามการให้บริการเว็บไซต์ประเภทต่างๆ ในวงกว้าง

ไม่ว่าจะเป็น ฟลิกเกอร์ (Flickr) ยูทูบ (Youtube) วิกิพีเดีย (Wikipedia) มายสเปซ (Myspace) และ บล็อกสป็อต (Blogspot) ทำให้เกิดคลื่นการต่อต้านในหลากหลายรูปแบบ ไม่ว่าจะเป็นการประท้วงเรียกร้องการสร้างซอฟท์แวร์โดยนักพัฒนาซอฟท์แวร์เพื่อจัดการกับการจำกัดเสรีภาพทางออนไลน์ของรัฐ กระทั่งการฟ้องร้องผู้ให้บริการอินเทอร์เน็ตที่รัฐบาลเป็นเจ้าของต่อศาลโดยกล่าวหาว่า การปิดกั้นเว็บไซต์เป็นเรื่องที่ผิดกฎหมาย เช่น กรณีที่ นาย Du Doongjing วิศวกรด้านเทคโนโลยีสารสนเทศฟ้องสำนักงานสาขาของบริษัทไชน่าเทเลคอม (China Telecom) ในข้อหาผิดสัญญาการให้บริการอินเทอร์เน็ต เพราะมีการปิดกั้นเว็บไซต์ที่เขาใช้ในการทำธุรกิจโดยไม่ได้รับคำอธิบายใดๆ และปราศจากการบอกกล่าวล่วงหน้า อย่างไรก็ตาม คดีของ Du Doongjing ถูกยกฟ้องโดยศาลเซี่ยงไฮ้ ขณะนี้อยู่ในระหว่างกระบวนการอุทธรณ์ Du Doongjing กล่าวว่า “ผมเชื่อว่าด้วยการสนับสนุนของประชาชน ผมสามารถชนะคดีนี้ได้ และผมก็จะมีส่วนในการสร้างและพัฒนาประชาธิปไตยในจีนด้วย”[48]

Li Xie Heng นักเขียนบล็อกซึ่งเป็นหนึ่งในผู้เคลื่อนไหวเรื่องสิทธิมนุษยชน ลงมือพัฒนาโปรแกรมชื่อ แกลดเดอร์ (Gladder) ขึ้น เพื่อเข้าถึงข้อมูลหรือเว็บไซต์ที่ถูกปิดกั้นโดยเกรตไฟร์วอลล์ให้กับผู้ใช้อินเทอร์เน็ตที่ใช้บราวเซอร์ของไฟร์ฟ็อกซ์ (Firefox)[49] ในขณะที่ Han Han นักเขียนบล็อกผู้มีชื่อเสียงโด่งดังในประเทศจีน มีผู้ติดตามบล็อกของเขากว่า 300 ล้านคน ก็เขียนบทความวิพากษ์วิจารณ์เหตุการณ์ปัจจุบัน โจมตีผู้นำจีน และนโยบายที่เขาคิดว่าได้สร้างความทุกข์ยากให้กับผู้คนที่โชคร้าย และยังไม่ได้มีโอกาสได้แสดงความคิดเห็นผ่านทางอินเทอร์เน็ต

ดังนั้นในช่วงหลายปีที่ผ่านมา ลักษณะของการเคลื่อนไหวภาคประชาชนผู้ใช้บริการอินเทอร์เน็ต (Netizens) ภายในประเทศจีน ส่วนใหญ่จึงเป็นปฏิกิริยาตอบโต้เกรตไฟร์วอลล์ของรัฐบาลจีนนั่นเอง ซึ่งอาจแบ่งออกได้ดังต่อไปนี้

• การสร้างโปรแกรมที่สามารถหลีกเลี่ยงการตรวจจับทางออนไลน์ (circumvention tools)

• เครือข่ายต่อต้านการตรวจสอบและจับผิด (censorship) อย่างไม่เป็นทางการ โดยมีกิจกรรมต่างๆ อาทิ การสอนใช้เครื่องมือการหลีกเลี่ยง (circumvention tools) เพื่อเข้าถึงเว็บไซต์ที่ถูกปิดกั้น และการบอกต่อ เช่น การเข้าถึงเว็บไซต์ทวิตเตอร์เพื่อที่จะได้เข้าถึงการสนทนาของสังคมระหว่างประเทศ

• เครือข่ายเพื่อจัดหาพื้นที่การใช้งานทางอินเทอร์เน็ต (web hosting) โดยผู้ใช้อินเทอร์เน็ตซื้อพื้นที่ในเว็บไซต์ของต่างประเทศ และสร้างบล็อกอิสระเพื่อช่วยเหลือผู้ใช้อินเทอร์เน็ตที่ไม่มีความรู้ทางเทคนิคแต่อยากมีเว็บไซต์ของตนเอง และสามารถหลีกเลี่ยงการถูกเพิกถอนเนื้อหา นอกจากนี้ จะมีอาสาสมัครหลายคนช่วยเหลือผู้เขียนบล็อก ด้วยการสลับชื่อโดเมนและที่อยู่ทางอินเทอร์เน็ต หากบล็อกนั้นได้รับความสนใจและสุ่มเสี่ยงที่จะโดนปิดกั้นจากเกรตไฟร์วอลล์

• สร้างทีมวิจัยที่คอยสืบค้นข้อมูลที่จะใช้ในการประท้วง หรือคัดค้านการปิดกั้นเสรีภาพในสื่อออนไลน์ของรัฐบาลจีน โดยมีการรวมกลุ่มกันแบบหลวมๆ เพื่อหาข้อมูล และจัดรายงานเกี่ยวกับซอฟแวร์เขื่อนสีเขียว (Green Dam) การเมือง ศาสนา กฎหมายต่างๆ ที่เกี่ยวข้องกับความมั่นคง รวมถึงข้อมูลและการรายงานต่างๆ ที่เผยแพร่ในวิกิลีกส์ (Wikileaks)

• สร้างนิสัยให้กับผู้ใช้บริการให้ดาวน์โหลดข้อมูล บทความ รูป วีดิโอ ที่มีแนวโน้มที่จะถูกปิดกั้นไว้ก่อน และนำเผยแพร่ต่อกันทางอีเมล หรือในเครือข่ายสังคมออนไลน์

นอกเหนือจากนี้ ก็เป็นการประท้วงและตอบโต้เป็นรายบุคคล อาทิ ปัญญาชนและนักเขียนเขียนบทความลงในบล็อกส่วนตัวเพื่อวิจารณ์รัฐบาลและนโยบายการควบคุมต่างๆ เสนอต่อสาธารณชนว่า การตรวจจับสื่อออนไลน์ส่งผลเป็นการปิดกั้นนวัตกรรมและความคิดสร้างสรรค์ของประชาชน เป็นต้นเหตุหนึ่งของการคอร์รัปชั่นและทำให้เกิดความไม่มีประสิทธิภาพทางเศรษฐกิจ และนอกจากประชาชนทั่วไปแล้ว Yuan Mingli นักเคลื่อนไหวประชาธิปไตย ซึ่งเป็นผู้สร้างกลุ่มผู้บุกรุกเกรตไฟร์วอลล์ (Anti Great Firewall Evasion Group) กล่าวว่า ตอนนี้รัฐบาลทำงานอย่างแข็งขัน

เพื่อสร้างเทคโนโลยีอินเทอร์เน็ตทันสมัยที่มุ่งโจมตีประชาชนและคนทั่วโลก แต่เขาทำนายว่ามันจะล้มเหลว ประชาชนชาวจีนเปลี่ยนไปแล้ว ระบบต่างๆ จะพังลง เนื่องจากประเทศจีนไม่สามารถตัดขาดการติดต่อจากประเทศภายนอกได้เหมือนเดิมแล้ว[50]

ความเคลื่อนไหวของภาคประชาชนดังกล่าวดำเนินการเรื่อยมานับตั้งแต่รัฐบาลจีนเริ่มใช้นโยบายเข้มงวดในการตรวจสอบและจับผิดสื่อออนไลน์ ทั้งนี้ ในช่วงปี 2551 ผู้ใช้สื่อออนไลน์ทั่วประเทศ นำโดย นาย Liu Xiaobao นักสิทธิมนุษยชน ซึ่งได้รับรางวัลโนเบลสาขาสันติภาพ ได้เสนอ “Charter 08” หรือคำประกาศเจตนาออนไลน์ ที่มีเนื้อหาเรียกร้องการปฏิรูประบอบประชาธิปไตย การเคารพสิทธิมนุษยชน การยกเลิกการเมืองระบบพรรคเดียว การบัญญัติกฎหมายที่เป็นอิสระ รวมทั้งเสรีภาพในโลกออนไลน์ด้วย อย่างไรก็ตาม Charter 08 ที่เผยแพร่ในอินเทอร์เน็ตถูกลบออกในเวลาต่อมา และเว็บไซต์ที่เผยแพร่ก็ถูกปิดโดยรัฐบาล โดยนาย Liu Xiaobao ถูกควบคุมตัวและถูกตัดสินจำคุกเป็นเวลาถึง 11 ปี

5.2 การประท้วงกฎหมาย และซอฟต์แวร์ “เขื่อนสีเขียว-ปกป้องเยาวชน” (Green Dam - Youth Escort)

ปฏิกิริยาของภาคประชาชนที่มีต่อนโยบายการตรวจสอบและปิดกั้นอินเทอร์เน็ตที่เข้มงวดของรัฐบาลจีนครั้งใหญ่ครั้งหนึ่ง สืบเนื่องมาจากแผนการของรัฐบาลที่จะผลักดันกฎหมายฉบับหนึ่ง ซึ่งกำหนดให้บริษัทคอมพิวเตอร์ต้องติดตั้งซอฟท์แวร์ชื่อว่า “เขื่อนสีเขียว-ปกป้องเยาวชน” (Green Dam-Youth Escort) ไว้ในคอมพิวเตอร์ทุกๆ เครื่อง ด้วยเหตุผลว่าเพื่อเป็นเครื่องมือในการปกป้องเยาวชน แต่ในความเป็นจริงแล้วซอฟท์แวร์ดังกล่าวไม่ได้มีประสิทธิภาพหรือมีเป้าหมายเพื่อตรวจสอบและปิดกั้นเว็บไซต์ลามกอนาจารเท่านั้น หากแต่สามารถตรวจสอบกิจกรรมของประชาชนที่ใช้อินเทอร์เน็ตได้ทำทุกย่างก้าว อีกทั้งยังเป็นซอฟต์แวร์ที่เป็นอันตรายต่อเครื่องคอมพิวเตอร์ (malware) ด้วย

Ai Wei Wei ศิลปินและนักเคลื่อนไหวทางสิทธิมนุษยชน ได้ส่ง

คำเชิญทางอีเมลถึงประชาชนให้ออกมาประท้วงคัดค้าน เห็นว่าจุดประสงค์ที่แท้จริงของกฎหมายดังกล่าวเป็นไปเพื่อให้รัฐบาลมีอำนาจควบคุมเบ็ดเสร็จต่อผู้ใช้บริการอินเทอร์เน็ตในแผ่นดินจีน ซอฟต์แวร์และกฎหมายถูกออกแบบมาเพื่อควบคุมเนื้อหาในอินเทอร์เน็ตโดยเฉพาะอย่างยิ่ง เนื้อหาที่รัฐบาลไม่พึงพอใจ เช่น ประชาธิปไตย ลัทธิฟาหลุนกง และเสรีภาพในการแสดงความคิดเห็น หาใช่เพื่อต่อสู้กับสื่อลามกอนาจารหรือเว็บไซต์ที่มีเนื้อหารุนแรงไม่ แผนการผลักดันกฎหมายฉบับนี้และผลจากการกระจายข่าวสารทางอีเมลและอินเทอร์เน็ต ยังผลให้ชาวจีนจำนวนกว่าพันคนออกมาเดินประท้วงใหญ่ในกรุงปักกิ่ง เพื่อเป็นการแสดงพลังคว่ำบาตรอินเทอร์เน็ตเป็นเวลาหนึ่งวัน รวมทั้งเรียกร้องให้การเซ็นเซอร์ในประเทศจีนสิ้นสุดลง และนอกจากการเดินประท้วงแล้ว นโยบายนี้ยังถูกวิพากษ์วิจารณ์อย่างกว้างขวางทั้งในประเทศและนอกประเทศ ถึงขนาดที่บริษัทและสมาคมการค้าพาณิชย์ซึ่งเป็นตัวแทนผู้ผลิตสินค้าจากประเทศต่างๆ ที่สำคัญของโลกต้องส่งจดหมายถึงประธานาธิบดีเรียกร้องให้รัฐบาลยกเลิกการผลักดันกฎหมายดังกล่าว

ในท้ายที่สุด ผลจากการประท้วงต่อต้านทั้งภายในและภายนอกประเทศ รัฐบาลจีนจึงต้องเลื่อนการประกาศใช้กฎหมายฉบับดังกล่าวไปอย่างไม่มีกำหนด ผู้สื่อข่าวและนักเคลื่อนไหวสิทธิมนุษยชนกล่าวแถลงถึงความพ่ายแพ้ของรัฐบาล กรณีนโยบายติดตั้งซอฟต์แวร์เขื่อนสีเขียว (Green Dam) ว่าเป็นสิ่งที่พิสูจน์ให้เห็นว่าอะไรก็เป็นไปได้ถ้าประชาชนผนึกกำลังและมีความพยายาม[51] อย่างไรก็ตาม Ai Wei Wei เห็นว่าการสู้รบในครั้งนี้ยังไม่จบสิ้นง่ายๆ ซึ่งเขากล่าวว่า “ในทางจริยธรรมแล้ว ไม่มีรัฐบาลใดสามารถมีสิทธิบอกว่าสิ่งไหนถูกสิ่งไหนผิด และการกระทำดังกล่าวก็เป็นการทำลายสิทธิของประชาชนในการติดตั้งซอฟแวร์ในเครื่องคอมพิวเตอร์ของตัวเอง”

5.3 บริษัทกูเกิลในประเทศจีน

ในช่วงปี 2010 บริษัทกูเกิลที่ประเทศจีนเดือดร้อนอย่างมากต่อการดำเนินนโยบายด้านอินเทอร์เน็ตของรัฐบาลจีน เพราะ

นอกจากบริษัทต้องคอยรับนโยบายคัดกรองถ้อยคำ และกิจกรรมต่างๆ ที่เกิดขึ้นภายใต้การให้บริการของตนแล้ว รัฐบาลจีนยังมีคำสั่งก้าวล่วงในการบริการจดหมายอิเล็กทรอนิกส์หรือจีเมล (Gmail) ของกูเกิลอีกด้วย โดยรัฐบาลจีนเคยพยายามขัดขวางการให้บริการจีเมลในประเทศจีน โดยขึ้นแสดงบนหน้าจอของผู้ใช้บริการว่า "ไม่สามารถให้บริการได้เนื่องจากมีปัญหาทางเทคนิคของกูเกิล" บริษัทกูเกิลกล่าวว่า "การกระทำของรัฐบาลจีนมีความซับซ้อนสูง และมีการเจาะจงเป้าหมายอย่างชัดเจนกับผู้ใช้บริการ ซึ่งบริษัทเชื่อว่ารัฐบาลจีนพุ่งเป้าโจมตีกลุ่มนักเคลื่อนไหวสิทธิมนุษยชนในจีนที่ใช้บัญชีจีเมลของกูเกิล"[52] อย่างไรก็ตาม กูเกิลพยายามเพิกเฉย และไม่ยอมรับนโยบายการตรวจสอบและปิดกั้นข้อมูลข่าวสารของรัฐบาลจีน ทั้งยังได้ให้สัญญาแก่ลูกค้าที่ไม่ยอมเซ็นเซอร์ตัวเองว่า กูเกิลจะไม่ปิดกั้นหรือเซ็นเซอร์แหล่งข้อมูลของลูกค้าเหล่านั้น และเมื่อมีกรณีที่เว็บไซต์ถูกปิดกั้นอันเป็นผลมาจากโปรแกรมกรองถ้อยคำที่รัฐบาลจีนติดตั้งไว้ กูเกิลก็จะใช้วิธีย้ายเว็บไซต์ที่ให้บริการสืบค้นไปยังเว็บที่เปิดดำเนินการในเขตปกครองพิเศษฮ่องกงแทน และตั้งแต่เดือนมีนาคม ปี 2010 เป็นต้นมา ผู้ใช้บริการอินเทอร์เน็ตในประเทศจีนก็สามารถค้นหาข้อมูลที่ต้องการได้ นอกเหนือจากสิ่งที่ประเทศจีนต้องการปิดกั้น[53] แน่นอนว่า การกระทำดังกล่าวสร้างความไม่พอใจให้กับรัฐบาลจีนยิ่งขึ้น จนมีความพยายามที่จะปิดกั้นกูเกิลในฮ่องกงด้วย และขู่ว่าจะเพิกถอนใบอนุญาตของกูเกิล ในขณะเดียวกันกูเกิลก็ยืนยันว่า หากรัฐบาลจีนยังมีนโยบายตรวจสอบข้อความในการค้นคว้าข้อมูลอยู่ต่อไป กูเกิลก็อาจยุติการดำเนินธุรกิจในประเทศจีนเช่นเดียวกัน[54] อย่างไรก็ตาม ในทางข้อเท็จจริงกลับปรากฏว่ากูเกิลพยายามแสวงหาแนวทางประนีประนอมกับประเทศจีน จนในท้ายที่สุดกูเกิลก็ยินยอมปฏิบัติตามกฎเกณฑ์ที่กำหนดไว้โดยประเทศจีนในปี 2010[55] ดังนั้นวิธีการย้ายการเชื่อมต่อ (redirect) ให้ผู้ใช้อินเทอร์เน็ตในประเทศจีนไปยังฮ่องกงจึงดำเนินการอยู่ได้เพียงไม่นาน และการสืบค้นเว็บไซต์ต่างๆ ในประเทศจีนก็ยังคงถูกตรวจสอบและเซ็นเซอร์อยู่ต่อไป

5.4 การปฏิวัติดอกมะลิ (Jasmine Revolution)

จากแรงบันดาลใจจากเหตุการณ์ประท้วงและเรียกร้องประชาธิปไตยในโลกอาหรับและแอฟริกา ในปี 2011 มีกลุ่มผู้ใช้บริการอินเทอร์เน็ตลงข้อความในเว็บไซต์ Sina Weibo[56] เรียกร้องให้ประชาชนที่อาศัยอยู่ใน 13 เมืองหลักของจีน ประท้วงและเรียกร้องรัฐบาลจีนบ้างภายใต้ชื่อ “Jasmine revolution” การประท้วงดังกล่าวได้กระตุ้นประชาชนจีนให้มีความรับผิดชอบต่ออนาคต และแสดงความคิดเห็นต่อประเด็นที่เร่งด่วนในสังคมประเทศจีน จนส่งผลให้คำว่า “Jasmine“ เป็นภัยคุกคามต่อโลกอินเทอร์เน็ตในสายตารัฐบาลจีนเป็นอย่างมาก จนในที่สุดคำว่า “Jasmine” และ “Wangfujing” (ชื่อย่านจับจ่ายในปักกิ่งซึ่งถูกใช้เป็นจุดรวมตัวในการประท้วง) ก็ถูกลบออกจากสารบบข้อมูลในอินเทอร์เน็ต และประชาชนไม่สามารถค้นหาคำทั้งสองโดยอาศัยเครื่องสืบค้นเว็บไซต์ได้อีก

ภายหลังการการประท้วงครั้งแรก ชาวอินเทอร์เน็ตใน 18 เมืองใหญ่ทั่วประเทศจีนก็ประท้วงอีกเป็นครั้งที่ 2 ภายใต้ชื่อว่าการปฏิวัติดอกมะลิครั้งที่สอง “The Second Jasmine Revolution” ทำให้รัฐบาลต้องเข้มงวดกับเว็บไซต์ที่ให้บริการค้นหาข้อมูลยิ่งขึ้น โดยเฉพาะอย่างยิ่ง ในกรุงปักกิ่งซึ่งมีระดับการการควบคุมสื่อออนไลน์เข้มงวดที่สุด อย่างไรก็ตาม ผู้ใช้อินเทอร์เน็ตส่วนใหญ่แก้ปัญหาด้วยการเผยแพร่หรือส่งต่อเนื้อหาที่มีประเด็นอ่อนไหวต่างๆ ในเว็บไซต์ข่าวที่ไม่โด่งดังมากนักแทน เนื่องจากถูกควบคุมน้อยกว่าโดยฝ่ายปกครองท้องถิ่น

5.5 ปฏิกิริยาอื่น ๆ

ปี 2011 ซึ่งเป็นปีแห่งการต่อสู้ทางการเมืองในหลายทวีปทั่วโลก โดยเฉพาะอย่างยิ่งในโลกอาหรับ ซึ่งมีการใช้อินเทอร์เน็ตเป็นสื่อกลางระหว่างกลุ่มผู้เรียกร้องประชาธิปไตย รวมทั้งจุดชนวนการประท้วงคัดค้านการกระทำต่างๆ ที่ไม่ชอบธรรมของรัฐ รัฐบาลจีนจึงเพิ่มการปิดกั้นการค้นหาคำจากเว็บไซต์สืบค้นข้อมูลในจีน โดยเพิ่มคำต้องห้ามหลายคำอาทิ “อียิปต์” และ “เสรีภาพ” ทั้งนี้ เพื่อหลีกเลี่ยงไม่ให้

ประชาชนจีนได้รับรู้หรืออภิปรายถึงการประท้วงเรียกร้องประชาธิปไตยในประเทศอียิปต์ รัฐบาลจีนยังเผยแพร่บทความในสื่อที่เป็นกระบอกเสียงของรัฐ เพื่อบอกกล่าวแก่ประชาชนของตนว่าเหตุการณ์เหล่านั้นเป็นเหตุการณ์โกลาหลอันเกิดจากความพยายามในการสร้างประชาธิปไตยในประเทศที่ยังไม่มีความพร้อมเพียงพอ

จากกรณีดังกล่าว ศาสตราจารย์ซูซาน แอล เชิร์ค แห่งมหาวิทยาลัยแคลิฟอร์เนียกล่าวว่า "ไม่มีทางเป็นไปได้เลยสำหรับสำนักข่าว ไม่ว่าจะเป็นสำนักข่าวซินหัวหรือสำนักข่าวของประเทศอื่นๆ ที่จะคงความน่าเชื่อถือไว้ได้อีก จากการที่ตนปกปิดข่าวที่ประชาชนสามารถรับรู้ได้จากอินเทอร์เน็ต"[57] ด้านศาสตราจารย์ Xiao Qiung แห่งมหาวิทยาลัยแคลิฟอร์เนีย เบิร์กลีย์ ผู้เชี่ยวชาญด้านการปิดกั้นอินเทอร์เน็ตในประเทศจีน กล่าวว่า "เจ้าหน้าที่ฝ่ายประชาสัมพันธ์ของรัฐบาลได้สั่งสำนักข่าวทั้งหลายและเว็บไซต์ต่างๆ ว่าให้รายงานข่าวสถานการณ์ในประเทศอียิปต์ตามสำนักข่าวซินหัว อย่างไรก็ตาม คำสั่งของรัฐบาลนี้เป็นสิ่งที่ไม่อาจยอมรับได้ของคนหลายกลุ่ม ดังนั้นในบล็อก ห้องอภิปรายในอินเทอร์เน็ต เว็บไซต์ หรือเครือข่ายสังคมออนไลน์จึงมีการติดตามข่าวสารและแลกเปลี่ยนข้อมูลกันและกันอย่างใกล้ชิด เพียงแต่ข้อมูลเหล่านั้นไม่ได้ปรากฏอยู่ในหน้าแรกของเว็บไซต์ที่รัฐบาลจีนจะเห็นได้เท่านั้นเอง"[58] ในขณะที่ Zhao Jing นักเขียนบล็อกชาวจีน กล่าวว่า "เป็นสิ่งน่าอัศจรรย์มากที่ได้เห็นชาวอินเทอร์เน็ตจำนวนมากเป็นห่วงสถานการณ์ในอียิปต์ ถึงขนาดที่มีการนำมาเปรียบเทียบความคล้ายคลึงกันระหว่างการประท้วงที่จตุรัสทาห์รีร์กับจตุรัสเทียนอันเหมิน"[59]

ในช่วงปีนี้ ประเทศจีนยังมีคำสั่งระงับใช้เว็บบล็อกอีกจำนวนมากไว้ชั่วคราว เนื่องจากกลัวการปล่อยข่าวลือต่างๆ ที่จะเป็นผลเสียแก่รัฐบาล โดยเฉพาะอย่างยิ่ง ข่าวลือเรื่องการหากำไรจากการขายโลหิตของสภากาชาดจีน ซึ่งสันนิษฐานว่ามีรัฐบาลอยู่เบื้องหลัง จนกระตุ้นให้เกิดการประท้วงอย่างมากในสื่อออนไลน์ โดยผู้ใช้บริการเว็บไซต์ Weibo ต่างพูดถึงการงดใช้เว็บบล็อกดังกล่าวว่า "คำสั่งที่ส่งถึงพวกเขานั้น เป็นตัวแพร่กระจายข่าวลือได้รวดเร็ว และมีประสิทธิภาพกว่าการลงเนื้อหาโดย

ผู้ใช้บริการเองเสียอีก เพราะผู้ใช้บริการจำนวนไม่น้อยที่ไม่เคยรู้เรื่องราวที่เกิดขึ้นเลย ก็ได้มารู้จากเว็บไซต์ Weibo ที่ประกาศงดให้บริการนั้นเอง" นอกจากนี้ ผู้ใช้บริการเว็บบล็อกจาก Weibo ยังตั้งคำถามต่อบริษัทด้วยว่าทางบริษัทรู้ได้อย่างไรว่าอะไรคือความจริง และอะไรคือความเท็จ

นโยบายเข้มงวดต่างๆ ที่เกิดขึ้นในช่วงหลายปี ไม่ว่าจะเป็นปฏิบัติการปิดกั้นสื่อออนไลน์ การจับกุม คุมขัง และลงโทษผู้ให้และผู้ใช้บริการอินเทอร์เน็ตนั้น สร้างความไม่พอใจอย่างมากให้เกิดขึ้นในหมู่ประชาชนชาวอินเทอร์เน็ตของจีน และกล่าวได้ว่ามันกลายเป็นชนวนที่ทำให้เกิดเหตุการณ์ประท้วงคัดค้าน ซึ่งส่งผลกระทบต่อนโยบายและการทำงานของรัฐบาลจีนหลายๆ เหตุการณ์ด้วย อาทิ ผู้ใช้บล็อกกว่าสิบล้านคนร่วมกันโจมตีการปฏิบัติหน้าที่ของพนักงานรถไฟของรัฐทางอินเทอร์เน็ตหลังจากเหตุการณ์รถไฟชนประชาชนกว่า 40 คนเสียชีวิต บริเวณย่าน Wenzhou โดยกล่าวหาถึงการขาดคุณสมบัติและการคอร์รัปชั่นของพนักงานขับรถไฟ รวมถึงการปิดข่าวสำคัญดังกล่าวไม่ยอมให้ประชาชนจีนได้รับรู้ หรือกรณีที่ผู้อาศัยอยู่ในเมืองต้าเหลียนทางตอนใต้ของจีน ลงรูปเกี่ยวกับโรงงานที่ปล่อยสารเคมีเพื่อเผยแพร่ไปทั่วอินเทอร์เน็ตโดยไม่แยแสว่าจะถูกปิดกั้น จนทำให้รัฐบาลไม่สามารถปิดกั้น หรือลบข้อความได้ทั้งหมดจริงๆ

6. บทสรุป

กล่าวได้ว่าจนถึงปัจจุบัน รัฐบาลจีนก็ยังคงเห็นข้อมูลข่าวสารเป็นเพียงเครื่องมือในการสร้างความชอบธรรมให้แก่พรรคคอมมิวนิสต์และรัฐบาลจีนเท่านั้น ในขณะที่สื่อประเภทต่างๆ โดยเฉพาะอย่างยิ่งสื่อออนไลน์ก็มีไว้เพื่อสร้างความบันเทิงให้กับประชาชน นอกจากนี้ แม้รัฐธรรมนูญจีนจะคุ้มครองให้ประชาชนมีเสรีภาพในการแสดงออกซึ่งความคิดเห็นต่อเรื่องใดๆ ก็ได้ แต่การวิพากษ์วิจารณ์การทำงานของรัฐบาล หรือพรรคคอมมิวนิสต์ถือเป็นสิ่งต้องห้าม โดยการแสดงความคิดเห็นที่ได้รับอนุญาตจะต้องมีลักษณะของการแสดงความจงรักภักดีต่อรัฐบาลจีน เพื่อ

ให้ประเทศมั่นคงไม่วุ่นวายและมีเสถียรภาพ และการแสดงความจงรักภักดีนี้ก็ถูกถือเป็นมาตรฐานทางวิชาชีพที่สำคัญสูงสุดของสื่อมวลชนจีนด้วย[60] ดังนั้น ในระยะกว่าทศวรรษที่ผ่านมา ข้ออ้างเรื่องการรักษาความปลอดภัยของสังคม และเมื่อความมั่นคงของรัฐบาลและประเทศจีน[61] จึงเป็นเหตุผลหลักที่จีนใช้เพื่อควบคุมตรวจสอบพฤติกรรม และจำกัดเสรีภาพในเรื่องนี้ของประชาชน ปิดกั้นสื่อทั้งกระแสหลักและสื่อทางเลือก รวมไปถึงเครื่องมือสืบค้นในอินเทอร์เน็ต

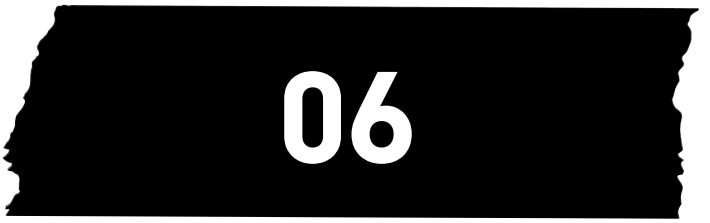
ปัจจุบัน ประเทศจีนจึงมีโครงการขนาดใหญ่จำนวนมากที่ออกแบบมาเพื่อการควบคุมข้อมูลอันไม่พึงปรารถนาโดยเฉพาะ[62] อย่างเกรตไฟร์วอลล์ซึ่งประกอบด้วยกลไกต่างๆ มีการตรากฎหมายเพื่อควบคุมผู้ให้บริการอินเทอร์เน็ตและผู้ใช้อินเทอร์เน็ต การใช้เทคโนโลยีที่ทันสมัยเพื่อให้เจ้าหน้าที่ตำรวจมีอำนาจสูงสุดในการควบคุมการกระทำผิดกฎหมายของจีนอย่างมีประสิทธิภาพโดยให้เจ้าหน้าที่ตำรวจสามารถตรวจสอบผู้ใช้อินเทอร์เน็ตได้มากกว่า 162 ล้านคน หรือการปฏิบัติการทางจิตวิทยาทั้งต่อบริษัทเอกชนผู้ให้บริการอินเทอร์เน็ตที่ประสงค์จะประกอบกิจการในประเทศจีนและต่อประชาชนที่ใช้บริการ ให้ต้องมีความรับผิดชอบต่อสังคม โดยไม่เสนอข้อมูลและทำลายข้อมูลที่เป็นอันตรายต่อประเทศชาติ หากฝ่าฝืนจะถูกลงโทษอย่างร้ายแรง[63]

กล่าวให้ถึงที่สุดแล้ว จึงย่อมเห็นได้ว่า สำหรับประเทศจีนแล้วไม่เพียงแต่การออกกฎหมาย หรือใช้กลไกทางองค์กรตุลาการเท่านั้น แต่รัฐบาลยังพร้อมที่จะทุ่มเททั้งงบประมาณ บุคลากร และเทคโนโลยีเพื่อให้การปิดกั้นสื่อมีประสิทธิภาพยิ่งขึ้นด้วย จนกล่าวได้ว่า ประเทศจีนเป็นประเทศที่มีการพัฒนาระบบเทคโนโลยีเพื่อใช้ปิดกั้นสื่อออนไลน์ที่มีประสิทธิภาพและซับซ้อนที่สุดในโลก

อย่างไรก็ตาม ไม่ว่ารัฐบาลจีนจะใช้ทั้งกฎหมาย มาตรการต่างๆ และดำเนินนโยบายอย่างเข้มข้นเพียงใดเพื่อสกัดกั้นเนื้อหาที่รัฐบาลเห็นว่าเป็นภัยคุกคามตน หรือปิดกั้นอินเทอร์เน็ต แต่จนถึงปัจจุบันก็ยังมีประชาชนชาวจีนที่ใช้บริการบล็อกอยู่กว่า 70 ล้านคน และจำนวนไม่น้อยที่เขียนบล็อก

ไปในเชิงวิพากษ์วิจารณ์ และแสดงความคิดเห็นต่อการกระทำของรัฐบาลและผู้นำจีน ซึ่งย่อมสะท้อนให้เห็นว่า ประชาชนจีนสมัยใหม่ได้ได้สยบยอมกับนโยบายปิดกั้นความคิดเห็นของรัฐบาลจีนอีกต่อไปแล้ว Guobin Yang นักเขียนอิสระผู้แต่งหนังสือ “The Power of the Internet in China: Citizen Activism Online” เคยให้ความเห็นไว้ครั้งหนึ่งว่า แม้ในขณะนี้จะยังไม่มีการปฏิวัติทางการเมือง แต่ประเทศจีนกำลังประสบกับการปฏิวัติทางการสื่อสารซึ่งเป็นการแผ่ขยายประชาธิปไตยอย่างไม่เป็นทางการของประชาชน ไม่ว่าประเทศจีนจะมีการตรวจสอบและการตรวจตราเข้มงวดเพียงใด แต่อินเทอร์เน็ตในประเทศจีนก็ยังเป็นพื้นที่สำคัญของการถกเถียงอย่างดุเดือดร้อนแรง สนุกสนานและมีชีวิตชีวา เป็นช่องทางที่ทำให้ประชาชนจีนได้แสดงความคิดเห็นของตน จนหลายๆ ครั้งทำให้เจ้าหน้าที่เกี่ยวข้องกับการคอร์รัปชั่นต้องออกจากตำแหน่ง ดังนั้น อินเทอร์เน็ตจึงมีอิทธิพลต่อรัฐบาลด้วย Guobin Yang เห็นว่า แม้องค์กรภาคประชาชนในประเทศจีนจะดำรงอยู่และเติบโตได้อย่างยากลำบาก เนื่องจากข้อจำกัดทางการเมือง แต่ก็ยังปรากฏว่าองค์กรใหม่ๆ หลายองค์กรใช้อินเทอร์เน็ตเป็นเครื่องมือสร้างความตระหนักในเหตุการณ์บ้านเมืองต่างๆ ที่เกิดขึ้นให้อยู่ในความสนใจของประชาชนทั่วไปได้ เช่นกรณีที่นักศึกษาและผู้ปกครองใช้อินเทอร์เน็ตเพื่อสร้างความตระหนักเกี่ยวกับการเลือกปฏิบัติต่อนักศึกษาที่เป็นโรคเบาหวานในระดับมหาวิทยาลัย เป็นต้น และการที่วัฒนธรรมอินเทอร์เน็ตในประเทศจีนมีลักษณะดังกล่าว ก็เนื่องมาจากอิทธิพลจากประเพณีดั้งเดิมในการประท้วงของสังคมในประวัติศาสตร์ประเทศจีนตลอดมานั่นเอง[64]

บทที่



กฎหมายมาเลเซีย
กับสิทธิเสรีภาพในสื่อออนไลน์

กฎหมายมาเลเซียกับสิทธิเสรีภาพในสื่อออนไลน์

ประเทศมาเลเซียเป็นประเทศหนึ่งในทวีปเอเชียตะวันออกเฉียงใต้ นอกเหนือจากประเทศอินโดนีเซีย ประเทศพม่า รวมทั้งประเทศไทย ที่มีประวัติอันยาวนานเกี่ยวกับการตรวจสอบและควบคุมสื่อโดยฝ่ายผู้ปกครองรัฐ ซึ่งหลายกรณีเป็นลักษณะของการควบคุม แทรกแซงการทำงาน กระทั่งคุกคามสื่อประเภทใดๆ ก็ตามที่แสดงข้อมูลที่มีเนื้อหาในเชิงปฏิปักษ์ หรืออยู่ฝ่ายตรงข้ามกับรัฐบาล ทั้งนี้ ได้ปรากฏว่าประเทศมาเลเซียมีกฎหมายหลายฉบับที่มักถูกใช้บังคับ โดยตีความให้ขยายออกไปจนกว้างขวาง ผู้ให้บริการสื่อจำนวนไม่น้อยถูกจับกุม และจำคุกเพียงเพราะเหตุที่นำเสนอข้อมูลในเชิงวิพากษ์วิจารณ์การทำงานของรัฐบาลหรือระบอบการปกครอง ส่งผลให้เสรีภาพในการแสดงความคิดเห็นของประชาชนถูกจำกัดลง ในขณะที่เสรีภาพในการเสนอข้อมูลข่าวสารก็ต้องถูกตรวจสอบ

1. การคุ้มครองเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นตามรัฐธรรมนูญมาเลเซีย

เสรีภาพในการพูดและการแสดงความคิดเห็นในประเทศมาเลเซียมีฐานคิดมาจากยุคการปฏิวัติโคราณิค (Koranic Revelation)[1] หาใช่ได้รับอิทธิพลมาจากประเทศในซีกโลกตะวันตกแต่อย่างใดไม่ นักคิดมาเลเซียต่างกล่าวกันว่า "ข้อความคิดในเรื่องเสรีภาพในการพูด" (the concept of free speech) เกี่ยวพันใกล้ชิดกับคำสอนของศาสนาอิสลาม และด้วยเหตุที่ศาสนาอิสลามเป็นศาสนาประจำชาติของประเทศมาเลเซีย[2] จึงทำให้โดยพื้นฐานแล้วคนมาเลเซียไม่ได้เป็นศัตรูกับเสรีภาพในการแสดงความคิดเห็น นักวิชาการอิสลามเคยให้ความเห็นไว้ทำนองว่า เหตุผลของมนุษย์ ย่อมเป็นอิสระจากคำแนะนำของพระเจ้า และคำแนะนำดังกล่าวก็ไม่ได้เป็นแรงบันดาลใจที่เพียงพอในการวางแผนชีวิตที่ดีที่สุดของมนุษย์ ดังนั้นสิทธิในการแสดงออกทางความคิดเห็น คำพูด และการเขียนจึงเป็นหนึ่งในสิทธิขั้นพื้นฐานของพลเมืองของรัฐอิสลาม[3] Mohammad Hashim Kamali ศาสตราจารย์กฎหมาย ณ มหาวิทยาลัยอิสลามสากล ประเทศมาเลเซีย กล่าวว่าเสรีภาพในการพูดเป็นเรื่องของการแสวงหาความจริงของมนุษย์ [4]

อย่างไรก็ตาม ในโลกอิสลามนั้น เสรีภาพในการพูด หรือการแสดงความคิดเห็นหาได้เป็นเสรีภาพแบบไร้ขอบเขตจำกัดไม่ พระคัมภีร์อัลกุรอ่านบทที่ 12 a ของ Universal Islamic Declaration ระบุข้อจำกัดดังกล่าวไว้ [5] ว่า

"ทุกคนมีเสรีภาพในการแสดงความคิด และความเชื่อของเขาตราบเท่าที่ยังคงอยู่ภายในขอบเขตที่กฎหมายกำหนด ไม่มีใครที่จะสามารถเผยแพร่ความเท็จ หรือเผยแพร่รายงานเพื่อทำลายความเรียบร้อยของประชาชน หรือใส่ร้าย เสียดสี หรือเพื่อทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง" [6]

ในขณะที่บทที่ 12 c เขียนไว้ว่า

"ถือเป็นสิทธิและหน้าที่ของคนมุสลิมทุกคนที่จะประท้วงต่อสู้ และพยายาม (ภายในขอบเขตที่กำหนดไว้โดยกฎหมาย) แม้จะเกี่ยวข้องกับ

การท้าทายอำนาจสูงสุดในรัฐ" [7]

และเป็นเช่นเดียวกันกับรัฐธรรมนูญของนานาประเทศ รัฐธรรมนูญประเทศมาเลเซีย ไม่ได้เขียนรับรองไว้เฉพาะแต่ "สิทธิความเป็นส่วนตัว" เท่านั้น หากแต่ยังให้การรับรองสิทธิอื่นๆ อีกหลายประการที่เกี่ยวข้อง ทั้งนี้ เพื่อเป็นหลักประกันให้กับพลเมืองของมาเลเซีย เสรีภาพในการพูด เสรีภาพในการรวมกลุ่ม และเสรีภาพในการจัดตั้งกลุ่ม หรือสมาคม ได้รับความคุ้มครองตาม มาตรา 10 แห่งรัฐธรรมนูญมาเลเซีย (The Constitution of Malaysia) ซึ่งบัญญัติว่า

"(1) ภายใต้ข้อ (2), (3) และ (4)

(a) ประชาชนทุกคนมีสิทธิและเสรีภาพในการพูดและการแสดงออก

(b) ประชาชนทุกคนมีสิทธิในการชุมนุมโดยสงบและปราศจากอาวุธ

(c) ประชาชนทุกคนมีสิทธิที่จะรวมกันก่อตั้งสมาคม

(2) รัฐสภาโดยกฎหมายกำหนด

(a) สิทธิตาม (a) ของข้อ (1) อาจถูกจำกัดได้ถ้าจำเป็นหรือเห็นสมควรเพื่อผลประโยชน์และความมั่นคงปลอดภัยของรัฐส่วนหนึ่งส่วนใด เพื่อความสัมพันธ์ฉันท์มิตรกับประเทศอื่นๆ เพื่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน หรือเพื่อปกป้องสิทธิของรัฐสภาหรือสภานิติบัญญัติ หรือการหมิ่นศาล การหมิ่นประมาททำให้เสื่อมเสียชื่อเสียง หรือการยั่วยุให้เกิดความผิดใดๆ ขึ้น..."

จะเห็นได้ว่า รัฐธรรมนูญมาเลเซียไม่ได้แตกต่างไปจากรัฐธรรมนูญแห่งราชอาณาจักรไทย (มาตรา 45) กล่าวคือ แม้มาตรา 10 (1) (a) จะบัญญัติรับรองเสรีภาพในการพูด และแสดงออกไว้แล้วโดยชัดแจ้งก็ตาม แต่ลักษณะการคุ้มครองเสรีภาพประเภทนี้ไม่ได้เป็นไปโดย "เด็ดขาด" ที่รัฐจะจำกัดตัดทอนไม่ได้เลย (อย่างเสรีภาพในการคิดหรือศรัทธาความเชื่อ) หากแต่เป็นเสรีภาพที่ได้รับการคุ้มครองแบบ "สัมพัทธ์" เท่านั้น ซึ่งรัฐสามารถออกกฎหมายภายใต้เงื่อนไขบางอย่างเพื่อจำกัดเสรีภาพประเภทนี้ได้ มาตรา

10 (2) (a) กำหนดข้อยกเว้น ให้รัฐสภาออกกฎหมายเพื่อจำกัดเสรีภาพในการพูดและการแสดงความคิดเห็นได้ด้วยเหตุผลหลายประการ คือ

1) เพื่อผลประโยชน์และความมั่นคงปลอดภัยของรัฐ

2) เพื่อความสัมพันธ์ฉันท์มิตรกับประเทศอื่นๆ

3) เพื่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน

4) เพื่อปกป้องสิทธิของรัฐสภา หรือสภานิติบัญญัติ และ

5) หมิ่นศาล หมิ่นประมาท หรือยั่วยุให้เกิดความผิดใดๆ ขึ้น

และ ภายหลังเหตุการณ์จลาจลครั้งใหญ่ในประเทศมาเลเซียเดือนพฤษภาคม ปี 1969 ฝ่ายนิติบัญญัติได้ทำการแก้ไขรัฐธรรมนูญ มาตรา 10 โดยเพิ่มคำสั่งใหม่เป็นมาตรา 10 (4)[8] ให้อำนาจรัฐสั่งห้ามประชาชนพูดคุยแลกเปลี่ยนกันในประเด็นอ่อนไหวต่างๆ อาทิ เรื่องที่เกี่ยวกับสิทธิพิเศษของคนเชื้อชาติมาเลย์ ภาษาประจำชาติ สถานะขององค์สุลต่าน หรือสิทธิพลเมืองของคนที่ไม่มีสัญชาติมาเลเซีย เป็นต้น ซึ่งส่งผลให้รัฐบาลใช้มาตรการสอดส่อง และควบคุมการแสดงความคิดเห็นของประชาชนอย่างเข้มงวดมากยิ่งขึ้น นอกจากนี้ ตามรัฐธรรมนูญมาเลเซียนั้น เสรีภาพต่างๆ ตามมาตรา 10 ยังอาจถูกยกเว้นได้อีกภายใต้สถานการณ์พิเศษ ซึ่งบัญญัติไว้ในมาตรา 149 และมาตรา 150 หมวดที่ว่าด้วยเรื่องในระหว่างที่รัฐตกอยู่ภายใต้สถานการณ์ฉุกเฉิน (Part XI – Special Powers Against Subversion, Organised Violence, and Acts and Crimes Prejudicial to the Public and Emergency Powers) ซึ่งฝ่ายบริหารมีอำนาจในการออกกฎหมายได้ แม้ว่ากฎหมายนั้นจะขัดหรือแย้งกับบทบัญญัติในรัฐธรรมนูญก็ตาม

ที่ผ่านมารัฐสภามาเลเซียตรากฎหมายจำนวนหนึ่งซึ่งมีบทบัญญัติให้อำนาจรัฐสามารถควบคุมการเผยแพร่ข่าวสาร หรือกำกับการเสนอข่าวของสื่อสารมวลชนในระดับต่างๆ ได้ กฎหมายฉบับที่สำคัญๆ ได้แก่ พระราชบัญญัติความลับราชการ (Official Secrets Act 1972) ที่ถูกตราขึ้นจากผลของเหตุการณ์จลาจล เมื่อเดือนพฤษภาคม ปี 1969 กำหนดให้การเผยแพร่ข้อมูลความลับของทางราชการ หรือความลับเกี่ยวกับการตัดสินใจที่สำคัญของรัฐบาลเป็นความผิดและมีโทษ ซึ่งปรากฏว่านักข่าวและ

นักการเมืองฝ่ายค้านหลายคนถูกจับกุมโดยกฎหมายฉบับนี้ พระราชบัญญัติว่าด้วยการยั่วยุปลุกระดม (Sedition Act 1948) ที่กำหนดข้อจำกัดการพูดและการแสดงความคิดเห็นในประเด็นต่างๆ อย่างเรื่องความเชื่อ เชื้อชาติ หรือศาสนา ที่อาจทำให้เกิดความขัดแย้งในระหว่างชนชั้น และชาติพันธุ์ ทั้งยังมีการบัญญัติถ้อยคำว่า “มีแนวโน้มในการก่อความไม่สงบ” เพิ่มเติมในส่วนองค์ประกอบของความผิด ทำให้การบังคับใช้เป็นไปอย่างกว้างขวางและมีบทลงโทษทั้งปรับและจำคุก พระราชบัญญัติการพิมพ์และสิ่งพิมพ์ (Printing Presses and Publications Act 1948) ซึ่งกำหนดให้ผู้ประกอบกิจการการพิมพ์ทุกประเภท ต้องขออนุญาตจากกระทรวงมหาดไทย ใบอนุญาตต้องต่ออายุเป็นรายปี ทั้งนี้ กระทรวงมหาดไทยสามารถระงับการพิมพ์ หรือห้ามจำหน่ายสิ่งพิมพ์ที่ขัดต่อความสงบเรียบร้อยและศีลธรรมของประชาชนได้ และที่สำคัญก็คือ พระราชบัญญัติความมั่นคงภายใน (Internal Security Act 1960 หรือ ISA) ซึ่งเป็นกฎหมายป้องกันภัยที่จะมีมาแก่รัฐ หรือรัฐบาลซึ่งมีบทบัญญัติที่ส่งผลกระทบต่อเสรีภาพในการพูดและแสดงความความคิดเห็นของประชาชนด้วย โดยกฎหมายฉบับนี้ให้อำนาจกระทรวงมหาดไทยดำเนินการต่างๆ ได้โดยไม่ต้องผ่านกระบวนการทางศาล ไม่ว่าจะเป็นการตั้งข้อหา หรือกระทั่งการควบคุมตัวบุคคลที่รัฐบาลเชื่อว่ากระทำการอันเป็นปฏิปักษ์ต่อรัฐบาล หรือแม้แต่ความผิดในฐานหมิ่นประมาทของประเทศมาเลเซีย ซึ่งยังมีโทษทางอาญาอยู่ ก็ถูกนำมาใช้เป็นเครื่องมือในการปิดกั้นการแสดงความคิดเห็นของฝ่ายตรงข้ามทางการเมืองอยู่เสมอ

ในสถานการณ์ปรกตินั้น แม้รัฐสภาจะสามารถตรากฎหมายเพื่อจำกัดเสรีภาพของประชาชนได้ภายใต้เงื่อนไขของรัฐธรรมนูญเอง แต่มิได้หมายความว่ารัฐสภาจะดำเนินการได้อย่างอิสระปราศจากการควบคุมตรวจสอบจากฝ่ายตุลาการ ทั้งนี้ เพราะอำนาจการออกกฎหมายมาจำกัดเสรีภาพตามมาตรา 10 (2) (a) นั้น ในที่สุดแล้วจะต้องถูกพิจารณาโดยคณะกรรมการ Reid (Reid Commission) เพื่อรับรองว่าเป็นสิ่งที่สามารถกระทำได้ตามรัฐธรรมนูญจริงหรือไม่ และโดยที่ศาลต้องยอมรับ ดังนั้น หากรัฐสภาพยายามออกกฎหมายจำกัดเสรีภาพของประชาชนโดยมีเนื้อหา

เกินเลยไปจากเงื่อนไขที่ปรากฏอยู่ในรัฐธรรมนูญ ศาลสามารถเพิกถอนกฎหมายดังกล่าวได้ ด้วยเหตุผลว่าขัดต่อรัฐธรรมนูญ เพื่อให้ประชาชนมั่นใจได้ว่าสิทธิเสรีภาพจะถูกจำกัดอยู่ภายในขอบเขตที่เหมาะสมเท่านั้น อย่างไรก็ตาม ในความเป็นจริง แม้รัฐธรรมนูญมาเลเซียจะบัญญัติคุ้มครองเสรีภาพในการแสดงความคิดเห็นของประชาชนไว้ แต่เมื่อใดก็ตามที่มีการควบคุมเสรีภาพดังกล่าวเกิดขึ้น “สิทธิ” ของฝ่ายผู้เสียหาย หรือผู้ถูกจำกัดเสรีภาพก็จะไม่ได้รับการกล่าวถึงเลย โดยเฉพาะอย่างยิ่งในประเด็นที่ว่า เขาเหล่านั้นจะสามารถเรียกร้องความเป็นธรรมได้จากที่ใด ซึ่งสอดคล้องกับคำบอกเล่าของสตีเวน กัน (Steven Gan) บรรณาธิการบริหาร และหนึ่งในสองผู้ก่อตั้งมาเลเซียกินี[9] ที่ว่า

“In Malaysia, we have freedom of speech. But not freedom after speech.” (ในมาเลเซียนั้น พลเมืองของเรามีสิทธิเสรีภาพในการพูดหรือแสดงความคิดเห็น แต่สิ่งที่ไม่มีก็คือ สิทธิเสรีภาพ-ภายหลัง-จากที่ได้พูดหรือแสดงความคิดเห็นไปแล้ว)[10]

กล่าวโดยสรุป เสรีภาพในการพูด และการแสดงความคิดเห็นในประเทศมาเลเซียนั้นได้รับความคุ้มครองอย่างจำกัดมากในทางความเป็นจริง เนื่องเพราะมีกฎหมายจำนวนไม่น้อยที่รัฐออกมาโดยมุ่งหมายเพื่อจำกัดเสรีภาพในการแสดงความคิดเห็น หรือแม้ไม่ได้มีเป้าประสงค์ดังกล่าวโดยตรง แต่ก็มักถูกนำมาบังคับใช้เพื่อการจำกัดสิทธิ หรือคุกคามผู้แสดงออกทางความคิดเห็น โดยเฉพาะอย่างยิ่งความคิดเห็นในทางการเมือง ในช่วงเวลาที่ผ่านมา นอกจากสื่อประเภทเดิมๆ อย่างหนังสือพิมพ์ นิตยสาร วิทยุ โทรทัศน์ ที่ถูกควบคุม หรือแทรกแซงมาอยู่ก่อนแล้ว ผู้ประกอบการสื่อออนไลน์อย่างเจ้าของเว็บข่าวออนไลน์ เช่น NutGraph Malaysia Insider และ Malaysiakini หรือบล็อกเกอร์ (Blogger) เช่น Articulations, Zorro unmasked, People’s Parliament และ Malaysia Today ซึ่งเติบโตและได้รับความนิยมอย่างมากในประเทศมาเลเซีย เพราะประชาชนเริ่มหันมาเชื่อถือในสื่อทางเลือกเหล่านี้มากกว่าสื่อกระแสหลัก

รวมทั้งนักข่าวออนไลน์จำนวนมากก็ถูกคุกคาม จับกุม และดำเนินคดีจากฝ่ายรัฐเช่นเดียวกัน

2. เนื้อหาต้องห้ามมิให้เผยแพร่ในสื่อสาธารณะตามกฎหมายมาเลเซีย

ในประเด็นการจัดการเนื้อหาในสื่ออินเทอร์เน็ตนั้น แม้ประเทศมาเลเซียจะเป็นประเทศแรกๆ ในทวีปเอเชียตะวันออกเฉียงใต้ ที่มีพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ (Computer Crime Act 1997) ใช้บังคับ แต่กฎหมายฉบับนี้กำหนดเฉพาะฐานความผิดที่ว่าด้วย “อาชญากรรมคอมพิวเตอร์โดยแท้” หรือความผิดที่อาชญากรอาศัยความรู้ความสามารถด้านเทคโนโลยีคอมพิวเตอร์กระทำต่อตัวระบบ หรือข้อมูลคอมพิวเตอร์ เช่น การเข้าถึงระบบหรือข้อมูลโดยมิชอบด้วยกฎหมาย การจารกรรมหรือดักรับข้อมูลของผู้อื่น การก่อวินาศกรรมคอมพิวเตอร์เท่านั้น ไม่มีบทมาตราใดที่กำหนดฐานความผิดเกี่ยวกับการเผยแพร่เนื้อหาไม่เหมาะสม หรือผิดกฎหมาย รวมทั้งไม่มีมาตราที่กำหนดให้อำนาจรัฐในการระงับการเผยแพร่ข้อมูลเหล่านั้นไว้โดยเฉพาะแบบที่ปรากฏในพ.ร.บ. คอมพิวเตอร์ฯ 2550 ของประเทศไทย อย่างไรก็ตาม การเผยแพร่ข้อมูลที่มีเนื้อหาบางประเภท อาทิ สิ่งลามกอนาจารเด็ก ข้อความหมิ่นประมาทบุคคลอื่น สิ่งที่ละเมิดทรัพย์สินทางปัญญา หรือเนื้อหาที่มีลักษณะยั่วยุปลุกระดม ผู้ผลิต หรือเผยแพร่เนื้อหาเหล่านี้ย่อมมีความเสี่ยงที่จะต้องรับผิดในทางแพ่ง หรือทางอาญา ตามฐานความผิดที่มีอยู่แล้วในกฎหมายฉบับต่างๆ

สำหรับการใช้มาตรการเซ็นเซอร์สื่อนั้น เป็นที่ทราบอยู่แล้วว่าประเทศมาเลเซียมีประวัติอันยาวนานว่าเป็นประเทศที่รัฐใช้มาตรการเซ็นเซอร์ แทรกแซง และตรวจสอบสื่ออย่างเคร่งครัด นอกเหนือจากสื่อดั้งเดิมรายใหญ่ ซึ่งมักมีความสัมพันธ์ใกล้ชิด ทั้งยังนำเสนอข่าวสนับสนุนฝ่ายรัฐบาลแล้ว สื่อทางเลือกหรือสื่อฝ่ายตรงข้ามต่างก็โดนตรวจสอบควบคุม ผ่านวิธีการจับกุม คุกคาม กระทั่งควบคุมตัว หรือจำคุกผู้สื่อข่าวหรือผู้เขียนบทความเชิงวิพากษ์วิจารณ์การทำงานของรัฐบาล อนึ่ง นับ

เป็นเรื่องน่าสนใจอย่างยิ่งที่ว่า ข้อความคิดที่เกี่ยวกับเสรีภาพในการแสดงความคิดเห็นในประเทศมาเลเซีย มีต้นกำเนิดสำคัญมาจากศาสนาอิสลาม ตามที่กล่าวถึงไปแล้วตอนต้น แต่ขอบเขตของการแสดงความคิดเห็นที่ควรได้รับเสรีภาพอย่างเต็มที่ในสายตาของศาสนาอิสลาม อาจหมายเฉพาะการแสดงความคิดเห็นที่เกี่ยวกับสิทธิ การกำหนดตนเองในทางการเมือง การปกครอง รวมทั้งการวิพากษ์วิจารณ์รัฐบาลหรือผู้ปกครองรัฐเท่านั้น มิได้หมายรวมไปถึงเรื่องอื่นๆ ด้วย โดยเฉพาะอย่างยิ่งประเด็นที่มีความเกี่ยวพันกับความเชื่อทางศาสนาเอง ทั้งนี้เพราะปรากฏว่า เนื้อหาประเภทอื่นๆ ซึ่งถือเป็นเรื่องต้องห้าม และรัฐควรปิดกั้นทั้งตามกฎหมาย และตามแนวทางในการเซ็นเซอร์ของประเทศมาเลเซีย (Malaysia's censorship guidelines) ล้วนมีสาเหตุส่วนหนึ่งมาจากเรื่องต้องห้ามของศาสนาอิสลามสายอนุรักษ์นิยมในประเทศมาเลเซียนั่นเอง

ในประเทศมาเลเซีย ฉากในละครหรือภาพยนตร์ที่แสดงเพียงการกอดจูบก็จะต้องถูกเซ็นเซอร์ในขณะที่ฉากเปลือยกายหรือมีเพศสัมพันธ์จะถูกตัดออก โดยเฉพาะอย่างยิ่งไม่ว่าในสื่อใดๆ หากมีการนำเสนอเนื้อหาที่มีความรุนแรง มีเรื่องของการดูหมิ่น หรือเรื่องอ่อนไหวต่างๆ ที่เกี่ยวกับความเชื่อทางศาสนาอิสลามจะถูกต้องห้ามโดยเด็ดขาด

สำหรับสื่อใหม่อย่างอินเทอร์เน็ต ประเทศมาเลเซียเคยให้การรับรองอย่างเป็นทางการว่า รัฐจะไม่ใช้มาตรการเซ็นเซอร์เนื้อหาในอินเทอร์เน็ต และรัฐบาลมีโอกาสที่จะถูกประชาชนฟ้องร้องได้หากมีการควบคุม หรือกลั่นกรองเว็บไซต์ที่มีเนื้อหาเกี่ยวกับการเมือง บทบัญญัติใดๆ ก็ตามที่ออกมาเพื่อการเหนี่ยวรั้งเสรีภาพในอินเทอร์เน็ต โดยทางทฤษฎีแล้ว ถือว่าขัดกับพระราชบัญญัติมัลติมิเดีย (The Multimedia Act) ที่มีผลใช้บังคับตั้งแต่ปี 1990 ปัจจุบัน บทบัญญัติลายลักษณ์อักษรที่รับรองการไม่เซ็นเซอร์อินเทอร์เน็ตปรากฏอยู่ที่ มาตรา 3 (3) แห่งพระราชบัญญัติการสื่อสารและมัลติมีเดีย ปี 1998 (The Communications and Multimedia Act (CMA) Article 3 (3) "... Nothing in this Act shall be construed as permitting the censorship of the Internet.") อย่างไร

ก็ตาม ในความเป็นจริงปรากฏว่า มาตรการควบคุมเนื้อหาที่รัฐบาลใช้กับสื่อดั้งเดิมอย่างทีวี หรือวิทยุ ก็ยังคงถูกนำมาใช้กับอินเทอร์เน็ตอยู่ตลอดมา เพียงแต่มีการปรับเปลี่ยนรูปแบบและวิธีการไป จนนำไปสู่ปัญหาการ “เซ็นเซอร์ตัวเอง” (self-censorship) ของผู้ให้บริการสื่อออนไลน์ ทั้งนี้ มีรายงานว่า แม้ที่ผ่านมาจะไม่พบพยานหลักฐานที่แสดงได้ว่ารัฐใช้เครื่องมือทางเทคนิคควบคุม ตรวจสอบ หรือกรองเนื้อหาอินเทอร์เน็ตก็ตาม แต่ก็พบว่ารัฐคุกคาม ทำร้ายบล็อกเกอร์ และสื่อพลเมืองจำนวนมากที่นำเสนอข่าวสารในทางตรงข้าม หรือเป็นปฏิปักษ์กับรัฐ รวมทั้งคอยตรวจสอบเนื้อหาในเว็บไซต์ที่เสนอข่าวแตกต่างจากที่รัฐต้องการ[11]

ปัจจุบัน ประเทศมาเลเซียมีกฎหมายที่กำหนดนโยบาย และแนวทางการประกอบกิจการสื่อสารโทรคมนาคม รวมทั้งควบคุมเนื้อหาและการสื่อสารในสื่อออนไลน์บังคับใช้โดยเฉพาะ คือ พระราชบัญญัติการสื่อสารและมัลติมิเดีย (The Communications and Multimedia Act of 1998 - CMA) และพระราชบัญญัติคณะกรรมการการสื่อสารและมัลติมีเดีย (The Communications and Multimedia Commission Act of 1998 – CMCA) โดย CMCA เป็นกฎหมายให้คณะกรรมการฯ มีอำนาจวางนโยบายหรือออกบทบัญญัติสำหรับควบคุมอุตสาหกรรมเทคโนโลยีสารสนเทศ และการสื่อสาร คณะกรรมการฯ ชุดนี้ จะมีบทบาทในการจัดการและควบคุมเนื้อหาในอินเทอร์เน็ตในเรื่องที่เกี่ยวกับ “เหตุผลในการเข้าถึง พื้นที่ส่วนตัว ความปลอดภัย และการคุ้มครองสิทธิส่วนบุคคล”[12] รวมทั้งกำหนดหลักเกณฑ์สำหรับการค้นหาข้อมูลทางคอมพิวเตอร์ และการเข้าถึงข้อมูลที่มีการใส่รหัสป้องกันการเข้าถึงไว้ ทั้งเจ้าหน้าที่ตำรวจยังสามารถขัดขวางการสื่อสารที่ไม่ชอบด้วยกฎหมายใดๆ ได้ โดยไม่ต้องมีใบอนุญาต หากเชื่อว่าการสื่อสารนั้นมีข้อมูลที่เกี่ยวข้องกับเรื่องที่กำลังสืบสวนสอบสวนอยู่

ในขณะที่ CMA เป็นกฎหมายที่ให้อำนาจคณะกรรมการฯ อีกชุดหนึ่งในการควบคุมการพูดออนไลน์ เพื่อไม่ให้ผู้ให้บริการหรือบุคคลอื่นใดให้หรือใช้บริการเนื้อหาที่ไม่เหมาะสม ลามกอนาจาร เป็นเท็จ เป็นอันตราย ล่วงละเมิด ก่อกวน หรือคุกคามบุคคลอื่น (มาตรา 211)[13] โดย

มาตรฐานหรือตัวชี้วัดว่าเนื้อหาใดไม่สามารถเผยแพร่ได้จะต้องพิจารณาโดยคำนึงถึงบริบททางสังคม ศาสนา ทัศนคติทางการเมือง การศึกษา รวมทั้งความจำเป็นที่ต้องรับรองความต้องการที่แตกต่างหลากหลายในโลกที่ไร้พรมแดนนี้ด้วย ทั้งนี้ ประเทศมาเลเซียกำหนดหลักเกณฑ์และวิธีการในเรื่องของการเผยแพร่ข้อมูลเนื้อหาในอินเทอร์เน็ตออกมาในรูปของ “แนวปฏิบัติเกี่ยวกับเนื้อหา” (Guidelines on Content) สำหรับผู้ประกอบการ ซึ่งมีเนื้อหาที่สอดคล้องกับ CMA เพื่อใช้เป็นมาตรฐานร่วมกัน และทำให้การปฏิบัติตามกฎหมายเกิดขึ้นจริง โดยผ่านระบบหรือกลไกการควบคุมกันเอง (self-regulation) ซึ่ง The Content Code[14] มีสาระสำคัญว่าด้วยเนื้อหาที่ต้องห้าม ควรหลีกเลี่ยง หรือระมัดระวังในการเผยแพร่ ดังนี้

2.1 เนื้อหาไม่เหมาะสม (Indecent Content)

คือ เนื้อหาที่มีเรื่องราวที่ไม่เหมาะสมทางศีลธรรม หรือไม่สอดคล้องกับมาตรฐานพฤติกรรมที่ยอมรับกันในสังคม ในที่นี้หมายรวมถึงภาพเปลือยและเรื่องที่เกี่ยวกับเพศ ทั้งนี้ ภาพโป๊เปลือย และเรื่องทางเพศห้ามมิให้แสดงไม่ว่าในสถานการณ์ใดๆ เว้นแต่ได้รับอนุมัติจากคณะกรรมการเซ็นเซอร์ภาพยนตร์ (The Film Censorship Board)

2.2 เนื้อหาลามก (Obscene Content)

ซึ่งมีลักษณะที่ก่อให้เกิดความรู้สึกน่ารังเกียจ ไม่เหมาะสม มีอิทธิพลในเชิงลบและบ่อนทำลายจิตใจ โดยวิธีการตรวจสอบว่าเป็นเนื้อหาที่ลามกหรือไม่ คือ การพิจารณาว่า เนื้อหานั้นน้อมนำไปในทางเสื่อมทรามทางจิตใจ หรือทำความเสียหายให้กับความรู้สึกของผู้พบเห็นหรือไม่ โดยเฉพาะอย่างยิ่ง การแสดงกิจกรรมในทางเพศอย่างชัดแจ้ง แสดงการร่วมประเวณีไม่ว่าจะยอมหรือไม่ยอม เนื้อหาที่มีลักษณะลดเกียรติบุคคลอื่นด้วยการทำให้บุคคลกลายเป็นเพียง “วัตถุในทางเพศ” ภาพลามกเด็ก กิจกรรมในทางเพศกับเด็ก หรือแม้แต่การแสดงอวัยวะส่วนหนึ่งส่วนใดของเด็กในลักษณะหรือบริบทที่เกี่ยวกับเรื่องในทางเพศ ซึ่งกรณีของ

ภาพลามกเด็กนั้นจะถูกห้ามเผยแพร่อย่างเคร่งครัด

2.3 เนื้อหาที่แสดงความรุนแรง (Violent Content)

เนื้อหาความรุนแรงมีอยู่หลายระดับ อาทิ ความรุนแรงที่เกิดจากภัยพิบัติทางธรรมชาติ การก่อการร้าย สงคราม ความขัดแย้งระหว่างมนุษย์ ไม่ว่าการนำเสนอจะมีรูปแบบอย่างไร นำเสนอผ่านเรื่องจริง ผ่านเรื่องสร้างนวนิยาย การ์ตูน กีฬา ฯลฯ ที่สะท้อนถึงความรุนแรงได้ เรื่องราวที่ก่อให้เกิดความรุนแรงต่อจิตใจ ความรุนแรงทางกายภาพ โดยเฉพาะอย่างยิ่งการยั่วยุให้เกิดการใช้ความรุนแรง การแสดงถึงความทารุณโหดร้าย ป่าเถื่อน ความทุกข์ทรมาน ฯลฯ ทั้งนี้ เนื้อหาบางประเภท จะต้องควบคุมอย่างเข้มงวด ในกรณีที่เด็กและเยาวชนอาจเห็นได้ อาทิ ความก้าวร้าวรุนแรงไม่ว่าต่อกายหรือใจ ที่สามารถกระตุ้น ปลุกเร้าให้ผู้ชมเกิดความหวาดกลัวเกินควร หรือส่งเสริมให้เกิดการเลียนแบบ

อนึ่ง ประเทศมาเลเซียไม่ได้ห้ามนำเสนอความรุนแรงในทุกๆ เรื่อง หรือทุกๆ กรณี การนำเสนอสามารถทำได้โดยเฉพาะอย่างยิ่งการนำเสนอภาพความรุนแรงในบริบทของการนำเสนอข่าวสาร การวิเคราะห์สถานการณ์ หรือในการแข่งขันกีฬาในลักษณะที่ได้รับการยอมรับ แต่ทั้งนี้ ต้องพอประมาณ เป็นไปด้วยความระมัดระวังในการคัดเลือกเนื้อหาที่จะนำเสนอและหลีกเลี่ยงสิ่งที่เกินพอดี หรือเกินความคาดหมายของประชาชน หรือหากจะมีการแสดงภาพ หรือฉากที่มีความรุนแรงเป็นพิเศษ เช่น ฉากที่มีคนตายซึ่งเกิดจากเหตุการณ์จริงอย่างการประหารชีวิตหรือฆาตกรรม จะต้องจัดให้มีคำเตือนที่เหมาะสมแก่ผู้ชม อย่างไรก็ตาม ภาพความรุนแรง หรือกระทำผิดในทางเพศ อาทิ การข่มขืน พยายามข่มขืน หรือกระทำการที่ปราศจากความยินยอม รวมทั้งพฤติกรรมในทางเพศที่ใช้ความรุนแรงจะไม่ได้รับอนุญาตให้เผยแพร่โดยเด็ดขาด

2.4 เนื้อหาที่เป็นอันตราย (Menacing Content)

โดยเฉพาะอย่างยิ่งเนื้อหาที่มีลักษณะของการคุกคาม ก่อ

ภยันตราย หรือส่งเสริมให้กระทำความผิดหรือก่ออาชญากรรม หรือสร้างความปั่นป่วนแก่สังคม หรือแก่ประชาชนถือเป็นสิ่งต้องห้ามทำนองเดียวกับการโฆษณาชวนเชื่อประเภทซึ่งสนับสนุนหรือส่งเสริมการฆ่าล้างเผ่าพันธุ์ หรือสร้างความเกลียดชัง หรือต่อต้านกลุ่มบุคคลที่สามารถระบุตัวได้ (Hate propaganda) ก็ไม่ได้รับอนุญาตให้เผยแพร่ นอกจากนี้ ข้อมูลที่อาจเป็นภัยคุกคามต่อความมั่นคงแห่งชาติ หรือสุขภาพ และความปลอดภัยของประชาชน ก็ห้ามนำเสนอ อาทิ การแนะนำวิธีการทำระเบิด การผลิตยาเสพติดที่ผิดกฎหมาย หรือสินค้าปลอม การเผยแพร่ข้อมูลที่เป็นเท็จเกี่ยวกับเหตุจลาจลทางเชื้อชาติในพื้นที่ที่เฉพาะเจาะจง การเผยแพร่ข้อมูลและคำสั่งที่เกี่ยวกับการโจมตีของผู้ก่อการร้ายที่อาจจะเกิดขึ้นได้ หรือการกระจายหรือให้ข้อมูลเกี่ยวกับการระบาดของโรคร้ายแรง หรือโรคติดต่อ เป็นต้น

2.5 การใช้ถ้อยคำที่หยาบคายและน่ารังเกียจ (Bad language)

การใช้ถ้อยคำที่หยาบคาย น่ารังเกียจต่อคนจำนวนมาก ส่วนใหญ่มักก่อให้เกิดการกระทำความผิด และโดยเฉพาะอย่างยิ่งเป็นภาษาหรือถ้อยคำที่ตรงข้ามกับความคาดหวังของผู้ชม ทั้งนี้ การใช้คำดูถูกเหยียดหยาม หรือในเชิงยั่วยุ คุกคามบุคคลหรือกลุ่มบุคคลอื่นใด เป็นสิ่งต้องห้าม หากกล่าวโดยมุ่งหมายไปในเรื่องหยาบโลน ลามก รวมทั้งการกล่าวถึงการมีเพศสัมพันธ์ หรืออวัยวะเพศอย่างดิบเถื่อน อย่างไรก็ดี คำเหล่านี้จะได้รับอนุญาตให้ใช้ได้ในบริบทของความหมายสามัญ และผู้กล่าวไม่ได้มีวัตถุประสงค์ หรือใช้อย่างหยาบคาย นอกจากนี้ ถ้อยคำที่สร้างความเกลียดชัง (Hate Speech) ก็ต้องห้ามเช่นกัน ทั้งนี้ไม่ว่าจะเป็นการใช้คำพูดหรือรูปภาพ เพื่อจะหมิ่นประมาท หรือเหยียดหยามบุคคลหรือกลุ่มบุคคลอื่นโดยเหตุที่เขามีความแตกต่างในด้านเชื้อชาติ ศาสนา สัญชาติ เพศ รสนิยมทางเพศ หรือความพิการ

2.6 เนื้อหาอันเป็นเท็จ (False Content)

หมายถึง ข้อมูลที่มีเนื้อหาซึ่งไม่เป็นความจริง หรือเนื้อหาที่จะ

ก่อให้เกิดความเข้าใจผิดแก่บุคคลอื่นได้เนื่องจากมีข้อมูลไม่ครบถ้วนสมบูรณ์ ทั้งนี้ ผู้ให้บริการเนื้อหาต้องปฏิบัติตามมาตรการที่ระบุไว้ใน The Content Code ซึ่งจะกำหนดแนวปฏิบัติที่จำเป็นไว้โดยเฉพาะ ทั้งนี้เพื่อจำกัดโอกาสในการสร้าง หรือสื่อสารกันด้วยเนื้อหาที่เป็นเท็จ เนื้อหาที่เป็นเท็จนี้ยังหมายความรวมถึงข้อมูลที่ก่อนที่จะมีการสื่อสารออกไปนั้นไม่ได้ผ่านการตรวจสอบความจริงโดยใช้มาตรการที่เหมาะสมด้วย โดยปกติแล้ว เนื้อหาที่เป็นเท็จถือเป็นสิ่งต้องห้ามโดยชัดแจ้งในประเทศมาเลเซีย เว้นแต่กรณีที่ใช้ในบริบทของการล้อเลียนหรือเสียดสี และกรณีที่เห็นโดยชัดเจนว่าใช้ในนิยาย

2.7 เนื้อหาสำหรับเด็ก (Children's Content)

ประเทศมาเลเซียเป็นประเทศหนึ่งที่ให้ความสำคัญกับการคุ้มครองเด็กจากสื่อประเภทต่าง ๆ ด้วยการควบคุมตรวจสอบ รวมทั้งวางหลักเกณฑ์สำหรับเนื้อหาที่ผลิตขึ้นเพื่อให้เด็กบริโภค เนื้อหาสำหรับเด็กอายุต่ำกว่า 14 ปี The Content Code จะดูแลและตรวจสอบการเลือกเนื้อหาอย่างใกล้ชิด รวมทั้งควบคุมและวางพล็อตเรื่องด้วย โดยประเด็นที่ต้องตรวจสอบเป็นพิเศษ ก็คือ ความรุนแรง โดยสื่อหรือเนื้อหาสำหรับเด็กจะแสดง หรือนำเสนอความรุนแรงได้ก็ต่อเมื่อเป็นสิ่งจำเป็นต่อพัฒนาการของตัวละคร หรือโครงเรื่อง เนื้อหาในหนังการ์ตูน (Animated Content) อาจแสดงความรุนแรงที่ไม่สมจริงได้ แต่ความรุนแรงนั้นไม่ควรเป็นแกนหรือเนื้อหาหลักของเรื่องและต้องไม่มีลักษณะเชิญชวนให้เด็กลอกเลียนแบบซึ่งอาจเป็นอันตรายได้ อย่างไรก็ตาม เนื้อหาสำหรับเด็กจะต้องไม่แสดงฉากของความรุนแรงในลักษณะของการลดทอน หรือหลีกเลี่ยงไม่กล่าวถึงผลเสียของความรุนแรงเหล่านั้น แต่จะต้องชี้ให้เห็นถึงบทสรุปของการตกเป็นเหยื่อ และการกระทำความผิด

สื่อหรือเนื้อหาสำหรับเด็กนี้จะต้องจัดการอย่างระมัดระวังอย่างยิ่ง เกี่ยวกับการนำเสนอเรื่องราวที่สามารถส่งผลกระทบต่อจิตใจ หรือคุกคามความรู้สึกในเรื่องความปลอดภัยของพวกเขาได้ อาทิ ความขัด

แย้งในประเทศ ความตายของพ่อแม่หรือญาติสนิท การเสียชีวิตหรือได้รับบาดเจ็บของสัตว์เลี้ยง การก่ออาชญากรรมบนท้องถนน หรือการใช้ยาเสพติด รวมทั้งเรื่องราวที่หากเด็กลอกเลียนแบบแล้วจะเกิดอันตรายต่อตัวเด็กเอง

กล่าวโดยสรุป จะเห็นได้ว่า แม้ปัจจุบันประเทศมาเลเซียจะไม่มีบทบัญญัติลายลักษณ์อักษรที่อนุญาต หรือให้อำนาจรัฐในการเซ็นเซอร์ หรือปิดกั้นการเข้าถึงเนื้อหาที่ไม่เหมาะสม หรือผิดกฎหมายไว้โดยตรง แต่รัฐก็มีความพยายามในการกำหนดแนวปฏิบัติให้กับผู้ประกอบการ หรือสร้างกลไกตรวจสอบควบคุมเนื้อหาในระหว่างผู้ประกอบการอินเทอร์เน็ตด้วยกันเองขึ้นโดยอาศัย The Content Code ซึ่งกำหนดเนื้อหาที่เผยแพร่ได้ หรือไม่ได้บนเครือข่ายอินเทอร์เน็ต แม้ The Content Code ไม่ได้มีสถานภาพเป็นกฎหมาย แต่ก็ถูกกำหนดขึ้นโดยอาศัยอำนาจจากบทบัญญัติของ CMA ทั้งนี้โดยมีเป้าหมายเพื่อให้การปฏิบัติตาม CMA เกิดขึ้นได้จริงๆ อย่างไรก็ตาม ปัจจุบัน นอกจาก The Content Code, CMCA และ CMA แล้ว รัฐบาลมาเลเซียยังใช้กฎหมายฉบับอื่นๆ ในการควบคุมเนื้อหาของสื่อออนไลน์และจำกัดเสรีภาพในการแสดงความคิดเห็นในสื่อออนไลน์ด้วย

3. กฎหมายที่เกี่ยวข้องกับการควบคุมเนื้อหาในสื่อออนไลน์และจำกัดเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็น

3.1 พระราชบัญญัติความมั่นคงภายใน (Internal Security Act 1960 - ISA)

กฎหมายความมั่นคงภายใน หรือกฎหมายรักษาความปลอดภัยภายใน (Akta Keselamatan Dalam Negeri) ถูกยกร่างขึ้นภายหลังประเทศมาเลเซียได้รับเอกราชจากประเทศอังกฤษในปี 1957 โดย ISA มีผลในปี 1960 เพื่อให้รัฐใช้เป็นเครื่องมือในการป้องกันเหตุร้าย และต่อต้านการก่อความไม่สงบของพรรคคอมมิวนิสต์ อย่างไรก็ตาม กล่าวได้ว่า ISA เป็นกฎหมายที่ตกทอดมาจากยุคอาณานิคม เพราะในยุคนั้น

ประเทศอังกฤษซึ่งปกครองมาเลเซียอยู่ ได้สร้างระบบกฎหมายความมั่นคงขึ้นโดยมีวัตถุประสงค์เพื่อควบคุมและจัดการพรรคคอมมิวนิสต์แห่งมาลายา ซึ่งอังกฤษมองว่าเป็นภัยคุกคาม กฎหมายที่อังกฤษนำมาใช้ในเวลานั้น ได้แก่ พระราชบัญญัติกบฏ (1948) และ พระราชบัญญัติสถานการณ์ฉุกเฉิน (1948) ต่อมากฎหมายทั้งสองฉบับถูกยกเลิกไป โดยมีการประกาศใช้กฎหมายความมั่นคงภายใน หรือ ISA แทน และกฎหมายฉบับนี้ก็ถูกใช้มาจนถึงปัจจุบัน ISA มีลักษณะที่เรียกว่า "กฎหมายภายใต้สภาวะการยกเว้น" (State of Exception) กล่าวคือ เขียนให้อำนาจอย่างมากแก่รัฐบาลเพื่อจัดการกับปัญหาภายใน รัฐมีอำนาจแทรกแซง หรือควบคุมสถานการณ์ที่เกิดขึ้นมากกว่าในยามปกติ

นอกจาก ISA จะอนุญาตให้เจ้าหน้าที่ตำรวจสามารถจับกุมและควบคุมตัวบุคคลโดยไม่ต้องตั้งข้อหาได้นานถึง 60 วัน รวมทั้งเข้าไปและค้นสิ่งของ หรือบุคคล และยึดพยานหลักฐานต่างๆ ได้โดยไม่ต้องมีหมายแล้ว กฎหมายยังให้อำนาจรัฐมนตรีสามารถออกคำสั่งควบคุมตัวบุคคลไว้ (โดยไม่ต้องมีองค์กรอื่นใดกลั่นกรอง) ได้นานถึง 2 ปี โดยปราศจากการดำเนินคดี หรือการตั้งข้อกล่าวหา[15] ที่ผ่านมารัฐบาล (โดยเฉพาะอย่างยิ่งในสมัยที่ ดร. มหาธีร์ เป็นนายกรัฐมนตรี) มักใช้ ISA สร้างเสถียรภาพให้แก่ฝ่ายตน หรือสร้างความได้เปรียบทางการเมือง ด้วยการควบคุมสื่อ ดักฟัง จับกุม หรือคุกคามลดทอนเสรีภาพทางวิชาการ กระทั่งสั่งปิดสถานศึกษาที่วิพากษ์วิจารณ์รัฐบาล ปัจจุบัน พบว่าผู้ถูกกล่าวหาตาม ISA ว่าเป็นผู้ก่อการร้ายจำนวนมากมีความเกี่ยวข้องโดยบังเอิญกับบุคคลที่อยู่ในฝ่ายค้าน หรือผู้มีความเห็นตรงข้ามกับรัฐบาล นับตั้งแต่ปี 1960 ที่ ISA มีผลใช้บังคับจนถึงปี 2005 มีคนถูกจับและได้รับผลกระทบจากกฎหมายฉบับนี้ราว 10,662 คน ในจำนวนนี้มี 4,139 คนที่ถูกควบคุมตัวโดยมีคำสั่งอย่างเป็นทางการ ในขณะที่อีกราว 2,066 ถูกสั่งให้ห้ามทำหรือจำกัดการทำกิจกรรม รวมทั้งกักขังในสถานที่อยู่อาศัย[16]

ก่อนวันที่ 11 กันยายน 2001 มีการกดดันจากสาธารณชนจำนวนมากทั้งจากภายในและนอกประเทศ เรียกร้องให้รัฐบาลยกเลิก ISA แต่

รัฐบาลก็ไม่ได้ดำเนินการใดๆ กระทั่งทุกวันนี้ Tunku Abdul Rahman นายกรัฐมนตรีคนแรกของมาเลเซียเคยระบุว่า

"วัตถุประสงค์ของ ISA มีขึ้นเพื่อต้านคอมมิวนิสต์ในประเทศมาเลเซียในช่วงสถานการณ์ฉุกเฉินของมาเลเซียเท่านั้น และรัฐบาลไม่เคยใช้ ISA จัดการ ข่มเหงฝ่ายตรงข้ามทางการเมือง หรือสกัดกั้นกิจกรรมในรูปแบบประชาธิปไตยที่ชอบด้วยกฎหมาย" [17]

ในขณะที่ Ismail Abdul Rahman รัฐมนตรีว่าการกระทรวงความมั่นคงและความปลอดภัยคนแรกของมาเลเซีย เคยกล่าวโต้ตอบคำวิจารณ์ที่ว่า ISA ละเมิดประชาธิปไตยว่า

"ISA เป็นสิ่งสำคัญ และจำเป็นต่อความมั่นคงของประเทศนี้ โดยเฉพาะอย่างยิ่งในสถานการณ์ที่มีความพยายามต่อต้านรัฐบาลประชาธิปไตยมิได้หมายถึงเสรีภาพอันสมบูรณ์ที่จะคุ้มครองให้แม้กับการพยายามล้มล้างชาติด้วย และตรงกันข้ามเสรีภาพหลายเรื่องที่ดำรงอยู่ในโลกนี้รังแต่จะก่อให้เกิดความวุ่นวายในสังคม และดังนั้น ISA จึงไม่ใช่กฎหมายที่ขัดกับหลักการพื้นฐานของระบอบประชาธิปไตย" [18]

ที่ผ่านมา คงมีก็แต่นักการเมืองฝ่ายค้านพรรคต่างๆ (โดยเฉพาะอย่างยิ่งที่สมาชิกในพรรคเคยโดนควบคุมตัวโดยกฎหมายฉบับนี้) เท่านั้นที่พยายามออกมาชี้ให้เห็นปัญหาของการใช้ ISA อย่างไรก็ดี น่าสนใจว่า Abdullah bin Haji Ahmad Badawi นายกรัฐมนตรีคนที่ห้าของประเทศมาเลเซียในช่วงปี 2003 - 2009 ซึ่งเป็นสมาชิกและเคยเป็นหัวหน้าพรรคอัมโน (United Malays National Organisation - UMNO) พรรคการเมืองที่ใหญ่ที่สุดครองเสียงข้างมาก และเป็นรัฐบาลมาอย่างยาวนานเอง ในยุคสมัยหนึ่ง (ปี 1988) ก็เคยวิพากษ์วิจารณ์ ISA ว่าเป็นกฎหมายที่เข้มงวดและป่าเถื่อน ทั้งยังกล่าวด้วยว่า ISA ไม่ควรมีอยู่อีกต่อไปแล้วในประเทศมาเลเซียที่ทันสมัย (no place in modern Malaysia) หากประเทศมาเลเซียและพรรคอัมโนต้องการอยู่รอด ดร.มหาธีร์ (นายกรัฐมนตรีสมัยนั้น) จะต้อง

ลาออก เพราะเขาใช้ ISA เพื่อปิดกั้นเสียงวิพากษ์วิจารณ์ตนเอง แต่เมื่อ Ahmad Badawi ได้ขึ้นเป็นนายกรัฐมนตรีในปี 2003 เขากลับเรียก ISA ว่าเป็น “กฎหมายที่จำเป็น” (a necessary law) และโต้เถียงฝ่ายที่เรียกร้องให้ยกเลิกว่า รัฐบาลของเขาไม่เคยใช้ ISA โดยไม่ชอบธรรมเลย ทุกคนที่ถูกคุมขังตามพระราชบัญญัติฉบับนี้ล้วนเป็นภัยคุกคามต่อสังคม

ความเป็นอิสระของศาลและผู้พิพากษาก็นับเป็นเรื่องที่ถูกวิพากษ์วิจารณ์มากที่สุด ในแง่ของการใช้อำนาจตามกฎหมายฉบับนี้ ทั้งนี้เพราะการพิจารณาคดีของศาลในความผิดตามข้อกล่าวหาตาม ISA จะถูกจำกัดการสืบพยานหลักฐานอย่างมากในชั้นกระบวนการพิจารณา เว้นแต่ เจ้าหน้าที่ฝ่ายรัฐเองจะต้องการพยานหลักฐาน หรือรายละเอียดเพิ่มเติม Hardial Singh Khaira นักกฎหมายและบล็อกเกอร์เคยเขียนวิเคราะห์ประเด็นนี้ไว้ในบทความของเขาว่า การพิพากษาคดีที่เกี่ยวกับ ISA ไม่เพียงแต่สะท้อนให้เห็นความล้มเหลวของศาลมาเลเซียเท่านั้น แต่ยังเป็นการละเมิดสิทธิขั้นพื้นฐานอีกด้วย โดยความล้มเหลวของศาลมาเลเซียที่เกี่ยวกับ ISA เริ่มต้นขึ้นเมื่อศาลให้การรับรองความชอบของการกระทำของฝ่ายบริหารในการควบคุมตัวบุคคล ทั้งยังกล่าวด้วยว่า ปัจจุบันศาลมาเลเซียเพียงทำหน้าที่ในการลดความรับผิดชอบให้กับฝ่ายบริหาร และเคารพเฉพาะสิทธิมนุษยชนภายใต้กฎหมายมาเลเซียเท่านั้น[19]

สำหรับกรณีที่ ISA เข้าไปเกี่ยวข้องกับเสรีภาพการแสดงความคิดเห็นในสื่อออนไลน์นั้น มีกรณีที่สำคัญๆ คือ ปี 1998 ตำรวจจับกุมบุคคลสี่คนตาม ISA โดยสันนิษฐานว่าเกี่ยวข้องกับการแพร่กระจายข่าวลือป่วนเมืองในกรุงกัวลาลัมเปอร์ โดยผู้ต้องสงสัยถูกควบคุมตัวหลังจากตำรวจติดตามดูพฤติกรรมโดยความช่วยเหลือของผู้ให้บริการอินเทอร์เน็ต เดือนมกราคมปี 2001 เว็บไซต์ของรัฐสภาถูกเจาะระบบ หลังจากนั้นก็มีรายงานว่ารัฐบาลอาจขยาย ISA เพื่อจัดการกับนักเจาะระบบ (Hacker) ทั้งหลายที่บังอาจเจาะระบบเว็บไซต์ของรัฐบาล และกรณีที่โด่งดังและเป็นที่รู้จักก็คือ เดือนกันยายน ปี 2008 Raja Petra Kamarudin คอลัมนิสต์ชื่อดังของเว็บไซต์ Malaysia Today ถูกควบคุมตัวภายใต้ ISA ซึ่งทนายความ

ของเขากล่าวว่าเป็นการควบคุมตัวโดยไม่ชอบด้วยกฎหมาย สาเหตุของการจับกุมและดำเนินคดี ก็คือ Raja Petra Kamaruddin โพสต์ข้อความที่เกี่ยวกับคดีในศาลซึ่งเป็นที่ถกเถียงอย่างมากกรณีเหตุการณ์ฆาตกรรมนักแปลสตรีชาวมองโกเลีย ทั้งนี้เพราะคดีดังกล่าวมีนายตำรวจและผู้อำนวยการด้านที่ปรึกษาที่มีสายสัมพันธ์ใกล้ชิดกับรองนายกรัฐมนตรีถูกดำเนินคดีด้วย อย่างไรก็ตาม เขาถูกปล่อยตัวโดยคำสั่งของศาลสูงในอีก 56 วันภายหลังถูกควบคุมตัว โดยศาลสูงให้เหตุผลว่า เหตุผลในการสั่งควบคุมตัว Raja Petra Kamarudin โดยรัฐมนตรีว่าการกระทรวงมหาดไทยไม่เข้าเงื่อนไขตามมาตรา 8 (1) ISA[20]

3.2 พระราชบัญญัติยั่วยุปลุกระดม (Sedition Act 1948)

พระราชบัญญัติยั่วยุปลุกระดม ถูกตราขึ้นในสมัยที่มาเลเซียตกเป็นอาณานิคมของอังกฤษในปี 1948 เป็นกฎหมายห้ามการกระทำ การพูด การสร้างวาทกรรม ผลิตซ้ำ หรือเผยแพร่สิ่งใดๆ ที่มีเนื้อหาเข้าข่ายเป็นการยั่วยุปลุกปั่น หรือในเรื่องที่มีแนวโน้มที่จะก่อให้เกิดความไม่สงบเรียบร้อยขึ้นได้ กฎหมายบัญญัติว่า

“การพูดที่เป็นความผิดอาญา คือ การพูดที่มีแนวโน้มว่าจะก่อให้เกิดความไม่สงบเรียบร้อยขึ้น รวมถึงการนำพาให้เกิดความเกลียดชัง การหมิ่นประมาท ปลุกระดมความไม่พอใจต่อรัฐบาล หรือทำให้เกิดความรู้สึกเกลียดชังระหว่างเชื้อชาติที่แตกต่างกัน”

สำหรับบทลงโทษนั้น หากเป็นการกระทำผิดครั้งแรก ต้องระวางโทษปรับไม่เกิน 5,000 ริงกิต หรือจำคุกไม่เกินสามปี หรือทั้งจำทั้งปรับ หากมีการกระทำความผิดซ้ำอีกก็อาจถูกจำคุกได้ถึงห้าปี ในขณะที่สิ่งพิมพ์ หรือเอกสารใดๆ ที่มีเนื้อหาเป็นการปลุกระดมซึ่งอยู่ในความครอบครองของผู้กระทำความผิด นอกจากใช้เป็นพยานหลักฐานในการดำเนินคดีแล้วก็จะถูกริบทำลาย นอกจากนี้ ผู้ที่เพียงมีไว้ในครอบครองซึ่งเอกสาร หรือสิ่งพิมพ์ปลุกระดมดังกล่าว ก็อาจถูกลงโทษได้เช่นเดียวกัน

ซึ่งมีโทษปรับไม่เกิน 2,000 ริงกิต หรือจำคุกไม่เกิน 18 เดือนหรือทั้งจำทั้งปรับสำหรับความผิดครั้งแรก แต่หากกระทำผิดซ้ำอีกอาจถูกตัดสินจำคุกได้นานถึงสามปี อนึ่ง ศาลอาจสั่งห้ามการเผยแพร่ต่อไปของสำเนาเอกสารดังกล่าวได้ ด้วยการห้ามทุกคนมีไว้ในความครอบครอง หากมีผู้ที่ไม่ปฏิบัติตามคำสั่งห้ามของศาลก็อาจถูกปรับไม่เกิน 1,000 ริงกิต หรือจำคุกหนึ่งปีหรือทั้งสองอย่าง

ปัจจุบันพระราชบัญญัติฉบับนี้ยังคงมีผลบังคับใช้ และกระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชนโดยตรง ไม่ว่าจะแสดงออกในรูปแบบหรือผ่านสื่อประเภทใด[21] ภายหลังเกิดเหตุจลาจลทางเชื้อชาติครั้งใหญ่ในเมืองหลวงเดือนพฤษภาคม ปี 1969 ทำให้มีประชาชนมาเลเซียอย่างน้อย 200 คนเสียชีวิต รัฐบาลจึงทำการแก้ไขเพิ่มเติมรัฐธรรมนูญขยายขอบเขตของข้อจำกัดเสรีภาพในการพูดตามรัฐธรรมนูญ มาตรา 152, 153, 181 และ Part III เรื่องความคุ้มครองพิเศษ โดยอนุญาตให้รัฐสภาผ่านกฎหมายที่เกี่ยวกับสัญญาประชาคมได้ [22] และด้วยอำนาจนี้เองทำให้ Sedition Act ซึ่งเดิมอาจถือว่าขัดหรือแย้งกับรัฐธรรมนูญในเรื่องของการรับรองเสรีภาพในการพูด ไม่ใช่บทบัญญัติที่ขัดหรือแย้งรัฐธรรมนูญอีกต่อไป โดยผลของมาตรา 10 (2) รัฐธรรมนูญที่บัญญัติให้รัฐสภามีอำนาจตราข้อจำกัดการแสดงความคิดเห็นได้หาก

“เห็นว่าจำเป็น หรือสมควรเพื่อประโยชน์แห่งการรักษาความมั่นคงของประเทศ ความสัมพันธ์ฉันท์มิตรกับประเทศอื่นๆ เพื่อสาธารณะหรือศีลธรรมอันดี โดยข้อจำกัดนั้นต้องเป็นไปเพื่อปกป้องสิทธิของรัฐสภา สภานิติบัญญัติ หรือศาล การทำให้เสื่อมเสียชื่อเสียง หรือการยั่วยุให้เกิดการกระทำความผิดใดๆ”

ทั้งนี้ ตามมาตรา 4 ของ Sedition Act ก็กำหนดว่าผู้ใดที่มีอยู่มีความพยายามที่จะทำ เตรียมการใดๆ ที่จะทำ หรือสนับสนุนบุคคลใดให้กระทำการที่มีแนวโน้มขัดต่อความสงบเรียบร้อย เช่น พูด ผลิตสิ่งพิมพ์ เผยแพร่ หรือนำเข้าวรรณกรรมที่เป็นการยุยงให้กระทำการอันขัดต่อความสงบ

เรียบร้อย ผู้นั้นต้องมีความผิดอาญา โดยปราศจากข้อแก้ตัวตามกฎหมาย ประเด็นสำคัญที่กฎหมายฉบับนี้ถูกวิพากษ์วิจารณ์ และมีการเรียกร้องให้ยกเลิก คือ การกำหนดความผิดไว้อย่างคลุมเครือ ไม่ชัดเจน ปล่อยให้เป็นดุลพินิจของเจ้าหน้าที่รัฐ ทำให้ลักษณะการใช้การตีความเป็นเรื่องทางการเมือง แทนที่จะชัดเจนเป็นหลักในทางกฎหมาย ในพระราชบัญญัติฉบับนี้กำหนดความผิดไว้ทั้งกรณีที่มีการกระทำแล้ว และเพียงการ “มีแนวโน้มก่อการปลุกระดม” (seditious tendency) โดยมีการระบุลักษณะของการมีแนวโน้มดังกล่าวไว้ใน มาตรา 3 ไม่ว่าจะเป็น การสร้างความเกลียดชัง ดูถูกเหยียดหยาม หรือเพื่อกระตุ้นความบาดหมาง ต่อต้านกฎหมาย หรือการกระทำของรัฐบาล การบริหารงานยุติธรรมทั้งในประเทศมาเลเซีย และประเทศอื่น เพื่อส่งเสริม หรือสร้างความรู้สึกไม่ดี หรือปรปักษ์ระหว่างเชื้อชาติ เผ่าพันธุ์ที่แตกต่างกัน หรือระหว่างชนชั้นของประชาชนในประเทศมาเลเซีย และประเทศอื่นๆ ตั้งคำถามกับเรื่องสิทธิ สถานะ ตำแหน่งอำนาจอธิปไตย หรืออำนาจของรัฐที่จัดตั้งขึ้น หรือได้รับการป้องกันไว้โดยรัฐธรรมนูญ เป็นต้น ทั้งนี้ ถ้อยคำที่คลุมเครือหลายอย่าง อาทิ การสร้างความรู้สึกที่ไม่ดี ความบาดหมาง การดูถูก หรือการสร้างความไม่พอใจ ไม่มีการนิยามความหมายและขอบเขตให้ชัดเจน แม้ตามมาตรา 3 (2) ของกฎหมายฉบับนี้ จะระบุข้อยกเว้นบางประการ ที่ไม่ถือว่าขัดต่อความไม่สงบเรียบร้อยไว้ เช่น การแสดงให้เห็นว่ากฎหมายใดผิดหรือเข้าใจผิดในการใช้เพื่อพยายามจัดให้มีความถูกต้องตามกฎหมาย ในการเปลี่ยนแปลงใดๆ ภายในอาณาเขตของรัฐ ทั้งนี้ตามที่กฎหมายได้จัดตั้งขึ้น หรือเพื่อนำไปสู่การยกเลิก หรือลดความรู้สึกไม่ดี หรือเป็นปฏิปักษ์ระหว่างความแตกต่างทางเชื้อชาติ หรือชนชั้นของประชากร แต่ก็หาได้ช่วยบรรเทาการใช้กฎหมายตามอำเภอใจของฟากฝ่ายการเมืองลงได้ไม่

ปัจจุบัน กฎหมายฉบับนี้มักถูกใช้เพื่อเล่นงานฝ่ายตรงข้ามกับรัฐบาล อาทิ กรณีที่ Lim Guan Eng อดีตสมาชิกสภาผู้แทนราษฎรจาก DAP ถูกจับในปี 1998 เนื่องจากกล่าวหาอัยการสูงสุดว่าล้มเหลวในการจัดการกรณีที่มุขมนตรีรัฐมะละกาถูกจับในความผิดฐานข่มขืน

นักเรียนหญิง ปี 2003 Abdullah Ahmad Badawi กล่าวว่า รัฐบาลจะจับกุมผู้ต่อต้านการเปลี่ยนแปลงนโยบายทางการศึกษา ซึ่งเน้นการเรียนการสอนวิทยาศาสตร์และคณิตศาสตร์เป็นภาษาอังกฤษ และผู้ใดต่อต้านจะมีความผิดฐานกระทำการอันขัดต่อความสงบเรียบร้อยฯ จากนั้นในปีเดียวกัน สื่อออนไลน์ Malaysiakini ก็ถูกปิดกั้นการเข้าถึงชั่วคราวโดยอาศัยอำนาจตาม Sedition Act หลังจากตีพิมพ์หนังสือวิจารณ์นโยบายทางการศึกษานี้

องค์กรสิทธิมนุษยชน กล่าวว่า Sedition Act มีความหมาย “คลุมเครือเกินไป” และวิจารณ์ว่าความไม่ชัดเจนนี้เอง ที่ถือเป็นการ “เชื้อเชิญให้เกิดการกระทำผิด และหน่วยงานรัฐอาจหาทางนำมันไปใช้เป็นเครื่องมือกับสถานการณ์ต่างๆ โดยไม่มีความสัมพันธ์กับเจตนารมณ์เดิมของกฎหมาย” ผู้พิพากษา Raja Alan Shah เคยวิจารณ์กฎหมายฉบับนี้ว่าเป็นกฎหมายที่จำกัดสิทธิเสรีภาพในการพูดโดยทำให้สิทธินั้นสิ้นสุดลง และแม้แต่ Lord Bach รัฐมนตรีว่าการกระทรวงยุติธรรมของอังกฤษเอง ยังเคยกล่าวว่า Sedition law เป็นกฎหมายที่ล้าหลัง และควรยกเลิก แต่ในขณะที่รัฐมนตรีว่าการกระทรวงเทคโนโลยีและสารสนเทศและรัฐมนตรีมหาดไทย Datuk Hussein Seri Hishammuddin กลับให้ความเห็นว่าไม่มีความจำเป็นต้องยกเลิก

3.3 กฎหมายฉบับอื่น ๆ

- กฎหมายต่อต้านการทุจริตคอร์รัปชั่น (The Anti Corruption Act) กำหนดให้อำนาจอัยการสูงสุดในการสกัดกั้นอีเมล และดักฟังโทรศัพท์ทั้งนี้ เพื่อตรวจสอบการทุจริต หรือเพื่อป้องกันการกระทำที่ถือว่าเป็นภัยต่อความมั่นคงของชาติหรือผลประโยชน์ของชาติ

- ประมวลกฎหมายอาญา (Section 509 Penal Code) ให้ลงโทษทางอาญาในความผิดฐานหมิ่นประมาทบุคคลใดๆ หรือล่วงละเมิดพื้นที่ส่วนบุคคล หรือความเป็นส่วนตัวของบุคคลอื่น โดยคำพูด ประโยค เสียง ท่าทาง หรือด้วยการแสดงออกที่ผู้กระทำมีเจตนาทำให้ถ้อยคำ เสียง ท่าทาง หรือการกระทำดังกล่าวถูกเห็นได้โดยบุคคลนั้น

- ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล (The Personal Data Protection) ที่ควรประกาศใช้ภายในเดือนมีนาคมปี 2002 แต่ต้องล่าช้าออกไปตามการร้องขอของภาคธุรกิจ กฎหมายนี้มีหลักการในการป้องกันการรวบรวมข้อมูลทางปกครอง การใช้ การเปิดเผยข้อมูลความถูกต้อง การเก็บรักษา การเข้าถึง และความปลอดภัยของข้อมูลส่วนบุคคล หากฝ่าฝืนมีโทษปรับถึง 250,000 ริงกิต หรือประมาณ 81,900 เหรียญสหรัฐ และจำคุกสี่ปี สำหรับผู้ทำให้เกิดความเสียหายในข้อมูล (รวมถึงค่าชดเชยความเสียหายทางความรู้สึก) โดยในส่วนที่สามของร่างกฎหมายนี้ ยังให้มีการจัดตั้งศาลพิเศษเพื่อช่วยปฏิบัติหน้าที่ตามอำนาจของ Commissioner ในส่วนที่เกี่ยวกับประโยชน์สาธารณะ และศาลพิเศษนี้ยังสามารถระงับกฎระเบียบข้อบังคับได้ ข้อสังเกตในแง่กฎหมายที่สำคัญอย่างมากก็คือ ร่างกฎหมายนี้ไม่ได้พยายามห้ามการรวบรวม การถือหุ้น การจัดการ หรือการเข้าถึง “ข้อมูลส่วนบุคคล” (ซึ่งไม่ใช่ของรัฐ หรือเป็นข้อมูลทางปกครอง) รวมทั้งไม่ได้มีมาตรการเพื่อจัดการการเข้าถึงข้อมูลใดๆ ที่ถูกรวบรวมไว้ กล่าวให้ง่ายก็คือ แม้กฎหมายฉบับนี้จะได้ชื่อว่าเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่โดยเนื้อหาและหลักการแล้วกลับไม่ใช่กฎหมายที่เกี่ยวกับสิทธิส่วนบุคคล หรือสิทธิเสรีภาพทางข้อมูลเลย

4. แนวนโยบาย และแนวทางปฏิบัติที่เกี่ยวกับการควบคุมสื่อออนไลน์

ดังกล่าวมาแล้วว่า แม้ประเทศมาเลเซียจะมีทั้งกฎหมายลายลักษณ์อักษร และคำมั่นสัญญาว่ารัฐบาลจะไม่ทำการตรวจสอบ หรือกรองเนื้อหาข้อมูลในสื่ออินเทอร์เน็ต หากยังไม่มีพยานหลักฐานทางด้านเทคโนโลยีที่ชัดเจน แม้ในเดือนเมษายน ปี 2011 Najib Raza นายกรัฐมนตรีเองก็ยังออกมายืนยันว่ารัฐบาลจะไม่ดำเนินการเซ็นเซอร์อินเทอร์เน็ต อย่างไรก็ตามในทางปฏิบัติกลับเป็นไปในทางตรงกันข้าม เพราะรัฐใช้กฎหมายหลายฉบับในการควบคุม และคุกคามสื่ออย่างแพร่หลายและต่อเนื่อง ทั้งกับสื่อแบบเดิม ไปจนถึงสื่อออนไลน์ ความกังวลต่อพลังอำนาจของสื่อใหม่ของรัฐบาล

มาเลเซียสะท้อนออกมาให้เห็นจากการดำเนินนโยบายและการพยายามใช้มาตรการต่างๆ เพื่อกดดันว่าสื่อใหม่ควรอยู่ข้างรัฐบาล หรือคุกคามจับกุมฝ่ายตรงข้าม กรณีที่เกิดขึ้นอย่างมาก ก็คือ การคุกคามบล็อกเกอร์ ซึ่งเขียนวิพากษ์วิจารณ์การทำงาน และใช้อำนาจของรัฐบาล Jonathan Kent ผู้สื่อข่าว BBC News ประจำกรุงกัวลาลัมเปอร์ ก็เคยรายงานว่า รัฐบาลมาเลเซียเริ่มมีความกังวลเพิ่มขึ้นกับสถานการณ์การวิพากษ์วิจารณ์รัฐบาลผ่านสื่อออนไลน์ เพราะมีจำนวนเพิ่มมากขึ้นทุกวัน[24]

ความกังวลใจต่อพลานุภาพของอินเทอร์เน็ตของฝ่ายผู้กุมอำนาจในมาเลเซียเริ่มปรากฏชัดขึ้นภายหลังการเลือกตั้งทั่วไปในเดือนมีนาคม ปี 2008 ซึ่งผลปรากฏว่าเสียงของฝ่ายพรรคร่วมรัฐบาล หรือกลุ่มพรรคแนวร่วมแห่งชาติ (Barison Nasional – BN) ได้รับคะแนนลดลง 58 ที่นั่ง มีที่นั่งในสภา 140 ที่นั่ง คิดเป็นสัดส่วนของเสียงที่หายไปมีมากถึงสองในสาม จากที่ไม่เคยเป็นเช่นนี้มาก่อนนับแต่ปี 1969 ในขณะที่พรรคร่วมฝ่ายค้าน หรือพันธมิตรประชาชน ได้รับคะแนนเสียงเพิ่มขึ้นถึง 61 ที่นั่ง ทำให้มีที่นั่งในสภาเป็น 82 ที่นั่ง ผลการเลือกตั้งครั้งนั้น นอกจากสะท้อนถึงการเสื่อมความนิยมของพรรคอัมโนและแกนพรรคร่วมรัฐบาล และกระแสความไม่พอใจเกี่ยวกับนโยบายการเลือกปฏิบัติด้านเชื้อชาติ (ให้สิทธิกับคนเชื้อชาติมลายูมากกว่าเชื้อชาติอื่น) จนเกิดการประท้วงใหญ่ในเดือนกุมภาพันธ์ ปี 2008 แล้ว ผู้สังเกตการณ์การเลือกตั้งยังเห็นว่าส่วนหนึ่งน่าจะเป็นผลมาจากการใช้อินเทอร์เน็ตอย่างมีประสิทธิภาพของพรรคร่วมฝ่ายค้านในการสื่อสารข้อมูลกับประชาชนโดยตรงด้วย โดยเฉพาะอย่างยิ่งในเกาะปีนังและรัฐสลังงอ ประกอบกับความนิยมและบทบาทที่เพิ่มขึ้นอย่างมากของสำนักข่าวอิสระออนไลน์ในหมู่ประชาชนมาเลเซีย ด้วยเหตุนี้ฝ่ายรัฐบาลจึงเริ่มเห็นว่า อินเทอร์เน็ตเป็นเครื่องมือเอื้อประโยชน์อย่างมากต่อการระดมเสียงสนับสนุนทางการเมืองของฝ่ายค้าน[25] และหลังจากนั้นเป็นต้นมาสถานการณ์การคุกคาม ดำเนินคดี และควบคุมตัวนักข่าวพลเมือง บล็อกเกอร์ รวมทั้งการปิดกั้นการเข้าถึงเว็บไซต์ก็เริ่มเกิดขึ้นโดยอาศัยกฎหมายด้านความมั่นคงฉบับต่างๆ ทั้งนี้ ภายใต้ข้อสัญญาว่ารัฐบาล

มาเลเซียจะไม่เซ็นเซอร์อินเทอร์เน็ต ในขณะที่ฝ่ายรัฐบาลเองก็เริ่มหันมาให้ความสนใจกับการสร้างเว็บไซต์และกระบอกเสียงของตนเองผ่านสื่อออนไลน์มากขึ้น

Wikileaks เว็บชื่อดังในการเผยแพร่เอกสารความลับของประเทศต่างๆ ทั่วโลก ก็เคยถูกผู้ให้บริการอินเทอร์เน็ตในมาเลเซียปิดกั้นการเข้าถึงมาแล้ว ซึ่งผู้ใช้อินเทอร์เน็ตจำนวนมากเชื่อว่ามีรัฐบาลอยู่เบื้องหลัง ทำให้ภายหลังการปิดกั้นดังกล่าว เว็บไซต์กระทรวงต่างๆ ของรัฐบาลก็ถูกโจมตีโดยกลุ่มนักเจาะระบบ (Hacker) ที่ไม่เห็นด้วยกับการปิดกั้น Wikileaks[26] นอกจากนี้ ตั้งแต่เดือนมิถุนายน 2011 คณะกรรมการโทรคมนาคมและมัลติมีเดีย (the Malaysian Communication and Multimedia Commission - MCMC) ยังใช้อำนาจตามกฎหมายลิขสิทธิ์ (The Copyright Act 1987) สั่งไปยังผู้ให้บริการอินเทอร์เน็ตทั่วประเทศมาเลเซียให้ปิดกั้นช่องทางการเข้าถึงเว็บไซต์แบ่งปันไฟล์ (File-Sharing) และเว็บเซิร์ฟเวอร์จำนวนมากที่มีการละเมิดทรัพย์สินทางปัญญา[27]

การดำเนินงานและแนวนโยบายสำคัญๆ ของรัฐบาลมาเลเซียที่เกี่ยวพัน หรือส่งผลกระทบกับเสรีภาพของสื่อและประชาชนในโลกออนไลน์ที่สำคัญๆ ในช่วงที่ผ่านมา อาทิ

- Rais Yatim รัฐมนตรีว่าการกระทรวงวัฒนธรรมและการสื่อสาร เคยเสนอให้รัฐบาลติดตั้งระบบซอฟต์แวร์เพื่อคัดกรองเว็บไซต์ โดยพิจารณาให้ใช้โปรแกรม Green Dam ซึ่งเป็นซอฟต์แวร์คัดกรอง ซึ่งประเทศจีนเคยนำไปใช้ ทั้งนี้ ภายใต้ข้ออ้างในเรื่องความจำเป็นในการรักษาความสามัคคีของชาติที่มีความหลากหลายทางวัฒนธรรมและเชื้อชาติ อย่างไรก็ดี ข้อเสนอดังกล่าวถูกโต้แย้งจากผู้ใช้อินเทอร์เน็ตชาวมาเลเซีย อีกทั้งรัฐบาลก็ยังไม่รับรอง หรือเห็นด้วยกับแผนการคัดกรองเนื้อหาบนสื่อออนไลน์[28]

- เดือนกรกฎาคมปี 2001 หัวหน้าพนักงานสืบสวนสอบสวนฝ่ายอาชญากรรมเทคโนโลยี ซึ่งเป็นหน่วยงานในกำกับของ Royal Malaysia Police เรียกร้องให้รัฐปรับปรุงพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ (Computer Crime Act) ด้วยเหตุผลว่ากฎหมายล้าสมัยแล้ว

และควรมีการปรับปรุงให้อำนาจหน้าที่แก่เจ้าพนักงานในการสอดส่องดูแลการกระทำความผิดเพิ่มขึ้น สอดคล้องกับ ดร. มหาธีร์ ที่ย้ำว่าต้องให้มีมาตรการรักษาความปลอดภัยเพิ่มมากขึ้น เพื่อรับมือกับอัตราที่เพิ่มขึ้นของอาชญากรรมไซเบอร์ รวมทั้งการใช้อินเทอร์เน็ตเพื่อเข้าถึงข้อมูลที่ผิดกฎหมาย

- เดือนมกราคมปี 2007 นายกรัฐมนตรีมาเลเซีย Abdullah Ahmad Badawi ระบุว่า กฎหมายบางฉบับที่ประกาศใช้แล้ว อาจมีความแตกต่างไปจากนโยบายของรัฐบาลที่ได้แถลงไว้ว่าจะไม่มีการตรวจสอบอินเทอร์เน็ต การเขียนบล็อกต่าง ๆ และโดยผลของกฎหมาย ย่อมมีผลผูกพันในเรื่องการหมิ่นประมาท ความสงบเรียบร้อย และการจำกัดเสรีภาพการพูด

- ปลายปี 2011 เป็นต้นมา Kong Cho Ha รัฐมนตรีช่วยว่าการกระทรวงวิทยาศาสตร์และเทคโนโลยี กล่าวถึงแผนที่ประเทศมาเลเซียจะแก้ไขเพิ่มเติม หรือออกกฎหมายอินเทอร์เน็ต (Cyber Law/ Internet Law) ฉบับใหม่ โดยมีเป้าหมายเพื่อควบคุมและป้องกันไม่ให้บรรดาบล็อกเกอร์เผยแพร่ข่าวสารได้มากขึ้น โดย Kong Cho Ha กล่าวว่า

"รัฐบาลจำเป็นต้องมีเครื่องมือ Cyber Laws ที่เข้มงวดเพื่อป้องกันไม่ให้บล็อกเกอร์เผยแพร่ข่าวสารที่สร้างความแตกแยก วุ่นวาย ก่อให้เกิดความไม่สงบเรียบร้อย และการโกหก เราต้องการให้คนเขียนบล็อกมีความรับผิดชอบ และต้องกระทำภายในขอบเขตของกฎหมาย และต้องไม่กระทำในสิ่งที่ก่อให้เกิดความไม่สงบเรียบร้อย"

โดยอ้างตัวอย่าง การโพสต์รูปบนเว็บไซต์ของนักการเมืองฝ่ายค้านคนหนึ่ง ซึ่งเป็นภาพถ่ายในห้องพักของโรงแรมโดยผู้ชายชาวมุสลิมสวมเสื้อคลุมและผู้หญิงมุสลิมนอนอยู่บนอก ภาพถ่ายนี้กลายเป็นเรื่องอื้อฉาวทางการเมือง เพราะเป็นภาพก่อนที่สองคนนี้จะแต่งงานกัน โดยทั้งคู่ถูกกล่าวหาว่ามีความผิดฐาน Khalwat หรือการที่ชายหรือหญิงมุสลิมที่ไม่ได้สมรสกันอยู่ด้วยกันสองต่อสองในที่ลับตาคน[29] และก่อนหน้านี้ในปี 2006 Kong Cho Ha ยังเคยประกาศว่าบล็อกเกอร์หน้าใหม่จะต้องมาขึ้นทะเบียน

กับกระทรวงไอซีที อย่างไรก็ตาม แผนการต่างๆ ดังกล่าวก่อให้เกิดกระแสการวิพากษ์วิจารณ์ในหมู่ประชาชน แต่จนถึงปัจจุบันรัฐบาลมาเลเซียก็ยังไม่ได้ดำเนินการแก้ไข หรือเพิ่มเติมกฎหมายอินเทอร์เน็ตแต่อย่างใด

สำหรับกรณีการปิดกั้นการเข้าถึงหรือตรวจสอบเว็บไซต์ และการคุกคามดำเนินคดีกับผู้ให้บริการเว็บไซต์ที่สำคัญ อาทิ

- Malaysiakini.com ซึ่งเป็นเว็บไซต์ข่าวอิสระ ถูกตรวจสอบ และสั่งให้ปลดเนื้อหาออกจากเว็บไซต์โดยคณะกรรมการสื่อสารและมัลติมีเดียของประเทศมาเลเซีย (MCMC) เนื่องจากมีการโพสต์วิดีโอที่เจ้าหน้าที่ถือว่าไม่เหมาะสม แม้จะเป็นการโพสต์ประกอบเรื่องที่อยู่ในความสนใจของสาธารณชนก็ตาม[30] และเดือนมกราคม ปี 2003 เว็บไซต์เดียวกันนี้ได้นำเสนอจดหมายฉบับหนึ่งที่เขียนวิพากษ์วิจารณ์การทำงานของรัฐบาล โดยไม่ได้ระบุว่าใครเป็นผู้เขียนจดหมายนี้ ทำให้ตำรวจยึดคอมพิวเตอร์ประมาณ 20 เครื่อง ที่มีข้อมูลสำคัญๆ บันทึกอยู่ ซึ่งอาจรวมถึงที่อยู่ของผู้ที่เขียนจดหมายนั้นด้วย

- Raja Petra Kamarudin เจ้าของบล็อกที่รู้จักกันดีในนาม RPK ซึ่งเป็นกรรมการบริหารเว็บไซต์ Malaysia's Today ถูกกล่าวหาหลายครั้งว่าก่อความไม่สงบเรียบร้อย เพราะเหตุเขียนข่าวในทำนองที่มีความหมายว่านายกรัฐมนตรีและภรรยาเข้าไปพัวพันกับกรณีฆาตกรรมล่ามชาวมองโกเลีย โดยเจาะจงประเด็นกรณีระเบิดที่เกี่ยวกับการเมืองและการขายอาวุธ เขาถูกเจ้าหน้าที่ขู่จะถอนสัญชาติมาเลเซีย และจะออกหมายจับระหว่างประเทศ อย่างไรก็ตาม เดือนพฤศจิกายน 2009 ศาลสั่ง "ระงับ" การพิจารณาคดีโดยอนุญาตให้ปล่อยตัว แต่ข้อกล่าวหายังคงมีอยู่เช่นเดิม และอาจถูกจับกุมอีกครั้งเมื่อใดก็ได้ นอกจากนี้ยังเคยถูกกล่าวหาว่าหมิ่นประมาทพระมหากษัตริย์ รวมถึงชาวอิสลามและความเกลียดชังทางเชื้อชาติ

- Khairul Nizam Abdul Ghani บล็อกเกอร์ www.adukataruna.blogspot.com ถูกกล่าวหาว่าดูหมิ่นสถาบันพระมหากษัตริย์ เพราะโพสต์ข้อความบนบล็อกตนเอง ด้วยข้อความที่แสดงความคิดเห็นเกี่ยวกับ

Sultan Iskandar Ismail ของรัฐ Johor ที่สวรรคตเมื่อเดือนมกราคม แม้เขาจะขอโทษและลบข้อความที่เป็นการดูหมิ่นนั้นออกจากบล็อกแล้วก็ตาม และเพราะเหตุกล่าวหาครั้งนั้นทำให้เขาอาจได้รับโทษสูงสุดถึงหนึ่งปีหรือทั้งจำทั้งปรับ

- มกราคม ปี 2007 Jeff Ooi เจ้าของ http://jeffooi.com/ และ Ahirudin Attan เจ้าของ http://rockybru.blogspot.com ถูกฟ้องพร้อมกันจากบทความที่โพสต์ และข้อความผู้อ่านที่เขียนวิจารณ์ โดยถูกกล่าวหาว่ามีเนื้อหาเป็นการสบประมาท บิดเบือนข้อเท็จจริง เป็นการเผยแพร่ภาพล้อเลียนของพระศาสดามูฮัมหมัด และขโมยคัดลอกบทความที่โพสต์ไว้เมื่อปี 2006 ซึ่งก่อนหน้านี้ Ooi ถูกตรวจสอบโดยคณะกรรมการ MCMC และเจ้าหน้าที่ตำรวจในส่วนที่ผู้อ่านได้แสดงความคิดเห็นที่ไม่เหมาะสมเกี่ยวกับภาพล้อเลียนศาสดามูฮัมหมัดดังกล่าว

- เดือนสิงหาคม ปี 2008 ผู้ให้บริการอินเทอร์เน็ตมาเลเซียจำนวน 21 ราย ปิดกั้นการเข้าถึงเว็บไซต์ Malaysia's Today ตามคำสั่งของคณะกรรมการ MCMC[31] ซึ่งให้เหตุผลว่า เป็นการปิดกั้นตามที่ได้รับการร้องเรียนจากประชาชนว่ามีการโพสต์แสดงความคิดเห็นที่ไม่เหมาะสมในเว็บไซต์ดังกล่าว และถือเป็นความผิดตามมาตรา 263 ของ Communications and Multimedia Act ซึ่งบัญญัติว่า "ผู้ขอรับใบอนุญาตต้องใช้ความพยายามอย่างดีที่สุด เพื่อป้องกันไม่ให้สิ่งที่ตนให้บริการถูกใช้ไปเพื่อการทำละเมิดกฎหมายใดๆ" จนเกิดการวิพากษ์วิจารณ์ว่าการประกาศปิดกั้นเว็บไซต์ เป็นประกาศที่ชอบหรือไม่ และตัวคณะกรรมการฯ เองก็น่าจะละเมิด MSC Bill Of Guarantees ข้อ7 กำหนดว่า "จะไม่มีการตรวจสอบ ปิดกั้นอินเทอร์เน็ต"[32] ในขณะที่มาตรา 3 (3) ในเรื่อง Act of State ระบุว่า "ไม่มีบทบัญญัติใดในพระราชบัญญัติที่สามารถตีความได้ว่า ให้อำนาจรัฐในการสั่งให้เซ็นเซอร์อินเทอร์เน็ต" ได้

- เดือนมีนาคม 2009 ผู้ใช้อินเทอร์เน็ต 8 รายถูกฟ้องร้องว่าดูหมิ่นสุลต่านของรัฐ Perak ว่าเกี่ยวข้องกับกระบวนการวิกฤตทางการเมือง หนึ่งในนั้นคือ Azrin Mohd Zain

- Karpal Singh ถูกฟ้องคดีโดยอาศัยอำนาจตาม มาตรา 4 (1) (b) แห่งพระราชบัญญัติยั่วยุปลุกระดม (Sedition Act) ด้วยเหตุที่เขาแสดงความคิดเห็นเกี่ยวกับสุลต่าน Perak

5. ปฏิกิริยา และความเคลื่อนไหวฝ่ายประชาชนหรือสังคมที่มีต่อกฎหมายหรือนโยบายที่กระทบเสรีภาพในสื่อออนไลน์

5.1 จัดตั้งองค์กรโดยมีเป้าหมายเพื่อเรียกร้องสิทธิมนุษยชน และให้รัฐบาลยกเลิกกฎหมายฉบับต่าง ๆ ที่ไม่เป็นธรรมโดยเฉพาะอย่างยิ่งกฎหมายความมั่นคงภายใน (ISA)

หลังจากรัฐบาลมาเลเซียใช้กำลังเข้าปราบปรามการเรียกร้องสิทธิของชาวจีนในประเทศมาเลเซีย (ซึ่งรัฐบาลเรียกว่า “ปฏิบัติการลาลัง”) ในปี 1987 ได้เกิดองค์กรเอกชนองค์กรหนึ่งขึ้น โดยใช้ชื่อว่า “SUARAM”[33] (เสียงประชาชนมาเลเซีย) ซึ่งตั้งขึ้นปี 1989 ในเหตุการณ์ดังกล่าว รัฐบาลใช้อำนาจตามกฎหมายความมั่นคงภายใน (ISA) บุกจับกุมนักการเมืองฝ่ายค้าน สื่อมวลชน นักเคลื่อนไหวทางการเมืองและสังคม และปัญญาชนกว่า 100 คน ทำให้ญาติพี่น้องของผู้ถูกจับกุมรวมตัวกันเพื่อคอยให้ความช่วยเหลือนักโทษดังกล่าว จนเมื่อนักโทษการเมืองเหล่านี้ได้รับการปล่อยตัว องค์กร SUARAM ก็ถูกก่อตั้งขึ้น เพื่อให้ความช่วยเหลือแก่ผู้ที่ได้รับผลกระทบจากการบังคับใช้กฎหมาย ISA และเรียกร้องให้รัฐบาลยกเลิก ISA มีการเผยแพร่ความรู้และข้อมูลเรื่องสิทธิเสรีภาพ อีกทั้งพยายามสร้างวัฒนธรรมประชาธิปไตยในองค์กรเพื่อเป็นแบบอย่างแก่สังคมมาเลเซีย นอกจากนี้ยังมีการเรียกร้องให้ปฏิรูปองค์กรตำรวจ รวมทั้งเรียกร้องเสรีภาพในการแสดงความคิดเห็นทางการเมืองและการเลือกตั้งอย่างเสรี โปร่งใส และยุติธรรม

ภายหลังเหตุการณ์ที่รัฐบาลมาเลเซียจับกุมตัวนายอันวา อิบรอฮิม ซึ่งหลายฝ่ายมองว่าเป็นการใช้อำนาจโดยไม่ชอบธรรม ยังผลให้กลุ่มแนวร่วมที่ทำงานต่อต้านรัฐบาลมาเลเซียขยายตัวขึ้น เกิดเป็นเครือข่าย

พันธมิตรของกลุ่มที่สนับสนุนนายอันวา อิบรอฮิม กลุ่มเรียกร้องสิทธิเสรีภาพ และองค์กร SUARAM ซึ่งได้กลายมาเป็นแกนหลักของแนวร่วมนี้ในการเรียกร้องให้รัฐบาลยกเลิกกฎหมายความมั่นคง ทำให้องค์กร SUARAM มีบทบาท และได้รับความนิยมเพิ่มมากขึ้น

5.2 ผลักดันประเด็นการเมือง ให้ความสำคัญกับเสรีภาพในการแสดงความคิดเห็น รวมทั้งประท้วงคัดค้านการคุกคามสิทธิเสรีภาพโดยกลุ่มบล็อกเกอร์ และนักข่าวพลเมือง

ผลจากการที่รัฐบาลมาเลเซียวางแผนการพัฒนาระบบเทคโนโลยีสารสนเทศในประเทศไว้หลายโครงการ โดยเฉพาะอย่างยิ่งโครงการ “Multimedia Super Corridor” ซึ่งเป็นโครงการพัฒนาเทคโนโลยีสารสนเทศขนาดใหญ่เพื่อทำให้ประเทศมาเลเซียเป็นฮับของเอเชียตะวันออกเฉียงใต้ ในเรื่องดังกล่าว ทำให้ประชาชนมาเลเซียกว่า 14 ล้านคน สามารถเข้าถึงอินเทอร์เน็ตได้ ซึ่งโครงการนี้จำเป็นต้องไม่มีข้อจำกัด หรือมีข้อจำกัดน้อยที่สุดในการเข้าถึงข้อมูลข่าวสาร เพื่อไม่ให้กลายเป็นจุดอ่อนทางการค้าการพาณิชย์ ประกอบกับรัฐบาลมาเลเซีย หลังยุคของ ดร.มหาธีร์ มูฮาหมัด ซึ่งมีความเป็นเผด็จการน้อยกว่า จึงทำให้เสรีภาพในการรับรู้ข้อมูลข่าวสารต่างๆ ผ่านอินเทอร์เน็ตเติบโตขึ้นด้วย และในช่วงหลายปีที่ผ่านมาได้เกิดบล็อกเกอร์ รวมทั้งนักข่าวพลเมือง (Citizen Journalist) จำนวนมากในประเทศมาเลเซีย ซึ่งจำนวนไม่น้อยรวมตัวกันเพื่อผลักดันให้ประเด็นทางการเมือง การตั้งคำถาม การวิพากษ์วิจารณ์นโยบายและการทำงานของรัฐบาล ซึ่งเป็นเรื่องที่ไม่เคยถูกพูดถึงอย่างเปิดเผยในที่สาธารณะเกิดขึ้นในสื่อออนไลน์

อย่างไรก็ตาม ดังกล่าวไปแล้วว่าแม้รัฐบาลมาเลเซียจะประกาศและให้คำมั่นสัญญานับตั้งแต่มีโครงการพัฒนาเทคโนโลยีสารสนเทศว่ารัฐบาลจะไม่เซ็นเซอร์ข้อมูลข่าวสารในอินเทอร์เน็ต แต่ในความเป็นจริงความพยายามในการแทรกแซง กระทั่งคุกคามเสรีภาพในสื่อออนไลน์โดยรัฐบาลมาเลเซียกลับเกิดขึ้นอย่างต่อเนื่อง เว็บไซต์ทั้งระดับภายในประเทศ

และระดับสากลถูกผู้ให้บริการอินเทอร์เน็ตในประเทศปิดกั้นช่องทางการเข้าถึงสำนักข่าวออนไลน์ถูกคณะกรรมการ MCMC สั่งให้ปลดหรือลบข้อความออก มีการจับกุมและดำเนินคดีกับบล็อกเกอร์ชาวมาเลเซียหลายคน โดยเฉพาะอย่างยิ่งบล็อกเกอร์ที่เขียนบทความวิพากษ์วิจารณ์สังคม และการเมืองของประเทศมาเลเซียที่ได้รับความนิยมจากผู้อ่านจนก่อให้เกิดกระแสการประท้วงคัดค้านการกระทำของรัฐบาล เหตุการณ์สำคัญที่เกิดขึ้น ก็อาทิ กรณีที่อาทันตูยา (Altantuya) นักแปลชาวมองโกเลียถูกฆาตกรรมและศพถูกนำไปทำลาย ซึ่งเกิดขึ้นเดือนตุลาคม ปี 2006 และบรรดานักข่าวพลเมืองรายงานว่า นอกจากเธอจะเป็นนักแปลแล้วอทันตูยายังเป็นนายหน้าค้าอาวุธด้วย ซึ่งการฆาตกรรมครั้งนี้เกี่ยวพันกับการคอร์รัปชั่นในรัฐบาลมาเลเซีย ยังผลให้ Raja Petra Kamarudin ซึ่งเป็นที่รู้จักกันดีจากเว็บไซต์ Malaysia Today ซึ่งรายงานข่าวเรื่องนี้ ถูกจับกุมและควบคุมตัวโดยอาศัยกฎหมายความมั่นคงภายใน (Internal Security Act) ซึ่งได้เกิดกระแสวิพากษ์วิจารณ์การกระทำของรัฐบาล และมีการประท้วงเรียกร้องโดยกลุ่มนักข่าวพลเมืองให้ปล่อยตัวเขา

อีกกรณีหนึ่ง คือ กรณีที่หนังสือพิมพ์ New Straits Times ซึ่งผู้ถือหุ้นใหญ่ คือ บริษัทการลงทุนของพรรคอัมโน ฟ้องบล็อกเกอร์ของบล็อก Jeff Ooi (www.jeffooi.com) ในความผิดฐานละเมิด เนื่องจากมีการโพสต์บทความที่มีเนื้อหาบางส่วนวิพากษ์วิจารณ์การรายงานข่าวของนิวสเตรทไทม์ พร้อมทั้งตั้งคำถามถึงจรรยาบรรณในการนำเสนอข่าว ยังผลให้เสื่อมเสียชื่อเสียงต่อหนังสือพิมพ์ จากเหตุฟ้องร้องนี้ทำให้นักข่าวพลเมืองจำนวนหนึ่งช่วยกันขยายประเด็นนี้ออกไปในวงกว้างมากขึ้นในอินเทอร์เน็ต ซึ่งได้รับการตอบรับและให้ความร่วมมือ กระทั่งมีการรวมตัวกันเป็นกลุ่มที่เรียกว่า “WWU: Walk With Us” เพื่อคัดค้านการฟ้องร้องดำเนินคดีดังกล่าว โดยระบุว่าสิทธิและเสรีภาพการแสดงความคิดเห็นเป็นสิ่งที่ต้องปกป้องไว้ให้ประชาชนทุกคน

กรณีล่าสุด ก็คือ การรวมตัวกันของกลุ่มผู้ใช้บริการเครือข่ายสังคมออนไลน์ร่วมกันเปิดประเด็น และสะท้อนปัญหาที่รัฐบาลมาเลเซีย

พยายามควบคุม และลิดรอนเสรีภาพในการแสดงความคิดเห็น สู่สาธารณะ ซึ่งได้รับการตอบรับอย่างมาก จนเมื่อวันที่ 10 พฤศจิกายน 2007 ซึ่งเป็นเวลาก่อนที่ประเทศมาเลเซียจะจัดการเลือกตั้งทั่วไปในปี 2008 บรรดานักกิจกรรมและประชาชนมาเลเซียกว่า 30,000 คน ร่วมกันเดินขบวนโดยใช้เวลา 2 วัน 2 คืน มีเป้าหมายเพื่อเรียกร้องให้รัฐบาลมาเลเซียเห็นความสำคัญของสิทธิมนุษยชน หยุดการลิดรอนเสรีภาพการแสดงความคิดเห็น และต้องจัดการเลือกตั้งที่กำลังจะเกิดขึ้นให้มีความบริสุทธิ์ยุติธรรม

5.3 เกิดลักษณะของการใช้มาตรการควบคุมสื่อมวลชนโดยสาธารณชน (Public Control)

หากพิจารณาตาม “ทฤษฎีเสรีภาพสื่อ”[34] อาจกล่าวได้ว่า สื่อมวลชนกระแสหลักในประเทศมาเลเซียนั้น เป็นสื่อมวลชนที่ทำงานโดยใช้แนวทางตามแบบ “ทฤษฎีอำนาจนิยม” (The Authoritarian Theory) กล่าวคือ เป็นสื่อที่คอยรับใช้อำนาจรัฐ ซึ่งสื่อในลักษณะนี้รัฐไม่จำเป็นต้องแทรกแซง เพราะสื่อเป็นกิจการของรัฐเองอยู่แล้ว มีหน้าที่ประชาสัมพันธ์กิจการงานให้แก่รัฐ ส่งเสริมนโยบาย และโครงการของรัฐ ไม่ใช่สื่อประเภทที่คอยทำหน้าที่เฝ้าระวังการทำงานของรัฐ (watch dog) แบบสื่อในประเทศเสรีนิยมทั่วๆ ไป ในประเทศมาเลเซีย สื่อกระแสหลักล้วนมีความใกล้ชิดหรือถือหุ้นหลักโดยพรรครัฐบาล แม้สื่อสิ่งพิมพ์ และสื่อกระจายเสียงจำนวนมากจะเป็นของเอกชน แต่ในประเทศมาเลเซียนั้นเอกชนผู้เป็นเจ้าของสื่อเหล่านั้นก็มักมีความสัมพันธ์ใกล้ชิดพรรคร่วมรัฐบาล เจ้าของสถานีโทรทัศน์ TV3, MegaTV หรือสถานีโทรทัศน์ดาวเทียมอย่าง Astro รวมทั้งเจ้าของหนังสือพิมพ์รายใหญ่อย่าง Berita Harian, Utusan Malaysia โดยเฉพาะอย่างยิ่ง New Straits Times ซึ่งถือเป็นหนังสือพิมพ์ที่มีอิทธิพลมากที่สุดในมาเลเซีย ล้วนแล้วแต่มีสัมพันธ์ใกล้ชิดกับพรรคพันธมิตร BN หรือมีหุ้นส่วนใหญ่เป็นบริษัทตัวแทนของพรรคอัมโน (Umno)[35]

อย่างไรก็ตาม ในระยะหลังที่ผ่านมา โดยเฉพาะอย่างยิ่งภายหลัง

โครงการ “Multimedia Super Corridor” ที่รัฐบาลมาเลเซียส่งสัญญาณว่าต้องการปล่อยเสรีสื่ออินเทอร์เน็ตเพื่อการพัฒนาประเทศ ก็มีรายงานอ้างอิงตัวเลขของสำนักตรวจสอบยอดพิมพ์มาเลเซีย ระบุว่า ยอดพิมพ์ของหนังสือพิมพ์รายวันในมาเลเซียของหนังสือพิมพ์เกือบทุกฉบับเริ่มลดลงอย่างต่อเนื่อง ในเดือนมิถุนายน ปี 2008 ยอดการพิมพ์ลดลงมาอยู่ที่ 2.5 ล้านฉบับต่อวัน จากเดิม 2.54 ล้านฉบับต่อวัน ในปีก่อนหน้า ทั้งกระแสที่พลเมืองมาเลเซียค่อยๆ หมดความเชื่อถือในเนื้อหาข่าวต่างๆ ที่นำเสนอโดยสื่อกระแสหลัก ในขณะที่สื่อออนไลน์ โดยเฉพาะอย่างยิ่งเว็บบล็อกที่เขียนวิเคราะห์ข่าวและเหตุการณ์บ้านเมืองที่สำคัญๆ เกิดขึ้นถึง 8 แห่ง ในระยะเวลาเพียง 2 ปีเท่านั้น โดยมีทั้งข่าวภาษาจีน ภาษามาเลย์ ภาษาทมิฬ และภาษาอังกฤษ ซึ่งบล็อกข่าวบางแห่งมีผู้ใช้บริการกดเข้าชมมากถึงเดือนละ 2 ล้านครั้ง ทั้งเว็บไซต์ที่มีเนื้อหาเป็นฝ่ายตรงข้ามกับรัฐบาลหรือเรียกร้องให้เกิดการปฏิรูปการเมืองเกิดขึ้นไม่ต่ำกว่า 50 เว็บไซต์ อัตราการลดลงของสื่อดั้งเดิม และอัตราขยายตัวของสื่อใหม่ รวมทั้งจำนวนบล็อกเกอร์ และนักข่าวพลเมืองที่เพิ่มขึ้นอย่างต่อเนื่องในประเทศมาเลเซีย สามารถสะท้อนให้เห็นภาพได้ว่าพลเมืองมาเลเซียจำนวนหนึ่งกำลังต้องการข้อมูลข่าวสารที่หลากหลายกว่าที่นำเสนออยู่เพียงแต่ในสื่อกระแสหลัก ทั้งอาจต้องการพื้นที่ในการแสดงความคิดเห็นของตนเพิ่มมากขึ้นด้วยและการลดอัตราการบริโภคหนังสือพิมพ์ลงนี้ นอกจากเป็นการส่งสัญญาณว่าสื่อออนไลน์กำลังค่อยๆ ยึดพื้นที่สื่อมากขึ้นแล้ว ยังเป็นการควบคุมหรือโต้ตอบการทำงานของสื่อกระแสหลักไปด้วยในตัว ซึ่งมีลักษณะของการใช้ “มาตรการควบคุมสื่อโดยสาธารณชน”[36] (Public Control) กล่าวคือ การที่สาธารณชนไม่ว่าจะเป็นบุคคลหรือกลุ่มบุคคลมีปฏิกิริยาตอบกลับไปยังสื่อมวลชน เพื่อควบคุมเนื้อหาของสื่อด้วยการงดใช้ งดรับสื่อเหล่านั้น

การรุกคืบพื้นที่ข่าว และบทความของสื่อออนไลน์ในประเทศมาเลเซีย และผลพวงจากการทำหน้าที่วิพากษ์วิจารณ์การเมือง และการนำเสนอข่าวที่แตกต่างไปจากสื่อกระแสหลักของสื่อออนไลน์บางสำนัก โดยเฉพาะอย่างยิ่ง Malaysiakini [37] ก่อให้เกิดปรากฏการณ์ครั้งสำคัญในวงการ

สื่อสารมวลชน คือ กระแสการเรียกร้องให้ “ปฏิรูปสื่อ” ในช่วงปี 1990 ถึง 2000 ซึ่งมีนักหนังสือพิมพ์ของสื่อกระแสหลักกว่า 900 คน ยื่นหนังสือต่อรัฐบาลเสนอให้แก้ไขพระราชบัญญัติการพิมพ์และสิ่งพิมพ์ (Printing Presses and Publications Act)

6. บทสรุป

แม้ประเทศมาเลเซียจะประกาศหรือพยายามแสดงเจตจำนงว่ารัฐบาลมาเลเซียจะไม่เซ็นเซอร์หรือปิดกั้นการเผยแพร่ข้อมูลในสื่ออินเทอร์เน็ต รวมทั้งออกกฎหมายมารับรองคุ้มครองเสรีภาพของประชาชนในเรื่องนี้ เพราะต้องการให้มาเลเซียเป็นศูนย์กลางด้านเทคโนโลยีสารสนเทศของกลุ่มประเทศอาเซียน แต่ในความเป็นจริงแล้ว หากพิจารณากฎหมายมาเลเซียทั้งระบบ ไม่เฉพาะกฎหมายที่เกี่ยวพันกับเทคโนโลยีคอมพิวเตอร์ หรืออินเทอร์เน็ต (Cyber Laws) เท่านั้น ย่อมพบว่า จนถึงปัจจุบันรัฐบาลมาเลเซียยังคงเข้มงวดอย่างมากกับการใช้กฎหมายฉบับต่างๆ โดยเฉพาะอย่างยิ่งกฎหมายที่เกี่ยวกับความมั่นคง เพื่อควบคุมการเผยแพร่ในลักษณะกระจายเสียงและสื่อสิ่งพิมพ์ รวมไปถึงการเผยแพร่คำพูดที่หมิ่นเหม่ทางกฎหมายหรือไม่เหมาะสมบนเว็บไซต์ด้วย ทั้งนี้รูปแบบของการควบคุมมีปรากฏทั้งในแง่ของการตั้งคณะกรรมการดูแลเนื้อหา (MCMC) และออกคำสั่งไปยังผู้ให้บริการอินเทอร์เน็ตภายในประเทศให้ปิดกั้นช่องทางการเข้าถึงเว็บไซต์ที่มีเนื้อหาไม่ถูกต้องเหมาะสม แจ้งเตือนไปยังเจ้าของเว็บไซต์ผู้เผยแพร่ข้อมูลให้ปลดเนื้อหาที่ผิดกฎหมาย หรือไม่เหมาะสมออกภายในระยะเวลากำหนด (Notice and Takedown) และจับกุม ดำเนินคดี หรือควบคุมตัว โดยไม่มีการแจ้งข้อกล่าวหากับนักเขียนบล็อกอิสระ หรือนักข่าวพลเมืองที่เผยแพร่ข่าว หรือนำเสนอบทวิเคราะห์สถานการณ์บ้านเมืองที่กระทบต่อรัฐบาลบนสื่อออนไลน์ ลักษณะของการควบคุมการนำเสนอข้อมูลข่าวสารไม่ว่าในสื่อประเภทใดๆ ที่เกิดขึ้นในประเทศมาเลเซียอีกประการหนึ่งที่ย่อมมีผลกระทบต่อเสรีภาพในการแสดง

ความคิดเห็นของประชาชนด้วย ก็คือ ผู้ประกอบการด้านสื่อในประเทศมาเลเซียมักมีความเกี่ยวข้องสัมพันธ์กับคนในพรรคร่วมรัฐบาล

ทัศนคติและแนวนโยบายในการมุ่งเน้นไปที่การจำกัดเสรีภาพในการแสดงความคิดเห็นในสื่อทุกๆ ประเภทนี้ เคยมีนักวิชาการพยายามอธิบายว่า เกิดจากหลายสาเหตุ เช่น เป็นผลมาจากโครงสร้างของรัฐบาลกลางที่ในช่วงแรกไม่เข้มแข็งพอภายใต้บริบทของการรวมตัวกันเป็นรัฐรวม จึงทำให้รัฐบาลพยายามหาช่องทางตามกฎหมายเพื่อบริหารประเทศและแก้ปัญหาต่างๆ แบบรวบอำนาจไว้ที่ตนเอง ซึ่งสามารถสะท้อนออกมาในหมวด 11 ของรัฐธรรมนูญมาเลเซีย โดยเฉพาะอย่างยิ่งอำนาจในการประกาศสถานการณ์ฉุกเฉินและควบคุมพรรคฝ่ายค้าน รวมทั้งการวิพากษ์วิจารณ์การทำงานของรัฐบาล ซึ่งแน่นอนว่าวิธีการเช่นนี้ย่อมส่งผลกระทบต่อเสรีภาพในการพูดและการแสดงความคิดเห็นของประชาชนด้วย นอกจากนี้ การที่มาตรา 10 (2) (a) รัฐธรรมนูญ ใช้คำว่า “รัฐสภาโดยกฎหมายกำหนด” ก็สามารถสื่อนัยได้ว่า ในความเป็นจริงแล้วรัฐสภาไม่ได้เป็นอิสระจากฝ่ายบริหาร ยังมีการอุปถัมภ์กันทางการเมืองระหว่างสมาชิกผู้สมัครของพรรคและหัวหน้าพรรคการเมืองที่ถูกเลือกตั้ง กับนายกรัฐมนตรี ซึ่งบุคคลเหล่านี้มีหนี้บุญคุณที่ค้างชำระกับฝ่ายบริหารอยู่ และในที่สุดแล้วก็ไม่มีประโยชน์อะไรที่จะต่อต้าน หรืออธิบายความหมายของการจำกัดเสรีภาพในการพูด เพราะ “ข้อจำกัดเสรีภาพ” แท้ที่จริงแล้วก็คือ “ข้อไม่จำกัดของผู้มีอำนาจ”

บทบาทและการใช้อำนาจของศาลในเรื่องเหล่านี้ก็ถูกตั้งคำถามอย่างมากในประเทศมาเลเซีย เพราะระหว่างปี 1957 และ 1981 องค์กรศาลถูกแทรกแซงจนขาดความเป็นอิสระ เพราะองค์ประกอบของคณะรัฐมนตรีประกอบด้วยหัวหน้าศาลและผู้นำทางการเมือง หลังสงครามโลกครั้งที่สองซึ่งมีภัยคุกคามจากคอมมิวนิสต์ ทั้งศาลและนักการเมืองจึงมีความรับผิดชอบร่วมกันในการสร้างชาติ ดังนั้น การพิพากษาคดีที่เกี่ยวกับความมั่นคงของชาติซึ่งหลายๆ กรณีมีผลกระทบโดยตรงต่อเสรีภาพในการพูดและการแสดงความคิดเห็นของประชาชน ศาลมักให้อำนาจและความอิสระที่กว้างขวางมากควบคุมสิ่งเหล่านี้โดยข้ออ้างเพื่อปกป้องรัฐ

มรดกทางความคิดอันสำคัญเกี่ยวกับเรื่องนี้ที่ตกทอดจากยุคก่อนมาถึงปัจจุบัน ก็คือ ฝ่ายบริหารไม่ให้ความสนใจอำนาจการตรวจสอบถ่วงดุลโดยองค์กรศาล และเชื่อมั่นในการกระทำของฝ่ายตนอย่างมาก ซึ่งย่อมไม่เป็นประโยชน์เลยต่อสังคมชาวมาเลเซีย ในขณะที่บทบัญญัติในรัฐธรรมนูญรวมทั้งกฎหมายปกครองฉบับอื่นๆ ที่เกี่ยวกับการใช้อำนาจโดยฝ่ายรัฐยังคงลักษณะของการเขียนให้รัฐเป็นผู้ตัดสินใจ และใช้อำนาจได้ตามอำเภอใจ

อย่างไรก็ตาม แม้การควบคุมเสรีภาพในการรับรู้ข้อมูลข่าวสารหรือการแสดงความคิดเห็นของสื่อและประชาชนจะยังเกิดขึ้น และเริ่มหนักขึ้นในประเทศมาเลเซีย แต่ด้วยความที่โครงการต่างๆ ด้านเทคโนโลยีสารสนเทศมาเลเซียประสบความสำเร็จอย่างสูง และทำให้ประชาชนมาเลเซียกว่าร้อยละ 60 เข้าถึงอินเทอร์เน็ตได้ในราคาไม่แพง เป็นผลทำให้เกิดเว็บไซต์ บล็อก และบริการอื่นๆ ในอินเทอร์เน็ตขึ้นจำนวนมาก ชุมชนออนไลน์มาเลเซียจึงค่อนข้างเข้มแข็ง และสามารถรวมตัวกันต่อสู้เรียกร้องสิทธิต่างๆ และการปฏิบัติที่ชอบธรรมจากรัฐบาลได้ ไม่ว่าจะเป็นการเรียกร้องให้ปล่อยตัวบล็อกเกอร์ที่ถูกควบคุมตัวภายใต้กฎหมายความมั่นคง ประท้วงการปิดกั้นการเข้าถึงบริการบนอินเทอร์เน็ต กระทั่งร่วมกันโจมตีระบบคอมพิวเตอร์ หรือเว็บไซต์ของหน่วยงานรัฐบาลเพื่อตอบโต้การกระทำที่ไม่ชอบธรรมของรัฐบาล เป็นต้น

บทที่

บทวิเคราะห์เปรียบเทียบ
กฎหมาย 4 ประเทศ

ไทย

เยอรมนี

สหรัฐอเมริกา

และมาเลเซีย

---

1. หลักการคุ้มครองสิทธิและเสรีภาพในสื่อออนไลน์

จากการศึกษาบทบัญญัติที่ว่าด้วยการคุ้มครองเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นของทั้งสี่ประเทศรวมทั้งประเทศไทย ย่อมเห็นได้ว่าทุกประเทศล้วนแล้วแต่มีบทบัญญัติเพื่อยืนยันหลักการไว้ในรัฐธรรมนูญว่ารัฐมีหน้าที่ต้องให้ความคุ้มครองเสรีภาพดังกล่าว และถือเป็นเรื่องที่ทุกประเทศ (ควรต้อง) ยอมรับร่วมกันว่าเสรีภาพชนิดนี้เป็นเสรีภาพที่มีความสำคัญและจำเป็นอย่างยิ่งต่อการสร้างระบอบประชาธิปไตยที่แท้จริงให้เกิดขึ้นได้ นอกจากนี้ ในประเทศเยอรมนีและสหรัฐอเมริกานั้น เพื่อให้เกิดความชัดเจนยิ่งขึ้นและตัดปัญหาข้อโต้แย้งใดๆ ที่อาจเกิดขึ้นได้ในอนาคต จึงไม่เพียงแต่ในตัวบทกฎหมายที่เป็นลายลักษณ์อักษรเท่านั้นที่เขียนรับรองเสรีภาพดังกล่าวไว้ แต่โดยผลของการใช้การตีความ โดยเฉพาะอย่างยิ่งการใช้การตีความโดยองค์กรตุลาการยังได้มีการวางหลัก และขยายขอบเขตของการคุ้มครองให้ครอบคลุมไปถึงการใช้เสรีภาพใน “สื่อออนไลน์” อีกด้วย

อย่างไรก็ตาม ดังกล่าวไว้แล้วในรายงานวิจัยว่า เสรีภาพในเรื่องนี้ โดยเฉพาะอย่างยิ่งเสรีภาพในการแสดงความคิดเห็น เป็นเสรีภาพที่ต้องมีการแสดงออกมาภายนอก โอกาสที่จะเกิดการใช้เสรีภาพของตนไปล่วงละเมิดเสรีภาพของบุคคลอื่นจึงยังคงมีอยู่ ดังนั้น ในทางกฎหมายแล้ว ไม่ว่ารัฐใดๆ จึงไม่อาจให้ความคุ้มครองเสรีภาพประเภทนี้แบบ “เด็ดขาด” หรือแบบ “สัมบูรณ์” เหมือนกับเสรีภาพทางความคิด ความเชื่อ ความศรัทธา ได้ ดังจะเห็นได้ว่า รัฐธรรมนูญของประเทศที่ศึกษาไม่ว่าจะเป็นประเทศสหรัฐอเมริกา เยอรมนี จีน มาเลเซีย และประเทศไทย จึงบัญญัติ “ข้อยกเว้น” ไม่คุ้มครองเสรีภาพเหล่านี้ในบางเรื่อง ซึ่งเป็นลักษณะของการคุ้มครองเสรีภาพแบบ “สัมพัทธ์”

2. เนื้อหา หรือประเภทของความคิดเห็นที่ไม่อนุญาตให้เผยแพร่ หรือแสดงออกได้

ในปัญหาที่ว่าเรื่องราวหรือเนื้อหาอย่างไรที่รัฐไม่ให้ความคุ้มครอง หรือกล่าวอีกอย่างว่ารัฐมีอำนาจกำหนดขอบเขตของการเผยแพร่ หรือจำกัดเสรีภาพลงได้นั้น ย่อมขึ้นอยู่กับลักษณะการเมืองการปกครอง ศาสนา ความเชื่อ ขนบธรรมเนียม วัฒนธรรม ทัศนคติ และความใจกว้างของผู้มีอำนาจ รวมทั้งระดับของการให้ความสำคัญกับเสรีภาพประเภทนี้ของประชาชนในประเทศนั้นๆ ด้วย ซึ่งย่อมแตกต่างกันไป สำหรับประเทศเยอรมนีนั้น เนื้อหาที่ไม่ได้รับความคุ้มครองตามรัฐธรรมนูญ และอาจถูกกฎหมายจำกัดการเผยแพร่ หรือผู้กระทำมีความผิดและถูกลงโทษได้ ที่สำคัญๆ ก็คือ การเผยแพร่ข้อมูลที่มีเนื้อหาเป็นภัยอันตรายต่อเด็กและเยาวชน เป็นอันตรายต่อสันติภาพของประชาชน การดูถูกศักดิ์ศรีความเป็นมนุษย์ การเหยียดหยามเชื้อชาติอื่น รวมทั้งการเผยแพร่ลัทธิชาตินิยมเยอรมัน (นาซี) เป็นต้น ในขณะที่แม้ว่าประเทศสหรัฐอเมริกาจะให้ความสำคัญกับการคุ้มครองเด็กและเยาวชนเช่นเดียวกัน แต่สำหรับการแสดงความคิดเห็น หรือการพูดจาในเชิงเหยียดหยามความเป็นมนุษย์

ของบุคคลอื่น คนชนชาติอื่น หรือผิวสีอื่น รวมทั้งการเผยแพร่ลัทธิความเชื่อใดๆ แล้ว ประชาชนในสหรัฐอเมริกายังสามารถทำได้โดยเสรี เพราะได้รับความคุ้มครองตามรัฐธรรมนูญ

สำหรับประเทศที่ปกครองโดยระบบพรรคการเมืองเดียว หรือยังไม่มีความเป็นประชาธิปไตยอย่างประเทศจีน และมาเลเซีย การพูด การเขียน หรือการแสดงความคิดเห็นด้วยวิธีการใดๆ โดยเฉพาะอย่างยิ่งในสื่อออนไลน์ที่มีผู้คนจำนวนมากเข้าถึงได้ ต่อระบอบการเมืองการปกครอง รวมทั้งการวิพากษ์วิจารณ์การทำงานของรัฐบาลถือเป็นเรื่องต้องห้าม ทั้งนี้ ทั้งแบบที่ต้องห้ามอย่างเป็นทางการอย่างในประเทศจีน หรือต้องห้ามอย่างไม่เป็นทางการแบบในประเทศมาเลเซีย เหตุผลในเรื่อง “ความมั่นคงแห่งรัฐ” มักถูกขับเน้นให้เป็นประเด็นหลักของการจำกัดเสรีภาพตามกฎหมายของประเทศเหล่านี้ ซึ่งแม้แต่ในประเทศไทยที่ได้รับการอธิบายว่าเป็นประเทศประชาธิปไตยเอง ก็ยังปรากฏว่าประเด็นด้านความมั่นคง ยังถือเป็นเหตุผลลำดับต้นๆ เช่นกัน ในอันที่รัฐจะออกกฎหมายหรือมาตรการอย่างใดอย่างหนึ่งมาจำกัดการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นของประชาชน โดยเฉพาะอย่างยิ่ง กฎหมายที่เกี่ยวกับสถาบันพระมหากษัตริย์ ซึ่งตามประมวลกฎหมายอาญาไทยระบุไว้ใน “หมวดความมั่นคง”

อย่างไรก็ดี สำหรับในมาเลเซียนั้น นอกจากประเด็นปัญหาด้านความมั่นคง และเสถียรภาพของรัฐบาลแล้ว ด้วยความเชื่อและเคร่งครัดทางศาสนา การเผยแพร่เนื้อหาในเชิงวิพากษ์วิจารณ์ศาสนา หรือบรรดาเนื้อหาใดๆ ก็ตามที่อาจขัดต่อความเชื่อ ความศรัทธา หรือกฎระเบียบในศาสนาก็ถือเป็นเรื่องหลักๆ ที่ถูกต้องห้ามด้วย

3. ประเภทของกฎหมายที่จำกัดเสรีภาพในสื่อออนไลน์

จากผลการศึกษาจะเห็นได้ว่า กฎหมายที่แต่ละประเทศใช้เป็นเครื่องมือในการจำกัดการแสดงความคิดเห็นของประชาชนนั้น ไม่ได้มีแต่เฉพาะกฎหมายที่ว่าด้วยการกระทำความผิดในระบบหรือเครือข่าย

คอมพิวเตอร์เท่านั้น หากแต่ยังมีกฎหมายอื่นๆ ด้วย โดยในประเทศเยอรมนีจะใช้ประมวลกฎหมายอาญา (StGB) เป็นหลักเพื่อฟ้องลงโทษผู้กระทำความผิด นอกจากนี้ ก็คือ กฎหมายที่ว่าด้วยการคุ้มครองเด็กและเยาวชนจากสื่อสาธารณะประเภทต่างๆ และกฎหมายที่เกี่ยวกับการให้บริการโทรคมนาคม และทำนองเดียวกัน ในประเทศสหรัฐอเมริกานั้นจะมีการตราและบังคับใช้กฎหมายที่เกี่ยวกับการคุ้มครองเด็กและเยาวชนมากมายหลายฉบับ นอกเหนือจากนี้ ก็คือ กฎหมายในยุคใหม่ๆ ที่ถูกตราขึ้นเพื่อจำกัดเสรีภาพของประชาชนมากขึ้น โดยอ้างเหตุผลเพื่อป้องกันและปราบปรามการก่อการร้าย สำหรับประเทศจีนและประเทศมาเลเซียนั้น ปรากฏว่า กฎหมายที่เข้ามามีบทบาทสำคัญในการจำกัดเสรีภาพในสื่อประเภทต่างๆ รวมทั้งสื่อออนไลน์ด้วย คือกลุ่มกฎหมายที่เกี่ยวกับความมั่นคง และความปลอดภัยของรัฐ

อย่างไรก็ตาม เป็นที่น่าสังเกตด้วยว่า ประเทศต่างๆ ดังกล่าวมาไม่ได้อาศัยกฎหมายที่ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรืออาชญากรรมคอมพิวเตอร์เพื่อการควบคุมเนื้อหาของข้อมูล หรือกำกับตรวจสอบการรับรู้ข้อมูลข่าวสารหรือการติดต่อสื่อสารในสื่อออนไลน์เหมือนกับกรณีของประเทศไทย เพราะแม้แต่ในประเทศจีนเอง กฎหมายด้านเทคโนโลยีสารสนเทศที่เข้ามากำกับเสรีภาพของประชาชนก็ไม่ใช่กฎหมาย “สารบัญญัติ” ที่ว่าด้วยความผิดในระบบหรือเครือข่ายคอมพิวเตอร์ แต่คือกฎหมายที่เกี่ยวกับการประกอบกิจการด้านโทรคมนาคม ทั้งนี้เพื่อกำกับเนื้อหาผ่านทางผู้ให้บริการโดยอาศัยระบบการให้ใบอนุญาต ในขณะที่ประเทศมาเลเซียก็เคยประกาศอย่างชัดเจนว่าจะไม่ออกกฎหมายลายลักษณ์อักษรใดๆ ที่มีผลเป็นการจำกัดเสรีภาพในสื่อออนไลน์ เพราะหวังให้ผู้ใช้บริการมีเสรีภาพ และมาเลเซียจะเป็นศูนย์กลางของการให้บริการข้อมูลสารสนเทศ

4. ลักษณะการบัญญัติกฎหมายเพื่อจำกัดเสรีภาพในสื่อออนไลน์

ดังกล่าวมาโดยตลอดในงานวิจัยฉบับนี้ว่าการคุ้มครองสิทธิและเสรีภาพของประชาชนในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นไว้ในรัฐธรรมนูญนั้นจะไม่มีวันสัมฤทธิ์ผล หรือเกิดขึ้นได้จริงในทางปฏิบัติเลย หากปรากฏว่ารัฐโดยฝ่ายนิติบัญญัติบัญญัติกฎหมาย (ที่มีผลเป็นการจำกัดสิทธิและเสรีภาพในเรื่องนี้ของประชาชน) ในฐานะที่เป็นเพียง “ข้อยกเว้นการคุ้มครองสิทธิและเสรีภาพ” ดังกล่าวไว้อย่างกว้างขวาง คลุมเครือไม่ชัดเจน เพราะกฎหมายเช่นว่านั้นจะกลับกลายเป็นช่องว่างของการคุ้มครอง ย่อมสุ่มเสี่ยงที่เจ้าหน้าที่รัฐ หรือฝ่ายผู้บังคับใช้กฎหมายจะตีความบทกฎหมายที่คลุมเครือเหล่านั้นเกินเลยไปจาก “หลักการ” จนทำให้กลายเป็นเครื่องมือละเมิดสิทธิของประชาชนได้ตามอำเภอใจ ซึ่งย่อมไม่สอดคล้องกับเจตนารมณ์แห่งรัฐธรรมนูญที่ต้องการให้รัฐ คุ้มครองสิทธิและเสรีภาพของประชาชนเป็นหลัก และให้การจำกัดเป็นเพียงข้อยกเว้น แต่จากการศึกษาพบว่าประเทศต่างๆ ก็ยังคงมีบทบัญญัติที่มีถ้อยคำอันคลุมเครือดังกล่าวปรากฏอยู่

อย่างไรก็ดี ปฏิเสธได้ยากว่าเรื่องใดๆ ก็ตามที่เกี่ยวข้องกับ “ความมั่นคงของรัฐ” นั้น ถือเป็นเรื่องนามธรรมที่หาคำจำกัดความหรือคำอธิบายที่ชัดเจนได้ยากว่าหมายถึงสิ่งใดกันแน่ ดังนั้น โดยปกติแล้วประเทศที่ไม่ได้ให้ความสำคัญกับ “ปัญหาความมั่นคง และเสถียรภาพของรัฐ” มากไปกว่า “ปัญหาความมั่นคง พฤติกรรมและนิติฐานะของประชาชน” จึงมักพยายามใช้ให้น้อยที่สุดเท่าที่จำเป็น หรือหลีกเลี่ยงไม่ใช้เหตุผลเรื่อง “ความมั่นคงแห่งรัฐ” มาเป็นข้อจำกัดเสรีภาพของประชาชนเลย ดังจะเห็นได้ว่า กฎหมายของประเทศเยอรมนีและประเทศสหรัฐอเมริกาไม่ค่อยปรากฏเรื่องดังกล่าวมากเท่ากับประเทศจีนหรือประเทศมาเลเซีย อนึ่ง แม้การห้ามเผยแพร่เนื้อหาที่จะทำให้เกิดความแตกแยกในหมู่ประชาชนตามประมวลกฎหมายอาญาของประเทศเยอรมนีจะยังปรากฏความคลุมเครือปรากฏอยู่บ้าง แต่ควรต้องสังเกตด้วยว่าบทบัญญัติดังกล่าวยังคงให้น้ำหนักกับ

การคุ้มครองความปลอดภัยของประชาชน มากกว่าการคุ้มครองเสถียรภาพของรัฐ หรือของรัฐบาล หรือในกรณีของประเทศสหรัฐอเมริกาก็มีแนวบรรทัดฐานคำพิพากษาของศาลกำกับกฎหมายไว้อีกชั้นหนึ่งว่า รัฐจะจำกัดเสรีภาพของประชาชนได้ก็ต่อเมื่อรัฐแสดงเหตุผลหรือพยานหลักฐานเบื้องต้นได้ว่า การใช้เสรีภาพเช่นว่านั้นจะส่งผลกระทบอย่างร้ายแรงต่อรัฐหรือส่วนรวมจริงเท่านั้น เป็นต้น ซึ่งลักษณะเหล่านี้ย่อมแตกต่างจากกฎหมายของประเทศไทยที่ยังปรากฏถ้อยคำอันคลุมเครืออยู่ในหลายมาตรา ไม่ว่าจะเป็นคำว่า “ขัดต่อความมั่นคง” “ทำให้ประชาชนตื่นตระหนก” “ขัดต่อความสงบเรียบร้อย” โดยเฉพาะอย่างยิ่ง “ขัดต่อศีลธรรมอันดีของประชาชน” ดังที่บัญญัติไว้ในมาตรา 14 และ 20 พ.ร.บ. คอมพิวเตอร์ฯ 2550 ซึ่งเป็นบทบัญญัติหลักที่เกี่ยวกับการเผยแพร่เนื้อหาในสื่อออนไลน์

5. ภาระหน้าที่ ความรับผิด และการลงโทษตัวกลาง หรือผู้ให้บริการสื่อออนไลน์

ด้วยปัญหาในแง่ของการสืบทราบและติดตามผู้กระทำความผิดซึ่งเป็นผู้เผยแพร่ข้อความในสื่อออนไลน์โดยตรงมาลงโทษ ทำให้ในปัจจุบันหลายๆ ประเทศพยายามหันมาสร้างกฎหมาย หรือหลักเกณฑ์อื่นใดเพื่อกำหนด “ภาระหน้าที่” และ “ความรับผิดชอบ” ให้กับบรรดาผู้ให้บริการโทรคมนาคมและผู้ให้บริการอินเทอร์เน็ต โดยหวังให้ผู้ประกอบการเหล่านี้คอยช่วยตรวจสอบการกระทำความผิด หรือช่วยแบ่งเบาภาระของเจ้าหน้าที่รัฐนั่นเอง อาทิเช่น ประเทศเยอรมนีเคยออกกฎหมายกำหนดให้ผู้ให้บริการโทรคมนาคมและอินเทอร์เน็ตจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการอินเทอร์เน็ตทุกคนไว้ไม่น้อยกว่า 6 เดือน (Telekommunikationsgesetz) เพียงแต่ในท้ายที่สุด บทบัญญัติดังกล่าวถูกศาลรัฐธรรมนูญพิพากษาว่าขัดกับรัฐธรรมนูญเยอรมันจึงทำให้สิ้นผลใช้บังคับไป นอกจากนี้เยอรมนียังมีกฎหมายที่เกี่ยวกับการบริการโทรคมนาคม (Telemediengesetz และ Mediendienste-Staatsvertrag)

เขียนจำแนกแยกแยะประเภทของการให้บริการอินเทอร์เน็ต เพื่อกำหนดภาระหน้าที่และความรับผิดชอบแก่ผู้ให้บริการอินเทอร์เน็ตแต่ละประเภท ทั้งนี้ ภายใต้เงื่อนไขที่ต้องพิจารณาบทบาท ความเกี่ยวข้องใกล้ชิดกับเนื้อหา รวมทั้งความรู้เห็นถึงการเผยแพร่เนื้อหาเหล่านั้นของผู้ให้บริการแต่ละประเภท และล่าสุดก็คือ กรณีที่กฎหมายฉบับหนึ่งกำหนดให้ผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต (Access Provider) มีหน้าที่ต้องปิดกั้นช่องทางการเข้าถึงเว็บไซต์ที่เผยแพร่ภาพลามกอนาจารเด็กและเยาวชนตามรายชื่อที่สำนักงานตำรวจแห่งชาติรวบรวมไว้ (Zugangserschwerungsgesetz) แต่ศาลรัฐธรรมนูญก็พิพากษาให้กฎหมายฉบับนี้สิ้นผลบังคับใช้ไปแล้ว เป็นต้น

เช่นเดียวกับประเทศเยอรมนี ในกรณีของประเทศสหรัฐอเมริกาก็มีบทบัญญัติที่กำหนดให้ผู้ให้บริการโทรคมนาคมต้องคอยจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ให้เจ้าหน้าที่ตรวจสอบเช่นกัน (Stored Communications หรือ SCA) รวมทั้งกำหนดความรับผิดแก่ผู้ให้บริการอินเทอร์เน็ตด้วย หากมีข้อเท็จจริงว่าบุคคลเหล่านี้เข้าไปมีส่วนรู้เห็นหรือเกี่ยวข้องกับการเผยแพร่เนื้อหาที่เป็นภัยต่อเด็กและเยาวชน (Communication Decency Act) อย่างไรก็ตาม มีข้อที่ควรสังเกตว่าลักษณะของการกำหนดภาระหน้าที่และความผิดแก่ผู้ให้บริการอินเทอร์เน็ตของทั้งประเทศเยอรมนีและสหรัฐอเมริกานี้มีหลักเช่นเดียวกันว่า ห้ามมิให้ปฏิบัติต่อผู้ให้บริการในลักษณะเช่นเดียวกับผู้ใช้บริการซึ่งเป็นผู้กระทำความผิดที่แท้จริง รวมทั้งจะนำผู้ให้บริการอินเทอร์เน็ตไปเทียบเคียงกับบรรณาธิการหรือผู้กลั่นกรองเนื้อหาในสื่อดั้งเดิมประเภทอื่นๆ ไม่ได้ เพราะทั้งจำนวนข้อมูล และความรวดเร็วของอินเทอร์เน็ตแตกต่างจากสื่อดั้งเดิมเหล่านั้นอย่างมาก ชนิดที่มิอาจกำหนดภาระหน้าที่และความรับผิดชอบแบบเดียวกันได้ ซึ่งกรณีนี้ย่อมแตกต่างจากลักษณะของมาตรา 15 แห่ง พ.ร.บ. คอมพิวเตอร์ฯ 2550 ของประเทศไทยที่กำหนดให้ผู้ให้บริการมีความรับผิดเท่ากับผู้กระทำความผิดที่แท้จริง

สำหรับประเทศจีนนั้นพบว่ามีกฎหมายหลายฉบับที่ใช้เพื่อควบคุมและกำกับบทบาทของผู้ให้บริการสื่อออนไลน์ โดยเฉพาะอย่างยิ่ง

กฎหมายที่เกี่ยวกับใบอนุญาตประกอบกิจการ ไม่ว่าจะเป็น Provisions on the Administration of Electronic Publications หรือ Provisions on the Administration of Internet Electronic Bulletin Board Service รวมทั้ง Measures for the Administration of Internet Information Services นอกจากนี้ ก็มีกฎหมายกำหนดให้ผู้ให้บริการร้านอินเทอร์เน็ตต้องจัดเก็บข้อมูลต่างๆ ของลูกค้าเพื่อให้เจ้าหน้าที่รัฐตรวจสอบด้วย (Regulation on the Administration of Internet Access Service Business Establishments [Internet Cafes]) ในส่วนของประเทศมาเลเซียนั้น เพื่อให้เป็นไปตามคำมั่นสัญญาที่รัฐบาลเคยประกาศไว้กับประชาชนและนานาชาติว่า ประเทศมาเลเซียจะไม่ออกกฎหมายใดๆ ที่มีลักษณะของการจำกัดเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นในอินเทอร์เน็ต ดังนั้น จนถึงปัจจุบันประเทศมาเลเซียจึงไม่ปรากฏกฎหมายพิเศษที่กำหนดความรับผิดต่อการเผยแพร่ข้อมูลใดๆ ของทั้งผู้ใช้บริการและผู้ให้บริการโดยตรง นอกเหนือจากที่มีอยู่แล้วในประมวลกฎหมายอาญาประเทศมาเลเซีย แม้จะได้ปรากฏข่าวการจับกลุ่มผู้ใช้อินเทอร์เน็ต รวมทั้งสื่อพลเมืองอยู่เนืองๆ แต่ก็เป็นไปตามกฎหมายความมั่นคง อย่างไรก็ดี ดังกล่าวมาแล้วว่าปัจจุบันประเทศมาเลเซียมีกฎหมายอย่างน้อย 2 ฉบับที่กำหนดให้อำนาจกับคณะกรรมการเฉพาะด้านโทรคมนาคม เข้ากับกำกับตรวจสอบการใช้สื่อเพื่อไม่ให้ผู้ให้บริการ หรือบุคคลอื่นใดให้หรือใช้บริการเนื้อหาที่ไม่เหมาะสม กล่าวคือ The Communications and Multimedia Act (CMA) และ The Communications and Multimedia Commission Act (CMCA) ซึ่งกฎหมายสองฉบับนี้เองที่ทำให้เกิด Guidelines on Content หรือ “แนวปฏิบัติเกี่ยวกับเนื้อหา” สำหรับผู้ประกอบการ เพื่อใช้เป็นมาตรฐานร่วมกัน และทำให้การปฏิบัติตามกฎหมายเกิดขึ้นจริง โดยผ่านระบบหรือกลไกการควบคุมกันเอง (self-regulation) ภายใต้ประมวลจริยธรรมหรือจรรยาบรรณของผู้ให้บริการ (The Content Code)

ข้อเปรียบเทียบนโยบายและแนวปฏิบัติแห่งรัฐ

1) การใช้มาตรการปิดกั้นช่องทางการเข้าถึงข้อมูล หรือเว็บไซต์

กล่าวได้ว่า การปิดกั้นเว็บไซต์เกิดขึ้นได้กับทุกๆ ประเทศ แตกต่างกันก็เพียงแต่ประเทศใดจะใช้มาตรการนี้มาก หรือน้อยกรณีกว่ากันเท่านั้น แม้แต่ในประเทศเยอรมนีที่มีลักษณะของความเป็นประชาธิปไตย และให้ความสำคัญกับการคุ้มครองเสรีภาพในการแสดงความคิดเห็นของประชาชนอย่างมากแล้วก็ตาม ทั้งนี้ ด้วยเหตุผลตามกฎหมายที่แตกต่างกันไป และนอกจากนี้การใช้อำนาจของรัฐเพื่อปิดกั้นการเข้าถึงนี้ก็อาจมีทั้งที่เป็นแบบ “ทางการ” เช่นปิดโดยอาศัยกฎหมายในสถานการณ์ปกติโดยผู้ว่าการรัฐฯ โดยคำสั่งศาลหรืออัยการ และการปิดกั้นอย่าง “ไม่เป็นทางการ” กล่าวคือ มีการใช้อำนาจอย่างลับๆ จากฝ่ายรัฐสั่งไปยังผู้ให้บริการกระทั่งตั้งหน่วยพิเศษคอยตรวจสอบและปิดกั้นโดยเฉพาะโดยไม่ให้ใครรู้ อย่างที่เคยเกิดขึ้นแล้วเช่นกันในประเทศสหรัฐอเมริกากับกรณีที่เกี่ยวกับสงครามตะวันออกกลาง หรือความไร้มนุษยธรรมในการกักขังเชลยศึก อย่างไรก็ตาม ดังกล่าวไปแล้วเช่นกันว่า กรณีของประเทศเยอรมนีนั้น การปิดกั้นช่องทางการเข้าถึงสื่อออนไลน์ที่ผ่านๆ มาอยู่ภายใต้ขอบเขตของกฎหมายที่ค่อนข้างชัดเจน และกระทำไปโดยยึดหลักแห่งความได้สัดส่วนหรือพอสมควรแก่เหตุ โดยเฉพาะอย่างยิ่ง การปิดกั้นมีกระบวนการขั้นตอนและวิธีการดำเนินการที่ประชาชนสามารถตรวจสอบ หรือโต้แย้งคัดค้านได้ จึงแตกต่างกับประเทศจีน มาเลเซีย หรือกระทั่งประเทศไทยเอง ที่นอกจากบทบัญญัติในตัวกฎหมายเองจะยังมีความคลุมเครือไม่ชัดเจนแล้ว เหตุผลในการปิดกั้นก็ไม่ชัดเจน ไม่มีการบอกแจ้งผู้ได้รับผลกระทบ หลายๆ กรณีเกิดขึ้นโดยอาศัยกฎหมายพิเศษที่มีโทษรุนแรง และให้อำนาจรัฐโดยไม่อนุญาตให้องค์กรอื่นใดหรือประชาชนตรวจสอบความชอบของการใช้อำนาจเหล่านั้นได้ นอกจากนี้ การปิดกั้นจำนวนไม่น้อยเกิดขึ้นอย่างไม่เป็นทางการ ซึ่งยากที่จะมีพยานหลักฐานพิสูจน์หรือตรวจสอบ และการปิดกั้นลักษณะนี้เกิดขึ้นไม่น้อยในประเทศมาเลเซีย ถึงแม้ว่าประเทศมาเลเซียจะมีบทบัญญัติ

ลายลักษณ์อักษรที่รับรองการไม่เซ็นเซอร์อินเทอร์เน็ตปรากฏอยู่ที่มาตรา 3 (3) แห่งพระราชบัญญัติการสื่อสารและมัลติมีเดีย ปี 1998 (The Communications and Multimedia Act (CMA) Article 3 (3) "... Nothing in this Act shall be construed as permitting the censorship of the Internet.") ด้วยก็ตาม

สำหรับประเทศจีนนั้น ด้วยเหตุที่รัฐบาลจีนมีทัศนคติว่ารัฐมีอำนาจเต็มที่ในการตรวจสอบ และปิดกั้นเว็บไซต์ทุกประเภทได้เพื่อประโยชน์ของชาติ การปิดเว็บไซต์จำนวนมากที่ผ่านมาจึงไม่มีการแจ้งเตือนผู้ให้บริการเว็บเหล่านั้นล่วงหน้าแต่อย่างใด โดยผู้ถูกปิดกั้นดังกล่าวไม่มีโอกาสในการอุทธรณ์การปิดกั้นนั้น อีกทั้งเครื่องมือในการปิดกั้นเว็บไซต์ของจีน (Great Firewall) ยังทรงประสิทธิภาพมากที่สุดในโลกเพราะนอกจากตรวจสอบหาถ้อยคำไม่พึงประสงค์ของรัฐได้แล้ว ยังสามารถป้องกันการใช้เสิร์ชเอนจินเพื่อค้นหาเว็บไซต์ที่รัฐไม่พึงประสงค์ได้อีกด้วย

อนึ่ง เป็นที่น่าสังเกตอย่างยิ่งว่า แม้ประเทศต่างๆ จะดำเนินการปิดกั้นเว็บไซต์ ซึ่งมีจำนวนมากน้อยแตกต่างกัน แต่ก็ไม่ปรากฏว่าหน่วยงานผู้รับผิดชอบในเรื่องนี้เปิดแถลงข่าวถึงจำนวนเว็บไซต์ที่ถูกปิดกั้นไปในฐานะที่เป็น "ผลงาน" การบริหาร อย่างที่กระทำกันอยู่ในประเทศไทยเกือบทุกสมัยของรัฐมนตรีว่าการกระทรวงไอซีที

2) องค์กรที่จัดตั้งขึ้นเพื่อกำกับดูแลเนื้อหาในสื่อออนไลน์

จากการศึกษาพบว่าทุกประเทศที่ศึกษาล้วนมีหน่วยงานพิเศษที่ถูกจัดตั้งขึ้นโดยเฉพาะเพื่อทำหน้าที่ในการตรวจสอบดูแลเนื้อหาในสื่อออนไลน์ โดยภารกิจของหน่วยงานเหล่านั้นอาจแตกต่างกันไปตามแนวนโยบายที่เกี่ยวกับอินเทอร์เน็ตและสื่อออนไลน์ของแต่ละประเทศ ในประเทศเยอรมนี มีองค์กรที่ทำหน้าที่ตรวจสอบเนื้อหาในสื่อที่เด็กและเยาวชนอาจเข้าถึงได้ ในขณะที่หน่วยงานพิเศษในสหรัฐอเมริกาจะเน้นหนักด้านการสอดแนมคนที่มีแนวโน้มจะเป็นผู้ก่อการร้าย และประเทศมาเลเซียมีองค์กรเฉพาะทำหน้าที่กำกับดูแลเนื้อหาในอินเทอร์เน็ตที่ตั้งขึ้นใหม่ตาม

กฎหมาย 2 ฉบับ The Communications and Multimedia Act (CMA) และ The Communications and Multimedia Commission Act (CMCA)

สำหรับประเทศจีนนั้น ได้ก่อตั้งหน่วยงานพิเศษขึ้นจำนวนมาก ทั้งยังขยายอำนาจให้หน่วยงานรัฐเดิมที่ควบคุมสื่อประเภทอื่นให้รวมถึงสื่อออนไลน์ด้วย เพื่อคอยควบคุมตรวจสอบเนื้อหาในสื่อออนไลน์ ทั้งนี้ ไม่ว่าจะเป็น General Administration of Press and Publication (GAPP) ซึ่งเป็นหน่วยงานพิจารณาให้ใบอนุญาตการประกอบกิจการพิมพ์ The State Administration of Radio, Film, and Television (SARFT) ที่มีหน้าที่พิจารณาใบอนุญาตประกอบกิจการสื่อออนไลน์ อยู่ภายใต้การบังคับบัญชาของ Ministry for Information Industry, The State Council Information Office เป็นหน่วยงานกำหนดกฎเกณฑ์ที่เกี่ยวกับการแสดงความคิดเห็นบนสื่อทุกประเภท รวมทั้งการจดทะเบียนเว็บไซต์ The Ministry of Industry and Information Technology (MIIT) มีหน้าที่กำหนดกฎเกณฑ์ด้านอุตสาหกรรม ข้อมูลข่าวสารและเทคโนโลยี เช่น กำหนดให้คอมพิวเตอร์ทุกเครื่องในประเทศจีนต้องติดตั้งโปรแกรมตรวจสอบ (Pre-installed), The Internet Affairs Bureau of the State Council Information Office มีหน้าที่ควบคุมการดำเนินกิจกรรมบนอินเทอร์เน็ตของประชาชนโดยเฉพาะ หน่วยงานนี้จะเฝ้าระวังและปิดกั้นการเข้าถึงเว็บไซต์ที่มีเนื้อหาเกี่ยวกับภาพลามกและการก่อการร้าย หรือองค์การที่เรียกว่า Bureau Five และ Bureau Nine ที่ถูกตั้งขึ้นเพื่อติดตามความเคลื่อนไหวต่างๆ ที่เกิดขึ้นบนสื่อออนไลน์ เป็นต้น เหล่านี้ยังไม่ได้รวมองค์กรที่ปฏิบัติการทางจิตวิทยาซึ่งรัฐบาลจัดตั้งขึ้นภายใต้ชื่อ “สมาคมอินเทอร์เน็ตแห่งประเทศจีน” (The Government-connected Internet Society) เพื่อรณรงค์ให้ผู้ให้บริการอินเทอร์เน็ตปิดกั้นเนื้อหาที่รัฐบาลจีนเห็นว่าไม่เหมาะสม รวมทั้งการว่าจ้างกลุ่มพลเมืองเน็ตที่ใช้ชื่อว่า “50 Cent Party” ให้คอยเผยแพร่ข้อความสนับสนุนนโยบายและการบริหารประเทศของรัฐบาลจีนด้วย

ทั้งนี้ จะพบว่าสถานการณ์ในประเทศจีนดังกล่าวคล้ายคลึงกับประเทศไทย ที่มีการจัดตั้งหน่วยงาน หรือองค์กรเฉพาะขึ้นหลาย

หน่วยงานเพื่อทำหน้าที่ตรวจสอบเนื้อหาในอินเทอร์เน็ต แต่สิ่งที่แตกต่างจากประเทศจีน ก็คือ หน่วยงานที่ตั้งขึ้นมาหลายหน่วยงานทำหน้าที่ซ้ำซ้อนกัน หรือมีอำนาจทับซ้อนกันอย่างมาก จนอาจทำให้ประชาชน รวมทั้งผู้ปฏิบัติงานเกิดความสับสนได้ เช่น “ศูนย์ประสานความร่วมมือปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศและการสื่อสาร” หรือ ICT CORP ซึ่งตั้งขึ้นในสมัยที่นายมั่น พัทธโนทัยเป็นรัฐมนตรีว่าการกระทรวงไอซีที เกิดจากความร่วมมือหลายหน่วยงาน เช่น กองปราบปราม สำนักข่าวกรองแห่งชาติ และกรมสอบสวนคดีพิเศษ (DSI) มีภารกิจในการสืบสวนการก่ออาชญากรรมคอมพิวเตอร์และอาชญากรรมประเภทอื่นๆ ที่กระทำผ่านคอมพิวเตอร์ ตรวจจับและเฝ้าระวังเว็บไซต์ที่มีเนื้อหาหมิ่นประมาทกษัตริย์ “ศูนย์ปฏิบัติการความปลอดภัยอินเทอร์เน็ต” หรือ Internet Security Operation Center (ISOC) เพื่อประสานการทำงานกับหน่วยงานทหารและตำรวจ ภาระหน้าที่หลัก คือ เฝ้าระวังภัยคุกคามจากเนื้อหาที่ไม่เหมาะสมบนอินเทอร์เน็ต รวมทั้งปฏิบัติการและสนับสนุนการดำเนินคดีผู้กระทำความผิดคดีหมิ่นประมาทกษัตริย์ฯ ซึ่งตั้งขึ้นโดยกระทรวงไอซีที ในสมัยของ ร.ต.หญิง ระนองรักษ์ สุวรรณฉวี กองบังคับการปราบปรามอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) และกองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี (บก.ปอท.) สำนักงานตำรวจแห่งชาติ รวมทั้ง สำนักคดีเทคโนโลยีและสารสนเทศ ของกรมสอบสวนคดีพิเศษ (ดีเอสไอ) เป็นต้น ซึ่งแม้อำนาจหน้าที่ของหน่วยงานเหล่านี้จะมีบางส่วนที่แตกต่างกันไปบ้าง แต่ภารกิจหลักในระยะหลังที่ทุกๆ องค์กรดังกล่าวมามีเหมือนกัน ก็คือ การตรวจสอบเนื้อหาที่มีการกล่าวถึง วิพากษ์วิจารณ์ หรือหมิ่นประมาทกษัตริย์ฯ อนึ่ง เหล่านี้ยังไม่ได้นับรวม “โครงการสร้างลูกเสือไซเบอร์” ในสมัยที่นายจุติ ไกรฤกษ์เป็นรัฐมนตรีไอซีที ซึ่งเปรียบเสมือนการตั้งองค์กรพิเศษขึ้นใหม่ เพื่ออบรมให้สมาชิกทำหน้าที่ตรวจสอบเนื้อหาที่เกี่ยวกับพระมหากษัตริย์ในอินเทอร์เน็ต

3) สถิติคดี หรือการคุกคามผู้ให้ และผู้ใช้บริการอินเทอร์เน็ต

ในรายงานวิจัยฉบับนี้ คณะผู้วิจัยไม่สามารถค้นหาสถิติที่เป็นปัจจุบันอันเกี่ยวกับการจับกุม และการดำเนินคดีกับผู้ใช้ หรือผู้ให้บริการอินเทอร์เน็ตของประเทศที่ศึกษาที่มีความชัดเจนเพียงพอจะนำมาเปรียบเทียบเพื่อให้เห็นความแตกต่างกับประเทศไทยได้ โดยเฉพาะอย่างยิ่งคดีความผิดที่ว่าด้วยการเผยแพร่เนื้อหาผิดกฎหมาย หรือไม่เหมาะสมในสายตาของรัฐในสื่อออนไลน์ อย่างไรก็ตาม อาจกล่าวได้ว่าในบรรดาสี่ประเทศที่ทำการศึกษานี้ ประเทศจีนน่าจะเป็นประเทศที่ทั้งผู้ใช้และผู้ให้บริการอินเทอร์เน็ต โดยเฉพาะอย่างยิ่งกลุ่มคนที่เป็น “นักข่าวพลเมือง” ถูกจับกุม คุกคาม หรือถูกล่วงละเมิดสิทธิจากฝ่ายรัฐมากที่สุด ทั้งนี้ องค์การนิรโทษกรรมสากล (Amnesty International) ยังเคยกล่าวไว้ว่า “China has the largest recorded number of imprisoned journalists and cyber-dissidents in the world.”

โดยรัฐบาลประเทศจีนเริ่มจับกุมและจำคุกบรรดานักท่องเน็ต หรือนักกิจกรรมต่างๆ ที่หันมาใช้อินเทอร์เน็ตเป็นเครื่องมือในการเผยแพร่ข่าวสาร รวมทั้งวิพากษ์วิจารณ์การทำงานของรัฐบาลจีนตั้งแต่ปี 2001 และทยอยจับกุมคุมขังเรื่อยมาจนถึงปัจจุบัน คดีที่น่าสนใจ ก็อาทิ การจับกุม Shi Tao นักข่าวชาวจีนที่ใช้อีเมลส่วนตัวของเขาเองส่งข้อมูลไปยังเว็บไซต์นักเคลื่อนไหวเรียกร้องประชาธิปไตยในสหรัฐอเมริกา เพื่อแจ้งข่าวที่รัฐบาลจีนสั่งให้องค์กรด้านโทรคมนาคมขัดขวางงานรำลึกครบรอบ 15 ปี กรณีการปราบปรามนักเคลื่อนไหวเรียกร้องประชาธิปไตยเมื่อปี 1989 ทั้งนี้ Shi Tao ถูกจับในปี 2004 ด้วยข้อหานำความลับของประเทศไปแจ้งแก่หน่วยงานต่างประเทศ[1] หรือการจับกุม Huang Qi ในปี 2008 เพียงเพราะเขาให้ข่าวกับสื่อต่างประเทศ และเผยแพร่ข้อมูลในเว็บไซต์ของตัวเองเกี่ยวกับชะตากรรมของพ่อแม่ชาวจีนที่ต้องสูญเสียลูกจากกรณีโรงเรียนพังเพราะมีแผ่นดินไหวในประเทศจีน ด้วยข้อหาว่ามีไว้ในครอบครองซึ่งความลับของรัฐโดยมิชอบด้วยกฎหมาย[2] สำหรับประเทศที่ปรากฏการจับกุมนักข่าวออนไลน์บ่อยครั้งรองลงมา ก็คือ ประเทศมาเลเซีย โดยมีหลายกรณีที่เป็น

ข่าวใหญ่ และได้รับความสนใจจากกลุ่มผู้ใช้อินเทอร์เน็ตไม่ว่าจะเป็น กรณีการจับกุม Raja Petra Kamarudin กรรมการบริหารเว็บไซต์ Malaysia's Today หรือกรณี Khairul Nizam Abdul Ghani บล็อกเกอร์ www.aduka-taruna.blogspot.com ที่ถูกกล่าวหาว่าดูหมิ่นสถาบันพระมหากษัตริย์ รวมทั้ง Karpal Singh บล็อกเกอร์ที่ถูกฟ้องคดีโดยอาศัยอำนาจตาม มาตรา 4 (1) (b) แห่งพระราชบัญญัติยั่วยุปลุกระดม (Sedition Act) ด้วยเหตุที่เขาแสดงความคิดเห็นเกี่ยวกับ Sultan Perak เป็นต้น

เมื่อนำมาพิจารณาเปรียบเทียบกับประเทศไทยแล้ว ย่อมเห็นได้ว่าประเทศไทยก็ถือเป็นอีกประเทศหนึ่งที่มีสถิติการจับกุมดำเนินคดีกับบุคคลในเรื่องที่เกี่ยวกับการเผยแพร่เนื้อหาที่เข้าข่ายเป็นความผิดในอินเทอร์เน็ตจำนวนมากเช่นกัน ถึงแม้ว่าความถี่ในการจับกุมจะไม่ได้สม่ำเสมออย่างกรณีของประเทศจีนและมาเลเซียก็ตาม กล่าวคือ คดีจำนวนมากของประเทศไทยมักเกิดขึ้นในช่วงที่ประเทศมีความขัดแย้งทางการเมือง แต่มีข้อที่น่าสังเกตประการหนึ่งคือ ยังไม่ค่อยพบการจับกุมและดำเนินคดีกับผู้ให้บริการในฐานะของ "ผู้ให้บริการ" กล่าวคือ จับกุมผู้ให้บริการ เพียงเพราะเขาเป็น "ผู้ให้บริการ" ไม่ใช่ผู้โพสต์เผยแพร่ข้อความเหล่านั้นด้วยตนเอง ซึ่งต่างจากประเทศไทยที่คดีจำนวนไม่น้อยที่เกิดขึ้นรัฐฟ้องร้องและดำเนินคดีกับ "ผู้ให้บริการ" เพื่อให้รับผิดชอบในข้อความหรือเนื้อหาของผู้อื่น (ผู้ใช้บริการ) ไม่ใช่ของผู้ให้บริการเอง โดยเรื่องนี้อาจพอวิเคราะห์ได้ว่า ประเทศจีนและมาเลเซียต้องการกำกับดูแลผู้ให้บริการด้วยวิธีกำหนด "ภาระหน้าที่ต่าง ๆ" อาทิเช่น เก็บข้อมูลจราจรคอมพิวเตอร์ จัดให้มีการลงทะเบียนผู้ใช้อินเทอร์เน็ต ติดตั้งโปรแกรมกรองถ้อยคำ ฯลฯ มากกว่าการกำหนดให้ผู้ให้บริการต้องมีความรับผิดในการกระทำของผู้อื่น ทั้งนี้ โดยอาศัย "ระบบการขอใบอนุญาต" หรือมิเช่นนั้นก็สนับสนุนให้มี Code of Conduct ในระหว่างผู้ให้บริการด้วยกันเอง รวมทั้งมีการใช้ระบบ Notice & Takedown ร่วมด้วย ซึ่งเป็นนโยบายที่แตกต่างจากของประเทศไทยที่มุ่งเน้นความรับผิดของผู้ให้บริการมากกว่า ทั้ง ๆ ที่ยังไม่มีการกำหนดรายละเอียดที่จำเป็นเกี่ยวกับเรื่องนี้

ข้อเปรียบเทียบปฏิกิริยาภาคประชาชน

1) การให้ความสำคัญกับสิทธิเสรีภาพในเรื่องนี้ และความตื่นตัวในการตรวจสอบการละเมิดสิทธิผ่านกฎหมาย หรือแนวนโยบายแห่งรัฐ

เป็นที่น่าสังเกตว่า เมื่อเปรียบเทียบประเทศไทยกับประเทศในซีกโลกตะวันตกอย่างประเทศเยอรมนีและประเทศสหรัฐอเมริกาแล้ว จะพบว่าระดับของการให้ความสำคัญกับสิทธิและเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นในประเทศแถบตะวันออกถือว่าต่ำอยู่มาก ประชาชนทั่วไป รวมทั้งองค์กร นักกิจกรรมเคลื่อนไหวด้านสิทธิประชาชนเอง ยังไม่ค่อยให้ความสำคัญกับสิทธิและเสรีภาพในเรื่องนี้มากนัก โดยเฉพาะอย่างยิ่งเสรีภาพในสื่อออนไลน์ (ต่างกับการปิดกั้นโทรทัศน์ หรือวิทยุ) ในขณะที่ในประเทศเยอรมนีและประเทศสหรัฐอเมริกานั้น ทั้งภาครัฐและประชาชนต่างเห็นว่าสิทธิและเสรีภาพในเรื่องดังกล่าวมีความสำคัญอย่างยิ่งต่อกระบวนการสร้างประชาธิปไตย เพราะทำให้ประชาชนได้มีส่วนรวมทางการเมืองการปกครอง และสามารถแสดงเจตจำนงในเรื่องต่างๆ ได้อย่างอิสระ ในขณะที่ประชาชนจำนวนไม่น้อยในแถบซีกโลกตะวันออกยังเห็นว่าอินเทอร์เน็ตเป็นเพียงเครื่องมือในการสื่อสารระหว่างกัน เพื่อความบันเทิง หรือเพื่อความสุขเท่านั้น ไม่ได้มีไว้เพื่อวัตถุประสงค์ในทางการเมือง หรือวิพากษ์วิจารณ์สถานการณ์ความเป็นไปต่างๆ นอกจากนี้ยังเห็นว่าสิทธิและเสรีภาพส่วนบุคคลหากขัดต่อความสงบสุข และผลประโยชน์ของชาติแล้วบุคคลย่อมไม่อาจอ้างสิทธิและเสรีภาพดังกล่าวได้ ทั้งยังควรถูกจำกัดสิทธิเพื่อประโยชน์สุขของมหาชนโดยรวมอีกด้วย วิธีคิดเช่นนี้ปรากฏอย่างมากในประเทศไทย หรือกล่าวอีกอย่างก็คือ ประชาชนไทยจำนวนไม่น้อยเห็นว่า เสรีภาพชนิดนี้ไม่ควรถูกหยิบยกขึ้นกล่าวอ้างได้เลย หากเกี่ยวพันกับสถาบันกษัตริย์ฯ ศีลธรรมอันดี ความสงบสุขปรองดอง หรือการพยายามหลีกเลี่ยงความขัดแย้ง ในขณะที่รัฐบาลก็พยายามเล่นบทบาทในเชิงรุก เพื่อเสริมความแข็งแกร่งให้กับแนวคิดและความเชื่อดังกล่าวด้วยการโฆษณาชวนเชื่อหลากหลาย

รูปแบบ กระทั่งมอบบทบาทในการตรวจจับ และปิดกั้นความคิดเห็นซึ่งเคยเป็นของรัฐให้กับประชาชนกลุ่มต่างๆ

อย่างไรก็ตาม ในขณะที่รัฐบาลจีนจำเป็นต้องว่าจ้างกลุ่มประชาชนเพื่อให้คอยตรวจสอบและแจ้งเนื้อหาที่ผิดกฎหมาย หรือไม่เหมาะสมให้รัฐบาลปิดกั้น รวมทั้งช่วยโฆษณาชวนเชื่อกิจกรรมของรัฐบาล แต่ในประเทศไทยมักเป็นไปในลักษณะของการจัดตั้ง “โครงการของรัฐ” อย่างเป็นทางการ (เช่น ลูกเสือไซเบอร์) หรือมิเช่นนั้นก็มีการรวมกลุ่มเพื่อตรวจสอบประชาชนด้วยกันเอง เช่น กลุ่มยุทธการณ์ลงทัณฑ์ทางสังคม หรือกลุ่มรักสถาบันฯ เป็นต้น และด้วยเหตุผลต่างๆ ดังกล่าวมา ประกอบกับประเทศไทยใช้ พ.ร.บ.คอมพิวเตอร์ฯ 2550 เป็นกฎหมายฉบับหลักในการจำกัดเสรีภาพในเรื่องนี้ จึงทำให้ประชาชน และองค์กรที่เข้ามาทำหน้าที่คอยเฝ้าระวัง ตรวจสอบกฎหมาย หรือการใช้อำนาจของรัฐบาลที่หมิ่นเหม่ต่อการล่วงละเมิดสิทธิเสรีภาพในการแสดงความคิดเห็นของประชาชนอย่างเกินสมควร มีอยู่เพียงในวงจำกัดเฉพาะที่เกี่ยวข้องกับกฎหมายไอที หรือคนที่ทำงานหรือมีความเกี่ยวพันกับเทคโนโลยีสารสนเทศเท่านั้น

เป็นที่น่าสังเกตว่าประชาชน และองค์กรต่างๆ ในประเทศมาเลเซียดูเหมือนจะมีความตื่นตัวในเรื่องนี้มากกว่า และมาจากกลุ่มองค์กรที่ทำงานหลากหลายด้านกว่า สาเหตุหนึ่งอาจเป็นเพราะกฎหมายที่รัฐบาลมาเลเซียใช้เพื่อควบคุมจำกัดการแสดงความคิดเห็นไม่ใช่กฎหมายไอที หรือกฎหมายที่เกี่ยวกับคอมพิวเตอร์อย่างกรณีของประเทศไทย หากแต่เป็นกฎหมายว่าด้วยความมั่นคงแห่งรัฐ ดังนั้น กลุ่มบุคคลที่รู้สึกว่าตนได้รับผลกระทบจึงกว้างกว่า ดังจะเห็นได้ว่า ในประเทศมาเลเซียนั้น นอกจากกลุ่มบล็อกเกอร์ และนักข่าวพลเมืองแล้ว เครือข่ายพันธมิตรทางการเมืองอย่างกลุ่มที่สนับสนุนนายอันวา อิบรอฮิม กลุ่มเรียกร้องสิทธิเสรีภาพ กระทั่งองค์กร SUARAM ที่เรียกร้องสิทธิและเสรีภาพทางการเมืองในเรื่องอื่นๆ เป็นหลักอยู่ก่อน ก็ยังมีกิจกรรมเรียกร้องเสรีภาพในการแสดงความคิดเห็นที่ถูกปิดกั้นโดยกฎหมายความมั่นคงฉบับต่างๆ ของรัฐบาลด้วย

2) ลักษณะ และวิธีการเรียกร้อง หรือการแสดงปฏิกิริยาต่อกฎหมาย หรือนโยบายที่ไม่ชอบธรรม รวมทั้งผลสัมฤทธิ์ของฝ่ายประชาชน

ดังเคยกล่าวไว้ในรายงานวิจัยแล้วว่า ลักษณะการเคลื่อนไหวของภาคประชาชนในประเทศแถบซีกโลกตะวันออกมักยังจำกัดอยู่ในรูปแบบของการประท้วงเรียกร้องเชิงนโยบายและทางสังคมเท่านั้น ไม่ค่อยปรากฏการตอบโต้ หรือเรียกร้องเพื่อให้เกิดผลบังคับทางกฎหมายเหมือนในประเทศตะวันตกอย่างประเทศเยอรมนีหรือสหรัฐอเมริกา ซึ่งประชาชนและองค์กรต่างๆ ของประเทศเหล่านี้ นอกจากการจัดรณรงค์ ให้ความรู้ ประท้วงคัดค้านเชิงนโยบายแล้ว มักรวมตัวกันเพื่อใช้สิทธิในทางศาลฟ้องร้องหน่วยงานหรือเจ้าหน้าที่รัฐ เมื่อพบการใช้อำนาจหน้าที่ในทางที่มิชอบหรือละเมิดเสรีภาพของประชาชนอย่างเกินขอบเขตด้วย หรือมิเช่นนั้นก็นำเรื่องขึ้นศาลสูงหรือศาลรัฐธรรมนูญให้ตรวจสอบความชอบด้วยรัฐธรรมนูญของกฎหมายที่รัฐตราออกมาบังคับใช้ ในขณะที่องค์กรตุลาการโดยเฉพาะอย่างยิ่งศาลรัฐธรรมนูญทั้งของประเทศเยอรมนี หรือศาลสูงของประเทศสหรัฐอเมริกาก็เคยพิพากษาว่ากฎหมาย และมาตรการที่มีลักษณะล่วงละเมิดสิทธิและเสรีภาพของประชาชนเกินสมควรนั้นขัดรัฐธรรมนูญ และให้สิ้นผลบังคับใช้ไปแล้วหลายต่อหลายกรณี

สาเหตุที่ทำให้รูปแบบการเคลื่อนไหวของภาคประชาชนและสังคมในประเทศตะวันออกขาดความหลากหลายอาจมาจากหลายปัจจัย อาทิ ระบบการเมืองการปกครองที่ยังไม่มีความเป็นเสรีประชาธิปไตยเพียงพอ การไม่ยอมรับในความคิดเห็นที่แตกต่างในระหว่างประชาชนด้วยกันเอง ช่องทางการใช้สิทธิตามกฎหมายขาดความชัดเจน บางกรณีไม่ปรากฏว่ามีบทบัญญัติที่เปิดช่องให้ประชาชนอุทธรณ์คัดค้านคำสั่ง หรือการกระทำของฝ่ายรัฐได้ รวมถึงลักษณะการถ่วงดุลตรวจสอบการใช้อำนาจของฝ่ายนิติบัญญัติ และรัฐบาลขององค์กรตุลาการยังมีปัญหาในเรื่องความชอบธรรม รวมทั้งอคติและความไม่เป็นกลางของผู้พิพากษาปรากฏอยู่ จึงเป็นผลทำให้กลุ่มนักเคลื่อนไหวภาคประชาชน ซึ่งมักมีจำนวนไม่มากอยู่แล้วขาดกำลังใจ ไม่มีพลังอำนาจในการต่อรองกับรัฐที่เพียงพอ โดยเฉพาะ

อย่างยิ่งขาดความเชื่อมั่นในกระบวนการยุติธรรม และความซอบธรรมใน
การวินิจฉัยขององค์กรศาล

บทที่

ข้อเสนอแนะ

1. ข้อเสนอแนะทางกฎหมาย

1.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ควรเป็นกฎหมายอาญาที่กำหนดความผิดและโทษสำหรับ “อาชญากรรมคอมพิวเตอร์โดยแท้” หรือใช้กับการกระทำความผิดที่ผู้กระทำ “มุ่งหมายกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์” โดยตรงเท่านั้น เช่น การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยไม่มีอำนาจ การจารกรรมหรือดักรับข้อมูลคอมพิวเตอร์ การก่อวินาศกรรมระบบคอมพิวเตอร์หรือทำลายข้อมูลคอมพิวเตอร์ และการฉ้อโกงคอมพิวเตอร์ เป็นต้น เนื่องจากการกระทำเหล่านี้มี “องค์ประกอบความผิด” ในทางกฎหมายอาญาแตกต่างไปจาก “อาชญากรรมพื้นฐาน” อย่างการทำให้เสียทรัพย์ ลักทรัพย์ หรือบุกรุก จึงทำให้ไม่สามารถตีความกฎหมายที่มีอยู่เดิม (เช่น ประมวลกฎหมายอาญา) ให้ครอบคลุมไปถึงการกระทำรูปแบบใหม่ดังกล่าวได้ จนเป็นเหตุให้เกิดช่องว่างของกฎหมาย ด้วยเหตุนี้เอง การบัญญัติกฎหมายเฉพาะที่ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ จึงควรมี

วัตถุประสงค์หลักเพื่ออุดช่องว่างของกฎหมายหรือเพื่อมารองรับการดำเนินคดีกับผู้กระทำความผิดในรูปแบบใหม่ที่มีลักษณะในทางกฎหมายแตกต่างไปจากอาชญากรรมพื้นฐาน

สำหรับความผิดที่เกี่ยวกับการเผยแพร่ “เนื้อหา” ที่เป็นความผิดในสื่อออนไลน์นั้น เนื่องจากไม่ใช่การกระทำที่มี “องค์ประกอบความผิด” ในส่วนสาระสำคัญแตกต่างไปจากการเผยแพร่เนื้อหา (ที่เป็นความผิด) ต่อสาธารณชนหรือในสื่อประเภทอื่น โดยปกติแล้วจึงสามารถนำกฎหมายที่มีอยู่เดิมมาบังคับใช้ด้วยได้ ยกตัวอย่างเช่น มาตรา 287 ประมวลกฎหมายอาญา ซึ่งเป็นความผิดฐานเผยแพร่ภาพหรือสิ่งลามกอนาจารเพื่อประโยชน์ในทางการค้าย่อมสามารถใช้บังคับกับการเผยแพร่สิ่งดังกล่าวในสื่อออนไลน์ได้ ในขณะที่การเผยแพร่ข้อความที่ขัดต่อความมั่นคงแห่งราชอาณาจักรไม่ว่าจะทำในสื่อประเภทใดย่อมใช้มาตรา 116 หรือมาตราอื่นที่เกี่ยวข้องในประมวลกฎหมายอาญามาลงโทษได้อยู่แล้ว ทำนองเดียวกันกับการหมิ่นประมาทบุคคลอื่นที่ไม่ว่าจะทำด้วยวิธีการใดหรือในสื่อใดก็มีมาตรา 326 หรือ 328 ประมวลกฎหมายอาญารองรับอยู่ หรือแม้กระทั่งการหมิ่นประมาทกษัตริย์ฯ ก็มีมาตรา 112 ประมวลกฎหมายอาญา เป็นต้น ทั้งนี้ การบัญญัติฐานความผิดที่มี “องค์ประกอบความผิด” ที่ไม่แตกต่างกันในสาระสำคัญ ไว้กระจัดกระจายในกฎหมายหลายๆ ฉบับ นอกจากจะทำให้เกิดความสับสนแก่ประชาชนและเจ้าหน้าที่ผู้บังคับใช้กฎหมายแล้ว หากผู้บัญญัติกฎหมายนั้นเลือกใช้ถ้อยคำที่คลุมเครือไม่ชัดเจน (อย่างที่ปรากฏอยู่ในมาตรา 14 พ.ร.บ.คอมพิวเตอร์ฯ 2550 โดยเฉพาะอย่างยิ่ง มาตรา 14 (2)) ก็ย่อมก่อให้เกิดปัญหาในแง่ของการใช้การตีความขึ้นได้อีก ทั้งเมื่อกฎหมายให้ดุลนิพิจการตีความกับเจ้าหน้าที่อย่างกว้างขวาง โอกาสที่การใช้กฎหมายนั้นจะไปละเมิดเสรีภาพในการแสดงความคิดเห็นของประชาชนจนเกินสมควรก็ย่อมมีสูงตามไปด้วย

อนึ่ง หากรัฐยังเห็นว่าควรมีบทบัญญัติเฉพาะเพื่อใช้บังคับกับการเผยแพร่เนื้อหาซึ่งเป็นความผิดบน “สื่อออนไลน์” หรือต้องการให้การเผยแพร่นี้มีองค์ประกอบความผิดที่เข้มงวดยิ่งกว่าเดิม เช่น ประสงค์ให้การเผย

แพร่ภาพลามกในสื่อออนไลน์ ไม่ว่าจะทำไปเพื่อการค้าหรือไม่ก็ตามเป็นความผิดด้วย หรือต้องการให้การเผยแพร่ภาพลามกเด็กและเยาวชนมีโทษหนักกว่าปกติ รัฐก็อาจใช้วิธีการแก้ไขเพิ่มเติมความผิดเหล่านั้นไว้ใน หมวดความผิดพื้นฐานในเรื่องเดียวกัน เพราะมีลักษณะของการกระทำความผิด (คือ การเผยแพร่) เหมือนกัน ไว้ในประมวลกฎหมายอาญา หรือในกฎหมายหลักฉบับอื่นๆ ได้ ดังที่หลายประเทศ อาทิ ประเทศเยอรมนี ออสเตรีย หรือสวิตเซอร์แลนด์ ก็ใช้วิธีนี้

1.2 หากในท้ายที่สุดแล้ว ประเทศไทยยืนยันว่ามีความจำเป็นต้องบัญญัติฐานความผิดที่ว่าด้วยการ “เผยแพร่เนื้อหาที่เป็นความผิด” ในสื่อออนไลน์ไว้ใน พ.ร.บ.คอมพิวเตอร์ ฯ ด้วย คณะผู้วิจัยเห็นว่าบทบัญญัติเหล่านั้นก็ควรต้องกำหนด “เนื้อหาต้องห้ามมิให้เผยแพร่” ไว้ให้ชัดเจนกว่าที่เป็นอยู่ใน พ.ร.บ.คอมพิวเตอร์ฯ 2550 อย่างน้อยที่สุดก็ต้องมีความชัดเจนในระดับเดียวกันกับที่บัญญัติไว้ในประมวลกฎหมายอาญา เพื่อไม่ให้ขัดหรือแย้งกับ “หลักประกันในทางกฎหมายอาญา” ที่ว่า “กฎหมายต้องบัญญัติให้ชัดเจนไม่คลุมเครือ” (lege certa) ผู้บัญญัติกฎหมายจึงต้องพยายามอย่างถึงที่สุดที่จะหลีกเลี่ยงการใช้ถ้อยคำกำกวม มีความหมายกว้าง มีนิยามอิงอยู่กับยุคสมัย หรือสถานการณ์ความเป็นไปของบ้านเมือง หรือปล่อยให้เจ้าพนักงานใช้ดุลพินิจมากเกินไป อย่างเช่นคำว่า “ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน” “ขัดต่อความมั่นคงแห่งรัฐ” หรือ “ทำให้ประชาชนตื่นตระหนก” อีกทั้งกฎหมายเฉพาะที่จะบัญญัติใหม่นั้นก็ควรสอดคล้อง หรือคำนึงถึงเจตนารมณ์แห่งกฎหมายที่อยู่เบื้องหลังการกำหนดฐานความผิดในเรื่องเดียวกันนั้นด้วย ยกตัวอย่างเช่น ความผิดฐานหมิ่นประมาทบุคคลธรรมดานั้น ในประมวลกฎหมายอาญากำหนดให้เป็นความผิด “อาญาส่วนตัว” จึงเท่ากับว่ากฎหมายมุ่งประสงค์ให้ “ผู้เสียหายที่แท้จริง” จากการหมิ่นประมาทนั้นเท่านั้น เป็นผู้แจ้งความหรือฟ้องคดีกับผู้กระทำความผิดได้ และเนื่องจากเป็นความผิดที่กระทบประโยชน์ “ส่วนตัว” ซึ่งไม่ร้ายแรงหรือถึงขนาดทำให้สังคมหรือประโยชน์สาธารณะเสียหาย กฎหมายจึงเปิดโอกาสให้คู่กรณีตกลง “ยอมความ” กันได้

นอกจากนี้ ผู้กระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญายังมีสิทธิพิสูจน์ถึง “เหตุยกเว้นความผิด” (มาตรา 329 ประมวลกฎหมายอาญา) หรือ “เหตุยกเว้นโทษ” (มาตรา 330 ประมวลกฎหมายอาญา) ได้อีกด้วย เช่นนี้ เมื่อรัฐต้องการบัญญัติความผิดในลักษณะเดียวกันนี้ซ้ำอีกในกฎหมายเฉพาะฉบับใหม่ ผู้บัญญัติก็ควรพิจารณาด้วยว่าจะต้องนำเงื่อนไขและลักษณะต่างๆ ตามที่ปรากฏอยู่ในประมวลกฎหมายอาญามาบัญญัติไว้ด้วยหรือไม่ หรือหากไม่ต้องการให้นำเงื่อนไขและลักษณะดังกล่าวมาใช้ด้วย ก็ต้องมีเหตุผลอธิบายได้ว่าเหตุใดจึงไม่นำมาใช้

1.3 สำหรับการกำหนดภาระหน้าที่และความรับผิดแก่ “ผู้ให้บริการ” ซึ่งย่อมมีผลต่อเสรีภาพในการแสดงความคิดเห็นของประชาชนทั่วไปด้วย นั้น ควรพิจารณาทบทวน มาตรา 15 และมาตราอื่นๆ ที่เกี่ยวข้องแห่ง พ.ร.บ. คอมพิวเตอร์ฯ 2550 เพื่อแก้ไขเพิ่มเติมกฎหมายหลายประการ ดังนี้

- บทนิยามของคำว่า “ผู้ให้บริการ”[1] ควรบัญญัติให้สอดคล้องกับลักษณะการประกอบกิจการ และควรหมายเฉพาะผู้ให้บริการที่มีความเกี่ยวข้องกับระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์จริงๆ เท่านั้น ทั้งนี้ คณะผู้วิจัยเห็นว่าไม่ควรบัญญัติรวมเอา “ผู้ให้บริการโทรคมนาคม” หรือผู้ให้บริการอุปกรณ์ เครื่องมือ หรือช่องทางการติดต่อสื่อสารประเภทอื่นๆ เช่น ผู้ให้บริการโทรศัพท์บ้าน โทรศัพท์มือถือ (ที่เข้าถึงอินเทอร์เน็ตไม่ได้) วงจรเช่า หรือให้บริการดาวเทียม[2] ที่ไม่เกี่ยวกับการบริการคอมพิวเตอร์ หรือข้อมูลในคอมพิวเตอร์โดยตรงไว้ในกฎหมายฉบับนี้ ทั้งนี้ เพื่อไม่ให้เกิดความสับสนแก่ประชาชน ผู้ให้บริการ และผู้บังคับใช้กฎหมาย และเพื่อให้เป็นไปตามเจตนารมณ์ของ พ.ร.บ.คอมพิวเตอร์ฯ ที่มุ่งหมายใช้กับกิจกรรม หรือการกระทำความผิดที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ เท่านั้น อย่างไรก็ตาม หากรัฐต้องการกำหนดภาระหน้าที่ หรือความรับผิดชอบบางประการให้กับผู้ให้บริการโทรคมนาคมประเภทอื่นๆ ด้วย ก็ควรไปกำหนดไว้ในกฎหมายฉบับอื่นที่มีเนื้อหาเกี่ยวข้องกับการบริการของผู้ให้บริการโทรคมนาประเภทนั้นๆ โดยตรง อนึ่ง เป็นที่น่าสังเกตว่า บทบัญญัติที่กำหนดหน้าที่แก่ “ผู้ให้บริการ”

ให้เก็บรักษาข้อมูลจราจรทางโทรคมนาคมนั้น ในต่างประเทศไม่ได้กำหนดไว้ในกฎหมายอาชญากรรมคอมพิวเตอร์ หากแต่บัญญัติแยกไว้ในกฎหมายที่เกี่ยวกับการประกอบกิจการโทรคมนาคม[3]

- การกำหนดความรับผิดและโทษแก่ "ผู้ให้บริการ" สำหรับ "เนื้อหา" ซึ่งเป็นความผิดตามกฎหมายที่ลูกค้า หรือผู้ใช้บริการอินเทอร์เน็ตนำมาเผยแพร่ในพื้นที่หรือช่องทางการให้บริการของตน นั้น คณะผู้วิจัยเห็นว่าผู้บัญญัติกฎหมายควรจำแนกแยกแยะระดับของความรับผิดตามลักษณะและประเภทของผู้ให้บริการอินเทอร์เน็ต โดยคำนึงถึงความเกี่ยวข้องเชื่อมโยงกับเนื้อหาซึ่งเป็นความผิดเป็นสำคัญ อาทิเช่น ผู้ให้บริการเนื้อหา (Content Provider) ควรมีความรับผิดโดยตรงในเนื้อหาเหล่านั้น หรือหากมีพื้นที่หรือบอร์ดให้แสดงความคิดเห็นต่อท้าย ก็อาจต้องรับผิดด้วย หากได้รู้เห็นว่าเป็นเนื้อหาที่เป็นความผิด ผู้ให้บริการทางเทคนิคโดยแท้อย่างผู้ให้บริการเชื่อมต่อคอมพิวเตอร์กับอินเทอร์เน็ต (Access Provider) โดยหลักแล้วไม่ควรมีความรับผิดต่อเนื้อหาใดๆ เลย เว้นแต่เข้าเงื่อนไขบางประการตามที่กฎหมายกำหนด เช่น ในกฎหมายของประเทศเยอรมนี ผู้ให้บริการกลุ่มนี้จะมีความรับผิดก็ต่อเมื่อ พิสูจน์ได้ว่าเขาเป็นผู้คัดเลือก ปรับปรุง หรือเปลี่ยนแปลงข้อมูลที่เผยแพร่นั้นด้วยตนเอง แม้ข้อมูลนั้นจะไม่ใช่ของเขาเองก็ตาม หรือมิเช่นนั้นก็สมรู้หรือยินยอมให้มีการเผยแพร่ข้อมูลเช่นว่านั้น[4] สำหรับผู้ให้บริการให้เช่าพื้นที่ในการเก็บรักษาข้อมูล (Host Service Provider) โดยหลักแล้วไม่ควรต้องรับผิดต่อการกระทำของผู้ใช้บริการเช่นกัน เว้นแต่ได้รู้ถึงการมีอยู่แห่งเนื้อหาที่เป็นความผิดนั้นแล้วไม่ดำเนินการอย่างหนึ่งอย่างใดที่เหมาะสม โดยเฉพาะอย่างยิ่งเมื่อการรับรู้นั้นเกิดจากการบอกแจ้งผู้ได้รับความเสียหายจากข้อมูลนั้นเองหรือเจ้าหน้าที่ของรัฐ เป็นต้น นอกจากนี้ กฎหมายไม่ควรกำหนด "ภาระหน้าที่โดยทั่วไป" แก่ "ผู้ให้บริการ" กล่าวคือ ภาระหน้าที่ที่จะให้ต้องคอยตรวจสอบดูแลเนื้อหาในทุกๆ พื้นที่ที่ให้บริการของตนเองตลอดเวลาแม้ไม่มีใครบอกแจ้งก็ตาม เนื่องจากเป็นการเพิ่มภาระทั้งในด้านเวลา บุคลากร และงบประมาณแก่ผู้ประกอบการมากเกินสมควร ทั้งยังไม่สอดคล้องกับธรรมชาติของ

อินเทอร์เน็ตที่มีข้อมูลถูกรับ-ส่งบนเครือข่ายจำนวนมหาศาลภายในหน่วยเวลาในระดับวินาที ซึ่งอาจส่งผลต่อแรงจูงใจในการประกอบกิจการการให้บริการอินเทอร์เน็ต และมีผลต่อ “ราคา” การใช้บริการของผู้ใช้บริการอินเทอร์เน็ตโดยรวมได้ในที่สุด

ในส่วนของการกำหนดอัตราโทษที่จะลงแก่ผู้ให้บริการอินเทอร์เน็ต โดยเฉพาะอย่างยิ่ง กรณีที่เขาไม่ใช่ตัวการหรือผู้กระทำความผิดเองนั้น หากผู้บัญญัติกฎหมายประสงค์ให้ผู้ให้บริการ เข้ามาร่วมรับผิดชอบต่อการกระทำของผู้ใช้บริการอินเทอร์เน็ต หรือลูกค้าของตน ซึ่งเป็นเรื่องของการรับผิดใน “ความผิดของบุคคลอื่น” กฎหมายก็ไม่ควรกำหนดโทษไว้ให้ “เท่ากับ” ผู้กระทำความผิดที่แท้จริง แต่ควรใช้อัตราที่เหมาะสม ได้สัดส่วน รวมทั้งสอดคล้องกับหลักการในเรื่อง “ผู้กระทำความผิดหลายคน” (ตัวการ ผู้ใช้ ผู้สนับสนุน) ซึ่งผู้ใช้ ผู้สนับสนุนมีโทษมากน้อยลดหลั่นกันไปจากอัตราโทษที่กฎหมายกำหนดไว้สำหรับผู้กระทำความผิดซึ่งเป็นตัวการ อย่างไรก็ตาม แม้ผู้บัญญัติกฎหมายประสงค์จะกำหนดความรับผิดให้แก่ผู้ให้บริการ เพราะเหตุผลว่าผู้ให้บริการฯ นั้น “ละเลยไม่ปฏิบัติหน้าที่ของตนเอง” (ซึ่งไม่ได้อิงอยู่กับความผิดของบุคคลอื่น อย่างกรณีแรก) อัตราโทษที่จะกำหนดสำหรับกรณีนี้ก็ยิ่งไม่ควรกำหนดให้ “เท่ากับ” โทษของการเผยแพร่ข้อมูลที่มีเนื้อหาเป็นความผิด เพราะทั้งลักษณะของการกระทำและเจตนาของผู้ให้บริการฯ (ที่เพียงแค่ละเลยไม่ปฏิบัติหน้าที่ โดยไม่ได้มีเจตนาให้เกิดความเสียหายต่อผู้อื่นโดยตรง) ย่อมมีความแตกต่างจากการกระทำความผิดด้วยการเผยแพร่ข้อมูลที่มีเนื้อหาผิดกฎหมายนั้นเสียเอง ดังนั้น การที่ มาตรา 15 แห่ง พ.ร.บ.คอมพิวเตอร์ฯ 2550 บัญญัติให้ผู้ให้บริการมีโทษเท่ากับผู้กระทำความผิด จึงไม่ชอบด้วยหลักการทั้งปวง

กฎหมายควรระบุ “วิธีดำเนินการ” ที่ผู้ให้บริการต้องทำกับเนื้อหาที่เข้าข่ายผิดกฎหมายที่แสดงอยู่ในพื้นที่หรือขอบเขตการให้บริการของตนไว้ให้ชัดเจน ซึ่งโดยทั่วไปแล้วควรหมายเฉพาะการ “ลบ หรือปลดเนื้อหานั้นออกทั้งหมด หรือบางส่วน” จากพื้นที่ที่ให้บริการอยู่ไม่ว่าจะเพียงชั่วคราวหรือถาวรตามที่ได้รับแจ้งจากผู้เกี่ยวข้องหรือมีอำนาจหน้าที่ เท่านั้น ไม่

ควรหมายรวมถึงการ “ปิดกั้นช่องทางการเข้าถึงข้อมูลหรือเว็บไซต์” นั้นด้วย ทั้งนี้ เนื่องจากการปิดกั้นการเข้าถึงข้อมูลเป็นมาตรการที่ค่อนข้างรุนแรง และอาจส่งผลกระทบต่อเสรีภาพของบุคคลอื่นได้ไม่เฉพาะแต่ผู้ที่เผยแพร่ข้อมูลนั้นๆ เท่านั้น ฉะนั้น ฝ่ายรัฐจึงควรมีอำนาจอย่างจำกัดที่สุดในการใช้มาตรการเช่นว่านี้ หรือจะใช้ได้ก็ต่อเมื่อผ่านการตรวจสอบกลั่นกรองโดยองค์กรอื่นนอกเหนือจากองค์กรผู้บังคับใช้กฎหมายเสียก่อน ดังที่ใน พ.ร.บ.คอมพิวเตอร์ฯ 2550 เองก็กำหนดให้เจ้าหน้าที่ต้องขอคำสั่งปิดกั้นเว็บไซต์จากศาลตามมาตรา 20 อนึ่ง การระบุ “วิธีดำเนินการ” กับเนื้อหาที่เป็นความผิดไว้ให้ชัดเจนเช่นนี้ นอกจากจะทำให้กฎหมายไม่คลุมเครือและไม่เกิดปัญหาในขั้นตอนของการใช้การตีความแล้ว ยังเป็นไปเพื่อป้องกันไม่ให้เจ้าหน้าที่รัฐ หรือผู้มีอำนาจปกครองหลีกเลี่ยงการขอคำสั่งศาล แล้วหันไปใช้วิธีการ “ขอความร่วมมือ” หรือ “สั่งการ” ไปยังผู้ให้บริการ โดยตรงเพื่อให้ปิดกั้นเว็บไซต์ด้วย

เพื่อให้เกิดหลักเกณฑ์ที่แน่ชัดในการบอกแจ้งแก่ผู้ให้บริการอินเทอร์เน็ตทราบถึงเนื้อหาที่เป็นความผิด และเพื่อให้ผู้ให้บริการ ดังกล่าวสามารถดำเนินการกับเนื้อหาที่ได้รับแจ้งนั้นภายในระยะเวลาที่เหมาะสมได้ รัฐควรบัญญัติกฎหมาย หรือระเบียบปฏิบัติแล้วแต่ความเหมาะสมไว้ให้ชัดเจนเป็นลายลักษณ์อักษรเพื่อกำหนดรายละเอียดเกี่ยวกับ 1) ผู้มีอำนาจหน้าที่ในการแจ้งเนื้อหาที่เป็นความผิดนั้นต่อผู้ให้บริการ 2) วิธีการแจ้งที่มีผลตามกฎหมาย 3) เหตุผล เหตุอันควร หรือพยานหลักฐานเบื้องต้นที่ต้องแสดงแก่ผู้ให้บริการ หรือที่จะทำให้ผู้ให้บริการ ต้องดำเนินการกับเนื้อหาที่ได้รับแจ้ง 4) รายละเอียดของเนื้อหา และตำแหน่งอ้างอิงหรือแหล่งที่ตั้งบนอินเทอร์เน็ต (ยูอาร์แอล) ของเนื้อหานั้นซึ่งผู้แจ้งควรมีหน้าที่ต้องระบุด้วย รวมทั้ง 5) ระยะเวลาที่เพียงพอ และเหมาะสมที่ผู้ให้บริการจะสามารถใช้สืบค้นเพื่อลบหรือดำเนินการกับเนื้อหาที่แจ้งได้ ฯลฯ การกำหนดหลักเกณฑ์ไว้เช่นนี้ย่อมทำให้การจำกัดเสรีภาพของประชาชนผ่านกลไกความร่วมมือจากผู้ให้บริการมีมาตรฐาน มีขอบเขตที่ชัดเจน ทั้งยังเป็นไปตามหลักการ “แจ้งและลบ” (Notice and Takedown[5]) ซึ่งหลายประเทศ

ให้การยอมรับว่าเป็นวิธีการที่เหมาะสม และนำไปบังคับใช้แล้ว นอกจากนี้ยังเป็นการให้ “ความเป็นธรรม” กับผู้ให้บริการ ที่ได้รับแจ้งเนื้อหาด้วย เพราะหากผู้ให้บริการฯ ดังกล่าวถูกเจ้าหน้าที่รัฐ หรือบุคคลอื่นใดฟ้องร้องดำเนินคดี ผู้ให้บริการ เหล่านั้นก็มีโอกาสแสดงความบริสุทธิ์ หรือสืบพิสูจน์ต่อสู้ (เพื่อให้ตนเองพ้นผิด) ได้ว่า การบอกแจ้งนั้นไม่ชอบหรือไม่มีผลตามกฎหมายอย่างไร ตนมีเหตุหรือมีอำนาจไม่ต้องปฏิบัติการตามที่บอกแจ้งหรือไม่ อย่างไร หรือตนได้ใช้ความพยายามอย่างเต็มที่เพื่อดำเนินการกับเนื้อหาที่เป็นความผิดเหล่านั้นแล้วหรือไม่ อย่างไร เป็นต้น

1.4 ในประเด็นเรื่องมาตรการระงับการเผยแพร่เนื้อหา หรือการปิดกั้นช่องทางการเข้าถึงข้อมูลหรือเว็บไซต์นั้น ควรได้มีการพิจารณาทบทวนหลักการ และบทบัญญัติใน พ.ร.บ.คอมพิวเตอร์ฯ 2550 เพื่อแก้ไขเพิ่มเติม ดังนี้

- แก้ไข มาตรา 20 หรือบทบัญญัติที่กำหนด “มาตรการระงับการเผยแพร่เนื้อหา หรือปิดกั้นช่องทางการเข้าถึงเว็บไซต์” ให้มีความชัดเจนว่า ต้องการใช้บังคับกับเนื้อหาประเภทใด โดยต้องไม่ใช้ถ้อยคำที่คลุมเครือ ตีความหมายได้หลายอย่าง อย่างคำว่า “ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน” หรือ “ขัดต่อความมั่นคงแห่งรัฐ” (เช่นที่เป็นอยู่ในปัจจุบัน) ซึ่งด้วยวิธีการบัญญัติแบบนี้เท่านั้น ที่จะช่วยสร้างดุลยภาพระหว่างการป้องกันและปราบปรามการกระทำความผิดที่เกี่ยวกับการเผยแพร่ข้อมูลบนสื่อออนไลน์ กับเสรีภาพในการแสดงความคิดเห็นของประชาชนให้เกิดขึ้นได้ ทั้งนี้บทบัญญัติดังกล่าวควรต้องวางอยู่บนหลักการพื้นฐานที่ว่า มาตรการปิดกั้นการเข้าถึงเว็บไซต์ต้องใช้กับเนื้อหาที่มีความร้ายแรง และอาจก่อให้เกิดความเสียหายต่อประชาชนหรือสังคมประชาธิปไตยอย่างถึงขนาด เท่านั้น กล่าวคือ มีการใช้ภาพ ถ้อยคำ หรือแสดงเจตนารมณ์บางอย่าง ชนิดที่หากไม่รีบปิดกั้นเนื้อหานั้นโดยเร็ว หรือต้องรอให้เจ้าหน้าที่ไปสืบหาตัวผู้เผยแพร่มาฟ้องคดีและให้ศาลพิจารณาพิพากษาว่าเนื้อหาเหล่านั้นเป็นความผิด และผู้กระทำมีความผิดจริงตามกฎหมายก่อน ก็จะเกิดความเสียหายอย่างมาก หรือสายเกินไป หรือไม่มี

วิธีการอื่นใดที่จะช่วยแก้ไข “ผล” ของเนื้อหาที่เผยแพร่นั้นได้อีกแล้ว เช่น ภาพลามกเด็กและเยาวชน การยั่วยุให้คนในประเทศฆ่าล้างเผ่าพันธุ์กันเอง เป็นต้น

- รัฐควรกำหนดวิธีการ กระบวนการ และเงื่อนไขการใช้อำนาจปิดกั้นการเข้าถึงเว็บไซต์ไว้ในกฎหมาย หรือระเบียบใดๆ ให้ชัดเจนเป็นลายลักษณ์อักษร ทั้งนี้ เพื่อกำกับให้เจ้าหน้าที่รัฐ รวมทั้งองค์กรผู้พิจารณาออกคำสั่ง ปฏิบัติหน้าที่ด้วยความสุจริต เป็นธรรม และสามารถถูกตรวจสอบได้ อาทิเช่น เจ้าหน้าที่ต้องแสดงเนื้อหาที่เข้าข่ายเป็นความผิดและต้องการปิดกั้นนั้น พร้อมเหตุผลอันสมควรอย่างยิ่งต่อศาลเพื่อขอคำสั่งให้ปิดกั้น องค์กรตุลาการหรือศาลผู้พิจารณาเองก็ต้อง “แสดงเหตุผล” ประกอบคำสั่งนั้นโดยชัดแจ้ง โดยเฉพาะอย่างยิ่ง กรณีที่มีคำสั่งอนุญาตให้ปิดกั้นเว็บไซต์ได้ กำหนดขั้นตอนและกระบวนการในการแจ้งคำสั่ง และเหตุผลของการปิดกั้นดังกล่าวต่อผู้ให้บริการ หรือต่อบุคคลผู้เกี่ยวข้องหรือได้รับผลกระทบโดยตรง นอกจากนี้ วิธีการและลักษณะของการปิดกั้นต้องเป็นไปตามหลักแห่งความได้สัดส่วน กล่าวคือ หากสามารถทำได้ในทางเทคนิค รัฐต้องปิดกั้น “เฉพาะส่วน” ที่ร้องขอ หรือที่เข้าข่ายเป็นความผิดเท่านั้น ต้องมีกำหนดระยะเวลาในการปิดกั้นที่ชัดเจน หรือศาลอาจกำหนด “เงื่อนไข” ให้ผู้ถูกปิดกั้นนั้นได้ปฏิบัติตาม หรือแก้ไขเนื้อหา เพื่อนำมาเป็นเหตุร้องขอให้ศาลยกเลิกการปิดกั้นเนื้อหาเหล่านั้นได้ เป็นต้น

อนึ่ง เพื่อเป็น “หลักประกัน” แก่ประชาชน ไม่ให้มาตรการปิดกั้นข้อมูลหรือเว็บไซต์ กลายเป็นเครื่องมือของฝ่ายผู้มีอำนาจที่จะใช้กลั่นแกล้งหรือเล่นงานกันทางการเมืองได้ หากมีคำสั่งศาลให้ปิดกั้นเว็บไซต์ใดแล้ว จะต้องมีกระบวนการต่อเนื่องเพื่อฟ้องร้อง และดำเนินคดีกับบุคคลผู้เผยแพร่ข้อมูลที่มีเนื้อหาอันเป็นเหตุให้ต้องมีคำสั่งปิดกั้นเว็บไซต์นั้นๆ ด้วย นอกจากนี้หากในท้ายที่สุดพบว่า ผู้กระทำไม่มีความผิด หรือเนื้อหาดังกล่าวไม่เป็นความผิดจริง ศาลต้องสั่งยกเลิกเพิกถอนคำสั่งปิดกั้นนั้นทันที รวมทั้งควรต้องมีมาตรการเยียวยาความเสียหายให้กับผู้ถูกสั่งดังกล่าวด้วย

- ปัจจุบัน มาตรา 20 แห่ง พ.ร.บ.คอมพิวเตอร์ ฯ 2550 กำหนดให้

ศาลเป็นองค์กรผู้มีอำนาจออกคำสั่งให้ระงับการเผยแพร่เนื้อหา หรือปิดกั้นเว็บไซต์ ซึ่งคณะผู้วิจัยเห็นว่าอาจไม่เหมาะสม โดยพิจารณาจากภาระงานของศาลที่มีอยู่แล้ว ความรู้และความเชี่ยวชาญในเรื่องเทคโนโลยีสารสนเทศ ความรวดเร็วในการทำคำสั่งที่จำเป็นต้องมาควบคู่กับการกลั่นกรองตรวจสอบเนื้อหาอย่างละเอียดรอบคอบ[6] รวมทั้งปัญหาและมุมมองในเรื่องเสรีภาพในการแสดงความคิดเห็นของประชาชน ฯลฯ จึงเสนอให้พิจารณาทบทวน เพื่อกำหนดองค์กรผู้มีอำนาจออกคำสั่งให้เหมาะสมกว่าที่เป็นอยู่ เช่น กำหนดให้องค์กรพิจารณาอยู่ในรูปของคณะกรรมการร่วม ซึ่งอาจสรรหาหรือตั้งขึ้นโดยเฉพาะเพื่อทำหน้าที่ตรวจสอบเนื้อหาที่ร้องขอให้ปิดกั้น โดยทั้งคุณสมบัติ องค์ประกอบ และที่มาของคณะกรรมการ ควรกำหนดให้มีตัวแทนทั้งจากฝ่ายรัฐ องค์กรที่ทำงานด้านสิทธิ องค์กรเอกชนที่ทำงานเทคโนโลยีสารสนเทศ ผู้ประกอบการ ฯลฯ ทั้งควรกำหนดกระบวนการในการพิจารณา รวมทั้งการโต้แย้งคัดค้านคำสั่งไว้ในกฎหมายด้วย

2. ข้อเสนอแนะเชิงนโยบาย

2.1 รัฐควรพิจารณาหามาตรการที่ได้ผลและใช้บังคับได้จริงเพื่อการกำกับดูแลเนื้อหาข้อมูลบนสื่อออนไลน์ ทั้งให้ได้ดุลยภาพกับการคุ้มครองเสรีภาพของประชาชน แทนการใช้มาตราการปิดกั้นช่องทางการเข้าถึงเว็บไซต์ เพราะมาตรการดังกล่าว นอกจากไม่ให้ผลสำเร็จใดๆ ที่ยั่งยืนและเป็นรูปธรรม และส่งผลกระทบต่อเสรีภาพในการแสดงความคิดเห็นของประชาชนอย่างมากแล้ว ยังเป็นตัวกระตุ้นให้เกิดกระแสต่อต้านกฎหมายและรัฐจากประชาชนในประเทศอีกด้วย ทั้งนี้ การปิดกั้นเว็บไซต์เป็นวิธีการที่ไม่สามารถจำกัดการเข้าถึงข้อมูลที่ผิดกฎหมายได้จริง ด้วยสาเหตุหลายประการ อาทิ ผู้ให้บริการเว็บไซต์ที่ถูกปิดกั้นสามารถเปลี่ยนแปลง หรือโยกย้ายเนื้อหาจากเครื่องคอมพิวเตอร์ที่ใช้เป็นสถานที่ฝากเว็บไซต์ (เซิร์ฟเวอร์) ที่โดนปิดกั้นนั้น ไปยังเซิร์ฟเวอร์เครื่องอื่นหรือเซิร์ฟเวอร์ที่อยู่ต่างประเทศได้ เกิดเว็บไซต์ที่มีเนื้อหาเหมือนหรือเลียนแบบเว็บไซต์ที่ถูกปิดกั้นไปแล้วขึ้น

อีกจำนวนมาก นอกจากนี้ เนื่องจากการปิดกั้นช่องทางการเข้าถึงเว็บไซต์ไม่ได้ทำให้เนื้อหาที่ผิดกฎหมายนั้นหายไปจากอินเทอร์เน็ตแต่อย่างใด เพียงแต่ทำให้ผู้ใช้อินเทอร์เน็ตไม่สามารถใช้วิธีการหรือช่องทางปกติเรียกให้เนื้อหามาแสดงผลได้เท่านั้น ดังนั้น หากผู้ใช้บริการอินเทอร์เน็ตสามารถหาวิธีการอื่นใด นอกเหนือจากวิธีการปกติได้ ก็ย่อมสามารถเข้าถึงเนื้อหาเหล่านั้นได้ ซึ่งปัจจุบันมีเครื่องมือและเทคโนโลยีจำนวนมากที่สามารถเข้าถึงเนื้อหาที่ถูกปิดกั้นได้ อาทิ Proxy, RSS กระทั่งผ่าน E-Mail และเป็นที่น่าสนใจด้วยว่า แม้แต่เจ้าหน้าที่รัฐที่เกี่ยวข้องกับการบังคับใช้มาตรการนี้เองก็เคยกล่าวว่าการขึ้นบัญชีดำเพื่อปิดกั้นเว็บไซต์นั้น นอกจากไม่เคยประสบความสำเร็จแล้ว ยังก่อให้เกิดภาระอันเกินจำเป็นแก่ฝ่ายผู้ให้บริการอินเทอร์เน็ตด้วย[7] ฉะนั้น รัฐจึงไม่ควรดำเนินนโยบายป้องกันและปราบปรามการกระทำความผิดโดยเน้นที่การระงับการเผยแพร่เนื้อหา หรือการปิดกั้นเว็บไซต์ เว้นแต่ มีความจำเป็นเร่งด่วน และเกิดความเสียหายอันถึงขนาดจริง ๆ ซึ่งก็ต้องมีกฎหมายบัญญัติเหตุแห่งการใช้อำนาจให้ชัดเจนไม่คลุมเครือ ดังที่คณะผู้วิจัยได้เสนอไว้แล้วในส่วน “ข้อเสนอแนะทางกฎหมาย“

คณะผู้วิจัยเห็นว่า ในที่สุดแล้ว มาตรการอื่นกลับน่าจะได้ผลในแง่ของการกำกับดูแลเนื้อหาที่ผิดกฎหมายได้มากกว่า อาทิเช่น การพยายามส่งเสริมการสร้างกระบวนการ หรือกลไกในการตรวจสอบควบคุมกันเองในระหว่างผู้ใช้และผู้ให้บริการอินเทอร์เน็ต โดยรัฐทำหน้าที่เป็นผู้คอยกำกับดูแลให้การควบคุมตรวจสอบกันเองเหล่านั้นอยู่ในกรอบแห่งกฎหมาย เช่น ไม่ให้ประชาชนละเมิดสิทธิระหว่างกันเอง หมิ่นประมาทกันเอง หรือชักชวนให้ใช้วิธีการที่ผิดกฎหมายตอบโต้บุคคลที่มีความคิดเห็นแตกต่างจากตน เป็นต้น นอกจากนี้ การบังคับใช้กฎหมายอย่างเคร่งครัดจริงจัง ไม่เลือกปฏิบัติ รวมทั้งพัฒนาความรู้ความสามารถด้านเทคโนโลยีคอมพิวเตอร์ของเจ้าหน้าที่รัฐให้ดีขึ้น เพื่อที่จะสามารถสืบหาแกะรอยผู้กระทำความผิดที่แท้จริงมาดำเนินคดีและลงโทษตามกฎหมายได้ ก็อาจส่งผลให้อัตราการกระทำความผิดบนเครือข่ายอินเทอร์เน็ตลดลงได้เช่นกัน เพราะทำให้ผู้ที่คิดจะกระทำความผิดได้เห็นว่าหากทำผิดแล้ว ก็มีโอกาสสูงที่จะถูกจับกุม และ

ดำเนินคดีได้จริงๆ อย่างไรก็ตาม บทบัญญัติที่เกี่ยวกับความผิดและโทษที่รัฐจะนำมาใช้ดำเนินคดีนี้ ก็จำเป็นอย่างยิ่งที่จะต้องเป็นบทบัญญัติที่มีความยุติธรรมเพียงพอด้วย คือ บัญญัติชัดเจนไม่คลุมเครือ เป็นการลงโทษการกระทำที่สร้างความเสียหายและขัดต่อมาตรฐานของสังคมภายใต้ระบอบการปกครองแบบประชาธิปไตยอย่างแท้จริง รวมทั้งมีอัตราโทษที่เหมาะสมได้สัดส่วนกับความเสียหายนั้น

2.2 ส่งเสริมให้มีการจัดตั้งศาลชำนัญพิเศษเพื่อพิจารณาคดีที่เกี่ยวกับคอมพิวเตอร์โดยเฉพาะ ทำนองเดียวกับศาลเยาวชนและครอบครัว ศาลแรงงาน ศาลภาษีอากร หรือศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ ซึ่งผู้พิพากษาศาลชำนัญพิเศษนี้ควรเป็นผู้มีความรู้ความเข้าใจอย่างดีในเรื่องเทคโนโลยีสารสนเทศ หรือระบบคอมพิวเตอร์ และอาจมีการแต่งตั้งบุคคลภายนอกซึ่งมิใช่ผู้พิพากษาอาชีพ แต่มีความรู้และความเชี่ยวชาญในเรื่องดังกล่าวให้เป็นผู้พิพากษาสมทบ เพื่อเข้าร่วมพิจารณาและพิพากษาคดีด้วย

2.3 จัดทำคู่มือในการปฏิบัติงาน หรืออธิบายกฎหมาย และกฎระเบียบต่างๆ ที่เกี่ยวข้อง ให้แก่พนักงานเจ้าหน้าที่ ผู้ให้บริการหรือผู้ประกอบการอินเทอร์เน็ต รวมทั้งประชาชนทั่วไปผู้ใช้อินเทอร์เน็ต โดยคู่มือดังกล่าว ต้องไม่มุ่งเน้นแต่เพียงประเด็นการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์ หรือการกระทำความผิดที่เกิดขึ้นในอินเทอร์เน็ตเท่านั้น แต่ควรให้ความสำคัญกับประเด็นการคุ้มครองเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็นด้วย

2.4 นอกจากการออกกฎหมายเพื่อกำหนดภาระหน้าที่และความรับผิดแก่ผู้ให้บริการอินเทอร์เน็ตควรต้องกระทำอย่างจำกัดขอบเขตที่สุด และเพียงเท่าที่จำเป็นแล้ว (ดังที่เสนอแนะไว้ใน “ข้อเสนอแนะทางกฎหมาย”) รัฐควรหันมาสนับสนุนให้กลุ่มผู้ประกอบการ จัดทำ “ประมวลจริยธรรม” (Code of Conduct) ในการให้บริการสื่อออนไลน์อย่างเป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางในการปฏิบัติร่วมกันด้วย รวมทั้งควรศึกษาวิจัย เพื่อออกแบบมาตรการ หรือกลไกอื่นๆ ในลักษณะของการ “สร้างแรง

จูงใจ" ให้ผู้ประกอบการเหล่านั้นตรวจสอบดูแลไม่ให้เกิดการกระทำความผิดหรือการเผยแพร่เนื้อหาที่ไม่ชอบด้วยกฎหมาย แทนที่จะใช้นโยบายปราบปราม หรือลงโทษผู้ประกอบการแต่เพียงอย่างเดียว

3. ข้อเสนอแนะต่อประชาชนผู้ให้ และผู้ใช้บริการสื่อออนไลน์

3.1 นอกเหนือจากสิทธิเสรีภาพในชีวิต ร่างกาย และทรัพย์สินแล้ว ในสังคมประชาธิปไตยและในยุคสมัยแห่งเทคโนโลยีสารสนเทศ ประชาชน สื่อมวลชน รวมทั้งองค์กรต่างๆ ที่ทำงานด้านการคุ้มครองสิทธิของประชาชน ควรให้ความสำคัญกับสิทธิในข้อมูลส่วนบุคคล เสรีภาพในการรับรู้ข้อมูลข่าวสาร และเสรีภาพในการแสดงความคิดเห็นให้มากขึ้น ซึ่งสิทธิและเสรีภาพเหล่านี้ประชาชนของประเทศในซีกโลกฝั่งตะวันตกได้ให้ความสำคัญ และตื่นตัวที่จะปกป้องคุ้มครองจากการล่วงละเมิดโดยรัฐและผู้ปกครองมานานแล้ว (ดังจะเห็นได้จาก ปฏิกิริยาของประชาชนที่มีต่อกฎหมายและนโยบายของรัฐ ในประเทศเยอรมนีและสหรัฐอเมริกา ในรายงานวิจัยฉบับนี้) ทั้งนี้ เพราะสิทธิและเสรีภาพดังกล่าวเป็นพื้นฐานของเสรีภาพด้านอื่นๆ ที่จะตามมาในระบอบการปกครองแบบประชาธิปไตย หากประชาชนในประเทศไม่สามารถเลือกที่จะรับรู้ข้อมูลข่าวสารที่มีความหลากหลาย ไม่อาจมั่นใจได้ในความปลอดภัยของข้อมูลส่วนบุคคล หรือไม่สามารถแสดงความคิดเห็นต่อเรื่องต่างๆ ได้โดยเสรี โดยเฉพาะอย่างยิ่งต่อการเมืองการปกครอง ต่อบทบาทของสถาบัน และองค์กรต่างๆ รวมทั้งกลุ่มผู้ใช้อำนาจปกครอง ก็ย่อมสุ่มเสี่ยงที่สิทธิและเสรีภาพที่สำคัญยิ่งกว่าในด้านอื่นๆ จะถูกรัฐและผู้ใช้อำนาจปกครองล่วงละเมิดได้โดยง่าย

3.2 ประชาชนและองค์กรต่างๆ ด้านการคุ้มครองสิทธิของประชาชนในเรื่องนี้ ควรตื่นตัว และคอยติดตามตรวจสอบการออกกฎหมาย กฎระเบียบต่างๆ รวมทั้งนโยบายของรัฐที่อาจส่งผลกระทบต่อเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นอย่างสม่ำเสมอ เพื่อป้องกันไม่ให้รัฐใช้อำนาจเกินขอบเขต และหากพบการใช้อำนาจใน

ลักษณะที่ไม่ชอบธรรม ก็ควรรวมตัวหรือร่วมมือกันร้องเรียนไปยังองค์กรหรือหน่วยงานผู้รับผิดชอบให้ตรวจสอบ หรือระงับยับยั้งการออกกฎหมายหรือกระบวนการดำเนินนโยบายดังกล่าว กระทั่งอาจใช้กระบวนการทางศาลเพื่อขอให้มีการตรวจสอบความชอบด้วยรัฐธรรมนูญของกฎหมาย หรือบทบัญญัติเหล่านั้นได้ (ดังเช่นที่เกิดขึ้นบ่อยครั้งในประเทศเยอรมนี และสหรัฐอเมริกา ตามที่ปรากฏในรายงานวิจัยฉบับนี้) ในขณะที่สื่อมวลชนเองก็ควรสนับสนุน ให้ความสำคัญ และติดตามนำเสนอกระบวนการเรียกร้องสิทธิและเสรีภาพของประชาชนต่อสาธารณะ เพื่อให้ประชาชนทั่วไปได้รับรู้ข้อมูล มีความตื่นตัว และเห็นความสำคัญในสิทธิและเสรีภาพของตนเอง

3.3 ผู้ให้บริการอินเทอร์เน็ต อาจรวมตัวกัน หรือจัดตั้งเป็นกลุ่มผู้ประกอบการให้เข้มแข็ง ทั้งคงต้องคอยติดตามเฝ้าระวังการออกกฎหมายและนโยบายที่เกี่ยวกับเรื่องนี้ของรัฐด้วยเช่นกันว่ามีการกำหนดภาระหน้าที่ หรือความรับผิดชอบที่ไม่เป็นธรรม หรือเกินสมควรแก่ผู้ให้บริการอินเทอร์เน็ตบ้างหรือไม่ อย่างไร เนื่องจากการเพิ่มภาระหน้าที่อันเกินสมควรแก่ผู้ให้บริการ ย่อมส่งผลกระทบต่อสิทธิและเสรีภาพประชาชนด้วย ทั้งนี้ทั้งในแง่ของสิทธิในการเข้าถึงอินเทอร์เน็ตซึ่งสะท้อนออกมาเป็นค่าใช้จ่ายที่เพิ่มขึ้น และในแง่ของเสรีภาพในการรับรู้ข้อมูลข่าวสาร และการแสดงความคิดเห็นของประชาชน เพราะอาจทำให้ผู้ให้บริการ จำเป็นต้องเซ็นเซอร์การนำเสนอข่าวสารของตนเอง อนึ่ง การรวมตัวกันและจัดการให้เป็นกลุ่มที่เข้มแข็งได้ย่อมช่วยเพิ่มอำนาจในการต่อรอง หรือเรียกร้องให้รัฐออกกฎหมายที่เป็นธรรม ทั้งไม่ผลักภาระในการป้องกันการกระทำความผิดในเครือข่ายคอมพิวเตอร์ให้กับเอกชนมากเกินไป

Research Title

Impact of the Computer-related Crime Act 2007 and State Policy on the Right to Freedom of Expression

1. Rationale

Section 45[1] of the 2007 Constitution clearly stipulates that the state must protect the rights and freedoms of the people to access information and express opinions by any means and through any type of media. However, under the rule of law and democracy, the exercise of the rights and freedoms by any person, particularly the right to freedom of expression, must always be subject to restrictions specified by law, in order to prevent the use of these rights and freedoms in such a way as to affect or violate the rights and freedoms of others.

Paragraph 2 of Section 45 of the Constitution enacts exceptions to the protection of freedom of expression, and authorizes the state to formulate 'legal measures' to restrict or control the exercise of this right and freedom for four main reasons: to maintain the security of the State, to maintain public order or

good morals, to safeguard the personal rights and reputation of others, and to prevent and end the deterioration of the mental or physical health of the public.

Although the state, in its status of holding administrative power, can pass laws or employ other measures to regulate or control the rights and freedoms of the people, such laws or measures must also be restricted in order to guarantee to the people that the administrative authorities do not use their powers arbitrarily or violate freedoms beyond what is appropriate. Section 29 of the Constitution, therefore, restricts the state to the enactment of laws to restrict the rights and freedoms of the people to the extent necessary, and such laws 'shall not affect the essential substances of such rights and liberties,' and 'shall be of general application and shall not be intended to apply to any particular case or person.'[2]

However, although the Constitution stipulates the protection of the people and sets limits to the enactment of laws, the past several years have seen the passage of many laws and measures by the responsible agencies of the Thai state to control and restrict rights, and even interfere with the media's freedom to present information and the Thai people's freedom of expression, resulting in questions as to whether this constitutes abuse of power. For example, the Emergency Decree on Public Administration in Emergency Situation 2005 aims to control news coverage of the political situation through various media including television, community radio and websites. The Computer-related Crime Act 2007 (CCA) contains unclear and ambiguous wording which authorizes the state to block the publication of information or close websites. This has actually happened in many cases where the authorities used

their powers without providing sufficiently clear reasons to the owners of websites that were blocked, or censoring websites many times without following the specified legal procedure (seeking court orders as required by Section 20 of the law[3]). The state instead asked for 'cooperation' from internet service providers or used its powers informally to block content or access to certain websites which the state deemed 'improper', though possibly not illegal.

Statistics which will be later presented in this report show a worrying trend that the more serious conflict in Thai society has grown, the more severe control and interference in the media became, particularly in online media or the internet (which is under the scope of this research), through the use of powers under the Emergency Decree.[4] This trend occured despite the fact that during political crises or conflict situations, the state should even be more firm in protecting the people's rights and freedoms to access information and express opinions, as this is the time when it is particularly necessary for the people to have complete and thorough information to make decisions, or to express their intentions and participate politically.

Moreover, many incidents have led to the belief that the state enforces the law and other measures selectively and unequally. While many news outlets present news coverage with the same degree of violence, the state has chosen to control only some of them or some groups which present information that the state considers to be unfriendly or belonging to the political opposition. For example, many community radio stations were closed down by the Democrat government in 2010[5], or by the Pheu Thai government in 2011[6]. These cases raise the question as to whether the state has violated or contravened the

provisions of the constitution, and also reflect the attitude held by the Thai state towards the rights and freedoms of the people in this regard. Although in the past, several groups have tried to make public appeals on this issue and bring cases to court to test the legality of state use of power, this has not yet met with an adequate response. In some cases, the court even refused to examine the use of state power in this way. For example, the Court of First Instance dismissed the Prachatai website's complaint against the Centre for the Resolution of the Emergency Situation during the Abhisit Vejjajiva government for using the powers under the Emergency Decree to order the illegal blocking the Prachatai website.[7]

In addition to the strict control and censorship of the media and websites in the past, it must also be noted that most cases prosecuted under the CCA involve the dissemination of information on the internet, not real crimes. Many of the accused were web service providers who did not post the information themselves. So in light of this, it cannot be denied that CCA has been turned into an important instrument in the restriction of freedom of online media.

With the facts cited above, it should be extremely useful to collect statistics and case studies, to record the number of websites which have been blocked, to classify the uses of the CCA by the state, and to survey policies and attitudes of the authorities and state officials regarding the people's rights and freedoms to access information and express opinions, so that an analysis could show the real reasons as to how the internet is coming under tight control in Thailand. However, this research may never be complete without studies of the same issue in other countries, so that comparisons can be made to lead to recom-

mendations and eventually the creation of a balance between the prevention and suppression of online offences and the protection of the people's rights and freedoms, based on the research team's view that the freedom of expression of the people is important and essential building a true democracy in Thai society.

2. Activities

Quantitative and qualitative research on the impacts of the CCA

3. Timeframe of study

July 2007 – December 2011

4. Goals

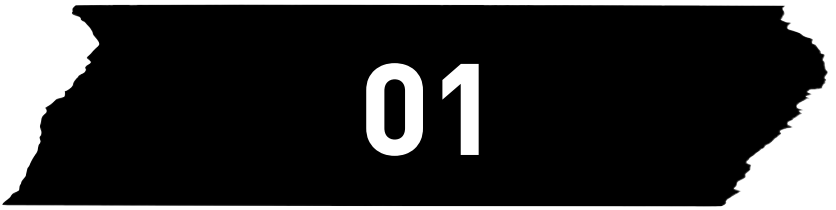
1) Collect statistics on cases under the CCA and the implementation of government policies regarding the people's freedom on the internet.

2) Collect information and opinions as well as solutions to the problems arising from the blocking and control of internet content from those who set policy and media control measures, agencies and officials who enforce the law, and those affected by enforcement of these measures;

3) Study problems resulting from the law and its enforcement in relation to the people's freedom to access information and express opinions on the internet, particularly the CCA Survey laws and policies relating to the people's freedom on the internet in other countries, to compare with those of Thailand;

4) Analyze and evaluate advantages and disadvantages (including comparisons with other countries) between the laws and policies which focus on the control and filtering of internet content and those which place importance on the people's rights and freedoms. Conclusions will be made and appropriate recommendations will be proposed to create a balance between the prevention and suppression of offences and the protection of the people's freedoms.

CHAPTER



Part 1

Statistic Study and Survey of the Opinions of State Officials and Online Media Service Providers regarding Enforcement of the Computer-related Crime Act 2007

The first part of the research study on the Impact of the Computer-related Crime Act 2007 (CCA) and State Policy on the Right to Freedom of Expression in a new media society (online media) aims to study the impact of the enforcement of the CCA since its enactment in July 2007 until December 2011, a period of three years and six months. This section is divided into two parts;

Quantitative study: statistics on the blocking of information and web access and on the number of legal proceedings.

Qualitative study: interviews and focus group discussions to collect data from persons concerned with enforcement of the CCA

1. Quantitative Study

The impact of the law's enforcement over three years

and six months was analyzed by two measures: the blocking of information and web access; and the number of prosecutions of citizens on various charges under the CCA.

Methodology

For statistics of blocking web access[1], the researchers relied on the Criminal Court database.[2] Supplementary information was then acquired from relevant people, particularly one large internet service provider (name withheld).

Statistics on legal proceedings were collected from state agencies, particularly those directly associated with enforcement of the CCA:

- the Ministry of Information and Communication Technology (MICT)
- the Economic Crime Division (ECD)
- Technology Crime Suppression Division (TCSD)
- the Department of Special Investigation (DSI), Ministry of Justice
- the Crime Suppression Division, (CSD) The Royal Thai Police
- the Criminal Court

Research Limitations

The statistics on legal proceedings in this research is only restricted to data accessible to the researchers. It cannot therefore be concluded that the figures include the total number of cases in Thailand. A number of cases are currently under investigation by the police at stations across country, where information

especially on pending cases is restricted, since it might affect the ongoing judicial process and the rights of defendants. Moreover, not all data from all provincial courts was accessible in the database. These restrictions mean that the statistics presented in this research, which are regarded as reliable, clearly sourced and accountable, are only a part of the actual totals.

Research Findings

1.1 Statistics on the restriction of data dissemination or blocking of website access

Ever since the CCA came into force, the Thai state, through the Ministry of Information and Communication Technology (MICT), has had the authority under Section 20 to take measures to censor or restrict computer data of a type "that is likely to damage the country's security or cause a public panic".

"Section 20. If an offence under this Act is to disseminate computer data that might have an impact on the Kingdom's security as stipulated in Division 2 type 1 or type 1/1 of the Criminal Code, or that it might be contradictory to the peace and concord or good morals of the people, the competent official appointed by the Minister may file a petition together with the evidence to a court with jurisdiction to restrain the dissemination of such computer data."

It has been found that since enactment there have been totally 156 court orders to block websites. In 2007, the court ordered the restriction of the access of two URLs; in 2008, 2,071 URLs; in 2009, 28,705 URLs; and in 2010, 45,357 URLs. The total number of the sites blocked by court order is therefore

Content	2007		2008		2009		2010		2011		Total	
	Court order	URL	Court order	URL	Court order	URL	Court order	URL	Court order	URL	Court order	URL
Insulting the king, the queen, or the heir	0	0	7	1,937	30	16,525	27	39,115	26	3,213	**90**	**60,790**
Obscene or pornographic	0	0	4	96	27	11,609	15	6,105	6	1,585	**52**	**19,395**
Abortion pills	0	0	1	37	3	320	0	0			**4**	**357**
Encourage gambling	0	0	0	0	2	246	0	0			**2**	**246**
Depreciate the religion	1	2	1	1	1	2	0	0			**3**	**5**
Other	0	0	0	0	1	3	3	137	1	280	**5**	**420**
Total	**1**	**2**	**13**	**2,071**	**64**	**28,705**	**45**	**45,357**	**33**	**5,078**	**156**	**81,213**

Figure 1 : The number of court orders and the number of URLs blocked classified by offence

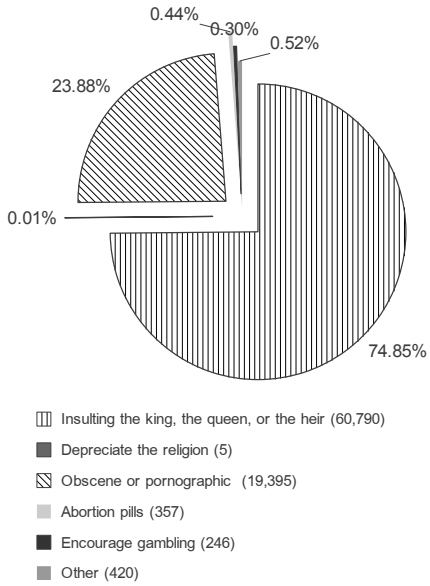


Figure 2: The percentage of URLs banned by court order classified by offence

81,213 URLs.

Note that the Criminal Court gives the type of offence as the reason to issue an order. These are one those with lèse majesté content, with 90 court orders to block 60,790 URLs; two those with the obscene or pornographic content, with 52 court orders to block 19,395 URLs; three those with content related to advertising morning-after abortion pills, with four court orders to block 357 URLs; four those with content encouraging gambling with two court orders to block 246 URLs; five those with blasphemous content, with three court orders to block five URLs; and six other offences such as phishing and spamming sites and misleading websites that possibly create misunderstanding and confusion among the people on the government's crackdown, with five court orders to block 420 URLs. The proportion of URLs banned by the court order is shown by offence in the graph below;

The criminal court database also shows monthly figures the number and the category of URLs blocked. This monthly breakdown (Figure 3) is useful in identifying the factors that influenced implementation of the law in different periods.

Analysis and Observations on the Statistics on Web Blocking or Web Access Restrictions

1) The rate of web blocking or web access restriction alters according to the political situation.

It is noted that relatively few web access restrictions were imposed between 2007 and 2008 compared to 2009-2010, where there was an overall increase, with 2010 having the highest rate of web access restrictions, followed by a decline.

Timing	Insulting the king, the queen, or the heir		Obscene or pornographic		Abortion pills		Encourage gambling		Depreciate the religion		Other		**Total**	
	Court order	URL	Court order	URL	Court order	URL	Court order	URL	Court order	URL	Court order	URL	**Court order**	**URL**
Oct 07									1	2			1	2
Jan 08									1	1			1	1
Feb 08			1	7									1	7
May 08			1	1									1	1
June 08	1	9	1	2									2	11
July 08													0	0
Aug 08	2	407											2	407
Sep 08	1	630	1	86									2	716
Oct 08	1	491											1	491
Nov 08													0	0
Dec 08	2	400			1	37							3	437
Jan 09	3	808											3	808
Feb 09	4	1,400	1	305	1	14							6	1,719
Mar 09	4	765	3	825					1	2			8	1,592
Apr 09	2	887	4	936									6	1,823
May 09	3	713	4	2,213			1	72					8	2,998
June 09	3	770	3	1,948									6	2,718
July 09	2	469	3	875									5	1,344
Aug 09	1	843	1	132							1	3	3	978
Sep 09	2	1,985	2	879	1	61	1	174					6	3,099
Oct 09	3	3,737	3	1,430									6	5,167
Nov 09	2	3,007	1	741									3	3,748
Dec 09	1	1,141	2	1,325	1	245							4	2,711
Jan 10	2	4,119											2	4,119
Feb 10	4	6,731	2	1,127							1	3	7	7,861
Mar 10	6	9,672	1	373									7	10,045
Apr 10	2	2,277	1	21									3	2,298
May 10													0	0
June 10	3	4,513											3	4,513
July 10													0	0
Aug 10	5	9,289	3	1,322							1	2	9	10,613
Sep 10	3	2,267	2	944									5	3,211
Oct 10			2	998									2	998
Nov 10	1	2	1	250									2	252
Dec 10	1	245	3	1,070							1	132	5	1,447
Jan 11	3	1,618	1	277									4	1,895
Feb 11			1	303									1	303
Mar 11	4	194	1	307									5	501
Apr 11	1	135	1	315									2	450
May 11	2	351	2	383									4	734
June 11	2	2											2	2
July 11	2	125											2	125
Aug 11	1	52											1	52
Sep 11	2	14									1	280	3	294
Oct 11	1	1											1	1
Nov 11	1	300											1	300
Dec 11	7	421											7	421
Total	90	60,790	52	19,395	4	357	2	246	3	5	5	420	156	81,213

Figure 3: Monthly number of court orders by offence.

The assumption can be made that the likely cause for the relatively low number of URLs blocked during 2007-2008 compared with the following years is that the CCA had been effective for only a short period of time since its enactment on 18 July 2007. No mandate was given to specific agencies to monitor offences under this law, and the state body that was later directly assigned to regulate online information, the Office of Information Technology[3] under the MICT, was established only in 2009. There was a lack of preparedness in the courts to issue orders under Section 20. Before the enactment of the CCA, the MICT had used the mandate provided the 5th declaration of the Council for Democratic Reform[4] to block several websites. This was done by simply giving direct orders to internet service providers without any process of consideration, justification or preparation of a petition for a court order to restrict web access. After 2008, the statistics rose. As mentioned earlier, most websites blocked during 2007-2011 allegedly had content and images which defamed the king, the queen or the heir apparent (60,790 URLs) or were obscene or pornographic (19,395 URLs). Website blocking for lèse majesté peaked when Lt. Ranongruk Suwanchawee and later Juti Krairiksh served as ICT Minister during the administration of then Prime Minister Abhisit Vejjajiva.

It is found that the months with the highest number of websites blocked for lèse majesté were March 2010 (9,672 URLs), August 2010 (9,289 URLs) and February 2010 (6,731 URLs). This was when conflicts between the people and the government, and between groups of people increased markedly. In February and March 2010 the United Front for Democracy

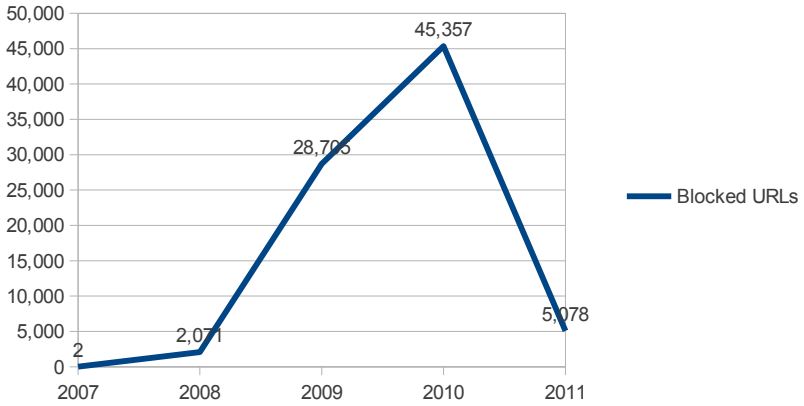


Figure 4: Number of blocked URLs by year

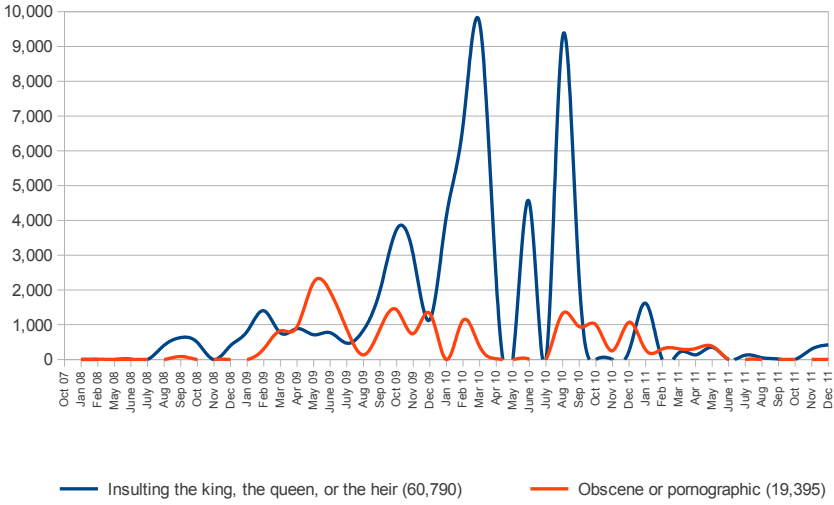


Figure 5: Number of websites blocked classified by offence (lèse majesté, and obscene or pornographic content) by month

against Dictatorship (UDD) and the red shirts were organizing for protests that began at Phan Fa Bridge in March before relocating to Ratchaprasong Intersection in April. In August 2010 the red shirts began to employ online media substantially to mobilize, as part of the 'Red Sundays,'[5] for a rally on September 19, the 4th anniversary of the 19 September coup.

No empirical evidence of whether the content of the blocked websites actually insulted or defamed the monarchy is available. The high numbers of blocked websites during the administration of Prime Minister Abhisit Vejjajiva was used to support accusations that the protesters aimed to overthrow the monarchy. This raises the question as to whether websites were blocked for lèse majesté because they really were offensive, or whether claims of increased lèse majesté activity were fabricated to attack the political opposition's freedom of expression.

Likewise, the reduction in the number of websites blocked during the end of the term of ICT Minister Juti Krairiksh in the Abhisit government and the beginning of that of Gp.Capt. Anudith Nakornthap in the Yingluck Shinawatra government could be interpreted in different ways. Possible causes are the efficiency of previous lèse majesté suppression, and the loss of interest by the Abhisit government in blocking websites as the election approached combined with a different approach by the newly elected government that came into power in 2011.

Aside from political conflict, state policy may also have an impact on website blocking. In June and July 2010, shortly after the announcement of the collaboration of MICT, the Ministry of Justice and the Ministry of Culture to establish the Cyber Scout project, the number of blocked websites increased sharply,

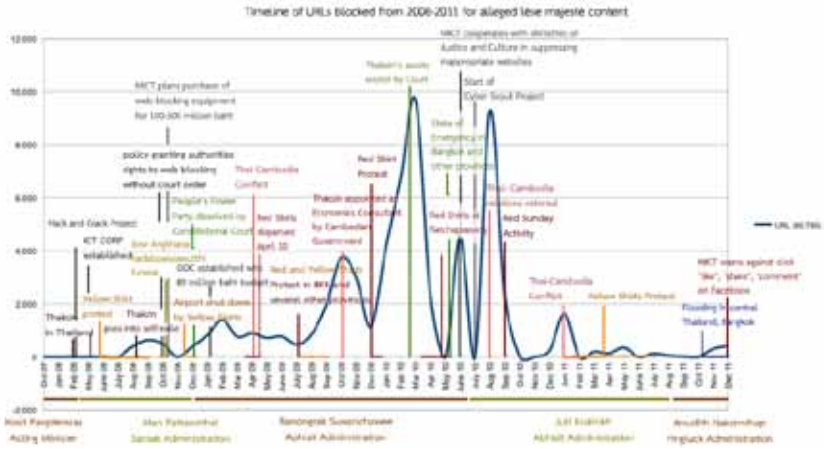


Figure 6: URLs blocked for lèse majesté monthly 2007- 20011, correlated to major relevant political and structural changes.

but then fell as interest in the project appeared to wane.

Section 20 of the CCA was not the only tool used by the state to censor information. Figure 6 shows a high degree of fluctuation from month to month fluctuation in the number of URLs blocked. In some months almost ten thousand URLs were blocked, while in preceding or following months, few URLs or none at all were blocked. In fact, a significant number of URLs were blocked not through court orders but through other instruments, especially the Emergency Decree on Public Administration in Emergency Situations 2005 (hereafter the "Emergency Decree"). On April 9 2010, PM Abhisit Vejjajiva declared the Emergency Decree in Bangkok, later expanded to other areas and continuing until December 2010.[6] He appointed the Center for Resolution of Emergency Situation (CRES) to implement the

decree, which included the power to block websites. The number of URLs blocked by orders of the CRES exceeded ten thousand, according to information from an internet service provider. The CRES procedure for blocking websites differed from that of the MICT. Under Section 20 of the CCA, websites could only be blocked when there was clearly an offence and only through the court orders; under Section 9 (3) of the Emergency Decree, the CRES could block websites in any way it wished without the need for court orders.[7]

It has been discovered that websites were blocked, either publicly or secretly, in sets. At least three CRES orders blocking over 600 websites/URLs/IP addresses/Phone numbers failed to specify the website names or particular URLs, but instead cited a range of IP addresses (i.e. block XXX.XXX.XXX.0 to XXX.XXX.XXX.255). This set included a website or websites that the CRES thought violated the Emergency Decree. However, many other websites that neither violated the law nor posed any threat were also blocked because their domain numbers fell within the set. This means that not only the websites that were really offensive, but also many general websites, were closed down.[8]

Blocking websites under the Emergency Decree, though not illegal, allowed the CRES to send orders to service providers without any scrutiny or oversight by other institutions. It was also found that Emergency Decree procedures lacked transparency in practice because no record was kept of each order, showing the legal procedure or the websites affected.

This has made it difficult for people affected both the directly and indirectly to prove whether the blocked websites were actually illegal, and whether the CRES actions were legitimate. It is suspected that some websites were blocked

merely because they disagreed with government policy. Also, the blocking of a website under the Emergency Decree would prevent everyone in the country from accessing those sites, not only those residing in Bangkok and those provinces where the Emergency Decree was declared. More interestingly, even after the Emergency Decree was withdrawn, a number of websites still continued to be blocked.[9] In addition to its legal authority the government also sought "cooperation" from internet service providers at different levels to block websites without orders from the courts or the CRES.

The figures show that in 2010 the greatest number of websites was blocked followed by a gradual decrease as Thailand went through a political transition. A general election paved the way for Ms. Yingluck Shinawatra from the Pheu Thai Party to become PM. The researchers believe that the reduction in the number of blocked websites still does not necessarily demonstrate an improvement in freedom of expression in Thailand. On the contrary, 3 months after Gp.Capt. Anudith Nakornthap became Minister in the Yingluck administration, the MICT sought "cooperation" from the webmaster of Facebook to block over 10,000 URLs[10] (this number is not included in the figures above since the blocking was not done under Section 20 of the CCA). Deputy Prime Minister Chalerm Yoobamrung also announced publicly that websites offending the institution of the monarchy would continue to be blocked, which would require a budget of more than 400 million Baht[11]. Moreover, the MICT also revealed that it sent representatives to negotiate cooperation from major global service providers to restrict access to their website for Thai users.[12] [13]

In conclusion, we see that the number of blocked web-

sites in Thailand after the enforcement of the CCA is related to and influenced by the degree of political conflict and the extent of public political expression in online media. However, the statistics on blocked websites from the court database cannot be used as the only indicator of suppression of the people's freedom of expression. This is firstly because the mechanism of blocking through court orders under Section 20 of the CCA has been used only under a normal circumstances and is discarded under unusual circumstances, when the state resorts to emergency measures (with extremely limited transparency) to censor information and suppress people's expression. Also, despite having the CCA and Emergency Decree, the Thai government has also sought informal "cooperation" from internet service providers block websites off the record without any legal mandate.

2) Judicial counterbalance to the MICT

Website blocking has always been opposed by the people because it is regarded as interference in the media and restriction of access to information. It also does not accord with the democratic principles either. Therefore, in the process of drafting the CCA, efforts were made to counterbalance the exercise of power of the state under the MICT by mechanisms that would prevent any violation of the rights and liberties of the people. Under the CCA, therefore, a judicial institution is assigned to approve petitions from the executive and issue orders to block websites under Section 20.

However, it is found that in practice the court did not spend much time approving the petitions filed by the MICT and issuing orders. Since the enforcement of the CCA, there have been 156 orders. Among these, 142 were issued on the same

Year	The total number of days spent in approving a petition	The total number of URLs	The average number of the URLs per day
2007	2	2	1
2008	35	2,071	59
2009	88	28,705	326
2010	46	45,357	986
2011	36	5,078	141
Total	**207**	**81,213**	**392**

Figure 7: Table showing the number of days and number of URLs that the court considered by year (2007-2010)

day that the MICT submitted the petition, resulting in 78,192 URLs being blocked. Between 2007 and 2009, when the MICT filed a petition to the court, the court would spend an average of 2-6 days to judge if it should issue an order to block a website or not. During 2009 and 2010, the number of petitions filed increased dramatically. The information on the number of court orders and the number of blocked URLs shows that the court had to consider on average 326 URLs per day in 2009 and 986 URLs per day in 2010.

The amount of time spent in considering the contents of websites in petition and issuing restriction orders is very important. Although Section 20 of the CCA does not prescribe a criminal penalty for offenders, the measures taken, of denying the public access to information, infringes on people's

right to freedom of expression, a basic right guaranteed by the Constitution of Thailand. The deprivation or limitation of any freedom should be implemented in a reasonable, thorough and appropriate manner. In this context, examination of petitions involving 200-300 URLs and issuing an order within one day by a single judge (or even by a panel of three judges as sometimes appointed) must have been completed with great difficulty. Or the court must have had a huge working team to examine the contents at an incredibly swift pace. However, there is no evidence of the existence of such teams. For this reason, the question has arisen among members of society and affected people as to whether the court has been an effective counterbalance to the executive as envisaged in the CCA.

According to Section 20, after the court has issued an order, a copy of the order will be forwarded to internet service providers to block access to internet users in Thailand.

1.2 Statistics on Prosecutions under the CCA

Data compiled for July 2007 - December 2011 show a total of 325 prosecutions under the CCA, 12 of which occurred in 2007, 32 in 2008, 80 in 2009, 104 in 2010 and 97 in 2011. (See figure 8)

Offences under the CCA can be divided into two groups: 1) true computer crimes or crimes relating to "the data or the system" of a computer under Sections 5–13,[14] such as illegal access, data filtering or system sabotaging through the spread of viruses, etc.; 2) crimes relating to the dissemination of "content" on computer systems under Sections 14-16, such as dissemination of obscene images, dissemination of information deemed a

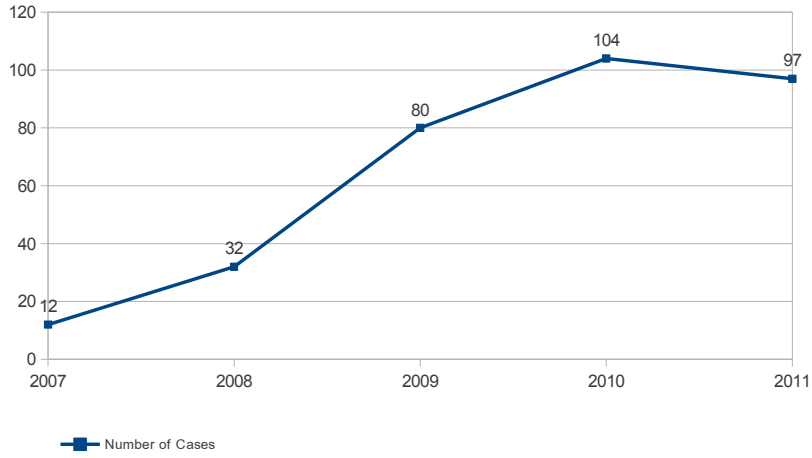


Figure 8: Annual prosecutions under the CCA (2007 – 2011)

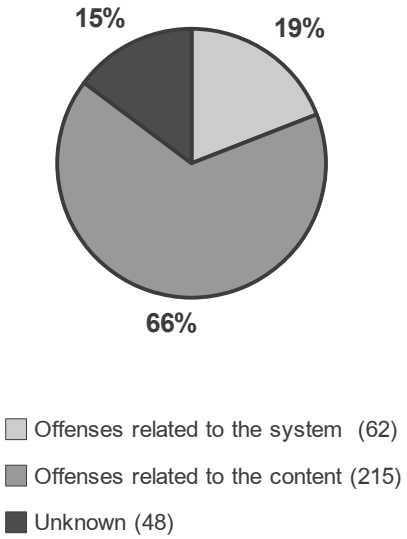


Figure 9: Prosecutions filed under the CCA by type

threat to national security or defamation by computer-generated or computer-modified images, etc.

In the three years and six months since the CCA came into force, 28 cases relate to crimes involving the computer data or system (true computer crimes) accounting for 17.18% of all cases, whereas 103 cases or 63.19% relate to crimes involving the dissemination of offensive computer content. The remaining 32 cases (19.63%) are unclear. (See figure 9-10)

Prosecutions can be further classified into seven categories by the types of offence: defamation (100 cases); true computer crimes (47); lèse majesté (40); online fraud (31); dissemination of pornography (31); sale of illegal software (12): security-related crimes (6). The remaining 58 cases are unclear and cannot come be categorized. (See figure 11)

When classified by case status and outcome, 89 cases are under investigation by inquiry officers; 70 cases have been filed by the prosecutor; one case has not been filed by the prosecutor; 20 cases have been mediated/compromised/withdrawn; 13 cases have been dismissed by the court; 73 cases have been ruled guilty; in two cases the inquiry officers have brought charges under the CCA but the prosecutor did not file the cases on those charges or the court did not render judgment under the act. The remaining 57 cases have already been tried by provincial courts, where the researchers do not have access to information. (See figure 12)

Figure 13 shows that defamation offences are not only the most numerous cases filed under the CCA, but also the most numerous to end with mediation, compromise or withdrawal. On the contrary, the other categories like computer crimes, lèse majesté or pornography, which are smaller in number, are likely

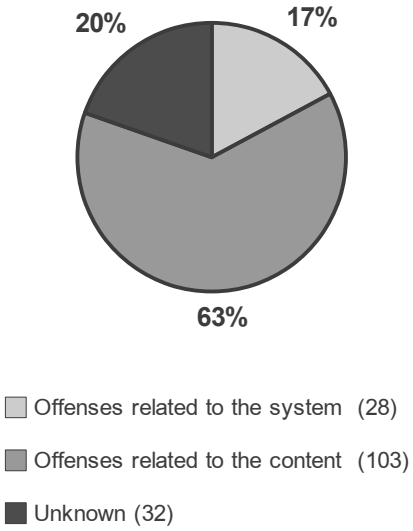


Figure 10: Cases tried by the Court of First Instance by type

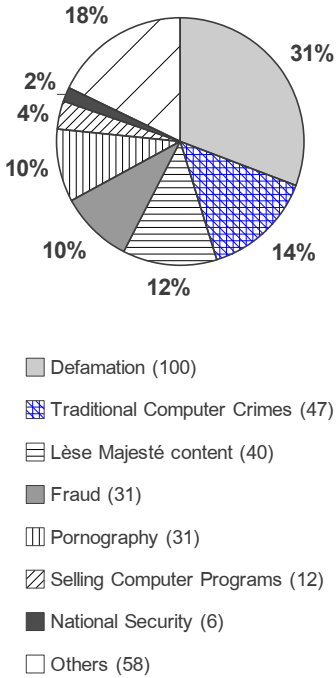


Figure 11: Prosecutions by category of offence

to be prosecuted and ruled guilty.

In the 73 cases where a verdict was reached (See figure 14), the defendants confessed in 62 and defended themselves in 11. In case of defamation and pornography where there is a confession, the court is most likely to suspend the sentence. When a defendant confesses, the overall behavior is not seen as harmful or the court believes it is appropriate to give the defendant the chance to reform so there is no need for imprisonment as. In some cases, the court orders community service or dharma courses in order to soften the mind through religion during the suspension period. However, computer crime, fraud and lèse majesté cases are much likely to receive sentences without suspension. For example, in Red Case No. Dor (ด.) 1945/2553 at Bangkok South Criminal Court, the defendant had hacked into the computer system of a hosting company and erased the data of a member. The court gave a sentence of imprisonment without suspension with the reason: "under the current circumstances, computer usage for economic purposes and for academic and general research has become widely popular. The crime that the defendant has committed has an effect on the confidence of computer users and on society in general. It is deemed a severe crime and therefore, there is no ground for suspension".

Classification of cases by complainants shows that that most cases (66) are brought by female citizens, followed by juristic persons (56 cases), male citizens (44 cases), TCSD (19 cases), MICT, (17 cases), DSI (13 cases), Crime Suppression Division (CSD) (12 cases), other state agencies (12 cases), local police officers (6 cases), CWD (4 cases), and ECD (3 cases). In 73 cases the origin is unclear.

Although official information shows only 17 cases filed

Category of Offense	Procedure of the Case								Total
		Prosecutor				Court			
	Investigating	Charge	Not Charge	Not Charge with CCA	Mediated / Disposed of the Case	Dismissed	Guilty	Tried, but inaccessible data	
Offenses under section 5-13	24	10	0	0	4	1	18	5	62
Offenses under section 14-16	62	48	1	1	15	12	54	22	215
Cannot be defined	3	12	0	1	1	0	1	30	48
Total	89	70	1	2	20	13	73	57	325

Figure 12: Number of cases classified by offence and the status of the case

Computer-related Crimes Act Cases	National Security	Defamation	Lèse Majesté content	Pornography	Fraud	Traditional Computer Crimes	Selling Computer Programs	Others	Total
With the investigator or with the police officials	1	15	28	1	11	14	10	9	89
charged by public prosecutor	2	32	4	3	8	9	0	12	70
Dismissed by public prosecutor	1	0	0	0	0	0	0	0	1
Cases filed or ruled not under the Computer-related Crimes Act*	0	1	0	0	1	0	0	0	2
Ended with mediation, case disposal	0	14	0	0	1	4	0	1	20
court dismissed the charge	1	10	1	0	0	1	0	0	13
the verdict rules that the defendant are guilty	1	17	7	23	5	16	0	4	73
the court has delivered the verdict but the researchers could not get the access to the result of the trial**	0	11	0	4	5	3	2	32	57
Total	**6**	**100**	**40**	**31**	**31**	**47**	**12**	**58**	**325**

** Cases that were charged with the Computer-related Crimes Act during investigation but not filed as such by the prosecutor or not ruled as such by the court*

*** Case information obtained from provincial courts, which only indicates the number of cases and the charges but not the details and the verdict.*

Figure 13: Outcome of cases classified by offence

by the MICT, one of these filed with the Crime Suppression Division involves a list of 1,037 URLs with content deemed in breach of Section 112 of the Criminal Code. This case is still pending under investigation by inquiry officers. This one case could lead to 997 prosecutions.

As far as the details of the accused and the defendants of the CCA are concerned, the general male individuals are the most to be charged and prosecuted with 153 cases, while the female counterparts are at 67 cases. Moreover, there are 24 cases that involve the internet service providers, which are regarded as a content provider or a communication service provider, like webmasters or webboard administrators. There is also a handful number of cases, where the defendants are media people and many other cases, whose offenders are unknown.

Offense	Guilty Verdict (73)				Dismissal	Mediated/ Disposed of the Case	Unaccessible Verdict		Total
	Confession (62)		Defense (11)				Confession	Defense	
	Imprisonment	Suspension	Imprisonment	Suspension					
National Security	0	1	0	0	1	0	0	0	**2**
Defamation	1	16	0	0	10	14	2	9	**52**
Lèse Majesté content	4	1	2	0	1	0	0	0	**8**
Pornography	2	19	2	0	0	0	3	1	**27**
Fraud	5	0	0	0	0	1	0	5	**11**
Traditional Computer Crimes	9	2	5	0	1	4	0	3	**24**
Selling Computer Programs	0	0	0	0	0	0	2	0	**2**
Others	0	2	2	0	0	1	19	13	**37**
Total	**21**	**41**	**11**	**0**	**13**	**20**	**26**	**31**	**163**

Figure 14: Verdicts and sentences by the court of first instance classified by offence

Complainants	National Security	Defamation	Lèse Majesté content	Pornography	Fraud	Traditional Computer Crimes	Selling Computer Programs	Others	Total
Male	0	24	1	1	5	9	0	4	**44**
Female	0	39	0	12	9	2	0	4	**66**
Private juristic persons	0	19	0	0	5	**25**	0	7	**56**
ECD	0	0	0	0	1	2	0	0	**3**
TCSD	1	0	3	0	2	2	10	1	**19**
CWD	0	0	0	4	0	0	0	0	**4**
CSD	2	1	8	0	0	0	0	1	**12**
DSI	1	0	9	0	0	3	0	0	**13**
MICT	0	0	**16**	0	0	0	0	1	**17**
Other state agencies	1	1	2	4	1	2	0	1	**12**
Local police	0	1	1	2	0	0	0	2	**6**
Unknown	1	15	0	8	8	2	2	37	**73**
Total	**6**	**100**	**40**	**31**	**31**	**47**	**12**	**58**	**325**

Figure 15: Complainants bringing charges by offence

Accused		National Security	Defamation	Lèse Majesté content	Pornography	Fraud	Traditional Computer Crimes	Selling Computer Programs	Others	Total
General Public	Male	3	42	15	21	18	26	9	19	**153**
	Female	1	23	4	3	8	9	1	18	**67**
	Private juristic persons	0	6	0	0	1	**1**	0	1	**9**
	Offenders unknown	0	6	14	0	1	**6**	0	3	**30**
	Information N/A	1	7	3	2	3	5	2	17	**40**
Service Providers	Service providers	1	15	3	5	0	0	0	0	**24**
	Other intermediaries	0	1	1	0	0	0	0	0	**2**
Total		**6**	**100**	**40**	**31**	**31**	**47**	***12***	**58**	**325**

Figure 16: Accused/defendants under the CCA by offence

Analysis and Observations on the Prosecution of the CCA Cases

From all cases to which the researchers has access were able to compile, a relatively high proportion of offenses concern content dissemination under Sections 14-16 of the CCA when compared to true computer crimes or crimes dealing with computer data or systems, under Sections 5-13. This includes cases brought under the provisions of the CCA alone and those based on both the CCA and other laws, such as the Criminal Code.

1) Use of Section14 (1) in Defamation Cases and Authenticity of Content

"Section 14 If any person commits any offence of the following acts shall be subject to imprisonment for not more than five years or a fine of not more than one hundred thousand baht or both:

(1) that involves import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to that third party or the public;"

Because users may use pseudonyms in online communication, the process of identifying users, though possible, is not as easy as with real names. Internet users may condemn, accuse or even sabotage someone's reputation by publishing personal information or images without fear of being arrested. This leads to the unprecedented increase of defamation cases brought to the court, frequently without the complainants knowing who

the offenders are. In the past, defamation cases appear to have been used as a political tool for politicians to sue each other or the media. In both criminal and civil cases involving huge compensation, Section 423[15] of the Civil Code or the Section 326[16] in combination with Section 328[17] of the Criminal Code cover online defamation offences already and there is no need for the specific provisions in the CCA. However in practice, it is found that many defamation cases on the internet made use of the CCA, with the injured party filing the case under the Civil or Criminal Code, in combination with Section 14 (1) of the CCA.

In fact, the genuine intention of the drafting committee of the CCA including Section 14 (1), as interpreted, was not meant to replicate the existing defamation laws.

The original intention of the drafters was for Section 14 (1) of the CCA to fill a gap in the Criminal Code on crimes related to "document forging"[18], where the Criminal Code can be interpreted as applying only to "paper objects or other materials"[19], and not to electronic document forging[20], thus leaving a loophole in the law. Section 14 (1) therefore was not intended to cover importing to a computer system data (whether true or false) that is likely to cause damage to the reputation of, or defame a third party, which constitutes a crime similar to defamation in the Civic and Criminal Codes. It was intended to mean "to import to a computer system of forged computer data, either in whole or in part, or false computer data" which constitutes a crime similar to that of document forging in the Criminal Code.

To use Section 14 (1) against defamation overlaps with other laws, and also creates confusion to those charged as well as the general public.[21]

2) Use of Section14 (2) and (3) in State's Security Related Cases

"Section 14. If any person commits any offence of the following acts shall be subject to imprisonment for not more than five years or a fine of not more than one hundred thousand baht or both:

(2) that involves import to a computer system of false computer data in a manner that is likely to damage the country's security or cause a public panic;

(3) that involves import to a computer system of any computer data related with an offence against the Kingdom's security under the Criminal Code;"

It seems that national security was particularly emphasized in the drafting of the CCA. Offences related to this were placed under Section 14 (2) and (3). At the same time, Section 14 (2) is also one of the most problematic articles regarding its scope. It is also criticized for being used by the state as a tool to restrict people's freedom of expression due to the ambiguous wording within the paragraph, namely "damage the country's security" or "cause a public panic"; the general public cannot understand at once what kind of information would constitute such a crime. It allows each case to be interpreted in its own way, which is subject to change according to the times and the attitude of those who control the law.

This section can be used for political harassment. When there were uncontested prosecutions, the vagueness of the charges would not be proved beyond reasonable doubt. For example, in a security-related case, the court sentenced the owner of texts and images of Kim Jong-Il, then President of

North Korea, on the grounds that they might create confusion and conflict among the people and affect Thai-North Korean relationships, regarded as a threat to the country's security. In this case, the defendant confessed and was found guilty without any explanation of how talking about the President of North Korea could affect international relations.

Case statistics indicate that most security-related cases are lèse majesté offences under the Section 112 of the Criminal Code, which is usually used in combination with Section 14 (2) or (3) (40 cases). Six cases concern other security-related offences or offences against public morals. Taking into account the social context, it is probably understandable that most accused on lèse majesté charges have been denied bail. They also face pressure to confess and gain the chance to beg for a royal pardon. Most of the accused, who are remanded in pre-trail detention, choose to confess even if they hope to win a trial, as it is not worth spending time in the prison without bail. In the four years and six months since the law's enforcement, there has been no single case study to analyze the definition of the word "security" in these two paragraphs.

So far, only two cases charged under Sections 14 (2) or (3) have been dismissed by the court. However, the reason for the dismissals was not the failure to prove that the dissemination of online information threatened national security, but the failure to prove that the defendants were the persons who disseminated the information.

Notable Cases under Section 14 (3)

Among all the security-related cases filed under the CCA, there are notable two examples cases, where service providers

were charged under Section 14 (3) of the CCA for intentionally supporting or allowing a crime to take place. The defendants in both cases were found guilty and sentenced.

In Red Case Number Or (อ.) 1226/2554 of Criminal Court, Tantawuth the designer of the Nor Por Chor (UDD) USA website, was accused of being the writer of two texts offending the institution of the monarchy and of allowing the publication of one offensive article. The defendant denied all charges and argued that he had logged into the system because he was hired to design it but he did not post the two texts as alleged and had no authority or responsibility to regulate the contents of the website. The prime evidence in this case was a log file, which showed that the defendant had logged in into to the system through an FTP (File Transfer Protocol) program under the name "noporch"; the police officers believed that to use such a program, a certain amount of skill is required, so they considered the defendant to be legally the "provider". The two texts in the complaint appeared to be posted by a user registered under the name "admin" (not "noporch" used by the defendant), which is usually understood to be the system administrator. The police, therefore, charged the defendant as both the originator of the text and the service provider by law. The sentence was 13 years in prison.

In Red Case Number Or (อ.) 2091/2555, the defendant, Chiranuch Premchaiporn, the director of the online newspaper website Prachatai, was responsible for the content and a web-board open for the public to express opinions. The case concerned third party comments posted on the Prachatai website. The court ruled that the defendant was guilty under Sections 14 (3) and 15 of the CCA and sentenced to a one-year prison

sentence and a 30,000 baht fine. Since the defendant cooperated in the judicial process, the court reduced the penalty by one-third to eight months in prison term and a 20,000 baht fine. Her jail term was suspended for one year because she had never been previously convicted. The court reasoned that the defendant has allowed the data which breached national security to be imported to the webboard for which she was the administrator. Most of the offensive texts were allowed to appear for one to ten days, but one text remained for 20 days. The court considered that this was enough time for the defendant to be aware of the text and delete it. The court therefore considered the failure to delete the text in a timely manner, as neglect of duty with implied consent to import false data in a computer system, constituting a crime under Sections 14 (3) and 15 of the CCA.[22]

The researchers find the case interesting in two ways. Firstly, even though the court in this case acknowledged that Thailand, unlike other countries, has at present no written regulation regarding the "timeframe" within which a service provider must take down messages when notified (Notice & Takedown), the court ruled against the defendant that 20 days were "unacceptably late." Secondly, the court used the 20-day duration to reason the "implied consent" of the defendant in allowing the import of the text in a computer system. This means that even though the prosecutor was not able to prove "beyond reasonable doubt" that the defendant "intentionally" consented to or supported the commission of a crime, the court still handed down a guilty verdict. These two issues raise the question how legitimate the ruling is, and whether it abides by "the principle of legality" (nullum crimen, nulla poena sine lege).

3) Use of Section 14 (4) in Dissemination of Pornography

"Section 14 If any person commits any offence of the following acts shall be subject to imprisonment for not more than five years or a fine of not more than one hundred thousand baht or both:

(4) that involves import to a computer system of any computer data of a pornographic nature that is publicly accessible;"

Quick and easily accessible, internet communication technology and the ability to hide one's identity facilitate the instant dissemination of sexual images, which can sometimes be interpreted as pornography. As with defamation, the dissemination of pornographic materials is already covered under Section 287 of the Criminal Code[23] but the CCA drafting committee thought that the definition needed to be extended through Section 14 (4) of the CCA. In the past this section has used mostly to request court orders to block pornographic sites. 22 prosecutions have been brought under Section 14 (4) with 18 cases already tried. With the exception of one case where the details could not be accessed, all ended with the defendants' confession. These cases were initiated by state authorities and, more frequently, the victims whose images were disseminated. In the prosecution process, Section 14 (4) was usually used in combination with Section 287 of the Criminal Code. Many cases also made use of Sections 326 and 328 of the Criminal Code on defamation because the obscene images or texts could destroy someone's reputation.

Notable Cases under Section 14 (4)

Of 22 cases under Section14 (4), five involved providers which all ended with their confession. They were therefore given suspended sentences by the court. However, there is no evidence that, after the victim has prosecuted the providers and the court has ruled on the cases, there was any attempt to prosecute the internet users who were the main principals in the import of the texts or images to a computer system.

One notable example is the case of the service provider of the 212cafe website, which allows the general public to create their own webboards. It appears that someone posted a nude image of the victim on a webboard on the 212cafe website. The victim reported it to the police and the police officers ordered the 212cafe webmaster as the service provider to remove the image, but as the webmaster was not at home when the order arrived, the police could not contact the service provider. Finally, the police forcibly arrested the service provider at his house on charges of "supporting or consenting" to the dissemination of the pornographic messages or pictures (Section 14 (4) and Section 15 of the CCA). The case is particularly interesting because the state official's inability to contact the service provider (regardless of the reasons) led to charges under the CCA against the service provider.

Notwithstanding the court's verdict, when such a case is prosecuted, the defendant is burdened with the trial process consequent from the actions of others. This service provider has had the trouble of having to fight the case. What must be considered is the size of the operation. The 212cafe webmaster is only a small-scale operator who wrote the webboard system to provide a free service to the public (at present there are many like this). The capacity in terms of budget and staff to monitor

content in his service cannot equal that of large service providers. Placing the burden of responsibility on service providers of all kinds, who are only intermediaries through whom information is passed online, will discourage this type of service and create a culture of fear in the business, especially among small enterprises. These conditions contribute to restricting opportunities for free communications online.

Conclusions from quantitative impacts study

It can be said that in the four and a half years from July 2007 to December 2011 the CCA has been used to control the content of online media rather than combat true computer crimes or crimes executed on data or computer systems according to Sections 5 to 13 of the CCA, which was the original intention of this law.

The CCA has been used to block a total of 81,213 URLs, the majority of which were censored for containing lèse majesté materials and pornography. The number of websites blocked can be observed to fluctuate according to the political situation.

Section 20 of the CCA grants authority to the state to block websites, and although the law is problematic for its ambiguity, the set procedures for exercising this authority were designed to prevent the state's abuse of power. Before a website can be censored, state officials have to file for the permission of the courts, which issue orders. However, the numbers of websites blocked by court orders in recent years raises questions concerning both the effectiveness of judiciary oversight and justice for webmasters and online media consumers affected by the law. It is extremely difficult, if not impossible, for the judges to give

full consideration to an average of 392 websites per day.

Further, the analysis shows that even without the CCA, the Thai state still has other measures to restrict access to websites, such as the Emergency Decree and other bills concerning national security, or by requesting cooperation from service providers. Neither of the Emergency Decree nor requests for cooperation require judicial oversight over state officials' exercise of authority. There is a current lack of protocol concerning the timeframe within which webmasters should be warned of the offensive material and the duration for blocking websites. Neither records of state officials' exercise of power exist nor are they required to justify the reasons for their actions.

Three years after the CCA came into force, more than half of prosecutions (66.15%) concerned the dissemination of content by online media websites. This is about three times the number of prosecutions for true computer crimes (19%).

The three most frequent types of cases are defamation, true computer crimes, and lèse majesté. Whereas complaints concerning defamation and true computer crimes mainly come from citizens or juristic persons, lèse majesté complaints originate primarily with state bodies: the MICT, the DSI, and the Crime Suppression Division of the Royal Thai Police.

The original intention of the CCA was to combat true computer crimes, where interpretation of provisions under the Criminal Code could not be applied because of the different nature of the offence. In practice however, the CCA has been used to control content disseminated by online media, which directly affects the people's rights and freedoms. Section 14 was used in many prosecutions, even though in terms of legislation is held to have content that overlaps with offences under the

Criminal Code. The difference is only that the CCA has more severe penalties. Both defamation penalties and offences concerning the distribution of pornographic material and images carry heavier penalties than under the Criminal Code. The CCA also turns some offences, especially defamation, into public offences, where anyone can lay charges with the authorities. Such duplication of legal provisions at the very least creates confusion among the general public as well as enforcement agencies, resulting in misinterpretation and distortion of the intention of the law.

Freedom of communication and expression is also limited by Section 15 in particular, which faults service providers who act as intermediaries without an attempt to understand the volume and nature of information disseminated through online media, where the service provider is unable to monitor closely all content in a website. This has created a culture of self-censorship in the media, where certain topics are omitted from reports and service users are prevented from expressing their opinions. Worse, reported news is sometimes distorted and incomplete as to avoid defamation and liability. An additional problem that surfaces from this research is that many allegations against service providers stem from the state's inability or lack of willingness to investigate and trace the true wrongdoer, both of which are more complicated tasks, requiring time and skills. Instead, allegations are aimed at webmasters and service providers alone, which conflicts with the original intention of the law that both perpetrators and intermediaries be prosecuted.

2. Qualitative Study

In addition to a quantitative study website blocking statistics and prosecutions in the last three years and six months, in-depth interviews and focus group discussions were conducted to collect the opinions of personnel in various organizations relevant to the enforcement of the CCA.

The results of the survey are divided into three parts.

Part 1: The role of state agencies in enforcing the law and policy which affect the right to freedom of expression

Study Method

Indepth interviews were conducted with randomly selected state personnel who have experience with and have enforced the CCA to survey their opinions. The researchers also asked for recommendations from other persons able to give reliable information through interviews, making a total seven persons.

1) Officer (name withheld) from the IT Crime Prevention and Suppression Bureau, MICT

2) Competent official (name withheld) under the CCA, MICT

3) High-ranking police officer (name withheld) of the Technology Crime Suppression Division (TCSD)

4) Pol Col Siripong Timula, Deputy Commander of Technology Crime Suppression Division

5) Krerkchai Srisukcharoen, Senior Investigating Officer, Bureau of Technology and Cyber Crime, DSI

6) Pol Col Anuchit Bunyapatiphak, Department of Computer Crime Detection, Central Scientific Crime Detection Division

7) Expert police officer in technology (name withheld), Royal Thai Police

Part 2: Duties and roles of internet business entrepreneurs under the CCA and implications concerning the right to freedom of expression

Study Method

A focus group discussions were used to collect information from service providers and internet business entrepreneurs, including internet service providers, web hosting service entrepreneurs and data center/storage service providers. Despite the diversity of background, all have similar experiences regarding the CCA.

The researchers submitted invitation letters to the focus group discussion to internet entrepreneurs using relevant networks to identify persons who could give reliable information. Participants comprised 14 persons from eight organizations. The internet service providers included two legal officers from CAT Telecom Public Company Limited, a legal officer from Advanced Info Service Public Company Limited, three public affairs officers from Total Access Communication Public Company Limited, two legal officers from TT&T Public Company Limited, and a representative from True Corporation Public Company Limited. Web hosting service providers included three representatives from ANET Company Limited, one

representative from Thai Host Talk, a web hosting entrepreneur association, and one representative from Proimage Engineering & Communication Company Limited, who provides both web hosting and data center services.

Part 3: The roles of webmasters and webboard administrators under the CCA and implications concerning the right to freedom of expression

Study Method

A focus group discussion included webmasters and webboard administrators chosen for the variety of website content including political news, technology news, variety news, professional associations, weblogs, webboards and internet business entrepreneur.

Political news websites:

1. Chuwat Rerksirisuk, editor of Prachatai (http://prachatai.com)

2. Varit Limthongkul, journalist and columnist of Manager ASTV (http://www.manager.co.th)

Technology news website:

3. Isriya Paireepairith, founder and webmaster of Blognone (http://blognone.com)

Variety news websites:

4. Somporn Suksamann, webmaster of MThai (http://mthai.com)

5. Sithichoke Supaporn, webmaster of MThai (http://mthai.com)

Webboard:

6. Thammaporn Seekhao, legal officer of Pantip (http://pantip.com

Weblog:

7. Pathinya Sa-ngiamchit, founder and webmaster of Exteen (http://exteen.com)

Professional association

8. Asina Proawasin, president of IT journalist club, and IT journalist of The Nation newspaper

Summary of the study on qualitative impact

The information and opinions of state personnel, service providers and webmasters based on their experience with the CCA and relevant suggestions can be summarized as follows.

1. Experience with the CCA

State sector The CCA provides a clear mandate for officials to block access to websites. Though various websites have been blocked for a variety of reasons, none have been prosecuted.

The CCA authorizes competent officials to carry out their duties and requires service providers to record computer traffic data which proves to be very useful during investigations. Nonetheless, real computer crimes have not been detected so far. Most cases have involved political conflicts and political changes and as a result the CCA has been increasingly applied to national security related cases.

Though the CCA authorizes competent officials, it has no effect on the operations of the Department of Special Investigation (DSI), since the DSI relies on the authority prescribed by the DSI Act, rather than the CCA.

Internet business entrepreneurs The CCA contains clear provisions governing cooperation with the state in terms of blocking access supported by corresponding legal procedure. It is clear for service providers to block websites when a court order is established. In addition, the CCA has changed the way the state treats computer traffic data. Formerly, service providers might have been able to refuse to store data with the claim that it was the private information of their clients, but the CCA makes it imperative for service providers to store data and provide it to competent officials, and any breach of this obligation may result in a punishable offence.

Webmaster The CCA has instigated internal regulations among service providers. For example, user content is now filtered prior to dissemination to the public and users are required to register prior to posting any messages or comments. More personnel and equipment have to be procured to meet additional filtering duties and even legal advisors are now needed to monitor any legal issues that may arise and to monitor compliance with requests from the state.

2. Implications of the CCA for the right to freedom of expression

State sector Four major issues are identified.

1) Interpretation of many sections of the law gives

the authorities broad latitude to use their own discretion. For example, the clause on forged or false computer data is extremely vague and it is difficult to prove "falsehood". In addition, online communication has often led to new issues and competent officials are always required to explore if those issues fall within the scope of the CCA.

2) There has been no clear application of the law to suppress true computer crimes and to protect the damaged parties. For example, when any victim of a computer crime reports it to the police, the police often refuse to accept the complaint claiming that it is outside their jurisdiction, or that they are not qualified to investigate since they are not competent officials under the CCA

3) There is a lack of personnel with sufficient knowledge and understanding of CCA cases due to the government service system where once the competence of officials has been developed, they may be rotated to other government departments. The appointment of competent officials under the CCA in many cases has not been drawn from those with the qualifications according to criteria set by the law, but has depended on the discretion of the Minister of Information and Communication Technology, or has chosen officials without sufficient knowledge and expertise to request information from service providers under the CCA. This has a direct impact on the credibility of state officials.

4) The clauses that authorize competent officials under the CCA to request information or computer data are interpreted so as to exclude other inquiry officials. As a result, certain criminal offences such as fraud, which fall within the scope of the Criminal Code, have in reality been prosecuted under the

CCA with competent officials simply seeking authorization to request necessary data from service providers. Online fraud cases are overwhelmingly handled by the central MICT authorities.

Internet business entrepreneurs Three major issues were identified.

1) Service providers feel unsure about the interpretation of Section 15 which penalizes service providers for "intentionally supporting or consenting to" the dissemination of offensive messages under Section 14 and exposes them to the penalties as those posting offensive information, and about the definition or indicators which can be used to prove intentional support or consent.

2) Collaboration with the state to block web access has led to problems since although the service providers are willing to block access, the information supplied by the authorities in some cases was wrong. Otherwise, the service providers are requested to carry out something that cannot be done promptly and the instructions given to them are on paper instead of in electronic form. In addition, there are currently no clear guidelines between the MICT and all service providers as to how to communicate with users the reasons for the blocking. Inconsistent legal enforcement was also identified, with some service providers receiving orders to close down access to certain websites, but others not, and so clients of the former complain.

3) Though the CCA is now in operation, "informal requests" have always been made by the authorities, mostly citing the urgency of the issue. The service providers have often been told to block access with the promised of a court order later, but

in some instances the orders have never been issued.

Webmasters Four major issues were identified.

1) The CCA penalizes intermediaries, holding them liable instead of attempting to bring to justice the real perpetrators.

2) Vague clauses provide for substantial room for interpretation according to the competent officials' discretion, for example with respect to forged and false data under Section 14 (1). The Section is in fact often invoked in libel suits, which makes it redundant with the provisions of the Criminal Code.

3) The CCA has tended to be used to impose restrictions rather than provide protection. According to the service providers, the law has not been designed to uphold freedom of information and law enforcement officers have failed to implement the law in a straightforward manner. They tend to lack understanding and misuse the law. As a result, the law has been used as a tool to suppress dissent.

4) The law requires business operators to shoulder additional expenses and extra legal liabilities. The problems have no effect on big media companies, but do affect operators of user-generated content websites and smaller websites since the operators of these websites never intended to run their websites for profit in the first place. As a result, they tend to self-censor or use other ways to evade legal requirements, such as by hosting their websites using services abroad. This problem affects the overall ICT business.

3. Comments and suggestions regarding the CCA and state policy

State sector State officials believe it is still necessary to have a legal mechanism to block websites to help ease some problems. In computer crime prosecutions, general investigating officers should also be authorized to invoke the CCA in order to view, copy and seize any electronic evidence. Meanwhile, competent officials appointed by the MICT under the CCA should help to provide specific technical expertise, rather than engage simply in submitting requests for IP addresses. According to some comments, a special Computer-related Crime Court should be established or associate judges be recruited to try computer crime cases.

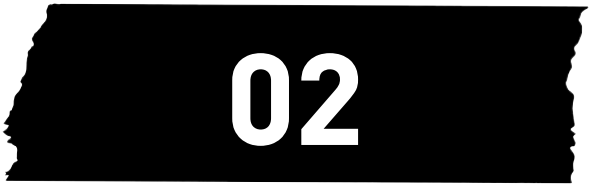
Internet business entrepreneurs Most service providers view it necessary to continue blocking web access, but the state should not resort to these measures indiscriminately since it can be tantamount to restricting the right to information of media and the public. In particular, political reasons should not be cited to justify any blocking. They also deem judicial review important, but propose that other measures be made available should it happen that the court orders prove unlawful. Nevertheless, according to the service providers, the CCA has simply been used as a tool by the state, rather to solve problems of injured parties. It was therefore proposed that the state should have to provide clear and actionable supporting evidence to prove that a website is offensive. Instead of simply blocking access, the state should stem the problem at source by prosecuting the offenders.

Service providers also recommended that if the CCA holds service providers liable for online contents, it should

categorize their liabilities and provide clear takedown procedures. Nonetheless, the state should issue a law based on the understanding that service providers simply function as "intermediaries" and it is very impractical to require service providers to monitor huge volumes of online information. Any legal amendments must take into account rapid changes in ICT.

Webmasters Content providers and webmasters still hold that the CCA is necessary to prevent the commission of offences, but at the same time, measures should also be taken to protect the rights of internet users. Many internet users' rights are currently not protected, including privacy of information. Too many duties and liabilities have been placed on service providers. It was therefore proposed that the law must be changed to adapt to constantly changing online communication. The state should also make more effective attempts to educate the public about the CCA. In addition, service providers believe that the state should respect people and instead of enforcing the law and imposing liabilities on service providers, they should change the policy to one of encouraging service providers to regulate themselves and to establish a separate body to work out which websites should be blocked.

CHAPTER



Part 2

Comparative Study of the Laws,
State Policy and Civil Reaction on Freedom of Expression
in Online Media in Thailand and
those of Other Countries:
Thai laws and online media freedom

Thai laws and online media freedom

1. Guarantee of Freedom of Expression under the Thai Constitution

Sections 26 - 69 in the 3rd Chapter of the Constitution of the Kingdom of Thailand 2007 guarantee the rights and liberties of all Thai citizens. These rights and liberties had already been officially recognized in the Constitution of the Kingdom of Thailand 1997 with the goal of preventing violations of the rights and liberties of citizens by each other and preventing state agencies from using the power of the state to arbitrarily violate the rights and freedoms of the people.[1] This is a confirmation of the "Rechtstaatsprincip", which is closely associated with democratic principles. The provisions on the protection of freedom of expression (of individuals as well as the media,

which automatically means the right to access information), are recognized by the 1997 Constitution and transferred to the 2007 Constitution in Section 45.

"A person shall enjoy the liberty to express his opinion, make speech, write, print, publicise, and make expression by other means.

The restriction on liberty under paragraph one shall not be imposed except by virtue of the law specifically enacted for the purpose of maintaining the security of State, protecting the rights, liberties, dignity, reputation, family or privacy rights of other person, maintaining public order or good morals or preventing or halting the deterioration of the mind or health of the public.

The closure of a newspaper or other mass media business in deprivation of the liberty under this section shall not be made.

The prevention of a newspaper or other mass media from printing news or expressing their opinions, wholly or partly, or interference in any manner whatsoever in deprivation of the liberty under this section shall not be made except by the provisions of the law enacted in accordance with the provisions of paragraph two.

The censorship by a competent official of news or articles before their publication in a newspaper or other mass media shall not be made except during the time when the country is in a state of war; provided that it must be made by virtue of the law enacted under the provisions of paragraph two.

The owner of a newspaper or other mass media business shall be a Thai national.

No grant of money or other properties shall be made by State as subsidies to private newspapers or other mass media."

According to these provisions, it is seen that the even the constitution, despite being the supreme law of the country, does not grant citizens unlimited freedom. Instead, it insists on the principle that the "state" as the representative of those exercising administrative authority can take legal measures to limit or control the freedom of the people or the media on four grounds: 1) to maintain State security; 2) to maintain public order or the morals of the people; 3) to protect personal rights or reputation of others; 4) to prevent or cease the physical or mental health deterioration (Section 45 Paragraph 2). Nevertheless, the state must bear in mind that the constitution also contains provisions preventing "abuse of power" by the state to prevent the arbitrary or inappropriate excercise of power to restrict the rights and liberties of the people as stated in Section 29 of the Constitution:

Section 29. "The restriction of such rights and liberties as recognised by the Constitution shall not be imposed on a person except by virtue of the law specifically enacted for the purpose determined by this Constitution and only to the extent of necessity and provided that it shall not affect the essential substances of such rights and liberties..."

This section shows that to protect the rights of the individual and prevent arbitrary use of power by organs of the state, the state has the power to restrict some rights under the Constitution. This must subject to at least four criteria:

1) Rights and liberties can be restricted only under specific legal provisions

2) The restriction of rights and liberties must be for the purposes determined by the Constitution, which is to protect the "public interest" as the ultimate goal or objective of the very existence of the state to respond to the needs of the majority

in society. In the case of freedom of expression, this restriction must be within the four criteria of Section 45 above.[2]

3) It must be only as far as is "necessary", or in other words, the rights and liberties of the people must be restricted in accordance with the "Principle of Proportionality", a universal principle designed to control the state's exercise of power[3] that contains three criteria:

(i) The "principle of achievement" means that the state must choose only those measures that would achieve the intentions or determination of the Constitution

(ii) The "principle of necessity" means that if the state has many measures to limit the freedom of the people, it must choose those measures with the least effect on freedom that are compatible with the intentions of the Constitution.

(iii) The "principle of appropriateness" means that if measures that the state uses to limit freedom have little benefit and are not worth the loss of freedom of the people, the state must not use such measures.

4) The restriction of rights and liberties must not change the essential substance of those rights and liberties. In other words, when the Constitution guarantees certain rights or liberties, the state may not "restrict" them to the extent that it has the effect to "eliminate" or "withdraw" those rights and liberties.[4] Even when provisions of certain laws might give such power, it would still be impossible to implement, because Section 6 of the Constitution of Thailand 2007[5] annuls the effect of any law that contradicts the Constitution.

In conclusion, even though the rights and liberties guaranteed by the Constitution do have some restrictions and the state has the power to define, limit or control those rights

and liberties through legislation and enforcing the provisions of certain laws, it does not mean that the state can issue any unjust laws or unfairly, arbitrarily or unnecessarily exercise its power to restrict those rights and liberties of the people.

2. History of the Computer-related Crimes Act 2007

The law of Thailand which aims to determine wrongful acts related to computer systems or computer data, both in terms of using the computer as a tool to commit crime or to commit crimes affecting computer systems or computer itself, is one of six laws[6] to be drafted and enforced in Thailand under the Project to Develop Information Technology Laws initiated by the Ministry of Science, Technology, and Environment in 1998. However, at present, only two laws in the program have come into effect, the CCA and the Electronic Transactions Act. 2001.[7] It remains unclear when the other laws in the project will be processed towards enforcement.

The CCA came into force more than six years after the Electronic Transactions Act. It was constructed from four drafts.[8] It should be noted that the original principle and justification of the provisions of this Act, at that time called the "Computer Crime Act", were announced in the Project to Develop Information Technology Laws. "The objective is to determine the criminal procedures to punish offenses against the operation of computer data systems and network systems. At present, there are no legal provisions to determine such offenses so as to guarantee rights and freedoms and protect of social harmony".[9] However, after several amendments to the drafts, when the law was enacted by the Extraordinary Committee of the National

Legislative Assembly (NLA), which was appointed after the 2006 coup d′ état,[10] it was discovered that not only there was no issue regarding guaranteed rights and freedoms in the principles and justification of the law, but also the wording of the offenses regarding the dissemination of content on the internet in Section 14 was vague, and Section 15 stipulates offences and punishment for service providers equal to those committing offences. Besides, service providers are identified in a way that does not correspond with the understanding of those in the field of information technology (Section 3). In particular, Section 20 authorizes the state to restrict the dissemination of information in computer systems as an urgent measure with broad conditions for restricting information, resulting in later problems of interpretation. In more than 3 years of enforcement, there has been constant criticism that the CCA was created for the state to use as a tool to control and block the lawful expression of public opinion.

3. Problems of the CCA with respect to Freedom of Expression

Careful consideration of the situation seriously with regard to rights to access information and to freedom of expression of the Thai people shows that over the past several years, the situation has caused concern. This is because since the middle of the Thaksin government, through the coup government, the Samak-Somchai governments, and the Abhisit government, especially during periods of declared emergency over the conflict in April-May 2010, until the beginning of the government of Prime Minister Yingluck Shinawatra, the mass media, especially

the secondary media such as websites, news boards, and individual or group communication channels of various forms such as telephone, SMS, electronic mail and social networks such as Facebook or Twitter have all been penetrated and controlled by the government sector.

However, it should be understood that content disseminated in public can be monitored and penetrated by the state or the private sector to prevent potential crime in the online world, like police patrols to monitor peace and order in various localities in the real world. But such operations must not violate the rights and freedoms of the people. On the contrary, if what happens is not just patrolling to keep the peace, but turns into threats, interference, deletion, blocking access or controlling expression in any way at all, with no process to prove an offence or hold a trial, such cases must be held to account by the people affected.

"The problem is not with the law itself but with those who enforce the law" is a phrase used by many sides to refer to the problems of the CCA. This "fact" actually applies not only to the CCA but is also the most common problem of law in Thailand. However, this remark overlooks "other problems" of the law, or is said with the intention of avoiding the actual problem in the provisions of the law that need to be improved. This is not correct. If we consider various provisions of the CCA related to the rights and freedom of information and expression in online media, as well as statistics on the use of the CCA and the opinions of state agents and internet entrepreneurs presented in the first part of this research, the true problem of this law is found to be not only with those enforcing the law, but the wording of this law has also created confusion and opened

loopholes making it easy for the state to violate the rights and freedom of the people. For these reasons, this research presents an analysis of the problems of the CCA, apart from the problems of enforcement.

3.1 Definition of terms

Section 4: " 'service provider' shall mean

(1) A person who provides service to the public with respect to access to the Internet or other mutual communication via a computer system, whether on their own behalf, or in the name of, or for the benefit of, another person.

(2) A person who provides services with respect to the storage of computer data for the benefit of the other person."

This definition seems to be the most troublesome for enforcement of the CCA, especially with regard to the issue of the right to information. The term "service provider" was criticized as unclear and the classification does not correspond with the understanding in information technology.[11] It is noteworthy that apart from unclear wordings in the CCA , the details specified in "Ministerial Regulations on Information And Communication Technology with Regard to Criteria for Retention of Computer Traffic Data of Service Providers 2007"[12] have problems in the classification of the service providers which does not correspond with the real definition. For example, Host Service Providers, who provide rental space to store the data of other persons, instead of falling within the category of "Data storage service provider" under (2), is classified as someone who provides a service for the public to access the internet or other communica-

tion via a computer system under (1), etc.

In addition, it is suspicious that the CCA stipulates an obligation and responsibility to the "service provider", even though some telecommunications service providers have not provided services directly associated with offenses under this Act, such as satellite service providers or ATM service providers. The records of the Council of State committee give the reason for this: "Service provider under (1) the Computer-related Crime Act B.E. 2550 includes a person who employs another to develop a program to create access to a computer system, as well as telephone and telecommunications service providers since to investigate an offence, computer traffic data is required from telephone and telecommunications service providers to understand clearly the path of communication...."[13] However, the broad definition of the term "service provider" to include telecommunication service providers and others in this way is in the opinion of the researchers a provision that does not give adequate overall consideration to the law. It can be seen that under the CCA, a "service provider" not only has the obligation to retain computer traffic data, or a log file but also may have liability for the content disseminated by others under Section 15 in combination with Section 14 of the CCA. When Section 15 uses the broad term where "service providers" must be liable, without defining neither the type of service provider nor the level to which the service provider is related to the content under this provision, this could render "all types of service provider" (even though the nature of their operations or their services might not directly concern the expression of content, but only technical services to connect computers or manage systems, etc.) may be held liable with those truly committing an offence because they

are within the definition of "service provider".

This issue of the lack of clarity which covers broad enforcement against service providers of different kinds and is not limited only to the service providers closely related to the "dissemination or expression" online content, has been constantly criticized. But in the past, legislators tended to argue on the basis that in the end, there must be a process to prove the "intention" of the service provider before conviction; therefore, if any service provider does not know about or is not related to the offence, he or she will not be liable. However, the question has been why the state itself and service providers must waste time and money on litigation to prove that the person has not given intentional support or consent, because the nature of the service provider was from the outset unrelated to the material published. In fact, the legislators should be able to draft legislation that determines a clear scope of "service provider". The fact that the law provides a broad coverage will create an atmosphere of fear, resulting in self-censorship among service providers, directly affecting the right to information and freedom of expression of the people. This will also indirectly affect the development of and incentives for information technology services.

3.2 The Basis of Offenses under the CCA which Affect the Right to Information and Freedom of Expression in Online Media

Section 14 prescribes if any person commits any offence of the following acts shall be subject to imprisonment for not more than five years or a fine of not more than one hundred thousand baht or both:

(1) That involves import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to that third party or the public;

(2) That involves import to a computer system of false computer data in a manner that is likely to damage the country's security or cause a public panic;

(3) That involves import to a computer system of any computer data related with an offence against the Kingdom's security under the Criminal Code;

(4) That involves import to a computer system of any computer data of a pornographic nature that is publicly accessible;

(5) That involves the dissemination or forwarding of computer data already known to be computer data under (1) (2) (3) or (4);

1) Section 14 (1): It is interesting that after the CCA came into force, Section 14 (1) has been used by both individuals and officials to prosecute those committing offences in the nature of defamation of others on the internet. Even though the goal of Section 14 (1) does not specify any elements of an offence on this basis, the statistical analysis in the first part of this research shows that most cases charged using Section 14 (1) are defamation cases in which the plaintiff pursues charges regarding defamation using false data on the internet or dissemination of private pictures or stories to cause damage to a person's reputation, dignity or expose them to hatred. This type of case is also the most common under the CCA.[14]

The original intention of Section 14 (1) by the legisla-

tors was to close a gap in criminal law in relation to "counterfeit documents". Previous law, enacted in an era where documents referred to only paper documents or other materials[15], cannot be interpreted to cover false electronic data[16], creating a loophole in the law. Therefore, Section 14 (1) does not mean the import of data (whether true or false) into a computer system containing information that may cause someone to lose their reputation or be disrespected or hated, which constitutes the offence of defamation under the Civil and Commercial Code and the Criminal Code of Thailand. Rather, it means the "import into a computer system of false computer data fabricated by persons without a legal authority to do so". It also means the "import into a computer system of true computer data (authored originally by those with legal authority), but later altered or modified by the offender" which constitutes offence similar to that of "document counterfeiting" in the Criminal Code. This is where those without legal authorization to create a document have fabricated a completely "false document" (whether there was earlier a genuine document or not is not an important matter) or modified a "genuine document" in part so as to change the original meaning or be different from the truth, in order to make others mistakenly believe that the document is a "genuine document[17]" For example, if an individual who is not an official of the state or who may be an official of the state but is not in the agency or does not have the authority to issue passports, has issued a passport for another person, even though the information in the passport is correct in every respect, such as the correct name and address of the passport holder, this passport a "counterfeit passport". Another example is when a person adds to, takes from, or alters the genuine passport of A to make

it B's passport. Both cases constitute an offence of document forging in the Criminal Code. In summary, if Section 14 (1) is to be interpreted in enforcement, it must be interpreted in the same way as offences of forging or falsifying documents only, not of defamation.

With regard to importing into computer systems "false computer data", the correct interpretation should be similar to "document forging" in the Criminal Code for "offences related to documents". In the case where a person with the legal authority to create document (or computer data) distorts the "content" in a document (or data) so that it is at variance with the truth, then even though the document or data will be called a "genuine" document or data (not fabricated), such act constitutes an offence because a document or data is produced with "false content", or will be called an offence of making a false (or importing false computer data into a computer system). In summary, it is obvious what this law is intended to cover is "the credibility and security of the document (or data)" used as evidence or reference. Therefore, Section 14 (1) is not intended to protect the reputation and dignity of a person, which is an offence of defamation stipulated in other chapter.

From the real objective of the Section 14 (1) above, it can therefore be said that with the problem of unclear wording, and the lack of sufficient knowledge and understanding of the intention, aim and meaning of this Section by officials, Section 14 (1) has been consistently misunderstood and applied inappropriately. The question still remains why when "false insinuations" occur on the Internet, it is necessary to prosecute under Section 14 (1) of the CCA in combination with civil and criminal law, which creates confusion for the offender and the general

public. In applying Section 14 (1) of the CCA to prosecute cases of defamation, the effect is to turn defamation into a "public offence". Apart from not allowing the parties in a case to reach a compromise, this allows anyone to file a complaint with officials to prosecute a case against anyone (which is not the case with "personal offences"). This creates ridiculous results that are incompatible with the basic provisions governing defamation under criminal law. It may also raise questions regarding the interpretation of the law if someone accused under this Section is able to prove exemption from liability (Section 329[18]) or exemption from punishment (Section 330) as stipulated in the Criminal Code. It can be said that interpreting Section 14 (1) to deal with defamation offences has turned the CCA into a law that makes defamation offence more serious than as stipulated in the Criminal Code, both in terms of longer terms of imprisonment and higher fines. The accused also cannot prove exemption from liability or punishment and the offence is non-compoundable, which may contradict the purpose of the law in this matter.

Also, the confusion in enforcing this provision could stem from where Section 14 (1) is located, because in principle, offences of "forgery" or "falsification" as explained above are not offences of the same kind as offences of "disseminating" information with "illegal" content, since the offences of fabricating false data are offences derived from the "action" (forgery, modification, falsification) which is not the same as disseminating information which is an offence because "the content is illegal per se" (pornography, material defamatory of others, incitement to seditious or terrorism). Therefore, when the intention of (1) is not the same as other subsections but is placed in the same provision, together with the wording in (1)

that says "in a manner that is likely to cause damage to that third party or the public", which can be interpreted broadly with no necessity to have an impact on the "credibility and security of data" only, this creates among enforcers confusion and the possibility of understanding that defamation of reputation and dignity constitutes offence under (1), without realizing that this interpretation makes (1) overlap with the offence of defamation, and creates the bizarre legal results mentioned above.

One case with interesting details under Section 14 (1), is Red Case Or (อ.) 4465/2552. The plaintiff charged Wanchat Padungrat, owner of the Pantip Website, one of the major webboard service providers in Thailand. The plaintiff claimed that someone wrote a message accusing the plaintiff of embezzling from his organization. The message appeared as a document on the free webboard Pantown, one service of Pantip that aims to allow users to create their own webboard. The plaintiff accused the defendant as the owner of the website with the responsibility to control, supervise, manage, monitor and inspect content on the website, who has consented to a false message being uploaded onto the website, and failed to remove from the website the "defamatory" message (which constitutes an important element of the offence of defamation - researchers). The court of first instance acquitted the defendant, since it did not constitute an offence under Section 14 (1). An important witness in this case was a representative of the Juridical Council who testified on the interpretation of Section 14 (1) that the term "forged or false data" cannot apply to an existing document that is placed on a website without any modification. If the plaintiff saw that the content in the document was false, this was a matter for the plaintiff to take up with the person who created the document.

The plaintiff still could not prove whether the information in the document was false or not. The court ruled that the burden of proof rested with the plaintiff, not the defendant.

This case shows that the interpretation of Section 14 (1) by the representative of the Juridical Council leads to the issue of "burden of proof" of the plaintiff who must prove the "authenticity" of the information disseminated. This is the same issue as the proof of "authenticity" of document in the offence of forging or falsifying documents under the Criminal Code, not an issue that concerns "slander" as an offence of defamation because if it were truly about slander, the law would not examine whether the slander is true or false. Therefore normally the plaintiff in a defamation case does not have the burden to prove to the court whether the disseminated information or message is true or false. This shows that even the Juridical Council does not recognize Section 14 (1) of the CCA as applicable to defamation offences.

2) Section 14 (2): It can be said that Section 14 (2) is the most problematic in relation to the scope of enforcement and is criticized for being used as a tool of the government to deprive the people of freedom of expression. This research suggests that the terms in this subsection of "damage to the country's security", or "cause a public panic" are contrary to "the principle of legality"[19] in criminal law (no offence, no punishment without law) in that "the law must be enacted clearly" (nullum crimen sine lege certa)[20]. This is because the general public, after reading such terms, cannot immediately understand which information has content that will be considered a threat to the national security or to what extent it would create a public panic. Section 14 (2) is a provision which opens a way for officials to use full

discretion to determine whether a piece of content constitutes an offence or not. This tends to risk over-interpretation since the meaning is uncertain and may be changed with time or the attitude of the authorities, while this offence carries a penalty of imprisonment for up to five years. The issue of provisions in contradiction to principles of criminal law clearly reflects that the problems of this Act do not depend only on the perspective or attitude of those enforcing the law but also on legislation that is entangled with politics and opens loopholes in the law itself through the choice of terms that are not clearly defined.

It should be noted that Section 14 (3) of the CCA also relates to national security since it specifies penalties for the import into a computer system of any data which is an offence relating to the security of the Kingdom, or an offence related to terrorism under the Criminal Code[21]. But Section 14 (3) is significantly different from Section 14 (2) because the offences in (3) are much clearer with respect to "the elements of the offence" than those in Section 14 (2), due to the connection with offences in the Criminal Code. Criminal law is not interested in whether the data which is imported is false or true as long as the elements of the act constitute an offence which is covered by the offence of 'violating national security'. Section 14 (2) refers only to importing false data. This therefore questions the reason why the CCA must include Section 14 (2) which uses vague language to protect national security in a separate clause, which may finally lead to the Section being used as a political tool.

3) Section 14 (3): Even though Section 14 (3) is a clearer provision than Section 14 (2), since it is connected to the Criminal Code which specifies the elements of the offence

more clearly than thoughtless expressions such as "damage the country's security" or "cause a public panic", but this difference does not mean that using Section 14 (3) in combination with other offences under other Sections in the Chapters on national security and terrorism offences in the Criminal Code would make things clearer to the general public, or allow the public to anticipate whether their acts or expressions of opinion, whether in the general media or online, will be offences against the law. It appears that certain Sections in the Chapters in the Criminal Code relating to the security of the state similarly create problems for the freedom of expression of the people.

Statistics in this report on prosecutions show that most cases filed under Sections 14 (3) and 14 (2) of the CCA, were brought in combination with Section 112 of the Criminal Code or the offence of defaming, insulting or threatening the King, the Queen or the Heir-apparent[22] (40 cases). In the past two years, Section 112 has also been under constant criticism for violating the democratic system of government. The problems of the content of the provision itself, its enforcement and the principles of its interpretation can be summarized into four points.

Section 112 is very "subjective" in nature. Normally, the person to consider if an expression or action against her/him is insulting or defamatory should that person. It should not be judged by someone else who was not insulted or defamed (similar to the nature of Section 326[23]) Therefore, the person with the authority to sue or to file a complaint to authorize the state to proceed against the offender should be the person who was insulted or defamed. In law this is known as a "personal offence". However, Section 112 has the status of a "public offence", with the result that anyone can file a complaint or make

a report to the state authorities to prosecute another person. Because of this, it opens the opportunity rooms for people to persecute each other.

Section 112 sets an unreasonably high penalty – three to 15 years' imprisonment –contradicting the principle of proportionality. The damage caused to the injured party and the punishment given to the offender are not proportional.

Section 112 does not specify exemptions of liability (where no offence is committed even though all the elements of the offence are present) to allow the accused the opportunity to plead that the expression of act was in "good faith" or was merely "criticism" within the framework of a democratic system of government. (This is different from the offence of defamation in Section 326 where Section 329[24] specifies exemptions of liability.)

Section 112 does not specify exemptions of penalty (where the action contains all the elements of the offence and is an offence but the offender is not punished), and denies the opportunity for the offender to prove the "truth" of his imputation. So even though the imputation is true and is of public benefit and does not concern personal matters of the defamed person, the offender must be guilty and receive punishment. (This is different from the offence of defamation in Section 326 where Section 330[25] specifies exemptions of penalty.)[26]

The nature of the Section 112 and its enforcement has directly impacted the freedom of expression of individuals "in good faith", and prevented Thai society from learning the "truth" from criticism of the institution or organization as one component of the democratic system under the constitution.

In conclusion, if one is to speak about the overall prob-

lems of the CCA in regards to its provisions and enforcement and its impact on the freedom the people in online media in many cases, one cannot avoid speaking of the provisions of other laws which are used in conjunction or together with the CCA. However, the findings of this part should not lead to the conclusion that "the existence of the CCA (especially Section 14) does not have a direct impact on freedom of expression in online media and thus requires no amendment." Many times the violations of the freedoms of the people have a tendency to broaden and become harsher because many laws offer opportunities for the state to use its powers and discretion to excess.

4) Section 15: "Any service provider intentionally supporting or consenting to an offence under Section 14 within a computer system under their control shall be subject to the same penalty as that imposed upon a person committing an offence under Section 14."

Section 15 of the CCA has also been constantly criticized since its enactment for its lack of clarity and reasonableness in specifying the liability of service providers who are only "intermediaries" in the dissemination of information in computer systems. The following issues should be considered.

Firstly, Section 15 stipulates the same penalty for service providers as for offenders or principals (here meaning those who produce or post and disseminate messages which may be an offence under Section 14), even though the service providers may not themselves import the offending content into the computer system. However consideration of the nature of service provision finds that if we rely on the general principles of criminal law in explaining this offence, the actions of service providers may fall merely into those of a "supporter"[27], whose penalty is

less severe than that of the principal, such as a service provider who sees a message with content that is clearly defamatory but refrains from taking any action, or allows dissemination to proceed. This specification of the severity of punishment of service providers, apart from indirectly affecting the freedom of expression of the public (service users) because the service providers are made to censor content within their service before they themselves are prosecuted by not doing so (self censorship), also affects the incentives for the internet service provider business and the development of the information technology. Also, in the prosecution of offenses in relation to computer systems in the three years since the CCA came into force, the officials have in practice tended to target service providers first, since identification was easier, while ignoring or making no attempt to bring to justice the offenders (who import data into a computer system). This is not in accordance with the spirit of the law.

Secondly, Thailand lacks clear criteria with regard to "measures to control content by oneself" to control internet content. These are measures that those overseeing information must accept to delete from their service information about which they have been notified, without prior examination of the legal offence by the courts (Notice and Takedown). This means that at present, neither officials of the state nor service providers have clear operating guidelines especially for the following problems..

• Who should have the authority to notify alleged offending content text to the service provider?

• The method of notification.

• The details necessary for notification, such as the offending statement, the section of law that is the basis for saying that a statement transgresses the law, the URL of the statement,

etc.

• Time limit for the service providers to take action on an offending statement after being notified.

• The procedure after notification should be deletion wholly or in part.

Many countries, such as the United States, United Kindom, Japan and Malaysia, have already set such regulations, both in the form of law, such as the Japanese "Act on the Limitation of Liability for Damage of Specified Telecommunications Service Providers 2001" or of Codes of Conduct such as in the United States or United Kindom. The absence of clear rules and guidance in accordance with the law means that some service providers may be prosecuted by state officials, despite their best efforts to delete or remove notified statements, only because this was not soon enough for the officials.

Thirdly, there are reasons to believe that there are those attempting to interpret Section 15 of the CCA with the intention to burden service providers with the duty of monitoring internet content. That is, even without notification from state officials or injured parties, service providers must take on the duty of monitoring and dealing with content within their service by themselves. And if they discover an offence has been committed, service providers must accept liability if they do not take action against information that they have found. The researchers believe that this interpretation is unlikely to be correct. It is inconsistent with the nature and characteristics of information dissemination on internet networks where vast amounts of data are shared rapidly. Therefore, it will of course not be easy to monitor or investigate whether all data imported each minute violates the law or not. However, from a study, the researchers

have found a report of an extraordinary meeting 9/2550 of the Commission (to consider the draft CCA) dated 10 February 2007, containing a discussion by the Commission accepting that Section 15 should not be used to define a general obligation on service providers or intermediaries to monitor content, since this would burden service providers more than appropriate.

5) Section 20: "If an offence under this Act is to disseminate computer data that might have an impact on the Kingdom's security as stipulated in Division 2 type 1 or type 1/1 of the Criminal Code, or that might be contradictory to the peace and concord or good morals of the people, the competent official appointed by the Minister may file a petition together with the evidence to a court with jurisdiction to restrain the dissemination of such computer data.

If the court gives an instruction to restrain the dissemination of computer data according to paragraph one, the relevant competent official shall conduct the restraint either by himself or instruct the Service Provider to restrain the dissemination of such computer data."

Section 20 is an additional provision inserted into the final draft by the Select Committee of the National Assembly before the law came into force in 2007. It was the most problematic regarding enforcement and the most controversial since it is an emergency measures that enables the state to stop dissemination of information to the public immediately without requiring a court verdict whether the data has content that is really illegal or not.

Before the CCA came into force, the researcher (Sawatree Suksri) expressed the opinion that Thailand may

eventually need to have an "emergency" measure of this kind called "post (dissemination) censorship" for certain types of content that is clearly illegal so that it can be used as a tool to suppress crime, as well as to restrain widespread damage that may occur. The laws of many democratic countries specify such measures for types of content that the state does not allow to be publicly disseminated, such as child pornography, violence or inhumane torture and racism.

However, such measures must set out clear conditions and criteria based on basic principles that protect the people's rights to freedom of access to information and to expression. The provisions should therefore have the nature of exemptions or have incontrovertible reasons for the state to use its authority to block content, where there must be written laws specifying what kind of content may be blocked.

However, Section 20 of the CCA moves in the opposite direction. It uses unclear terms to define what categories of content can be blocked. The law is written to give the state the power to block as the main principle, not to exempt, which needs strict and watertight interpretation. It also gives state authorities discretion to block by themselves. Even though Section 20 stipulates the conditions that require prior screening of officials' use of discretion by the court, there have been problems and controversy over the limitations of the court duty in carrying out this responsibility. For example, the court has its main duty of conducting trials and issuing many warrants, which may make it unable to give time to a sufficiently careful examination of website content (which must be done quickly) especially when the data sent to the court to seek approval for order is voluminous[28], as well as the court's perspective and at-

titudes towards the right to freedom of information in computer systems. The statistics compiled in Part 1 show that in the four years after the CCA came into force, the court issued over 100 court orders allowing the authorities to block webpages of over 80,000 URLs.[29] It was also found that court orders were rapidly issued, which led to questions whether, to judge from the time spent, the courts considered the content in full detail. This creates insecurity among the people.

Another problem that may not have been raised for clarification is what the meaning and scope of "restrain dissemination" is under this section. Should the court order restraint of dissemination of an entire website or should it restrain only that part with information that appears to be offensive. From previous cases, even though it can be specified which "content" on the website may be an offence, the whole website was blocked, though most of it was used to disseminate general news which was not offensive, such as the blocking of Prachatai. This violates the people's rights and freedom to access to information and such actions go beyond what is reasonable or what action is needed to prevent damage according to the intention of the law.

3.3 Overview of problems of offences concerning the dissemination content in online media

The most problematic provisions of the CCA in terms of interpretation, yet the most used, are those regarding offences related to dissemination of content. The first objective of this Act was to eliminate loopholes in the law because existing laws could not be interpreted to cover new forms of offences with elements different from other basic offences. For example, the offences

of theft or mischief cannot be easily used for data theft, data interception, or causing damage to data or computer systems. In the same way, the offence of trespass can not be applied to accessing computer systems of others, etc. These offences are entirely new technological issues which old laws cannot cover, while for offences relating to dissemination of content, various existing laws can be applied, in particular the Criminal Code. This is because these actions do not have new characteristics or elements. Merely the "site" used to commit the offence may have changed. The dissemination of pornography, even in a computer network, can use Section 287[30] of the Criminal Code. Similarly, the offence of defamation can apply to Sections 326 and 328. Content violating national security is applicable to Sections 112 or 116. These offences are not included in computer-related crime law in many countries.[31] In most cases, amendments can be made to clarify offences in the Criminal Code or other laws. Today, many parties, whether law enforcement agencies, internet entrepreneurs, and number of service users, agree that the CCA should be a law that regulates only offences truly related to the technology, such as unlawful access to computer systems, distortion of information, data interception, computer fraud, or computer sabotage.

3.4 Conclusion

It cannot be denied that today computers and the internet have become the "new media" with a significant impact on people's thinking and as an area with opportunities for free expression. The potential of this new media combined with its speed and the volume of information in circulation make it ap-

pear that the state or those with political or commercial power in many countries see the internet as both friend and enemy. The internet is likely to be greatly beneficial if the state can use it as an effective instrument of communication with its people. But at the same time, if the state cannot monitor or manage communication and dissemination of information over the internet to be with the framework of what the state wants its people to know, then the new media may become a danger in the eyes of the state. In July 2007, the CCA came into force with the important role of "regulating" internet communication.

The results of the statistical study in Part 1 of the consequence of the CCA reveal the number of 80,000 blocked ULRs is grossly out of proportion to the number of cases in the legal process (with the police, prosecutors and courts), which number only in the hundreds. Apart from raising questions about the speed and capacity of state officials to process cases, this also reflects that the relevant state agencies have chosen to use emergency measures rather than trying to identify for the perpetrator or the source of the offence. At the same time, a number of the cases that have occurred raise questions concerning the validity of the "accusations" and the confusion and overlap with other existing laws. This is likely to affect directly the rights and freedom of information and expression of the people. The research found that these questions and problems do not stem only from enforcement or the attitudes of those enforcing the law, but also the law itself because it uses broad, confusing and overlapping definitions without clear principles. In particular, the term "service provider", which does not correspond to the understanding among business and communication technology circles, has a broad meaning that includes other "telecom-

munication service providers", who may not be related at all to the computer systems or data which is the "material" of the CCA. This may waste the time of both the prosecution and the defendant when it is eventually found that the defendant does not possess the qualifications or characteristics of liability for the offence that has occurred.

The section in particular that specifies the basis for an offence in a vague provision is Section 14, which is within the scope of and related to this research topic. The problem starts from offences under Clause (1) of Section 14 which is in fact the provision governing "forgery" and "falsification", and not offences related to "dissemination" of data containing "illegal information". But this provision is usually applied in conjunction with other clauses, resulting in confusion among those using it with an interpretation as a defamation offence. This leads to many bizarre results. The offences in clause (2), "damage national security" and "cause a public panic" use vague language that opens a path for excessive use of discretion by state authorities. The meanings change with time and attitudes of the authorities. This leads to public "insecurity" because they do not know when they will face criminal prosecution. Clause (2) overlaps with clause (3), which prohibits dissemination of information that violates national security or terrorism as offences. Section 15 of the CCA, meanwhile, has a problem at the level of principle, especially in specifying a severe penalty inappropriate with the nature of the offence, and without recognizing the nature of information on the internet. Service providers, who are not the ones who commit the crime themselves, risk the same penalty as the principal. This creates a climate of fear and a situation of self-censorship. Section 20

especially is the most problematic section in this law, because it empowers the state authorities to block websites under the vaguely-worded condition of being "contradictory to the peace and concord or good morals of the people". This has resulted in a high number of blocked websites which does not correspond to the number of prosecutions to prove on what basis the content that the state has blocked in advance is an offence or even whether it is truly an offence.

Even though the prevention and suppression of crimes related to computers and computer networks is an extremely important issue in the age of information, in countries that claim to be governed by the rule of law and democracy, guarantees of freedom of information and expression and respect for opinions, beliefs, and use of discretion of the people must be of critical importance to the state. The state must try its utmost to seek a balance with the prevention and suppression of such wrongdoings.

4. State Policies Regarding the Freedom of Expression on Online Media

This part of the research will discuss state policies and practices toward online media. Many cases reflect the attitudes of the state authorities and officials at many levels towards the rights to freedom of information and expression. This section is structured in line with the terms of the Ministers of Information and Communication Technology, whose ministry is directly responsible for the enforcement of the CCA, with the goal of facilitating an understanding of policy changes and development according to different time periods and factors that played a role in each minister's approach.

From 18 July 2007, the day the CCA came into force, until the time of writing (2011 under Prime Minister Yingluck Shinawatra's administration), the data and problems on the implementation of the law and state policies which affect the people's right to freedom of information and expression can be divided into 6 time periods following the tenure of the Ministers:

Mr. Sittichai Pookaiyaudom (9 October 2006 – 30 September 2007)

Mr. Kosit Panpiemrat (Acting Minister) (1 October 2007 – 6 February 2008)

Mr. Man Pattanothai (6 February 2008 – 2 December 2008)

Ms. Ranongrak Suwanchawee (20 December 2008 – 6 June 2010)

Mr. Juti Krairiskh (6 June 2010 – 3 July 2011)

Gp.Capt Anudith Nakornthap (9 August 2011 - present)

4.1. State Policies under Minister Sittichai Pookaiyaudom (9 October 2006 – 30 September 2007)

4.1.1 Background

Mr. Sittichai Pookaiyaudom assumed the position of Minister under the administration of Gen. Surayud Chulanont. He has a degree in engineering and was a professor at King Mongkut's Institute of Technology Ladkrabang. During his term, the main objectives of the MICT were the allocation of 3G mobile phone technology concessions and solving the dispute over satellites between Thaicom and the Temasek Group of Singapore. However, his very first achievement as Minister

was putting a Computer-related Crimes Bill onto the agenda of the National Legislative Assembly. Mr. Sittichai explained the reason for this.

"...there is as yet no law that can control crime, prevent hackers and the posting of depraved, obscene texts, defamation and texts offending the institution of monarchy. There will some amendments on the exercise of power and discretion by the authorities but this law will not be allowed either to censor academic information or political expression..."[32]

In late November 2006, after two months in office, the Minister held a press conference focusing on the success in solving problems related to the misuse of the communication technology. The MICT had blocked access to over 3,100 inappropriate websites, and received over 15,000 daily reports on URLs. However, the press conference did not elaborate on the content of the blocked or reported websites or which laws the MICT used to block access because at that time the CCA was not yet in effect.

During this period websites might have been blocked solely by orders from the MICT without seeking court approval, but instead using the authority of the Fifth Announcement issued by the Council for Democratic Reform (CDR) under the Constitutional Monarchy after it carried out the coup d'état on September 19, 2006.[33] However, it should be noted that in the press conference, the MICT did not refer to the Fifth Announcement of the CDR in exercising its authority. This has given rise to criticism in society about which law MICT used to block the people's access to websites.

4.1.2 Camfrog Case

In late December 2006, there was a trend among Thai teenagers to use Camfrog, a webcam application, for sexual entertainment. In response to this, the Permanent Secretary of the Ministry of Culture consulted with Mr. Sittichai for possible action to censor this. This led to the blocking of the application through CAT Telecom Company. Mr. Sittichai spoke about this case.

"...even though the root of the problem is not tackled, I believe it will solve the problem anyway. I would like to apologize those who were affected because Camfrog did not just cause damage, but also brought some benefit to the blind, who could still listen..."[34]

This case also led to the establishment of an ad hoc police agency to suppress computer crimes. The first unit to be established was the Children, Juveniles and Women Division (CWD), which was later renamed as the Anti-Human Trafficking Division (AHTD). During the same period, there was a controversial case where a Buddha statue was used as the logo of a pornographic site. Mr. Sittichai assigned the Permanent Secretary of MICT to coordinate with CAT Telecom Company and internet service providers to close the obscene website immediately. The agencies that played a key role during this time were the Cultural Surveillance Group of the Ministry of Culture and the Buddhism Protection Center of Thailand, who monitored inappropriate websites and reported them to the MICT so that it could block them. By early January 2007, the MICT had already blocked over 15,000 pornographic websites[35] using the authority of the Fifth Announcement of the CDR, since the

CCA had not yet been enacted.

4.1.3 YouTube Case and Pantip.com Ratchadamnern Room Case

The event related to the right to information that sparked widespread public discussion and criticism of Mr. Sittichai's role was the blocking of YouTube around April 2007, when someone published content violating Section 112 of the Criminal Code by offending the institution of the monarchy. Mr. Sittichai explained:

"...initially I attempted to close just the URL because I find the website quite useful in general. But it could not be done so I had to block the whole website. From now I have to see if there are any more similar posts. If not, I might consider lifting the restriction.."[36]

Only a few days after the blocking of YouTube, the MICT decided to close down the Ratchadamnern Room webboard of Pantip.com for the reason that many posts could threaten security. But after the webmaster successfully proved to the MICT that they would examine content thoroughly to prevent any expressions defaming HM the King, Gen. Prem Tinsulanonda, President of the Privy Council, and others, Pantip.com was allowed to continue to operate. After the government reported the problem to the YouTube webmaster in the United States and discussed for the responsibility of service providers, the conclusion was reached that the website agreed to delete problematic content so the MICT would stop blocking access.

These two cases brought about regulations that all internet service providers must monitor and block websites with

anti-royal content. This was regarded as the first time that the MICT referred to the Fifth Announcement of the CDR as the law authorizing it to block websites. There were other aggressive measures like establishing a specific agency to monitor web content, a center to receive reports on inappropriate websites, etc.

4.1.4 PTV Case and the United Front of Democracy against Dictatorship

In late May 2007, there was an anti-government rally by the United Front of Democracy against Dictatorship (UDD). Apart from the mass protest, there were news reports and live online coverage, which were later blocked by the MICT. Mr. Sittichai clarified that it threatened security by inciting people to join the rally. In July 2007, the MICT declared to the cabinet that it had blocked 20 provocative websites and said that the level of human rights violations in restricting online media was considered very small compared with Thaksin Shinawatra's 'war on drugs'.[37]

4.1.5 Conclusion and Analysis

We can see that the policies and practices of MICT under Mr. Sittichai Pookaiyaudom's leadership were quite strict and harsh to the point of endangering the rights to freedom of information and expression of the people which are guaranteed by the Constitution. It was observed that during his tenure, many acts had no legal authority because they occurred before the CCA came into force. The MICT also never gave its reasons or clear references to any law. Eventually in April 2007, a reference was

made to the Fifth Announcement of the CDR. After the UDD's websites were blocked, the CCA came into effect and the Fifth Announcement of the CDR was annulled.[38]

In addition, this period saw the beginning of new agencies specifically tasked to monitor online content, many of which operate and function today.

4.2 State Policies under Acting Minister Kosit Panpiemrat (1 October 2007 – 6 February 2008)

4.2.1 Background

Under Mr. Kosit Panpiemrat, there were no new policies because apart from acting for the resigned Minister, he also held the position of Deputy Prime Minister for economics affairs and the Election of the Members of the House of Representatives was being prepared for 23 December 2007. Therefore, the policies and practices under Mr. Sittichai remained intact, focusing on monitoring online content and blocking access to inappropriate websites, carried out under the cooperation of three agencies, the MICT, the Ministry of Culture and the Royal Thai Police. Most blocked websites were pornographic or defamed the Buddhist religion.[39]

4.2.2 Conclusion and Analysis

The policies and practices on pornographic websites remained the same under the surveillance of the Cultural Surveillance Group of the Ministry of Culture. There were almost no new policies during this period as the election approached.

4.3 State Policies under Minister Man Pattanothai (6 February 2008 – 2 December 2008)

4.3.1 Background

Mr. Man Pattanothai was appointed the Minister under the administrations of Samak Sundaravej and Somchai Wongsawat. With a Law degree, he admitted that he was not knowledgeable about information technology and not prepared to become minister either. For this reason, the MICT and its policies in this period were particularly watched by society. The focus was the drafting of the Act on Organization to Assign Radio Frequency and to Regulate the Broadcasting and Telecommunications Services. Policies toward freedom of online media became more aggressive. More initiatives and agencies were established to monitor websites, possibly as a result of the growing popularity of social networks, on which obscenity and deception were widespread. There was also a large increase in online football betting. During this period, possible amendments to the CCA were mentioned to increase its efficiency in enforcement and monitoring websites that offend the monarchy.

4.3.2 Hack and Crack Project

One month after Mr. Man took his position, the MICT initiated a project called "Hack and Crack" with the goal of eliminating or narrowing the gaps in state monitoring of sites offending the monarchy or defaming the Buddhism. The reason behind this project was that they had come across many foreign websites. In order to censor the data there, there was a need to

form a team of hackers to hack into the website and delete it. Mr. Man spoke about this project:

"Such an action may not be completely legal but we can't help it as it is unacceptable."[40]

Nonetheless, this project was opposed by a number of both legal and computer experts because, apart from the fact that the government should not itself violate the law (at that time, hacking was already criminalized in most countries), the government was criticized for not adequately assessing the capacity of Thai officers and agencies, which was still behind that of Western countries. This project was eventually cancelled.

4.3.3 The Establishment of ICT CORP and the Budget Allocation for Web Access Blocking

In May 2009, the ICT CORP was founded with cooperation between many departments including the Crime Suppression Division, National Intelligence Agency, DSI, etc. Their assignment was to investigate computer crimes and other crimes committed through computers, mostly fraud, defamation, and pornography. Apart from finding the perpetrators, this centre also had the duty to keep a close eye on websites deemed to offend the monarchy. Mr. Man said in an interview "...the Ministry had a unit with only 10 officers called ICT CORP to keep a close eye on over 200 websites 24 hours a day. In the past, more than 200 internet service providers have been quite cooperative and many meetings were held..."[41]

In July 2009, Mr. Man revealed that over 1,200 websites had been identified, among which over 700 contained contents offending the monarchy. The court had already issued orders

to block 416 websites.[42]

Under Mr. Man's tenure, besides establishing this centre, the MICT allocated a budget to purchase equipment from foreign countries to help with its mission to block inappropriate websites, in particular those offending the monarchy. Each piece of equipment cost about 100-500 million baht, about which Mr. Man said "There will be consultations on the purchase of equipment costing 100-500 million baht each to block inappropriate websites including terrorist or pornographic websites"[43]

4.3.4 Amendments to the CCA

Amendments to the CCA were first mentioned in August 2008, especially with respect to provisions that did not reflect the reality of the online society and technological development. The requirement for internet service providers to keep log files for 90 days created a huge financial burden. However, in the end no one came up with concrete proposals to fix the problem. It was not until October 2009, as the number of lèse majesté websites increased, that a MICT meeting suggested an amendment to enable the authorities to block websites without court orders before they moved to another server. In addition, the National Electronics and Computer Technology Center (NECTEC) proposed purchasing equipment to raise the existing monitoring and censoring system to US Department of Defense standards. In this regard Mr. Man said:

"I am confident that we will not face prosecution from blocking websites defaming the supreme institution because the Ministry of ICT will keep all evidence before blocking. Those who dare prosecute us will automatically reveal themselves as

the webmasters of the websites defaming the supreme institution"

4.3.5 Other Practices

In November 2008, the MICT launched 5 measures to tackle with lèse majesté cases: [44]

1) Service providers immediately block access to websites offending the monarchy.

2) The service providers first identify the perpetrators before blocking.

3) The MICT verifies the perpetrators and reports them to the Royal Thai Police for prosecution. the MICT then seeks cooperation from service providers to submit the list of perpetrators' names for publication.

4) After three warning letters with no response from service providers to delete inappropriate websites, the MICT sends a final request to the Office of National Telecommunications Commission (NTC) to withdraw their license. However, a final decision can be made before three warnings in the most serious cases. The MICT has received good cooperation from NTC.

5) Service providers under TOT Plc and CAT Telecom Plc strictly follow the MICT orders. The surveillance centre must operate 24 hours a day to receive complaints or reports on inappropriate websites from the public.

Apart from the MICT under Mr. Man, the Royal Thai Police, headed by its Director-General, Pol.Gen. Patcharawat Wongsuwan, approved the establishment of a commission to investigate and judge the content on the internet and local radio with the potential to offend the monarchy, and to receive

complaints from people and other agencies for processing to agencies that can initiate legal proceedings.

4.3.6 Conclusion and Analysis

Towards the last months of Mr. Man's term, the People's Alliance for Democracy held a mass rally and the Constitutional Court ordered the dissolution of the People's Power Party. This created an unstable political situation and made it hard to continue with normal administration. However, it can be seen that the policies and practices of the MICT under Mr. Man and the attitudes of other agencies tended to become more aggressive, as seen from the huge budget allocation. Even though Mr. Man was regarded as standing on the opposite side of the political spectrum to the two former Ministers, Mr. Sittichai and Mr. Kosit, policies and practices followed the same direction in the sense that they focused on monitoring content and blocking websites, in particular those with content insulting the monarchy. Special units were set up to monitor content on the internet by the MICT, the DSI and the Royal Thai Police.

It should also be observed that during Mr. Man's tenure, despite the fact that the CCA was already in effect, the MICT opted for supportive measures or cooperation from internet service providers to block websites as soon as they see them, instead of reporting them to the appropriate officials to request court orders. The researchers see that these orders and such use of power contradict the CCA and Section 45 of the Thai constitution, since such matters would directly affect the people's freedom of expression. If the state wishes to limit this freedom, the constitution stipulates that specific laws must be drafted,

not merely resolutions or other enforcement measures. Besides, under Mr. Man's tenure as a minister who is a lawyer himself, there was an attempt to violate the law by initiating the Hack and Crack project to access and damage computer systems in other countries.

4.4 Policies and Practices under Minister Ranongrak Suwanchawee (20 December 2008 – 6 June 2010)

4.4.1 Background

Sub. Lt. Ranongrak became Minister in the administration of Prime Minister Abhisit Vejjajiva. On her first day of the job, she said:

"The first mission to accomplish urgently and consistently is to deal with websites offending the monarchy, which is regarded as the most important."

This means that over and above ongoing issues like the privatization of the Thaicom Satellite concession and 3G technology, the suppression of websites insulting the monarchy or damaging security was the highest priority for Ms. Ranongrak. In addition to ICT CORP, established since Mr. Man's tenure, Ms.Ranongrak created another agency, called the Internet Security Operation Centre (ISOC), to enhance the state's ability to monitor web content. Furthermore, during her tenure, the two red shirts demonstrations, between March and April 2009 and between April and May 2010, paved the way for the declaration of the Emergency Decree on Public Administration in Emergency Situations B.E. 2548 (2005). The government also created the Centre for the Resolution of the Emergency Situation

(CRES), which, besides controlling the emergency situation, also played a role in controlling the public media.

4.4.2 Internet Security Operation Centre (ISOC)

On 29 January 2009, Prime Minister Abhisit Vejjajiva issued a Prime Minister's Office Order 34/2552 to appoint a Steering Committee to set Policy on the Prevention and Suppression of Illegal and/or Inappropriate Information on Information and Communication Technology Systems under. Minister Ranongrak as chair. After the first Committee meeting, the ISOC,[45] later restructured as the Cyber Security Operation Centre (CSOC) under Gp. Capt. Anudith Nakornthap's tenure as Minister,[46] was established with a budget of 80 million baht to coordinate with the military and police. The centre's main duty was to guard against the threat of inappropriate content on the internet and to cooperate with and support operations related to the policy on prosecuting lèse majesté offenders under the CCA. The ISOC announced the following achievements throughout Ms. Ranongrak's tenure:

1) 4 February 2009 access to 4,818 URLs blocked, of which 4,683 are lèse majesté, 98 are pornography and 37 are false advertising.[47]

2) 24 April 2009 access to 8,955 URLs blocked, of which 6,218 affect security, 2,307 are pornography and 430 are gambling.[48]

3) 24 July 2009 16,944 URLs blocked, of which 11,000 affect security, 5,872 are pornography and 72 are gambling.[49]

4) 15 September 2009 19,124 URLs blocked, of which 10,578 affect security, 8,474 are pornography and 72 are gam-

bling.[50]

After October 2009, there were no more formal announcements from ISOC but in an interview given in May 2010, Pol. Col. Suchart Wongananchai, Inspector-General of MICT, reported that ISOC had blocked access to approximately 50,000 URLs but gave no details on the categories of content.

4.4.3 Opinions on the Red Shirt Demonstrations during March-April 2009 and April-May 2010

As mentioned above, two major political rallies occurred during Ms. Ranongrak's tenure. As an example of an important event related to control of public media, in April 2009, the government interrupted the satellite feed that was broadcasting a speech by former Prime Minister Pol. Lt. Col. Thaksin Shinawatra, without consulting the NTC for legal authority. Ms. Ranongrak said on this regard: "...We have to see which laws we can use. If the broadcast threatens security or creates divisions, we might use the law to control it. If we want to see if DTV were wrong, we have to look if the broadcast content is related to national security or whether the content causes divisions..."

After the crackdown on 10 April 2009, Ms. Ranongrak expressed her views on blocking inappropriate and harmful websites:

"For those who run new websites disseminating content, images or text in a manner that incites unrest or chaos, or websites that defame people or institutions affecting national security, the MICT will enforce law seriously and strictly..."[51]

Prior to the declaration of the Emergency Situation at the April-May 2010 demonstrations, the government set up

the Centre for Administration of Peace and Order (CAPO) to give orders to the MICT to block provocative websites without going through the courts.[52] Once the Emergency Situation was declared, the Centre for the Resolution of the Emergency Situation (CRES) was then established as an agency under the direct authority of the Emergency Decree on Public Administration in Emergency Situations B.E. 2548 (2005) to restrict access to all kinds of media and information including online media. CAPO and CRES announced that the following numbers of blocked websites:

1) 9 April 2010: 350 URLs
2) 30 April 2010: 420 URLs
3) 8 May 2010: 612 URLs
4) 17 May 2010: 770 URLs

4.4.4 Numerous State Agencies Set up to Monitor and Block Websites

In September 2010, a seminar was held on "Integrated Measures to Monitor and Block Inappropriate and Illegal Websites" to reflect on the problems of state operations to monitor and block access to inappropriate websites, by either the MICT, the DSI or the NTC. The main problem lay with bad coordination between the agencies. In other words, data on blocking websites from the MICT was not forwarded to other agencies resulting in a lack of integrated control of online content. For example, if the NTC did not receive reports on MICT blocks, it could not punish the operators with suspension, withdrawal or refusal to extend their license. Ms. Ranongrak said regarding this issue:

"The Ministry of ICT alone cannot succeed. We need

close cooperation from many agencies especially with inappropriate websites that are quickly spreading in the internet world, including websites that damage the country's security, in terms of either nation, religion or the king. Therefore, everyone must help."[53]

As a result of the seminar, many security institutions, especially from the military side, realized the inefficiency in suppressing websites containing inappropriate content, security-related content or lèse majesté content. On 25 September 2009, Gen. Prawit Wongsuwan, Minister of Defense, said at a meeting of the Defense Council that he would assign the ISOC and the army to coordinate with MICT in eliminating lèse majesté websites, while a police unit with this specific responsibility was the Office of Information and Communication Technology, Royal Thai Police. Consequently, during the tenure of Ms. Ranongrak, many agencies from the MICT, the army and the police started to help monitor and censor online media.

4.4.5 Sniffer Project against Intellectual Property Rights Violation

During Ms. Ranongrak's tenure, apart from activities to monitor web content in violation of the Criminal Code and the CCA, many countries in the western hemisphere were at that time giving great importance to preventing violations of intellectual property on the internet through the use of file-sharing programmes. In order to show awareness regarding this problem, the Working Group on Illegal Internet Content Suppression under the MICT proposed that Thailand should install a systematic method of intercepting data on computer

systems or sniffer programme to prevent intellectual property violations.[54] It claimed that the United States used this tool and all telecommunication service providers also used it regularly so Thai internet service providers should have it too in order to analyze everyone's data traffic on the system to identify users and sources of pirated products. The committee claimed that this kind of monitoring and prevention measure would tackle the root of the problem, instead of only using the CCA to deal with crimes already committed.

However, in response to this policy, many internet users have expressed their objection because they perceived the policy as allowing violation of people's privacy beyond reasonable cause. This is because the sniffer tool can filter computer traffic data or log files, and the content of that data. The increased cost for operators may also be passed on to the consumers who would have to pay higher service fees. Also, misuse of the intercepted data would also result in negative implications for internet users such as the sale of personal information to business entrepreneurs to monitor behaviour and send spam advertisements. The state might even take the opportunity to use such information to monitor people's behaviour and opinions, especially on political issue, as proven to have happened in some foreign countries. And from the facts gathered, it appears that the sniffer policy in Thailand aims not only to prevent violations of intellectual property, but also to scrutinize information affecting national security, and monitor internet users' behaviour in general.

According to Mr. Ajin Jirachiefpattana, Director of the Information and Communication Technology Promotion Agency, who was the driving force behind this project:

"For the people that oppose this, we have to ask them

what they are opposing. In this case, the government wants to create peace in the online society and protect youth from threats from the internet. Its action can be compared to that of immigration officers, whereby the travellers must sacrifice some of their privacy for the sake of society. And on the internet, this job is done by the state..."[55]

4.4.6 Conclusion and Analysis

The policies and practices of Ms. Ranongrak were clear from the first day she assumed office, focusing on the eradication of inappropriate websites. Due to the political demonstrations, the number of blocked websites was much higher than in previous periods. Most of these websites contained political or "inappropriate" contents. In many cases, where there was no prosecution of the webmasters, the reason was never made public, especially in the case of websites owned or operated by red shirts, who had different opinions from the government or criticized the government. The inability of the state to define clearly the word "security" in the CCA led to a wave of criticism of the violation of the people's right to information. However, we need to bear in mind that under the declaration of emergency, the Emergency Decree on Public Administration in Emergency Situations 2005 accelerated the process of blocking websites because court orders are obligatory only under the Section 20 of the CCA.

The direction of state policies and practices affecting the rights to freedom of information and expression in online media, only tended to get stricter with significant budget and personnel allocated from many agencies in the MICT, the police, the DSI

and the military to monitor and scrutinize online content and pry into internet users' behaviour and ideas. Even though many cases threatened unreasonable violations of people's rights and liberties, no facts were found to show that state agencies recognized or gave importance to this issue. The main reasons cited by the state for blocking websites, setting up special agencies and pouring in budget were threats to security and lèse majesté.

4.5 Policies and Practices under Minister Juti Krairiksh (6 June 2010 – 9 August 2011)

4.5.1. Background

Mr. Juti Krairiksh succeeded Ms. Ranongrak Suwanchawee, who was forced to resign from the cabinet. It should be noted that while Ms. Ranongrak was in office, Mr. Juti, as a Member of Parliament, had asked in front of the President of the House of Representatives on how the MICT managed lèse majesté websites and what kind of indicators it used to evaluate its success. This could very well reflect the stance Mr. Juti took on this issue. This was confirmed once he took office and held a press conference stating that he was assigned by the Prime Minister to take care of four issues: 1) transparency; 2) support for e-banking initiatives; 3) regulation websites with security- and monarchy-related content; and 4) the Thaicom Satellite concession. He also said that he would form a youth volunteer group called "Cyber Scouts" to enhance monitoring and blocking operations.[56]

Within only a week of taking office, Mr. Juti proved his ability by closing over 246 football betting URLs and within

two weeks, he blocked more than 43,000 URLs that may have fallen within the scope of lèse majesté.[57] This number was almost double that of the entire tenure of Ms. Ranongrak. A Memorandum of Understandiing (MOU) was also agreed between three ministries, ICT, Justice and Culture, to suppress information technology crimes.[58]

4.5.2 Project to Create Cyber Scouts

The Cyber Scout Project was under the responsibility of the MICT but took as its model the Thai Scout Curriculum Development Plan of the Ministry of Education. From an initial 200 volunteers, they planned to recruit 100,000 volunteers by the end of 2010 from school and university students, teachers, professors, and representatives from the state and private sectors with computer and internet skills to attend workshops on ethics, techniques and laws from experts. These young people were expected to act as a network to monitor offenses, inappropriate content and threats to the monarchy and national security. Prime Minister Abhisit Vejjajiva said of this project:

"...this Cyber Scout project is considered an important first step and the start of an online community that follows an ethical and moral code of conduct and acts as a role model for social networks to promote a proper use of the internet by helping each other monitor threats and information harmful to the monarchy..."

At the same event, Mr. Juti said: "In order to express gratitude and loyalty towards the King, the Ministry has initiated the Cyber Scout project to recruit volunteers, who possess ethics and morals, to act as a social network to promote the safe

use of the internet. These Cyber Scouts have the duty to keep watch on any data or behaviour which is a threat to the country from information technology..."[59]

It can be seen that this project was meant not only to create immunity and awareness of online information consumption among children, youth and the general public, but also to fill the gap in the practice of state officials, who were unable to prevent and suppress all websites with content affecting security, particularly those that the state sees as constituting lèse majesté. This objective was reflected in the words of both Mr. Abhisit and Mr. Juti, who needed to have agencies from the people's sector, including children and youth, to help investigate and check content, as well as coordinate with the state sector in suppressing the targeted websites.

4.5.3 The Memorandum of Understanding (MOU) between the Ministry of Information and Communication Technology, Ministry of Justice and Ministry of Culture

On 17 June 2010, the MICT, under the leadership of Mr. Juti, signed a MOU with the Ministry of Justice, under Mr. Peeraphan Saleeratwipak, and the Ministry of Culture, under Mr. Nipit Intarasombat, to prevent and suppress information technology offences. Apart from cooperation in maintaining the security of state data systems, another important duty is to expedite suppression of the illegal business or activities and examine all inappropriate websites with an operational budget from the year 2010 of 127 million baht. Mr. Peeraphan Saleeratwipak, the Minister of Justice, said:

"Within 3 months, we will urgently seek cooperation

from state agencies providing internet services to block inappropriate websites, especially lèse majesté websites, which must be blocked through all channels so that they would not occur. Then we will seek cooperation from private internet service providers."

Apart from appointing officers to carry out this specific task, the MOU encouraged recruiting volunteers to help filter and collect basic information relating to offences affecting the main national institutions, pornography, online gambling, drugs, food, medicine, etc., and send it to MICT.

4.5.4 Regulation of Election Campaigning on Social Networks

While the United States, various European countries and neighbouring Singapore[60] all allow political parties and politicians to use information technology or social networks like Facebook or Twitter as election campaign tools and to communicate their policies to the public, in Thailand this is strictly controlled and regulated by the state with content filtered before being publicly disseminated. Before the General Election on 3 July 2011, the MICT and the Election Commission of Thailand (ECT) consulted each other on this matter. Mrs. Jirawan Boonperm, Permanent Secretary of MICT during the tenure of Mr. Juti, expressed her opinion:

"Right now we are in consultation with the ECT to invite webmasters, web hosting services, and internet service providers for a consultation to determine guidelines for filtering information before it goes to the public. For example, comments on websites might be filtered before they are published..."[61]

To supervise the use of social networks by political parties or politicians to campaign for votes, the MICT used its various powers under the CCA. Even though election campaigning on social networks cannot ultimately be prohibited by any law, be it the CCA or the Royal Election Decree, the ECT, under advice from MICT, handed a policy to candidates and their parties: "It is prohibited to campaign for votes through electronic media after 18.00 on the day before the election." A technical team was assigned to monitor any violations.[62]

4.5.5 The Computer-related Crime Bill

Mr. Juti's last piece of work before leaving office, which was criticized in IT circles and where the MICT was most strongly opposed, was the hurried attempt to push through the Computer-related Crime Bill, which would replace the CCA of 2007, without sufficiently broad people's participatiom[63] despite the fact that the new draft contained provisions that prescribed new offences and many additional new agencies, which would directly affect the people's right to freedom of information and expression. For example, the responsibility of system administrators for content was increased by making the mere copying of others' data an offence. A Commission for the Prevention and Suppression of Computer Crimes was to be created with broad powers, but with a large proportion of commissioners from the state sector and security agencies.[64] However, due to many factors, the presentation of the draft law for consideration of the Cabinet was postponed.[65]

4.5.6 Conclusion and Analysis

It can be said that state policies on online media freedom under the tenure of Mr. Juti Krairiksh as the Minister of ICT did not change at all from those of previous Ministers, especially the emphasis on operations to block both illegal and merely inappropriate websites. It is worth observing that, even though during the time Mr. Juti held office the problem of political conflict became less intense and the general election was approaching, shortly after taking office the number of blocked websites exceeded that during the tenure of Ms. Ranongrak. What is worse, most websites had content seen by the state as constituting lèse majesté. However, the fact is that the number of cases brought to court was less than the number of blocked websites.[66] This phenomenon may be interpreted in many ways. In one way, it could be a matter of limitations concerning offences on the internet, making it difficult to find offenders. But in another way, it could mean that the state is comfortable in choosing to use immediate blocking measures, rather than trying to find the owner of the content that the state sees as an offence. Whatever the reason, this has raised questions among the people as to under what law the content of the blocked websites constitutes an offence, or even whether it constitutes an offence.

During Mr. Juti's tenure, apart from a huge budget and a large number of personnel monitoring and blocking various kinds of data in online media, there was also a clear and formal search for cooperation from other state agencies (the MOU among three ministries) and from the people's sector (Cyber Scouts) to close operational gaps or reduce the burden of state officials. Although the MICT tried to encourage people to think

that the cooperation and various projects were brought about to provide information and recommendations for self-protection in using online media and to guard against data with all forms of illegal content, the statements and expressed opinions of both Mr. Juti and Prime Minister Abhisit Vejjajiva suggest that the state at that time emphasized the blocking and suppression of data with content that constituted lèse majesté or affected security. This raises questions in society because until now, the state itself has not been able to define or specify the characteristics of content that conflicts with security or defames the monarchy. Is mere general criticism held to be insulting or defamation? This is still an ideologically divisive issue in society as well as in its legal interpretation. Therefore, is it appropriate to bring in children and youth with the duty of scrutinizing and reporting for the state to proceed with blocking websites with such content amidst political conflict between the government and people with dissenting views?

Apart from a policy of stricter enforcement of the current CCA, there was also during the tenure of Mr. Juti the concept of amending the Act to increase the number of people responsible for content, to increase the powers of state officials or to increase the number of mechanisms to suppress offences related to the dissemination of data in computer networks.

4.6 Policies and Practices under Minister Gp. Capt. Anudith Nakornthap (9 August 2011 - Present)

4.6.1 Background

Group Captain Anudith Nakornthap, of the Pheu Thai

Party, took office as the Minister of Information and Communication Technology under the administration of Ms. Yingluck Shinawatra on 9 August 2011. He formerly served as secretary to the Minister of Defence and advisor to the Minister of Agriculture and Agricultural Cooperatives. He may be the first Minister to use social networks such as Facebook and Twitter.

Apart from the ongoing tasks that Gp. Capt. Anudith had to clear up, i.e. the problem of satellite orbit maintenance, telecommunications contracts, the auction of 3G networks etc., monitoring and blocking websites with content that constitutes lèse majesté was also an urgent matter for this government.

4.6.2 Continued Urgent Suppression of Lèse Majesté Websites

Gp. Capt. Anudith announced the operational policies of the MICT when he assumed office:

"From now on, civil servants and ministry officials at all levels will be urged to be even more strict in controlling and suppressing offences under the Computer-related Crime Act and lèse majesté on websites by resolutely enforcing the law ..."[67]

Apart from a policy of resolutely blocking websites, there was also an idea of pulling in computer game shop owners to take on the duty of watching out for illegal content. In one interview Gp. Capt. Anudith said:

"This government will be strict in closing down or blocking lèse majesté websites. This government will certainly do no less but I do not wish to give any information because covering up is the equivalent of shooting and makes people interested in looking that. Previously, I have called the relevant executives in

the ministry for consultation. We will brush off the Games Shop Project and coordinate with games shop proprietors to help us be our ears and eyes."[68]

After only a few months of this government, it appears that the MICT sought cooperation from Facebook headquarters to block over 10,000 URLs of lèse majesté pages[69]. There was also a warning from the MICT about using Facebook, that anyone finding posts or content that constitutes lèse majesté should not click on the 'Share' or 'Like' buttons or comment on the post because they may have to accept responsibility under the CCA,[70] since the MICT regards it as indirect dissemination of content. This warning provoked much criticism among both legal and IT circles as an interpretation that exceeds the provisions and conflicts with the principles of criminal law.

4.6.3 Opinions on the CCA

"This is not up-to-date because it was enacted in 2007, so the parts that have loopholes or the parts that are out-of-date must be improved. The ministry is working on it and will propose amendments to the Cabinet." Gp. Capt. Anudith.

Although Gp. Capt. Anudith insisted that enforcement of the CCA would follow a single standard, and thought that blocking websites could not solve the problem of dissemination of illegal content because it would be never ending, in the opinion of Gp. Capt. Anudith, the MICT must operate strictly and resolutely with respect to lèse majesté websites, and consider blocking as a matter of urgency, unlike the dissemination of other forms of data where there was time to give case-by-case consideration whether there was an offence or not. Moreover,

the current ICT Minister also expressed the opinion that websites blocked by the court order (Section 20 of the CCA) should be different from those blocked under the Emergency Decree on Public Administration in Emergency Situations B.E. 2548 (2005).

"...among all the cooperating integrated agencies, we agree that the suppression is not the solution to the problem because we cannot suppress all... We have priorities. If it is a matter of lèse majesté websites, the process must be strict, firm and decisive, but if it is a matter of other issues, we must look if an offence has actually occurred not.... For some news websites that have been blocked by the Act (probably means the Emergency Decree – Researchers) when the Act is lifted and they have no court order to block them, they have the right to request to be un-blocked.... because the websites blocked at that time came from the expression of politically different opinions. This is different from lèse majesté websites which will be blocked by court order and cannot be un-blocked by any means..."[71]

It can be seen that Gp. Capt. Anudith's view on this matter may be questioned whether it is right and just or whether the MICT really had a policy and operational approach according to what Gp. Capt. Anudith said, because with regard to being correct, it does not matter what kind of content constitutes an offence, the state should give careful and equal consideration before blocking it.

However, Gp. Capt. Anudith has not yet addressed other problems related to the CCA, in terms of its content, ambiguous and unclear wording, and problems of interpretation. He also never addressed the draft Computer-related Crime Bill, which

under the tenure of Mr. Juti, the MICT tried to push for consideration of the Abhisit Vejjajiva Cabinet around March 2011.

4.6.4 Other Policies Related to the People's Right to Information

This might be considered the first time that the MICT has concrete policies of trying to provide more comprehensive internet access for the Thai people, whether a policy of free wifi, giving internet access equipment to students, or creating linkages with the National Information Data Center.

Although these policies were debated on issues of appropriate budgets and age of students, difficulty of implementation, and effectiveness in achieving the objective of increasing access to infornation, they may serve to show that the MICT, which gave them importance and thought up policies in support of the people's right to information, was not aiming simply to block or control information. Gp. Capt. Anudith has said:

"On free wifi, we must be clear. Today we can say that we will definitely provide at least 20,000 hotspots before the end of the year. The models are ready. We only need to decide which model is the easiest one because each operator already has their own areas of coverage. We will use the USO funds of the NBTC or the government budget. This expansion will help stimulate both content-related industry and all forms of entertainment. Application developers will also be supported to assist the state's service to the public.."[72]

4.6.5 Conclusion and Analysis

Even though Gp. Capt. Anudith became Minister of ICT in a government under PM Yingluck Shinawatra that came from a democratic election and there have been no violent political conflicts during his term, which should have led to fewer policies restricting freedom of expression in online media than in previous times, it appears that the MICT continues to block websites. Apart from relying on the powers under Section 20 of the CCA and court orders enforced on internet service providers in Thailand, the MICT still requests for cooperation from internet service providers overseas to block certain content.

Gp. Capt. Anudith is an ICT Minister who uses internet services and monitors their role and importance, especially online social networks (unlike the tenure of Mr. Juti Krairiksh), which have become popular and are rapidly spreading among Thai users to the point where they will have a broad influence on users' behaviour and thoughts. It seems that the space for expressing opinions of various kinds in online social networks, be it Facebook, Google+ or Twitter has become a target that the MICT under Gp. Capt. Anudith sees as important to scrutinize, monitor and block. The attempt by the MICT to cut off freedom of expression on social networks that received heavy criticism was the prohibition on Facebook against expressing their opinion or clicking 'Like' on comments deemed by the state as constituting lèse majesté merely on the grounds that it was thought to be indirect dissemination of content and hence an offence under the CCA.

However, the researchers believe that this explanation for the prohibition against expressing opinions and clicking 'Like' is

incomplete and inherently problematic. The state can be seen as trying to use the law and criminal penalties to create a climate of fear among online social network users by reducing the essence of the problem that in principle, to commit an offence carrying criminal penalties, the perpetrator must act with "intent". If intent is lacking, it may not be considered an offence. The prior assumption of belief that the offender has the "intent" to commit an offence cannot occur in criminal law. For this issue, cases which are offences are those where the perpetrator knows that the content breaks the law and yet intends to disseminate it. The question is, how can the expression of opinion or approval of something written in online social media, done in an ordinary way, be automatically considered in every case to have the "intent" to disseminate illegal content directly or indirectly.

Certain facts should be taken into consideration in analyzing implementation of policy under Gp. Capt. Anudith, especially on blocking websites. Some opposition politicians (Democrats) tried to call for and put pressure on the MICT to take decisive measures against websites or social networks or even websites with video files like YouTube that have lèse majesté content, otherwise the government would be thought to be disloyal or supportive of people who defame the institution.[73] This demand or accusation might be one factor that has prevented the current MICT from implementing its policy on the dissemination of possible lèse majesté content in ways other than ever more strict and precipitate blocking. This research is not able to analyze the entire policy approach of the MICT under Gp. Capt. Anudith Nakornthap because the time period for this research does not cover until the end of his term.

4.7 Conclusion

All policies and practices of the Thai state elaborated above are just one element that reflects the attitude of individuals in the state sector towards the people's right to freedom of information and expression. It can be said that the monitoring of online media content and blocking of access to this content, especially content breaching state security, content constituting a lèse majesté offence, or even content critical of the monarchy which the state generally believes constitutes lèse majesté, are the main tasks of every government, and it is not important what political situation befalls the nation. The main legal provisions used to implement this are Sections 14, 15 and 20 of the CCA in normal situations, and the Emergency Decree on Public Administration in Emergency Situation (together with the Internal Security Act and Martial Law in the three southern border provinces) when the government declares an emergency. At present, aside from monitoring the behaviour and expression of opinion of people on news sites, webboards and general internet services, the state also monitors communities in online social networks, and even tries to inspect private areas like email and other channels through the Sniffer tool.

It should be acknowledged that, measures by the state to block access to online media were in use since before the enactment of the CCA on 18 July 2007. In many cases, the state acted without any legal authority to act.[74] In some cases, the method of 'seeking cooperation' from individual service providers resulted in users periodically being unable to access the websites they needed. This raised suspicions in the people's sector about whether there were technical problems or whether

the websites were blocked. It may be said that the Fifth Announcement of the Council for Democratic Reform (CDR) issued after 19 September 2006 coup d'état was the first order clearly authorizing the MICT to use its discretion to block every kind of media, regardless of whether the country was in an emergency situation or not, if the MICT considered that the information or content "might affect the democratic reform under a Constitutional Monarchy." Even though the Announcement was in use for only a short period of time before the enactment of the CCA, the MICT, under the administration of then ICT Minister Sittichai Pookaiyaudom, used its authority under this Fifth Announcement of the CDR to block almost 20,000 websites by its own admission. However, the researchers believe that the use of authority under this Announcement to restrict the people's freedom of information and expression, apart from problems of unclear wording like "affect democratic reform", resulted in granting excessively broad discretion to state agencies. It may also be thought that the state exploited this Announcement to seize the opportunity to define four additional "new reasons" for excluding to the rights and freedoms of the people as stipulated in the 1997 constitution.

In terms of blocked content, under the powers of no matter which law, it is found that for many blocked websites, the state could not explain clearly under which law and sections the content was an offence, or even whether it truly constituted an offence, because after the blocking, there was no trial for judgement by a court, while the people could not scrutinize the authority of the state because they could not see the content. Many doubts that arose among internet users thus have not received answers. Did the blocked content truly violate national

security or stability, or was it merely political opinion that might impact the stability of the government or ruling class? Was the content really strong enough to defame, insult and threaten the monarchy, or merely well-intentioned criticism which is permitted under the rule of law and the democratic system?

In conclusion, considering web blocking statistics, the prosecutions of internet service providers and users, the problem of unclear wording of the CCA as well as problems of interpretation and the policies and attitudes of those who enforce the law, it should not be very surprising why in 2011, Freedom House[75] listed Thailand among the group of countries that are "Not Free" in the "Freedom on the Net" report, along with China and Myanmar.[76]

5. Reactions and Responses among People's Movements and Civil Society Sector toward State's Laws and Policies of the State Affecting Online Media Freedom

5.1 Reactions to the CCA

5.1.1 Reactions to the CCA

After the 19 September 2006 coup, the government of Prime Minister Gen. Surayud Chulanont appointed a National Legislative Assembly (NLA) with the duty of considering legislation. The Computer-related Crime Bill was tabled for deliberation by the NLA as an urgent motion on 15 November 2006. The NGO Freedom Against Censorship Thailand (FACT) was the first to propose to NLA 1) that Thailand should not pass this Bill as an urgent matter; 2) that there are many offences

in the Bill, to which already existing laws could be amended to apply; and 3) that the government should avoid excessive control over the internet. It also called for any law to be clear and unambiguous and not allow for state officials too much discretion in interpretation since it might open a way for using the law as a tool to suppress political opinion and silence dissent.

In terms of law enforcement, FACT proposed 1) that the government should ensure accountability and transparency in searches and seizures of any computer equipment; 2) that at least one state official have full responsibility; and 3) that individual internet traffic data must be treated as private property which is not to be subjected to seizure or storage by the state or service providers without a court warrant, since the guarantee that all data concerning internet usage is purely private information is one reason why computer users pay monthly internet fees to service providers. FACT expressed serious objection to the fact that the Computer-related Crime Bill proposed that some offences carry the death penalty and life imprisonment.[77]

5.1.2 Reactions to CCA

After the CCA was promulgated on 18 July 2007, civil society both approved and disapproved of the law, supported by different reasons. Those who approvaled believed that the CCA gives greater protection to privacy rights since it criminalizes unauthorized access or penetration of a computer system and changes to or addition of information in other people's computer system without the consent of the owner, which are not covered by other existing laws.[78] The disapproving side was concerned about the effect on freedom of expression and other freedoms as

a result of the interpretation of the law by state officials, since the wording in the law on many points is ambiguous and unclear such as the prohibition against sending obscene or doctored images which harm other people's reputation. In particular, Section 14, which has broad provisions including the prohibition against dissemination of information which affects national security, does not have clear definitions, making its interpretation subject to the discretion and attitudes of the authorities and the volatile political situation. This opens a way for the CCA to be used improperly or for political defamation.[79] In addition, the heavy penalties on service providers under Section 15 will have an impact on technological development and the telecommunications service industry.[80]

At the same time, the law enforcement agency, through Pol. Col. Siripohng Timula, Superintendent of the High-Tech Crime Center (HTCC), expressed the opinion that though Thailand now has a law specifying the basis for computer-related offences, he did not expect computer-related offences to decrease compared to the period before the law came into force, because of rapid technological progress and external factors such as the economic crunch. Therefore, the people should first learn to protect themselves from committing offences, and the state must expedite giving the people information about the law.[81]

5.1.3 Reactions to the Enforcement and Prosecution of Offenders under the CCA

Interestingly, the CCA has so far often been applied to a very few kinds of criminal offences. The Sections that are used the most are 14 and 15 which concern offences in the

dissemination of online information prohibited by the law and the liability of service providers. As said above, issues that have constantly raised questions and concerns in civil society are the unclear wording and elements of offences of these Sections, which gives an opportunites for officials to use their discretion with a broad interpretations. Many prosecutions have thus led to frequent protests by people and civil society, for example, a statement on Mr. Nat Sattayapornphisut case.[82] During 13-15 October 2009, three alleged offenders were arrested, Dr. Thatsaporn Rattanawongsa, Mr. Katha Pajariyapong, and Miss Theeranun Wipuchanin, over the dissemination of news on the Stock Exchange of Thailand which caused panic among many investors and a selling spree.[83] Many people's groups were opposed to the arrest including the Thai Netizen Network which issued the statement demanding clarification in cases using the CCA to arrest internet users in October 2009[84]; Fah Diew Kan webboard community also issued a statement condemning the arrest of scapegoats in the dumping of shares;[85] the Social Move Assembly opposed the use of this law as a threat to freedom of expression and information concerning the dumping of shares in October 2009 and called on freedom lovers to protest against the CCA.[86] Even DJs on a taxi community radio station criticized the CCA as a law that inflicts structural violence against people's freedoms and political rights and runs counter to democratic development.[87]

Apart from the prosecutions against online media under Section 14 and other sub-sections of the CCA, prosecutions against service providers under Section 15 were also closely watched, particularly the case against Ms. Chiranuch Premchaiporn, Director of Prachatai news website. (On 30 May 2012, the

court sentenced her to 8 months in prison, suspended, and a fine of 20,000 baht.) The general public, academics and many civil society organizations inside and outside the country questioned the inappropriateness of this Section in terms of both offence and penalty, which affects the mass media and those who have only been doing their duty as intermediaries of online news. There were also protests against the court proceedings. The Human Rights Lawyers Association (HRLA) issued a statement to oppose this unfair prosecution;[88] the Thai Netizen Network issued a statement urging MPs to amend Section 15 of the CCA;[89] Amnesty International Thailand urged the Thai authorities to withdraw all charges against Chiranuch;[90] Reporters without Borders issued a statement calling on the Thai state to withdraw charges against Chiranuch[91]; 11 UK Members of Parliament from three major political parties signed an Early Day Motion proposed by Mr. Tom Watson, a Labour Party MP, to express concerns over Chiranuch's prosecution under the CCA[92]; Reporters for Freedom Club condemned the arrest and demanded immediate withdrawal of the charges and urged media associations and human rights organizations including the Lawyers Council of Thailand not to ignore the case,[93] etc. In addition, public fora have been organized to discuss concerns about the law, including the Ratchadamnoen Sewana no. 17/2551 on "Computer-related Crime Act: Protection or Threat?" organized by the Thai Journalists Association (TJA) and the Issara Institute[94]; and a seminar "Three Years of Enforcement of the Computer-related Crime Act: the rule of law and accountability of the state" organized by the Thai Netizen Network, Campaign for Popular Media Reform (CPMR) and the Southeast Asia Press Alliance.[95]

5.1.4 Recommendations to the Government regarding Amendments and Improvements in enforcement of the CCA

Because of various problems arising from enforcement of the CCA, which involve certain wordings in the law and their interpretation, civic groups and organizations that have been directly and indirectly affected by the law, including law enforcement agencies, have proposed a review of the principle and rationale of the law and even amendments to it. The Thai Netizen Network offered three recommendations during a public discussion on "Laws concerning computer-related crime: international perspectives and guidance"; 1) Officials should attempt to arrest the perpetrators but not the intermediary. 2) An alleged offender should be treated as an innocent person who should enjoy her or his constitutional rights. 3) Regulation of online media must be based on reality.[96] Mr. Prasong Lertrattanawisut, former TJA President, made the observation in the "Three Years of Enforcement of the Computer-related Crime Act: the rule of law and accountability of the state" seminar that Section 20 of the CCA does not authorize the court to close down an entire website, but only stop the dissemination of the information found to be in violation of the law. He then proposed that concerned agencies, including the Office of the Ombudsman and the National Human Rights Commission (NHRC) should be pressured to petition the Constitutional Court for a ruling on the constitutionality of such measures.[97] On 5 October 2011, civil society groups organized a forum on "Summary of the UN Universal Periodic Review (UPR) on Human Rights in Thailand: Experience from Geneva", after the submission of the country report by Thailand to the UN Human Rights Council (UNHRC)

and the issues of human rights violations under the CCA were reported to be among issues that drew attention in Geneva.[98]

It is a well-known fact that the internet is a borderless information technology and enables people around the world to have the same access to information; any regulations levied against the kind of medium, particularly by draconian laws that are liable to affect freedom of information and expression, which are protected by civilized countries around the world, would be noticeable to everyone. In fact, such regulations are treated as an indicator of the level of the protection of civil and political rights enjoyed by the citizens of a country. With respect to the CCA, Reporters Without Borders, on the occasion of His Majesty the King Bhumibol Adulyadej's birthday on 5 December 2009, wrote a letter asking him to grant amnesties to internet users who were incarcerated or facing prosecution on charges related to the expression of dissenting opinions the internet.[99] A representative from Forum Asia also made an intervention during a meeting of the UN Human Rights Council concerning infringement of freedom on the internet in Thailand and the grave ramifications of increased application of Section 112 of the Criminal Code and Section 14 of the CCA against internet users. Apart from high penalty tariff of 3-15 years imprisonment, it was reported that most alleged offenders were denied bail. In addition to prosecuting users and service providers, the Thai government has also blocked access to many websites without disclosing the URLs and without giving reasons for its actions. Forum Asia's representative demanded that "intermediaries" (service providers) should neither be held liable for the posts they had not authored nor be forced to censor any content on behalf of the state, and that Thailand should also repeal Section

15 of the CCA which criminalizes intermediaries.[100]

The demands echoed a call from ASEAN civil society at the Asia-Pacific Regional Internet Governance Forum 2011 (APrIGF) held in Singapore, which emphasized the notion that any censorship should be conducted in accordance with the recommendations by the UN Special Rapporteur that 1) any restriction must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); 2) it must pursue a legitimate purpose as set out in article 19, paragraph 3, of the International Covenant on Civil and Political Rights, namely: (i) to protect the rights or reputations of others; (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and 3) it must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality). Persons who are not involved should not be held liable, such as intermediaries who simply functions as a conduit of information. Legitimate expression must not be criminalized.[101] In addition, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, issued a statement in Geneva calling on the Thai government to amend the lèse majesté law and the CCA and offered to "cooperate creatively" with the Law Reform Commission to make necessary amendments to the law to ensure its com pliance with international human rights principles.[102] Apart from rights organizations, global investors and business corporations operating in Thailand, including Google, Yahoo, eBay, etc., also expressed their concerns regarding an attempt to impose restrictions on internet traffic in Thailand, claiming that it may compromise Thailand's economic growth potential.[103]

5.1.5 Reactions to New Draft of the CCA

Reports of attempts to amend the CCA have continued for many years without progress until on 28 March 2011, the working group on a new draft of the CCA organized a public hearing and invited only computer and law experts to comment on the new draft. The hearing led to public outcry against this hurried and non-transparent process. Concerns were also raised that the draft could potentially cause even more human rights violations than the current act.[104] As a result, the Faculty of Law, Thai Chamber of Commerce University, organized a public discussion on "Websurfers can end up in jail: is the new Computer-related Crime Act protective or repressive?", focusing on several flaws in Section 16 of the new draft concerning the copying of computer data while browsing.[105]

The main impetus in raising the issue to public attention came from the iLaw project which issued an open letter to people and internet users calling for the public to collaborate in monitoring the draft Computer-related Crime Act and to sign online to "stop" the submission of the draft to the cabinet without public participation. According to iLaw, apart from not solving existing problems, the new draft may lead to increased infringement of rights and freedoms in online media and does not help resolve computer-related crime.[106] More than 560 internet users signed. iLaw, Thai Netizen Network, HRLA and FACT submitted an open letter to the then Prime Minister, Mr. Abhisit Vejjajiva, demanding that the cabinet stop the process of passing the new draft proposed by MICT. As a result, the draft law was not submitted to the cabinet.[107] It was a successful campaign by civic movements.

5.1.6 Civic Groups and Recommendations for the Draft Computer-related Crime Act

As a response to the state's proposal of draft legislation, without adequate public participation, which was opposed by many experts from both legal and information technology circles, the "My Computer Law" project was established.[108] This aims to compile input from the people, including the users and providers of internet services, to develop a people's version of a draft Computer-related Crime Bill. Project activities comprise educational activities on the internet and computer-related laws, exchange fora among groups of people and dialogues with concerned agencies, the drafting of a Computer-related Crime Bill and submission of the draft to Parliament, and advocacy work to ensure the draft gets a reading in Parliament. In addition, Thailand Development Research Institute (TDRI) organized a brainstorming session on the Computer-related Crime Bill and distributed an analysis of the new draft prepared by MICT. Written by Savitri Sooksri, a law lecturer from the Faculty of Law, Thammasat University, the analysis identifies in detail the pros and cons as well as various problems in the new draft in comparison to the current act and was to be presented to the relevant agencies.[109]

5.2 Reactions to State Policies and Guidelines which Affect Freedom of Online Media

5.2.1 Reactions against the Ban on Information Dissemination and Blocking of Websites under Section 20 of the CCA and Other Legislation

On 9 March 2010, the cabinet declared part of the Bangkok Metropolitan region plus seven provinces and 21 districts as areas with a situation that threatened internal security, invoking the Internal Security Act B.E. 2551 (2008) from 11 March onward. The administration of security in these areas was given entirely to the Centre for Administration of Peace and Order (CAPO). As a result of the declaration, the administration was empowered to enforce 18 laws, including the CCA. The MICT was authorized to control the production and dissemination of electronic information over the internet and other information networks; it could order a stop to the dissemination of any information, or block any signals. Anyone disobeying would face criminal prosecution. In response, the Thai Netizen Network issued a statement condemning the blocking of communication channels and demanded its immediate end.[110] In addition, the Thai Netizen Network issued an open letter requesting disclosure of the websites blocked by orders under the Emergency Decree on Government Administration in States of Emergency B.E. 2548 (2005) and demanding revocation of the declaration of a state of emergency[111]; it also issued another statement on the political crisis and the blocking of news and information.[112]

The blocking of websites under normal circumstances by virtue of Section 20 of the CCA including requests for cooperation from individual service providers has not met with much opposition in the form of an open letters or public statements. The only protest statement was that opposing the blocking of Fah Diew Kan webboard in 2009, for which the MICT could not produce a court order on demand.[113] Academic seminars were organized on the issue of freedom in the cyber world and the

CCA at the national and international levels in order to propose solutions and exchange experience regarding censorship.[114] Advocacy against website blocking was periodically organized, including the "Censor Jung" activity to oppose indiscriminate website blocking[115] and the "Thailand: Censorship Paradise" campaign in 2011 by Reporters Without Borders to reflect problems of rights and freedom and information censorship in Thailand, Vietnam, and Mexico with tourists as the target group.[116]

The Thai authorities have made attempts to censor online information and block websites. In 2006, even before the CCA came into effect, Freedom Against Censorship Thailand (FACT) submitted a complaint to the NHRC[117] on the excessive use of power by the state without supporting laws, which was tantamount to violations of the right to freedom of expression and a breach of the Constitution. The petition was signed online by more than 1,200 people.[118]

5.2.2 Reactions Against Other State Policies Likely to Affect the Right to Freedom of Expression in Online Media

State policies and measures aimed at controlling or regulating people's behaviour and expression in online media are not limited only to information dissemination or website blocking, but also include projects for which public cooperation is requested and notification of warnings. As soon as such policy guidelines were announced among internet users, however, criticism and protests ensued, resulting in cancellation of some MICT initiatives. One such project was the installation of a sniffer system during the time Ranongrak was Minister; internet users and service providers formed the 'Thailand No Sniffer'

group and mobilized support through Twitter and Facebook[119] so strongly that MICT decided to scrap the project.[120] Another example is the reaction to the warning against making comments or clicking 'Like' on Facebook during the term of Minister Anudit, which included the public statement "Clicking 'Like' is not a Crime" by Thai Netizen Network.[121] Public outcries were also heaped against the recruitment of young people in the Cyber Scout program during the term of Minister Juti Krairiksh.

5.2.3 Reactions in Support of Law Enforcement and State Policies Aimed at Censoring Opinions in Online Media

Interestingly, in Thailand, a number of internet users agree with and support government measures to censor online information and block websites, not only those which allegedly defame, insult or threaten the monarchy but also those with any criticism of the monarchy. They form groups through online social networks to help monitor the content of websites and make reports to the authorities. One such group is the "Report Association of Thailand" which states succinctly on its home-page: "This webpage does not have a policy of disseminating insults that damage the monarchy. We disseminate information to prevent threats in the cyber world and have no policy to discuss politics, the King, or any individuals. Join in preventing threats through Facebook..." This Facebook page also encourages internet users to "stop 'Like' ", "stop 'Comment' ", "stop 'Share' " and "Report! to web admin"; a "Bomb Report" action is organized from time to time for Facebook users to simultaneously report Facebook pages to the Facebook admin.[122] Royalists have also formed a Cyber Warrior Club[123] to mobilize

internet users from all walks of life to help monitor web pages and video clips for possible lèse majesté, breaches of national security, and involvement with drugs, gambling and obscenity, in order to report the URLs to the MICT for prosecution.

Mr. Akrawuth Tamrarieng, Vice President of the Thailand Webmasters Association, once offered an opinion that it was an extremely important priority to deal with websites containing lèse majesté and that the Association proposed that this should be done mainly through legal measures. Civil so ciety organizations and the public should be asked to cooperate by reporting and compiling evidence to seek court orders to block the access to and prosecute the owners of websites which demonstrate the intention to destroy Thailand's monarchy.[124]

On 18 August 2011, 300 members of the Network to Safeguard and Protect the Monarchy and the Chakri Dynasty Protection Network met Grp. Capt. Anudith Nakornthap, ICT Minister, to give him moral support for the blocking of lèse majesté websites. Mr. Chatchai Phukhokwai, the Network Secretary said: "Most of the groups with the tendency to defame the monarchy are closely associated with the Pheu Thai Party. We are therefore here to insist that the ICT Minister, who is a member of the Party, take decisive action taken to close down lèse majesté websites immediately when detected."[125]

It should also be noted here that a number of pros-ecutions under the lèse majesté law and CCA have thus far been made possible by the cooperation of the Social Sanction Facebook group which monitors any criticisms made against the monarchy and posts the picture of the authors for members to "impale on a stake". They also search for and disseminate personal information of those on public display. Some of the

individuals condemned by the group have been reported to and later investigated by the Department of Special Investigation (DSI).[126]

5.3 Analysis of Reactions and Movements of the People's Sector

From the documented information, it can be seen that there are fewer than a handful of civic groups that monitor on an ongoing basis the issues of the right to freedom of expression in online media and ramifications from enforcement of the CCA, and at times exercise their rights to protest, issue statements or voice their opposition to government agencies' measures that impose restrictions on the right to freedom of expression. These groups include FACT, Thai Netizen Network, and iLaw. Apart from these, other groups are formed on an ad hoc basis, for example, the 'Thailand No Sniffer' group which mounted opposition to data sniffing by MICT; other existing groups launched protest campaigns when they became direct targets of any repressive policy such as the Fah Diew Kan community web-board, or HRLA, etc. There has been no litigation effort which may yield legal consequences like in other countries whereby judicial reviews are sought to hold state agencies or officials accountable when they commit abuses or when they infringe on people's rights and freedom, or where the constitutionality of certain legal provisions is challenged in court.

Based on the study, there has only been one case in which a victim of website censorship has challenged a state order in court, namely, Prachatai Online (prachatai.com) Prachatai sued the Prime Minister and the Centre for Resolu-

tion of Emergency Situation (CRES) as defendants in a civil suit to oppose their order to block access to the website under the Emergency Decree on Government Administration in States of Emergency 2005 and demanded damages from the action. Prachatai claimed that the order was issued unlawfully since no specific reasons or descriptions have been given as to what part of the content necessitated the action. CRES was also accused of committing an act in breach of the "proportionality" principle by blocking access to the whole website, even though unlawful content could at best only be found in the webboard section, which has its own unique URL separate from the main website containing news and analysis. The case was dismissed by the court of first instance and is now at the appeal level.[127]

This low level of active participation in defence of people's rights and freedoms adversely affected by the CCA could be attributed to the fact that the relevant laws are not well-known to public. Due to the technicalities involved in the laws, the majority of people are not interested, or find it difficult to understand them. Also, the Thai people in general do not give much importance to the issues of freedom of communication, freedom of information and the right to freedom of expression (unless they themselves are directly affected). Moreover, a great number of the Thai people agree with the suppression of others' dissenting opinions on certain issues on which they are passionate and want to see more stringent measures against them, particularly on issues concerning the monarchy. Thus, there have not been strong calls for the state to verify carefully if the content that is blocked are in fact unlawful (as far as Section 112 of the Criminal Code is concerned).

According to a Suan Dusit Poll conducted in 2001, al-

most a half the respondents did not know of the CCA and only 0.98% of them said they know the law quite well.[128] Meanwhile, Paiboon Amornbhinyokiat, Legal Advisor to Paiboon Law and Consultancy Co. Ltd., once said that in the more than three years since the CCA came into effect, most people are still unaware of its existence. According to his preliminary survey, 70% of respondents did not know there was such a law, 10% knew something about it, 7% understood it well and only 2-3% understood it very well. Their low level of understanding of the law can be attributed to the legal technical terms used and their knowledge of information technology. Even among law enforcement officers, very few understand the law. At present, fewer than ten police officials are experts in information technology.[129]

CHAPTER

Legal Comparison

1. Principles of Protecting Online Media Rights and Freedoms

The study of the provisions on the protection of right to information and freedom of expression in four countries and Thailand shows that every country has provisions in its constitutions to ensure that these freedoms will be secured. They all have provisions that the state must protect this right. All countries (should) accept that this kind of freedom is important and necessary for creating a truly democratic regime. Furthermore, in the cases of Germany and United States, to ensure greater clarity and to avoid possible future disputes, these freedoms are not only guaranteed in the written legal code, but embodied in legal interpretation, especially the interpretations by judicial organizations that have established and extended the scope of protection for the exercise of these freedoms in "online media".

However, as stated earlier, these freedoms, especially freedom of expression, are freedoms that have to be expressed externally. There is the chance that the exercise of one's own freedom will violate that of another. So in law, no state has "absolute" or "complete" protection of this kind of freedom as in the case for freedom of thought, belief and faith. We can see that the constitutions of the countries in this study, the United States, Germany, China, Malaysia and Thailand, always provide "exceptions" to the protection of this freedom in some matters. This can be characterized as "relative" protection of freedom.

2. Contents and ŧypes of Opinion Where Dissemination or Expression is Forbidden

The problem of which issues or content the state does not protect, in other words, or where the state has the authority to restrict dissemination or to limit this freedom depends on a particular country's political system, religions, beliefs, traditions, cultures, attitudes and broad understanding of the authorities and the importance of this kind of freedom in the eyes of the countries' citizens which can differ from one country to another. In Germany, there is content that is not protected by the constitution and may face further legal restrictions to, or penalties for their dissemination. Important examples include content that is harmful to children and youth, harmful to public peace, humiliating to human dignity, contemptuous of other races, propagating German nationalism or Nazism, etc. In the United States, while protection of children and youth from harmful content is asserted by law, expressions against the integrity of other people, nationalities and races, as well as the dissemination

of any ideology are permitted freely because they are protected under the constitution.

For countries under one-party political systems or is which democracy is not fully established such as China and Malaysia, any speech, writing or any kind of expression, especially on online media that is accessible to a large number of people, that are critical of the system and the government are prohibited either formally, as in China, or informally, as in Malaysia. "State security" tends to be the primary reason for the legal restrictions on freedoms in such cases. Even in countries described as democratic such as Thailand, the security issue is the primary reason for the state to legislate or impose some kind of measures to restrict the dissemination of information and expression of opinion, especially the law related to the monarchy which is in the "security section" of the Thai criminal code.

In Malaysia, apart from the issue of security and government stability, any content that is critical of or in conflict with beliefs, faiths and religious rules are also prohibited due to the strictness of religious beliefs in the country.

3. Types of Legislation that Limit Freedoms of Online Media

The study shows that the laws that are used in each country to restrict freedom of expression are not limited to the laws related to crimes in computer systems or networks, but include other laws. In Germany, offenders are prosecuted mainly through the criminal code (StGB) and also through laws related to the protection of children from various of types public media and laws related to telecommunication services. In the same way, in the United States, there is a great deal of legislation related

to the protection of children and youth. Furthermore, there is also new legislation to restrict the freedom of American citizens for the reasons of anti-terrorism. For China and Malaysia, the laws restricting the freedom on various media, including online media, mainly relate to state security and safety.

Nevertheless, it should be noted that in all the countries mentioned there is no specification legislation related to computers or computer crimes to control the content of the online information or to monitor the consumption of information and interaction in online media such as exists in Thailand. Even in China, the ICT law that is used to regulate the freedom of the public is not a "substantive" provision on offences committed in computer systems or networks, but one that regulates telecommunication entreprises, holding ISPs accountable for content through the issuing of licenses. At the same time, the Malaysian government has clearly announced that it will not legislate any law that would restrict freedom in online media since it wants the users to have freedom and wants Malaysia to become a centre for information services.

4. Characteristics of Legislation that Restricts Freedom in Online Media

As mentioned throughout this research, the protection of the rights to freedom of information and expression of the people as specified in the constitution will never be achieved or realized in practice if state legislators pass laws (that effectively restrict such rights and freedoms) on the basis that they are "exceptions to rights and freedom protection", which are broad in scope, ambiguous and unclear. This kind of legislation would

only create loopholes and would risk being interpreted by government officials and the law enforcement officers beyond the "principles" and end being used by them to violate the people's rights at their own discretion. This would not be consistent with the spirit of the constitution that requires the state to protect the rights and freedom of the people on principle and restrict these rights and freedom only exceptionally. However, the study has found that legislation with ambiguous wording still exists in various countries.

Nevertheless, it is hard to dispute that any issues related to "state security" are abstract issues that cannot be clearly defined. Therefore, normally, countries that have less concern about "state security and stability" than "behavioural and legal status stability of the citizens" tend to use "state security" as the reason to restrict its citizens' freedom as little as possible or even not at all. As can be seen in the laws of Germany and the United States, this kind of reasoning is used less than in the laws of China and Malaysia. Even though there is some ambiguity in the prohibition in the German criminal code against disseminating content that would create division among the public, it should be noted that this legislation still gives more weight to the protection of public safety than to protecting the stability of the state or government. In the same way, in the United States, there are nominal guidelines for court judgments to regulate the law at another level which affirm that the state can restrict the freedom of its people only when it can demonstrate the reason or evidence that the exercise of such freedom would be seriously detrimental to the state or to the public. These characteristics are different from Thai law in which vague wordings exist many articles, such as "contrary to security", "creating panic among

the people", "contrary to peace and order" and, especially, "contrary to good morality of the people" in articles 14 and 20 of the CCA which is the main provision related to online distribution of content.

5. Duties, Liabilities and Penalties of Intermediaries or Online Media Service Providers

Because investigating and tracing a person who disseminates illegal online content is a difficult task, today many countries have tried to create new laws or regulations that place "duties" and "liabilities" on the telecommunications and internet service providers to make those providers help monitor illegal activities or alleviate the burden of state officials. For example, Germany has passed a law that requires telecommunications and internet service providers to store the computer traffic data of all their internet users for no less than 6 months (Telekommunikationsgesetz). Eventually, the provision was judged by the constitutional court to be unconstitutional and was revoked. Furthermore, Germany also has telecommunication services laws (Telemediengesetz and Mediendienste-Staatsvertrag) that differentiate among types of internet services to designate different duties and liabilities of internet service providers of each type under conditions that take into account the role and relatedness with respect to content including the knowledge of the dissemination of the content of each service provider. The latest law to be passed is one that requires internet access providers to block child pornography sites listed by the national police office (Zugangserschwerungsgesetz), but the constitutional court ruled that it is unconstitutional and ended its legal enforcement.

Similarly, the United States has provisions that require telecommunication service providers to store computer traffic data for official inspection (Stored Communications Act or SCA) and set liabilities for internet service providers that have knowledge of the dissemination of content harmful to children and youth (Communication Decency Act). Nevertheless, it should be noted that the provisions on the duties and liabilities of internet service providers in both Germany and the United States have the same principle that prohibits the treatment of service providers in the same manner as the user who is the primary offender including the comparison of internet service providers with editors or content screeners of traditional media since the volume of data and speed of data dissemination on the internet is significantly different from those in traditional media, making it impossible to attribute the same duties and liabilities. In this respect, these laws are different from article 15 of CCA that imposes the same penalty on the service provider as the actual offenders.

In China, there are several laws that control and regulate the role of the online media service provider, especially through business licences such as Provisions on the Administration of Electronic Publications, Provisions on the Administration of Internet Electronic Bulletin Board Services and Measures for the Administration of Internet Information Services. Furthermore there is a Regulation on the Administration of Internet Access Service Business Establishments (Internet Cafes) that requires internet cafes to collect data on their clients for the state to examine. In Malaysia, as the government promised its people and the international community that there would be no legislation in Malaysia to restrict the freedom of information and of expression

on the internet, until now, Malaysia has not passed any special law beyond what already exists in the Malaysian criminal code to prescribe the liability of either service users or providers for disseminating information. Although there have been reports of the arrests of internet users including citizen reporters, these are done under security laws. However, as mentioned, Malaysia has at least two laws, the Communications and Multimedia Act (CMA) and the Communications and Multimedia Commission Act (CMCA), which give authority to a special committee on telecommunications to examine online media usage to prevent the inappropriate content from being disseminated. The two laws create the common "Guidelines on Content" for service providers to comply with the laws in a system of self-regulation under a code of ethics or "Content Code".

Comparisons of State Policies and Practices

1. Measures to Block Access to Information or Websites

It can be said that sites are blocked in every country, including Germany, where much weight is given to democracy and the protection of freedom of speech of its citizens. The differences are the extent to which these measures are used and the legal reasons for the blocking. It can be "formal" such as normal law enforcement by the state, through the courts or prosecutors' orders. It can be "informal", where orders are given secretly to service providers or a special agency is secretly established to monitor and block websites as happened in the United States with sites related to Middle East wars or the inhumane treatment of war prisoners. However, as mentioned, in the case of

Germany, blocking of online media access has all been clearly within the scope of law and under the proportionality principle. The most important aspect is that blocking follows procedures that the public can examine and oppose, which differs from the practice in China, Malaysia or even Thailand. In these countries, blocking occurs not only under vague legislation, but the reasons for blocking are unclear and not declared to the affected party. In many cases, blocking occurs under special laws with severe penalties and the state has sole authority to prosecute without allowing any external organizations or the public to check the exercise of such authority. Furthermore, blocking is frequently informal, which makes it difficult to find any witness or evidence. This type of blocking occurs in Malaysia despite the existence of Article 3 (3) of the Communications and Multimedia Act (CMA) which states that "... Nothing in this Act shall be construed as permitting the censorship of the Internet".

In China, the state has the attitude that it has full authority to examine and block websites of every type in the interests of the whole nation, so many websites in the past were closed with no prior notification and no possibility of appeal. Furthermore, China's Great Firewall is, by far, the world's most effective blocking tool. Apart from seeking out undesirable words in the eyes of the state, it can also prevent search engines from finding sites.

Incidentally, even though various countries have blocked different numbers of websites, no state agency responsible for this has announced the figures to the press in their 'performance portfolio'.

2. Organizations Established to Regulate Online Content

The study found that in all the countries studied special agencies were established to monitor online media content. The tasks of these agencies may vary according to the policy of each country. In Germany, an agency monitors content accessible to children and youth. In the United States, the focus of the special agency is to gather intelligence on potential terrorists. In Malaysia, a special agency established under two laws, the Communications and Multimedia Act and the Communications and Multimedia Commission Act, regulates internet content.

In China, many special agencies have been established and the authority of the existing media regulation agencies has been expanded to include the internet. These agencies include: the General Administration of Press and Publication (GAPP) which issues publishing licenses; the State Administration of Radio, Film, and Television (SARFT) which is tasked with issuing licenses for online media businesses and which is under the control of the Ministry for Information Industry; the State Council Information Office which establishes rules and criteria to regulate the expression of opinion in all media and registers websites; the Ministry of Industry and Information Technology (MIIT) that establishes the rules for the information technology industry, such as that requirement that every computer in China have a pre-installed monitoring programme; the Internet Affairs Bureau of the State Council Information Office, which regulates the internet activities of the public and blocks pornographic sites or sites related to terrorism; and the agencies known as Bureau Five and Bureau Nine, which monitor movements in online media. In addition, there is also an agency for psychological

operations called the Government-connected Internet Society which campaigns the internet service providers to block content deemed inappropriate by the government. The government also hires groups of internet citizens called "50 Cent Parties" to spread support for government policies and administration.

The situation in Thailand can be seen as similar to China in that several agencies have been established specifically to monitor internet content. The difference is that the Thai agencies have overlapping tasks and authority to the extent that can cause confusion among the people or the officials themselves. The Centre for Cooperation for the Suppression of Information and Communication Technology Crime, or ICT Corp, was established when Man Pattanothai was the ICT minister and involves the cooperation of various agencies such as the Crime Suppression Division, National Intelligence Agency and Department of Special Investigation (DSI). The task of the Centre is to investigate crimes committed through the internet including lèse majesté offences. Another agency, the Internet Security Operation Centre (ISOC), coordinates between the police and army in monitoring threats from inappropriate content on the internet and supporting the prosecution of lèse majesté offenders. This Centre was also established by MICT, but during the tenure of Sub. Lt. Ranongruk Suwanchawee. Other agencies include the Economic Crime Suppression Division and Technological Crime Suppression Division of the Royal Thai Police, and the Office of Technological and ICT Crime under DSI. Despite some differences in the authority of these agencies, lately the main task of all of them has been to detect content critical of or even insulting and defaming HM the King. Added to this is the Cyber Scout Project that was initiated when Juti Krairiksh

was Minister, which is comparable to establishing a new special agency to train its members to monitor content related to HM the King on the internet.

3. Statistics on Prosecutions or Threats to Internet Users and Service Providers

In this research study was unable to find up-to-date statistics on arrests and prosecutions of internet users and service providers in the countries studied that were clear enough to be compared to Thailand, especially offences related to online dissemination of illegal content or content seen as inappropriate by the state. Nevertheless, of the four countries in this study, China seems to be the one with the highest number of internet users and service providers, especially "citizen journalists", arrested or threatened or have their rights violated by the state. Amnesty International stated that "China has the largest recorded number of imprisoned journalists and cyber-dissidents in the world.".

From 2001, the Chinese government started to arrest and imprison internet surfers and activists who use the internet as the medium to distribute news and information critical of the Chinese government. This continues until today. An interesting case is the arrest in 2004 of the journalist Shi Tao who used his personal email to send information to a democracy activist website in the United States to inform them that the Chinese government had ordered its telecommunications organization to obstruct the events commemorating the 15th anniversary of the 1989 democratic uprising. Shi Tao was charge with revealing national secrets to foreign organizations.[1] Another is the arrest in 2008 of Huang Qi for giving information to the foreign me-

dia and publicizing on his own website the plight of Chinese parents who lose their children in schools that collapsed during an earthquake. The charge was that illegal possession of state secrets.[2] The country with the second highest number of reported arrests of online reporters is Malaysia. Several prominent cases caught internet users' attention, such as the arrests of Raja Petra Kamarudin, editor of Malaysia Today, and Khairul Nizam Abdul Ghani, a blogger from adukataruna.blogspot.com, who was accused of lèse majesté, or the prosecution of blogger Karpal Singh under Article 4 (1) (b) of the Sedition Act for his opinions on the Sultan of Perak.

Thailand in comparison can be considered one of the countries with a high number of arrests and prosecutions on charges related to dissemination of content through the internet, though at a lower frequency China and Malaysia. Most cases in Thailand were initiated in periods of political conflict. However, in China and Malaysia we have to note the absence of arrests or prosecutions of service providers simply because they provide the services through which the offensive content is disseminated. This is in sharp contrast to Thailand, since in a few cases, the state prosecuted the service provider making them responsible for the expression or information of others (the users). An analysis of the situation could be that China and Malaysia prefer to regulate service providers by means of prescribing duties and compliance, such as collecting and storing computer traffic data, registering internet users, installing word-filtering programmes, etc. These regulations are also enforced by a "licensing system" or by encouraging the establishment of a common code of conduct among service providers including Notice & Takedown systems. These policies are in contrast

with those in Thailand which aim to make the service providers liable for users' offences, even without, as yet, the necessary details for such procedures.

Comparison of Public Reaction

1. Importance Given to Rights and Freedoms and Awareness of Violations of Rights Through Legislation or State Policy

It should be noted that compared to western countries such as Germany and the United States, the right to information and freedom of expression have been given much less importance in the east. The general public and rights activists and organizations have not normally focussed on the issue, especially freedom in online media which receives even less attention than that given to TV and radio. In Germany and the United States, both the state and the public see the importance of these rights and freedoms for the democratization process because they enable the public to participate in governance and express their will freely. However, most Chinese citizens see the internet only as a personal communication tool just for entertainment and pleasure, not for political or analytical purposes. Furthermore, the public also believes that any exercise of the rights and freedoms of private individuals should never infringe on peace and order and the national interest. The individual may not claim these rights and freedoms which should be limited for the good of the Chinese mass public. This type of thinking is also pervasive Thailand. Many members of the Thai pubic are of the opinion that this kind of freedom should not be raised at all when it comes to issues related to the monarchy, good mo-

rality, peace and harmony or conflict avoidance. Nevertheless, while the Chinese government has to hire a group of people to monitor and report on illegal or inappropriate content for the government to block and to propagandize government activities, the Thai government established official state projects (such as the cyber scouts) and encouraged people to form groups to monitor each other such as the Social Sanction group or the monarchist group, etc. Because of these activities and because the CCA is the main law to restrict freedom of expression, the Thai people and organizations that monitor the law and the use of government authority so that it poses an excessive threat to the people's rights and freedoms are limited to those involved in the use of information technology.

It should be noted that the general public and organizations in Malaysia seem to be more active and come from a greater variety of backgrounds. One of the reasons might be that the laws that Malaysian government uses for controlling and limiting expressions of opinions do not focus on IT or computer-related communication, but on state security, so the groups of people affected are more broad-based. Apart from bloggers and citizen journalists, political alliances, such as the supporters of Anwar Ibrahim, and right groups such as SUARAM that have long advocated political rights and freedoms are also active in opposing government restrictions on freedom of expression by various state security laws.

2. Ways that the People React to or Protest Unjustified Laws or Policies and their Outcomes

As mentioned previously in the study, the characteristics

of people's advocacy movements in the eastern world are limited to social and policy issue protests, and there are few reactions or calls related to law enforcement as in the west. In Germany or the United States, for example, people's groups and organizations not only organize information campaigns and protests, but they also join together to use their legal rights and means to sue state organizations or officials when they notice the inappropriate or excessive use of authority that violates the rights of the people. They have also brought issues to the supreme court or the constitutional court for deliberation on the constitutional legitimacy of the legislation in question. The judicial bodies, especially the German Constitutional Court and the US Supreme Court, have in many cases ruled that certain laws and measures were in violation of the rights and freedoms of the people and therefore unconstitutional, resulting in the termination of their enforcement.

There are various reasons for the lack of diversity among social and public movements in the east: the political systems are not yet fully democratic; the people themselves lack respect for different opinions; the legal channels to defend rights are unclear; and in some cases there is no provision for appeal against the power of legislators. Moreover, there are problems of illegitimacy and bias among government and judicial agencies and officials. All these factors discourage activists that are already small in number. They feel powerless against the state and distrust the justice system and the legitimacy of court rulings.

CHAPTER

Recommendations

1. Legal Recommendations

1.1 The Computer-related Crime Act should be a criminal law that defines criminal offences and penalties only for crimes that are truly computer-based, or for offences aimed at computer data or the entire computer system directly, such as unauthorized access of another's computer, spying on or intercepting computer data, sabotaging computer systems or destroying computer data, and computer fraud. Since in comparison to criminal law, these acts have different "elements of the offence" from basic crimes such as property theft or trespass causing loss of assets, it is impossible to interpret the existing law (such as the Criminal Code) to cover these new forms of actions, resulting in gaps in the law. For this reason, specialized legislation on computer-related crimes should aim at filling such legal gaps or supporting the prosecution of the perpetrators of offences that are legally

different from basic crimes.

For offences related to the distribution of illegal "content" in online media, since this Act does not have "elements of the offences" that are substantially different from distributing illegal content to the public via other forms of media, existing laws can be applied to these offences. For example, Section 287 of the Criminal Code which covers the commercial distribution of pornographic material could also be applied to online distribution. Meanwhile, the distribution of content contrary to state security in any form of media can be prosecuted under Section 116 and related articles in the Criminal Code. In the same way, defamation of a third party by any means or in any form of media is already covered under Sections 326 or 328 of the Criminal Code. Even lèse majesté offences are already covered under Section 112 of the Criminal Code. New legislation for offences that are not substantially different in the "elements of the offence" from what is specified in existing laws not only causes confusion to both the public and law enforcement agencies alike, but, if legislators also choose to use vague wordings (such as exists in Section 14 of the CCA, especially Section 14 (2)), it also creates problems at the level of legal interpretation. Furthermore, when such a law gives officers the authority to use a broad interpretation, there is more chance that the application of the law will inappropriately infringe on the freedom of expression of the people.

Incidentally, if the government sees the need for specific provisions to control the distribution of illegal content in "online media" or wants to expand further the elements of the offence of such acts, such as criminalizing both the commercial and non-commercial distribution of pornographic material in

online media or increasing the penalty for the distribution of child pornography, it could add these provisions in the relevant sections of the Criminal Code or other basic laws since they are offences of the same nature (distribution). Many countries such as Germany, Austria and Switzerland have used this method.

1.2 If Thailand still insists that it is necessary to include the offence of "disseminating illegal content" in online media within the CCA, the researchers see the need to define "content forbidden to disseminate" more clearly than the existing description in the CCA. The description should be at least as clear as in the Criminal Code, so that it will not violate "the principle of legality in criminal law" which requires that "the elements of an offence must be defined exactly" (lege certa). Legislators must try their best to avoid broad and ambiguous wordings whose meanings depend on the context of the particular time or situation in the country and that allow officials excessive discretion in interpretation. Furthermore, legislators must avoid wordings such as "contrary to public order or the good morals of the people", "contrary to state security" or "causing public panic". In addition, new specialized legislation should be consistent with the spirit of the law that is the basis for the same offence. For example, in the case of ordinary offences of individual defamation, the Criminal Code defines them as "private offences" which means that the law intends that only "true victims" of defamation can report a case or file charges against offenders. And because it is an offence that affects only "private" interests, and not so severe as to damage society or the public interest, the law allows for both parties to agree on a compromise. Moreover, the offenders against defamation under criminal law also

have the right to prove a "justifiable act" (Section 329 of the Criminal Code) or "exclusion of liability" (Section 330 of the Criminal Code). If the state wants to prescribe similar offences in the new specialized law, legislators should consider whether to include in the new law the conditions and characteristics of the offences that appear in the Criminal Code. If not, they must provide reasons for this decision.

1.3 In determining the responsibilities and liabilities of "service providers" which also affect the freedom of expression of the general public, legislators should revise Section 15 and other Sections of the CCA to make the following amendments.

- The definition "service provider"[1] should be consistent with actual business practice and should be limited only to the provider of the services that are related to the actual computer systems or networks. The researchers are of the opinion that the CCA should not include "telecommunication service providers" or providers of other communication equipment or tools or other communication channels such as telephone lines, mobile phone connections (without access to the internet), system rental and satellite service providers[2] which are not directly related to computer services or computer data. This is to avoid confusion among the general public, the service providers themselves and law enforcement officers, and to be consistent with the spirit of the CCA that is aimed only at offences related to computer systems or networks. Nevertheless, if the state wants to prescribe certain responsibilities or liabilities to providers of other types of telecommunication service, it should do this under other legislation directly related to those particular services.

It is noteworthy that in other counties, provisions that require "service providers" to collect and store computer traffic data are not part of their computer crime laws, but part of the laws related to telecommunication services.[3]

- In prescribing the liability and penalty of "service providers" for illegal "content" that their clients disseminate in the space or channels that are provided as services, the researchers recommend that legislators should calibrate the level of liability according to the characteristic and type of internet service. For example, content providers should be directly liable for their content and if a space or board is attached at the end, the content provider may also be liable if s/he has knowledge that the content there is illegal. The providers of purely technical services such as internet access should not in principle be liable for any content at all, unless under certain conditions as prescribed by law. For example, under German law, this group of service providers will be liable only if it can be proved that they themselves engage in the selection, adjustment or modification of information even if it does not belong to them or they have conspired in or given consent to the dissemination of the information.[4] Host service providers who rent out storage space should also not, in principle, be liable for any action of their clients, unless they have knowledge of the existence of illegal content and take no appropriate action against this, especially when they have been notified by the offended party or by state officials. Moreover, the law should not prescribe "general responsibility" to "service providers". The service provider should not be made responsible for monitoring all content in all their service space all times even without any notification. This would increase the service provider's burden exceedingly

in terms of time, personnel and budget. It is also in conflict with the nature of the internet with an enormous amount of information traffic every second. Such burdens would affect the business incentive for engaging in internet services and affect the "price" that internet users as a whole have to pay for the service.

As to the penalty for internet service providers, especially in cases where they are not the actual offenders, if the legislators want them to be responsible for their clients' offences, which is a case of "liability for others' offences", the law should not prescribe a penalty that is "equal to" that of the actual offenders, but should be at a proportionate and appropriate level and consistent with the principle of "various offenders" (principals, instigators and supporters) in which instigators and supporters receive proportionately lower penalties than that prescribed by the law for the principal offenders. Nevertheless, even if legislators aim to prescribe liability for service providers due to their "negligence of duty", which is not based on others' offences as in the first case, the penalty in this case should not be "equal to" the penalty of disseminating illegal content since the nature and the intent of the act by the service provider, that is only neglect of duty, without intending to harm others directly, would be different from the intentional act of directly committing an offence by disseminating illegal content. Therefore, the fact that Section 15 of the CCA prescribes the same penalty for the service provider as for the offender is not justified by all principles.

- The law should clearly prescribe a "procedure" that service providers are required to follow in dealing with illegal content that appears in the space or scope of their services. Generally, this procedure should include only "deleting or removing

all or part of the content" from the space of their service either temporarily or permanently in accordance with notification from a related or authorized party. The procedure should not require the service provider to "block access to the information or the websites" since blocking access to information is a severe measure that could also affect the freedom of others, not only the distributors of such information. Therefore, the state should have power as limited as possible in using this kind of measure or should be allowed able to use such a measure only after it has been scrutinized and approved by organizations other than law enforcement agencies as prescribed in Section 20 of the CCA, that officials must request court orders to block websites. The clarity of the prescribed procedure to deal with illegal content not only makes the law unambiguous and less prone to create problems at the level of enforcement and interpretation, but also prevents state officials or those with government authority from bypassing the process of obtaining court orders and instead using the method of directly "asking for cooperation" or "ordering" service providers to block sites.

- In order to provide clear guidelines on how to notify internet service providers about illegal content so that they can proceed appropriately on the notified content within a reasonable period of time, the state should enact a law or issue regulations as appropriate clearly detailing: 1) the persons with the authority to notify service providers about illegal content; 2) the method of notification that has legal effect; 3) reasonable grounds and preliminary evidence that must be presented to service providers as justification for the action to be undertaken against the notified content; 4) the details and reference point of the location of the content on the internet (URL) should be included in the

notification; 5) a sufficient and appropriate timeframe for the service provider could use to locate, delete or take action against the content. If such guidelines are established, the limitation on the people's liberty through the co-operation of service providers will be standardized with clear limits and will also follow the "notice and takedown" principle[5] that many countries accept as the appropriate procedure and have already put into force. Moreover, this process is also "fair" to service providers that receive notifications, since when service providers are prosecuted by government officials or any other person, they will have the opportunity to prove their innocence or to defend themselves in court by proving how the notification is not justified or does not have legal effect, or why they have the authority not to comply a notification, or whether and how they have done their best to take measures against illegal content, etc.

1.4 On the issue of suppressing the dissemination of content or blocking access to information or websites, the principles and the provisions in the CCA should be reconsidered with a view towards the following amendments:

- Section 20, which prescribes the "measures to curb the dissemination of content or to block access to websites", should be amended to clarify the type of content to which the provision is meant to apply. The provision should not use ambiguous wordings that are open to a wide range of interpretations, such as "contrary to public order or the good morals of the people"or "contrary to state security" that it currently contains. Only clarity concerning the intent of the provision can help to create a balance between the prevention and suppression of offences

related to disseminating information in online media and the freedom of expression of the people. The provision should be based on the basic principle that the measures to block access to websites are to be applied only to content of such gravity that could cause severe damage to the people or to democratic society. That is to say the blocking should be aimed only at sites where images, words or expressions are displayed with certain intent such that if there are not blocked immediately and if the investigation and prosecution process is allowed to take its full course, there will be enormous damage or it would be too late to remedy the "effect" of the content disseminated; examples of such grave offences include child pornography or incitement to genocide within the country.

- The state should specify clearly in the law or regulations the methods, processes and conditions under which it will exercise the power to block access to websites, so that the officials and agencies authorized to issue orders can act with integrity, fairness and accountability. For example, the authorized official has to present to the court the content that is deemed illegal and which is to be blocked together with appropriate reasons for the action. The judicial agencies or the court should also clearly "show reason" for the order. Especially in cases where the court issues an order to block a website, there must be specified procedures for delivering the order and its reasons to the service provider and related persons or the persons that will be directly affected by the order. Moreover, the procedure and characteristics of the blocking must adhere to the principle of proportionality which means that if technically possible, the state must block only the "specific parts" of the site where the allegedly illegal content is located. The period of the blocking

must be clearly specified. The court may prescribe "conditions" to which the affected parties must comply or amendments to the content, which can later be cited as reasons for requesting the court to cancel the blocking order.

In addition, in order to "guarantee" to the public that the blocking measures do not become a political tool of those in power to abuse or harass the opposition, once there is a court order to block a website, there must be a follow-up process to prosecute the distributor of the content that prompted the blocking and if the court finally finds the perpetrator not guilty or that the content in question is not illegal, the court must revoke the blocking order immediately. In such cases, there should be remedial measures in place for those who have been affected by the order.

- Currently, Section 20 of the CCA states that the court is the agency with the authority to issue orders to suppress dissemination of information or to block access to websites. The researchers are of the opinion that may be inappropriate considering the current burden of the court, the court's knowledge and expertise in ICT, the necessity for speed in process orders vis-à-vis the thoroughness in scrutinizing the content in question[6], the problems and perspectives regarding the freedom of expression of the people, etc. Therefore the researchers propose that the role of the court in this regard be revised under a more appropriate agency. For example, the authorized entity could be in the form of a joint committee whose members may be selected or appointed to examine offending content upon request. The qualifications, composition, and origins of committee members should include the government representatives, representatives of rights advocacy organizations, representatives of private ICT

organizations, representatives from the business sector, etc. The state should also include clearly in the law the process for issuing an order and the process for opposing an order.

2. Policy Recommendations

2.1 The state should consider and identify effective and enforceable measures to regulate content and information in online media, which strikes a balance with the protection of the people's freedom, to replace the blocking of access to websites, which not only has no concrete and long-lasting achievements while heavily infringing on the freedom of expression of the people, and also provoking protests against the law and the state by its citizens. The blocking measure is an ineffective way to suppress access to illegal content for various reasons. For instance, the blocked site provider can shift or transfer the content from the server computer to other local or foreign server computers, creating many more websites identical or similar to the blocked website. Moreover, the blocking of site access does not make the illegal content disappear from the internet; it just makes internet users unable to access the site in the normal manner. If internet users can find other ways to access the blocked site, they can gain access to the content. There are today many tools and technologies available that could help internet users in this regard, such as proxy, RSS or even ordinary e-mailing. Interestingly, even the state officials involved in the enforcement of site blocking measures themselves say that blacklisting websites has not only been unsuccessful, but also creates an excessive burden on internet service providers.[7] Consequently the state should not proceeds with its policy of prevention and suppression of inter-

net crime by focusing on illegal content dissemination through website blocking unless it is an urgent necessity and significant damage has occurred. And the law must specify explicitly the circumstances under which such authority is to be exercised as proposed in "Legal Recommendations" above.

The researchers suggest that in the end, other measures could be more effective in controlling illegal content. The state could promote the process or mechanisms of self-regulation among internet users and internet service providers while the state plays a monitoring role to ensure that self-regulation operates within the scope of law, such as preventing people from violating each other's rights, from defaming each other or from inciting illegal acts against people with different opinions. Moreover, strict and indiscriminate law enforcement and improvement in computer technological knowledge and skills of government officials to enable them to trace actual offenders for prosecution and punishment should also contribute to a reduction in offences on internet networks since it would increase the possibility of offenders being arrested and prosecuted and would deter potential offenders. However, the provisions on offences and penalties that the state should use for prosecution must be sufficiently just. This means the provisions must be clear and unambiguous, aimed only at penalizing acts that cause real damage or are truly contrary to social standards in a democratic society and must set penalties that are proportionate to the damage.

2.2 The state should encourage the establishment of a specialized court to prosecute cases related to computers in particular similar to the existing juvenile and family court,

labour court, tax court, and court of intellectual property and international trade. The judges of this specialized court should be persons with good knowledge and understanding of ICT or computer systems. The state may also appoint external personnel who are not professional judges, but have the required knowledge and expertise as associate judges to participate in trials and judgments.

2.3 The state should provide an operational handbook which includes explanations of related laws and regulations for the officers, internet service providers and general public who are internet users. The handbook should not only focus on preventing and suppressing computer crimes or internet offences, but should also pay attention to the issue of protecting freedom of information and expression.

2.4 Besides prescribing a limited scope of responsibility and liability necessary for internet service providers by means of legislation (as suggested in "Legal Recommendations"), the state should encourage business owners to establish a written "code of conduct" for internet services providers to serve as a common guideline. The state should also conduct research on other possible measures and mechanisms to create "incentives" among business owners to monitor and prevent offences or the dissemination of illegal content, instead of relying solely on suppressing and penalizing service providers.

3. Recommendations for Internet Service Providers and Users

3.1 In democratic society and in the era of information technology, in addition to rights over one's own life, body and property, the people, mass media and organizations working for the protection of rights should all pay more attention to the rights to privacy of information, to access to information and to freedom of expression. All these rights and freedoms have long been important to citizens of western countries and they have long been active in protecting these rights from violations by the state and their rulers, as exemplified by the people's reaction to state laws and policies in Germany and the US reported above. These rights are important because they are the foundation of other rights under a democratic form of government. If the people could not have access to any view and information of their choice, could not be confident about the security of their private information, or could not freely express their opinions on various issues, especially on politics and the role of institutions and organizations including the ruling group with authority, their other more essential rights and freedoms would be at risk of violation by the state and those in power.

3.2 Both individuals and organizations involved in the protection of these rights should be constantly alert and actively monitor the enactment of laws, regulations and state policies that may infringe on the rights to freedom of information and expression to prevent the state from exceeding its authority. If state use of power is found to be illegitimate, people should unite or collaborate to send complaints to the responsible organiza-

tions or agencies for reconsideration or repeal of the legislation or policy measures in question. The people may even make use of the judicial process to request the constitutional court to examine whether a law or provision is consistent with the constitution, as frequently happened in Germany and the US. At the same time, the mass media should support, pay attention to and report to the public on the people's struggle for their rights and freedoms, so that the general public would become aware and alert and see the importance of their rights and freedoms.

3.3 Internet service providers may unite or form a strong trade organization. They should also monitor state legislation and policies related to the issue to see whether the responsibilities and liabilities prescribed for them are excessive, since this would ultimately affect the rights and freedoms of the people. Such effects include increasing costs of services as well as restriction on freedom of information and expression in view of potential censorship by service providers. Strong organization could help increase the negotiating power of service providers in demanding fair legislation without placing an excessive burden of internet crime prevention on private business.

เชิงอรรถ

บทนำ

[1] มาตรา 45 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550, "บุคคลย่อมมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น

การจำกัดเสรีภาพตามวรรคหนึ่ง จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อรักษาความมั่นคงของรัฐเพื่อคุ้มครองสิทธิ เสรีภาพ เกียรติยศ ชื่อเสียง สิทธิในครอบครัวหรือความเป็นอยู่ส่วนตัวของบุคคลอื่น เพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเพื่อป้องกันหรือระงับความเสื่อมทรามทางจิตใจหรือสุขภาพของประชาชน

การสั่งปิดกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่นเพื่อลิดรอนเสรีภาพตามมาตรานี้จะกระทำมิได้

การห้ามหนังสือพิมพ์หรือสื่อมวลชนอื่นเสนอข่าวสารหรือแสดงความคิดเห็นทั้งหมดหรือบางส่วน หรือการแทรกแซงด้วยวิธีการใดๆ เพื่อลิดรอนเสรีภาพตามมาตรานี้ จะกระทำมิได้เว้นแต่ โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายซึ่งได้ตราขึ้นตามวรรคสอง

การให้นำข่าวหรือบทความไปให้เจ้าหน้าที่ตรวจก่อนนำไปโฆษณาในหนังสือพิมพ์หรือสื่อมวลชนอื่นจะกระทำมิได้ เว้นแต่จะกระทำในระหว่างเวลาที่ประเทศอยู่ในภาวะสงคราม แต่ทั้งนี้จะต้องกระทำโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายซึ่งได้ตราขึ้นตามวรรคสอง

เจ้าของกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่นต้องเป็นบุคคลสัญชาติไทย

การให้เงินหรือทรัพย์สินอื่นเพื่ออุดหนุนกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่นของเอกชนรัฐจะกระทำมิได้"

[2] มาตรา 29 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550, "การจำกัดสิทธิและเสรีภาพของบุคคลที่รัฐธรรมนูญรับรองไว้จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เฉพาะเพื่อการที่รัฐธรรมนูญนี้กำหนดไว้และเท่าที่จำเป็น และจะกระทบกระเทือนสาระสำคัญแห่งสิทธิและเสรีภาพนั้นมิได้

กฎหมายตามวรรคหนึ่งต้องมีผลใช้บังคับเป็นการทั่วไป และไม่มุ่งหมายให้ใช้บังคับแก่กรณีใดกรณีหนึ่งหรือ แก่บุคคลใดบุคคลหนึ่งเป็นการเจาะจง ทั้งต้องระบุบทบัญญัติแห่งรัฐ ธรรมนูญที่ให้อำนาจในการตรากฎหมายนั้นด้วย

บทบัญญัติในวรรคหนึ่งและวรรคสองให้นำมาใช้บังคับกับกฎที่ออกโดยอาศัยอำนาจตาม บทบัญญัติแห่งกฎหมายด้วยโดยอนุโลม"

[3] มาตรา 20 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.

2550, "ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่ง ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่ กำหนดไว้ในภาคสองลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้อง พร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้ แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้ ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้"

[4] มาตรา 9 พระราชกำหนดบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548, "ในกรณีที่มีความจำเป็นเพื่อแก้ไขสถานการณ์ฉุกเฉินให้ยุติลงได้โดยเร็ว หรือป้องกันมิให้เกิดเหตุการณ์ร้ายแรงมากขึ้น ให้นายกรัฐมนตรีมีอำนาจออกข้อกำหนด ดังต่อไปนี้...

(3) ห้ามการเสนอข่าว การจำหน่าย หรือทำให้แพร่หลายซึ่งหนังสือ สิ่งพิมพ์ หรือสื่ออื่นใดที่มีข้อความอันอาจทำให้ประชาชนเกิดความหวาดกลัวหรือเจตนา บิดเบือนข้อมูลข่าวสารทำให้เกิดความเข้าใจผิดในสถานการณ์ฉุกเฉิน จนกระทบต่อความมั่นคงของรัฐ หรือความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ทั้งในเขตพื้นที่ที่ประกาศสถานการณ์ฉุกเฉินหรือทั่วราชอาณาจักร..."

[5] มุทิตา เชื้อชั่ง. (2554, เมษายน 29). รายงาน: สำรวจสถานการณ์หลังปิดวิทยุชุมชนเสื้อแดง (ระลอกแรก). *ประชาไท*. สืบค้นเมื่อ 7 พฤษภาคม 2555, จาก http://www.prachatai.com/journal/2011/04/34291

[6] ไทยรัฐออนไลน์. (2554, กรกฎาคม 6). ปชป.สับพท.แค่48ชม.ลุอำนาจไล่ปิดวิทยุชุมชน. สืบค้นเมื่อ 7 พฤษภาคม 2555, จาก http://www.thairath.co.th/content/pol/184129

[7] iLaw. (ม.ป.ป.). Case # 116: คดีปิดเว็บประชาไท. สืบค้นเมื่อ 7 พฤษภาคม 2555, จาก http://freedom.ilaw.or.th/th/case/116 ผลการศึกษาภาคที่ 1

การศึกษาสถิติที่เกี่ยวกับการบังคับใช้พ.ร.บ.คอมพิวเตอร์ฯ 2550 และสำรวจความคิดเห็นที่มีต่อการบังคับใช้กฎหมายดังกล่าวจากมุมมองเจ้าหน้าที่รัฐ และผู้ให้บริการหรือดูแลสื่อออนไลน์

[1] เนื่องจากพ.ร.บ.คอมพิวเตอร์ฯ 2550 มาตรา 20 กำหนดขั้นตอนการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ (วิธีปิดกั้นเว็บไซต์) โดยให้พนักงานเจ้าหน้าที่โดยความเห็นชอบของรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศ (ไอซีที) ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอคำสั่งระงับการเผยแพร่ข้อมูลคอมพิวเตอร์ได้ และศาลอาญาเป็นศาลที่มีเขตอำนาจทั่วราชอาณาจักร

[2] งานบริการข้อมูลคดี ศาลอาญา. (ม.ป.ป.). งานบริการข้อมูลคดี ศาลอาญา. สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://aryasearch.coj.go.th/aryaweb/main.php

[3] ต่อมาในปี 2553 เปลี่ยนชื่อเป็น สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ

[4] ประกาศคณะปฏิรูปการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข ฉบับที่ 5, “ตามที่คณะปฏิรูปการปกครองในระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็น ประมุขได้ทำการยึดอำนาจการปกครองแล้วนั้น จึงให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการควบคุม ยับยั้ง สกัดกั้น และทำลายการเผยแพร่ข้อมูลข่าวสารในระบบสารสนเทศ ผ่านระบบเครือข่ายการสื่อสารทั้งปวง ที่มีบทความ ข้อความ คำพูด หรืออื่นใด อันอาจส่งผลกระทบต่อการปฏิรูปการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข ตามที่คณะปฏิรูปการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข ได้มีประกาศไว้ในเบื้องต้นแล้ว - สั่ง ณ วันที่ 20 กันยายน พ.ศ. 2549”

[5] กิจกรรมวันอาทิตย์สีแดงเป็นกิจกรรมที่เริ่มต้นหลังเหตุการณ์สลายการชุมนุมในเดือนพฤษภาคม 2553 แต่ยังอยู่ในภาวะสถานการณ์ฉุกเฉิน เริ่มโดยนายสมบัติ บุญงามอนงค์ เป็นกิจกรรมรณรงค์ทางสัญลักษณ์ ให้เกิดการรวมตัวกันของคนเสื้อแดง, วิกิพีเดีย สารานุกรมเสรี. (ม.ป.ป.). กลุ่มวันอาทิตย์สีแดง. สืบค้นเมื่อ 29 กุมภาพันธ์ 2555, จาก http://th.wikipedia.org/wiki/กลุ่มวันอาทิตย์สีแดง

[6] นับแต่มีพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉินในปี 2548 รัฐบาลทุกรัฐบาลก็ประกาศพื้นที่ฉุกเฉินในสามจังหวัดภาคใต้มาอย่างต่อเนื่อง แต่อำนาจดังกล่าวไม่ได้ถูกนำมาใช้เพื่อปิดเว็บไซต์ดังที่ปรากฏในพื้นที่กรุงเทพฯ เมื่อปี 2553

[7] มาตรา 9 พระราชกำหนดบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548, “ในกรณีที่มีความจำเป็นเพื่อแก้ไขสถานการณ์ฉุกเฉินให้ยุติลงได้โดยเร็ว หรือป้องกันมิให้เกิดเหตุการณ์ร้ายแรงมากขึ้น ให้นายกรัฐมนตรีมีอำนาจออกข้อกำหนด ดังต่อไปนี้...

(3) ห้ามการเสนอข่าว การจำหน่าย หรือทำให้แพร่หลายซึ่งหนังสือ สิ่งพิมพ์ หรือสื่ออื่นใดที่มีข้อความอันอาจทำให้ประชาชนเกิดความหวาดกลัวหรือเจตนาบิดเบือนข้อมูลข่าวสารทำให้เกิดความเข้าใจผิดในสถานการณ์ฉุกเฉินจนกระทบต่อความมั่นคงของรัฐ หรือความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ทั้งในเขตพื้นที่ที่ประกาศสถานการณ์ฉุกเฉินหรือทั่วราชอาณาจักร...“

[8] เว็บไซต์บางแห่งที่ไม่มีเนื้อหาเกี่ยวกับการเมืองแต่ถูกปิดกั้นในช่วงประกาศสถานการณ์ฉุกเฉินไปด้วย เจ้าหน้าที่จากกระทรวงไอซีทีให้ข้อมูลว่า มีชาวต่างชาติโทรศัพท์ร้องเรียนเข้าไปยังกระทรวง ว่าเว็บไซต์ Justin.tv ซึ่งเป็นเว็บแบ่งปันไฟล์ ซึ่งไม่มีเนื้อหากระทบต่อความมั่นคงถูกปิดกั้นไปในช่วงเวลาดังกล่าวด้วย

[9] ยกตัวอย่างเช่น www.sanamluang.tv ซึ่งเป็นเว็บไซต์ทีวีออนไลน์ที่ถ่ายทอดข่าวงานกิจกรรมต่างๆ และถูกสั่งให้ปิดกั้นการเข้าถึงโดย คำสั่งศอฉ. ฉบับลงวันที่ 10 พฤษภาคม 2553 หรือ www.prachatai.com เว็บไซต์เสนอข่าวออนไลน์ โดยคำสั่งศอฉ. ฉบับลงวันที่ 7 เมษายน 2553 เป็นต้น

[10] ประชาไท. (2554, พฤศจิกายน 23). รมว. ไอซีทีเผย ขอเฟซบุ๊กปิดเพจหมิ่นฯ

แล้วกว่าหมื่นยูอาร์แอล. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://prachatai.com/journal/2011/11/38004

[11] ไทยรัฐออนไลน์. (2554, ธันวาคม 14). ได้ที 'เฉลิม' ของบ 400 ล้านบ. ซื้อเครื่องดักเว็บหมิ่นฯ. สืบค้นเมื่อ 14 ธันวาคม 2554, จาก http://www.thairath.co.th/content/pol/223580

[12] โพสต์ทูเดย์. (2554, ธันวาคม 8). เฟซบุ๊กร่วมบล็อกคนโพสต์หมิ่นแล้ว6หมื่นราย. สืบค้นเมื่อ 8 ธันวาคม 2554, จาก http://www.posttoday.com/อาชญากรรม/125948/เฟซบุ๊คร่วมบล็อกคนโพสต์หมิ่นแล้ว6หมื่นราย

[13] ประชาไท. (2554, ธันวาคม 9). ดูแนวทาง 'เฉลิม' ปราบเว็บหมิ่น จัดมาตรการ 'ขอร่วมมือ กฎหมาย และ...ประจาน'. สืบค้นเมื่อ 9 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2011/12/38245

[14] มาตรา 5 – 13 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550,

"มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 6 ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 8 ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 10 ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา 12 ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10

(1) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(2) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา 13 ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ"

[15] มาตรา 14 - 16 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, "มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

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

มาตรา 15 ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

มาตรา 16 ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย"

[16] มาตรา 423 ประมวลกฎหมายแพ่งและพาณิชย์, "ผู้ใดกล่าวหรือไขข่าวแพร่หลาย ซึ่งข้อความอันฝ่าฝืน ต่อความจริง เป็นที่เสียหายแก่ชื่อเสียงหรือเกียรติคุณของบุคคลอื่น ก็ดีหรือเป็นที่เสียหายแก่ทางทำมาหาได้ หรือทางเจริญของเขาโดย ประการอื่นก็ดี ท่านว่าผู้นั้นจะต้องใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อ ความเสียหายอย่างใดๆ อันเกิดแต่การนั้น แม้ทั้งเมื่อตนมิได้รู้ว่าข้อ ความนั้นไม่จริง แต่หากควรจะรู้ได้ ..."

[17] มาตรา 326 ประมวลกฎหมายอาญา, "ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สาม โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นหรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือ ปรับไม่เกินสองหมื่นบาทหรือทั้งจำทั้งปรับ"

[18] มาตรา 328 ประมวลกฎหมายอาญา, "ถ้าความผิดฐานหมิ่นประมาทได้กระทำโดยการโฆษณา ด้วยเอกสาร ภาพวาด ภาพระบายสี ภาพยนตร์ ภาพหรือตัวอักษรที่ ทำให้ปรากฏด้วยวิธีใดๆ แผ่นเสียง หรือสิ่งบันทึกเสียง บันทึกภาพ หรือบันทึกอักษร กระทำโดยการกระจายเสียง หรือการกระจายภาพ หรือโดยกระทำการป่าวประกาศด้วยวิธีอื่น ผู้กระทำต้องระวางโทษ จำคุกไม่เกินสองปีและปรับไม่เกินสองแสนบาท"

[19] มาตรา 1 (7) ประมวลกฎหมายอาญา "เอกสาร" หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผังหรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น

[20] บันทึกสำนักงานคณะกรรมการกฤษฎีกา ประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ... เรื่องเสร็จที่ 257/2548. (ม.ป.ป.). สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://www.dms.moph.go.th/dmsict/doc_file/policy.doc, หน้า 2

[21] รายละเอียดเพิ่มเติมเกี่ยวกับประเด็นปัญหาในทางกฎหมายและการใช้การตีความมาตรา 14 (1) โปรดดูในรายงานฉบับนี้ส่วนของบทวิเคราะห์กฎหมายไทย

[22] ประชาไท. (2555, พฤษภาคม 30). ศาลตัดสิน "ผอ.ประชาไท" ผิดคดีตัวกลาง สั่งจำคุกแต่ให้รอลงอาญา. สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://prachatai.com/node/40757

[23] มาตรา 287 ประมวลกฎหมายอาญา, "ผู้ใด

(1) เพื่อความประสงค์แห่งการค้า หรือโดยการค้าเพื่อการแจกจ่ายหรือเพื่อ การแสดงอวดแก่ประชาชน ทำ ผลิต มีไว้ นำเข้าหรือยังให้นำเข้าในราชอาณาจักร ส่งออก หรือยังให้ส่งออกไปนอกราชอาณาจักรพาไปหรือยังให้พาไปหรือทำให้แพร่หลายโดยประการใดๆ ซึ่งเอกสารภาพเขียน ภาพพิมพ์ ภาพระบายสี สิ่งพิมพ์ รูปภาพภาพโฆษณา เครื่องหมาย รูปถ่าย ภาพยนตร์ แถบบันทึกเสียงแถบบันทึกภาพหรือสิ่งอื่นใดอันลามก

(2) ประกอบการค้า หรือมีส่วนหรือเข้าเกี่ยวข้องในการค้าเกี่ยวกับวัตถุหรือสิ่งของ

ลามกดังกล่าวแล้ว จ่ายแจกหรือแสดงอวดแก่ประชาชนหรือให้เช่าวัตถุหรือสิ่งของเช่นว่านั้น

(3) เพื่อจะช่วยการทำให้แพร่หลาย หรือการค้าวัตถุหรือสิ่งของลามกดังกล่าวแล้ว โฆษณาหรือไขข่าวโดยประการใดๆ ว่ามีบุคคลกระทำการอันเป็นความผิดตามมาตรานี้ หรือโฆษณาหรือไขข่าวว่าวัตถุหรือสิ่งของลากดังกล่าวแล้วจะหาได้จากบุคคลใด หรือโดยวิธีใด

ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาทหรือทั้งจำทั้งปรับ"

[24] เดือนกันยายน 2552 มีการแบ่งส่วนราชการให้กองบังคับการนี้ถูกเปลี่ยนชื่อเป็นกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ

[25] ThaiLawtoday. (2552, กันยายน 7). กฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการอย่างอื่นในสำนักงานตำรวจแห่งชาติ พ.ศ.2552. สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://www.thailawtoday.com/laws-commentaries/1202--2552.html

[26] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547

[27] iLaw. ติดดาบดีเอสไอ. (2555, เมษายน 20). เพิ่ม 9 คดีพิเศษ ตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ. สืบค้นเมื่อ 20 เมษายน 2555, จาก http://ilaw.or.th/node/1465.

[28] Internet Service Provider-ISP หมายถึง ผู้ให้บริการอินเทอร์เน็ต

[29] มาตรา 18 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, "ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้

ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้"

[30] มาตรา 32 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547, "ในกรณีที่คณะกรรมการคดีพิเศษเห็นว่า เพื่อประสิทธิภาพในการปราบปรามการกระทำความผิดคดีพิเศษ คณะกรรมการคดีพิเศษจะให้ความเห็นชอบให้คดีพิเศษคดีหนึ่งคดีใดหรือคดีประเภทใดต้องมีพนักงานอัยการหรืออัยการทหาร แล้วแต่กรณี มาสอบสวนร่วมกับพนักงานสอบสวนคดีพิเศษหรือมาปฏิบัติหน้าที่ร่วมกับพนักงานสอบสวนคดีพิเศษเพื่อให้คำแนะนำและตรวจสอบพยานหลักฐานตั้งแต่ชั้นเริ่มการสอบสวน แล้วแต่กรณี ก็ได้ เว้นแต่การสอบสวนคดีพิเศษที่มีลักษณะอย่างหนึ่งอย่างใดตามมาตรา 21 วรรคหนึ่ง (1) (ค) หรือ (ง) ต้องมีพนักงานอัยการหรืออัยการทหารมาสอบสวนร่วมกับพนักงานสอบสวนคดีพิเศษทุกคดี แล้วแต่กรณี ทั้งนี้ การสอบสวนร่วมกันหรือการปฏิบัติหน้าที่ร่วมกันดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด"

[31] มาตรา 25 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547, "ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ พนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

(1) มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ

(2) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

(3) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวันโดยกำหนดเงื่อนไขใด ๆ ก็ได้ และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อพนักงานสอบสวนคดีพิเศษได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการ

ดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

บรรดาข้อมูลข่าวสารที่ได้มาตามวรรคหนึ่ง ให้เก็บรักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษซึ่งได้รับอนุญาตตามวรรคหนึ่ง และให้ใช้ประโยชน์ในการสืบสวนหรือใช้เป็นพยานหลักฐานเฉพาะในการดำเนินคดีพิเศษดังกล่าวเท่านั้น ส่วนข้อมูลข่าวสารอื่นให้ทำลายเสียทั้งสิ้น ทั้งนี้ ตามข้อบังคับที่คณะกรรมการคดีพิเศษกำหนด"

[32] *อ้างแล้ว 29*.

[33] มาตรา 26 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, "ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท"

[34] ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[35] ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ข้อ 3 ระบุว่า ในกรณีที่มีความจำเป็นเพื่อประโยชน์ของทางราชการในการสืบสวนและสอบสวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จำเป็นต้องมีบุคลากรซึ่งมีความรู้ ความชำนาญ หรือประสบการณ์สูง เพื่อดำเนินการสืบสวนและสอบสวนกระกระทำผิดหรือคดีเช่นว่านั้น หรือเป็นบุคลากรในสาขาที่ขาดแคลน รัฐมนตรีอาจยกเว้นคุณสมบัติตามข้อ 2 ไม่ว่าทั้งหมดหรือบางส่วนสำหรับการบรรจุและแต่งตั้งบุคคลใดเป็นการเฉพาะก็ได้

[36] มาตรา 20 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, "ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง

ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้"

[37] มาตรา 15 พ.ร.บ.คอมพิวเตอร์ฯ 2550ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

[38] คำว่าเว็บ 2.0 เป็นคำที่เกิดขึ้นในปี 2547 เกิดในการประชุมร่วมกันระหว่าง O'Reilly and MediaLive International หมายถึงยุคสมัยการสื่อสารที่เทคโนโลยีเอื้ออำนวยให้ผู้ใช้ทั่วไปเป็นผู้ส่งสาร, O'Reilly, Tim. (2005, September 30). What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. Retrieved March 3, 2012, from http://oreilly.com/web2/archive/what-is-web-20.html

[39] ตั้งแต่ปี 2524 เป็นต้นมา การระบุที่อยู่ของเครื่องคอมพิวเตอร์เมื่อเชื่อมต่ออินเทอร์เน็ตใช้ไอพีแอดเดรสเป็นตัวอ้างอิง โดยสังคมโลกใช้มาตรฐานอินเทอร์เน็ตโปรโตคอลเวอร์ชั่นที่สี่ (Internet Protocal version 4 - IPv4) ซึ่งมีช่องสัญญาณ 4 ช่อง 32 บิต (แบบ xxx.xxx.xxx.xxx) แต่การขยายตัวของอัตราการใช้อินเทอร์เน็ต ทำให้จำนวนไอพีแอดเดรสมีไม่เพียงพอ นำไปสู่การพัฒนาโปรโตคอลรุ่นใหม่ เรียกว่า อินเทอร์เน็ตโปรโตคอลเวอร์ชั่นที่หก (Internet Protocal version 6 - IPv6) ซึ่งมีช่องสัญญาณเพิ่มจากสี่ช่องเป็นหกช่อง และมี 128 บิต, SchoolNet. (2555, กุมภาพันธ์ 28). ไอพีวี 6 จุดเปลี่ยนโลกออนไลน์. สืบค้นเมื่อ 30 เมษายน 2555, จาก http://www.school.net.th/schoolnet/news/news_read.php?news_id=2945

กฎหมายไทย กับสิทธิเสรีภาพในสื่อออนไลน์

[1] มาตรา 26-27 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550, "มาตรา 26 การใช้อำนาจโดยองค์กรของรัฐทุกองค์กร ต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพตามบทบัญญัติแห่งรัฐธรรมนูญนี้

มาตรา 27 สิทธิและเสรีภาพที่รัฐธรรมนูญนี้รับรองไว้โดยชัดแจ้ง โดยปริยาย หรือโดยคำวินิจฉัยของศาลรัฐธรรมนูญ ย่อมได้รับความคุ้มครองและผูกพันรัฐสภา คณะรัฐมนตรี ศาล รวมทั้งองค์กรตามรัฐธรรมนูญ และหน่วยงานของรัฐโดยตรงในการตรากฎหมาย การใช้บังคับกฎหมาย และการตีความกฎหมายทั้งปวง"

[2] บวรศักดิ์ อุวรรณโณ, *กฎหมายมหาชนเล่ม 3 ที่มาและนิติวิธี,* (กรุงเทพฯ: นิติธรรม, 2538), หน้า 333.

[3] อ่านคำอธิบาย "หลักแห่งความได้สัดส่วน" กับการจำกัดสิทธิและเสรีภาพที่คุ้มครองตามรัฐธรรมนูญใน, ธีระ สุธีวรางกูร. การคุ้มครองสิทธิและเสรีภาพของบุคคลที่รัฐธรรมนูญรับรอง. *วารสารนิติศาสตร์,* 29(4), (2542). หน้า 587.

[4] ดู, วรพจน์ วิศรุตพิชญ์, *สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540*, (กรุงเทพฯ: วิญญูชน, 2543), หน้า 78.

[5] มาตรา 6 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550, "รัฐธรรมนูญเป็นกฎหมายสูงสุดของประเทศ บทบัญญัติใดของกฎหมาย กฎหรือข้อบังคับ ขัดหรือแย้งต่อรัฐธรรมนูญนี้ บทบัญญัตินั้นเป็นอันใช้บังคับมิได้"

[6] กฎหมาย 6 ฉบับนั้น ได้แก่ พระราชบัญญัติประกอบธุรกรรมทางอิเล็กทรอนิกส์, พระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์, พระราชบัญญัติเกี่ยวกับการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน (กฎหมายลำดับรองของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 78), พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, พระราชบัญญัติการโอนเงินทางอิเล็กทรอนิกส์ และพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ (เปลี่ยนชื่อเป็นพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในภายหลัง)

[7] ต่อมาได้รับการแก้ไขเพิ่มเติม และมีการยุบเอาเรื่องที่ว่าด้วย "ลายมือชื่ออิเล็กทรอนิกส์" (ซึ่งแผนเดิมต้องการยกร่างเป็นกฎหมายอีกฉบับหนึ่ง) รวมไว้ในกฎหมายฉบับเดียวกัน

[8] ร่างที่หนึ่ง พ.ศ. 2545 "ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์", ร่างที่สอง พ.ศ.2546 "ร่างพระราชบัญญัติว่าด้วยอาชญากรรมคอมพิวเตอร์", ร่างที่สาม พ.ศ.2548 "ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์" (ซึ่งเป็นฉบับที่ผ่านคณะกรรมการกฤษฎีกา และเข้าสู่การพิจารณาของคณะรัฐมนตรีเมื่อวันที่ 15 พฤศจิกายน 2549) และร่างที่สี่ พ.ศ.2549 "ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์" (ฉบับกรรมการวิสามัญพิจารณาร่างฯ ของสภานิติบัญญัติแห่งชาติ)

[9] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, *รวมร่างกฎหมายเทคโนโลยีสารสนเทศ ภายใต้โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ*, (กรุงเทพฯ: โรงพิมพ์เดือนตุลาคม, 2544), หน้า 9.

[10] ประชาไท. (2549, พฤศจิกายน 19). สนช.ลงมติรับหลักการร่าง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.... วาระแรก. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.prachatai.com/journal/2006/11/10527

[11] ดูสรุปปัญหาบทนิยามของคำว่า "ผู้ให้บริการ" ซึ่งรวบรวมจากการประชุมร่างกฎหมายและการให้เหตุผลโดยกลุ่มผู้ประกอบการอินเทอร์เน็ตที่, เช กูวารา (นามแฝง). (2555, ตุลาคม 24). กฎหมาย ที่ร่างกันแบบไม่เร่ง แต่ผ่านกันแบบรีบ ๆ (ตอน 1-5). *iLaw* สืบค้นเมื่อ 24 ตุลาคม 2555 จาก http://ilaw.or.th/node/1748

[12] ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550, ตามความแห่งข้อ 5 ของประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 กำหนดว่า

1. ผู้ให้บริการแก่บุคคลทั่วไปในการ เข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกัน โดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ 4 ประเภท ดังนี้

ก) ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication

and Broadcast Carrier)

ข) ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)

ค) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ (Host Service Provider)

ง) ผู้ให้บริการร้านอินเทอร์เน็ต

2. ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของผู้ใช้ในข้อ 1 (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่าง ๆ (Application Service Provider)

[13] บันทึกสำนักงานคณะกรรมการกฤษฎีกา ประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ... เรื่องเสร็จที่ 257/2548. (ม.ป.ป.). สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://www.dms.moph.go.th/dmsict/doc_file/policy.doc, หน้า 12

[14] คดีที่ฟ้องตามมาตรา 14 (1) โดยมากเป็นเนื้อหาหมิ่นประมาท กล่าวข้อความเท็จ รวมถึงความเท็จที่หวังผลเพื่อฉ้อโกง เช่น โพสต์ข้อความในเว็บบอร์ดว่าจะขายของแต่เมื่อผู้ซื้อโอนเงินไปให้กลับไม่มีการส่งของให้ตามตกลง อย่างไรก็ดี ในงานวิจัยนี้มุ่งศึกษาผลจากกฎหมายที่ส่วนที่กระทบต่อสิทธิเสรีภาพในการแสดงความคิดเห็นเท่านั้น ตัวอย่าง คดีหมิ่นประมาท เช่น กรณีของ ปรียานันท์ ล้อเสริมวัฒนา ประธานเครือข่ายผู้เสียหายทางการแพทย์ นักกิจกรรมด้านสิทธิผู้ป่วย ที่เผยแพร่รูปภาพและกราฟแสดงสถิติผู้ป่วยที่เสียชีวิตจากความผิดพลาดในการให้การรักษา ผ่านทางเฟซบุคและเว็บไซต์อื่น ๆ ยังผลให้กลุ่มวิชาชีพแพทย์จำนวนมากออกมาโต้แย้งคัดค้าน โดยมีแพทย์หญิงประชุมพร บูรณ์เจริญ ประธานสมาพันธ์แพทย์โรงพยาบาล ศูนย์โรงพยาบาลทั่วไปแจ้งความร้องทุกข์ที่สถานีตำรวจภูธรสุรินทร์ ด้วยข้อกล่าวหาว่าเป็นการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จ ทั้งนี้ คดียังอยู่ในระหว่างการพิจารณา

[15] มาตรา 1 (7) ประมวลกฎหมายอาญา, “เอกสาร” หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผังหรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น

[16] “บันทึกสำนักงานคณะกรรมการกฤษฎีกา ประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ....เรื่องเสร็จที่ 257/2548”, *อ้างแล้ว 13*, หน้า. 2.

[17] ดูคำอธิบายเรื่องความผิดในฐานปลอมเอกสารใน จิตติ ติงศภัทิย์, *คำอธิบายประมวลกฎหมายอาญา, ภาค 2 ตอน 1*, พิมพ์ครั้งที่ 7, (กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา), หน้า 592 – 594.

[18] มาตรา 329 ประมวลกฎหมายอาญา, “ผู้ใดแสดงความคิดเห็นหรือข้อความใดโดยสุจริต

(1) เพื่อความชอบธรรม ป้องกันตนหรือป้องกันส่วนได้เสียเกี่ยวกับตนตามคลองธรรม

(2) ในฐานะเป็นเจ้าพนักงานปฏิบัติการตามหน้าที่

(3) ติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ หรือ

(4) ในการแจ้งข่าวด้วยความเป็นธรรมเรื่องการดำเนินการอันเปิดเผยในศาลหรือในการประชุม

ผู้นั้นไม่มีความผิดฐานหมิ่นประมาท

[19] หลัก “ไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย” ซึ่งระบบกฎหมายไทยก็รับมาใช้ และบัญญัติรับรองไว้ทั้งในประมวลกฎหมายอาญา มาตรา 2 ความว่า “บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการ อันกฎหมายที่ใช้ในขณะกระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้และโทษที่จะลงแก่ผู้กระทำความผิดนั้น ต้องเป็นโทษที่ บัญญัติไว้ในกฎหมาย ถ้าตามบทบัญญัติของกฎหมายที่บัญญัติในภายหลังการกระทำ เช่นนั้นไม่เป็นความผิดต่อไป ให้ผู้ที่ได้กระทำการนั้นพ้นจากการ เป็นผู้กระทำความผิด และถ้าได้มีคำพิพากษาถึงที่สุดให้ลงโทษแล้ว ก็ให้ถือว่าผู้นั้นไม่เคยต้องคำพิพากษาว่าได้กระทำความผิดนั้น ถ้ารับ โทษอยู่ก็ให้การลงโทษนั้นสิ้นสุดลง”

[20] ดู, คณิต ณ นคร, *กฎหมายอาญาภาคทั่วไป*, พิมพ์ครั้งที่ 3, (กรุงเทพฯ: วิญญูชน, 2551), หน้า 72.

[21] ความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร ตั้งแต่มาตรา 107 -135 ความผิดเกี่ยวกับการก่อการร้าย ตั้งแต่มาตรา 135/1 – 135/4 ประมวลกฎหมายอาญา

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

[23] มาตรา 326 ประมวลกฎหมายอาญา, “ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สาม โดยประการที่น่าจะ ทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นหรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือ ปรับไม่เกินสองหมื่นบาทหรือทั้งจำทั้งปรับ”

[24] มาตรา 329 ประมวลกฎหมายอาญา, *อ้างแล้ว 18*.

[25] มาตรา 330 ประมวลกฎหมายอาญา, “ในกรณีหมิ่นประมาท ถ้าผู้ถูกหาว่ากระทำความผิด พิสูจน์ได้ว่าข้อที่หาว่าเป็นหมิ่นประมาทนั้นเป็นความจริง ผู้นั้นไม่ต้อง รับโทษ

แต่ห้ามไม่ให้พิสูจน์ ถ้าข้อที่หาว่าเป็นหมิ่นประมาทนั้นเป็นการใส่ ความในเรื่องส่วนตัว และการพิสูจน์จะไม่เป็นประโยชน์แก่ประชาชน”

[26] ดูรายละเอียดเกี่ยวกับปัญหาของมาตรา 112 รวมทั้งประเด็นที่ควรปรับปรุงแก้ไขได้ที่ นิติราษฎร์: นิติศาสตร์เพื่อราษฎร. (2554, ธันวาคม 26). ข้อเสนอเพื่อการรณรงค์แก้ไขเพิ่มเติมประมวลกฎหมายอาญามาตรา 112. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.enlightened-jurists.com/download/67

[27] มาตรา 86 ประมวลกฎหมายอาญา, “ผู้ใดกระทำด้วยประการใดๆ อันเป็นการช่วยเหลือหรือให้ความสะดวกในการที่ผู้อื่นกระทำความผิดก่อนหรือขณะกระทำความผิด แม้ผู้กระทำความผิดจะมิได้รู้ถึงการช่วยเหลือหรือให้ความสะดวกนั้นก็ตาม ผู้นั้นเป็นผู้สนับสนุนการกระทำความผิด ต้องระวางโทษสองในสามส่วนของโทษที่กำหนดไว้สำหรับความผิดที่สนับสนุนนั้น”

[28] ดูสถิติการพิจารณาเพื่อสั่งปิดกั้นเว็บไซต์ได้ในผลการรายงานส่วนที่หนึ่ง

[29] ดู, คณะวิจัยผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น. (2553, ธันวาคม 8). รายงานสถานการณ์ การควบคุมและปิดกั้นสื่อออนไลน์ ด้วยการอ้างกฎหมายและแนวนโยบายแห่งรัฐไทย. *iLaw*. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.scribd.com/doc/44961877/รายงานสถานการณ์การควบคุมและปิดกั้นสื่อออนไลน์ด้วยการอ้างกฎหมายและแนวนโยบายแห่งรัฐไทย, หน้า 13.

[30] มาตรา 287 ประมวลกฎหมายอาญา, ผู้ใด

(1) เพื่อความประสงค์แห่งการค้า หรือโดยการค้า เพื่อการแจกจ่ายหรือเพื่อการแสดงอวดแก่ประชาชน ทำ ผลิต มีไว้ นำเข้าหรือยังให้นำเข้าในราชอาณาจักร ส่งออกหรือยังให้ส่งออกไปนอกราชอาณาจักร พาไปหรือยังให้พาไปหรือทำให้แพร่หลายโดยประการใดๆ ซึ่งเอกสาร ภาพเขียน ภาพพิมพ์ ภาพระบายสี สิ่งพิมพ์ รูปภาพ ภาพโฆษณา เครื่องหมาย รูปถ่าย ภาพยนตร์ แถบบันทึกเสียง แถบบันทึกภาพหรือสิ่งอื่นใดอันลามก

(2) ประกอบการค้า หรือมีส่วนหรือเข้าเกี่ยวข้องในการค้าเกี่ยวกับวัตถุหรือสิ่งของลามกดังกล่าวแล้ว จ่ายแจกหรือแสดงอวดแก่ประชาชน หรือให้เช่าวัตถุหรือสิ่งของเช่นว่านั้น

(3) เพื่อจะช่วยการทำให้แพร่หลาย หรือการค้าวัตถุหรือสิ่งของลามกดังกล่าวแล้ว โฆษณาหรือไขข่าวโดยประการใดๆ ว่ามีบุคคลกระทำการอันเป็นความผิดตามมาตรานี้ หรือโฆษณาหรือไขข่าวว่าวัตถุ หรือสิ่งของลามกดังกล่าวแล้วจะหาได้จากบุคคลใด หรือโดยวิธีใด

ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ

[31] อาทิ ประเทศญี่ปุ่น แก้ไขเพิ่มเติมความผิดฐานเผยแพร่ภาพลามกเด็กที่เป็นข้อมูลดิจิตอลไว้ใน Penal Code of Japan และ Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children ทำนองเดียวกับกฎหมายฮ่องกงที่บัญญัติเรื่องดังกล่าวไว้ใน Control of Obscene and Indecent Articles Ordinance แทนที่จะอยู่ใน Computer Crimes Ordinance 1993 หรือ Telecommunication Ordinance 1993 ส่วนประเทศฟิลิปปินส์ มีแผนที่จะบัญญัติเรื่องนี้ไว้ที่ Anti-Child Pornography ซึ่งไม่ใช่กฎหมายคอมพิวเตอร์อย่าง Electronic Commerce ACT 2000 ในขณะที่ประเทศสหพันธรัฐเยอรมนี แก้ไขเพิ่มเติมบทดังกล่าวไว้ในประมวลกฎหมายอาญา (Strafgesetzbuch) แต่ไม่มีการแก้ไขเพิ่มเติมบทบัญญัติเกี่ยวกับการเผยแพร่เนื้อหาดูถูกเชื้อชาติ (racism) เพราะเป็นความผิดที่ใช้บังคับได้กับสื่อทุกประเภทอยู่แล้วตามประมวลกฎหมายอาญา เป็นต้น

[32] คมชัดลึก. (ม.ป.ป.). สนช. ผ่านร่าง พรบ. ว่าด้วยการกระทำผิดคอมพิวเตอร์. สืบค้นเมื่อ 15 ตุลาคม 2554, จาก http://.komchadluek.com

[33] ประกาศ คปค.ฉบับที่ 5 (ประกาศวันที่ 20 กันยายน พ.ศ. 2549) มีขึ้นเพื่อวัตถุประสงค์ในการควบคุมการเผยแพร่ข้อมูลข่าวสารระบบเทคโนโลยีสารสนเทศภายหลังการรัฐประหาร 19 กันยายน 2549 ความว่า “ตามที่คณะปฏิรูปการปกครองในระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข ได้ทำการยึดอำนาจการปกครองแล้วนั้น จึงให้กระทรวงเทคโนโลยี

สารสนเทศและการสื่อสาร ดำเนินการควบคุม ยับยั้ง สกัดกั้น และทำลาย การเผยแพร่ข้อมูลข่าวสารในระบบสารสนเทศ ผ่านระบบเครือข่ายการสื่อสารทั้งปวง ที่มีบทความ ข้อความ คำพูด หรืออื่นใด อันอาจส่งผลกระทบต่อการปฏิรูปการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข ตามที่ คณะปฏิรูปการปกครองในระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข ได้มีประกาศไว้ในเบื้องต้นแล้ว”

[34] ไทยรัฐออนไลน์. (2550, มกราคม 30).ไอซีทีบล็อกแคมฟรอกแล้ว หลังโจ๋ไทยไม่หยุดโชว์. อ้างใน *news.sanook*. สืบค้นเมื่อ 5 ตุลาคม 2555 จาก http://news.sanook.com/crime/crime_88511.php

[35] เดลินิวส์. (2550, มกราคม 9). ไอซีทีเผยไล่บล็อกเว็บโป๊แล้วกว่าหมื่น! หนักใจเว็บนอกคุมยาก. อ้างใน *TLCNews*. สืบค้นเมื่อ 5 ตุลาคม 2554, จาก http://news.tlcthai.com/news-interest/112.html

[36] สยามจดหมายเหตุ. (ม.ป.ป.). สั่งปิดเว็บไซต์แพร่คลิปวิดีโอหมิ่นพระบรมเดชานุภาพ. สืบค้นเมื่อ 5 ตุลาคม 2554, จาก http://www.siamarchives.com/สั่งปิดเว็บไซต์แพร่คลิ/

[37] ไทยรัฐออนไลน์. (2550, พฤษภาคม 30). ถูกหาละเมิดสิทธิ ‘สิทธิชัย’ ยกสถิติปิด เว็บ 2 รบ.เปรียบเทียบ. อ้างใน *MakeWebExy.com* สืบค้นเมื่อ 30 กรกฎาคม 2554, จาก http://www.makewebez.com/tips/index.php?page=show&id=233

[38] สำนักข่าวไทย. (ม.ป.ป.). ยกเลิกประกาศคปค. ฉบับที่ 5 เรื่องควบคุมเว็บไซต์. อ้างใน *oxygen*. สืบค้นเมื่อ 30 กรกฎาคม 2554, จาก http://oxygen.readyplanet.com/index.php?lay=show&ac=article&Id=416946&Ntype=20

[39] โลโก้พระพุทธเจ้า“เว็บ”ลามก“พระ”เปิดเจอ-ร้องจ๊าก. *ข่าวสด*. (2550, มกราคม 8). หน้า 1.

[40] กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย. (2551, มีนาคม 18). “แฮค & แครก” เว็บหมิ่น ไอซีทีรู้ผิดกฎหมายแต่จะทำ. สืบค้นเมื่อ 18 สิงหาคม 2554, จาก http://facthai.wordpress.com/2008/03/18/ict-to-hack-and-crack-thai/

[41] คมชัดลึก. (2551, มิถุนายน 10). มั่น พัธโนทัยไอซีทีคอร์ปผู้ปิดทองหลังพระ. อ้างใน *news.sanook*. สืบค้นเมื่อ 9 ตุลาคม 2554, จาก http://news.sanook.com/politic/politic_276054.php

[42] ประชาชาติธุรกิจออนไลน์. (ม.ป.ป.). ยกเครื่องมาตรการสกัดเว็บต้องห้าม. อ้างใน *decha.com*. สืบค้นเมื่อ 9 ตุลาคม 2554, จาก http://www.decha.com/main/showTopic.php?id=2737

[43] สำนักข่าวอินโฟเควสท์ (IQ). (2551, ตุลาคม 28). รมว.ไอซีที เล็งซื้ออุปกรณ์บล็อคเว็บหมิ่นสถาบัน 100-500 ลบ./เครื่อง. อ้างใน *RYT9*. สืบค้นเมื่อ 10 ตุลาคม 2554, จาก http://www.ryt9.com/s/iq02/458881

[44] กรุงเทพธุรกิจออนไลน์. (2551, พฤศจิกายน 7). ไอซีทีออก 5 มาตรการด้านเว็บหมิ่น. สืบค้นเมื่อ 10 ตุลาคม 2554, จาก http://www.bangkokbiznews.com/2008/11/07/news_309786.php

[45] ASTVผู้จัดการออนไลน์. (2552, กุมภาพันธ์ 5). ระนองรักษ์ ตั้ง ISOC สกัดเว็บหมิ่น – ยันไม่ปิดไฮไฟว์. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.manager.co.th/cyberbiz/ViewNews.aspx?NewsID=9520000013365

[46] ประชาไท. (2554, ธันวาคม 1). ไอซีทีเปิดตัวศูนย์ความมั่นคงไซเบอร์ สุดเข้ม ปราบเว็บหมิ่นฯ สถาบัน. สืบค้นเมื่อ 20 มกราคม 2555, จาก http://prachatai.com/journal/2011/12/38121

[47] ไทยรัฐออนไลน์. (2552, เมษายน 24). 'ระนองรักษ์' ตื่นลุยปราบผู้ใช้เน็ตป่วนชาติ. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.thairath.co.th/content/tech/1669

[48] เดลินิวส์. (2552, กรกฎาคม 29). ไอซีทีอวดผลงานศูนย์ปฏิบัติการปลอดภัยเน็ต. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.dailynews.co.th/technology/32235

[49] newswit. (2552, กันยายน 15). รมว.ไอซีที แถลงความคืบหน้าผลงานกระทรวงไอซีที. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.newswit.com/gen/2009-09-15/4eda0e4334ccee57a7e26008d6635d23

[50] ไทยรัฐออนไลน์. (2552, เมษายน 24). ระนองรักษ์...ตื่นลุยปราบผู้ใช้เน็ตป่วนชาติ, *อ้างแล้ว 47*.

[51] กรุงเทพธุรกิจออนไลน์. (2553, เมษายน 9). รัฐลุยปิด"พีทีวี-บล็อกเว็บไซต์" แดงประกาศแผนตอบโต้วันนี้. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.bangkokbiznews.com/2010/04/09/news_30664968.php

[52] ประชาไท. (2552, กันยายน 4). ย้ำ !! กทช.มีอำนาจเต็มถอน-พักใบอนุญาตไอเอสพี ไม่ปิดกั้นเว็บไม่เหมาะสม. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://prachatai.com/journal/2009/09/25693

[53] ฐานเศรษฐกิจ. (2553, มกราคม 22). ไอซีที เตรียมบังคับ ISP ติดตั้ง Sniffer ดักข้อมูลของไทย. อ้างใน *RMUTL NOC*. สืบค้นเมื่อ 9 มกราคม 2555, จาก http://noc.rmutl.ac.th/main/?p=761

[54] ASTVผู้จัดการออนไลน์. (2553, มกราคม 21). ไอซีทียันดักข้อมูลชาวเน็ตไทยไม่ละเมิด "ประเทศไหนๆก็ติด Sniffer". สืบค้นเมื่อ 9 มกราคม 2555, จาก http://www.manager.co.th/cyberbiz/ViewNews.aspx?NewsID=9530000009163

[55] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (ม.ป.ป.). รมว.ไอซีที แถลงนโยบาย 1 ปี เร่งผลักดันธุรกรรมทางอิเล็กทรอนิกส์ และถนนไร้สาย. สืบค้นเมื่อ 9 มกราคม 2555, จาก http://www.mict.go.th/ewt_news.php?nid=3360&filename=index

[56] ASTVผู้จัดการออนไลน์. (2553, มิถุนายน 18). สั่งปิด 4.3 หมื่นเว็บหมิ่น 3 กระทรวงร่วมป้องสถาบัน. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9530000083941

[57] *เพิ่งอ้าง*

[58] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (ม.ป.ป.). นายกรัฐมนตรี เปิดโครงการ

Cyber Scout หนุน ก.ไอซีที สร้างลูกเสือดูแลโลกออนไลน์. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.mict.go.th/ewt_news.php?nid=3430&filename=index

[59] สุกรี แมนชัยนิมิต. (2554, กรกฎาคม 30). โมเดลสหรัฐฯ – สิงคโปร์. Positioning. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.positioningmag.com/magazine/details.aspx?id=92268

สำนักข่าวไทย. (2554, เมษายน 22). สื่อสังคมออนไลน์มีบทบาทต่อการเลือกตั้งสิงคโปร์เดือนหน้า. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.mcot.net/cfcustom/cache_page/199287.html

[60] ไอเอ็นเอ็น. (ม.ป.ป.). ไอซีทีเตรียมวางกรอบหาเสียงผ่านสังคมออนไลน์. อ้างใน *hilight.kapook*. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://hilight.kapook.com/view/59263

[61] MThai. (2554, มิถุนายน 30). เตือน ! ห้ามหาเสียงออนไลน์ทั้งทวิตเตอร์ โพสต์เฟส คืนหมาหอน. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://news.mthai.com/politics-news/120492.html

[62] ประชาไท. (2554, เมษายน 18). สัมภาษณ์ อรพิณ ยิ่งยงพัฒนา: ทำไมต้องต้าน พ.ร.บ. คอมฯ ฉบับใหม่. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://prachatai.com/journal/2011/04/34110

[63] ดูรายละเอียดใน สาวตรี สุขศรี. บทวิเคราะห์ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.... *วารสารกสทช*. 2554(1). 267-285.

[64] ไอเอ็นเอ็น. (ม.ป.ป.). นายกฯ ชะลอร่างพ.ร.บ.คอมพิวเตอร์. อ้างใน *hilight.kapook*. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://hilight.kapook.com/view/58062

[65] ดูสถิติคดีความผิดที่เกี่ยวกับคอมพิวเตอร์ได้ในรายงานวิจัยฉบับนี้

[66] ASTVผู้จัดการออนไลน์. (2554, สิงหาคม 23). อนุดิษฐ์ลั่น 5 นโยบาย กระทรวงไอซีที. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://www.manager.co.th/cyberbiz/ViewNews.aspx?NewsID=9540000106190

[67] กรุงเทพธุรกิจออนไลน์. (2554, กันยายน 12). อนุดิษฐ์ นาครทรรพ 8 คำตอบกับคำถามคาใจ. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://www.bangkokbiznews.com/home/detail/it/it/20110912/408928/อนุดิษฐ์-นาครทรรพ-8-คำตอบกับคำถามคาใจ.html

[68] ประชาไท. (2554, พฤศจิกายน 23). รมว. ไอซีทีเผย ขอเฟซบุ๊กปิดเพจหมิ่นฯ แล้วกว่าหมื่นยูอาร์แอล. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://prachatai.com/journal/2011/11/38004

[69] MThai. (2554, พฤศจิกายน 25). รมว.ไอซีที เตือนประชาชน อย่ากด Like Comment เว็บหมิ่นสถาบันฯ. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://news.mthai.com/general-news/142656.html

ประชาไท. (2554, ธันวาคม 30). ไอซีที ย้ำอีก นักท่องเว็บอย่า 'ไลค์-แชร์-เม้นต์' เว็บหมิ่นฯ. สืบค้นเมื่อ 20 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/12/38534

[70] ไทยโพสต์. (2554, ตุลาคม 9). มาตรฐานเดียว น.อ.อนุดิษฐ์ นาครทรรพ. สืบค้นเมื่อ 12 พฤศจิกายน 2554, จาก http://www.thaipost.net/node/46277

[71] ASTVผู้จัดการออนไลน์. (2554, ตุลาคม 10). อนุดิษฐ์ รับสิ้นปี wifi ฟรี 2 หมื่นจุด. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9540000128730

[72] MThai. (2554, พฤศจิกายน 26). ประชาธิปัตย์ แนะแบน ยูทูบ-เฟซบุ๊ก แบบจีนสกัดเว็บหมิ่นฯ. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://news.mthai.com/headline-news/142706.html

คมชัดลึก. (2555, มกราคม 27). มัลลิกา โวย รัฐเมินปราบเว็บหมิ่นฯ. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://www.komchadluek.net/detail/20120127/121412/มัลลิกาโวยรัฐเมินปราบเว็บหมิ่นฯ.html

มติชนออนไลน์. (2555, มกราคม 27). มัลลิกา ขู่ฟ้องรัฐบาลละเว้นการปฏิบัติหน้าที่หลังคดีเว็บหมิ่นไม่คืบ. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://www.matichon.co.th/news_detail.php?newsid=1327662962&grpid=03&catid=03

[73] ดูรายละเอียดเกี่ยวกับการปิดกั้นเว็บไซต์ก่อนพ.ร.บ.คอมพิวเตอร์ ฯ มีผลบังคับใช้ และการตั้งคำถามจากภาคประชาชนถึงการใช้อำนาจดังกล่าวของรัฐใน กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย. (2549, พฤศจิกายน 22). คำร้องต่อคณะกรรมการสิทธิมนุษยชนแห่งชาติ. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://facthai.wordpress.com/2006/11/22/a-petition-to-the-national-human-rights-commission-thai/

[74] Freedom House, http://www.freedomhouse.org/

[75] Sanja Kelly & Sarah Cook. [Eds.]. (2011, April 18). Freedom on the Net 2011: A Global Assessment of Internet and Digital Media. Retrieved June 30, 2012, from http://www.freedomhouse.org/sites/default/files/FOTN2011.pdf, p. 310-320.

MarkJ. (2011, April 18). UPDATE Freedom House Warns UK Internet Users at Risk of Growing Censorship. Retrieved June 6, 2012, from http://www.ispreview.co.uk/story/2011/04/18/freedom-house-warns-uk-internet-users-at-risk-of-growing-censorship.html

[76] กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย. (2550, มีนาคม 25). ข้อเสนอของ FACT ต่อ “ร่าง พ.ร.บ.ความผิดเกี่ยวกับคอมพิวเตอร์. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://facthai.wordpress.com/2007/03/25/facts-formal-recommendations-for-cybercrime-bill-thai/

[77] เดลินิวส์. (2551, สิงหาคม 30). คนบันเทิงชอบใจ พ.ร.บ.คอมพิวเตอร์ฯ 2550. อ้างใน *teenee*. เข้าถึงเมื่อ20 ธันวาคม 2554, จาก http://entertain.teenee.com/thaistar/25224.html

[78] สำนักข่าวชาวบ้าน. (ม.ป.ป.). ชาวไซเบอร์?บ่นพ.ร.บ.คอมลิดรอนสิทธิ. สืบค้นเมื่อ 17/12/2554, จาก http://www.peoplepress.in.th/archives/autopagev3/show_page.

php?group_id=1&auto_id=19&topic_id=1060&topic_no=21&page=1&gaction=on

[79] Darknews. (2552, พฤศจิกายน). พ.ร.บ.คอมพิวเตอร์ฯ – เครื่องมือการเมือง. *OK Natoin Blog*. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://www.oknation.net/blog/print.php?id=520872

[80] ASTVผู้จัดการออนไลน์. (2551, กรกฎาคม 22). ประเมิน พ.ร.บ.คอมพ์แค่เครื่องมือของรัฐ. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9510000085990

[81] เครือข่ายพลเมืองเน็ต. (2552, พฤศจิกายน 9). แถลงการณ์ เรื่อง การร้องขอความชัดเจนกรณีใช้ พ.ร.บ.คอมพิวเตอร์ฯ จับกุมผู้ใช้เน็ตในเดือนตุลาคม 2552. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://thainetizen.org/2009/11/statement-on-computer-crime-oct-2009/

[82] มติชนออนไลน์. (2552, พฤศจิกายน 18). ตร.จับเพิ่มอีกแพทย์หญิง รพ.ดัง ร่วมแพร่ข่าวลือทุบหุ้น. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://www.matichon.co.th/news_detail.php?newsid=1258551109&grpid=03&catid

[83] เครือข่ายพลเมืองเน็ต. (2552, พฤศจิกายน 9), *อ้างแล้ว 81*.

[84] ประชาไท. (2552, พฤศจิกายน 8). ชุมชน “ฟ้าเดียวกัน” ออกแถลงการณ์ประณามการการจับแพะกรณีทุบหุ้น. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2009/11/26510

[85] ประชาไท. (2552, พฤศจิกายน 25). สมัชชาสังคมก้าวหน้าเรียกร้องผู้รักเสรีภาพต่อต้าน พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์. สืบค้นเมื่อ 3 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2009/11/26744

[86] DJ. อ้น ประชาชื่น (วิทยุชุมชนคนแท็กซี่). (2552, พฤศจิกายน 11). สถานการณ์การใช้อำนาจรัฐกรณี พ.ร.บ. คอมพิวเตอร์อีกเกมหนึ่งของอำมาตย์ เกมกำจัดคู่แข่งการเมือง. *ประชาไท*. สืบค้นเมื่อ 3 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2009/11/26541

[87] ประชาไท. (2553, กันยายน 27). แถลงการณ์เครือข่ายนักสิทธิฯ ร้องยุติการดำเนินคดีที่ไม่เป็นธรรม ผอ.เว็บประชาไท. สืบค้นเมื่อ 3 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2010/09/31277

[88] ประชาไท. (2553, ตุลาคม 20). เครือข่ายพลเมืองเน็ตจี้ ส.ส.แก้ด่วน ม.15 ‘จับแพะ’ พรบ.คอมพิวเตอร์. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2010/10/31556

[89] ประชาไท. (2554, กุมภาพันธ์ 11). แอมเนสตี้ฯ เรียกร้อง รบ.ไทยยกฟ้องทุกข้อกล่าวหาต่อ ผอ.ประชาไท. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2011/02/33063

[90] ประชาไท. (2554, กุมภาพันธ์ 2ข). ผู้สื่อข่าวไร้พรมแดนแถลงเรียกร้องรัฐไทยถอนฟ้องคดีผอ. ประชาไท. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/

journal/2011/02/32923

[91] ประชาไท. (2554, กุมภาพันธ์ 2ก). 11 ส.ส.อังกฤษ ลงชื่อหนุน ผอ.ประชาไท เตือน รบ.ไทย ส่อลิดรอนเสรีภาพ ปชช. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2011/02/32915

[92] ประชาไท. (2553, กันยายน 24). ชมรมนักข่าวเพื่อเสรีภาพแถลงประณามกรณีจับผอ.ประชาไท. สืบค้นเมื่อ 24 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2010/09/31240

[93] Siam Intelligence Unit. (2552, มีนาคม 27). ถก พรบ.คอมพิวเตอร์ ยังขัดแย้ง มุมมองจากรัฐและภาคประชาชน. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.siamintelligence.com/computer-crime-act-tja-discussion/

[94] ไทยเอ็นจีโอ. (2553, สิงหาคม 2). 3 ปี พรบ.คอมฯ รัฐไทยยังสืบสานแนวคิดอำนาจนิยมและละเมิดสิทธิเสรีภาพประชาชน. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.thaingo.org/writer/view.php?id=1656

[95] เครือข่ายพลเมืองเน็ต. (2552, กรกฎาคม 27). ข้อเสนอเครือข่ายพลเมืองเน็ตต่อการบังคับใช้กฎหมายกับคดีทางคอมพิวเตอร์และอินเทอร์เน็ต. สืบค้นเมื่อ19 มกราคม 2555, จาก http://thainetizen.org/docs/netizen-press-20090727/

[96] iLaw. (2553, กรกฎาคม 23). นายกสมาคมสื่อแนะ ยื่นพ.ร.บ.คอมพิวเตอร์ให้ศาลรธน. ตีความ. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://ilaw.or.th/node/433

[97] ประชาไท. (2554, ตุลาคม 11). เอ็นจีโอสรุปเวทียูเอ็น รัฐไทยปัดตกประเด็นร้อน รับ 100 ข้อจาก 172. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/10/37341

[98] ประชาไท. (2552, ธันวาคม 6). องค์กรผู้สื่อข่าวไร้พรมแดนเรียกร้องขอพระราชทานอภัยโทษแก่ผู้ใช้อินเทอร์เน็ตที่โดนตั้งข้อหาหมิ่นฯ. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2009/12/26888

[99] ประชาไท. (2554, มิถุนายน 8). UNHRC ถกประเด็นไทยละเมิดเสรีภาพออนไลน์และสิทธิแรงงานข้ามชาติ. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/06/35324

[100] เครือข่ายพลเมืองเน็ต. (2554, มิถุนายน 22). ประชาสังคมอาเซียน: หยุด “คิด” ก่อนเซ็นเซอร์อินเทอร์เน็ต. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://thainetizen.org/2011/06/asean-think-before-censor-internet/

[101] iLaw. (2554, ตุลาคม 14). รอบอาทิตย์ที่สอง ต.ค. 54: UN ย้ำไทยต้องแก้กฎหมายหมิ่น พ.ร.บ.คอม. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://ilaw.or.th/node/1225

[102] ประชาไท. (2554, กันยายน 16). บรรษัทระดับโลกหวั่นมาตรการควบคุมเน็ตในไทย ทำธุรกิจชะงัก. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/09/36956

[103] ประชาชาติธุรกิจออนไลน์. (2554, เมษายน 20). รุมต้านร่างพ.ร.บ.คอมพ์ฉบับใหม่ กม.คุมเข้มครอบจักรวาล "ธุรกิจ-คนใช้เน็ต"เสี่ยงคุก!!. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachachat.net/news_detail.php?newsid=1303289856&grpid=03&catid=06

[104] iLaw. (2554, พฤษภาคม 5). อัด ร่าง พ.ร.บ.คอมฯใหม่ "ซักซื้อ-ห่วยขั้นเทพ" มั่วเรื่องลิขสิทธิ์. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://ilaw.or.th/node/921

[105] ประชาไท. (2554, เมษายน 17). iLaw ล่าชื่อ หยุดร่าง พ.ร.บ.คอมฯฉบับใหม่ ก่อนเข้าครม. สืบค้นเมื่อ 18 เมษายน 2554, จาก http://prachatai.com/journal/2011/04/34085

[106] เครือข่ายพลเมืองเน็ต. (2554, เมษายน 19). ผู้ใช้เน็ตยื่นค้านพ.ร.บ.คอมฯฉบับใหม่หน้าสภา นายกบอกไม่ต้องห่วง. สืบค้นเมื่อ 19 เมษายน 2554, จาก http://thainetizen.org/2011/04/netizens-new-cca-protest/

[107] ไอเอ็นเอ็น. (ม.ป.ป.). นายกฯ ชะลอร่างพ.ร.บ.คอมพิวเตอร์, *อ้างแล้ว 64*.

[108] ดูรายละเอียดของโครงการได้ที่ http://mycomputerlaw.in.th/

[109] แนวหน้า. (2554, กันยายน 22). นักวิชาการหนุนรื้อ พ.ร.บ.คอมพ์ ปี 50 แยกหมิ่นประมาณออกจากตัวก.ม. อ้างใน *RYT9*. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.ryt9.com/s/nnd/1241239

[110] เครือข่ายพลเมืองเน็ต. (2553, เมษายน 8). แถลงการณ์เครือข่ายพลเมืองเน็ต เรื่องการปิดกั้นอินเทอร์เน็ตและการสื่อสารของประชาชน. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก https://thainetizen.org/2010/04/statement-on-blocking-internet-and-website/

Thai Netizen Network and Reporters Without Borders. (2010, April 27). Joint statement on the further censorship of websites and media under Emergency Decree. *Reporters Without Borders*. Retrieved December 20, 2011, from http://en.rsf.org/thailand-thai-netizen-network-s-statement-27-04-2010,37164.html

[111] เครือข่ายพลเมืองเน็ต. (2553, มิถุนายน 23). จดหมายเปิดผนึกถึงรัฐบาล และ ศอฉ. ให้ยุติการปิดกั้นสื่อ คืนพื้นที่การสื่อสารให้สังคม. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://thainetizen.org/2010/06/open-letter-togov-and-capo-to-stop-blocking-the-media/

[112] Siam Intelligence Unit. (2552, เมษายน 21). เครือข่ายพลเมืองเน็ตค้านปิดเว็บไซต์จี้ยุติ พรก. ฉุกเฉิน. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.siamintelligence.com/thai-netizen-network-on-the-political-crisis-and-information-censorship/

[113] ชุมชนคนเหมือนกัน. (2553, เมษายน 11). แถลงการณ์ชุมชนคนเหมือนกัน. อ้างใน *กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย*. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://facthai.wordpress.com/2010/04/11/แถลงการณ์-ชุมชนคนเหมือน/

[114] อาทิเช่น งานเสวนา "เสรีภาพอินเทอร์เน็ตในเอเชียตะวันออกเฉียงใต้: แนวคิดใหม่อุปสรรคใหม่ (A Public Forum on Internet Freedom in Southeast Asia: New Frontier, New Barrier) ดู, ประชาไท. (2554, กุมภาพันธ์ 18). เสวนา: ไทย-อินโด-มาเลย์ เผยประสบการณ์สื่ออินเทอร์เน็ตถูกปิดกั้น. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://prachatai.com/jour-

nal/2011/02/33174

งานเสวนา "สิทธิพลเมืองเน็ต และ เสรีภาพสื่อออนไลน์: ปัญหา ข้อท้าทาย และทางออกที่ควรจะเป็น" ดู, อิทธิพล ปรีติประสงค์. (2551, ธันวาคม 4).สิทธิพลเมืองชาวเน็ต แตกต่าง แปลกแยก คู่ขนาน ... กับโลกแห่งความเป็นจริง ? ตอนที่ 1. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://www.gotoknow.org/blogs/posts/227241

กิจกรรมตอบแบบสอบถาม "สิทธิเสรีภาพในการใช้งานอินเทอร์เน็ต" และเสวนาหัวข้อ "การเมืองกับโลกออนไลน์" ดู, bact. (2552, มกราคม 21). แบบสำรวจ "สิทธิเสรีภาพในอินเทอร์เน็ต" – An Online Survey on Internet Rights and Freedom. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://bact.cc/2009/internet-freedom-survey/

[115] ดูภาพกิจกรรมการรณรงค์ได้ที่, สุนิตย์ เชรษฐา. (2550, มิถุนายน 12). ร่วมรณรงค์ "เซ็นเซอร์จัง" ต่อต้านการปิดเว็บแบบมั่วๆ. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://www.learners.in.th/blogs/posts/33725

[116] ประชาไท. (2554, ตุลาคม 31). 'ผู้สื่อข่าวไร้พรมแดน' เปิดตัวแคมเปญ ไทยแลนด์ - 'แดนสวรรค์การเซ็นเซอร์'. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://prachatai.com/journal/2011/10/37683

[117] กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย. (2549, พฤศจิกายน 22). คำร้องต่อคณะกรรมการสิทธิมนุษยชนแห่งชาติ, *อ้างแล้ว 73*.

[118] กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย. (ม.ป.ป.). FACT petition signers รายชื่อผู้ลงชื่อสนับสนุน. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://facthai.wordpress.com/sign/signer-list/

[119] candy strawberry milk (2553, มกราคม 22). Thai No Sniff - ความตื่นตัวเรื่องสิทธิของ netizen ไทย. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://my.dek-d.com/sweetsin/blog/?blog_id=10050555

[120] กนกรัตน์ โกวิชัย. (2553, กุมภาพันธ์ 1). ไอซีที ฝันค้าง "สนิฟเฟอร์" ตกหลุมอากาศ. ไทยรัฐออนไลน์. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://www.thairath.co.th/content/tech/62414

lew. (2553, มกราคม 26). ไอซีทียอมแพ้, เลิกแนวคิดใช้ sniffer. *Blognone*. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://www.blognone.com/node/14785

[121] เครือข่ายพลเมืองเน็ต. (2554, พฤศจิกายน 30). แถลงการณ์เครือข่ายพลเมืองเน็ต: กดไลค์ไม่ใช่อาชญากรรมกระทรวงไอซีทีต้องทบทวนมาตรการจัดการ "เฟซบุ๊กหมิ่น" และ ข้อแนะนำต่อพลเมืองเน็ตเมื่อเจอหน้าเว็บที่ไม่ถูกใจ. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://thainetizen.org/2011/11/click-like-is-not-a-crime/

[122] ประชาไท. (2554, พฤศจิกายน 23). รมว. ไอซีทีเผย ขอเฟซบุ๊กปิดเพจหมิ่นฯแล้วกว่าหมื่นยูอาร์แอล, *อ้างแล้ว 68*.

[123] ชมรมนักรบไซเบอร์ E-mail : FightBadWeb@gmail.com

[124] ไทยรัฐออนไลน์. (ม.ป.ป.). สมาคมผู้ดูแลเว็บฯ ติงไอซีที แก้ปัญหาเว็บหมิ่นไม่ตรงจุด. อ้างใน *highlight.kapook*. สืบค้นเมื่อ 20 กุมภาพันธ์ 2555, จาก http://hilight.kapook.com/view/30448

[125] ASTVผู้จัดการออนไลน์. (2554, สิงหาคม 18). จี้ “รมว. ไอซีที” เร่งปราบเว็บหมิ่น. สืบค้นเมื่อ 20 กุมภาพันธ์ 2555, จาก http://www.manager.co.th/CyberBiz/ViewNews.aspx?NewsID=9540000103856

[126] วิธีการเสียบประจานเกิดขึ้นและแพร่หลายไปในเว็บบอร์ดหลายแห่ง เมื่อปลายเดือนเมษายน 2553 มีผู้ใช้เฟซบุครายหนึ่งเขียนข้อความในเฟซบุคของตน ถูกนำมาเสียบประจานกล่าวหาว่าดูหมิ่นสถาบันฯ กลุ่มผู้ใช้เว็บบอร์ดจำนวนหนึ่งช่วยกันค้นหารายละเอียดของบุคคลนั้นแล้วนำมาเผยแพร่ หลังจากนั้นกรมสอบสวนคดีพิเศษเข้าจับกุมบุคคลนี้ในวันถัดมา นอกจากนี้ ยังมีผู้ใช้เฟซบุคอีกรายที่เข้าไปตอบความเห็นท้ายข้อความที่ถูกกล่าวหาว่าหมิ่นสถาบันฯ ถูกเสียบประจานในเว็บบอร์ดด้วยในเวลาต่อมา ปัจจุบันทั้งคู่ถูกจับกุมดำเนินคดีแล้ว ภายใต้ความดูแลของกรมสอบสวนคดีพิเศษ

[127] สงกรานต์ ป้องบุญจันทร์. (2553, พฤษภาคม 11). บทวิเคราะห์คำพิพากษาศาลแพ่งคดีปิดเว็บประชาไท. *ประชาไท*. สืบค้นเมื่อ 28 มกราคม 2555, จาก http://prachatai.com/journal/2010/05/29391

[128] ASTVผู้จัดการออนไลน์. (2554, มิถุนายน 6). งามไส้ไอซีที ประชาชนรู้จักพ.ร.บ.คอมฯดีแค่ 0.98%. สืบค้นเมื่อ 6 มิถุนายน 2555, จาก http://mgr.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9540000069083

[129] แม่สายนิวส์. (2554, มีนาคม 28). นักกฎหมายชำแหละ พรบ.คอมพิวเตอร์ 3 ปี คนไม่รู้ว่ามี 70% เหตุขาดการประชาสัมพันธ์-ปัญหาตีความการบังคับใช้กฎหมาย. สืบค้นเมื่อ 28 มกราคม 2555, จาก http://www.maesainews.com/plus/index.php?name=knowledge&file=readknowledge&id=268

กฎหมายเยอรมัน กับสิทธิเสรีภาพในสื่อออนไลน์

[1] § 5 GG “(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.

(2) Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre.

(3) Kunst und Wissenschaft, Forschung und Lehre sind frei. Die Freiheit der Lehre entbindet nicht von der Treue zur Verfassung.“

[2] § 5 GG “(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten..“

[3] § 5 GG “(1)...und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten....”

[4] Herbert Bethge, Grundgesetz, Kommentar, Art. 5, in: Sachs, Michael (Hrsg.), Rn. 54.\

[5] § 5 GG “(1)...Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.”

[6] BverfGE 10, 118, 121; BverfG 1999, 2106.

[7] Hoffmann - Riem, Grundgesetz Art. 5, in: Alternativkommentar zum GG (AK-GG), Rn. 138, 145.

[8] Thomas Clemens, Grundgesetz Art. 5, in: Umbach, Dieter C./Clemens, Thomas (Hrsg.), Rn. 69a.

[9] Thomas Stadler, *Haftung für Information im Internet*, (Berlin: Schmidt, 2002), p. 170;

Martin Bullinger. Strukturwandel von Rundfunk und Presse : Rechtliche Folgewirkungen der neuen elektronische Medien. *NJW*, 1984, p. 385, 390.

[10] Thomas Clemens, Grundgesetz Art. 5, in: Umbach, Dieter C./Clemens, Thomas (Hrsg.), Rn.69b; Herbert Bethge, Grundgesetz Kommentar Art. 5, in: Sachs, Michael (Hrsg.), Rn. 88.

[11] Spiegel online. (2010, January 5). Kunstfreiheit gilt für Großköpfe und Kleinhirne. Retrieved July 20, 2011, from: http://www.spiegel.de/kultur/gesellschaft/0,1518,670130,00.html;

Boulevard Baden. (2011, September 25). Nils Schmid verteidigt Kunstfreiheit auch bei Mohammed-Karikaturen. Retrieved July 20, 2011, from http://www.boulevard-baden.de/lokales/nachrichten/2011/09/25/nils-schmid-verteidigt-kunstfreiheit-auch-bei-mohammed-karikaturen-podiumsdiskussion-anlasslich-60-jahrfeier-des-bundesverfassungsgerichts-426953/

[12] Ulrich Sieber and Malaika Nolde, *Sperrverfügungen im Internet: Nationale Rechtsdurchsetzung im globalen Cyberspace?* (Berlin: Duncker & Humblot, 2008), p. 176;

Das Verhältnismäßigkeitsprinzip. (n.d.). Retrieved July 25, 2011, from www.jur-dinn.de/Studi-Ecke/Verhaeltnism.pdf ;

Spiegel online. (2010, January 5). Kunstfreiheit gilt für Großköpfe und Kleinhirne,

อ้างแล้ว 11 ;

Boulevard Baden. (2011, September 25). Nils Schmid verteidigt Kunstfreiheit auch bei Mohammed-Karikaturen, *อ้างแล้ว 11*.

[13] ดู ธีระ สุธีวรางกูร. การคุ้มครองสิทธิและเสรีภาพของบุคคลที่รัฐธรรมนูญรับรอง. *วารสารนิติศาสตร์,* 29(4), (2542), หน้า 588.

[14] *เพิ่งอ้าง.*

[15] ตามประมวลกฎหมายอาญาเยอรมัน ซึ่งได้รับการแก้ไขเพิ่มเติมเมื่อปลายปี ค.ศ. 2008 (BGBl. I, S. 32149 ff.) ภาพลามกอนาจารเด็กและเยาวชน (ตามมาตรา 184b และ 184c StGB) หมายถึง ภาพกิจกรรมทางเพศของ, กับ หรือต่อหน้าบุคคลซึ่งมีอายุต่ำกว่า 18 ปี (die sexuelle Handlungen von, an oder vor Personen unter 18 Jahren)

[16] ตามกฎหมายเยอรมันในเรื่องนี้ "เด็ก" คือ บุคคลที่อายุยังไม่ถึง 14 ปี (§ 184b StGB) และ "เยาวชน" คือ บุคคลที่มีอายุตั้งแต่ 14 ปีแต่ยังไม่เกิน 18 ปี (§ 184c StGB) § 4 JMStV Unzulässige Angebote "(1) Unbeschadet strafrechtlicher Verantwortlichkeit sind Angebote unzulässig, wenn sie ...

[17] § 4 JMStV Unzulässige Angebote "(1) Unbeschadet strafrechtlicher Verantwortlichkeit sind Angebote unzulässig, wenn sie...10. pornografisch sind und Gewalttätigkeiten, den sexuellen Missbrauch von Kindern oder Jugendlichen oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand haben; dies gilt auch bei virtuellen Darstellungen, oder..."

[18] § 4 JMStV Unzulässige Angebote "(2) Unbeschadet strafrechtlicher Verantwortlichkeit sind Angebote ferner unzulässig, wenn sie ... 1. in sonstiger Weise pornografisch sind,..."

[19] Erwachsene หรือ ผู้ใหญ่ คือ บุคคลที่มีอายุเกินกว่า 18 ปี

[20] AG Mülheim, Urteil vom 14.03.1997 (Az.: 14 Cs 17 Js 55/96 (861/96)); BayObLG, MMR 2000, 758 zu § 184 a.F.

[21] Roland Derksen. Perspektiven für eine wirksame Bekämpfung von Rechtsradikalismus und Rassismus im Internet. *ZFIS* 1999, p.150, 151.

[22] มีผู้นำทฤษฎีวิวัฒนาการดังกล่าวของดาร์วิน ไปประยุกต์ใช้อธิบายปรากฏการณ์ต่างๆ ในสังคมและแนวคิดในการจัดระเบียบสังคมในขณะนั้น ทำให้เกิดการเปลี่ยนแปลงทางความคิดของผู้คนและสังคมตะวันตกในช่วงปลายคริสต์ ศตวรรษที่ 19 จนก่อให้เกิดผลกับโลกในหลายด้านทั้งแง่ดีและแง่เสีย ที่เกี่ยวกับเนื้อหาต้องห้ามนี้ก็คือ เคยมีการนำทฤษฎีนี้ไปอธิบายระบบเศรษฐกิจหรือระบบนายทุนและลัทธิชาตินิยมว่า "คนที่แข็งแรงที่สุดหรือเผ่าพันธุ์ที่เข้มแข็งที่สุดเท่านั้นจึงจะอยู่รอดได้" ความเหลื่อมล้ำทางสังคมเป็นผลมาจากความสามารถที่แตกต่างกันของมนุษย์ซึ่งเป็นไปตามการเลือกสรรของธรรมชาติ ลัทธินี้เชื่อมโยงสัมพันธ์อย่างยิ่งกับลัทธิชาตินิยมนาซี เพราะเป็นลัทธิที่ใช้อ้างความชอบธรรมของการฆ่าล้างเผ่าพันธุ์ชาวยิวทั่วยุโรป

ผ่าน “มาตรการแก้ปัญหาชาวยิวครั้งสุดท้าย” (Final Solution) ของฮิตเลอร์ในช่วงสงครามโลกครั้งที่ 2 (ค.ศ 1939 - 1945) ดู, Wikipedia Die freie Enzyklopädie. (n.d.). Sozialdarwinismus. Retrieved November 6, 2010, from http://de.wikipedia.org/wiki/Sozialdarwinismus

[23] Oliver Decker and Elmar Brähler. (2006). Vom Rand zur Mitte: Rechtsextreme Einstellung und ihre Einfl ussfaktoren in Deutschland. Retrieved November 8, 2010, from http://www.fes.de/rechtsextremismus/pdf/Vom_Rand_zur_Mitte.pdf

[24] Monika Ermert. (2007, April 18). Provider sollen mehr gegen Hass-Seiten in Internet tun. Heise online. Retrieved November 8, 2010, from http://www.heise.de/newsticker/meldung/Provider-sollen-mehr-gegen-Hass-Seiten-im-Internet-tun-168724.html

[25] Rainer Fromm and Barbara Kernbach, Rechtsextremismus im Internet: die neue Gefahr. (München: Olzog, 2001), p. 84.

[26] *เพิ่งอ้าง, p. 29.*

[27] Sperrverfügung der Bezirksregierung Düsseldorf. (n.d.) Retrieved November 23, 2010, from http://odem.org/material/verfuegung/sperrungsverfuegung.pdf

[28] รวมข่าว “Amoklauf von Erfurt” ดู, Spiegel online. (n.d.). Amoklauf von Erfurt. Retrieved November 25, 2010, from http://www.spiegel.de/thema/amoklauf_erfurt/

[29] § 4 JMStV Unzulässige Angebote “(1) Unbeschadet strafrechtlicher Verantwortlichkeit sind Angebote unzulässig, wenn sie ... 8. gegen die Menschenwürde verstoßen, insbesondere durch die Darstellung von Menschen, die sterben oder schweren körperlichen oder seelischen Leiden ausgesetzt sind oder waren, wobei ein tatsächliches Geschehen wiedergegeben wird, ohne dass ein berechtigtes Interesse gerade für diese Form der Darstellung oder Berichterstattung vorliegt; eine Einwilligung ist unbeachtlich,...”

[30] AG Rheinbach, Einstellungsbeschluß v. 12.2.1996 (Akz.: 2 Ds 397/95), zitiert bei Tobias H. Strömer, *Online-Recht: Rechtsfragen im internetund in Mailboxnetzen*, (Heidelberg: dpunkt, Verl, 1997), p. 234.

[31] Marcus Schreibauer. Strafrechtliche Verantwortlichkeit für Delikte im Internet. In *Handbuch zum Internetrecht: Electronic Commerce - Informations-, Kommunikations- und Mediendienste*. Detlef Kröger and Marc A. Gimmy (eds.). (Berlin: Springer-Verlag, 2000). P. 580 (594).

[32] Karl-Heinz Ladeu, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, (ZUM, 1997), p. 373.

[33] ดังเช่นคำพิพากษาในเดือนพฤษภาคม ปี 1998 โดยศาลมิวนิก (AG München) เคยตัดสินให้ผู้จัดการการให้บริการอินเทอร์เน็ต (บริษัท CompuServer GmbH) ต้องรับผิดในฐานะ

เป็นผู้สนับสนุนการเผยแพร่ภาพลามกอนาจารเด็กด้วยโทษจำคุก แต่ให้รอลงอาญาเป็นเวลา 2 ปีและปรับอีก 100,000 มาร์คเยอรมัน (Süddeutschzeitung v. 29.5.1998)

[34] ปัจจุบันมีหลายฝ่ายตั้งข้อสังเกตว่า แม้เนื้อหา แนวทาง และข้อกำหนดต่างๆ เกี่ยวกับความผิดในอนุสัญญาที่ออกโดยคณะมนตรียุโรป (Europarat) ได้กำหนดถึงพฤติกรรมความผิดหลายประการที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยไม่จำเป็นต้องเชื่อมต่อเป็นโครงข่ายบนอินเทอร์เน็ตเท่านั้น แต่ด้วยชื่อของอนุสัญญาฉบับนี้เองที่ใช้คำว่า Cybercrime แทนที่จะเป็น Computer crime หรือ Computer related Crime จึงทำให้เกิดความไม่ชัดเจนและเป็นข้อจำกัดในการตีความและขยายขอบเขตของความผิดที่เกิดขึ้นในปัจจุบัน

[35] 5 ประเทศ ได้แก่ อัลบาเนีย, โครเอเชีย, เอสโตเนีย, ฮังการี และ ลิทัวเนีย ดู, Council of Europe Treaty Office. (n.d.). Retrieved March 3, 2010, from http://conventions.coe.int/

[36] ดูลำดับการลงนาม การให้สัตยาบัน และการอนุวัติการตามอนุสัญญา เข้าถึงได้ที่ Council of Europe Treaty Office. (n.d.). Convention on Cybercrime CETS No.: 185. Retrieved March 3, 2010, from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

[37] “Zweites Gesetzes zur Bekämpfung der Wirtschaftskriminalität“ (2. WiKG), BGBl. I p. 721; Hans .Achenbach, “Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität”, *NJW* 1986, p. 1835 ff.; Tiedeman Klaus, “Die Bekämpfung der. Wirtschaftskriminalität durch den Gesetzgeber“, *JZ* 1986, p. 865 ff.

[38] Das Urheberstrafrecht.

[39] Das Teledienstegesetz (TDG) und Der Mediendienste-Staatsvertrag (MDStV).

[40] Artikel 22 MDStV “…(2) Stellt die jeweils zuständige Aufsichtsbehörde nach Absatz 1 einen Verstoß gegen die Bestimmungen dieses Staatsvertrages mit Ausnahme der § 10 Abs. 3, § 11 Abs. 2 und 3, §§ 14, 16 bis 20 fest, trifft sie die zur Beseitigung des Verstoßes erforderlichen Maßnahmen gegenüber dem Diensteanbieter. Sie kann insbesondere Angebote untersagen und deren Sperrung anordnen...”

[41] Artikel 22 MDStV “…(2)... Die Untersagung darf nicht erfolgen, wenn die Maßnahme außer Verhältnis zur Bedeutung des Angebots für den Diensteanbieter und die Allgemeinheit steht. Eine Untersagung darf nur erfolgen, wenn ihr Zweck nicht in anderer Weise erreicht werden kann. Die Untersagung ist, soweit ihr Zweck dadurch erreicht werden kann, auf bestimmte Arten und Teile von Angeboten oder zeitlich zu beschränken...”

[42] Das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie

2006/24/EG. (2007, June 27). Retrieved March 5, 2011, from http://dip.bundestag.de/btd/16/058/1605846.pdf

[43] ประเภทข้อมูลจราจรที่ต้องจัดเก็บ อาทิ เลขหมายโทรศัพท์ทุกประเภททั้งโทรศัพท์บ้านและเคลื่อนที่ ที่มีการเรียกเข้า - เรียกออก, เวลาเริ่มต้นและจบการติดต่อ, วัน เวลา รวมทั้งสถานที่ที่ใช้เครื่อง ในกรณีที่เป็นโทรศัพท์ที่ใช้ผ่านอินเทอร์เน็ตต้องเก็บหมายเลขเครื่อง (IP-Adresse) นอกจากนี้ ก็ยังรวมถึงข้อมูลจราจรในการส่งข้อความ (SMS), การรับ-ส่งอีเมล และการใช้บริการอินเทอร์เน็ตประเภทต่างๆ ด้วย

[44] Spiegel online. (2010, March 2). Vorratsdatenspeicherung verstößt gegen Verfassung. Retrieved June 17, 2010, from http://www.spiegel.de/netzwelt/netzpolitik/0,1518,681122,00.html;

คำพิพากษาศาลรัฐธรรมนูญ ดู, Urteil vom 2. März 2010 zu 1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08. (n.d.). Retrieved June 18, 2010, from http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

[45] Detlef Borchers. (2007, July 25). Online-Durchsuchung: Ist die Festplatte eine Wohnung? *Heise online*. Retrieved August 12, 2011, from http://www.heise.de/newsticker/meldung/Online-Durchsuchung-Ist-die-Festplatte-eine-Wohnung-155439.html

[46] Stern.de (2009, April 11). Stoppschild gegen Kinderpornos im Web. Retrieved August 15, 2011, from http://www.stern.de/digital/online/internetsperren-stoppschild-gegen-kinderpornos-im-web-661190.html

[47] ประกอบด้วย Deutsche Telekom, Vodafone/Arcor, Telefo'nica Germany, Kabel Deutschland และ HanseNet/Alice.

[48] ZugErschwG. (2009, July 11). Das Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz). Retrieved August 3, 2011, from http://www.zugerschwg.com/2009/07/zugangserschwerungsgesetz-volltext.html

[49] Zeit online. (2011, May 25). Bundesregierung hebt Sperrgesetz gegen Kinderpornos auf. Retrieved August 3, 2011, from http://www.zeit.de/politik/deutschland/2011-05/streichung-kinderpornosperre

[50] Markus Franz. (2010, April 22). Zensur im Netz: Ein Blick über den Tellerrand. *Netzwelt*. Retrieved September 18, 2011, from http://www.netzwelt.de/news/82506-zensur-netz-blick-ueber-tellerrand.html

[51] GERMANY CENSORS DUTCH WEBSITE WWW.XS4ALL.NL, WITH 3100 WEBPAGES. (n.d.) Retrieved September 18, 2011, from http://www.nadir.org/nadir/archiv/Medien/Zeitschriften/radikal/netzzensur/96090501.html

[52] http://ourworld.compuserve.com/ homepages/angela1/homepage.htm และ http://

ourworld.compuserve.com/homepages/angela1/*.*

[53] Zur Zensur der Seiten von Angela Marquardt bei Compuserve. (1997, July 17). Retrieved October 12, 2011, from http://nadir.org/nadir/initiativ/r_ver/hinter/zensur/zensu08.htm

[54] Sabine Helmers. (1996, September 24). Hyperlink-Prozeß: Freispruch für Angela Marquardt. *Heise online*. Retrieved October 15, 2011, from http://www.heise.de/tp/artikel/1/1236/1.html

[55] Martin Fiutak. (2006, August 11). Deutsche Behörden wollen Zugang zu Bwin sperren. *ZDNet*. Retrieved October 17, 2011, from http://www.zdnet.de/news/39146183/deutsche-behoerden-wollen-zugang-zu-bwin-sperren.htm

[56] เว็บไซต์เปิดให้ลงชื่อไม่เห็นด้วยกับคำสั่งปิดกั้นฯ ดู, Internet-Zensur in Deutschland. (n.d.). Retrieved October 15, 2011, from http://odem.org/informationsfreiheit/

[57] VG Düsseldorf, 10.05.2005 - 27 K 5968/02.

58 Das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG. (2007, June 27). Retrieved March 5, 2011, from http://dip.bundestag.de/btd/16/058/1605846.pdf

[59] ประเภทข้อมูลจราจรที่ต้องจัดเก็บ อาทิ เลขหมายโทรศัพท์ทุกประเภททั้งโทรศัพท์บ้านและเคลื่อนที่ ที่มีการเรียกเข้า - เรียกออก, เวลาเริ่มต้นและจบการติดต่อ, วัน เวลา รวมทั้งสถานที่ที่ใช้เครื่อง ในกรณีที่เป็นโทรศัพท์ที่ใช้ผ่านอินเทอร์เน็ตต้องเก็บหมายเลขเครื่อง (ที่อยู่ไอพี) นอกจากนี้ ก็ยังรวมถึงข้อมูลจราจรในการส่งข้อความ (SMS), การรับ-ส่งอีเมล และการใช้บริการอินเทอร์เน็ตประเภทต่างๆ ด้วย

[60] Spiegel online. (2007, December 31). 30.000 klagen in Karlsruhe - größte Verfassungs-Beschwerde aller Zeiten. Retrieved August 6, 2011, from http://www.spiegel.de/netzwelt/web/0,1518,525970,00.html

[61] ดู, Verfassungsbeschwerde Vorratsdatenspeicherung. (n.d.). Retrieved July, 11, 2011, from http://wiki.vorratsdatenspeicherung.de/images/Verfassungsbeschwerde_Vorratsdatenspeicherung.pdf

[62] เว็บไซต์รณรงค์ และเผยแพร่ข้อมูลที่จัดทำขึ้นโดย German Working Group on Data Retention ดู, German Working Group on Data Retention. (n.d.) Retrieved July 15, 2011, from http://www.vorratsdatenspeicherung.de/component/option,com_frontpage/Itemid,1/lang,en/

[63] Spiegel online. (2010, March 2). Vorratsdatenspeicherung verstößt gegen Verfassung. Retrieved June 17, 2010, from http://www.spiegel.de/netzwelt/netzpolitik/0,1518,681122,00.html;

คำพิพากษาศาลรัฐธรรมนูญ ดู, Urteil vom 2. März 2010 zu 1 BvR 256/08, 1 BvR

263/08 und 1 BvR 586/08. (n.d.). Retrieved June 18, 2010, from http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

[64] Petition: Internet - Keine Indizierung und Sperrung von Internetseiten vom 22.04.2009. (2009, April 22). Retrieved December 14, 2011, from https://epetitionen.bundestag.de/petitionen/_2009/_04/_22/Petition_3860.html

[65] Patrick Beuth. (2009, June 18). Das Gesicht des Internets. *Frankfurter Rundschau.* Retrieved December 14, 2011, from http://www.fr-online.de/datenschutz/franziska-heine-das-gesicht-des-internets,1472644,2706570.html

[66] Arbeitskreis gegen Internet-Sperren und Zensur (AK Zensur). (n.d.) Retrieved December 16, 2011, from http://ak-zensur.de/

[67] MOGiS e.V. – Eine Stimme für Betroffene. (n.d.). Retrieved December 14, 2011, from http://mogis-verein.de/wer-wir-sind/impressum/

[68] Chaos Computer Club. (n.d.). Retrieved December 14, 2011, from http://www.ccc.de/de/home

[69] Holger Bleich and Axel Kossel. (n.d.). Verschleierungstaktik Die Argumente für Kinderporno-Sperren laufen ins Leere. *Heise online*. Retrieved July 3, 2011, from http://www.heise.de/ct/artikel/Verschleierungstaktik-291986.html

[70] Offener Brief zur Gesetzesvorlage Internetsperren. (n.d.) Retrieved September 16, 2011, from http://www.trotzallem.de/Offener_Brief_Familienministerin.pdf

[71] Marita Wagner. (2009, May 18). Straverfolgung oder Internetsperren? *Heise online*. Retrieved September 21, 2011, from http://www.heise.de/tp/artikel/30/30344/1.html

[72] Simon Moeller. (2009, April 24). Netsaperren: Der neue Entwurf und siene Rechtsmaessigkeit. *Telemedicus*. Retrieved September 15, 2011, from http://www.telemedicus.info/article/1271-Netzsperren-Der-neue-Entwurf-und-seine-Rechtsmaessigkeit.html

[73] ดู, ZDF.de. (2007, September 14). Politbarometer: 65 Prozent für Online-Durchsuchung. Cited in Internet Archive. Retrieved September 15, 2011, from http://web.archive.org/web/20080102140653/http://www.zdf.de/ZDFde/inhalt/0/0,1872,7004800,00.html

[74] ดู, WinFuture. (2008, November 23). Online-Durchsuchung: 57% der Deutschen sind dafür. Retrieved September 15, 2011, from http://winfuture.de/news,43732.html

[75] Heise online. (2011, October 15) Staatstrojaner: Bundesinnennminister verteidigt den Einsatz und greift CCC an. Retrieved September 15, 2011, from http://www.heise.de/newsticker/meldung/Staatstrojaner-Bundesinnenminister-verteidigt-den-Einsatz-und-

greift-CCC-an-1361814.html

[76] Urteil vom 27. Februar 2008 zu 1 BvR 370/07 und 1 BvR 595/07. (n.d.). Retrieved September 18, 2011, from http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html

กฎหมายสหรัฐอเมริกา กับสิทธิเสรีภาพในสื่อออนไลน์

[1] American Civil Liberties Union v. Reno, 926 F.Supp. 824 (1996) อ้างใน Patricia L. Bellia, et al. *Cyberlaw: Problems of Policy and Jurisprudence in the Information Age*, 2nd ed. (MN: Thomson West, 2004), p.14-15.

[2] Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof, or abridging the freedom of speech, or the press, or the right of the people peaceably to assembly, and to petition the Government for a redress of grievance.

[3] ในปี ค.ศ.2009 Reporters Without Borders for Press Freedom รายงานว่า สหรัฐอเมริกา มีเสรีภาพในการแสดงความคิดเห็น อยู่ลำดับที่ 20 ในขณะที่ ประเทศเดนมาร์ก และ กลุ่มประเทศตะวันตกอยู่ในลำดับต้นๆ ส่วนประเทศไทยและมาเลเซีย อยู่ในลำดับที่ 130-131 ตามลำดับ ดีกว่าจีนซึ่งอยู่ในลำดับที่ 168 จาก 175 ประเทศ เท่านั้น โปรดดูรายละเอียดใน Reporters Without Borders. (n.d.). Press Freedom Index 2009. Retrieved March 13, 2012, from http://en.rsf.org/press-freedom-index-2009,1001.html

[4] Stephen C. Jacques. Comment: Reno v. ACLU : Insulating The Internet, The First Amendment, and The Marketplace of Ideas. *46 Am. U.L. Rev*. 1945, 1949 (1997)

[5] Steven L. Emanuel. *Constitutional Law*. (New York: Aspen, 2003). p. 448-575.

[6] Abrams v. U.S. 250 U.S. 616 (1919)

[7] Ronald D. Rotunda, *Modern Constitutional Law: Case and Notes*, 8th ed. (MN: Thomson West, 2007), p. 944-1390.

[8] ตัวอย่างเช่น ข้อห้ามของโรงเรียนที่ห้ามใส่สายข้อมือซึ่งมีข้อความต่อต้านสงครามเวียดนาม แม้จะมีข้ออ้างว่าเป็นการควบคุมวิธีการ (manner) ในการแสดงความคิดเห็นเท่านั้น แต่แท้จริงแล้วมุ่งที่จะควบคุมเนื้อหาในการแสดงความคิดเห็นดังกล่าว ศาลจึงเห็นว่าการห้ามดังกล่าว ขัดต่อรัฐธรรมนูญ (Tinker v. Des Moines School District, 393 U.S. 503 (1969))

[9] ประเทศสหรัฐฯ ถือว่าคำพิพากษาเป็นสาธารณะ ประชาชนจึงมีสิทธิอันชอบธรรมในการวิพากษ์วิจารณ์ได้ เว้นแต่ การวิพากษ์วิจารณ์ในช่วงที่คดียังอยู่ระหว่างการพิจารณา อาจจะมีความผิดฐานละเมิดอำนาจศาล (Contempt of court) ได้ แต่ศาลสูงสุดสหรัฐฯ ได้กำหนดหลักการใช้อำนาจเกี่ยวกับการละเมิดอำนาจศาลไว้ว่าจะต้องมีข้อเท็จจริงที่จะต้องร้ายแรงถึงขนาดที่จะเรียกได้ว่าจะกระทบต่อความยุติธรรมในการพิจารณาคดีอย่างชัดแจ้ง (Clear and

Present Danger) เท่านั้น ดังนั้น ศาลไม่อาจจะลงโทษโดยอาศัยอำนาจนี้ได้ตามอำเภอใจ

[10] R.A.V. v. St. Paul, 505 U.S. 377 (1992)

[11] ศาลสูงสุดได้พิพากษาว่า การที่ผู้นำแรงงานวิพากษ์วิจารณ์คำพิพากษาของศาลล่างว่าไม่มีคุณภาพอย่างร้ายแรง (outrageous) และข่มขู่ว่า ถ้าคำพิพากษาที่ไม่ได้เรื่องนั้น ไม่ถูกพิพากษากลับจะมีการนัดหยุดงานขึ้น การกระทำนี้ไม่มีความผิดใดๆ และ ไม่อาจจะถูกลงโทษฐานละเมิดอำนาจศาลได้ โปรดดู Craig v. Harney, 331 U.S. 367 (1947) และ คดี Bridges v. California, 314 U.S. 252 (1941)

[12] Landmark Communications, inc. v. Virginia, 435 U.S. 829 (1978)

[13] ตัวอย่างการกำหนดภาษีที่เกี่ยวข้องกับวัสดุ อุปกรณ์ ที่จำเป็นต้องใช้ในสื่อประเภทนั้น (Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue, 460 U.S. 525 (1983) ทำให้หมึกและกระดาษสำหรับโรงพิมพ์สูงกว่าคนทั่วไป

[14] Walker v. City of Birmingham, 388 U.S. 307 (1967)

[15] Kathleen M. Sullivan, et al., *Constitutional Law*, 14th ed., (NY: Foundation Press, 2001). p. 956-1434.

[16] New York v. Ferber, 458 U.S. 747 (1982)

[17] รายละเอียดโปรดดูใน Cybertelecom. (n.d.). Cybertelecom: Federal Internet Law and Policy. Retrieved March 13, 2012, from http://www.cybertelecom.org

[18] Stephen C. Jacques, *อ้างแล้ว 4*, p. 1986, 1989 (ก่อนที่จะมีการตรากฎหมาย CDA ได้มีการฟ้องร้องและดำเนินคดีที่เกี่ยวข้องกับอินเทอร์เน็ตจำนวนมาก โดยใช้กฎหมายที่มีอยู่เดิม เช่น ในส่วนของภาพลามกอนาจาร (obscenity) ซึ่งมีการดำเนินคดีตามความผิดเกี่ยวกับคอมพิวเตอร์ ตามกฎหมาย 18 U.S.C. §1465 การเผยแพร่ภาพอนาจารทางเพศของเด็ก (child pornography) ที่มีการเผยแพร่และจำหน่ายภาพดังกล่าวผ่านอินเทอร์เน็ต ตามกฎหมาย 18 U.S.C. § 2252(a) หรือ การส่งข้อความหรือการรบกวนรังควาน หรือข่มขู่ให้กลัว (stalking) ผ่านระบบอินเทอร์เน็ตหรือเครื่องมือสื่อสารทางอิเล็กทรอนิกส์ ตามกฎหมาย 18 U.S.C. § 875(c) เป็นต้น)

[19] BRANDENBURG v. OHIO (SUPREME COURT OF THE UNITED STATES 395 U.S. 444 June 9, 1969), Retrieved March 13, 2012, from http://law2.umkc.edu/faculty/projects/ftrials/conlaw/brandenburg.html

[20] อย่างไรก็ตาม การครอบครองสิ่งลามกอนาจารโดยผู้ใหญ่ไม่อาจจะถือว่าเป็นความผิดทางอาญาได้ (Standley v. Georgia, 394 U.S. 557 (1969)) เพราะมีผลประโยชน์ที่รัฐเข้ามาเกี่ยวข้องน้อย เนื่องจากเป็นเสรีภาพของผู้ใหญ่ที่จะมีวัตถุดังกล่าวไว้ในครอบครองโดยชอบ รัฐไม่มีอำนาจโดยชอบที่จะกำหนดกฎเกณฑ์ใดๆ ในการจะกำหนดวิถีชีวิตของบุคคลทั่วไป โดยเฉพาะสิทธิในพื้นที่ส่วนตัว (right of privacy) แต่รัฐอาจจะกำหนดห้ามการส่งทางไปรษณีย์สำหรับวัตถุลามกอนาจารที่เสนอขายนั้นได้ (U.S. v. Reidel, 402 U.S.351 (1971)) โดยศาลเห็นว่าเป็นเพียงการจำกัดวิธีการในการดำเนินธุรกิจเท่านั้น

[21] Roth v. U.S., 354 U.S. 476 (1957)

[22] Miller v. California, 413 U.S. 15 (1973)

[23] นอกจากนี้ รัฐบาลกลางสหรัฐอเมริกา ยังได้บัญญัติกฎหมายลำดับรอง (Code of Federal Regulations) เช่น 47 C.F.R. § 64.201 ข้อจำกัดเกี่ยวกับการให้บริการข้อความทางโทรศัพท์ที่มีลักษณะไม่เหมาะสม (Restrictions on indecent telephone message services) , 47 C.F.R. § 73.4165 การกระจายเสียงที่ไม่เหมาะสม (Indecent broadcasts) , 47 C.F.R. § 73.4170 การกระจายเสียงที่ลามกอนาจาร (Obscene broadcasts) , 47 C.F.R. § 76.227 การจำกัดหรือปิดกั้นสำหรับ สถานีวิทยุโทรทัศน์ ที่มีรายการที่มีการชี้นำทางเพศที่ไม่เหมาะสม (Blocking of indecent sexually-oriented programming channels)

[24] กฎหมายเดิม มีสาระสำคัญอยู่ที่มาตรา 18 U.S.C. § 1460 กำหนดความผิดสำหรับการครอบครองวัตถุลามกอนาจาร โดยเจตนาที่จะจำหน่าย มาตรา 1462 การนำเข้าและขนส่งซึ่งวัตถุลามกอนาจาร มาตรา 1464 การแพร่กระจายเสียงด้วยภาษาลามกอนาจาร มาตรา 1465 การขนส่งวัตถุลามกอนาจารเพื่อการขายหรือจำหน่าย มาตรา 1466 การประกอบธุรกิจเพื่อการขาย หรือ ส่งสื่อลามกอนาจาร และ มาตรา 2251 แสวงประโยชน์ทางเพศจากเด็ก (Sexual exploitation of children)

[25] กฎหมายนี้ ยังได้มีข้อกำหนดในบทนิยามให้ชัดเจนว่า คำว่า Telecommunication devices ตามกฎหมายนี้ ไม่ก่อให้เกิดภาระหน้าที่ใดเพิ่มเติมกับสถานีวิทยุโทรทัศน์ หรือ ผู้ประกอบการเคเบิ้ลทีวี นอกจากกฎหมายว่าด้วย สิ่งลามกอนาจาร และสิ่งไม่เหมาะสม ตามหลัก Freedom of speech และ ไม่ถือว่าเป็นส่วนหนึ่งของอุปกรณ์สื่อสารและให้บริการเชื่อมต่อทางคอมพิวเตอร์ (interactive computer service)

[26] Reno v. ACLU, 929 F. Supp. 824 (1996), 521 U.S. 844 (1997)

[27] โปรดดู American Civil Liberties Union v. Reno, 217 F.3d 162 (3d Cir.2000) , Ashcroft v. American Civil Liberties Union, 535 U.S. 564 (2001) และ American Civil Liberties Union v. Ashcroft, 322 F.3d 240 (3d Cir. 2003), cert. granted, 124 S.Ct. 399 (2003)

[28] United States v. American Library Association, Inc., 539 U.S. 194 (2003)

[29] Feiner v. New York, 340 U.S. 315 (1951)

[30] โปรดดู Wayne Madsen. (2005, December 9). Internet Censorship, Retrieved March 12, 2012, from http://www.rense.com/general69/intercens.htm

[31] E.E.B., et al. Plugging the Leak: The Case for A Legislative Resolution of the Conflict Between The Demands of Secrecy and The Need for an Open Government. *71 Va. L. Rev*. 802, 805 (1985)

[32] *เพิ่งอ้าง. p. 831.*

[33] Am.Civil Liberties Union v. Dep't of Def., 543 F.3d 59 (2d Cir. 2008)

[34] แตกต่างจาก กรณีกฎหมายในอดีต เช่น Espionage Act หรือ National Security

Document Act ที่ให้อำนาจแก่ประธานาธิบดี และ ผู้อำนวยการ CIA ในการใช้ดุลพินิจในการที่จะเปิดเผยข้อมูลใดๆ หรือไม่ โดยศาลไม่มีอำนาจตรวจสอบใดๆ อีกต่อไป แต่นับแต่ปี ค.ศ. 1988 เป็นต้นมา สภาคองเกรส ได้แก้ไขกฎหมายให้ศาลตรวจสอบความถูกต้องในการไม่เปิดเผยกฎหมายดังกล่าวภายในกฎหมาย FOIA ทุกกรณีไป

[35] Devin S. Schindler, Between Safety and Transparency: Prior Restraints, FOIA, and the Power of the Executive. 38 *Hastings Const.* L.Q. 1 (2010)

[36] Devin S. Schindler. *เพิ่งอ้าง p. 9-10.* (นักวิชาการท่านนี้เห็นว่า ฝ่ายบริหารควรจะมีอำนาจดุลพินิจเด็ดขาดที่จะพิจารณาว่าข้อมูลข่าวสารใด ไม่ควรเปิดเผย ภายใต้หลักความมั่นคงของชาติ โดยเฉพาะข้อมูลบางส่วนที่เปิดเผยแล้วจะเป็นอันตรายต่อชีวิตของประชาชน รวมถึงความมั่นคงของชาติโดยรวม เช่น กรณีการเปิดเผยข้อมูลและภาพที่มีลักษณะเป็น Inflammatory Material แต่ไม่ถึงขนาดเป็นความลับ ในช่วงปฏิบัติการของประธานาธิบดี บุช ที่ทหารอเมริกันทำร้ายและก่อให้เกิดความอับอายหรือการเหยียบย่ำศักดิ์ศรีของชาวมุสลิมในสงครามต่อต้านการก่อการร้าย ซึ่งท้ายที่สุดภายหลังคดีนี้ ศาลได้สั่งให้รัฐบาลกลางสหรัฐฯ เปิดเผยภาพดังกล่าวให้ประชาชนทั่วไปสามารถเข้าถึงได้ รายละเอียดโปรดดูคดี Am.Civil Liberties Union v. Dep't of Def., 543 F.3d 59 (2d Cir. 2008))

[37] ในอดีตที่ผ่านมา รัฐบาลสหรัฐอเมริกาใช้ช่องทางนี้โดยไม่ชอบธรรม เพื่อตรวจสอบและเข้าถึงข้อมูลของชนชาติศัตรูของสหรัฐอเมริกา รวมทั้งรัฐบาลกลางยังเคยใช้ช่องทางเดียวกันนี้ในการเข้าถึงข้อมูลของนักการเมืองคู่แข่งโดยไม่มีหมายศาล เพื่อใช้ดำเนินคดีหรือทำลายกันในทางการเมือง ภายใต้ข้ออ้างว่ากระทำไปเพื่อความมั่นคงของประเทศ ดูใน William C. Banks, et al. Executive Authority for National Security Surveillance. *50 Am. U.L. Rev.* 1, 10 (2000), นอกจากนี้ยังพบว่า การปิดบังข้อมูลนั้น กระทำไปเพียงเพื่อหลีกเลี่ยงความละอายที่รัฐไม่ดำเนินการตามขั้นตอนของกฎหมาย หาใช่เพื่อความมั่นคงแห่งชาติไม่ ดูใน Charles E. Simmons. Fundamental Rights: United States Foreign Policy v. The Press and the American Information Consumer : The Embattled First Amendment. 1987 *How. L. J.* 849 (1987).

[38] Elizbeth Gillingham Daily. Comment: Beyond "Persons, Houses, Papers, and Effects": Rewriting the Fourth Amendment for National Security Surveillance. *10 Lewis & Clark L. Rev.* 641, 654-659 (2006)

[39] *เพิ่งอ้าง p. 80-81.*

[40] *เพิ่งอ้าง p. 90.*

[41] United States v. Charbonneau, 979 F.Supp. 1177, 1184 (S.D. Ohio 1997)

[42] Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007)

[43] United States v. Gines-Perez, 214 F.Supp. 2d 205, 224-26 (D.P.R. 2002)

[44] United States v. Butler, 151 F.Supp. 2d 82, 83-84 (D. Me.2001)

[45] Free Encyclopedia of Ecommerce. (n.d.). National Information Infrastructure

Protection Act (NIIPA) of 1996. Retrieved March 12, 2012, from http://ecommerce.hostip.info/pages/769/National-Information-Infrastructure-Protection-Act-NIIPA-1996.html

[46] ความผิดตามกฎหมายเดิม จะครอบคลุมไปถึงความผิดทางอาญากรณีบุกรุกเข้าไปในระบบคอมพิวเตอร์โดยปราศจากอำนาจ และก่อให้เกิดความเสียหายแก่ระบบหรือข้อมูลดังกล่าว นอกจากนี้ ยังได้กำหนดความผิดทางอาญา ในการเข้าถึงข้อมูลคอมพิวเตอร์ของทางราชการ และมีผลทำให้การเผยแพร่ หรือการส่งผ่านซึ่งข้อมูลอันเป็นความลับของทางราชการ รวมถึงการป้องกันการเจาะระบบข้อมูลในสถาบันทางการเงิน ไม่ว่าจะเป็นของรัฐหรือภาคเอกชน ประการต่อมา ยังได้ห้ามเข้าถึงข้อมูลทางราชการสำหรับคอมพิวเตอร์ที่ไม่ได้ใช่เป็นของสาธารณะ และ การห้ามเข้าถึงข้อมูลของคอมพิวเตอร์ที่มีการตั้งรหัสไว้ โดยปราศจากอำนาจหรือการอนุญาตโดยมีเจตนาที่จะฉ้อโกง หรือ ได้รับประโยชน์ทางทรัพย์สินจากข้อมูลนั้น เป็นต้น โปรดดูรายละเอียดเพิ่มเติมใน Free Encyclopedia of Ecommerce. (n.d.). National Information Infrastructure Protection Act (NIIPA) of 1996. Retrieved March 12, 2012, from http://ecommerce.hostip.info/pages/769/National-Information-Infrastructure-Protection-Act-NIIPA-1996.html

[47] ศาลสูงสุดได้เคยพิพากษาไว้ในคดี Warden v. Hayden, 387 U.S. 294, 309 (1967) ว่า เจ้าหน้าที่ตำรวจไม่อาจจะขอหมายค้น เพียงเพื่อพบพยานหลักฐานในการดำเนินคดี แต่จะต้องขอหมายค้นเพื่อยึดสิ่งของที่มีไว้เป็นความผิดตามกฎหมาย หรือ ได้ใช้ในการกระทำผิด หรือ ได้มาจากการกระทำผิด แต่ถ้าหากเป็นเพียงภาพของผู้กระทำผิด หรือ ผู้เดินขบวนประท้วง ฯลฯ เหล่านี้ เป็นเพียงพยานหลักฐานที่จะนำไปสู่การดำเนินคดีกับผู้ประท้วง ฯลฯ เท่านั้น ดังนั้น การออกหมายค้นในกรณีนี้ จึงไม่อาจจะกระทำได้

[48] รายละเอียด โปรดดู Computer Crime and Intellectual Property Section, Criminal Division, DoJ (2009). Searching and Seizing Computer and Obtaining Electronic Evidence in Criminal Investigations. Retrieved March 12, 2012, from http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

[49] เว็บไซต์ต่างประเทศที่ละเมิดทรัพย์สินทางปัญญา (foreign infringing sites) คือ เว็บไซต์ที่อยู่นอกเหนือเขตอำนาจศาลของสหรัฐอเมริกา แต่มีผลกระทบโดยตรงต่อสหรัฐอเมริกาในการ “กระทำการ สนับสนุน ส่งเสริม ก่อให้เกิด” การละเมิดทรัพย์สินทางปัญญา (“a website outside of US Jurisdiction but directed at the US, “committing “or “facilitating” intellectual property infringement.)

[50] “Dedicated to theft of intellectual property” หรือ เว็บไซต์ที่ให้บริการไปในทางที่ทำให้มีการละเมิด หรือผู้ให้บริการได้กระทำการในลักษณะหลีกเลี่ยงการยืนยันความเป็นได้อย่างมากของการละเมิดของเว็บไซต์

[51] Masurlaw. (n.d.). Summary of SOPA PIPA. Retrieved January 18, 2012, from http://www.masurlaw.com/resources/summary-of-sopa-and-pipa/

[52] First Amendment: “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances” The Supreme Court interprets the extent of the protection afforded to these rights. โปรดดูเพิ่มเติม Cornell University Law School. (2010, August 19). FIRST AMENDMENT: AN OVERVIEW. Retrieved January 18, 2012, from http://www.law.cornell.edu/wex/first_amendment

[53] Nebraska Press Assn. v. Stuart, 427 U.S. 539(1976)

[54] Freedman v. Maryland, 380 U.S. 51 58 (1965)

[55] Digital Millennium Copyright Act คือ กฎหมายที่คุ้มครองลิขสิทธิ์ ซึ่งอนุวัตรการตามพิธีสารขององค์การทรัพย์สินทางปัญญาโลกสองฉบับ คือ สนธิสัญญาลิขสิทธิ์ (WIPO Copyright Treaty 1996) และสนธิสัญญาการแสดงและสิ่งบันทึกเสียง (WIPO Performances and Phonograms Treaty 1996) สาระสำคัญของกฎหมาย คือ ปกป้องเทคโนโลยี และระบบบริหารลิขสิทธิ์ (Technological Protection and Copyright Management Systems) ซึ่งกำหนดมาตรการที่นำมาใช้เพื่อห้ามมิให้เกิดการกระทำรบกวน แก้ไข หรือเปลี่ยนแปลงเทคโนโลยีที่นำมาใช้ควบคุมการเข้าถึงหรือกระทำซ้ำงานอันมีลิขสิทธิ์

[56] Safe Harbor ตาม Digital Millennium Copyright Act 2008 คือ การให้ความคุ้มกันแก่ผู้ให้บริการจากการถูกฟ้องร้องดำเนินคดี ตราบใดที่ผู้ให้บริการเหล่านั้นกระทำการโดยสุจริตในการถอดเนื้อหาที่กระทำละเมิดทันทีที่ผู้ทรงสิทธิในทรัพย์สินทางปัญญาได้บอกกล่าว

[57] Rebecca Mackinnon. (2011, November 15). Firewall law could infringe free speech. *The New York Times*. Retrieved January 18, 2012, from http://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html

[58] Non-domestic domain name: a domain name for which the domain name registry is not located on the United States

[59] Information location tools: “a service that refers or links users to an online location on the World Wide Web. Such term includes directories, indices, references, pointers, and hypertext links.”

[60] Letter from Mark Lemley, Professor, Standford Law School, et al. to Sen. Judiciary Comm (2011, June 27), Retrieved January 18, 2012, from http://volokh.com/2011/07/04/amd-speaking-of-the-inalienable-right-to-pursuit-of-happiness

[61] Neil Richards, cited in Jessica Martin. (2012, January 17). SOPA, Protect IP will stifle creativity and diminish free speech. Retrieved January 18, 2012, from http://news.wustl.edu/news/pages/23260.aspx

[62] Gregory P. Magarian, cited in Jessica Martin. (2012, January 17). SOPA, Protect IP will stifle creativity and diminish free speech. Retrieved January 18, 2012, from

http://news.wustl.edu/news/pages/23260.aspx

[63] การก่อการร้ายตามกฎหมายสหรัฐอเมริกา หมายถึง การดำเนินกิจกรรมใดๆ ที่เกี่ยวข้องกับการกระทำการที่เป็นภยันตรายต่อชีวิตมนุษย์ หรือ จะมีผลอย่างแน่แท้ในการทำลายสาธารณูปโภคหรือทรัพยากรสำคัญของชาติอย่างร้ายแรง และ เป็นการกระทำที่ละเมิดหรือขัดต่อกฎหมายอาญาของสหรัฐฯ และการกระทำดังกล่าวข้างต้น จะต้องปรากฏว่า เป็นการกระทำที่มีลักษณะเป็นการข่มขู่หรือภัยคุกคามต่อพลเรือน หรือ ต้องการบังคับรัฐบาลโดยวิธีการเดียวกัน หรือ การกระทำที่เป็นการทำลายล้างอย่างร้ายแรง การลอบสังหาร หรือ การลักพาตัว ดังนั้น กฎหมายนี้ จึงไม่ได้ให้อำนาจใดๆ แก่รัฐบาลในการใช้อำนาจพิเศษกระทำการใดๆ ต่อประชาชนของตนเอง

[64] Reno v. ACLU, 929 F. Supp. 824 (1996), 521 U.S. 844 (1997)

[65] Specially Designated Global Terrorist (SDGTS) are entities and individuals who Office of Foreign Assets Control (OFAC) finds have committed or pose a significant risk of committing acts of terrorism, or who OFAC finds provide support, services, or assistance to, or otherwise associate with, terrorists and terrorist organizations designated under OFAC Counter Terrorism Sanctions programs, as well as such persons' subsidiaries, front organizations, agents, or associates. They are designated under OFAC's Counter Terrorism Sanction programs.

[66] Electronic Frontier Foundation. (n.d.). EFF Analysis Of The Provisions Of The USA PATRIOT Act. Retrieved August 1, 2012, from https://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php

[67] *เพิ่งอ้าง*.

[68] IFEX. (2012, January 19). IFEX member websites go dark in protest against online piracy bills. Retrieved August 1, 2012, from http://www.ifex.org/international/2012/01/19/sopa_pipa_protests/

[69] Wikipedia, the free encyclopedia. (n.d.). Protest against SOPA and PIPA. Retrieved August 1, 2012, from http://en.wikipedia.org/wiki/Protests_against_SOPA_and_PIPA

[70] เว้นแต่ Hate Speech นั้นจะมีลักษณะผสมผสานกับการกระทำที่นำไปสู่ความรุนแรง รัฐอาจจะกำหนดโทษทางอาญาเพราะการกระทำ (conduct) ดังกล่าวก็ได้ แต่ไม่ใช่เพราะการแสดงความคิดเห็น (speech) ตัวอย่างเช่น การเผาไม้กางเขน มีวัตถุประสงค์เพื่อข่มขู่หรือทำให้กลุ่มอื่นหวาดกลัวต่อกลุ่มผู้นับถือศาสนาที่แตกต่างกัน รัฐย่อมสามารถห้ามการกระทำดังกล่าวได้ (Virginia v. Black, 123 S.Ct. 1536 (2003))

[71] Kristina M. Reed. From The Great Firewall of China to the Berlin Firewall : The Cost of Content Regulation on Internet Commerce. *13 Transnat'l Law*. 451 (2000)

[72] Steven L. Emanuel, *อ้างแล้ว 5*, p. 445

[73] นอกจากนี้ ในกรณีที่รัฐได้ตรากฎเกณฑ์ในการควบคุมการแสดงความคิดเห็นใดๆ กฎเกณฑ์ดังกล่าวจะต้องไม่มีลักษณะที่มีผลบังคับใช้กว้างขวางเกินสมควร (over breadth) และจะต้องไม่มีลักษณะที่คลุมเครือ (vagueness) จนไม่ทราบว่าจะต้องดำเนินการอย่างไรบ้างเพื่อมิให้ขัดต่อกฎหมาย

กฎหมายจีน กับสิทธิเสรีภาพในสื่อออนไลน์

[1] โปรดดูรายละเอียดใน Reporter Without Borders. (n.d.). Press Freedom Index 2010. Retrieved July 20, 2011, from http://en.rsf.org/press-freedom-index-2010,1034.html

[2] ตัวอย่างเช่น พื้นที่การปกครอง Xingjiang Uyghur Autonomous Region (XURA) ในปี ค.ศ.2008 ทางการจีนได้จับกุมนาย Miradil Yasin และนาย Mutellip Teyip ที่แจกใบปลิวในมหาวิทยาลัย Xinjiang ชักชวนนักศึกษาร่วมรณรงค์ต่อต้านการขายบุหรี่และสุราในมหาวิทยาลัย แต่เจ้าหน้าที่จับกุมเพราะเห็นว่าเป็นการก่อความไม่สงบเรียบร้อยบนถนนหนทาง เป็นต้น โปรดดู Congressional-Executive Commission on China. (2009, October 10). Congressional – Executive Commission on China Annual Report 2009. Retrieved July 20, 2011, from http://www.cecc.gov/pages/annualRpt/annualRpt09/CECCannRpt2009.pdf, pp.48-199; และเว็บไซต์ของ The Congressional-Executive Commission on China ที่ http://www.cecc.gov

[3] โปรดดู Congressional-Executive Commission on China. (2010, February 26). Beijing High People's Court Affirms Liu Xiaobo's 11-Year Sentence. Retrieved October 10, 2010, from http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle-136147, (ทางการจีนปิดกั้นเว็บไซต์ที่เกี่ยวข้องกับ ดาไล ลามะ การสลายการชุมนุมที่จัตุรัสเทียนอันเหมิน เรื่องราวเกี่ยวกับลัทธิฝ่าหลุนกง การเรียกร้องให้ปฏิรูปทางการเมือง ในปี 2008 ที่นักวิชาการและประชาชนเข้าร่วมลงชื่อในเอกสาร Charter 08 กว่า 9,700 คน ซึ่งในปี 2009 รัฐบาลจีน ได้จับกุมนาย Liu Xiaobo ผู้ร่วมลงชื่อในเอกสารดังกล่าว โดยเขาไม่มีสิทธิมีทนายความ และญาติไม่อาจเข้าเยี่ยมเกินกว่า 6 เดือน และถูกดักฟังตลอดเวลา ภายหลังเขาได้ถูกฟ้องร้องในข้อหายุยงส่งเสริมให้ประชาชนล้มล้างการปกครองของรัฐบาลจีน (Inciting subversion) โดยการเผยแพร่ข้อความอันเป็นข่าวลือ และให้ร้ายรัฐบาลจีน ท้ายที่สุด ศาลได้พิพากษาจำคุกเขาเป็นเวลา 11 ปี ต่อมาเขาก็ได้รับรางวัลโนเบล สาขาสันติภาพ ปี 2010 จากประเทศนอร์เวย์ เนื่องจากได้รณรงค์เพื่อสิทธิมนุษยชนอย่างสงบในประเทศจีนมาเป็นเวลากว่า 20 ปีแล้ว โปรดดูรายละเอียด The Nobel Peace Prize 2010. (n.d.). Retrieved October 10, 2010, from http://www.nobelprize.org/nobel_peace_prizes/laureates/2010/press.html

[4] ตัวอย่างเช่น ตาม Notice Regarding Certain Problems with Recent Publishing of Periodicals ค.ศ. 1998 กำหนดให้ผู้เสนอข้อมูลข่าวจะต้องปฏิบัติตามวิธีการที่กำหนดโดย

พรรคคอมมิวนิสต์ รวมถึงนโยบายต่างๆ ที่ประเทศได้กำหนดไว้ โดยข้อมูลที่เสนอนั้นจะต้องสอดคล้องกับข้อกำหนดของจิตวิญญาณประชาชนสังคมนิยม

[5] Cont. of People's Republic of China. Art. 35 "Citizens of the PRC have freedom of speech, publication, assembly, association, procession and demonstration."

[6] มาตรา 5 แห่ง ระเบียบการบริหารงานสื่อสิ่งพิมพ์ (Regulations on the Administration of Publishing 2001)

[7] มาตรา 24 แห่ง ระเบียบการบริหารงานสื่อสิ่งพิมพ์ (Regulations on the Administration of Publishing 2001)

[8] สำหรับ Notice Regarding Prohibiting the Transmission of Harmful Information and Further Regulating Publishing Order ค.ศ.2001 ข้อ 2 นั้น กำหนดว่าการก่อตั้งสำนักงานเผยแพร่ข้อมูลข่าวสารจะต้องได้รับอนุญาต โดยยื่นคำขอต่อ Press and Publication Administration Agency ส่วนการจัดตั้งสำนักพิมพ์เพื่อการค้า จะต้องได้รับใบอนุญาต Printer Operating License ตาม Regulations on the Administration of Printing Enterprises ค.ศ.2001 และก่อนตีพิมพ์จะต้องผ่านการตรวจสอบก่อน (censor) ถ้าฝ่าฝืนจะมีความผิดทางอาญา ส่วนการจัดพิมพ์ข้อมูลเกี่ยวกับความมั่นคงของประเทศและประวัติผู้นำประเทศจะต้องจัดพิมพ์โดยสำนักงานพิมพ์ของรัฐ (A Publishing Work Unit) เท่านั้น

[9] ตามกฎหมาย Telecommunication Regulation of China, Measure on the Administration of International Communication Ports รัฐบาลจีนถือหลัก เสรีภาพมีค่าน้อยกว่าผลประโยชน์ของชาติ หรือ Freedom of the press should be subordinate to the interest of the nation. โปรดดู Charles Li. Internet Content Control in China. 8 Int'l J. Comm. L. & Pol'y 1, 7-8 (Winter 2003/2004)

[10] คำว่าข้อมูลข่าวสารในมาตรา 111 แห่งประมวลกฎหมายอาญา หมายถึง สิ่งใดๆ ซึ่งเกี่ยวข้องกับความปลอดภัยและผลประโยชน์ของชาติ ซึ่งต้องห้ามตีพิมพ์เผยแพร่ต่อสาธารณะภายใต้กฎเกณฑ์ที่เกี่ยวข้อง โดยข้อมูลข่าวสารนั้นถูกห้ามไม่ให้ตีพิมพ์เผยแพร่สู่สาธารณะ

ใน "อรรถาธิบายประเด็นที่เกี่ยวข้องกับกฎหมายเฉพาะด้านที่ใช้ในการพิจารณาคดีว่าด้วยการขโมยหรือจารกรรมเพื่อการได้มาซึ่ง หรือการไขความลับหรือการข่าวของรัฐโดยผิดกฎหมายแก่ชาวต่างชาติ" มาตรา 5 ระบุว่า บุคคลใดก็ตามที่รู้ หรือ ควรจะรู้ว่าข้อมูลใดๆ ซึ่งแม้ว่าจะไม่ได้ถูกแสดงเครื่องหมายไว้ว่าเป็นความลับ และได้มาโดยการล้วงความลับหรือการซื้อหา หรือ วิธีการอื่นๆ ที่ผิดกฎหมาย และกระจายข่าวสารดังกล่าวไปยังชาวต่างชาติ จะต้องถูกฟ้องร้องดำเนินคดีและลงโทษ ตามมาตรา 111 แห่งประมวลกฎหมายอาญา และ มาตรา 6 ระบุว่า บุคคลใดก็ตามที่ใช้อินเทอร์เน็ต เพื่อการส่งข้อมูลลับของประเทศ หรือ ข้อมูลข่าวสารใดๆ ถึงชาวต่างชาติ องค์กร หรือ เอกชน จะต้องถูกฟ้องร้องและลงโทษ ภายใต้บทบัญญัติในมาตรา 111 แห่งประมวลกฎหมายอาญา และหากข้อมูลที่ส่งนั้นเป็นความลับและได้รับการประกาศว่าเป็นข้อมูลที่มีความสำคัญแล้ว บุคคลที่กระทำผิดข้างต้น จะต้องถูกดำเนินคดีอาญาตาม มาตรา 398 แห่งประมวลกฎหมายอาญา

[11] รัฐบาลจีนได้ตรามาตรการสำหรับการดำเนินงานภายใต้กฎหมายความมั่นคงของรัฐ (Measures for the Implementation of the Law on State Security ค.ศ. 1994) เพื่อขยายความกฎหมายดังกล่าว เพื่อทำให้การสอบสวนดำเนินคดีกับผู้ถูกกล่าวหามีประสิทธิภาพยิ่งขึ้น เช่น

มาตรา 7 ดังที่ได้บัญญัติไว้ใน มาตรา 4 ของกฎหมายว่าด้วยความมั่นคงของรัฐ (The Law on State Secrets) คำว่า วางแผนร่วมกัน หรือ สมคบกัน (collude) เพื่อที่จะกระทำการซึ่งจะก่อให้เกิดความไม่มั่นคงของรัฐ อันเกี่ยวข้องกับการกระทำขององค์กร หรือ บุคคล ในอาณาเขตของประเทศจีน ในการกระทำการดังต่อไปนี้

(1) การวางแผนร่วมกัน หรือดำเนินการร่วมกับรัฐบาลต่างประเทศ องค์กร หรือปัจเจกชน ในการทำให้เกิดภยันตรายต่อความมั่นคงของรัฐ

(2) การได้รับทุนจากบุคคลตามข้อ (1) เพื่อช่วยเหลือ หรือดำเนินกิจกรรมซึ่งเป็นภยันตรายต่อความมั่นคงของรัฐ

(3) การก่อตั้งสมาคมหรือองค์กรที่ร่วมกัน หรือได้รับความช่วยเหลือจาก หรือ ช่วยเหลือ หรือ ดำเนินการร่วมกับบุคคลตามข้อ (1) ซึ่งกิจกรรมอันจะเป็นภยันตรายต่อความมั่นคงของรัฐ

มาตรา 8 การกระทำต่อไปนี้ ถือเป็นการกระทำกิจกรรมการอื่นใด ซึ่งจะเป็นอันตรายต่อความมั่นคงของรัฐ ภายใต้ มาตรา 4 ของกฎหมายว่าด้วยความมั่นคงของรัฐ จัดตั้งองค์กรอาชญากรรม หรือวางแผน หรือดำเนินการซึ่งการก่อการร้าย อันเป็นอันตรายต่อความมั่นคงของรัฐ การสร้างพยานหลักฐานอันเป็นเท็จ หรือ การบิดเบือนข้อเท็จจริง หรือการเผยแพร่ข้อมูลใดๆ หรือ การทำให้แพร่หลายซึ่งข้อเขียน หรือการพูด หรือการผลิต หรือการส่งต่อซึ่งผลิตภัณฑ์ภาพและเสียง ซึ่งจะเป็นอันตรายต่อความมั่นคงของรัฐ การแสวงประโยชน์ จากกลุ่มหรือบรรษัทที่จัดตั้งขึ้น เพื่อดำเนินกิจกรรมที่จะเป็นอันตรายต่อความมั่นคงของรัฐ ก่อให้เกิดความแตกแยกในหมู่ชน หรือก่อให้ประชาชนกระด้างกระเดื่อง ให้เกิดการแตกแยกระหว่างประชาชนในลักษณะที่จะก่อให้เกิดภยันตรายต่อความมั่นคงของรัฐ บุคคลชาวต่างชาติใดๆ ซึ่งได้กระทำการละเมิดกฎเกณฑ์ที่เกี่ยวข้อง โดยปราศจากอำนาจ ได้พบกับบุคลากรในประเทศจีน ผู้ซึ่งกระทำกิจกรรมที่เป็นภยันตรายต่อความมั่นคงของรัฐ หรือ บุคคลผู้ต้องสงสัยว่าจะกระทำกิจกรรมที่เป็นอันตรายต่อความมั่นคงของรัฐ

[12] Yutian Ling. Upholding Free Speech and Privacy Online: A Legal-Based and Market-Based Approach for Internet Companies in China. *Santa Clara Computer & High Tech. L. J.*, Vol.27, (February, 2011), p. 175, 179-180

[13] การจัดตั้งสำนักพิมพ์ ผู้ขออนุญาตต้องมีรายได้ไม่น้อยกว่า 300,000 หยวน (37,500 เหรียญสหรัฐอเมริกา) และมีหน่วยงานรัฐรับรอง ทั้งๆ ที่รายได้จากการจำหน่ายหนังสือพิมพ์อาจจะไม่เกิน 10,000 หยวน (1,250 เหรียญสหรัฐอเมริกา) เท่านั้น

[14] Wikipedia, the free encyclopedia. (n.d.). Internet in the People's Republic of China. Retrieved July 20, 2011, from http://en.wikipedia.org/wiki/Internet_in_the_People's_Republic_of_China (ปัจจุบัน จะมีหน่วย telecom provider ให้บริการอินเทอร์เน็ต

ประจำอยู่ตามจังหวัด เพื่อให้เอกชนมาขอดำเนินการให้บริการอีกต่อหนึ่ง)

[15] Business-in-Asia. (n.d.). The Internet in China. Retrieved 2011, June 19, from http://www.business-in-asia.com/internet_report.html, (บริษัทดังกล่าว จะมีที่ตั้งอยู่ที่เมืองใหญ่ๆ เช่น Beijing, Shanghai, Guangzhou, Tianjin และ Xiamen เป็นต้น โดยมีบริษัท China Telecom ซึ่งเป็นของรัฐบาลจีนเอง เป็นผู้ให้บริการที่ใหญ่ที่สุด และมี China United Telecommunications Corporation บริษัทใหญ่อันดับสอง ที่ให้บริการกว่า 100 เมือง นอกจากนี้ ยังมี 263.net และ gznet.com ที่ดำเนินการโดยบริษัท Guangzhou Favour Telecom Co. ส่วน Shanghai Online ซึ่งดำเนินการโดยรัฐบาลท้องถิ่นแห่ง Shanghai ก็มีส่วนแบ่งทางการตลาดในจีนจำนวนมากเช่นกัน

[16] มาตรา 70, บุคคลใดก็ตาม โดยปราศจากการอนุมัติ ที่ก่อตั้งสำนักพิมพ์ การจัดทำสำเนา หรือ การเผยแพร่งานสำคัญทางอิเล็กทรอนิกส์ หรือ มีวัตถุประสงค์ที่จะประกอบธุรกิจการตีพิมพ์ การจัดทำสำเนา หรือ การนำเข้า และ การกระจายสินค้าทางอิเล็กทรอนิกส์ จะถูกสั่งปิด และวัสดุอุปกรณ์ หรือ เครื่องมือที่ใช้สำหรับการกระทำผิดดังกล่าว รวมถึง เงินรายได้ซึ่งมาจากการกระทำผิดดังกล่าว จะต้องถูกริบให้สิ้น และจะต้องถูกปรับระหว่าง 2 - 10 เท่า ของรายได้ที่ได้มาจากการกระทำผิดกฎหมายนั้น

[17] ตัวอย่างที่อาจจะมีการเผยแพร่ข้อมูลเกี่ยวกับ การวิจารณ์ผู้นำพรรค หรือ ชาติ ผู้เผยแพร่ข้อมูลจะต้องปฏิบัติตาม Regulations Regarding Strengthening the Administration of Publications Describing Major Party and National Leaders ค.ศ. 1990

[18] มาตรา 3 แห่ง Measures on the Administration of Foreign Satellite Television Channel Reception

[19] มาตรา 4 แห่ง Measures on the Administration of Foreign Satellite Television Channel Reception

[20] มาตรา 6 แห่ง Measures on the Administration of Foreign Satellite Television Channel Reception

[21] แปลจาก Congressional-Executive Commission on China. (n.d.). Domestic Laws and Regulations: Vague and Overbroad Regulations. Retrieved July 20, 2011, from http://www.cecc.gov/pages/virtualAcad/exp/explaws.php

[22] Yutian Ling, *อ้างแล้ว 12*, p. 177.

[23] Notice Regarding Further Strengthening the Administration of Periodicals Relating to Current Affairs and Politics, General Lifestyle, Information Tabloids and Scientific Theory ค.ศ. 2000

[24] Yutian Ling, *อ้างแล้ว 12*, p. 184.

[25] www.china.org.cn

[26] Congressional-Executive Commission on China. (2006, September 20). Congressional – Executive Commission on China Annual Report 2009. Retrieved July 7,

2010, from http://www.cecc.gov/pages/annualRpt/annualRpt06/CECCannRpt2006.pdf

[27] Supreme People's Court Interpretation Regarding Certain Questions About the Specific Laws to be Used in Adjudicating Criminal Cases of Illegal Publication.

[28] Congressional-Executive Commission on China. (n.d.). Agencies Responsible for Censorship in China. Retrieved July 7, 2010, from http://www.cecc.gov/pages/virtualAcad/exp/expcensors.php

[29] ตัวอย่างเช่น การปิดกั้นได้แก่ รายการ Voice of America และ รายการ Radio Free Asia ซึ่งเป็นความถี่คลื่นสั้นไปยังประเทศจีน ซึ่งมีการร้องเรียนไปยังรัฐบาลจีนตั้งแต่ปี 2000 รวมถึงกฎเกณฑ์ต่างๆ ที่จำกัดสิทธิของปัจเจกชนในการมีกรรมสิทธิ์เครื่องรับสัญญาณดาวเทียม ยกเว้น โรงแรมสามดาวขึ้นไป และบ้านพักสำหรับชาวต่างชาติเท่านั้น โดยจะต้องขอรับอนุญาตจากรัฐเสียก่อน หากเห็นว่าการถ่ายทอดรายการดังกล่าวเป็นอันตรายต่อรัฐ เจ้าหน้าที่ของรัฐก็จะตัดสัญญาณทันที ซึ่งอาจจะตัดสัญญาณชั่วคราว หรือตลอดไปก็แล้วแต่กรณี

[30] Steven Seidenberg. Breaking China: WTO complaint could end the "Great Firewall" Internet ban. *96 A.B.A.J.*, November 2010, p. 20

[31] Larry X. Wu, Second Secretary for Science and Technology at the Embassy of the People's Republic of China in Washington, DC, quoted in Patrick Di Justo. (2003, March 18). Does the End Justify the Means? Retrieved July 7, 2010, from http://www.wired.com/politics/law/news/2003/03/58082

[32] Keith J. Winstein. China Blocks MIT Web Addresses. *The Tech*, 22 November 2002, Volume 122, Number 58

[33] Congressional-Executive Commission on China. (n.d.). Blocking, Filtering, and Monitoring. Retrieved July 7, 2010, from http://www.cecc.gov/pages/virtualAcad/exp/expjamming.php

[34] อย่างไรก็ตาม ผู้ใช้อินเทอร์เน็ตในประเทศจีน ซึ่งค้นหาข้อมูลในภาษาอังกฤษ หากเป็นการรายงานข่าวจากประเทศตะวันตกทั่วไปแล้ว ก็อาจจะผ่าน National Firewall ได้บ้าง แต่หากมีการใช้ภาษาจีนแล้ว เจ้าหน้าที่ของรัฐก็จะปิดกั้นข่าวสารภาษาจีนโดยเฉพาะเนื้อหาสาระที่เกี่ยวข้องกับเว็บไซต์ภาษาอังกฤษที่รัฐบาลจีนไม่อาจจะควบคุมได้ ตัวอย่างเช่น ผู้ใช้อินเทอร์เน็ต อาจจะเข้าเว็บไซต์ BBC และ Radio Canada ในภาคภาษาอังกฤษได้ แต่ในภาคภาษาจีนไม่อาจจะเข้าถึงได้ การปิดกั้นหรือกลั่นกรองเว็บไซต์ต่างๆ ของประเทศจีน ยังจะยิ่งเข้มงวดยิ่งขึ้นในบางสถานการณ์ และ อาจจะผ่อนคลายในบางช่วงเวลา ตัวอย่างเช่น รัฐบาลจีน ได้ปิดกั้นการเข้าถึงเว็บไซต์ข่าวสารของสำนักข่าวต่างประเทศ แม้บางกรณีจะเป็นภาษาอังกฤษ เช่น New York Times , Washington Post, Wall Street Journal, และ สำนักข่าว CNN โดยเฉพาะในช่วงการประชุมเมื่อครั้งที่ 16 ของสภาคองเกรส เมื่อเดือน พฤศจิกายน ค.ศ. 2002 และ การประชุมครั้งที่ 10 ของสภาคองเกรส เมื่อเดือนมีนาคม ค.ศ. 2003 ซึ่งมีการวิพากษ์วิจารณ์นโยบายในการปิดกั้นเสรีภาพในการแสดงความคิด และ อินเทอร์เน็ตใน

ประเทศจีน เป็นต้น

[35] Edward Wong and David Barboza. (2011, January 31). Wary of Egypt Unrest, China Censors Web. *The New York Times*. Retrieved July 20, 2011, from http://www.nytimes.com/2011/02/01/world/asia/01beijing.html?_r=0

[36] Andrew Jacobs. (2010, July 30). China Imprisons 3 Men Who Maintained Uighur Web Sites. *The New York Times*. Retrieved August 21, 2012, from http://www.nytimes.com/2010/07/31/world/asia/31china.html

[37] For a thorough study of how BBSs in China are censored, see Reporters Without Borders. (2003, May 12). Living Dangerously on the Net. Retrieved July 20, 2011, http://en.rsf.org/china-living-dangerously-on-the-net-12-05-2003,06793.html

[38] Congressional-Executive Commission on China. (n.d.). Measures for the Administration of Internet Information Services. Retrieved July 7, 2010, from http://www.cecc.gov/pages/virtualAcad/exp/explaws.php#internetmeasures

[39] Congressional-Executive Commission on China. (n.d.). Regulations on the Administration of Internet Access Service Business Establishments [Internet Cafes], Retrieved July 7, 2010, from http://www.cecc.gov/pages/virtualAcad/exp/explaws.php#internetcaferegs

[40] อย่างไรก็ตาม ร้านอินเทอร์เน็ตคาเฟ่บางแห่ง ก็ละเลยไม่ได้ดำเนินการอย่างเข้มงวดไปทุกกรณีก็มีเช่นกัน

[41] Nellie L. Viner. The Global Online Freedom Act: Can U.S. Internet Companies Scale the Great Chinese Firewall at the Gates of the Chinese Century? *93 Iowa L. Rev*. 361, 363 (November, 2007) (ตัวอย่างเช่น ในปี ค.ศ. 2004 รัฐบาลจีนได้กดดันให้ Yahoo เปิดเผยข้อมูลนาย Shi Tao บรรณาธิการของหนังสือพิมพ์ Contemporary Business News ผู้เผยแพร่ผ่านระบบอีเมลผ่านบัญชีของ Yahoo ไปยังต่างประเทศ ถึงคำเตือนของรัฐบาลจีนที่ห้ามเสนอบทความที่ก่อให้เกิดความวุ่นวายในวาระครบรอบ 15 ปีของเหตุการณ์ Tiananmen Square Massacre ทำให้เขาถูกจำคุกนานถึง 10 ปี)

[42] ตัวอย่าง เช่น เดือนมีนาคม 2009 เจ้าหน้าที่ตำรวจจากเมือง Lingbao จังหวัด Henan ได้เดินทางมาถึงเมือง Shanghai ด้วยระยะทาง 1,200 กิโลเมตร เพื่อจับกุม Wang Shuai หลังจากที่เขาได้โพสต์ข้อความว่า เจ้าหน้าที่ของเมือง Lingbao ได้ยักยอกงบประมาณแก้ปัญหาภัยแล้ง แล้วนำตัวกลับไปที่เมือง Lingpao และ เดือนเมษายน 2009 หนังสือพิมพ์ China Daily รายงานว่า ตำรวจจับกุมนาย Shi Zhixian นักเขียนอิสระ (blogger) เป็นเวลา 3 วัน ซึ่งวิจารณ์เจ้าหน้าที่เลือกตั้งที่มีการกระทำไม่สุจริต โปรดดู, Sophie Beach. (2009, May 6). Joshua Rosenzweig: China's Battle Over the Right to Criticize. China Digital Time. Retrieved July 20, 2011, from http://chinadigitaltimes.net/2009/05/joshua-rosenzweig-chinas-battle-over-the-right-to-criticize/

[43] รัฐบาลจีน ได้จับกุมประชาชนที่จัดกิจรรมระลึกเหตุการณ์จัตุรัสเทียนอันเหมิน อย่างต่อเนื่อง เช่น ใน เดือนมีนาคม 2009 ได้จับกุมนาย Zhang Shijun ผู้เขียนจดหมายเปิดผนึกถึงรัฐบาลจีนให้สืบสวนเหตุการณ์ดังกล่าวใหม่ และได้สัมภาษณ์ต่อสื่อมวลชนต่างประเทศ เดือนเมษายน 2009 ได้จับกุมนาย Qi Zhiyong ซึ่งสูญเสียขาจากการสลายการชุมนุม ปี 1989 หลังจากให้สัมภาษณ์สื่อมวลชนต่างประเทศ เดือนมีนาคม และ พฤษภาคม ต่อเนื่องกัน เจ้าหน้าที่ฝ่ายความมั่นคงได้จับกุมตัว Dr. Jiang Qisheng นักเขียนและรองประธาน Independent Chines PEN Center พร้อมกับยึดเครื่องคอมพิวเตอร์ หนังสือ และรายงานการสลายการชุมนุมและผลการสลายการชุมนุมดังกล่าว เดือนมิถุนายน ปีเดียวกัน รัฐบาลจีนได้ส่งนาย Zhang Huaiyang ไปทำงานเป็นเวลาหนึ่งปีครึ่ง ในข้อหาพยายามล้มล้างอำนาจรัฐบาล อันเป็นผลมาจากการที่เขาได้ร่วมลงชื่อใน Charter 08 และเผยแพร่บทความบนระบบออนไลน์ในหัวข้อ “Is There Really No One Who Dares To Take to the Street Commemorate 6-4? รวมถึงการคุกคามนักกิจกรรม 65 คน เพื่อมิให้พวกเขาจัดงานรำลึกเหตุการณ์ดังกล่าว และควบคุมตัว Wu Gaoxing ที่ได้แต่งกายโดยมีข้อความรำลึกถึงเหตุการณ์นั้น ในขณะขับขี่รถจักรยานยนต์ไปตามทางสาธารณะ ฯลฯ รายละเอียดอื่นๆ โปรดดูใน The Congressional-Executive Commission on China ที่ http://www.cecc.gov

[44] Congressional-Executive Commission on China. (n.d.) Congressional-Executive Commission on China 2006 Annual Report, Monitoring Compliance with Human Rights. Retrieved July 7, 2010, from http://www.cecc.gov/pages/annualRpt/annualRpt06/Expression.php?PHPSEESID=767f...

[45] Michael Kan. (2012, June 15). Protests, Not Criticism, the Target for China’s Internet Censors, Study Says. *PCWorld*. Retrieved August 15, 2012, from http://www.pcworld.com/businesscenter/article/257707/protests_not_criticism_the_target_for_chinas_internet_censors_study_says.html

[46] Larry X. Wu, Second Secretary for Science and Technology at the Embassy of the People’s Republic of China in Washington, DC, cited in Patrick Di Justo. (2003, March 18). Does the End Justify the Means? Retrieved July 7, 2010, from http://www.wired.com/politics/law/news/2003/03/58082

[47] French, Howard W. (2008, February 4). Chinese begin to protest censorship of Internet. *The New York Times*. Retrieved July 21, 2011, from http://www.nytimes.com/2008/02/04/world/asia/04iht-wall.1.9716090.html

[48] *เพิ่งอ้าง*.

[49] *เพิ่งอ้าง*.

[50] *เพิ่งอ้าง*.

[51] Asianews. (2009, February 7). Public protest in Beijing against internet censorship. Retrieved July 21,2011, from http://www.asianews.it/news-en/Public-protest-in-Beijing-

against-internet-censorship-15677.html

[52] Freedom house. (n.d.). Google Applauded for Stance on China Internet Censorship. Retrieved July 21,2011, from http://www.freedomhouse.org/article/google-applauded-stance-china-internet-censorship

[53] Editorial. (2010, July 1). Google vs. China, the Sequel. *The New York Times*. Retrieved July 21,2011, from http://www.nytimes.com/2010/07/02/opinion/02fri3.html?_r=1&ref=internet_censorship

[54] *เพิ่งอ้าง*.

[55] Stone, Brad and David Barboza. (2010, July 29). Google to Stop Redirecting China Users. *The New York Times*. Retrieved July 21, 2011, from http://www.nytimes.com/2010/06/30/technology/30google.html?ref=internet_censorship

[56] เว็บไซต์ไมโครบล็อก (microblog) ยอดนิยมของประเทศจีน มีระบบเหมือนทวิตเตอร์ ซึ่งไม่สามารถใช้ได้ในประเทศจีนอันเป็นผลจากนโยบายการปิดกั้นอินเทอร์เน็ต

[57] Wong, Edward and David Barboza. (2011, January 31). Wary of Egypt Unrest, China Censors Web, *อ้างแล้ว 35*.

[58] *เพิ่งอ้าง*.

[59] *เพิ่งอ้าง*.

[60] ตัวอย่างเช่น ตาม Notice Regarding Certain Problems with Recent Publishing of Periodicals ค.ศ. 1998 กำหนดให้ผู้เสนอข้อมูลข่าวจะต้องปฏิบัติตามวิธีการที่กำหนดโดยพรรคคอมมิวนิสต์ รวมถึงนโยบายต่างๆ ที่ประเทศได้กำหนดไว้ โดยข้อมูลที่เสนอนั้นจะต้องสอดคล้องกับข้อกำหนดของจิตวิญญาณประชาชนสังคมนิยม

[61] Congressional-Executive Commission on China. (2009, October 10). Congressional – Executive Commission on China Annual Report 2009, *อ้างแล้ว 2*, pp. 3-4

[62] Nellie L. Viner, *อ้างแล้ว 41*.

[63] Jennifer Shyu. Speak No Evil: Circumventing Chinese Censorship. *45 San Diego L. Rev*. 211, 225 (Winter, 2008)

[64] Guobin Yang. *The Power of the Internet in China: Citizen Activism Online*, (New York: Columbia University Press, 2009).

กฎหมายมาเลเซีย กับสิทธิเสรีภาพในสื่อออนไลน์

[1] Ann Elizabeth Mayer, *Islam and Human Rights: Tradition and Politics*, (Boulder, Colo.: Westview Press, 1999), p. 52.

[2] Article 3 (1) Federal Constitution of Malaysia, “Islam is the religion of the Federation; but other religions may be practised in peace and harmony in any part of the Federation.”

[3] Ann Elizabeth Mayer, *อ้างแล้ว 1*, p. 52.

[4] Mohammad Hashim Kamali, *Freedom of Expression in Islam*, (Malaysia: Ilmiah Publishers Sdn Bhd, 2000), p. 8.

[5] Christopher Weeramantry, *Islamic Jurisprudence: An International Perspective*, (Malaysia: The Other Press, 2001), p. 180.

[6] "Every person has the right to express his thoughts and beliefs so long as he remains within the limits prescribed by the Law. No one, however, is entitled to disseminate falsehood or to circulate reports that may outrage public decency, or to indulge in slander, innuendo, or to cast defamatory aspersions on other persons".

[7] "It is the right and duty of every Muslim to protest and strive [within the limits set out by the Law] against oppression even if it involves challenging the highest authority in the State".

[8] Article 10 Federal Constitution of Malaysia, "...(4) In imposing restrictions in the interest of the security of the Federation or any part thereof or public order under Clause (2) (a), Parliament may pass law prohibiting the questioning of any matter, right, status, position, privilege, sovereignty or prerogative established or protected by the provisions of Part III, article 152, 153 or 181 otherwise than in relation to the implementation thereof as may be specified in such law."

[9] http://malaysiakini.com

[10] Steven Gan. (2001, April 29). Ending the government's monopoly on the truth. *The guardian*. Retrieved March 21, 2012, from http://www.guardian.co.uk/technology/2001/apr/29/freespeech.observercampaignpressfreedom

[11] ดูรายละเอียดใน OpenNet. (n.d.). Malaysia. Retrieved March 20, 2012, from http://opennet.net/research/profiles/malaysia หรือดาวน์โหลดเอกสารรายงานได้ที่ http://opennet.net/sites/opennet.net/files/malaysia.pdf

[12] ดูรายละเอียดเพิ่มเติมใน The Communications and Multimedia Content Forum of Malaysia. (n.d.). Retrieved March 20, 2012, from http://www.cmcf.my/home.php

[13] Article 211 The Communications and Multimedia Act of 1998, "(1) No content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.

(2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of one thousand ringgit for every day or part of a day during which the offence is continued after conviction.

[14] The Communications and Multimedia Content Forum of Malaysia. (2004, September 1). The Malaysian Communications and Multimedia Content Code. Retrieved March 20, 2012, from http://www.cmcf.my/download/cmcf-content-code-english.pdf

[15] Section 8 Internal Security Act 1960, Power to order detention or restriction of persons. "(i) If the Minister is satisfied that the detention of any person is necessary with a view to preventing him from acting in any manner prejudicial to the security of Malaysia or any part thereof or to the maintenance of essential services therein or the economic life thereof, he may make an order (hereinafter referred to as a detention order) directing that that person be detained for any period not exceeding two years."

[16] The star online. (2009, April 12). Time to repeal the ISA. Retrieved June 12, 2012, from http://thestar.com.my/news/story.asp?file=/2009/4/12/focus/3658721&sec=focus

[17] Road to Independence. (n.d.). Retrieved June 12, 2012, from http://countrystudies.us/singapore/10.htm

[18] New Straits Times. (2007, January 2). Ismail's struggle to form Malaysia and Asean. cited in accessmylibrary. Retrieved June 12, 2012, from http://www.accessmylibrary.com/article-1G1-156712021/ismail-struggle-form-malaysia.html;

Malaysiana1. (2008, August.). Tun Dr Ismail - The Man Who Saved Malaysia. Retrieved June 12, 2012, from http://malaysiana1.blogspot.com/2008/08/tun-dr-ismail-man-who-saved-malaysia.html

[19] Hardial Singh Khaira. (2009, March 18). Is it the I.S.A. per se or the Interpretations Given by the Judiciary that makes it Such a Draconian Law Now? Retrieved June 3, 2012, from http://www.scribd.com/doc/13365695/Internal-Security-Act-the-Judiciary

[20] BBC. (2008, November 7). Malaysia blogger's joy at release. Retrieved June 3, 2012, from http://news.bbc.co.uk/2/hi/asia-pacific/7714696.stm

[21] cijmy. (2010, September 25). The Sedition Act 1948. *Centre for Independent Journalism*. Retrieved June 3, 2012, from http://cijmalaysia.org/miniportal/2010/09/the-sedition-act-1948/

[22] *เพิ่งอ้าง*.

[23] Clara Chooi. (2011, April 24). Najib repeats promise of no Internet censorship. *The Malaysian insider*. Retrieved June 3, 2012, from http://www.themalaysianinsider.com/malaysia/article/najib-repeats-promise-of-no-internet-censorship/

[24] Jonathan Kent. (2003, May 29). Malaysia's censorship strangles growth. *BBC*. Retrieved June 5, 2012, from http://news.bbc.co.uk/2/hi/business/2947264.stm

[25] Sanja Kelly & Sarah Cook. [Eds.]. (2011, April 18). Freedom on the Net 2011: A Global Assessment of Internet and Digital Media. Retrieved June 30, 2012, from http://www.freedomhouse.org/sites/default/files/FOTN2011.pdf, p. 229-238.

[26] Reuters. (2011, June 17). Hackers strike Malaysian websites for a second day. Retrieved June 10, 2012, from http://www.reuters.com/article/2011/06/17/us-malaysia-hackers-idUSTRE75G1OE20110617

[27] M. Kumar, Wong Pek Mei and Jo Timbuong. (2011, June 11). No more free downloads as MCMC blocks 10 file sharing sites. *The star online*. Retrieved June 5, 2012, from http://thestar.com.my/news/story.asp?file=/2011/6/11/nation/8879884&sec=nation

[28] The Malaysian insider. (2010, August 16). New survey revives spectre of Malaysian - Green Dam. Retrieved June 5, 2012, from http://www.themalaysianinsider.com/malaysia/article/new-survey-revives-spectre-of-malaysian-green-dam/

[29] The Sidney Morning Herald. (n.d.). Malaysia Mulls Internet Laws against Bloggers. Cited in *iBLS*. Retrieved June 7, 2012, from http://www.ibls.com/internet_law_news_portal_view.aspx?id=1872&s=latestnews

Vpn Accounts. (n.d.). Malaysian Internet Censorship - Bypass it!. Retrieved June 7, 2012, from http://www.vpnaccounts.com/malaysian-internet-censorship.html

[30] Malaysiakini. (2009, September 4). MCMC tells Malaysiakini: Take down videos. Retrieved June 8, 2012, from http://www.malaysiakini.com/news/112111

[31] Nurbaiti Hamdan and Cheok Li Peng. (2008, August 28). ISPs ordered to cut access to Malaysia Today website. *The star online*. Retrieved June 7, 2012, from http://thestar.com.my/news/story.asp?file=/2008/8/28/nation/22187596&sec=nation

[32] Bill of Guarantees (BoGs) คือ บันทึกหลักประกันสิทธิ หรือสิทธิประเภทต่างๆ ที่จะได้รับการรับรองคุ้มครองโดยหน่วยงานของรัฐ อย่างไรก็ตาม สิทธิและสิทธิพิเศษที่จะได้รับตาม BoGs จะยังคงตกอยู่ภายใต้ข้อกำหนดตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง สิทธิที่ได้รับตาม BoGs ยังเป็นเงื่อนไขให้ต้องปฏิบัติตาม MSC Malaysia ทั้งนี้เพื่อเป้าหมายในการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) และหลักประกันนี้อาจถูกกระทบได้จากเหตุการณ์ที่ไม่ได้อยู่ในการควบคุมของรัฐบาล บันทึกหลักประกันของ MSC ประกอบด้วย

1. เพื่อให้ติดอันดับโลกทางด้านกายภาพ และโครงสร้างข้อมูลพื้นฐาน

2. การอนุญาตจ้างงานโดยไม่จำกัดทั้งในประเทศและแรงงานต่างชาติที่มีความรู้

3. เพื่อให้แน่ใจในเสรีภาพการเป็นเจ้าของกรรมสิทธิ์ โดยยกเว้นบริษัทของ MSC Malaysia จากความต้องการของเจ้าของกรรมสิทธิ์ในประเทศ

4. เพื่อให้มีอิสระในแหล่งเงินทุนทั่วโลก สำหรับโครงสร้างพื้นฐานของ MSC Malaysia และสิทธิในการกู้ยืมเงินทั่วโลก

5. การกระตุ้นการแข่งขันกันทางการค้า รวมถึง Pioneer Status (ยกเว้นภาษี 100%) ไม่เกินสิบปีหรือการผ่อนปรนภาษีการลงทุนไม่เกินห้าปีและไม่ต้องชำระภาษีสำหรับการนำเข้าอุปกรณ์มัลติมีเดีย

6. ก้าวไปสู่ความเป็นผู้นำระดับภูมิภาคในการคุ้มครองทรัพย์สินทางปัญญาและ Cyber Laws

7. เพื่อให้ความเชื่อมั่นว่าจะไม่มีการตรวจสอบอินเทอร์เน็ต

8. เพื่อการแข่งขันกันในระดับโลกสำหรับอัตราภาษีกิจการโทรคมนาคม

9. การประกวดราคาเป็นหัวใจสำคัญพื้นฐานของการทำสัญญากับ บริษัทชั้นนำที่ยินดีจะใช้ MSC Malaysia เป็นศูนย์กลางในภูมิภาคของเขา

10. ให้พลังอย่างเต็มที่กับตัวแทนในการดำเนินการให้ประสบผลสำเร็จและมีประสิทธิภาพครบวงจร

[33] http://www.suaram.net/

[34] ทฤษฎีเสรีภาพของสื่อมวลชน ประกอบด้วย 4 ทฤษฎีหลักๆ คือ 1) ทฤษฎีอำนาจนิยม (authoritarian theory) ถือว่า สื่อมวลชนเป็นผู้รับใช้รัฐ รัฐไม่จำเป็นต้องแทรกแซง เพราะเป็นกิจการของรัฐเอง มีหน้าที่ประชาสัมพันธ์ให้รัฐ ส่งเสริมนโยบาย และโครงการของรัฐ ฯลฯ การควบคุมและกลไกการควบคุมจะอยู่ในรูปของกฎหมาย 2) ทฤษฎีเสรีนิยม (libertarian theory) นอกจากมีหน้าที่แจ้งข่าวสารให้กับมวลชนแล้ว ยังมีส่วนช่วยในการค้นหาความจริงและแก้ไขปัญหาด้วยการเสนอหลักฐานและแนวความคิด ตรวจสอบรัฐบาล เป็นผู้เฝ้าดู (watch dog) การดำเนินการของรัฐบาลอย่างเสรี การควบคุมมักใช้กลไกการคุมกันเอง โดยสาธารณะและบางเรื่องคุมโดยกฎหมาย 3) ทฤษฎีความรับผิดชอบทางสังคม (social responsibility theory) เสรีภาพสื่อมีพันธะอยู่กับความรับผิดชอบที่มีต่อสังคม จะมีหลักเกณฑ์ที่ชัดเจนเกี่ยวกับจริยธรรมสื่อ และ 4) ทฤษฎีแนวเศรษฐศาสตร์การเมืองวิพากษ์ (critical political-economic theory) มีลักษณะสื่อที่ถูกควบคุมโดยทุน หรือกลไกทางเศรษฐกิจและการเมือง มักขาดความหลากหลายทางความคิด สื่อเป็นอุตสาหกรรมที่ทำการผลิตเพื่อหวังผลกำไร โดยเนื้อหาจะถูกควบคุมโดยกลไกตลาดและนายทุน

[35] ดูรายละเอียดและเส้นทางความเป็นมาของความสัมพันธ์ระหว่างเจ้าของสื่อ กับพรรครัฐบาลใน, อาทิตย์ สุริยะวงศ์กุล. (2553, ธันวาคม 25). สื่อและขบวนการทางสังคมในมาเลเซีย: กรณีศึกษาหนังสือพิมพ์มาเลเซียกินี. หน้า 8. สืบค้นเมื่อ 20 มีนาคม 2555, จาก http://bact.cc/2010/malaysiakini-malaysia-media-social-movement/

[36] ปีเตอร์ เอ็ม แชนด์แมน และคณะฯ เคยจำแนกลักษณะ ของ มาตรการในการควบคุมสื่อมวลชน ออกเป็น 7 ประการ 1) มาตรการควบคุมตนเอง Self Control ซึ่งเป็นคนละเรื่องกับ Self Censorship โดยใช้จรรยาบรรณวิชาชีพเป็นแนวทาง 2) มาตรการควบคุมภายใน Internal Control คือ คุมจากเจ้าของกิจการหรือผู้บริหาร โดยอาศัยเหตุผลทางธุรกิจและเหตุผลทางการเมือง 3) มาตรการควบคุมโดยการผูกขาด (Monopoly Control) 4) มาตรการควบคุมโดยโฆษณา (Advertise Control) 5) มาตรการควบคุมโดยแหล่งข่าวสาร (Source Control) โดยแหล่งข่าวมักอาศัยเทคนิคในการให้ข่าวแก่สื่อเพื่อควบคุมเนื้อหาที่สื่อจะนำไปนำเสนอ 6) มาตรการควบคุมโดยรัฐบาล (Government Control) 7) มาตรการควบคุมโดยสาธารณชน (Public Control) คือ การที่สาธารณชนไม่ว่าจะเป็นบุคคลหรือกลุ่มบุคคลได้มีปฏิกิริยาตอบกลับไปยังสื่อมวลชน เพื่อ1. ควบคุมเนื้อหาของสื่อ เช่น งดใช้ งดรับ หรือ 2. เพื่อเข้าไปมีส่วนร่วมในการแสดงความคิดเห็นในเรื่องต่างๆ โดยผ่านสื่อ โดยการเขียนจดหมาย เอสเอ็มเอส ฯลฯ

[37] ดูรายละเอียดเกี่ยวกับประวัติการดำเนินการของสำนักข่าวมาเลเซียกินี ใน อาทิตย์ สุริยะ

วงศ์กุล. (2553, ธันวาคม 25). สื่อและขบวนการทางสังคมในมาเลเซีย: กรณีศึกษาหนังสือพิมพ์มาเลเซียกินี, *อ้างแล้ว 35.*

บทเปรียบเทียบทางกฎหมาย ไทย เยอรมนี สหรัฐอเมริกา และมาเลเซีย

[1] Amnesty International. (n.d.). Imprisoned for Peaceful Expression. Retrieved July 12, 2012, from http://www.amnestyusa.org/our-work/cases/china-shi-tao

[2] Jake Hooker. (2008, July 11). Voice seeking answers for parents about school collapse in China is silenced. *The New York Times*. Retrieved July 12, 2012, from http://www.nytimes.com/2008/07/11/world/asia/11iht-11china.14412092.html?_r=1

ข้อเสนอแนะ

[1] ดู สรุปปัญหาบทนิยามของคำว่า "ผู้ให้บริการ" ซึ่งรวบรวมจากการประชุมร่างกฎหมายและการให้เหตุผลโดยกลุ่มผู้ประกอบการอินเทอร์เน็ตที่, เช กูวารา (นามแฝง). (2555, ตุลาคม 24). กฎหมาย ที่ร่างกันแบบไม่เร่ง แต่ผ่านกันแบบรีบ ๆ (ตอน 1-5). *iLaw* สืบค้นเมื่อ 24 ตุลาคม 2555 จาก http://ilaw.or.th/node/1748

[2] กลุ่มผู้ประกอบกิจการโทรคมนาคม และกิจการกระจายภาพและเสียง ตาม ข้อ 5 (1) ก ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

[3] เช่น Das Telekommunikationsgesetz (TKG) ของประเทศเยอรมนี

[4] Gesetz über die Nutzung von Telediensten (Teledienstegesetz -TDG): § 9 Durchleitung von Informationen

[5] ศึกษาหลักการ Notice and Takedown (NTD) เพิ่มเติม ได้ใน Christian Ahlert, Chris Marsden and Chester Yung. (n.d.). How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation. Retrived June 10, 2011, from http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf

[6] นอกจากตัวเลขสถิติเกี่ยวกับจำนวนคำสั่งศาล กับจำนวนเว็บเพจที่ถูกปิด ตามที่คณะผู้วิจัยได้แสดงไว้ในรายงานวิจัยฉบับนี้แล้ว ล่าสุดยังพบว่าภายในระยะเวลา 4 เดือน ศาลได้ออกคำสั่งทั้งสิ้น 28 ครั้ง เพื่อปิดกั้นเว็บเพจมีจำนวนถึง 5,064 URL ดู, ASTVผู้จัดการออนไลน์. (2555, มีนาคม 14). ตร.พอใจผลปราบเว็บหมิ่นสถาบัน-ชี้ 4 เดือนปิดแล้ว 5 พันยูอาร์เอล. สืบค้นเมื่อ 10 มิถุนายน 2555, จาก http://www.manager.co.th/Crime/ViewNews.aspx?NewsID=9550000033137

[7] ประชาไท. (2553, พฤศจิกายน 22). จนท.ไอซีทีเผย การขึ้นบัญชีดำบล็อคเว็บ "ล้มเหลว". สืบค้นเมื่อ 10 มิถุนายน 2555, จาก http://prachatai.com/journal/2010/11/31998

Notes

Introduction

[1] Section 45 of Constitution of the Kingdom of Thailand, B.E. 2550 (2007), "A person shall enjoy the liberty to express his or her opinion, make speeches, write, print, publicise, and make expression by other means.

The restriction on the liberty under paragraph one shall not be imposed except by virtue of the provisions of the law specifically enacted for the purpose of maintaining the security of the State, safeguarding the rights, liberties, dignity, reputation, family or privacy rights of other persons, maintaining public order or good morals or preventing the deterioration of the mind or health of the public.

The closure of a newspaper or other mass-media business in deprivation of the liberty under this section shall not be made.

The prohibition of a newspaper or other mass-media business from presenting information or expressing opinions in whole or in part or imposition of interference by any means in deprivation of the liberty under this section shall not be made except by virtue of the law enacted under paragraph two.

The censorship by a competent official of news or articles before their publication in a newspaper or other mass media shall not be made except during the time when the country is in a state of war; provided that it must be made by virtue of the law enacted under paragraph two.

The owner of a newspaper or other mass-media business shall be a Thai national.

No grant of money or other properties shall be made by the State as subsidies to private newspapers or other mass media."

[2] Section 29 of Constitution of the Kingdom of Thailand, B.E. 2550 (2007), "The restriction of such rights and liberties as recognised by the Constitution shall not be imposed on a person except by virtue of provisions of the law specifically enacted for the purpose determined by this Constitution and to the extent of necessity and provided that it shall not affect the essential substances of such rights and liberties.

The law under paragraph one shall be of general application and shall not be intended to apply to any particular case or person; provided that the provision of the Constitution authorising its enactment shall also be mentioned therein.

The provisions of paragraph one and paragraph two shall also apply mutatis mutandis to by-laws issued by virtue of provisions of law."

[3] Section 20 of Computer-related Crime Act B.E. 2550 (2007), "If an offence under this Act is to disseminate computer data that might have an impact on the Kingdom's security as stipulated in Division 2 type 1 or type 1/1 of the Criminal Code, or that it might be contradictory to the peace and concord or good morals of the people, the competent official appointed by the Minister may file a petition together with the evidence to a court with jurisdiction to restrain the dissemination of such computer data.

If the court gives an instruction to restrain the dissemination of computer data according to paragraph one, the relevant competent official shall conduct the restraint either by himself or instruct the Service Provider to restrain the dissemination of such computer data."

[4] Section 9 of the Emergency Decree on Public Administration in Emergency Situation, B.E. 2548 (2005), "In the case of necessity in order to remedy and promptly resolve an emergency situation or to prevent the worsening of such situation, the Prime Minister shall have the power to issue the following Regulations:…

(3) to prohibit the press release, distribution or dissemination of letters, publications or any means of communication containing texts which may instigate fear amongst the people or is intended to distort information which misleads understanding of the emergency situation to the extent of affecting the security of state or public order or good moral of the people both in the area or locality where an emergency situation has been declared or the entire Kingdom"

[5] มุทิตา เชื้อชั่ง. (2554, เมษายน 29). รายงาน: สำรวจสถานการณ์หลังปิดวิทยุชุมชนเสื้อแดง (ระลอกแรก). *ประชาไท*. สืบค้นเมื่อ 7 พฤษภาคม 2555, จาก http://www.prachatai.com/journal/2011/04/34291 ["A Report on a situational survey of the crackdown on redshirts' community radio stations (the first round)" by Mutita Cheuchang (2011, April 29) from Prachatai, in Thai]

[6] ไทยรัฐออนไลน์. (2554, กรกฎาคม 6). ปชป.สับพท.แค่ 48 ชม.ลุอำนาจไล่ปิดวิทยุชุมชน. สืบค้นเมื่อ 7 พฤษภาคม 2555, จาก http://www.thairath.co.th/content/pol/184129 ["Democrats savage Pheu Thai for taking only 48 hrs to abuse its power to close community radios" from Thai Rath online (2011, July 6), in Thai]

[7] iLaw. (n.d.). Case # 116: Prachatai Blocked. Retrieved May 7, 2012, from http://freedom.ilaw.or.th/case/116

Statistical Study and Survey of the Opinions of State Officials and Online Media Service Providers regarding Enforcement of the Computer-related Crimes Act B.E. 2550

[1] Section 20 of the CCA stipulates that in order to block a website, a competent officials authorized by the Minister of Information and Communication Technology must submit a request for a court order; hence the Criminal Court should have records of all requests.

[2] งานบริการข้อมูลคดี ศาลอาญา. (ม.ป.ป.). งานบริการข้อมูลคดี ศาลอาญา. สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://aryasearch.coj.go.th/aryaweb/main.php [Case Information Service, Criminal Court, in Thai]

[3] The name was changed to the Office of Prevention and Suppression of Information Technology Crime in 2010

[4] The 5th Announcement of the Council for Democratic Reform, "Since the Council for Democratic Reform under the Constitutional Monarchy has seized power, the Ministry of Information and Communication Technology is assigned to control, restrain, restrict and destroy all information in information systems through all networks of communication, either in forms of articles, statements, speeches and the like, which might affect democratic reform under the Constitutional Monarchy, as the Council for Democratic Reform under the Constitutional Monarchy has declared above – Effective on 20 September 2006"

[5] Red Sundays were rallies that began after the May 2010 crackdown and while the Emergency Decree was still imposed. It was symbolic activity led by Sombat Boonngam-anong, and brought the mobilization of the red shirt back again. วิกิพีเดีย สารานุกรมเสรี. (ม.ป.ป.). กลุ่มวันอาทิตย์สีแดง. สืบค้นเมื่อ 29 กุมภาพันธ์ 2555, จาก http://th.wikipedia.org/wiki/กลุ่มวันอาทิตย์สีแดง ["Red Sunday" from Wikipedia the free encyclopedia, in Thai]

[6] The Emergency Decree has been continuously in force in the 3 southernmost provinces since 2005. However, as far as is known, the enforcement of the Emergency Decree in these provinces has never been used to authorize the blocking of websites

[7] Section 9 of Emergency Decree on Public Administration in Emergency Situation, B.E. 2548, "In the case of necessity in order to remedy and promptly resolve an emergency situation or to prevent the worsening of such situation, the Prime Minister shall have the power to issue the following Regulations: …

(3) to prohibit the press release, distribution or dissemination of letters, publications or any means of communication containing texts which may instigate fear amongst

the people or is intended to distort information which misleads understanding of the emergency situation to the extent of affecting the security of state or public order or good moral of the people both in the area or locality where an emergency situation has been declared or the entire Kingdom"

[8] Certain websites with no political content were also blocked during the emergency. According to MICT officials, some foreigners made phone complaints to the Ministry that the website Justin.tv, a file-sharing website with no content that breached national security, was blocked during that period.

[9] For example, www.sanamluang.tv, an online TV website that broadcasts live events, was blocked by a CRES order on 10 May 2010 and www.prachatai.com , an online news site, was blocked on 7 April 2010 and both continue to be blocked.

[10] ประชาไท. (2554, พฤศจิกายน 23). รมว. ไอซีทีเผย ขอเฟซบุ๊กปิดเพจหมิ่นฯแล้วกว่าหมื่นยูอาร์แอล. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://prachatai.com/journal/2011/11/38004 ["ICT Minister requested Facebook to closing down over 10,000 urls of lese-majesty pages" from Prachatai (2011, November 23), in Thai]

[11] ไทยรัฐออนไลน์. (2554, ธันวาคม 14). ไต้ที 'เฉลิม' ของบ 400 ล้านบ. ซื้อเครื่องดักเว็บหมิ่นฯ. สืบค้นเมื่อ 14 ธันวาคม 2554, จาก http://www.thairath.co.th/content/pol/223580 ["Deputy Prime Minister request 400M budget for lese-majeste web filter machine" from Thai Rath online (2011, December 14), in Thai]

[12] โพสต์ทูเดย์. (2554, ธันวาคม 8). เฟซบุ๊กร่วมบล็อกคนโพสต์หมิ่นแล้ว6หมื่นราย. สืบค้นเมื่อ 8 ธันวาคม 2554, จาก http://www.posttoday.com/อาชญากรรม/125948/เฟซบุ๊คร่วมบล็อกคนโพสต์หมิ่นแล้ว6หมื่นราย ["Facebook collaborate to block 60,000 lese-majesty users" from Post Today (2011, December 8), in Thai]

[13] ประชาไท. (2554, ธันวาคม 9). ดูแนวทาง 'เฉลิม' ปราบเว็บหมิ่น งัดมาตรการ 'ขอร่วมมือ กฎหมาย และ...ประจาน'. สืบค้นเมื่อ 9 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2011/12/38245 [Deputy prime minister measures on lese-majesty websites: 'Request for cooperation, enforce law, and ... revile'" from Prachatai (2011, December 9), in Thai]

[14] Computer-related Crime Act B.E. 2550 (2007), "Section 5. Any person illegally accessing a computer system for which a specific access prevention measure that is not intended for their own use is available shall be subject to imprisonment for no longer than six months or a fine of not more than ten thousand baht or both.

Section 6. If any person knowing of a measure to prevent access to a computer system specifically created by a third party illegally discloses that measure in a manner that is likely to cause damage to the third party, then they shall be subject to imprisonment

for no longer than one year or a fine of not more than twenty thousand baht or both.

Section 7. If any person illegally accesses computer data, for which there is a specific access prevention measure not intended for their own use available, then he or she shall be subject to imprisonment for no longer than two years or a fine of not more than forty thousand baht or both.

Section 8. Any person who illegally commits any act by electronic means to eavesdrop a third party's computer data in process of being sent in a computer system and not intended for the public interest or general people's use shall be subject to imprisonment for no longer than three years or a fine of not more than sixty thousand baht or both.

Section 9. Any person who illegally damages, destroys, corrects, changes or amends a third party's computer data, either in whole or in part, shall be subject to imprisonment for no longer than five years or a fine of not more than one hundred thousand baht or both.

Section 10. Any person who illegally commits any act that causes the working of a third party's computer system to be suspended, delayed, hindered or disrupted to the extent that the computer system fails to operate normally shall be subject to imprisonment for no longer than five years or a fine of not more than one hundred thousand baht or both.

Section 11. Any person sending computer data or electronic mail to another person and covering up the source of such aforementioned data in a manner that disturbs the other person's normal operation of their computer system shall be subject to a fine of not more than one hundred thousand baht.

Section 12. The perpetration of an offence under Section 9 or Section 10 that:

(1) causes damage, whether it be immediate or subsequent and whether it be synchronous to the public shall be subject to imprisonment for no longer than ten years or a fine of not more than two hundred thousand baht.

(2) is an act that is likely to damage computer data or a computer system related to the country's security, public security and economic security or public services or is an act against computer data or a computer system available for public use shall be subject to imprisonment from three years up to fifteen years and a fine of sixty thousand baht up to three hundred thousand baht. The commission of an offence under (2) that causes death to another person shall be subject to imprisonment from ten years up to twenty years.

Section 13. Any person who sells or disseminates sets of instructions developed

as a tool used in committing an offence under Section 5, Section 6, Section 7, Section 8, Section 9, Section 10 and Section 11 shall be subject to imprisonment for not more than one year or a fine of not more than twenty thousand baht, or both.

Section 14. If any person commits any offence of the following acts shall be subject to imprisonment for not more than five years or a fine of not more than one hundred thousand baht or both:

(1) that involves import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to that third party or the public;

(2) that involves import to a computer system of false computer data in a manner that is likely to damage the country's security or cause a public panic;

(3) that involves import to a computer system of any computer data related with an offence against the Kingdom's security under the Criminal Code;

(4) that involves import to a computer system of any computer data of a pornographic nature that is publicly accessible;

(5) that involves the dissemination or forwarding of computer data already known to be computer data under (1) (2) (3) or (4)"

[15] Section 423 of Civil and Commercial Code, "A person who, contrary to the truth, asserts or circulates as a fact that which injurious to the reputation or the credit of another or his earnings or prosperity in any other manner, shall compensate the other for any damage arising therefrom, even if he does not know of its untruth, provided he ought to know it..."

[16] Section 326 of Criminal Code, "Whoever, imputes anything to the other person before a third person in a manner likely to impair the reputation of such other person or to expose such other person to be hated or scorned, is said to commit defamation, and shall be punished with imprisonment not exceeding one year or fined not exceeding twenty thousand Baht, or both."

[17] Section 328 of Criminal Code, "If the offence of defamation be committed by means of publication of a document, drawing, painting, cinematography film, picture or letters made visible by any means, gramophone record or an other recording instruments, recording picture or letters, or by broadcasting or spreading picture, or by propagation by any other means, the offender shall be punished with imprisonment not exceeding two years and fined not exceeding two hundred thousand Baht"

[18] Section 264 of Criminal Code, "Whoever, in a manner likely to cause injury to another person or the public, fabricates a false document or part of a document, or

adds to, takes from or otherwise alters a genuine document by any means whatever, or puts a false seal or signature to a document, if it is committed in order to make any person to believe that it is a genuine document, is said to forge a document, and shall be punished with imprisonment not exceeding three years or fined not exceeding six thousand Baht, or both."

[19] Section 1 (7) of Criminal Code, "'Document' means any paper or other material for expressing the meaning by letters, figures, plan or an other design, whether it be by way of printing, photographing or any other means, which is evidence of such meaning;"

[20] บันทึกสำนักงานคณะกรรมการกฤษฎีกา ประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ... เรื่องเสร็จที่ 257/2548. (ม.ป.ป.). สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://www.dms.moph.go.th/dmsict/doc_file/policy.doc, หน้า 2 ["Record of the Council of State committee in relation to the draft Computer Crime Act BE .. No. 257/2548" p. 2.]

[21] Further details about legal problem and interpretation of Section 14 (1), please see the analysis of Thai law in chapter in this report.

[22] ประชาไท. (2555, พฤษภาคม 30). ศาลตัดสิน "ผอ.ประชาไท" ผิดคดีตัวกลาง สั่งจำคุกแต่ให้รอลงอาญา. สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://prachatai.com/node/40757 ["Prachatai director gets suspended jail term" from Prachatai (2012, May 30), in Thai]

[23] Section 287 of Criminal Code, "Whoever:

1. For the purpose of trade or by trade, for public distribution or exhibition, makes, produces, possesses, brings or causes to be brought into the Kingdom, sends or causes to be sent out of the Kingdom, takes away or causes to be taken away, or circulates by any means whatever, any document, drawing, print, painting, printed matter, picture, poster, symbol, photograph, cinematograph film, noise tape, picture tape or any other thing which is obscene;

2. Carries on trade, or takes part or participates in the trade concerning the aforesaid obscene material or thing, or distributes or exhibits to the public, or hires out such material or thing;

3. In order to assist in the circulation or trading of the aforesaid obscene material or thing, propagates or spreads the news by any means whatever that there is a person committing the act which is an offence according to this Section, or propagates or spreads the news that the aforesaid obscene material or thing may be obtained from any person or by any means, shall be punished with imprisonment not exceeding three years or fined not exceeding six thousand Baht, or both."

[1] Sections 26 - 27 of Constitution of the Kingdom of Thailand, B.E. 2550 (2007), "Section 26. In exercising powers of all State authorities, regard shall be had to human dignity, rights and liberties in accordance with the provisions of this Constitution.

Section 27. Rights and liberties recognised by this Constitution explicitly, by implication or by decisions of the Constitutional Court shall be protected and directly binding on the National Assembly, the Council of Ministers, the Courts, the Constitutional organisations and all State organs in enacting, applying and interpreting laws."

[2] บวรศักดิ์ อุวรรณโณ, *กฎหมายมหาชนเล่ม 3 ที่มาและนิติวิธี*, (กรุงเทพฯ: นิติธรรม, 2538), หน้า 333. ["Public Law Volume 3 Source and Legal procedure" (book) by Bavornsak Uwanno (1995) p. 333, in Thai]

[3] See an explanation of the "principle of proportionality" that limits the rights and freedoms protected by the Constitution in ธีระ สุธีวรางกูร. การคุ้มครองสิทธิและเสรีภาพของบุคคลที่รัฐธรรมนูญรับรอง. *วารสารนิติศาสตร์*, 29(4), (2542). หน้า 587. ["Protection of the rights and liberties of the people guaranteed by the Constitution" by Teera Sutheewarangkul from Thammasat Journal of Law 29(4) (1999) p 587, in Thai]

[4] See, วรพจน์ วิศรุตพิชญ์, *สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540*, (กรุงเทพฯ: วิญญูชน, 2543), หน้า 78. ["Rights and Freedoms under the Constitution" (book) by Worapot Visrootpitch (2000) p. 78, in Thai]

[5] Section 6 of Constitution of the Kingdom of Thailand, B.E. 2550 (2007), "The Constitution is the supreme law of the State. The provisions of any law, rule or regulation, which are contrary to or inconsistent with this Constitution, shall be unenforceable. "

[6] 6 laws are such as the Act on Electronic Transactions, Electronic Signatures Act; the Act on the Development of Information Infrastructure Thoroughly and Equally (secondary law of the Constitution of the Kingdom of Thailand BE 2540, Section 78); the Personal Data Protection Act; the Electronic Funds Transfer Act; and the Computer Crime Act (later renamed the Computer-related Crime Act).

[7] This has been amended and combined into the same law as the Electronic Signature Act (originally planned as a separate law).

[8] The first draft BE 2545 "Draft of Computer Crime Act", the second draft BE 2546 "Draft of Computer Crime Act", the third BE 2548 "Draft of Computer Crime Act" (which is the version that passed the Council of State and to the consideration by the Cabinet on 15 November BE 2549) and the fourth draft BE 2549 " Draft of Computer Crime Act " (the ad hoc committee's draft of the National Assembly).

[9] See, สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, *รวมร่างกฎหมายเทคโนโลยีสารสนเทศ ภายใต้โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ*, (กรุงเทพฯ: โรงพิมพ์เดือนตุลาคม, 2544), หน้า 9. ["The Law of Information Technology under information technology law development projects" published by National Information Technology Committee Secretariat (2001) p. 9, in Thai]

[10] ประชาไท. (2549, พฤศจิกายน 19). สนช.ลงมติรับหลักการร่าง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.... วาระแรก. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.prachatai.com/journal/2006/11/10527 ["NLA made principle approval for Computer-related Crime Bill" from Prachatai (2006, November 19), in Thai]

[11] See a summary of the problem in defining the term. "service provider" from the drafting process and validation by a group of internet entrepreneurs at, เช กูวารา (นามแฝง). (2555, ตุลาคม 24). กฎหมาย ที่ร่างกันแบบไม่เร่ง แต่ผ่านกันแบบรีบๆ (ตอน 1-5). *iLaw* สืบค้นเมื่อ 24 ตุลาคม 2555 จาก http://ilaw.or.th/node/1748 ["Slowly draft, but hurriedly pass the bill (part 1-5)" by Che Guevara (pseudonym) from iLaw (2012, October 24), in Thai]

[12] Section 5 of Ministerial Regulations on Information And Communication Technology with Regard to Criteria for Retention of Computer Traffic Data of Service Providers 2550, "A. a person who provides services to people in general or access to the iInternet or other means available via a computer system whether it is available in its own name or for the benefit of others can be divided into 4 types.

a) Telecommunication and Broadcast Carrier

b) Access Service Provider

c) Host Service Provider

d) Internet Service Provider.

B. a person who provides computer data storage for the benefit of users in 1 (Content Service Provider) as a service provider of computer data across various applications (Application Service Provider)."

[13] บันทึกสำนักงานคณะกรรมการกฤษฎีกา ประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ... เรื่องเสร็จที่ 257/2548. (ม.ป.ป.). สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://www.dms.moph.go.th/dmsict/doc_file/policy.doc, หน้า 12 ["Record of the Council of State committee in relation to the draft Computer Crime Act BE .. No. 257/2548" (n.d.) p. 12, in Thai]

[14] Cases filed with Section 14 (1) mostly concern defamation, libel and fraud, such as posting texts on webboards to advertise products, but when buyers transfer the money, the products aren't delivered as promised. However, this research aims to study

the impact of this law only on freedom of expression. An example of a defamation case is that of Preeyanan Lorsermvattana, President of the Medical Malpractice Victim Network and a health activist. She disseminated pictures and graphs on Facebook and various websites, concerning patients who died from medical malpractice. The information prompted opposition from many medical association groups. Dr. Prachumporn Buranacharoen, President of Thai Federation of Doctors, Main Hospitals and General Hospitals later filed a complaint against Preeyanan for importing false data to a computer system. The case is still on trial.

[15] Section 1 (7) of Criminal Code, "'Document' means any paper or other material for expressing the meaning by letters, figures, plan or an other design, whether it be by way of printing, photographing or any other means, which is evidence of such meaning."

[16] บันทึกสำนักงานคณะกรรมการกฤษฎีกา ประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ... เรื่องเสร็จที่ 257/2548. *supra note 13*. p.2.

[17] See explanation regarding offences of document forgery in, จิตติ ติงศภัทิย์, *คำอธิบายประมวลกฎหมายอาญา, ภาค 2 ตอน 1*, พิมพ์ครั้งที่ 7, (กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2543), หน้า 592 – 594. ["Explanation of the Criminal Code, Section 2 part 1" 7th edition by Chitti Tingsaphat (2000). p. 592-594, in Thai]

[18] Section 329 of Criminal Code, "Whoever, in good faith, expresses any opinion or statement:

(1) By way of self justification or defense, or for the protection of a legitimate interest;

(2) In the status of being an official in the exercise of his functions;

(3) By way of fair comment on any person or thing subjected to public criticism; or

(4) By way of fair report of the open proceeding of any Court or meeting,

shall not be guilty of defamation."

[19] The "nullum crimen, nulla poena sine lege" principle or "no offense, no punishment without law" was adopted by the Thai legal system and is stipulated in Section 2 of the Criminal Code: "Section 2: A person shall be criminally punished only when the act done by such person is provided to be an offence and the punishment is defined by the law in force at the time of the doing of such act, and the punishment to be inflicted upon the offender shall be that provided by the law.

If, according to the law as provided afterwards, such act is no more an offence, the person doing such act shall be relieved from being an offender; and, if there is a final judgment inflicting the punishment, such person shall be deemed as not having

ever been convicted by the judgment for committing such offence. If, however, such person is still undergoing the punishment, the punishment shall forthwith terminate."

[20] See, คณิต ณ นคร, *กฎหมายอาญาภาคทั่วไป*, พิมพ์ครั้งที่ 3, (กรุงเทพฯ: วิญญูชน, 2551), หน้า 72. ["General Criminal Law" 3rd edition by Kanit Na Nakorn (2008) p. 72, in Thai]

[21] Offences related to the security of the Kingdom are in Sections 107-135 and offenses related to terrorism in Sections 135/1-135/4 of the Criminal Code.

[22] Section 112 of Criminal Code "Whoever, defames, insults or threatens the King, the Queen, the Heir-apparent or the Regent, shall be punished with imprisonment of three to fifteen years."

[23] Section 326 of Criminal Code, "Whoever, imputes anything to another person before a third person in a manner likely to impair the reputation of such other person or to expose such other person to be hated or scorned, is said to commit defamation, and shall be punished with imprisonment not exceeding one year or fined not exceeding twenty thousand Baht, or both."

[24] Section 329 of Criminal Code, *supra note 18*.

[25] Section 330 of Criminal Code, "In case of defamation, if the person prosecuted for defamation can prove that the imputation made by him is true, he shall not be punished. But he shall not be allowed to prove if such imputation concerns personal matters, and such proof will not be of benefit to the public."

[26] See details on the problems of Section 112 and suggestions for amendment in, Nitirassadorn: Law for the People. (2011, December 26). Proposed amendments to the law on defamation of the King, the Queen, the Heir-apparent and the Regent (Section 112 of the Criminal Code)" Retrieved January 7, 2012, from http://www.enlightened-jurists.com/download/68

[27] Section 86 of Criminal Code, "Whoever for any reason whatsoever assists or facilitates any other person committing an offence before or during the commission of the offence, even though such assistance or facility is not known by the offender, is deemed to be a supporter in committing such offence and shall be punished by two-thirds of the punishment provided for such offence."

[28] See the statistics on website blocking requests for court approval in Part 1 of this research.

[29] See, คณะวิจัยผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น. (2553, ธันวาคม 8). รายงานสถานการณ์ การควบคุมและปิดกั้นสื่อออนไลน์ ด้วยการอ้างกฎหมายและ

แนวนโยบายแห่งรัฐไทย. *iLaw.* สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.scribd.com/doc/44961877/รายงานสถานการณ์การควบคุมและปิดกั้นสื่อออนไลน์ด้วยการอ้างกฎหมายและแนวนโยบายแห่งรัฐไทย, หน้า 13. ["Situational Report on Control and Censorship of Online Media, through the Use of Law and the Imposition of Thai State Policies." by The researcher of the Impact of the Computer-related Crimes Act B.E. 2550 and the State Policy on Rights and Freedom of Expression. (2010, December 8) p. 13, in Thai]

[30] Section 287 of Criminal Code, "Whoever:

(1) For the purpose of trade or by trade, for public distribution or exhibition, makes, produces, possesses, brings or causes to be brought into the Kingdom, sends or causes to be sent out of the Kingdom, takes away or causes to be taken away, or circulates by any means whatever, any document, drawing, print, painting, printed matter, picture, poster, symbol, photograph, cinematograph film, noise tape, picture tape or any other thing which is obscene;

(2) Carries on trade, or takes part or participates in the trade concerning the aforesaid obscene material or thing, or distributes or exhibits to the public, or hires out such material or thing;

(3) In order to assist in the circulation or trading of the aforesaid obscene material or thing, propagates or spreads the news by any means whatever that there is a person committing the act which is an offence according to this Section, or propagates or spreads the news that the aforesaid obscene material or thing may be obtained from any person or by any means, shall be punished with imprisonment not exceeding three years or fined not exceeding six thousand Baht, or both."

[31] For example, Japan amended the Penal Code of Japan and the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children to include the offense of digital dissemination of child pornography. Similarly, Hong Kong uses the Control of Obscene and Indecent Articles Ordinance rather than in the Computer Crimes Ordinance 1993 or the Telecommunication Ordinance 1993. The Philippines plans to have provisions in the Anti-Child Pornography Act, not in computer-related law like the Electronic Commerce ACT 2000, while the Federal Republic of Germany amended the relevant section in the Criminal Code (Strafgesetzbuch), but there was no amendment to provisions about racist content since the Criminal Code already applies to offenses in all types of media.

[32] คมชัดลึก. (ม.ป.ป.). สนช. ผ่านร่าง พรบ. ว่าด้วยการกระทำผิดคอมพิวเตอร์. สืบค้นเมื่อ 15 ตุลาคม 2554, จาก http://komchadluek.com ["NLA pass the Computer Crime Bill" from Kom Chad Luek. (n.d.), in Thai]

[33] The 5th Announcement of the Council for Democratic Reform: “Since the Council for Democratic Reform under the Constitutional Monarchy has seized power, the Ministry of Information and Communication Technology is assigned to control, restrain, restrict and destroy all information in information systems through all networks of communication, either in forms of articles, statements, speeches and the like, which might affect democratic reform under the Constitutional Monarchy, as the Council for Democratic Reform under the Constitutional Monarchy has declared above – Effective on 20 September 2006”

[34] ไทยรัฐออนไลน์. (2550, มกราคม 30).ไอซีทีบล็อกแคมฟรอกแล้ว หลังโจ๋ไทยไม่หยุดโชว์. อ้างใน *news.sanook*. สืบค้นเมื่อ 5 ตุลาคม 2555 จาก http://news.sanook.com/crime/crime_88511.php [“MICT blocks Camfrog after kids won’t stop showing” from Thai Rath online (2007, January 30) cited in news.sanook, in Thai)

[35] เดลินิวส์. (2550, มกราคม 9). ไอซีทีเผยไล่บล็อกเว็บโป๊แล้วกว่าหมื่น! หนักใจเว็บนอกคุมยาก. อ้างใน *TLCNews*. สืบค้นเมื่อ 5 ตุลาคม 2554, จาก http://news.tlcthai.com/news-interest/112.html [“MICT reveals more than 10,000 pornographic websites blocked! Worried that foreign websites are hard to control” from Daily News (2007, January 9) cited in TLCNews, in Thai]

[36] สยามจดหมายเหตุ. (ม.ป.ป.). สั่งปิดเว็บไซต์แพร่คลิปวิดีโอหมิ่นพระบรมเดชานุภาพ. สืบค้นเมื่อ 5 ตุลาคม 2554, จาก http://www.siamarchives.com/สั่งปิดเว็บไซต์แพร่คลิ/ [“Order to block website showing lèse majesté video clip” from Siam Archives (n.d.), in Thai]

[37] ไทยรัฐออนไลน์. (2550, พฤษภาคม 30). ถูกหาละเมิดสิทธิ 'สิทธิชัย' ยกสถิติปิด เว็บ 2 รบ.เปรียบเทียบ. อ้างใน *MakeWebExy.com* สืบค้นเมื่อ 30 กรกฎาคม 2554, จาก http://www.makewebez.com/tips/index.php?page=show&id=233 [“Rights violated; Sittichai compares statistics from 2 governments” from Thai Rath. (2007, May 30) cited in MakeWebExy.com, in Thai]

[38] สำนักข่าวไทย. (ม.ป.ป.). ยกเลิกประกาศคปค. ฉบับที่ 5 เรื่องควบคุมเว็บไซต์. อ้างใน *oxygen*. สืบค้นเมื่อ 30 กรกฎาคม 2554, จาก http://oxygen.readyplanet.com/index.php?lay=show&ac=article&Id=416946&Ntype=20 [“Annulment of 5th Announcement of the CDR on control of websites” from MCOT (n.d.) cited in oxygen, in Thai]

[39] โลโก้พระพุทธเจ้า“เว็บ”ลามก“พระ”เปิดเจอ-ร้องจ้าก. *ข่าวสด*. (2550, มกราคม 8). หน้า 1. [“Obscene website Buddha logo; monks find and file complaints” from Khaosod (Newspaper) (2007, January 8) p. 1, in Thai]

[40] กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย. (2551, มีนาคม 18). “แฮค & แครก” เว็บหมิ่น ไอซีทีรู้ผิดกฎหมายแต่จะทำ. สืบค้นเมื่อ 18 สิงหาคม 2554, จาก http://facthai.wordpress.com/2008/03/18/ict-to-hack-and-crack-thai/ [“ICT to ‘hack & crack’ foreign

websites offensive to Thai supreme institution" from Freedom Against Censorship Thailand. (2008, March 18), in Thai]

[41] คมชัดลึก. (2551, มิถุนายน 10). มั่น พัธโนทัยไอซีทีคอร์ปผู้ปิดทองหลังพระ. อ้างใน *news.sanook*. สืบค้นเมื่อ 9 ตุลาคม 2554, จาก http://news.sanook.com/politic/politic_276054.php ["Man Pattanothai: ICT CORP working behind the scenes" from Kom Chad Leuk. (2008, June 10) cited in news.sanook, in Thai]

[42] ประชาชาติธุรกิจออนไลน์. (ม.ป.ป.). ยกเครื่องมาตรการสกัดเว็บต้องห้าม. อ้างใน *decha.com*. สืบค้นเมื่อ 9 ตุลาคม 2554, จาก http://www.decha.com/main/showTopic.php?id=2737 ["Measures to cut off banned websites" from Prachachat online (n.d.) cited in decha.com, in Thai]

[43] สำนักข่าวอินโฟเควสท์ (IQ). (2551, ตุลาคม 28). รมว.ไอซีที เล็งซื้ออุปกรณ์บล็อคเว็บหมิ่นสถาบัน 100-500 ลบ./เครื่อง. อ้างใน *RYT9*. สืบค้นเมื่อ 10 ตุลาคม 2554, จาก http://www.ryt9.com/s/iq02/458881 ["ICT Minister aims to buy equipment to block lèse majesté websites at 100-500 m baht each" from Infoquest. (2008, October 28) cited in RYT9, in Thai]

[44] กรุงเทพธุรกิจออนไลน์. (2551, พฤศจิกายน 7). ไอซีทีออก 5 มาตรการด้านเว็บหมิ่น. สืบค้นเมื่อ 10 ตุลาคม 2554, จาก http://www.bangkokbiznews.com/2008/11/07/news_309786.php ["ICT reveals 5 measures to block lèse majesté websites" from Bangkokbiznews (2008, November 7), in Thai]

[45] ASTVผู้จัดการออนไลน์. (2552, กุมภาพันธ์ 5). ระนองรักษ์ ตั้ง ISOC สกัดเว็บหมิ่น – ยันไม่ปิดไฮไฟว์. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.manager.co.th/cyberbiz/ViewNews.aspx?NewsID=9520000013365 ["Ranongrak sets up ISOC to cut off lèse majesté websites – not to close hi-fi" from Manager Online. (2009, February 5), in Thai]

[46] ประชาไท. (2554, ธันวาคม 1). ไอซีทีเปิดตัวศูนย์ความมั่นคงไซเบอร์ สุดเข้มปราบเว็บหมิ่นฯ สถาบัน. สืบค้นเมื่อ 20 มกราคม 2555, จาก http://prachatai.com/journal/2011/12/38121 ["ICT opens cyber security centre, focus on suppressing lèse majesté websites" from Prachatai. (2011, December 1), in Thai]

[47] ไทยรัฐออนไลน์. (2552, เมษายน 24). 'ระนองรักษ์' ตื่นลุยปราบผู้ใช้เน็ตป่วนชาติ. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.thairath.co.th/content/tech/1669 ["Ranongrak alert, wades into suppression of net users disrupting the nation" from Thai Rath online (2009, April 24), in Thai]

[48] เดลินิวส์. (2552, กรกฎาคม 29). ไอซีทีอวดผลงานศูนย์ปฏิบัติการปลอดภัยเน็ต. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.dailynews.co.th/technology/32235 ["ICT boasts results of Internet Security Operations Centre" from Daily News (2009, July 29), in Thai]

[49] newswit. (2552, กันยายน 15). รมว.ไอซีที แถลงความคืบหน้าผลงานกระทรวงไอซีที. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.newswit.com/gen/2009-09-15/4eda0e4334ccee57a7e26008d6635d23 ["ICT Minister announces progresses in Ministry's results" from newswit (2009, September 15), in Thai]

[50] ไทยรัฐออนไลน์. (2552, เมษายน 24), *supra note 48*.

[51] กรุงเทพธุรกิจออนไลน์. (2553, เมษายน 9). รัฐลุยปิด"พีทีวี-บล็อกเว็บไซต์" แดงประกาศแผนตอบโต้วันนี้. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.bangkokbiznews.com/2010/04/09/news_30664968.php ["The state closes PTV and webblogs; reds announce plans for a massive response" from Bangkokbiznews. (2010, April 9), in Thai]

[52] ประชาไท. (2552, กันยายน 4). ย้ำ !! กทช.มีอำนาจเต็มถอน-พักใบอนุญาตไอเอสพี ไม่ปิดกั้นเว็บไม่เหมาะสม. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://prachatai.com/journal/2009/09/25693 ["Again!! NBTC has full authority to withdraw/suspend ISP licences, not to close inappropriate websites" from Prachatai (2009, September 4), in Thai]

[53] ฐานเศรษฐกิจ. (2553, มกราคม 22). ไอซีที เตรียมบังคับ ISP ติดตั้ง Sniffer ดักข้อมูลของไทย. อ้างใน *RMUTL NOC*. สืบค้นเมื่อ 9 มกราคม 2555, จาก http://noc.rmutl.ac.th/main/?p=761 ["MICT prepares to require ISPs to install Sniffer to intercept Thai data" from Thansettakij (2010 June, 22) cited in RMUTL NOC, in Thai]

[54] ASTVผู้จัดการออนไลน์. (2553, มกราคม 21). ไอซีทียันดักข้อมูลชาวเน็ตไทยไม่ละเมิด "ประเทศไหนๆก็ติด Sniffer". สืบค้นเมื่อ 9 มกราคม 2555, จาก http://www.manager.co.th/cyberbiz/ViewNews.aspx?NewsID=9530000009163 ["MICT insists intercepting Thai net users' data is no violation. 'Many countries install Sniffer"' from Manager Online (2010, January 21), in Thai]

[55] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (ม.ป.ป.). รมว.ไอซีที แถลงนโยบาย 1 ปี เร่งผลักดันธุรกรรมทางอิเล็กทรอนิกส์ และถนนไร้สาย. สืบค้นเมื่อ 9 มกราคม 2555, จาก http://www.mict.go.th/ewt_news.php?nid=3360&filename=index ["ICT Minister announces 1-year policy pushing e-commerce and no-wire roads" from MICT (n.d.), in Thai]

[56] ASTVผู้จัดการออนไลน์. (2553, มิถุนายน 18). สั่งปิด 4.3 หมื่นเว็บหมิ่น 3 กระทรวงร่วมป้องสถาบัน. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9530000083941 ["4300 lèse majesté websites ordered blocked; 3 ministries cooperate to protect the institution" from Manager Online (2010, June 18), in Thai]

[57] *Id.*

[58] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (ม.ป.ป.). นายกรัฐมนตรี เปิดโครงการ Cyber Scout หนุน ก.ไอซีที สร้างลูกเสือดูแลโลกออนไลน์. สืบค้นเมื่อ 7 มกราคม 2555, จาก

http://www.mict.go.th/ewt_news.php?nid=3430&filename=index [“PM opens Cyber Scout projects; MICT creates scouts to monitor online world” from MICT (n.d.), in Thai]

[59] สุกรี แมนชัยนิมิต. (2554, กรกฎาคม 30). โมเดลสหรัฐฯ – สิงคโปร์. *Positioning*. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.positioningmag.com/magazine/details.aspx?id=92268 [“US-Singapore model” by Sugree Manchainimit from Positioning (2011. June 10), in Thai]

สำนักข่าวไทย. (2554, เมษายน 22). สื่อสังคมออนไลน์มีบทบาทต่อการเลือกตั้งสิงคโปร์เดือนหน้า. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.mcot.net/cfcustom/cache_page/199287.html [“Social networks have a role in next month’s Singapore elections” from MCOT (2011, April 22), in Thai]

[60] ไอเอ็นเอ็น. (ม.ป.ป.). ไอซีทีเตรียมวางกรอบหาเสียงผ่านสังคมออนไลน์. อ้างใน *hilight.kapook*. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://hilight.kapook.com/view/59263 [“MICT prepares framework for online election campaigning” from INN (n.d.) cited in hilight.kapook, in Thai]

[61] MThai. (2554, มิถุนายน 30). เตือน ! ห้ามหาเสียงออนไลน์ทั้งทวิตเตอร์ โพสต์เฟส คืนหมาหอน. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://news.mthai.com/politics-news/120492.html [“Warning! No online campaigning on Twitter, Facebook on the night the dogs howl” from MThai (2011, June 30), in Thai]

[62] ประชาไท. (2554, เมษายน 18). สัมภาษณ์ อรพิณ ยิ่งยงพัฒนา: ทำไมต้องต้าน พ.ร.บ. คอมฯ ฉบับใหม่. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://prachatai.com/journal/2011/04/34110 [“Interview with Orapin Yingyongphatthana: Why the new Computer Act must be opposed” from Prachatai (2011, April 18), in Thai]

[63] See details in, สาวตรี สุขศรี. บทวิเคราะห์ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.... *วารสารกสทช*. 2554(1). 267-285. [“Analysis of the Draft Computer-related Crime Act” by Sawitree Suksri, NTC Annual Review 2011, issue 1/2, p. 267-285, in Thai]

[64] ไอเอ็นเอ็น. (ม.ป.ป.). นายกฯ ชะลอร่างพ.ร.บ.คอมพิวเตอร์. อ้างใน *hilight.kapook*. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://hilight.kapook.com/view/58062 [“PM delays Computer Law” from INN (n.d.) cited in hilight.kapook, in Thai]

[65] See statistics on the cases under the Computer-related Crimes Act in this research

[66] ASTVผู้จัดการออนไลน์. (2554, สิงหาคม 23). อนุดิษฐ์ลั่น 5 นโยบาย กระทรวงไอซีที. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://www.manager.co.th/cyberbiz/ViewNews.aspx?NewsID=9540000106190 [“Anudith fires off 5 ICT policies” from Manager Online (2011, August 23), in Thai]

[67] กรุงเทพธุรกิจออนไลน์. (2554, กันยายน 12). อนุดิษฐ์ นาครทรรพ 8 คำตอบกับคำถามคาใจ. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://www.bangkokbiznews.com/home/detail/it/it/20110912/408928/อนุดิษฐ์-นาครทรรพ-8-คำตอบกับคำถามคาใจ.html ["Anudith: 8 answers to suspicious questions" from Bangkokbiznews (2011, September 12), in Thai]

[68] ประชาไท. (2554, พฤศจิกายน 23). รมว. ไอซีทีเผย ขอเฟซบุ๊กปิดเพจหมิ่นฯ แล้วกว่าหมื่นยูอาร์แอล. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://prachatai.com/journal/2011/11/38004 ["MICT reveals it has asked Facebook to block more than 10,000 URLS of lèse majesté pages" from Prachatai (2011, November 23), in Thai]

[69] MThai. (2554, พฤศจิกายน 25). รมว.ไอซีที เตือนประชาชน อย่ากด Like Comment เว็บหมิ่นสถาบันฯ. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://news.mthai.com/general-news/142656.html ["ICT Minister warns: Don't click Like, Share, Comment on lèse majesté webpages or risk 5 years in jail, 100,000 baht" from Mthai (2011, November 25), in Thai]

ประชาไท. (2554, ธันวาคม 30). ไอซีที ย้ำอีก นักท่องเว็บอย่า 'ไลค์-แชร์-เม้นต์' เว็บหมิ่นฯ. สืบค้นเมื่อ 20 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/12/38534 ["MICT repeats: web surfers must not 'Like, Share, Comment' on lèse majesté webpages" from Prachatai (2011, December 30), in Thai]

[70] ไทยโพสต์. (2554, ตุลาคม 9). มาตรฐานเดียว น.อ.อนุดิษฐ์ นาครทรรพ. สืบค้นเมื่อ 12 พฤศจิกายน 2554, จาก http://www.thaipost.net/node/46277 ["Single standard of Gp. Capt. Anudith Nakornthap" from Thaipost (2011, October 9), in Thai]

[71] ASTVผู้จัดการออนไลน์. (2554, ตุลาคม 10). อนุดิษฐ์ รับสิ้นปี wifi ฟรี 2 หมื่นจุด. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9540000128730 ["Anudhit promises 20,000 free wifi spots by year end" from Manager Online (2011, October 10), in Thai]

[72] MThai. (2554, พฤศจิกายน 26). ประชาธิปัตย์ แนะแบน ยูทูบ-เฟซบุ๊ก แบบจีนสกัดเว็บหมิ่นฯ. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://news.mthai.com/headline-news/142706.html ["Democrat Mallika proposes ban to block YouTube, Facebook, to block lèse majesté websites" from Mthai (2011, November 26), in Thai]

คมชัดลึก. (2555, มกราคม 27). มัลลิกา โวย รัฐเมินปราบเว็บหมิ่นฯ. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://www.komchadluek.net/detail/20120127/121412/มัลลิกาโวยรัฐเมินปราบเว็บหมิ่นฯ.html ["Mallika cries government not bothered about lèse majesté websites" from Kom Chad Luek (2012, January 27), in Thai]

มติชนออนไลน์. (2555, มกราคม 27). มัลลิกา ขู่ฟ้องรัฐบาลละเว้นการปฏิบัติหน้าที่หลังคดีเว็บหมิ่นไม่คืบ. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://www.matichon.co.th/

news_detail.php?newsid=1327662962&grpid=03&catid=03 ["Democrat Mallika proposes ban to block YouTube, Facebook, to block lèse majesté websites" from Matichon (2012, January 27), in Thai]

[73] See details on the web blocking prior to the enactment of the CCA, and the questions raised from civil society on the state's exercise of such power in, กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย. (2549, พฤศจิกายน 22). คำร้องต่อคณะกรรมการสิทธิมนุษยชนแห่งชาติ. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://facthai.wordpress.com/2006/11/22/a-petition-to-the-national-human-rights-commission-thai/ ["Petitions to the National Human Rights Commission" from Freedom Against Censorship Thailand (2006, November 22), in Thai]

[74] Freedom House, http://www.freedomhouse.org/

[75] Sanja Kelly & Sarah Cook. [Eds.]. (2011, April 18). Freedom on the Net 2011: A Global Assessment of Internet and Digital Media. Retrieved June 30, 2012, from http://www.freedomhouse.org/sites/default/files/FOTN2011.pdf, p. 310-320.

MarkJ. (2011, April 18). UPDATE Freedom House Warns UK Internet Users at Risk of Growing Censorship. Retrieved June 6, 2012, from http://www.ispreview.co.uk/story/2011/04/18/freedom-house-warns-uk-internet-users-at-risk-of-growing-censorship.html

[76] กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย. (2550, มีนาคม 25). ข้อเสนอของ FACT ต่อ "ร่างพ.ร.บความผิดเกี่ยวกับคอมพิวเตอร์. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://facthai.wordpress.com/2007/03/25/facts-formal-recommendations-for-cybercrime-bill-thai [Recommendations by FACT as per the draft Computer-related Crime Act" from Freedom Against Censorship Thailand (2007, March 25), in Thai]

[77] เดลินิวส์. (2551, สิงหาคม 30). คนบันเทิงชอบใจ พ.ร.บ.คอมพิวเตอร์ฯ 2550. อ้างใน *teenee*. เข้าถึงเมื่อ20 ธันวาคม 2554, จาก http://entertain.teenee.com/thaistar/25224.html ["Stars rejoice at Computer Act" from Daily News (2008, August 30) cited in Teenee, in Thai]

[78] สำนักข่าวชาวบ้าน. (ม.ป.ป.). ชาวไซเบอร์?บ่นพ.ร.บ.คอมลิดรอนสิทธิ. สืบค้นเมื่อ 17/12/2554, จาก http://www.peoplepress.in.th/archives/autopagev3/show_page.php?group_id=1&auto_id=19&topic_id=1060&topic_no=21&page=1&gaction=on ["Cyberpeople complain Computer Law gags rights" from People Press (n.d.), in Thai]

[79] Darknews. (2552, พฤศจิกายน). พ.ร.บ.คอมพิวเตอร์ฯ – เครื่องมือการเมือง. *OK Natoin Blog*. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://www.oknation.net/blog/print.php?id=520872 ["Computer Law a political tool" by Darknews from OK Natoin Blog (2009, November), in Thai]

[80] ASTVผู้จัดการออนไลน์. (2551, กรกฎาคม 22). ประเมิน พ.ร.บ.คอมพ์แค่เครื่องมือของรัฐ. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9510000085990 ["Assessing the Computer Act as a tool of the state" from Manager Online (2008, July 22), in Thai]

[81] เครือข่ายพลเมืองเน็ต. (2552, พฤศจิกายน 9). แถลงการณ์ เรื่อง การร้องขอความชัดเจนกรณีใช้ พ.ร.บ.คอมพิวเตอร์ฯ จับกุมผู้ใช้เน็ตในเดือนตุลาคม 2552. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://thainetizen.org/2009/11/statement-on-computer-crime-oct-2009/ ["Request for Clarification Regarding the Arrests of Internet Users" from Thai Netizen Network (2009, November 9), in Thai]

[82] มติชนออนไลน์. (2552, พฤศจิกายน 18). ตร.จับเพิ่มอีกแพทย์หญิง รพ.ดัง ร่วมแพร่ข่าวลือทุบหุ้น. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://www.matichon.co.th/news_detail.php?newsid=1258551109&grpid=03&catid ["Police arrest a female doctor from famous hospital for conspiring to disseminate news of share dumping" from Matichon (2009, November 18), in Thai]

[83] เครือข่ายพลเมืองเน็ต. (2552, พฤศจิกายน 9), *supra note 82*.

[84] ประชาไท. (2552, พฤศจิกายน 8). ชุมชน "ฟ้าเดียวกัน" ออกแถลงการณ์ประณามการการจับแพะกรณีทุบหุ้น. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2009/11/26510 ["Fah Diew Kan community issues statement condemning arrests of scapegoats in share dumping" from Prachatai (2009, November 8), in Thai]

[85] ประชาไท. (2552, พฤศจิกายน 25). สมัชชาสังคมก้าวหน้าเรียกร้องผู้รักเสรีภาพต่อต้าน พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์. สืบค้นเมื่อ 3 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2009/11/26744 ["Social Move Assembly calls on freedom lovers to oppose the Computer-related Crime Act" from Prachatai (2009, November 25), in Thai]

[86] DJ. อ้น ประชาชื่น (วิทยุชุมชนคนแท็กซี่). (2552, พฤศจิกายน 11). สถานการณ์การใช้อำนาจรัฐกรณี พ.ร.บ. คอมพิวเตอร์ อีกเกมหนึ่งของอำมาตย์ เกมกำจัดคู่แข่งการเมือง. ประชาไท. สืบค้นเมื่อ 3 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2009/11/26541 ["The use of state power in Computer Act cases is another game of the establishment to restrict political rivals" by DJ. On Prachachuen from Prachatai (2009, November 11), in Thai]

[87] ประชาไท. (2553, กันยายน 27). แถลงการณ์เครือข่ายนักสิทธิฯ ร้องยุติการดำเนินคดีที่ไม่เป็นธรรม ผอ.เว็บประชาไท. สืบค้นเมื่อ 3 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2010/09/31277 ["Statement of human rights activist network calls for end to unjust prosecution of Prachatai website director" from Prachatai (2010, September 27), in Thai]

[88] ประชาไท. (2553, ตุลาคม 20). เครือข่ายพลเมืองเน็ตจี้ ส.ส.แก้ด่วน ม.15 'จับแพะ' พรบ.คอมพิวเตอร์. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2010/10/31556 ["Thai Netizen Network pushes MPs to amend 'scapegoat' Section 15 of the Computer Act" from Prachatai (2010, October 20), in Thai]

[89] ประชาไท. (2554, กุมภาพันธ์ 11). แอมเนสตี้ฯ เรียกร้อง รบ.ไทยยกฟ้องทุกข้อกล่าวหาต่อ ผอ.ประชาไท. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2011/02/33063 ["Amnesty urges Thai government to withdraw all charges against Prachatai director" from Prachatai (2011, February 11), in Thai]

[90] ประชาไท. (2554, กุมภาพันธ์ 2ข). ผู้สื่อข่าวไร้พรมแดนแถลงเรียกร้องรัฐไทยถอนฟ้องคดีผอ. ประชาไท. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2011/02/32923 ["Reporters Without Borders calls for Thai state to withdraw charges against Prachatai director" from Prachatai (2011, February 2), in Thai]

[91] ประชาไท. (2554, กุมภาพันธ์ 2ก). 11 ส.ส.อังกฤษ ลงชื่อหนุน ผอ.ประชาไท เตือน รบ.ไทย ส่อลิดรอนเสรีภาพ ปชช. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2011/02/32915 ["11 'UK MPs endorse support for Prachatai director; warn Thai government of rights infringement" from Prachatai (2011, February 2), in Thai]

[92] ประชาไท. (2553, กันยายน 24). ชมรมนักข่าวเพื่อเสรีภาพแถลงประณามกรณีจับผอ.ประชาไท. สืบค้นเมื่อ 24 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2010/09/31240 ["Reporters for Freedom condemn arrest of Prachatai director" from Prachatai (2010, September 24), in Thai]

[93] Siam Intelligence Unit. (2552, มีนาคม 27). ถก พรบ.คอมพิวเตอร์ ยังขัดแย้ง มุมมองจากรัฐและภาคประชาชน. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.siamintelligence.com/computer-crime-act-tja-discussion/ ["Denate on Computer Act; conflicting views of government and the people" from Siam Intelligence Unit (2009, March 27), in Thai]

[94] ไทยเอ็นจีโอ. (2553, สิงหาคม 2). 3 ปี พรบ.คอมฯ รัฐไทยยังสืบสานแนวคิดอำนาจนิยมและละเมิดสิทธิเสรีภาพประชาชน. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.thaingo.org/writer/view.php?id=1656 ["3 years of the Computer Act; Thai state continues with authoritarian law and violations of human rights" from ThaiNGO (2010, August 2), in Thai]

[95] Thai Netizen Network. (2011, June 2). Proposals for Legal Reform for Laws Concerning Freedom of Expression. Retrieved January 19, 2012, from https://thainetizen.org/2011/06/proposal-for-legal-reform-for-laws-concerning-freedom-of-expression/

[96] iLaw. (2553, กรกฎาคม 23). นายกสมาคมสื่อแนะ ยื่นพ.ร.บ.คอมพิวเตอร์ให้ศาล ร.ธ.น.ตีความ. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://ilaw.or.th/node/433 ["TJA President suggests submitting Computer Act for Constitutional Court interpretation" from iLaw

(2010, July 23), in Thai]

[97] ประชาไท. (2554, ตุลาคม 11). เอ็นจีโอสรุปเวทียูเอ็น รัฐไทยปัดตกประเด็นร้อน รับ 100 ข้อจาก 172. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/10/37341 ["NGO summary of UPR; Thai state refutes omitting hot issues; accepts 100 out of 172 items" Prachatai (2011, October 11), in Thai]

[98] ประชาไท. (2552, ธันวาคม 6). องค์กรผู้สื่อข่าวไร้พรมแดนเรียกร้องขอพระราชทานอภัยโทษแก่ผู้ใช้อินเทอร์เน็ตที่โดนตั้งข้อหาหมิ่นฯ. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2009/12/26888 ["Reporters Without Borders calls for royal amnesty for internet users facing lèse majesté charges" from Prachatai (2009, December 6), in Thai]

[99] ประชาไท. (2554, มิถุนายน 8). UN HRC ถกประเด็นไทยละเมิดเสรีภาพออนไลน์และสิทธิแรงงานข้ามชาติ. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/06/35324 ["UN HRC discuss about Thailand's internet freedom and migrant worker's right" from Prachatai (2011, June 8), in Thai]

[100] เครือข่ายพลเมืองเน็ต. (2554, มิถุนายน 22). ประชาสังคมอาเซียน: หยุด "คิด" ก่อนเซ็นเซอร์อินเทอร์เน็ต. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://thainetizen.org/2011/06/asean-think-before-censor-internet/ ["ASEAN civil society: Stop and "think" before censoring internet content" from Thai Netizen Network (2011, June 22), in Thai]

[101] iLaw. (2554, ตุลาคม 14). รอบอาทิตย์ที่สอง ต.ค. 54: UN ย้ำไทยต้องแก้กฎหมายหมิ่น พ.ร.บ.คอม. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://ilaw.or.th/node/1225 ["Second week of October: UN emphasizes Thailand must amen lèse majesté and computer laws" from iLaw (2011, October 14), in Thai]

[102] ประชาไท. (2554, กันยายน 16). บรรษัทระดับโลกหวั่นมาตรการควบคุมเน็ตในไทย ทำธุรกิจชะงัก. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/09/36956 ["Global corporations fear Thai internet regulations stalling business" Prachatai (2011, September 16), in Thai]

[103] ประชาชาติธุรกิจออนไลน์. (2554, เมษายน 20). รุมต้านร่างพ.ร.บ.คอมพ์ฉบับใหม่ กม.คุมเข้มครอบจักรวาล"ธุรกิจ-คนใช้เน็ต"เสี่ยงคุก !!. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachachat.net/news_detail.php?newsid=1303289856&grpid=03&catid=06 ["Many oppose new Computer Bill; intensive restrictions put businesses and internet users at risk of jail!!" from Prachachat Online (2011, April 20), in Thai]

[104] iLaw. (2554, พฤษภาคม 5). อัด ร่าง พ.ร.บ.คอมฯใหม่ "ซักซ้ด-ห่วยขั้นเทพ" มั่วเรื่องลิขสิทธิ์. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://ilaw.or.th/node/921 ["Attacks on new draft "succeeds as worst ever" messing with copyrights" from iLaw (2011, May 5), in Thai]

[105] ประชาไท. (2554, เมษายน 17). iLaw ล่าชื่อ หยุดร่างพ.ร.บ.คอมฯฉบับใหม่ ก่อนเข้าครม. สืบค้นเมื่อ 18 เมษายน 2554, จาก http://prachatai.com/journal/2011/04/34085 ["iLaw collect signs to stop the new computer law" from Prachatai (2011, April 17), in Thai]

[106] เครือข่ายพลเมืองเน็ต. (2554, เมษายน 19). ผู้ใช้เน็ตยื่นค้านพ.ร.บ.คอมฯฉบับใหม่หน้าสภา นายกบอกไม่ต้องห่วง. สืบค้นเมื่อ 19 เมษายน 2554, จาก http://thainetizen.org/2011/04/netizens-new-cca-protest/ ["Net users protest new CCA draft at Parliament. PM says don't worry" from Thai Netizen Network (2011, April 19), in Thai]

[107] ไอเอ็นเอ็น. (ม.ป.ป.), *supra note 65*.

[108] For more details see http://mycomputerlaw.in.th/

[109] แนวหน้า. (2554, กันยายน 22). นักวิชาการหนุนรื้อ พ.ร.บ.คอมพ์ ปี50 แยกหมิ่นประมาณออกจากตัวก.ม. อ้างใน *RYT9*. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.ryt9.com/s/nnd/1241239 ["Academics push for dismantling computer act, separating lèse majesté" from Naewna (2011, September 22) cited in RYT9, in Thai]

[110] เครือข่ายพลเมืองเน็ต. (2553, เมษายน 8). แถลงการณ์เครือข่ายพลเมืองเน็ต เรื่องการปิดกั้นอินเทอร์เน็ตและการสื่อสารของประชาชน. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก https://thainetizen.org/2010/04/statement-on-blocking-internet-and-website/ ["Statement of Thai Netizen's Network on blocking the internet and communications of the people" from Thai Netizen Network (2010, April 8), in Thai]

Thai Netizen Network and Reporters Without Borders. (2010, April 27). Joint statement on the further censorship of websites and media under Emergency Decree. *Reporters Without Borders*. Retrieved December 20, 2011, from http://en.rsf.org/thailand-thai-netizen-network-s-statement-27-04-2010,37164.html

[111] เครือข่ายพลเมืองเน็ต. (2553, มิถุนายน 23). จดหมายเปิดผนึกถึงรัฐบาล และ ศอฉ. ให้ยุติการปิดกั้นสื่อ คืนพื้นที่การสื่อสารให้สังคม. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://thainetizen.org/2010/06/open-letter-togov-and-capo-to-stop-blocking-the-media/ ["Open letter to government and CRES to end media blocking and return communication spaces to the people" from Thai Netizen Network (2010, June 23), in Thai]

[112] Siam Intelligence Unit. (2552, เมษายน 21). เครือข่ายพลเมืองเน็ตค้านปิดเว็บไซต์จี้ยุติ พรก. ฉุกเฉิน. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.siamintelligence.com/thai-netizen-network-on-the-political-crisis-and-information-censorship/ ["Thai Netizen Network opposes blocking of websites, demands repeal of Emergency Decree" from Siam Intelligence Unit (2009, April 21), in Thai]

[113] ชุมชนคนเหมือนกัน. (2553, เมษายน 11). แถลงการณ์ชุมชนคนเหมือนกัน. อ้างใน *กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย*. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://facthai.wordpress.com/2010/04/11/แถลงการณ์-ชุมชนคนเหมือน/ ["Freedom Against

Censorship Thailand. (1 April 2010). 'Statement of People Also Community" by We are All Human (2010, April 11) cited in FACT, in Thai]

[114] for example see, ประชาไท. (2554, กุมภาพันธ์ 18). เสวนา: ไทย-อินโด-มาเลย์ เผยประสบการณ์สื่ออินเทอร์เน็ตถูกปิดกั้น. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://prachatai.com/journal/2011/02/3317 ["Seminar: Thailand-Indonesia-Malaysia reveal internet blocking experience" from Prachatai (2011, February 18), in Thai]

อิทธิพล ปรีติประสงค์. (2551, ธันวาคม 4). สิทธิพลเมืองชาวเน็ต แตกต่าง แปลกแยก คู่ขนาน ... กับโลกแห่งความเป็นจริง ? ตอนที่ 1. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://www.gotoknow.org/blogs/posts/227241 ["Netizen Rights & Liberty 'Netizen's rights: different, alienated, parallel … to the real world? Part 1" by Ittipol Preetiprasong (2008, December 4), in Thai]

bact. (2552, มกราคม 21). แบบสำรวจ "สิทธิเสรีภาพในอินเทอร์เน็ต" – An Online Survey on Internet Rights and Freedom. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://bact.cc/2009/internet-freedom-survey/ ["An Online Survey on Internet Rights and Freedom" by bact (2009, January 21), in Thai]

[115] For pictures of the campaign see, สุนิตย์ เชรษฐา. (2550, มิถุนายน 12). ร่วมรณรงค์ "เซ็นเซอร์จัง" ต่อต้านการปิดเว็บแบบมั่วๆ. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://www.learners.in.th/blogs/posts/33725 ["Join the 'Censor Jung' campaign against indiscriminate website blocking" by Sunit Chetha (2007, June 12), in Thai]

[116] ประชาไท. (2554, ตุลาคม 31). 'ผู้สื่อข่าวไร้พรมแดน' เปิดตัวแคมเปญ ไทยแลนด์ - 'แดนสวรรค์การเซ็นเซอร์'. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://prachatai.com/journal/2011/10/37683 ["Reporters without Borders launch new campaign, Thailand – 'censorship paradise'" from Prachatai (2011, October 31), in Thai]

[117] กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย. (2549, พฤศจิกายน 22). คำร้องต่อคณะกรรมการสิทธิมนุษยชนแห่งชาติ, *supra note 74*.

[118] กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย. (ม.ป.ป.). FACT petition signers รายชื่อผู้ลงชื่อสนับสนุน. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://facthai.wordpress.com/sign/signer-list/ ["FACT petition signers" from Freedom Against Censorship Thailand (n.d.), in Thai]

[119] candy strawberry milk (2553, มกราคม 22). Thai No Sniff - ความตื่นตัวเรื่องสิทธิของ netizen ไทย. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://my.dek-d.com/sweetsin/blog/?blog_id=10050555 ["Thai No Sniff – Thai neitzens' alert on rights" by candy strawberry milk (2010, January 22), in Thai]

[120] กนกรัตน์ โกวิชัย. (2553, กุมภาพันธ์ 1). ไอซีที ฝันค้าง "สนิฟเฟอร์" ตกหลุมอากาศ. *ไทยรัฐออนไลน์*. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://www.thairath.co.th/content/

tech/62414 ["ICT dream collapses, Sniffer falls through air holes" by Konokrat Kovichai from Thai Rath Online (2010, February 1), in Thai]

lew. (2553, มกราคม 26). ไอซีทียอมแพ้, เลิกแนวคิดใช้ sniffer. *Blognone*. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://www.blognone.com/node/14785 ["ICT gives in, idea scrapped" by lew from Blognone (2010, January 26), in Thai]

[121] เครือข่ายพลเมืองเน็ต. (2554, พฤศจิกายน 30). แถลงการณ์เครือข่ายพลเมืองเน็ต: กดไลค์ ไม่ใช่อาชญากรรมกระทรวงไอซีทีต้องทบทวนมาตรการจัดการ "เฟซบุ๊กหมิ่น" และ ข้อแนะนำต่อพลเมืองเน็ตเมื่อเจอหน้าเว็บที่ไม่ถูกใจ. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://thainetizen.org/2011/11/click-like-is-not-a-crime/ ["Statement of Thai Netizen Network: Clicking 'Like' is not a crime" from Thai Netizen Network (2011, November 30), in Thai]

[122] ประชาไท. (2554, พฤศจิกายน 23). รมว. ไอซีทีเผย ขอเฟซบุ๊กปิดเพจหมิ่นฯแล้วกว่าหมื่นยูอาร์แอล, *supra note 69*.

[123] Cyber Warrior Club, FightBadWeb@gmail.com

[124] ไทยรัฐออนไลน์. (ม.ป.ป.). สมาคมผู้ดูแลเว็บฯ ติงไอซีที แก้ปัญหาเว็บหมิ่นไม่ตรงจุด. อ้างใน *highlight.kapook*. สืบค้นเมื่อ 20 กุมภาพันธ์ 2555, จาก http://hilight.kapook.com/view/30448 ["Webmaster Association Criticizes MICT for not effectively addressing the problem of lèse majesté websites" from Thai Rath Online (n.d.) cited in highlight.kapook, in Thai]

[125] ASTVผู้จัดการออนไลน์. (2554, สิงหาคม 18). จี้ "รมว. ไอซีที" เร่งปราบเว็บหมิ่น. สืบค้นเมื่อ 20 กุมภาพันธ์ 2555, จาก http://www.manager.co.th/CyberBiz/ViewNews.aspx?NewsID=9540000103856 ["Network to Safeguard and Protect the Monarchy and the Chakri Dynasty Protection Network encourage MICT minister to stop lèse majesté websites" from Manager Online (2011, August 18), in Thai]

[126] Literally translated as 'impaling on a stake for public display', this form of public ridicule has spread among many webboards. In late April 2010, a Facebook user posted a message, and his personal identity was exposed and publicly ridiculed. He was accused of defaming the monarchy. A number of webboarders helped to dig out his personal information and distribute it without his consent. The next day, he was raided and arrested by officials from Department of Special Investigation (DSI). In addition, another Facebook user who made a comment in a posting deemed lèse majesté was also exposed to public ridicule. At present, both are facing lèse majesté charges under the supervision of DSI.

[127] สงกรานต์ ป้องบุญจันทร์. (2553, พฤษภาคม 11). บทวิเคราะห์คำพิพากษาศาลแพ่งคดีปิดเว็บประชาไท. *ประชาไท*. สืบค้นเมื่อ 28 มกราคม 2555, จาก http://prachatai.com/journal/2010/05/29391 ["Analysis of the Civil Court verdict on the Prachatai website

blocking case" by Songkran Pongboonchan from Prachatai (2010, May 11), in Thai]

[128] ASTVผู้จัดการออนไลน์. (2554, มิถุนายน 6). งามไส้ไอซีที ประชาชนรู้จักพ.ร.บ.คอมฯดีแค่ 0.98%. สืบค้นเมื่อ 6 มิถุนายน 2555, จาก http://mgr.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9540000069083 ["ICT: only 0.98% of people know Computer Act well" from Manager Online (2011, June 6), in Thai]

[129] แม่สายนิวส์. (2554, มีนาคม 28). นักกฎหมายชำแหละ พรบ.คอมพิวเตอร์ 3 ปี คนไม่รู้ว่ามี 70% เหตุขาดการประชาสัมพันธ์-ปัญหาตีความการบังคับใช้กฎหมาย. สืบค้นเมื่อ 28 มกราคม 2555, จาก http://www.maesainews.com/plus/index.php?name=knowledge&file=readknowledge&id=268 ["Lawyer dissects Computer Act: 70% don't know it exists after 3 years of enforcement" from Maesainews (2011, March 28), in Thai]

Legal Comparison

[1] Amnesty International. (n.d.). Imprisoned for Peaceful Expression. Retrieved July 12, 2012, from http://www.amnestyusa.org/our-work/cases/china-shi-tao

[2] Jake Hooker. (2008, July 11). Voice seeking answers for parents about school collapse in China is silenced. *The New York Times*. Retrieved July 12, 2012, from http://www.nytimes.com/2008/07/11/world/asia/11iht-11china.14412092.html?_r=1

Recommendations

[1] See a summary of the problem in defining the term. "service provider" from the drafting process and validation by a group of internet entrepreneurs at, เช กูวารา (นามแฝง). (2555, ตุลาคม 24). กฎหมาย ที่ร่างกันแบบไม่เร่ง แต่ผ่านกันแบบรีบ ๆ (ตอน 1-5). *iLaw* สืบค้นเมื่อ 24 ตุลาคม 2555 จาก http://ilaw.or.th/node/1748 ["Slowly draft, but hurriedly pass the bill (part 1-5)" by Che Guevara (pseudonym) from iLaw (2012, October 24), in Thai]

[2] The telecommunication and broadcasting business group under Section 5 (1) of the Notification of the Ministry of Information and Communication Technology regarding Procedures for Storage of Computer Traffic Data of Service Providers B.E. 2550

[3] Such as Germany's Telekommunikationsgesetz (TKG)

[4] Gesetz über die Nutzung von Telediensten (Teledienstegesetz -TDG): § 9 Durchleitung von Informationen

[5] For more on Notice and Takedown (NTD) see, Christian Ahlert, Chris Marsden and Chester Yung. (n.d.). How 'Liberty' Disappeared from Cyberspace: The Mystery

Shopper Tests Internet Content Self-Regulation. Retrived June 10, 2011, from http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf

[6] Apart from the statistics about the number of court orders and of the web pages blocked shown in this report, a recent news report found that within 4 months, the court has issued a total of 28 orders to block 5,064 URLs. see, ASTVผู้จัดการออนไลน์. (2555, มีนาคม 14). ตร.พอใจผลปราบเว็บหมิ่นสถาบัน-ชี้ 4 เดือนปิดแล้ว 5 พันยูอาร์เอล. สืบค้นเมื่อ 10 มิถุนายน 2555, จาก http://www.manager.co.th/Crime/ViewNews.aspx?NewsID=9550000033137 ["Police satisfied with the result of combating lèse majesté sites and points out 5000 URLs already shut down in 4 months" by Manager Online (2021, March 14), in Thai]

[7] ประชาไท. (2553, พฤศจิกายน 22). จนท.ไอซีทีเผย การขึ้นบัญชีดำบล็อคเว็บ "ล้มเหลว". สืบค้นเมื่อ 10 มิถุนายน 2555, จาก http://prachatai.com/journal/2010/11/31998 ["ICT officer reveals that blacklisting sites fails" from Prachatai (2010, November 22), inThai]

บรรณานุกรม

สิ่งพิมพ์ภาษาไทย

คณิต ณ นคร. (2551). *กฎหมายอาญาภาคทั่วไป*. (พิมพ์ครั้งที่ 3). กรุงเทพฯ: วิญญูชน.

โลโก้พระพุทธเจ้า“เว็บ”ลามก“พระ”เปิดเจอ-ร้องจ๊าก. *ข่าวสด*. (2550, มกราคม 8). หน้า 1.

จิตติ ติงศภัทิย์. (2543). *คำอธิบายประมวลกฎหมายอาญา, ภาค 2 ตอน 1*. (พิมพ์ครั้งที่ 7). กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา.

ธีระ สุธีวรางกูร. การคุ้มครองสิทธิและเสรีภาพของบุคคลที่รัฐธรรมนูญรับรอง. *วารสารนิติศาสตร์*, 29(4) (2542), 578-592.

บัณฑิต จำรูญวงศ์สกุล. (2554). *การกำกับดูแลและแทรกแซงเว็บบอร์ดทางการเมืองหลังเหตุการณ์รัฐประหาร 19 กันยายน 2549*. วิทยานิพนธ์นิเทศศาสตร์มหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย.

บวรศักดิ์ อุวรรณโณ. (2538). *กฎหมายมหาชนเล่ม 3 ที่มาและนิติวิธี*. กรุงเทพฯ: นิติธรรม.

วรพจน์ วิศรุตพิชญ์. (2543). *สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540*. กรุงเทพฯ: วิญญูชน.

สาวตรี สุขศรี. บทวิเคราะห์ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ..... *วารสารกสทช*. 2554(1). 267-285.

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ. (2544). *รวมร่างกฎหมายเทคโนโลยีสารสนเทศ ภายใต้โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ*. กรุงเทพฯ: โรงพิมพ์เดือนตุลาคม.

ข้อมูลอิเล็กทรอนิกส์ภาษาไทย

กนกรัตน์ โกวิชัย. (2553, กุมภาพันธ์ 1). ไอซีที ฝันค้าง “สนิฟเฟอร์” ตกหลุมอากาศ. *ไทยรัฐออนไลน์*. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://www.thairath.co.th/content/tech/6241

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (ม.ป.ป.). นายกรัฐมนตรี เปิดโครงการ Cyber Scout หนุน ก.ไอซีที สร้างลูกเสือดูแลโลกออนไลน์. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.mict.go.th/ewt_news.php?nid=3430&filename=index

_____. (ม.ป.ป.). รมว.ไอซีที แถลงนโยบาย 1 ปี เร่งผลักดันธุรกรรมทางอิเล็กทรอนิกส์และถนนไร้สาย. สืบค้นเมื่อ 9 มกราคม 2555, จาก http://www.mict.go.th/ewt_

news.php?nid=3360&filename=index

กรุงเทพธุรกิจออนไลน์. (2551, พฤศจิกายน 7). ไอซีทีออก 5 มาตรการต้านเว็บหมิ่น. สืบค้นเมื่อ 10 ตุลาคม 2554, จาก http://www.bangkokbiznews.com/2008/11/07/news_309786.php

_____. (2553, เมษายน 9). รัฐลุยปิด"พีทีวี-บล็อกเว็บไซต์" แดงประกาศแผนตอบโต้วันนี้. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.bangkokbiznews.com/2010/04/09/news_30664968.php

_____. (2554, กันยายน 12). อนุดิษฐ์ นาครทรรพ 8 คำตอบกับคำถามคาใจ. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://www.bangkokbiznews.com/home/detail/it/it/20110912/408928/อนุดิษฐ์-นาครทรรพ-8-คำตอบกับคำถามคาใจ.html

กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย. (2549, พฤศจิกายน 22). คำร้องต่อคณะกรรมการสิทธิมนุษยชนแห่งชาติ. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://facthai.wordpress.com/2006/11/22/a-petition-to-the-national-human-rights-commission-thai/

_____. (2550, มีนาคม 25). ข้อเสนอของ FACT ต่อ “ร่างพ.ร.บความผิดเกี่ยวกับคอมพิวเตอร์. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://facthai.wordpress.com/2007/03/25/facts-formal-recommendations-for-cybercrime-bill-thai/

_____. (2551, มีนาคม 18). “แฮค & แครก” เว็บหมิ่น ไอซีทีรู้ผิดกฎหมายแต่จะทำ. สืบค้นเมื่อ 18 สิงหาคม 2554, จาก http://facthai.wordpress.com/2008/03/18/ict-to-hack-and-crack-thai/

_____. (ม.ป.ป.). FACT petition signers รายชื่อผู้ลงชื่อสนับสนุน. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://facthai.wordpress.com/sign/signer-list/

คณะวิจัยผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น. (2553, ธันวาคม 8). รายงานสถานการณ์ การควบคุมและปิดกั้นสื่อออนไลน์ ด้วยการอ้างกฎหมายและแนวนโยบายแห่งรัฐไทย. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.scribd.com/doc/44961877/รายงานสถานการณ์การควบคุมและปิดกั้นสื่อออนไลน์ด้วยการอ้างกฎหมายและแนวนโยบายแห่งรัฐไทย

คมชัดลึก. (2551, มิถุนายน 10). มั่น พัธโนทัยไอซีทีคอร์ปผู้ปิดทองหลังพระ. อ้างใน *news.sanook*. สืบค้นเมื่อ 9 ตุลาคม 2554, จาก http://news.sanook.com/politic/politic_276054.php

_____. (2555, มกราคม 27). มัลลิกา โวย รัฐเมินปราบเว็บหมิ่นฯ. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://www.komchadluek.net/detail/20120127/121412/มัลลิกาโวยรัฐเมินปราบเว็บหมิ่นฯ.html

_____. (ม.ป.ป.). สนช.ผ่านร่าง พรบ. ว่าด้วยการกระทำผิดคอมพิวเตอร์. สืบค้นเมื่อ 15

ตุลาคม 2554, จาก http://kmochadluek.com
เครือข่ายพลเมืองเน็ต. (2552, กรกฎาคม 27). ข้อเสนอเครือข่ายพลเมืองเน็ตต่อการบังคับใช้กฎหมายกับคดีทางคอมพิวเตอร์และอินเทอร์เน็ต. สืบค้นเมื่อ19 มกราคม 2555, จาก http://thainetizen.org/docs/netizen-press-20090727/
_____. (2552, พฤศจิกายน 9). แถลงการณ์ เรื่อง การร้องขอความชัดเจนกรณีใช้ พ.ร.บ.คอมพิวเตอร์ฯ จับกุมผู้ใช้เน็ตในเดือนตุลาคม 2552. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://thainetizen.org/2009/11/statement-on-computer-crime-oct-2009/
_____. (2553, เมษายน 8). แถลงการณ์เครือข่ายพลเมืองเน็ต เรื่องการปิดกั้นอินเทอร์เน็ตและการสื่อสารของประชาชน. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก https://thainetizen.org/2010/04/statement-on-blocking-internet-and-website/
_____. (2553, มิถุนายน 23). จดหมายเปิดผนึกถึงรัฐบาล และ ศอฉ. ให้ยุติการปิดกั้นสื่อ คืนพื้นที่การสื่อสารให้สังคม. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://thainetizen.org/2010/06/open-letter-togov-and-capo-to-stop-blocking-the-media/
_____. (2554, เมษายน 19). ผู้ใช้เน็ตยื่นค้านพ.ร.บ.คอมฯฉบับใหม่หน้าสภา นายกบอกไม่ต้องห่วง. สืบค้นเมื่อ 19 เมษายน 2554, จาก http://thainetizen.org/2011/04/netizens-new-cca-protest/
_____. (2554, มิถุนายน 22). ประชาสังคมอาเซียน: หยุด "คิด" ก่อนเซ็นเซอร์อินเทอร์เน็ต. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://thainetizen.org/2011/06/asean-think-before-censor-internet/
_____. (2554, พฤศจิกายน 30). แถลงการณ์เครือข่ายพลเมืองเน็ต: กดไลค์ ไม่ใช่อาชญากรรมกระทรวงไอซีทีต้องทบทวนมาตรการจัดการ “เฟซบุ๊กหมิ่น” และข้อแนะนำต่อพลเมืองเน็ตเมื่อเจอหน้าเว็บที่ไม่ถูกใจ. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://thainetizen.org/2011/11/click-like-is-not-a-crime/
งานบริการข้อมูลคดี ศาลอาญา. (ม.ป.ป.). งานบริการข้อมูลคดี ศาลอาญา. สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://aryasearch.coj.go.th/aryaweb/main.php
เช กูวารา (นามแฝง). (2555, ตุลาคม 24). กฎหมาย ที่ร่างกันแบบไม่เร่ง แต่ผ่านกันแบบรีบๆ (ตอน 1-5). *iLaw* สืบค้นเมื่อ 24 ตุลาคม 2555 จาก http://ilaw.or.th/node/1748
ชุมชนคนเหมือนกัน. (2553, เมษายน 11). แถลงการณ์ชุมชนคนเหมือนกัน. อ้างใน *กลุ่มเสรีภาพต่อต้านการเซ็นเซอร์แห่งประเทศไทย*. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://facthai.wordpress.com/2010/04/11/แถลงการณ์-ชุมชนคนเหมือน/
ฐานเศรษฐกิจ. (2553, มกราคม 22). ไอซีที เตรียมบังคับ ISP ติดตั้ง Sniffer ดักข้อมูลของไทย. อ้างใน *RMUTL NOC*. สืบค้นเมื่อ 9 มกราคม 2555, จาก http://noc.

rmutl.ac.th/main/?p=761
เดลินิวส์. (2550, มกราคม 9). ไอซีทีเผยไล่บล็อกเว็บโป๊แล้วกว่าหมื่น! หนักใจเว็บนอกคุมยาก. อ้างใน *TLCNews*. สืบค้นเมื่อ 5 ตุลาคม 2554, จาก http://news.tlcthai.com/news-interest/112.html
_____. (2551, สิงหาคม 30). คนบันเทิงชอบใจ พ.ร.บ.คอมพิวเตอร์ฯ 2550. อ้างใน teenee. เข้าถึงเมื่อ20 ธันวาคม 2554, จาก http://entertain.teenee.com/thaistar/25224.html
_____. (2552, กรกฎาคม 29). ไอซีทีอวดผลงานศูนย์ปฏิบัติการปลอดภัยเน็ต. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.dailynews.co.th/technology/32235
ไทยโพสต์. (2554, ตุลาคม 9). มาตรฐานเดียว น.อ.อนุดิษฐ์ นาครทรรพ. สืบค้นเมื่อ 12 พฤศจิกายน 2554, จาก http://www.thaipost.net/node/46277
ไทยรัฐออนไลน์. (2550, มกราคม 30).ไอซีทีบล็อกแคมฟรอกแล้ว หลังโจ๋ไทยไม่หยุดโชว์. อ้างใน *news.sanook*. สืบค้นเมื่อ 5 ตุลาคม 2555 จาก http://news.sanook.com/crime/crime_88511.php
_____. (2550, พฤษภาคม 30). ถูกหาละเมิดสิทธิ 'สิทธิชัย' ยกสถิติปิด เว็บ 2 รบ. เปรียบเทียบ. อ้างใน *MakeWebExy.com* สืบค้นเมื่อ 30 กรกฎาคม 2554, จาก http://www.makewebez.com/tips/index.php?page=show&id=233
_____. (2552, เมษายน 24). 'ระนองรักษ์' ตื่นลุยปราบผู้ใช้เน็ตป่วนชาติ. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.thairath.co.th/content/tech/1669
_____. (2554, กรกฎาคม 6). ปชป.สับพท.แค่48ชม.ลุอำนาจไล่ปิดวิทยุชุมชน. สืบค้นเมื่อ 7 พฤษภาคม 2555, จาก http://www.thairath.co.th/content/pol/184129
_____. (2554, ธันวาคม 14). ได้ที 'เฉลิม' ของบ 400 ล้านบ. ซื้อเครื่องดักเว็บหมิ่นฯ. สืบค้นเมื่อ 14 ธันวาคม 2554, จาก http://www.thairath.co.th/content/pol/223580
_____. (ม.ป.ป.). สมาคมผู้ดูแลเว็บฯ ติงไอซีที แก้ปัญหาเว็บหมิ่นไม่ตรงจุด. อ้างใน *highlight.kapook*. สืบค้นเมื่อ 20 กุมภาพันธ์ 2555, จาก http://hilight.kapook.com/view/30448
ไทยเอ็นจีโอ. (2553, สิงหาคม 2). 3 ปี พรบ.คอมฯ รัฐไทยยังสืบสานแนวคิดอำนาจนิยมและละเมิดสิทธิเสรีภาพประชาชน. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.thaingo.org/writer/view.php?id=1656
นิติราษฎร์: นิติศาสตร์เพื่อราษฎร. (2554, ธันวาคม 26). ข้อเสนอเพื่อการรณรงค์แก้ไขเพิ่มเติมประมวลกฎหมายอาญามาตรา 112. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.enlightened-jurists.com/download/67
แนวหน้า. (2554, กันยายน 22). นักวิชาการหนุนรื้อ พ.ร.บ.คอมพ์ ปี50 แยกหมิ่นประมาณ

ออกจากตัวก.ม. อ้างใน *RYT9*. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.ryt9.com/s/nnd/1241239

บันทึกสำนักงานคณะกรรมการกฤษฎีกา ประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ... เรื่องเสร็จที่ 257/2548. (ม.ป.ป.). สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://www.dms.moph.go.th/dmsict/doc_file/policy.doc

ประชาชาติธุรกิจออนไลน์. (2554, เมษายน 20). รุมต้านร่างพ.ร.บ.คอมพ์ฉบับใหม่ กม.คุมเข้มครอบจักรวาล"ธุรกิจ-คนใช้เน็ต"เสี่ยงคุก !!. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachachat.net/news_detail.php?newsid=1303289856&grpid=03&catid=06

_____. (ม.ป.ป.). ยกเครื่องมาตรการสกัดเว็บต้องห้าม. อ้างใน *decha.com*. สืบค้นเมื่อ 9 ตุลาคม 2554, จาก http://www.decha.com/main/showTopic.php?id=2737

ประชาไท. (2549, พฤศจิกายน 19). สนช.ลงมติรับหลักการร่าง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.... วาระแรก. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.prachatai.com/journal/2006/11/10527

_____. (2552, กันยายน 4). ย้ำ !! กทช.มีอำนาจเต็มถอน-พักใบอนุญาตไอเอสพี ไม่ปิดกั้นเว็บไม่เหมาะสม. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://prachatai.com/journal/2009/09/25693

_____. (2552, พฤศจิกายน 8). ชุมชน “ฟ้าเดียวกัน” ออกแถลงการณ์ประณามการจับแพะกรณีทุบหุ้น. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2009/11/26510

_____. (2552, พฤศจิกายน 25). สมัชชาสังคมก้าวหน้าเรียกร้องผู้รักเสรีภาพต่อต้าน พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์. สืบค้นเมื่อ 3 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2009/11/26744

_____. (2552, ธันวาคม 6). องค์กรผู้สื่อข่าวไร้พรมแดนเรียกร้องขอพระราชทานอภัยโทษแก่ผู้ใช้อินเทอร์เน็ตที่โดนตั้งข้อหาหมิ่นฯ. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2009/12/26888

_____. (2553, กันยายน 24). ชมรมนักข่าวเพื่อเสรีภาพแถลงประณามกรณีจับ ผอ.ประชาไท. สืบค้นเมื่อ 24 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2010/09/31240

_____. (2553, กันยายน 27). แถลงการณ์เครือข่ายนักสิทธิฯ ร้องยุติการดำเนินคดีที่ไม่เป็นธรรม ผอ.เว็บประชาไท. สืบค้นเมื่อ 3 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2010/09/31277

_____. (2553, ตุลาคม 20). เครือข่ายพลเมืองเน็ตจี้ ส.ส.แก้ด่วน ม.15 'จับแพะ' พรบ. คอมพิวเตอร์. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/

journal/2010/10/31556
_____. (2553, พฤศจิกายน 22). จนท.ไอซีทีเผย การขึ้นบัญชีดำบล็อคเว็บ “ล้มเหลว”. สืบค้นเมื่อ 10 มิถุนายน 2555, จาก http://prachatai.com/journal/2010/11/31998
_____. (2554, กุมภาพันธ์ 2ก). 11 ส.ส.อังกฤษ ลงชื่อหนุน ผอ.ประชาไท เตือน รบ.ไทยส่อลิดรอนเสรีภาพ ปชช. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2011/02/32915
_____. (2554, กุมภาพันธ์ 2ข). ผู้สื่อข่าวไร้พรมแดนแถลงเรียกร้องรัฐไทยถอนฟ้องคดีผอ. ประชาไท. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2011/02/32923
_____. (2554, กุมภาพันธ์ 11). แอมเนสตี้ฯ เรียกร้อง รบ.ไทยยกฟ้องทุกข้อกล่าวหาต่อ ผอ.ประชาไท. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2011/02/33063
_____. (2554, กุมภาพันธ์ 18). เสวนา: ไทย-อินโด-มาเลย์ เผยประสบการณ์สื่ออินเทอร์เน็ตถูกปิดกั้น. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://prachatai.com/journal/2011/02/33174
_____. (2554, เมษายน 17). iLaw ล่าชื่อ หยุดร่างพ.ร.บ.คอมฯฉบับใหม่ ก่อนเข้า ครม. สืบค้นเมื่อ 18 เมษายน 2554, จาก http://prachatai.com/journal/2011/04/34085
_____. (2554, เมษายน 18). สัมภาษณ์ อรพิณ ยิ่งยงพัฒนา: ทำไมต้องต้าน พ.ร.บ. คอมฯ ฉบับใหม่. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://prachatai.com/journal/2011/04/34110
_____. (2554, มิถุนายน 8). UN HRC ถกประเด็นไทยละเมิดเสรีภาพออนไลน์และสิทธิแรงงานข้ามชาติ. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/06/35324
_____. (2554, กันยายน 16). บรรษัทระดับโลกหวั่นมาตรการควบคุมเน็ตในไทยทำธุรกิจชะงัก. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/09/36956
_____. (2554, ตุลาคม 11). เอ็นจีโอสรุปเวทียูเอ็น รัฐไทยปัดตกประเด็นร้อนรับ 100 ข้อจาก 172. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/10/37341
_____. (2554, ตุลาคม 31). ‘ผู้สื่อข่าวไร้พรมแดน’ เปิดตัวแคมเปญ ไทยแลนด์ - ‘แดนสวรรค์การเซ็นเซอร์’. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://prachatai.com/journal/2011/10/37683
_____. (2554, พฤศจิกายน 23). รมว. ไอซีทีเผย ขอเฟซบุ๊กปิดเพจหมิ่นฯ ไปแล้วกว่าหมื่นยูอาร์แอล. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://prachatai.com/journal/2011/11/38004

_____. (2554, ธันวาคม 1). ไอซีทีเปิดตัวศูนย์ความมั่นคงไซเบอร์ สุดเข้มปราบเว็บหมิ่นฯ สถาบัน. สืบค้นเมื่อ 20 มกราคม 2555, จาก http://prachatai.com/journal/2011/12/38121

_____. (2554, ธันวาคม 9). ดูแนวทาง 'เฉลิม' ปราบเว็บหมิ่น งัดมาตรการ 'ขอร่วมมือกฎหมาย และ...ประจาน'. สืบค้นเมื่อ 9 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2011/12/38245

_____. (2554, ธันวาคม 30). ไอซีที ย้ำอีก นักท่องเว็บอย่า 'ไลค์-แชร์-เม้นต์' เว็บหมิ่นฯ. สืบค้นเมื่อ 20 มกราคม 2555, จาก http://www.prachatai3.info/journal/2011/12/38534

_____. (2555, พฤษภาคม 30). ศาลตัดสิน “ผอ.ประชาไท” ผิดคดีตัวกลาง สั่งจำคุกแต่ให้รอลงอาญา. สืบค้นเมื่อ 30 มิถุนายน 2555, จาก http://prachatai.com/node/40757

โพสต์ทูเดย์. (2554, ธันวาคม 8). เฟซบุ๊กร่วมบล็อกคนโพสต์หมิ่นแล้ว6หมื่นราย. สืบค้นเมื่อ 8 ธันวาคม 2554, จาก http://www.posttoday.com/อาชญากรรม/125948/เฟซบุ๊คร่วมบล็อกคนโพสต์หมิ่นแล้ว6หมื่นราย

มติชนออนไลน์. (2552, พฤศจิกายน 18). ตร.จับเพิ่มอีกแพทย์หญิง รพ.ดัง ร่วมแพร่ข่าวลือทุบหุ้น. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://www.matichon.co.th/news_detail.php?newsid=1258551109&grpid=03&catid

_____. (2555, มกราคม 27). มัลลิกา ขู่ฟ้องรัฐบาลละเว้นการปฏิบัติหน้าที่ หลังคดีเว็บหมิ่นไม่คืบ. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://www.matichon.co.th/news_detail.php?newsid=1327662962&grpid=03&catid=03

มุทิตา เชื้อชั่ง. (2554, 29 เมษายน). รายงาน: สำรวจสถานการณ์หลังปิดวิทยุชุมชนเสื้อแดง (ระลอกแรก). *ประชาไท*. สืบค้นเมื่อ 7 พฤษภาคม 2555, จาก http://www.prachatai.com/journal/2011/04/34291

แม่สายนิวส์. (2554, มีนาคม 28). นักกฎหมายชำแหละ พรบ.คอมพิวเตอร์ 3 ปี คนไม่รู้ว่ามี 70% เหตุขาดการประชาสัมพันธ์-ปัญหาตีความการบังคับใช้กฎหมาย. สืบค้นเมื่อ 28 มกราคม 2555, จาก http://www.maesainews.com/plus/index.php?name=knowledge&file=readknowledge&id=268

วิกิพีเดีย สารานุกรมเสรี. (ม.ป.ป.). กลุ่มวันอาทิตย์สีแดง. สืบค้นเมื่อ 29 กุมภาพันธ์ 2555, จาก http://th.wikipedia.org/wiki/กลุ่มวันอาทิตย์สีแดง

สงกรานต์ ป้องบุญจันทร์. (2553, พฤษภาคม 11). บทวิเคราะห์คำพิพากษาศาลแพ่งคดีปิดเว็บประชาไท. *ประชาไท*. สืบค้นเมื่อ 28 มกราคม 2555, จาก http://prachatai.com/journal/2010/05/29391

สยามจดหมายเหตุ. (ม.ป.ป.). สั่งปิดเว็บไซต์แพร่คลิปวิดีโอหมิ่นพระบรมเดชานุภาพ. สืบค้นเมื่อ 5 ตุลาคม 2554, จาก http://www.siamarchives.com/สั่งปิดเว็บไซต์แพร่คลิป/

สุกรี แมนชัยนิมิต. (2554, กรกฎาคม 30). โมเดลสหรัฐฯ – สิงคโปร์. *Positioning*. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.positioningmag.com/magazine/details.aspx?id=92268

สุนิตย์ เชรษฐา. (2550, มิถุนายน 12). ร่วมรณรงค์ "เซ็นเซอร์จัง" ต่อต้านการปิดเว็บแบบมั่วๆ. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://www.learners.in.th/blogs/posts/33725

สำนักข่าวชาวบ้าน. (ม.ป.ป.). ชาวไซเบอร์?บ่นพ.ร.บ.คอมลิดรอนสิทธิ. สืบค้นเมื่อ 17/12/2554, จาก http://www.peoplepress.in.th/archives/autopagev3/show_page.php?group_id=1&auto_id=19&topic_id=1060&topic_no=21&page=1&gaction=on

สำนักข่าวไทย. (2554, เมษายน 22). สื่อสังคมออนไลน์มีบทบาทต่อการเลือกตั้งสิงคโปร์เดือนหน้า. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.mcot.net/cfcustom/cache_page/199287.html

_____. (ม.ป.ป.). ยกเลิกประกาศคปค. ฉบับที่ 5 เรื่องควบคุมเว็บไซต์. อ้างใน *oxygen*. สืบค้นเมื่อ 30 กรกฎาคม 2554, จาก http://oxygen.readyplanet.com/index.php?lay=show&ac=article&Id=416946&Ntype=20

สำนักข่าวอินโฟเควสท์ (IQ). (2551, ตุลาคม 28). รมว.ไอซีที เล็งซื้ออุปกรณ์บล็อคเว็บหมื่นสถาบัน 100-500 ลบ./เครื่อง. อ้างใน *RYT9*. สืบค้นเมื่อ 10 ตุลาคม 2554, จาก http://www.ryt9.com/s/iq02/458881

อาทิตย์ สุริยะวงศ์กุล. (2553, ธันวาคม 25). สื่อและขบวนการทางสังคมในมาเลเซีย: กรณีศึกษาหนังสือพิมพ์มาเลเซียกินี. สืบค้นเมื่อ 20 มีนาคม 2555, จาก http://bact.cc/2010/malaysiakini-malaysia-media-social-movement/

อิทธิพล ปรีติประสงค์. (2551, ธันวาคม 4).สิทธิพลเมืองชาวเน็ต แตกต่าง แปลกแยก คู่ขนาน ... กับโลกแห่งความเป็นจริง ? ตอนที่ 1. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://www.gotoknow.org/blogs/posts/227241

ไอเอ็นเอ็น. (ม.ป.ป.). นายกฯ ชะลอร่างพ.ร.บ.คอมพิวเตอร์. อ้างใน *hilight.kapook*. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://hilight.kapook.com/view/58062

_____. (ม.ป.ป.). ไอซีทีเตรียมวางกรอบหาเสียงผ่านสังคมออนไลน์. อ้างใน *hilight.kapook*. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://hilight.kapook.com/view/59263

ASTV ผู้จัดการออนไลน์ (2551, กรกฎาคม 22). ประเมิน พ.ร.บ.คอมพ์แค่เครื่องมือของรัฐ. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9510000085990

_____. (2552, กุมภาพันธ์ 5). ระนองรักษ์ ตั้ง ISOC สกัดเว็บหมิ่น – ยันไม่ปิดไฮไฟว์. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.manager.co.th/cyberbiz/

ViewNews.aspx?NewsID=9520000013365

_____. (2553, มกราคม 21). ไอซีทียันตักข้อมูลชาวเน็ตไทยไม่ละเมิด "ประเทศไหนๆ ก็ติด Sniffer". สืบค้นเมื่อ 9 มกราคม 2555, จาก http://www.manager.co.th/cyberbiz/ViewNews.aspx?NewsID=9530000009163

_____. (2553, มิถุนายน 18). สั่งปิด 4.3 หมื่นเว็บหมิ่น 3 กระทรวงร่วมป้องสถาบัน. สืบค้นเมื่อ 7 มกราคม 2555, จาก http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9530000083941

_____. (2554, มิถุนายน 6). งามไส้ไอซีที ประชาชนรู้จักพ.ร.บ.คอมฯดีแค่ 0.98%. สืบค้นเมื่อ 6 มิถุนายน 2555, จาก http://mgr.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9540000069083

_____. (2554, สิงหาคม 18). จี้ “รมว. ไอซีที” เร่งปราบเว็บหมิ่น. สืบค้นเมื่อ 20 กุมภาพันธ์ 2555, จาก http://www.manager.co.th/CyberBiz/ViewNews.aspx?NewsID=9540000103856

_____. (2554, สิงหาคม 23). อนุดิษฐ์ลั่น 5 นโยบาย กระทรวงไอซีที. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://www.manager.co.th/cyberbiz/ViewNews.aspx?NewsID=9540000106190

_____. (2554, ตุลาคม 10). อนุดิษฐ์ รับสิ้นปี wifi ฟรี 2 หมื่นจุด. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9540000128730

_____. (2555, มีนาคม 14). ตร.พอใจผลปราบเว็บหมิ่นสถาบัน-ชี้ 4 เดือนปิดแล้ว 5 พันยูอาร์เอล. สืบค้นเมื่อ 10 มิถุนายน 2555, จาก http://www.manager.co.th/Crime/ViewNews.aspx?NewsID=9550000033137

bact. (2552, มกราคม 21). แบบสำรวจ “สิทธิเสรีภาพในอินเทอร์เน็ต” – An Online Survey on Internet Rights and Freedom. สืบค้นเมื่อ 22 ธันวาคม 2554, จาก http://bact.cc/2009/internet-freedom-survey/

candy strawberry milk (2553, มกราคม 22). Thai No Sniff - ความตื่นตัวเรื่องสิทธิของ netizen ไทย. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://my.dek-d.com/sweetsin/blog/?blog_id=10050555

Darknews. (2552, พฤศจิกายน). พ.ร.บ.คอมพิวเตอร์ฯ – เครื่องมือการเมือง. *OK Natoin Blog*. สืบค้นเมื่อ 17 ธันวาคม 2554, จาก http://www.oknation.net/blog/print.php?id=520872

DJ. อ้น ประชาชื่น (วิทยุชุมชนคนแท็กซี่). (2552, พฤศจิกายน 11). สถานการณ์การใช้อำนาจรัฐกรณี พ.ร.บ. คอมพิวเตอร์ อีกเกมหนึ่งของอำมาตย์ เกมกำจัดคู่แข่งการเมือง. *ประชาไท*. สืบค้นเมื่อ 3 ธันวาคม 2554, จาก http://www.prachatai3.info/journal/2009/11/26541

iLaw. (2553, กรกฎาคม 23). นายกสมาคมสื่อแนะ ยื่นพ.ร.บ.คอมพิวเตอร์ให้ศาล ร.ธ.น.ตีความ. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://ilaw.or.th/node/433

_____. (2554, พฤษภาคม 5). อัด ร่างพ.ร.บ.คอมฯใหม่ "ซักซี้ด-ห่วยขั้นเทพ" มั่วเรื่องลิขสิทธิ์. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://ilaw.or.th/node/921

_____. (2554, ตุลาคม 14). รอบอาทิตย์ที่สอง ต.ค. 54: UN ย้ำไทยต้องแก้กฎหมายหมิ่นพ.ร.บ.คอม. สืบค้นเมื่อ 19 มกราคม 2555, จาก http://ilaw.or.th/node/1225

_____. (2555, เมษายน 20). ติดดาบดีเอสไอ. เพิ่ม 9 คดีพิเศษ ตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ. สืบค้นเมื่อ 20 เมษายน 2555, จาก http://ilaw.or.th/node/1465

_____. (ม.ป.ป.). Case # 116: คดีปิดเว็บประชาไท. สืบค้นเมื่อ 7 พฤษภาคม 2555, จาก http://freedom.ilaw.or.th/th/case/116

lew. (2553, มกราคม 26). ไอซีทียอมแพ้, เลิกแนวคิดใช้ sniffer. Blognone. สืบค้นเมื่อ 25 ธันวาคม 2554, จาก http://www.blognone.com/node/14785

MThai. (2554, มิถุนายน 30). เตือน ! ห้ามหาเสียงออนไลน์ทั้งทวิตเตอร์ โพสต์เฟส คืนหมาหอน. สืบค้นเมื่อ 12 มกราคม 2555, จาก http://news.mthai.com/politics-news/120492.html

_____. (2554, พฤศจิกายน 25). รมว.ไอซีที เตือนประชาชน อย่ากด Like Comment เว็บหมิ่นสถาบันฯ. สืบค้นเมื่อ 15 มกราคม 2555, จาก http://news.mthai.com/general-news/142656.html

_____. (2554, พฤศจิกายน 26). ประชาธิปัตย์ แนะแบน ยูทูบ-เฟซบุ๊ก แบบจีนสกัด เว็บหมิ่นฯ. สืบค้นเมื่อ 8 กุมภาพันธ์ 2555, จาก http://news.mthai.com/headline-news/142706.html

newswit. (2552, กันยายน 15). รมว.ไอซีที แถลงความคืบหน้าผลงานกระทรวงไอซีที. สืบค้นเมื่อ 15 กันยายน 2554, จาก http://www.newswit.com/gen/2009-09-15/4eda0e4334ccee57a7e26008d6635d23

SchoolNet. (2555, กุมภาพันธ์ 28). ไอพีวี 6 จุดเปลี่ยนโลกออนไลน์. สืบค้นเมื่อ 30 เมษายน 2555, จาก http://www.school.net.th/schoolnet/news/news_read.php?news_id=2945

Siam Intelligence Unit. (2552, มีนาคม 27). ถก พรบ.คอมพิวเตอร์ ยังขัดแย้ง มุมมองจากรัฐและภาคประชาชน. สืบค้นเมื่อ 23 ธันวาคม 2554, จาก http://www.siamintelligence.com/computer-crime-act-tja-discussion/

_____. (2552, เมษายน 21). เครือข่ายพลเมืองเน็ตค้านปิดเว็บไซต์ จี้ยุติ พรก. ฉุกเฉิน. สืบค้นเมื่อ 20 ธันวาคม 2554, จาก http://www.siamintelligence.com/thai-netizen-network-on-the-political-crisis-and-information-censorship/

ThaiLawtoday. (2552, กันยายน 7). กฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการอย่างอื่นในสำนักงานตำรวจแห่งชาติ พ.ศ.2552. สืบค้นเมื่อ 30

มิถุนายน 2555, จาก http://www.thailawtoday.com/laws-commentaries/1202--2552.html

สิ่งพิมพ์ภาษาอังกฤษ

Banks, William C., et al, Executive Authority for National Security Surveillance, *50 Am. U.L. Rev.* 1 (2000)

Bellia, Patricia L. et al. (2004). *Cyberlaw: Problems of Policy and Jurisprudence in the Information Age.* 2nd ed. MN: Thomson West.

Cannici Jr., William J. The Global Online Freedom Act: A Critique of Its Objectives, Methods, and Ultimate Effectiveness Combating American Business That Facilitate Internet Censorship in the People Republic of China. *32 Seton Hall Legis. J.* 123 (2007)

Charles Li. Internet Content Control in China. *8 Int'l J. Comm. L. & Pol'y. 1* (Winter 2003/2004)

Colbridge, Thomas D.. Electronic Surveillance: A Matter of Necessity. *The FBI Law Enforcement Bulletin.* 25 (1 February 2000)

Daily, Elizbeth Gillingham. Comment: Beyond "Persons, Houses, Papers, and Effects": Rewriting the Fourth Amendment for National Security Surveillance. *10 Lewis & Clark L. Rev.* 641 (2006)

Dickerson, Nicholas P.. The Thirteenth Annual Frankel Lecture: Comment: What Makes the Internet So Special? And Why, Where, How, And By Whom Should Its Content Be Regulated? *46 Hous. L. Rev*. 61, 101 (2009)

E.E.B., et al. Plugging the Leak: The Case for A Legislative Resolution of the Conflict Between The Demands of Secrecy and The Need for an Open Government. *71 Va. L. Rev*. 802 (1985)

E. John Park. Protecting the Core Values of the First Amendment in an Age of New Technologies: Scientific Expression vs. National Security. *2 Va. J.L. & Tech*. 3 (1997)

Emanuel, Steven L. (2003). *Constitutional Law.* New York: Aspen Publishers.

Guobin Yang. (2009). *The Power of the Internet in China: Citizen Activism Online*. New York: Columbia University Press.

Jacques, Stephen C., Comment: Reno v. ACLU : Insulating The Internet, The First Amendment, and The Marketplace of Ideas, *46 Am. U.L. Rev*. 1945 (1997)

Jennifer Shyu. Speak No Evil: Circumventing Chinese Censorship. *45 San Diego L.*

Rev. 211 (Winter, 2008)

Kamali, Mohammad Hashim. (2000). *Freedom of Expression in Islam*. Malaysia: Ilmiah Publishers Sdn Bhd.

Lyon, David, and Elia Zureik, (ed.). (1996). *Computers, Surveillance, and Privacy.* Minneapolis: University of Minnesota Press.

Mayer, Ann Elizabeth. (1999). *Islam and Human Rights: Tradition and Politics.* Boulder, Colo.: Westview Press.

Ray, Diana.. Big Brother Is Watching You (Electronic Surveillance). *Insight on the News* (23 July 2001). 1–3.

Reed, Kristina M.. From The Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce. *13 Transnat'l Law*. 451 (2000)

Rotunda, Ronald D. (2007). *Modern Constitutional Law: Case and Notes*. 8th ed. MN: Thomson West.

Schindler, Devin S.. Between Safety and Transparency : Prior Restraints, FOIA, and the Power of the Executive. *38 Hastings Const. L.Q.* 1 (2010)

Seidenberg, Steven. Breaking China: WTO complaint could end the "Great Firewall" Internet ban. *96 A.B.A.J.* 20 (November, 2010)

Simmons, Charles E.. Fundamental Rights: United States Foreign Policy v. The Press and the American Information Consumer : The Embattled First Amendment. *1987 How. L. J.* 849 (1987)

Sinrod, Eric J., et al, Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace, 1999 Stand. *Tech. L. Rev*. 1 (1999)

Stevenson, Christopher. Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World. *30 B.C. Int'l & Comp. L. Rev*. 531 (Spring, 2007)

Sullivan, Kathleen M. et al. (2001). *Constitutional Law*. 14th ed. NY: Foundation Press.

Viner, Nellie L.. The Global Online Freedom Act: Can U.S. Internet Companies Scale the Great Chinese Firewall at the Gates of the Chinese Century? *93 Iowa L. Rev.* 361 (November, 2007)

Weeramantry, Christopher. (2001). *Islamic Jurisprudence: An International Perspective*. Malaysia: The Other Press.

Winstein, Keith J.. China Blocks MIT Web Addresses. *The Tech*, 22 November 2002, Volume 122, Number 58.

Yutian Ling. Upholding Free Speech and Privacy Online: A Legal-Based and

Market-Based Approach for Internet Companies in China. *27 Santa Clara Computer & High Tech. L. J.* 175 (February, 2011)

ข้อมูลอิเล็กทรอนิกส์ภาษาอังกฤษ

Ahlert, Christian, Chris Marsden and Chester Yung. (n.d.). How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation. Retrieved June 10, 2011, from http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf

American Civil Liberties Union. (1997, June 27). State by State Internet Censorship Bills. Retrieved July 21, 2011 from http://www.aclu.org/technology-and-liberty/state-state-internet-censorship-bills

Amnesty International. (n.d.). Imprisoned for Peaceful Expression. Retrieved July 12, 2012, from http://www.amnestyusa.org/our-work/cases/china-shi-tao

Ansfield, Jonathan. (2010, April 16). China Starts New Bureau to Curb Web. *The New York Times.* Retrieved July 21, 2011, from http://www.nytimes.com/2010/04/17/world/asia/17chinaweb.html

Answers.com. (n.d.). Electronic Surveillance. Retrieved July 21, 2011 from http://www.answers.com/topic/electronic-surveillance-3

Asisnews. (2009, February 7). Public protest in Beijing against internet censorship. Retrieved July 21,2011, from http://www.asianews.it/news-en/Public-protest-in-Beijing-against-internet-censorship-15677.html

BBC. (2008, November 7). Malaysia blogger's joy at release. Retrieved June 3, 2012, from http://news.bbc.co.uk/2/hi/asia-pacific/7714696.stm

BRANDENBURG v. OHIO (SUPREME COURT OF THE UNITED STATES 395 U.S. 444 June 9, 1969), Retrieved March 13, 2012, from http://law2.umkc.edu/faculty/projects/ftrials/conlaw/brandenburg.html

Business-in-Asia. (n.d.). The Internet in China. Retrieved 2011, June 19, from http://www.business-in-asia.com/internet_report.html

cijmy. (2010, September 25). The Sedition Act 1948. *Centre for Independent Journalism*. Retrieved June 3, 2012, from http://cijmalaysia.org/miniportal/2010/09/the-sedition-act-1948/

Clara Chooi. (2011, April 24). Najib repeats promise of no Internet censorship. *The Malaysian insider*. Retrieved June 3, 2012, from http://www.themalaysianinsider.com/malaysia/article/najib-repeats-promise-of-no-internet-censor

ship/

Computer Crime and Intellectual Property Section, Criminal Division, DoJ (2009). Searching and Seizing Computer and Obtaining Electronic Evidence in Criminal Investigations. Retrieved March 12, 2012, from http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

Congressional-Executive Commission on China. (2006, September 20). Congressional – Executive Commission on China Annual Report 2009. Retrieved July 7, 2010, from http://www.cecc.gov/pages/annualRpt/annualRpt06/CECCannRpt2006.pdf

_____. (2009, October 10). Congressional – Executive Commission on China Annual Report 2009. Retrieved July 20, 2011, from http://www.cecc.gov/pages/annualRpt/annualRpt09/CECCannRpt2009.pdf

_____. (2010, February 26). Beijing High People's Court Affirms Liu Xiaobo's 11-Year Sentence. Retrieved October 10, 2010, from http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle-136147

_____. (n.d.). Agencies Responsible for Censorship in China. Retrieved July 7, 2010, from http://www.cecc.gov/pages/virtualAcad/exp/expcensors.php

_____. (n.d.). Blocking, Filtering, and Monitoring. Retrieved July 7, 2010, from http://www.cecc.gov/pages/virtualAcad/exp/expjamming.php

_____. (n.d.). Congressional-Executive Commission on China 2006 Annual Report, Monitoring Compliance with Human Rights. Retrieved July 7, 2010, from http://www.cecc.gov/pages/annualRpt/annualRpt06/Expression.php?PHPSEESID=767f...

_____. (n.d.). Domestic Laws and Regulations: Vague and Overbroad Regulations. Retrieved July 20, 2011, from http://www.cecc.gov/pages/virtualAcad/exp/explaws.php

_____. (n.d.). Measures for the Administration of Internet Information Services. Retrieved July 7, 2010, from http://www.cecc.gov/pages/virtualAcad/exp/explaws.php#internetmeasures

_____. (n.d.). Regulations on the Administration of Internet Access Service Business Establishments [Internet Cafes], Retrieved July 7, 2010, from http://www.cecc.gov/pages/virtualAcad/exp/explaws.php#internetcaferegs

Cornell University Law School. (2010, August 19). FIRST AMENDMENT: AN OVERVIEW. Retrieved January 18, 2012, from http://www.law.cornell.edu/wex/first_amendment

Council of Europe Treaty Office. (n.d.). Convention on Cybercrime CETS No.: 185. Retrieved March 3, 2010, from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

_____. (n.d.). Retrieved March 3, 2010, from http://conventions.coe.int/

Cybertelecom. (n.d.). Cybertelecom: Federal Internet Law and Policy. Retrieved March 13, 2012, from http://www.cybertelecom.org

Editorial. (2010, July 1). Google vs. China, the Sequel. *The New York Times.* Retrieved July 21,2011, from http://www.nytimes.com/2010/07/02/opinion/02fri3.html?_r=1&ref=internet_censorship

Electronic Frontier Foundation. (n.d.). EFF Analysis Of The Provisions Of The USA PATRIOT Act. Retrieved August 1, 2012, from https://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php

Federal Trade Commission. (n.d.). spam. Retrieved July 21, 2011 from www.ftc.gov/spam

Foerstel, Herbert, et al. (2003). The USA Patriot Act: Uncensored. Retrieved June 10, 2011, from: http://www.thirdworldtraveler.com/Civil_Liberties/USA PatriotAct_Uncensored.html

Freedom house. (n.d.). Google Applauded for Stance on China Internet Censorship. Retrieved July 21,2011, from http://www.freedomhouse.org/article/google-applauded-stance-china-internet-censorship

Free Encyclopedia of Ecommerce. (n.d.). National Information Infrastructure Protection Act (NIIPA) of 1996. Retrieved March 12, 2012, from http://ecommerce.hostip.info/pages/769/National-Information-Infrastructure-Protection-Act-NIIPA-1996.html

French, Howard W. (2008, February 4). Chinese begin to protest censorship of Internet. *The New York Times.* Retrieved July 21, 2011, from http://www.nytimes.com/2008/02/04/world/asia/04iht-wall.1.9716090.html

Gan, Steven. (2001, April 29). Ending the government's monopoly on the truth. *The guardian*. Retrieved March 21, 2012, from http://www.guardian.co.uk/technology/2001/apr/29/freespeech.observercampaignpressfreedom

Hardial Singh Khaira. (2009, March 18). Is it the I.S.A. per se or the Interpretations Given by the Judiciary that makes it Such a Draconian Law Now? Retrieved June 3, 2012, from http://www.scribd.com/doc/13365695/Internal-Security-Act-the-Judiciary

Hooker, Jake. (2008, July 11). Voice seeking answers for parents about school collapse in China is silenced. *The New York Times*. Retrieved July 12, 2012, from http://www.nytimes.com/2008/07/11/world/asia/11iht-11china.14412092.html?_r=1

IFEX. (2012, January 19). IFEX member websites go dark in protest against online piracy bills. Retrieved August 1, 2012, from http://www.ifex.org/international/2012/01/19/sopa_pipa_protests/

iLaw. (n.d.). Case # 116: Prachatai Blocked. Retrieved May 7, 2012, from http://freedom.ilaw.or.th/case/116

Jacobs, Andrew. (2010, July 30). China Imprisons 3 Men Who Maintained Uighur Web Sites. *The New York Times*. Retrieved August 21, 2012, from http://www.nytimes.com/2010/07/31/world/asia/31china.html

Kan, Michael. (2012, June 15). Protests, Not Criticism, the Target for China's Internet Censors, Study Says. *PCWorld.* Retrieved August 15, 2012, from http://www.pcworld.com/businesscenter/article/257707/protests_not_criticism_the_target_for_chinas_internet_censors_study_says.html

Kelly, Sanja & Sarah Cook. [Eds.]. (2011, April 18). Freedom on the Net 2011: A Global Assessment of Internet and Digital Media. Retrieved June 30, 2012, from http://www.freedomhouse.org/sites/default/files/FOTN2011.pdf

Kent, Jonathan. (2003, May 29). Malaysia's censorship strangles growth. *BBC*. Retrieved June 5, 2012, from http://news.bbc.co.uk/2/hi/business/2947264.stm

Letter from Mark Lemley, Professor, Standford Law School, et al. to Sen. Judiciary Comm (2011, June 27), Retrieved January 18, 2012, from http://volokh.com/2011/07/04/amd-speaking-of-the-inalienable-right-to-pursuit-of-happiness

Los Angeles Chinese Leaning Center. (n.d.). Internet Censorship in China. Retrieved July 7, 2010, from http://chinese-school.netfirms.com/Internet-censorship.html

Mackinnon, Rebecca. (2011, November 15). Firewall law could infringe free speech. *The New York Times*. Retrieved January 18, 2012, from http://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html

Madsen, Wayne. (2005, December 9). Internet Censorship, Retrieved March 12, 2012, from http://www.rense.com/general69/intercens.htm

Malaysiakini. (2009, September 4). MCMC tells Malaysiakini: Take down videos.

Retrieved June 8, 2012, from http://www.malaysiakini.com/news/112111

Malaysiana1. (2008, August.). Tun Dr Ismail - The Man Who Saved Malaysia. Retrieved June 12, 2012, from http://malaysiana1.blogspot.com/2008/08/tun-dr-ismail-man-who-saved-malaysia.html

MarkJ. (2011, April 18). UPDATE Freedom House Warns UK Internet Users at Risk of Growing Censorship. Retrieved June 6, 2012, from http://www.ispreview.co.uk/story/2011/04/18/freedom-house-warns-uk-internet-users-at-risk-of-growing-censorship.html

Martin, Jessica. (2012, January 17). SOPA, Protect IP will stifle creativity and diminish free speech. Retrieved January 18, 2012, from http://news.wustl.edu/news/pages/23260.aspx

Masurlaw. (n.d.). Summary of SOPA PIPA. Retrieved January 18, 2012, from http://www.masurlaw.com/resources/summary-of-sopa-and-pipa/

M. Kumar, Wong Pek Mei, and Jo Timbuong. (2011, June 11). No more free downloads as MCMC blocks 10 file sharing sites. *The star online*. Retrieved June 5, 2012, from http://thestar.com.my/news/story.asp?file=/2011/6/11/nation/8879884&sec=nation

New Straits Times. (2007, January 2). Ismail's struggle to form Malaysia and Asean. cited in accessmylibrary. Retrieved June 12, 2012, from http://www.accessmylibrary.com/article-1G1-156712021/ismail-struggle-form-malaysia.html

Nitirassadorn: Law for the People. (2011, December 26). Proposed amendments to the law on defamation of the King, the Queen, the Heir-apparent and the Regent (Section 112 of the Criminal Code)" Retrieved January 7, 2012, from http://www.enlightened-jurists.com/download/68

Nurbaiti Hamdan and Cheok Li Peng. (2008, August 28). ISPs ordered to cut access to Malaysia Today website. *The star online*. Retrieved June 7, 2012, from http://thestar.com.my/news/story.asp?file=/2008/8/28/nation/22187596&sec=nation

OpenNet. (n.d.). Malaysia. Retrieved March 20, 2012, from http://opennet.net/research/profiles/malaysia

O'Reilly, Tim. (2005, September 30). What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. Retrieved March 3, 2012, from http://oreilly.com/web2/archive/what-is-web-20.html

Patrick Di Justo. (2003, March 18). Does the End Justify the Means? Retrieved July 7, 2010, from http://www.wired.com/politics/law/news/2003/03/58082

Reporters Without Borders. (2003, May 12). Living Dangerously on the Net. Retrieved July 20, 2011, http://en.rsf.org/china-living-dangerously-on-the-net-12-05-2003,06793.html

_____. (n.d.). Press Freedom Index 2009. Retrieved March 13, 2012, from http://en.rsf.org/press-freedom-index-2009,1001.html

_____. (n.d.). Press Freedom Index 2010. Retrieved July 20,2011, from http://en.rsf.org/press-freedom-index-2010,1034.html

Reuters. (2011, June 17). Hackers strike Malaysian websites for a second day. Retrieved June 10, 2012, from http://www.reuters.com/article/2011/06/17/us-malaysia-hackers-idUSTRE75G1OE20110617

Road to Independence. (n.d.). Retrieved June 12, 2012, from http://countrystudies.us/singapore/10.htm

Sophie Beach. (2009, May 6). Joshua Rosenzweig: China's Battle Over the Right to Criticize. *China Digital Time*. Retrieved July 20, 2011, from http://chinadigitaltimes.net/2009/05/joshua-rosenzweig-chinas-battle-over-the-right-to-criticize/

Stone, Brad and David Barboza. (2010, July 29). Google to Stop Redirecting China Users. *The New York Times*. Retrieved July 21, 2011, from http://www.nytimes.com/2010/06/30/technology/30google.html?ref=internet_censorship

Thai Netizen Network. (2011, June 2). Proposals for Legal Reform for Laws Concerning Freedom of Expression. Retrieved January 19, 2012, from https://thainetizen.org/2011/06/proposal-for-legal-reform-for-laws-concerning-freedom-of-expression/

Thai Netizen Network and Reporters Without Borders. (2010, April 27). Joint statement on the further censorship of websites and media under Emergency Decree. *Reporters Without Borders*. Retrieved December 20, 2011, from http://en.rsf.org/thailand-thai-netizen-network-s-statement-27-04-2010,37164.html

The Communications and Multimedia Content Forum of Malaysia. (2004, September 1). The Malaysian Communications And Multimedia Content Code. Retrieved March 20, 2012, from http://www.cmcf.my/download/cmcf-content-code-english.pdf

_____. (n.d.). Retrieved March 20 2012, from http://www.cmcf.my/home.php

The Malaysian insider. (2010, August 16). New survey revives spectre of Malaysian - Green Dam. Retrieved June 5, 2012, from http://www.themalaysianinsider.

com/malaysia/article/new-survey-revives-spectre-of-malaysian-green-dam/

The Nobel Peace Prize 2010. (n.d.). Retrieved October 10, 2010, from http://www.nobelprize.org/nobel_peace_prizes/laureates/2010/press.html

The star online. (2009, April 12). Time to repeal the ISA. Retrieved June 12, 2012, from http://thestar.com.my/news/story.asp?file=/2009/4/12/focus/3658721&sec=focus

Vpn Accounts. (n.d.). Malaysian Internet Censorship - Bypass it! Retrieved June 7, 2012, from http://www.vpnaccounts.com/malaysian-internet-censorship.html

Wikipedia, the free encyclopedia. (n.d.). Internet in the People's Republic of China. Retrieved July 20, 2011, from http://en.wikipedia.org/wiki/Internet_in_the_People's_Republic_of_China

_____. (n.d.). Protest against SOPA and PIPA. Retrieved August 1, 2012, from http://en.wikipedia.org/wiki/Protests_against_SOPA_and_PIPA

Wine, Michael, Sharon LaFraniere and Jonathan Ansfield. (2010, April 7). China's Censors Tackle and Trip Over the Internet. *The New York Times*. Retrieved July 21, 2011, from http://www.nytimes.com/2010/04/08/world/asia/08censor.html

Wong, Edward. (2010, May 14). After Long Ban, Western China Is Back Online. *The New York Times*. Retrieved May 14, 2010, from http://www.nytimes.com/2010/05/15/world/asia/15china.html

Wong, Edward and David Barboza. (2011, January 31). Wary of Egypt Unrest, China Censors Web. *The New York Times*. Retrieved July 20, 2011, from http://www.nytimes.com/2011/02/01/world/asia/01beijing.html?_r=0

Zittrain, Jonathan and Benjamin Edelman. (n.d.). Documentation of Internet Filtering Worldwide, Retrieved July 7, 2010, from http://cyber.law.harvard.edu/filtering/

สิ่งพิมพ์ภาษาเยอรมัน

Achenbach, Hans. Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität. *NJW* 1986, p.1835ff

Bethge, Herbert, Grundgesetz, Kommentar, Art. 5, in: Sachs, Michael (Hrsg.), Rn. 54, 88.

Bullinger, Martin. Strukturwandel von Rundfunk und Presse : Rechtliche Folgewirkungen der neuen elektronische Medien. *NJW,* 1984, p. 385.

Clemens, Thomas, Grundgesetz Art. 5, in: Umbach, Dieter C./Clemens, Thomas (Hrsg.), Rn. 69a-b.

Derksen, Roland. Perspektiven für eine wirksame Bekämpfung von Rechtsradikalismus und Rassismus im Internet. *ZFIS* 1999, p.150.

Fromm, Rainer and Barbara Kernbach. (2001). *Rechtsextremismus im Internet: die neue Gefahr*. München: Olzog.

Hoffmann - Riem, Grundgesetz Art. 5, in: Alternativkommentar zum GG (AK-GG), Rn. 138, 145.

Klaus, Tiedeman. Die Bekämpfung der. Wirtschaftskriminalität durch den Gesetzgeber. *JZ* 1986, p. 865 ff.

Ladeu, Karl-Heinz. Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet. (*ZUM*, 1997), p. 373.

Schreibauer, Marcus. (2000). “Strafrechtliche Verantwortlichkeit für Delikte im Internet”. In *Handbuch zum Internetrecht: Electronic Commerce - Informations-, Kommunikations- und Mediendienste*. Detlef Kröger and Marc A. Gimmy (eds.).Berlin: Springer-Verlag.

Sieber, Ulrich and Malaika Nolde. (2008). *Sperrverfügungen im Internet: Nationale Rechtsdurchsetzung im globalen Cyberspace?* Berlin: Duncker & Humblot.

Stadler, Thomas. (2002). *Haftung für Information im Internet.* Berlin: Schmidt

Strömer, Tobias H. (1997). *Online-Recht: Rechtsfragen im internetund in Mail boxnetzen.* Heidelberg: dpunkt, Verl.

ข้อมูลอิเล็กทรอนิกส์ภาษาเยอรมัน

Arbeitskreis gegen Internet-Sperren und Zensur (AK Zensur). (n.d.) Retrieved December 16, 2011, from http://ak-zensur.de/

Beuth, Patrick. (2009, June 18). Das Gesicht des Internets. *Frankfurter Rundschau.* Retrieved December 14, 2011, from http://www.fr-online.de/datenschutz/franziska-heine-das-gesicht-des-internets,1472644,2706570.html

Bleich, Holger and Axel Kossel. (n.d.). Verschleierungstaktik Die Argumente für Kinderporno-Sperren laufen ins Leere. *Heise online*. Retrieved July 3, 2011, from http://www.heise.de/ct/artikel/Verschleierungstaktik-291986.html

Borchers, Detlef. (2007, July 25). Online-Durchsuchung: Ist die Festplatte eine Wohnung? *Heise online.* Retrieved August 12, 2011, from http://www.heise.de/newsticker/meldung/Online-Durchsuchung-Ist-die-Festplatte-eine-

Wohnung-155439.html

Boulevard Baden. (2011, September 25). Nils Schmid verteidigt Kunstfreiheit auch bei Mohammed-Karikaturen. Retrieved July 20, 2011, from http://www.boulevard-baden.de/lokales/nachrichten/2011/09/25/nils-schmid-verteidigt-kunstfreiheit-auch-bei-mohammed-karikaturen-podiumsdiskussion-anlasslich-60-jahrfeier-des-bundesverfassungsgerichts-426953/

Chaos Computer Club. (n.d.). Retrieved December 14, 2011, from http://www.ccc.de/de/home

Das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG. (2007, June 27). Retrieved March 5, 2011, from http://dip.bundestag.de/btd/16/058/1605846.pdf

Das Verhältnismäßigkeitsprinzip. (n.d.). Retrieved July 25, 2011, from www.jur-dinn.de/Studi-Ecke/Verhaeltnism.pdf

Decker, Oliver and Elmar Brähler. (2006). Vom Rand zur Mitte: Rechtsextreme Einstellung und ihre Einfl ussfaktoren in Deutschland. Retrieved November 8, 2010, from http://www.fes.de/rechtsextremismus/pdf/Vom_Rand_zur_Mitte.pdf

Ermert, Monika. (2007, April 18). Provider sollen mehr gegen Hass-Seiten in Internet tun. *Heise online*. Retrieved November 8, 2010, from http://www.heise.de/newsticker/meldung/Provider-sollen-mehr-gegen-Hass-Seiten-im-Internet-tun-168724.html

Fiutak, Martin. (2006, August 11). Deutsche Behörden wollen Zugang zu Bwin sper ren. *ZDNet*. Retrieved October 17, 2011, from http://www.zdnet.de/news/39146183/deutsche-behoerden-wollen-zugang-zu-bwin-sperren.htm

Franz, Markus. (2010, April 22). Zensur im Netz: Ein Blick über den Tellerrand. *Netzwelt.* Retrieved September 18, 2011, from http://www.netzwelt.de/news/82506-zensur-netz-blick-ueber-tellerrand.html

German Working Group on Data Retention. (n.d.) Retrieved July 15, 2011, from http://www.vorratsdatenspeicherung.de/component/option,com_frontpage/Itemid,1/lang,en/

GERMANY CENSORS DUTCH WEBSITE WWW.XS4ALL.NL, WITH 3100 WEB PAGES. (n.d.) Retrieved September 18, 2011, from http://www.nadir.org/nadir/archiv/Medien/Zeitschriften/radikal/netzzensur/96090501.html

Heise online. (2011, October 15) Staatstrojaner: Bundesinnennminister verteidigt

den Einsatz und greift CCC an. Retrieved September 15, 2011, from http://www.heise.de/newsticker/meldung/Staatstrojaner-Bundesinnenminister-verteidigt-den-Einsatz-und-greift-CCC-an-1361814.html

Helmers, Sabine. (1996, September 24). Hyperlink-Prozeß: Freispruch für Angela Marquardt. *Heise online*. Retrieved October 15, 2011, from http://www.heise.de/tp/artikel/1/1236/1.html

Internet-Zensur in Deutschland. (n.d.). Retrieved October 15, 2011, from http://odem.org/informationsfreiheit/

MOGiS e.V. – Eine Stimme für Betroffene. (n.d.). Retrieved December 14, 2011, from http://mogis-verein.de/wer-wir-sind/impressum/

Moeller, Simon (2009, April 24). Netsaperren: Der neue Entwurf und siene Rechts maessigkeit. *Telemedicus*. Retrieved September 15, 2011, from http://www.telemedicus.info/article/1271-Netzsperren-Der-neue-Entwurf-und-seine-Rechtsmaessigkeit.html

Offener Brief zur Gesetzesvorlage Internetsperren. (n.d.) Retrieved September 16, 2011, from http://www.trotzallem.de/Offener_Brief_Familienministerin.pdf

Petition: Internet - Keine Indizierung und Sperrung von Internetseiten vom 22.04.2009. (2009, April 22). Retrieved December 14, 2011, from https://epetitionen.bundestag.de/petitionen/_2009/_04/_22/Petition_3860.html

Sperrverfügung der Bezirksregierung Düsseldorf. (n.d.) Retrieved November 23, 2010, from http://odem.org/material/verfuegung/sperrungsverfuegung.pdf

Spiegel online. (2010, January 5). Kunstfreiheit gilt für Großköpfe und Klein hirne. Retrieved July 20, 2011, from: http://www.spiegel.de/kultur/gesellschaft/0,1518,670130,00.html

_____. (2010, March 2). Vorratsdatenspeicherung verstößt gegen Verfassung. Retrieved June 17, 2010, from http://www.spiegel.de/netzwelt/netzpolitik/0,1518,681122,00.html

_____. (2007, December 31). 30.000 klagen in Karlsruhe - größte Verfassungs-Beschwerde aller Zeiten. Retrieved August 6, 2011, from http://www.spiegel.de/netzwelt/web/0,1518,525970,00.html

_____. (n.d.). Amoklauf von Erfurt. Retrieved November 25, 2010, from http://www.spiegel.de/thema/amoklauf_erfurt/

Stern.de (2009, April 11). Stoppschild gegen Kinderpornos im Web. Retrieved August 15, 2011, from http://www.stern.de/digital/online/internetsperren-stoppschild-gegen-kinderpornos-im-web-661190.html

Urteil vom 2. März 2010 zu 1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08. (n.d.). Retrieved June 18, 2010, from http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

Urteil vom 27. Februar 2008 zu 1 BvR 370/07 und 1 BvR 595/07. (n.d.). Retrieved September 18, 2011, from http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html

Verfassungsbeschwerde Vorratsdatenspeicherung. (n.d.). Retrieved July, 11, 2011, from http://wiki.vorratsdatenspeicherung.de/images/Verfassungsbeschwerde_Vorratsdatenspeicherung.pdf

Wagner, Marita (2009, May 18). Straverfolgung oder Internetsperren? *Heise online.* Retrieved September 21, 2011, from http://www.heise.de/tp/artikel/30/30344/1.html

WinFuture. (2008, November 23). Online-Durchsuchung: 57% der Deutschen sind dafür. Retrieved September 15, 2011, from http://winfuture.de/news,43732.html

Wikipedia Die freie Enzyklopädie. (n.d.). Sozialdarwinismus. Retrieved November 6, 2010, from http://de.wikipedia.org/wiki/Sozialdarwinismus

Zeit online. (2011, May 25). Bundesregierung hebt Sperrgesetz gegen Kinderpornos auf. Retrieved August 3, 2011, from http://www.zeit.de/politik/deutschland/2011-05/streichung-kinderpornosperre

ZDF.de. (2007, September 14). Politbarometer: 65 Prozent für Online-Durchsuchung. Cited in *Internet Archive*. Retrieved September 15, 2011, from http://web.archive.org/web/20080102140653/http://www.zdf.de/ZDFde/inhalt/0/0,1872,7004800,00.html

ZugErschwG. (2009, July 11). Das Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz). Retrieved August 3, 2011, from http://www.zugerschwg.com/2009/07/zugangserschwerungsgesetz-volltext.html

Zur Zensur der Seiten von Angela Marquardt bei Compuserve. (1997, July 17). Retrieved October 12, 2011, from http://nadir.org/nadir/initiativ/r_ver/hinter/zensur/zensu08.htm

การจำกัดตัดทอนเสรีภาพในการรับรู้ข้อมูลข่าวสารและการแสดงความคิดเห็น จำเป็นต้องอยู่ภายใต้ขอบเขตของกฎหมายที่ยุติธรรม คือ ต้องชัดเจน ไม่ครอบคลุมเครือได้สัดส่วน พอสมควรแก่เหตุ มีวิธีดำเนินการที่โปร่งใส และมีกลไกให้ประชาชนตรวจสอบการใช้อำนาจโดยรัฐได้

หากรัฐสามารถทำได้ตามเงื่อนไขต่างๆ ที่กล่าวมา ดุลยภาพระหว่างการป้องกันและปราบปรามการกระทำผิดกับการคุ้มครองสิทธิและเสรีภาพของประชาชนก็ย่อมเป็นสิ่งที่เกิดขึ้นได้

Limits or restrictions to freedoms of information and expression must be within the confines of a just law. That is, the law must be clear, unambiguous, proportional, reasonable, transparent in its process, and accountable to the public

If the state can fulfill these conditions, a balance between the prevention and suppression of offences and the protection of the rights and liberties of the people may be achievable.

POLICE CRIME?

ISBN 978-616-91463-0-8

420 บาท

9 786169 146308

Cover Design: wrongdesign