รายงานการวิจัยฉบับสมบูรณ์

เรื่อง

โครงการวิจัยเพื่อพัฒนาข้อเสนอแนะในการส่งเสริมและคุ้มครองสิทธิมนุษยชน กรณีการดำเนินการด้านเทคโนโลยี (สิทธิดิจิทัล)

โดย

นายบัณฑิต หอมเกษ

สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

ได้รับทุนอุดหนุนการวิจัยจากกองทุนวิทยาศาสตร์ วิจัยและนวัตกรรม

ปีงบประมาณ พ.ศ. 2564

กันยายน 2565

กิตติกรรมประกาศ

งานวิจัยฉบับนี้ สำเร็จลงได้ด้วยความกรุณาและความช่วยเหลืออย่างดียิ่งจากกรรมการสิทธิมนุษยชนแห่งชาติ ผู้บริหารสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ ผู้อำนวยการสำนักกิจการคณะกรรมการสิทธิมนุษยชนแห่งชาติ ผู้อำนวยการกลุ่มงานวิจัยสิทธิมนุษยชน ตลอดจนเพื่อนร่วมงานในกลุ่มงานวิจัยสิทธิมนุษยชน เพื่อน ๆ พี่ ๆ น้อง ๆ ในสำนักกิจการคณะกรรมการสิทธิมนุษยชนแห่งชาติ และพี่ ๆ กลุ่มงานคลัง สำนักบริหารกลาง ซึ่งคอยให้แนะนำ ให้คำปรึกษา อำนวยความสะดวก และช่วยเหลือจนงานวิจัยชิ้นนี้สำเร็จลุล่วงออกมาได้

ผู้วิจัยขอบคุณสำนักงานคณะกรรมการวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.) ที่เห็นความสำคัญของงานวิจัยด้านสิทธิมนุษยชนและให้การสนับสนุนทุนในการทำวิจัยชิ้นนี้ และขอบคุณเป็นอย่างสูงสำหรับเจ้าหน้าที่ของ สกสว. ที่คอยให้คำแนะนำปรึกษาด้านเทคนิคการบริหารจัดการทุนด้วยดีเสมอมา

ที่ขาดไม่ได้ ผู้วิจัยขอขอบคุณเพื่อน ๆ พี่ ๆ น้อง ๆ นักปกป้องสิทธิมนุษยชน นักกิจกรรมทางสังคมในองค์กรต่าง ๆ ที่อนุเคราะห์ให้ข้อมูลต่าง ๆ ซึ่งเป็นประโยชน์อย่างยิ่งกับงานวิจัย

นอกจากนี้ ผู้วิจัยต้องขอขอบคุณตัวแทนหน่วยงานรัฐต่าง ๆ ที่เกี่ยวข้อง ที่สนใจเข้ามาร่วมให้ข้อมูลและความเห็นในการประชุมกลุ่มย่อยที่จัดขึ้น ซึ่งข้อมูลที่ทุกท่านให้มาเป็นประโยชน์อย่างยิ่งต่องานวิจัย

สุดท้ายนี้ ผู้วิจัยหวังเป็นอย่างยิ่งว่างานวิจัยชิ้นนี้จะเป็นประโยชน์ไม่มากก็น้อยต่องานด้านสิทธิมนุษยชนในสังคมไทย โดยเฉพาะในมิติที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล และหากมีข้อผิดพลาดใด ๆ ในงานวิจัยชิ้นนี้ ผู้วิจัยขอน้อมรับผิดแต่เพียงผู้เดียว หากท่านใดประสงค์ที่จะให้ข้อเสนอแนะหรือให้ข้อมูลเพิ่มเติม โปรดติดต่อผู้วิจัยได้ที่ bandit.nhrc@gmail.com

บัณฑิต หอมเกษ

นักวิจัย

ชื่อเรื่อง โครงการวิจัยเพื่อพัฒนาข้อเสนอแนะในการส่งเสริมและคุ้มครองสิทธิมนุษยชน กรณีการดำเนินการด้านเทคโนโลยี (สิทธิดิจิทัล)

ผู้วิจัย นายบัณฑิต หอมเกษ

หน่วยงาน สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

ปีที่ทำวิจัยเสร็จ 2565

บทคัดย่อ

งานวิจัยชิ้นนี้มุ่งศึกษากรอบบรรทัดฐานสิทธิมนุษยชนระหว่างประเทศและแนวปฏิบัติที่ดีสำหรับการส่งเสริมและคุ้มครองสิทธิมนุษยชนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์ (สิทธิดิจิทัล) และจัดทำข้อเสนอแนะสำหรับประเทศไทย โดยเน้นศึกษาเชิงลึกในประเด็นสิทธิในการเข้าถึงอินเทอร์เน็ต เสรีภาพในการแสดงออก และสิทธิในความเป็นส่วนตัว โดยใช้ระเบียบวิธีวิจัยเชิงคุณภาพ ประกอบด้วย การศึกษาเอกสาร การสัมภาษณ์เชิงลึก และการประชุมกลุ่มย่อย

ผลการวิจัยพบว่า กรอบสิทธิมนุษยชนที่ปรากฏในตราสารสิทธิมนุษยชนระหว่างประเทศที่มีอยู่นั้น ยังสามารถตีความเพื่อปรับใช้ในยุคดิจิทัลได้ ภายใต้หลักการที่ยอมรับในทางสากลว่าสิทธิมนุษยชนที่บังคับใช้ในทางออฟไลน์ ยังมีผลบังคับใช้ในทางออนไลน์ด้วย

เมื่อพิจารณาบริบทของประเทศไทย พบว่า กรอบรัฐธรรมนูญได้รับรองสิทธิมนุษยชนที่ค่อนข้างสอดคล้องกับตราสารสิทธิมนุษยชนระหว่างประเทศอยู่ ซึ่งสามารถนำมาปรับใช้ในทางออนไลน์หรือกับเทคโนโลยีได้ แต่อาจจะมีบางประเด็นที่จำเป็นต้องทำให้ชัดเจนขึ้น เช่น สิทธิในการเข้าถึงอินเทอร์เน็ต และสิทธิในการมีความคิดเห็นกับเสรีภาพในการแสดงออก เป็นต้น นอกจากนี้ การศึกษาเชิงลึกใน 3 ประเด็น พบว่า 1) สิทธิทางอินเทอร์เน็ต ยังไม่ได้ถูกรับรองว่าเป็นสิทธิมนุษยชนหรือสิทธิพลเมืองในรัฐธรรมนูญและกฎหมายไทย แต่ในทางปฏิบัติ ประเทศไทยได้มีการดำเนินการเพื่อให้ประชาชนสามารถเข้าถึงอินเทอร์เน็ตได้อย่างทั่วถึงผ่านกฎหมายและนโยบายต่าง ๆ ที่มีอยู่ 2) ประเด็นเสรีภาพในการแสดงออก โดยเน้นไปที่การจำกัดเนื้อหาทางออนไลน์นั้น พบว่า มีทั้งส่วนที่ก้าวหน้าในเรื่องของการพัฒนาหลักประกันเชิงกระบวนการสำหรับการปิดกั้นเนื้อหาทางออนไลน์ แต่ก็ยังมีส่วนข้อกังวลเกี่ยวกับการดำเนินคดีต่อการเผยแพร่เนื้อหาทางออนไลน์ โดยเฉพาะต่อการแสดงออกที่เป็นการวิพากษ์วิจารณ์รัฐบาลและสถาบันทางการเมือง โดยส่วนหนึ่งเป็นผลมาจากกฎหมายที่คลุมเครือ ตลอดจนอัตราโทษที่ไม่ได้สัดส่วน และ 3) สิทธิในความเป็นส่วนตัว โดยเน้นไปที่ประเด็นการสอดส่องโดยรัฐ พบว่า ยังมีช่องว่างของกรอบกฎหมายในการคุ้มครองสิทธิความเป็นส่วนตัวในมิติของการสอดส่อง และยังพบข้อท้าทายเกี่ยวกับการสอดส่องแบบลับ ซึ่งยากที่การตรวจสอบและเป็นอุปสรรคในการแสวงหาการเยียวยาของผู้ที่ได้รับผลกระทบ

งานวิจัยชิ้นนี้ จึงได้เสนอแนะให้มีการตรากฎหมายรับรองสิทธิในการเข้าถึงอินเทอร์เน็ต และทบทวนกฎหมายเกี่ยวกับการจำกัดเนื้อหา และการสอดส่อง ให้มีความชัดเจน แน่นอน คาดหมายได้ และสอดคล้องกับพันธกรณีด้านสิทธิมนุษยชนระหว่างประเทศ ตลอดจนมีกลไกตรวจสอบและเยียวยาผู้ได้รับผลกระทบจากการถูกละเมิดสิทธิดังกล่าวอย่างมีประสิทธิผล

คำสำคัญ สิทธิดิจิทัล, สิทธิทางอินเทอร์เน็ต, เสรีภาพในการแสดงออก, สิทธิความเป็นส่วนตัว, การสอดส่อง

Research Title The Research Project for Developing the Human Rights Promotion and Protection Recommendations, in Cases of the Operations with Technology

Researcher Mr. Bandit Homket

Institute Office of the National Human Rights Commission of Thailand

Year 2022

Abstract

This research aims to study on international human rights norms and proper practices for promoting and protecting human rights related to information technology and online communication, and make a recommendation for promoting and protecting human rights related to information technology and online communication in Thailand focusing on the issue of the rights to access the internet, freedom of expression and the rights to privacy by using qualitative research methodology consisting of document study, in-dept interview and focus group.

The result showed that the human rights framework that present in the existing human rights instrument, can also be interpreted for adapting in the digital age under the universally accepted principle that the human rights that enforced in the offline platform is also applicable in the online platform. Considering Thailand context, the constitutional framework has already recognized the human rights that are quite consistent with the international human rights instruments which can be applied in the online platform and technology, but there may be some issues that, if they are revised in the future, they will need to be clearer, especially the rights to express the opinions and freedom of expression.

Furthermore, an in-dept study in 3 issues found that 1) Internet rights have not been recognized to be human rights or civil rights in the Constitutional and Thai law, but in practice, Thailand implemented to provide people to access the internet equally through various laws and policies. 2) The issue of freedom of expression found to be a breakthrough in the development of guaranteed process for blocking online contents, but there are still concerns about the prosecution on online content distribution, especially on expressions that criticize the government and political institutions. This is partly due to ambiguous laws including

disproportionate penalties. And 3) Right to privacy focusing on state surveillance issues found that there are gaps in the legal framework about the privacy rights protection in the dimension of surveillance and it also faces the challenge about covert surveillance which is hard to investigate and seek remedy for those who are affected.

This research therefore suggests implementing a certified law on the rights to access the internet and review the law about content restriction and surveillance to be clear, certain, predictable, and consistent with the international human rights obligations as well as having effective monitoring systems and remedy mechanisms.

Keywords Digital rights, Internet rights, Freedom of expression, Right to Privacy, State Surveillance

สารบัญ

เรื่อง	หน้า
กิตติกรรมประกาศ	**ก**
บทคัดย่อ	**ข**
Abstract	**ง**
สารบัญ	**ฉ**
สารบัญตาราง	**ซ**
สารบัญรูปภาพ	**ฌ**
สารบัญแผนภูมิ	**ญ**
บทที่ 1 บทนำ	**1**
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการวิจัย	6
1.3 ขอบเขตและวิธีการวิจัย	6
1.4 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย	7
บทที่ 2 กรอบหลักการสิทธิมนุษยชนในยุคดิจิทัล	**9**
2.1 ส่วนนำ	9
2.2 กรอบสิทธิมนุษยชนระหว่างประเทศ	10
2.3 สิทธิมนุษยชนในยุคดิจิทัล	14
2.4 สรุปส่งท้าย	33
บทที่ 3 สิทธิทางอินเทอร์เน็ต	**35**
3.1 ส่วนนำ	35
3.2 โครงสร้างพื้นฐานของอินเทอร์เน็ต	36
3.3 การอภิบาล/การกำกับดูแลอินเทอร์เน็ตระดับโลก (Internet Governance)	41
3.4 กรอบแนวคิดสิทธิทางอินเทอร์เน็ต	46
3.5 สิทธิในการเข้าถึงอินเทอร์เน็ตในประเทศไทย	51
3.6 สรุปส่งท้าย	77

สารบัญ (ต่อ)

บทที่ 4 เสรีภาพในการแสดงออกกับการจำกัดเนื้อหาออนไลน์ **79**

4.1 ส่วนนำ 79

4.2 กรอบหลักการทั่วไปของเสรีภาพในการแสดงออก 80

4.3 เสรีภาพในการแสดงออกและการจำกัดเนื้อหาทางออนไลน์ 102

4.4 การจำกัดเนื้อหาทางอินเทอร์เน็ตในประเทศไทย 111

4.5 สรุปส่งท้าย 146

บทที่ 5 สิทธิในความเป็นส่วนตัว และการสอดส่องการสื่อสารทางดิจิทัลโดยรัฐ **149**

5.1 ส่วนนำ 149

5.2 กรอบหลักการสิทธิความเป็นส่วนตัว (Right to privacy) 150

5.3 สิทธิในความเป็นส่วนตัว และการสอดส่องการสื่อสารทางดิจิทัล 160

5.4 สิทธิในความเป็นส่วนตัวและการสอดส่องการสื่อสารทางดิจิทัลในประเทศไทย 175

5.5 สรุปส่งท้าย 189

บทที่ 6 บทสรุปและข้อเสนอแนะ **193**

บรรณานุกรม **207**

ภาคผนวก **227**

ภาคผนวก ก สรุปการประชุมกลุ่มย่อย 228

ประวัติผู้วิจัย **235**

สารบัญตาราง

หน้า

ตารางที่ 2.1 ภาพรวมเอกสารที่เกี่ยวกับสิทธิดิจิทัล จำแนกตามประเภทสิทธิ 19

ตารางที่ 3.1 ดัชนีชี้วัดความครอบคลุมของอินเทอร์เน็ตประเทศไทย ระหว่างปี 2561 – 2564 64

ตารางที่ 4.1 กรอบการประเมินตามเกณฑ์การทดสอบเกณฑ์หกส่วนจากแผนปฏิบัติการราบัต 91

ตารางที่ 4.2 ตัวอย่างประเภทของเนื้อหาที่ถูกจำกัดได้ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ 96

ตารางที่ 5.1 สรุปของเขตการใช้อำนาจสอดส่องตามกฎหมายฉบับต่าง ๆ ของประเทศไทย 186

สารบัญรูปภาพ

หน้า

ภาพที่ 3.1 โครงสร้างพื้นฐานของอินเทอร์เน็ต 35

ภาพที่ 3.2 แผนที่ Regional Internet Registries (RIRs) 37

ภาพที่ 3.3 ร้อยละของผู้ใช้อินเทอร์เน็ต จำแนกตามในเขตเทศบาลและนอกเขตเทศบาล และเพศ 67

ภาพที่ 3.4 ความเร็วในการเชื่อมต่ออินเทอร์เน็ตมือถือและประจำที่ในประเทศไทย สิงหาคม 2565 69

ภาพที่ 3.5 แผนที่ความพร้อมใช้งาน 5G ทั่วโลก 70

ภาพที่ 4.1 ปิรามิดวาจาสร้างความเกลียดชัง (The Hate Speech Pyramid) 90

สารบัญแผนภูมิ

หน้า

แผนภูมิที่ 3.1 ร้อยละของประชาชนที่ใช้อินเทอร์เน็ต จำแนกตามอายุและเพศ 68

แผนภูมิที่ 3.2 ราคาบรอดแบนด์ประจำที่ และบรอดแบนด์มือถือของไทย ระหว่างปี 2556 – 2565 71

แผนภูมิที่ 3.3 การครองส่วนแบ่งตลาดอินเทอร์เน็ตในประเทศไทย ปี 2564 73

แผนภูมิที่ 4.1 อันดับ Freedom on Internet ประเทศไทย ระหว่างปี 2559 – 2564 113

แผนภูมิที่ 4.2 การแจ้งเว็บไซต์และคำสั่งศาลในการปิดกั้น 123

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในโลกยุคปัจจุบัน เป็นโลกที่เทคโนโลยีใหม่ ๆ เกิดขึ้นและเปลี่ยนแปลงอย่างรวดเร็วและไม่หยุดยั้ง และส่วนใหญ่เป็นเทคโนโลยีที่ขับเคลื่อนด้วยข้อมูล ส่งผลให้เกิดการแปลงข้อมูลในโลกจริงไปเป็นข้อมูลดิจิทัล (Datafication) มากขึ้น[1] โดยเป็นดำเนินการภายใต้กระบวนการที่เป็นวงจรหมุนวน คือ การที่ทำให้ข้อมูลจากโลกจริงไหลไปสู่โลกอินเทอร์เน็ตแล้วย้อนกลับสู่โลกจริงอีกครั้ง (physical-digital-physical loop) ซึ่งมีลักษณะเฉพาะ 3 ขั้นตอน ดังนี้[2]

(1) การแปลวัตถุในโลกจริงเป็นดิจิทัล (Datafication) ผ่านการใช้อินเทอร์เน็ต สมาร์ทโฟน อินเทอร์เน็ตของสรรพสิ่ง (IoT) โดรน (Drone) ไบโอเมตริกซ์ (Biometrics) และเทคโนโลยีที่สวมใส่ได้ต่าง ๆ

(2) การกระจายและถ่ายโอนข้อมูลดิจิทัล (Distribution) ภายในและระหว่างองค์กร และ/หรือการจัดเรียงข้อมูลใหม่ในรูปแบบใหม่ ซึ่งอาจใช้เทคโนโลยีหลายอย่าง เช่น คลาวด์คอมพิวติ้ง (Cloud Computing) บล็อกเชน (Blockchain) เทคโนโลยีโลกเสมือนผสานโลกจริง (Augmented Reality - AR) รวมถึงอินเทอร์เน็ตของสรรพสิ่ง

(3) การตัดสินใจ (Decision-making) เป็นการร่องรอยดิจิทัลเพื่อออกแบบนโยบายหรือการตัดสินใจที่มีผลกระทบต่อผู้คนในโลกแห่งความเป็นจริงผ่านการตัดสินใจโดยใช้อัลกอริทึม ระบบอัตโนมัติ

การเปลี่ยนแปลงของเทคโนโลยีดังกล่าวเป็นโอกาสในการพัฒนาเศรษฐกิจ สังคม และคุณภาพชีวิตของประชาชน ประชาชนสามารถเข้าถึงข้อมูลข่าวสารได้ง่ายขึ้น การใช้บริการต่าง ๆ ได้สะดวกขึ้น สำหรับงานด้านสิทธิมนุษยชนเองก็มีการนำเทคโนโลยีดิจิทัลมาใช้เช่นกัน อาทิ การใช้ข้อมูลขนาดใหญ่ (Big Data) และปัญญาประดิษฐ์ (Artificial Intelligence : AI) เพื่อเพิ่มประสิทธิภาพในการสืบสวนสอบสวนการละเมิดสิทธิมนุษยชน การรวบรวมข้อมูลเพื่อเฝ้าระวังและประเมินสถานการณ์สิทธิมนุษยชน เป็นต้น[3] แต่ในอีกด้านหนึ่ง การเปลี่ยนแปลงทางเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็ว ได้ทำให้เกิดช่องว่างในการละเมิดสิทธิมนุษยชน เกิดความเหลื่อมล้ำระหว่างคนที่มีโอกาสและทรัพยากรต่างกัน ทำให้กลุ่มคนบางส่วนที่ไม่เท่าทันเทคโนโลยีตกเป็นเหยื่อหรือถูกละเมิดผ่านเทคโนโลยีเหล่านั้น

ความกังวลเกี่ยวกับเทคโนโลยีต่อมิติสิทธิมนุษยชนสะท้อนผ่านสุนทรพจน์ของนายอันโตนิโอ กูเตอร์เรส (Mr. António Guterres) เลขาธิการองค์การสหประชาชาติ (UN) ต่อที่ประชุมคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ เมื่อวันที่ 24 กุมภาพันธ์ 2563 ตอนหนึ่งว่า เทคโนโลยีใหม่ ๆ กลับถูกนำมาใช้

---

[1] A/HRC/47/52, 19 May 2021, para 5 - 8

[2] A/HRC/47/52, 19 May 2021, para 6.

[3] The Human Rights, Big Data and Technology Project , https://www.hrbdt.ac.uk/

มากจนเกินไปเพื่อละเมิดสิทธิมนุษยชน ผ่านการเฝ้าระวัง การกดขี่ การคุกคาม และความเกลียดชังในโลกออนไลน์ เครื่องมือเหล่านี้ยังถูกใช้โดยผู้ก่อการร้ายและขบวนการค้ามนุษย์ และเข้าเน้นย้ำด้วยว่าความก้าวหน้าต่าง ๆ เช่น ซอฟต์แวร์จดจำใบหน้า หุ่นยนต์ การระบุตัวตนทางดิจิทัล และเทคโนโลยีชีวภาพ จะต้องไม่ถูกนำมาใช้เพื่อลิดรอนสิทธิมนุษยชน ทำให้รอยร้าวแห่งความไม่เท่าเทียม และการเลือกปฏิบัติที่มีอยู่เลวร้ายยิ่งขึ้น[4]

ในปี 2562 คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ (United Nations Human Rights Council) ได้ขอให้คณะกรรมการที่ปรึกษา (Human Rights Council Advisory Committee)[5] จัดทำรายงานผลกระทบ โอกาส และความท้าทายของเทคโนโลยีใหม่เกี่ยวกับการส่งเสริมและคุ้มครองสิทธิมนุษยชน ซึ่งคณะกรรมการที่ปรึกษาได้เสนอรายงานเมื่อเดือนพฤษภาคม 2564 ระบุว่า เทคโนโลยีใหม่มีศักยภาพที่ดีในการสนับสนุนการใช้สิทธิและเสรีภาพของบุคคล แต่ขณะเดียวกันก็ก่อให้เกิดความท้าทายต่อการส่งเสริมและคุ้มครองสิทธิมนุษยชน โดยสรุปดังนี้[6]

ในศักยภาพที่ดีในการสนับสนุนการใช้สิทธิและเสรีภาพของบุคคลนั้น รายงานระบุว่า พลังในการสื่อสารที่เพิ่มขึ้นได้ขยายศักยภาพในการสื่อสารและแบ่งปันความคิดไปทั่วโลกอย่างมีนัยสำคัญ ซึ่งมีส่วนทำให้เกิดการตระหนักและการใช้สิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน รวมถึงเสรีภาพในการแสดงออก และช่วยอำนวยความสะดวกในการชุมนุมและการสมาคม และเทคโนโลยีใหม่สามารถเสริมพลังให้กับบุคคล โดยการเพิ่มศักยภาพโดยตรงในโลกจริง ตัวอย่างที่ชัดเจนคือ ในช่วงการระบาดของ COVID-19 หากไม่มีเทคโนโลยีใหม่ การสร้างสมดุลระหว่างการรักษาระยะห่างทางสังคมและการรักษากิจกรรมทางเศรษฐกิจและสังคม ก็ย่อมเป็นไปได้ยาก นอกจากนี้ เทคโนโลยีช่วยทำให้บริการสาธารณะมีประสิทธิภาพมากขึ้น ถูกขึ้น และมีส่วนร่วมมากขึ้น ส่งเสริมการเป็นพลเมืองประชาธิปไตย และช่วยให้กระบวนการตัดสินใจที่โปร่งใสและเป็นประชาธิปไตย เทคโนโลยีใหม่ยังช่วยให้การสนับสนุนการส่งเสริมและการคุ้มครองสิทธิมนุษยชน เช่น ภาพถ่ายดาวเทียมทำให้สามารถบันทึกการละเมิดสิทธิมนุษยชนได้ สำนักงานข้าหลวงใหญ่ผู้ลี้ภัยแห่งสหประชาชาติได้พัฒนาระบบการจัดการข้อมูลประจำตัวแบบไบโอเมตริกใหม่สำหรับการขึ้นทะเบียนและปกป้องผู้คนที่ดีขึ้น ยืนยันตัวตนและกำหนดเป้าหมายความช่วยเหลือ เทคโนโลยีใหม่ยังมีศักยภาพที่จะพัฒนาความเท่าเทียมทางเพศ เช่น การเพิ่มการเข้าถึงการศึกษาของผู้หญิงผ่านบทเรียนอิเล็กทรอนิกส์ (e-Learning) เป็นต้น

ขณะเดียวกันในมิติของความท้าทายที่เกี่ยวข้องกับการละเมิดสิทธิมนุษยชนที่อาจเกิดขึ้นจากการใช้เทคโนโลยีใหม่ รายงานชิ้นเดียวกันระบุประเด็นความท้าทาย ดังนี้

- การแปลงข้อมูลในโลกจริงไปสู่โลกดิจิทัล (Datafication) ที่มากเกินไป ย่อมส่งผลให้ผู้คนสูญเสียความเป็นส่วนตัว จากการเกิดผลิตภัณฑ์และบริการที่ปรับให้เข้ากับ

[4] United Nation Thailand, https://thailand.un.org/index.php/en/88045-remarks-secretary-general-un-human-rights-council-highest-aspiration-call-action-human-rights

[5] Human Rights Council Resolution 41/11 of 11 July 2019

[6] A/HRC/47/52, 19 May 2021

ลักษณะเฉพาะและความชอบของบุคคล ทำให้เกิดการรวบรวมและเข้าถึงข้อมูลส่วนบุคคลอย่างไม่เคยปรากฏมาก่อน และในหลายกรณี การรวบรวมข้อมูลดังกล่าวเกิดขึ้นโดยปราศจากการรับรู้ของบุคคลที่เกี่ยวข้องอย่างเต็มที่ เพราะมักใช้อัลกอริทึม (Algorithm) การประมวลผลข้อมูลที่ปิดทึบและยากแก่การเข้าใจ

- การรักษาความปลอดภัยทางไซเบอร์ที่ไม่ดี อาจนำไปสู่การละเมิดสิทธิในความเป็นส่วนตัวอย่างรุนแรง เช่น การแฮ็กบ้านอัจฉริยะและอุปกรณ์สวมใส่ รวมถึงอุปกรณ์อัจฉริยะอื่น ๆ อาจสร้างความเสี่ยงใหม่ๆ รวมถึงการเปิดเผยตัวตนของบุคคล ทำให้เสี่ยงต่อการลักทรัพย์และอาชญากรรมอื่น ๆ
- อินเทอร์เน็ตได้เปลี่ยนวิธีการผลิตและสัมผัสเนื้อหาสื่ออย่างลึกซึ้ง ผู้คนได้รับข้อมูลข่าวสารทางออนไลน์เป็นส่วนใหญ่ จึงมีความท้าทายมากขึ้นในการประเมินความถูกต้องของข้อมูล เช่น เป็นเรื่องยากมากขึ้นในการแยกแยกความจริงและของปลอมจากการใช้เทคโนโลยี "deep fakes" ยิ่งกว่านั้น ยังมีความกังวลเกี่ยวกับการเผยแพร่ข้อมูลเท็จหรือข่าวปลอมโดยตัวแทนรัฐและเอกชนเพื่อต่อต้านฝ่ายตรงข้ามบนอินเทอร์เน็ต
- การทำให้รุนแรงขึ้น (Radicalization) การแบ่งแยก และการเลือกปฏิบัติ เทคโนโลยีใหม่โดยเฉพาะสื่อดิจิทัลและสื่อสังคมออนไลน์ทำให้วาจาสร้างความเกลียดชังแพร่กระจายอย่างรวดเร็ว ส่งผลให้มีความรุนแรงยิ่งขึ้น และยังมีคำถามต่อเทคโนโลยีปัญญาประดิษฐ์และการตัดสินใจโดยอัตโนมัติ โดยเฉพาะการตัดสินใจโดยใช้อัลกอริทึมเชิงคาดการณ์ในหน่วยงานบังคับใช้กฎหมายและตุลาการ และระบบการจ้างงาน ที่มีแนวโน้มสูงที่จะส่งผลให้เกิดการเลือกปฏิบัติเนื่องจากมีอคติในตัวต่อชนกลุ่มน้อยและกลุ่มเสี่ยง
- การลดทอนอำนาจ (Disempowerment) และความไม่เท่าเทียม (inequality) เนื่องจากอินเทอร์เน็ตกลายเป็นวิธีการหลักในการสื่อสารและเข้าถึงข้อมูลในปัจจุบัน ประชากรกลุ่มเปราะบางที่ขาดการเข้าถึงทางดิจิทัลจึงมีความเสี่ยงที่จะถูกละเมิดสิทธิมนุษยชนมากขึ้น การเสริมอำนาจจากเทคโนโลยีมีแนวโน้มว่าจะดำเนินไปอย่างไม่เท่าเทียม สร้างความเหลื่อมล้ำ และช่องโหว่รูปแบบใหม่ รวมถึงมีแนวโน้มที่จะมีผลกระทบทางสังคมและเศรษฐกิจที่แตกต่างกันระหว่างผู้หญิงและผู้ชาย ในแง่เศรษฐกิจ งานบางส่วนอาจถูกแทนที่ด้วยระบบอัตโนมัติ และผู้ปฏิบัติงานในอุตสาหกรรมเทคโนโลยีใหม่อาจไม่ได้รับการคุ้มครองจากกฎหมายแรงงานแบบเดิม
- การสอดส่องในวงกว้าง (Mass surveillance) ซึ่งเกี่ยวข้องกับการเฝ้าติดตามแบบไม่เลือกประชากร เทคโนโลยีใหม่เพิ่มศักยภาพในการสอดส่องให้กับรัฐบาล บ่อยครั้งไม่มี

การป้องกันที่เหมาะสม ซึ่งกระทบต่อความเป็นส่วนตัวของผู้บริสุทธิ์อย่างไม่ได้สัดส่วน และเป็นอันตรายต่อบรรทัดฐานประชาธิปไตย นอกจากนี้ พื้นที่ดิจิทัลยังใช้เพื่อจำกัดสิทธิเสรีภาพในการแสดงออก การเข้าถึงข้อมูล และเสรีภาพในการชุมนุมอย่างสันติอีกด้วย รัฐบาลจำกัดสิทธิโดยปิดบริการอินเทอร์เน็ตหรือเลือกบล็อกการเข้าถึงแหล่งข้อมูลออนไลน์ เซ็นเซอร์สื่อต่าง ๆ และข่มเหงผู้คนที่แสดงความคิดเห็นทางออนไลน์ รวมถึงการใช้อินเทอร์เน็ตคุกคามต่อนักปกป้องสิทธิมนุษยชน

- ความรุนแรงทางไซเบอร์ (Cyberviolence) เทคโนโลยีใหม่ ได้สร้างความท้าทายเกี่ยวกับอาชญากรรม เช่น การแสวงหาประโยชน์ทางเพศ การล่วงละเมิดทางเพศ และการแจกจ่ายรูปภาพส่วนตัวโดยไม่ได้รับความยินยอม การละเมิดลิขสิทธิ์ การกรรโชกทางการเงิน การล่วงละเมิดและการกลั่นแกล้งบนอินเทอร์เน็ต และการเผยแพร่ภาพถ่ายและวิดีโอที่ถ่ายอย่างผิดกฎหมาย ซึ่งเทคโนโลยีใหม่ได้ขยายรูปแบบการล่วงละเมิดทางเพศบางรูปแบบ รวมถึงได้เพิ่มความถี่และความร้ายแรงของอาชญากรรมรูปแบบต่าง ๆ ด้วย

ในมิติสิทธิมนุษยชนระดับสากล คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ และกลไกพิเศษภายใต้คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ ซึ่งรวมถึงผู้รายงานพิเศษด้านการส่งเสริมและคุ้มครองสิทธิในเสรีภาพในการแสดงความคิดเห็นและการแสดงออก[7] ผู้รายงานพิเศษด้านสิทธิในความเป็นส่วนตัว[8] ผู้รายงานพิเศษว่าด้วยรูปแบบร่วมสมัยของการเหยียดเชื้อชาติ การเลือกปฏิบัติทางเชื้อชาติ ความหวาดกลัวชาวต่างชาติ และการเหยียดหยามที่เกี่ยวข้อง[9] ผู้รายงานพิเศษด้านความรุนแรงต่อสตรี สาเหตุและผลที่ตามมา[10] ผู้รายงานพิเศษด้านสิทธิในการศึกษา[11] ผู้รายงานพิเศษในการขายเด็ก การค้าประเวณีเด็กและภาพลามกอนาจารเด็ก[12] ผู้รายงานพิเศษด้านการส่งเสริมและคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานในขณะต่อต้านการก่อการร้าย[13] ผู้รายงานพิเศษด้านความยากจนและสิทธิมนุษยชน[14] และผู้เชี่ยวชาญอิสระด้านสิทธิมนุษยชนโดยผู้สูงวัย[15] ได้พยายามศึกษาและเสนอแนะเกี่ยวกับการจัดการกับเทคโนโลยีใหม่ตามแนวทางสิทธิมนุษยชน

ในระดับภูมิภาคอาเซียน การประชุมหารือของคณะกรรมาธิการระหว่างรัฐบาลอาเซียนว่าด้วยสิทธิมนุษยชน (AICHR) ว่าด้วยเสรีภาพในการแสดงความคิดเห็น การแสดงออก และข้อมูลข่าวสารใน

---

[7] A/74/486 ; A/73/348 ; A/HRC/38/35 ; A/HRC/35/22 ; A/HRC/32/38 ; A/HRC/29/32

[8] A/HRC/37/62 ; A/73/438 ; A/HRC/34/60

[9] A/HRC/38/52 ; A/HRC/38/53 ; A/73/305 ; A/73/312

[10] A/HRC/38/47 ; A/73/301

[11] A/HRC/32/37.

[12] A/HRC/28/56.

[13] A/69/397.

[14] A/74/493.

[15] A/HRC/36/48

อาเซียน (ข้อ 23 ของปฏิญญาสิทธิมนุษยชนอาเซียน) หรือ AICHR Consultation on Freedom of Opinion, Expression and Information in ASEAN (Article 23 of the ASEAN Human Rights Declaration – AHRD) ระหว่างวันที่ 8 - 10 ธันวาคม 2562 ณ เมือง Nusa Dua เกาะบาหลี สาธารณรัฐอินโดนีเซีย หัวข้อ “สิทธิมนุษยชนในยุคดิจิทัล” ได้ถูกหยิบยกหารือในการประชุมดังกล่าวด้วย โดยที่ประชุมให้ความสนใจกับดิจิทัลในฐานะเป็นพื้นที่ใหม่ที่มีความสำคัญ เพราะเป็นทั้งโอกาส และความท้าทายของประเด็นสิทธิมนุษยชน ซึ่งที่ประชุมได้อภิปรายเกี่ยวกับพัฒนาการของรูปแบบเกี่ยวกับการใช้ถ้อยคำที่แสดงความเกลียดชังที่ค่อย ๆ เพิ่มขึ้นในภูมิภาคและวิธีการในการบิดเบือนข้อมูลที่กำลังถูกนำมาใช้อย่างแพร่หลายมากยิ่งขึ้น

ประเทศไทย ให้ความสำคัญกับการใช้ประโยชน์จากเทคโนโลยีใหม่ในด้านเศรษฐกิจและสังคม โดยในช่วงที่ผ่านมาได้มีการจัดทำและแก้ปรับปรุงกฎหมายหลายฉบับเกี่ยวกับดิจิทัล รวมถึง พ.ร.บ. การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560 พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 พ.ร.บ. สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย พ.ศ. 2562 พ.ร.บ. การบริหารงานและให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นอกจากนี้ ในระดับนโยบาย ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 – 2580) ให้ความสำคัญกับการพัฒนาโครงสร้างพื้นฐานด้านดิจิทัล การนำระบบดิจิทัลมาใช้ในการบริการสาธารณะต่าง ๆ รวมถึงการกำหนดให้นำเทคโนโลยีข้อมูลขนาดใหญ่ (Big Data) ข้อมูลเปิด (Open data) ปัญญาประดิษฐ์ (AI) มาใช้ในการพัฒนาประเทศด้านต่าง ๆ ทั้งนี้ ปัจจุบัน นโยบายเฉพาะด้านดิจิทัลถูกกำหนดในนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 – 2580) ซึ่งเป็นกลไกที่เกิดขึ้นจาก พ.ร.บ. การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560

อย่างไรก็ดี ยังมีสถานการณ์ที่น่ากังวลด้านสิทธิมนุษยชนหลายประการที่เกี่ยวกับโลกดิจิทัลในประเทศไทย โดยเฉพาะการใช้สื่อสังคมออนไลน์เพื่อละเมิดสิทธิมนุษยชน รวมถึงสิทธิในความเป็นส่วนตัว (Privacy Rights) การกลั่นแกล้ง (Cyberbullying) การแสดงออกที่สร้างความเกลียดชัง (hate speech) รวมถึงการสร้างข่าวปลอม (Fake news) ภายใต้ข้อกังวลเหล่านี้ ทำให้รัฐพยายามเข้ามาสอดส่องและควบคุมพื้นที่โลกออนไลน์ ผ่านเครื่องมือทางกฎหมายต่าง ๆ โดยเฉพาะ พ.ร.บ. ว่าด้วยกระกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ซึ่งถูกนำมาใช้ปิดกั้นเว็บไซต์หรือลบเนื้อหาที่รัฐอ้างว่าละเมิดกฎหมาย รวมถึงการฟ้องร้องดำเนินคดีเอาผิดกับการเผยแพร่ "เนื้อหา" ที่ละเมิดกฎหมายบนโลกออนไลน์ ซึ่งการใช้อำนาจดังกล่าวของรัฐ บ่อยครั้งถูกมองว่าเป็นการใช้กฎหมายเพื่อจำกัดเสรีภาพการแสดงออกของประชาชน โดยเฉพาะผู้ที่วิพากษ์วิจารณ์สถาบันทางการเมืองและการทำงานของรัฐบาล[16] นอกจากนี้ ประเด็นการสอดแนมโดยรัฐ ถูกหยิบยกขึ้นมากล่าวถึงมากขึ้นในปัจจุบันหลังจากมีรายงานว่าโทรศัพท์ของนักการเมือง

[16] โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw), พ.ร.บ.คอมพิวเตอร์ฯ 2560: กฎหมายใหม่แต่ยังถูกใช้ปิดปากเหมือนเดิม เข้าถึง https://ilaw.or.th/node/4901

ฝ่ายค้าน นักกิจกรรมทางการเมือง นักวิชาการ และคนทำงานในภาคประชาสังคมจำนวนไม่น้อยกว่า 30 คน ถูกสอดแนมโดยสปายแวร์ที่ชื่อ “เพกาซัส (Pegasus)” ซึ่งผลิตโดยบริษัท NSO Group สัญชาติอิสราเอล[17]

ด้วยเหตุที่การเปลี่ยนแปลงทางเทคโนโลยีดิจิทัลนำมาซึ่งโอกาสและความท้าทายด้านสิทธิมนุษยชนดังกล่าวไปแล้ว ดังนั้น ในงานวิจัยชิ้นนี้ จึงสนใจที่จะศึกษากรอบหลักการสิทธิมนุษยชนที่บังคับใช้กับเทคโนโลยีดิจิทัล เพื่อเป็นฐานความรู้สำหรับใช้ในการวิเคราะห์และจัดทำข้อเสนอแนะตามหน้าที่และอำนาจของคณะกรรมการสิทธิมนุษยชนในประเด็นที่เกี่ยวข้องกับเทคโนโลยีและสิทธิมนุษยชน โดยงานชิ้นนี้จะให้ความสนใจเป็นพิเศษกับเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) และมุ่งเน้นศึกษาเชิงลึกใน 3 ประเด็นหลัก ได้แก่ สิทธิทางอินเทอร์เน็ตและความเหลื่อมล้ำทางดิจิทัล (Digital divide) เสรีภาพในการแสดงออกซึ่งเกี่ยวข้องกับการควบคุมเนื้อหาออนไลน์ และประเด็นสุดท้ายคือ สิทธิในความเป็นส่วนตัวในยุคดิจิทัล ซึ่งเน้นไปที่ประเด็นการสอดส่องโดยรัฐ

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษา รวบรวม สังเคราะห์และวิเคราะห์บรรทัดฐานด้านสิทธิมนุษยชนระหว่างประเทศและแนวปฏิบัติที่ดี (Best Practice) ในการส่งเสริมและคุ้มครองสิทธิมนุษยชนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์

2. เพื่อศึกษารวบรวม สังเคราะห์และวิเคราะห์สถานการณ์สิทธิมนุษยชนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์ โดยเน้นประเด็นสิทธิทางอินเทอร์เน็ต เสรีภาพในการแสดงออกและสิทธิในความเป็นส่วนตัว

3. เพื่อจัดทำข้อเสนอแนะเชิงกฎหมาย นโยบาย และมาตรการในการส่งเสริมและคุ้มครองสิทธิมนุษยชนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์ โดยเน้นประเด็นสิทธิทางอินเทอร์เน็ต เสรีภาพในการแสดงออก และสิทธิในความเป็นส่วนตัว

1.3 ขอบเขตและวิธีการวิจัย

<u>ขอบเขตการวิจัย</u>

การวิจัยชิ้นนี้มุ่งศึกษาประเด็นสิทธิมนุษยชนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์ โดยจะศึกษาภาพรวมเกี่ยวกับกรอบบรรทัดฐานด้านสิทธิมนุษยชนที่บังคับใช้ในพื้นที่ดิจิทัล ส่วนการศึกษาเชิงลึกของการปรับใช้กรอบบรรทัดฐานดังกล่าวในประเทศไทย จะมุ่งศึกษาในประเด็นที่เป็นข้อกังวลปัจจุบันเป็นหลัก ได้แก่ สิทธิในการเข้าถึงอินเทอร์เน็ต เสรีภาพในการแสดงออกทางออนไลน์ และสิทธิในความเป็นส่วนตัวในยุคดิจิทัล

[17] โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw),. ปรสิตติดโทรศัพท์ : การส่งเพกาซัสติดตามนักการเมืองก้าวหน้า-ก้าวไกล. 21 กรกฎาคม 2565. https://freedom.ilaw.or.th/node/1090

วิธีการวิจัย

การวิจัยชิ้นนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Methods) โดยการเก็บรวบรวมข้อมูลแบบผสมผสานทั้งการศึกษาเอกสาร การใช้กรณีศึกษา การสัมภาษณ์ รวมถึงการประชุมกลุ่ม ดังนี้

1. การศึกษาเอกสาร (Documentary Research) ซึ่งแบ่งเป็น 2 ส่วนหลัก คือ

1.1 การศึกษา รวมรวม สังเคราะห์และวิเคราะห์หลักการ มาตรฐานและแนวปฏิบัติด้านสิทธิมนุษยชนที่เกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์หรือดิจิทัล จะเน้นสืบค้นจากตราสารด้านสิทธิมนุษยชนระหว่างประเทศซึ่งมีผลผูกพัน โดยเฉพาะกติการะหว่างประเทศว้าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) และเอกสารเชิงหลักการ การตีความ ความเห็น หรือข้อเสนอแนะ ซึ่งไม่ได้มีผลผูกพันทางกฎหมาย แต่อาจถือว่าเป็นแนวปฏิบัติที่ดีของหน่วยงานต่าง ๆ ทั้งในระบบสหประชาชาติ อาทิ ความเห็นทั่วไป (General comments) ข้อสังเกตโดยสรุป (Concluding observations) ของคณะกรรมการประจำสนธิสัญญา (treaty bodies) รายงานของกลไกพิเศษภายของสหประชาชาติ และเอกสารของที่พัฒนาขึ้นหรือเป็นการริเริ่มของภาคเอกชนและองค์กรพัฒนาเอกชนระหว่างประเทศอื่น ๆ

1.2 การศึกษา รวบรวม สังเคราะห์ และวิเคราะห์ข้อมูลสถานการณ์สิทธิมนุษยชนกับเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์ในประเทศไทย จะเน้นศึกษากฎหมาย มาตรการ กลไกและแนวปฏิบัติ และรายงานของหน่วยงานต่าง ๆ ทั้งของภาครัฐและหน่วยงานนอกภาครัฐ ที่เกี่ยวกับการดำเนินการด้านเทคโนโลยีสารสนเทศและการสื่อสารทางออนไลน์

2. การสัมภาษณ์เชิงลึก (In depth interview) เป็นการสัมภาษณ์รายบุคคล โดยใช้วิธีการสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-Structured Interview) โดยเน้นสัมภาษณ์ภาคประชาชน/ประชาสังคม/องค์กรพัฒนาเอกชน/ภาควิชาการ ที่ได้รับผลกระทบหรือทำงานเกี่ยวข้องกับประเด็นสิทธิมนุษยชนกับเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์

3. การประชุมกลุ่มย่อย (Focus Group Discussion) เป็นการจัดประชุมแลกเปลี่ยนและรับฟังความคิดเห็นจากหน่วยงานภาครัฐที่เกี่ยวข้อง ทั้งหน่วยงานกำกับดูแล หน่วยงานบังคับใช้กฎหมาย และหน่วยงานตุลาการ

1.4 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1. องค์ความรู้เกี่ยวกับบรรทัดฐานด้านสิทธิมนุษยชนระหว่างประเทศและแนวปฏิบัติที่ดี (Best Practice) ในการส่งเสริมและคุ้มครองสิทธิมนุษยชนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์

2. ข้อเสนอแนะในการส่งเสริมและคุ้มครองสิทธิมนุษยชนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์ โดยเฉพาะใน 3 ประเด็นหลัก ได้แก่ สิทธิทางอินเทอร์เน็ต เสรีภาพในการแสดงออกและสิทธิในความเป็นส่วนตัว

บทที่ 2
กรอบหลักการสิทธิมนุษยชนในยุคดิจิทัล

ในบทนี้จะสำรวจกรอบคิดสิทธิมนุษยชนที่ใช้กับพื้นที่ดิจิทัลหรือออนไลน์ โดยศึกษาตราสารหลักด้านสิทธิมนุษยชน อาทิ กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและการเมือง (ICCPR) กติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคมและวัฒนธรรม ฯลฯ และตราสารหลักด้านสิทธิมนุษยชนระดับภูมิภาค ประกอบกับศึกษาคำอธิบายการปรับใช้หลักการต่าง ๆ จากความเห็นทั่วไป (General comment) ข้อมติของคณะมนตรีสิทธิมนุษยชนและสมัชชาใหญ่แห่งสหประชาชาติ รายงานของกระบวนการพิเศษของคณะมนตรีสิทธิมนุษยชน (Special Procedures of the Human Rights Council) รายงานของข้าหลวงใหญ่สิทธิมนุษยชนแห่งสหประชาชาติ (OHCHR) รวมถึงเอกสารหลักการหรือแนวปฏิบัติที่กำหนดขึ้นโดยองค์กรต่าง ๆ ทั้งภาครัฐบาล ภาคเอกชน องค์กรสิทธิมนุษยชน องค์กรพัฒนาเอกชน

2.1 ส่วนนำ

การเปลี่ยนแปลงทางเทคโนโลยีอย่างรวดเร็ว ทำให้เกิดการตั้งคำถามมากขึ้นเกี่ยวกับกรอบงานด้านสิทธิมนุษยชน โดยเฉพาะที่ปรากฏในตราสารหลัก เช่น ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights - UDHR) กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) กติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม (ICESCR) ยังสามารถปรับใช้กับการเปลี่ยนแปลงนี้ได้หรือไม่ ซึ่งข้อกังวลดังกล่าวได้กระตุ้นให้เกิดการหันกลับมาพิจารณากรอบคิดสิทธิมนุษยชนกับเทคโนโลยีใหม่มากขึ้น

รายงานของคณะกรรมการที่ปรึกษาของคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ (Human Rights Council Advisory Committee) ที่เสนอต่อคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติเมื่อเดือนพฤษภาคม 2564 ซึ่งได้เกี่ยวกับผลกระทบ โอกาส และความท้าทายที่เป็นไปได้ของเทคโนโลยีใหม่เกี่ยวกับการส่งเสริมและคุ้มครองสิทธิมนุษยชน ได้ระบุถึงช่องว่างของกรอบงานด้านสิทธิมนุษยชนในการจัดการกับเทคโนโลยีดิจิทัลใหม่หรืออุบัติใหม่ (New and emerging digital technologies) ไว้ 3 ประการ ดังนี้[18]

ประการแรก ช่องว่างทางแนวคิดเทคโนโลยีใหม่กำลังสร้างโลกที่แตกต่าง ซึ่งไม่สอดคล้องกับกระบวนทัศน์ดั้งเดิม ภาษาและสำนวนบางส่วนในเอกสารสิทธิมนุษยชนไม่สะท้อนแนวปฏิบัติของยุคดิจิทัล เพราะตราสารสิทธิมนุษยชนระหว่างประเทศส่วนใหญ่ถูกร่างขึ้นครั้งแรกสำหรับโลกออฟไลน์ และอาจไม่สะท้อนความเป็นจริงของยุคดิจิทัล ประกอบกับความสัมพันธ์ระหว่างเทคโนโลยีกับสิทธิมนุษยชนมีความ

[18] A/HRC/47/52, 19 May 2021, para 49 – 57.

ซับซ้อน ชุมชนทางเทคนิคมักขาดความเข้าใจสิทธิมนุษยชน ส่วนชุมชนสิทธิมนุษยชนก็มักไม่มีความเข้าใจในเทคโนโลยี

ประการที่สอง ช่องว่างในการปฏิบัติงาน มุ่งเน้นไปที่วิธีที่เทคโนโลยีใหม่ก่อให้เกิดความท้าทายในทางปฏิบัติสำหรับรัฐ องค์กรระหว่างประเทศ และสถาบันที่ต้องการปกป้องและส่งเสริมสิทธิมนุษยชน เมื่อความสามารถทางเทคนิคขยายตัว จำเป็นต้องปรับปรุงกฎหมายและกฎระเบียบที่เกี่ยวข้อง ซึ่งฉันทามติทางสังคมและการปรึกษาหารือจำเป็นต้องนำหน้าการตรากฎหมาย ช่องว่างในการปฏิบัติงานมักเกี่ยวข้องกับคำถามเกี่ยวกับธรรมาภิบาลระหว่างประเทศที่กว้างขึ้น เทคโนโลยีใหม่มีขอบเขตทั่วโลกและข้ามชาติ แต่ความพยายามด้านกฎระเบียบมักจะยังคงเป็นระดับชาติหรือระดับภูมิภาค เนื่องจากเทคโนโลยีใหม่ไม่ได้ขึ้นอยู่กับโครงสร้างทางกายภาพหรือสถานที่ตั้ง จึงเป็นเรื่องยากและมักจะเป็นไปไม่ได้ที่จะกำหนดขอบเขตของประเทศในไซเบอร์สเปซ ซึ่งสภาพดังกล่าว ส่งผลกระทบต่อการคุ้มครองที่เหมาะสมหรือการเยียวยาที่มีประสิทธิภาพต่อเหยื่อที่ถูกละเมิดในโลกดิจิทัล เพราะรัฐไม่สามารถควบคุมพื้นที่ไซเบอร์หรือควบคุมผู้กระทำความผิดได้เนื่องจากขาดเขตอำนาจศาล

ประการที่สาม ภาคเอกชนมีบทบาทเพิ่มมากขึ้นในยุคดิจิทัล เนื่องจากเทคโนโลยีใหม่จำนวนมากทำหน้าที่เป็นส่วนสำคัญของโมเดลทางธุรกิจ ทำให้เกิดความเสี่ยงต่อการละเมิดสิทธิมนุษยชน โดยเฉพาะสิทธิในความเป็นส่วนตัวและการคุ้มครองข้อมูล แม้ว่าจะมีความคืบหน้าในการพัฒนากรอบงานเพื่อให้การดำเนินการของภาคธุรกิจเป็นไปตามพันธกรณีด้านสิทธิมนุษยชน โดยเฉพาะการรับรองหลักการชี้แนะของสหประชาชาติว่าด้วยธุรกิจกับสิทธิมนุษยชน (United Nations Guiding Principles on Business and Human Rights: UNGPs) โดยคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติด้วยมติเอกฉันท์ เมื่อเดือนมิถุนายน 2554 แต่ก็ยังคงมีช่องว่างในการนำหลักการดังกล่าวไปปรับใช้ ความพยายามที่จะบูรณาการแนวทางสิทธิมนุษยชนเข้ากับการพัฒนาเทคโนโลยีอาจเผชิญการตอบโต้เมื่อความสามารถในการทำกำไรถูกคุกคาม

ที่ผ่านมา มีความพยายามของหลายองค์กรหรือหลายกลุ่ม/เครือข่ายทั้งในระบบสหประชาชาติ รัฐบาล ภาคเอกชน องค์กรภาคประชาสังคมต่าง ๆ ได้อภิปรายเกี่ยวกับประเด็นเหล่านี้ รวมถึงมีความพยายามในการพัฒนามาตรฐานหรือแนวปฏิบัติเกี่ยวกับสิทธิมนุษยชนกับเทคโนโลยีดิจิทัลขึ้นมาจำนวนมาก ดังนั้น ในบทนี้จึงต้องการที่จะรวบรวมและสังเคราะห์เอกสารเหล่านั้น เพื่อทำความเข้าใจสิทธิมนุษยชนที่บังคับใช้กับพื้นที่ดิจิทัลหรือออนไลน์

2.2 กรอบสิทธิมนุษยชนระหว่างประเทศ

แม้ว่าพัฒนาการของแนวคิดสิทธิมนุษยชนสามารถโยงไปถึงงานเขียนเชิงปรัชญาโบราณเกี่ยวกับกฎหมายธรรมชาติ และการต่อสู้ของผู้คนเพื่อเสรีภาพและความยุติธรรมในอดีต แต่กรอบหลักการสิทธิมนุษยชนสมัยใหม่มีจุดเริ่มต้นนับตั้งแต่การลงมติรับรองและประกาศใช้ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights หรือ UDHR) เมื่อวันที่ 10 ธันวาคม พ.ศ. 2491 โดยสมัชชาใหญ่

แห่งสหประชาชาติ ซึ่งประกอบด้วยสมาชิกประเทศต่าง ๆ รวมถึงประเทศไทย เพื่อเป็นหลักการสำคัญในการคุ้มครองสิทธิมนุษยชนและรักษาสันติภาพของประชาคมโลก จากนั้นได้มีการจัดทำสนธิสัญญาด้านสิทธิมนุษยชน โดยถือเป็นตราสารหลักด้านสิทธิมนุษยชนรวม 9 ฉบับ ได้แก่ กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) กติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคมและวัฒนธรรม (ICESCR) และอนุสัญญาอีก 7 ฉบับ ซึ่งกำหนดมาตรฐานที่มุ่งคุ้มครองสิทธิเฉพาะกลุ่มและเฉพาะประเด็น อาทิ ผู้หญิง เชื้อชาติ คนพิการ เด็ก แรงงานข้ามชาติ การป้องกันการทรมานและบังคับสูญหาย เป็นต้น[19]

2.2.1 หลักการทั่วไป

หลักการสิทธิมนุษยชนกำหนดมาตรฐานขั้นต่ำสำหรับคุ้มครองมนุษย์ทุกคนให้สามารถดำรงชีวิตอยู่ได้อย่างมีศักดิ์ศรี โดยมีหลักการพื้นฐานสำคัญ คือ[20]

- *เป็นสากล (Universal)* ซึ่งเรียกร้องให้หลักการสิทธิมนุษยชนถูกปรับใช้กับมนุษย์ทุกคนอย่างเท่าเทียมกัน โดยไม่ขึ้นกับพรมแดนประเทศ
- *เชื่อมโยงและสัมพันธ์กัน (Interdependent and Interrelated)* การทำให้สิทธิมนุษยชนอย่างใดอย่างหนึ่งดีขึ้น ย่อมอำนวยให้เกิดการส่งเสริมสิทธิมนุษยชนอื่นด้วย และการลิดรอนสิทธิอย่างใดอย่างหนึ่ง ย่อมส่งผลเสียต่อสิทธิมนุษยชนอื่นด้วยเช่นกัน และ
- *แบ่งแยกจากกันไม่ได้ (Indivisible)* สิทธิมนุษยชนทั้งหมดมีสถานะเท่าเทียมกัน ไม่สามารถแยกออกจากกันได้ ไม่มีสิทธิใดที่สำคัญกว่าสิทธิอื่น

นอกจากนี้ หลักการสิทธิมนุษยชนถือเป็นหลักการที่คุ้มครองมนุษย์ทุกคนตั้งแต่เกิด จึงถ่ายโอนแก่กันไม่ได้ ด้วยหลักการพื้นฐานดังกล่าว ทำให้สิทธิมนุษยชนมีผลบังคับใช้แล้ว แม้จะยังไม่มีการออกกฎหมายภายในประเทศรองรับก็ตาม ในแง่นี้สิทธิมนุษยชนจึงมีความหมายกว้างกว่า “สิทธิตามกฎหมาย” ที่จะมีผลบังคับได้จะต้องมีบทบัญญัติของกฎหมายรองรับเสียก่อน อย่างไรก็ดี เพื่อให้สิทธิมนุษยชนได้รับการเคารพและคุ้มครองจริงในทางปฏิบัติ ICCPR เรียกร้องให้แต่ละรัฐนำหลักการสิทธิมนุษยชนมาบัญญัติไว้เป็นส่วนหนึ่งของกฎหมายภายในประเทศ[21]

หลักการความเสมอภาคและปราศจากการเลือกปฏิบัติเป็นหัวใจของสิทธิมนุษยชน ดังที่ระบุไว้ในข้อ 1 ของ UDHR ข้อ 2 ของ ICCPR และข้อ 2 ของ ICESCR ซึ่งยืนยันว่ามนุษย์ทุกคนเกิดมาอย่างเสรีและ

---

[19] ได้แก่ 1. กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง 2. กติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคมและวัฒนธรรม 3. อนุสัญญาว่าด้วยการเลือกปฏิบัติต่อสตรีในทุกรูปแบบ 4. อนุสัญญาว่าด้วยสิทธิเด็ก 5. อนุสัญญาว่าด้วยการขจัดการเลือกประติบัติทางเชื้อชาติในทุกรูปแบบ 6. อนุสัญญาว่าด้วยการต่อต้านการทรมาน และการกระทำอื่นๆ ที่โหดร้าย ไร้มนุษยธรรม หรือที่ย่ำยีศักดิ์ศรี 7. อนุสัญญาว่าด้วยสิทธิผู้พิการ 8. อนุสัญญาระหว่างประเทศว่าด้วยการคุ้มครองบุคคลทุกคนจากการหายสาบสูญโดยถูกบังคับ และ 9. อนุสัญญาว่าด้วยการคุ้มครองสิทธิของแรงงานโยกย้ายถิ่นฐานและสมาชิกในครอบครัว โดยปัจจุบันประเทศไทยเข้าเป็นภาคีสนธิสัญญาทั้งสิ้น 7 ฉบับคือลำดับที่ 1 - 7 ส่วนอนุสัญญาข้อ 8 ได้ลงนามแล้ว แต่ยังไม่ได้ให้สัตยาบัน ส่วนอนุสัญญาข้อ 9 ยังไม่ได้ลงนามและให้สัตยาบัน

[20] UN General Assembly, Vienna Declaration and Programme of Action, A/CONF.157/23 (12 July 1993) para 5.

[21] ICCPR ข้อ 2 (2)

เท่าเทียมกันในศักดิ์ศรีและสิทธิ มนุษย์ทุกคนจึงมีสิทธิที่จะได้รับสิทธิทั้งหมดอย่างเท่าเทียมกัน โดยปราศจากการเลือกปฏิบัติใด ๆ บนฐานของเชื้อชาติ สีผิว เพศ ภาษา ศาสนา ความคิดเห็นทางการเมืองหรือความคิดเห็นอื่นใด ชาติหรือสังคมดั้งเดิม ทรัพย์สิน กำเนิดหรือสถานะอื่น โดยรสนิยมทางเพศ (sexual orientation) รวมอยู่ในขอบเขตนี้ด้วย[22]

ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ มีสิทธิบางประการที่ถือเป็นสิทธิ "สัมบูรณ์" ที่ไม่สามารถจำกัดหรือลิดรอนได้ แม้ในภาวะฉุกเฉินสาธารณะซึ่งคุกคามความอยู่รอดของชาติ อาทิ สิทธิที่จะไม่ถูกทรมาน เสรีภาพที่จะไม่ถูกบังคับให้เป็นทาส และสิทธิที่จะได้รับยอมรับตามกฎหมาย[23]

ส่วนสิทธิมนุษยชนที่ไม่ใช่สิทธิ "สัมบูรณ์" จะสามารถจำกัดได้ภายใต้เงื่อนไขที่กฎหมายระหว่างประเทศกำหนดไว้ อาทิ เสรีภาพในการแสดงออก ถือเป็นสิทธิที่อาจถูกจำกัดได้ แต่การจำกัดต้องอยู่ภายใต้เงื่อนไขของความชอบด้วยกฎหมาย (legality) ที่จำเป็น (necessity) เพื่อวัตถุประสงค์ที่ชอบธรรม (legitimate aim) ตามที่กำหนดไว้ ได้แก่ ความมั่นคงของชาติ (National security) ความสงบเรียบร้อยสาธารณะ (Public order) ศีลธรรมอันดีของประชาชน (Public morals) ความปลอดภัยสาธารณะ (Public safety) การสาธารณสุข (Public health) และการปกป้องสิทธิของบุคคลอื่น และต้องเป็นไปตามหลักความได้สัดส่วน (proportionality) อีกทั้งมาตรการใด ๆ ของรัฐในการจำกัดหรือลิดรอนสิทธิต้องไม่เป็นการเลือกปฏิบัติ[24]

2.2.2 พันธกรณีของรัฐด้านสิทธิมนุษยชน

โดยทั่วไปทุกองคาพยพในสังคม ไม่ว่าจะเป็นรัฐบาล ภาคธุรกิจ องค์กรภาคประชาสังคม และปัจเจกบุคคลล้วนมีส่วนรับผิดชอบในด้านสิทธิมนุษยชน แต่ในทางกฎหมายสิทธิมนุษยชนระหว่างประเทศรัฐถือเป็นผู้มีหน้าที่โดยตรงอย่างน้อย 3 ประการ ได้แก่ **พันธกรณีในการเคารพ (respect)** โดยรัฐต้องไม่ละเมิดสิทธิมนุษยชนเสียเอง **พันธกรณีในการคุ้มครอง (protect)** โดยรัฐต้องออกและบังคับใช้กฎหมายและดำเนินมาตรการต่าง ๆ เพื่อคุ้มครองบุคคลไม่ให้ถูกละเมิดสิทธิมนุษยชนโดยบุคคลอื่น รวมถึงจากภาคธุรกิจ[25] ตลอดจนการจัดให้มีการเยียวยาที่มีประสิทธิผลและเพียงพอสำหรับผู้ที่ถูกละเมิดสิทธิมนุษยชน ผ่านกลไกทาง

---

[22] A/67/357, para 34. อ้างถึง CCPR/C/KWT/CO/2, CCPR/C/TGO/CO/4, CCPR/C/JPN/CO/5, CCPR/C/JAM/CO/3, CCPR/C/USA/CO/3/Rev.1, CCPR/CO/78/SLV, CCPR/CO/81/NAM, CCPR/C/CO/IRN/CO/3, CCPR/C/MNG/CO/5, CCPR/C/MEX/CO/5, CCPR/C/MDA/CO/2, CCPR/C/ETH/CO/1, CCPR/C/CMR/CO/4, CCPR/CO/83/GRC, CCPR/C/POL/CO/6, CCPR/C/79/Add.119, CCPR/C/RUS/CO/6, CCPR/C/UZB/CO/3, CCPR/CO/82/POL, CCPR/CO/70/TTO and CCPR/C/CHL/CO/5.

[23] ICCPR ข้อ 4

[24] โปรดดู ICCPR ข้อ 4 และ 19 และ Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, E/CN.4/1985/4, Annex (1985) และ CCPR General comment No. 34

[25] โปรดดู หลักการชี้แนะของสหประชาชาติว่าด้วยธุรกิจและสิทธิมนุษยชน (UN Guiding Principles on Business and Human Rights (UNGPs)), pp. 3 – 10.

ตุลาการ การบริหาร นิติบัญญัติหรือการกำกับดูแลอื่น[26] ด้วย[27] และ**พันธกรณีในการเติมเต็ม (fulfill)** โดยการดำเนินการเชิงบวกเพื่ออำนวยความสะดวกในการเข้าถึงและใช้สิทธิมนุษยชน[28]

2.2.3 ความรับผิดชอบของภาคธุรกิจต่อสิทธิมนุษยชน

แม้ว่ากฎหมายสิทธิมนุษยชนระหว่างประเทศจะบังคับใช้โดยตรงกับรัฐ แต่ปัจจุบันมีการยอมรับมากขึ้นว่าผู้กระทำการที่ไม่ใช่รัฐ (non-state actors) รวมถึงภาคธุรกิจ มีหน้าที่ด้านสิทธิมนุษยชนเช่นกัน

หลักการชี้แนะของสหประชาชาติว่าด้วยธุรกิจและสิทธิมนุษยชน (UN Guiding Principles on Business and Human Rights : UNGPs) ที่ถูกรับรองโดยคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติเมื่อปี 2554 ถือเป็นเครื่องมือระหว่างประเทศฉบับแรกที่กล่าวถึงความรับผิดชอบของบริษัทในด้านสิทธิมนุษยชน และเป็นมาตรฐานสำหรับการป้องกันและจัดการกับความเสี่ยงของผลกระทบทางลบที่เชื่อมโยงกับกิจกรรมทางธุรกิจ[29] UNGPs กำหนดกรอบงานไว้ 3 เสาหลัก ได้แก่ 1) หน้าที่ของรัฐในการคุ้มครองบุคคลจากการถูกละเมิดสิทธิมนุษยชนโดยบริษัท 2) ความรับผิดชอบขององค์กรธุรกิจในการเคารพสิทธิมนุษยชน และ 3) การเข้าถึงการเยียวยาที่มีประสิทธิผลของผู้ที่ตกเป็นเหยื่อการละเมิด[30]

UNGPs วางกรอบหลักการให้ทุกบริษัท มีความรับผิดชอบในการเคารพสิทธิมนุษยชน ซึ่งรวมถึงความรับผิดชอบในการก่อให้เกิดหรือมีส่วนทำให้เกิดผลกระทบด้านลบต่อสิทธิมนุษยชนผ่านกิจกรรมของตน และใช้มาตรการที่เพียงพอเพื่อป้องกัน ลดผลกระทบ หรือเยียวยาผลกระทบดังกล่าว รวมถึงการจัดให้มีนโยบายและกระบวนการตรวจสอบสิทธิมนุษยชนอย่างรอบด้าน (Human Rights Due Diligence : HRDD) เพื่อระบุ ป้องกัน ลดผลกระทบด้านสิทธิมนุษยชน รวมถึงการประเมินผลกระทบด้านสิทธิมนุษยชนที่เกิดขึ้นจริงและที่อาจเกิดขึ้น[31]

ในกรณีที่องค์กรธุรกิจระบุว่าตนได้ก่อให้เกิดหรือมีส่วนทำให้เกิดผลกระทบด้านลบต่อสิทธิมนุษยชน องค์กรควรจัดให้มีหรือให้ความร่วมมือในการแก้ไขผ่านกระบวนการที่ถูกต้องตามกฎหมาย[32] โดยการสร้างกลไกการร้องทุกข์เพื่อให้สามารถจัดการข้อร้องทุกข์ได้ตั้งแต่ต้น และกลไกการร้องทุกข์ที่ไม่เกี่ยวข้องกับการพิจารณาคดีทั้งที่เป็นของรัฐและไม่ใช่รัฐ ควรมีลักษณะชอบธรรม (legitimate) สามารถ

---

[26] UNGPs, pp. 27 – 35.

[27] ICCPR ข้อ 2 และ ICESCR ข้อ 2 และ UNGPs, pp. 27 – 35.

[28] UN General Assembly, Vienna Declaration and Programme of Action A/CONF.157/23, 12 July 1993

[29] Human Rights Council Resolution 17/4, A/HRC/RES/17/4, 6 July 2011.

[30] OHCHR, UN Guiding Principles on Business and Human Rights,
https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf

[31] UNGPs, pp. 13 – 18.

[32] UNGPs, pp. 22

เข้าถึงได้ (accessible) คาดหมายได้ (predictable) และเสมอภาค ตลอดจนสร้างความมั่นใจว่าผลลัพธ์และการเยียวยาสอดคล้องกับสิทธิมนุษยชนที่เป็นที่ยอมรับในระดับสากล[33]

2.3 สิทธิมนุษยชนในยุคดิจิทัล

2.3.1 เกริ่นนำ

ประเด็นสิทธิมนุษยชนกับเทคโนโลยีใหม่ หรือสิทธิมนุษยชนในยุคดิจิทัล หรือในยุคอินเทอร์เน็ตนั้น ได้รับการอภิปรายอย่างกว้างขวางทั้งในระดับนานาชาติ ระดับภูมิภาค และระดับชาติ และทั้งโดยกลไกในระบบสหประชาชาติ องค์กรเอกชน องค์ภาคประชาสังคม รวมถึงรัฐบาลหลายประเทศ ซึ่งพยายามที่จะกำหนดกรอบสิทธิมนุษยชนในยุคดิจิทัลหรืออินเทอร์เน็ต และหลายครั้งนำไปสู่การพัฒนาเป็นเอกสารที่เรียกชื่อต่าง ๆ ทั้งกฎบัตร (Charter) ปฏิญญา (Declaration) หลักการ (Principle) คำแนะนำ (Recommendation) ตลอดจนแถลงการณ์ (Statement) และเชื่อเรียกอื่นที่หลากหลาย โดยทั่วไปแล้วสิ่งเหล่านี้จะได้รับการพัฒนาภายในองค์กรระหว่างประเทศหรือกลุ่มผู้มีส่วนได้ส่วนเสียหลายฝ่าย เนื้อหาของเอกสารเหล่านี้มีความหลากหลายอย่างมาก ตั้งแต่การอธิบายหลักการพื้นฐานอย่างละเอียดเฉพาะเรื่อง เช่น หลักการกำกับดูแลอินเทอร์เน็ต (Internet governance principles) ของสภายุโรป (Council of Europe) ไปจนถึงเอกสารที่ให้รายละเอียดที่ครอบคลุมสิทธิมนุษยชนหลากหลายประเด็น เช่น กฎบัตรสิทธิมนุษยชนและหลักการสำหรับอินเทอร์เน็ต (The Charter of Human Rights and Principles for the Internet) ของ The Internet Rights and Principles Dynamic Coalition หรือกฎบัตรสิทธิอินเทอร์เน็ต (APC Internet Rights Charter) โดย Association for Progressive Communications (APC) เป็นต้น ซึ่งจะกล่าวถึงรายละเอียดต่อไป

แต่ก่อนจะกล่าวถึงสิทธิมนุษยชนในยุคดิจิทัล จำเป็นต้องเข้าใจก่อนว่าโลกดิจิทัลเปลี่ยนมุมมองต่อเรื่องต่าง ๆ โดยเฉพาะความเป็นบุคคล พลเมือง และรัฐ ซึ่งเกี่ยวข้องกับการพิจารณามิติสิทธิมนุษยชนไปอย่างไรบ้าง โดยประเด็นนี้ บทความเรื่อง “Internet Governance and the Universal Declaration of Human Rights, Part 1: Foundations” ของ Mr. Klaus Stoll ซึ่งเป็นผู้มีประสบการณ์เชิงปฏิบัติในด้านธรรมาภิบาลอินเทอร์เน็ต ได้อธิบายถึงการเปลี่ยนกรอบคิดว่าด้วยชาติ พลเมือง และบุคคลในยุคดิจิทัล[34] โดยสรุปดังนี้

ชาติดิจิทัล (The Digital Nation) หรือชาติไซเบอร์ (Cybernation) เทคโนโลยีดิจิทัลที่เข้าถึงได้ทั่วโลก กำลังก้าวข้ามและกำหนดปัจจัยหลายประการของสิ่งที่ประกอบขึ้นเป็นประเทศ ชาติ หรือรัฐ

[33] UNGPs, pp. 29 – 31.

[34]Klaus Stoll and Prof Sam Lanfranco, Internet Governance and the Universal Declaration of Human Rights, Part 1: Foundations, 10 December 2019, https://circleid.com/posts/20191210_internet_governance_and_universal_declaration_human_rights_part_1

การเปลี่ยนแปลงดังกล่าวท้าทายโดยตรงต่อแนวคิดของรัฐชาติแบบเก่า การขยายตัวของอินเทอร์เน็ตทั่วโลกทำให้ผู้คนจำนวนมากมีที่อยู่อาศัยในพื้นที่ไซเบอร์ ทำให้แนวคิดของ “ตัวตนดิจิทัล (digital persona)” และชาติไซเบอร์ (cybernation) ถูกสร้างขึ้นควบคู่กันไปด้วย ในแง่นี้ มิติสิทธิมนุษยชนและพันธกรณีของรัฐก็ควรถูกพัฒนาขึ้นเพื่อกำกับดูแลพื้นที่ไซเบอร์ด้วยเช่นกัน

ตัวตนดิจิทัล (The Digital Persona) ความก้าวหน้าที่เกิดจากเทคโนโลยีดิจิทัลได้สร้างตัวตนดิจิทัลของเราขึ้นควบคู่ไปกับตัวตนทางกายภาพ ตัวตนดิจิทัลประกอบด้วยโครงสร้างข้อมูลส่วนบุคคลดิจิทัลที่เชื่อมโยงกับตัวตนที่แท้จริงของเราในฐานะมนุษย์ บ่อยครั้งตัวตนดิจิทัลเหล่านี้ตัดสินคุณค่าที่ส่งผลต่อชื่อเสียงในโลกจริง ทั้งเรื่องความน่าเชื่อถือ และอาจรวมถึงสวัสดิการขั้นพื้นฐานของมนุษย์ เทคโนโลยีสร้างตัวตนดิจิทัลของเราจากข้อมูลที่ถูกรวบรวมและประมวลผลจากหลายแหล่ง ทำให้เราอาจจะมีตัวตนดิจิทัลหลายตัวตนพร้อมกัน สิ่งเหล่านี้นำไปสู่คำถามว่า หลักการสิทธิมนุษยชนปัจจุบันกำหนดสิทธิและหน้าที่ของบุคคลดิจิทัลอย่างไร

ความเป็นพลเมืองดิจิทัล (Digital Citizenship) พื้นที่ไซเบอร์มอบความเป็นบุคคลทั้งทางกายภาพและทางดิจิทัล สิ่งนี้ทำให้เรากลายเป็นพลเมืองดิจิทัลที่มีสิทธิและหน้าที่ที่เกี่ยวข้อง และเราอาจได้รับผลกระทบไม่ทางใดก็ทางหนึ่ง ด้วยเหตุนี้ หลักประกันสิทธิขั้นพื้นฐานที่เรามีในโลกจริงก็ควรได้รับในโลกดิจิทัลด้วย

บทความของ Mr. Klaus Stoll แสดงให้เห็นว่าการเปลี่ยนแปลงในยุคดิจิทัล ทำให้เกิดความซับซ้อนในการบังคับใช้สิทธิมนุษยชน แต่ไม่ว่าจะอย่างไรหลักการสิทธิมนุษยชนต้องถูกพัฒนาและปรับใช้ในโลกดิจิทัลหรือไซเบอร์ ดังนั้น ในส่วนถัดไปจะสำรวจกรอบสิทธิมนุษยชนที่พัฒนาขึ้นเพื่อปรับใช้ในพื้นที่ดิจิทัลหรือไซเบอร์

2.3.2 คำจำกัดของสิทธิมนุษยชนในยุคดิจิทัล

ปัจจุบัน จึงยังไม่มีคำจำกัดความที่ยอมรับร่วมกันโดยทั่วกันในระดับสากลของ “สิทธิมนุษยชนในยุคดิจิทัล” หรือบางครั้งอาจเรียกสั้น ๆ ว่า “สิทธิดิจิทัล” แต่คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ (UN Human Rights Council: UNHRC) [35] และสมัชชาใหญ่แห่งสหประชาชาติ (UN General Assembly) [36] ได้ยืนยันในหลายมติเกี่ยวกับสิทธิมนุษยชนในยุคดิจิทัลว่า *“สิทธิมนุษยชนที่มีอยู่ทางออฟไลน์ ย่อมมีผลบังคับใช้ในทางออนไลน์ด้วย”* ซึ่งหลักการดังกล่าวได้ถูกอ้างอิงนำไปใช้อย่างกว้างขวางเมื่อต้องปรับใช้สิทธิมนุษยชนเกี่ยวกับเทคโนโลยีดิจิทัล

นอกจากนี้ จากการสำรวจเบื้องต้นพบว่า องค์กรที่ทำงานเกี่ยวกับสิทธิมนุษยชนในยุคดิจิทัลได้มีการใช้คำว่า “สิทธิดิจิทัล” แต่ส่วนใหญ่ยังไม่ได้กำหนดคำจำกัดความของคำนี้อย่างชัดเจน

---

[35] A/HRC/RES/12/16, A/HRC/RES/20/8, A/HRC/RES/23/2, A/HRC/RES/26/13, A/HRC/RES/28/16, A/HRC/RES/32/13

[36] A/RES/68/198 ; A/RES/69/166

The Media Legal Defence Initiative ใช้คำว่า “สิทธิดิจิทัล” เพื่ออ้างถึงสิทธิมนุษยชนในยุคดิจิทัลแบบกว้าง ๆ ครอบคลุมสิทธิที่เกี่ยวข้องกับการเข้าถึงและการใช้อินเทอร์เน็ตและ ICT อื่น ๆ รวมถึงการควบคุมเนื้อหาออนไลน์ ความเป็นส่วนตัวและการเฝ้าระวัง เสรีภาพของสื่อ การแพร่กระจายของสิ่งที่เรียกว่า 'ข่าวปลอม' และการบิดเบือนข้อมูลบนแพลตฟอร์มโซเชียลมีเดีย เป็นต้น[37]

Association for Progressive Communications (APC) ได้พัฒนาคำจำกัดความการทำงานของ "สิทธิดิจิทัล" เพื่อเป็นนิยามสำหรับการศึกษาเรื่อง Unshackling expression: A study on laws criminalising expression online in Asia (2017) โดยอธิบายว่า สิทธิดิจิทัลเป็นสิทธิมนุษยชนที่จัดตั้งขึ้นโดยปฏิญญาสากลว่าด้วยสิทธิมนุษยชน มติของสหประชาชาติ อนุสัญญาระหว่างประเทศ กฎบัตรระดับภูมิภาค กฎหมายภายในประเทศ และกฎหมายสิทธิมนุษยชนที่เกิดจากคำพิพากษาของศาล (Case Law) ที่ถูกอ้างใช้ในพื้นที่เครือข่ายดิจิทัล โดยพื้นที่เหล่านั้นอาจเป็นพื้นที่กายภาพ (physical) เช่น โครงสร้างพื้นฐานโปรโตคอล และอุปกรณ์ เป็นต้น หรืออาจสร้างขึ้นแบบเสมือนจริง (virtual) เช่น อัตลักษณ์และชุมชนออนไลน์และการแสดงออกในรูปแบบอื่น ๆ ตลอดจนตัวแทนที่ดำเนินการเกี่ยวกับการแสดงออกนั้น เช่น การจัดการข้อมูลส่วนบุคคล นามแฝง การไม่เปิดเผยตัวตน และการเข้ารหัส ทั้งนี้ พื้นที่ดังกล่าวรวมถึงอินเทอร์เน็ตและเครือข่ายมือถือ อุปกรณ์และแนวทางปฏิบัติที่เกี่ยวข้องด้วย[38]

The Digital Freedom Fund ให้คำอธิบาย “สิทธิดิจิทัล” ในบทความ Digital rights are *all* human rights, not just civil and political โดยกล่าวถึง "สิทธิดิจิทัล" คือ สิทธิมนุษยชนที่ใช้บังคับในพื้นที่ดิจิทัล (digital sphere) รวมถึงสิทธิทางเศรษฐกิจและสังคม เช่น สิทธิในการ การศึกษา สิทธิในการเคหะสถาน สิทธิด้านสุขภาพ รวมถึงสิทธิในการประกันสังคม เป็นต้น[39]

ส่วน The World Economic Forum ได้อธิบายคำว่าสิทธิดิจิทัล ในบทความ What are your digital rights ? ว่า สิทธิดิจิทัล เป็นสิทธิมนุษยชนในยุคอินเทอร์เน็ต สิทธิในความเป็นส่วนตัวออนไลน์และเสรีภาพในการแสดงออก ซึ่งเป็นการต่อยอดจากสิทธิที่เท่าเทียมกันและไม่อาจเพิกถอนได้ตามที่ปรากฏในปฏิญญาสากลว่าด้วยสิทธิมนุษยชนของสหประชาชาติ[40]

นอกจากนี้ องค์กรสนับสนุนสิทธิดิจิทัลอื่น เช่น Access Now ซึ่งเป็นองค์กรรณรงค์ที่ไม่แสวงหาผลกำไรระดับสากล กล่าวไว้ในหน้าโฮมเพจเว็บไซต์องค์กรว่า "เราปกป้องและขยายสิทธิดิจิทัลของผู้ใช้ที่มีความเสี่ยงทั่วโลก" อย่างไรก็ตาม ไม่มีที่ไหนบนเว็บไซต์กำหนดสิทธิดิจิทัล แต่เมื่อดูกิจกรรมหรือโครงการ

---

[37] the Media Legal Defence Initiative, 2018, Mapping Digital Rights and Online Freedom of Expression in East, West and Southern Africa, page 6.

[38] Association for Progressive Communications (APC), (2017), UNSHACKLING EXPRESSION - A STUDY ON LAWS CRIMINALISING EXPRESSION ONLINE IN ASIA, https://giswatch.org/2017-special-report-unshackling-expression-study-law-criminalising-expression-online-asia

[39] Jonathan McCully, 27th February 2019, Digital rights are *all* human rights, not just civil and political, https://digitalfreedomfund.org/digital-rights-are-all-human-rights-not-just-civil-and-political/

[40] What are your digital rights?, https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/

ที่องค์กรขับเคลื่อนนั้น จะครอบคลุมประเด็นเรื่องความปลอดภัยทางดิจิทัล เสรีภาพในการแสดงออก การเลือกปฏิบัติทางอินเทอร์เน็ต และความเป็นส่วนตัว[41] ส่วน European Digital Rights (EDRi) ซึ่งเป็นสมาคมขององค์กรสิทธิมนุษยชนและพลเมืองจากทั่วยุโรป เลือกใช้คำว่า “สภาพแวดล้อมดิจิทัล” ซึ่งก็ไม่มีนิยาม แต่เมื่อดูภารกิจขององค์กรแล้ว พบว่า องค์กรทำงานเกี่ยวข้องกับประเด็นสิทธิในความเป็นส่วนตัว ลิขสิทธิ์ เสรีภาพในการแสดงออก ความปลอดภัย และการเฝ้าระวัง[42]

มีความพยายามมากมายทั้งในระดับโลก ภูมิภาค และท้องถิ่นในการกำหนดขอบเขตและรายละเอียดของสิทธิดิจิทัล เช่น กฎบัตรสิทธิทางอินเทอร์เน็ตของ APC (APC Internet Rights Charter)[43] และกฎบัตรสิทธิมนุษยชนและหลักการสำหรับอินเทอร์เน็ต (Charter of Human Rights and Principles for the Internet) โดยพันธมิตรเชิงพลวัตว่าด้วยสิทธิและหลักการอินเทอร์เน็ต (The Internet Rights and Principles Dynamic Coalition)[44] ซึ่งกฎบัตรทั้งสองได้วางกรอบด้านสิทธิมนุษยชนที่ควรถูกนำไปประยุกต์ใช้กับพื้นที่อินเทอร์เน็ตหรือดิจิทัล

ในระดับภูมิภาค ปฏิญญาแอฟริกาว่าด้วยสิทธิและเสรีภาพอินเทอร์เน็ต (The African Declaration on Internet Rights and Freedoms) เป็นข้อตกลงระดับภูมิภาคที่อธิบายหลักการที่จำเป็นในการปกป้องเสรีภาพบนอินเทอร์เน็ต ตลอดจนการสร้างสภาพแวดล้อมออนไลน์ที่จะเป็นประโยชน์ต่อการพัฒนาทางสังคมและเศรษฐกิจของทวีปแอฟริกาโดยเฉพาะ และล่าสุดในเดือนมกราคม 2565 คณะกรรมาธิการยุโรป (European Commission) ก็ได้นำข้อเสนอ “ปฏิญญายุโรปว่าด้วยสิทธิดิจิทัลและหลักการสำหรับทศวรรษดิจิทัล (European Declaration on Digital Rights and Principles for the Digital Decade)” เพื่อใช้เป็นกรอบการทำงานของผู้กำหนดนโยบาย บริษัท และสหภาพยุโรปในการจัดการกับการเปลี่ยนแปลงทางดิจิทัล[45]

ส่วนในระดับอาเซียน ยังไม่พบว่ามีเอกสารที่จัดทำโดยองค์กรระดับรัฐบาล แต่ภาคประชาสังคมในฟิลิปปินส์เคยจัดทำปฏิญญาฟิลิปปินส์ว่าด้วยเสรีภาพและหลักการอินเทอร์เน็ต (the Philippine Declaration on Internet Rights and Principles) เมื่อปี 2558 โดยมีองค์กรต่าง ๆ ร่วมลงนาม 23 องค์กร ปฏิญญาได้กล่าวถึงสิทธิและหลักการทางอินเทอร์เน็ตไว้ 10 ด้าน อาทิ การเข้าถึงอินเทอร์เน็ตสำหรับทุกคน การทำให้สถาปัตยกรรมของอินเทอร์เน็ตเป็นประชาธิปไตย เสรีภาพในการแสดงออกและการสมาคม สิทธิในความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล ความเท่าเทียมทางเพศ การศึกษาและความรู้ดิจิทัล เสรีภาพ ความปลอดภัย และการรักษาความปลอดภัยบนอินเทอร์เน็ต อินเทอร์เน็ตและไอซีทีเพื่อความยั่งยืนด้านสิ่งแวดล้อม ฯลฯ[46]

---

[41] https://www.accessnow.org/

[42] https://edri.org/

[43] https://www.apc.org/en/pubs/about-apc/apc-internet-rights-charter

[44] https://internetrightsandprinciples.org/charter/

[45] https://op.europa.eu/en/publication-detail/-/publication/969edb7b-7f7f-11ec-8c40-01aa75ed71a1/language-en

[46] https://fma.ph/ph-declaration-internet-rights-principles/

ศูนย์เบิร์กแมนไคลน์เพื่อินเทอร์เน็ตและสังคม ณ มหาวิทยาลัยฮาร์วาร์ด (The Berkman Klein Center for Internet & Society at Harvard University) เคยศึกษาวิเคราะห์เอกสารรวม 30 ฉบับที่เกี่ยวข้องกับสิทธิทางอินเทอร์เน็ต (Internet Bill of Rights) ที่รับรองโดยกลุ่มต่าง ๆ ซึ่งมีทั้งเอกสารที่มีผลผูกพันทางกฎหมาย และไม่มีผลผูกพันทางกฎหมาย งานชิ้นดังกล่าวได้สรุปแง่มุมของสิทธิทางอินเทอร์เน็ตเป็น 7 ประเภทหลัก ได้แก่ สิทธิและเสรีภาพขั้นพื้นฐานหรือขั้นพื้นฐาน ข้อจำกัดทั่วไปเกี่ยวกับอำนาจรัฐ ธรรมาภิบาลอินเทอร์เน็ตและการมีส่วนร่วมของพลเมือง สิทธิความเป็นส่วนตัวและการเฝ้าระวัง การเข้าถึงและการศึกษา การเปิดกว้างและเสถียรภาพของเครือข่าย และสิทธิทางเศรษฐกิจและความรับผิดชอบ[47] โดยงานวิจัยชิ้นนี้จะใช้ข้อมูลที่รวบรวมโดยงานดังกล่าวเป็นส่วนหนึ่งของการวิเคราะห์ด้วย

นอกจากนี้ ในงานวิจัยเกี่ยวกับสิทธิดิจิทัลในอาเซียนโดย Jun-E Tan (2019) ซึ่งศึกษาจากกรณีประเทศมาเลเซีย ไทย และฟิลิปปินส์ ได้ให้แง่มุมที่น่าสนใจในการกำหนดขอบเขตสิทธิดิจิทัล โดยงานชิ้นนี้ได้นำเสนอขอบเขตกรอบคิดเรื่องสิทธิดิจิทัล 4 ขอบเขตด้วยกัน คือ[48]

1) สิทธิแบบดั้งเดิมในพื้นที่ดิจิทัล (Conventional rights in digital spaces) มองว่าสิทธิดิจิทัลเป็นของปัจเจกในพื้นที่ดิจิทัลหรืออินเทอร์เน็ต โดยจะเน้นพูดถึงสิทธิในเสรีภาพในการแสดงออก การสมาคม และการชุมนุมออนไลน์ สิทธิที่จะไม่ถูกเลือกปฏิบัติ การคุ้มครองผู้บริโภค การแสดงหาความสุข สิทธิที่จะปราศจากความรุนแรง คำพูดแสดงความเกลียดชัง และการล่วงละเมิด และสิทธิในการมีส่วนร่วม

2) สิทธิที่ถือเอาข้อมูลเป็นศูนย์กลาง (Data-centred rights) ซึ่งมองว่าดิจิทัลเป็นข้อมูลตัวแทนของตัวตนทางกายภาพ ดังนั้น สิทธิดิจิทัลจึงพุ่งเป้าไปที่ความปลอดภัยของข้อมูลและความเป็นส่วนตัว อาทิ สิทธิในความเป็นส่วนตัวของข้อมูล สิทธิที่จะไม่ถูกสอดส่องทางดิจิทัล สิทธิในการควบคุมและเป็นเจ้าของข้อมูล สิทธิในความปลอดภัยและการคุ้มครองข้อมูล

3) การเข้าถึงดิจิทัล (Access to the digital) มองเรื่องการเข้าถึงพื้นที่ดิจิทัลและการมีส่วนร่วมอย่างมีความหมาย อาทิ สิทธิในการเข้าถึงบริการของรัฐและอื่น ๆ ทางออนไลน์ สิทธิในการเข้าถึงอินเทอร์เน็ต สิทธิในการเข้าถึงข้อมูลสารสนเทศและเนื้อหา และสิทธิในการเข้าถึงซอฟแวร์และฮาร์ดแวร์

4) ธรรมาภิบาล/การกำกับดูแลดิจิทัล (Governance of the digital) ซึ่งมองเรื่องการมีส่วนร่วมในระบบกำกับดูแลดิจิทัลและอินเทอร์เน็ต รวมถึงการปรึกษาหารือเกี่ยวกับประเด็นนโยบายอินเทอร์เน็ต

จากข้อมูลดังกล่าว แสดงให้เห็นว่าการกำหนดนิยามและขอบเขตสิทธิมนุษยชนในยุคดิจิทัลหรือสิทธิดิจิทัลนั้น ขึ้นอยู่กับมุมมองและความสนใจของแต่ละองค์กร ดังนั้น จากการพิจารณานิยามข้างต้นแล้ว

---

[47] Gill, Lex and Redeker, Dennis and Gasser, Urs, Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights (November 9, 2015). Berkman Center Research Publication No. 2015-15, Available at SSRN: https://ssrn.com/abstract=2687120 or http://dx.doi.org/10.2139/ssrn.2687120

[48] Jun-E , "Exploring the Nexus Between Technologies and Human Rights: Opportunities and Challenges in Southeast Asia", pages 19 – 27., http://shapesea.com/wp-content/uploads/2019/12/Exploring-the-Nexus-Between-Technologies-and-Human-Rights-r3.pdf

ในงานวิจัยชิ้นนี้ จะกำหนดนิยามหรือขอบเขตความหมายของ “สิทธิมนุษยชนในยุคดิจิทัล” หรือ “สิทธิดิจิทัล” ว่าหมายถึง “สิทธิมนุษยชนที่ปรากฏในตราสารระหว่างประเทศด้านสิทธิมนุษยชนที่อ้างใช้กับสภาพแวดล้อมทางดิจิทัล (Digital sphere) ทั้งที่เป็นกายภาพและเสมือนจริง”

ในส่วนถัดไป จะทำการสำรวจเอกสารที่เกี่ยวข้องกับสิทธิอินเทอร์เน็ตและสิทธิดิจิทัล แล้วนำมาจำแนกและเปรียบเทียบกับเนื้อหาสิทธิมนุษยชนตามที่ปรากฏในตราสารหลักด้านสิทธิมนุษยชน โดยเฉพาะปฏิญญาสากลว่าด้วยสิทธิมนุษยชน อย่างไรก็ดี แม้มีบางประเด็นที่อาจหลุดกรอบออกไปจากปฏิญญาสากลว่าด้วยสิทธิมนุษยชน แต่หากเกี่ยวกับมิติสำคัญของสภาพแวดล้อมดิจิทัล ผู้วิจัยก็จะรวบรวมไว้ด้วยเช่นกัน

2.3.3. ขอบเขตสิทธิมนุษยชนในยุคดิจิทัลหรือสิทธิดิจิทัล

2.3.3.1 ภาพรวม

จากการศึกษาเอกสารที่เกี่ยวข้องกับสิทธิอินเทอร์เน็ต และสิทธิดิจิทัล ซึ่งรวมถึงกฎบัตร (Charter) ปฏิญญา (declaration) คำแนะนำ (Recommendation) แถลงการณ์ (Statement) และอื่น ๆ จำนวน 41 ฉบับ โดยเอกสารเก่าที่สุดที่รวบรวมมาคือ APC Internet Rights Charter ที่จัดทำขึ้นโดย Association for Progressive Communications (APC) ในปี 2545 (ค.ศ. 2002) และเอกสารฉบับใหม่ที่สุดที่รวบรวมมาคือ European Declaration on Digital Rights and Principles for the Digital Decade ที่รับรองโดย European Commission ภายใต้สหภาพยุโรป (EU) ในปี 2565 (ค.ศ. 2022)[49] และเอกสารส่วนใหญ่ที่รวบรวมมาเป็นเอกสารที่จัดทำขึ้นในปี 2557 (ค.ศ. 2014) จำนวน 9 ฉบับ

ในภาพรวมเอกสาร 24 ฉบับ จัดทำโดยภาคประชาสังคม ภาคเอกชน และผู้มีส่วนได้ส่วนเสียหลายฝ่าย จำนวน 8 ฉบับ จัดทำโดยหน่วยงานระหว่างรัฐบาลในระดับภูมภาค (สภายุโรป, สหภาพยุโรป, OECD) จำนวน 6 ฉบับ จัดทำโดยหน่วยงาน/องค์กรที่เป็นรัฐบาลในระดับประเทศ และ 3 ฉบับ จัดทำโดยหน่วยงานในระบบสหประชาชาติ (UNESCO, ผู้รายงานพิเศษแห่งสหประชาชาติ)

เมื่อพิจารณาจากสถานะของเอกสาร พบว่า มีเอกสารที่ได้รับการรับรองแล้วจำนวน 33 ฉบับ นอกนั้น ยังเป็นเอกสารที่อยู่ระหว่างนำเสนอ

หากดูจากลักษณะสภาพบังคับหรือระดับความผูกพันนั้น หากนับเฉพาะที่มีการรับรองแล้ว พบว่า มีเพียง 1 ฉบับ คือ Marco Civil da Internet ของประเทศบราซิลเท่านั้นที่อาจจะมีสภาพบังคับทางกฎหมาย เนื่องจากเป็นเอกสารทางกฎหมายที่จัดทำขึ้นโดยรัฐบาลในระดับชาติ แต่เอกสารส่วนใหญ่ จำนวน 37 ฉบับ เป็นเอกสารที่ไม่ได้มีผลผูกพันทางกฎหมายให้ต้องปฏิบัติตาม (non-binding) เนื่องจากไม่ได้มีสถานะเป็นกฎหมายระหว่างประเทศที่มีผลผูกพัน อย่างไรก็ตาม เอกสารแต่ละชิ้นอาจมีพลังทางศีลธรรมในระดับที่แตกต่างกัน โดยเฉพาะเอกสารที่จัดทำขึ้นจากองค์กรระหว่างประเทศที่เป็นที่ยอมรับ (เช่น UNESCO, OECD,

[49] โปรดดูรายละเอียดข้อมูลเอกสารฉบับต่าง ๆ ที่ https://datastudio.google.com/reporting/69cc286d-a501-4061-967c-7a7d3b18910c

สหภาพยุโรป, สภายุโรป) อาจมีอิทธิพลในการถูกนำไปใช้กำหนดกฎเกณฑ์ได้มากกว่า เพราะสามารถแรงจูงใจทางอ้อมให้ประเทศสมาชิกปฏิบัติตามหลักการที่เกี่ยวข้อง ขณะที่เอกสารที่พัฒนาขึ้นโดยภาคประชาสังคมหรือเอกสารที่เป็นแถลงการณ์หรือเอกสารที่เจรจาระหว่างผู้เข้าร่วมจำนวนน้อยมักจะมีผลกระทบจำกัด

เมื่อพิจารณาประเด็นสิทธิมนุษยชนที่เอกสารเหล่านี้ระบุไว้ โดยจำแนกตามประเภทหลักการสิทธิมนุษยชนที่ระบุไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (UDHR) กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) และกติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคมและวัฒนธรรม (ICESCR) โดยพบว่า เอกสารส่วนใหญ่กล่าวถึงเสรีภาพในการแสดงออกและแสดงความคิดเห็น สิทธิในความเป็นส่วนตัว สิทธิในการเข้าถึงอินเทอร์เน็ต ความเสมอภาคและการไม่เลือกปฏิบัติ สิทธิทางวัฒนธรรม/ความหลากหลายของภาษา รายละเอียดตามตามตาราง 2.1

ทั้งนี้ สิทธิทางอินเทอร์เน็ตนั้น ตราสารหลักด้านสิทธิมนุษยชนปัจจุบันยังไม่ได้รับรองไว้อย่างชัดเจน แต่ก็มีการตีความว่าการอินเทอร์เน็ตเป็นสิ่งที่เอื้ออำนวยต่อการใช้เสรีภาพในการแสดงออกและสิทธิมนุษยชนอื่น ๆ ในยุคดิจิทัล ดังนั้น รัฐมีพันธกรณีในการประกันการเข้าถึงอินเทอร์เน็ต โดยประเด็นนี้จะกล่าวถึงอย่างละเอียดในบทถัดไป

ตาราง 2.1 ภาพรวมเอกสารที่เกี่ยวกับสิทธิดิจิทัล จำแนกตามประเภทสิทธิ

ที่	ประเด็นสิทธิ/หลักการ	ตราสารสิทธิมนุษยชน	จำนวน (ฉบับ)
1	**เสรีภาพในการแสดงออกและความคิดเห็น**	UDHR 19; ICCPR 19, 20	39
2	**สิทธิในความเป็นส่วนตัว**	UDHR 12; ICCPR 17	35
3	**สิทธิทางอินเทอร์เน็ต**		35
4	**ความเสมอภาคและการไม่เลือกปฏิบัติ**	UDHR 1, 2, 7; ICCPR 2 (1), 3, 26; ICESCR 2 (2), 3	23
5	**สิทธิทางวัฒนธรรม/ความหลากหลายของภาษา**	UDHR 27 (1); ICCPR 27; ICESCR 1 (a)	20
6	**สิทธิในความมั่งคงปลอดภัย**	UDHR 3; ICCPR 9	14
7	**เสรีภาพในการชุมนุมและสมาคม**	UDHR 20; ICCPR 21, 22	14
8	**สิทธิที่จะได้รับการพิจารณาอย่างเป็นธรรม**	UDHR 10; ICCPR 14	13
9	**สิทธิที่จะได้รับการเยียวยา**	UDHR 8; ICCPR 2 (3)	11
10	**สิทธิในการศึกษา**	UDHR 26; ICESCR 13	11
11	**สิทธิเด็ก**	UDHR 2 (2); ICCPR 24 (1); ICESCR 10 (3); CRC	12
12	**สิทธิในการมีส่วนร่วมทางการเมืองการปกครอง**	UDHR 21; ICCPR 25	10

13	**สิทธิผู้บริโภค**		10
14	**สิทธิแรงงาน**	UDHR 23; ICESCR 6 - 8	8
15	**สิทธิคนพิการ**	CRPD	4
15	**เสรีภาพในการนับถือศาสนา**	UDHR 18; ICCPR 18	3

ที่มา ผู้วิจัย

2.3.3.1 รายละเอียดของสิทธิประเภทต่าง ๆ

ในส่วนนี้จะกล่าวถึงรายละเอียดของสิทธิประเภทต่าง ๆ ตามที่มีการระบุไว้ในเอกสารที่เลือกศึกษาโดยสังเขป และเพื่อให้ง่ายต่อการสื่อสาร จะแบ่งการนำเสนอเป็น 4 หมวดหลัก ได้แก่ 1) สิทธิอินเทอร์เน็ต 2) สิทธิพลเมืองและการเมือง 3) สิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม และ 4) สิทธิของกลุ่มเฉพาะ อาทิ สิทธิเด็ก สิทธิผู้บริโภค สิทธิคนพิการ

1) สิทธิทางอินเทอร์เน็ต (Internet Rights)

จากเอกสารที่ศึกษา แม้จะมีรายละเอียดในประเด็นนี้แตกต่างกันไป แต่เอกสารส่วนใหญ่มีการระบุถึงประเด็นสำคัญเกี่ยวกับสิทธิทางอินเทอร์เน็ตดังต่อไปนี้

1.1) สิทธิในการเข้าถึงอินเทอร์เน็ต

คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติยอมรับว่าอินเทอร์เน็ต ซึ่งเชื่อมต่อระหว่างกันทั่วโลก มีศักยภาพที่ดีเยี่ยมในการเร่งความก้าวหน้าของมนุษย์ การลดความเหลื่อมล้ำทางดิจิทัลและการพัฒนาสังคมแห่งความรู้ ส่งเสริมเสรีภาพในการแสดงออก ความเป็นส่วนตัว และสิทธิมนุษยชนอื่น ๆ[50] คณะมนตรีสิทธิมนุษยชนยังเน้นย้ำด้วยว่าเพื่อให้อินเทอร์เน็ตยังคงครอบคลุมทั่วโลก (global) เปิดกว้าง (open) และใช้งานร่วมกันได้ (interoperable) จำเป็นที่รัฐจะต้องจัดการกับข้อกังวลด้านความปลอดภัยตามพันธกรณีด้านสิทธิมนุษยชนระหว่างประเทศของตน[51]

สิทธิในการเข้าถึงอินเทอร์เน็ตรวมถึง[52]

1) ทุกคนมีสิทธิเท่าเทียมกันในการเข้าถึงและใช้อินเทอร์เน็ตที่ปลอดภัยและเปิดกว้าง สำหรับประชากรทุกกลุ่มโดยไม่มีการเลือกปฏิบัติ รัฐต้องใช้มาตรการที่เหมาะสมเพื่อประกันว่าผู้มีรายได้น้อยสามารถเข้าถึงอินเทอร์เน็ตในชนบทหรือพื้นที่ห่างไกลทางภูมิศาสตร์ได้และผู้ที่มีความต้องการพิเศษ เช่น คนพิการต้องสามารถเข้าถึงได้เช่นกัน

[50] A/HRC/RES/32/13, 18 July 2016 ; A/HRC/32/L.20, 27 June 2016

[51] A/HRC/RES/26/13, 14 July 2014

[52] โปรดดู The Charter of Human Rights and Principles for the Internet, Principle 1., https://internetrightsandprinciples.org/charter/ ; APC Internet Rights Charter, Theme 1, 6, https://www.apc.org/sites/default/files/APC_charter_EN_0_1_2.pdf

2) สิทธิในองค์ความรู้และทักษะทางอินเทอร์เน็ตหรือดิจิทัล (Internet/Digital literacy) ทุกคนมีสิทธิในการศึกษาและฝึกอบรมเกี่ยวกับอินเทอร์เน็ตและดิจิทัล ซึ่งเป็นตัวตั้งต้นของการเข้าถึงและการมีส่วนร่วมของพลเมืองอย่างมีความหมาย รัฐมีพันธกรณีในการส่งเสริมการพัฒนาทักษะและความรู้ดังกล่าว โดย Frank La Rue อดีตผู้รายงานพิเศษว่าด้วยการส่งเสริมและคุ้มครองสิทธิในเสรีภาพในการแสดงความคิดเห็นและการแสดงออก แนะนำให้รัฐรวมทักษะการรู้อินเทอร์เน็ตไว้ในหลักสูตรของโรงเรียนและสนับสนุนโมดูลการเรียนรู้ที่คล้ายคลึงกันนอกโรงเรียน นอกเหนือจากการฝึกอบรมทักษะพื้นฐานแล้ว โมดูลต่าง ๆ ควรชี้แจงประโยชน์ของการเข้าถึงข้อมูลทางออนไลน์และการส่งข้อมูลอย่างมีความรับผิดชอบ การฝึกอบรมยังสามารถช่วยให้บุคคลเรียนรู้วิธีป้องกันตนเองจากเนื้อหาที่เป็นอันตรายด้วย[53]

3) สิทธิในตัวประสาน (interface) เนื้อหา และแอพพลิเคชั่นที่สามารถเข้าถึงได้สำหรับทุกคน (inclusive design) รวมถึงผู้ที่มีความบกพร่องทางร่างกายประสาทสัมผัสหรือการรับรู้ ผู้คนที่ไม่สามารถอ่านออกเขียนได้และผู้ที่พูดภาษาของชนกลุ่มน้อย หลักการของการออกแบบสากล (Universal design) และการใช้เทคโนโลยีอำนวยความสะดวกต้องได้รับการส่งเสริมและสนับสนุนเพื่อให้คนพิการได้รับประโยชน์อย่างเต็มที่และเท่าเทียมกับคนอื่น

4) สิทธิในการเข้าถึงที่เท่าเทียมกันสำหรับชายและหญิง ในหลาย ๆ พื้นที่ ผู้หญิงและผู้ชายไม่สามารถเข้าถึงได้อย่างเท่าเทียมกัน โดยการเพิ่มการเข้าถึงต้องยอมรับและแก้ไขความไม่เท่าเทียมทางเพศที่มีอยู่ ผู้หญิงต้องมีส่วนร่วมอย่างเต็มที่ในทุกด้านที่เกี่ยวข้องกับการพัฒนาอินเทอร์เน็ต

5) สิทธิในการเข้าถึงได้ในราคาที่ไม่แพง ผู้กำหนดนโยบายและผู้กำกับดูแลต้องประกันว่าประชาชนทุกคนสามารถเข้าถึงอินเทอร์เน็ตได้ในราคาประหยัด การพัฒนาโครงสร้างพื้นฐานโทรคมนาคมและการกำหนดกฎเกณฑ์ ราคา ภาษีและค่าธรรมเนียม ควรทำให้ทุกกลุ่มรายได้สามารถเข้าถึงได้

6) สิทธิในการเข้าถึงสาธารณะ เพราะหลายคนอาจจะไม่สามารถเข้าถึงคอมพิวเตอร์หรืออินเทอร์เน็ตแบบส่วนตัวได้ ดังนั้น จุดเชื่อมต่อสาธารณะ เช่น ศูนย์วิทยุ ห้องสมุด ศูนย์ชุมชน คลินิกและโรงเรียนต้องทำให้ทุกคนสามารถเข้าถึงอินเทอร์เน็ตได้ง่ายในระยะที่ไม่ห่างจากที่อาศัยหรือทำงาน สิ่งนี้มีความสำคัญอย่างยิ่งในประเทศที่อินเทอร์เน็ตยังไม่พร้อมใช้งานหรือราคาแพง และต้องรองรับการเข้าถึงอินเทอร์เน็ตผ่านสื่อมือถือด้วย

7) เสรีภาพในการเลือกระบบและการใช้ซอฟต์แวร์ เพื่ออำนวยความสะดวกในเรื่องนี้และเพื่อรักษาการเชื่อมต่อระหว่างกันและนวัตกรรม ควรกระจายอำนาจของโครงสร้างพื้นฐานการสื่อสารและโปรโตคอล

---

[53] A/66/290, 10 august 2011, para 84.

8) สิทธิในสถาปัตยกรรมแบบเปิด (Open architecture) อินเทอร์เน็ตในฐานะ "เครือข่ายของเครือข่าย" ประกอบด้วย เครือข่ายที่เชื่อมต่อกันจำนวนมาก จึงจำเป็นต้องคุ้มครองสถาปัตยกรรมแบบเปิด ซึ่งสามารถรวมและเผยแพร่เครือข่ายประเภทใดก็ได้ในทุกที่

9) สิทธิในมาตรฐานแบบเปิด (Open standards) โปรโตคอลส่วนใหญ่ที่เป็นแกนกลางของอินเทอร์เน็ตเป็นโปรโตคอลที่อิงตามมาตรฐานแบบเปิดที่มีประสิทธิภาพ เชื่อถือได้และเปิดให้ใช้งานได้ทั่วโลก โดยมีข้อจำกัดด้านใบอนุญาตเพียงเล็กน้อยหรือไม่มีเลย ข้อกำหนดของโปรโตคอลต้องพร้อมใช้งานสำหรับทุกคน โดยไม่มีค่าใช้จ่าย

10) ความเป็นกลางทางเนตหรือเครือข่าย (Net neutrality) สถาปัตยกรรมอินเทอร์เน็ตที่ครอบคลุมทั่วโลกจะต้องได้รับการคุ้มครองและส่งเสริมให้เป็นพาหนะในการแลกเปลี่ยนข้อมูล การสื่อสารโดยเสรี เปิดกว้าง เท่าเทียมกัน และไม่เลือกปฏิบัติ ดังนั้น จึงไม่ควรให้สิทธิพิเศษหรือสร้างอุปสรรคต่อเนื้อหาใด ๆ เกี่ยวกับเศรษฐกิจ สังคม วัฒนธรรม หรือการเมือง แต่ไม่รวมถึงการเลือกปฏิบัติในเชิงบวกเพื่อส่งเสริมความเท่าเทียมและความหลากหลายบนและผ่านอินเทอร์เน็ต

1.2) การกำกับดูแลอินเทอร์เน็ต (Internet Governance)

อินเทอร์เน็ตและระบบการสื่อสารจะต้องถูกควบคุมในลักษณะที่จะรักษาและขยายสิทธิมนุษยชนอย่างเต็มที่ การกำกับดูแลอินเทอร์เน็ตต้องขับเคลื่อนด้วยหลักการของการเปิดกว้าง ความครอบคลุม และความรับผิดชอบ โดยตราสารที่รวบรวมได้นำเสนอหลักการสำคัญของการกำกับดูแลอินเทอร์เน็ต ดังนี้

1) การกำกับดูแลแบบมีส่วนร่วมและผู้มีส่วนได้ส่วนเสียหลายฝ่าย (Multistakeholder) รูปแบบการกำกับดูแลต้องยอมรับและเอื้อต่อการมีส่วนร่วมที่เท่าเทียมกันของทุกคนจากทุกที่ในกระบวนการกำหนดนโยบายอินเทอร์เน็ต โดยทุกภาคส่วนของสังคม รวมถึงภาครัฐ ภาคเอกชน ภาคประชาสังคม สถาบันการศึกษา และชุมชนด้านเทคนิค รวมถึงองค์กรระหว่างประเทศ มีสิทธิที่จะมีส่วนร่วมในกระบวนการกำกับดูแลอย่างเต็มที่ นอกจากนี้ ผู้ที่ได้รับผลกระทบจากการตัดสินใจเกี่ยวกับการกำกับดูแลอินเทอร์เน็ตควรมีสิทธิที่จะมีส่วนร่วมและเป็นตัวแทนในกระบวนการ

2) ความโปร่งใสและการเปิดกว้าง กระบวนการตัดสินใจทั้งหมดที่เกี่ยวข้องกับการกำกับดูแลและการพัฒนาอินเทอร์เน็ตควรเป็นระบบเปิดและสามารถเข้าถึงได้ทั้งในระดับโลก ระดับภูมิภาค และระดับประเทศ

2) สิทธิพลเมืองและการเมือง

2.1) หลักความเสมอภาคและการไม่เลือกปฏิบัติ

ตามที่ได้ระบุไว้ในข้อ 2 ของ UDHR ทุกคนมีสิทธิและเสรีภาพทั้งหมดตามที่ระบุไว้ใน UDHR โดยปราศจากการแบ่งแยกไม่ว่าชนิดใด อาทิ ชาติพันธุ์ สีผิว เพศ ภาษา ศาสนา ความคิดเห็นทางการเมืองหรือความคิดเห็นอื่น ชาติกำเนิดหรือสังคม ทรัพย์สิน กำเนิดหรือสถานะอื่น ๆ

บุคคลต้องไม่ถูกเลือกปฏิบัติในสภาพแวดล้อมดิจิทัล ทั้งในแง่ของโครงสร้างพื้นฐานทางเทคนิค และภายในชุมชนออนไลน์ โดยต้องประกันว่าโครงสร้างพื้นฐานดิจิทัลเอื้ออำนวยสำหรับทุกคน ไม่มีใครถูกกีดกันไม่ให้เข้าถึง รวมถึงต้องเพิ่มการเข้าถึงของกลุ่มที่มีอุปสรรคในการเข้าถึง โดยเฉพาะกลุ่มคนชายขอบ ซึ่งรวมถึงผู้สูงอายุ ชนกลุ่มน้อยทางชาติพันธุ์และทางภาษา ชนพื้นเมือง คนพิการ และผู้มีอัตลักษณ์ทางเพศที่หลากหลาย ด้วยเหตุนี้ ฮาร์ดแวร์ โค้ด แอปพลิเคชัน และเนื้อหาทั้งหมดควรได้รับการออกแบบโดยใช้หลักการออกแบบที่เป็นสากล เพื่อให้ทุกคนใช้งานได้อย่างเต็มที่[54]

ปัจจุบัน โมเดลธุรกิจดิจิทัลแบบแสวงประโยชน์จำนวนมากมีการแบ่งแยก และลดการมีส่วนร่วมทางดิจิทัลของผู้คน รวมถึงการแสวงหาประโยชน์จากข้อมูลส่วนบุคคล ซึ่งอาจนำไปสู่ผลลัพธ์ของการเลือกปฏิบัติ จึงจำเป็นต้องมีกลไกการกำกับดูแลที่ยุติธรรมและมีประสิทธิภาพ[55]

2.2) สิทธิที่จะได้รับการเยียวยาอย่างเป็นผล

ข้อ 8 ของ UDHR ระบุว่าทุกคนมีสิทธิที่จะได้รับการเยียวยาอย่างมีประสิทธิผลจากศาลที่มีอำนาจแห่งรัฐต่อการกระทำอันล่วงละเมิดสิทธิขั้นพื้นฐาน ซึ่งตนได้รับตามรัฐธรรมนูญหรือกฎหมาย

รัฐต้องประกันว่าทุกคนที่ถูกละเมิดสิทธิในสภาพแวดล้อมดิจิทัลมีสิทธิได้รับการเยียวยาที่มีประสิทธิผลโดยองค์กรที่เหมาะสมและมีอำนาจ ซึ่งรวมถึงการประกันการเข้าถึงกลไกอื่น ๆ เพื่อแสวงหาการเยียวยา เช่น ผ่านสถาบันสิทธิมนุษยชนแห่งชาติ เป็นต้น ทั้งนี้ ต้องไม่มีอุปสรรคทางกฎหมาย ขั้นตอน การเงิน หรือการปฏิบัติอื่น ๆ ในการแสวงหาการเยียวยาที่มีประสิทธิผล

นอกจากนี้ เนื่องจากการดำเนินการด้านเทคโนโลยีดิจิทัลส่วนใหญ่อยู่ในมือของภาคธุรกิจ รัฐจึงควรใช้นโยบายและมาตรการเพื่อส่งเสริมให้ภาคเอกชนเคารพสิทธิมนุษยชนเกี่ยวกับอินเทอร์เน็ต โดยเฉพาะอย่างยิ่งโดยการจัดตั้งกลไกการร้องเรียนที่มีประสิทธิภาพเพื่อจัดการกับปัญหาตั้งแต่เนิ่น ๆ และเยียวยาโดยตรงให้กับบุคคลที่ถูกละเมิดสิทธิหรือได้รับผลกระทบในทางลบ[56]

2.3) สิทธิในเสรีภาพและความปลอดภัยของบุคคล

---

[54] โปรดดู The Charter of Human Rights and Principles for the Internet, Principle 2

[55] Klaus Stoll and Prof Sam Lanfranco, Internet Governance and the Universal Declaration of Human Rights, Part 3: Article 6-12, https://circleid.com/posts/20200203_internet_governance_and_universal_declaration_human_rights_part_3

[56] โปรดดู UNGPs

ข้อ 3 ของ UDHR ระบุว่าทุกคนมีสิทธิในการมีชีวิต เสรีภาพ และความมั่นคงของบุคคล

สิทธิในการมีชีวิต เสรีภาพ และความปลอดภัยในสภาพแวดล้อมดิจิทัล รวมถึง[57]

1) การป้องกันอาชญากรรมทุกรูปแบบ ทุกคนจะได้รับการคุ้มครองจากอาชญากรรมทุกรูปแบบที่กระทำบนหรือใช้อินเทอร์เน็ต รวมถึงการล่วงละเมิด การคุกคามทางอินเทอร์เน็ต การค้ามนุษย์ และการใช้อินเทอร์เน็ตในทางที่ผิด การละเมิดข้อมูลส่วนบุคลและข้อมูลดิจิทัล

2) ความปลอดภัยของอินเทอร์เน็ต ทุกคนมีสิทธิที่จะเพลิดเพลินกับการเชื่อมต่อที่ปลอดภัยบนอินเทอร์เน็ต ซึ่งรวมถึงการป้องกันจากบริการและโปรโตคอลที่คุกคามการทำงานทางเทคนิคของอินเทอร์เน็ต เช่น ไวรัส มัลแวร์ และฟิชชิง เป็นต้น

รัฐต้องคุ้มครองบุคคลจากอาชญากรรมทางอินเทอร์เน็ตผ่านกระบวนการยุติธรรมที่มีประสิทธิภาพหรือมาตรการอื่น ๆ รวมถึงการกำหนดนโยบายและใช้มาตรการเพื่อให้ภาคธุรกิจดำเนินการตาม UNGPs เพื่อประกันสภาพแวดล้อมดิจิทัลที่ปลอดภัย

อย่างไรก็ดี มาตรการรักษาความปลอดภัยทั้งหมดต้องสอดคล้องกับกฎหมายและมาตรฐานสิทธิมนุษยชนระหว่างประเทศ โดยเฉพาะอย่างยิ่ง หากการใช้มาตรการเหล่านั้นมีการแทรกแซงสิทธิมนุษยชนอื่น เช่น เสรีภาพในการแสดงออก สิทธิในความเป็นส่วนตัว การแทรกแซงดังกล่าวต้องถูกกำหนดโดยกฎหมาย และเป็นไปเพื่อวัตถุประสงค์ที่ชอบธรรม มีความจำเป็นและได้สัดส่วนในสังคมประชาธิปไตย ไม่เลือกปฏิบัติ และจัดให้มีการเยียวยาที่มีประสิทธิผลเมื่อเกิดการละเมิดด้วย ซึ่งหลักการจำกัดสิทธินี้จะกล่าวถึงรายละเอียดในบทต่อไป

2.4) สิทธิในกระบวนการยุติธรรม

ข้อ 10 ของ UDHR ระบุว่าทุกคนย่อมมีสิทธิในความเสมอภาคอย่างเต็มที่ในการได้รับการพิจารณาคดีที่เป็นธรรมและเปิดเผยจากศาลที่อิสระและเป็นกลางในการพิจารณากำหนดสิทธิและหน้าที่ของตนและข้อกล่าวหาอาญาใดต่อตน

เป็นเรื่องปกติที่สิทธิในการพิจารณาคดีอย่างเป็นธรรมจะถูกละเมิดในสภาพแวดล้อมดิจิทัล/อินเทอร์เน็ต เช่น กรณีมีการขอให้ตัวกลางทางอินเทอร์เน็ตลบเนื้อหาที่ผิดกฎหมาย ซึ่งกรณีเช่นนี้สิทธิในการพิจารณาคดีอย่างเป็นธรรมต้องได้รับการเคารพ และคุ้มครองตามมาตรฐานที่กำหนดโดย UDHR (ข้อ 9-11) และ ICCPR (ข้อ 9 และ 14-16) ตลอดจนตราสารด้านสิทธิมนุษยชนที่เกี่ยวข้องอื่นๆ

2.5) เสรีภาพในความเชื่อและศาสนา

ข้อ 18 ของ UDHR ระบุว่าทุกคนมีสิทธิในอิสรภาพแห่งความคิด มโนธรรม และศาสนา ทั้งนี้สิทธินี้รวมถึงอิสรภาพในการเปลี่ยนศาสนาหรือความเชื่อ และอิสรภาพในการแสดงออกทางศาสนาหรือ

[57] โปรดดู The Charter of Human Rights and Principles for the Internet, Principle 3

ความเชื่อถือของตนในการสอน การปฏิบัติการสักการะบูชา และการประกอบพิธีกรรม ไม่ว่าจะโดยลำพังหรือในชุมชนร่วมกับผู้อื่น และในที่สาธารณะหรือส่วนบุคคล

ทุกคนมีสิทธิในเสรีภาพในความเชื่อและมโนธรรมทางศาสนา และแสดงความเชื่อเหล่านั้นให้ประจักษ์ในพื้นที่ดิจิทัลเช่นกัน

2.6) สิทธิในเสรีภาพในการแสดงออกและแสดงความคิดเห็น

ข้อ 19 ของ UDHR และข้อ 19 ของ ICCPR ระบุว่าทุกคนมีสิทธิที่จะถือเอาความคิดเห็นโดยปราศจากการแทรกแซง และมีเสรีภาพในการแสดงออก ซึ่งรวมถึงเสรีภาพในการแสวงหา รับ และส่งข้อมูลและความคิดผ่านสื่อใดๆ และโดยไม่คำนึงถึงพรมแดน

สิทธิในเสรีภาพในการแสดงออกและข้อมูลทางออนไลน์/บนอินเทอร์เน็ต หมายรวมถึงสิทธิของบุคคลในการใช้อินเทอร์เน็ตโดยไม่มีการเซ็นเซอร์ในทุกรูปแบบ ไม่ว่าจะเป็นการข่มขู่ผู้ใช้อินเทอร์เน็ตหรือปิดการแสดงออกทางออนไลน์ การโจมตีทางไซเบอร์และการล่วงละเมิดทางออนไลน์ รวมถึงการบล็อกและการกรอง ซึ่งมีจุดมุ่งหมายเพื่อป้องกันการเข้าถึงเนื้อหา นอกจากนี้ ตัวกลางทางอินเทอร์เน็ตจะต้องไม่ถูกกดดันจากรัฐหรือฝ่ายอื่น ๆ ให้ลบ ซ่อนหรือบล็อกเนื้อหา หรือเปิดเผยข้อมูลเกี่ยวกับผู้ใช้อินเทอร์เน็ต

สิทธิในเสรีภาพในการแสดงออกอาจถูกจำกัดได้ภายใต้เงื่อนไขข้อ 19 (3) ของ ICCPR โดยข้อจำกัดใด ๆ จะต้องตอบสนองต่อการทดสอบดังนี้[58] (1) ชอบด้วยกฎหมาย (Legality) โดยเป็นกฎหมายที่สามารถเข้าถึงได้ ชัดเจน ไม่คลุมเครือ และแม่นยำเพียงพอที่จะทำให้ปัจเจกสามารถควบคุมความประพฤติของตนได้ และควบคุมดุลยพินิจของหน่วยงานรัฐเกี่ยวกับการดำเนินการตามข้อจำกัด (2) วัตถุประสงค์ที่ชอบธรรม (Legitimate purpose) ได้แก่ เพื่อการเคารพสิทธิหรือชื่อเสียงของผู้อื่น หรือการรักษาความมั่นคงของชาติ ความสงบเรียบร้อยของประชาชน หรือสาธารณสุขหรือศีลธรรม และ (3) สอดคล้องกับหลักความจำเป็น (Necessity) และได้สัดส่วน (Proportionality) ซึ่งดำเนินการบนพื้นฐานของการตัดสินใจของศาลที่มีอำนาจ เป็นอิสระและเป็นกลาง การตัดสินใจควรกำหนดเป้าหมายรายกรณีและเฉพาะเจาะจง และเป็นวิธีจำกัดน้อยที่สุดที่มีอยู่เพื่อให้บรรลุเป้าหมายที่ชอบธรรม[59]

2.7) เสรีภาพในการชุมนุม

ข้อ 20 ของ UDHR และข้อ 21 ของ ICCPR รับรองสิทธิในเสรีภาพในการชุมนุมโดยสงบ

สิทธิในเสรีภาพในการชุมนุมสามารถใช้ทางออนไลน์ด้วย โดยบุคคลมีอิสระในการใช้แพลตฟอร์มอินเทอร์เน็ต เช่น โซเชียลมีเดียและ ICT อื่น ๆ เพื่อจุดประสงค์ในการชุมนุมอย่างสงบ

การจำกัดเทคโนโลยีการสื่อสารสามารถขัดขวางสิทธิในการชุมนุม เนื่องจากเทคโนโลยีเหล่านี้เปิดโอกาสให้มีการชุมนุมทั้งหมดหรือบางส่วนทางออนไลน์ และมักจะมีบทบาทสำคัญในการจัดการ

---

[58] CCPR General comment No. 34, paras. 33 - 35.

[59] รายละเอียดจะกล่าวถึงเพิ่มเติมในบทที่ว่าด้วยเสรีภาพในการแสดงออกและการจำกัดเนื้อหาออนไลน์

การเข้าร่วม และติดตามการชุมนุมทางกายภาพ[60] ดังนั้น รัฐต้องไม่ปิดกั้นหรือขัดขวางการเชื่อมต่ออินเทอร์เน็ตที่เกี่ยวข้องกับการชุมนุมโดยสงบ หรือใช้การแทรกแซงต่อเทคโนโลยีหรือกำหนดเป้าหมายตามภูมิศาสตร์เพื่อจำกัดการเชื่อมต่อหรือการเข้าถึงเนื้อหา[61]

มาตรการของรัฐที่นำไปใช้ในจำกัดการใช้สิทธิในการชุมนุม ซึ่งเป็นการปิดกั้นหรือจำกัดแพลตฟอร์มอินเทอร์เน็ต เช่น โซเชียลมีเดียและ ICT อื่นๆ ต้องสอดคล้องกับข้อ 21 ของ ICCPR กล่าวคือ (1) ชอบด้วยกฎหมาย (Legality) การจำกัดต้องถูกกำหนดโดยกฎหมาย ซึ่งสามารถเข้าถึงได้ ชัดเจน ไม่คลุมเครือ และไม่เลือกปฏิบัติ (2) มีวัตถุประสงค์ที่ชอบธรรม (legitimate purpose) กล่าวคือ เพื่อประโยชน์แห่งความมั่นคงของชาติหรือความปลอดภัย ความสงบเรียบร้อย การสาธารณสุข หรือศีลธรรมของประชาชนหรือการคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น และ (3) สอดคล้องกับหลักความจำเป็น (necessity) และได้สัดส่วน (proportionality) โดยมีความจำเป็นในสังคมประชาธิปไตยและได้สัดส่วนกับวัตถุประสงค์ที่ชอบธรรม มีความต้องการทางสังคมที่เร่งด่วนสำหรับการจำกัด มีความสมดุลระหว่างการใช้สิทธิเสรีภาพในการชุมนุมกับผลประโยชน์ของสังคมโดยรวม เป็นวิธีการที่ล่วงล้ำน้อยที่สุด ข้อจำกัดมีการตีความและบังคับใช้อย่างแคบ และไม่ล่วงล้ำสาระสำคัญของสิทธิในเสรีภาพในการชุมนุม[62]

2.8) เสรีภาพในการสมาคม

ข้อ 20 ของ UDHR และข้อ 22 ของ ICCPR รับรองสิทธิในเสรีภาพในการสมาคม

สิทธิในเสรีภาพในการสมาคมสามารถใช้ทางออนไลน์ได้ด้วย กล่าวคือ บุคคลมีอิสระในการใช้แพลตฟอร์มอินเทอร์เน็ต เช่น โซเชียลมีเดียและ ICT อื่น ๆ เพื่อเชื่อมโยงซึ่งกันและกันและจัดตั้งสมาคมเพื่อกำหนดวัตถุประสงค์ของสมาคม รวมถึงการจัดตั้งสหภาพแรงงาน และดำเนินกิจกรรมภายในขอบเขตที่กำหนดไว้ตามกฎหมายที่เป็นไปตามมาตรฐานสากล นอกจากนี้ สมาคมต่าง ๆ สามารถใช้อินเทอร์เน็ตได้อย่างอิสระเพื่อใช้สิทธิในเสรีภาพในการแสดงออกและมีส่วนร่วมในการอภิปรายทางการเมืองและประเด็นสาธารณะ

ในการจำกัดเสรีภาพในการสมาคมนั้น บทบัญญัติข้อ 22 ของ ICCPR กำหนดเงื่อนไขการจำกัดไว้เช่นเดียวกับเสรีภาพในการชุมนุม กล่าวคือ ข้อจำกัดที่จะกำหนดเกี่ยวกับสิทธิเหล่านี้จะต้องสอดคล้องกับหลักการของความชอบด้วยกฎหมาย ความชอบธรรม และความจำเป็นและได้สัดส่วน

2.9) สิทธิในการมีส่วนร่วมทางการเมืองการปกปกครอง

<u>สิทธิในการมีส่วนร่วมทางการเมืองการปกปกครอง</u>

ข้อ 21 (1) ของ UDHR และข้อ 25 ของ ICCPR ระบุว่าทุกคนมีสิทธิที่จะมีส่วนร่วมในการปกครองประเทศตนโดยตรง หรือผ่านผู้แทนซึ่งได้รับเลือกตั้งโดยอิสระ

---

[60] UN Human Rights Committee, General Comment No. 37, para. 10

[61] CCPR General comment No. 37, para. 34.

[62] รายละเอียดเพิ่มเติมโปรดดู CCPR General comment No. 37

การเข้าถึงอินเทอร์เน็ตเป็นเงื่อนไขเบื้องต้นสำหรับการมีส่วนร่วมของพลเมือง ทั้งภายในชุมชนดิจิทัลและในสังคมโดยรวม การเข้าถึงอินเทอร์เน็ตไม่ควรเป็นอุปสรรคต่อการมีส่วนร่วมในสังคม ชุมชนวัฒนธรรม หรือการดำเนินการของรัฐบาล การมีส่วนร่วมของพลเมืองควรได้รับการอำนวยความสะดวกและได้รับการเอื้ออำนวยโดยอินเทอร์เน็ต

สิทธิในการเข้าถึงบริการสาธารณะ

ข้อ 21 (2) ของ UDHR และข้อ 25 ของ ICCPR ระบุว่าทุกคนมีสิทธิที่จะเข้าถึงบริการสาธารณะในประเทศตนโดยเสมอภาค

รัฐควรส่งเสริมการเข้าถึงบริการสาธารณะทางดิจิทัล แต่ต้องมีทางเลือกอื่นในโลกทางกายภาพที่รับประกันสิทธิของผู้ที่ไม่ต้องการหรือไม่สามารถใช้ทรัพยากรดิจิทัลได้

2.10) สิทธิในความเป็นส่วนตัว

ข้อ 12 ของ UDHR และข้อ 17 ของ ICCPR ระบุว่าบุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าว

สมัชชาใหญ่แห่งสหประชาชาติยืนยันว่ารัฐมีหน้าที่ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ เพื่อป้องกันการละเมิดสิทธิในความเป็นส่วนตัวในบริบทของการสื่อสารทางดิจิทัล[63] คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติและสำนักงานข้าหลวงใหญ่สิทธิมนุษยชนแห่งสหประชาชาติได้ยืนยันหลักการของความชอบด้วยกฎหมาย ความชอบธรรม ความจำเป็นและได้สัดส่วนที่ต้องนำมาใช้แทรกแซงสิทธิในความเป็นส่วนตัวในลักษณะเดียวกับที่ใช้จำกัดเสรีภาพในการแสดงออกและเสรีภาพพื้นฐานอื่น ๆ[64]

สิทธิในความเป็นส่วนตัวในสภาพแวดล้อมดิจิทัล รวมถึงการคุ้มครองข้อมูล สิทธิที่จะไม่เปิดเผยชื่อ (Right to Anonymity) สิทธิในการเข้ารหัส (Right to encryption) สิทธิที่จะไม่ถูกสอดส่อง รวมถึงสิทธิที่จะถูกลืม[65] โดยรายละเอียดส่วนนี้จะกล่าวถึงในบทที่ว่าด้วยสิทธิในความเป็นส่วนตัวต่อไป

3) สิทธิทางสังคม เศรษฐกิจ และวัฒนธรรม

อินเทอร์เน็ตมีศักยภาพสูงในการบรรลุสิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม รวมถึงสิทธิแรงงาน หลักประกันทางสังคม สิทธิการศึกษา ฯลฯ

3.1) สิทธิแรงงาน

---

[63] A/RES/68/167, 18 December 2013

[64] A/HRC/39/29, 3 August 2018, para 10; Human Rights Council, A/HRC/RES/34/7, 7 April 2017, para. 2.

[65] โปรดดู The Charter of Human Rights and Principles for the Internet, Principle 8, 9., https://internetrightsandprinciples.org/charter/; APC Internet Rights Charter, Theme 5.

ข้อ 23 ของ UDHR รับรองสิทธิในการทำงาน รวมถึงสิทธิของทุกคนในการทำงาน การเลือกงานโดยอิสระ ในเงื่อนไขที่ยุติธรรมและเอื้ออำนวยต่อการทำงาน และในการคุ้มครองต่อการว่างงาน สิทธิที่จะได้รับค่าจ้างที่เท่าเทียมกันสำหรับงานที่เท่าเทียมกัน โดยปราศจากการเลือกปฏิบัติใด สิทธิที่จะได้รับค่าตอบแทนที่ยุติธรรมและเอื้ออำนวยต่อการประกันความเป็นอยู่อันควรค่าแก่ศักดิ์ศรีของมนุษย์สำหรับตนเองและครอบครัว และสิทธิที่จะจัดตั้งและที่จะเข้าร่วมสหภาพแรงงานเพื่อความคุ้มครองผลประโยชน์ของตน

สิทธิในการทำงานในสภาพแวดล้อมดิจิทัล รวมถึง[66]

- การเข้าถึงอินเทอร์เน็ตในที่ทำงาน นายจ้างมีหน้าที่รับผิดชอบในการจัดหาการเข้าถึงอย่างยุติธรรม การศึกษา และนโยบายที่ชัดเจนเกี่ยวกับวิธีการจัดการการเข้าถึงอินเทอร์เน็ตในที่ทำงาน หากมีข้อจำกัดใด ๆ เกี่ยวกับการใช้อินเทอร์เน็ตในที่ทำงาน จะต้องระบุไว้อย่างชัดเจนในนโยบายขององค์กร
- บุคคลทุกคนมีสิทธิที่จะหางานและทำงานผ่านหรือผ่านทางอินเทอร์เน็ต
- การได้รับการฝึกทักษะใหม่ เพื่อการปรับตัวในสภาพแวดล้อมดิจิทัล
- สิทธิที่จะตัดการเชื่อมต่อทางดิจิทัล การพักผ่อน และการรักษาความสมดุลระหว่างงานและชีวิตส่วนตัวและครอบครัว

3.2) สิทธิในการศึกษา

ข้อ 26 ของ UDHR รับรองสิทธิของทุกคนการศึกษา และการศึกษาจะต้องมุ่งไปสู่การพัฒนาบุคลิกภาพของมนุษย์อย่างเต็มที่ และการเสริมสร้างความเคารพต่อสิทธิมนุษยชนและอิสรภาพขั้นพื้นฐาน

ทุกคนมีสิทธิที่จะได้รับการศึกษาเกี่ยวกับอินเทอร์เน็ตและใช้อินเทอร์เน็ตเพื่อการศึกษา รวมถึง[67]

- การศึกษาผ่านอินเทอร์เน็ต สภาพแวดล้อมการเรียนรู้เสมือนจริงและมัลติมีเดีย แพลตฟอร์มการเรียนรู้และการสอนประเภทอื่น ๆ จะต้องคำนึงถึงความผันแปรของท้องถิ่นและภูมิภาคในแง่ของภาษา การสอน และประเพณีความรู้
- การส่งเสริมโอกาสในการฝึกอบรมความรู้และทักษะเกี่ยวข้องกับดิจิทัลและอินเทอร์เน็ตโดยไม่มีค่าใช้จ่ายหรือเสียค่าใช้จ่าย เพื่อการพัฒนาสังคมและทำให้ผู้คนสามารถใช้และกำหนดรูปแบบอินเทอร์เน็ตเพื่อตอบสนองความต้องการของพวกเขา

---

[66] The Charter of Human Rights and Principles for the Internet, Principle 14 ; European Declaration on Digital Rights and Principles for the Digital Decade, Chapter 2, https://op.europa.eu/en/publication-detail/-/publication/969edb7b-7f7f-11ec-8c40-01aa75ed71a1/language-en

[67] The Charter of Human Rights and Principles for the Internet, Principle 10

- การศึกษาเกี่ยวกับอินเทอร์เน็ตและสิทธิมนุษยชน รวมถึงการสร้างความตระหนักและความเคารพต่อสิทธิมนุษยชน (ออนไลน์และออฟไลน์)

3.3) สิทธิด้านสุขภาพ

ข้อ 25 (1) ของ UDHR ระบุว่าทุกคนมีสิทธิในมาตรฐานการครองชีพอันเพียงพอสำหรับสุขภาพและความอยู่ดีของตนและของครอบครัว รวมทั้งการดูแลรักษาทางการแพทย์ และข้อ 12 (1) และ 12 (2) (c) ถึง (d) ของ ICESCR กำหนดให้รัฐดำเนินการตามขั้นตอนเพื่อให้บรรลุการป้องกัน การรักษา และการควบคุมการแพร่ระบาดเฉพาะถิ่น การประกอบอาชีพ และโรคอื่น ๆ ตลอดจนการสร้างสภาพที่จะให้การบริการทางการแพทย์และการรักษาพยาบาลในกรณีเจ็บป่วย

การส่งเสริมเทคโนโลยีที่ช่วยให้ประชาชนสามารถเข้าถึงระบบการแพทย์ทางไกลและระบบทางไกลได้อย่างทั่วถึง และสามารถจ่ายได้ สำหรับการใช้ระบบช่วยเหลือในการวินิจฉัยทางดิจิทัล โดยเฉพาะอย่างยิ่ง กระบวนการที่ใช้ปัญญาประดิษฐ์ จะต้องไม่จำกัดสิทธิในการตัดสินใจอย่างอิสระของบุคลากรทางการแพทย์ นอกจากนี้ สภาพแวดล้อมด้านสุขภาพแบบดิจิทัลจะต้องรับประกันความชอบด้วยกฎหมาย ความเป็นอิสระของผู้ป่วย ความปลอดภัยของข้อมูล ความโปร่งใสในการใช้อัลกอริทึม การเข้าถึงได้ และความเคารพอย่างเต็มที่ต่อสิทธิขั้นพื้นฐานของผู้ป่วย และโดยเฉพาะอย่างยิ่ง สิทธิในความเป็นส่วนตัวและข้อมูลส่วนบุคคล[68]

3.4) สิทธิทางวัฒนธรรม ความหลากหลาย วิทยาศาสตร์ และทรัพย์สินทางปัญญา

ข้อ 27 ของ UDHR ระบุว่าทุกคนมีสิทธิที่จะเข้าร่วมโดยอิสระในชีวิตทางวัฒนธรรมของชุมชน ที่จะเพลิดเพลินกับศิลปะ และมีส่วนในความก้าวหน้า และคุณประโยชน์ทางวิทยาศาสตร์ และทุกคนมีสิทธิที่จะได้รับการคุ้มครองผลประโยชน์ทางจิตใจและทางวัตถุ อันเป็นผลจากประดิษฐกรรมใดทางวิทยาศาสตร์ วรรณกรรม และศิลปกรรมซึ่งตนเป็นผู้สร้าง

สิทธินี้รวมถึง[69]

- สิทธิที่จะใช้อินเทอร์เน็ต เพื่อเข้าถึงความรู้ ข้อมูล และการวิจัย ทุกคนมีอิสระในการเข้าถึงและแบ่งปันข้อมูลที่มีคุณค่าต่อสาธารณะโดยไม่อยู่ภายใต้การคุกคามหรือข้อจำกัด การปกป้องผลประโยชน์ของผู้สร้างสรรค์ต้องเกิดขึ้นในวิถีทางที่สอดคล้องกับการมีส่วนร่วมอย่างเปิดกว้างและเสรีในกระแสความรู้ทางวิทยาศาสตร์และวัฒนธรรม

---

[68] Carta de derechos digitales (Charter for Digital Rights), 5.XXIII, https://www.lamoncloa.gob.es/presidente/actividades/Paginas/2021/140721-derechos-digitales.aspx

[69] โปรดดู The Charter of Human Rights and Principles for the Internet, Principle 11., https://internetrightsandprinciples.org/charter/ ; APC Internet Rights Charter, Theme 4

- อินเทอร์เน็ตจะต้องเป็นตัวแทนของวัฒนธรรมและภาษาที่หลากหลายทั้งในแง่ของรูปลักษณ์และการใช้งาน รวมถึงการส่งเสริมและคุ้มครองความรู้ของชนพื้นเมืองทางออนไลน์
- บุคคลและชุมชนทั้งหมดมีสิทธิที่จะใช้ภาษาของตนเองเพื่อสร้าง เผยแพร่ และแบ่งปันข้อมูลและความรู้ผ่านทางอินเทอร์เน็ต ต้องให้ความสนใจเป็นพิเศษในการส่งเสริมการเข้าถึงภาษาชนกลุ่มน้อย
- สิทธิของผู้สร้างผลงาน ผู้สร้างมีสิทธิได้รับค่าตอบแทนและเป็นที่ยอมรับสำหรับงานและนวัตกรรมของตน อย่างไรก็ดี ทรัพย์สินทางปัญญาเป็นผลผลิตทางสังคมและมีหน้าที่ทางสังคม ดังนั้น การคุ้มครองทรัพย์สินทางปัญญา จึงต้องสร้างสมดุลระหว่างสิทธิของผู้สร้างกับผลประโยชน์สาธารณะ ระบอบลิขสิทธิ์ต้องไม่จำกัดนวัตกรรมเพิ่มเติมหรือการเข้าถึงความรู้และทรัพยากรของสาธารณะและการศึกษา และต้องไม่จำกัดความสามารถของอินเทอร์เน็ตอย่างไม่ได้สัดส่วนเพื่อสนับสนุนการเข้าถึงความรู้และวัฒนธรรมของสาธารณชน ทั้งนี้ งานวิจัยที่ได้รับทุนสนับสนุนจากสาธารณะและงานทางปัญญาและวัฒนธรรมต้องเผยแพร่สู่สาธารณะโดยเสรีหากเป็นไปได้
- สิทธิในซอฟต์แวร์ฟรีและโอเพ่นซอร์ส (FOSS) โดยการทำงานกับ FOSS เป็นการเพิ่มขีดความสามารถด้วยการสร้างทักษะ ทำให้มีความยั่งยืนมากขึ้นและส่งเสริมนวัตกรรมในท้องถิ่น รัฐบาลจึงควรกำหนดนโยบายที่สนับสนุนการใช้ FOSS โดยเฉพาะในภาครัฐ
- สิทธิในมาตรฐานเทคโนโลยีเปิดมาตรฐานทางเทคนิคที่ถูกใช้บนอินเทอร์เน็ตต้องเปิดอยู่เสมอ เพื่อให้สามารถใช้งานร่วมกันได้ การพัฒนาเทคโนโลยีใหม่จะต้องตอบสนองความต้องการของทุกภาคส่วนในสังคม โดยเฉพาะอย่างยิ่งผู้ที่เผชิญกับข้อจำกัดและอุปสรรคเมื่อใช้งานออนไลน์

4) สิทธิของกลุ่มเฉพาะ

4.1) สิทธิเด็ก

ข้อ 25 ของ UDHR เด็กมีสิทธิได้รับการดูแลและช่วยเหลือเป็นพิเศษ และตามที่ระบุไว้ในมาตรา 5 ของอนุสัญญาว่าด้วยสิทธิเด็ก (CRC) เด็กมีสิทธิที่จะเคารพในความสามารถที่พัฒนาของพวกเขา

ในแง่ของอินเทอร์เน็ต เด็กจะต้องได้รับอิสระในการใช้อินเทอร์เน็ตและได้รับการปกป้องจากอันตรายที่เกี่ยวข้องกับอินเทอร์เน็ต ความสมดุลระหว่างลำดับความสำคัญเหล่านี้จะขึ้นอยู่กับความสามารถของเด็ก รัฐต้องเคารพสิทธิและความรับผิดชอบของบิดามารดาและครอบครัวในการให้คำแนะนำแก่เด็กอย่างเหมาะสมกับความสามารถของเด็กที่กำลังพัฒนา

สิทธิเด็กบนอินเทอร์เน็ต รวมถึง[70]

- สิทธิ์ในการได้รับประโยชน์จากอินเทอร์เน็ต เด็กควรได้รับประโยชน์จากอินเทอร์เน็ตตามอายุ เด็กต้องมีโอกาสใช้อินเทอร์เน็ตเพื่อใช้สิทธิพลเมือง การเมือง เศรษฐกิจ วัฒนธรรม และสังคมของตน
- สิทธิที่จะปลอดพ้นจากการแสวงประโยชน์และการทารุณกรรม เด็กมีสิทธิที่จะเติบโตและพัฒนาในสภาพแวดล้อมที่ปลอดภัย ซึ่งปราศจากการแสวงประโยชน์ทางเพศหรือการแสวงประโยชน์ประเภทอื่น จึงต้องดำเนินการตามขั้นตอนเพื่อป้องกันการใช้อินเทอร์เน็ตเพื่อละเมิดสิทธิของเด็ก อย่างไรก็ตาม มาตรการดังกล่าวต้องกำหนดเป้าหมายให้แคบและได้สัดส่วน และต้องมีการพิจารณาอย่างเหมาะสมเกี่ยวกับผลกระทบของมาตรการที่ใช้กับการไหลของข้อมูลออนไลน์อย่างเสรี
- สิทธิในการรับฟังความคิดเห็น เด็กที่สามารถสร้างความคิดเห็นของตนเองได้มีสิทธิที่จะแสดงความคิดเห็นในเรื่องนโยบายอินเทอร์เน็ตทั้งหมดที่มีผลกระทบต่อพวกเขา และความคิดเห็นของพวกเขาจะได้รับการพิจารณาตามอายุและวุฒิภาวะ
- ผลประโยชน์สูงสุดของเด็กจะต้องเป็นข้อพิจารณาเบื้องต้น ทั้งนี้ ตามที่บัญญัติไว้ในข้อ 3 ของอนุสัญญาว่าด้วยสิทธิเด็ก

4.2) สิทธิผู้บริโภค

ทุกคนต้องเคารพ คุ้มครอง และปฏิบัติตามหลักการคุ้มครองผู้บริโภคบนอินเทอร์เน็ต[71]

ธุรกิจอีคอมเมิร์ซต้องได้รับการควบคุมเพื่อประกันว่าผู้บริโภคได้รับการคุ้มครองในระดับเดียวกับที่ได้รับในการทำธุรกรรมที่ไม่ใช่ทางอิเล็กทรอนิกส์

บริษัทมีความรับผิดชอบในการจัดการกับผู้ใช้อย่างยุติธรรมและซื่อสัตย์ และเคารพสิทธิของผู้ใช้บนอินเทอร์เน็ต ผู้ใช้ต้องมีส่วนร่วมในการปฏิบัติตามสัญญาที่โปร่งใสและจัดทำข้อกำหนดในภาษาที่เข้าใจง่ายและเข้าถึงได้

4.3) สิทธิของคนพิการ

ข้อ 3 (f) และ 9 ของอนุสัญญาว่าด้วยสิทธิของคนพิการ รัฐมีพันธกรณีที่ต้องใช้มาตรการที่เหมาะสมเพื่อประกันว่าคนพิการสามารถเข้าถึงสิ่งแวดล้อมทางกายภาพได้บนพื้นฐานที่เท่าเทียมกับผู้อื่น

ข้อ 4 วรรค 2 (g) ของอนุสัญญาฯ กำหนดว่ารัฐควรจัดให้มีสารสนเทศที่สามารถเข้าถึงได้แก่คนพิการเกี่ยวกับเครื่องช่วยในการเคลื่อนย้าย เครื่องมือ เทคโนโลยีสิ่งอำนวยความสะดวก รวมถึงเทคโนโลยีใหม่

---

[70] โปรดดู The Charter of Human Rights and Principles for the Internet, Principle 12.

[71] โปรดดู The Charter of Human Rights and Principles for the Internet, Principle 16.

และข้อ 9 วรรค 2 (g) กำหนดให้รัฐดำเนินมาตรการที่เหมาะสมในการส่งเสริมการเข้าถึงเทคโนโลยีและระบบสารสนเทศและการสื่อสารใหม่สำหรับคนพิการ รวมถึงอินเทอร์เน็ต

ทั้งนี้ สหภาพโทรคมนาคมระหว่างประเทศ (ITU) ได้แนะนำหลักการสำหรับการเข้าถึง ICT ได้แก่ การเข้าถึงอย่างเสมอภาค (equal access) ความเท่าเทียมกันเชิงหน้าที่ (functional equivalency) การเข้าถึงได้ (accessibility) การจ่ายได้ (affordability) และการออกแบบสำหรับทุกคน (design for all)[72]

หลักการของการออกแบบสากล (universal design) เป็นพื้นฐานในการบรรลุการเข้าถึงอย่างเต็มรูปแบบ เพื่อให้มั่นใจถึงความสม่ำเสมอและความก้าวหน้าอย่างมีประสิทธิผลสู่การเข้าถึงอย่างเต็มรูปแบบ รัฐควรกำหนดมาตรฐานและข้อบังคับระดับชาติเกี่ยวกับการเข้าถึงได้และการออกแบบที่เป็นสากล รวมถึงการเข้าถึงเทคโนโลยีสารสนเทศและการสื่อสาร[73]

2.4 สรุปส่งท้าย

จากการสำรวจเอกสารที่เกี่ยวข้องกับสิทธิดิจิทัลหรืออินเทอร์เน็ตข้างต้น พบว่า เอกสารให้ความสนใจกับหลักการสิทธิมนุษยชนที่หลากหลาย โดยบางเรื่องอาจถือเป็นเรื่องใหม่ในยุคดิจิทัลและยังไม่มีความชัดเจนในตราสารสิทธิมนุษยชนที่ใช้อยู่ในปัจจุบัน เช่น สิทธิในอินเทอร์เน็ต แต่หลายเรื่องเป็นการปรับใช้หลักการที่ปรากฏในตราสารสิทธิมนุษยชนที่มีอยู่กับพื้นที่ดิจิทัลหรืออินเทอร์เน็ต โดยเฉพาะเสรีภาพในการแสดงออกและความเป็นส่วนตัว ซึ่งเป็นประเด็นสำคัญที่มีการพูดถึงมากที่สุดในแทบทุกเอกสารที่รวบรวมมา

เอกสารส่วนใหญ่ไม่ได้กล่าวถึงสิทธิดิจิทัลโดยตรง โดยเฉพาะเอกสารที่ถูกจัดทำขึ้นในระยะแรก อย่างไรก็ดี เอกสารในช่วงหลัง โดยเฉพาะนับตั้งแต่ปี 2557 (ค.ศ. 2014) เป็นต้นมา มีการใช้คำว่าสิทธิดิจิทัลมากขึ้น ดังเช่นที่ปรากฏใน Charter of Digital Rights (2014) ของ European Digital Rights (EDRi), Carta de derechos digitales (Charter for Digital Rights, 2021) ของ รัฐบาลสเปน และ European Declaration on Digital Rights and Principles for the Digital Decade (2022) ที่เสนอโดย European Commission, European Union (EU) เป็นต้น

อย่างไรก็ดี เอกสารเหล่านี้ก็ยังไม่ครอบคลุมสิทธิมนุษยชนตามที่ระบุในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน และหลายเรื่องยังขาดไป อาทิ สิทธิที่จะได้รับการยอมรับว่าเป็นบุคคลตามกฎหมาย สิทธิที่จะไม่ถูกบังคับให้เป็นทาส สิทธิที่จะไม่ถูกทรมาน ประเด็นเหล่านี้ถือเป็นเรื่องสำคัญ เพราะดังที่กล่าวไปแล้วว่าในสภาพแวดล้อมดิจิทัล เรามีทั้งตัวตนทางกายภาพและตัวตนดิจิทัล และการละเมิดสิทธิในตัวตนดิจิทัล อาจ

---

[72] ITU, “e-Accessibility Policy Handbook for Persons with Disabilities”, 2010, https://g3ict.org/publication/e-accessibility-policy-handbook-for-persons-with-disabilities

[73] A/71/314, 9 August 2016, para 35.

ส่งผลกระทบต่อตัวตนทางกายภาพได้ ซึ่งผลกระทบเหล่านี้อาจเห็นได้ชัดมากขึ้นเมื่อเราเข้าสู่โลกเสมือน (Metaverse) มากขึ้น ดังนั้น จึงอาจต้องมีการศึกษาในประเด็นเหล่านี้เพิ่มเติมต่อไปในอนาคต [74]

เทคโนโลยีดิจิทัลได้สร้างความท้าทายใหม่ ๆ ต่อกรอบงานด้านสิทธิมนุษยชน และมีหลายประเด็นที่จำเป็นต้องศึกษาเชิงลึกต่อไป อย่างไรก็ดี ภายใต้ระยะเวลาที่จำกัดของงานวิจัย จึงจำเป็นต้องเลือกบางประเด็นที่เห็นว่าสำคัญและเป็นปัญหาในปัจจุบันเพื่อทำการศึกษาเชิงลึก ได้แก่ สิทธิทางอินเทอร์เน็ต เสรีภาพในการแสดงออกและการควบคุมเนื้อหาออนไลน์ และสิทธิในความเป็นส่วนตัวในยุคดิจิทัล โดยเน้นประเด็นการคุ้มครองข้อมูลและการสอดส่องโดยรัฐ

ประเด็นแรก สิทธิทางอินเทอร์เน็ต ถือเป็นความท้าทายพื้นฐานที่สุด เพราะเป็นตัวเปิดในการเข้าถึงและใช้สิทธิมนุษยชนอื่นในยุคดิจิทัล โดยสิทธิทางอินเทอร์เน็ตยังเป็นประเด็นที่เชื่อมโยงกับความเหลื่อมล้ำทางดิจิทัลอีกด้วย

ประเด็นที่สอง เสรีภาพในการแสดงออกทางออนไลน์ ซึ่งเป็นสิทธิมนุษยชนประการสำคัญ เพราะเป็นหลักประกันสิทธิมนุษยชนอื่น ๆ เช่นกัน อย่างไรก็ดี การแสดงออกบนอินเทอร์เน็ตในปัจจุบัน นำมาสู่ข้อกังวลหลายประการ รวมถึงการแสดงออกซึ่งความเกลียดชัง และการเผยแพร่ข่าวปลอมที่ระบาดอย่างหนัก โดยเฉพาะในช่วงของความขัดแย้งทางการเมืองและการระบาดของไวรัสโคโรนา 2019 ดังนั้น จึงจำเป็นต้องศึกษาเพื่อแสวงหาทางออกในการจัดการเนื้อหาดังกล่าวอย่างเหมาะสมภายใต้หลักการสิทธิมนุษยชน

ประเด็นที่สาม สิทธิในความเป็นส่วนตัว โดยเฉพาะในมิติเกี่ยวกับความเป็นส่วนตัวในข้อมูลและการสื่อสารนั้น ถือว่าได้รับผลกระทบอย่างลึกซึ้งจากการเปลี่ยนแปลงสู่ยุคดิจิทัล ซึ่งเปิดโอกาสให้มีการรวบรวมและประมวลผลข้อมูลส่วนบุคคลได้อย่างกว้างขวางและง่ายดาย อีกทั้ง สิ่งที่น่ากังวลอย่างมากในปัจจุบัน คือ การสอดส่องโดยใช้เทคโนโลยีใหม่เป็นเครื่องมือ ซึ่งส่งผลกระทบอย่างมากต่อสิทธิในความเป็นส่วนตัว และยากที่จะตรวจสอบและแสวงหาการเยียวยาได้ ดังนั้น จึงเป็นประเด็นสำคัญที่จำเป็นต้องศึกษาเพื่อแสดงหาแนวทางจัดการที่เหมาะสมโดยสอดคล้องกับหลักการสิทธิมนุษยชน

[74]โปรดดูงานเขียนของ Klaus Stoll and Prof Sam Lanfranco, Internet Governance and the Universal Declaration of Human Rights, Part 3: Article 6-12

บทที่ 3

สิทธิทางอินเทอร์เน็ต

ปัจจุบัน อินเทอร์เน็ตกลายเป็นปัจจัยพื้นฐานชีวิตในการดำเนินชีวิตประจำวันของผู้คน และเป็นองค์ประกอบสำคัญของการใช้สิทธิมนุษยชนในยุคดิจิทัล ในบทนี้ ต้องการที่จะทบทวนพัฒนาการและกรอบแนวคิดของสิทธิทางอินเทอร์ในระดับสากล และวิเคราะห์สถานการณ์สิทธิทางอินเทอร์เน็ตในประเทศไทย

3.1 ส่วนนำ

มีการกล่าวว่า อินเทอร์เน็ต (Internet) คือ “เครือข่ายแห่งเครือข่าย” (network of networks) อันเป็นโครงสร้างพื้นฐานทางข้อมูลข่าวสารอันประกอบขึ้นจากเครือข่ายคอมพิวเตอร์ที่มาเชื่อมต่อกันเป็นจำนวนมากจากทั่วโลก โดยอาศัยโปรโตคอลและมาตรฐานกลาง (standard protocol) ในการรับส่งข้อมูลร่วมกัน ทำให้คอมพิวเตอร์ในเครือข่ายสามารถสื่อสารกันได้[75]

อินเทอร์เน็ต ถูกพัฒนาในฐานะโครงการของรัฐบาลสหรัฐอเมริกา ในช่วงปลายทศวรรษ 1960 โดยรัฐบาลสหรัฐให้ทุนสนับสนุนการจัดทำเครือข่ายหน่วยงานของโครงการวิจัยเพื่อการป้องกันประเทศระดับสูง (Defense Advanced Research Project Agency Network - DARPA Net) พอถึงกลางทศวรรษ 1970 มีการคิดค้นทรานสมิชชันคอนโทรลโปรโตคอล/อินเทอร์เน็ตโปรโตคอล (Transmission Control Protocol/Internet Protocol - TCP/IP) ซึ่งเป็นเครือข่ายที่พัฒนามาเป็นระบบอินเทอร์เน็ตในปัจจุบัน หนึ่งในหลักการสำคัญของอินเทอร์เน็ต คือลักษณะที่กระจายตัว โดยกลุ่มข้อมูลสามารถเคลื่อนตัวไปยังทิศทางต่างๆ ผ่านเครือข่าย สามารถหลีกเลี่ยงอุปสรรคแบบเดิมและกลไกควบคุม ทั้งนี้ คณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต (Internet Engineering Task Force - IETF) ที่ก่อตั้งขึ้นเมื่อปี 1986 ได้ช่วยพัฒนาอินเทอร์เน็ตโดยผ่านกระบวนการตัดสินใจแบบร่วมมือกัน โดยไม่มีการควบคุมจากส่วนกลาง[76]

ในยุคที่อินเทอร์เน็ตเป็นส่วนหนึ่งของชีวิตประจำวันของมนุษย์ คำถามที่ว่าอินเทอร์เน็ตเปลี่ยนแปลงสิทธิและเสรีภาพที่กำหนดไว้ในตราสารสิทธิมนุษยชนที่มีอยู่หรือไม่นั้น เป็นเรื่องที่มีการหยิบยกขึ้นมาพูดคุยกันอย่างกว้างขวางในช่วงที่ผ่านมา ดังนั้น การทำความเข้าใจโครงสร้างพื้นฐานและการทำงานของอินเทอร์เน็ตจึงมีความสำคัญอย่างยิ่งเพื่อที่จะเข้าใจว่าอินเทอร์มีผลต่อสิทธิมนุษยชนอย่างไร

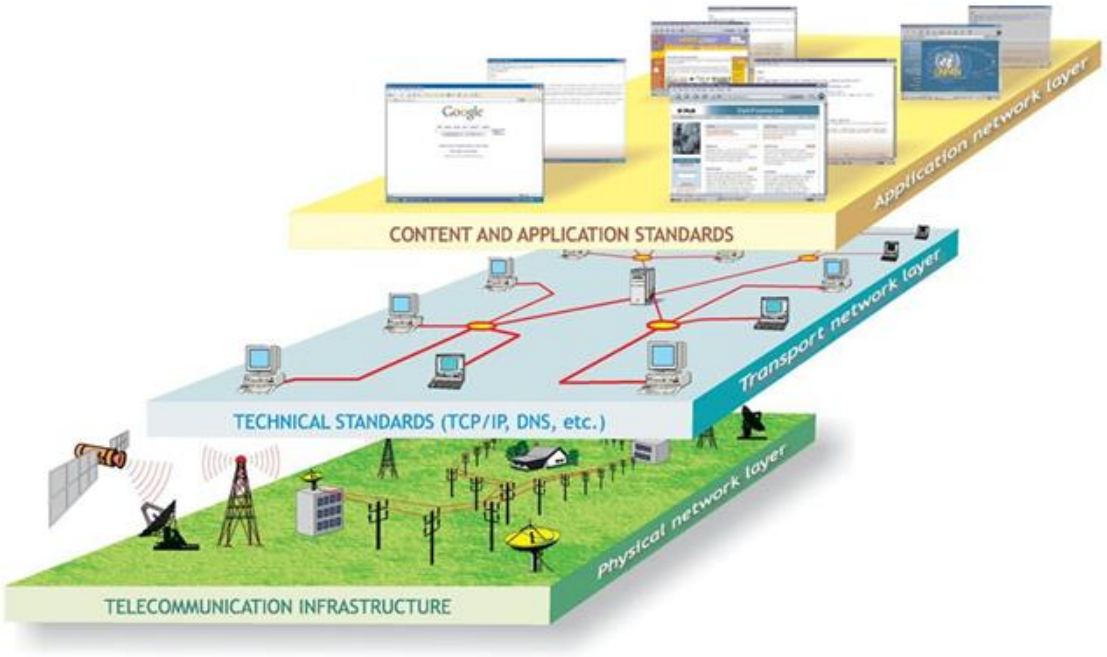
---

[75]พิรงรอง รามสูต รณะนันทน์ และ นิธิมา คณานิธินันท์. 2547. รายงานวิจัยเรื่อง การกำกับดูแลเนื้อหาอินเทอร์เน็ต. สกว. หน้า 2

[76] เคอร์บาลิจา, โจวาน. เปิดประตูสู่การอภิบาลอินเทอร์เน็ต.-- กรุงเทพฯ : มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง, 2558. หน้า 16.

3.2 โครงสร้างพื้นฐานของอินเทอร์เน็ต

ภาพที่ 3.1 โครงสร้างพื้นฐานของอินเทอร์เน็ต



ที่มา: DiploFoundation, graphic library.

โครงสร้างพื้นฐานและการกำหนดมาตรฐาน ประกอบด้วยปัญหาพื้นฐานในการบริหารงานอินเทอร์เน็ต ซึ่งส่วนใหญ่เป็นเรื่องทางเทคนิค โดยสามารถแบ่งปัญหาออกเป็น 3 เลเยอร์ ดังนี้[77]

เลเยอร์แรก โครงสร้างพื้นฐานทางโทรคมนาคม เป็นช่องทางการจราจรทุกสายในอินเทอร์เน็ต (สายเคเบิล คอมพิวเตอร์ ดาวเทียม) ซึ่งการพัฒนาเทคโนโลยีและนวัตกรรมมีแนวโน้มที่จะนำเสนอโครงสร้างพื้นฐานประเภทใหม่ ๆ รวมถึงโดรนและบอลลูน การกำกับดูแลโครงสร้างพื้นฐานด้านการสื่อสารมีผลกระทบสำคัญต่อการพัฒนาและใช้งานอินเทอร์เน็ต[78]

[77] เพื่อความเข้าใจในประเด็นนี้อย่างละเอียด โปรดศึกษาต่อในเอกสาร Commission on Science and Technology for Development, Mapping of international Internet public : policy issues, E/CN.16/2015/CRP.2, 17 April 2015, https://unctad.org/system/files/official-document/ecn162015crp2_en.pdf และ เคอร์บาลิจา, โจวาน. อ้างแล้ว.

[78] Commission on Science and Technology for Development, Ibid., page 9.

เลเยอร์ที่สอง มาตรฐานทางเทคนิค (Technical standards) เป็นโครงสร้างพื้นฐานที่ทำให้อินเทอร์เน็ตสามารถทำงานได้ เช่น ทรานสมิชชันคอนโทรลโปรโตคอล/อินเทอร์เน็ตโปรโตคอล (Transmission Control Protocol/Internet Protocol) : TCP/IP) ระบบชื่อโดเมน (DNS) ซีเคียวร์ซ็อกเก็ตเลเยอร์ (secure sockets layer - SSL) และรูทเซิร์ฟเวอร์ (root server)

สถาปัตยกรรมของอินเทอร์เน็ตขึ้นอยู่กับชุดของมาตรฐานทางเทคนิค ซึ่ง TCP/IP เป็นพื้นฐานในการกำหนดเส้นทางและที่อยู่ของการรับส่งข้อมูลทางอินเทอร์เน็ต โดยอุปกรณ์ทุกเครื่องที่เชื่อมต่ออินเทอร์เน็ตจะมี IP (เช่น 216.191.141.45) ไม่ซ้ำกัน และจะมีระบบชื่อโดเมน (Domain Name System : DNS) ที่จะทำหน้าที่แปลที่อยู่ IP เป็นชื่อที่สามารถเข้าใจได้ง่ายกว่า (เช่น google.com)

มาตรฐาน TCP/IP ถูกกำหนดโดยคณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต (IETF) และได้รับการคุ้มครองที่เข้มงวด การเปลี่ยนแปลงใด ๆ ที่กระทำต่อ TCP/IP ต้องผ่านการอภิปรายล่วงหน้าอย่างรอบด้าน[79] โดยการตัดสินใจผ่านกระบวนการที่เปิดกว้างและอิงตามฉันทามติ[80]

ส่วนระบบการกระจายหมายเลข IP จะอยู่ภายใต้โครงสร้างการบริหารแบบลำดับชั้น โดยหน่วยงานส่วนบนสุดคือ IANA (Internet Assigned Numbers Authority) ซึ่งเป็นหน่วยงานย่อยของ ICANN (Internet Corporation for Assigned Names and Numbers) จะทำหน้าที่แจกจ่ายบล็อกของหมายเลข IP ตามระบบทะเบียนอินเทอร์เน็ตภูมิภาค (Regional Internet Registries (RIRs)) ทั้ง 5 แห่ง และ RIRs จะแจกจ่ายให้กับสำนักทะเบียนอินเทอร์เน็ตในพื้นที่ภูมิภาคของตน (LIR) และจะแจกจ่ายให้กับผู้ให้บริการอินเทอร์เน็ต (ISP) ต่อไป[81]

ภาพที่ 3.2 แผนที่ Regional Internet Registries (RIRs)

ที่มา: Regional Internet Registries (https://www.nro.net/about/rirs/)

[79] เคอร์บาลิจา, โจวาน. อ้างแล้ว. หน้า 54.

[80] Commission on Science and Technology for Development, Ibid., page 10.

[81] Commission on Science and Technology for Development, Ibid., page 12. ; https://www.nro.net/about/rirs/

เมื่อเดือนกุมภาพันธ์ 2554 (ค.ศ. 2011) หมายเลข IP ในระบบ IPv4 (อินเทอร์เน็ตโปรโตคอล รุ่น 4) ซึ่งมีอยู่ประมาณ 4.3 พันล้านรายการ ถูกจัดสรรให้กับ RIRs ทั้ง 5 แห่งจนหมดแล้ว ซึ่งเป็นผลจากการเพิ่มขึ้นของอุปกรณ์เชื่อมต่ออินเทอร์เน็ตใหม่ ๆ เป็นเหตุให้ชุมชนด้านเทคนิคต้องดำเนินการแก้ไขปัญหาดังกล่าว แนวทางแก้ไจประการหนึ่งคือการนำโปรโตคอล TCP/IP รุ่นใหม่หรือ IPv6 มาใช้ เพื่อขยายจำนวนที่อยู่ที่มีอยู่จาก 32 เป็น 128 บิต ซึ่งทำให้มีกลุ่มหมายเลข IP เพิ่มขึ้นมากถึง 340 พันล้านรายการ[82]

ส่วนระบบชื่อโดเมน (DNS) เป็นเหมือนกับสมุดโทรศัพท์สำหรับอินเทอร์เน็ต (address book)[83] ซึ่งจะแปลที่อยู่ IP ที่จำยาก เช่น 216.191.141.45 เป็นชื่อที่จำง่ายขึ้นเช่น www.google.com โดย DNS ประกอบด้วยรูทเซิร์ฟเวอร์ (root server) เซิร์ฟเวอร์ของโดเมนระดับบนสุด (top-level domain : TLD) และหมายเลขของเซิร์ฟเวอร์ ทั้งนี้ โดเมนระดับบนสุด หรือ TLD จะมีอยู่ 3 แบบ ได้แก่ แบบแรก โดเมนระดับบนสุดหมวดทั่วไป (generic : gTLD) เช่น .com, .info, .net และ.org แบบที่สอง คือ โดเมนระดับบนสุดตามอักษรย่อของแต่ละประเทศหรือดินแดน (country code : ccTLD) เช่น .uk, .cn, .in และแบบที่สามคือ ชื่อโดเมนแบบมีสปอนเซอร์ (sponsored : sTLD) ซึ่งถูกจำกัดเฉพาะบางกลุ่มเท่านั้น เช่น .aero เปิดให้ลงทะเบียนเฉพาะอุตสาหกรรมขนส่งทางอากาศ[84]

ท่ามกลางความพยายามในการสร้างชื่อโดเมนระดับบนสุดหมวดทั่วไป (gTLD) ใหม่ ๆ รวมถึงที่ไม่ใช่อักษรละติน ทำให้เกิดข้อถกเถียงและแรงต่อต้าน โดยเฉพาะในประเด็นเกี่ยวกับการคุ้มครองเครื่องหมายการค้า เป็นเหตุให้ ICANN จัดให้มีการปรึกษาหารือเพื่อออกแบบนโยบายใหม่ในประเด็นนี้ รวมถึงประเด็นเกี่ยวกับศีลธรรมทางสังคม เช่น กรณีการเสนอให้นำโดเมน .xxx มาใช้[85] ทั้งนี้ ในปี 2554 (ค.ศ. 2011) ICANN ได้อนุมัติโปรแกรม gTLD ใหม่ ซึ่งจะยุติข้อจำกัดส่วนใหญ่ใน gTLD และอนุญาตให้องค์กรต่าง ๆ สามารถใช้และเรียกใช้ gTLD ของตนได้ รวมถึง gTLD ในภาษาที่ไม่ใช่ภาษาละติน[86] โดยข้อมูล ณ เดือนมิถุนายน 2555 ICANN ได้รับใบสมัครสำหรับ gTLD ใหม่ จำนวน 1,930 รายการ อาทิ .blog, .shop, .apple, .books[87] บริษัทที่ส่งใบสมัครชำระค่าธรรมเนียมการสมัคร 185,000 ดอลลาร์สหรัฐให้กับ ICANN ค่าธรรมเนียมการสมัครทำให้เกิดข้อกังวลที่สำคัญ

---

[82] เคอร์บาลิจา, โจวาน. อ้างแล้ว. หน้า 55.

[83] European Digital Rights, 2012, ibid.

[84] Commission on Science and Technology for Development, Ibid., page 14.

[85] เคอร์บาลิจา, โจวาน. อ้างแล้ว. หน้า 59 – 60.

[86] James Seng. 2009. “Why ICANN TLD Policy Imposes Severe Constraint on Development of Internationalized Domain Names”. https://circleid.com/posts/20090720_icann_tld_policy_imposes_constraint_internationalized_domains/

[87] ETDA. ชื่อโดเมนระดับบนสุดแบบทั่วไปแบบใหม่ (New Generic Top Level Domains). https://www.etda.or.th/getattachment/f4b6163d-0411-4422-b1f3-9adc699d3b14/2-4-New-gTLDs_1-July-2014-Thai-V05-04(1).pdf.aspx?lang=th-TH

หลายประการเกี่ยวกับการแข่งขัน และ gTLD ใหม่สามารถสร้างความขัดแย้งระหว่างผู้สมัครทางภูมิศาสตร์และเชิงพาณิชย์ ดังเช่นกรณีที่ประเทศบราซิลและประเทศเปรูคัดค้านการประมูลของ Amazon สำหรับ .amazon[88]

ส่วนการบริหารจัดการโดเมนประเทศ (ccTLD) ก็มีข้อถกเถียงเช่นเดียวกัน โดยเฉพาะข้อถกเถียงด้านการเมือง ผู้ที่จะทำหน้าที่บริหารจัดการ รวมถึงประเด็นที่เกี่ยวข้องกับการที่ผู้บริหารโดเมนประเทศหลายแห่งไม่ประสงค์จะเป็นส่วนหนึ่งของระบบ ICANN ปัจจุบันผู้บริหารโดเมนประเทศมีการจัดตั้งเป็นกลุ่มระดับภูมิภาค (เช่น ยุโรป - CENTR แอฟริกา - AFTLD เอเชีย - APTLD อเมริกาเหนือ - NATLD และอเมริกาใต้ - LACTLD)[89]

ส่วนรูทเซิร์ฟเวอร์ (root server) ปัจจุบัน มีอยู่ 13 แห่ง ดำเนินการโดยองค์กรอิสระ 12 องค์กร ซึ่งตั้งอยู่ใน 4 ประเทศ โดยรูทเซิร์ฟเวอร์ 10 แห่งอยู่ในสหรัฐฯ และอยู่ในสวีเดน เนเธอร์แลนด์ และญี่ปุ่น ประเทศละหนึ่งแห่ง[90]

การกำกับดูแลรูทเซิร์ฟเวอร์เป็นหนึ่งในประเด็นที่มีการโต้เถียงกันมากที่สุดในการอภิปรายนโยบายอินเทอร์เน็ตระหว่างประเทศ ประเด็นหลักที่ยังมีมุมมองแตกต่างกันอยู่นั้นเป็นเรื่องเกี่ยวกับบทบาทของสหรัฐอเมริกาในการดูแลผ่านกระบวนการ IANA[91] หลายประเทศแสดงข้อกังวลเกี่ยวกับรูปแบบในปัจจุบัน ซึ่งทำให้ความรับผิดชอบหลักในการตัดสินใจเกี่ยวกับการจัดการเนื้อหาของรูทเซิร์ฟเวอร์ตกอยู่กับประเทศเดียว (สหรัฐอเมริกา) มีข้อเสนอหลายประการ รวมทั้งการรับรองอนุสัญญารูท (Root Convention) ซึ่งจะทำให้ประชาคมนานาชาติมีบทบาทกำกับดูแลนโยบายเกี่ยวกับรูทเซิร์ฟเวอร์[92]

<u>เลเยอร์ที่สาม</u> มาตรฐานเกี่ยวกับเนื้อหาและการใช้งาน เช่น ภาษา HTML (HyperText Markup Language) ภาษา XML (eXtensible Markup Language)

มาตรฐานเว็บ (Web standards) ถูกกำหนดโดย World Wide Web Consortium (W3C) ซึ่งเปิดให้สมาชิกภาพสำหรับองค์กรและบุคคลทุกประเภท มาตรฐานได้รับการพัฒนาผ่านกระบวนการที่เป็นเอกฉันท์อย่างละเอียดถี่ถ้วน และเผยแพร่ในฐานะข้อเสนอแนะของ W3C (W3C Recommendations)[93]

---

[88] Wats, J. 2013 “Amazon v the Amazon: internet retailer in domain name battle”. The Guardian. https://www.theguardian.com/environment/2013/apr/25/amazon-domain-name-battle-brazil

[89] เคอร์บาลิจา, โจวาน. อ้างแล้ว. หน้า 60 – 61.

[90] ดู รายชื่อเซอร์เวอร์รูตโซน ได้ที่ http://www.root-servers.org/

[91] Commission on Science and Technology for Development, Ibid., page 17.

[92] เคอร์บาลิจา, โจวาน. อ้างแล้ว. หน้า 63.

[93] Commission on Science and Technology for Development, Ibid., page 11.

เวิลด์ไวด์เว็บ (WWW) ถูกสร้างขึ้นโดยใช้รูปแบบภาษา HTML (HyperText Markup Language) เพื่ออำนวยความสะดวกในการแบ่งปันข้อมูล การแสดงเนื้อหา และการโต้ตอบกับเว็บ ซึ่ง HTML ได้รับการปรับปรุงเป็นประจำด้วยคุณลักษณะใหม่ (ปัจจุบัน HTML5) มาตรฐานเว็บทำให้มั่นใจได้ว่าเนื้อหาอินเทอร์เน็ตสามารถเข้าถึงได้และดูได้อย่างเหมาะสมด้วยแอปพลิเคชันอินเทอร์เน็ตส่วนใหญ่

ในยุคแรกของการคิดค้นระบบ WWW ขึ้นมา หรือที่เรียกว่า Web 1.0 นั้น เว็บยังไม่ได้มีความทันสมัยมากนัก และเป็นระบบที่ทำหน้าที่ให้ข้อมูลข่าวสารในรูปแบบสื่อสารทางเดียว ไม่สามารถโต้ตอบกันได้ คนที่จะสามารถแก้ไขหน้าตาเว็บไซต์ได้จะมีแต่เจ้าของเว็บไซต์ (Webmaster) เท่านั้น ต่อมาเว็บถูกพัฒนาให้สามารถสื่อสารได้สองทาง หรือที่เรียกว่า Web 2.0 ซึ่งทำให้เกิดสื่อสังคมออนไลน์ (Social media) และมีตัวกลาง เช่น Facebook (Meta), ทวิตเตอร์ (Twitter) เข้ามาทำหน้าที่คอยดูแลจัดการข้อมูลทั้งหมด อย่างไรก็ดี การสื่อสารทางสื่อสังคมออนไลน์ผ่านตัวกลาง ทำให้เกิดปัญหาบางประการ โดยเฉพาะการเซ็นเซอร์ ความเป็นส่วนตัวและการคุ้มครองข้อมูล จึงมีความพยายามที่จะพัฒนาไปสู่การกระจายอำนาจมากขึ้น (Decentralization) ทำให้เข้าสู่ยุคที่เรียกว่า Web 3.0[94]

มีการคาดการณ์ไว้ว่า Web 3.0 จะสามารถทำงานได้อัตโนมัติคล้ายมนุษย์ ฉลาดมากขึ้นและรองรับเทคโนโลยีอัจฉริยะอย่าง Machine Learning (ML), Big Data, AI, Blockchain และอื่น ๆ ได้ นอกจากนี้ Web 3.0 จะขจัดการควบคุมจากส่วนกลาง (Decentralization) และให้การควบคุมกลับมายังผู้ใช้ ปัจจุบันยังไม่มีการนำแนวคิดของ Web 3.0 มาใช้งานอย่างสมบูรณ์ในรูปแบบเน้นการกระจายอำนาจและไร้จุดศูนย์กลางอย่างแท้จริง สิ่งที่ใกล้เคียงแนวคิดของ Web 3.0 มากที่สุดในปัจจุบันอาจเป็นการใช้งานกุญแจส่วนบุคคล (Private Key) เงินดิจิทัล (Cryptocurrency) และโลกเสมือนจริง (Metaverse)[95]

กล่าวโดยสรุป จะเห็นได้ว่าการออกแบบ นโยบาย และแนวปฏิบัติที่เกี่ยวข้องของโครงสร้างพื้นฐานแต่ละเลเยอร์ แม้ส่วนใหญ่จะเป็นเรื่องทางเทคนิคและกำกับดูแลโดยหน่วยงานเชิงเทคนิค แต่จากข้อมูลข้างต้นแสดงให้เห็นถึงข้อถกเถียงและข้อเรียกร้องบางประการ โดยเฉพาะเกี่ยวกับกลไกการกำกับดูแลอินเทอร์เน็ตในระดับโลก โดยในเดือนตุลาคม 2556 มีการเคลื่อนไหวที่สำคัญ กล่าวคือ ICANN และองค์กรอินเทอร์เน็ตทางเทคนิคหลายแห่ง ได้แก่ Internet Activities Board, Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), Internet Society (ISOC) และ Regional Internet registries (RIR) ได้ออกคำชี้แจง

---

[94] https://web3.foundation/

[95] Techsauce, Web 3.0 คืออะไร ทำไมถึงเป็นอินเทอร์เน็ต The Next Era โครงสร้างพื้นฐานสำคัญ ในการสร้างจักรวาล Metaverse, https://techsauce.co/tech-and-biz/what-is-web-three-point-zero

เกี่ยวกับอนาคตของความร่วมมือทางอินเทอร์เน็ตของมอนเตวิเดโอ (Montevideo Statement on the Future of Internet Cooperation) ซึ่งกล่าวถึงความจำเป็นในการเสริมสร้างและพัฒนาความร่วมมือทางอินเทอร์เน็ตของผู้มีส่วนได้ส่วนเสียจากทั่วโลก[96]

จะเห็นได้ว่า การออกแบบ นโยบาย และการกำกับดูแลโครงสร้างพื้นฐานทางอินเทอร์เน็ต อาจมีผลกระทบทั้งในแง่บวกหรือแง่ลบต่อสิทธิมนุษยชน อาทิ การเข้าถึงและความเหลื่อมล้ำ ความปลอดภัยในโลกดิจิทัล เสรีภาพในการแสดงออก และการคุ้มครองความเป็นส่วนตัว โดยในส่วนถัดไปจะกล่าวถึงความพยายามในการปรับปรุงระบบการกำกับดูแลอินเทอร์เน็ตทั่วโลก

3.3 การอภิบาล/การกำกับดูแลอินเทอร์เน็ตระดับโลก (Internet Governance)

ระบบการกำกับดูแลอินเทอร์เน็ตมีความกว้างขวางและหลากหลาย โดยเกี่ยวข้องกับผู้ดำเนินการในระดับประเทศ ระดับภูมิภาค และระดับนานาชาติ ทั้งในภาครัฐ ภาคเอกชน สถาบันการศึกษาและภาคประชาสังคม แต่มีเพียงบางองค์กรที่เป็นผู้กำหนดและพัฒนามาตรฐานทางเทคนิคของอินเทอร์เน็ต โดยเฉพาะ ICANN ซึ่งกำหนดนโยบายสำหรับการจดทะเบียนชื่อโดเมนระดับบนสุด และอาจมีองค์กรอื่นที่มีบทบาทในการกำหนดนโยบาย เช่น สหภาพโทรคมนาคมระหว่างประเทศ (ITU) ซึ่งมีบทบาทในการพัฒนาและประสานงานนโยบายโทรคมนาคมทั่วโลก

การกำกับดูแลอินเทอร์เน็ตในช่วงต้น ส่วนใหญ่จะเกี่ยวข้องกับการจัดการมาตรฐานทางเทคนิค เช่น ชื่อโดเมน (DNS) ที่อยู่ IP และระบบรูตเซิร์ฟเวอร์ และถูกจัดการโดยชุมชนทางเทคนิค ซึ่งประเด็นต่างๆ จะได้รับการแก้ไขโดยฉันทามติแบบคร่าว ๆ และหลักปฏิบัติที่ได้รับการอธิบายว่าเป็น “การกำกับดูแลโดยปราศจากรัฐบาล”[97]

ในปี 2541 (ค.ศ. 1998) มีการก่อตั้ง ICANN ขึ้น ในฐานะองค์กรเอกชนที่ไม่แสวงหากำไรภายใต้กฎหมายของรัฐแคลิฟอร์เนีย โดยกระทรวงพาณิชย์ของสหรัฐฯ ยังคงกำกับดูแลผ่านบันทึกความเข้าใจ (MoU) เกี่ยวกับการจัดการโดเมนระดับบนสุด ซึ่งเป็นแกนหลักทางเทคนิคของอินเทอร์เน็ต

---

[96] ICANN. 2013. “Montevideo Statement on the Future of Internet Cooperation”. https://www.icann.org/en/announcements/details/montevideo-statement-on-the-future-of-internet-cooperation-7-10-2013-en

[97] Kleinwächter, Wolfgang (2008). Multi-Stakeholder Internet Governance: the Role of Governments. In: Benedek, Wolfgang; Bauer, Veronika and Kettemann, Matthias C. Internet governance and the information society, global perspectives and European dimensions, eleven international publishing, Utrecht, 9-30, 10ff

ความสัมพันธ์ดังกล่าว ทำให้เกิดการตั้งคำถามถึงความชอบธรรมของ ICANN ประกอบกับปัญหาใหม่ๆ ที่เกิดขึ้นจากอินเทอร์เน็ต ประเด็นการกำกับดูแลอินเทอร์เน็ตจึงกลายเป็นประเด็นที่ได้รับความสนใจในระดับโลก โดยเมื่อปี 2545 ที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติ (UNGA) ได้รับรองการเสนอให้มีการจัดประชุมสุดยอดโลกว่าด้วยสังคมข้อมูลข่าวสาร (World Summit on the Information Society (WSIS)) ซึ่งนำมาสู่การประชุม 2 ครั้ง ในปี 2546 (ค.ศ. 2003) และ 2548 (ค.ศ. 2005)[98] โดยประเด็นการกำกับดูแลอินเทอร์เน็ต เป็นหัวข้อสำคัญของ WSIS ด้วย

ในการประชุม WSIS ครั้งแรก ณ กรุงเจนีวา เมื่อปี 2546 (ค.ศ. 2003) นำไปสู่การจัดทำปฏิญญาเจนีวาของหลักการและแผนปฏิบัติการเจนีวา (the Geneva Declaration of Principles and Geneva Plan of Action) ซึ่งรับรองหลักการสำคัญของการมีส่วนร่วมในสังคมข้อมูลข่าวสารว่า “ทุกคน ในทุกที่ ควรมีโอกาสได้มีส่วนร่วม และไม่ควรมีใครถูกกีดกันจากการได้รับผลประโยชน์ที่สังคมข้อมูลข่าวสารเสนอให้”[99]

ปฏิญญาเจนีวาของหลักการ (Declaration of Principles) ได้ระบุถึงหลักการสิทธิมนุษยชนในฐานะองค์ประกอบสำคัญสำหรับการกำกับดูแลอินเทอร์เน็ต โดยเอกสารของ WSIS ได้แสดงให้เห็นแนวทางแบบองค์รวมในการปกป้องสิทธิมนุษยชนโดยอ้างถึงปฏิญญาสากลว่าด้วยสิทธิมนุษยชน[100] และเน้นย้ำแนวทางของผู้มีส่วนได้ส่วนเสียหลายฝ่ายในการกำกับดูแลอินเทอร์เน็ต ไว้ในข้อ 49[101] ว่า

> *“การจัดการอินเทอร์เน็ตครอบคลุมทั้งประเด็นทางเทคนิคและนโยบายสาธารณะ และควรเกี่ยวข้องกับผู้มีส่วนได้ส่วนเสียทั้งหมดและองค์กรระหว่างรัฐบาลและระหว่างประเทศที่เกี่ยวข้อง ในแง่นี้เป็นที่ยอมรับว่า*
>
> *a. อำนาจเชิงนโยบายสำหรับประเด็นนโยบายสาธารณะที่เกี่ยวข้องกับอินเทอร์เน็ตเป็นสิทธิอธิปไตยของรัฐ พวกเขามีสิทธิและความรับผิดชอบสำหรับประเด็นนโยบายสาธารณะที่เกี่ยวข้องกับอินเทอร์เน็ตระหว่างประเทศ*
>
> *b. ภาคเอกชนมีบทบาทสำคัญต่อการพัฒนาอินเทอร์เน็ตอย่างต่อเนื่องและควรดำเนินต่อไป ทั้งในด้านเทคนิคและเศรษฐกิจ*
>
> *c. ภาคประชาสังคมมีบทบาทสำคัญในเรื่องอินเทอร์เน็ต โดยเฉพาะในระดับชุมชนและควรมีบทบาทดังกล่าวต่อไป*

---

[98] UNGA resolution No 56/183 of 21 December 2001. World Summit on the Information Society

[99] Geneva Declaration of Principles, Building the Information Society: a global challenge in the new Millennium, WSIS-03/GENEVA/DOC/4-E, 12 December 2003

[100] Geneva Declaration of Principles 2003, paras. 1, 3; Tunis Commitment 2005) and para. 2

[101] Geneva Declaration of Principles, para. 49

d. องค์กรระหว่างรัฐบาลมีบทบาทและควรยังคงมีบทบาทอำนวยความสะดวกในการประสานงานด้านนโยบายสาธารณะที่เกี่ยวข้องกับอินเทอร์เน็ต

e. องค์กรระหว่างประเทศมีบทบาทและควรยังคงมีบทบาทสำคัญในการพัฒนามาตรฐานทางเทคนิคที่เกี่ยวข้องกับอินเทอร์เน็ตและนโยบายที่เกี่ยวข้อง

WSIS ครั้งแรก ยังนำมาสู่การตั้งคณะทำงานด้านการกำกับดูแลอินเทอร์เน็ต (Working Group on Internet Governance - WGIG) ซึ่งได้รับมอบหมายให้หารือเกี่ยวกับความเป็นไปได้ของการกำกับดูแลระหว่างประเทศเกี่ยวกับทรัพยากรอินเทอร์เน็ตที่สำคัญ ตลอดจนร่างข้อเสนอแนะสำหรับผู้มีอำนาจตัดสินใจทางการเมือง

การประชุม WSIS ครั้งที่สอง ณ เมืองตูนิส ได้มีการจัดทำเอกสารข้อตกลงของตูนิสและวาระตูนิสสำหรับสังคมข้อมูลข่าวสาร (Tunis Commitments and Tunis Agenda for the Information Society) โดยในส่วนของเอกสารวาระตูนิสสำหรับสังคมข้อมูลข่าวสาร (Tunis Agenda for the Information Society) ได้ให้คำจำกัดความเชิงปฏิบัติงานของธรรมาภิบาลอินเทอร์เน็ต (Internet Governance) ว่า

“การพัฒนาและการประยุกต์ใช้โดยรัฐบาล ภาคเอกชน และภาคประชาสังคม ในบทบาทที่เกี่ยวข้องกันของหลักการ บรรทัดฐาน กฎเกณฑ์ ขั้นตอนการตัดสินใจ และโปรแกรมร่วมกัน ที่หล่อหลอมวิวัฒนาการและการใช้อินเทอร์เน็ต”[102]

และในเอกสารฉบับเดียวกันนั้นยังได้เน้นย้ำถึงแนวทางและบทบาทของผู้มีส่วนได้เสียหลายฝ่าย[103] และยอมรับว่าการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียหลายฝ่ายมีความสำคัญต่อความสำเร็จของงคมข้อมูลข่าวสาร และยังได้เน้นย้ำถึงการสนับสนุนการพัฒนากระบวนการของผู้มีส่วนได้ส่วนเสียหลายฝ่ายในระดับชาติ ระดับภูมิภาค และระดับนานาชาติ เพื่อหารือและร่วมมือในการขยายและเผยแพร่อินเทอร์เน็ตเพื่อเป็นแนวทางในการสนับสนุนความพยายามในการพัฒนาเพื่อให้บรรลุเป้าหมายการพัฒนาที่ตกลงกันในระดับสากล[104]

ในการประชุม WSIS ครั้งที่สอง ยังได้มีการอภิปรายและเสนอทางเลือกในการจัดการปัญหานโยบายสาธารณะเกี่ยวกับอินเทอร์เน็ต โดยเสนอให้จัดเวทีการอภิปรายเกี่ยวกับการกำกับดูแลอินเทอร์เน็ต หรือ Internet Governance Forum (IGF) ขึ้น สำหรับผู้ที่เกี่ยวข้องกับอินเทอร์เน็ตในหลายระดับ โดยมีการนำเสนอแบบจำลองของการบริหารจัดการที่มีวิธีการปฏิบัติที่แตกต่างกันออกไป 4 แบบ ได้แก่

1) สร้างคณะมนตรีอินเทอร์เน็ตโลก (Global Internet Council (GIC)) อันประกอบด้วยรัฐบาลและผู้มีส่วนเกี่ยวข้องเพื่อเข้ารับบทบาทการกำกับดูแลแทนที่ ICANN

---

[102] Tunis Agenda for The Information Society, para 34.

[103] Tunis Agenda for The Information Society, para. 35

[104]Tunis Agenda for The Information Society, para. 80 and 97

2) ประกันว่าคณะกรรมการที่ปรึกษาของ ICANN จะเป็นเวทีทางการในการอภิปราย โดยการสนับสนุนจากรัฐบาลประเทศต่าง ๆ

3) ขจัดบทบาททางเทคนิคของ ICANN และก่อตั้งคณะมนตรีอินเทอร์เน็ตระหว่างประเทศ หรือ International Internet Council (IIC) เพื่อกำกับดูแลอินเทอร์เน็ต

4) ก่อตั้งหน่วยงานใหม่ ได้แก่ คณะมนตรีอินเทอร์เน็ตโลก (Global Internet Council (GIC)) เพื่อจัดการปัญหานโยบายสาธารณะเกี่ยวกับอินเทอร์เน็ต หน่วยงานอินเทอร์เน็ตโลกสำหรับการกำกับดูแลชื่อโดเมน (World Internet Corporation for Assigned Names and Numbers (WICANN)) เพื่อดำเนินงานแทนที่ ICANN และฟอรัมการกำกับดูแลอินเทอร์เน็ต (Global Internet Governance Forum (GIGF)) เพื่อเป็นเวทีศูนย์กลางในการอภิปรายโต้แย้งสำหรับรัฐบาล[105]

อย่างไรก็ดี แม้จะมีความพยายามอภิปรายเกี่ยวกับการกำกับดูแลอินเทอร์เน็ตอย่างกว้างขวาง แต่ก็ไม่ได้มีการเปลี่ยนแปลงการกำกับดูแลอินเทอร์เน็ตของ ICANN แต่อย่างใด

เพื่อหลีกเลี่ยงความล้มเหลว WSIS ได้มีการตกลงที่จะเพิ่มฟอรัมการกำกับดูแลอินเทอร์เน็ต (Internet Governance Forum (IGF)) ตามวาระของตูนิสสำหรับสังคมข้อมูล โดย IGF จะเป็นเวทีของผู้มีส่วนได้ส่วนเสียหลายฝ่าย (multi-stakeholder) ทั้งรัฐบาล องค์กรระหว่างรัฐบาล ธุรกิจ ภาคประชาสังคม และสถาบันการศึกษา ในการดำเนินการในประเด็นต่าง ๆ เกี่ยวกับการกำกับดูแลอินเทอร์เน็ต[106] โดย IGF จัดประชุมขึ้นครั้งแรกในปี 2549 (ค.ศ. 2006) ณ กรุงเอเธนส์ และได้มีการจัดเป็นประจำทุกปี อย่างไรก็ดี IGF ไม่ได้มีอำนาจในการตัดสินใจ มีเพียงบทบาทในการออกคำแนะนำที่ไม่ผูกมัดเท่านั้น[107]

IGF ได้ทำให้เกิด "กลุ่มพันธมิตรที่มีพลวัต (IGF Dynamic Coalition)" ซึ่งทำงานในแนวทางของผู้มีส่วนได้ส่วนเสียหลายฝ่ายในประเด็นที่เป็นปัญหาร่วมกัน เช่น เสรีภาพในการแสดงออก ความหลากหลายทางภาษา ความเป็นส่วนตัว เพศ ค่านิยมอินเทอร์เน็ตหลัก อินเทอร์เน็ตในทุกสิ่ง การเข้าถึงและความพิการ การเปลี่ยนแปลงสภาพภูมิอากาศ หรือการพัฒนา ตัวอย่างที่ดีสำหรับกลุ่มพันธมิตรที่แข็งขันซึ่งมีกิจกรรมเกี่ยวกับสิทธิมนุษยชน ได้แก่ Dynamic Coalition on Internet Rights and Principles (ปัจจุบันคือ Internet Rights and Principles Coalition) ซึ่งมีบทบาทสำคัญในการจัดทำกฎบัตรสิทธิมนุษยชนและหลักการสำหรับอินเทอร์เน็ต (Charter of Human Rights and Principles)[108]

---

[105] Report of the Working Group on Internet Governance (2015), https://www.wgig.org/docs/WGIGREPORT.pdf

[106] WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November 2005, para 72.

[107] https://www.intgovforum.org/en

[108] Internet Rights and Principles Coalition, Charter of Human Rights and Principles, http://internetrightsandprinciples.org/node/367

มีความพยายามในการผลักดันให้ IGF มีบทบาทที่แข็งแกร่งมากขึ้น ตัวอย่างของความพยายามดังกล่าวเช่น กลไกไตรภาคี ซึ่งประกอบด้วยอินเดีย บราซิล และแอฟริกาใต้ (IBSA) ได้เสนอการแก้ไขอาณัติเดิมของ IGF เพื่อให้มีผลลัพธ์เชิงเป้าหมายมากขึ้น มีความสามารถในการเสนอแนะเชิงนโยบาย มีสำนักเลขาธิการอยู่ภายในระบบ UN เป็นต้น[109]

แม้ดูเหมือนว่าจะมีฉันทามติบางอย่างเกิดขึ้นหลังจากการประชุม WSIS ทั้งสองครั้ง แต่ประเด็นการกำกับดูแลอินเทอร์เน็ตระดับโลกยังคงคลุมเครือและเป็นที่ถกเถียงกันอยู่ ในการประชุมระดับโลกว่าด้วยโทรคมนาคมระหว่างประเทศ (World Conference on International Telecoms : WCIT) เมื่อเดือนธันวาคม 2555 (ค.ศ. 2012) ณ นครดูไบ มีประเด็นที่ขัดแย้งกันอย่างมากเกี่ยวกับการลงมติที่ไม่มีผลผูกพันในการส่งเสริมบทบาทของ ITU ในการกำกับดูแลอินเทอร์เน็ต ซึ่งรัฐที่เข้าร่วมแตกออกเป็นสองฝ่ายใหญ่ ๆ ได้แก่ ประเทศตะวันตก ให้การสนับสนุนรูปแบบผู้มีส่วนได้ส่วนเสียหลายฝ่าย ในขณะที่อีกฝ่าย เช่น จีน รัสเซีย และกลุ่มประเทศอาหรับ ต่างมีแนวโน้มสนับสนุนรูปแบบที่หน่วยงานระหว่างรัฐบาลทำหน้าที่กำกับดูแล[110]

กล่าวโดยสรุป แม้ในระดับสากลจะยังเห็นไม่ตรงกันว่าการกำกับดูแลอินเทอร์จะประกอบด้วยหลักการและแนวทางแบบใดบ้าง แต่จากความคิดริเริ่มที่ผ่านมา ทั้งผลลัพธ์ของ WSIS และ IGF และข้อเสนอแนะของกลไกสิทธิมนุษยชนแห่งสหประชาชาติ ก็พอที่จะเป็นหลักการและแนวทางในการกำกับดูแลอินเทอร์เน็ต ดังนี้

1) การมีส่วนร่วมและแนวทางผู้มีส่วนได้ส่วนเสียหลายฝ่าย (Multi-Stakeholder Approach) ในการกำกับดูแลอินเทอร์เน็ตควรรับประกันการมีส่วนร่วมอย่างเต็มที่ของรัฐบาล ภาคเอกชน ภาคประชาสังคม ชุมชนด้านเทคนิค และผู้ใช้ โดยคำนึงถึงบทบาทและความรับผิดชอบเฉพาะของภาคส่วนต่าง ๆ อย่างเปิดเผย

2) หลักความโปร่งใสและการเปิดกว้าง กระบวนการตัดสินใจทั้งหมดที่เกี่ยวข้องกับการกำกับดูแลและการพัฒนาอินเทอร์เน็ตควรเป็นระบบเปิดและสามารถเข้าถึงได้

3) ยึดแนวทางสิทธิมนุษยชน (human rights-based approach) โดยใช้แนวทางที่ยึดหลักสิทธิมนุษยชนอย่างครอบคลุมในการออกแบบและบังคับใช้นโยบาย รวมถึงการกำกับดูแลอินเทอร์เน็ต ซึ่งถูกเน้นย้ำในรายงานปี 2551 (ค.ศ. 2008) ของผู้รายงานพิเศษแห่งสหประชาชาติว่าด้วยเสรีภาพในการแสดงออกฯ ซึ่งได้เสนอแนะให้จัดตั้งองค์กรระหว่างประเทศเพื่อกำกับดูแลอินเทอร์เน็ตด้วยแนวทางสิทธิมนุษยชน โดยให้มีหน้าที่ในการพัฒนาบรรทัดฐานและหลักการระดับโลกเพื่อรับประกันว่าอินเทอร์เน็ตจะสามารถพัฒนาเป็นสื่อกลางในการแสดงออกทางประชาธิปไตยที่สอดคล้องกับหลักสิทธิมนุษยชนอย่างครบถ้วน รวมถึงประกันเสรีภาพในการ

---

[109] Human Rights and Information and Communication Technology, Proceedings of the 12th Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights, 27 – 29 June 2012, Seoul, Republic of Korea, page 50.

[110] เคอร์บาลิจา, โจวาน. 2558. อ้างแล้ว. หน้า 21.

แสดงออก[111] และคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชนเน้นย้ำถึงความสำคัญของการใช้แนวทางที่ยึดหลักสิทธิมนุษยชนอย่างครอบคลุมในการจัดหาและขยายการเข้าถึงอินเทอร์เน็ตและเพื่อให้อินเทอร์เน็ตเปิดกว้างเข้าถึงได้[112]

3.4 กรอบแนวคิดสิทธิทางอินเทอร์เน็ต

การประกันการเข้าถึงอินเทอร์เน็ตถือว่ามีความจำเป็นอย่างยิ่งยุคปัจจุบัน เพราะการเข้าไม่ถึงอินเทอร์เน็ตอาจทำให้บุคคลนั้นไม่สามารถเข้าถึงหรือใช้สิทธิมนุษยชนอื่นได้ และสภาวะของการเข้าถึงอินเทอร์เน็ตที่แตกต่างกัน หรือมักถูกนิยามว่า “ความเหลื่อมล้ำทางดิจิทัล (Digital Divide)” นั้น ถือเป็นประเด็นที่สหประชาชาติให้ความสนใจ

ความเหลื่อมล้ำทางดิจิทัล หมายถึง “ช่องว่างระหว่างบุคคลที่เข้าถึงเทคโนโลยีดิจิทัลและข้อมูลสารสนเทศได้ กับผู้ที่เข้าถึงได้น้อยหรือไม่สามารถเข้าถึงได้เลย” [113] ซึ่งอาจเกิดจากสถานะทางเศรษฐกิจ เพศสภาพ ลักษณะทางภูมิศาสตร์และชนชั้นในสังคม คนในชนบทมักประสบปัญหาการเข้าถึงอินเทอร์เน็ต เนื่องจากขาดเทคโนโลยี สามารถเชื่อมต่ออินเทอร์เน็ตได้ช้า และ/หรือมีค่าใช้จ่ายสูง นอกจากนั้น กลุ่มผู้เสียเปรียบในสังคม เช่น คนพิการหรือชนกลุ่มน้อยด้านภาษา ก็มักประสบปัญหาการเข้าถึงอินเทอร์เน็ตเช่นกัน[114]

ปัจจุบัน สถานการณ์การเข้าถึงอินเทอร์เน็ตทั่วโลกมีแนวโน้มเพิ่มขึ้นต่อเนื่อง สหภาพโทรคมนาคมระหว่างประเทศ (ITU) ประมาณการว่าในปี 2565 ประชากรประมาณ 5.3 พันล้านคน หรือ 66 เปอร์เซ็นต์ของประชากรโลกกำลังใช้อินเทอร์เน็ต อย่างไรก็ดี ข้อมูลแสดงให้เห็นว่ามีประชากรประมาณ 2.7 พันล้านคนที่ยังคงอยู่ในภาวะที่เข้าไม่ถึงอินเทอร์เน็ต[115] ซึ่งข้อมูลจากรายงาน Global Connectivity Report 2022 ของ ITU แสดงให้เห็นว่าประชากรในประเทศกำลังพัฒนาส่วนใหญ่ยังเข้าไม่ถึงอินเทอร์เน็ต ทั้งยังมีความแตกต่างในการเข้าถึงระหว่างชนบทกับเมือง ระหว่างเพศหญิงกับชาย ระหว่างเด็กและผู้สูงอายุอายุ ระหว่างระดับการศึกษา[116]

สมัชชาใหญ่แห่งสหประชาชาติได้เน้นย้ำในหลายข้อมติถึงความจำเป็นในการลดความเหลื่อมล้ำทางดิจิทัลและประกันว่าทุกคนจะได้รับประโยชน์จากเทคโนโลยีใหม่[117] ส่วนคณะมนตรีสิทธิมนุษยชนเรียกร้อง

---

[111] Ambeyi Ligabo, A/HRC/7/14, 28 February 2008, para 74.

[112] A/HRC/RES/26/13, 14 July 2014 ; A/HRC/RES/32/13, 18 July 2016

[113] Frank La Rue, A/HRC/17/27, 16 May 2011, para 61.

[114] Ibid.

[115] https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[116] ITU. Global Connectivity Report 2022. https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/

[117] UN General Assembly, A/RES/63/202, 28 January 2009 ; A/RES/69/204, 21 January 2015

ให้รัฐต่าง ๆ พยายามลดความเหลื่อมล้ำทางดิจิทัลในรูปแบบต่าง ๆ รวมถึงด้วยเหตุแห่งเพศสภาพ[118] และอำนวยความสะดวกในการมีส่วนร่วมอย่างเท่าเทียมในการเข้าถึงและใช้เทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงอินเทอร์เน็ต[119]

ปัจจุบัน อินเทอร์เน็ตยังไม่ถูกรับรองว่าเป็นสิทธิมนุษยชนอย่างชัดเจนภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ แต่การเข้าถึงอินเทอร์เน็ตอย่างทั่วถึง ได้รับการกล่าวถึงบ่อยครั้งทั้งโดยกลไกของสหประชาชาติ หน่วยงานระดับภูมิภาค และภาคประชาสังคม

โดยในปี 2553 (ค.ศ. 2010) BBC World Service ได้สำรวจความคิดเห็นเกี่ยวกับสิทธิอินเทอร์เน็ต จากกลุ่มตัวอย่างที่เป็นผู้ใหญ่ 27,000 คนใน 26 ประเทศ ผลการสำรวจพบว่า เกือบ 4 ใน 5 คนทั่วโลก เห็นว่าการเข้าถึงอินเทอร์เน็ตควรเป็น “สิทธิ์พื้นฐานของทุกคน”[120]

อย่างไรก็ดี มีมุมมองที่แตกต่างกันอยู่บ้างว่าสิทธิในการเข้าถึงอินเทอร์เน็ตควรจะเป็นสิทธิมนุษยชนหรือไม่ โดย Vinton Cerf ผู้ร่วมสร้างโปรโตคอล TCP/IP ให้เหตุผลว่าเทคโนโลยีเป็นตัวเปิดทางของสิทธิ ไม่ใช่ตัวสิทธิ และเทคโนโลยี เช่น อินเทอร์เน็ต ไม่จำเป็นต้องถือเป็นสิทธิเนื่องจากเทคโนโลยีเปลี่ยนแปลงอยู่ตลอดเวลา แต่เขาเห็นว่าการเข้าถึงอินเทอร์เน็ตควรถือเป็นสิทธิพลเมือง[121]

นอกจากนี้ ยังมีข้อถกเถียงเกี่ยวกับมุมมองของการบรรลุถึงสิทธิดังกล่าว บางส่วนมองว่าสิทธิในการเข้าถึงอินเทอร์เน็ตไม่สามารถบรรลุผลสำหรับทุกคนในเวลาอันสั้น อย่างไรก็ตาม มีข้อเสนอว่าสิทธิมนุษยชนในลักษณะของการเข้าถึง ไม่จำเป็นต้องดำเนินการอย่างครบถ้วนในทันที ดังเช่นแนวปฏิบัติของกติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม (ICESCR) ซึ่งใช้แนวทางการบรรลุสิทธิแบบค่อยเป็นค่อยไป (approach of progressive realisation) [122] ดังนั้น การเข้าถึงอินเทอร์เน็ต ก็อาจใช้แนวทางดังกล่าวได้เช่นกัน

คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ ได้เน้นย้ำในหลายข้อมติเกี่ยวกับการส่งเสริมคุ้มครองและการใช้สิทธิมนุษยชนเกี่ยวกับอิเทอร์เน็ต ถึงความสำคัญของการปรับใช้แนวทางสิทธิมนุษยชนที่ครอบคลุม (a comprehensive human rights-based approach) ในการจัดหาและขยายการเข้าถึง

---

[118] Human Rights Council, A/HRC/RES/32/13, 18 July 2016

[119] Human Rights Council, A/HRC/RES/12/16, 12 October 2009, para. 5 (m).

[120] BBC. “Is access to the internet a fundamental human right?”. 8 March 2010., https://www.bbc.co.uk/blogs/haveyoursay/2010/03/is_access_to_the_internet_a_fu.html

[121] Cerf, Vint (2012). Internet Access is not a Human Right. In: New York Times, https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html

[122] Human Rights and Information and Communication Technology, Proceedings of the 12th Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights, 27 – 29 June 2012, Seoul, Republic of Korea, page 58.

อินเทอร์เน็ต ซึ่งเป็นแรงผลักดันไปสู่การพัฒนาในรูปแบบต่างๆ ช่วยอำนวยให้การพัฒนาและนวัตกรรม การส่งเสริมการใช้สิทธิมนุษยชน รวมถึงการพัฒนาที่ยั่งยืน[123]

ในคำแถลงร่วมปี 2554 (ค.ศ. 2011) ของผู้เชี่ยวชาญด้านเสรีภาพในการแสดงออกฯ ได้กล่าวถึงหลักการ “การเข้าถึงอินเทอร์เน็ต” โดยเรียกร้องให้รัฐดำเนินการตามพันธกรณีเชิงบวกในการอำนวยความสะดวกในการเข้าถึงอินเทอร์เน็ตอย่างทั่วถึง อย่างน้อยที่สุด รัฐควรดำเนินการดังต่อไปนี้[124]

- วางกลไกการกำกับดูแล ซึ่งรวมถึงระบบการกำหนดราคา ข้อกำหนดด้านการบริการสากล (Universal Services) และข้อตกลงใบอนุญาตที่ส่งเสริมการเข้าถึงอินเทอร์เน็ตให้มากขึ้น รวมถึงการเข้าถึงปลายทาง (last mile) สำหรับคนยากจนและในพื้นที่ชนบท
- จัดหาการสนับสนุนโดยตรงเพื่ออำนวยความสะดวกในการเข้าถึง รวมถึงการจัดตั้งศูนย์ ICT ชุมชนและจุดเข้าถึงสาธารณะอื่นๆ
- ส่งเสริมความตระหนักรู้อย่างเพียงพอเกี่ยวกับวิธีการใช้อินเทอร์เน็ตและประโยชน์ที่จะได้รับ โดยเฉพาะอย่างยิ่งในหมู่คนยากจน เด็ก ผู้สูงอายุ และประชากรในชนบทห่างไกล
- กำหนดมาตรการพิเศษเพื่อให้คนพิการและผู้ด้อยโอกาสสามารถเข้าถึงอินเทอร์เน็ตได้อย่างเท่าเทียมกัน

ในการดำเนินการข้างต้น คำแถลงร่วมดังกล่าวเสนอให้รัฐใช้แผนปฏิบัติการระยะเวลาหลายปีและรายละเอียดเพื่อเพิ่มการเข้าถึงอินเทอร์เน็ต รวมถึงกำหนดเป้าหมายที่ชัดเจนและเฉพาะเจาะจง ตลอดจนมีมาตรฐานของความโปร่งใส มีระบบการรายงานต่อสาธารณะและสามารถตรวจสอบได้

ทำนองเดียวกัน ในรายงานปี 2554 (ค.ศ. 2011) ผู้รายงานพิเศษว่าด้วยเสรีภาพในการแสดงออกฯ ย้ำว่ารัฐควรปรับใช้นโยบายและยุทธศาสตร์ที่มีประสิทธิผลและเป็นรูปธรรม ซึ่งพัฒนาขึ้นด้วยการปรึกษาหารือกับทุกภาคส่วนของสังคม เพื่อทำให้อินเทอร์เน็ตสามารถใช้ประโยชน์ได้อย่างกว้างขวาง เข้าถึงได้ และสามารถจ่ายได้สำหรับทุกคน[125]

---

[123] A/HRC/RES/20/8, para. 2.; A/HRC/RES/26/13, para. 2.; A/HRC/RES/28/16 ; A/HRC/RES/32/13, para. 2. ; UN General Assembly, A/RES/68/167, para. 2.; A/RES/69/166, para. 2. ; A/RES/71/199, para. 2.; UN General Assembly, A/RES/73/179, para. 2.

[124] Joint declaration on freedom of expression and the internet, 1 June 2011, https://www.osce.org/files/f/documents/e/9/78309.pdf

[125] A/66/290, para. 63.

นอกจากนี้ ประเด็นการเข้าถึงอินเทอร์เน็ต ยังถูกรวมเข้าเป็นส่วนหนึ่งของเป้าหมายการพัฒนาที่ยั่งยืน (SDGs) โดยเฉพาะในเป้าหมายที่ 9.C ซึ่งกำหนดให้ “เพิ่มการเข้าถึงเทคโนโลยีด้านข้อมูลและการสื่อสาร และพยายามที่จะจัดให้มีการเข้าถึงอินเทอร์เน็ตโดยถ้วนหน้าและในราคาที่สามารถจ่ายได้ ในประเทศพัฒนาน้อยที่สุดภายในปี 2563”

ในส่วนของการริเริ่มโดยภาคประชาสังคม ในปี 2546 (ค.ศ. 2006) Association for Progressive Communications (APC)[126] ได้เผยแพร่กฎบัตรสิทธิทางอินเทอร์เน็ต (APC Internet Rights Charter) ซึ่งร่างขึ้นด้วยแรงบันดาลใจจากกฎหมายสิทธิมนุษยชนระหว่างประเทศหลายฉบับ โดยกฎบัตรดังกล่าวได้รับรองการเข้าถึงอินเทอร์เน็ตสำหรับทุกคน ซึ่งประกอบด้วยเนื้อหา ได้แก่ 1. การพัฒนาและความยุติธรรมทางสังคม 2. สิทธิในการเข้าถึงโครงสร้างพื้นฐาน 3. สิทธิในทักษะเพื่อใช้และกำหนดรูปแบบอินเทอร์เน็ต 4. สิทธิในอินเทอร์เฟซ (interface) เนื้อหา และแอปพลิเคชันที่ออกแบบมาสำหรับทุกคน (inclusive design) 5. สิทธิในการเข้าถึงที่เท่าเทียมกันสำหรับชายและหญิง 6. สิทธิในการเข้าถึงในราคาที่ไม่แพง 7. สิทธิในการเข้าถึงในสถานที่ทำงาน 8. สิทธิในการเข้าถึงในพื้นที่สาธารณะ และ 9. สิทธิในการเข้าถึงและสร้างเนื้อหาที่มีความหลากหลายทางวัฒนธรรมและภาษา[127]

และในปี 2553 (ค.ศ. 2010) กลุ่มพันธมิตรที่มีพลวัตว่าด้วยสิทธิและหลักการทางอินเทอร์เน็ต (The Internet Rights and Principles Dynamic Coalition)[128] ได้จัดทำเอกสารที่เรียกว่า “10 Internet Rights & Principles”[129] ซึ่งกำหนดสิทธิและหลักการสำคัญ 10 ประการสำหรับการกำกับดูแลอินเทอร์เน็ต และในปี 2554 (ค.ศ. 2011) ได้จัดทำกฎบัตรสิทธิมนุษยชนและหลักการสำหรับอินเทอร์เน็ต (The Charter of Human Rights and Principles for the Internet) ซึ่งมีจำนวน 21 ข้อ เกือบทั้งหมดเชื่อมโยงกับบรรทัดฐานด้านสิทธิมนุษยชนที่มีอยู่ โดยเฉพาะปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (UDHR) สิทธิเดียวที่อาจถือได้ว่าเป็นสิทธิใหม่คือสิทธิในการเข้าถึงอินเทอร์เน็ต (มาตรา 1) ซึ่งประกอบด้วย a) คุณภาพการบริการ b) เสรีภาพในการเลือกใช้ระบบ

---

[126] เป็นสมาคมไม่แสวงหาผลกำไรของเครือข่ายสมาชิกและพันธมิตรทั่วโลก มุ่งมั่นที่จะทำให้อินเทอร์เน็ตตอบสนองความต้องการของภาคประชาสังคมทั่วโลก

[127] APC Internet Rights Charter, https://www.apc.org/en/pubs/about-apc/apc-internet-rights-charter

[128] เครือข่ายแบบเปิดของบุคคลและองค์กรใน UN Internet Governance Forum (IGF) ซึ่งทำงานเพื่อรักษาสิทธิมนุษยชนในสภาพแวดล้อมอินเทอร์เน็ต, https://internetrightsandprinciples.org/

[129] 10 Internet Rights & Principles, https://drive.google.com/file/d/1MKByykdwe1Om1y_J6vXWVyIkZ6kSAII9/view

และซอฟแวร์ c) การประกันการนับรวมทางดิจิทัล (digital inclusion) และ d) ความเป็นกลางทางเน็ตและความเท่าเทียมทางเน็ต (Net neutrality and net equality)[130]

ในระดับประเทศ การเข้าถึงอินเทอร์เน็ตได้รับการยอมรับอย่างชัดแจ้งว่าเป็นสิทธิในรัฐที่พัฒนาแล้วบางแห่ง ดังที่เห็นได้จากการศึกษาของ OSCE พบว่ามีหลายประเทศในยุโรปที่มีกฎหมายรับรองการเข้าถึงอินเทอร์เน็ต[131] อาทิ ปี 2552 (ค.ศ. 2009) ฟินแลนด์ได้ผ่านพระราชกฤษฎีกา ระบุว่าความเร็วในการเชื่อมต่ออินเทอร์เน็ตทุกครั้งจะต้องไม่น้อยกว่า 1 เมกะบิทต่อวินาที (บรอดแบนด์)[132] และปี 2554 (ค.ศ. 2011) สเปนผ่านกฎหมายชื่อ The Law No. 2/11 of March 2011, Sustainable Economy ได้รวมการเชื่อมต่อบรอดแบนด์เป็นส่วนหนึ่งของบริการสากลที่อนุญาตให้มีการสื่อสารข้อมูลด้วยความเร็ว 1 เมกะบิตต่อวินาที[133]

กล่าวโดยสรุป ตราสารสิทธิมนุษยชนระหว่างประเทศยังไม่ได้รับรองอย่างชัดแจ้งว่าการเข้าถึงอินเทอร์เน็ตมีฐานะเป็นสิทธิมนุษยชน แต่ที่ผ่านมามีความพยายามจากหลายภาคส่วนในการรับรองและคุ้มครองสิทธิในการเข้าถึงอินเทอร์เน็ต ไม่ว่าจะโดยการตีความของกลไกสิทธิมนุษยชนของสหประชาชาติ โดยการเชื่อมโยงการเข้าถึงอินเทอร์เน็ตกับสิทธิมนุษยชนที่ปรากฏในตราสารด้านสิทธิมนุษยชนระหว่างประเทศที่มีอยู่แล้ว โดยเฉพาะเสรีภาพในการแสดงออก นอกจากนี้ บางประเทศ โดยเฉพาะประเทศที่พัฒนาทางเศรษฐกิจแล้ว ได้รับรองสิทธิในการเข้าถึงอินเทอร์เน็ตในกฎหมายระดับชาติ

---

[130]The Charter of Human Rights and Principles for the Internet, https://drive.google.com/file/d/1dyhXJLBLKJ0v_0sUHHRNEaUzKzp2dFr_/view

[131] OSCE (2011): The Office of the Representative on Freedom of the Media, Report on Freedom of Expression on the Internet, Study of legal provisions and practices related to freedom of expression, the free low of information and media pluralism on the Internet in OSCE participating states. Vienna, http://www.osce.org/fom/80723

[132] "732/2009, Decree of the Ministry of Transport and Communications on the minimum rate of a functional Internet access as a universal service," FINLEX, 22 October 2009., https://www.finlex.fi/en/laki/kaannokset/2009/en20090732.pdf

[133] Article 52 of The Law No. 2/11 of March 2011, Sustainable Economy, http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-4117

3.5 สิทธิในทางอินเทอร์เน็ตในประเทศไทย

3.5.1 กรอบกฎหมายและนโยบายที่เกี่ยวข้องกับการเข้าถึงอินเทอร์เน็ตในประเทศไทย

1) รัฐธรรมนูญแห่งราชอาณาจักรไทย

ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 หมวดหน้าที่ของรัฐ มาตรา 56 ระบุว่า

"รัฐต้องจัดหรือดำเนินการให้มีสาธารณูปโภคขั้นพื้นฐานที่จำเป็นต่อการดำรงชีวิตของประชาชนอย่างทั่วถึงตามหลักการพัฒนาอย่างยั่งยืน

โครงสร้างหรือโครงข่ายขั้นพื้นฐานของกิจการสาธารณูปโภคขั้นพื้นฐานของรัฐอันจำเป็นต่อการดำรงชีวิตของประชาชนหรือเพื่อความมั่นคงของรัฐ รัฐจะกระทำด้วยประการใดให้ตกเป็นกรรมสิทธิ์ของเอกชนหรือทำให้รัฐเป็นเจ้าของน้อยกว่าร้อยละห้าสิบเอ็ดมิได้

การจัดหรือดำเนินการให้มีสาธารณูปโภคตามวรรคหนึ่งหรือวรรคสอง รัฐต้องดูแลมิให้มีการเรียกเก็บค่าบริการจนเป็นภาระแก่ประชาชนเกินสมควร

การนำสาธารณูปโภคของรัฐไปให้เอกชนดำเนินการทางธุรกิจไม่ว่าด้วยประการใด ๆ รัฐต้องได้รับประโยชน์ตอบแทนอย่างเป็นธรรม โดยคำนึงถึงการลงทุนของรัฐ ประโยชน์ที่รัฐและเอกชนจะได้รับและค่าบริการที่จะเรียกเก็บจากประชาชนประกอบกัน

แม้รัฐธรรมนูญแห่งราชอาณาจักรไทยจะไม่ได้บัญญัติรับรองสิทธิในการเข้าถึงอินเทอร์เน็ตไว้อย่างชัดแจ้ง แต่เมื่อพิจารณามาตรา 56 ข้างต้น ซึ่งกำหนดให้รัฐมีหน้าที่ "ต้องจัดหรือดำเนินการให้มีสาธารณูปโภคขั้นพื้นฐานที่จำเป็นต่อการดำรงชีวิตของประชาชนอย่างทั่วถึงตามหลักการพัฒนาอย่างยั่งยืน" ประเด็นที่ต้องพิจารณาคือว่า อินเทอร์เน็ตถือว่าเป็น "สาธารณูปโภคขั้นพื้นฐานที่จำเป็นต่อการดำรงชีวิตของประชาชน" หรือไม่ หากเป็น ย่อมเป็นหน้าที่ของรัฐที่จะต้องจัดหาให้กับประชาชนอย่างทั่วถึง หากรัฐไม่ดำเนินการ และถ้าการนั้นเป็นการทำเพื่อให้เกิดประโยชน์แก่ประชาชนโดยตรง ก็ย่อมเป็นสิทธิของประชาชนที่จะติดตามและเร่งรัดให้รัฐดำเนินการ รวมตลอดทั้งฟ้องร้องหน่วยงานของรัฐที่เกี่ยวข้อง เพื่อจัดให้ประชาชนได้รับประโยชน์นั้น[134]

เมื่อพิจารณาจากนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 – 2580) มีหลายส่วนที่ระบุถึงอินเทอร์เน็ตความเร็วสูงจะกลายเป็นสาธารณูปโภคขั้นพื้นฐาน[135] ซึ่ง

---

[134] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 51

[135] นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 – 2580), หน้า 3, 15, 20, 25.

อาจจะตีความได้ว่า ในฐานะของนโยบายรัฐนั้น “อินเทอร์เน็ต” ถือเป็น “สาธารณูปโภคขั้นพื้นฐาน” อย่างหนึ่ง แต่ยังไม่ชัดเจนว่าเป็นสาธารณูปโภคขั้นพื้นฐานที่จำเป็นต่อการดำรงชีวิตของประชาชนหรือไม่

2) กฎหมายระกับพระราชบัญญัติ

ประเทศไทยยังไม่มีการรับรองสิทธิในการเข้าถึงอินเทอร์เน็ตไว้ชัดเจนไว้ในกฎหมายระดับพระราชบัญญัติ แต่มีกฎหมายบางฉบับที่กำหนดให้มีการพัฒนาโครงข่ายพื้นฐานด้านคมนาคม รวมถึงอินเทอร์เน็ต เพื่อให้ทุกคนสามารถเข้าถึงได้และในราคาที่ไม่แพง โดยกฎหมายฉบับหลัก ๆ ได้แก่ พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์และกิจการโทรคมนาคม พ.ศ. 2553 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 และ (ฉบับที่ 3) พ.ศ. 2562 (ต่อไปนี้เรียก พ.ร.บ. กสทช.ฯ) และพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 (ต่อไปนี้เรียก พ.ร.บ. โทรคมนาคมฯ)

<u>การเข้าถึงสำหรับทุกคน</u>

พ.ร.บ. กสทช.ฯ มาตรา 27 (13) กำหนดให้ กสทช. มีอำนาจหน้าที่ในการส่งเสริมสิทธิเสรีภาพและความเสมอภาคของประชาชนในการเข้าถึงและใช้ประโยชน์คลื่นความถี่ที่ใช้ในกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม

และ พ.ร.บ. กสทช.ฯ มาตรา 27 (12) กำหนดให้ กสทช. มีอำนาจหน้าที่ในการกำหนดมาตรการให้มีการกระจายบริการด้านโทรคมนาคมให้ทั่วถึงและเท่าเทียมกันตามมาตรา 50

โดยมาตรา 50 ของ พ.ร.บ. กสทช.ฯ กำหนดว่า *“เพื่อประโยชน์ในการจัดให้มีบริการโทรคมนาคมพื้นฐานโดยทั่วถึงและบริการเพื่อสังคมตามกฎหมายว่าด้วยการประกอบกิจการโทรคมนาคม ให้ กสทช. กำหนดแผนการจัดให้มีบริการโทรคมนาคมพื้นฐานโดยทั่วถึงและบริการเพื่อสังคม โดยในแผนอย่างน้อยจะต้องกำหนดพื้นที่และกลุ่มเป้าหมาย ระยะเวลาในการดำเนินการ พร้อมทั้งประมาณการค่าใช้จ่ายที่จะเกิดขึ้นจากการดำเนินการดังกล่าว”*

มาตรา 50 ดังกล่าว เป็นบทบัญญัติเรื่องการบริการสากล (Universal Service) ซึ่งถูกระบุไว้ทั้งใน พ.ร.บ. กสทช.ฯ และ พ.ร.บ. โทรคมนาคมฯ โดย พ.ร.บ. โทรคมนาคมฯ กำหนดให้คณะกรรมการ (ปัจจุบันคือ กสทช.) มีหน้าที่จัดให้มีการบริการโทรคมนาคมพื้นฐานโดยทั่วถึง และให้มีอำนาจกำหนดให้ผู้รับใบอนุญาตต้องจัดให้มีการบริการโทรคมนาคมดังต่อไปนี้ด้วย[136]

[136] พ.ร.บ. การประกอบกิจการโทรคมนาคมฯ 17.

(1) จัดให้มีบริการโทรคมนาคมในพื้นที่ชนบท หรือพื้นที่ที่มีผลตอบแทนการลงทุนต่ำ หรือท้องที่หนึ่งท้องที่ใดที่ยังไม่มีผู้ให้บริการหรือมีแต่ไม่ทั่วถึงหรือไม่เพียงพอแก่ความต้องการของผู้ใช้บริการในท้องที่นั้น

(2) จัดให้มีบริการโทรคมนาคมสำหรับสถานศึกษา ศาสนสถาน สถานพยาบาล และหน่วยงานอื่นที่ให้ความช่วยเหลือแก่สังคม

(3) จัดให้มีบริการโทรคมนาคมสาธารณะในบางลักษณะหรือบางประเภทตามที่คณะกรรมการกำหนดแก่ผู้มีรายได้น้อย

(4) จัดให้มีการให้บริการอำนวยความสะดวกในการใช้บริการโทรคมนาคมสาธารณะสำหรับคนพิการ เด็ก คนชรา และผู้ด้อยโอกาสในสังคม

ในกรณีที่ผู้รับใบอนุญาตใดไม่สามารถจัดให้มีบริการโทรคมนาคมตามที่กำหนดข้างต้นได้ หรือในกรณีที่เห็นสมควรให้ผู้รับใบอนุญาตมีส่วนร่วมรับผิดชอบในการจัดให้มีบริการโทรคมนาคมพื้นฐานโดยทั่วถึง ให้คณะกรรมการมีอำนาจกำหนดให้ผู้รับใบอนุญาตนั้นต้องจัดสรรรายได้ที่ได้รับจากการให้บริการโทรคมนาคมให้แก่กองทุนพัฒนากิจการโทรคมนาคมเพื่อประโยชน์สาธารณะตาม พ.ร.บ. กสทช. เพื่อนำไปดำเนินการจัดให้มีการบริการโทรคมนาคมพื้นฐานโดยทั่วถึง[137]

ทั้งนี้ ตาม พ.ร.บ. กสทชฯ กำหนดให้จัดตั้งกองทุนขึ้นในสำนักงาน กสทช. เรียกว่า “กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ” โดยมีวัตถุประสงค์ประการหนึ่งเพื่อ “ดำเนินการให้ประชาชนได้รับบริการด้านกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม อย่างทั่วถึง” และ “ส่งเสริมและสนับสนุนความสามารถในการรู้เท่าทันสื่อเทคโนโลยีด้านการใช้คลื่นความถี่ เทคโนโลยีสารสนเทศ เทคโนโลยีสิ่งอำนวยความสะดวกสำหรับผู้พิการ ผู้สูงอายุ หรือผู้ด้อยโอกาส ตลอดจนอุตสาหกรรมโทรคมนาคม และอุตสาหกรรมต่อเนื่อง”[138]

<u>การเข้าถึงในราคาที่ไม่แพง</u>

พ.ร.บ. กสทช.ฯ มาตรา 27 กำหนดหน้าที่และอำนาจของ กสทช. ในประเด็นเกี่ยวกับการกำกับดูแลด้านราคาค่าบริการโทรคมนาคมไว้ดังนี้

- พิจารณาอนุญาตและกำกับดูแลการประกอบกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อให้ผู้ใช้บริการได้รับบริการที่มีคุณภาพ ประสิทธิภาพ รวดเร็ว ถูกต้อง และเป็นธรรม

[137] พ.ร.บ. การประกอบกิจการโทรคมนาคมฯ 18. และโปรดดู พ.ร.บ. กสทชฯ มาตรา 50 วรรคสองและสาม

[138] พ.ร.บ. กสทชฯ มาตรา 52

- กำหนดหลักเกณฑ์และวิธีการในการกำหนดอัตราค่าใช้หรือค่าเชื่อมต่อโครงข่ายในการประกอบกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม ให้เป็นธรรมต่อผู้ใช้บริการ โดยคำนึงถึงประโยชน์สาธารณะเป็นสำคัญ[139]
- กำหนดโครงสร้างอัตราค่าธรรมเนียมและโครงสร้างอัตราค่าบริการในกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม ให้เป็นธรรมต่อผู้ใช้บริการและผู้ให้บริการโดยคำนึงถึงประโยชน์สาธารณะเป็นสำคัญ

3) กรอบนโยบายระดับชาติ

กรอบนโยบายระดับชาติ โดยเฉพาะยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 – 2580) แผนแม่บทภายใต้ยุทธศาสตร์ชาติ แผนปฏิรูปประเทศ แผนแม่บทกิจการโทรคมนาคม ฉบับที่ 2 (พ.ศ. 2562 - 2566) และนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 – 2580) มีการกำหนดประเด็นเกี่ยวกับการเข้าถึงอินเทอร์เน็ตไว้ดังนี้

<u>ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 – 2580)</u>

มียุทธศาสตร์ที่เกี่ยวข้องกับส่งเสริมการเข้าถึงอินเทอร์เน็ตในหลายยุทธศาสตร์ โดยเฉพาะในมิติการพัฒนาโครงสร้างพื้นฐาน และการส่งเสริมการรู้ดิจิทัล ดังนี้

- ยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน ในประเด็นการพัฒนาโครงสร้างพื้นฐานเทคโนโลยีสมัยใหม่ ระบุถึงการเสริมสร้างความรู้และโอกาสในการเข้าถึงโครงข่ายบรอดแบนด์หลากรูปแบบตามความเหมาะสมของพื้นที่ รวมถึงการวางกรอบในการจัดการทรัพยากรคลื่นความถี่ให้เพียงพอรองรับบริการที่มีคุณภาพในราคาที่ประชาชนทั่วไปเข้าถึงได้[140]
- ยุทธศาสตร์ชาติด้านการสร้างโอกาสและความเสมอภาคทางสังคม ในประเด็นการพัฒนาศูนย์กลางความเจริญทางเศรษฐกิจ สังคม และเทคโนโลยีในภูมิภาค ระบุว่า “กระจายโครงสร้างพื้นฐานด้านเทคโนโลยี คมนาคมและการสื่อสาร เพื่อให้ประชาชนสามารถพึ่งตนเองได้ภายในกลุ่มจังหวัด[141]

<u>แผนแม่บทภายใต้ยุทธศาสตร์ชาติ</u>

---

[139] โปรดดู พ.ร.บ. กสทชฯ มาตรา 29 เพิ่มเติม

[140] ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 – 2580). หน้า 27.

[141] ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 – 2580). หน้า 40 – 41.

แผนแม่บทภายใต้ยุทธศาสตร์ชาติ (7) ประเด็น โครงสร้างพื้นฐาน ระบบโลจิสติกส์ และดิจิทัล (พ.ศ. 2561 - 2580) ในแผนย่อยโครงสร้างพื้นฐานด้านดิจิทัล กำหนดแนวทางในการพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลทั้งในส่วนของโครงข่ายสื่อสารหลักภายในประเทศและโครงข่ายบรอดแบรนด์ความเร็วสูงให้ครอบคลุมทั่วประเทศ พร้อมทั้งกำหนดรูปแบบ สถาปัตยกรรมโครงข่ายให้สามารถเชื่อมต่อถึงกันได้ในลักษณะโครงข่ายเชื่อมต่อแบบเปิด ให้เป็นโครงข่ายเดียวสามารถให้บริการประชาชนอย่างมีคุณภาพและทั่วถึง โดยกำหนดเป้าหมายและตัวชี้วัดเมื่อสิ้นสุดแผน (ปี 2580) ให้ประชาชนสามารถเข้าถึงอินเทอร์เน็ตมากขึ้น ร้อยละ 95[142]

นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม เกิดขึ้นตามพระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560 ถือเป็นนโยบายหลักในการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศ โดยนโยบายและแผนดังกล่าวได้ระบุถึงปัญหาความเหลื่อมล้ำทางดิจิทัล (Digital Divide) รวมถึงความเหลื่อมล้ำในการเข้าถึงโครงสร้างพื้นฐานด้านอินเทอร์เน็ต[143] ความเหลื่อมล้ำทางด้านเนื้อหา (Content Divide)[144] รวมถึงรับรู้ถึงสถานการณ์ด้านราคาค่าบริการอินเทอร์เน็ตความเร็วสูงที่ยังสูงกว่าประเทศเพื่อนบ้าน[145]

ในเป้าหมายที่ 2 ของนโยบายและแผนฯ ระบุถึงการสร้างโอกาสทางสังคมอย่างเท่าเทียม โดยกำหนดตัวชี้วัดให้ “ประชาชนทุกคนต้องสามารถเข้าถึงอินเทอร์เน็ตความเร็วสูงเสมือนเป็นสาธารณูปโภคพื้นฐานประเภทหนึ่ง” ทั้งนี้ ได้กำหนดยุทธศาสตร์ในการดำเนินการที่เกี่ยวข้องกับการเข้าถึงอินเทอร์เน็ตโดยตรง ได้แก่

ยุทธศาสตร์ที่ 1 การพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ โดยมีเป้าหมายที่สำคัญ อาทิ โครงข่ายอินเทอร์เน็ตความเร็วสูงเข้าถึงทุกหมู่บ้าน และค่าบริการอินเทอร์เน็ตความเร็วสูงไม่เกินร้อยละ 2 ของรายได้มวลรวมประชาชาติต่อหัว

และยุทธศาสตร์ที่ 3 การสร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล โดยมีเป้าหมายที่สำคัญ อาทิ ประชาชนทุกกลุ่มโดยเฉพาะกลุ่มผู้อาศัยในพื้นที่ห่างไกล ผู้สูงอายุ และคนพิการสามารถเข้าถึง และใช้ประโยชน์จากเทคโนโลยีดิจิทัล และประชาชนทุกคนมีความตระหนัก ความรู้ ความเข้าใจ และทักษะในการใช้เทคโนโลยีดิจิทัลให้เกิดประโยชน์อย่างสร้างสรรค์ (Digital Literacy)

---

[142] แผนแม่บทภายใต้ยุทธศาสตร์ชาติ (7) ประเด็น โครงสร้างพื้นฐาน ระบบโลจิสติกส์ และดิจิทัล (พ.ศ. 2561 - 2580). หน้า 12. http://nscr.nesdb.go.th/wp-content/uploads/2019/04/07-โครงสร้างพื้นฐาน-ระบบโลจิสติกส์-และดิจิทัล.pdf

[143] นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 – 2580). หน้า 7 – 8.

[144] นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 – 2580). หน้า 9.

[145] นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 – 2580). หน้า 8.

แผนแม่บทกิจการโทรคมนาคม ฉบับที่ 2 พ.ศ. 2562- 2566

เป็นแผนที่เกิดขึ้นตาม พ.ร.บ. กสทช.ฯ ซึ่งแผนดังกล่าวได้กล่าวถึงปัญหางความเหลื่อมล้ำในการเข้าถึงบริการอินเทอร์เน็ตเช่นกัน[146] และกำหนดยุทธศาสตร์เพื่อแก้ไขปัญหาดังกล่าว โดยเฉพาะในยุทธศาสตร์ที่ 4 การบริการโทรคมนาคมพื้นฐานโดยทั่วถึงและบริการเพื่อสังคม ซึ่งมุ่งเน้นการพัฒนาโครงข่ายบรอดแบนด์และบริการโทรคมนาคมสาธารณะในพื้นที่ชนบทหรือพื้นที่ที่มีผลตอบแทนการลงทุน เพื่อเพิ่มโอกาสในการเข้าถึงบริการโทรคมนาคม โดยมีตัวชี้วัดสำคัญ ได้แก่ มีบริการอินเทอร์เน็ตบรอดแบนด์ความเร็วสูงครอบคลุมตามเป้าหมายที่กำหนดไว้ในแผนการจัดให้มีบริการโทรคมนาคมพื้นฐานโดยทั่วถึงและบริการเพื่อสังคม และประชาชนกลุ่มเป้าหมายได้รับการส่งเสริมการใช้งานและใช้ประโยชน์จากบริการโทรคมนาคมพื้นฐานตามที่กำหนดไว้ในแผนการจัดให้มีบริการโทรคมนาคมพื้นฐานโดยทั่วถึงและบริการเพื่อสังคม

โครงการริเริ่มที่สำคัญ

ปี 2559 รัฐบาลได้ริเริ่มดำเนิน “โครงการเน็ตประชารัฐ” หรือ “โครงการอินเทอร์เน็ตหมู่บ้าน” ซึ่งได้กำหนดหมู่บ้านที่อยู่ในพื้นที่ห่างไกล (Zone C) และเป็นพื้นที่เป้าหมาย จำนวน 40,432 หมู่บ้าน โดยมีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมดำเนินการขยายโครงข่ายอินเทอร์เน็ตความเร็วสูงด้วยสื่อสัญญาณสายเคเบิลใยแก้วนำแสง (Fiber Optic) ให้ครอบคลุมหมู่บ้านเป้าหมายที่มีลักษณะเป็นพื้นที่ซึ่งไม่ศักยภาพในเชิงพาณิชย์และยังไม่มีบริการอินเทอร์เน็ตความเร็วสูง จำนวน 24,700 หมู่บ้าน พร้อมทั้งจัดให้มีจุดให้บริการอินเทอร์เน็ตแบบไร้สายสาธารณะประจำหมู่บ้าน หมู่บ้านละ 1 จุด โดยไม่คิดค่าใช้จ่ายกับผู้ใช้บริการที่ระดับความเร็วไม่ต่ำกว่า 100/50 Mbps (Download/Upload) โดยในการออกแบบและติดตั้งโครงข่ายเคเบิลใยแก้วนำแสงมีลักษณะทางกายภาพเป็นโครงข่ายแบบเปิด (Open Access Network) ที่สามารถรองรับการเชื่อมต่อของผู้ให้บริการอื่นได้โดยสะดวก โดยดำเนินการติดตั้งเรียบร้อยแล้วเดือนธันวาคม 2560[147]

ส่วนหมู่บ้านที่เหลืออีกจำนวน 15,732 หมู่บ้าน และพื้นที่ชายขอบ (Zone C+) อีก 3,920 หมู่บ้าน กสทช. จะรับผิดชอบดำเนินการโดยใช้งบประมาณกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม (USO)

กล่าวโดยสรุป แม้รัฐธรรมนูญและกฎหมายไทยยังไม่ได้รับรองสิทธิในการเข้าถึงอินเทอร์เน็ตไว้อย่างชัดแจ้ง แต่กฎหมาย โดยเฉพาะ พ.ร.บ. กสทชฯ และ พ.ร.บ. โทรคมนาคมฯ ก็เอื้อให้เกิดการส่งเสริมการเข้าถึงอินเทอร์เน็ตในฐานสาธารณูปโภคขั้นพื้นฐาน นอกจากนี้ นโยบายระดับชาติ ตั้งแต่ยุทธศาสตร์ชาติลงมา

---

[146] แผนแม่บทกิจการโทรคมนาคมฉบับที่ 2 (พ.ศ.2562-2566). หน้า 5.

[147] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. ผู้นำการเปลี่ยนแปลงดิจิทัล กิจกรรมสร้างการรับรู้ประโยชน์เน็ตประชารัฐ รอบที่ 3. https://npcradm.netpracharat.com//mediadetail/cUaQNKUgwt.pdf ;
https://npcr.netpracharat.com/AboutNetpracharat/About.aspx

จนถึงนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และแผนแม่บทกิจการโทรคมนาคม ได้แสดงให้เห็นความมุ่งมั่นของรัฐไทยในการส่งเสริมให้ประชาชนเข้าถึงบริการอินเทอร์เน็ตได้อย่างทั่วถึง ในราคาที่ไม่แพง รวมถึงการส่งเสริมการเข้าถึงของประชากรที่อยู่ในพื้นที่ห่างไกลและประชากรกลุ่มเฉพาะโดยเฉพาะผู้สูงอายุ และคนพิการ อย่างไรก็ดี นโยบายและโครงการดังกล่าวจะมีประสิทธิผลในการส่งเสริมการเข้าถึงอินเทอร์เน็ตของประชาชนได้หรือไม่ หรือมากน้อยเพียงใดนั้น อยู่นอกเหนือขอบเขตวัตถุประสงค์ของงานวิจัยชิ้นนี้ แต่ทั้งนี้งานวิจัยนี้จะพยายามนำเสนอภาพรวมสถานการณ์ของการเข้าถึงอินเทอร์ในประเทศไทยในลำดับต่อไป

3.5.2 บทบาท กสทช. ในฐานะหน่วยงานหลักในการกำกับดูแลอินเทอร์เน็ต

ที่มาและองค์ประกอบของ กสทช.

หน่วยงานที่มีบทบาทสำคัญต่ออินเทอร์เน็ตของประเทศไทยมีหลายหน่วยงาน ซึ่งมีหน้าที่กำกับดูแลเฉพาะด้าน เช่น ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านอาชญากรรมทางคอมพิวเตอร์ รวมถึงด้านความมั่นคลอดภัยทางไซเบอร์ ซึ่งในส่วนนี้จะไม่ได้กล่าวถึงบทบาทของกลไกเฉพาะด้านเหล่านั้น แต่จะเน้นกลไกที่มีบทบาทหลักเกี่ยวกับนโยบายและการกำกับดูแลการเข้าถึงอินเทอรืเน็ต คือ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือ “กสทช.”

กสทช. เป็นองค์กรของรัฐที่เป็นอิสระ ซึ่งเกิดขึ้นครั้งแรกตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540[148] และพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553 โดยมีหน้าที่หลักในด้านนโยบาย การจัดสรรคลื่นความถี่ การอนุมัติอนุญาตและกำกับดูแลการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม รวมถึงอินเทอร์เน็ต

ปี 2560 สภานิติบัญญัติแห่งชาติ ได้ผ่าน พ.ร.บ. กสทช. ฉบับที่ 2 พ.ศ. 2560 ซึ่งปรับปรุงกระบวนการสรรหา องค์ประกอบ คุณสมบัติและอำนาจหน้าที่ของ กสทช. โดยลดจำนวน กสทช. จากเดิมที่มี 11 คน ให้เหลือ 7 คน ซึ่งจะได้รับการแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญด้านกิจการกระจายเสียง ด้านกิจการโทรทัศน์ ด้านกิจการโทรคมนาคม ด้านวิศวกรรม ด้านกฎหมาย ด้านเศรษฐศาสตร์ และด้านการคุ้มครองผู้บริโภคหรือส่งเสริมสิทธิและเสรีภาพของประชาชน ด้านละหนึ่งคน

กฎหมายที่แก้ไขใหม่ ยังได้เปลี่ยนแปลงกลไกการสรรหา กสทช. ที่จากเดิมดำเนินการโดยคณะกรรมการสรรหา 15 คน ซึ่งมีที่มาจากหลากหลาย ทั้งจากหน่วยงานรัฐที่เกี่ยวข้อง ภาคประชาสังคม องค์กรวิชาชีพต่าง ๆ รวมถึงประธานกรรมการสิทธิมนุษยชนแห่งชาติ เป็นเหลือคณะกรรมการสรรหา 7 คน ซึ่งส่วน

[148] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 มาตรา 40 ; รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 47 ; ฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 60.

ใหญ่มาจากฝ่ายตุลาการและองค์กรอิสระบางแห่ง โดยประธานคณะกรรมการสิทธิมนุษยชนแห่งชาติ ซึ่งเคยเป็นหนึ่งในกรรมการสรรหาตามกฎหมายฉบับเดิมได้ถูกตัดออกไปจากกลไกการสรรหา ซึ่งถือเป็นเรื่องที่อาจไม่สมเหตุสมผลนัก เพราะกฎหมายใหม่กำหนดให้ กสทช. 1 คนต้องสรรหาจากผู้มีความรู้ความเชี่ยวชาญด้านการคุ้มครองผู้บริโภคหรือส่งเสริมสิทธิและเสรีภาพของประชาชน แต่กลไกการสรรหากลับไม่มีตัวแทนของผู้ที่มีความรู้ความเชี่ยวชาญด้านสิทธิมนุษยชนเข้าร่วมเลย

มีข้อสังเกตเพิ่มเติมเกี่ยวกับสัดส่วนของ กสทช. ซึ่ง กสทช. ทุกชุดที่ผ่านมา รวมถึงชุดปัจจุบันล้วนประกอบด้วยเพศชายเป็นส่วนใหญ่[149] แสดงให้เห็นว่ามิติความเท่าเทียมด้านเพศสภาพซึ่งเป็นแนวทางสำคัญของหลักการสิทธิมนุษยชนยังไม่ถูกให้ความสำคัญในกลไกการกับกับดูแลอินเทอร์เน็ต ซึ่งทั้งองค์ประกอบของ กสทช. และกลไกการสรรหาข้างต้นได้แสดงให้เห็นว่ากลไกกำกับดูแลอินเทอร์เน็ตของไทยยังห่างไกลจากแนวทางของผู้มีส่วนได้ส่วนเสียหลายฝ่าย

<u>ขอบเขตอำนาจหน้าที่</u>

หน้าที่และอำนาจของ กสทช. ถูกกำหนดไว้ในมาตรา 27 ของ พ.ร.บ. กสทช.ฯ ซึ่งครอบคลุมมิติเชิงนโยบาย การพิจารณาอนุญาตและกำกับดูแลการประกอบกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม รวมถึงอินเทอร์เน็ต ดังนี้

- ด้านนโยบาย โดยการจัดทำแผนแม่บทการบริหารคลื่นความถี่ และรวมถึงแผนแม่บทกิจการโทรคมนาคม และดำเนินการให้เป็นไปตามแผนดังกล่าว โดยแผนต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม[150]
- ด้านการจัดสรร การพิจารณาอนุญาตและกำกับดูแลการใช้คลื่นความถี่ในการประกอบกิจการฯ และกำหนดหลักเกณฑ์และวิธีการเกี่ยวกับการอนุญาต เงื่อนไข หรือค่าธรรมเนียมการอนุญาตดังกล่าว รวมถึงกำหนดหลักเกณฑ์การใช้คลื่นความถี่ให้เป็นไปอย่างมีประสิทธิภาพและปราศจากการรบกวนซึ่งกันและกัน และการวินิจฉัยและแก้ไขปัญหาการใช้คลื่นความถี่ที่มีการรบกวนซึ่งกันและกัน
- ด้านการอนุญาตและกำกับดูแลการประกอบกิจการฯ เพื่อให้ผู้ใช้บริการได้รับบริการที่มีคุณภาพ ประสิทธิภาพ รวดเร็ว ถูกต้อง และเป็นธรรมและกำหนดหลักเกณฑ์และวิธีการเกี่ยวกับการอนุญาต เงื่อนไข หรือค่าธรรมเนียมการอนุญาตดังกล่าว รวมถึง

[149] https://www.nbtc.go.th/About/Commissioners.aspx?lang=th-th

[150] เป็นไปตาม พ.ร.บ. กสทช. ฉบับที่ 2 พ.ศ. 2560 ซึ่งแก้ไขให้สอดคล้องกับพระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560

ติดตามตรวจสอบและให้คำปรึกษาแนะนำการประกอบกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคม

- ด้านการควบคุมราคา
  - กำหนดหลักเกณฑ์และวิธีการในการใช้หรือเชื่อมต่อ และหลักเกณฑ์และวิธีการในการกำหนดอัตราค่าใช้หรือค่าเชื่อมต่อโครงข่ายในการประกอบกิจการ ฯ ให้เป็นธรรมต่อผู้ใช้บริการ ผู้ให้บริการและผู้ลงทุน หรือระหว่างผู้ให้บริการโทรคมนาคม โดยคำนึงถึงประโยชน์สาธารณะเป็นสำคัญ
  - กำหนดโครงสร้างอัตราค่าธรรมเนียมและโครงสร้างอัตราค่าบริการในกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม ให้เป็นธรรมต่อผู้ใช้บริการและผู้ให้บริการโดยคำนึงถึงประโยชน์สาธารณะเป็นสำคัญ
  - การกำหนดอัตราค่าใช้หรือค่าเชื่อมต่อโครงข่าย ค่าธรรมเนียมใด ๆ หรือค่าบริการในการประกอบกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม ให้ กสทช. คำนึงถึงประโยชน์สาธารณะและภาระของผู้บริโภคความสอดคล้องกับต้นทุนการให้บริการ ความคุ้มค่า และการจัดสรรทรัพยากรที่มีประสิทธิภาพด้วย[151]
  - สำหรับรายละเอียดเกี่ยวกับการกำหนดอัตราค่าธรรมเนียมและค่าบริการในกิจการโทรคมนาคม เป็นไปตาม พ.ร.บ. โทรคมนาคมฯ มาตรา 55 - 59 กล่าวโดยสรุปคือ การกำหนดอัตราขั้นสูงของค่าธรรมเนียมและค่าบริการ จะต้องมีวิธีการคำนวณที่ชัดเจน เป็นอัตราที่ยุติธรรมแก่ผู้รับใบอนุญาตและผู้ใช้บริการ และไม่มีลักษณะเป็นการเลือกปฏิบัติ แบ่งแยก หรือกีดกันผู้ใช้บริการหรือบุคคลหนึ่งบุคคลใด และผู้รับใบอนุญาตแต่ละรายจะเรียกเก็บค่าธรรมเนียมหรือค่าบริการนอกเหนือหรือเกินกว่าอัตราขั้นสูงที่กำหนดไม่ได้ และผู้รับใบอนุญาตต้องเผยแพร่อัตราค่าธรรมเนียมและค่าบริการของตนเป็นการทั่วไปและต้องแจ้งให้ผู้ใช้บริการทุกรายทราบ และต้องแสดงอัตราดังกล่าวไว้ในที่เปิดเผยเห็นได้ง่าย
- ด้านการกำหนดมาตรฐานทางเทคนิค โดยกำหนดมาตรฐานและลักษณะพึงประสงค์ทางด้านเทคนิคในการประกอบกิจการกระจายเสียง กิจการโทรทัศน์ กิจการโทรคมนาคม และในกิจการวิทยุคมนาคม
- ด้านการป้องกันการผูกขาด

[151] โปรดดู มาตรา 29 ของ พ.ร.บ. กสทช.ฯ

- การจัดทำแผนแม่บทกิจการโทรคมนาคม อย่างน้อยต้องมีแนวทางการพัฒนาและการส่งเสริมแข่งขันโดยเสรีอย่างเป็นธรรมระหว่างผู้ประกอบกิจการ[152]
- กำหนดมาตรการเพื่อป้องกันมิให้มีการกระทำอันเป็นการผูกขาดหรือก่อให้เกิดความไม่เป็นธรรมในการแข่งขันในกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม
- กำหนดลักษณะการควบรวม การครองสิทธิข้ามสื่อ หรือการครอบงำกิจการกระจายเสียงและกิจการโทรทัศน์ที่ใช้คลื่นความถี่ ระหว่างสื่อมวลชนด้วยกันเอง หรือโดยบุคคลอื่นใด ซึ่งจะมีผลเป็นการขัดขวางเสรีภาพในการรับรู้ข้อมูลข่าวสาร หรือปิดกั้นการได้รับข้อมูลข่าวสารที่หลากหลายของประชาชน โดยให้รับฟังความคิดเห็นจากประชาชนและผู้เกี่ยวข้องประกอบด้วย

บทบาทในการป้องกันการผูกขาดนั้น มีกรณีตัวอย่างร่วมสมัยที่ท้าทายบทบาทของ กสทช. คือ กรณีการรวมธุรกิจระหว่างบริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน) (TRUE) และบริษัท โทเทิ่ล แอ็คเซ็ส คอมมูนิเคชั่น จำกัด (มหาชน) (DTAC) ซึ่งทั้งสองบริษัทเป็น 2 ใน 3 บริษัทรายใหญ่ที่มีส่วนแบ่งในตลาดโทรคมนาคมสูงสุด (อีกหนึ่งบริษัทคือ AIS) (ดูข้อมูลส่วนแบ่งตลาดในส่วนถัดไป) หากมีการควบรวม บริษัทใหม่จากการครองส่วนแบ่งตลาดมากที่สุด คือ 54 % และจะทำให้ตลาดโทรคมนาคมถูกครองด้วยบริษัทรายใหญ่ 2 ราย ซึ่งแน่นอนว่ามีทั้งผลดีและผลเสีย แต่ในมุมมองของสิทธิผู้บริโภคแล้ว มีความกังวลเรื่องคุณภาพและราคาการบริการที่อาจสูงขึ้น ประเด็นดังกล่าวถือเป็นโจทย์ท้าทายบทบาทของ กสทช. และกฎหมาย ตลอดจนกฎระเบียบการกำกับดูแลที่มีอยู่

- ด้านการคุ้มครองสิทธิและเสรีภาพ
  - การคุ้มครองสิทธิและเสรีภาพของประชาชนมิให้ถูกเอาเปรียบจากผู้ประกอบกิจการและคุ้มครองสิทธิในความเป็นส่วนตัวและเสรีภาพของบุคคลในการสื่อสารถึงกันโดยทางโทรคมนาคมและส่งเสริมสิทธิเสรีภาพและความเสมอภาคของประชาชนในการเข้าถึงและใช้ประโยชน์คลื่นความถี่ที่ใช้ในกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม
  - จัดให้มีมาตรการป้องกันมิให้มีการแสวงหาประโยชน์จากผู้บริโภคโดยไม่เป็นธรรมหรือสร้างภาระแก่ผู้บริโภคเกินความจำเป็น รวมตลอดทั้งป้องกันการกระทำที่มีผลเป็นการขัดขวางเสรีภาพในการรับรู้หรือปิดกั้นการรับรู้ข้อมูลหรือข่าวสารที่ถูกต้องตามความเป็นจริงของประชาชนและป้องกันมิให้บุคคลหรือกลุ่มบุคคลใดใช้

[152] โปรดดู มาตรา 49 วรรคแรก ของ พ.ร.บ. กสทช.ฯ

ประโยชน์จากคลื่นความถี่โดยไม่คำนึงถึงสิทธิของประชาชนทั่วไป รวมถึงป้องกันผลกระทบต่อสุขภาพของประชาชนที่อาจเกิดขึ้นจากการใช้คลื่นความถี่[153]

- ตรวจสอบและสั่งระงับการดำเนินการของผู้ประกอบกิจการฯ ที่ดำเนินการในประการที่น่าจะเป็นการเอาเปรียบผู้บริโภค โดยอาศัยการใช้เครือข่ายหรือการโฆษณาอันมีลักษณะเป็นการค้ากำไรเกินควร หรือก่อให้เกิดความเดือดร้อนรำคาญไม่ว่าด้วยวิธีการใดตามหลักเกณฑ์ที่ กสทช. กำหนด[154]
- กำหนดมาตรการคุ้มครองสิทธิของผู้ใช้บริการฯ เกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม หากมีการกระทำความผิดโดยการดักรับไว้ ใช้ประโยชน์ หรือเปิดเผยข้อความข่าวสารหรือข้อมูลอื่นใดที่มีการสื่อสารทางโทรคมนาคมโดยไม่ชอบด้วยกฎหมาย ให้ถือว่า กสทช. เป็นผู้เสียหายตามประมวลกฎหมายวิธีพิจารณาความอาญา และในกรณีที่ผู้ได้รับใบอนุญาตประกอบกิจการฯ เป็นผู้กระทำความผิด หรือรู้ว่ามีการกระทำความผิด แต่เพิกเฉยหรือไม่ดำเนินการตามกฎหมายภายในเวลาอันสมควร ให้ กสทช. มีอำนาจสั่งพักใช้หรือเพิกถอนใบอนุญาตประกอบกิจการโทรคมนาคมได้[155]
- นอกจากนี้ พ.ร.บ. โทรคมนาคมฯ มาตรา 50 ยังกำหนดให้คณะกรรมการกำหนดมาตรการเพื่อคุ้มครองผู้ใช้บริการเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม และให้ผู้รับใบอนุญาตมีหน้าที่ปฏิบัติตามมาตรการที่คณะกรรมการกำหนด หากพบว่ามีบุคคลใดกระทำการละเมิดสิทธิของผู้ใช้บริการ ให้ผู้รับใบอนุญาตหรือคณะกรรมการดำเนินการเพื่อระงับการกระทำดังกล่าว และแจ้งให้ผู้ใช้บริการทราบโดยเร็ว

ทั้งนี้ ในการดำเนินการด้านการกำกับดูแลกิจการด้านโทรคมนาคม โปรดดูรายละเอียดตามพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 (พ.ร.บ. การประกอบกิจการโทรคมนาคมฯ)

<u>การมีส่วนร่วมของสาธารณะ</u>

พ.ร.บ. กสทช.ฯ กำหนดการมีส่วนร่วมของประชาชนในขั้นตอนต่าง ๆ ดังนี้

- จัดการรับฟังความคิดเห็นจากประชาชนและผู้เกี่ยวข้องประกอบการกำหนดลักษณะการควบรวม การครองสิทธิข้ามสื่อ หรือการครอบงำกิจการกระจายเสียงและกิจการโทรทัศน์ที่

[153] โปรดดู มาตรา 27 วรรคสอง พ.ร.บ. กสทช.ฯ

[154] โปรดดู มาตรา 13 ของ พ.ร.บ. กสทช.ฯ

[155] โปรดดู มาตรา 32 ของ พ.ร.บ. กสทช.ฯ

ใช้คลื่นความถี่ ซึ่งจะมีผลเป็นการขัดขวางเสรีภาพในการรับรู้ข้อมูลข่าวสารหรือปิดกั้นการได้รับข้อมูลข่าวสารที่หลากหลายของประชาชน[156]

- จัดให้มีการรับฟังความคิดเห็นของผู้มีส่วนได้เสียและประชาชนทั่วไปเพื่อประกอบการพิจารณาก่อนออกระเบียบ ประกาศ หรือคำสั่ง เกี่ยวกับการกำกับดูแลการประกอบกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมที่มีผลใช้บังคับเป็นการทั่วไปและเกี่ยวข้องกับการแข่งขันในการประกอบกิจการหรือมีผลกระทบต่อประชาชนอย่างมีนัยสำคัญ[157]
- การรับฟังความคิดเห็นของประชาชนผู้ประกอบกิจการ และหน่วยงานของรัฐที่เกี่ยวข้อง เพื่อเป็นแนวทางในการพิจารณาจัดทำแผนแม่บทกิจการโทรคมนาคม และในกรณีที่ กสทช. วินิจฉัยเรื่องใดไม่สอดคล้องกับความคิดเห็นดังกล่าว กสทช. ต้องชี้แจงและแสดงเหตุผลให้ทราบ ทั้งนี้ หากประชาชน ผู้ประกอบกิจการ หรือหน่วยงานของรัฐ เห็นว่าแผนแม่บทที่ กสทช. กำหนดขัดต่อบทบัญญัติของรัฐธรรมนูญแห่งราชอาณาจักรไทย ให้มีสิทธิฟ้องคดีต่อศาลปกครองได้[158]

แม้ พ.ร.บ. กสทช. จะกำหนดการมีส่วนร่วมของภาคส่วนต่าง ๆ ไว โดยเฉพาะในขั้นตอนของการจัดทำแผนแม่บท แต่การมีส่วนร่วมเหล่านั้นอาจจะยังไม่เพียงพอสำหรับการกำกับดูแลอินเทอร์เน็ตตามแนวทางผู้มีส่วนได้ส่วนเสียหลายฝ่ายและแนวทางสิทธิมนุษยชน ยิ่งกว่านั้น การกำกับดูแลปัจจุบันดูเหมือนจะถอยห่างออกจากแนวทางดังกล่าว หลังจากการแก้ไข พ.ร.บ. กสทช. ฉบับที่ 2 พ.ศ. 2560 ซึ่งได้ปรับเปลี่ยนองค์ประกอบการสรรหา กสทช. แม้จะทำให้กลไกการสรรหาสะดวกขึ้น แต่ในแง่หนึ่งก็ลดทอนความหลากหลาย โดยเฉพาะการลดทอนบทบาทของภาคส่วนต่าง ๆ ในกระบวนการสรรหา นอกจากนี้ ยังมีข้อสังเกตสัดส่วนของคณะกรรมการเป็นเพศชายเกือบ 100 % แสดงให้เห็นการคำนึงถึงมิติเพศสภาพ อันเป็นหลักการสำคัญในมิติสิทธิมนุษยชนในเรื่องความเสมอภาคทางเพศสภาพ ดังนั้น ประเด็นเหล่านี้ อาจจะต้องถูกหยิบยกมาพิจารณาและตระหนักให้มากขึ้นในอนาคต

กล่าวโดยสรุป จากอำนาจหน้าที่ของ กสทช. ดังกล่าว แสดงให้เห็นว่า กสทช. เป็นกลไกสำคัญในกำกับดูแลอินเทอร์เน็ต และการส่งเสริมและคุ้มครองสิทธิทางอินเทอร์เน็ต รวมถึง

- การส่งเสริมสิทธิในการเข้าถึงอินเทอร์เน็ต ผ่านการควบคุมราคาบริการให้มีความเป็นธรรม การป้องกันการผูกขาดที่จะส่งผลต่อราคา รวมถึงการจัดทำโครงการเพื่อขยาย

---

[156] โปรดดู มาตรา 27 (17) ของ พ.ร.บ. กสทช.ฯ

[157] โปรดดู มาตรา 28 ของ พ.ร.บ. กสทช.ฯ

[158] โปรดดู มาตรา 49 วรรคสี่ - ห้า ของ พ.ร.บ. กสทช.ฯ

บริการไปยังพื้นที่ด้อยโอกาสของประเทศ ผ่านการบริการสากล (Universal Service and Access)

- การกำหนดนโยบาย กำกับดูแลและตรวจสอบการดำเนินการ เพื่อคุ้มครองสิทธิมนุษยชน รวมถึงผู้บริโภค สิทธิในความเป็นส่วนตัว รวมถึงการคุ้มครองเสรีภาพในการแสดงออก รวมถึงการแสวงหาและรับข้อมูลข่าวสารของประชาชน ผ่านการตรวจสอบการสกัดกั้นโดยไม่ชอบด้วยกฎหมายของผู้กระกอบกิจการโทรคมนาคม

อย่างไรก็ดี อำนาจหน้าที่ของ กสทช. บางประการก็อาจนำมาซึ่งความเสี่ยงต่อสิทธิมนุษยชนเช่นกัน กล่าวคือ

- กฎหมายกำหนดให้ กสทช. ต้องดำเนินการ “เพื่อประโยชน์สูงสุดของประชาชน ความมั่นคงของรัฐ และประโยชน์สาธารณะ”[159] ซึ่งเป็นถ้อยคำที่ค่อนข้างกว้างและคลุมครือ จึงอาจทำให้เกิดการตีความในลักษณะที่ละเมิดสิทธิมนุษยชนได้ ดังนั้น ควรมีการกำหนดขอบเขตการตีความที่ชัดเจน เพื่อป้องกันการใช้ดุลพินิจที่ไม่ชอบในอนาคต โดยเฉพาะในสภาวะที่กลไกเหล่านี้อาจถูกใช้เป็นเครื่องมือทางการเมืองโดยผู้มีอำนาจ
- การใช้อำนาจเข้าไปควบคุมเนื้อหา ซึ่งอาจละเมิดเสรีภาพสื่อมวลชนและสิทธิในการรับรู้ข้อมูลข่าวสารของประชาชน ดังเช่นกรณีที่ กสทช. ระงับการออกอากาศของช่อง “วอยซ์ ทีวี” เป็นเวลา 15 วัน ในเดือนกุมภาพันธ์ 2562 ซึ่งต่อมาศาลปกครองมีคำพิพากษาให้เพิกถอนคำสั่ง กสทช. ดังกล่าว โดยเห็นว่าผู้ดำเนินรายการเสนอการวิเคราะห์จากการเรียบเรียงเนื้อหาและมีการวิพากษ์วิจารณ์การดำเนินงานของหน่วยงานรัฐ รวมถึงบุคคลสาธารณะ แม้จะมีเพิ่มเติมจากแหล่งข่าว และมีการแสดงความเห็นสนับสนุนบางพรรคการเมือง ก็ไม่ได้ก่อให้เกิดความสับสนต่อสาธารณะ[160]

3.5.3 สถานการณ์การเข้าถึงอินเทอร์เน็ตในประเทศไทย

ดัชนีชี้วัดความครอบคลุมของอินเทอร์เน็ตประจำปี 2564 (Inclusive Internet Index 2021) ซึ่งเป็นโครงการของนิตยสาร The Economist ประเทศไทยถูกจัดลำดับอยู่ในลำดับที่ 49 จาก 120 ประเทศ

[159] โปรดดู มาตรา 27 วรรคสาม ของ พ.ร.บ. กสทช.ฯ กอบ

[160] Thai PBS. ศาลปกครอง เพิกถอนคำสั่ง กสทช. จอดำ "วอยซ์ ทีวี". 27 กุมภาพันธ์ 2562. https://www.thaipbs.or.th/news/content/278034

โดยอยู่ในอันดับ 10 ของเอเชีย จาก 27 ประเทศ และอันดับ 3 ของอาเซียน จาก 9 ประเทศ รองจากสิงคโปร์และมาเลเซีย ตามลำดับ โดยดัชนีดังกล่าวมีการประเมินและให้คะแนนใน 4 หมวด คือ[161]

- ความพร้อมใช้งาน (Availability) เป็นการตรวจสอบคุณภาพและความกว้างของโครงสร้างพื้นฐานที่มีอยู่ซึ่งจำเป็นสำหรับการเข้าถึงและระดับของการใช้งานอินเทอร์เน็ต
- ความสามารถในการจ่ายได้ (Affordability) เป็นการตรวจสอบค่าใช้จ่ายในการเข้าถึงเมื่อเทียบกับรายได้และระดับการแข่งขันในตลาดอินเทอร์เน็ต
- ความเกี่ยวข้อง (Relevance) เป็นการตรวจสอบการมีอยู่และขอบเขตของเนื้อหาในภาษาท้องถิ่นและเนื้อหาที่เกี่ยวข้อง
- ความพร้อม (Readiness) เป็นการตรวจสอบความสามารถในการเข้าถึงอินเทอร์เน็ตซึ่งรวมถึงทักษะ การยอมรับทางวัฒนธรรม และนโยบายที่สนับสนุน

ตารางที่ 3.1 ดัชนีชี้วัดความครอบคลุมของอินเทอร์เน็ตประเทศไทย ระหว่างปี 2561 - 2564

ปี พ.ศ.	overall	Availability	Affordability	Relevance	Readiness
2562	34	36	28	54	29
2562	43	36	34	57	88
2563	48	42	27	69	88
2564	49	30	30	76	102

ที่มา The Inclusive Internet Index 2018 - 2021, The Economist Intelligence Unit
หมายเหตุ ยิ่งคะแนนสูงยิ่งเป็นแนวโน้มที่ไม่ดี

หากดูจากตาราง จะเห็นว่าในปี 2564 อันดับในภาพรวมของไทยอยู่ที่อันดับ 49 แย่ลงกว่าปี 2563 ที่อยู่อันดับ 48 แต่หากพิจารณาตามหมวดการประเมิน จะพบว่า ด้านความพร้อมใช้งาน (Availability) ถือว่ามีการพัฒนาที่ดีขึ้น ส่วนด้านอื่น อันดับแย่ลงจากปีก่อนหน้า โดยด้านที่น่าเป็นห่วงมากที่สุดคือ ความพร้อม (Readiness)

[161] The Inclusive Internet Index 2021, The Economist Intelligence Unit, https://internet-org.ps.aws.economist.com/explore/countries/performance?year=2021

ในส่วนถัดไปจะนำเสนอรายละเอียดของการเข้าถึงอินเทอร์เน็ตในประเทศไทยจากแง่มุมต่าง ๆ โดยอิงจากแง่มุมของดัชนีชี้วัดความครอบคลุมของอินเทอร์เน็ตข้างต้น แต่จะนำเสนอประกอบกับข้อมูลจากแหล่งอื่น ๆ ที่สามารถเข้าถึงได้ ดังนี้

1) การเข้าถึงได้/ความพร้อมใช้งาน (Availability)

เมื่อพิจารณาจากสถานการณ์ปัจจุบันของการเข้าถึงอินเทอร์เน็ตของประเทศไทย รายงาน Digital 2022 ที่เผยแพร่เมื่อเดือนมกราคม 2565 โดย We Are Social และ Hootsuite ระบุว่า ผู้ใช้อินเทอร์เน็ตในประเทศไทยมีอยู่ราว 54.50 ล้านคน หรือมีอัตราการเข้าถึงอินเทอร์เน็ตอยู่ที่ 77.8 เปอร์เซ็นต์ของประชากรทั้งหมดในเดือนมกราคม 2565 ซึ่งเพิ่มขึ้นจากปีที่แล้ว 0.2 เปอร์เซ็นต์ หรือประมาณ 108,000 คน โดย 96.2 เปอร์เซ็นต์ใช้อินเทอร์เน็ตผ่านมือถือ[162]

เมื่อดูประกอบข้อมูลผู้ใช้อินเทอร์เน็ตในประเทศไทยจากแหล่งอื่น พบว่า มีตัวเลขที่แตกต่างกันอยู่บ้าง[163] ซึ่งน่าจะเกิดจากวิธีการเก็บข้อมูล และช่วงเวลาที่นำเสนอข้อมูล อย่างไรก็ดี ทุกแหล่งข้อมูลแสดงให้เห็นจำนวนผู้ใช้อินเทอร์เน็ตในประเทศไทยที่มีแนวโน้มเพิ่มขึ้นต่อเนื่อง แต่ขณะเดียวข้อมูลเหล่านั้นก็สะท้อนให้เห็นว่ายังมีประชากรจำนวนไม่น้อยเข้าไม่ถึงอินเทอร์เน็ต ซึ่งอาจมีมากกว่า 10 ล้านคน หรือราวร้อยละ 15 - 20 ของจำนวนประชากรทั้งหมด

<u>การใช้งานเครือข่ายบรอดแบนด์</u>

จำนวนผู้ลงทะเบียนใช้บริการอินเทอร์เน็ตบรอดแบนด์ (Broadband Subscribers) ในประเทศไทยสูงขึ้นต่อเนื่อง โดยข้อมูล ณ วันที่ 4 กรกฎาคม 2565 ระบุว่า มีจำนวนผู้ลงทะเบียน 12.6 ล้านคน[164]

ข้อมูลจาก ITU ในปี 2564 ได้จำแนกผู้ลงทะเบียนใช้บริการอินเทอร์เน็ตบรอดแบนด์ประจำที่และมือถือ ดังนี้[165]

- จำนวนผู้ลงทะเบียนใช้บริการอินเทอร์เน็ตบรอดแบนด์ประจำที่ (Fixed Broadband Subscribers) มีสัดส่วน 18 คน ต่อประชากร 100 คน เพิ่มขึ้นจากปี 2563 ที่มีสัดส่วนอยู่ที่ 16 และถือว่าสูงกว่าค่าเฉลี่ยของภูมิภาคเอเชียแปซิฟิกที่มีสัดส่วนอยู่ที่ 16 ต่อ

[162] Simon Kemp, “Digital 2022: Thailand,” Datareportal February 15, 2022, https://datareportal.com/reports/digital-2022-thailand

[163] โปรดดู รายงานตัวชี้วัด ITU (International Telecommunication Union) 2564 ที่จัดทำโดยสำนักงานสถิติแห่งชาติ และดูฐานข้อมูลของ กสทช. ที่ http://ttid.nbtc.go.th/internet_sub

[164] http://ttid.nbtc.go.th/internet_sub ทั้งนี้ ตัวเลขดังกล่าวยังไม่รวมอินเทอร์เน็ตตามโครงการเน็ตประชารัฐซึ่งครอบคลุมประชากรประมาณ 20 ล้านคน

[165] ITU. Digital Development Dashboard. https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx

ประชากร 100 คน โดยไทยอยู่ในอันดับ 3 ของอาเซียน รองจากสิงคโปร์ และเวียดนาม ตามลำดับ ทั้งนี้ ในแง่คุณภาพ อินเทอร์เน็ตบรอดแบนด์ประจำที่เกือบทั้งหมด (99 %) มีความเร็วในการดาวน์โหลดเท่ากับหรือสูงกว่า 10 Mbit/s[166] และจากข้อมูลของ Speedtest Global Index เมื่อเดือนสิงหาคม 2565 แสดงให้เห็นว่าบรอดแบนด์ประจำที่ของไทยมีความเร็วเป็นอันดับ 3 ของโลก แต่น่าเสียดายที่การใช้บรอดแบนด์ประจำที่ในไทยยังอยู่ในอัตราไม่สูงนัก

- จำนวนผู้ลงทะเบียนใช้บริการอินเทอร์เน็ตบรอดแบนด์มือถือ (Mobile Broadband Subscribers) มีสัดส่วน 92 คน ต่อประชากร 100 คน เพิ่มขึ้นจากปี 2563 ที่มีสัดส่วนอยู่ที่ 88 และถือว่าสูงกว่าค่าเฉลี่ยของภูมิภาคเอเชียแปซิฟิกที่มีสัดส่วนอยู่ที่ 86 ต่อประชากร 100 คน โดยไทยอยู่อันดับที่ 7 ของอาเซียน รองจากสิงคโปร์ บรูไน มาเลเซีย เมียนมา อินโดนีเซีย และกัมพูชา ตามลำดับ และเวียดนาม ตามลำดับ

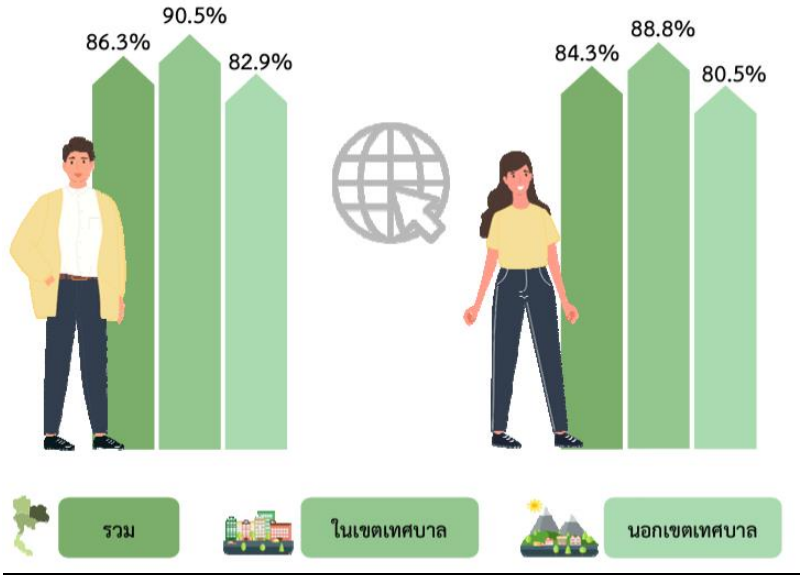
<u>การเข้าถึงอย่างเท่าเทียม</u>

ในหัวข้อก่อนได้กล่าวถึงภาพรวมการเข้าถึงอินเทอร์เน็ตในประเทศไทย ส่วนนี้จะดูข้อมูลการเข้าถึงของกลุ่มเฉพาะบางกลุ่ม โดยใช้ข้อมูลจากผลการสำรวจของสำนักงานสถิติแห่งชาติในช่วงสิ้นปี 2564[167] ซึ่งมีการนำเสนอข้อมูลการเข้าถึงอินเทอรีเน็ตจำแนกตามการเข้าถึงตามภูมิศาสตร์ (ในเขตเทศบาล/นอกเขตเทศบาล) เพศ (หญิง/ชาติ) และอายุ อย่างไรก็ดี ผู้วิจัยพยายามสืบค้นข้อมูลเพิ่มเติมในส่วนที่เกี่ยวข้องกับกลุ่มเฉพาะอื่นแล้ว เช่น ชุมชนชาติพันธุ์ และคนพิการ แต่ยังไม่พบว่ามีข้อมูลดังกล่าว

[166] https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx

[167] สำนักงานสถิติแห่งชาติ. รายงานตัวชี้วัด ITU (International Telecommunication Union) 2564. https://bit.ly/3UP8muZ .เป็นผลการสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในปี 2564 (ไตรมาส 4) มีประชาชนอายุ 6 ปีขึ้นไป 64.0 ล้านคน อยู่ในเขตเทศบาล 28.9 ล้านคน (ร้อยละ 45.1) นอกเขตเทศบาล 35.1 ล้านคน (ร้อยละ 54.9) เป็นผู้ชาย 31.0 ล้านคน (ร้อยละ 48.5) ผู้หญิง 32.9 ล้านคน (ร้อยละ 51.5)

ภาพที่ 3.3 ร้อยละของผู้ใช้อินเทอร์เน็ต จำแนกตามในเขตเทศบาลและนอกเขตเทศบาล และเพศหญิงและชาย



ที่มา สำนักงานสถิติแห่งชาติ, รายงานตัวชี้วัด ITU (International Telecommunication Union) 2564

จากผลการสำรวจของสำนักงานสถิติแห่งชาติในปี 2564 (ไตรมาส 4) พบว่า มีผู้ใช้อินเทอร์เน็ต 54.6 ล้านคน หรือร้อยละ 85.3 ของประชากรทั้งหมด (64 ล้านคน) โดยในเขตเทศบาล พบว่า มีผู้ใช้อินเทอร์เน็ต 25.9 ล้านคน หรือร้อยละ 89.6 ของประชากรทั้งหมดในเขตเทศบาล (28.9 ล้านคน) และนอกเขตเทศบาล มีผู้ใช้อินเทอร์เน็ต 28.7 ล้านคน หรือร้อยละ 81.7 ของประชากรทั้งหมดในเขตเทศบาล (35.1 ล้านคน)[168]

และเมื่อพิจารณาในมิติทางเพศ พบว่า เพศชายใช้อินเทอร์เน็ต ร้อยละ 86.3 ของจำนวนประชากรชายทั้งหมด (31 ล้านคน) และเพศหญิงใช้อินเทอร์เน็ต ร้อยละ 84.3 ของจำนวนประชากรหญิงทั้งหมด (32.9 ล้านคน)[169]

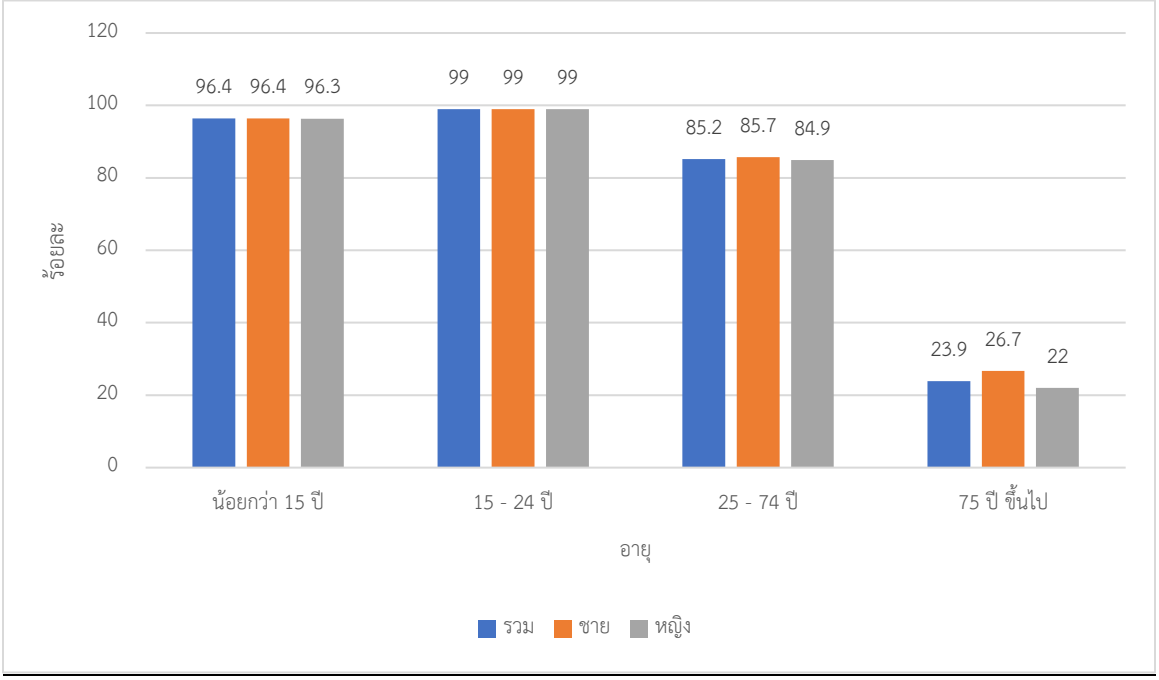
ผลการสำรวจดังกล่าวชี้ให้เห็นว่า มีช่องว่างในการใช้อินเทอร์เน็ตระหว่างพื้นที่เมืองและชนบท โดยในเขตเทศบาล ซึ่งแทนความเป็นพื้นที่เมืองนั้นมีอัตราการเข้าถึงได้มากกว่านอกเขตเทศบาลซึ่งแทนพื้นที่ชนบท และมีความแตกต่างระหว่างการใช้ของเพศชายและหญิง โดยเพศชายใช้อินเทอร์เน็ตมากกว่าผู้หญิง แต่ช่องว่างดังกล่าวมีความแตกต่างกันเพียงเล็กน้อย อย่างไรก็ดี ไม่อาจฟันธงได้ว่าความแตกต่างระหว่างการใช้งานในเขตเทศบาลและนอกเขตเทศบาล หรือความแตกต่างระหว่างชาติและหญิง จะสรุปว่าเกิดจากปัญหาการเข้าถึงอินเทอร์เน็ตเสมอไป เพราะการใช้หรือไม่ใช้งานอินเทอร์เน็ตนั้นขึ้นอยู่กับหลายปัจจัย ซึ่งรวมถึงการไม่ต้องการใช้

[168] สำนักงานสถิติแห่งชาติ, รายงานตัวชี้วัด ITU (International Telecommunication Union) 2564. หน้า 6.

[169] สำนักงานสถิติแห่งชาติ, รายงานตัวชี้วัด ITU (International Telecommunication Union) 2564. หน้า 6.

งาน เพราะเห็นว่าไม่จำเป็นหรือไม่สนใจที่จะใช้ ดังเช่นข้อมูลที่ปรากฏในรายงานตัวชี้วัด ITU (International Telecommunication Union) 2564 ของสำนักงานสถิติแห่งชาติ ซึ่งเกิดจากการสำรวจครัวเรือน ระบุว่า เหตุผลที่ครัวเรือนไม่เชื่อมต่ออินเทอร์เน็ตเกิดจากเห็นว่าไม่มีความจำเป็น/ไม่สนใจ สูงเกินร้อยละ 80

แผนภูมิที่ 3.1 ร้อยละของประชาชนที่ใช้อินเทอร์เน็ต จำแนกตามอายุและเพศ



ที่มา สำนักงานสถิติแห่งชาติ, รายงานตัวชี้วัด ITU (International Telecommunication Union) 2564

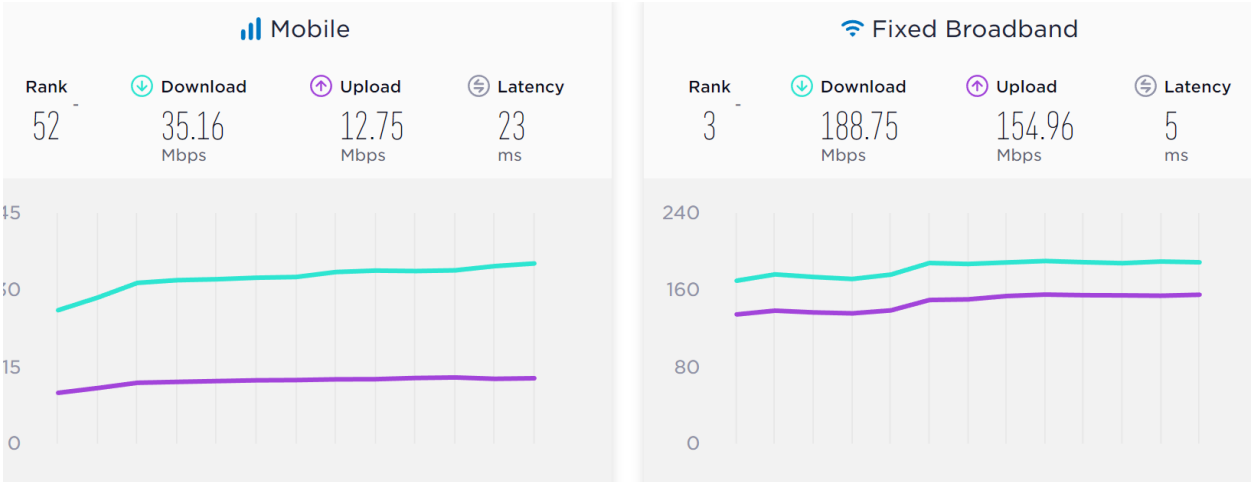
เมื่อพิจารณาการใช้อินเทอร์เน็ตโดยจำแนกตามกลุ่มอายุแล้ว พบว่า ประชาชนกลุ่มอายุ 15 – 24 ปี ใช้อินเทอร์เน็ตสูงที่สุดร้อยละ 99 รองลงมาคือกลุ่มอายุน้อยกว่า 15 ปี ร้อยละ 96.4 ส่วนกลุ่มอายุ 75 ปีขึ้นไป มีการใช้อินเทอร์เน็ตต่ำที่สุดร้อยละ 23.9 ซึ่งแสดงให้เห็นว่ากลุ่มผู้สูงอายุใช้อินเทอร์เน็ตอย่างจำกัด ส่วนมิติด้านเพศเทียบกลุ่มอายุ พบว่า มีความใกล้เคียงกัน เว้นแต่กลุ่มอายุ 75 ปีขึ้นไปที่มีความแตกต่างกันเล็กน้อย

การใช้งานอินเทอร์ในอัตราที่ค่อนข้างต่ำในกลุ่มผู้สูงอายุอาจจะเกิดจากหลายปัจจัย รวมถึงการรู้และทักษะทางดิจิทัล ดังเช่นที่งานวิจัยของสถาบันพระปกเกล้าที่เผยแพร่เมื่อปี 2564 ซึ่งได้สำรวจสถานะความเป็นพลเมืองกับการรู้ดิจิทัล พบว่ากลุ่มช่วงอายุ 57 ปีขึ้นไป มีค่าเฉลี่ยการรู้ดิจิทัลต่ำกว่าทุกกลุ่ม[170]

ความเร็วในการเชื่อมต่อ

การจัดอันดับ Speedtest Global Index โดย Ookla เมื่อเดือนสิงหาคม 2565 โดยพิจารณาจากความเร็วในการเชื่อมต่ออินเทอร์เน็ตมือถือและประจำที่ ซึ่งนำเสนอการจัดอันดับจากค่าเฉลี่ย (ใช้ค่ามัธยฐาน (Median))[171] ของความเร็วในการดาวโหลด[172]

ภาพที่ 3.4 ความเร็วในการเชื่อมต่ออินเทอร์เน็ตมือถือและประจำที่ในประเทศไทย เดือนสิงหาคม 2565



ที่มา Thailand Median Speeds August 2022

ความเร็วการเชื่อมต่ออินเทอร์เน็ตประจำที่ของไทยอยู่ในลำดับที่ 3 จาก 182 ประเทศ รองจากสิงคโปร์และชิลี ตามลำดับ โดยมีความเร็วเฉลี่ยในการดาวโหลดเท่ากับ 188.75 เมกะบิตต่อวินาที (Mbps) และความเร็วเฉลี่ยในการอัปโหลดเท่ากับ 154.96 เมกะบิตต่อวินาที (Mbps) และมีค่า Latency เท่ากับ 5 มิลลิวินาที (ms)

---

[170] ศุภณัฐ เพิ่มพูนวิวัฒน์, ศรัณยุ หมั้นทรัพย์, จารุวรรณ แก้วมะโน. 2564. รายงานวิจัย เรื่อง ความเป็นพลเมือง: บทสำรวจสถานะความเป็นพลเมืองกับการรู้ดิจิทัล. สำนักส่งเสริมการเมืองภาคพลเมือง สถาบันพระปกเกล้า. หน้า 99. https://www.kpi.ac.th/knowledge/research/data/1194?page=4

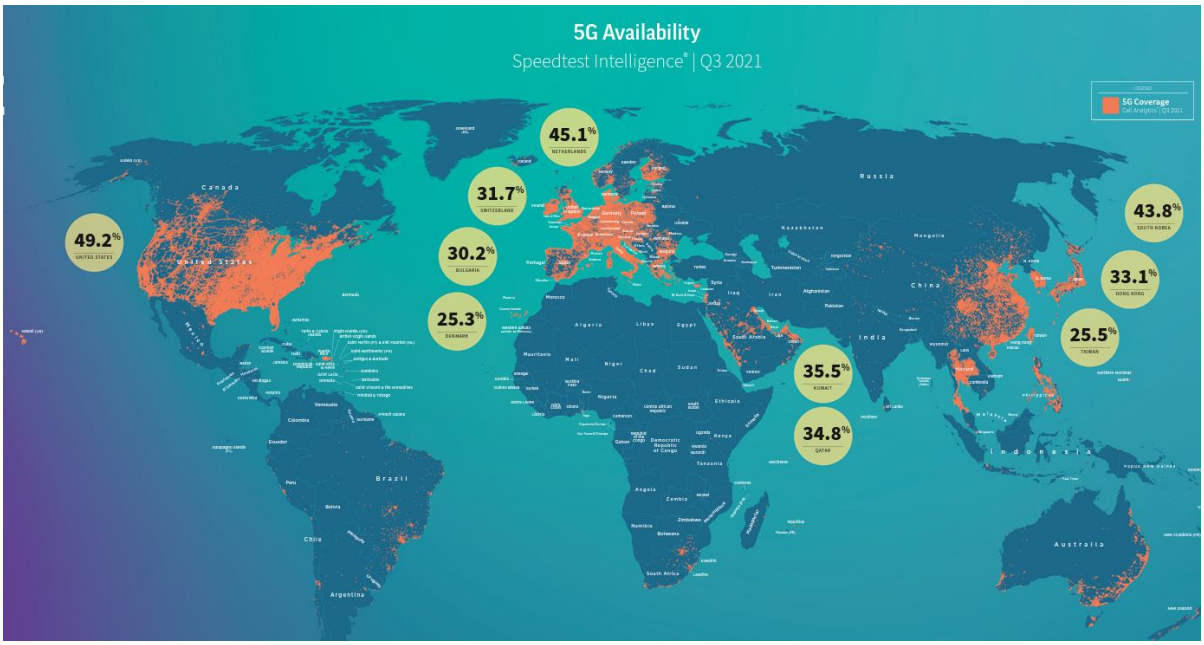
[171] ค่ามัธยฐานคือการวัดที่รวบรวมประสบการณ์ของผู้ใช้ทั่วไป ในแง่สถิติ ค่ามัธยฐานมีแนวโน้มที่จะได้รับอิทธิพลจากค่าผิดปกติน้อยกว่าค่าเฉลี่ย

[172] Thailand Median Speeds August 2022. https://www.speedtest.net/global-index/thailand#mobile

ส่วนความเร็วของการเชื่อมต่ออินเทอร์เน็ตบนมือถือ ประเทศไทยอยู่ในลำดับที่ 52 จาก 140 ประเทศ โดยอยู่ในอันดับ 4 ของเซียน รองจากบรูไน สิงคโปร์ และเวียดนาม ตามลำดับ โดยมีความเร็วเฉลี่ยนในการดาวโหลดเท่ากับ 35.16 เมกะบิตต่อวินาที (Mbps) และความเร็วเฉลี่ยในการอัปโหลดเท่ากับ 12.75 เมกะบิตต่อวินาที (Mbps) และมี Latency เท่ากับ 23 มิลลิวินาที (ms)

ประเทศไทยมีการเปิดประมูลคลื่น 5G ไปเมื่อต้นปี 2563 และหากพิจารณาจากภาพด้านล่างจะพบว่า ประเทศไทยเป็นหนึ่งในประเทศที่มีคลื่น 5G ครอบคลุมมากเป็นอันดับต้น ๆ ของโลก[173]

ภาพที่ 3.5 แผนที่ความพร้อมใช้งาน 5G ทั่วโลก



ที่มา Ookla’s State of 5G Worldwide poster[174]

2) ความสามารถในการจ่ายได้ (Affordability)

ราคาของบริการโทรคมนาคม รวมถึงอินเทอร์เน็ตถือเป็นหนึ่งในอุปสรรคสำคัญในการเข้าถึงและใช้งานอินเทอร์เน็ต การตรวจสอบราคาเป็นเรื่องยาก เนื่องจากราคาขึ้นอยู่กับประเภทบริการ การรวมกลุ่มของบริการ ผู้ประกอบการที่แตกต่างกัน นอกจากนี้ ความสามารถในการจ่ายได้นั้น ไม่ได้ขึ้นอยู่กับราคาและรายได้เท่านั้น แต่ยังขึ้นอยู่กับตัวเลือกการใช้จ่ายอื่นด้วย

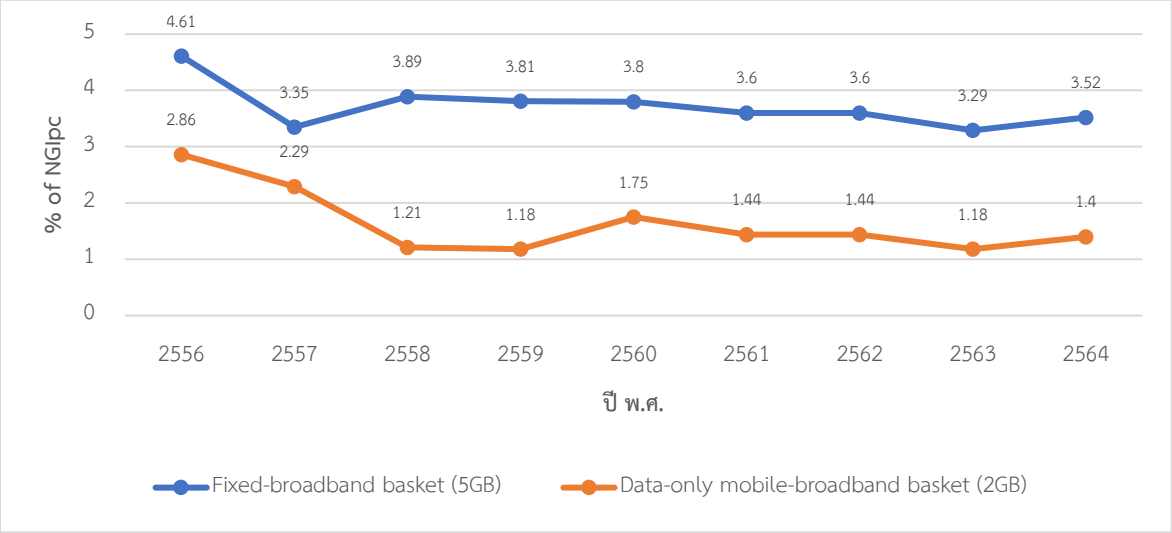
[173] โปรดดู OOKLA 5G MAP™. https://www.speedtest.net/ookla-5g-map

[174] https://www.ookla.com/articles/worldwide-state-5g-poster-download และหากดูข้อมูลอัพเดทกว่าโปรดดูที่ https://www.speedtest.net/ookla-5g-map

การทำให้บรอดแบนด์มีราคาไม่แพงเป็นขั้นตอนสำคัญในการบรรลุการเชื่อมต่อสากลตามเป้าหมายการสนับสนุนบรอดแบนด์ ค.ศ. 2025 (2025 Broadband Advocacy Targets) ของคณะกรรมการบรอดแบนด์เพื่อการพัฒนาที่ยั่งยืน (Broadband Commission for Sustainable Development) ซึ่งเป้าหมายที่ 2 กำหนดให้ภายในปี 2568 (ค.ศ. 2025) ค่าบริการบรอดแบนด์ระดับเริ่มต้นในประเทศที่มีรายได้ต่ำและปานกลาง ควรต่ำกว่า 2 % ของรายได้มวลรวมประชาชาติ (GNI) ต่อเดือนต่อหัว (GNI per capita)[175]

ITU ได้จัดทำข้อมูล “ตะกร้าราคา ICT (ICT Price Baskets)” ของแต่ละประเทศ โดยแสดงเป็นเปอร์เซ็นต์ของรายได้รวมประชาชาติ (GNI) ต่อหัว (GNI per capita) เพื่อแสดงราคาที่สัมพันธ์กับขนาดเศรษฐกิจของแต่ละประเทศ ซึ่งชี้ไปที่ความสามารถในการจ่ายได้ของบริการ ICT แต่ละรายการในระดับประเทศ โดยแบ่งออกเป็น 5 ตะกร้า (Baskets) รวมถึงบรอดแบนด์ประจำที่ (Fixed broadband) และบรอดแบนด์มือถือ (เฉพาะข้อมูลเท่านั้น) [176]

แผนภูมิที่ 3.2 ราคาบรอดแบนด์ประจำที่ และบรอดแบนด์มือถือของไทย ระหว่างปี 2556 - 2565



ที่มา ITU, ICT Price Baskets[177]

หากดูแนวโน้มรายปีตามแผนภูมิที่ 3.2 จะพบว่า ค่าบริการบรอดแบนด์มือถือเฉพาะข้อมูลเท่านั้น (2GB) ของไทยมีแนวโน้มลดลงหลังจากปี 2557 และในปี 2564 มีแนวโน้มเพิ่มขึ้นจากปี 2563 เล็กน้อย แต่ยังคง

[175] Broadband Commission for Sustainable Development, ITU, UNESCO, https://www.broadbandcommission.org/advocacy-targets/2-affordability

[176] ดูรายละเอียดใน ITU. https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/IPB.aspx

[177] https://www.broadbandcommission.org/advocacy-targets/2-affordability/

ต่ำกว่าเป้าหมายที่คณะกรรมการบรอดแบนด์เพื่อการพัฒนาที่ยั่งยืนกำหนด คือ 2 เปอร์เซ็นต์ของรายได้รวมประชาชาติ (GNI) ต่อเดือนต่อหัว

จากข้อมูลปี 2564 ความสามารถในการจ่ายของบริการบรอดแบนด์มือถือของไทยอยู่ในลำดับที่ 84 มีค่าเฉลี่ยอยู่ที่ 1.40 เปอร์เซ็นต์ของรายได้รวมประชาชาติ (GNI) ต่อเดือนต่อหัว โดยอยู่ในลำดับที่ 6 ของอาเซียน รองจากสิงคโปร์ บรูไน เวียดนาม อินโดนีเซีย และมาเลเซีย ตามลำดับ

ส่วนความสามารถในการจ่ายของบริการบรอดแบนด์ประจำที่ของไทยมีแนวโน้มลดลงระหว่างปี 2561 – 2563 แต่ก็ยังสูงกว่าเป้าหมายที่คณะกรรมการบรอดแบนด์เพื่อการพัฒนาที่ยั่งยืนกำหนดคือ 2 เปอร์เซ็นต์ของรายได้รวมประชาชาติ (GNI) ต่อเดือนต่อหัว และยังสูงกว่าค่าเฉลี่ยของภูมิภาคเอเชีย-แปรซิฟิก ในปี 2564 ที่มีค่าเฉลี่ยอยู่ที่ 3.08 % ของรายได้มวลรวมประชาชาติ (GNI) ต่อเดือนต่อหัว โดยค่าบริการมีแนวโน้มเพิ่มขึ้นในปี 2564 โดยอยู่ในลำดับที่ 90 มีค่าเฉลี่ยอยู่ที่ 3.52 เปอร์เซ็นต์ของรายได้ประชาชาติ (GNI) ต่อหัว (GNI per capita) โดยอยู่ในลำดับที่ 4 ของอาเซียน รองจากสิงคโปร์ บรูไน และมาเลเซีย ตามลำดับ

เมื่อดูประกอบกับรายงาน Inclusive Internet Index ปี 2564 ในส่วนของ “ความสามารถในการจ่ายได้” พบว่ามีข้อมูลที่ค่อนข้างสอดคล้องกัน ซึ่งแสดงให้เห็นว่าความสามารถในการจ่ายได้ของไทยในปี 2564 แย่ลงกว่าปี 2563

เมื่อดูรายละเอียดจากรายงานสภาพตลาดโทรคมนาคมของประเทศไทย ประจำปี 2564 โดยสำนักงาน กสทช. ระบุว่า ราคาเฉลี่ยของอินเทอร์เน็ตบรอดแบนด์ประจำที่ คือ 504 บาทต่อเดือน ผู้ให้บริการบรอดแบนด์ประจำที่ มีการแข่งขันกันด้านความเร็วและเทคโนโลยี มีการนำเสนอรายงานส่งเสริมการขายที่หลากหลาย ส่งผลให้ผู้ใช้บริการมีทางเลือกเพิ่มขึ้น[178] ส่วนอินเทอร์เน็ตบรอดแบนด์มือถือ ซึ่งให้บริการทั้งในระบบ 3G, 4G และ 5G มีแนวโน้มของราคาที่ลดลง โดยข้อมูลปี 2564 อัตราค่าบริการอินเทอร์เน็ตมือถือเฉลี่ยอยู่ที่ 0.10 บาท/MB เนื่องจากผู้ให้บริการนำเสนอรายการส่งเสริมการขายที่ให้สิทธิการใช้งานบริการอินเทอร์เน็ตเคลื่อนที่แบบไม่จำกัด (Unlimited) เพื่อตอบสนองความต้องการในการใช้บริการในช่วงสถานการณ์ Covid-19 ทั้งนี้ ข้อมูลอัพเดทจากรายงานข้อมูลการกำกับดูแลกิจการโทรคมนาคม ไตรมาส 1 ปี 2565 ระบุว่ามีอัตราค่าบริการเพิ่มขึ้นเล็กน้อยเป็น 0.11 บาท/MB[179]

นอกจากนี้ มีข้อมูลเพิ่มเติมว่า ราคาที่ลดลงส่วนหนึ่งอาจเป็นผลมาจากการขยายความจุโครงข่ายเคเบิลใต้น้ำระหว่างประเทศ ซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้อนุญาตให้บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ใช้สิทธิการใช้งานความจุจากการขยายระบบเคเบิลใต้น้ำระหว่างประเทศดังกล่าวแล้ว โดยได้กำหนดเงื่อนไขให้ลดค่าบริการลง 20% ซึ่งรายงานของกระทรวงดิจิทัลฯ ระบุว่า การดำเนินการดังกล่าวส่งผลให้

[178] ที่มา กสทช. รายงานอัตราค่าบริการโทรคมนาคมประจำปี 2564 หน้า 78.

[179] กสทช., รายงานข้อมูลการกำกับดูแลกิจการโทรคมนาคม ไตรมาส 1 ปี 2565

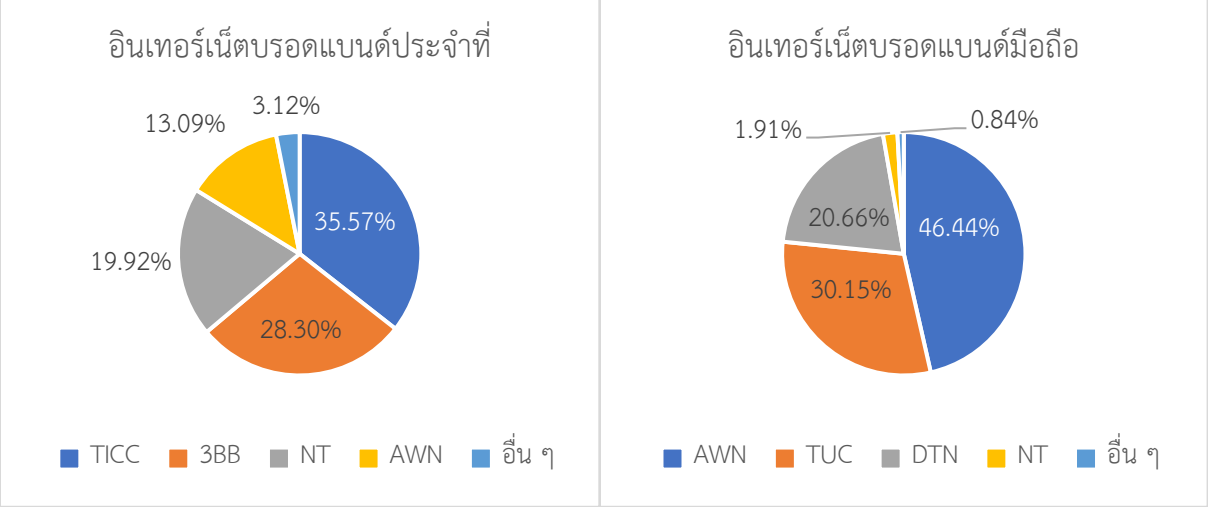
ราคาการให้บริการอินเทอร์เน็ตบรอดแบนด์ในประเทศไทยลดลงอย่างต่อเนื่องตั้งแต่ปี 2562 อัตราลงลงเฉลี่ยไตรมาสละ 2 เปอร์เซ็นต์ อัตราลดลงภายหลังเริ่มโครงการ 15 เปอร์เซ็นต์ พร้อมทั้งระบุว่าปัจจุบันราคาค่าบริการอินเทอร์เน็ตบรอดแบรนด์ต่อวงจรต่ำกว่า 500 บาท/เดือน[180]

ตลาดอินเทอร์เน็ต

สภาพการแข่งขันและการผูกขาดของตลาดการประกอบกิจการภายในประเทศ อาจนำมาซึ่งความท้าทายในการประกันการเข้าถึงอินเทอร์เน็ตในระดับประเทศ ทั้งในมิติคุณภาพและราคาของการบริการ กล่าวคือ หากตลาดมีการแข่งขันน้อย มีลักษณะการผูกขาดโดยรายใหญ่ไม่กี่ราย ย่อมเป็นไปได้ที่การกำหนดราคาบริการจะสูงขึ้น และอาจส่งผลให้ประชาชนบางส่วนไม่สามารถเข้าถึงอินเทอร์เน็ตได้

ผู้ให้บริการอินเทอร์เน็ต (ISP) ในประเทศไทยมีอยู่ประมาณ 20 ราย โดยปี 2564 กสทช. มีการออกใบอนุญาตสำหรับบริการโทรคมนาคมทั้งหมด 721 รายการ ในจำนวนนี้เป็นใบอนุญาตสำหรับอินเทอร์เน็ต 230 รายการ[181] ซึ่ง ISP ภายใต้ใบอนุญาตที่ออกให้โดย กสทช. จะถูกกำกับดูแลภายใต้ พ.ร.บ. กสทช.ฯ ซึ่งกฎหมายดังกล่าวถือเป็นเครื่องมือสำหรับการกำกับดูแลการประกอบกิจการโทรคมนาคม รวมถึงกำกับดูแลไม่ให้มีการควบรวมกิจการและผูกขาดในกิจการโทรคมนาคม

แผนภูมิที่ 3.3 การครองส่วนแบ่งตลาดอินเทอร์เน็ตในประเทศไทย ปี 2564



ที่มา กสทช. รายงานสภาพตลาดโทรคมนาคมของประเทศไทย ประจำไตรมาสที่ 3 ปี 2564.

[180] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. รายงานผลการดำเนินงานของรัฐบาล พลเอกประยุทธ์ จันทร์โอชา นายกรัฐมนตรี ปีที่ 3 (ระหว่างวันที่ 25 กรกฎาคม 2564 - 25 กรกฎาคม 2565) ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. หน้า 7. https://bit.ly/3RyMbXe

[181] กสทช. สรุปสถิติที่น่าสนใจในกิจการโทรคมนาคม ปี 2564. https://bit.ly/3CrG7LW

จากแผนภูมิที่ 3.3 แสดงให้เห็นว่าผู้ให้บริการรายใหญ่ไม่กี่ราย ยังคงครองส่วนแบ่งตลาดอินเทอร์เน็ตในประเทศไทย โดยในปี 2564 บริการอินเทอร์เน็ตบรอดแบนด์ประจำที่ มีผู้ให้บริการรายใหญ่ที่สุด 2 ราย ได้ส่วนแบ่งตลาดเกือบร้อยละ 65 โดยบริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด (TICC) มีส่วนแบ่งสูงสุดร้อยละ 35.57 ตามมาด้วยบริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน) (3BB) ร้อยละ 28.30 และบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (NT) ซึ่งเป็นรัฐวิสาหกิจที่เกิดจากการควบรวม CAT และ TOT เมื่อวันที่ 7 มกราคม 2564 อยู่อันดับที่สาม โดยมีส่วนแบ่งร้อยละ 13.09 ส่วนบริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด (AWN) มีส่วนแบ่งร้อยละ 13.09

สำหรับบริการอินเทอร์เน็ตบรอดแบนด์มือถือ มีผู้ให้บริการรายใหญ่ 3 ราย ครองส่วนแบ่งตลาดเกือบร้อยละ 100 โดยบริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด (AWN) มีส่วนแบ่งสูงสุดร้อยละ 46.44 ตามมาด้วยบริษัท ทรูมูฟ เอช ยูนิเวอร์แซล คอมมิวนิเคชั่น จำกัด (TUC) ร้อยละ 30.15 และบริษัท ดีแทค ไตรเน็ต จำกัด (DTN) อยู่อันดับที่สาม มีส่วนแบ่งร้อยละ 20.66 ซึ่งรายงานสภาพตลาดโทรคมนาคมของประเทศไทย ประจำไตรมาสที่ 3 ปี 2564 ของ กสทช. ยอมรับว่าตลาดอาจมีการกระจุกตัวสูงเล็กน้อยและอาจขาดประสิทธิภาพในการแข่งขัน[182]

AWN หรือเครือข่าย AIS และ TICC หรือเครือข่าย TRUE ถือเป็นผู้เล่นหลักในตลาดบรอดแบนด์ทั้งสองประเภท และหาก TRUE รวมกิจการกับ DTAC ได้สำเร็จก็อาจจะทำให้ส่วนแบ่งตลาดบรอดแบนด์มือถือเปลี่ยนไปด้วย

3) การรู้ดิจิทัล (Digital Literacy)

อินเทอร์เน็ต จะมีความหมายสำหรับผู้คนก็ต่อเมื่อพวกเขามีความรู้และทักษะที่จำเป็นในการใช้งาน การรู้ดิจิทัลและทักษะดิจิทัลจึงมีความสำคัญต่อการเข้าถึง การมีส่วนร่วม และความปลอดภัยในโลกอินเทอร์เน็ต

การรู้ดิจิทัลเป็นอุปสรรคต่อการเข้าถึงอินเทอร์เน็ตสำหรับประชากรส่วนต่างๆ โดยผู้สูงอายุและคนยากจนมีความเสี่ยงเป็นพิเศษ ดังเช่นที่ผลการสำรวจของสำนักงานสถิติแห่งชาติเมื่อปี 2564 แสดงให้เห็นว่ากลุ่มผู้สูงอายุคือกลุ่มที่มีอัตราการเข้าถึงอินเทอร์เน็ตต่ำกว่าทุกกลุ่มอายุ[183]

ผู้กำหนดนโยบายต้องตระหนักว่าการเข้าถึงอินเทอร์เน็ตนั้น นอกจากจำเป็นต้องมีการขยายโครงสร้างพื้นฐาน เนื้อหา และอุปกรณ์แล้ว การสอนทักษะที่จำเป็นสำหรับการใช้งานดิจิทัลเป็นเรื่องสำคัญ และยิ่ง

[182]กสทช. รายงานสภาพตลาดโทรคมนาคมของประเทศไทย ประจำไตรมาสที่ 3 ปี 2564. หน้า 23.

[183] สำนักงานสถิติแห่งชาติ. อ้างแล้ว

สำคัญมากขึ้นเรื่อย ๆ เมื่อเทคโนโลยีพัฒนาไปอย่างรวดเร็วและซับซ้อนขึ้น โดยเฉพาะเมื่อมีการใช้ระบบอัตโนมัติเพิ่มมากขึ้น ซึ่งอาจจะยิ่งเพิ่มความเสี่ยงสำหรับกลุ่มเปราะบางต่าง ๆ มากขึ้นตามไปด้วยเช่นกัน

อดีตผู้รายงานพิเศษว่าด้วยเสรีภาพในการแสดงออกฯ เน้นย้ำถึงความสำคัญของการให้การศึกษาแก่บุคคลเกี่ยวกับความปลอดภัยทางอินเทอร์เน็ต โดยเด็กควรได้รับการฝึกอบรมตั้งแต่อายุยังน้อยในเรื่องความปลอดภัยของอินเทอร์เน็ต[184] และกลยุทธ์การรู้ดิจิทัลควรได้รับการรวมเข้ากับโปรแกรมที่เกี่ยวข้องกับการศึกษา โดยเฉพาะในหลักสูตรของโรงเรียน และในโมดูลการเรียนรู้นอกโรงเรียน รวมถึงการฝึกอบรมครูเกี่ยวกับวิธีใช้ ICT[185]

ประเทศไทยให้ความสำคัญกับการส่งเสริมการรู้ดิจิทัล โดยนโยบายดังกล่าวเป็นนโยบายระดับชาติที่ปรากฏทั้งยุทธศาสตร์ชาติ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ แผนปฏิรูปประเทศ รวมถึงนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

ยุทธศาสตร์ชาติด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์ ระบุถึงการพัฒนาทักษะความสามารถการเรียนรู้ที่สอดรับกับทักษะในศตวรรษที่ 21 รวมถึงความสามารถในการใช้เทคโนโลยี[186] และการพัฒนาทักษะดิจิทัล[187] และยุทธศาสตร์ชาติด้านการสร้างโอกาสและความเสมอภาคทางสังคม กำหนดให้มีการเพิ่มความสามารถและทักษะในการใช้ความรู้และเทคโนโลยีอย่างสร้างสรรค์เพื่อแก้ปัญหาและยกระดับขีดความสามารถของชุมชนในการจัดการตนเองและสร้างหลักประกันให้คนทุกกลุ่มได้รับโอกาสและเข้าถึงการเรียนรู้ตลอดชีวิตเพื่อพัฒนาศักยภาพของตนเองโดยไม่จำกัดวัยหรือเพศสภาวะ[188]

มีหลายภาคส่วนในสังคมไทยที่ดำเนินการในเรื่องการรู้ดิจิทัล ทั้งที่เป็นการดำเนินการโดยบทบาทหน้าที่หรือโดยความสนใจ ในส่วนที่เป็นไปโดยบทบาทหน้าที่นั้นส่วนใหญ่ดำเนินการโดยหน่วยงานภาครัฐและองค์กรอิสระต่างๆ อาทิ กระทรวงศึกษาธิการ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) และสถาบันสื่อเด็กและเยาวชน (สสย.) เป็นต้น ส่วนกลุ่มที่ดำเนินการตามความสนใจส่วนใหญ่คือนักวิจัยและนักวิชาการที่มีความสนใจศึกษาการรู้เท่าทันดิจิทัล ซึ่งที่ผ่านมาสามารถแบ่งความพยายามในการส่งเสริมการรู้ดิจิทัลให้กับพลเมืองออกได้เป็น 3 ประการคือ 1) การส่งเสริมการเข้าถึงดิจิทัล

---

[184] A/66/290, para. 47.

[185] A/66/290, para. 46.

[186] ยุทธศาสตร์ชาติด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์ ข้อ 4.2.2

[187] ยุทธศาสตร์ชาติด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์ ข้อ 4.3.6

[188] ยุทธศาสตร์ชาติด้านการสร้างโอกาสและความเสมอภาคทางสังคม ข้อ 4.4.4

(digital access) 2) การส่งเสริมการใช้งานดิจิทัล (digital usage) และ 3) การส่งเสริมการรู้เท่าทันดิจิทัล (digital literacy)[189]

ข้อมูลจาก ITU ปี 2563[190] ให้ข้อมูลการประเมินทักษะ ICT ของไทย โดยจำแนกเป็น 3 ทักษะ พบว่า ทักษะพื้นฐาน (basic skills)[191] ได้คะแนน 17 (เต็ม 100) ทักษะมาตรฐาน (standard skills)[192] ได้คะแนน 10 (เต็ม 100) และทักษะขั้นสูง (advanced skills)[193] ได้คะแนน 1 คะแนน

รายงานตัวชี้วัด ITU (International Telecommunication Union) 2563 โดยสำนักงานสถิติแห่งชาติ ซึ่งสำรวจทักษะการใช้คอมพิวเตอร์ในแต่ละระดับการศึกษาของประชาชน พบว่า ประชาชนที่มีระดับการศึกษาตั้งแต่ประถมศึกษาลงมา ระดับมัธยมศึกษาตอนต้น มัธยมศึกษาตอนปลาย/อนุปริญญา และระดับอุดมศึกษามีทักษะในการคัดลอก/ตัด/วาง (Copy/Cut/Paste) ข้อความในเอกสารมากที่สุด คือ ร้อยละ 70.4, 89.6, 87.1 และ 90.6 ตามลำดับ รองลงมาคือทักษะในการคัดลอก (Copy) เคลื่อนย้าย (Move) ไฟล์งานหรือแฟ้มงาน (Folder) ร้อยละ 68.1, 88.6, 86.4 และ 90.4 ตามลำดับ ส่วนทักษะที่มีน้อยที่สุดคือ การเขียนโปรแกรมด้วยภาษาคอมพิวเตอร์[194]

นอกจากนี้ งานวิจัยของสถาบันพระปกเกล้าที่เผยแพร่เมื่อปี 2564 ได้สำรวจสถานะความเป็นพลเมืองกับการรู้ดิจิทัล โดยใช้กรอบการรู้ดิจิทัลของ UNESCO ซึ่งประเมินครอบคลุมมิติต่าง ๆ ทั้งความรู้ ความเข้าใจ และทักษะ ได้แก่ 1. การรู้และเข้าใจคอมพิวเตอร์และอุปกรณ์ในการเข้าถึงสื่อดิจิทัล 2. การเข้าถึงและประเมินข้อมูล 3. การจัดการข้อมูล 4. การดัดแปลงข้อมูล 5. การสร้างสรรค์ข้อมูล 6. การส่งต่อข้อมูล และ 7. การใช้ข้อมูลอย่างปลอดภัย ซึ่งสำรวจความคิดเห็นจากกลุ่มตัวอย่าง 400 คน จากจังหวัดตัวแทน 4 ภาค[195] งานวิจัยดังกล่าวชี้ให้เห็นว่าทักษะในการใช้ดิจิทัลของพลเมืองไทยส่วนใหญ่มีระดับการเป็นพลเมืองดิจิทัลในเรื่องของการใช้งานแค่ระดับพื้นฐาน (การเข้าใช้งาน การอ่าน การเขียน การโพสต์ข้อความ การแสดงความเห็น) และ

---

[189] ศุภณัฐ เพิ่มพูนวิวัฒน์, ศรัณยุ หมั้นทรัพย์, จารุวรรณ แก้วมะโน. 2564. รายงานวิจัย เรื่อง ความเป็นพลเมือง : บทสำรวจสถานะความเป็นพลเมืองกับการรู้ดิจิทัล. สำนักส่งเสริมการเมืองภาคพลเมือง สถาบันพระปกเกล้า. https://www.kpi.ac.th/knowledge/research/data/1194?page=4

[190] https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd_THA.pdf

[191] ทักษะพื้นฐาน : ค่าสูงสุดในบรรดากิจกรรมที่ใช้คอมพิวเตอร์ 4 อย่าง ได้แก่ การคัดลอกหรือย้ายไฟล์หรือโฟลเดอร์ การใช้เครื่องมือคัดลอกและวางเพื่อทำซ้ำหรือย้ายข้อมูลภายในเอกสาร การส่งอีเมลพร้อมไฟล์แนบ และการถ่ายโอนไฟล์ระหว่างคอมพิวเตอร์และอุปกรณ์อื่นๆ

[192] ทักษะมาตรฐาน: ค่าสูงสุดของ กิจกรรมที่ใช้คอมพิวเตอร์ 4 อย่าง ได้แก่ การใช้สูตรเลขคณิตพื้นฐานในสเปรดชีต เชื่อมต่อและติดตั้งอุปกรณ์ใหม่ การสร้างงานนำเสนอทางอิเล็กทรอนิกส์ด้วยซอฟต์แวร์การนำเสนอ และค้นหา ดาวน์โหลด ติดตั้งและการกำหนดค่าซอฟต์แวร์

[193] ทักษะขั้นสูง: คุณค่าสำหรับการเขียนโปรแกรมคอมพิวเตอร์โดยใช้ภาษาโปรแกรมเฉพาะทาง

[194] รายงานตัวชี้วัด ITU (International Telecommunication Union) 2563. หน้า 7

[195] ศุภณัฐ เพิ่มพูนวิวัฒน์, ศรัณยุ หมั้นทรัพย์, จารุวรรณ แก้วมะโน. 2564. อ้างแล้ว

ระดับกลาง (การส่งต่อข้อมูล) เท่านั้น ส่วนใหญ่ยังไม่มีทักษะระดับสูง (การผลิตและสร้างสรรค์สื่อดิจิทัล) และยังขาดความตระหนักรู้ในการปกป้องตรวจสอบข้อมูลก่อนเชื่อและส่งต่อไปยังผู้อื่น

การขาดความรู้และทักษะด้านดิจิทัล เป็นอุปสรรคสำคัญสำหรับผู้คนในการเข้าถึงและใช้ประโยชน์จากอินเทอร์เน็ตและเครื่องมือดิจิทัลต่าง ๆ ซึ่งจากข้อมูลแสดงให้เห็นว่าประชาชนไทยยังขาดทักษะดิจิทัลอยู่พอสมควร ขณะเดียวกันประเทศไทยก็มีนโยบายในการส่งเสริมการรู้ดิจิทัล ซึ่งปรากฏทั้งในยุทธศาสตร์ชาติและนโยบายและแผนการพัฒนาดิจิทัลระดับชาติ และหน่วยงานในประเทศทั้งมีหน้าที่รับผิดชอบโดยตรงและสมัครใจก็ได้มีการทำงานในด้านการรู้ดิจิทัล แต่ส่วนใหญ่จะเป็นกิจกรรมรมอบรมให้ความรู้ การส่งเสริมความรู้ผ่านสื่อ กระทรวงศึกษาธิการ ซึ่งรับผิดชอบด้านการศึกษาก็ได้มีการส่งเสริมและทำหลักสูตรและคู่มือเกี่ยวกับเรื่องดังกล่าวเช่นกัน[196] ดังนั้น เพื่อส่งเสริมการรู้ดิจิทัลอย่างครอบคลุม จึงควรให้ความสำคัญกับการผลักดันเข้าสู่ระบบการศึกษาผ่านทั้งหลักสูตรการศึกษาในระบบ การเรียนรู้ตลอดชีวิต รวมถึงการฝึกอบรมสำหรับครู[197]

3.6 สรุปส่งท้าย

อินเทอร์เน็ตได้กลายเป็นสิ่งจำเป็นสำหรับการใช้สิทธิมนุษยชนในยุคดิจิทัล อุปสรรคในการเข้าถึงอินเทอร์เน็ตมักเกิดขึ้นได้จากหลายสาเหตุ ซึ่งรวมถึงการขาดโครงสร้างพื้นฐานทางอินเทอร์เน็ต ค่าใช้จ่ายสูง หรือการขาดทักษะและการไม่รู้ดิจิทัล นอกจากนี้ คนบางกลุ่มมีแนวโน้มที่จะเผชิญกับอุปสรรคในการเข้าถึงเหล่านี้มากกว่ากลุ่มอื่น เป็นสิ่งสำคัญที่ผู้กำหนดนโยบายและผู้มีส่วนได้ส่วนเสียตระหนักถึงความท้าทายเหล่านี้ เพื่อที่อินเทอร์เน็ตจะยังคงเป็นแพลตฟอร์มเปิดที่ส่งเสริมสิทธิมนุษยชนในทุกภาคส่วนของสังคมต่อไปในอนาคต

จากข้อมูลที่นำเสนอข้างต้น แม้ว่าประเทศไทยยังไม่ได้รับรองให้อินเทอร์เน็ตเป็นสิทธิ แต่จากเนื้อหาของรัฐธรรมนูญ กฎหมาย นโยบายระดับชาติที่เกี่ยวข้อง ก็ถือว่าประเทศไทยมีกรอบงานที่เอื้ออำนวยต่อการทำให้อินเทอร์เน็ตเป็นสิ่งที่เข้าถึงได้สำหรับทุกคน และที่ผ่านมา ประเทศไทยก็ได้มีการดำเนินการเพื่อการปรับปรุงโครงสร้างพื้นฐานทางอินเทอร์เน็ตโดยผ่านโครงการต่าง ๆ รวมถึงโครงการเน็ตประชารัฐ ที่มุ่งส่งเสริมการเข้าถึงอินเทอร์เน็ต ดยเฉพาะอย่างยิ่งในพื้นที่ชนบท พื้นที่ห่างไกลและยากต่อการเข้าถึง

---

[196] การประชุมกลุ่มย่อย (ครั้งที่ 1) โครงการศึกษาวิจัยเพื่อพัฒนาข้อเสนอแนะในการส่งเสริมและคุ้มครองสิทธิมนุษยชน กรณีการดำเนินการด้านเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์ (ดิจิทัล) วันที่ 31 มีนาคม 2565.

[197] สำหรับการฝึกอบรมครู โปรดดูแนวทางจาก UNESCO. 2011. UNESCO ICT Competency Framework for Teachers. https://unesdoc.unesco.org/ark:/48223/pf0000213475

แม้งานวิจัยชิ้นนี้จะไม่ได้มีศึกษาผลสำฤทธิ์ของการดำเนินโครงการดังกล่าวอย่างจริงจัง แต่จากข้อมูลสถานการณ์ดังที่กล่าวไป ชี้ให้เห็นแล้วว่าผู้ใช้อินเทอร์เน็ตในประเทศไทยเพิ่มขึ้นต่อเนื่อง ซึ่งส่วนหนึ่งก็อาจมาจากโครงการส่งเสริมการเข้าถึงอินเทอร์เน็ตที่ดำเนินการโดยรัฐบาล และยังคงรักษาสภาพการแข่งขันในตลาดเอาไว้ได้

อย่างไรก็ดี งานวิจัยชิ้นนี้ยังคงเสนอให้มีการพิจารณาว่า ประเทศไทยควรกำหนดให้อินเทอร์เน็ตเป็นสิทธิมนุษยชนหรือไม่ เพราะการรับรองอย่างชัดเจนทางกฎหมาย ก็ย่อมหมายถึงการมีหลักประกันที่มั่นคงยิ่งขึ้น อีกทั้งการรับรองให้เป็นสิทธิ จะทำให้เกิดข้อผูกพันสำหรับรัฐมากขึ้น กล่าวคือ รัฐย่อมมีพันธกรณีในเชิงบวกที่จะต้องทำให้สิทธินั้นบรรลุผล ซึ่งเป็นประเด็นที่ไม่ได้น่ากังวลมากนักสำหรับประเทศไทย เพราะมีการดำเนินการได้ดีอยู่แล้วในช่วงที่ผ่านมา ส่วนอีกมิติหนึ่งคือ รัฐจะเกิดพันธกรณีเชิงลบในการที่จะต้องเคารพและคุ้มครองสิทธิดังกล่าว กล่าวคือรัฐต้องไม่ละเมิดเสียเอง ทั้งโดยการปิดหรือทำให้อินเทอร์เน็ตหยุดชะงัก ซึ่งประเด็นนี้จะมีการอภิปรายต่อในหัวข้อว่าด้วยเสรีภาพในการแสดงออกออนไลน์ นอกจากนี้ รัฐยังมีพันธกรณีในการคุ้มครองไม่ให้บุคคลที่สาม ทำให้อินเทอร์เน็ตต้องหยุดชะงักด้วย

บทที่ 4
เสรีภาพในการแสดงออกกับการจำกัดเนื้อหาออนไลน์

4.1 ส่วนนำ

คุณลักษณะที่โดดเด่นของอินเทอร์เน็ตคือ ความเร็ว การข้ามพรมแดนและการไม่แสดงตัวตน อินเทอร์เน็ตจึงสามารถเป็นทั้งโอกาสและภัยคุกคามด้านสิทธิมนุษยชน อินเทอร์เน็ตกลายเป็นเครื่องมือที่ทรงพลังในการสนับสนุนการเคลื่อนไหวเพื่อความยุติธรรม ความเท่าเทียม และสิทธิมนุษยชน ด้วยการสนับสนุนการใช้เสรีภาพในการแสดงออก สิทธิในการศึกษาหรือการเข้าถึงความรู้ สิทธิในการมีส่วนร่วมทางการเมืองและประชาธิปไตย โดยเฉพาะในสภาวะที่สื่อกระแสหลักอยู่ภายใต้การควบคุม รวมถึงให้โอกาสใหม่ ๆ แก่ภาคประชาสังคมและองค์กรด้านสิทธิมนุษยชนในการส่งเสริมและคุ้มครองสิทธิมนุษยชน

ขณะเดียวกัน อินเทอร์เน็ตอาจถูกใช้เพื่อปลุกระดมให้เกิดความรุนแรง การขยายขอบเขตการเข้าถึงและผลกระทบของความเกลียดชัง การโฆษณาชวนเชื่อ การแพร่กระจายของความเท็จ การข่มขู่คุกคามทางออนไลน์ การกลั่นแกล้งทางออนไลน์ การส่งภาพลามกอนาจารของเด็ก หรืออาชญากรรมทางอินเทอร์เน็ตรูปแบบอื่น รวมถึงสิ่งที่เรียกว่า “การล่าแม่มดทางออนไลน์”[198] ซึ่งอาจส่งผลให้เกิดความรุนแรงในโลกแห่งความเป็นจริงได้ ข้อกังวลเหล่านี้นำมาสู่ข้อถกเถียงเกี่ยวกับการจำกัดเนื้อหาทางอินเทอร์เน็ตหรือออนไลน์

ข้อถกเถียงเกี่ยวกับการจำกัดเนื้อหาออนไลน์ปรากฏขึ้นในสังคมไทยอยู่เสมอ ๆ โดยเฉพาะในช่วงความขัดแย้งทางการเมืองและการระบาดใหญ่ของ COVID-19 ที่คำพูดแสดงความเกลียดชัง (Hate speech) และข่าวปลอมทางออนไลน์ มีการแพร่กระจายอย่างกว้างขวาง[199]

รัฐบาลพยายามตอบสนองต่อปัญหาดังกล่าวด้วยวิธีการที่หลากหลาย รวมถึงการปิดกั้นเนื้อหา การดำเนินคดีกับผู้เผยแพร่ การตั้งศูนย์ต่อต้านข่าวปลอม (Anti-Fake News Center) เพื่อตรวจสอบข่าวสารทางออนไลน์ อย่างไรก็ตาม บ่อยครั้งที่การตอบสนองดังกล่าวของรัฐ ถูกวิจารณ์ว่าจำกัดเสรีภาพในการแสดงออกที่ชอบ

---

[198] ไทยรัฐ และ DTAC. https://www.thairath.co.th/spotlight/dtacstopcyberbullying/ ; Thai PBS. “ล่าแม่มด – เซ็กส์ - ความรุนแรง ภัยเงียบออนไลน์ที่สังคมไทยต้องรู้ให้เท่าทัน”. 9 ตุลาคม 2555. https://www.thaipbs.or.th/news/content/117202

[199] Bangkok Post. การระบาดของ "ข่าวปลอม" ในสถานการณ์ Covid-19. https://www.bangkokpost.com/specials/data-visualization/th

ธรรม โดยเฉพาะการปิดกั้นเนื้อหาหรือดำเนินคดีกับผู้แสดงออกวิพากษ์วิจารณ์รัฐบาลหรือสถาบันของรัฐหรือนโยบายสาธารณะต่าง ๆ

ด้วยเหตุนี้ จึงมีความท้าทายอย่างยิ่งที่จะต้องหาจุดสมดุลของการจำกัดหรือควบคุมเนื้อหาออนไลน์ที่อันตรายเพื่อคุ้มครองสิทธิต่าง ๆ ของผู้คนบนพื้นที่ออนไลน์ รวมถึงประโยชน์อื่น อย่างเช่นความมั่นคงของรัฐ ความสงบเรียนร้อยของประชาชน ไปพร้อม ๆ กับการเคารพและคุ้มครองเสรีภาพในการแสดงออกบนพื้นที่ออนไลน์ ซึ่งแท้จริงแล้วคุณค่าเหล่านั้นไม่ได้ขัดแย้งกัน

ในบทนี้ จึงต้องการศึกษาเกี่ยวกับกรอบหลักการด้านสิทธิมนุษยชนที่เกี่ยวข้องกับการจำกัดเนื้อหาออนไลน์ โดยเฉพาะมิติที่เกี่ยวข้องกับเสรีภาพในการแสดงออก และศึกษาการจำกัดเนื้อหาออนไลน์ในประเทศไทย เพื่อวิเคราะห์ช่องว่างและความท้าทายที่มีอยู่ และจัดทำข้อเสนอแนะที่เกี่ยวข้องต่อไป

4.2 กรอบหลักการทั่วไปของเสรีภาพในการแสดงออก

4.2.1 หลักการทั่วไปเกี่ยวกับเสรีภาพในการแสดงออก

ตราสารสิทธิมนุษยชนระหว่างประเทศยอมรับว่าสิทธิในการมีความคิดเห็นและเสรีภาพในการแสดงออก เป็นสิทธิขั้นพื้นฐานของมนุษย์ทุกคน และเป็นเงื่อนไขที่ขาดไม่ได้สำหรับการพัฒนาบุคลิกภาพอย่างเต็มที่ และเป็นรากฐานของสังคมเสรีในการประกันความโปร่งใสและความรับผิดชอบ ซึ่งมีความสำคัญต่อการส่งเสริมและคุ้มครองสิทธิอื่นๆ อีกมากมาย[200]

สิทธิในการมีความคิดเห็นและเสรีภาพในการแสดงออกถูกรับรองในข้อ 19 ของปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (UDHR) และข้อ 19 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) นอกจากนี้ ยังถูกระบุในตราสารสิทธิมนุษยชนระหว่างประเทศอื่น ๆ ซึ่งได้เน้นย้ำสิทธิดังกล่าวในบริบทที่เฉพาะเจาะจง เช่น สิทธิเด็ก สตรี เป็นต้น[201]

<u>สิทธิที่จะมีความคิดเห็น (Right to hold opinions)</u>

ข้อ 19 (1) ของ ICCPR ระบุว่า “ทุกคนมีสิทธิที่จะมีความคิดเห็นโดยปราศจากการแทรกแซง”

---

[200] CCPR General Comment No. 34, paras. 2 - 4.

[201] เช่น ข้อ 13 ของอนุสัญญาว่าด้วยสิทธิเด็ก ; ข้อ 5 ของอนุสัญญาว่าด้วยการขจัดการเลือกปฏิบัติทางเชื้อชาติ ; ข้อ 21 ของอนุสัญญาว่าด้วยสิทธิของคนพิการ ; ข้อ 1 ของอนุสัญญาว่าด้วยการขจัดการเลือกปฏิบัติต่อสตรี

สิทธิที่จะมีความคิดเห็นถือเป็นสิทธิสัมบูรณ์หรือเด็ดขาด โดยหลักการแล้วจึงไม่อนุญาตให้มีข้อยกเว้นหรือข้อจำกัดใดๆ[202] ความเห็นทุกรูปแบบจะได้รับการคุ้มครอง รวมทั้งความเห็นทางการเมือง ประวัติศาสตร์ ศีลธรรมหรือศาสนา และการกำหนดให้การมีความเห็นเป็นอาชญากรรม การทำร้าย ข่มขู่ หรือสร้างตราบาปแก่บุคคล รวมถึงการจับกุม การกักกัน การไต่สวน หรือการจำคุกเนื่องจากความเห็นของบุคคลนั้น ถือว่าละเมิดข้อ 19 (1) ของ ICCPR[203]

สิทธินี้ ยังรวมถึงสิทธิที่จะไม่มีความคิดเห็น และสิทธิในการเปลี่ยนแปลงความคิดเห็นของตนเมื่อใดก็ได้หรือด้วยเหตุผลใดก็ได้ตามที่บุคคลเลือกอย่างอิสระ[204] การพยายามที่จะข่มขู่ให้บุคคลมีหรือไม่มีความเห็นใด ถือเป็นสิ่งต้องห้าม[205]

สิทธิที่จะมีความคิดเห็น ประกอบด้วย 2 แง่มุม คือ แง่มุมภายใน ซึ่งเชื่อมโยงใกล้ชิดกับสิทธิในความเป็นส่วนตัวและเสรีภาพในความคิด และแง่มุมภายนอก ซึ่งเกี่ยวข้องกับเสรีภาพในการแสดงออก โดยแง่มุมหลังนี้ ได้รับความสนใจมากขึ้นในยุคดิจิทัล เพราะมีการใช้เทคนิคการบิดเบือนโดยโซเชียลมีเดีย เพื่อโน้มน้าวบุคคลในลักษณะที่อาจละเมิดสิทธิที่จะมีความคิดเห็น[206] โลกดิจิทัลอนุญาตให้รัฐและผู้ที่ไม่ใช่รัฐเข้าถึงและมีอิทธิพลต่อความคิดและความเห็นของผู้คนโดยปราศจากการรับรู้หรือยินยอม เช่น การดูแลจัดการเนื้อหาผ่านการแนะนำของแพลตฟอร์มหรือการกำหนดเป้าหมายการโฆษณาในระดับบุคคล เทคนิคดังกล่าวสามารถบิดเบือนกระบวนการคิดโดยไม่สมัครใจหรือไม่ได้รับความยินยอมของบุคคล จึงอาจถือว่าละเมิดสิทธิที่จะมีความคิดเห็น[207]

นอกจากนี้ ในยุคดิจิทัล บุคคลมักเก็บความคิดเห็นในรูปแบบดิจิทัล เช่น ประวัติการค้นหาและเรียกดู การเก็บข้อมูลในระบบคลาวด์ และอีเมลที่เก็บถาวร ทำให้การถือครองความคิดเห็นไม่ได้เป็นเพียงแนวคิดนามธรรมที่อยู่ภายในใจอีกต่อไป และการถือครองความคิดเห็นในพื้นที่ดิจิทัลกำลังถูกโจมตีและแทรกแซง รวมถึงความพยายามในการสอดส่องโดยรัฐและผู้ที่ไม่ใช่รัฐ ซึ่งอาจบ่อนทำลายสิทธิในการมีความคิดเห็น เพราะจะทำให้ผู้คนเกิดความกลัวเกี่ยวกับการเปิดเผยกิจกรรมออนไลน์โดยไม่เต็มใจ เช่น ผลการค้นหาและการเรียกดู เป็นต้น ซึ่งการเข้ารหัสและการไม่เปิดเผยตัวตนทำให้บุคคลสามารถหลีกเลี่ยงหรือบรรเทาการคุกคามดังกล่าวได้[208]

---

[202] CCPR General Comment No. 34, para. 9.; A/HRC/29/32, para 19.

[203] CCPR General Comment No. 34, para. 9.

[204] CCPR General Comment No. 34, para. 9. 10.

[205] CCPR General Comment No. 34, para. 10.

[206] A/HRC/47/25, 13 April 2021, para 33.

[207] A/HRC/47/25, 13 April 2021, para 36. อ้างจาก Evelyn Aswad, “Losing the freedom to be human”, 29 February 2020, p. 329

[208] A/HRC/29/32, para 20, 21.

สิทธิในเสรีภาพแห่งการแสดงออก (Right to Freedom of expression)

มาตรา 19 (2) ของ ICCPR ระบุว่า “บุคคลทุกคนมีสิทธิในเสรีภาพแห่งการแสดงออก สิทธินี้รวมถึงเสรีภาพในการแสวงหา รับ และเผยแพร่ข้อมูลข่าวสารและความคิดทุกประเภท โดยไม่คำนึงถึงพรมแดน ทั้งนี้ ไม่ว่าด้วยวาจา เป็นลายลักษณ์อักษร หรือในการตีพิมพ์ ในรูปแบบของศิลปะ หรือผ่านสื่ออื่นใดที่ตนเลือก”

คำว่า “การแสดงออก” ถูกตีความแบบกว้างๆ เพื่อรวมการสื่อสารทุกรูปแบบเข้าด้วยกัน โดยคำว่า “สื่ออื่นใดที่ตนเลือก” รวมถึงการสื่อสารแบบไม่ใช้คำพูด เช่น รูปภาพ การแต่งกาย หรือท่าทาง ซึ่งสื่อถึงความหมาย และสื่อทุกรูปแบบ ทั้งแบบดั้งเดิม (หนังสือ หนังสือพิมพ์ การแพร่ภาพกระจายเสียง) และสื่อใหม่และที่กำลังพัฒนา รวมถึงอินเทอร์เน็ตและระบบอิเล็กทรอนิกส์ต่าง ๆ[209] ตลอดจนการแสดงออกทางออนไลน์อื่น ๆ ดังที่คณะมนตรีสิทธิมนุษยชน (Human Rights Council) ได้ยืนยันในหลายข้อมติว่า “สิทธิแบบเดียวกันที่ผู้คนมีในออฟไลน์ ต้องได้รับการคุ้มครองทางออนไลน์ด้วย โดยเฉพาะเสรีภาพในการแสดงออก...”[210]

การแสดงออก "ทุกประเภท" ได้รับการคุ้มครอง ซึ่งรวมถึงประเด็นทางการเมือง ศาสนา วัฒนธรรมและศิลปะ การวิจัยทางวิทยาศาสตร์และเทคโนโลยี วารสารศาสตร์ และเนื้อหาประเภทอื่นๆ รวมถึงการแสดงออกที่อาจทำให้ขุ่นเคือง (offend) ตกใจ (shock) หรือรบกวน (disturb)[211] นอกจากนี้ การแสดงออกยังได้รับการคุ้มครอง แม้เนื้อหาที่แสดงออกนั้นจะผิดพลาดไปจากข้อเท็จจริงก็ตาม รวมถึงการแสดงความคิดเห็นที่ผิดพลาดหรือการตีความเหตุการณ์ในอดีตที่ไม่ถูกต้อง[212] และการเผยแพร่โดยผิดพลาดซึ่งข้อความที่ไม่เป็นความจริงและไม่ชอบด้วยกฎหมาย แต่ไม่มีเจตนาร้าย[213]

นอกจากนี้ สิทธิในเสรีภาพแห่งการแสดงออก ยังใช้ "โดยไม่คำนึงถึงพรมแดน" ซึ่งหมายความว่าบุคคลมีสิทธิในการเข้าถึงข้อมูลจากต่างประเทศและสื่อสารกับผู้คนในประเทศอื่น ๆ

สิทธิในการเข้าถึงข้อมูลข่าวสาร (Right of access to information)

สิทธิในการเข้าถึงข้อมูลข่าวสาร หรือสิทธิในการแสวงหาและรับข้อมูลข่าวสาร เป็นส่วนหนึ่งของเสรีภาพแห่งการแสดงออก ตามที่รับรองในข้อ 19 ของ ICCPR

---

[209] CCPR General Comment No. 34, para 12.

[210] A/HRC/RES/20/8. Para 1.; A/HRC/RES/26/13. Para 1. and A/HRC/RES/32/13. Para 1.

[211] CCPR General Comment No. 34, para. 11. ; European Court of Human Rights, Handyside v. the United Kingdom, application No. 5493/72, judgment, 7 December 1976, para. 49.

[212] CCPR General Comment No. 34, para. 49.

[213] CCPR General Comment No. 34, para. 47.

สิทธิในการเข้าถึงข้อมูลข่าวสารยังถูกรับรองในตราสารสิทธิมนุษยชนระหว่างประเทศอื่นด้วย[214] นอกจากนี้ ตัวชี้วัดเป้าหมาย 16.10 ของเป้าหมายการพัฒนาที่ยั่งยืน (SDGs) ยังระบุถึงการสร้างหลักประกันว่าสาธารณชนสามารถเข้าถึงข้อมูลและมีการปกป้องเสรีภาพขั้นพื้นฐาน

สิทธิในการเข้าถึงข้อมูลข่าวสารยังเป็นส่วนสำคัญในการประกันสิทธิที่จะมีส่วนร่วมในกิจการสาธารณะ ซึ่งได้รับการคุ้มครองตามข้อ 25 ของ ICCPR[215]

คณะมนตรีสิทธิมนุษยชนเรียกร้องให้ทุกรัฐประกันว่าจะมีการเปิดเผยข้อมูลข่าวสารที่ถือครองโดยหน่วยงานของรัฐ และนำกฎหมายและนโยบายที่โปร่งใส ชัดเจน และเหมาะสม มาใช้เพื่อให้มีการเปิดเผยข้อมูลที่ถือครองโดยหน่วยงานรัฐอย่างมีประสิทธิภาพ ส่วนข้อจำกัดของการเปิดเผยควรถูกนิยามไว้อย่างชัดเจน อย่างแคบได้สัดส่วน และเท่าที่จำเป็น[216]

สิทธิในการเข้าถึงข้อมูลข่าวสารที่อยู่ในความครอบครองของรัฐเป็นข้อกำหนดพื้นฐานสำหรับการรับรองการมีส่วนร่วมในระบอบประชาธิปไตย การดำเนินกิจการสาธารณะที่ดีและโปร่งใส และมีธรรมาภิบาล ข้อมูลที่อยู่ในความครอบครองของรัฐ จะครอบคลุมถึงข้อมูลที่จัดขึ้นโดยหน่วยงานของรัฐทั้งหมด ไม่ว่าจะเป็นฝ่ายนิติบัญญัติ บริหาร หรือตุลาการ และมีผลบังคับใช้กับหน่วยงานอื่น เมื่อปฏิบัติหน้าที่สาธารณะ[217]

นอกจากนี้ สิทธิในการเข้าถึงข้อมูลข่าวสารไม่ได้ขึ้นอยู่กับการร้องขอข้อมูลเท่านั้น รัฐควรให้ข้อมูลในเชิงรุก โดยการใส่ข้อมูลข่าวสารของรัฐบาลที่เป็นประโยชน์สาธารณะให้เป็นสาธารณะสมบัติ (public domain) และควรใช้ความพยายามทุกวิถีทางเพื่อประกันว่าการเข้าถึงข้อมูลดังกล่าวเป็นไปโดยง่าย รวดเร็ว มีประสิทธิภาพ และสามารถนำไปใช้ได้จริง โดยควรกำหนดขั้นตอนที่จำเป็นสำหรับการเข้าถึงข้อมูล เช่น การออกกฎหมายเสรีภาพของข้อมูล เป็นต้น และควรจัดให้มีการดำเนินการตามคำขอข้อมูลอย่างทันท่วงที ไม่ควรมีค่าธรรมเนียมสำหรับการขอข้อมูลที่เป็นอุปสรรคต่อการเข้าถึงข้อมูลโดยไร้มีเหตุผล เจ้าหน้าที่ควรให้เหตุผลในการปฏิเสธการเข้าถึงข้อมูล ควรให้มีการอุทธรณ์กรณีที่มีการปฏิเสธการเข้าถึงข้อมูล ตลอดจนในกรณีที่ไม่สามารถตอบสนองต่อคำขอข้อมูลข่าวสารได้[218]

ทั้งนี้ การออกแบบและการดำเนินการตามกฎหมายว่าด้วยเสรีภาพของข้อมูลข่าวสาร ควรได้รับการชี้นำโดยหลักการของ (ก) การเปิดเผยสูงสุด (ข) พันธกรณีในการเผยแพร่ (ค) การส่งเสริมรัฐบาลแบบเปิด

---

[214] อาทิ อนุสัญญาว่าด้วยสิทธิของเด็ก (ข้อ 17) และอนุสัญญาว่าด้วยสิทธิของคนพิการ (ข้อ 9)

[215] CCPR General Comment No. 25, para. 25

[216] A/HRC/RES/31/32, para. 13 ; A/HRC/RES/34/20, para. 5 (b).

[217] CCPR General Comment No. 34, para 7, 18.

[218] CCPR General Comment No. 34, para 19.

(ง) ขอบเขตของข้อยกเว้นที่จำกัด (จ) กระบวนการเพื่ออำนวยความสะดวกในการเข้าถึง และ (ฉ) ต้นทุน โดยบุคคลไม่ควรถูกขัดขวางด้วยค่าใช้จ่ายที่มากเกินไป (ช) การประชุมแบบเปิด การประชุมของหน่วยงานทางปกครองจะเปิดให้สาธารณชนเข้าชมได้ (ซ) การเปิดเผยต้องถูกให้สำคัญมากกว่า (ฌ) การคุ้มครองบุคคลที่เปิดเผยข้อมูล (ผู้แจ้งเบาะแส)[219] ทั้งนี้ กรอบสำหรับการออกกฎหมายเสรีภาพในข้อมูลข่าวสารนั้น อาจดูได้คำแนะนำเพิ่มเติมจากความเห็นทั่วไปของคณะกรรมการสิทธิมนุษยชนแห่งสหประชาชาติ ฉบับที่ 34 (Human Rights Committee, General Comment No. 34) เอกสาร The Public's Right to Know: Principles on Right to Information Legislation ขององค์กร ARTICLE 19[220] และแถลงการณ์ร่วมของผู้รายงานพิเศษแห่งสหประชาชาติว่าด้วยเสรีภาพในการแสดงความเห็นและการแสดงออก ผู้แทน OSCE ด้านเสรีภาพของสื่อ และผู้รายงานพิเศษ OAS ด้านเสรีภาพในการแสดงออก ค.ศ. 2004[221]

4.2.2 หลักการทั่วไปในการจำกัดสิทธิในเสรีภาพแห่งการแสดงออก

สิทธิในเสรีภาพแห่งการแสดงออก ไม่ได้เป็นสิทธิสัมบูรณ์หรือเด็ดขาด จึงสามารถอยู่ภายใต้ข้อจำกัดบางประการภายใต้เงื่อนไขที่เข้มงวดและแคบซึ่งถูกกำหนดในข้อ 19 (3) ของ ICCPR

ข้อ 19 (3) ของ ICCPR ระบุว่า "*การใช้สิทธิตามที่บัญญัติในข้อ 19 (2) ต้องมีหน้าที่และความรับผิดชอบพิเศษควบคู่ไปด้วย การใช้สิทธิดังกล่าวอาจมีข้อจำกัดในบางเรื่อง แต่ทั้งนี้ข้อจำกัดต้องถูกกำหนดไว้ในกฎหมายและจำเป็นต่อ*

ก) สำหรับการเคารพสิทธิหรือชื่อเสียงของผู้อื่น หรือ

ข) เพื่อคุ้มครองความมั่นคงของชาติหรือความสงบเรียบร้อยของประชาชน (หรือสาธารณะ) หรือการสาธารณสุขหรือศีลธรรม"

ผู้รายงานพิเศษแห่งสหประชาชาติว่าด้วยเสรีภาพในการแสดงออกฯ ระบุว่า "หน้าที่และความรับผิดชอบ" ภายใต้มาตรา 19 (3) ไม่ปรากฏในส่วนอื่นของ ICCPR ปรากฏเฉพาะในคำปรารภเท่านั้น ซึ่งเน้นย้ำว่า "ปัจเจกมีหน้าที่ต่อบุคคลอื่นและต่อชุมชนที่ตนสังกัดอยู่..." ถ้อยคำใน ICCPR และในข้อ 29 ของ UDHR ไม่ได้ระบุ

---

[219] A/68/362, 4 September 2013, para. 76.

[220] Article 19, https://www.article19.org/resources/international-standards-right-information

[221] Joint declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression. 6 December 2004. https://www.osce.org/files/f/documents/6/f/38632.pdf

หน้าที่หรือความรับผิดชอบของปัจเจกบุคคลต่อรัฐ ดังนั้น คำว่า “หน้าที่และความรับผิดชอบ” ไม่ได้เพิ่มการสนับสนุนอำนาจรัฐในการจำกัดสิทธิแต่อย่างใด[222]

ข้อ 19 (3) ของ ICCPR ประกอบกับคำแนะนำของกลไกสิทธิมนุษยชนแห่งสหประชาชาติ[223] ได้ให้กรอบในการจำกัดสิทธิในเสรีภาพแห่งการแสดงออก หรือที่เรียกว่า “การทดสอบสามส่วน” ได้แก่ 1) ความชอบด้วยกฎหมาย (Legality) 2) วัตถุประสงค์ที่ชอบธรรม (Legitimate objective) และ 3) ความจำเป็น (Necessity) และได้สัดส่วน (Proportionality) โดยรัฐมีภาระในการพิสูจน์ข้อจำกัดว่าเป็นไปตามการทดสอบดังกล่าวหรือไม่[224]

1) ความชอบด้วยกฎหมาย (Legality) ข้อ 19 (3) กำหนดให้การจำกัดต้องกำหนดโดยกฎหมาย (Provided by law) ซึ่งถือเป็นข้อกำหนดของหลักความชอบด้วยกฎหมาย (Legality) ซึ่งกฎหมายที่กำหนดข้อจำกัดจะต้องเป็นไปตามกฎเกณฑ์ดังต่อไปนี้[225]

- กำหมายต้องมีความชัดเจน แม่นยำ และคาดหมายได้ เพื่อให้บุคคลสามารถตรวจสอบและควบคุมความประพฤติของตนได้ และให้คำแนะนำแก่ผู้บังคับใช้กฎหมายเพื่อที่จะทราบว่าการแสดงออกประเภทใดบ้างที่อยู่ภายใต้การจำกัด และเป็นการป้องกันไม่ให้มีการใช้ดุลยพินิจตามอำเภอใจในการจำกัดเสรีภาพในการแสดงออก[226] คำศัพท์ เช่น “ความมั่นคงของชาติ” “การต่อสู้กับการก่อการร้าย” “สุดโต่ง (extremism)” หรือ “ยุยงให้เกิดความเกลียดชัง” รวมถึงคำศัพท์อื่น ๆ เช่น “ความสงบเรียบร้อย” “ศีลธรรมของสังคม” และ "ก่อความวุ่นวายต่อระเบียบสังคม" ควรถูกนิยามอย่างชัดเจนและแคบ[227]
- กฎหมายต้องเข้าถึงได้โดยสาธารณะ เพื่อให้บุคคลสามารถทราบอย่างเพียงพอถึงสิ่งที่ต้องห้ามและไม่ให้เกิดการเซ็นเซอร์ตัวเองเกินกว่าที่กฎหมายกำหนด

---

[222] A/71/373, 6 September 2016, para 8.

[223] CCPR General Comment No. 34, para 21 - 36.; A/HRC/17/27, 16 May 2011 ; A/71/373, 6 September 2016. และโปรดดู Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, adopted in 1985 (E/CN.4/1985/4, annex) และ Article 19. 1 October 1995. The Johannesburg Principles on National Security, Freedom of Expression and Access to Information

[224] CCPR General Comment No. 34, para 27

[225] CCPR General Comment No. 34, paras. 24-26.

[226] A/HRC/47/25, 13 April 2021, para 40.

[227] A/71/373, 6 September 2016, paras. 13 – 14. ; Joint Declaration on media independence and diversity in the digital age, 2 May 2018. Para 3.f. (Joint Declaration, 2018).
https://www.ohchr.org/Documents/Issues/Opinion/JointDeclaration2May2018_EN.pdf

- กฎหมายต้องสอดคล้องกับพันธกรณีภายใต้กฎหมายสิทธิมนุษยชน รวมถึงหลักการห้ามเลือกปฏิบัติ และการกำหนดบทลงโทษต้องสอดคล้องกับกฎหมายสิทธิมนุษยชน กฎหมายที่กำหนดโทษที่โหดร้ายและผิดปกติ ถือว่าไม่สอดคล้อง[228]

2) วัตถุประสงค์หรือเป้าหมายที่ชอบธรรม (Legitimate objective/goal) กฎหมายที่จำกัดสิทธิในเสรีภาพแห่งการแสดงออก ต้องมีวัตถุประสงค์ที่ชอบธรรมตามที่กำหนดไว้ในข้อ 19 (3) (a) และ (b) ของ ICCPR ได้แก่ การเคารพสิทธิหรือชื่อเสียงของผู้อื่น การคุ้มครองความมั่นคงของชาติ ความสงบเรียบร้อยของประชาชน หรือการสาธารณสุขหรือศีลธรรมเท่านั้น ไม่มีเหตุอื่นใดนอกจากนี้ที่ชอบธรรมสำหรับการจำกัดสิทธิในเสรีภาพแห่งการแสดงออก[229]

- การเคารพในสิทธิหรือชื่อเสียงของบุคคลอื่น รวมถึงสิทธิมนุษยชนที่รับรองใน ICCPR และกฎหมายสิทธิมนุษยชนระหว่างประเทศอื่น[230]
- การคุ้มครองความมั่นคงของชาติ ซึ่งกลไกสิทธิมนุษยชนของสหประชาชาติ และเอกสารการตีความด้านสิทธิมนุษยชนต่าง ๆ ได้แนะนำว่า เหตุผลด้านความมั่นคงของชาติ ควรใช้เฉพาะในสถานการณ์ที่ผลประโยชน์ของชาติทั้งมวลตกอยู่ในอันตราย รวมถึงการคุ้มครองความเป็นอิสระทางการเมืองของรัฐและบูรณภาพแห่งดินแดน และไม่ควรใช้เหตุผลด้านความมั่นคงของชาติเป็นข้ออ้างในการปกป้องรัฐบาลจากความอับอายหรือปกปิดการกระทำผิด หรือใช้เป็นเหตุผลในปราบปรามหรือระงับจากข้อมูลสาธารณะที่เป็นประโยชน์สาธารณะ หรือดำเนินคดีนักข่าว นักปกป้องสิทธิมนุษยชน หรืออื่นๆ[231]
- ความสงบเรียบร้อยของประชาชน (หรือสาธารณะ) จะต้องถูกจำกัดให้อยู่ในสถานการณ์เฉพาะ[232]

---

[228] CCPR General Comment No. 34, para 26

[229] CCPR General Comment No. 34, para 22

[230] CCPR General Comment No. 34, para 28

[231] CCPR General Comment No. 34, para 30; Siracusa Principles, Ibid. ; The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, principle 2 (b) ; A/71/373, 6 September 2016, para. 18.

[232] A/71/373, 6 September 2016, para. 18. ; Siracusa Principles. Ibid. paras. 22 – 24.

- การสาธารณสุข หรือศีลธรรม เป็นสิ่งที่กำหนดได้ยาก และศีลธรรมอาจเปลี่ยนแปลงได้ตลอดเวลาและข้ามวัฒนธรรม ดังนั้น ข้อจำกัดต้องอยู่บนหลักการที่ไม่ได้มาจากประเพณีเดียว[233] ข้อจำกัดต้องยึดมั่นในหลักการไม่เลือกปฏิบัติ[234]

อนึ่ง กลไกสิทธิมนุษยชนแห่งสหประชาชาติได้ตีความและให้ข้อเสนอแนะเกี่ยวกับการจำกัดเนื้อหาบางประเภทที่ไม่ชอบธรรมหรือไม่อาจยอมรับได้ (Impermissible restrictions) ดังนี้[235]

- การอภิปรายเกี่ยวกับนโยบายรัฐบาลและทางการเมือง รวมถึงการวิพากษ์วิจารณ์รัฐบาล หรือระบบสังคมการเมืองที่ดำเนินการโดยรัฐบาล การรายงานเกี่ยวกับสิทธิมนุษยชน กิจกรรมของรัฐบาล และการทุจริตในรัฐบาล กิจกรรมทางการเมือง สันติภาพ ประชาธิปไตย และการแสดงความเห็นเกี่ยวกับศาสนาหรือความเชื่อ[236]
- การวิพากษ์วิจารณ์หรือดูหมิ่นประเทศชาติ รัฐหรือสัญลักษณ์ของรัฐ รัฐบาล หน่วยงานของรัฐ หรือเจ้าหน้าที่ของรัฐทั้งในประเทศและต่างประเทศ[237] ทั้งนี้ การลงโทษการวิพากษ์วิจารณ์รัฐบาลหรือเจ้าหน้าที่ของรัฐเป็นการเซ็นเซอร์ในลักษณะที่บ่อนทำลายการมีส่วนร่วมสาธารณะและการอภิปรายโดยตรง และขัดต่อวัตถุประสงค์ของ ICCPR ข้อ 19[238]
- การแสดงออกในเรื่องที่เป็นสาธารณประโยชน์ รวมถึงการวิพากษ์วิจารณ์รัฐบาลและผู้นำทางการเมืองและคำพูดของนักการเมือง และบุคคลสาธารณะอื่น ๆ การจำกัดดังกล่าวจำเป็นต้องมีเกณฑ์ขั้นสูงของความชอบด้วยกฎหมาย ความชอบธรรม ความจำเป็นและความได้สัดส่วน และการจำกัดตีความอย่างแคบ มีเวลาจำกัด และหลีกเลี่ยงการจำกัดการอภิปรายทางการเมือง[239]
- การห้ามการไหลของข้อมูลและความคิดอย่างเสรี รวมถึงการห้ามหรือปิดสิ่งพิมพ์หรือสื่ออื่น และการใช้มาตรการทางปกครองและการเซ็นเซอร์ในทางที่ผิด
- การเข้าถึงหรือการใช้เทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงวิทยุ โทรทัศน์ และอินเทอร์เน็ต

---

[233] CCPR General Comment No. 34, para 32.

[234] CCPR General Comment No. 34, para 32. ; CCPR General comment No. 22 ; Joint declaration, May 6 2014, para 1 (e)-(f), https://www.osce.org/fom/118298

[235] HRC Resolution No. 12/16, 12 October 2552, para 5 (p)(i). ; CCPR General Comment No. 34 ; The Johannesburg Principles, Principle 7.

[236] CCPR General Comment No. 34, para. 43 ; A/HRC/47/25, 13 April 2021, para 42.

[237] The Johannesburg Principles, Principle 7.

[238] A/67/357; A/71/373, 6 September 2016, para. 29.

[239] CCPR General Comment No. 34, para.38 ; A/HRC/47/25, 13 April 2021, para 42.

- การจำกัดเพียงเพราะ “ข้อมูลเท็จ (misinformation)” และ “ความจริงที่บิดเบือน (distorted truth)” ถือเป็นข้อจำกัดที่ไม่ชอบธรรมตามข้อ 19 (3)[240]
- การลงโทษการแสดงความคิดเห็นเกี่ยวกับข้อเท็จจริงทางประวัติศาสตร์ที่ผิดพลาดหรือการตีความเหตุการณ์ในอดีตที่ไม่ถูกต้อง[241]

ทั้งนี้ เมื่อรัฐอ้างเหตุผลความชอบธรรมในการจำกัดเสรีภาพในการแสดงออก รัฐนั้นต้องพิสูจน์ให้เห็นถึงลักษณะที่เฉพาะเจาะจงและเป็นรายกรณีเกี่ยวกับลักษณะที่แท้จริงของภัยคุกคาม และความจำเป็นและได้สัดส่วนของการดำเนินการเฉพาะ โดยเฉพาะอย่างยิ่งการชี้ให้เห็นความเชื่อมโยงโดยตรงและใกล้ชิด (immediate) ระหว่างการแสดงออกและภัยคุกคามนั้น[242]

3) ความจำเป็น (necessity) และได้สัดส่วน (proportionality)

ข้อจำกัดไม่เพียงแต่ต้องเป็นไปตามกฎหมายสำหรับวัตถุประสงค์ที่ชอบธรรมข้างต้นเท่านั้น แต่ข้อจำกัดจะต้องสอดคล้องกับหลักความจำเป็นและได้สัดส่วนด้วย

ข้อจำกัดต้อง "จำเป็น" เพื่อปกป้องวัตถุประสงค์ที่ชอบธรรมอย่างใดอย่างหนึ่งที่กล่าวถึงข้างต้น ซึ่งหมายความว่า รัฐภาคีมีหน้าที่ต้องพิสูจน์ถึงความจำเป็นและสัดส่วนของการดำเนินการเฉพาะ[243]

และภายใต้หลักความได้สัดส่วน มาตรการจำกัดใด ๆ จะต้องได้สัดส่วนกับการคุ้มครองวัตถุประสงค์ที่ชอบธรรม กล่าวอีกนัยหนึ่ง ข้อจำกัดต้องได้สัดส่วนในการบรรลุประโยชน์ที่ได้ถูกคุ้มครอง โดยการประเมินข้อจำกัดว่าได้สัดส่วนหรือไม่นั้น ต้องพิจารณารูปแบบการแสดงออกที่เป็นประเด็น ตลอดจนวิธีการเผยแพร่[244]

องค์ประกอบของความได้สัดส่วนอีกประการหนึ่งคือ การจำกัดต้องไม่กว้างเกินไป และแทรกแซงการใช้สิทธิน้อยที่สุด โดยต้องไม่ทำให้สิทธิตกอยู่ในอันตราย (not put in jeopardy the right itself) และความสัมพันธ์ระหว่างสิทธิกับข้อจำกัด และระหว่างบรรทัดฐานกับข้อยกเว้นต้องไม่กลับกัน (reversed)[245] ดังนั้น หากมีวิธีการอื่นที่มีประสิทธิภาพในการคุ้มครองวัตถุประสงค์ที่ชอบธรรมที่ถูกอ้างถึง จะต้องใช้วิธีทางเลือกนั้นแทน หรือหากการบรรลุวัตถุประสงค์ที่ชอบธรรมสามารถทำได้ด้วยวิธีการที่หลากหลาย ต้องเลือกวิธีการที่จำกัดสิทธิให้น้อยที่สุด

---

[240] David Kaye, A/71/373, 6 September 2016, para. 27.

[241] Human Rights Committee, General comment No. 34 (2011), para. 49

[242] CCPR General Comment No. 34, para. 35. .; Johannesburg Principles, Principle 6(c)

[243] CCPR General Comment No. 34, para. 35.

[244] CCPR General Comment No. 34, para. 34.

[245]CCPR General Comment No. 34, para 21.

หลักความได้สัดส่วนยังจำเป็นสำหรับการกำหนดมาตรการลงโทษสำหรับการจำกัดเสรีภาพในการแสดงออก ผู้รายงานพิเศษว่าด้วยเสรีภาพในการแสดงออกฯ ได้เน้นย้ำว่า การลงโทษทางอาญาถือเป็นการแทรกแซงอย่างร้ายแรงต่อเสรีภาพในการแสดงออก และเป็นการตอบสนองที่ไม่ได้สัดส่วน ยกเว้นกรณีที่ร้ายแรงที่สุด[246]

นอกจากนี้ ข้อจำกัดที่ถูกกำหนดขึ้นจะต้องบังคับใช้โดยองค์กรที่เป็นอิสระจากอิทธิพลทางการเมือง การค้า หรืออิทธิพลซึ่งไม่ถูกรับรองอื่น (unwarranted influences) ในลักษณะที่ไม่เป็นไปตามอำเภอใจหรือเลือกปฏิบัติ และมีการป้องกันที่เพียงพอต่อการละเมิด รวมถึงสิทธิในการเข้าถึงศาลหรือตุลาการที่เป็นอิสระ[247]

4.2.3 กรอบการจำกัดเนื้อหาภายใต้หลักประกันสิทธิในเสรีภาพแห่งการแสดงออก

เมื่อพิจารณาจากกรอบกฎหมายสิทธิมนุษยชนระหว่างประเทศ ประกอบกับความเห็นของผู้เชี่ยวชาญภายใต้กลไกสิทธิมนุษยชนแห่งสหประชาชาติ[248] โดยเฉพาะข้อเสนอของ Frank La Rue อดีตผู้รายงานพิเศษว่าด้วยเสรีภาพในการแสดงความคิดเห็นและการแสดงออกฯ ได้เน้นย้ำถึงการให้แยกความแตกต่างระหว่างเนื้อหาที่ผิดกฎหมาย ซึ่งรัฐต้องห้ามภายใต้กฎหมายระหว่างประเทศ และสิ่งที่ถูกพิจารณาว่าเป็นอันตราย ก้าวร้าว น่ารังเกียจ หรือไม่พึงประสงค์ แต่รัฐไม่จำเป็นต้องห้าม หรือทำให้เป็นอาชญากร โดยเขาแนะนำให้แยกความแตกต่างระหว่างการแสดงออก 3 ประเภท ซึ่งเรียกร้องให้มีการตอบสนองทางกฎหมายและเทคโนโลยีที่แตกต่างกัน ได้แก่[249]

- การแสดงออกที่ก่อให้เกิดความผิดภายใต้กฎหมายระหว่างประเทศ ซึ่งอาจดำเนินคดีทางอาญาได้
- การแสดงออกที่ไม่ควรถูกลงโทษทางอาญา แต่อาจมีความสมเหตุสมผลที่จะจำกัด และการดำเนินคดีทางแพ่ง
- การแสดงออกที่ไม่ก่อให้เกิดการลงโทษทางอาญาหรือทางแพ่ง แต่ยังคงก่อให้เกิดความกังวลในแง่ของความอดทนอดกั้น (tolerance) ความสุภาพ (civility) และการเคารพผู้อื่น

ARTICLE 19 ซึ่งเป็นองค์กรสิทธิมนุษยชนระหว่างประเทศที่ทำงานเพื่อปกป้องและส่งเสริมเสรีภาพในการแสดงออกและเสรีภาพของข้อมูลทั่วโลก ได้นำเสนอ The Hate Speech Pyramid ในเอกสาร

---

[246] A/HRC/47/25, 13 April 2021, para 41.

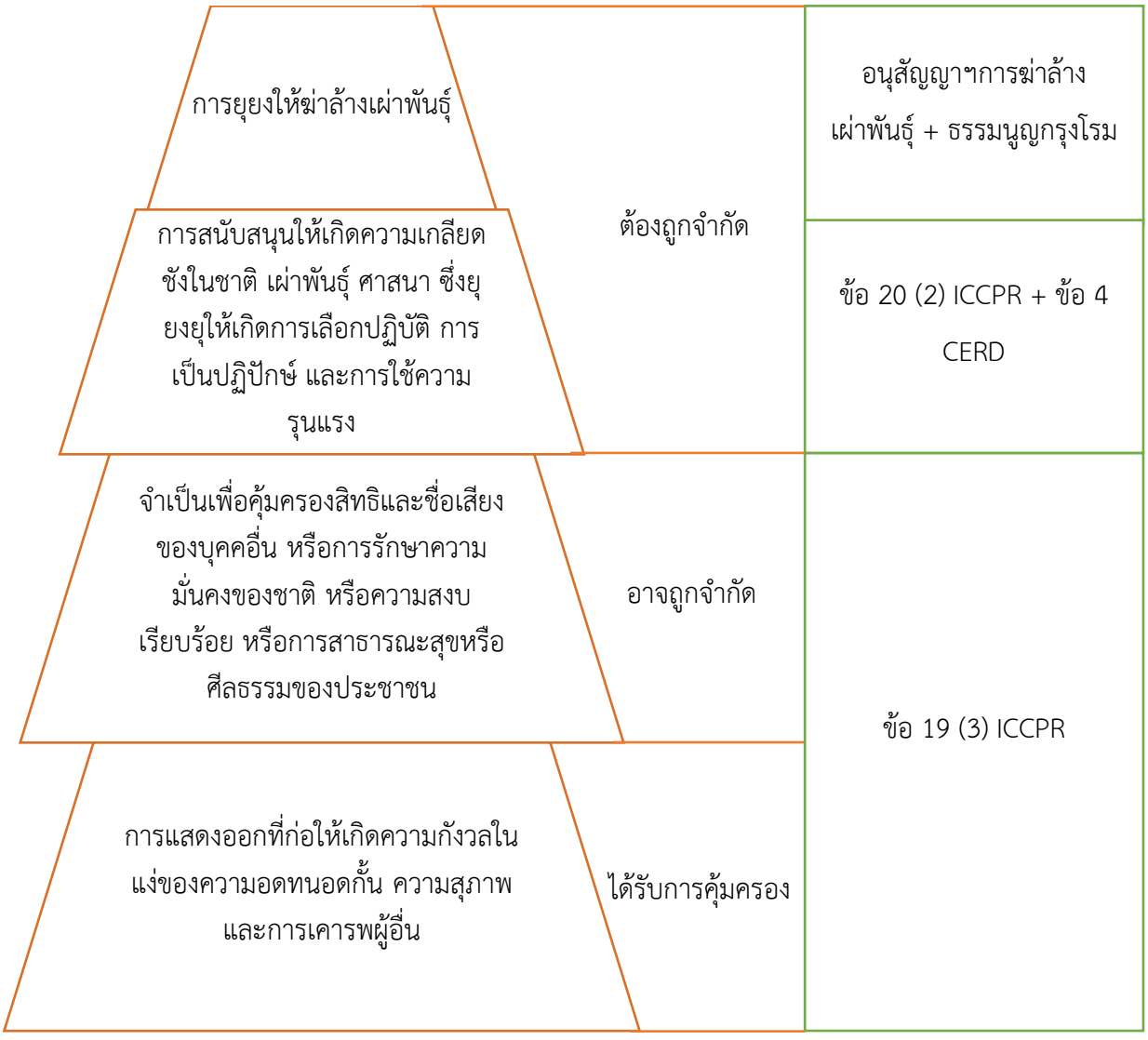
[247] A/67/357, 7 September 2012, para. 42. ; A/HRC/17/27

[248] อาทิ A/HRC/17/27, 16 May 2011, para. 24.; A/66/290, 10 August 2011, para. 18.

[249] Frank La Rue, A/66/290, 10 August 2011, para. 18.

“Hate Speech” Explained: A Toolkit (2015) และถูกนำมาอ้างอิงต่อโดยองค์การสหประชาชาติในยุทธศาสตร์และแผนปฏิบัติการของสหประชาชาติว่าด้วยวาจาสร้างความเกลียดชัง (United Nations Strategy and Plan of Action on Hate Speech, 2020) ซึ่งแม้เอกสารจะนำเสนอในบริบทของวาจาสร้างความเกลียดชังเป็นหลัก แต่ผู้วิจัยเห็นว่ากรอบดังกล่าวสามารถใช้เป็นแนวทางในการพิจารณาจัดการเนื้อหาที่เป็นอันตรายหรือไม่พึงประสงค์อื่นภายใต้กรอบเสรีภาพในการแสดงออกได้

ภาพที่ 4.1 ปิรามิดวาจาสร้างความเกลียดชัง (The Hate Speech Pyramid)



ที่มา ARTICLE 19, The ‘Hate Speech Pyramid’, 2015 and United Nations Strategy and Plan of Action on Hate Speech, 2020

ยุทธศาสตร์และแผนปฏิบัติการของสหประชาชาติว่าด้วยวาจาสร้างความเกลียดชัง ได้ให้คำอธิบายเกี่ยวกับปิรามิดวาจาสร้างความเกลียดชังดังกล่าว โดยแบ่งการแสดงออกเป็น 3 ประเภทตามระดับความรุนแรง ภายใต้กฎหมายระหว่างประเทศ ดังนี้[250]

1) ระดับบนสุด (Top Level)

รูปแบบที่รุนแรงที่สุดของวาจาสร้างความเกลียดชัง และเป็นสิ่งต้องห้ามภายใต้กฎหมายระหว่างประเทศ การแสดงออกดังกล่าวรวมถึง (ก) การยุยงให้กระทำการฆ่าล้างเผ่าพันธุ์โดยตรงและโดยสาธารณะ ตามที่กำหนดโดยกฎหมายอาญาระหว่างประเทศ[251] และ (ข) การสนับสนุนให้เกิดความเกลียดชังในชาติ เชื้อชาติ หรือศาสนาใด ๆ ที่ยุยงให้เกิดการเลือกปฏิบัติ ความเกลียดชัง หรือความรุนแรง ตามที่กำหนดไว้ในข้อ 20 (2) ของ ICCPR และข้อ 4 ของอนุสัญญาระหว่างประเทศว่าด้วยการขจัดการเลือกปฏิบัติทางเชื้อชาติทุกรูปแบบ (CERD)

สำหรับการพิจารณาว่าแสดงออกตามข้อ 20 (2) ของ ICCPR นั้น รุนแรงพอที่จะทำให้เกิดความผิดทางอาญาหรือไม่นั้นควรพิจารณาตามเกณฑ์ "การทดสอบเกณฑ์หกส่วน (six-part threshold test)" ที่ระบุไว้ในแผนปฏิบัติการของราบัต (Rabat Plan of Action) [252]

ตารางที่ 4.1 กรอบการประเมินตามเกณฑ์การทดสอบเกณฑ์หกส่วนจากแผนปฏิบัติการราบัต

เกณฑ์	ตัวชี้วัด	คำถาม
1. บริบท (Context)	บริบททางกฎหมาย การเมือง สังคม และเศรษฐกิจ	• มีความขัดแย้งที่ดำเนินการต่อเนื่องหรือมีเหตุการณ์ความรุนแรงต่อกลุ่มที่ตกเป็นเป้าหมายหรือไม่ • กฎหมายยอมรับอัตลักษณ์ของบุคคลหรือกลุ่มที่ตกเป็นเป้าหมายหรือไม่ • มีกฎหมายต่อต้านการเลือกปฏิบัติหรือไม่ และสอดคล้องกับบรรทัดฐานและมาตรฐานด้านสิทธิมนุษยชนระหว่างประเทศหรือไม่ • สื่อรายงานเกี่ยวกับกลุ่มที่ตกเป็นเป้าหมายอย่างไร ถ้าจะมีอยู่บ้าง • สื่อเป็นอิสระหรือไม่

[250] United Nations. (2020). United Nations Strategy and Plan of Action on Hate Speech : Detailed Guidance on Implementation for United Nations Field Presences. Pages 12 – 15.

[251] ข้อ 3 (c) ของอนุสัญญาว่าด้วยการป้องกันและลงโทษความผิดอาญาฐานฆ่าล้างเผ่าพันธุ์ ; ข้อ 6 25 (3) (e) ของธรรมนูญกรุงโรมว่าด้วยศาลอาญาระหว่างประเทศ.

[252] Rabat Plan of Action, para. 29.

เกณฑ์	ตัวชี้วัด	คำถาม
		• จะมีการเลือกตั้งที่กำลังจะเกิดขึ้นหรือไม่ • อะไรคือบทบาทของการเมืองเชิงอัตลักษณ์ในการรณรงค์หาเสียงเลือกตั้ง • มีผ้าทายหรือโต้แย้งคำพูดแสดงความเกลียดชังหรือไม่ ถ้าเป็นเช่นนั้นพวกเขาเป็นใคร
2. ผู้พูด (Speaker)	ตำแหน่งหรือสถานะของผู้พูดในสังคมและอำนาจหน้าที่หรืออิทธิพลที่มีต่อผู้ฟัง	• ผู้พูดมีอำนาจหรืออิทธิพลในสังคมหรือไม่ • พวกเขาเป็นผู้นำ นักการเมือง เจ้าหน้าที่ของรัฐ ผู้นำทางศาสนาหรือศรัทธา หรือผู้มีอิทธิพลในโซเชียลมีเดียในระดับชาติหรือไม่ • ชื่อเสียงและความนิยมของพวกเขาในสังคมเป็นอย่างไร • ความสัมพันธ์ของพวกเขากับกลุ่มที่ตกเป้าหมายเป็นอย่างไร
3. เจตนา (Intent)	สภาวะทางจิตใจ (state of mind) ของผู้พูด	• ผู้พูดมีเจตนาที่จะมีส่วนร่วมในการสนับสนุนความเกลียดชังต่อบุคคลหรือกลุ่มบุคคลบนพื้นฐานของลักษณะที่ได้รับการคุ้มครองหรือไม่ • ผู้พูดเจตนาที่จะยุยงผู้ฟังให้ต่อต้านกลุ่มเป้าหมายหรือไม่ (ในกรณียุยง) • ผู้พูดเพียงแค่ละเลยหรือประมาทเลินเล่อในการแสดงออกของพวกเขาหรือไม่ • การสื่อสารของผู้พูดหยาบโลน (in poor taste) หรือแสดงให้เห็นถึงการขาดวิจารณญาณหรือไม่
4. เนื้อหาและรูปแบบ (Content and form)	ลักษณะและสไตล์ของการแสดงออก	• คำพูดยั่วยุอารมณ์และตรงไปตรงมามากน้อยเพียงใด • รูปแบบ สไตล์ และลักษณะของข้อโต้เถียง (argument) ที่ใช้ในการพูดเป็นอย่างไร • มีความสมดุลในการใช้ข้อโต้เถียงที่ใช้ในการพูดหรือไม่ • เป็นการแสดงออกในเรื่องประโยชน์สาธารณะหรือไม่

เกณฑ์	ตัวชี้วัด	คำถาม
		● เป็นการแสดงออกทางศิลปะหรือทางวิชาการหรือไม่
5. ขอบเขตและขนาดของการแสดงออก (Extent and magnitude of the expression)	การเข้าถึงการแสดงออก	● การแสดงออกถูกทำให้เป็นสาธารณะเพียงใด ● การแสดงออกถูกเผยแพร่อย่างกว้างขวางเพียงใด ● ผู้ฟังที่ได้สัมผัสกับการแสดงออกนั้นมีขนาดใหญ่แค่ไหน ● การแสดงออกถูกเผยแพร่ทางออฟไลน์และ/หรือทางออนไลน์
6. ความเป็นไปได้ รวมถึงความใกล้จะถึง (Likelihood, including imminence)	ระดับความเสี่ยงของอันตราย	● มีความเป็นไปได้ที่สมเหตุสมผลที่การสื่อสารของผู้พูดจะประสบความสำเร็จในการยุยงให้ผู้ชมกระทำการจริงต่อกลุ่มเป้าหมายหรือไม่ (เฉพาะกรณียุยง) ● มีความเป็นไปได้ที่สมเหตุสมผลที่อันตรายจะเป็นผลมาจากการแสดงออกหรือไม่ (เช่น อันตรายทางร่างกายและ/หรือจิตใจต่อบุคคลหรือกลุ่ม หรือความเสียหายต่อความเชื่อมแน่นในสังคม (social cohesion)) ● อันตรายดังกล่าวจะส่งผลกระทบกับบุคคลเฉพาะในกลุ่มเป้าหมาย (เช่น ผู้หญิง เด็ก หรือเยาวชน) มากกว่าคนอื่นๆ หรือไม่ ● อันตรายจะมีผลกระทบต่อผู้หญิงและผู้ชายแตกต่างกันหรือไม่

ที่มา แปลจาก United Nations Strategy and Plan of Action on Hate Speech : Detailed Guidance on Implementation for United Nations Field Presences[253]

2. ระดับกลาง (Intermediate Level)

คำพูดแสดงความเกลียดชังบางรูปแบบ อาจถูกห้ามภายใต้กฎหมายระหว่างประเทศ แม้ว่าจะไม่ถึงเกณฑ์ตามที่กล่าวถึงข้างต้น โดยเฉพาะการถูกจำกัดภายใต้ข้อ 19 (3) ของ ICCPR ด้วยเหตุนี้ การจำกัดเสรีภาพในการแสดงออกอาจเกิดขึ้นได้เพื่อปกป้องบุคคลจากคำพูดแสดงความเกลียดชังบนพื้นฐานของลักษณะที่ได้รับการ

[253] United Nations. (2020). Ibid. Pages 17 – 18.

คุ้มครอง หรือปัจจัยด้านอัตลักษณ์ (เช่น ผู้หญิง เยาวชน หรือผู้ย้ายถิ่นฐาน)[254] ตราบเท่าที่เป็นไปตามเงื่อนไขของการทดสอบสามส่วนสำหรับการจำกัดเสรีภาพในการแสดงออกภายใต้ข้อ 19 (3) ของ ICCPR

3. ระดับล่าง (Bottom Level)

รูปแบบคำพูดแสดงความเกลียดชังที่รุนแรงน้อยที่สุด ยังคงได้รับการคุ้มครองตามข้อ 19 ของ ICCPR จึงต้องไม่อยู่ภายใต้ข้อจำกัดทางกฎหมาย ซึ่งรวมถึงคำพูดประเภทต่อไปนี้ แม้ว่าจะมีส่วนทำให้เกิดความเกลียดชังก็ตาม

- การแสดงออกที่ให้ขุ่นเคือง ก้าวร้าว ตกใจ หรือรบกวน (offensive, shocking or disturbing)[255]
- การให้อภัยหรือการปฏิเสธเหตุการณ์ทางประวัติศาสตร์ รวมทั้งอาชญากรรมการฆ่าล้างเผ่าพันธุ์หรืออาชญากรรมต่อต้านมนุษยชาติ
- การดูหมิ่นศาสนา รวมทั้งดูหมิ่นความรู้สึกทางศาสนา ขาดความเคารพในศาสนาหรือระบบความเชื่ออื่นๆ และการหมิ่นประมาททางศาสนา
- ข้อมูลข่าวสารที่ผิดพลาด (misinformation) ซึ่งหมายถึงข้อมูลข่าวสารเท็จ โดยไม่มีเจตนาที่จะให้เกิดอันตราย/หรือเจตนาร้าย ข้อมูลข่าวสารบิดเบือน (disinformation) ซึ่งหมายถึงข้อมูลข่าวสารเท็จ โดยรู้อยู่แล้วว่าจะก่อให้เกิดอันตราย และข้อมูลข่าวสารที่แฝงเจตนาร้าย (malinformation) ซึ่งหมายถึงข้อมูลข่าวสารที่แท้จริง เพื่อก่อให้เกิดอันตราย[256]

ทั้งนี้ เว้นแต่ การแสดงออกดังกล่าวเข้าเงื่อนไขของข้อ 19 (3) หรือยังก่อให้เกิดการยุยงให้เกิดความเป็นปรปักษ์ การเลือกปฏิบัติ หรือความรุนแรงตามข้อ 20 (2) แห่ง ICCPR[257]

---

[254] United Nations Strategy and Plan of Action on Hate Speech : Detailed Guidance on Implementation for United Nations Field Presences ระบุถึง "ปัจจัยด้านอัตลักษณ์ (identity factor)" โดยอ้างอิงถึง ศาสนา ชาติพันธุ์ สัญชาติ เชื้อชาติ สีผิว เชื้อสาย เพศ หรือปัจจัยด้านอัตลักษณ์อื่นๆ ซึ่งอิงตามบริบทเฉพาะที่ดำเนินการ และต้องเป็นปัจจัยระบุที่เป็นที่ยอมรับ เช่น ภาษา ความคิดเห็นทางการเมืองหรืออื่น ๆ ความเชื่อ ชาติกำเนิดหรือสังคม ทรัพย์สิน การเกิดหรือสถานะอื่น ๆ รวมถึงแหล่งกำเนิดหรืออัตลักษณ์ของชนพื้นเมือง วรรณะ ความพิการ สถานะสุขภาพ สถานะผู้อพยพหรือผู้ลี้ภัย ที่อยู่อาศัย สถานการณ์ทางเศรษฐกิจและสังคม สถานภาพการสมรสและครอบครัว รสนิยมทางเพศ อัตลักษณ์ทางเพศสภาพ สถานะข้ามเพศ อายุ เผือก และเอชไอวี

[255] Arslan v. Turkey, European Court of Human Rights, 1999.

[256] ดูเพิ่มเติมจาก Colomina, C., Sánchez Margalef, H., Youngs, R., et al.. (2021). The impact of disinformation on democratic processes and human rights in the world, European Parliament. European Parliament, Directorate-General for External Policies of the Union.

[257] Human Rights Committee, general comment No. 34, paras. 48–49; and ARTICLE 19, The Camden Principles on Freedom of Expression and Equality, principle 12.

อย่างไรก็ดี แม้ว่าการแสดงออกประเภทดังกล่าวจะไม่ได้รับอนุญาตให้จำกัดทางกฎหมาย แต่อาจเรียกร้องการตอบสนองที่ไม่ใช่กฎหมายได้ ซึ่งในยุทธศาสตร์และแผนปฏิบัติการของสหประชาชาติว่าด้วยวาจาสร้างความเกลียดชัง และผู้เชี่ยวชาญด้านสิทธิมนุษยชนแห่งสหประชาชาติอื่น ๆ ได้แนะนำให้รัฐและผู้ที่ไม่ใช่รัฐตอบสนองผ่านนโยบาย การปฏิบัติและมาตรการที่หลากหลาย รวมถึงการเน้นจัดการที่รากเหง้าของปัญหา การสนับสนุนการสนทนาข้ามวัฒนธรรมด้วยความอดทนอดกั้น การติดตามรายงานการสร้างความเกลียดชังทางออนไลน์ การส่งเสริมเรื่องเล่าตอบโต้ (counter-speech) การใช้ระบบการศึกษาของโรงเรียนและการรณรงค์ข้อมูลสาธารณะที่เข้มแข็งโดยหน่วยงานของรัฐหรืออื่น ๆ การฝึกอบรม/สิทธิมนุษยชนศึกษา ตลอดจนการให้ความสำคัญกับการเยียวยาเหยื่อที่ได้รับผลกระทบ[258]

นอกจากนี้ รัฐควรสนับสนุนการใช้สิทธิในเสรีภาพในการแสดงออกในเชิงบวก โดยการส่งเสริมสภาพแวดล้อมของการสื่อสารที่เสรี เป็นอิสระและหลากหลาย รวมถึงความหลากหลายของสื่อ ซึ่งเป็นวิธีการสำคัญในการจัดการกับการแสดงออกหรือเนื้อที่ไม่พึงประสงค์ รวมถึงการสร้างความเกลียดชัง การบิดเบือนข้อมูลและการโฆษณาชวนเชื่อ และที่สำคัญรัฐต้องไม่เข้าไปดำเนินการ ให้การสนับสนุน ส่งเสริมหรือเผยแพร่ข้อความที่รู้หรือมีเหตุอันควรรู้ว่าเป็นเท็จ หรือโฆษณาชวนเชื่อเสียเอง ไม่ว่าทั้งโดยจงใจหรือประมาท[259]

---

[258] United Nations. (2020). Ibid. Page 16. ; A/67/357 ; .Rabat Plan of Action ; Gagliardone, Iginio, et al.. (2015). Countering online hate speech. UNESCO.

[259] Joint declaration, 2017 ; A/HRC/RES/12/16, A/HRC/RES/26/13, A/HRC/RES/32/13 ; A/74/486

ตารางที่ 4.2 ตัวอย่างประเภทของเนื้อหาที่ถูกจำกัดได้ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ

ประเภทของเนื้อหา	ตราสารที่เกี่ยวข้อง	การตอบสนองที่เป็นไปได้ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ[63]
สื่อลามกที่เกี่ยวกับเด็ก (Child pornography)	ข้อ 2 (c) และข้อ 3 วรรค 1 ของพิธีสารเลือกรับของอนุสัญญาว่าด้วยสิทธิเด็ก เรื่อง การค้าเด็ก การค้าประเวณี และสื่อลามกที่เกี่ยวกับเด็ก กำหนดให้รัฐภาคีต้องประกันว่า การผลิต แจกจ่าย เผยแพร่ นำเข้า ส่งออก เสนอ ขาย หรือครอบครองเพื่อความมุ่งประสงค์ดังกล่าว ซึ่งสื่อลามกที่เกี่ยวกับเด็ก จะได้รับการป้องกันอย่างเต็มที่ภายใต้กฎหมายอาญา	• กำหนดห้ามโดยกฎหมายอาญาหรือกฎหมายที่มีโทษทางอาญาอย่างเต็มที่ • รัฐยังต้องจัดการกับรากเหง้าของการแสวงประโยชน์จากเด็กแบบองค์รวมและต้องสอบสวนและดำเนินคดีกับบรรดาผู้ต้องรับผิดชอบ นอกจากนี้ ความเป็นส่วนตัวของเหยื่อจะต้องได้รับการคุ้มครองและต้องมีมาตรการคุ้มครองที่เหมาะสมและการดูแลที่ปรับให้เข้ากับความต้องการและลักษณะของเด็ก[64]
การยุยงโดยตรงและโดยสาธารณะให้กระทำการฆ่าล้างเผ่าพันธุ์	ข้อ 3 (c) ของอนุสัญญาว่าด้วยการป้องกันและลงโทษความผิดอาญาฐานฆ่าล้างเผ่าพันธุ์ ระบุว่า การยุยงโดยตรงและสาธารณะเพื่อให้มีการฆ่าล้างเผ่าพันธุ์จะต้องได้รับโทษในฐานความผิดทางอาญา ข้อ 6 และ 25 (3) (e) ของธรรมนูญกรุงโรมว่าด้วยศาลอาญาระหว่างประเทศ	• กำหนดห้ามโดยกฎหมายอาญาหรือกฎหมายที่มีโทษทางอาญาอย่างเต็มที่ • การห้ามในกฎหมายและการจำกัดใดๆ ที่ถูกกำหนดขึ้น เช่น ผ่านการบล็อคหรือลบเนื้อหาทางอินเทอร์เน็ต จะต้องถูกใช้หลังจากการประเมินอย่างรอบคอบถึงภัยคุกคามของการแสดงออกดังกล่าวต่อการยุยงให้ฆ่าล้างเผ่าพันธุ์โดยตรงเท่านั้น รวมถึงการประเมินปัจจัยต่าง ๆ เช่น ผู้พูด ผู้ฟังที่เป็นกลุ่มเป้าหมาย เนื้อหาหรือความหมาย

[63] ARTICLE 19, “Hate Speech” Explained: A Toolkit, p. 19.

[64] A/66/290, 10 August 2011, paras. 21 - 22.

ประเภทของเนื้อหา	ตราสารที่เกี่ยวข้อง	การตอบสนองที่เป็นไปได้ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ[63]
		ของคำพูด บริบททางสังคมและประวัติศาสตร์ รูปแบบการถ่ายทอด และตัวชี้วัดอื่นๆ[65]
การโฆษณาชวนเชื่อเพื่อการสงคราม และ การสนับสนุนให้เกิดความเกลียดชังในชาติ เผ่าพันธุ์ หรือศาสนา ซึ่งยุยงให้เกิดการเลือกปฏิบัติ การเป็นปฏิปักษ์ หรือการใช้ความรุนแรง	ข้อ 20 ของ ICCPR กำหนดให้ *“(1) การโฆษณาชวนเชื่อเพื่อการสงครามเป็นสิ่งต้องห้ามตามกฎหมาย* *(2) การสนับสนุนให้เกิดความเกลียดชังในชาติ เผ่าพันธุ์ หรือศาสนา ซึ่งยุยงให้เกิดการเลือกปฏิบัติ การเป็นปฏิปักษ์ หรือการใช้ความรุนแรง เป็นสิ่งต้องห้ามตามกฎหมาย”* ข้อ 4 ของอนุสัญญาระหว่างประเทศว่าด้วยการขจัดการเลือกปฏิบัติทางเชื้อชาติทุกรูปแบบ ซึ่งกำหนดว่ารัฐภาคี *“(a) จะประกาศให้การเผยแพร่ความคิดที่ตั้งอยู่บนพื้นฐานของความเหนือกว่าทาง*	• ข้อ 20 ของ ICCPR ได้ระบุถึงการตอบสนองเฉพาะที่ต้องการจากรัฐ คือการกำหนดข้อห้ามตามกฎหมาย[66] • กรอบกฎหมายภายในประเทศตามข้อ 20 (2) ของ ICCPR ควรมีความชัดเจน โดยอาจนำคำจำกัดความ[67] เช่น ความเกลียดชัง การเลือกปฏิบัติ ความรุนแรง และการเป็นปฏิปักษ์ ตามที่กำหนดโดยหลักการของแคมเดนว่าด้วยเสรีภาพในการแสดงออกและความเท่าเทียมกัน (The Camden principles on freedom of expression and equality)[68] มาพิจารณาประกอบในการบัญญัติกฎหมาย[69] • การกำหนดกฎหมายภายใต้มาตรา 20 ไม่จำเป็นต้องใช้โทษทางอาญาเสมอไป เฉพาะกรณีที่ร้ายแรงและรุนแรงที่สุด (serious and extreme) ซึ่งผ่านการทดสอบ 6 ส่วน (six-part threshold test) ในแผนปฏิบัติการของราบัตเท่านั้นที่ควรจะถูกกำหนดเป็นความผิด

[65] A/66/290, 10 August 2011, para. 24.

[66] Human Rights Committee, General comment No. 34, para. 51.

[67] A/67/357, paras. 44–46.

[68] พัฒนาโดยองค์กร Article 19 ซึ่งเป็น International Non-government organization. https://www.article19.org/wp-content/uploads/2009/04/Camden-Principles-ENGLISH-web.pdf

[69] Rabat Plan of Action, para. 21; and ARTICLE 19, The Camden Principles on Freedom of Expression and Equality (London, 2009), principle 12.

ประเภทของเนื้อหา	ตราสารที่เกี่ยวข้อง	การตอบสนองที่เป็นไปได้ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ[63]
	เชื้อชาติ หรือความเกลียดชังอันเกิดจากความแตกต่างทางเชื้อชาติ การยั่วยุให้เกิดการเลือกปฏิบัติทางเชื้อชาติ ตลอดจนการกระทำรุนแรงหรือการยุยงให้กระทำการดังกล่าวต่อเชื้อชาติหรือกลุ่มบุคคลที่มีสีผิวหรือชาติพันธุ์อื่น....เป็นการกระทำที่ต้องได้รับโทษตามกฎหมาย *(b) จะประกาศว่าองค์กร กิจกรรมจัดตั้งและกิจกรรมโฆษณาชวนเชื่ออื่นๆ ทั้งหมดซึ่งส่งเสริมและยุยงให้เกิดการเลือกปฏิบัติทางเชื้อชาติ เป็นสิ่งผิดกฎหมายและต้องห้าม...”*	ทางอาญา[70] ได้แก่ (1) บริบท (2) ผู้พูด (3) เจตนาของผู้พูด (4) เนื้อหาหรือรูปแบบของการพูด (5) ขอบเขตของการพูด (6) ความเป็นไปได้ รวมถึง อันตรายที่ใกล้จะถึง (Imminence) ● กรณีที่ไม่ผ่านเกณฑ์การทดสอบดังกล่าว รัฐควรปรับใช้กฎหมายแพ่ง โดยจัดให้มีการเยียวยาที่หลากหลาย รวมถึงการเยียวยาเชิงกระบวนการ เช่น การเข้าถึงความยุติธรรมและการประกันประสิทธิผลของสถาบันภายในประเทศ และการเยียวยาเชิงเนื้อหา เช่น การชดเชยที่เพียงพอ ทันท่วงที และได้สัดส่วนกับความรุนแรงของการแสดงออก ซึ่งอาจรวมถึงการฟื้นคืนชื่อเสียง การป้องกันการเกิดขึ้นอีก และการให้ค่าเสียหายเป็นเงิน[71] ● ข้อ 19 และ 20 ของ ICCPR เข้ากันได้และส่งเสริมกัน การกระทำในข้อ 20 ล้วนอยู่ภายใต้ข้อจำกัดตามข้อ 19 (3) ดังนั้น การจำกัดที่สมเหตุสมผลตามข้อ 20 จึงต้องเป็นไปตามของข้อ 19 (3) ด้วย[72] ● การแสดงออกที่ต้องห้ามภายใต้ข้อ 20 (2) มีองค์ประกอบสำคัญ 2 ประการ ได้แก่ 1) ครอบคลุมเฉพาะการสนับสนุนความเกลียดชังเท่านั้น 2) การสนับสนุนต้องเป็นการยุยงให้เกิดผลลัพธ์อย่างใดอย่างหนึ่ง ได้แก่ การเลือกปฏิบัติ การเป็นปฏิปักษ์ หรือการใช้ความ

[70] A/67/357, 7 September 2012, para. 47. ; Rabat Plan of Action, para. 29.

[71] A/67/357, 7 September 2012, para. 48.

[72] Human Rights Committee, General comment No. 34, para. 50.

ประเภทของเนื้อหา	ตราสารที่เกี่ยวข้อง	การตอบสนองที่เป็นไปได้ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ[63]
		รุนแรง ดังนั้น การสนับสนุนให้เกิดความเกลียดชังบนพื้นฐานของชาติ เผ่าพันธุ์ หรือศาสนาเท่านั้น จึงไม่ถือเป็นความผิดในตัวเอง[73] ● รัฐควรเน้นความพยายามในการต่อสู้กับปัญหารากเหง้าของการพูดเหยียดผิวหรือการพูดที่ก้าวร้าว ซึ่งรวมถึงการส่งเสริมการพูดมากขึ้นเพื่อตอบโต้การแสดงออกในเชิงลบดังกล่าว การปรับปรุงความเข้าใจในหมู่ประชาชนในโลก และสร้างวัฒนธรรมแห่งสันติภาพ[74]
การยุยงให้เกิดการก่อการร้าย (Incitement to terrorism)	ข้อ 19 (3) ของ ICCPR (วัตถุประสงค์ด้านความมั่นคงของชาติ) มติคณะมนตรีความมั่นคงที่ 1624 ปี ค.ศ. 2005 เรียกร้องให้รัฐต่างๆ “ห้ามโดยกฎหมายสำหรับการยุยงให้กระทำการของผู้ก่อการร้ายหรือกลุ่มผู้ก่อการร้าย”[75]	● กฎหมายอาญาในประเทศที่ห้ามการยุยงให้ก่อการร้ายต้องพิสูจน์ตามการทดสอบสามส่วนของการจำกัดสิทธิในเสรีภาพแห่งการแสดงออก[76] ● กฎหมายไม่ควรใช้คำที่คลุมเครือ เช่น "การยกย่อง (glorifying)" หรือ "ส่งเสริม (‘promoting)" การก่อการร้าย ทั้งนี้ การยุยงควรเข้าใจว่าเป็นการเรียกร้องโดยตรงให้มีส่วนร่วมในการก่อการร้าย โดยมีเจตนาที่จะส่งเสริมการก่อการร้าย และในบริบทที่การเรียกร้องนั้นเป็นความรับผิดชอบโดยตรงต่อการเพิ่มโอกาสที่แท้จริงของการเกิดการก่อการร้าย[77]

[73] A/66/290, 10 August 2011, para. 28. ; A/67/357, 7 September 2012, para. 43.

[74] A/66/290, 10 August 2011, para. 83.

[75] UN Security Council resolution 1624. Para 1 (a). adopted unanimously at the 2005 World Summit on 14 September 2005

[76]A/66/290, 10 August 2011, para. 34.

[77] Joint declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 28 December 2005, (Joint Declarations, 2005)

ประเภทของเนื้อหา	ตราสารที่เกี่ยวข้อง	การตอบสนองที่เป็นไปได้ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ[63]
		• การใช้อินเทอร์เน็ตในฐานะที่เป็นวิธีการเชิงบวกในการต่อต้านการยุยงให้เกิดการก่อการร้าย รวมถึงการเผยแพร่เรื่องเล่าตอบโต้ (counter-narrative) อย่างรวดเร็ว ไปยังข้อความสุดโต้งซึ่งเป็นการยั่วยุให้เกิดการก่อการร้าย อาจเป็นยุทธศาสตร์ที่มีประสิทธิภาพมากกว่าการพยายามจำกัดเนื้อหาที่ถือว่ายุยงให้เกิดการก่อการร้าย[78]
การหมิ่นประมาท	ข้อ 19 (3) (a) ของ ICCPR (การเคารพในสิทธิหรือชื่อเสียงของบุคคลอื่น) ข้อ 17 ของ ICCPR ระบุใน (1) ว่า บคคลจะถูกลบหลู่เกียรติและชื่อเสียงโดยไม่ชอบด้วยกฎหมายมิได้ และ (2) บุคคลทุกคนมีสิทธิที่จะได้รับการคุ้มครองตามกฎหมายมิให้ถูกลบหลู่เช่นว่านั้น	• กฎหมายหมิ่นประมาทต้องตราขึ้นด้วยความระมัดระวังเพื่อประกันว่ากฎหมายเป็นไปตามเงื่อนไขของมาตรา 19 (3) ของ ICCPR และต้องไม่ใช้เพื่อยับยั้งเสรีภาพในการแสดงออก[79] • การหมิ่นประมาททางอาญา ไม่ใช่ข้อจำกัดที่สมเหตุสมผลสำหรับเสรีภาพในการแสดงออก และควรถูกยกเลิกหรือลดทอนความเป็นอาชญากรรม หากจำเป็น อาจแทนที่ด้วยกฎหมายหมิ่นประมาททางแพ่งที่เหมาะสม[80] ซึ่งการลงโทษทางแพ่ง ควรเคารพหลักการของความได้สัดส่วน และควรให้ความสำคัญกับการใช้การเยียวยาอื่น ๆ[81]

[78] A/66/290, 10 August 2011, paras. 35 - 36.

[79] CCPR General Comment No. 34, para. 47.

[80] UN, OSCE and OAS Special Rapporteurs for Freedom of Expression. Joint Declaration on Freedom of Expression and the Administration of Justice, Commercialisation and Freedom of Expression and Criminal Defamation. 2002. (Joint Declaration, 2002) https://www.osce.org/files/f/documents/8/f/39838.pdf และโปรดดู CCPR General Comment No. 34, para. 47. ; A/67/357; A/71/373, 6 September 2016, para. 33.

[81] A/HRC/7/14, 28 February 2008, para 43, 78

ประเภทของเนื้อหา	ตราสารที่เกี่ยวข้อง	การตอบสนองที่เป็นไปได้ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ[63]
		• กฎหมายสิทธิมนุษยชนระหว่างประเทศถูกออกแบบขึ้นเพื่อคุ้มครองบุคคล ไม่ใช่ค่านิยมหรือสถาบันที่เป็นนามธรรม เช่น อัตลักษณ์ประจำชาติ ศาสนา สัญลักษณ์ของรัฐ สถาบันหรือผู้แทนของรัฐ เช่น ประมุขแห่งรัฐ[82] • ความจริงของข้อความควรสามารถใช้เป็นข้อต่อสู้เสมอ[83] • กฎหมายหมิ่นประมาทไม่ควรปกป้องบุคคลสาธารณะจากการถูกวิพากษ์วิจารณ์หรือยับยั้งการโต้เถียงในเรื่องประโยชน์สาธารณะ และประโยชน์สาธารณะควรถูกยอมรับในฐานะข้อต่อสู้[84] • ควรละเว้นจากการเสนอบรรทัดฐานใหม่ซึ่งจะมุ่งสู่เป้าหมายเช่นเดียวกับกฎหมายหมิ่นประมาท เช่น การบิดเบือนข้อมูลและการเผยแพร่ข้อมูลเท็จ[85]

[82]CCPR General comment No. 34 (2011), para. 38. ; A/HRC/7/14, 28 February 2008, para 40.

[83] CCPR General comment No. 34 (2011), para. 47.

[84] CCPR General comment No. 34 (2011), para. 47.

[85] A/HRC/7/14, 28 February 2008, para 79.

4.3 เสรีภาพในการแสดงออกและการจำกัดเนื้อหาทางออนไลน์

4.3.1 หลักการทั่วไป

อินเทอร์เน็ตกลายเป็นเครื่องมือหลักสำหรับการใช้สิทธิในเสรีภาพในการแสดงออกและข้อมูล โดยการช่วยอำนวยความสะดวกให้บุคคลในการแสวงหา รับและเผยแพร่ข้อมูลและความคิดทุกประเภทในทันที[86] ดังนั้น อินเทอร์เน็ตที่เปิดกว้างและปลอดภัยจึงควรถูกนับเป็นหนึ่งในข้อกำหนดเบื้องต้นชั้นสำหรับการเพลิดเพลินกับเสรีภาพในการแสดงออกในปัจจุบัน[87]

กรอบกฎหมายสิทธิมนุษยชนระหว่างประเทศที่เกี่ยวข้องกับสิทธิในเสรีภาพในการแสดงออกยังคงมีความเกี่ยวข้องและบังคับใช้กับอินเทอร์เน็ต ดังที่อ้างแล้วว่า “สิทธิแบบเดียวกันที่ผู้คนมีในทางออฟไลน์จะต้องได้รับการคุ้มครองทางออนไลน์ด้วย รวมถึงเสรีภาพในการแสดงออก”[88]

ข้อจำกัดใด ๆ เกี่ยวกับการทำงานของเว็บไซต์ บล็อก หรือระบบอื่นใดบนอินเทอร์เน็ต อิเล็กทรอนิกส์ หรือระบบเผยแพร่ข้อมูลอื่น ๆ รวมถึงระบบที่สนับสนุนการสื่อสารดังกล่าว เช่น ผู้ให้บริการอินเทอร์เน็ตหรือเสิร์ชเอ็นจิ้นจะได้รับอนุญาตเฉพาะในขอบเขตที่เข้ากันได้กับข้อ 19 (3) ของ ICCPR[89] กล่าวคือ ต้องผ่านการทดสอบสามส่วน ได้แก่ (1) ต้องกำหนดโดยกฎหมาย และ (2) มีวัตถุประสงค์ที่ชอบธรรม และ (3) จำเป็นและได้สัดส่วน

นอกจากนี้ ผู้เชี่ยวชาญด้านสิทธิในเสรีภาพแห่งการแสดงออก ได้แนะนำแนวทางเกี่ยวกับการจำกัดเสรีภาพในการแสดงออกทางอินเทอร์เน็ตหรือออนไลน์ไว้ดังนี้[90]

- การประเมินความได้สัดส่วนของการจำกัดเสรีภาพในการแสดงออกทางอินเทอร์เน็ตต้องมีการชั่งน้ำหนักผลกระทบของการจำกัดระหว่างความสามารถของอินเทอร์เน็ตที่จะนำเสนอเสรีภาพแห่งการแสดงออกในเชิงบวกกับการคุ้มครองผลประโยชน์อื่น[91]

---

[86] A/HRC/17/27, para 19.

[87] A/HRC/29/32, para. 11; see also A/HRC/17/27

[88] A/HRC/RES/38/7 ; A/HRC/RES/32/13 ; A/HRC/RES/26/13 ; A/HRC/RES/20/8

[89] CCPR General comment No. 34 (2011), para. 43.

[90] Joint declaration on freedom of expression and the Internet, signed by the UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information on 1 June 2011. (Joint declaration, 2011).

[91] Joint declaration, 2011. Para 1.b.

- ไม่ควรกำหนดข้อจำกัดแบบพิเศษสำหรับการเผยแพร่เนื้อหาทางอินเทอร์เน็ต[92] ไม่ควรกำหนดข้อจำกัดของเนื้อหาบนอินเทอร์เน็ตที่ไปไกลกว่าที่ใช้กับวิธีการจัดส่งเนื้อหาอื่น[93] และรัฐไม่ควรกำหนดบทลงโทษที่รุนแรงกว่าสำหรับการแสดงออกทางออนไลน์เมื่อเทียบกับออฟไลน์[94] ทั้งนี้ กิจกรรมดิจิทัลรูปแบบใหม่หรือแตกต่างจากกิจกรรมออฟไลน์โดยพื้นฐาน (เช่น สแปม)" เท่านั้น ที่ควรอยู่ภายใต้ข้อจำกัดพิเศษที่ออกแบบมาสำหรับการสื่อสารดิจิทัล[95]
- รัฐควรจัดหารายละเอียดอย่างเต็มที่เกี่ยวกับความจำเป็นและเหตุผลในการปิดกั้นเว็บไซต์หนึ่ง ๆ และการพิจารณาว่าเนื้อหาใดควรถูกปิดกั้นจะต้องดำเนินการโดยหน่วยงานตุลาการที่มีอำนาจหรือหน่วยงานที่มีความเป็นอิสระจากอิทธิพลทางการเมือง ทางการค้า หรืออิทธิพลที่ไม่ถูกรับรองอื่นๆ เพื่อประกันว่าการปิดกั้นจะไม่ถูกใช้เพื่อเซ็นเซอร์[96]

4.3.2 สิทธิมนุษยชนกับวิธีการจำกัดเนื้อหาทางออนไลน์

การจำกัดเนื้อทางออนไลน์อาจสามารถทำได้ผ่าน 3 รูปแบบ ดังนี้[97]

1) การจำกัดการเข้าถึงอินเทอร์เน็ต (Access) ซึ่งเกี่ยวข้องกับ (ก) การควบคุมวิธีการเข้าถึง (ผู้ให้บริการคอมพิวเตอร์และอินเทอร์เน็ต) และ (ข) การควบคุมโครงสร้างทางกายภาพของอินเทอร์เน็ต (เกตเวย์ เครือข่ายเคเบิล เราเตอร์ ดาวเทียม และอื่น ๆ) ผู้กระทำการทั้งรัฐและนอกภาครัฐอาจกำหนดระดับการควบคุมที่แตกต่างกันในพื้นที่หนึ่งหรือทั้งสองพื้นที่

2) การจำกัดการทำงานของอินเทอร์เน็ต (functionality) เป็นการควบคุมคุณภาพทางเทคนิคของการใช้อินเทอร์เน็ต โดยเฉพาะ (ก) คุณภาพของการเชื่อมต่อ (แบนด์วิดท์และความเร็ว) (ข) คุณภาพของซอฟต์แวร์การสื่อสาร (เช่น เบราว์เซอร์ อีเมล โปรแกรมแชท ซอฟแวร์ส่งต่อไฟล์ บริการเสียงและวิดีโอ) และ

---

[92] Joint declaration, 2011. Para 1.d.

[93] Council of Europe Committee of Ministers, Declaration on Freedom of Communication on the Internet, 28 May 2003, Principle 1. https://rm.coe.int/16805dfbd5.

[94] Joint Declaration, 2018, paras. 3 (a) and 3(b)

[95] Joint Declaration, 2018, para. 3 (c).

[96] A/66/290, 10 August 2011, para. 82.

[97] Johan Eriksson and Giampiero Giacomello. “Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State”. International Studies Review, Volume 11, Issue 1, March 2009, Pages 205–230, https://doi.org/10.1111/j.1468-2486.2008.01841.x

(ค) โปรโตคอลทางเทคนิคของการสื่อสารทางอินเทอร์เน็ต (IP, TCP, เป็นต้น) ซึ่งโปรโตคอลทางเทคนิคทำให้เกิดการเข้าถึงได้ทั่วโลก ด้วยเหตุนี้ จึงเป็นหนึ่งในแหล่งพลังพื้นฐานที่สุดในการควบคุมอินเทอร์เน็ต นอกจากนี้ การทำงานของอินเทอร์เน็ตอาจได้รับผลกระทบจากการกระทำโดยเจตนา เช่น การโจมตีแบบปฏิเสธการให้บริการ (DDoS Attack) สแปม และไวรัส เป็นต้น รวมถึงอาจจะเกิดจากเหตุการณ์ภายนอก เช่น ไฟฟ้าดับ เป็นต้น

คุณภาพของการเชื่อมต่อและซอฟต์แวร์ถูกควบคุมโดยตลาดเป็นส่วนใหญ่ บริษัทเอกชนโดยทั่วไปมีหน้าที่รับผิดชอบสำหรับแอปพลิเคชัน แบนด์วิดท์ ความเร็วและความเสถียรของการเชื่อมต่ออินเทอร์เน็ต ซึ่งรัฐบาลอาจควบคุมการทำงานของอินเทอร์เน็ตผ่านกฎระเบียบภายในประเทศ เช่น การออกใบอนุญาต และการติดตามตรวจสอบการประกอบกิจการของภาคเอกชน

3) การจำกัดกิจกรรมบนอินเทอร์เน็ตหรือกิจกรรมออนไลน์ (Activity) ซึ่งสามารถทำได้หลายรูปแบบ ได้แก่ (ก) การกรองและการปิดกั้นเนื้อหาทางออนไลน์ (ข) การสอดแนมกิจกรรมออนไลน์ เช่น บันทึกการท่องเว็บ สปายแวร์ และการดักฟังการสื่อสารทางอิเล็กทรอนิกส์ และ (ค) การกำหนดและควบคุมวาทกรรมทางสังคมและการเมืองด้วยวิธีการต่างๆ อาทิ การโฆษณาชวนเชื่อ การใช้กฎหมาย รวมถึงการกำหนดความรับผิดของแหล่งข้อมูลและตัวกลาง ซึ่งเป็นผู้ผลิต ผู้บริโภค และโฮสต์ของเนื้อหาดิจิทัล (โดยเฉพาะ ISP)

ต่อไปจะกล่าวถึงบางรูปแบบของการจำกัดเนื้อหาทางอินเทอร์เน็ต ซึ่งเป็นรูปแบบที่น่ากังวลต่อสิทธิในเสรีภาพแห่งการแสดงออก ดังนี้

<u>การปิด/ตัดการเชื่อมต่ออินเทอร์เน็ต (Internet Shutdowns)</u>

รายงาน Internet shutdowns and human rights ของ Association for Progressive Communications (APC) ซึ่งส่งตามคำขอของ OHCHR เพื่อเป็นข้อมูลสำหรับรายงานเรื่อง internet shutdowns and human rights to the fiftieth session of the Human Rights Council in June 2022 ระบุถึงผลกระทบของการหยุดชะงักของการสื่อสาร การวิจัยแสดงให้เห็นว่าการปิดอินเทอร์เน็ตเป็นอันตรายต่อชุมชน ส่งผลกระทบต่อการพัฒนาเศรษฐกิจ และละเมิดสิทธิมนุษยชนในมิติต่าง ๆ รวมถึงการจำกัดการเข้าถึงข้อมูล การยับยั้งการเข้าถึงการศึกษาและสุขภาพ และบริการอื่นๆ เช่น การธนาคาร เป็นต้น[98]

การปิดระบบอินเทอร์เน็ต (Internet shutdowns) หรือ “kill switches” รวมถึงการทำให้อินเทอร์เน็ตชะลอตัว เกี่ยวข้องกับมาตรการที่มีเจตนาป้องกันหรือขัดขวางการเข้าถึงหรือการเผยแพร่ข้อมูลทาง

[98] https://www.apc.org/sites/default/files/internet_shutdowns_and_human_rights_ohchr_submission_2022.pdf

ออนไลน์ ซึ่งเป็นการละเมิดกฎหมายสิทธิมนุษยชน[99] โดยคณะมนตรีสิทธิมนุษยชนประณามอย่างชัดแจ้งต่อการใช้มาตรการปิดอินเทอร์เน็ต[100] และเรียกร้องให้ทุกรัฐละเว้นและยุติมาตรการดังกล่าว[101]

ผู้รายงานพิเศษฯ เน้นว่าการปิดระบบเป็นการละเมิดเสรีภาพในการแสดงออกและสิทธิอื่น ๆ ดังนั้น จึงจำเป็นผ่านบททดสอบสามส่วนของการจำกัดเสรีภาพในการแสดงออกตามข้อ 19 (3) ของ ICCPR[102]

- การปิดอินเทอร์เน็ตที่ได้รับคำสั่งอย่างลับๆ หรือไม่มีพื้นฐานทางกฎหมายที่ชัดเจน รวมถึงการปิดระบบตามคำสั่งทางกฎหมายและข้อบังคับที่ไม่ชัดเจน หรือกฎหมายและข้อบังคับที่นำมาใช้และดำเนินการอย่างลับๆ หรือกฎหมายที่ไม่เปิดเผยขั้นตอนการดำเนินงานต่อสาธารณะ ซึ่งเอื้อให้เจ้าหน้าที่หลบเลี่ยงการตรวจสอบทางกฎหมายและความรับผิดชอบสาธารณะ เป็นการฝ่าฝืนข้อกำหนดของความชอบด้วยกฎหมาย[103]
- การปิดอินเทอร์เน็ตระหว่างการประท้วง การเลือกตั้ง และกิจกรรมอื่นๆ ที่เป็นประโยชน์สาธารณะเป็นพิเศษ โดยไม่มีการให้คำอธิบายที่ชัดเจน ขัดต่อข้อกำหนดวัตถุประสงค์ที่ชอบธรรม[104]
- การปิดอินเทอร์เน็ตมักจะไม่เป็นไปตามข้อกำหนดความจำเป็น เพราะการปิดอินเทอร์เน็ตยิ่งจะทำให้ประโยชน์ที่มุ่งคุ้มครองตกอยู่ในอันตราย รัฐบาลบางแห่งโต้แย้งว่าเป็นสิ่งสำคัญที่จะห้ามการเผยแพร่ข่าวเกี่ยวกับการโจมตีของผู้ก่อการร้าย เพื่อป้องกันความตื่นตระหนกและการกระทำเลียนแบบ อย่างไรก็ดี พบว่า การรักษาการเชื่อมต่อเครือข่ายอาจบรรเทาความกังวลด้านความปลอดภัยสาธารณะและช่วยฟื้นฟูความสงบเรียบร้อยของประชาชนได้ดีกว่าการปิดเครือข่าย[105]
- โดยทั่วไปการปิดอินเทอร์เน็ตจะไม่เป็นไปตามข้อกำหนดของความได้สัดส่วน เพราะผู้ใช้จะถูกตัดขาดจากบริการฉุกเฉินและข้อมูลด้านสุขภาพ การรายงานเกี่ยวกับวิกฤตการณ์และเหตุการณ์สำคัญ[106]

---

[99] A/HRC/35/22., para. 8.

[100]HRC Resolution No. 44/12.

[101] HRC Resolution No. 2/13, para. 10

[102] A/HRC/35/22, paras. 9 - 15.

[103] A/HRC/35/22, paras. 9 - 10.

[104] A/HRC/35/22, para 11.

[105] A/HRC/35/22, para 14.

[106] A/HRC/35/22, para 15.

- การปฏิเสธสิทธิในการเข้าถึงอินเทอร์เน็ตของปัจเจกบุคคลเพื่อเป็นการลงโทษ ถือเป็นมาตรการที่รุนแรง ซึ่งอ้างความสมเหตุสมผลได้ต่อเมื่อไม่มีมาตรการที่จำกัดน้อยกว่าและเมื่อได้รับคำสั่งจากศาล โดยคำนึงถึงผลกระทบของมาตรการดังกล่าวที่มีต่อการใช้สิทธิมนุษยชน[107]

การปิดกั้นและการกรองเนื้อหา (blocking or filtering of content)

"การกรอง" และ "การปิดกั้น" เป็นคำที่มักใช้สลับกันเพื่ออ้างถึงกิจกรรมที่มุ่งป้องกันไม่ให้ผู้ใช้อินเทอร์เน็ตเข้าถึงเนื้อหาบางอย่าง เช่น การป้องกันไม่ให้ผู้ใช้งานเข้าถึงเว็บไซต์บางแห่ง ไม่สามารถเข้าถึงหมายเลข IP บางชุด ไม่สามารถเข้าถึงโดเมนเนม การลบเว็บไซต์ออกจากเซิร์ฟเวอร์ซึ่งเป็นที่ตั้ง การใช้ซอฟต์แวร์หรือฮาร์ดแวร์ที่ตรวจสอบการสื่อสารและตัดสินใจตามเกณฑ์ที่กำหนดไว้ล่วงหน้าว่าจะป้องกันการรับหรือไม่ หรือการใช้เทคโนโลยีคัดกรองเพื่อป้องกันไม่ให้เข้าถึงเว็บไซต์บางหน้าที่มีถ้อยคำหรือเนื้อหาบางอย่าง เช่น คำว่า “ประชาธิปไตย” และ “สิทธิมนุษยชน”[108]

ความแตกต่างระหว่าง "การกรอง" และ "การปิดกั้น" เป็นเรื่องของขนาดและมุมมอง การกรองมักเกี่ยวข้องกับการใช้เทคโนโลยีที่ปิดกั้นหน้าเว็บโดยอ้างอิงถึงลักษณะเฉพาะบางอย่าง เช่น รูปแบบการรับส่งข้อมูล โปรโตคอล หรือคำหลัก หรือบนพื้นฐานของการรับรู้ถึงความเชื่อมโยงไปยังเนื้อหาที่ถือว่าไม่เหมาะสมหรือผิดกฎหมาย ส่วนการปิดกั้นมักจะหมายถึงการป้องกันการเข้าถึงเว็บไซต์ โดเมน ที่อยู่ IP โปรโตคอล หรือบริการเฉพาะที่รวมอยู่ในบัญชีดำ[109]

นอกจากนี้ การปิดกั้นและการกรองจะแตกต่างจากการลบเนื้อหาออก เพราะการปิดกั้น/การกรองจะจำกัดการเข้าถึงเนื้อหาที่ยังมีอยู่ในเครือข่าย ในขณะที่การลบเนื้อหาออกนั้น เนื้อหาจะถูกลบออกจากเซิร์ฟเวอร์ที่เก็บเลย[110]

การกรองและการปิดกั้น สามารถดำเนินการได้อย่างน้อย 4 ระดับดังต่อไปนี้[111]

- ระดับประเทศ/โครงสร้างพื้นฐาน อาจเรียกได้ว่าเป็นระดับเกตเวย์ ซึ่งถือว่าเป็นวิธีการที่มีประสิทธิภาพมากที่สุด เนื่องจากเป็นการใช้การกรองและการปิดกั้นโดยตรงบน

---

[107] Joint Declaration. 2011. para. 6c).

[108] A/HRC/17/27, 16 May 2011, para 30. ; Article 19, Freedom of Expression Unfiltered: How Blocking and Filtering Affect Free Speech (London, 2016), p. 6. https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf.

[109] Article 19. Ibid. page 7.

[110] Article 19. Ibid. page 7.

[111] Article 19. Ibid. page 10.

โครงสร้างพื้นฐานของอินเทอร์เน็ต หรือผู้ให้บริการเครือข่าย (NSP) ที่ให้การเชื่อมต่ออินเทอร์เน็ตกับผู้ให้บริการอินเทอร์เน็ต (ISP) และรักษาแกนหลัก (backbone) ทางกายภาพ และจุดแลกเปลี่ยนอินเทอร์เน็ต (IXP) ซึ่งรักษาปริมาณการใช้อินเทอร์เน็ตภายในประเทศไว้ภายในโครงสร้างพื้นฐานในท้องถิ่น

- ระดับผู้ให้บริการอินเทอร์เน็ต (ISP) มักจะผ่านสายการเข้าถึงแบบประจำที่ (Fixed) หรือมือถือ เช่น dial-up , DSL, 3G, WiMAX หรือสายเคเบิลใยแก้วนำแสง หน่วยงานของรัฐอาจบังคับให้ผู้ให้บริการอินเทอร์เน็ตติดตั้งซอฟต์แวร์การกรองหรือปฏิบัติตามรายการสอดส่องเฉพาะ
- ระดับเครือข่ายเชิงสถาบัน (institutional networks) เช่น ห้องสมุด โรงเรียน มหาวิทยาลัย อินเทอร์เน็ตคาเฟ่ หรือแม้แต่เครือข่ายคอมพิวเตอร์ขององค์กร
- ระดับผู้ใช้ปลายทาง เป็นการกรองบนคอมพิวเตอร์ส่วนบุคคลแต่ละเครื่อง ซึ่งอาจถูกติดตั้งซอฟต์แวร์การกรองและติดตามตรวจสอบ หรือซอฟต์แวร์ดังกล่าวอาจถูกโจมตีผ่านการโจมตีที่ประสงค์ร้ายและการดาวน์โหลดโดยไม่ได้ตั้งใจ

รัฐมักจะปิดกั้นและกรองเนื้อหาด้วยความช่วยเหลือจากภาคเอกชน ผู้ให้บริการอินเทอร์เน็ตอาจบล็อกการเข้าถึงคำสำคัญ หน้าเว็บ หรือเว็บไซต์ทั้งหมด บนแพลตฟอร์มที่โฮสต์เนื้อหา ประเภทของเทคนิคการกรองจะขึ้นอยู่กับลักษณะของแพลตฟอร์มและเนื้อหาที่เป็นปัญหา เช่น บริษัทโซเชียลมีเดียอาจลบการโพสต์หรือระงับบัญชี เสิร์ชเอนจิน (Search Engines) อาจลบผลการค้นหาที่เชื่อมโยงไปยังเนื้อหาที่ผิดกฎหมาย[112]

การจำกัดการดำเนินงานของเว็บไซต์ บล็อก หรือระบบการเผยแพร่ข้อมูลทางอินเทอร์เน็ตอิเล็กทรอนิกส์ หรือข้อมูลอื่นใด รวมถึงระบบที่สนับสนุนการสื่อสารดังกล่าว เช่น ผู้ให้บริการอินเทอร์เน็ต หรือเสิร์ชเอ็นจิ้น จะได้รับอนุญาตเฉพาะในขอบเขตที่สอดคล้องกับข้อ 19 (3) (การทดสอบสามส่วน) กล่าวคือ[113]

- บทบัญญัติการปิดกั้น/การกรองควรกำหนดไว้อย่างชัดเจนตามกฎหมาย และควรได้รับการออกแบบและนำไปใช้เพื่อให้ส่งผลกระทบกับเนื้อหาที่ผิดกฎหมายเฉพาะ โดยไม่กระทบต่อเนื้อหาอื่น[114]
- เป็นไปตามวัตถุประสงค์ที่ชอบธรรม เพื่อจัดการกับหมวดหมู่ของเนื้อหาที่ห้ามภายใต้กฎหมายระหว่างประเทศ อาทิ สื่อลามกอนาจารของเด็ก เป็นต้น ส่วนการห้ามไซต์หรือ

[112] A/HRC/32/38, 11 May 2016, para. 46.

[113]CCPR General Comment No. 34, para. 43. ; A/HRC/17/27, 16 May 2011, para 70, 71.

[114] A/HRC/17/27. May 16, 2011. Para. 25, 26 and 32.

ระบบการเผยแพร่ข้อมูลเพียงเพราะการวิพากษ์วิจารณ์รัฐบาลหรือระบบสังคมการเมืองที่สนับสนุนโดยรัฐบาล ถือว่าไม่สอดคล้องกับข้อ 19 (3)[115]

- คำสั่งการปิดกั้นต้องจำกัดขอบเขตอย่างเคร่งครัดตามข้อกำหนดของความจำเป็นและได้สัดส่วน ข้อจำกัดที่อนุญาตควรเป็นเนื้อหาเฉพาะ การห้ามทั่วไปในการดำเนินการของไซต์และระบบบางอย่าง ถือว่าไม่สอดคล้องกับข้อ 19 (3)[116]
- การปิดกั้นเนื้อหา จะต้องกระทำโดยหน่วยงานตุลาการ ผู้มีอำนาจ หรือหน่วยงานที่เป็นอิสระจากอิทธิพลทางการเมือง พาณิชย์ หรืออิทธิพลที่ไม่พึงประสงค์อื่นใด เพื่อให้มั่นใจว่าการปิดกั้นจะไม่ถูกใช้เป็นวิธีเซ็นเซอร์[117] และผู้ใช้ต้องได้รับสิทธิในการโต้แย้ง[118]
- ควรมีการรายงานรายชื่อเว็บไซต์ที่ถูกปิดกั้น พร้อมกับรายละเอียดที่อธิบายถึงความจำเป็นและความชอบธรรมที่จะต้องปิดกั้นการเข้าถึงเว็บไซต์แต่ละแห่ง และในหน้าของเว็บไซต์ที่ถูกปิดกั้นจะต้องมีคำอธิบายอย่างชัดเจนว่าเหตุใดจึงถูกปิดกั้น[119]
- ระบบการกรองเนื้อหาที่กำหนดโดยรัฐบาลหรือผู้ให้บริการเชิงพาณิชย์และไม่ได้ควบคุมโดยผู้ใช้ปลายทางเป็นรูปแบบของการเซ็นเซอร์ก่อนหน้าและไม่สมเหตุสมผลในการจำกัดเสรีภาพในการแสดงออก[120]
- ผลิตภัณฑ์ที่ออกแบบมาเพื่ออำนวยความสะดวกในการกรองผู้ใช้ปลายทาง ควรให้ข้อมูลที่ชัดเจนสำหรับผู้ใช้ปลายทางเกี่ยวกับวิธีการทำงานและข้อผิดพลาดที่อาจเกิดขึ้นในแง่ของการกรองแบบกว้างขวางมากเกินไป[121]

มีข้อสังเกตเพิ่มเติมเกี่ยวกับการกรอง ปิดกั้น หรือลบเนื้อหาโดยระบบอัตโนมัติ ซึ่งแม้จะมีประโยชน์ในการช่วยประเมินเนื้อหาที่ผู้ใช้สร้างขึ้นจำนวนมาก[122] แต่ก็ก่อให้เกิดความเสี่ยงต่อการดำเนินการกับ

---

[115] CCPR General Comment No. 34, para. 43. ; Joint declaration, 2011, para. 3.

[116] CCPR General Comment No. 34, para. 43. และโปรดดูตัวอย่างการปิดกั้นที่ไม่ได้สัดส่วนเพิ่มเติมที่ Article 19, Freedom of Expression Unfiltered: How Blocking and Filtering Affect Free Speech (London, 2016), page 18.

[117] A/HRC/17/27, 16 May 2011, para 31. ; A/66/290, 10 August 2011, para. 38.

[118] Article 19 ibid. page 22.

[119] A/HRC/17/27, 16 May 2011, para 70.

[120] Joint declaration, 2011, para. 3.

[121] Joint declaration, 2011, para. 3.

[122] Center for Democracy and Technology, Mixed Messages? The Limits of Automated Media Content Analysis (November 2017), p. 9.

เนื้อหาที่อาจไม่สอดคล้องกับกฎหมายสิทธิมนุษยชน[123] เช่น การปิดกั้นเนื้อหาที่มากเกินไป และการเซ็นเซอร์ก่อนการเผยแพร่ ซึ่งถือว่าไม่ได้สัดส่วน[124]

Association for Progressive Communications (APC) ได้ตั้งข้อสังเกตว่า ระบบอัตโนมัติ เช่น อัลกอริทึมการกรอง อาจส่งผลให้มีการนำเนื้อหาที่ไม่ละเมิดข้อกำหนดในการให้บริการและเป็นสาธารณประโยชน์ออก ตัวอย่างเช่น ระบบอาจทำการลบเนื้อหาที่เป็นหลักฐานของอาชญากรรมสงคราม เนื่องจากถูกตั้งค่าสถานะว่าเป็นเนื้อหาที่มีความรุนแรง/ส่งเสริมแนวคิดสุดโต่ง ดังนั้น APC จึงแนะนำให้การใช้กระบวนการอัตโนมัติ ควรมีความโปร่งใส และควรได้รับการตรวจสอบโดยเจ้าหน้าที่ และผู้ใช้ควรมีความสะดวกในการไล่เบี้ยเพื่อโต้แย้งการลบซึ่งเชื่อว่าเป็นไปตามอำเภอใจหรือไม่ยุติธรรม[125]

<u>การกำหนดความรับผิดของตัวกลาง (intermediary liability)</u>

การเผยแพร่ข้อมูลทางอินเทอร์เน็ตต้องพึ่งพาตัวกลาง หรือบริษัทที่ให้บริการและให้พื้นที่เพื่อให้สื่อสารหรือทำธุรกรรมทางอินเทอร์เน็ตระหว่างบุคคลได้[126] ตัวกลางครอบคลุมตั้งแต่ผู้ให้บริการอินเทอร์เน็ต (ISPs) ไปจนถึงเครื่องมือเพื่อการค้นหา (search engines) บริการจัดทำเว็บบล็อก (blogging services) และบริการเว็บบอร์ดต่างๆ[127]

ตัวกลางทางอินเทอร์เน็ต มีบทบาทสำคัญในการช่วยให้ผู้คนทั่วโลกสามารถสื่อสารกันได้ ตัวกลางจึงอยู่ภายใต้แรงกดดันจากรัฐบาลและกลุ่มผลประโยชน์ รัฐหลายแห่งได้นำกฎหมายที่กำหนดความรับผิดของตัวกลางมาใช้สำหรับกรณีที่ตัวกลางไม่ยอมกรอง ลบข้อมูล หรือปิดกั้นเนื้อหาตามที่รัฐเห็นว่าผิดกฎหมาย[128] การกำหนดให้ตัวกลางต้องรับผิดต่อเนื้อหาที่ผู้ใช้เผยแพร่หรือสร้างขึ้น เป็นมาตรการที่ปิดกั้นการเข้าถึงสิทธิที่มีเสรีภาพในการแสดงความเห็นและการแสดงออกอย่างร้ายแรง เพราะทำให้เกิดการเซ็นเซอร์ตัวเองและมีการควบคุมของภาคเอกชนมากเกินไป และมักเป็นการควบคุมที่เกิดขึ้นโดยไม่โปร่งใสและไม่สอดคล้องกับกระบวนการที่ชอบด้วยกฎหมาย (due process of law)[129]

---

[123] A/HRC/38/35, 6 April 2018, para 56.

[124] A/HRC/38/35, 6 April 2018, para 32.

[125] Association for Progressive Communications (APC). Content regulation in the digital age: Submission to the United Nations Special Rapporteur on the right to freedom of opinion and expression. March 2018, page 16.

[126] Organisation for Economic Cooperation and Development, The Economic and Social Role of Internet Intermediaries (April 2010).

[127] A/HRC/17/27, 16 May 2011, para 38.

[128] A/HRC/17/27, 16 May 2011, para 38, 39.

[129] A/HRC/17/27, 16 May 2011, para 40.

การกำหนดความรับผิดให้กับตัวกลางจึงควรเป็นไปตามมาตรฐานสากลด้านสิทธิมนุษยชน[130] โดยผู้เชี่ยวชาญด้านสิทธิมนุษยชนของสหประชาชาติและระดับภูมิภาค ได้แนะนำแนวทางสำหรับการกำหนดความรับผิดของตัวอย่างไว้ดังนี้

- บุคคลที่เพียงให้บริการอินเทอร์เน็ตทางเทคนิค เช่น การให้การเข้าถึง หรือการค้นหา หรือการส่งหรือการแคชข้อมูล รวมถึงตัวกลางอื่นๆ ทั้งหมด ไม่ควรรับผิดชอบต่อเนื้อหาที่ผู้อื่นสร้างขึ้น ซึ่งเผยแพร่โดยใช้บริการเหล่านั้น ตราบใดที่ไม่ได้เข้าไปแทรกแซงเนื้อหาโดยเฉพาะหรือปฏิเสธที่จะเชื่อฟังคำสั่งศาลให้ลบเนื้อหานั้นออก ทั้งที่สามารถดำเนินการได้ (mere conduit principle)[131]
- ตัวกลางไม่ควรต้องตรวจสอบเนื้อหาที่ผู้ใช้สร้างขึ้น และไม่ควรอยู่ภายใต้กฎการลบเนื้อหานอกกฎหมาย ซึ่งไม่สามารถให้ความคุ้มครองเพียงพอสำหรับเสรีภาพในการแสดงออก[132]
- การขอความร่วมมือใดๆ ต่อผู้เป็นสื่อกลางเพื่อให้ปิดกั้นการเข้าถึงเนื้อหาบางอย่าง เช่น เพื่อประโยชน์ในการบริหารงานยุติธรรมทางอาญา ควรกระทำโดยผ่านคำสั่งจากศาล หรือหน่วยงานผู้มีอำนาจที่เป็นอิสระจากอิทธิพลทางการเมือง พาณิชย์ หรืออิทธิพลที่ไม่พึงประสงค์อื่นใด[133]
- เขตอำนาจศาลในคดีที่เกี่ยวข้องกับเนื้อหาทางอินเทอร์เน็ตควรถูกจำกัดไว้เฉพาะรัฐที่ผู้เขียนสร้างเนื้อหาขึ้น (established) หรือที่เนื้อหาถูกการจัดการโดยเฉพาะ (directed) ไม่ควรสถาปนาเขตอำนาจศาลเพียงเพราะเนื้อหาถูกดาวน์โหลดในบางรัฐ[134]

แม้ว่าระบบ “แจ้งและลบออก (Notice and take down)” เป็นวิธีการหนึ่งเพื่อป้องกันไม่ให้ผู้เป็นตัวกลางมีส่วนร่วมหรือสนับสนุนพฤติการณ์ที่ไม่ชอบด้วยกฎหมาย แต่ก็อาจกลายเป็นเครื่องมือที่รัฐและหน่วยงานเอกชนนำไปใช้อย่างมิชอบได้ ผู้ใช้ที่ได้รับแจ้งจากผู้ให้บริการว่าเนื้อหาของตนเข้าข่ายไม่ชอบด้วยกฎหมาย มักไม่มีช่องทางหรือไม่มีโอกาสที่จะขอให้ทบทวนคำสั่งให้ลบข้อมูลนั้น การขาดความโปร่งใสในกระบวนการตัดสินใจของตัวกลางทำให้คนทั่วไปไม่สามารถเห็นถึงพฤติกรรมเลือกปฏิบัติหรือแรงกดดันที่มีผลต่อการตัดสินใจนั้น และตัวกลางที่เป็นหน่วยงานเอกชนไม่อยู่ในสถานะที่จะสามารถตัดสินใจได้ดีสุดว่าเนื้อหาข้อมูลใด

---

[130] Joint Declaration, 2018, para. 3(d).

[131] Joint Declarations, 2005 ; Joint declaration, 2011. Para 2.a. and 2.b.

[132] Joint declaration, 2011. Para 2.b.

[133] A/HRC/17/27, 16 May 2011, para 75.

[134] Joint Declarations, 2005

ไม่ชอบด้วยกฎหมาย เพราะเป็นภารกิจที่ต้องกระทำอย่างระมัดระวังเพื่อให้เกิดความสมดุลระหว่างประโยชน์ในเชิงการแข่งขันและการปกป้องตนเอง[135]

มีอีกวิธีหนึ่งคือระบบ "แจ้งและแจ้ง (notice and notice)" ซึ่งเรียกร้องให้ตัวกลางแจ้งให้ผู้ใช้ทราบถึงข้อกล่าวหาและให้โอกาสผู้ใช้เหล่านั้นในการลบหรือยืนยันและปกป้องเนื้อหาของตนเอง ในกรณีที่ผู้ใช้ไม่สามารถดำเนินการใดๆ ได้ ตัวกลางควรนำเนื้อหาออก ซึ่งเป็นการคุ้มครองอีกชั้นหนึ่งสำหรับทั้งตัวกลางและเสรีภาพในการแสดงออก เนื่องจากช่วยให้ผู้ใช้มีโอกาสปกป้องเนื้อหาของตนด้วย[136]

ผู้รายงานพิเศษฯ แนะนำให้ตัวกลางนำหลักการชี้แนะของสหประชาชาติว่าด้วยธุรกิจกับสิทธิมนุษยชน (UNGPs) มาใช้เป็นเครื่องมือเพื่อลดผลกระทบที่จะมีต่อผู้ใช้[137] รวมถึงการประเมินผลกระทบด้านสิทธิมนุษยชนอย่างรอบด้าน (Due diligence)[138] ดำเนินการด้วยความโปร่งใส (Transparency) โดยมีการรายงานคำขอของรัฐที่มีรายละเอียดเกี่ยวกับประเภทของคำขอที่ได้รับ การดำเนินการ และเหตุผลของการตัดสินใจดำเนินการเช่นนั้น[139] นอกจากนี้ เมื่อบริษัทได้รับคำขอจากรัฐภายใต้ข้อกำหนดในการให้บริการหรือด้วยวิธีนอกกฎหมายอื่นๆ ควรส่งคำขอเหล่านี้ผ่านกระบวนการปฏิบัติตามกฎหมายและประเมินความถูกต้องของคำขอดังกล่าวภายใต้กฎหมายท้องถิ่นที่เกี่ยวข้องและมาตรฐานสิทธิมนุษยชน[140]

4.4 การจำกัดเนื้อหาทางอินเทอร์เน็ตในประเทศไทย

อินเทอร์เน็ตเข้ามามีบทบาทในชีวิตทางสังคมและการเมืองของประชาชนไทย โดยช่วยนำเสนอโอกาสใหม่ ๆ ในการสร้างการสื่อสาร อำนวยความสะดวกในการชุมนุม สนับสนุนเสรีภาพในการแสดงออก รวมถึงช่วยในการรณรงค์หรือระดมความคิดในประเด็นทางสังคมการเมืองที่สำคัญ ยกตัวอย่างการสร้างแฮชแท็ก เพื่อสนับสนุนการเคลื่อนไหวในประเด็นต่าง ๆ อาทิ ในช่วงที่มีการเคลื่อนไหวทางการเมืองเมื่อปลายปี 2563 ผู้ใช้ทวิต

---

[135] A/HRC/17/27, 16 May 2011, para 42.

[136] UNESCO (2021), The Training Manual for Judges on International Standards on Freedom of Opinion and Expression, page 108.

[137] A/HRC/17/27, 16 May 2011, para 45, 47, 48, 77. และโปรดดู Global Network Initiative, Principles on Freedom of Expression and Privacy

[138] A/HRC/47/25, 13 April 2021, para 96.

[139] A/HRC/38/35, 6 April 2018, para 52. ; A/HRC/47/25, 13 April 2021, para 90, 100.

[140] A/HRC/38/35, 6 April 2018, para 51.

เตอร์ได้สร้างแฮชแท็กขึ้นมากมาย ซึ่งหลายอันติดเทรนด์ อาทิ #WhatsHappeningInThailand[141] #ถ้าการเมืองดี[142] ซึ่งได้ช่วยกระตุ้นให้เกิดการพูดคุยแลกเปลี่ยนว่าการเมืองที่ดีควรเป็นอย่างไร

ในอีกด้านของพื้นที่ออนไลน์ได้กลายเป็นพื้นที่ในการสื่อสารนานาอคติ รวมถึงการกลั่นแกล้ง (Cyber bullying) การคุกคาม การล่าแม่มด การเผยแพร่วาทกรรมหรือเนื้อหาที่สร้างความเกลียดชัง (Hate speech) ข่าวปลอม (Fake news)[143] โดยเฉพาะในสถานการณ์ที่มีความแตกต่างทางความคิด การใช้วาจาสร้างความเกลียดชังต่อฝ่ายที่มีความเห็นตรงข้ามปรากฏให้เห็นอย่างต่อเนื่อง ซึ่งอาจนำไปสู่การใช้ความรุนแรงต่อกันได้ และอาจลุกลามบานปลายได้[144]

ขณะเดียวกัน รัฐได้พยายามจำกัดเนื้อหาทางออนไลน์ที่ผิดกฎหมายหรือที่เห็นว่าไม่เหมาะสมด้วยวิธีการต่าง ๆ ทั้งทางกฎหมาย ทางเทคนิค และวิธีการอื่น ๆ เช่น ติดตามกดดันให้ลบเนื้อหา[145] เป็นต้น ซึ่งหลายครั้งก่อให้เกิดความกังวลด้านสิทธิมนุษยชน โดยเฉพาะเสรีภาพในการแสดงออกและความเป็นส่วนตัว

Freedom House ซึ่งเป็นองค์กรพัฒนาเอกชนอิสระ ได้รวบรวมข้อมูลและประเมินระดับเสรีภาพทางอินเทอร์เน็ตใน 70 ประเทศทั่วโลก และเผยแพร่ผ่านรายงาน Freedom on the Net ประจำปี โดยการประเมินดังกล่าวพิจารณาจาก 3 ปัจจัยหลัก ได้แก่ อุปสรรคในการเข้าถึง (คะแนนเต็ม 25) การจำกัดเนื้อหา (คะแนนเต็ม 35) และการละเมิดสิทธิของผู้ใช้ (คะแนนเต็ม 40) และนำมาจัดระดับตามคะแนนที่ได้ โดยแบ่งระดับของประเทศเป็นไม่เสรี (Not Free) (0-39 คะแนน) เสรีบางส่วน (Partly Free) (40-69 คะแนน) และเสรี (Free) (70-100 คะแนน) โดยในปี 2564 (2021) ประเทศไทยยังคงถูกจัดอันดับเป็นประเทศไม่เสรี (Not - Free) โดยมีคะแนน 36 คะแนน อยู่ในอันดับที่ 6 ของอาเซียน (จาก 8 ประเทศ) โดยอยู่ในลำดับรองจากฟิลิปปินส์ (65) มาเลเซีย (58) สิงคโปร์ (54) อินโดนีเซีย (48) กัมพูชา (43) ตามลำดับ ซึ่งทั้งหมดเป็นประเทศที่มีเสรีบางส่วน (Partly Free)

---

[141] THE STANDARD. Twitter เผย ‘10 แฮชแท็ก’ ยอดนิยมของไทยช่วงครึ่งปีแรก 2021 มาครบทั้งเรื่องสังคมและวัฒนธรรม เช่น โควิด-19, น้าค่อม, ย้ายประเทศกันเถอะ, อแมนด้า และ แบมแบม เป็นต้น. 23 สิงหาคม 2564. https://thestandard.co/twitter-unveiled-10-thai-famous-hashtags-for-2021/

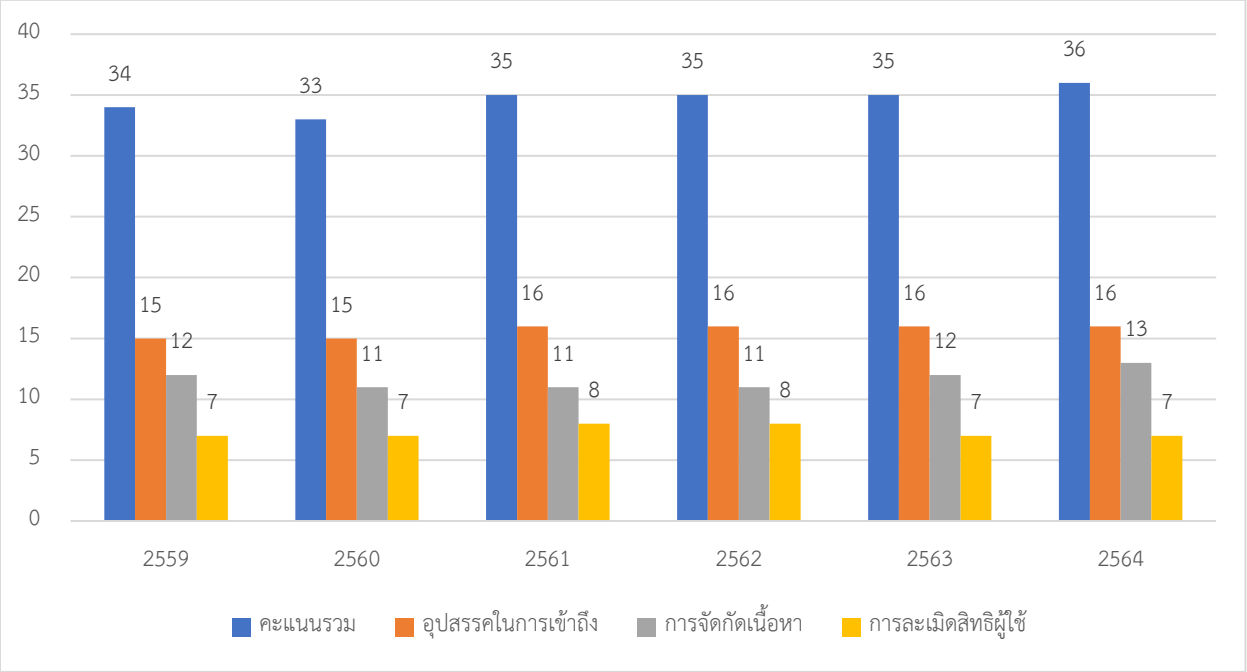
[142] ไทยรัฐออนไลน์. โซเชียลแชร์ความเห็น ติดแฮชแท็ก ถ้าการเมืองดี จะเห็น-ไม่เห็นอะไรในประเทศไทย. 20 กรกฎาคม 2563. https://www.thairath.co.th/news/society/1893643

[143]https://www.the101.world/social-networks-dilemma/?fbclid=IwAR3qQH6DOev95MqRoTimCDCx46JUG4IqmQrr3KOlC0rRHHKTRqeqJ_h4TQQ

[144] คณะกรรมการสิทธิมนุษยชนแห่งชาติ, รายงานผลการประเมินสถานการณ์ด้านสิทธิมนุษยชนของประเทศไทย ประจำปี 2563 หน้า 68

[145] ศูนย์ทนายความเพื่อสิทธิมนุษยชน, สันติบาลไปหา นร.ม.ปลาย ข่มขู่ให้ลบโพสต์เกี่ยวกับสถาบันกษัตริย์ อ้างเจตนาดี, 23 กุมภาพันธ์ 2564, https://tlhr2014.com/archives/26277

แผนภูมิที่ 4.1 อันดับ Freedom on Internet ประเทศไทย ระหว่างปี 2559 - 2564



ที่มา Freedom House[146]

สำหรับประเด็นที่ทำให้ประเทศไทยถูกจัดอันดับไม่เสรีมาตลอดหลายปีนั้น เป็นผลมาจากการจำกัดเนื้อหาบนอินเทอร์เน็ต (Limits on Content) และการละเมิดสิทธิผู้ใช้งานอินเทอร์เน็ต (Violations of User Rights) ซึ่งประเด็นการละเมิดสิทธิผู้ใช้นี้ ในรายงานปี 2563 และล่าสุดปี 2564 ประเทศไทยได้คะแนนเพียง 7 คะแนนจากคะแนนเต็ม 40 โดยรายงานปี 2564 ระบุว่า การได้คะแนนน้อยในประเด็นนี้เป็นผลมาจากการมีกฎหมายที่กำหนดโทษทางอาญาและทางแพ่งสำหรับการกระทำความผิดทางออนไลน์ในอัตราที่สูง มีการดำเนินคดีเพื่อปิดปากนักการเมืองฝ่ายค้าน นักเคลื่อนไหว นักปกป้องสิทธิมนุษยชน และกลุ่มประชาสังคมในช่วงระยะเวลาของการประกาศภาวะฉุกเฉิน รวมถึงการลงโทษในข้อหาหมิ่นประมาทพระมหากษัตริย์ในอัตราโทษที่สูง นอกจากนี้ยังเป็นผลมาจากตรวจสอบโซเชียลมีเดียและการสื่อสารส่วนตัวอย่างแข็งขัน การสอดส่องและละเมิดสิทธิความเป็นส่วนตัวของผู้ใช้ ตลอดจนการข่มขู่และใช้กระบวนการนอกกฎหมายกับนักเคลื่อนไหวเพื่อประชาธิปไตยและบุคคลที่วิพากษ์ที่วิจารณ์สถาบันพระมหากษัตริย์

[146]Freedom House, Freedom on the Net, https://freedomhouse.org/country/thailand/freedom-net/2021

ในส่วนถัดไป จะศึกษารายละเอียดเกี่ยวกับการจำกัดเนื้อหาทางอินเทอร์เน็ตในประเทศไทย โดยใช้กรอบเสรีภาพในการแสดงออกมาเป็นกรอบในการวิเคราะห์หลัก โดยจะศึกษาจากทั้งกรอบกฎหมายภายในประเทศที่เกี่ยวข้อง และข้อเท็จจริงเกี่ยวกับการจำกัดเนื้อหาทางออนไลน์ที่เกิดขึ้น

4.4.1 กรอบการคุ้มครองเสรีภาพในการแสดงออกตามรัฐธรรมนูญ

เสรีภาพในการแสดงความคิดเห็นและการแสดงออกได้รับการคุ้มครองโดยชัดแจ้งตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

มาตรา 34 บุคคลย่อมมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น การจำกัดเสรีภาพดังกล่าวจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเฉพาะเพื่อรักษาความมั่นคงของรัฐ เพื่อคุ้มครองสิทธิหรือเสรีภาพของบุคคลอื่น เพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเพื่อป้องกันสุขภาพของประชาชน

เสรีภาพทางวิชาการย่อมได้รับความคุ้มครอง แต่การใช้เสรีภาพนั้นต้องไม่ขัดต่อหน้าที่ของปวงชนชาวไทยหรือศีลธรรมอันดีของประชาชน และต้องเคารพและไม่ปิดกั้นความเห็นต่างของบุคคลอื่นมาตรา 35 บุคคลซึ่งประกอบวิชาชีพสื่อมวลชนย่อมมีเสรีภาพในการเสนอข่าวสารหรือการแสดงความคิดเห็นตามจริยธรรมแห่งวิชาชีพ

การสั่งปิดกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่นเพื่อลิดรอนเสรีภาพตามวรรคหนึ่ง จะกระทำมิได้

การให้นำข่าวสารหรือข้อความใด ๆ ที่ผู้ประกอบวิชาชีพสื่อมวลชนจัดทำขึ้นไปให้เจ้าหน้าที่ตรวจก่อนนำไปโฆษณาในหนังสือพิมพ์หรือสื่อใด ๆ จะกระทำมิได้ เว้นแต่จะกระทำในระหว่างเวลาที่ประเทศอยู่ในภาวะสงคราม

เจ้าของกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่นต้องเป็นบุคคลสัญชาติไทย

การให้เงินหรือทรัพย์สินอื่นเพื่ออุดหนุนกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่นของเอกชน รัฐจะกระทำมิได้ หน่วยงานของรัฐที่ใช้จ่ายเงินหรือทรัพย์สินให้สื่อมวลชนไม่ว่าเพื่อประโยชน์ในการโฆษณาหรือประชาสัมพันธ์ หรือเพื่อการอื่นใดในทำนองเดียวกันต้องเปิดเผยรายละเอียดให้

คณะกรรมการตรวจเงินแผ่นดินทราบตามระยะเวลาที่กำหนดและประกาศให้ประชาชนทราบด้วย

เจ้าหน้าที่ของรัฐซึ่งปฏิบัติหน้าที่สื่อมวลชนย่อมมีเสรีภาพตามวรรคหนึ่ง แต่ให้คำนึงถึงวัตถุประสงค์และภารกิจของหน่วยงานที่ตนสังกัดอยู่ด้วย

มาตรา 41 บุคคลและชุมชนย่อมมีสิทธิ

(1) ได้รับทราบและเข้าถึงข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐตามที่กฎหมายบัญญัติ

มาตรา 59 รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก (อยู่ในหมวดหน้าที่ของรัฐ)

จะเห็นได้ว่าบทบัญญัติของรัฐธรรมนูญเกี่ยวกับเสรีภาพในการแสดงออกนั้น มีการกำหนดครอบคลุมเสรีภาพในการแสดงความคิดเห็น เสรีภาพในการแสดงออก เสรีภาพในทางวิชาการ (มาตรา 34) เสรีภาพสื่อมวลชน (มาตรา 35) และสิทธิในการเข้าข้อมูลข่าวสาร (มาตรา 41) ทั้งนี้ มีการกำหนดข้อจำกัดสิทธิแต่ละประเภทไว้แตกต่างกัน

ในส่วนของเสรีภาพในการแสดงความคิดเห็นและการแสดงออกนั้น หากเทียบกับกรอบหลักการข้อ 19 ของ ICCPR แล้ว ผู้วิจัยมีความเห็นดังนี้

- ข้อ 19 ของ ICCPR รับรองสิทธิที่จะมีความคิดเห็นโดยปราศจากการแทรกแซง กล่าวอีกแง่หนึ่งคือ เป็นสิทธิที่ไม่อาจถูกจำกัดได้ แต่ในรัฐธรรมนูญของไทยใช้คำ “เสรีภาพในการแสดงความคิดเห็น” และเขียนรวมไว้ในส่วนของเสรีภาพในการแสดงออก (การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น) ซึ่งรัฐธรรมนูญของไทยกำหนดให้มีข้อจำกัดได้ ดังนั้น การรับรองเสรีภาพในการแสดงความคิดเห็นในรัฐธรรมนูญของไทย จึงไม่น่าจะสอดคล้องกับข้อ 19 ของ ICCPR อย่างไรก็ดี มีข้อสังเกตว่า การใช้ถ้อยคำในส่วนที่เกี่ยวข้องกับการเสรีภาพในการแสดงความคิดเห็นนี้ รัฐธรรมนูญไทยและ ICCPR ไม่ได้ใช้ถ้อยคำที่เหมือนกัน จึงเป็นไปได้ว่ารัฐธรรมนูญไทยอาจมุ่งหมายให้เสรีภาพในการแสดงความคิดเห็นนี้ เป็นส่วนหนึ่งของเสรีภาพในการแสดงออกก็เป็นได้

- ในส่วนของเสรีภาพในการแสดงออกนั้น เมื่อพิจารณาเทียบกับข้อจำกัดข้อ 19 (3) ของ ICCPR แล้ว พบว่า มีความสอดคล้องในเรื่องเกณฑ์ของการกำหนดโดยกฎหมาย และวัตถุประสงค์ที่ชอบธรรม กล่าวคือ ความมั่นคงของรัฐ การคุ้มครองสิทธิหรือเสรีภาพของบุคคลอื่น การรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือด้านสุขภาพของประชาชน อย่างไรก็ดี มีข้อสังเกตว่าเกณฑ์ความจำเป็นและได้สัดส่วนนั้น รัฐธรรมนูญของไทยไม่ได้ใช้ถ้อยคำว่า “จำเป็นต่อ..” เช่นเดียวกับที่ปรากฏในข้อ 19 (3) ของ ICCPR ซึ่งสิ่งนี้อาจมีผลต่อการสร้างกรอบคิดในการตีความ “หลักความจำเป็นและได้สัดส่วน” ตามมา

ในส่วนของเสรีภาพทางวิชาการ และเสรีภาพสื่อมวลชนนั้น ใน ICCPR ไม่ได้รับรองเสรีภาพดังกล่าวไว้อย่างชัดเจน แต่มีการตีความว่าเสรีภาพดังกล่าวเป็นส่วนหนึ่งของเสรีภาพในการแสดงออก[147] เมื่อกลับมาพิจารณาข้อจำกัดเสรีภาพดังกล่าวตามรัฐธรรมนูญไทย พบว่า หลักเกณฑ์การจำกัดสิทธิยังคงมีความคลุมเครือ กล่าวคือ การจำกัดเสรีภาพทั้งสองประการ ไม่ได้ถูกกำหนดอย่างชัดเจนว่าต้องจำกัดด้วยกฎหมาย ส่วนวัตถุประสงค์ที่เสรีภาพดังกล่าวอาจถูกจำกัดได้นั้น ก็กำหนดไว้ค่อนข้างกว้าง กล่าวคือ ในส่วนของเสรีภาพในทางวิชาการ รัฐธรรมนูญกำหนดวัตถุประสงค์ในการจำกัดไว้ในเรื่อง “หน้าที่ของปวงชนชาวไทยหรือศีลธรรมอันดีของประชาชน และต้องเคารพและไม่ปิดกั้นความเห็นต่างของบุคคลอื่น” ซึ่งวัตถุประสงค์บางประการ โดยเฉพาะหน้าที่ของปวงชนชาวไทยนั้น ไม่ใช่วัตถุประสงค์ที่ถือว่าชอบธรรมสำหรับการจำกัดเสรีภาพในการแสดงออกที่ปรากฏในข้อ 19 (3) ของ ICCPR

สำหรับสิทธิในการเข้าถึงข้อมูลข่าวสาร ในฐานะมิติหนึ่งของเสรีภาพในการแสดงออกนั้น มีการกำหนดไว้ในสองส่วนคือ ในมาตรา 41 ซึ่งอยู่ในหมวดสิทธิและเสรีภาพของปวงชนชาวไทย และมาตรา 59 ในหมวดหน้าที่ของรัฐ ซึ่งโดยกรอบของข้อ 19 (3) ของ ICCPR นั้น สิทธิในการเข้าถึงข้อมูลข่าวสารสามารถถูกจำกัดได้ภายใต้เงื่อนไขเดียวกับการจำกัดเสรีภาพในการแสดงออก ซึ่งมาตรา 41 ของรัฐธรรมนูญไม่ได้กำหนดวัตถุประสงค์ที่ชอบธรรมในการจำกัดไว้ อย่างไรก็ดี ดูเหมือนว่าวัตถุประสงค์ในการจำกัดจะถูกกำหนดในมาตรา 59 ซึ่งเป็นเรื่องความมั่นคงของรัฐหรือเป็นความลับของทางราชการ

กล่าวโดยสรุป การเขียนข้อจำกัดสิทธิในการมีความคิดเห็นและสิทธิในเสรีภาพแห่งการแสดงออกตามรัฐธรรมนูญของไทย ยังค่อนข้างคลุมเครือ ซึ่งอาจเปิดช่องให้มีการออกกฎหมายลำดับรองที่กำหนดข้อจำกัดกว้างขวางและคลุมเครือตามมาด้วย

[147] โปรดดู CCPR General Comment No. 34

4.4.2 การจำกัดเสรีภาพในการแสดงออกและควบคุมเนื้อหาออนไลน์

ประเทศไทยมีการจำกัดเนื้อหาทางออนไลน์โดยใช้ทั้งวิธีการทางกฎหมาย ทางเทคนิค รวมถึงวิธีการนอกกฎหมาย ซึ่งจะนำเสนอตามวิธีการใช้อำนาจ ดังนี้

4.4.2.1 การปิดกั้นและการกรองเนื้อหา

<u>ขอบเขตของกฎหมายสำหรับการปิดกั้นหรือกรองเนื้อหาทางคอมพิวเตอร์</u>

พ.ร.บ. คอมพิวเตอร์ฯ มาตรา 20 ที่แก้ไขในปี 2560 กำหนดให้พนักงานเจ้าหน้าที่ได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่ง “ระงับการทำให้แพร่หลาย” หรือ “ลบ” ข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้ สำหรับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ดังต่อไปนี้

(1) ข้อมูลที่เป็นความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ (มาตรา 14, 16)

(2) ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาค 2 ลักษณะ 1 (ความผิดต่อองค์พระมหากษัตริย์ พระราชินี รัชทายาท และผู้สำเร็จราชการแทนพระองค์ ความผิดต่อความมั่นคงของรัฐภายในราชอาณาจักร ความผิดต่อความมั่นคงของรัฐภายนอกราชอาณาจักร ความผิดต่อสัมพันธไมตรีกับต่างประเทศ) หรือลักษณะ 1/1 (ความผิดเกี่ยวกับการก่อการร้าย) แห่งประมวลกฎหมายอาญา

(3) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา (กฎหมายลิขสิทธิ์ สิทธิบัตร หรือเครื่องหมายการค้า) หรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนและเจ้าหน้าที่ตามกฎหมายนั้นหรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาได้ร้องขอ

ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์จะมอบหมายให้พนักงานเจ้าหน้าที่ยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบซึ่งข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้

พ.ร.บ.คอมพิวเตอร์ฯ กำหนดให้ข้อมูลที่ "มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน" จะต้องดำเนินการพิจารณากลั่นกรองโดยคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ ซึ่งมีปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธาน และมีกรรมการอีก 7 คน มาจากผู้ทรงคุณวุฒิด้านต่าง ๆ

อาทิ ด้านสิทธิมนุษยชน ด้านสื่อสารมวลชน ด้านเทคโนโลยีสารสนเทศ หรือด้านอื่นที่เกี่ยวข้อง โดยคณะกรรมการมีอำนาจในการกำหนดแนวทางและลักษณะข้อมูลคอมพิวเตอร์ที่อาจมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และพิจารณาและตรวจสอบข้อมูลคอมพิวเตอร์ตามแนวทางดังกล่าว โดยให้ยึดถือตามแนวคำพิพากษาของศาลฎีกาประกอบบริบทของสังคมไทยเป็นสำคัญ[148] หากคณะกรรมการเห็นว่า เป็นข้อมูลที่ควรถูกระงับการเผยแพร่ก็ส่งเรื่องต่อไปให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบต่อไป

สำหรับการพิจารณาของศาล พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 20 วรรคสี่ กำหนดให้นำประมวลกฎหมายวิธีพิจารณาความอาญามาใช้บังคับโดยอนุโลม ซึ่งในทางปฏิบัติแต่เดิม ศาลจะพิจารณาและออกคำสั่งไปฝ่ายเดียว ซึ่งไม่ปรากฏชัดเจนว่า ศาลได้ไต่สวนพยานผู้เกี่ยวข้องอย่างไรก่อนออกคำสั่ง อย่างไรก็ดี นับตั้งแต่ปลายปี 2563 เป็นต้นมา เริ่มปรากฏว่าศาลให้มีการไต่สวนก่อนออกคำสั่ง

ในกรณีการขอให้ระงับการเข้าถึงคลิปยูทูปเรื่อง "วัคซีนพระราชทาน ใครได้ใครเสีย?" ของคณะก้าวหน้า ในช่วงต้นปี 2564 ซึ่งนายธนาธร ประธานคณะก้าวหน้า ได้ยื่นคำร้องคัดค้าน พร้อมกับขอให้ศาลไต่สวนก่อนออกคำสั่ง ซึ่งศาลตอบสนองคำขอโดยกำหนดให้มีการไต่สวนและต่อมามีคำสั่งสั่งเพิกถอนคำสั่งเดิมที่ให้ระงับการเผยแพร่ โดยเหตุผลส่วนหนึ่งของศาลระบุว่า

> *“การออกคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์อันมีลักษณะเป็นการจำกัดสิทธิเสรีภาพของบุคคลโดยชัดแจ้งและถาวร การอนุโลมใช้กฎหมายวิธีพิจารณาความอาญาที่ถูกต้องแก่คำร้องเช่นนี้ สมควรที่จะรับพิจารณาเสมือนเป็นคดีอาญาคดีหนึ่ง ซึ่งต้องให้โอกาสคู่ความทุกฝ่ายได้ต่อสู้คดีเท่าที่จะเป็นไปได้”*

ในปัจจุบันก่อนมีคำสั่งสั่งระงับการเผยแพร่หรือลบข้อมูลคอมพิวเตอร์ ศาลจะเปิดโอกาสให้เจ้าของข้อมูลมีสิทธิคัดค้านหรือเข้ามาไต่สวนก่อนออกคำสั่ง โดยจะออกหมายนัดไต่สวนคำร้องส่งไปยังผู้ที่น่าจะเป็นเจ้าของข้อมูลคอมพิวเตอร์ที่ถูกขอให้ระงับหรือลบ ซึ่งหลายกรณีที่ไม่ทราบตัวเจ้าของบัญชีที่จะขอให้ระงับหรือลบ จะมีการใช้วิธีการส่งหมายนัดไปทางช่องแชทของแพลตฟอร์มที่จะขอระงับหรือลบข้อมูล ทั้งนี้ หากเจ้าของ

---

[148] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง แต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พ.ศ. 2560

ข้อมูลไม่ไปคัดค้าน ศาลจะดำเนินการไต่สวนผู้ร้องไปฝ่ายเดียว ถ้าศาลเห็นว่าเนื้อหาเข้าข่ายตามมาตรา 20 ศาลก็จะสั่งให้ระงับเนื้อหา ซึ่งหากไม่มีผู้คัดค้านและผู้ยื่นคำร้องมีเหตุผลตามสมควรก็มีโอกาสสูงที่ศาลจะสั่งเช่นนั้น[149]

อย่างไรก็ดี การไปแสดงตัวต่อศาลและยื่นคำร้องคัดค้านก็เป็นการเปิดเผยตัว ซึ่งอาจมีความเสี่ยงที่จะถูกดำเนินคดีตามมาในภายหลัง

> *"...กรณีของน้องที่เขาแชร์รูป Crop Top แล้วก็ข้อความวิพากษ์วิจารณ์การแต่งตัว กระทรวง DE ก็ไปร้องศาลให้ไปลบ แล้วเจ้าตัวก็ยอมเสี่ยงที่จะไปไต่สวนเพื่อคัดค้าน ยอมเปิดตัวตน อันนี้ก็มีความกังวลว่าถ้าเขาไปปรากฏตัวแบบนั้นแล้วในอนาคตมันจะนำไปสู่การดำเนินคดี 112 รึเปล่า"*[150]

อย่างไรก็ดี คำชี้แจงจากสำนักงานศาลยุติธรรมออกเอกสารแจกให้สื่อมวลชน เมื่อ 26 กรกฎาคม 2564 ระบุว่า

> *"เมื่อไต่สวนแล้ว แม้ว่าศาลจะมีคำสั่งปิดหรือไม่ปิดเว็บไซต์ หรือลบข้อความบนเว็บไซต์ก็ไม่ได้แปลว่าผู้รับผิดชอบเว็บไซต์หรือเจ้าของข้อมูลนั้นจะต้องผิดหรือไม่ผิดกฎหมายอาญาหรือแพ่ง หรือรับโทษใดในทันที"*[151]

นอกจากนี้ คำชี้แจงของศาลระบุด้วยว่า ได้มีการออก"คำแนะนำอธิบดีผู้พิพากษาศาลอาญาว่าด้วยแนวทางการพิจารณาคำร้องขอให้ระงับการเผยแพร่ข้อมูลคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 20" เพื่อให้ผู้พิพากษาศาลอาญามีแนวทางในการปฏิบัติและพิจารณาคำร้องอย่างมีประสิทธิภาพและชัดเจน คำแนะนำดังกล่าวกำหนดแนวทางการดำเนินการ อาทิ ผู้ร้องต้องแยกคำร้องเป็นรายข้อกล่าวหา แต่ละคำร้องควรมีฐานความผิดเดียว โดยแต่ละคำร้องอาจขอให้ปิดข้อมูลคอมพิวเตอร์หลายชุด (URL) ก็ได้ ให้มีการไต่สวนโดยการส่งสำเนาให้ผู้ดูแลเว็บไซต์ที่ถูกกล่าวหาเพื่อให้โอกาสที่จะคัดค้าน หากไม่มีคำคัดค้านก็ให้ไต่สวนฝ่ายเดียว โดยพิจารณาจากเอกสารของผู้ร้องเป็นหลัก คือภาระการพิสูจน์จะอยู่ที่ฝ่ายผู้ร้องจะต้องนำหลักฐานมายืนยันให้ศาลเห็น[152]

---

[149] iLaw. ขั้นตอน วิธีการสั่ง "บล็อคเว็บ" ตามพ.ร.บ.คอมพิวเตอร์ฯ และช่องทางการคัดค้าน. 4 มิถุนายน 2565. https://freedom.ilaw.or.th/blog/BlockProcess

[150] สัมภาษณ์ผู้แทนจาก iLaw, วันที่ 21 กรกฎาคม 2565, ผ่านระบบอิเล็กทรอนิกส์ (ZOOM)

[151] เพจเฟ็ซบุ๊ค "สื่อศาล". เผยแพร่ 26 กรกฎาคม 2564. https://www.facebook.com/121882511847085/posts/832187710816558/?d=n

[152] สำนักงานศาลยุติธรรม. ศาลอาญา วางแนวปฏิบัติพิจารณาคำร้องปิดเว็บ เน้นไต่สวน 2 ฝ่ายให้โอกาสคัดค้านควบคู่ทำเร็วแจ้งไต่สวนไม่เกิน 7 วัน มองความมั่นคงมิติตุลาการสร้างกระบวนพิจารณาเป็นธรรม สังคมศรัทธาเชื่อใจ ไม่มุ่งแค่ปราบปราม. https://iprd.coj.go.th/th/content/category/detail/id/10/cid/10241/iid/255030

"ในมุมมองขององค์กรศาล เราเชื่อว่าถ้าประชาชนทุกฝ่ายรู้ว่ามีกระบวนการที่เป็นธรรมต่อเขา ประชาชนจะเชื่อฟังและศรัทธาในกระบวนการทำงานในกระบวนการของรัฐ และสิ่งนี้ในที่สุดแล้วจะสร้างความมั่นคงของรัฐในระยะยาว ยิ่งกว่าการปราบปราม ไม่ใช่เราไม่แคร์ความมั่นคง เราแคร์ความมั่นคง แต่เรามีมุมมองเกี่ยวกับความมั่นคงในอีกมุมหนึ่งด้วยในฐานะที่เป็นองค์กรตุลาการ คือมิติเรื่องความเป็นธรรม ถ้ามีความเป็นธรรมประเทศก็จะมั่นคง ซึ่งก็เป็นภาพที่องค์กรตุลาการทั่วโลกจะมองแบบที่เรามอง คำวินิจฉัยของศาลที่ออกไปในช่วงหลังที่แสดงว่าศาลให้ความสำคัญกับสิทธิและเสรีภาพในการแสดงความคิดเห็น ไม่ใช่เพราะว่าศาลหยิบยกคุณค่าขึ้นมาตามอำเภอใจ แต่เป็นเพราะรัฐธรรมนูญกำหนดรับรองสิทธินี้ไว้ชัดเจนและกำหนดว่าการที่รัฐจะใช้เหตุผลอื่น ๆ รวมทั้งเรื่องความมั่นคงในการจำกัดสิทธินั้นเป็นข้อยกเว้น ดังนั้นศาลจึงตีความกฎหมายและคุ้มครองสิทธิเสรีภาพสอดคล้องกับรัฐธรรมนูญ"[153]

ท่าทีของฝ่ายตุลาการข้างต้น เป็นสิ่งที่น่าชื่นชมในแง่ของความพยายามในการสร้างหลักประกันการคุ้มครองเสรีภาพในการแสดงออกกับการลบหรือปิดกั้นเนื้อหา โดยเฉพาะการเปิดโอกาสให้ผู้เจ้าของเนื้อหาที่ถูกร้องให้ลบหรือปิดกั้นได้เข้าคัดค้านในชั้นการไต่สวนก่อนออกคำสั่ง นอกจากนี้ คำชี้แจงของศาลบางส่วนยังได้อธิบายถึงความพยายามในการสร้างหลักประกันความจำเป็นและได้สัดส่วนของการลบหรือปิดกั้นเนื้อหาด้วย

“สำหรับเว็บไซต์ให้ข้อมูลข่าวสาร ศาลจะไม่ปิดช่องทางการสื่อสารของสื่อหรือบุคคล การสั่งลบหรือห้ามเผยแพร่จะทำได้เฉพาะข้อความที่ศาลเห็นว่าขัดต่อกฎหมายเป็นรายข้อความ และไม่ปิดกั้นการสื่อสารในอนาคตเนื่องจากเนื้อหารัฐธรรมนูญ มาตรา 35 วรรคสอง คุ้มครองสิทธิของสื่อมวลชนในการเสนอข่าวสาร และมาตรา 36 คุ้มครองสิทธิในการสื่อสาร”[154]

กล่าวโดยสรุป จะเห็นว่า พ.ร.บ. คอมพิวเตอร์ฯ กำหนดหลักประกันเชิงกระบวนการสำหรับการลบหรือปิดกั้นเนื้อหาทางคอมพิวเตอ์ไว้ในระดับหนึ่ง โดยเฉพาะการกำหนดให้การลบหรือปิดกั้นเนื้อหาต้องทำโดยคำสั่งของฝ่ายตุลาการ ประกอบกับปัจจุบันฝ่ายตุลาการแสดงให้เห็นมุมมองและการดำเนินการต่อการลบหรือปิดกั้นเนื้อหาในทิศทางที่เป็นบวกต่อสิทธิมนุษยชนมากขึ้น

อย่างไรก็ดี หากพิจารณาในแง่ของเนื้อหาของกฎหมายที่กำหนดประเภทเนื้อหาที่อาจนำไปสู่การของให้ลบหรือปิดกั้นได้นั้น ขอบเขตบทบัญญัติของกฎหมายในหลายเรื่องมีลักษณะที่คลุมเครือและเปิดช่องให้มีการนำไปใช้หรือตีความได้อย่างกว้างขวาง เช่น “ข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอม” หรือ “ข้อมูลคอมพิวเตอร์

[153] เพจเฟ็ซบุ๊ค “สื่อศาล”. เผยแพร่ 26 กรกฎาคม 2564. อ้างแล้ว

[154] เพจเฟ็ซบุ๊ค “สื่อศาล”. เผยแพร่ 26 กรกฎาคม 2564. อ้างแล้ว

อันเป็นเท็จ”หรือ “ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก” รวมถึง “ความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน” ซึ่งไม่ได้มีการกำหนดคำนิยามไว้ในกฎหมาย ทำให้ไม่รู้ว่าขอบเขตของถ้อยคำเหล่านี้กินความกว้างแค่ไหนเพียงใด ทำให้เปิดช่องให้เกิดการกำหนดขอบเขตในกฎหมายลำดับรองที่กว้างขวางและมีการตีความเพื่อบังคับใช้อย่างกว้างขวาง และเสี่ยงต่อการนำมาใช้ละเมิดเสรีภาพในการแสดงออก

สถานการณ์การกรองและการปิดกั้นเนื้อหา

การกรองทางอินเทอร์เน็ตถูกนำมาใช้ครั้งแรกในปี 2545 โดยหน่วยงานของกระทรวงเทคโนโลยีสารเทศและการสื่อสารในขณะนั้น ตั้งแต่ยังไม่ได้มีกฎหมายจนกระทั่งมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (พ.ร.บ. คอมพิวเตอร์ฯ) โดยนับตั้งแต่มี พ.ร.บ. คอมพิวเตอร์ฯ จึงถึงปี 2556 รายงานสถิติการระงับการเผยแพร่เนื้อหา หรือการปิดเว็บไซต์ผ่านคำสั่งศาลจำนวน 380 ฉบับ จำนวนทั้งสิ้น 107,830 ยูอาร์แอล ทั้งนี้ เนื้อหาที่ถูกปิดกั้นเป็นอันดับหนึ่ง คือ เนื้อหาและภาพดูหมิ่น หมิ่นประมาท พระมหากษัตริย์ พระราชินี และรัชทายาท ซึ่งมีคำสั่งศาล จำนวน 267 ฉบับให้ระงับการเข้าถึง 82,418 ยูอาร์แอล หรือคิดเป็นร้อยละ 76.4 ของจำนวนยูอาร์แอลที่ถูกปิดกั้นทั้งหมด อันดับสอง คือ เนื้อหาและภาพลามกอนาจาร มีคำสั่งศาล 84 ฉบับ ให้ระงับการเข้าถึง 24,139 ยูอาร์แอล หรือคิดเป็นร้อยละ 22.38 ของจำนวนยูอาร์แอลที่ถูกปิดกั้นทั้งหมด[155] โดยเฉพาะในปี 2553 ซึ่งเป็นปีที่มีความขัดแย้งทางการเมืองสูง มีจำนวนเว็บไซต์ที่ถูกปิดกั้นในปีดังกล่าวสูงถึง 45,357 URLs

และสถิติการระงับการเผยแพร่เนื้อหาและการสั่งปิดเว็บไซต์ ในช่วงเดือนมกราคม 2556 จนถึงเดือนธันวาคม 2557 ศาลอาญามีคำสั่งระงับการเผยแพร่เนื้อหาทั้งสิ้น 123 ฉบับ รวมจำนวน 9,328 URL โดยเนื้อหาที่ถูกปิดกั้นการเข้าถึงเป็นอันดับหนึ่งคือ เนื้อหาและภาพซึ่งมีลักษณะดูหมิ่น หมิ่นประมาท พระมหากษัตริย์ ราชินี และรัชทายาท จำนวน 92 ฉบับ รวม 7,726 ยูอาร์แอล (URL) คิดเป็นร้อยละ 82.83 ของจำนวนยูอาร์แอลทั้งหมด อันดับที่สองคือ เนื้อหาและภาพซึ่งมีลักษณะลามกอนาจาร จำนวน 18 ฉบับ รวม 1,547 ยูอาร์แอล คิดเป็นร้อยละ 16.58 ของจำนวนยูอาร์แอลทั้งหมด และอับดับที่สามคือ เนื้อหาและภาพที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน จำนวน 6 ฉบับ รวม 30 ยูอาร์แอล คิดเป็นร้อยละ 0.32 ของจำนวนยูอาร์แอลทั้งหมด[156]

---

[155] iLaw. สถิติการปิดกั้นเว็บไซต์ในประเทศไทย นับตั้งแต่ปี 2550-2556. 21 เมษายน 2556. https://freedom.ilaw.or.th/en/node/97

[156] iLaw. สถิติการปิดกั้นเว็บไซต์ในประเทศไทย นับตั้งแต่ปี 2556-2557. 2 กุมภาพันธ์ 2557. https://freedom.ilaw.or.th/blog/webblockstat20132014

ภายหลังจากการยึดอำนาจโดยคณะรักษาความสงบแห่งชาต (คสช.) เมื่อเดือนพฤษภาคม 2557 คสช. ได้ออกประกาศ คสช. ฉบับที่ 17/2014 เรื่อง การเผยแพร่ข้อมูลข่าวสารผ่านช่องทางอินเทอร์เน็ต ซึ่งประกาศ ณ วันที่ 22 พฤษภาคม 2557 โดยสั่งให้ผู้ให้บริการอินเทอร์เน็ตทุกรายดำเนินการติดตาม ตรวจสอบและระงับยับยั้งการเผยแพร่ข้อมูลข่าวสารใด ๆ ที่มีการบิดเบือน ยุยง ปลุกปั่น อันจะก่อให้เกิดความไม่สงบเรียบร้อยภายในราชอาณาจักร หรือมีผลกระทบต่อความมั่นคงของรัฐหรือศีลธรรมอันดีของประชาชน และให้มารายงานตัว ณ สำนักงาน กสทช. ด้วย

คำสั่งดังกล่าวให้อำนาจผู้ให้บริการอินเทอร์เน็ตปิดกั้นเนื้อหาทางอินเทอร์เน็ตโดยตรงภายใต้วิจารณญาณของตนเอง เป็นผลให้ไม่มีสถิติการเซ็นเซอร์อย่างเป็นทางการ อย่างไรก็ดี Citizen Lab ได้ดำเนินการวัดเครือข่ายของการเข้าถึงเว็บไซต์ในประเทศไทย ตั้งแต่วันที่ 22 พฤษภาคม ถึง 26 มิถุนายน 2557 โดยทดสอบตัวอย่าง 433 URL บนเครือข่ายผู้ให้บริการอินเทอร์เน็ต (ISP) ได้แก่ 3BB, INET และ ServeNet และทดสอบตัวอย่าง URL 4 รายการที่มีขนาดเล็กกว่าบนเครือข่ายของ CAT และ TOT ผลลัพธ์ระบุว่า URL ทั้งหมด 56 รายการถูกบล็อกในประเทศ เนื้อหาที่ถูกบล็อกรวมถึงเนื้อหาทางการเมือง เช่น สำนักข่าวอิสระในประเทศและการรายงานข่าวของสื่อต่างประเทศที่วิพากษ์วิจารณ์รัฐประหาร บัญชีโซเชียลมีเดียที่แชร์สื่อต่อต้านการรัฐประหาร เว็บไซต์การพนัน และภาพลามกอนาจาร[157]

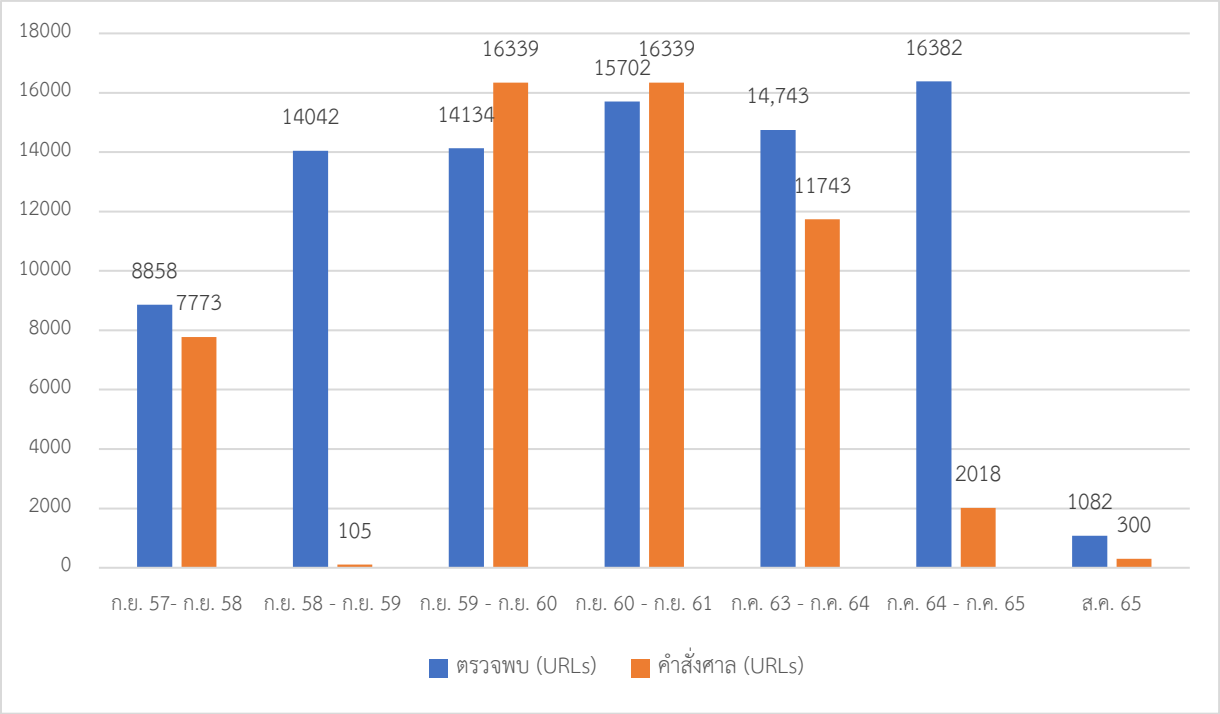
รายงาน The State of Internet Censorship in Thailand ที่เผยแพร่โดย Open Observatory of Network Interference (OONI) ซึ่งทดสอบการเข้าถึงไซต์ 1,525 แห่ง ระหว่าง 6 พฤศจิกายน 2559 - 27 กุมภาพันธ์ 2560 ผลการวิจัยพบว่า ผู้ให้บริการอินเทอร์เน็ตในประเทศไทยใช้การเซ็นเซอร์เป็นหลักผ่านการจี้ DNS (DNS hijacking) และผ่าน middle boxes (HTTP transparent proxies) โดยการทดสอบ HTTP invalid request line เผยให้เห็นว่ามี middle boxes ในหลายเครือข่าย ซึ่งสกัดกั้นคำขอ HTTP ที่ส่งไปยัง echo servers ส่วนการทดสอบการเชื่อมต่อเว็บ พบว่ามี 13 เว็บไซต์ถูกบล็อกจากผู้ให้บริการอินเทอร์เน็ต 6 ราย (DTAC, Realmove Company Limited, TOT 3BB, Triple-T Internet Co., Ltd, True Internet Co., Ltd, JasTel Network International) เว็บไซต์เหล่านี้รวมถึงเว็บข่าว (nypost.com และ dailymail.co.uk), wikileaks.org, ไซต์เครื่องมือหลบเลี่ยง (เช่น hotspotshield.com) และภาพอนาจาร อย่างไรก็ดี เว็บไซต์เหล่านี้ไม่ได้ถูกบล็อกในทุกเครือข่าย ทำให้ในรายงานเชื่อว่าผู้ให้บริการในไทยอาจกรองเนื้อหาตามคำสั่งของรัฐบาลให้ปิดกั้นเนื้อหาที่ถือว่า

[157] Citizen Lab. Information Controls during Thailand's 2014 Coup. July 9, 2014. https://citizenlab.ca/2014/07/information-controls-thailand-2014-coup/

ละเมิดกฎหมายหมิ่นพระบรมเดชานุภาพ และรายงานตั้งข้อสังเกตว่า ผู้ให้บริการในไทยอาจอยู่ในฐานะที่จะกรองเนื้อหาออนไลน์ตามดุลยพินิจของตนเองได้[158]

ปัจจุบัน กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ดำเนินโครงการเฝ้าระวังเว็บไซต์ผิดกฎหมายเพื่อแก้ปัญหาการมีข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายเกี่ยวกับความมั่นคง (สถาบันพระมหากษัตริย์) และอาชญากรรมอื่น ๆ ที่แพร่หลายในโลกโซเชียล โดยได้จัดให้มีเจ้าหน้าที่เฝ้าระวัง รับแจ้ง และจัดเก็บข้อมูล ที่เผยแพร่บนโลกโซเชียลทุกวันตลอด 24 ชั่วโมง และเปิดเพจอาสาจับตาออนไลน์ เพื่อให้ประชาชนแจ้งเบาะแสเว็บไซต์ที่ผิดกฎหมาย โดยมีการรายงานผลการดำเนินการปิดกั้นเว็บไซต์ที่เข้าข่ายความผิดกฎหมายตามแผนภูมิที่ 4.2

แผนภูมิที่ 4.2 การแจ้งเว็บไซต์และคำสั่งศาลในการปิดกั้น



ที่มา สำนักเลขาธิการคณะรัฐมนตรี[159] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม[160]

หมายเหตุ ข้อมูลคำสั่งศาล ก.ย. 58 – ก.ย. 59 อาจจะเป็นไปได้ที่จะนับตามจำนวนคำสั่ง ไม่ใช่นับจาก URLs

[158] OONI. The State of Internet Censorship in Thailand. https://ooni.org/post/thailand-internet-censorship/

[159] สำนักเลขาธิการคณะรัฐมนตรี, รายงานผลการดำเนินงานของรัฐบาล พลเอกประยุทธ จันทร์โอชา, https://www.soc.go.th/?page_id=10338

[160]กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, รายงานผลการดำเนินงานตามนโยบายรัฐบาลประจำปี, https://bit.ly/3CailNq

นับตั้งแต่เดือนเมษายน 2564 เป็นต้น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รายงานว่า เนื่องจากวิธีการพิจารณาของศาลได้เปลี่ยนไปจากเดิมโดยเพิ่มเติมขั้นตอนการแจ้งคู่กรณีและการไต่สวน ทำให้คดีอยู่ในระหว่างการพิจารณามากขึ้นและทำให้คดีเสร็จช้าลง ซึ่งก็สอดคล้องกับแนวโน้มสถิติตามแผนภูมิข้างต้น โดยเว็บไซตที่ไม่เหมาะสมส่วนใหญ่คือ เว็บไซต์เกี่ยวกับสถาบันพระมหากษัตริย์[161]

นอกจากนี้ จากข้อมูลรายงานความโปร่งใสของบริษัทแพลตฟอร์มขนาดใหญ่ แสดงให้เห็นว่าจำนวนคำขอจากรัฐบาลเพิ่มขึ้นอย่างต่อเนื่อง

รายงานของ Facebook แสดงให้เห็นการจำกัดเนื้อหาเพิ่มขึ้นต่อเนื่องนับตั้งแต่ปี 2560 โดยในรายงานล่าสุดระหว่างเดือนกรกฎาคม – ธันวาคม 2564 มีรายงานการจำกัดการเข้าถึงในประเทศไทยเพื่อตอบสนองต่อรายงานนโยบายผู้บริโภคที่ร้องขอโดยสำนักงานคณะกรรมการอาหารและยา จำนวน 1,754 รายการ และเพื่อตอบสนองต่อรายงานจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมในข้อหาละเมิดกฎหมายหมิ่นพระบรมเดชานุภาพจำนวน 77 รายการ และหากดูข้อมูลภาพรวมตั้งแต่ปี 2557 – 2564 การจำกัดเนื้อหาส่วนใหญ่เป็นไปเพื่อตอบสนองต่อข้อหาละเมิดกฎหมายหมิ่นประมาทพระมหากษัตริย์[162]

ส่วน Google รายงานว่านับตั้งแต่เดือนมกราคม 2554 – ธันวาคม 2564 ได้รับคำขอของรัฐบาลให้ลบเนื้อหา 1,382 คำขอ รวม 31,269 รายการ เหตุผลของคำขอส่วนใหญ่กว่าร้อยละ 90 คือการวิพากษ์วิจารณ์รัฐบาล และผลิตภัณฑ์ที่ถูกขอส่วนใหญ่คือ YouTube นอกจากนี้ บริษัทมีอัตราการนำเนื้อหาออกมากกว่าร้อยละ 70 แทบทุกปี โดยรายงานล่าสุดระหว่างเดือนกรกฎาคม - ธันวาคม 2564 มีการนำเนื้อหาออกร้อยละ 70.6[163]

รายงานความโปร่งใสของ Twitter ซึ่งเป็นรายงานที่ปรากฏล่าสุดระหว่างเดือนกรกฎาคม-ธันวาคม 2564 ระบุว่ามีจำนวนข้อเรียกร้องทางกฎหมายของรัฐบาลไทยอยู่ 50 คำขอ โดยเป็นคำสั่งศาล 3 คำขอ และคำขอทางกฎหมายอื่นอีก 47 คำขอ โดย Twitter มีอัตราการปฏิบัติตามอยู่ที่ร้อยละ 12 โดยส่วนใหญ่ร้อยละ 33 เป็นการตอบสนองต่อคำสั่งศาล[164]

ในปี 2563 พร้อม ๆ กับการระบาดของไวรัสโคโรนา 2019 กลุ่มประชาชนที่นำโดยเยาวชนได้เคลื่อนไหวทั้งในโลกออฟไลน์และออนไลน์เพื่อเรียกร้องให้นายกรัฐมนตรีลาออก ให้แก้ไขรัฐธรรม รวมถึงการปฏิรูป

---

[161] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, อ้างแล้ว

[162]Meta Transparency Cente, https://transparency.fb.com/data/content-restrictions/country/TH/

[163] Google Transparency Report, Government Requests to Remove Content, “Requests: Thailand,” https://transparencyreport.google.com/government-removals/government-requests/TH

[164] Twitter Transparency, https://transparency.twitter.com/en/reports/countries/th.html

สถาบันพระมหากษัตริย์ ปรากฏการใช้แฮชแท็กอย่างแพร่หลายบนทวิตเตอร์ เพื่อตั้งคำถามต่อรัฐบาลและสถาบันพระมหากษัตริย์

ก่อนการนัดชุมนุมของกลุ่มราษฎรที่จะจัดขึ้นวันที่ 8 พฤศจิกายน 2563 เพื่อเดินขบวนไปสำนักพระราชวัง บริเวณวัดพระศรีรัตนศาสดารา ปรากฏว่าก่อนหน้าการชุมนุม 2 วัน คือ วันที่ 6 พฤศจิกายน 2563 มีรายงานว่า บัญชีผู้ใช้งานทวิตเตอร์ของกลุ่มเยาวชนปลดแอก (@FreeYOUTHth) และแกนนำเยาวชน 2 ราย[165] ได้ถูกระงับการใช้งานชั่วคราว ก่อนจะกลับมาใช้ได้ตามปกติ โดย Twitter ประเทศไทย ชี้แจงว่า เป็นเพราะการละเมิดกฎเกี่ยวกับการควบคุมการบิดเบือนระบบและสแปม (Platform Manipulation and Spam Policy)[166]

นอกจากนี้ รัฐยังได้มีความพยายามในการปิดกั้นเนื้อหาบนแพลตฟอร์มออนไลน์ที่เกี่ยวข้องวิพากษ์วิจารณ์สถาบันพระมหากษัตริย์อีกหลายกรณี เช่น ความพยายามในการปิดเพจเฟซบุ๊ค Royalist Market Place (ตลาดหลวง) เมื่อเดือนสิงหาคม 2563 การปิดกั้นวิดีโอบน YouTube ของอานนท์ นำภา แกนนำที่เรียกร้องให้มีการปฏิรูปสถาบันกษัตริย์ เมื่อเดือนตุลาคม 2563[167] นอกจากจากนี้ เมื่อวันที่ 16 ตุลาคม 2563 พบว่ามีการปิดกั้นการเข้าถึงเว็บไซต์ Change.org หลังจากมีแคมเปญเรียกร้องให้รัฐบาลเยอรมันเพิกถอนความคุ้มกันทางการทูตของพระมหากษัตริย์[168] และวันที่ 4 มกราคม 2564 มีรายงานว่า YouTube ได้ปิดกั้นการเข้าถึงมิวสิกวิดีโอเพลง “ปฏิรูป” ของกลุ่มแร็ปเปอร์ Rap Against Dictatorship ซึ่งเป็นที่มีเนื้อหาวิพากษ์การบริหารของรัฐบาล ความเหลื่อมล้ำเชิงอำนาจและต้องการการปฏิรูปเพื่อสร้างความเป็นธรรม รวมถึงสนับสนุนการเรียกร้องทางการเมืองของคณะราษฎร[169]

จากตัวอย่างที่ยกมาข้างต้น จะเห็นได้ว่าการปิดกั้นเนื้อหาทางออนไลน์จำนวนมากได้ถูกนำมาใช้เพื่อห้ามการเผยแพร่ข้อมูลที่วิพากษ์วิจารณ์รัฐบาล รวมถึงสถาบันทางการเมือง ซึ่งถือเป็นวัตถุประสงค์ที่ไม่ชอบธรรมตามข้อ 19 (3) ของ ICCPR[170]

---

[165] Spring News, ทวิตเตอร์ "เยาวชนปลดแอก-ฟอร์ด-เจมส์" กลับมาใช้งานได้ตามปกติแล้ว, 6 พฤศจิกายน 2563, https://www.springnews.co.th/news/802001

[166] THE STANDARD, Twitter ประเทศไทยแจงกรณีแอ็กเคานต์ เยาวชนปลดแอก และฟอร์ด ทัตเทพ ถูกระงับ เหตุละเมิดกฎการบิดเบือนระบบ สแปม , 6 พฤศจิกายน 2563, https://thestandard.co/twitter-thailand-discusses-account-suspension-cases/

[167] Prachatai, “YouTube locally blocks speech about monarchy reform at Thai government’s request”, 9 October 2020, https://prachatai.com/english/node/8833

[168] BBC, “Thailand blocks Change.org as petition against king gains traction”, 16 October 2020, available at: https://www.bbc.com/news/world-asia-54566767.

[169]Voice online, เพลง 'ปฏิรูป' กลุ่ม R.A.D. ถูกปิดกั้นการเข้าถึงใน YOUTUBE, 4 มกราคม 2564, https://www.voicetv.co.th/read/u84RrAnG6

[170] CCPR General Comment No. 34, paras. 42 – 43.

<u>กรณีศึกษาตัวอย่างที่ดีของการตรวจสอบการปิดกั้นเนื้อหาของฝ่ายตุลาการ</u>

กรณีแรก การขอปิดสื่อออนไลน์

ในช่วงเดือนตุลาคม 2563 ท่ามกลางการชุมชุมของประชาชนฝ่ายต่อต้านรัฐบาลเกิดขึ้นอย่างกว้างขวางนั้น รัฐพยายามที่จะใช้กฎหมายเพื่อปิดแพลตฟอร์มสื่อออนไลน์ โดยมีรายงานว่าเมื่อวันที่ 20 ตุลาคม 2563 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ยื่นคำร้องขอให้ศาลอาญาสั่งปิดแพลตฟอร์มออนไลน์ของวอยซ์ทีวี ประชาไท เดอะรีพอร์ตเตอร์ และเยาวชนปลดแอก ฐานเผยแพร่ “ข้อมูลเท็จ” เกี่ยวกับการประท้วง อันเป็นการฝ่าฝืน พ.ร.บ. คอมพิวเตอร์ฯ และ พ.ร.ก.ฉุกเฉินฯ อย่างไรก็ดี เมื่อวันที่ 21 ตุลาคม 2563 ศาลอาญาได้เปิดการไต่สวนอีกครั้งและมีคำสั่งให้ยกเลิกคำสั่งศาลที่ให้ระงับการแพร่หลายซึ่งข้อมูลคอมพิวเตอร์ โดยศาลระบุว่า รัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 35 วรรคสอง บัญญัติห้ามรัฐปิดสื่อมวลชนเพื่อลิดรอนเสรีภาพในการเสนอข่าวสาร มาตรา 36 วรรคหนึ่งบัญญัติรับรองเสรีภาพของบุคคลในการสื่อสารถึงกัน การตีความ พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 20 ก็ดี พ.ร.ก.ฉุกเฉินฯ มาตรา 9 (3) ก็ดี จะต้องเป็นไปโดยสอดคล้องกับบทบัญญัติของรัฐธรรมนูญ โดยศาลเห็นว่าเจตนารมณ์ของกฎหมายมุ่งหมายที่จะให้สั่งห้ามโดยเฉพาะเจาะจงซึ่งข้อมูลที่เป็นความผิด หาได้มีเจตนารมณ์ที่จะให้ศาลมีคำสั่งปิดช่องทางการสื่อสารของบุคคลหรือสื่อสารมวลชนทั้งช่องทางซึ่งมีผลการนำเสนอข้อความในอนาคตที่ยังไม่มีการพิสูจน์ความผิดด้วย[171]

กรณีที่สอง ออกข้อกำหนดตามพ.ร.ก. ฉุกเฉินฯ เพื่อคุมสื่อ

รัฐได้เพิ่มระดับการปราบปรามการแสดงออกที่ไม่พึงปรารถนาบนพื้นที่ออนไลน์ โดยอาศัย พ.ร.ก. ฉุกเฉินฯ ที่ถูกนำมาใช้เมื่อเดือนมีนาคม 2563 เพื่อควบคุมการแพร่ระบาดของไวรัสโคโรนา 2019 เป็นเครื่องมือในการปิดกั้นเนื้อหาออนไลน์ด้วย โดยเมื่อวันที่ 29 กรกฎาคม 2564 ได้มีการประกาศใช้ข้อกำหนดที่ออกตามความในมาตรา 9 แห่ง พ.ร.ก.ฉุกเฉินฯ (ฉบับที่ 29) ซึ่งมีเนื้อหาในการห้ามการนำเสนอข่าว จำหน่าย หรือทำให้แพร่หลายซึ่งหนังสือ สิ่งพิมพ์ หรือสื่ออื่นใด ที่มีข้อความอันอาจทำให้ประชาชนเกิดความหวาดกลัว หรือเจตนาบิดเบือนข้อมูลข่าวสาร ทำให้เกิดความเข้าใจผิดในสถานการณ์ฉุกเฉินจนกระทบต่อความมั่นคงของรัฐ หรือความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน และหากเป็นการแพร่ผ่านอินเทอร์เน็ต ให้สำนักงาน กสทช. แจ้งให้ผู้บริการทราบ และผู้ให้บริการมีหน้าที่ตรวจสอบข้อความ และให้แจ้ง กสทช. ระงับการให้บริการอินเทอร์เน็ตแก่เลขที่อยู่ไอพี (IP address) ที่เป็นปัญหานั้นทันที หากผู้ให้บริการไม่ดำเนินการ จะต้องถูกดำเนินการตามกฎหมายต่อไป

[171] ประชาไทย, ด่วน! ศาลอาญายกเลิกคำร้องปิดวอยซ์ทีวี รวมทั้ง 'เยาวชนปลดแอก' ด้วย, 21 ตุลาคม 2563, https://prachatai.com/journal/2020/10/90074

หลังจากมีการออกข้อกำหนดดังกล่าว องค์กรสื่อออนไลน์และภาคประชาสังคม12 องค์กร นำโดย The Reporters, Voice TV, The Standard ฯลฯ ได้ยื่นฟ้องต่อศาลแพ่ง ขอให้ศาลมีคำพิพากษาเพิกถอนข้อกำหนดดังกล่าว พร้อมทั้งขอให้คุ้มครองชั่วคราวในกรณีฉุกเฉินโดยขอให้ศาลมีคำสั่งระงับการบังคับใช้ข้อกำหนดดังกล่าว ไปจนกว่าศาลจะมีคำพิพากษาถึงที่สุด

โดยศาลแพ่งได้ไต่สวนและมีคำสั่งคุ้มครองชั่วคราว เนื้อหาของคำสั่งศาลแพ่ง ระบุว่า ข้อกำหนดที่ห้ามเผยแพร่ข้อความอันอาจทำให้ประชาชนเกิดความหวาดกลัว ไม่ได้จำกัดเฉพาะข้อความอันเป็นเท็จ ดังเหตุผลและความจำเป็นตามที่ระบุไว้ในการออกข้อกำหนดดังกล่าว ข้อกำหนดนี้ ย่อมเป็นการลิดรอนสิทธิเสรีภาพของโจทก์ทั้ง 12 ซึ่งเป็นสื่อมวลชน รวมทั้งประชาชน ตามที่รัฐธรรมนูญ 2560 คุ้มครองไว้ ส่วนข้อกำหนดที่ให้อำนาจ กสทช. ระงับการให้บริการอินเทอร์เน็ต ศาลระบุว่า ไม่ปรากฏว่าในมาตรา 9 ของ พ.ร.ก.ฉุกเฉินฯ ให้อำนาจนายกรัฐมนตรีในการออกข้อกำหนดเช่นนี้ ดังนั้น ข้อกำหนดให้ดำเนินการระงับการให้บริการอินเทอร์เน็ตจึงเป็น "ข้อกำหนดที่ไม่ชอบด้วยกฎหมาย" ทั้งนี้ หลังจากศาลแพ่งมีคำสั่ง รัฐบาลก็ได้ประกาศยกเลิกข้อกำหนดดังกล่าว

กรณีที่สาม การปิดกั้นเว็บรณรงค์ Change.org

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ขอปิดเว็บรณรงค์ Change.org ซึ่งเป็นแพลตฟอร์มออนไลน์สำหรับการลงชื่อเพื่อเข้าร่วมแคมเปญรณรงค์หรือสนับสนุนประเด็นต่างๆ โดยในปี 2564 มีแคมเปญชวนคนมาลงชื่อที่เป็นเรื่องร้อนแรงหลายเรื่อง เช่น เรียกร้องให้รัฐมนตรีว่าการกระทรวงสาธารณสุข อนุทิน ชาญวีรกูล ลาออก[172] หรือเรียกร้องให้ลดงบประมาณกระทรวงกลาโหม เปลี่ยนอาวุธสงคราม เป็นอาวุธป้องกันเชื้อโรค[173]

โดยเหตุผลในการขอปิดกั้นนั้น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอ้างว่าเว็บไซต์ Change.org มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ที่มีเนื้อหาไม่เหมาะสม มีการนำเข้าข้อมูลคอมพิวเตอร์ที่มีเนื้อหาอันเข้าข่ายความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร

กรณีนี้ เดิมทีศาลได้ทำการไต่สวนฝ่ายเดียวไปเมื่อวันที่ 15 ตุลาคม 2563 และมีคำสั่งให้ระงับการเผยแพร่ข้อมูลของเว็บไซต์ กระทรวงฯ จึงได้อาศัยอำนาจตามคำสั่งศาลดังกล่าวปิดเว็บไซต์ Change.org ทำให้ไม่สามารถเข้าถึงได้ทั้งเว็บตั้งแต่ 15 ตุลาคม 2563 แต่ภายหลังทาง change.org ยื่นคำร้องคัดค้านและขอให้ศาลไต่สวนเพื่อเพิกถอนคำสั่งปิดกั้นเว็บไซต์ดังกล่าว

---

[172] http://chng.it/rdck5RkFVd

[173] http://chng.it/wQhbg6KWNm

ศาลได้คำสั่งยกเลิกการระงับการปิดกั้นดังกล่าวตั้งแต่วันที่ 3 มีนาคม 2564 ทำให้เว็บไซต์กลับมาใช้งานได้ตามปกติในวันที่ 22 เมษายน 2564 โดยตอนหนึ่งของคำสั่งศาลระบุว่า

> *"...ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2560 มาตรา 36 วรรคหนึ่ง บัญญัติรับรองเสรีภาพของบุคคลในการสื่อสารถึงกัน การตีความตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 20 จึงต้องเป็นไปโดยสอดคล้องกับบทบัญญัติของรัฐธรรมนูญดังกล่าว ทั้งนี้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 20 ให้อำนาจศาลระงับการทำให้เผยแพร่หรือลบข้อมูลออกจากระบบคอมพิวเตอร์และมาตรา 3 ของพระราชบัญญัติระบุว่า "ข้อมูลคอมพิวเตอร์" หมายถึง ข้อมูล ข้อความ...ในระบบคอมพิวเตอร์ ดังนั้นเจตนารมณ์ของกฎหมายย่อมมุ่งหมายที่จะให้ศาลห้ามโดยเฉพาะเจาะจงซึ่งข้อมูลที่เป็นความผิด ตามมาตรา 20 (1) - (3) โดยเฉพาะเจาะจงเป็นรายข้อความ ดังนั้นการที่ศาลมีคำสั่งระงับการแพร่หลายซึ่งข้อมูลคอมพิวเตอร์ของ URL ที่ 2. www.Change.org ซึ่งเป็นการปิดกั้นการเข้าถึงเว็บไซต์ www.Change.org ทั้งเว็บไซต์ โดยที่ผู้ร้องไม่ได้แสดงให้ชัดเจนในชั้นไต่สวนว่าเป็นการขอปิดเว็บไซต์ทั้งเว็บไซต์ ทำให้ศาลมิได้รู้ข้อเท็จจริงอันถูกต้องเข้าใจว่าเป็นการปิดกั้นเฉพาะเนื้อหาบางส่วนที่ละเมิดต่อกฎหมาย คำสั่งศาลดังกล่าวจึงไม่ถูกต้อง"*[174]

กรณีที่สี่ คลิปวัคซีนพระราชทาน : ใครได้ ใครเสีย?

วันที่ 29 มกราคม 2564 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ยื่นคำขอให้ศาลระงับการเผยแพร่เว็บไซต์ข้อความภาพและคลิปวีดีโอการไลฟ์สดหัวข้อ "วัคซีนพระราชทาน : ใครได้ ใครเสีย? ของนายธนาธร จึงรุ่งเรียงกิจ ประธานคณะก้าวหน้า ที่จัดขึ้นเมื่อวันที่ 18 มกราคม 2564 ซึ่งคลิปดังกล่าวมีเนื้อหาเกี่ยวกับการวิจารณ์แผนการทำงานของรัฐบาลที่ไม่มีประสิทธิภาพในการจัดหาและบริหารวัคซีนโควิดที่ช้าและน้อยเกินไป โดยกระทรวงดิจิทัลฯ ขอให้ศาลสั่งระงับการเผยแพร่ 3 URLs (รายการ) ซึ่งมีทั้งเว็บไซต์ ยูทูป และเฟซบุ๊ค

โดยเหตุผลในการของปิดกั้นนั้น กระทรวงฯ อ้างว่ามีข้อความ ภาพ และคลิปวิดีโอ ที่มีเนื้อหาอันเข้าข่ายเป็นความผิดเกี่ยวกับความมั่นคงในราชอาณาจักร อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรตามประมวลกฎหมายอาญา มาตรา 112 ซึ่งเป็นความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มาตรา 14 (3) จึงขอให้ศาลสั่งระงับการเผยแพร่ตามมาตรา 20 สั่งระงับการทำให้แพร่หลาย 3 URLs ดังกล่าว

---

[174] iLaw. เปิดคำสั่งศาล ให้เว็บ Change.org "ฆ่าไม่ตาย" กลับมาใช้งานได้. 3 มิถุนายน 2563. https://freedom.ilaw.or.th/node/917

ศาลอาญาไต่สวนและมีคำสั่งให้ปิดกั้นการเข้าถึงทั้ง 3 URLs ในวันเดียวกันนั้น ต่อมานายธนาธรยื่นคำร้องคัดค้านคำสั่ง ศาลอาญาได้ไต่สวนเมื่อวันที่ 8 กุมภาพันธ์ 2564 โดยมีเจ้าหน้าที่กระทรวงดิจิทัลฯ และนายธนาธรร่วมเบิกความ และศาลได้มีคำสั่งให้เพิกถอนคำสั่งที่ให้ปิดกั้นก่อนหน้านี้ โดยศาลมองว่าเนื้อหาของคลิปวีดิโอไม่ได้ต้องห้ามตามกฎหมาย เป็นเพียงการวิพากษ์วิจารณ์กระบวนการจัดการผลิตและสนับสนุนการผลิตวัคซีนโควิดของรัฐบาล อันเป็นการวิพากษ์วิจารณ์การทำงานของรัฐบาลโดยทั่วไป เป็นการใช้สิทธิเสรีภาพในการแสดงความคิดเห็นตามรัฐธรรมนูญ

กรณีนี้ศาลอาญาวางบรรทัดฐานไว้ด้วยว่า การพิจารณาเรื่องการปิดกั้นเว็บไซต์ ตามมาตรา 20 ของ พ.ร.บ.คอมพิวเตอร์ฯ ต้องให้โอกาสเจ้าของเว็บไซต์โต้แย้งแสดงพยานหลักฐานอย่างเต็มที่ เสมือนการพิจารณาคดีอาญาคดีหนึ่ง และยังระบุเหตุผลว่า การตีความคำว่า “อาจกระทบต่อความมั่นคง” ต้องตีความอย่างเคร่งครัดและเป็นภาวะวิสัย ซึ่งต้องแปลความโดยพิจารณากรอบของรัฐธรรมนูญด้วย โดยศาลได้หยิบยกรัฐธรรมนูญมาตรา 34 เกี่ยวกับเสรีภาพในการแสดงความคิดเห็นและการแสดงออกมาวินิจฉัย

> *“...การที่รัฐธรรมนูญรับรองสิทธิเสรีภาพในการแสดงความคิดเห็นเช่นนี้ หมายความว่าการห้ามหรือระงับการแพร่หลายซึ่งข้อมูลเป็นข้อยกเว้นในขณะที่การเผยแพร่ข้อมูลโดยเสรีเป็นหลัก ในการนี้ควรพิจารณาว่าสิทธิเสรีภาพในการแสดงความคิดเห็นเป็นสาระสำคัญในการปกครองระบอบประชาธิปไตยซึ่งเป็นระบอบการปกครองที่ยอมรับความหลากหลายและอดทนอดกลั้นต่อความเห็นต่าง สิทธิเสรีภาพในการแสดงความคิดเห็นนี้จึงถือเป็นสิทธิเสรีภาพขั้นพื้นฐานที่ต้องได้รับความคุ้มครองโดยเคร่งครัด ทั้งนี้ตามหลักสากลของการปกครองในระบบประชาธิปไตยที่มีนิติรัฐและมีพันธกรณีในการปกป้องสิทธิมนุษยชนตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชนแห่งสหประชาชาติและกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองซึ่งประเทศไทยรับรองและเป็นภาคี ดังนั้น การจำกัดสิทธิเสรีภาพในการแสดงความคิดเห็นจะทำได้เมื่อมีความจำเป็นอย่างยิ่งยวดและเร่งด่วนเพื่อคุ้มครองประโยชน์อันชอบธรรมของรัฐและต้องได้สัดส่วนกับความจำเป็นโดยต้องใช้มาตรการที่เป็นภาระน้อยที่สุดเท่าที่จะเป็นไปได้ การตีความคำว่า “อาจกระทบต่อความมั่นคง” ตามมาตรา 20 (2) จึงต้องตีความอย่างเคร่งครัดและเป็นภาวะวิสัย”*[175]

[175] iLaw. ศาลอาญากลับคำสั่ง ไม่ให้บล็อค คลิป "วัคซีนพระราชทาน" ของคณะก้าวหน้า. 9 กุมภาพันธ์ 2564. https://freedom.ilaw.or.th/blog/reversebolckorder

จากกรณีศึกษาที่ยกว่า ได้เห็นความก้าวหน้าของศาลในระดับหนึ่งในการวางบรรทัดฐานเกี่ยวกับการพิจารณาคำร้องปิดกั้นเนื้อหาทางออนไลน์ โดยเฉพาะการวางแนวทางของการพิจารณาคำขอที่ศาลต้องให้เจ้าของเนื้อหาที่ถูกยื่นคำขอให้ปิดกั้นได้มีโอกาสมาคัดค้านเสียก่อนที่จะมีการออกคำสั่ง และการพิจารณาจะต้องให้ความสำคัญกับความจำเป็นและได้สัดส่วน

4.4.2.2 การดำเนินคดีกับเนื้อหาออนไลน์

กฎหมายหลายฉบับได้ถูกนำมาใช้จำกัดเนื้อหาทางออนไลน์ ผ่านการดำเนินคดีกับผู้ที่แสดงออกในพื้นที่ออนไลน์ ทั้งการโพส การแชร์ หรือการแสดงความเห็นในโพสต่าง ๆ ซึ่งนอกจาก พ.ร.บ. คอมพิวเตอร์ฯ แล้ว กฎหมายอีกหลายฉบับที่บังคับใช้ในพื้นที่ออฟไลน์ยังถูกนำมาใช้ในทางออนไลน์ด้วย โดยเฉพาะ ข้อหาหมิ่นประมาทพระมหากษัตริย์ (ประมวลกฎหมายอาญา มาตรา 112) ข้อหายุยงปลุกปั่น (ประมวลกฎหมายอาญา มาตรา 116) ข้อหาหมิ่นประมา (ประมวลกฎหมายอาญา มาตรา 326, 328) ซึ่งกฎหมายเหล่านี้ถูกนำมาใช้ทั้งโดยรัฐและภาคธุรกิจเพื่อปิดกั้นการวิพากษ์วิจารณ์ของประชาชนที่เป็นคู่ขัดแย้ง[176]

1) พ.ร.บ. คอมพิวเตอร์ฯ

ความผิดตาม พ.ร.บ. คอมพิวเตอร์ฯ สามารถแบ่งเป็น 2 ประเภทใหญ่ๆ คือ ความผิดที่เป็นการทำต่อตัวระบบหรือข้อมูลคอมพิวเตอร์ เช่น การจารกรรมข้อมูล การแฮ็กระบบ เป็นต้น (ตามมาตรา 5 – 13) และความผิดต่อเนื้อหา ซึ่งเกี่ยวข้องกับการเผยแพร่เนื้อหาทางออนไลน์ (มาตรา 14 – 16) โดยการบังคับใช้ พ.ร.บ. คอมพิวเตอร์ฯ ในยุคแรก (เดือนกรกฎาคม พ.ศ. 2550 ถึงกรกฎาคม พ.ศ. 2553) การดำเนินคดีส่วนใหญ่เป็นเรื่อง "เนื้อหา" โดยเฉพาะที่เกี่ยวกับการหมิ่นประมาท และหมิ่นประมาทพระมหากษัตริย์ ฯลฯ ขณะที่คดีเกี่ยวกับ "ระบบ" เช่น การเข้าสู่ระบบโดยมิชอบ การฉ้อโกงโดยใช้ระบบคอมพิวเตอร์ การเผยแพร่โปรแกรมที่ผิดกฎหมาย มีจำนวนเพียงเล็กน้อยเท่านั้น[177]

ในส่วนนี้จะกล่าวถึงเฉพาะความผิดในส่วนที่เกี่ยวข้องกับเนื้อหา เพราะเป็นการกระทำที่เกี่ยวกับการใช้เสรีภาพในการแสดงออกทางออนไลน์

<u>ความผิดเกี่ยวกับการเผยแพร่เนื้อหาทางออนไลน์</u>

มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

---

[176] สมาคมนักกฎหมายสิทธิมนุษยชน, รายงานข้อเสนอแนะต่อการคุ้มครองผู้ใช้สิทธิและเสรีภาพเพื่อการมีส่วนร่วมในประเด็นสาธารณะจากการถูกฟ้องคดี, https://naksit.net/2019/06/report_slapps-public-participation/ และสถานการณ์การฟ้องคดีปิดปากในประเทศไทย : มีกลไกกลั่นกรองแล้วแต่ทำไมแนวโน้มคดียังสูงขึ้นต่อเนื่อง,https://naksit.net/2021/03/reportslapp/

[177] iLaw. สรุปสถานการณ์การควบคุมและปิดกั้นสื่อออนไลน์ พ.ศ.2550 – 2553. https://ilaw.or.th/node/631

(1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

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

ถ้าการกระทำความผิดตามวรรคหนึ่ง (1) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

เดิมที พ.ร.บ. คอมพิวเตอร์ฯ มาตรา 14 (1) มักถูกนำมาใช้กับการเผยแพร่ข้อมูลและการแสดงออกทางออนไลน์ และที่ผ่านมามักถูกใช้ควบคู่กับข้อหาหมิ่นประมาทด้วยการโฆษณา ตามมาตรา 328 แห่งประมวลกฎหมายอาญา คดีเด่น ๆ ที่เป็นส่วนหนึ่งของการทำให้เกิดการแก้ไข พ.ร.บ. คอมพิวเตอร์ฯ มาตรา 14 (1) เมื่อปี 2560 คือ คดีที่กองทัพเรือดำเนินคดีกับสำนักข่าวภูเก็ตหวาน เมื่อเดือนธันวาคม 2556 จากการเผยแพร่ข่าวเป็นภาษาอังกฤษในเว็บไซต์ของสำนักข่าว ซึ่งอ้างอิงจากรายงานของสำนักข่าวรอยเตอร์ เนื้อหาของข่าวเกี่ยวกับการมีทหารเรือบางนายมีส่วนเกี่ยวข้องและได้รับผลประโยชน์จากขบวนการค้ามนุษย์ชาวโรฮิงญา โดยสำนักข่ายภูเก็ตหวานถูกฟ้องทั้งในความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14 (1) และความผิดฐานหมิ่นประมาทด้วยการโฆษณา ตามประมวลกฎหมายอาญามาตรา 328 คดีนี้ ศาลจังหวัดภูเก็ตมีคำพิพากษายกฟ้อง เพราะเห็นว่า ไม่ปรากฏว่าข้อความตามฟ้องที่จำเลยอ้างมาจากรอยเตอร์สเป็นข้อมูลคอมพิวเตอร์อันเป็นเท็จ หรือเป็นข้อมูลที่อาจก่อให้เกิดความเสียหายต่อความมั่นคงของรัฐ อันจะเป็นความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14 (1) ส่วนความผิดฐานหมิ่นประมาทนั้น ศาลมองว่า ข้อความที่เผยแพร่นำมาจากรายงานของสำนักข่าว Reuters ซึ่งเป็น

สำนักข่าวที่น่าเชื่อถือ เป็นที่ยอมรับทั่วโลกและสามารตรวจสอบได้ ไม่ไม่ใช่ข้อเท็จจริงและความคิดเห็นที่จำเลยเขียนขึ้นเอง ข้อความที่เผยแพร่จึงไม่ได้เป็นความผิดฐานหมิ่นประมาทโดยการโฆษณา นอกจากนี้ ศาลยังได้วินิจฉัยด้วยว่า เจตนารมณ์ของ พ.ร.บ.คอมพิวเตอร์ฯ ไม่ได้มุ่งเอาผิดกับความผิดฐานหมิ่นประมาทด้วยการโฆษณา เพราะมีประมวลกฎหมายอาญามาตรา 328 บัญญัติความผิดฐานนี้ไว้แล้ว[178]

คดีภูเก็ตหวานสะท้อนให้เห็นการใช้ พ.ร.บ.คอมพิวเตอร์ฯ ที่มุ่งหมายปิดกั้นเสรีภาพในการแสดงออกและเสรีภาพสื่อ ซึ่งผิดไปจากเจตนารมณ์ของกฎหมายที่มุ่งปราบปรามอาชญากรรมไซเบอร์ โดยเฉพาะการกระทำต่อระบบ และคดีได้นำไปสู่การแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 โดยการแก้ไขมาตรา 14 (1) ระบุอย่างชัดเจนว่าไม่ใช้มาตราดังกล่าวกับการกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา หลังจากนั้นพบว่า ข้อหาตามมาตรา 14 (1) ที่ถูกใช้ควบคู่กับข้อหาหมิ่นประมาท พนักงานอัยการ หรือศาลแล้วแต่กรณี มักจะยุติคดีในข้อหาดังกล่าวด้วยการสั่งไม่ฟ้อง (กรณีพนักงานอัยการ) หรือมีคำพิพากษายกฟ้อง (กรณีของศาล)

ยังมีอีกหลายคดีที่ พ.ร.บ. คอมพิวเตอร์ฯ มาตรา 14 (1) ถูกนำมาใช่เพื่อปิดปากประชาชน เช่น กรณีนักข่าวพลเมืองชาวลาหู่ ถูกทหารดำเนินคดีเมื่อเดือนมกราคม 2558 ตามมาตรา 14 (1) ของ พ.ร.บ. คอมพิวเตอร์ฯ จากการบันทึกวิดีโอเหตุการณ์ในหมู่บ้าน และแชร์ภาพดังกล่าวบนบัญชีเฟซบุ๊คส่วนตัว โดยใส่ข้อความประกอบคลิปวิดีโอ มีใจความตอนหนึ่งว่า “ทหารตบเด็ก เยาวชนและคนแก่” ทหารอ้างว่าเนื้อหาของคลิปวิดีโอนั้นเป็น “ข้อมูลเท็จ” ที่ทำลายชื่อเสียงของทหาร อย่างไรก็ดี คดีนี้ ศาลจังหวัดเชียงใหม่มีคำพิพากษายกฟ้อง โดยศาลเห็นว่า จำเลยโพสต์คลิปลงในเฟซบุ๊กเพราะเข้าใจว่าเป็นความจริง[179]

นอกจากนี้ บ่อยครั้งที่ พ.ร.บ. คอมพิวเตอร์ฯ มาตรา 14 (1) ถูกนำมาใช้โดยภาคธุรกิจ เพื่อปิดปากนักกิจกรรมหรือชาวบ้านที่แสดงออกทางออนไลน์ในลักษณะคัดค้านหรือตรวจสอบการละเมิดสิทธิของบริษัท อาทิ บริษัทน้ำผลไม้กระป๋องแห่งหนึ่งฟ้องนักวิจัยด้านสิทธิมนุษยชนแรงงานจากการจัดทำและเผยแพร่รายงานเกี่ยวกับการละเมิดสิทธิแรงงานของบริษัทดังกล่าวทางเว็บไซต์ 3 แห่ง[180] และกรณีบริษัทเหมืองแร่ทองคำแห่งหนึ่งดำเนินคดีกับแกนนำชาวบ้านจากการโพสต์หนังสือร้องเรียนที่ชาวบ้านยื่นต่อผู้ว่าราชการจังหวัดลงในเพจเฟซบุ๊ก[181]

ส่วน พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14 (2) มักถูกนำมาใช้ดำเนินคดีกับผู้ที่วิพากษ์วิจารณ์รัฐบาลและหน่วยงานรัฐ โดยเชื่อมโยงกับความผิดอื่น ๆ ที่มีอยู่ตามประมวลกฎหมายอาญา เช่น ความผิดฐานยุยงปลุกปั่น (มาตรา 116) ดูหมิ่นศาลหรือผู้พิพากษา (มาตรา 198) ตัวอย่างการกระทำที่ถูกดำเนินคดี อาทิ การเผยแพร่

---

[178] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, กองทัพเรือ vs สำนักข่าวภูเก็ตหวาน, https://freedom.ilaw.or.th/th/case/554

[179] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, ไมตรี: เผยแพร่คลิปหมิ่นประมาททหาร, https://freedom.ilaw.or.th/th/case/669

[180] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, https://freedom.ilaw.or.th/case/469

[181] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, https://freedom.ilaw.or.th/case/694

ข้อความในเฟซบุ๊กตั้งคำถามถึงความยุติธรรมของคำตัดสินของศาล[182] โพสต์เฟซบุ๊กวิจารณ์ยุทธศาสตร์ชาติ โพสเฟซบุ๊กวิจารณ์คดีจำนำข้าว[183] แชร์เนื้อหาจากเพจโดยอ้างว่าตำรวจเพิกเฉยต่อการถูกกล่าวหาว่าข่มขืนนักท่องเที่ยวชาวอังกฤษบนเกาะเต่า[184] การไลฟ์สดในทางเฟซบุ๊กเพจพาดพิง คสช. ดูด ส.ส.[185] การโพสต์เฟซบุ๊กวิพากษ์วิจารณ์ระบบคัดกรองโควิด-19 ของสนามบินสุวรรณภูมิ[186] เป็นต้น

มีการใช้ พ.ร.บ.คอมพิวเตอร์ฯ กับการแสดงออกทางการเมืองเพิ่มมากขึ้นนับตั้งแต่การชุมนุมทางการเมืองปี 2563 โดยศูนย์ทนายความเพื่อสิทธิมนุษยชน รายงานว่า นับตั้งแต่เริ่มการชุมนุมของ “เยาวชนปลดแอก” เมื่อวันที่ 18 กรกฎาคม 2563 จนถึงวันที่ 30 กันยายน 2565 มีประชาชนที่ถูกดำเนินตาม พ.ร.บ. คอมพิวเตอร์ฯ ไม่น้อยกว่า 151 คดี จำนวน 171 คน[187]

พ.ร.บ.คอมพิวเตอร์ฯ ได้ถูกนำมาใช้กับการวิพากษ์วิจารณ์รัฐบาล และนโยบายสาธารณะต่าง ๆ และผู้ที่ถูกดำเนินคดีจำนวนหนึ่งคือ นักข่าว นักการเมือง นักกิจกรรมทางสังคมและสิ่งแวดล้อม รวมถึงนักปกป้องสิทธิมนุษยชนในระดับชุมชน[188]

นอกจากนี้ พ.ร.บ.คอมพิวเตอร์ฯ ยังมีเนื้อหาสาระบางส่วนทับซ้อนกับความผิดตามที่กำหนดไว้ในประมวลกฎหมายอาญา แต่ พ.ร.บ. คอมพิวเตอร์ฯ มีโทษที่รุนแรงกว่าและส่วนใหญ่เป็นความผิดอาญาแผ่นดิน ไม่อาจยอมความได้ ทำให้เกิดความลักลั่นในการบังคับใช้กฎหมาย ซึ่งที่ผ่านมากรณีที่เห็นได้ชัดคือ ความผิดหมิ่นประมาท อย่างไรก็ดี ปัญหานี้ได้รับการแก้ไขแล้วในปัจจุบัน หลังการแก้ไข พ.ร.บ. คอมพิวเตอร์ฯ 2560 แต่ความผิดฐานอื่นที่ทับซ้อนกัน โดยเฉพาะความผิดเกี่ยวกับความมั่นคงที่ไปซ้อนทับกับประมวลกฎหมายอาญา ก็อาจจะก่อให้เกิดความลักลั่นอยู่เช่นเดิม

---

[182] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, อานนท์: คดีดูหมิ่นศาล จากการโพสต์เฟซบุ๊ก, https://freedom.ilaw.or.th/th/case/814

[183] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, ตารางคดี "ปิดปาก" ประชาชนด้วย พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14(2), https://freedom.ilaw.or.th/blog/ART14-2-CAA-STAT

[184] สำนักข่าวอิศรา, 'ฮิวแมนไรท์' ร้องไทยหยุดดำเนินคดี 12 มือโพสต์ข้อมูลสาวอังกฤษอ้างถูกข่มขืนบนเกาะเต่า, 7 กันยายน 2561, https://www.isranews.org/content-page/item/69280-mgr-69280.html

[185] ไทยรัฐออนไลน์, ธนาธร เข้าให้ข้อมูล ปอท. คดีไลฟ์สด พาดพิง คสช.ดูดอดีต ส.ส., 31 กรกฎาคม 2561, https://www.thairath.co.th/news/local/bangkok/1345135

[186] ศูนย์ทนายความเพื่อสิทธิมนุษยชน, คดีความเปลี่ยนชีวิตของ ‘ดนัย’ ศิลปินกราฟิตี้ ผู้โพสต์ไม่พบ จนท. คัดกรองที่สุวรรณภูมิ, 23 เมษายน 2563, https://tlhr2014.com/archives/17352

[187] ศูนย์ทนายความเพื่อสิทธิมนุษยชน. กันยายน 65: จำนวนผู้ถูกดำเนินคดีทางการเมืองยอดรวมอย่างน้อย 1,860 คน ใน 1,139 คดี. วัทที่ 4 กันยายน 2565. https://tlhr2014.com/archives/49210?fbclid=IwAR3EhGbrpKXUCihBsm1HyJ-D2JstI85_Ssq-z8Y7KHZ6w5x6-kW6XAx8dao

[188] โปรดดูข้อมูลเพิ่มเติมที่ ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, ตารางคดี "ปิดปาก" ประชาชนด้วย พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14(2), https://freedom.ilaw.or.th/blog/ART14-2-CAA-STAT และ แดชบอร์ดคดี SLAPPs โดยภาคธุรกิจ, https://datastudio.google.com/u/1/reporting/9b79cca7-80ab-4f14-bfb1-2c7a29d4204d/page/Su0fC

พ.ร.บ. คอมพิวเตอร์ฯ มาตรา 14 มีการใช้ถ้อยคำบางส่วนที่คลุมเครือ เช่น ข้อมูลคอมพิวเตอร์ที่เป็น "เท็จ" "บิดเบือน" “ปลอม” “ความสงบเรียร้อย” ซึ่งไม่ได้มีนิยามที่ชัดเจนในกฎหมาย ด้วยเหตุนี้ จึงสุ่มเสี่ยงที่จะละเมิดเสรีภาพในการแสดงออก โดยเฉพาะการแสดงออกในประเด็นนโยบายสาธารณะบนอินเทอร์เน็ต ดังที่ยกตัวอย่างไปบ้างแล้วข้างต้น ดังนั้น แทนที่กฎหมายดังกล่าวจะช่วยจัดการกับข้อมูลเท็จ ปลอม หรือบิดเบือน ผลอาจเป็นไปในทางตรงข้ามคือ กลับจะยิ่งเป็นการปิดกั้นการเข้าถึงความจริง เพราะทุกคนจะอยู่ในสภาวะที่เซ็นเซอร์ตัวเอง เพราะไม่มั่นใจว่าสิ่งที่แสดงออกไปจะถูกกล่าวหาว่าเป็นเท็จหรือไม่ ซึ่งในระยะยาวย่อมไม่เป็นผลดีต่อระบอบประชาธิปไตยและระบอบธรรมาภิบาลของรัฐบาล

ปัญหาประการหนึ่งของมาตรา 14 โดยเฉพาะ (2) นั้น คือความไม่ชัดเจนของเส้นแบ่งระหว่างข้อมูลเท็จที่เป็นเจตนาร้าย กับข้อมูลเท็จที่เผยแพร่โดยผิดพลาด แต่ไม่มีเจตนาร้าย ซึ่งประเด็นลักษณะนี้ คณะกรรมการสิทธิมนุษยชนแห่งสหประชาชาติแนะนำให้รัฐหลีกเลี่ยงการลงโทษข้อความที่ไม่เป็นความจริงและที่ผิดกฎหมายซึ่งได้รับการตีพิมพ์โดยผิดพลาด แต่ไม่มีความมุ่งร้าย[189]

<u>ความรับผิดของตัวกลาง</u>

มาตรา 15 ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ

ตามคำนิยามของ พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 3 “ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

พ.ร.บ.คอมพิวเตอร์ฯ กำหนดความรับผิดของผู้ให้บริการในฐานะตัวกลาง (Intermediary) สำหรับเนื้อหาที่ไม่ได้รับอนุญาตบนแพลตฟอร์ม และไม่ปฏิบัติตามคำสั่งให้ลบออก โดยตัวกลางต้องเสี่ยงที่จะถูก

[189] CCPR General Comment No. 34, para. 47, 49.

ลงโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ เฉกเช่นเดียวกับผู้สร้างเนื้อหา โดยกฎหมายที่ได้แก้ไขเพิ่มเติมตาม พ.ร.บ.คอมพิวเตอร์ฯ ปี 2560 นี้ ให้การคุ้มครองบางส่วนแก่ผู้ให้บริการในฐานะตัวกลางผ่านระบบการแจ้งเตือนและนำออก (Notice-and-takedown system)

นอกจากภาระหน้าที่ตามมาตรา 15 แล้ว ตัวกลางยังมีหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 27 ที่ต้องปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา 18 (ให้ความร่วมมือในการสืบสวนและสอบสวนการกระทำความผิด) หรือมาตรา 20 (ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์) หรือตามคำสั่งของศาลตามมาตรา 21 (การจัดการกับชุดคำสั่งไม่พึงประสงค์) หากฝ่าฝืนต้องระวางโทษปรับไม่เกิน 200,000 บาท และปรับเป็นรายวันอีกไม่เกินวันละ 5,000 บาทจนกว่าจะปฏิบัติให้ถูกต้อง

ในแง่ของหน้าที่ของตัวกลางในระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ตามมาตรา 20 นั้น ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือผู้ให้บริการ พ.ศ. 2560 ข้อ 8 กำหนดให้ *“เมื่อผู้ให้บริการได้รับคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์จากพนักงานเจ้าหน้าที่แล้ว ต้องดำเนินการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ตามรายละเอียดที่ปรากฏในคำสั่งของพนักงานเจ้าหน้าที่ในทันทีที่ได้รับคำสั่ง แต่ต้องไม่เกินกว่าระยะเวลาที่ระบุไว้ในคำสั่ง เว้นแต่ในกรณีที่มีเหตุจำเป็นอันสมควรซึ่งพนักงานเจ้าหน้าที่อนุญาตให้ดำเนินการเกินกว่าระยะเวลาที่ระบุไว้ในคำสั่ง แต่ต้องไม่เกิน 15 วัน”*

บางครั้งรัฐบาลกดดันผู้โฮสต์เนื้อหาให้ลบเนื้อหา เช่น ในเดือนกันยายน 2563 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เข้าแจ้งความต่อกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ให้ดำเนินคดีกับผู้ให้บริการสื่อสังคมออนไลน์ รวมทั้งเฟซบุ๊ก ที่ไม่ดำเนินการปิดกั้นการเข้าถึงเนื้อหาภายใน 15 วัน ตามคำสั่งศาล ซึ่งเป็นเนื้อหาเกี่ยวกับการพนัน สื่อลามก ละเมิดลิขสิทธิ์ รวมถึงหมิ่นประมาทพระมหากษัตริย์[190] เฟซบุ๊กออกแถลงการณ์เมื่อเดือนสิงหาคม 2563 ระบุว่ากำลังเตรียมความพร้อมเพื่อโต้แย้งทางกฎหมาย ภายหลังรัฐบาลไทยมีคำขอให้จำกัดการเข้าถึงเนื้อหาบนเฟซบุ๊กที่มีเนื้อหาเกี่ยวข้องกับการพูดคุยเรื่องราชวงศ์และสถาบันกษัตริย์

> *"ข้อเรียกร้องจากรัฐบาลเช่นครั้งนี้ถือเป็นเรื่องที่รุนแรง และขัดต่อหลักสิทธิมนุษยชนสากล และยังส่งผลกระทบต่อเสรีภาพในการแสดงออก การดำเนินงานของเฟซบุ๊กมีจุดมุ่งหมาย*

[190]บีบีซีไทย. เฟซบุ๊ก: กระทรวงดิจิทัลฯ แจ้งความดำเนินคดีเฟซบุ๊ก-ทวิตเตอร์ ไม่ปิดการเข้าถึงเพจผิดกฎหมาย. 24 กันยายน 2563. https://www.bbc.com/thai/thailand-54275519

เพื่อปกป้องและรักษาไว้ซึ่งสิทธิต่าง ๆ ของผู้ใช้งานอินเทอร์เน็ตทุกคน และขณะนี้เรากำลังเตรียมความพร้อมเพื่อโต้แย้งในข้อกฎหมายต่อข้อเรียกร้องครั้งนี้"[191]

2) ประมวลกฎหมายอาญา มาตรา 112 (หมิ่นประมาทพระมหากษัตริย์)

มาตรา 112 แห่งประมวลกฎหมายอาญาหรือความผิดฐานหมิ่นพระบรมเดชานุภาพ (ในงานชิ้นนี้จะใช้คำว่า หมิ่นประมาทพระมหากษัตริย์) อยู่ในลักษณะความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร

"ผู้ใดหมิ่นประมาท ดูหมิ่น หรือแสดงความอาฆาตมาดร้ายพระมหากษัตริย์ พระราชินี รัชทายาท หรือผู้สำเร็จราชการแทนพระองค์ ต้องระวางโทษจำคุกตั้งแต่ 3 ปีถึง 15 ปี"

ท่ามกลางกระแสเรียกร้องให้มีการปฏิรูปสถาบันกษัตริย์อย่างเข้มข้นในปี 2563 เป็นต้นมา ข้อหาหมิ่นประมาทกษัตริย์ถูกนำกลับมาบังคับใช้อีกครั้งหลังจากงดการบังคับใช้มา 2 ปี ศูนย์ทนายความเพื่อสิทธิมนุษยชน รายงานว่า นับตั้งแต่เริ่มการชุมนุมของ "เยาวชนปลดแอก" เมื่อวันที่ 18 กรกฎาคม 2563 จนถึงวันที่ 30 กันยายน 2565 มีประชาชนที่ถูกดำเนินคดีมาตรา 112 ไม่น้อยกว่า 215 คดี รวมจำนวน 234 คน[192] โดยหลายคดีเกิดจากประชาชนฝ่ายที่เห็นต่างไปเป็นผู้กล่าวโทษ และยังพบว่ามีการดำเนินคดีด้วยข้อหานี้อย่างกว้างขวางกับการแสดงออกในหลายรูปแบบ รวมถึงการแสดงออกทางออนไลน์ เช่น การโพสข้อความ #กล้ามาก #เก่งมาก #ขอบใจนะ[193] และในปี 2564 มีการยื่นฟ้องนายธนาธร จึงรุ่งเรืองกิจ จากการไลฟ์สดวิพากษ์วิจารณ์การผูกขาดการผลิตวัคซีนโควิด-19 โดยบริษัท Siam Bioscience ซึ่งเกี่ยวข้องกับสถาบันพระมหากษัตริย์

ยิ่งไปกว่านั้น คดีข้อหาหมิ่นประมาทพระมหากษัตริย์ ถือว่ามีอัตราโทษสูงและไม่ได้สัดส่วนเมื่อเทียบกับลักษณะของการกระทำความผิดที่เป็นเพียงการสดงออก มีคดีที่หญิงรายหนึ่งถูกศาลพิพากษาจำคุกมากถึง 87 ปี ฐานแชร์คลิปบนยูทูปและเฟซบุ๊คที่ถูกพิจารณาว่าเป็นการหมิ่นประมาทพระมหากษัตริย์ ใน 29 กรรม แม้จะได้รับการลดโทษเหลือ 43 ปี 6 เดือน จากการรับสารภาพ แต่อัตราโทษก็ยังคงสูงมาก และเธอไม่อนุญาตให้ปล่อยตัวระหว่างอุทธรณ์คำพิพากษา

เมื่อวันที่ 8 กุมภาพันธ์ 2564 กลุ่มผู้เชี่ยวชาญอิสระที่แต่งตั้งโดยคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติได้แสดงความกังวลต่อการดำเนินคดีดังกล่าว

---

[191] บีบีซีไทย. เฟซบุ๊ก: กระทรวงดิจิทัลฯ แจ้งความดำเนินคดีเฟซบุ๊ก-ทวิตเตอร์ ไม่ปิดการเข้าถึงเพจผิดกฎหมาย. 24 กันยายน 2563. https://www.bbc.com/thai/thailand-54275519

[192] ศูนย์ทนายความเพื่อสิทธิมนุษยชน. วันที่ 4 กันยายน 2565. อ้างแล้ว

[193]ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, https://freedom.ilaw.or.th/node/884

“เราขอเรียกร้องให้ศาลอุทธรณ์พิจารณาคดีของอัญชัน ปรีเลิศ สอดคล้องกับมาตรฐานสิทธิมนุษยชนสากล และละเว้นโทษที่รุนแรง”

นอกจากนี้ ผู้เชี่ยวชาญอิสระยังเน้นย้ำว่า กฎหมายหมิ่นประมาทพระมหากษัตริย์ “ไม่มีที่ในประเทศประชาธิปไตย” และ “เรียกร้องให้เจ้าหน้าที่แก้ไขและยกเลิกกฎหมายหมิ่นประมาทพระมหากษัตริย์ ยกฟ้องทุกคนที่กำลังถูกดำเนินคดีอาญา”[194]

เช่นเดียวกับคณะกรรมการสิทธิมนุษยชนแห่งสหประชาชาติ ในการบทสรุปเชิงสังเกตเกี่ยวกับการทบทวนรายงาน ICCPR ของประเทศไทยครั้งที่สอง เมื่อปี2560 คณะกรรมการได้แนะนำให้รัฐไทยควรทบทวนมาตรา 112 แห่งประมวลกฎหมายอาญา ให้สอดคล้องกับมาตรา 19 แห่ง ICCPR ตามความเห็นทั่วไปฉบับที่ 34 คณะกรรมการย้ำว่าการจำคุกบุคคลเพื่อใช้เสรีภาพในการแสดงออกเป็นการละเมิดมาตรา 19[195]

ในความเห็นทั่วไปฉบับที่ 34 ระบุว่าบุคคลสาธารณะทั้งหมด “อยู่ภายใต้การวิพากษ์วิจารณ์และคัดค้านทางการเมืองโดยชอบธรรม” และ “กฎหมายไม่ควรให้มีบทลงโทษที่รุนแรงกว่านี้เพียงบนพื้นฐานของอัตลักษณ์ของบุคคลที่อาจถูกกล่าวหา"[196]

ในรอบ UPR ที่ 3 (ปี 2564) ประเทศต่าง ๆ โดยเฉพาะประเทศในยุโรปเสนอแนะให้ประเทศไทยพิจารณาทบทวนแก้ไขประมวลกฎหมายอาญามาตรา 112 ให้สอดคล้องกับ ICCPR อาทิ ลักเซมเบิร์ก ฝรั่งเศส สวิตเซอร์แลนด์ เบลเยียม แคนาดา เดนมาร์ก และบางส่วนเสนอให้ยกเลิกการกำหนดอัตราโทษขั้นต่ำในฐานความผิดนั้น (สวีเดน) อย่างไรก็ดี ข้อเสนอเหล่านั้นดังกล่าวไม่ได้รับการตอบรับจากรัฐบาลไทย[197]

3) ประมวลกฎหมายอาญา มาตรา 116 (ยุยงปลุกปั่น)

“มาตรา 116 ผู้ใดกระทำให้ปรากฏแก่ประชาชนด้วยวาจา หนังสือหรือวิธีอื่นใดอันมิใช่เป็นการกระทำภายในความมุ่งหมายแห่งรัฐธรรมนูญ หรือมิใช่เพื่อแสดงความคิดเห็นหรือติชมโดยสุจริต

(1) เพื่อให้เกิดการเปลี่ยนแปลงในกฎหมายแผ่นดินหรือรัฐบาล โดยใช้กำลังข่มขืนใจหรือใช้กำลังประทุษร้าย

---

[194] OHCHR, “Thailand: UN experts alarmed by rise in use of lèse-majesté laws”, 8 February 2021, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26727&LangID=E.

[195] UN Human Rights Committee, CCPR/C/THA/CO/2 (‘Concluding observations on Thailand’), 25 April 2017, paras. 37 – 38.

[196] CCPR General Comment No. 34, para. 38.

[197] United Nations Human Rights Council, Universal Periodic Review – Thailand, Third Cycle, https://www.ohchr.org/en/hr-bodies/upr/th-index

(2) เพื่อให้เกิดความปั่นป่วนหรือกระด้างกระเดื่องในหมู่ประชาชนถึงขนาดที่จะก่อความไม่สงบขึ้นในราชอาณาจักร หรือ

(3) เพื่อให้ประชาชนล่วงละเมิดกฎหมายแผ่นดิน ต้องระวางโทษจำคุกไม่เกินเจ็ดปี"

ประมวลกฎหมายอาญา มาตรา 116 หรือเรียกสั้น ๆ ว่าความผิดฐาน "ยุยงปลุกปั่น" เป็นความผิดที่อยู่ในลักษณะความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร บ่อยครั้งที่ข้อหานี้ถูกนำไปใช้กับการแสดงออกทางออนไลน์ที่เป็นการวิพากษ์วิจารณ์รัฐบาล หรือพระมหากษัตริย์ โดยเฉพาะในช่วงที่มีการงดใช้มาตรา 112 และเมื่อถูกนำมาใช้กับการแสดงออกทางออนไลน์ มักจะใช้ร่วมกับ พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14 (2) หรือ (3)

ภายหลังการรัฐประหารของ คสช. การดำเนินคดีด้วยมาตรา 116 เพิ่มขึ้นอย่างมีนัยสำคัญ จากข้อมูลที่รวมรวมโดยศูนย์ข้อมูลกฎหมายและคดีเสรีภาพ (iLaw) (ข้อมูลถึงวันที่ 21 พฤษภาคม 2562) ระบุว่ามีผู้ถูกดำเนินคดีด้วยมาตรา 116 จำนวน 117 ราย[198] ขณะที่ศูนย์ทนายความเพื่อสิทธิมนุษยชน ระบุว่ามีอย่างน้อย 14 กรณี เป็นคดีเกี่ยวกับการโพสต์ต่อต้านและวิพากษ์วิจารณ์บุคคลในคณะรัฐบาล และ คสช.[199] และบุคคลที่ตกเป็นเป้าหมายส่วนใหญ่คือนักเคลื่อนไหว นักกิจกรรมทางการเมืองและนักการเมืองฝ่ายตรงข้ามกับ คสช. มีกรณีตัวอย่างที่น่าสนใจ อาทิ การโพสเฟซบุ๊กและทวิตเตอร์นัดหมายให้ประชาชนออกมาชุมนุมต่อต้าน คสช.[200] โพสต์ภาพบุคคลที่เกี่ยวข้องกับโครงการก่อสร้างอุทยานราชภักดิ์ ซึ่งมีเรื่องอื้อฉาวเกี่ยวกับอุทยานราชภักดิ์[201] โพสต์เผยแพร่ ภาพ ข้อความ แสดงความคิดเห็น และแชร์เฟซบุ๊กของผู้อื่นที่มีเนื้อหาต่อต้านรัฐบาล กองทัพ และบุคคลสำคัญ[202] เป็นต้น

ปัจจุบัน หลังการชุมนุมของประชนชนนับตั้งแต่ปี 2563 มาตรา 116 ยังคงถูกนำมาใช้อย่างกว้างขวาง ศูนย์ทนายความเพื่อสิทธิมนุษยชน รายงานว่า นับตั้งแต่เริ่มการชุมนุมของ "เยาวชนปลดแอก" เมื่อวันที่ 18 กรกฎาคม 2563 จนถึงวันที่ 30 กันยายน 2565 มีประชาชนที่ถูกดำเนินคดีมาตรา 116 จำนวน 127 คดี จำนวน 39 คน[203]

---

[198] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย iLaw https://freedom.ilaw.or.th/node/209 เข้าถึง 4 มกราคม 2562

[199] ศูนย์ทนายความเพื่อสิทธิมนุษยชน https://www.tlhr2014.com/?p=11636

[200] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, สมบัติ บุญงามอนงค์ : 116, https://freedom.ilaw.or.th/th/case/604

[201] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, กดไลค์เพจหมิ่นฯ และเสียดสีสุนัขทรงเลี้ยง, https://freedom.ilaw.or.th/case/702

[202] ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดย ไอลอว์, โพสต์เฟซบุ๊กวิจารณ์รัฐบาลและกองทัพ, https://freedom.ilaw.or.th/case/698

[203] ศูนย์ทนายความเพื่อสิทธิมนุษยชน. วันที่ 4 กันยายน 2565. อ้างแล้ว

หากพิจารณาในแง่ของผลทางคดี ที่ผ่านมาการใช้ข้อหายุยงปลุกปั่นตามมาตรา 116 อาจไม่ค่อยประสบความสำเร็จมากนั้น เพราะคดีส่วนใหญ่มักจะยุติไป[204] แต่ไม่ว่าจะอย่างไร การดำเนินคดีด้วยข้อหาที่มีโทษสูงเช่นนี้ ย่อมมีผลกระทบในแง่อื่น เช่น การสร้างความกลัวเพื่อให้หยุดเคลื่อนไหว การเพิ่มภาระให้จำเลย โดยเฉพาะภาระทางคดี ซึ่งต้องหาหลักทรัพย์ประกันตัวสูงตามอัตราโทษ ผู้ที่ถูกดำเนินคดีส่วนใหญ่ต้องยื่นหลักทรัพย์ประกันตัวโดยเฉพาะคนละประมาณ 70,000 – 75,000 บาท บางคดีอาจสูงถึงถึงหลักแสน[205]

อย่างไรก็ดี มีแนวโน้มที่น่ากังวลในปัจจุบันคือ คดีของนายทิวากร ซึ่งถูกดำเนินคดีมาตรา 116 และ พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14 (3) จากกรณีการโพสต์บนเฟซบุ๊กชวนคนลงชื่อทำประชามติเลือกว่าจะคงไว้หรือยกเลิกระบอบกษัตริย์ผ่านเว็บไซต์ change.org โดยศาลจังหวัดลำปางมีคำพิพากษาเมื่อวันที่ 4 ตุลาคม 2565 ให้ลงโทษจำคุกเขา 3 ปี แต่รอลงอาญาไว้ 3 ปี เนื่องจากจำเลยมิเคยมีคำพิพากษาให้ลงโทษจำคุกมาก่อนนั้น

เช่นเดียวกับข้อหาอื่นที่กล่าวมา ข้อหายุยงปลุกปั่นตามมาตรา 116 ก็มีบทบัญญัติบางส่วนที่มีความคลุมเครือ สามารถตีความได้กว้าง เช่น คำว่า “เพื่อให้เกิดความปั่นป่วน หรือกระด้างกระเดื่องในหมู่ประชาชน” ซึ่งไม่แน่ชัดว่า การกระทำเช่นใดบ้างจึงจะเป็นการแสดงออกที่ขัดต่อ มาตรา 116 ดังกล่าว

ในรอบ UPR ที่ 3 (ปี 2564) ของประเทศไทยนั้น ประเทศต่าง ๆ โดยเฉพาะประเทศในยุโรปก็เสนอแนะให้ประเทศไทยพิจารณาทบทวนแก้ไขประมวลกฎหมายอาญามาตรา 116 ให้สอดคล้องกับ ICCPR อาทิ ลักเซมเบิร์ก สวิตเซอร์แลนด์ แคนาดา อย่างไรก็ดี ข้อเสนอเหล่านั้นดังกล่าวไม่ได้รับการตอบรับจากรัฐบาลไทย เช่นเดียวกับข้อเสนอให้ทบทวนแก้ไขประมวลกฎหมายอาญา มาตรา 112[206]

4) ประมวลกฎหมายอาญา มาตรา 326 และ 328 (หมิ่นประมาทบุคคลธรรมดา)

ประเทศไทยกำหนดความผิดฐานหมิ่นประมาทไว้ในประมวลกฎหมายอาญา ดังนี้

มาตรา 326 ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สาม โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา328 ถ้าความผิดฐานหมิ่นประมาทได้กระทำโดยการโฆษณาด้วยเอกสาร ภาพวาด ภาพระบายสี ภาพยนตร์ ภาพหรือตัวอักษรที่ทำให้ปรากฏไม่ว่าด้วยวิธีใด ๆ แผ่นเสียง หรือสิ่ง

---

[204] ไอลอว์, มาตรา 116: เมื่อข้อหา “ยุยงปลุกปั่น” ถูกใช้เป็นเครื่องมือปิดกั้นการแสดงออก, 30 สิงหาคม 22560, https://freedom.ilaw.or.th/node/532

[205] iLaw, “ยุยงปลุกปั่น” ตามมาตรา 116 ข้อหาเพื่อประโยชน์ทางการเมืองในยุครัฐบาลคสช., 13 กรกฎาคม 258, https://freedom.ilaw.or.th/blog/116NCPO

[206] United Nations Human Rights Council, Universal Periodic Review – Thailand, Third Cycle, https://www.ohchr.org/en/hr-bodies/upr/th-index

บันทึกเสียง บันทึกภาพ หรือบันทึกอักษร กระทำโดยการกระจายเสียง หรือการกระจายภาพ หรือโดยกระทำการป่าวประกาศด้วยวิธีอื่น ผู้กระทำต้องระวางโทษจำคุกไม่เกินสองปี และปรับไม่เกินสองแสนบาท

โดยมีข้อยกเว้นความรับผิดและโทษตามมาตรา 329 และ 330 ดังนี้

มาตรา 329 ผู้ใดแสดงความคิดเห็นหรือข้อความใดโดยสุจริต

(1) เพื่อความชอบธรรม ป้องกันตนหรือป้องกันส่วนได้เสียเกี่ยวกับตนตามคลองธรรม

(2) ในฐานะเป็นเจ้าพนักงานปฏิบัติการตามหน้าที่

(3) ติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ หรือ

(4) ในการแจ้งข่าวด้วยความเป็นธรรมเรื่องการดำเนินการอันเปิดเผยในศาลหรือในการประชุม

ผู้นั้นไม่มีความผิดฐานหมิ่นประมาท

มาตรา 330 ในกรณีหมิ่นประมาท ถ้าผู้ถูกหาว่ากระทำความผิด พิสูจน์ได้ว่าข้อที่หาว่าเป็นหมิ่นประมาทนั้นเป็นความจริง ผู้นั้นไม่ต้องรับโทษ

แต่ห้ามไม่ให้พิสูจน์ ถ้าข้อที่หาว่าเป็นหมิ่นประมาทนั้นเป็นการใส่ความในเรื่องส่วนตัว และการพิสูจน์จะไม่เป็นประโยชน์แก่ประชาชน

ข้อหาหมิ่นประมาททางอาญา โดยเฉพาะมาตรา 328 การหมิ่นประมาทโดยการโฆษณานั้น มักถูกนำมาใช้ดำเนินคดีกับการแสดงออกทางออนไลน์ โดยเฉพาะจากภาคเอกชนที่ได้นำข้อหานี้มาใช้ฟ้องคดีกับนักกิจกรรม นักปกป้องสิทธิมนุษยชน รวมถึงแกนนำชาวบ้านที่คัดค้านกิจการของบริษัทหรือตรวจสอบการละเมิดสิทธิมนุษยชนโดยบริษัท[207] ซึ่งเดิมข้อหานี้มักถูกใช้คู่กับ พ.ร.บ. คอมพิวเตอร์ฯ มาตรา 14 (1) แต่ทิศทางดังกล่าวเปลี่ยนไปภายหลังการประกาศใช้ พ.ร.บ. คอมพิวเตอร์ฯ (ฉบับที่ 2) พ.ศ. 2560 ซึ่งแก้ไขมาตรา 14 (1) กำหนดชัดเจนว่าไม่ให้ใช้ข้อหาหมิ่นประมาทควบคู่กับมาตรา 14 (1)

การใช้ข้อหาหมิ่นประมาททางอาญาโดยบริษัทในการฟ้องปิดปาก (SLAPPs) ต่อนักข่าว นักสิ่งแวดล้อม นักกิจกรรม นักปกป้องสิทธิมนุษยชน และแกนนำชาวบ้านที่เคลื่อนไหวหรือแสดงออกคัดค้านการ

---

[207] สมาคมนักกฎหมายสิทธิมนุษยชน, รายงานข้อเสนอแนะต่อการคุ้มครองผู้ใช้สิทธิและเสรีภาพเพื่อการมีส่วนร่วมในประเด็นสาธารณะจากการถูกฟ้องคดี, https://naksit.net/2019/06/reportslapps-public-participation/ ; แดชบอร์ดการฟ้อง SLAPPs โดยภาคธุรกิจ, https://datastudio.google.com/u/1/reporting/9b79cca7-80ab-4f14-bfb1-2c7a29d4204d/page/Su0fC

ดำเนินการหรือตรวจสอบการดำเนินการของบริษัทนั้น ยังคงเป็นความกังวลสำคัญในปัจจุบัน แม้จะมีประเทศไทยจะประกาศใช้ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 161/1 และ 165/2 ในฐานะเครื่องมือทางกฎหมายของศาลในการกลั่นกรองคดีที่ฟ้องมาโดยไม่สุจริต หรือแกล้งฟ้อง ซึ่งอาจรวมถึงคดีลักษณะ SLAPP ด้วยนั้น แต่นับตั้งแต่กฎหมายดังกล่าวใช้บังคับ ผู้วิจัยรวบรวมได้ ยังไม่พบว่ามาตรา 161/1 ถูกนำมาใช้จัดการกับคดีฟ้องปิดปากหรือ SLAPPs เลย

ประเด็นสำคัญอีกประการหนึ่งของความผิดฐานหมิ่นประมาทคือ การยังคงกำหนดให้เป็นความผิดที่มีโทษทางอาญา ซึ่งดังที่กล่าวไปแล้วว่า กลไกสิทธิมนุษยชนของสหประชาชาติได้เน้นย้ำข้อเรียกร้องให้มีการยกเลิกโทษทางอาญาของความผิดฐานหมิ่นประมาท โดยเฉพาะโทษจำคุก เพราะถือว่าไม่ได้สัดส่วนสำหรับการจำกัดเสรีภาพในการแสดงออก

กล่าวโดยสรุป กฎหมายหลายเรื่องที่ถูกนำมาใช้จำกัดเนื้อหาทางออนไลน์ ยังมีถ้อยคำที่คลุมเครือ นอกจากนี้ กฎหมายบางฉบับมีการใช้โทษทางอาญาที่ค่อยข้างสูง เช่น มาตรา 112 แห่งประมวลกฎหมายอาญาที่กำหนดโทษจำคุกขั้นต่ำเริ่มต้นจาก 3 ปี รวมถึงการยังคงกำหนดให้ความผิดฐานหมิ่นประมาทเป็นความผิดทางอาญา ถือว่าไม่ได้สัดส่วนและขัดต่อข้อกำหนดข้องข้อ 19 (3) ของ ICCPR

นอกจากนี้ การฟ้องคดีโดยใช้ข้อหาทางอาญายังเอื้อให้เกิดการละเมิดสิทธิในกระบวนการยุติธรรม ทั้งการจับกุมควบคุมตัวโดยอำเภอใจ โดยไม่มีหมายจับ การอายัดตัวซ้ำซาก การกีดกันการพบญาติและทนายความ การทำให้สูญเสียเสรีภาพจากการถูกคุมขังระหว่างพิจารณาคดี[208] ซึ่งล้วนละเมิดสิทธิในการพิจารณาคดีที่เป็นธรรม (Right to Fair trial) ตามที่ ICCPR ข้อ 9 และ 14 รับรองไว้ ตัวอย่างที่เห็นได้ชัดในปัจจุบันคือ การดำเนินคดีในข้อหาหมิ่นประมาทกษัตริย์ ตามประมวลกฎหมายอาญา มาตรา 112 ที่ผู้ถูกดำเนินคดีต้องพบกับอุปสรรคที่จะได้รับการปล่อยตัวระหว่างการดำเนินคดี[209] และต้องหยุดเคลื่อนไหวหรือยอมเซ็นเซอร์ตนเองไปในที่สุด

4.4.2.3 การตัดการเชื่อมต่อ/ปิดอินเทอร์เน็ต (Internet shutdowns)

รายงาน Traffic and Disruptions ของ Google ที่เผยแพร่ผ่านรายงานเพื่อความโปร่งใสของ Google ซึ่งวัดความสามารถในการเข้าถึงผลิตภัณฑ์ต่างๆ ของ Google และบันทึกการหยุดชะงักอย่างกะทันหัน

---

[208] สมาคมนักกฎหมายสิทธิมนุษยชน, สถานการณ์การฟ้องคดีปิดปากในประเทศไทย : มีกลไกกลั่นกรองแล้ว แต่ทำไมแนวโน้มคดียังสูงขึ้นต่อเนื่อง ,https://naksit.net/2021/03/reportslapp/

[209]ศูนย์ทนายความเพื่อสิทธิมนุษยชน ,https://tlhr2014.com/archives/27450?fbclid=IwAR3bi44QN3gSE3jZ4r7z7WA9BLy8HG4BkJ_F0Bzh2W_OIUHAK7FODASOxeA

ของผลิตภัณฑ์เหล่านั้น ซึ่งเกิดจากการตรวจพบของ google เอง และที่รายงานโดยบุคคลภายนอก พบว่า ในส่วนของประเทศไทย ตั้งแต่ปี 2541 ถึงปัจจุบัน (กันยายน 2565) ยังไม่มีรายงานการหยุดชะงัก[210]

และจากข้อมูลของ Access Now ผ่านแคมเปญ #KeepItOn โครงการ Shutdown Stories[211] และโครงการ Shutdown Tracker Optimization (STOP) ได้รวบรวมข้อมูลเกี่ยวกับการหยุดชะงักของอินเทอร์เน็ต ซึ่งจากข้อมูลดังกล่าวยังไม่พบการรายงานข้อมูลการหยุดชะงักในส่วนของประเทศไทย[212]

อย่างไรก็ดี ในช่วงวันหลังรัฐประหารหนึ่งวัน คือวันที่ 28 พฤษภาคม 2557 มีรายงานว่าเฟซบุ๊คล่มในช่วงเวลา 15.35 น. เป็นเวลา 30 นาที โดยในช่วงต้นมีการให้ข่าวที่ค่อนข้างสับสนว่าการล่มดังกล่าวเกิดจากการสั่งปิดของผู้มีอำนาจ หรือเป็นความผิดพลาดทางเทคนิค แต่ในช่วงหลังมีการปฏิเสธและชี้แจงว่าเป็นเรื่องความผิดพลาดทางเทคนิค[213]

DTAC ซึ่งเป็นบริษัทโทรคมนาคมของ Norwegian Telenor Group เปิดเผยต่อสาธารณะเมื่อวันที่ 9 มิถุนายน 2557 และออกแถลงการณ์ยอมรับว่าในวันที่ 28 พฤษภาคม 2557 ได้รับการแจ้งเตือนเวลา 15:00 น. ตามเวลาท้องถิ่นจาก กสทช. ถึงการจำกัดการเข้าถึงเฟซบุ๊คชั่วคราว[214] อย่างไรก็ดี ประธาน กสทช. ในขณะนั้น ออกมากล่าวในอีกสองวันต่อมา ปฏิเสธการมีอยู่ของการแจ้งเตือนดังกล่าว[215] และหนึ่งสัปดาห์หลังจากออกแถลงการณ์ DTAC ถูกบังคับให้ขอโทษต่อสาธารณชน และเป็นเรื่องที่น่าสนใจที่คำแถลงดังกล่าวไม่ได้ถอนการอ้างว่าได้รับคำสั่งให้ปิดเฟซบุ๊ค[216]

นอกจากข้อน่าสงสัยเกี่ยวกับการปิดเฟซบุ๊คภายหลังรัฐประหารดังกล่าวแล้ว ในช่วงที่มีสถานการณ์การชุมนุมทางการเมืองปี 2563 พบว่า อินเทอร์เน็ตในพื้นที่ชุมนุมมีความเร็วลดลงหรือใช้ไม่ได้ เมื่อเทียบกับนอกพื้นที่ชุมนุม[217] อย่างไรก็ดี ปัญหาการเข้าใช้อินเทอร์เน็ตดังกล่าวอาจจะมาจากหลายสาเหตุ รวมถึง

---

[210] https://transparencyreport.google.com

[211] คำให้การส่วนบุคคลจากการหยุดทำงาน ซึ่งส่วนใหญ่ส่งมาโดยอาสาสมัครและนักเคลื่อนไหวในพื้นที่

[212] https://docs.google.com/spreadsheets/d/1DvPAuHNLp5BXGb0nnZDGNoiIwEeu2ogdXEIDvT4Hyfk/edit#gid=1098610033

[213] ปริศนา เฟซบุ๊คล่ม กว่าครึ่งชั่วโมง?, Sanook, 29 พ.ค. 2557, https://www.sanook.com/hitech/1389193/ ; คสช.แถลง ไม่ได้สั่งปิดเฟซบุ๊ก (28พ.ค.57), Thai PBS, https://www.youtube.com/watch?v=gf9UJM3ZzAw&t=32s

[214] TNW, Telenor says Thailand's recent Facebook outage was ordered by the government , 9 June 2014, https://thenextweb.com/news/operator-DTAC-says-thailands-government-forced-shut-access-facebook

[215] The Nation, Telenor must comply with martial law: NBTC, 12 June 2014, https://www.nationmultimedia.com/news/business/corporate/30236007

[216]The Nation, Telenor Group apologises for saying dtac ordered to block Facebook, 15 June 2014, https://www.nationmultimedia.com/news/breakingnews/aec/30236306

[217] การรับฟังความเห็นคู่มือ พ.ร.บ. ชุมนุมสาธารณะ วันที่ 30 กันยายน 2565

การที่มีผู้ใช้งานเป็นจำนวนมากก็อาจส่งผลต่อการเข้าถึงได้ ส่วนการถูกรบกวนหรือตัดสัญญาณโดยเจตนาก็อาจจะเป็นไปได้เช่นกัน

ทั้งนี้ ในช่วงของการชุมนุมเมื่อวันที่ 23 สิงหาคม 2563 ณ ลานคนเมืองนั้น มีรายงานว่ามีการเผยแพร่หนังสือราชการทางสื่อสังคมออนไลน์ เกี่ยวกับการให้จัดรถยนต์อุปกรณ์ต่อต้าน ตัดสัญญาณสื่อสาร (Jammer) ในการจัดกิจกรรมชุมนุม เมื่อวันที่ 23 สิงหาคม 2563 บริเวณลานคนเมือง ศาลาว่าการกรุงเทพมหานคร อย่างไรก็ดี ฝ่ายตำรวจมีการชี้แจงว่า การจัดรถยนต์อุปกรณ์ต่อต้านตัดสัญญาณสื่อสาร (Jammer) ถูกนำมาใช้เป็นประจำในบริเวณสถานที่จัดงานขนาดใหญ่ เป็นการปฏิบัติหน้าที่โดยปกติของเจ้าหน้าที่ตำรวจ หน่วยเก็บกู้วัตถุระเบิด เนื่องจากกรณีที่พบวัตถุต้องสงสัยในขณะเข้าไปตรวจสอบหรือเก็บกู้ เจ้าหน้าที่จะต้องตัดสัญญาณโทรศัพท์ ณ จุดดังกล่าวในห้วงเวลาการปฏิบัติสั้น ๆ เพื่อความปลอดภัยของเจ้าหน้าที่ และประชาชนบริเวณโดยรอบ ส่วนเหตุที่มีการอ้างว่าเจ้าหน้าที่ใช้เครื่องตัดสัญญาณ จนสัญญาณอินเตอร์เน็ตใช้ไม่ได้ทั้งบริเวณการชุมนุม ไม่เป็นความจริง เพราะเครื่องตัดสัญญาณสามารถใช้ได้ในรัศมี จำกัด และในช่วงเวลาสั้น ๆ เท่านั้น[218]

4.4.2.4 แคมเปญข้อมูลบิดเบือน

แนวทางที่สร้างสรรค์ในการจัดการข้อกังวลด้านเนื้อหา ซึ่งสอดคล้องกับเจตนารมณ์ของกับเสรีภาพในการแสดงออกมากที่สุด คือการทำให้เกิดการสนทนาอย่างกว้างขวาง ซึ่งรัฐมีหน้าที่ที่จะจัดสภาพแวดล้อมให้เอื้ออำนวย รวมถึงการให้ข้อมูลแก่สาธารณะอย่างถูกต้องและเพียงพอ ถือเป็นพันธกรณีตามกฎหมายสิทธิมนุษยชนระหว่างประเทศประการหนึ่งที่รัฐต้องดำเนินการ อย่างไรก็ดี การดำเนินการดังกล่าวต้องมีความโปร่งใส เพื่อลดความเคลือบแคลงสงสัย และสร้างความไว้เนื้อเชื่อใจระหว่างกัน

ที่ผ่านมารัฐบาลไทยถูกกล่าวหาว่ามีการสนับสนุนแคมเปญบิดเบือนข้อมูล หรือบางครั้งเรียกว่าปฏิบัติการข้อมูลข่าวสาร (IO) ซึ่งมักไม่โปร่งใสและดำเนินไปอย่างลับ ๆ รัฐบาลถูกกล่าวหาว่ามีการจ้างผู้แสดงความเห็นที่สนับสนุนรัฐบาลงอย่างลับๆ เพื่อโฆษณาชวนเชื่อและการบิดเบือนข้อมูลบนอินเทอร์เน็ต ก่อกวนและโพสต์โจมตีลดทอนความน่าเชื่อถือของฝ่ายตรงข้ามรัฐบาล[219]

มีการอภิปรายประเด็นการปฏิบัติการข้อมูลข่าวสาร หรือ IO โดยรัฐอย่างกว้างขวางในช่วงเวลาหลายปีที่ผ่านมาทั้งในสภาและนอกสภา โดยเฉพาะการสนับสนุน IO ของหน่วยงานในกองทัพ

---

[218] สำนักข่าวไทย, บช.น. ชี้แจงกรณีใช้รถตัดสัญญาณในพื้นที่ชุมนุม, 24 สิงหาคม 2563, https://tna.mcot.net/crime-515851

[219] บีบีซีไทย, ไอโอ : คณะก้าวหน้าเปิดโปงข้อมูลเครือข่ายปฏิบัติการข่าวสารกองทัพ ด้านเอกชนแถลงโต้ชี้ข้อมูลบิดเบือน, 1 ธันวาคม 2563, https://www.bbc.com/thai/thailand-55145803

ประเด็น IO มีบทบาทไม่ใช่เฉพาะในประเด็นความขัดแย้งทางการเมืองที่ส่วนกลาง ในพื้นที่จังหวัดชายแดนภาคใต้ IO มีบทบาทอย่างสำคัญในการโจมตีนักสิทธิมนุษยชนสตรีที่ทำงานด้านการต่อต้านการซ้อมทรมานและตรวจสอบกองทัพในพื้นที่จังหวัดชายแดนภาคใต้ โดยผู้กระทำสร้างโปรไฟล์ปลอมเพื่อสร้างความเกลียดชัง ซึ่งมุ่งเป้าไปที่การหมิ่นประมาทและเป็นการล่วงละเมิด ด้วยการโพสต์เรื่องราว และบทความที่มีเป้าหมายในการทำลายชื่อเสียงของนักปกป้องสิทธิมนุษยชน

> *“ช่วงก่อนหน้านี้ มันไม่ได้เป็นระบบขนาดนี้ แล้วมันก็จะมีการถ่วงดุลโดยสื่ออื่น ๆ แต่คิดว่า IO มีบทบาทสูงมากในช่วงหลัง เว็บไซต์ Pulony ถือเป็นช่องทางหลักที่ใช้ด่าพวกนักปกป้องสิทธิผู้หญิงในจังหวัดชายแดนภาคใต้ตลอด 10 ปีที่ผ่านมา แต่มันก็หยุดลง หลังจากพรรคก้าวไกลเอาประเด็น IO ไปอภิปรายในสภา มันหยุดลงหลังจากที่ปิงบประมาณปีที่แล้วหมดลง เดือนกันยายน 2563 Pulony ก็ไม่ Active อีกเลย แต่ไม่ได้หมายความว่ามันจะหมดไป เขาก็โผล่เพจอื่นซึ่งก็เป็นภาระของพวกเราหรือภาระของหน่วยงานที่ทำการตรวจสอบ หรือแม้กระทั่ง ส.ส. ที่สนใจประเด็นนี้ ก็ต้องไปสืบเสาะอีกว่ากระแสการเงินจากงบทหารลงไปสู่เพจเหล่านั้นจริงหรือไม่ จากการตรวจสอบอภิปรายในสภา มีข้อมูลที่หลุดออกมาจากการตรวจสอบของเขา มีพยานหลักฐานชัดเจนว่า Pulony เป็นเว็บเพจที่ใช้เงินภาษี....”*[220]

ประเด็น IO เริ่มชัดเจนเมื่อเฟซบุ๊ค และทวิตเตอร์ได้แจ้งการดำเนินการปิดบัญชีที่น่าสงสัยในไทยหลายร้อยบัญชี

โดยในเดือนกรกฎาคม 2562 เฟซบุ๊คได้เปิดเผยเกี่ยวกับการลบบัญชีผู้ใช้ที่มีพฤติกรรมร่วมกันในการสร้างความเข้าใจผิดเกี่ยวกับตัวตน (coordinated inauthentic behavior หรือ CIB) โดยพบว่าจุดเริ่มต้นของเครือข่ายดังกล่าว มาจาก 4 ประเทศ รวมถึงประเทศไทย ซึ่งเครือข่ายเหล่านี้ไม่มีความเชื่อมโยงกัน แต่มีการใช้วิธีการที่คล้ายคลึงกัน คือสร้างเครือข่ายบัญชีผู้ใช้ที่ไม่สามารถตรวจสอบตัวตนได้ โดยในส่วนของประเทศไทย เฟซบุ๊คได้ลบบัญชีผู้ใช้จำนวน 12 บัญชี และแฟนเพจจำนวน 10 เพจ[221] ต่อมาในเดือนกุมภาพันธ์ 2564 เฟซบุ๊คแจ้งว่าได้ลบบัญชีผู้ใช้และกลุ่มที่เกี่ยวข้องกับปฏิบัติการข้อมูลข่าวสารของกองทัพ (IO) ในไทยรวม 185 บัญชี โดยบัญชีที่ถูกลบประกอบด้วยบัญชีผู้ใช้ 77 บัญชี เพจ 72 เพจ และกลุ่มใน Facebook อีก 18 กลุ่ม นอกจากนี้ยังมีบัญชีผู้ใช้ใน Instagram อีก 18 บัญชี ซึ่งนี้ถือเป็นครั้งแรกที่ดำเนินการกับบัญชีผู้ใช้ที่มีความเชื่อมโยงกับกองทัพไทย[222]

---

[220] สัมภาษณ์ตัวแทนมูลนิธิผสานวัฒนธรรม, วันที่ 13 กรกฎาคม 2564, ผ่านระบบอิเล็กทรอนิกส์ (ZOOM)

[221] ฐานเศรษฐกิจ, Facebook ลบเพจและบัญชีผู้ใช้ 'ป่วน' ในไทยกว่า 20 ราย, 25 กรกฎาคม 2562, https://www.thansettakij.com/tech/innovation/405874

[222] The Standard, Facebook ลบ 185 บัญชีและกลุ่มที่เกี่ยวข้องกับปฏิบัติการ IO ของกองทัพไทย, 4 มีนาคม 2564, https://thestandard.co/facebook-removes-thai-military-linked-information-influencing-accounts/

ส่วนทวิตเตอร์ เมื่อวันที่ 9 ตุลาคม 2563 ได้ปล่อยรายงานการตรวจสอบเครือข่ายปฏิบัติการข้อมูลข่าวสาร (IO) โดยละเมิดนโยบายการใช้งานของทวิตเตอร์ จำนวน 1,589 บัญชี พบมาจากประเทศไทย อิหร่าน รัสเซีย คิวบา และซาอุดีอาระเบีย ทวิตเตอร์ได้ระงับการใช้งานบัญชี IO ทุกบัญชีเรียบร้อยแล้ว โดยในส่วนที่พูดถึงประเทศไทยนั้น ทวิตเตอร์อธิบายว่า จากการตรวจสอบทางเครือข่าย พบเป็นบัญชีที่มีความเกี่ยวข้องกับกองทัพบก จำนวน 926 บัญชี[223] นอกจากนี้ ทวิตเตอร์ได้ส่งข้อมูลชุดนี้ไปให้ศูนย์นโยบายไซเบอร์ของมหาวิทยาลัยสแตนฟอร์ด และทีมวิจัยในโปรแกรม Stanford Internet Observatory ได้เผยแพร่รายงานการวิเคราะห์ชื่อว่า “ Cheerleading Without Fans: A Low-Impact Domestic Information Operation by the Royal Thai Army” ชี้ว่าปฏิบัติการข้อมูลข่าวสารของกองทัพบกครั้งนี้มีขึ้นเพื่ออวยกันเอง (Cheerleading Without Fans) เป็นปฏิบัติการที่ส่งผลกระทบน้อย (Low-Impact) และใช้วิธีที่ไม่ซับซ้อน (Unsophisticated) โดยบัญชีเหล่านี้มีพฤติกรรมสำคัญ ได้แก่ การสนับสนุนกองทัพและทหาร เช่น การยกย่องการช่วยเหลือประชาชนของทหารในภาพรวม การชื่นชมกองทัพและรัฐบาลเรื่องโควิด-19 การเบี่ยงเบนประเด็นและลดการวิจารณ์กองทัพจากเหตุการณ์กราดยิงโคราช และโจมตีพรรคอนาคตใหม่/พรรคก้าวไกล ด้วยการทวีตข้อมูลทับถม (Dogpile) ซ้ำเติมหรือสนับสนุนการยุบพรรคอนาคตใหม่[224]

อย่างไรก็ดี หลังจาก ทวิตเตอร์ได้เปิดเผยข้อมูลการปิดบัญชีผู้ใช้งานดังกล่าว กองทัพบกได้ออกมาชี้แจงว่า ที่ผ่านมากองทัพบกใช้โซเชียลมีเดียต่างๆ เพื่อการประชาสัมพันธ์งานของกองทัพบก โดยเฉพาะงานที่สำคัญที่สุดคือการช่วยประเทศไทยในภูมิภาคต่าง ๆ ที่มีสถานการณ์วิกฤต เช่น ภัยพิบัติ โดยใช้โซเชียลมีเดียในการติดตามและสั่งการหน่วยงานต่าง ๆ ให้ลงพื้นที่เร็วที่สุด และยืนยันว่าไม่มีการใช้โซเชียลมีเดียในลักษณะตามที่ถูกกล่าวหาแต่อย่างใด และมองว่าการที่ทวิตเตอร์สรุปว่ามีความเกี่ยวข้องกับกองทัพบกนั้น น่าจะเป็นข้อสรุปที่ไม่เป็นธรรมกับกองทัพบก เพราะการประมวลผลภาพรวมขาดการวิเคราะห์เชิงลึก พร้อมทั้งยืนยันว่าเรื่องปฏิบัติการ IO เป็นความเข้าใจที่คลาดเคลื่อน กองทัพบกไม่ได้มีการดำเนินการในเรื่องดังกล่าว เพราะไม่ใช่ภารกิจหรือวัตถุประสงค์ในการใช้ Twitter ของกองทัพ[225]

การสนับสนุนแคมเปญบิดเบือนของมูลโดยรัฐนั้น เป็นเรื่องที่ยากแก่การตรวจสอบ เพราะมักจะเป็นเรื่องปิดลับ รัฐจึงต้องตระหนักถึงพันธกรณีด้านสิทธิมนุษยชนของตน ดังที่ถูกเรียกร้องในคำแถลงร่วมปี 2560

---

[223] Twitter Blog, Disclosing networks to our state-linked information operations archive, 8 October 2020, https://blog.twitter.com/en_us/topics/company/2020/disclosing-removed-networks-to-our-archive-of-state-linked-information

[224] Josh A. Goldstein, et al., Cheerleading Without Fans: A Low-Impact Domestic Information Operation by the Royal Thai Army, 8 October 2020, https://stacks.stanford.edu/file/druid:ym245nv3149/twitter-TH-202009.pdf

[225] มติชน, ‘ทบ.’ โต้ ‘ทวิตเตอร์’ กองทัพไม่มีบัญชีไอโอโจมตีฝ่ายค้าน มีแค่บัญชีใช้ประชาสัมพันธ์, 9 ตุลาคม 2563, https://www.matichon.co.th/politics/news_2386935

(ค.ศ. 2017) ผู้รายงานพิเศษว่าด้วยเสรีภาพในการแสดงความคิดเห็นและการแสดงออกของสหประชาชาติ และพันธมิตรอีกหลายองค์กร เรียกร้องให้

> *"ผู้กระทำการรัฐไม่ควรจัดทำ สนับสนุน ส่งเสริม หรือเผยแพร่ข้อความที่พวกเขารู้หรือควรทราบอย่างมีเหตุผลว่าเป็นเท็จ (Disinformation) หรือแสดงการเพิกเฉยโดยประมาทต่อข้อมูลที่ตรวจสอบได้ (Propaganda) .... ควรปฏิบัติตามพันธกรณีทางกฎหมายในประเทศและระหว่างประเทศและหน้าที่สาธารณะของตน ดูแลเพื่อประกันว่ามีการเผยแพร่ข้อมูลที่เชื่อถือได้และน่าไว้วางใจได้ ซึ่งรวมถึงเรื่องที่สาธารณประโยชน์ เช่น เศรษฐกิจ สาธารณสุข ความมั่นคงและสิ่งแวดล้อม"*[226]

นอกจากนี้ รัฐควรยืนยันถึงความมุ่งมั่นต่อเสรีภาพ ความหลากหลาย และความเป็นอิสระของสื่อ การรับรองความปลอดภัยของนักข่าวออนไลน์และออฟไลน์ และการยุติการไม่ต้องรับโทษสำหรับการคุกคามประชาชนในรูปแบบต่าง ๆ[227]

4.5 สรุปส่งท้าย

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้รับรองเสรีภาพในการแสดงออกไว้ค่อนข้างสอดคล้องกับข้อ 19 ของ ICCPR แต่มีบางเรื่องที่อาจยังมีความคลุมเครือ เช่น สิทธิในการมีความคิดเห็นโดยปราศจากการแทรกแซง ซึ่งรัฐธรรมนูญแห่งราชอาณาจักรไทยได้รับรองไว้ในส่วนเดียวกับเสรีภาพในการแสดงออก ซึ่งทำให้ถูกมองว่าเป็นสิทธิที่อาจถูกจำกัดได้ จึงอาจไม่สอดคล้องกับข้อ 19 ของ ICCPR

เมื่อพิจารณาจากสถานการณ์การจำกัดเนื้อหาทางออนไลน์ ซึ่งเชื่อมโยงกับเสรีภาพในการแสดงออกนั้น มีทั้งการพัฒนาในเชิงบวกและสิ่งที่ยังน่ากังวล โดยพัฒนาการเชิงบวก เกิดจากการที่ศาลได้วางบรรทัดฐานของศาลเกี่ยวกับการพิจารณาปิดกั้นเนื้อหาทางออนไลน์ โดยกำหนดให้มีการไต่สวนคัดค้านการขอปิดกั้นเว็บไซต์ และศาลเองก็พยายามแสดงให้เห็นว่าได้ให้ความสำคัญกับเรื่องสิทธิมนุษยชนในการพิจารณาปิดกั้นเนื้อหา

ส่วนสิ่งที่ยังคงน่ากังวลของการจำกัดเนื้อหาทางออนไลน์ คือสถานการณ์การฟ้องคดีต่อการเผยแพร่เนื้อหาหรือการแสดงออกทางออนไลน์ที่ยังมีแนวโน้มน่าเป็นห่วง โดยเฉพาะภายใต้สถานการณ์ความขัดแย้งทางการเมืองในปัจจุบัน ซึ่งรัฐได้เข้ามาเป็นผู้เล่นหลักในการดำเนินคดีกับประชาชน โดยมีการนำกฎหมาย

---

[226] 2017 Joint declaration on freedom of expression and "fake news", disinformation and propaganda, https://www.law-democracy.org/live/wp-content/uploads/2017/03/mandates.decl_.2017.fake-news.pdf

[227] A/HRC/47/25, 13 April 2021, para 93.

หลายเรื่องมาใช้ดำเนินคดีกับประชาชน โดยเฉพาะข้อหาเกี่ยวกับประมวลกฎหมายอาญา มาตรา 116 และมาตรา 112

หากจะสรุปโดยวิเคราะห์ผ่านการทดสอบสามส่วนสำหรับการจำกัดเสรีภาพในการแสดงออกตามข้อ 19 (3) ของ ICCPR อาจจะพอสรุปข้อท้าทายได้ดังนี้

ความชอบด้วยกฎหมาย

ตามหลักความชอบด้วยกฎหมาย เรียกร้องให้รัฐจำกัดเนื้อหาทางออนไลน์บนพื้นฐานของกฎหมายที่ชัดเจน แน่นอน คาดหมายได้ และไม่เลือกปฏิบัติ อย่างไรก็ดี พบว่า กฎหมายที่ถูกนำมาใช้จำกัดเนื้อหาทางออนไลน์ในประเทศไทย ไม่ว่าจะโดยการปิดกั้นเนื้อหา หรือการดำเนินคดีกับการเผยแพร่เนื้อหา กฎหมายหลายฉบับยังมีถ้อยคำที่คลุมเครือ โดยเฉพาะที่ปรากฏใน พ.ร.บ. คอมพิวเตอร์ฯ ซึ่งเป็นกฎหมายหลักที่บังคับใช้ในพื้นที่ออนไลน์ เช่น คำว่า ข้อมูลฯ “บิดเบือน” “ปลอม” “เท็จ” "ความสงบเรียบร้อยของประชาชน" ซึ่งไม่มีการนิยามความหมายไว้อย่างชัดเจนว่ามีขอบเขตแค่ไหน จึงอาจทำให้มีความเสี่ยงที่จะถูกนำมาใช้ละเมิดเสรีภาพในการแสดงออก

ดังที่ข้อมูลแสดงให้เห็นแล้วว่า รัฐยังคงใช้ประโยชน์จากมาตรา 14 ของ พ.ร.บ. คอมพิวเตอร์ฯ เพื่อดำเนินคดีกับนักการเมืองฝ่ายค้าน นักเคลื่อนไหว นักปกป้องสิทธิมนุษยชน และกลุ่มประชาสังคมที่ตั้งคำถามหรือวิพากษ์วิจารณ์นโยบายสาธารณะ หรือรัฐบาล หรือผู้นำในรัฐบาล รวมถึงนโยบายการจัดการกับการแพร่ระบาดของไวรัสโคโรนา 2019 ที่บางกรณีถูกแปะป้ายว่าเป็นข้อมูล "ปลอม" หรือ “เท็จ”

ความจำเป็นและได้สัดส่วน

กฎหมายบางฉบับที่ถูกนำมาใช้ยังคงกำหนดอัตราโทษจำคุกไว้ค่อนข้างสูง โดยเฉพาะประมวลกฎหมายอาญา มาตรา 112 ที่กำหนดระวางโทษจำคุกตั้งแต่ 3 ปีถึง 15 ปี ซึ่งถือเป็นโทษที่สูงเกินไปเมื่อเทียบกับลักษณะของการกระทำที่เป็นการวิพากษ์วิจารณ์สถาบันทาการเมืองในระบอบประชาธิปไตย

นอกจากนี้ กฎหมายหมิ่นประมาทยังคงเป็นความผิดอาญาและมีโทษจำคุก 1 ปี สำหรับการหมิ่นประมาททั่วไป และ 2 ปี สำหรับการหมิ่นประมาทโดยการโฆษณา ซึ่งดังกล่าวไว้แล้วว่า กลไกสิทธิมนุษยชนแห่งสหประชาชาติแนะนำให้ลดทอนความเป็นอาชญากรรมของความผิดฐานดังกล่าว โดยเฉพาะการยกเลิกโทษจำคุก เพราะถือว่าไม่ได้สัดส่วนสำหรับการจำกัดเสรีภาพในการแสดงออกตามข้อ 19 (3) ของ ICCPR

บทที่ 5
สิทธิในความเป็นส่วนตัว และการสอดส่องการสื่อสารทางดิจิทัลโดยรัฐ

5.1 ส่วนนำ

เทคโนโลยีใหม่ โดยเฉพาะอย่างยิ่ง อินเทอร์เน็ต สมาร์ทโฟน การวิเคราะห์บิ๊กดาต้า อุปกรณ์สวมใส่ พลังงานอัจฉริยะ และเมืองอัจฉริยะ สร้างความสามารถใหม่สำหรับหน่วยงานภาครัฐและเอกชนในการวิเคราะห์ข้อมูล สร้างโอกาสในเชิงพาณิชย์ และการดำเนินการบริการสาธารณะต่าง ๆ แต่ความก้าวหน้าทางเทคโนโลยีประกอบกับความกังวลด้านความมั่นคงของประเทศที่เพิ่มขึ้น ได้อำนวยความสะดวกและสร้างแรงจูงใจในการรวบรวมข้อมูลจำนวนมาก ทำให้บุคคลและชุมชนเสี่ยงต่อการถูกสอดส่องโดยรัฐบาลและบริษัท

การเปิดเผยรายละเอียดของโครงการการสอดส่องในวงกว้างโดยรัฐบาลสหรัฐและอังกฤษของเอ็ดเวิร์ด สโนว์เดน อดีตนักวิเคราะห์ข่าวกรองชาวอเมริกัน ในเดือนมิถุนายน 2556 ทำให้เกิดความกังวลเกี่ยวกับการสอดส่องการสื่อสารของรัฐบาลในยุคดิจิทัล อันเป็นที่มาให้ในเดือนธันวาคม 2556 สมัชชาใหญ่แห่งสหประชาชาติได้เรียกร้องให้รัฐต่าง ๆ “ทบทวนขั้นตอน แนวทางปฏิบัติ และกฎหมายเกี่ยวกับการสอดส่องการสื่อสาร การสกัดกั้น และการรวบรวมข้อมูลส่วนบุคคล รวมถึงการสอดส่องมวลชน การสกัดกั้น และการรวบรวมเพื่อรักษาสิทธิความเป็นส่วนตัวโดยรับรองการปฏิบัติตามพันธกรณีทั้งหมดภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศอย่างเต็มที่และมีประสิทธิภาพ”[1] รวมทั้งขอให้สำนักงานข้าหลวงใหญ่สิทธิมนุษยชน (OHCHR) จัดทำรายงานเกี่ยวกับสิทธิความเป็นส่วนตัวในยุคดิจิทัล และในปี 2557 คณะมนตรีสิทธิมนุษยชนจัดตั้งอาณัติพิเศษด้านสิทธิในความเป็นส่วนตัว[2] Prof. Joe Cannataci ได้รับการแต่งตั้งให้เป็นผู้รายงานพิเศษว่าด้วยสิทธิในความเป็นส่วนตัวคนแรกในปี 2558[3]

บทนี้จะกล่าวถึงภาพรวมของกรอบกฎหมายระหว่างประเทศในประเด็นที่เกี่ยวข้องกับสิทธิในความเป็นส่วนตัวในยุคดิจิทัล โดยเน้นประเด็นการสอดส่องและสกัดกั้นการสื่อสาร และนำมาวิเคราะห์กรอบกฎหมายที่มีการอนุญาตให้สอดส่องการสื่อสารทางดิจิทัลในประเทศไทย

---

[1] A/RES/68/167, December 18, 2013

[2] A/RES/69/66, December 18, 2014.

[3] A/HRC/RES/28/16, April 1, 2015

5.2 กรอบหลักการสิทธิความเป็นส่วนตัว (Right to privacy)

5.2.1 การคุ้มครองสิทธิความเป็นส่วนตัวในกฎหมายสิทธิมนุษยชน

สิทธิความเป็นส่วนตัวได้รับการรับรองตามข้อ 12 ของ UDHR และข้อ 17 ของ ICCPR และตราสารสิทธิมนุษยชนระหว่างประเทศก็ได้รับรองสิทธิความเป็นส่วนตัวในบริบทเฉพาะไว้เช่นกัน[4]

ข้อ 17 ของ ICCPR ระบุว่า

1. บุคคลจะถูกแทรกแซงความเป็นส่วนตัว ครอบครัว เคหสถาน หรือการติดต่อสื่อสารโดยพลการหรือไม่ชอบด้วยกฎหมายมิได้ และจะถูกลบหลู่เกียรติและชื่อเสียงโดยไม่ชอบด้วยกฎหมายมิได้

2. บุคคลทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายมิให้ถูกแทรกแซงหรือลบหลู่เช่นว่านั้น

คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ[5] และสมัชชาใหญ่แห่งสหประชาชาติ[6] ยืนยันว่าสิทธิเช่นเดียวกันที่บุคคลมีในทางออฟไลน์ ต้องได้รับการคุ้มครองทางออนไลน์ด้วย รวมทั้งสิทธิในความเป็นส่วนตัว

สิทธิในความเป็นส่วนตัวไม่มีคำจำกัดความที่ตกลงร่วมกัน โดยบทความของ Warren และ Brandeis เรื่อง “The Right to Privacy” ที่ตีพิมพ์ในปี 1890 กำหนดให้เป็น “สิทธิที่จะถูกทิ้งให้อยู่ตามลำพัง (right to be left alone)”[7]

ส่วนกลไกพิเศษสิทธิมนุษยชนแห่งสหประชาชาติ กล่าวถึง สิทธิในความเป็นส่วนตัวว่าเป็นสิ่งที่ถูกกำหนดขึ้นเพื่อปกป้อง “ปริมณฑลส่วนตัว (private sphere)” ของปัจเจกบุคคล ทั้งพื้นที่ที่มีและไม่มีปฏิสัมพันธ์กับผู้อื่น โดยปราศจากการแทรกแซงของรัฐและการแทรกแซงที่ไม่พึงประสงค์มากเกินสมควรโดยบุคคลที่ไม่ได้รับเชิญ[8]

องค์กร Privacy International พยายามที่จะสร้างความกระจ่างในประเด็นนี้ด้วยการเสนอความเป็นส่วนตัว 4 ประเภท ได้แก่[9]

---

[4] ข้อ 16 อนุสัญญาว่าด้วยสิทธิเด็ก ; ข้อ 14 อนุสัญญาว่าด้วยการคุ้มครองสิทธิของแรงงานโยกย้ายถิ่นฐานและสมาชิกในครอบครัว ; ข้อ 22 อนุสัญญาว่าด้วยสิทธิคนพิการ

[5] A/HRC/RES/28/16, para. 3. ; A/HRC/RES/26/13, para. 5. ; A/HRC/RES/32/13 ; A/HRC/RES/34/7, para. 4.

[6] A/RES/68/167, para 3. ; A/RES/69/166, para. 3. ; A/RES/71/199, para. 3. ; A/RES/73/179, para. 3.

[7] “The Right to Privacy” (1890) 4 Harvard Law Review 193, pp. 195.

[8] เช่น A/HRC/13/37 para 11 and A/HRC/23/40 para 22, 41..

[9] Privacy International. “Privacy and Human Rights: An International Survey of Privacy Laws and Practice”. from http://gilc.org/privacy/survey/intro.html#defining

- ความเป็นส่วนตัวของข้อมูล (information privacy) ซึ่งเกี่ยวข้องกับการจัดตั้งกฎเกณฑ์ที่ควบคุมการรวบรวมและการจัดการข้อมูลส่วนบุคคล
- ความเป็นส่วนตัวของร่างกาย (bodily privacy) ซึ่งเกี่ยวข้องกับการปกป้องร่างกายของผู้คนจากการบุกรุก
- ความเป็นส่วนตัวของการสื่อสาร (privacy of communications) ซึ่งครอบคลุมความปลอดภัยและความเป็นส่วนตัวในการสื่อสารทุกรูปแบบ รวมทั้งผ่านอินเทอร์เน็ต สิทธิที่จะสามารถติดต่อสื่อสารอย่างเป็นส่วนตัวเป็นเหตุให้รัฐมีพันธกรณีที่จะต้องประกันว่าการสื่อสารทางอินเทอร์เน็ตทุกรูปแบบจะถึงมือผู้รับที่ต้องการ โดยปราศจากการแทรกแซงหรือการตรวจสอบของหน่วยงานของรัฐหรือบุคคลที่สาม[10]
- ความเป็นส่วนตัวในอาณาเขต (territorial privacy) ซึ่งเกี่ยวข้องกับการกำหนดขอบเขตการบุกรุกในบ้านและสภาพแวดล้อมอื่น ๆ เช่น สถานที่ทำงานหรือพื้นที่สาธารณะ

ในยุคดิจิทัล ซึ่งเป็นยุคที่ขับเคลื่อนด้วยข้อมูล ความเป็นส่วนตัวของข้อมูลและการสื่อสารจึงเป็นสิ่งที่ได้รับผลกระทบมากที่สุด

ความสะดวกและพลังในการกระจายข้อมูลผ่านเทคโนโลยีใหม่ ส่งผลกระทบอย่างมากต่อการปกป้องความเป็นส่วนตัว การคุ้มครองสิทธิในความเป็นส่วนตัวไม่ได้จำกัดอยู่เฉพาะในพื้นที่ส่วนตัวอีกต่อไป แต่ได้ขยายไปถึง “พื้นที่สาธารณะ” รวมถึงข้อมูลส่วนบุคคลที่ใช้ประโยชน์ในทางสาธารณะ โดยเฉพาะเมื่อรัฐบาลมีการสอดส่องพื้นที่สาธารณะเพื่อเฝ้ามองบุคคล ในทำนองเดียวกันเมื่อมีการรวบรวมและวิเคราะห์ข้อมูลเกี่ยวกับบุคคลบนโซเชียลมีเดียที่มีการเปิดเผยต่อสาธารณะก็ย่อมมีผลกระทบต่อสิทธิในความเป็นส่วนตัวด้วยเช่นกัน[11]

5.2.2 การจำกัดสิทธิในความเป็นส่วนตัว: หลักการทั่วไป

ตามข้อ 17 ของ ICCPR ระบุชัดเจนว่า การแทรกแซงใด ๆ เกี่ยวกับสิทธิความเป็นส่วนตัวจะต้องไม่เป็นไปตามอำเภอใจหรือไม่ชอบด้วยกฎหมาย

คำว่า "ไม่ชอบด้วยกฎหมาย" หมายความว่าจะไม่มีการแทรกแซงใด ๆ ยกเว้นในกรณีที่กฎหมายกำหนด การให้อำนาจแทรกแซงโดยรัฐสามารถเกิดขึ้นได้เพียงบนพื้นฐานของกฎหมายเท่านั้น ซึ่งต้องเป็นไปตามบทบัญญัติ จุดมุ่งหมาย และวัตถุประสงค์ของ ICCPR[12]

---

[10] Manfred Nowak, UN Covenant on Civil and Political Rights. CCPR Commentary (Kehl am Rhein, Engel, 2005), p. 401.

[11] A/HRC/39/29, para. 6.

[12] CCPR General comment No. 16, para. 3.

ส่วนคำว่า "การแทรกแซงโดยพลการ" ยังขยายไปถึงการแทรกแซงที่บัญญัติไว้ภายใต้กฎหมายอีกด้วย การแนะนำแนวคิดเกี่ยวกับความพลการ (arbitrariness) มีจุดมุ่งหมายเพื่อรับประกันว่าแม้การแทรกแซงที่กฎหมายกำหนดไว้ ก็ควรเป็นไปตามบทบัญญัติ จุดมุ่งหมาย และวัตถุประสงค์ของ ICCPR และควรมีเหตุผลในสถานการณ์เฉพาะไม่ว่าในกรณีใด[13]

ข้อ 17 ไม่ได้ระบุเงื่อนไขที่เป็นข้อจำกัดอย่างชัดเจน ซึ่งแตกต่างจากข้อ 19 และข้อบทอื่น ๆ ของ ICCPR อย่างไรก็ดี ภายใต้เงื่อนที่ที่ข้อ 17 ของ ICCPR การแทรกแซงต้องไม่ “โดยพลการหรือไม่ชอบด้วยกฎหมาย” ประกับกับตามคำของกลไกสิทธิมนุษยชนของสหประชาชาติและภูมิภาค รวมถึงคำแนะนำที่พัฒนาโดยผู้เชี่ยวชาญอิสระอื่น ๆ[14] ยืนยันว่า การแทรกแซงสิทธิในความเป็นส่วนตัวจะต้องอยู่ภายใต้เงื่อนไขของหลักความชอบด้วยกฎหมาย (legality) มีเป้าหมายที่ชอบธรรม (legitimate aim) สอดคล้องกับหลักความจำเป็นและความได้สัดส่วน (necessity and proportionality) หรือการทดสอบสามส่วนดังที่กล่าวไว้แล้วในบทก่อน ดังนี้

<u>ความชอบด้วยกฎหมาย</u>

รัฐต้องประกันว่า การแทรกแซงใด ๆ ต่อความเป็นส่วนตัว ครอบครัว เคหสถานหรือการติดต่อสื่อสาร ต้องเป็นไปตามกรอบกฎหมายที่ (ก) เข้าถึงได้อย่างเปิดเผย (ข) ตอบสนองเป้าหมายที่ชอบธรรมอย่างชัดเจน (ค) มีเนื้อหาชัดเจนเพียงพอ ต้องระบุรายละเอียดเกี่ยวกับสถานการณ์ที่แม่นยำซึ่งอนุญาตให้มีการแทรกแซง พร้อมกับกำหนดเงื่อนไขอย่างเฉพาะเจาะจงเกี่ยวกับการดำเนินการแทรกแซง และ (ง) กำหนดมาตรการคุ้มครองที่มีประสิทธิผลเพื่อป้องกันการปฏิบัติที่มิชอบ การตัดสินใจใช้การแทรกแซงดังกล่าวจะต้องกระทำโดยผู้มีอำนาจที่ได้รับมอบหมายภายใต้กฎหมายเท่านั้นและเป็นรายกรณีไป[15]

กฎระเบียบลับและการตีความกฎหมายแบบลับ ถือว่าไม่มีคุณสมบัติเป็น “กฎหมาย”[16] และกฎหมายหรือระเบียบต้องไม่ให้อำนาจวินิจฉัยอย่างเกินขอบเขตกับหน่วยงานฝ่ายบริหาร ไม่ว่าจะเป็นหน่วยงานความมั่นคงและข่าวกรอง กล่าวคือ ในกฎหมายหรือระเบียบนั้นต้องมีตัวบทที่แสดงอย่างชัดเจนถึงขอบเขตและลักษณะการใช้อำนาจวินิจฉัยนั้น (ทั้งในตัวกฎหมายเอง หรือในแนวปฏิบัติที่มีผลบังคับใช้และมีการประกาศใช้)

---

[13] CCPR General Comment No. 16, para. 4.

[14] CCPR General Comment No. 16 ; CCPR General comment No. 31, para. 6; Human Rights Council Resolution No. 34/7. Para 2. ; A/HRC/13/37. Para 16–19. ; A/HRC 27/37 para 21–27 ; A/HRC/48/31, para. 8. ; A/HRC/39/29, para. 10. ; A/HRC/29/32 para 33 ; A/69/397 para 51 ; A/HRC/23/40, para 29. ; A/HRC/27/37, 30 June 2014, para. 22. ; Siracusa Principles ; European Court of Human Rights, Uzun v. Germany, 2 September 2010 and Kruslin v. France, 24 April 1990 ; International Principles on the Application of Human

Rights to Communications Surveillance, available from https://en.necessaryandproportionate.org/text.

[15]CCPR General Comment No. 16, para. 8. ; A/HRC/27/37, 30 June 2014, para. 28.

[16] See CCPR /C/USA/CO/4, para. 22

พร้อมกับแสดงความชอบด้วยเหตุผลที่ชัดเจน เพื่อประกันการเข้าถึงได้ กรอบกฎหมายควรต้องจัดทำขึ้นโดยผ่านการพิจารณาของรัฐสภา แทนที่จะเป็นกฎหมายลูกที่ฝ่ายบริหารเป็นผู้ประกาศใช้[17]

วัตถุประสงค์ที่ชอบธรรม

ข้อ 17 ไม่ได้ระบุรายการของวัตถุประสงค์ที่ชอบธรรม ซึ่งอาจเป็นพื้นฐานของการให้เหตุผลในการแทรกแซงสิทธิความเป็นส่วนตัวไว้อย่างละเอียด อย่างไรก็ตาม การสอดส่องข้อมูลด้วยเหตุผลความมั่นคงแห่งชาติและเพื่อป้องกันลัทธิก่อการร้ายหรืออาชญากรรมอื่น ๆ อาจเป็น “เป้าหมายที่ชอบธรรม” เพราะการก่อการร้ายสามารถทำให้ชุมชนไม่มั่นคง คุกคามการพัฒนาทางสังคมและเศรษฐกิจ ทำลายบูรณภาพแห่งดินแดนของรัฐ และบ่อนทำลายสันติภาพและความมั่นคงระหว่างประเทศ[18] วัตถุประสงค์ที่ชอบธรรม อาจรวมถึงการบริหารงานยุติธรรมทางอาญาหรือการป้องกันอาชญากรรม[19]

อย่างไรก็ดี รัฐต้องประกันว่ามาตรการใด ๆ ที่ใช้ต่อสู้กับการก่อการร้ายเป็นไปตามพันธกรณีภายใต้กฎหมายระหว่างประเทศ โดยเฉพาะอย่างยิ่งกฎหมายสิทธิมนุษยชน กฎหมายผู้ลี้ภัย และกฎหมายมนุษยธรรมระหว่างประเทศ [20] และต้องมีการประเมินระดับของการแทรกแซง เปรียบเทียบกับความจำเป็นของมาตรการเพื่อให้บรรลุวัตถุประสงค์ดังกล่าว กับผลประโยชน์ที่จะเกิดขึ้นจริงจากการปฏิบัติเช่นนั้น[21]

สมัชชาใหญ่แห่งสหประชาชาติ และคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ ได้ตั้งข้อสังเกตว่าในขณะที่ความกังวลเกี่ยวกับความปลอดภัยสาธารณะอาจเป็นเหตุให้มีการเก็บรวบรวมและปกป้องข้อมูลที่ละเอียดอ่อนบางอย่าง รัฐต้องประกันการปฏิบัติตามพันธกรณีของตนภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศอย่างเต็มที่[22]

---

[17] A/HRC/27/37, 30 June 2014, para. 29. ; A/HRC/14/46

[18] A/HRC/20/14, para 21. ; A/69/397, para 33.

[19] A/HRC/17/27 para 84

[20] UN General Assembly, A/RES/69/166, 10 February 2015 ; Human Rights Council, A/HRC/RES/28/16, 1 April 2015 ; UN General Assembly, A/RES/71/199, 25 January 2017 ; Human Rights Council, A/HRC/RES/34/7, 7 April 2017 ; UN General Assembly, A/RES/73/179, 21 January 2019

[21] A/HRC/27/37, 30 June 2014, para. 24.

[22] UN General Assembly, A/RES/68/167, 18 December 2013 ; A/RES/69/166, 10 February 2015 ; Human Rights Council, A/HRC/RES/28/16, 1 April 2015 ; UN General Assembly, A/RES/71/199, 25 January 2017 ; Human Rights Council, A/HRC/RES/34/7, 7 April 2017 ; UN General Assembly, A/RES/73/179, 21 January 2019

จำเป็นและได้สัดส่วน

การทดสอบ “ความจำเป็น” และ “ความจำเป็นในสังคมประชาธิปไตย” เป็นการทดสอบที่สำคัญสำหรับมาตรการใด ๆ ที่ดำเนินการโดยรัฐที่อาจเป็นการละเมิดความเป็นส่วนตัว นอกจากนี้ยังต้องนำมาพิจารณาเมื่อตรวจสอบการละเมิดสิทธิอื่น ๆ ซึ่งการใช้สิทธินั้นขึ้นอยู่กับสิทธิในความเป็นส่วนตัวด้วย[23]

การจำกัดสิทธิจะกระทำได้เท่าที่จำเป็นเพื่อวัตถุประสงค์ที่ชอบธรรม รวมทั้งได้สัดส่วนกับเป้าหมายและเป็นทางเลือกที่ละเมิดสิทธิน้อยที่สุด นอกจากนั้น การจำกัดสิทธิใด ๆ เช่น การแทรกแซงความเป็นส่วนตัวเพื่อเป้าประสงค์ในการคุ้มครองความมั่นคงแห่งชาติ หรือสิทธิที่จะมีชีวิตรอดของบุคคลอื่น จะกระทำได้เมื่อมีการพิสูจน์ให้เห็นว่ามีโอกาสจะบรรลุเป้าหมายดังกล่าว โดยเป็นภาระของรัฐที่จะต้องแสดงให้เห็นว่า การจำกัดสิทธิมีส่วนเชื่อมโยงกับเป้าหมายที่ชอบธรรม นอกจากนั้น การจำกัดสิทธิความเป็นส่วนตัวใด ๆ ต้องไม่กระทบต่อสารัตถะของสิทธินั้น นอกจากนี้ การจำกัดต้องสอดคล้องกับสิทธิมนุษยชนอื่น ๆ รวมทั้งข้อห้ามต่อการเลือกปฏิบัติ การจำกัดซึ่งไม่สอดคล้องกับหลักเกณฑ์เหล่านี้ ย่อมถือเป็นการจำกัดสิทธิที่ไม่ชอบด้วยกฎหมาย และ/หรือเป็นการแทรกแซงสิทธิความเป็นส่วนตัวโดยพลการ[24]

กรณีที่มีวัตถุประสงค์ที่ชอบธรรมและมีมาตรการคุ้มครองสิทธิที่เหมาะสม รัฐอาจสามารถปฏิบัติการสอดส่องข้อมูลในเชิงรุกได้ เพียงแต่รัฐมีภาระต้องพิสูจน์ให้เห็นว่าการแทรกแซงเช่นนั้นมีความจำเป็นและมีสัดส่วนเหมาะสมกับภารกิจที่ต้องการปฏิบัติ ยกตัวอย่าง โครงการสอดส่องในวงกว้าง หรือ “เหวี่ยงแห” แม้จะมีเป้าหมายที่ชอบธรรม และเป็นการปฏิบัติบนพื้นฐานของกฎหมายที่เข้าถึงได้ แต่อาจไม่ได้สัดส่วน และอาจถือว่าเป็นการกระทำโดยพลการ กล่าวอีกนัยหนึ่งคือ การใช้มาตรการที่มีเป้าหมายเพียงเพื่อค้นหาเข็มบางเล่มในกองฟาง จำเป็นต้องมีการประเมินผลกระทบต่อกองฟางอันเนื่องมาจากการใช้มาตรการเหล่านั้น โดยคำนึงถึงอันตรายที่อาจจะเกิดขึ้นด้วย เพื่อตัดสินว่ามาตรการนั้นมีความจำเป็นและมีสัดส่วนเหมาะสมหรือไม่[25]

ปัจจัยหนึ่งที่ต้องคำนึงถึงเพื่อพิจารณาความได้สัดส่วนคือ วิธีการจัดการกับข้อมูลแบบเหวี่ยงแหและผู้ที่จะเข้าถึงข้อมูลหลังจากจัดเก็บแล้ว การอนุญาตให้เก็บข้อมูลเพื่อวัตถุประสงค์ทางกฎหมายอย่างหนึ่ง แต่ในภายหลังมีการนำข้อมูลนั้นไปใช้เพื่อวัตถุประสงค์อย่างอื่น ส่งผลให้มีการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานบังคับใช้กฎหมาย หน่วยงานข่าวกรอง และหน่วยงานของรัฐอื่น ๆ ซึ่งเสี่ยงจะละเมิดข้อ 17 ของ ICCPR เนื่องจากมาตรการสอดส่องข้อมูลที่อาจจำเป็นและได้สัดส่วนเพื่อวัตถุประสงค์ที่ชอบธรรมอย่างหนึ่ง อาจไม่เป็นเช่นนั้นหากนำไปใช้เพื่อวัตถุประสงค์อย่างอื่น ยิ่งหน่วยงานความมั่นคงแห่งชาติและหน่วยงานบังคับใช้กฎหมายสามารถเข้าถึงและใช้ประโยชน์จากข้อมูลของภาคเอกชนได้ง่ายมากขึ้นเท่าไร ยิ่งส่งผลให้หน่วยงานเหล่านั้นมีอิสระในการ

---

[23] A/HRC/40/63. Para 16 – 19. ; A/HRC/40/63, para 32.

[24] A/HRC/27/37, 30 June 2014, para. 23.

[25] A/HRC/27/37, 30 June 2014, para. 25.

แลกเปลี่ยนข้อมูลมากยิ่งขึ้น และเสี่ยงที่จะมีการนำไปใช้เพื่อวัตถุประสงค์อื่น นอกเหนือจากที่กำหนดไว้ตอนที่เก็บข้อมูล ซึ่งจะทำให้มาตรการคุ้มครองข้อมูลแบบดั้งเดิมอ่อนแอลง[26]

อีกตัวอย่างหนึ่งเกี่ยวกับการพิจารณาความจำเป็นและได้สัดส่วน คือ การวินิจฉัยของศาลสิทธิมนุษยชนแห่งยุโรป (European Court of Human Rights) ในคดี Catt v the United Kingdom ซึ่ง Mr. Catt นักเคลื่อนไหวเพื่อสันติภาพซึ่งได้ชุมนุมสาธารณะและถูกตำรวจบันทึกข้อมูลส่วนบุคคลของเขา ทั้งยังระบุว่าเขาเป็นพวกนิยมลัทธิสุดโต่ง Mr. Catt ได้ยื่นคำร้องภายใต้ The UK's Data Protection Act 1998 ขอให้ตำรวจลบข้อมูลที่เกี่ยวข้องกับตัวเขาที่เก็บไว้ในฐานข้อมูลของตำรวจ และที่อยู่ในบันทึกของบุคคลอื่น แต่ตำรวจปฏิเสธที่จะลบให้ คดีนี้ศาลสิทธิมนุษยชนแห่งยุโรปเห็นว่า แม้การรวบรวมข้อมูลส่วนบุคคลเพื่อป้องกันอาชญากรรม (crime) และความไม่สงบ (disorder) เป็นวัตถุประสงค์ที่ชอบด้วยกฎหมายและถูกต้องตามกฎหมาย แต่การเก็บรักษา (retention) ข้อมูลส่วนบุคคลโดยปราศจากการทบทวนตามกำหนดเวลาและนอกเหนือจากข้อจำกัดที่กำหนดไว้นั้นเป็นสิ่งที่ไม่ได้สัดส่วนและไม่จำเป็น ศาลจึงตัดสินว่าตำรวจละเมิดสิทธิในความเป็นส่วนตัวและชีวิตครอบครัวของ Mr. Catt[27]

5.2.3 พันธกรณีของรัฐต่อสิทธิในความเป็นส่วนตัว

ข้อ 2 (1) ของ ICCPR กำหนดให้รัฐต้องเคารพและรับรองสิทธิที่รับรองใน ICCPR สำหรับบุคคลทุกคนภายในอาณาเขตของตนและอยู่ภายใต้เขตอำนาจศาลของตน โดยไม่มีการเลือกปฏิบัติ กล่าวอีกนัยหนึ่งรัฐปฏิบัติตามพันธกรณีเชิงลบของตนโดยไม่รบกวนสิทธิของบุคคล เว้นแต่จะปฏิบัติตามกฎหมาย เพื่อบรรลุผลประโยชน์โดยชอบธรรม และในลักษณะที่จำเป็นและได้สัดส่วนกับการบรรลุผลสำเร็จของผลประโยชน์นั้น[28]

รัฐยังมีพันธะในการคุ้มครองการใช้สิทธิด้วย โดยใช้มาตรการทางกฎหมายและมาตรการอื่น ๆ ที่เพียงพอเพื่อคุ้มครองบุคคลจากการแทรกแซงในความเป็นส่วนตัว ไม่ว่าจะมาจากหน่วยงานของรัฐหรือจากบุคคลธรรมดาหรือนิติบุคคล[29] รวมถึงการคุ้มครองจากการถูกสกัดกั้นการสื่อสารหรือการแฮ็กข้อมูล[30]

สมัชชาใหญ่แห่งสหประชาชาติ และคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ เรียกร้องให้รัฐ[31]

- ให้ความเคารพและปกป้องสิทธิความเป็นส่วนตัว รวมถึงในบริบทของการสื่อสารทางดิจิทัล

---

[26] A/HRC/14/46, annex, practice 23. ; A/HRC/27/37, 30 June 2557, para 27.

[27] European Court of Human Rights, Application No 43514/15, 24 January 2019

[28] CCPR General Comment No. 31, paras. 6., 10. ; A/HRC/27/37, 30 June 2014, para. 36.

[29] A/HRC/39/29, para. 23. ; CCPR General Comments No. 16, paras. 1 and 9 ; CCPR General Comment No. 31 ; UNGPs

[30] A/HRC/39/29, 3 August 2018, para. 25.

[31] A/RES/68/167, 18 December 2013, para. 5. ; A/RES/69/166, 10 February 2015, para. 4. ; A/RES/73/179, 21 January 2019, para. 6.

- ดำเนินมาตรการเพื่อยุติการละเมิดสิทธิเหล่านั้น และสร้างเงื่อนไขในการป้องกันการละเมิดดังกล่าว รวมถึงการประกันว่ากฎหมายระดับชาติที่เกี่ยวข้องปฏิบัติตามพันธกรณีภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ
- ทบทวนขั้นตอน แนวปฏิบัติ และกฎหมายเกี่ยวกับการสอดส่องการสื่อสาร การสกัดกั้น และการรวบรวมข้อมูลส่วนบุคคล รวมถึงการสอดส่องในวงกว้าง เพื่อรักษาสิทธิความเป็นส่วนตัว โดยปฏิบัติตามพันธกรณีทั้งหมดภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศอย่างเต็มที่และมีประสิทธิภาพ
- สร้างหรือคงไว้ซึ่งกลไกการกำกับดูแลภายในประเทศทางตุลาการ บริหาร และ/หรือ รัฐสภา ที่เป็นอิสระ มีประสิทธิภาพ มีทรัพยากรเพียงพอ และเป็นกลาง ที่สามารถประกันความโปร่งใส และความรับผิดชอบสำหรับการสอดส่องการสื่อสารของรัฐ การสกัดกั้น และการรวบรวมข้อมูลส่วนบุคคล ตามความเหมาะสม
- จัดให้บุคคลที่ถูกละเมิดสิทธิในความเป็นส่วนตัวจากการสอดส่องโดยมิชอบด้วยกฎหมายหรือตามอำเภอใจ สามารถเข้าถึงการเยียวยาที่มีประสิทธิภาพ ซึ่งสอดคล้องกับพันธกรณีด้านสิทธิมนุษยชนระหว่างประเทศ[32]
- พัฒนาหรือคงไว้ซึ่งมาตรการป้องกันและการเยียวยาสำหรับการละเมิดและการละเมิดเกี่ยวกับสิทธิในความเป็นส่วนตัวในยุคดิจิทัลที่อาจส่งผลกระทบต่อบุคคลทั้งหมด รวมทั้งในกรณีที่มีผลกระทบเฉพาะสำหรับผู้หญิง เด็กและบุคคลในสถานการณ์ที่เปราะบางหรือกลุ่มคนชายขอบ[33]
- พิจารณามาตรการที่เหมาะสมที่จะช่วยให้องค์กรธุรกิจสามารถนำมาตรการความโปร่งใสโดยสมัครใจที่เพียงพอเกี่ยวกับคำขอของหน่วยงานของรัฐในการเข้าถึงข้อมูลและข้อมูลส่วนตัวของผู้ใช้[34]
- พิจารณานำและดำเนินการตามกฎหมายคุ้มครองข้อมูล กฎระเบียบ และนโยบาย รวมถึงข้อมูลการสื่อสารดิจิทัลที่สอดคล้องกับพันธกรณีด้านสิทธิมนุษยชนระหว่างประเทศ ซึ่งอาจรวมถึงการจัดตั้งหน่วยงานอิสระระดับชาติที่มีอำนาจและทรัพยากรในการตรวจสอบแนวทางปฏิบัติด้านความเป็นส่วนตัวของข้อมูล สอบสวนการละเมิดและ

[32] A/RES/69/166, 10 February 2015, para. 4. ; A/RES/71/199, 25 January 2017, para. 5. ; A/HRC/RES/34/7, 7 April 2017, para. 5.

[33] A/RES/71/199, 25 January 2017, para. 5. ; A/RES/73/179, 21 January 2019, para. 6. ; A/HRC/RES/34/7, 7 April 2017, para. 5.

[34] A/RES/71/199, 25 January 2017, para. 5. ; A/HRC/RES/34/7, 7 April 2017, para. 5.

ปฏิบัติที่มิชอบ และรับการติดต่อจากบุคคลและองค์กร และเพื่อให้การเยียวยาที่เหมาะสม[35]

- ให้คำแนะนำที่มีประสิทธิภาพแก่ผู้ประกอบการธุรกิจเกี่ยวกับวิธีการเคารพสิทธิมนุษยชน โดยให้คำแนะนำเกี่ยวกับวิธีการที่เหมาะสม ซึ่งรวมถึงการตรวจสอบวิเคราะห์สถานะสิทธิมนุษยชน และการพิจารณาประเด็นเรื่องเพศ ความเปราะบาง และ/หรือการทำให้เป็นชายขอบอย่างมีประสิทธิผล[36]

5.2.4 ความรับผิดชอบขององค์กรธุรกิจ

สมัชชาใหญ่แห่งสหประชาชาติ และคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ ยืนยันว่าผู้ประกอบการธุรกิจมีความรับผิดชอบในการเคารพสิทธิมนุษยชนตามที่กำหนดในกฎหมายที่บังคับใช้ หลักการและมาตรฐานสากล[37] โดยเฉพาะตามหลักการชี้แนะเรื่องสิทธิมนุษยชนสำหรับธุรกิจ : ตามกรอบงานองค์การสหประชาชาติในการคุ้มครอง เคารพ และเยียวยา (UNGPs)[38] โดยดำเนินการ อาทิ

- ดำเนินการป้องกันทางการบริหาร ทางเทคนิค และทางกายภาพ เพื่อประกันว่าข้อมูลได้รับการประมวลผลอย่างถูกต้องตามกฎหมาย และประกันว่าการประมวลผลดังกล่าวจำกัดเฉพาะสิ่งที่จำเป็นที่เกี่ยวข้องกับวัตถุประสงค์ของการประมวลผลและความชอบธรรมของวัตถุประสงค์ดังกล่าว เช่นเดียวกับ ต้องประกันความถูกต้อง ความสมบูรณ์ และความลับของการประมวลผล[39]
- ประกันการเคารพในสิทธิความเป็นส่วนตัวและสิทธิมนุษยชนระหว่างประเทศอื่น ๆ โดยการรวมสิทธิดังกล่าวเข้าในการออกแบบ การดำเนินงาน การประเมินและข้อบังคับของเทคโนโลยีการตัดสินใจอัตโนมัติและการเรียนรู้ด้วยเครื่อง (automated decision-making and machine-learning technologies) และจัดให้มีการเยียวยาการละเมิดสิทธิมนุษยชนที่เกิดขึ้น[40]

---

[35] A/RES/73/179, 21 January 2019, para. 6.

[36] UN General Assembly, A/RES/73/179, 21 January 2019, para. 6.

[37] A/RES/71/199, 25 January 2017

[38] A/RES/69/166, 10 February 2015 ; A/HRC/RES/28/16, 1 April 2015 ; A/RES/71/199, 25 January 2017, para. 6. ; A/HRC/RES/34/7, 7 April 2017, para. 8. ; A/RES/73/179, 21 January 2019, para. 7. ; A/HRC/39/29, 3 August 2018, para 62.

[39] A/RES/73/179, 21 January 2019, para. 7.

[40] A/RES/73/179, 21 January 2019, para. 7.

- ส่งเสริมให้องค์กรธุรกิจทำงานเพื่อเปิดใช้งานโซลูชันทางเทคนิคในการรักษาความปลอดภัยและปกป้องความลับของการสื่อสารดิจิทัล จากการแทรกแซงความเป็นส่วนตัวโดยพลการหรือไม่ชอบด้วยกฎหมาย[41] ซึ่งอาจรวมถึงมาตรการสำหรับการเข้ารหัสและการไม่เปิดเผยชื่อ และเรียกร้องให้รัฐไม่เข้าไปยุ่งเกี่ยวกับการใช้โซลูชั่นทางเทคนิคดังกล่าว ทั้งนี้ ข้อจำกัดใด ๆ ต้องปฏิบัติตามพันธกรณีของรัฐภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ[42]

การปฏิบัติตามความรับผิดชอบในการเคารพสิทธิมนุษยชนนั้น กำหนดให้ผู้ประกอบการธุรกิจ (ก) หลีกเลี่ยงการก่อให้เกิดผลกระทบทางลบผ่านกิจกรรมของตนเอง (ข) หลีกเลี่ยงการมีส่วนทำให้เกิดผลกระทบผ่านกิจกรรมของตนเอง ไม่ว่าโดยตรงหรือผ่านหน่วยงานภายนอก (รัฐบาล ธุรกิจ หรืออื่น ๆ) และ (ค) พยายามป้องกันหรือบรรเทาผลกระทบด้านสิทธิมนุษยชนที่ไม่พึงประสงค์ซึ่งเชื่อมโยงโดยตรงกับการดำเนินงาน ผลิตภัณฑ์หรือบริการโดยความสัมพันธ์ทางธุรกิจของตน แม้ว่าจะไม่ได้มีส่วนทำให้เกิดผลกระทบเหล่านั้นก็ตาม[43] เช่น บริษัทที่ให้ข้อมูลเกี่ยวกับผู้ใช้แก่รัฐบาลที่ใช้ข้อมูลดังกล่าวเพื่อติดตามและดำเนินคดีกับผู้ไม่เห็นด้วยทางการเมืองจะถือว่ามีส่วนทำให้เกิดการละเมิดสิทธิมนุษยชนดังกล่าว บริษัทที่ผลิตและจำหน่ายเทคโนโลยีที่ใช้สำหรับการบุกรุกโดยมิชอบด้วยกฎหมายหรือโดยพลการก็จะมีส่วนทำให้เกิดผลกระทบด้านสิทธิมนุษยชนในทางลบด้วยเช่นกัน[44]

หากมีข้อเรียกร้องที่ขัดแย้งกันระหว่างการเคารพกฎหมายสิทธิมนุษยชนระหว่างประเทศและพันธกรณีภายใต้กฎหมายภายในประเทศ บริษัทต่าง ๆ ควรพยายามให้ความเคารพต่อกฎหมายสิทธิมนุษยชนระหว่างประเทศให้มากที่สุดเท่าที่จะเป็นไปได้ และบรรเทาผลกระทบด้านลบต่าง ๆ ให้มากที่สุด ตัวอย่างเช่น โดยการตีความข้อเรียกร้องของรัฐบาลให้แคบที่สุด[45]

ตามหลักการ UNGPs ทุกบริษัทมีหน้าที่ในการตรวจสอบด้านสิทธิมนุษยชนอย่างรอบด้าน (HRDD) เพื่อระบุและแก้ไขผลกระทบด้านสิทธิมนุษยชนจากกิจกรรมของตน บริษัทจำเป็นต้องประเมินความเสี่ยงด้านความเป็นส่วนตัวที่เกี่ยวข้องกับคำขอข้อมูลของรัฐที่อาจเกิดขึ้น รวมถึงสภาพแวดล้อมทางกฎหมายและสถาบันของรัฐที่เกี่ยวข้อง บริษัทต้องจัดให้มีกระบวนการและการป้องกันที่เพียงพอเพื่อป้องกันและบรรเทาผลกระทบต่อความเป็นส่วนตัวที่อาจเกิดขึ้น รวมถึงต้องดำเนินการประเมินผลกระทบด้านสิทธิมนุษยชน (Human

---

[41] A/RES/73/179, 21 January 2019, para. 8.

[42] A/RES/71/199, 25 January 2017, para. 7. ; A/HRC/RES/34/7, 7 April 2017, para. 9.

[43] Guiding Principle 13. ; OHCHR, “The corporate responsibility to respect human rights: an interpretive guide” (2012).

[44] A/HRC/39/29, 3 August 2018, para. 43.

[45] A/HRC/39/29, 3 August 2018, para. 44. ; A/HRC/27/37, 30 June 2014, para. 45.

rights impact assessments) ซึ่งเป็นส่วนหนึ่งของการนำข้อกำหนดในการให้บริการและการออกแบบและทางเลือกทางวิศวกรรมมาใช้ ซึ่งมีผลกับความปลอดภัยและความเป็นส่วนตัว[46]

ทั้งนี้ สำหรับแนวทางเกี่ยวกับการปรับใช้หลักการ UNGP ในบริบทของภาคธุรกิจด้านเทคโนโลยีนั้น อาจดูเพิ่มเติมได้จากเอกสารดังต่อไปนี้

- The UN Guiding Principles in the Age of Technology ภายใต้โครงการ B-Tech ของสำนักงานข้างหลวงใหญ่สิทธิมนุษยชนแห่งสหประชาชาติ (UNOHCHR)[47]
- ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights ของคณะกรรมาธิการยุโรป (European Commission) ซึ่งพัฒนาโดย Shift and Institute for Human Rights and Business (IHRB) โดยแนวทางดังกล่าวใช้หลักการ UNGP มาปรับให้เข้ากับบริบทเฉพาะของภาคส่วนเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)[48]
- the Practical Application of the UNGPs in the Technology Sector โดย Global Network Initiative ซึ่งจัดทำขึ้นเพื่อส่งให้ข้าหลวงใหญ่สิทธิมนุษยชนแห่งสหประชาชาติเกี่ยวกับการประยุกต์ใช้ UNGPs ในภาคเทคโนโลยี[49]

<u>การเยียวยาเมื่อมีการละเมิดความเป็นส่วนตัว</u>

ผู้ที่ได้รับผลกระทบจากการละเมิดความเป็นส่วนตัวโดยรัฐและ/หรือองค์กรธุรกิจ ต้องสามารถเข้าถึงการเยียวยาที่มีประสิทธิผล รัฐไม่เพียงแต่มีภาระหน้าที่ในการตรวจสอบความรับผิดชอบและการเยียวยาสำหรับการละเมิดสิทธิมนุษยชนที่กระทำโดยรัฐเท่านั้น แต่ยังต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อประกันว่าเหยื่อที่ถูกละเมิดสิทธิมนุษยชนที่เกี่ยวข้องกับธุรกิจ สามารถเข้าถึงวิธีการแก้ไขที่มีประสิทธิผล[50] ทั้งนี้ขึ้นอยู่กับลักษณะของกรณีหรือสถานการณ์ที่เฉพาะเจาะจง ผู้ที่ได้รับผลกระทบควรสามารถได้รับการเยียวยาโดยใช้กลไกการร้องทุกข์ที่เป็นไปตามกระบวนการยุติธรรมหรือที่ไม่ใช่กระบวนการยุติธรรม[51]

---

[46] A/HRC/32/38, para 11. ;A/HRC/39/29, 3 August 2018, para. 46.

[47] OHCHR, The UN Guiding Principles in the Age of Technology : A B-Tech Foundational Paper, 2020, https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf ; B-Tech Project, https://www.ohchr.org/en/business-and-human-rights/b-tech-project

[48] Shift and Institute for Human Rights and Business (IHRB), ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights , 2011, https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf

[49] Global Network Initiative (GNI), https://globalnetworkinitiative.org/wp-content/uploads/2022/03/GNI-OHCHR-UNGPs-ICTs.pdf

[50] เสาหลักที่ 3 ของ UNGPs

[51] A/HRC/32/19, Corr. 1 and Add. 1 and A/HRC/38/20 and Add. 1

บุคคลที่ได้รับผลกระทบควรสามารถยื่นคำร้องต่อกลไกอิสระที่สามารถทำการตรวจสอบอย่างละเอียดถี่ถ้วนและเป็นกลาง ด้วยการเข้าถึงเนื้อหาที่เกี่ยวข้องทั้งหมดและการรับประกันตามกระบวนการที่เหมาะสม กลไกความรับผิดชอบต้องมีอำนาจสั่งการเยียวยาที่มีผลผูกพัน[52] และการทำให้การละเมิดอย่างต่อเนื่องยุติลงถือเป็นองค์ประกอบสำคัญของสิทธิที่จะได้รับการเยียวยาอย่างเป็นผล[53]

ภายใต้หลักการ UNGPs องค์กรธุรกิจที่พิจารณาว่าตนได้ก่อให้เกิดหรือมีส่วนในผลกระทบด้านสิทธิมนุษยชน ควรจัดเตรียมหรือให้ความร่วมมือในการแก้ไขผลกระทบด้านสิทธิมนุษยชนที่อาจก่อให้เกิดหรือมีส่วนร่วมผ่านกระบวนการที่ชอบธรรม[54] ส่วนในกรณีที่องค์กรธุรกิจไม่ได้ก่อให้เกิดหรือมีส่วนทำให้เกิดผลกระทบในทางลบ เพียงแต่เข้าไปเกี่ยวข้องเพราะถูกเชื่อมโยงโดยตรงกับการดำเนินการผลิต ผลิตภัณฑ์ หรือบริการของธุรกิจที่มีความสัมพันธ์ด้วย การดำเนินการที่เหมาะสมจะมีรายละเอียดอยู่ในหลักการ UNGPs ข้อ 19 ซึ่งอาจรวมถึงการใช้ประโยชน์ใด ๆ ที่องค์กรอาจมีเหนือพันธมิตรทางธุรกิจหรือลูกค้าเพื่อให้มีการแก้ไข[55]

ผู้ได้รับผลกระทบอาจต้องเผชิญกับความท้าทายใหม่ ๆ ที่เพิ่มมากขึ้นในบริบทของการตัดสินใจโดยใช้อัลกอริทึม ซึ่งอาจไม่สามารถเข้าถึงข้อมูลนำเข้า (input) หรือโต้แย้งการค้นพบที่อัลกอริทึมได้มาเองหรือการใช้การค้นพบดังกล่าวในการตัดสินใจ รัฐและองค์กรธุรกิจร่วมกับผู้มีส่วนได้ส่วนเสียอื่น ๆ ควรพิจารณากลไกที่เป็นไปได้ในการแก้ไขปัญหา เช่น การสร้างหน่วยงานตรวจสอบของผู้เชี่ยวชาญ (expert auditing bodies) ที่มีทรัพยากรเหมาะสม เป็นต้น[56]

5.3 สิทธิในความเป็นส่วนตัว และการสอดส่องการสื่อสารทางดิจิทัล

ความก้าวหน้าทางเทคโนโลยีส่งผลให้รัฐสามารถสอดส่องข้อมูลได้อย่างไม่มีข้อจำกัดในแง่ของขอบเขตและระยะเวลา ต้นทุนด้านเทคโนโลยีและที่จัดเก็บข้อมูลที่ลดลงทำให้อุปสรรคด้านการเงินหรือในทางปฏิบัติของการสอดส่องข้อมูลหมดไป ในปัจจุบันรัฐมีศักยภาพเพิ่มขึ้นมากในการสอดส่องข้อมูลหลายครั้งในเวลาเดียวกัน และเป็นไปอย่างกว้างขวางมากกว่าที่เคยเป็น[57]

---

[52] A/69/397, 23 September 2014, para 61.

[53] A/HRC/27/37, 30 June 2557, para 39.

[54]UNGPs Principle 22.

[55] UNGP Principle 19 และคำอธิบายประกอบ

[56] A/HRC/39/29, 3 August 2018, para 55.

[57] A/HRC/27/37, 30 June 2014, para. 2.

5.3.1 ความเข้าใจทั่วไปเกี่ยวกับการสอดส่องการสื่อสาร

1) ระดับของการสอดส่องการสื่อสาร

การสอดส่องการสื่อสาร อาจแบ่งออกเป็น 2 ระดับ ได้แก่

- ระดับแรก การเข้าถึงข้อมูลแวดล้อม (ข้อมูลจราจรคอมพิวเตอร์) ซึ่งเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ โดยแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น หรืออาจเรียกว่า “เมทาดาทา” (metadata) หรือ “ข้อมูลเกี่ยวกับข้อมูล” (data about data)
- ระดับที่สอง การเข้าถึงข้อมูลเนื้อหา (content) คือ เนื้อหาสาระของการสื่อสารของประชาชนสื่อต่าง ๆ ผู้สอดส่องสามารถที่จะทราบเนื้อหาของการสนทนาได้ ดังนั้นจะเห็นได้ว่า การสอดส่อง โดยสภาพเป็นการล่วงล้ำ สิทธิส่วนบุคคลในข้อมูลและการสื่อสารระหว่างบุคคล[58]

วิธีการของการสอดส่อง[59]

ก. การเข้าถึงข้อมูลการสื่อสารโดยขอความร่วมจากผู้ให้บริการ

รัฐอาจแสวงหาการเข้าถึงข้อมูลการสื่อสารที่ถือครองโดยผู้ให้บริการเอกชน รัฐสามารถใช้ข้อมูลการสื่อสารที่รวบรวมโดยผู้ให้บริการ เพื่อจัดทำโปรไฟล์ที่ครอบคลุมของบุคคลที่เกี่ยวข้อง รวมทั้งสภาพทางการแพทย์ มุมมองทางการเมืองและศาสนา ปฏิสัมพันธ์และความสนใจ ที่ตั้ง อัตลักษณ์ และกิจกรรมต่าง ๆ[60]

ข. การจำกัดการเข้ารหัส และการไม่เปิดเผยตัวตน (Encryption, Anonymity)

การเข้ารหัส คือ กระบวนการทางคณิตศาสตร์ในการแปลงข้อความ ข้อมูลสารสนเทศ หรือข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้โดยคนอื่น ยกเว้นผู้รับที่กำหนดไว้ โดยปกป้องความลับและความสมบูรณ์ของเนื้อหาจากการเข้าถึงหรือการจัดการของบุคคลที่สาม[61]

ในสภาพแวดล้อมที่มีการเซ็นเซอร์อย่างแพร่หลาย บุคคลอาจถูกบังคับให้พึ่งพาการเข้ารหัสและการไม่เปิดเผยตัวตน เพื่อหลีกเลี่ยงข้อจำกัดและใช้สิทธิ์ในการแสวงหา รับ และให้ข้อมูล นอกจากนี้ ในระบอบที่

---

[58] คณาธิป ทองรวีวงศ์, ย้อนเหตุการณ์ “สอดส่องการสื่อสาร” ปี 2558 และแนวโน้มความเป็นส่วนตัวออนไลน์ปี 2559

[59] A/HRC/41/35

[60] A/HRC/23/40, para 42.

[61] A/HRC/29/32, 22 May 2015, para. 7.

คุกคาม ฝ่ายค้าน นักข่าว นักปกป้องสิทธิมนุษยชน และนักเคลื่อนไหว อาจพึ่งพาการเชื่อมต่อ VPN หรือการใช้ Tor หรือพร็อกซีเซิร์ฟเวอร์ (Proxy Server) รวมกับการเข้ารหัส เพื่อที่จะสามารถเข้าถึงหรือแบ่งปันข้อมูลในสภาพแวดล้อมที่ปลอดภัยได้[62]

การจำกัดการไม่เปิดเผยตัวตน สามารถทำได้โดยการกำหนดให้บุคคลต้องระบุตัวตนเมื่อใช้บริการอินเทอร์เน็ตคาเฟ่ หรือบันทึกธุรกรรมของตนบนคอมพิวเตอร์สาธารณะ การลงทะเบียนเมื่อซื้อซิมการ์ดหรืออุปกรณ์โทรศัพท์มือถือ การลงทะเบียนเพื่อเข้าชมเว็บไซต์สำคัญบางแห่ง หรือแสดงความคิดเห็นในเว็บไซต์สื่อหรือบล็อก ข้อจำกัดในการไม่เปิดเผยชื่ออาจช่วยอำนวยความสะดวกในการสอดส่องการสื่อสารของรัฐ[63]

อย่างไรก็ดี ปัญหาของการเข้ารหัสและการไม่เปิดเผยเป็นประเด็นที่ถกเถียงกัน ระหว่างการปกป้องเสรีภาพในการแสดงออกและความเป็นส่วนตัวกับการจัดการกับอาชญากรรมทางออนไลน์ ซึ่งเกี่ยวพันกับมิติการเยียวยาด้วยบางส่วน เช่น การไม่เปิดเผยตัวตนทางออนไลน์อาจนำไปสู่การล่วงละเมิดและกลั่นแกล้งผู้อื่น รวมถึงการก่ออาชญากรรมทางอินเทอร์เน็ต

กลไกสิทธิมนุษยชนของสหประชาชาติแนะนำให้รัฐปกป้องการเข้ารหัสและการไม่เปิดเผยตัวตน[64] โดยคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติได้เรียกร้องให้รัฐต่าง ๆ ไม่แทรกแซงการใช้เครื่องมือเข้ารหัสและการไม่เปิดเผยตัวตน และการจำกัดควรเป็นไปตามกฎหมายสิทธิมนุษยชนระหว่างประเทศ[65] เช่นเดียวกับผู้รายงานพิเศษฯ ได้เรียกร้องให้รัฐประกันว่าบุคคลจะสามารถแสดงความเห็นทางอินเทอร์เน็ตโดยไม่เปิดเผยตัวตน และหลีกเลี่ยงการนำระบบการลงทะเบียนด้วยชื่อจริงมาใช้ ข้อยกเว้นสามารถทำได้ในสถานการณ์บางอย่างเท่านั้น เช่น หากเป็นไปเพื่อประโยชน์ในการบริหารงานยุติธรรมทางอาญา หรือเพื่อป้องกันอาชญากรรม ถึงอย่างนั้น ผู้รายงานพิเศษย้ำว่ามาตรการควบคุมที่นำมาใช้จะต้องสอดคล้องกับกรอบสิทธิมนุษยชนระหว่างประเทศ โดยมีมาตรการป้องกันการใช้อำนาจอย่างมิชอบอย่างเพียงพอ เช่น การประกันว่ามาตรการจำกัดสิทธิความเป็นส่วนตัวใด ๆ ที่นำมาใช้โดยหน่วยงานของรัฐต้องมีกฎหมายรองรับอย่างชัดเจน และต้องสอดคล้องกับหลักความจำเป็นและการมีสัดส่วนที่เหมาะสม[66]

---

[62] A/HRC/29/32, para 23.

[63] A/HRC/23/40, para 48.

[64] A/HRC/17/27, p.22.

[65] Human Rights Council Resolution 38/7, para. 9

[66] A/HRC/17/27, 16 May 2011, para 84.

ค. การแฮ็ก (hacking)

การแทรกแซงคอมพิวเตอร์ (Computer interference) โดยเทคโนโลยีการสอดส่องอาจทำให้ผู้บุกรุกสามารถเข้าถึงคอมพิวเตอร์หรือเครือข่ายของแต่ละบุคคลได้ โดยเฉพาะการใช้มัลแวร์ ซึ่งสามารถบันทึกการสนทนาทางวิดีโอทางอินเทอร์เน็ต อีเมล และการสื่อสารอื่น ๆ รวมถึงการบันทึกการกดแป้นพิมพ์ ส่งข้อมูลกลับไปยังเซิร์ฟเวอร์ การแฮ็กประเภทนี้ช่วยให้สามารถสกัดกั้นและรวบรวมการสื่อสารและข้อมูลทุกประเภทโดยไม่จำกัดเฉพาะบุคคล ไม่ว่าจะเข้ารหัสหรือไม่ก็ตาม และยังอนุญาตให้เข้าถึงอุปกรณ์ส่วนตัวและข้อมูลที่เก็บไว้ในอุปกรณ์จากระยะไกลและเป็นความลับได้ ทำให้สามารถดำเนินการสอดส่องแบบเรียลไทม์และจัดการข้อมูลบนอุปกรณ์ดังกล่าว[67]

ตัวอย่างที่ชัดเจนคือ สปายแวร์ Pegasus ของกลุ่ม NSO ซึ่งมักถูกนำมาใช้กับเป้าหมาย นักข่าว นักการเมือง ผู้สอบสวนขององค์การสหประชาชาติ ผู้สนับสนุนสิทธิมนุษยชน และคนอื่น ๆ สปายแวร์ Pegasus ทำให้สามารถตรวจสอบเป้าหมายได้จากระยะไกล รายงานของ Citizen Lab ที่เผยแพร่เมื่อเดือนพฤศจิกายน 2561 ระบุว่ามีการใช้ซอฟต์แวร์ Pegasus เป็นเครื่องมือเฝ้าระวังโดยกำหนดเป้าหมายไปยังบุคคลใน 45 ประเทศ รวมถึงไทย[68]

ง. การสอดส่องเครือข่าย (Network surveillance)

เป็นการใช้เทคโนโลยีบางอย่างทำงานบนเครือข่ายเพื่อเปิดใช้งานการสอดส่องเป้าหมาย เช่น การติดตั้งอุปกรณ์บนเครือข่ายโทรคมนาคมที่เปิดใช้งานการสกัดกั้นการสื่อสาร

การติดตามสื่อสังคมออนไลน์ รัฐมีความสามารถในการตรวจสอบกิจกรรมบนเว็บไซต์เครือข่ายสังคม บล็อกและสื่อต่าง ๆ เพื่อทำแผนที่การเชื่อมต่อและความสัมพันธ์ ความคิดเห็น หรือแม้แต่สถานที่[69]

จ. การจดจำใบหน้า (Facial recognition)

เทคโนโลยีการจดจำใบหน้าถูกนำมาใช้จับภาพและตรวจจับลักษณะใบหน้าของบุคคล และอาจนำไปสู่การสร้างโปรไฟล์ของบุคคลตามเชื้อชาติ เชื้อชาติ ชาติกำเนิด เพศ และลักษณะอื่น ๆ ซึ่งมักเป็นพื้นฐานสำหรับการเลือกปฏิบัติที่ผิดกฎหมาย

---

[67] A/HRC/38/35/Add.1

[68] Bill Marczak and others, “Hide and seek: tracking NSO Group’s Pegasus spyware to operations in 45 countries”, Citizen Lab, 18 September 2018.

[69] A/HRC/23/40, para 40.

ฉ. International Mobile Subscriber Identity catchers

เป็นเทคโนโลยีที่สกัดกั้นการสื่อสารและข้อมูลตำแหน่งที่ถูกส่งโดยอุปกรณ์สื่อสารส่วนบุคคล ซึ่งสามารถติดตั้งในสถานที่ชั่วคราว (เช่น ที่ประท้วงหรือเดินขบวน) หรือถาวร (เช่น ที่สนามบินหรือจุดผ่านแดนอื่น ๆ) เครื่องดักจับเหล่านี้เลียนแบบเสาโทรศัพท์มือถือโดยส่งและตอบสนองต่อสัญญาณโทรศัพท์มือถือเพื่อแยกหมายเลข SIM การ์ดเฉพาะของโทรศัพท์มือถือทั้งหมดภายในพื้นที่ที่กำหนด[70]

ช. Deep Packet Inspection

ช่วยให้สามารถตรวจสอบ วิเคราะห์ และเปลี่ยนเส้นทางการรับส่งข้อมูลผ่านการสื่อสารและเครือข่ายอินเทอร์เน็ต นอกจากนี้ยังสามารถใช้เพื่อเปลี่ยนเส้นทางผู้ใช้ไปยังไซต์ที่ติดมัลแวร์และบล็อกไม่ให้เข้าถึงบางเว็บไซต์

2) รูปแบบของการสอดส่องการสื่อสาร

โดยทั่วไปรูปแบบของการสอดส่องการสื่อสารอาจแบ่งเป็น 2 รูปแบบหลัก คือ การสอดส่องแบบกำหนดเป้าหมาย (Targeted surveillance) และการสอดส่องในวงกว้าง (Mass surveillance) ซึ่งความแตกต่างระหว่างการสอดส่องทั้งสองแบบมีความสำคัญในด้านการกำกับดูแล[71]

ก. การสอดส่องแบบกำหนดเป้าหมาย

การสอดส่องแบบกำหนดเป้าหมายมุ่งเน้นไปที่บุคคล กลุ่มบุคคล หรือภูมิภาค ซึ่งโดยทั่วไปอาจยอมรับได้ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ ซึ่งในด้านเทคนิควิธี รัฐอาจดำเนินการได้ในหลายรูปแบบ รวมถึงการใช้ International Mobile Subscriber Identity catchers[72]

นอกจากนี้ รัฐอาจใช้ซอฟต์แวร์ที่สามารถแทรกซึมเข้าไปในคอมพิวเตอร์ โทรศัพท์มือถือ หรืออุปกรณ์ดิจิทัลอื่น ๆ ของบุคคลอีกด้วย ซอฟต์แวร์เหล่านี้รวมถึงที่เรียกว่า "โทรจัน" (หรือที่เรียกว่าสปายแวร์หรือมัลแวร์) สามารถใช้เพื่อเปิดไมโครโฟนหรือกล้องของอุปกรณ์ เพื่อติดตามกิจกรรมที่ดำเนินการบนอุปกรณ์และเพื่อเข้าถึง แก้ไข หรือ ลบข้อมูลใด ๆ ที่เก็บไว้ในอุปกรณ์ ซอฟต์แวร์ดังกล่าวทำให้รัฐสามารถควบคุมอุปกรณ์ที่ถูกแทรกซึมได้อย่างสมบูรณ์ และแทบจะตรวจไม่พบ[73]

---

[70] A/HRC/23/40, para 35.

[71] A/HRC/23/40

[72] A/HRC/23/40, para 35.

[73] Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixi Hawtin, and Natalia Torres, Global Survey on Internet Privacy and Freedom of Expression, UNESCO Series on Internet Freedom (2012), p. 41.

ข. การสอดส่องในวงกว้าง (Mass surveillance)

การสอดส่องในวงกว้างมุ่งเน้นไปที่การรวบรวมข้อมูลทั้งหมดที่เป็นไปได้จากอินเทอร์เน็ต ซึ่งเป็นการปฏิบัติแบบไม่เลือก ซึ่งมีแนวโน้มว่าจะละเมิดข้อ 17 ของ ICCPR

บางรัฐมีการบังคับให้เก็บรักษาข้อมูล ทำให้มีข้อมูลการสื่อสารจำนวนมหาศาล ซึ่งสามารถนำมาคัดกรองและวิเคราะห์ได้ในภายหลัง โดยใช้เทคโนโลยีที่เรียกว่า deep-packet inspection เพื่อตรวจค้นข้อมูลที่ส่งผ่านอินเทอร์เน็ต เพื่อกรองและถอดรหัสข้อมูลทุกประการที่เกี่ยวข้องกับการใช้งานอินเทอร์เน็ต ซึ่งทำให้รัฐได้ข้อมูลลึกกว่าแค่ข้อมูลการเข้าเยี่ยมชมเว็บไซต์[74]

บางรัฐใช้การติดตามสื่อสังคมออนไลน์ ประกอบกับการใช้อัลกอริธึม "การทำเหมืองข้อมูล" แบบอัตโนมัติ เพื่อดึงข้อมูลจราจรการสื่อสารทั้งมวลโดยไร้ขีดจำกัด ด้วยการวางสายใยแก้วนำแสง (fiber-optic cables) ผ่านสิ่งที่ซึ่งการสื่อสารแบบดิจิทัลส่วนใหญ่เดินทาง รัฐที่เกี่ยวข้องจึงสามารถทำการสอดส่องเนื้อหาและข้อมูลเมตา (metadata) ของการสื่อสารได้เป็นจำนวนมาก ทำให้หน่วยงานด้านข่าวกรองและหน่วยงานบังคับใช้กฎหมายมีโอกาสติดตามและบันทึกไม่เพียงแต่การสื่อสารของประชาชนของตนเองเท่านั้น แต่ยังรวมถึงการสื่อสารของบุคคลที่อยู่ในรัฐอื่นด้วย ศักยภาพนี้มักจะเสริมด้วยกฎหมายว่าด้วยการเก็บรักษาข้อมูลเชิงบังคับ การใช้ซอฟต์แวร์สแกน การทำโปรไฟล์ และเงื่อนไขการค้นหาเฉพาะที่ช่วยให้หน่วยงานที่เกี่ยวข้องสามารถกรองข้อมูลที่เก็บไว้จำนวนมากเพื่อระบุรูปแบบของการสื่อสารระหว่างบุคคลและองค์กร อัลกอริธึมการขุดเหมืองข้อมูลอัตโนมัติจะเชื่อมโยงชื่อที่ใช้ระบุทั่วไป ตำแหน่งที่ตั้ง หมายเลข และที่อยู่อินเทอร์เน็ตโปรโตคอล (IP address) และค้นหาความสัมพันธ์ จุดตัดทางภูมิศาสตร์ของข้อมูลตำแหน่งที่ตั้ง และรูปแบบในสังคมออนไลน์และความสัมพันธ์อื่น ๆ[75]

หลายรัฐยังคงมีส่วนร่วมในการสอดส่องในวงกว้างอย่างลับ ๆ และบางรัฐอ้างว่าการสอดส่องในวงกว้างเป็นสิ่งจำเป็นในการคุ้มครองความมั่นคงของชาติ ซึ่งการสอดส่องในวงกว้างก่อให้เกิดความท้าทายที่สำคัญต่อข้อกำหนดความชอบด้วยกฎหมายของข้อ 17 ของ ICCPR[76]

5.3.2 กรอบสิทธิความเป็นส่วนตัวกับการสอดส่องการสื่อสาร

ความเป็นส่วนตัวในการติดต่อสื่อสารเป็นไปเพื่อจำกัดอำนาจของรัฐบาลในการติดตามตรวจสอบประชากร และคุ้มครองพื้นที่ที่บุคคลสามารถพัฒนาและแสดงความคิดเห็นอย่างมั่นใจ[77]

ข้อ 17 ของ ICCPR กล่าวถึงการป้องกันการแทรกแซง "การติดต่อสื่อสาร" โดยตรง ซึ่งเป็นคำที่ควรตีความให้ครอบคลุมการสื่อสารทุกรูปแบบ ทั้งทางออนไลน์และออฟไลน์ สิทธินี้ก่อให้เกิดภาระหน้าที่ที่

[74] A/HRC/23/40, para 39.

[75] A/69/397, para 8.

[76] A/69/397, para 38.

[77] A/HRC/23/40

ครอบคลุมของรัฐ ในการหนดให้รับประกันความถูกต้องและความลับของการติดต่อสื่อสารโดยทางนิตินัยและโดยพฤตินัย เพื่อประกันว่าอีเมลและรูปแบบการสื่อสารออนไลน์อื่นๆ ถูกส่งไปยังผู้รับที่ต้องการอย่างแท้จริงโดยไม่มีการรบกวนหรือการตรวจสอบ โดยหน่วยงานของรัฐหรือบุคคลที่สาม ทั้งนี้ การสอดส่อง ไม่ว่าจะเป็นทางอิเล็กทรอนิกส์หรืออย่างอื่นเป็นสิ่งต้องห้าม[78]

สมัชชาใหญ่แห่งสหประชาชาติเรียกร้องให้ทุกรัฐทบทวนกระบวนการ แนวทางปฏิบัติ และกฎหมายที่เกี่ยวข้องกับการสอดส่องการสื่อสาร การดัก และการรวบรวมข้อมูลส่วนบุคคล โดยเน้นย้ำถึงความจำเป็นที่รัฐต้องประกันการปฏิบัติตามพันธกรณีภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศอย่างเต็มที่และมีประสิทธิผล[79]

ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ โดยเฉพาะสิทธิความเป็นส่วนตัวดังกล่าวไปแล้ว ประกอบกับการตีความของผู้เชี่ยวชาญของสหประชาชาติและกลไกระดับภูมิภาค อาจสรุปหลักการสำคัญสำหรับประกันว่าการสอดส่องสอดคล้องกับกฎหมายสิทธิมนุษยชน ดังนี้[80]

1) ความชอบด้วยกฎหมาย

การสอดส่องการสื่อสารดิจิทัลจะต้องสอดคล้องกับพันธกรณีด้านสิทธิมนุษยชนระหว่างประเทศและต้องดำเนินการบนพื้นฐานของกรอบกฎหมายที่ได้รับการชี้นำโดยมาตรฐานขั้นต่ำ ดังต่อไปนี้[81]

- กฎหมายต้องสามารถเข้าถึงได้โดยสาธารณะ กฎความลับและการตีความกฎหมายอย่างลับ ๆ ไม่ใช่คุณสมบัติที่จำเป็นของ "กฎหมาย" กฎหมายต้องชัดเจนเพียงพอ ดุลยพินิจที่มอบให้กับผู้บริหารหรือผู้พิพากษา และวิธีการใช้ดุลยพินิจดังกล่าวจะต้องถูกจำกัดด้วยความชัดเจนตามสมควร[82] ทั้งกฎหมายหรือระเบียบต้องไม่ให้อำนาจวินิจฉัยอย่างเกินขอบเขตกับหน่วยงานฝ่ายบริหาร ไม่ว่าจะเป็นหน่วยงานความมั่นคงและข่าวกรอง กฎหมายหรือระเบียบนั้นต้องมีตัวบทที่แสดงอย่างชัดเจนถึงขอบเขตและลักษณะการใช้อำนาจวินิจฉัยนั้น (ทั้งในตัวกฎหมายเอง หรือในแนวปฏิบัติที่มีผลบังคับใช้และมีการประกาศใช้) พร้อมกับแสดงความชอบด้วยเหตุผลที่ชัดเจน กฎหมายที่เข้าถึงได้แต่ไม่ทำ

---

[78] CCPR General Comment No. 16, para. 8.

[79] A/RES/68/167, 18 December 2013

[80]A/RES/69/166 ; A/RES/68/167 ; A/RES/71/199 ; A/RES/73/179 ; A/HRC/39/29, para. 34 – 36., 71. ; A/HRC/23/40; A/HRC/27/37 ; A/69/397 ; A/HRC/41/35 ; A/HRC/28/39, para 44.; A/75/147 ; A/HRC/13/37 ; Joint Declaration, 21 June 2013, para. 9. ; International Principles on the Application of Human Rights to Communications Surveillance, https://en.necessaryandproportionate.org/

[81] A/HRC/39/29, 3 August 2018, para. 34 – 36., 71. ; A/HRC/23/40 ; A/RES/68/167; A/HRC/27/37 ; A/69/397

[82] A/HRC/28/39, 19 December 2014, para. 11.

ให้เห็นผลลัพธ์ที่ชัดเจน ย่อมถือว่าบกพร่อง เพื่อประกับการเข้าถึงได้ รัฐหลายแห่งยังกำหนดให้กรอบกฎหมายในลักษณะเช่นนี้ต้องจัดทำขึ้นโดยผ่านการพิจารณาของรัฐสภาแทนที่จะเป็นกฎหมายลูกที่ฝ่ายบริหารเป็นผู้ประกาศใช้ เพื่อให้ประชาชนเข้าถึงได้ทั้งหลังมีการประกาศใช้ และในช่วงที่มีการแก้ไขเพิ่มเติม[83]

- กฎหมายต้องมีความชัดเจนและความแม่นยำเพียงพอที่จะช่วยให้ผู้ที่ได้รับผลกระทบควบคุมพฤติกรรมของตนโดยคาดหมายถึงสถานการณ์ที่อาจเกิดการสอดส่องที่ล่วงล้ำได้ ในความเห็นทั่วไปฉบับที่ 16 คณะกรรมการสิทธิมนุษยชนเน้นว่ากฎหมายที่อนุญาตให้มีการแทรกแซงการสื่อสารส่วนตัว “ต้องระบุรายละเอียดเกี่ยวกับสถานการณ์ที่แน่นอนซึ่งการแทรกแซงอาจได้รับอนุญาต” ข้อกำหนดนี้กำหนดให้กฎหมายภายในประเทศต้องระบุเงื่อนไขต่าง ๆ อย่างชัดเจน กฎหมายต้องกำหนดให้มีหลักประกันที่ระบุรายละเอียดขอบเขต และระยะเวลาที่อนุญาตให้ใช้มาตรการดังกล่าวได้ หลักเกณฑ์ให้อนุญาตหน่วยงานที่มีอำนาจซึ่งสามารถอนุมัติ ดำเนินการ และกำกับดูแล และการเยียวยาที่เป็นไปตามกฎหมายในประเทศ ตลอดจนการจัดเก็บข้อมูลที่ได้รับ และสถานการณ์ที่การบันทึกอาจหรือต้องถูกลบหรือทำลาย[84]
- กฎหมายต้องไม่ทำให้สาระสำคัญของสิทธิไร้ความหมายและต้องสอดคล้องกับสิทธิมนุษยชนอื่น ๆ รวมถึงการห้ามการเลือกปฏิบัติ
- กรอบกฎหมายสำหรับการสอดส่องควรครอบคลุมคำขอของรัฐต่อองค์กรธุรกิจ นอกจากนี้ยังควรครอบคลุมการเข้าถึงข้อมูลที่จัดขึ้นนอกอาณาเขตหรือการแบ่งปันข้อมูลกับรัฐอื่น ๆ โครงสร้างที่ประกันความรับผิดชอบและความโปร่งใสภายในองค์กรของรัฐที่ดำเนินการสอดส่องจำเป็นต้องกำหนดไว้อย่างชัดเจนในกฎหมาย[85]

2) วัตถุประสงค์ที่ชอบธรรม

ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ การจำกัดสิทธิในความเป็นส่วนตัว เสรีภาพในการแสดงออก และเสรีภาพในการสมาคม จะต้องดำเนินการตาม “วัตถุประสงค์ที่ชอบด้วยกฎหมาย” อย่างน้อยหนึ่งข้อ ซึ่งถูกระบุไว้อย่างละเอียดข้อบทที่เกี่ยวข้อง โดยใช้ถ้อยคำอย่างกว้างๆ และรวมถึงความปลอดภัย

[83] A/HRC/27/37, 30 June 2557, para 29.

[84] A/69/397, 23 September 2014, para 36. ; A/HRC/23/40, para 81 - 87. ; A/HRC/13/37. ; ; A/HRC/41/35, para 50.

[85] A/HRC/39/29, 3 August 2018, paras. 36, 61.

สาธารณะ การป้องกันอาชญากรรม การปกป้องศีลธรรมและสิทธิของผู้อื่น และความมั่นคงของชาติ (ข้อ 19 (3) ของ ICCPR)[86]

อย่างไรก็ดี การส่องสอดถือว่าเป็นมาตรการที่ล่วงล้ำอย่างมาก จึงต้องใช้เฉพาะภายใต้สถานการณ์พิเศษที่สุดหรือกรณีที่เป็นข้อยกเว้นมากสุดเท่านั้น (เพื่อการสืบสวนหรือป้องกันอาชญากรรมหรือภัยคุกคามที่ร้ายแรงที่สุด)[87] และเฉพาะเมื่อมีการกำกับดูแลจากหน่วยงานศาลที่เป็นอิสระ[88]

3) ความจำเป็นและได้สัดส่วน

เป็นหน้าที่ของรัฐที่จะต้องแสดงให้เห็นว่าการแทรกแซงใด ๆ ต่อสิทธิความเป็นส่วนตัว เป็นวิธีการที่จำเป็นในการบรรลุจุดมุ่งหมายที่ชอบธรรม ข้อกำหนดนี้ต้องการให้มีการเชื่อมโยงที่สมเหตุสมผลระหว่างวิธีการที่ใช้และเป้าหมายที่พยายามจะบรรลุ นอกจากนี้มาตรการที่เลือกนำมาใช้เป็นเครื่องมือที่แทรกแซงสิทธิน้อยที่สุดในบรรดาเครื่องมือที่อาจบรรลุผลลัพธ์ที่ต้องการ[89] ดังนั้น การสอดส่องควรถูกนำมาใช้เฉพาะเมื่อมาตรการที่เป็นไปได้อื่นซึ่งละเมิดสิทธิน้อยกว่าเพื่อการจัดการกับภัยคุกคามนั้น ไม่มีอยู่แล้ว[90]

การสอดส่องควรเป็น "การแทรกแซงเฉพาะกรณี (case-specific interferences) บนพื้นฐานของเหตุอันควรสงสัยที่สมเหตุสมผล (reasonable suspicion) ว่าบุคคลใดกระทำความผิดหรือกำลังกระทำความผิดทางอาญาหรือมีส่วนร่วมในการกระทำที่เป็นภัยคุกคามต่อความมั่นคงของชาติ[91]

รัฐไม่ควรเก็บรักษาหรือกำหนดให้มีการเก็บรักษาข้อมูลเฉพาะอย่างหมดจดเพื่อวัตถุประสงค์ในการสอดส่อง[92] เพราะการรวบรวมและการเก็บรักษาข้อมูลการสื่อสารถือเป็นการแทรกแซงสิทธิ์ในความเป็นส่วนตัว ไม่ว่าข้อมูลนั้นจะเข้าถึงหรือวิเคราะห์โดยหน่วยงานรัฐในภายหลังหรือไม่ก็ตาม[93] ทั้งนี้ การเก็บรักษาข้อมูลเชิงบังคับ โดยที่บริษัทโทรศัพท์และผู้ให้บริการอินเทอร์เน็ตจำเป็นต้องจัดเก็บเมตาดาต้า (Meta Data) เกี่ยวกับการสื่อสารของลูกค้า เพื่อการเข้าถึงในภายหลังโดยหน่วยงานบังคับใช้กฎหมายและหน่วยงานข่าวกรอง ดูเหมือนไม่จำเป็นหรือได้สัดส่วน[94]

---

[86] A/HRC/41/35, para 50. ; “Necessary and proportionate: International Principles on the Application of Human Rights to Communications Surveillance” (May 2014).

[87] A/HRC/41/35, para 50. ; A/HRC/29/32, para 60.

[88] A/HRC/23/40, para 81 - 87. ; A/HRC/13/37.

[89] A/HRC/13/37, para 60.

[90] A/HRC/23/40, para 83.

[91] A/HRC/25/59, paras. 52, 59; A/69/397

[92] A/HRC/29/32, para 90.

[93] Ben Emmerson, A/69/397, 23 September 2014, para 54.

[94] A/HRC/28/39, 19 December 2014, para. 10.

อำนาจในการสอดส่องแบบลับสามารถอ้างอย่างสมเหตุสมผลได้เฉพาะเท่าที่จำเป็นอย่างยิ่งสำหรับการบรรลุเป้าหมายที่ชอบธรรมและเป็นไปตามข้อกำหนดของความได้สัดส่วน[95] มาตรการสอดส่องอย่างลับต้องถูกจำกัด เฉพาะการป้องกันหรือสอบสวนอาชญากรรมหรือภัยคุกคามที่ร้ายแรงที่สุด ระยะเวลาของการสอดส่องควรถูกจำกัดไว้ที่ขั้นต่ำที่สุดอย่างเคร่งครัด ซึ่งจำเป็นสำหรับการบรรลุเป้าหมายที่กำหนด และจำเป็นต้องกำหนดไว้อย่างชัดเจนเกี่ยวกับกฎเกณฑ์ที่เข้มงวดในการใช้และจัดเก็บข้อมูลที่ได้รับ และสถานการณ์ที่ข้อมูลที่รวบรวมและจัดเก็บต้องถูกลบ โดยพิจารณาจากความจำเป็นและสัดส่วนที่เข้มงวด การแบ่งปันข่าวกรองจะต้องอยู่ภายใต้หลักการความชอบด้วยกฎหมาย ความจำเป็นที่เข้มงวดและความได้สัดส่วนเช่นเดียวกัน[96]

การสอดส่องในวงกว้าง

การวิเคราะห์ความได้สัดส่วนของการสอดส่องในวงกว้างเปลี่ยนจากระดับจุลภาค (การประเมินเหตุผลสำหรับการบุกรุกความเป็นส่วนตัวของบุคคลหรือองค์กรโดยเฉพาะ) เป็นระดับมหภาค (การประเมินความสมเหตุสมผลสำหรับการใช้ระบบที่เกี่ยวข้องกับการแทรกแซงอย่างกว้างขวางต่อสิทธิความเป็นส่วนตัวของบุคคลและของกลุ่มของผู้ใช้อินเทอร์เน็ตทั้งหมด)[97]

การปรับใช้เทคโนโลยีการสอดส่องในวงกว้างโดยไม่มีข้อสงสัยล่วงหน้าต่อบุคคลนั้น กระทบต่อสาระสำคัญของสิทธิความเป็นส่วนตัวของบุคคลจำนวนมาก จึงอาจไม่สอดคล้องกับหลักการที่ว่ารัฐควรใช้วิธีการที่ล่วงล้ำสิทธิน้อยที่สุด ดังนั้น การมีอยู่ของโปรแกรมการสอดส่องในวงกว้างถือเป็นการแทรกแซงที่อาจไม่ได้สัดส่วนกับสิทธิในความเป็นส่วนตัว[98] เว้นแต่รัฐสามารถให้เหตุผลได้ถึงความได้สัดส่วนของการแทรกแซงอย่างเป็นระบบกับสิทธิ์ความเป็นส่วนตัวทางอินเทอร์เน็ตของผู้บริสุทธิ์ที่อาจไม่จำกัดจำนวนในส่วนใด ๆ ของโลกได้[99]

ทั้งนี้ เพื่อให้สามารถประเมินความได้สัดส่วนได้ รัฐที่ใช้เทคโนโลยีการสอดส่องในวงกว้างต้องรายงานสาธารณะอย่างมีความหมายเกี่ยวกับประโยชน์ที่เป็นรูปธรรมที่เกิดขึ้นจากการใช้งาน การประเมินความได้สัดส่วนในบริบทนี้เกี่ยวข้องกับการสร้างสมดุลระหว่างผลประโยชน์ของสังคมในการคุ้มครองความเป็นส่วนตัวออนไลน์ กับความจำเป็นที่ไม่อาจปฏิเสธได้ของการต่อต้านการก่อการร้ายและการบังคับใช้กฎหมายที่มีประสิทธิภาพ การกำหนดจุดสมดุลนั้นจำเป็นต้องมีการอภิปรายสาธารณะอย่างมีข้อมูล[100]

---

[95] A/HRC/23/40, para 83 (b).

[96] A/HRC/39/29, 3 August 2018, para 37.

[97] Ben Emmerson, A/69/397, 23 September 2014, para 13.

[98] A/69/397, 23 September 2014, para 18. ; A/HRC/27/37, para 25. ; A/HRC/23/40 , para. 62;

[99] Ben Emmerson, A/69/397, 23 September 2014, para 51.

[100] Ben Emmerson, A/69/397, 23 September 2014, para 14.

ตามหลักกฎหมายสิทธิมนุษยชนระหว่างประเทศ รัฐมีหน้าที่ต้องพิสูจน์การทดสอบสามส่วนสำหรับการใช้มาตรการสอดส่อง โดยต้องให้เหตุผลที่ชัดเจนและอิงตามหลักฐานสำหรับการใช้มาตรการดังกล่าว[101]

4) กระบวนการอนุญาตและการกำกับดูแลอย่างมีประสิทธิผล

ข้อ 17 (2) ของ ICCPR ระบุว่า ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายมิให้ถูกแทรกแซง ซึ่งการ “คุ้มครองตามกฎหมาย” จะเป็นจริงได้เมื่อมีขั้นตอนปฏิบัติเพื่อคุ้มครอง รวมทั้งมีโครงสร้างเชิงสถาบันที่มีประสิทธิผลและได้รับการอุดหนุนด้านทรัพยากรอย่างเพียงพอ[102]

จะต้องไม่อนุญาตให้มีระบบสอดส่องข้อมูลอย่างเป็นความลับที่ไม่ถูกตรวจสอบโดยหน่วยงานกำกับดูแลที่เป็นอิสระ และการแทรกแซงใด ๆ ต้องได้รับอนุมัติจากหน่วยงานอิสระ[103]

ในมติที่ 69/166 สมัชชาใหญ่แห่งสหประชาชาติเรียกร้องให้รัฐจัดตั้งหรือคงไว้ซึ่งกลไกการกำกับดูแลภายในประเทศทางตุลาการ บริหาร และ/หรือรัฐสภา ที่เป็นอิสระ มีประสิทธิภาพ มีทรัพยากรเพียงพอ และเป็นกลาง ที่สามารถประกันความโปร่งใส และความรับผิดชอบตามความเหมาะสมสำหรับการสอดส่องการสื่อสารของรัฐ การสกัดกั้นการสื่อสาร และการรวบรวมข้อมูลส่วนบุคคล[104]

มาตรการสอดส่อง รวมถึงคำขอข้อมูลการสื่อสารไปยังองค์กรธุรกิจและการแบ่งปันข้อมูลข่าวกรองควรได้รับการตรวจสอบและกำกับดูแลโดยหน่วยงานอิสระในทุกขั้นตอน รวมถึงควรมีข้อกำหนดการอนุญาตและการกำกับดูแลที่เพียงพอ ทั้งเมื่อมาตรการได้รับอนุญาตครั้งแรก ระหว่างกำลังดำเนินการ หรือหลังจากสิ้นสุดมาตรการ[105]

กรอบการกำกับดูแลอาจมีหลายรูปแบบ แต่แนวปฏิบัติที่ดีที่สุดต้องอาศัยการมีส่วนร่วมของฝ่ายบริหาร นิติบัญญัติ และตุลาการ ตลอดจนการกำกับดูแลของพลเรือนที่เป็นอิสระ[106] ทั้งนี้ หน่วยงานกำกับดูแลควรเป็นอิสระจากเจ้าหน้าที่ที่ดำเนินการสอดส่องและมีความเชี่ยวชาญ มีอำนาจหน้าที่และทรัพยากรที่เหมาะสมและเพียงพอ การอนุญาตและการกำกับดูแลควรแยกออกจากกัน หน่วยงานกำกับดูแลที่เป็นอิสระควรตรวจสอบและติดตามกิจกรรมของผู้ที่ดำเนินกาสอดส่องและเข้าถึงผลิตภัณฑ์ของการสอดส่องในเชิงรุก และดำเนินการทบทวนความสามารถในการสอดส่องและพัฒนาการทางเทคโนโลยีเป็นระยะ หน่วยงานที่ดำเนินการสอดส่องควรต้องให้

---

[101] A/69/397, 23 September 2014, para 12. ; A/HRC/23/40, para 83.

[102] A/HRC/27/37, 30 June 2557, para 37.

[103] A/HRC/13/37, para. 62.

[104] A/RES/69/166, para 4 (d).

[105] European Court of Human Rights, Zakharov v. Russia.

[106] A/HRC/27/37, 30 June 2014, para. 37. ; General Assembly resolution 71/199, para. 5 (d).

ข้อมูลทั้งหมดที่จำเป็นเพื่อการกำกับดูแลที่มีประสิทธิภาพเมื่อมีการร้องขอและรายงานไปยังหน่วยงานกำกับดูแลอย่างสม่ำเสมอ และหน่วยงานที่กำกับดูแลควรจะต้องเก็บบันทึกของมาตรกาสอดส่องทั้งหมดที่ดำเนินการ[107]

การมีส่วนร่วมของฝ่ายตุลาการที่เป็นไปตามมาตรฐานสากลถือเป็นหลักประกันที่สำคัญ[108] โดยหน่วยงานตุลาการจำเป็นต้องประกันว่ามีหลักฐานที่ชัดเจนเพียงพอเกี่ยวกับภัยคุกคาม และการสอดส่องที่เสนอมีความจำเป็นและได้สัดส่วนอย่างเคร่งครัดเพื่อการบรรลุเป้าหมายที่ชอบธรรม และการอนุญาต หรือปฏิเสธควรทำก่อนใช้มาตรการสอดส่อง (ex ante)[109] และควรถือว่าการอนุญาตล่วงหน้าของการสอดส่องควรเป็นบรรทัดฐาน[110] ยกเว้นในกรณีที่มีความจำเป็นเร่งด่วนที่ถูกกำหนดขึ้นอย่างมีเหตุผล และบุคคลที่ได้รับผลกระทบควรได้รับแจ้งว่าได้รับการเข้าถึงข้อมูลที่เก็บไว้ทันทีที่การแจ้งเตือนดังกล่าวไม่ก่อให้เกิดความเสี่ยงต่อการสืบสวนอีกต่อไป[111]

ในบริบทของการสอดส่องแบบกำหนดเป้าหมาย (Targeted surveillance) อย่างน้อยต้องให้โอกาสสำหรับการตรวจสอบล่วงหน้า (Ex ante review) ถึงความจำเป็นและได้สัดส่วนของมาตรการสอดส่อง ส่วนการสอดส่องในวงกว้าง (Mass surveillance) ซึ่งโดยทั่วไปไม่ได้ขึ้นอยู่กับความสงสัยล่วงหน้าต่อบุคคล การทบทวนก่อนหน้าจึงถูกจำกัด ดังนั้น จึงควรจัดตั้งหน่วยงานกำกับดูแลอิสระที่เข้มแข็งซึ่งมีทรัพยากรและได้รับมอบอำนาจอย่างเพียงพอในการดำเนินการตรวจสอบล่วงหน้าเกี่ยวกับการใช้เทคนิคการสอดส่องให้สอดคล้องกับข้อกำหนดของความชอบกฎหมาย ความจำเป็น และได้สัดส่วน[112]

มิติเชิงกระบวนการอื่น ๆ ของมาตรา 17 คือข้อกำหนดสำหรับการตรวจสอบข้อเท็จจริงย้อนหลัง (ex post facto review) ของมาตรการสอดส่อง บางรัฐจัดให้มีผู้ตรวจสอบอิสระในการติดตามการดำเนินการของกฎหมายสอดส่องโดยการวิเคราะห์ลักษณะและขอบเขตของการใช้งานและการให้เหตุผลในการนั้น การทบทวนดังกล่าวควรรวมการวิเคราะห์ความสอดคล้องของแนวปฏิบัติของรัฐกับข้อกำหนดของ ICCPR ด้วยเสมอ[113]

---

[107] European Court of Human Rights, Kennedy v. United Kingdom, application No. 26839/05, judgment of 18 May 2010, para. 165, and Roman Zakharov v. Russia, para. 272.

[108] A/69/397, 23 September 2014, para 46.

[109] A/HRC/39/29, 3 August 2018, para 39. ; A/75/147, 27 July 2020, para 43.

[110] Schrems and Digital Rights Ireland, which deal with communications data, require prior independent authorization. ; CCPR/C/GRB/CO/7, para. 24 (c) and CCPR/C/CAN/CO/6, para. 10.

[111] Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others.

[112] A/HRC/13/37, para 62.

[113] Ben Emmerson, A/69/397, 23 September 2014, para 48.

เพื่อประกันว่าจะมีการกำกับดูแลอย่างเข้มงวดในการใช้เทคนิคการสอดส่องและการประมวลผลข้อมูลส่วนบุคคล ต้องไม่มีระบบสอดส่องที่เป็นความลับซึ่งไม่อยู่ภายใต้การตรวจสอบของหน่วยงานกำกับดูแลที่มีประสิทธิภาพและการแทรกแซงทั้งหมดจะต้องได้รับอนุญาตผ่านหน่วยงานอิสระ[114]

การอนุญาตให้สอดส่องต้องอยู่ภายใต้ข้อกำหนดในการเก็บบันทึกโดยละเอียด เนื่องจากมีความเสี่ยงสูงที่จะเกิดการล่วงละเมิด คำขอให้สอดส่องควรได้รับการจัดทำเป็นเอกสารและการออกใบสำคัญแสดงสิทธิสำหรับการดำเนินการดังกล่าวเท่านั้น[115]

นอกจากนี้ แม้กลไกกำกับดูแลโดยตุลาการจะเป็นสอดคล้องกับหลักกฎหมายสิทธิมนุษยชนระหว่างประเทศ และมีความจำเป็น แต่อาจไม่เพียงพอ จึงมีความสนใจมากขึ้นต่อแม่แบบผสมระหว่างการกำกับดูแลของกลไกฝ่ายบริหาร ตุลาการ และรัฐสภา โดยเฉพาะการกำหนดให้มีตำแหน่ง “public interest advocacy” ภายในกระบวนการอนุมัติการสอดส่อง เนื่องจากบุคคลที่สาม อย่างเช่น ผู้ให้บริการอินเทอร์เน็ต มีบทบาทเพิ่มมากขึ้น จึงอาจจำเป็นต้องส่งเสริมให้หน่วยงานเหล่านี้มีส่วนร่วมในการอนุมัติมาตรการการสอดส่องข้อมูลที่ส่งผลกระทบต่อผลประโยชน์ของพวกเขา หรือเปิดโอกาสให้หน่วยงานเหล่านี้สามารถคัดค้านมาตรการที่เป็นอยู่ได้[116]

ที่สำคัญคือ กระบวนการกำกับดูแลต้องโปร่งใสและอยู่ภายใต้การตรวจสอบของสาธารณะอย่างเหมาะสมภายในระบอบการกำกับดูแล จะต้องมีการรายงานต่อสาธารณชนอย่างสม่ำเสมอว่ารัฐบาลได้ดำเนินกิจกรรมการสอดส่องอย่างเหมาะสมหรือไม่ ในลักษณะที่ช่วยให้สาธารณชนเข้าใจว่ารัฐบาลได้ปฏิบัติตามขั้นตอนหรือไม่[117] รวมถึงหลังจากการสอดส่องจบลงแล้ว อาจจะมีการรายงานต่อรัฐสภาหรือสาธารณะ เพื่อตรวจสอบสอบว่าการสอดส่องที่เกิดขึ้นแล้วนั้น เป็นไปตามกรอบการทำงานที่กำหนดไว้หรือไม่

ผู้ให้บริการด้านการสื่อสารก็มีศักยภาพที่จะตรวจสอบบริการข่าวกรองและหน่วยงานบังคับใช้กฎหมาย[118] ผู้ให้บริการที่ดำเนินการตามคำสั่งศาลเพื่อการสอดส่องสามารถโต้แย้งคำสั่งที่กว้างเกินไปหรือผิดกฎหมายได้[119] และสามารถเพิ่มความโปร่งใสเกี่ยวกับวิธีการดำเนินการสอดส่อง โดยเปิดเผยจำนวนคำขอสำหรับการสกัดกั้นและข้อมูลการสื่อสารที่ได้รับ[120] ทั้งนี้ มีความจำเป็นในการคุ้มครองผู้ที่กระทำการโดยสุจริตเมื่อเปิดเผย

---

[114] A/HRC/13/37, para. 62.

[115] A/HRC/41/35, para 50.

[116] A/HRC/27/37, 30 June 2014, para. 38..

[117] A/HRC/39/29, 3 August 2018, para 40.

[118] Zakharov v. Russia, para. 270.

[119] A/HRC/27/37, para. 38.

[120] A/HRC/23/40, para. 92.

ข้อมูล “ต่อสื่อหรือสาธารณชนในวงกว้างหากเป็นมาตรการสุดท้าย และเกี่ยวข้องกับเรื่องที่สาธารณชนให้ความสนใจเป็นอย่างมาก”[121]

นอกจากนี้ ผู้รายงานพิเศษฯ ยกตัวอย่างของชุมชนบางแห่งที่ได้จัดตั้งคณะกรรมการพลเรือนขึ้นเพื่อควบคุมการใช้และการซื้อเทคโนโลยีการสอดส่อง เช่น เมืองโอ๊คแลนด์ในมลรัฐแคลิฟอร์เนียได้ออกกฎหมายเกี่ยวกับคุณสมบัติในการซื้อเทคโนโลยีการสอดส่อง ซึ่งรวมถึง (ก) กระบวนการอนุมัติที่ดำเนินการโดยหน่วยงานที่เกี่ยวข้อง ซึ่งคำนึงถึงพันธกรณีด้านสิทธิมนุษยชนของรัฐ (ข) ประกาศต่อสาธารณะเกี่ยวกับการซื้อดังกล่าวผ่านกระบวนการปกติและการปรึกษาหารือสาธารณะในประเด็นต่างๆ เช่น ผลกระทบด้านสิทธิมนุษยชนของการซื้อดังกล่าว และเทคโนโลยีที่เป็นประเด็นจะมีประสิทธิภาพในการบรรลุวัตถุประสงค์ที่ตั้งใจไว้หรือไม่ (ค) การรายงานต่อสาธารณะเป็นประจำเกี่ยวกับการอนุมัติ การซื้อ และการใช้งานดังกล่าว[122]

เทคนิคการสอดส่องนอกกฎหมายต้องอยู่ภายใต้การควบคุมของฝ่ายนิติบัญญัติ เพราะเป็นการบ่อนทำลายหลักการพื้นฐานของประชาธิปไตยและมีแนวโน้มที่จะส่งผลกระทบทางการเมืองและสังคมที่[123]

5) <u>การเยียวยาที่มีประสิทธิผล</u>

ข้อ 2 ของ ICCPR กำหนดให้รัฐภาคีประกันให้ผู้เสียหายจากการละเมิด ICCPR ได้รับการเยียวยาอย่างเป็นผล โดยจะต้องประกันว่าบุคคลใดที่เรียกร้องการเยียวยาดังกล่าว มีสิทธิจะได้รับการพิจารณาจากฝ่ายตุลาการ ฝ่ายบริหาร หรือฝ่ายนิติบัญญัติที่มีอำนาจ หรือจากหน่วยงานอื่นที่มีอำนาจตามที่กำหนดไว้

กรณีที่รัฐไม่สามารถสอบสวนตามข้อกล่าวหาว่ามีการละเมิด อาจส่งผลและโดยตัวของมันเองอาจเป็นการละเมิด ICCPR[124] นอกจากนั้น การทำให้การละเมิดอย่างต่อเนื่องยุติลงเป็นองค์ประกอบสำคัญของสิทธิที่จะได้รับการเยียวยาอย่างเป็นผล[125]

การเยียวยาที่เป็นผลสำหรับการละเมิดความเป็นส่วนตัวที่เกิดจากการสอดส่องข้อมูลดิจิทัลอาจปรากฏในหลายรูปแบบทั้งผ่านศาล นิติบัญญัติ หรือบริหาร โดยการเยียวยาที่เป็นผลมักจะมีลักษณะร่วมกันบางประการ[126]

---

[121] A/HRC/13/37, para 16; A/HRC/23/40, paras. 52, 79, 84.

[122] A/HRC/41/35, para 52.

[123] A/HRC/23/40, para 87.

[124] 4 CCPR/C/21/Rev.1/Add. 13, para. 15.

[125] A/HRC/27/37, para. 39.

[126] A/HRC/27/37, para. 40 - 41. และอ้างถึง Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law (General Assembly resolution 60/147, annex).

- การเยียวยาต้องเป็นที่รับรู้และเข้าถึงได้โดยบุคคลทุกคนที่อ้างว่าสิทธิของตนได้ถูกละเมิด การรับแจ้งข้อมูล และสิทธิการฟ้องคดีเพื่อคัดค้านการใช้มาตรการดังกล่าว จึงเป็นประเด็นสำคัญ[127]
- การเยียวยาที่เป็นผลต้องเกิดขึ้นพร้อมกับการสอบสวนโดยพลัน อย่างรอบด้านและไม่ลำเอียงต่อข้อกล่าวหาว่ามีการละเมิดเกิดขึ้น ซึ่งสัมพันธ์กับข้อกำหนดให้มีหน่วยงานกำกับดูแลที่เป็นอิสระดังกล่าวมาแล้ว
- เพื่อให้การเยียวยาเป็นผล การเยียวยานั้นต้องสามารถยุติการละเมิดอย่างต่อเนื่องได้ หน่วยงานที่ให้การเยียวยาจะต้องสามารถเข้าถึงข้อมูลที่เกี่ยวข้องอย่างเต็มที่และไม่ถูกขัดขวาง เข้าถึงทรัพยากรและความชำนาญที่จำเป็นต่อการสอบสวน และสามารถออกระเบียบที่มีผลผูกพันตามกฎหมาย
- กรณีที่การละเมิดสิทธิมนุษยชนเพิ่มสูงขึ้นจนถึงระดับที่เป็นการละเมิดอย่างร้ายแรง การเยียวยาจากหน่วยงานอื่นที่ไม่ใช่ศาลอาจไม่เพียงพอ จึงจำเป็นต้องมีการฟ้องคดีทางอาญาด้วย

อย่างไรก็ดี การเยียวยากรณีการสอดส่องเป็นสิ่งที่เกิดขึ้นได้ยาก โดยเฉพาะในบริบทของมาตรการสอดส่องอย่างลับ ๆ เนื่องจากปัจเจกบุคคลมักไม่ทราบว่าตนอยู่ภายใต้การถูกสอดส่อง และการพิสูจน์ความเสียหาย เพื่อเรียกร้องสิทธิในการเยียวยาก็เป็นเรื่องยาก มีรัฐเพียงไม่กี่แห่งที่มีบทบัญญัติกำหนดให้ต้องแจ้งภายหลังการสอดส่องไปยังผู้ถูกสอดส่อง[128] ด้วยเหตุนี้ รัฐบาลต่างๆ จำเป็นต้องมีความโปร่งใสมากขึ้นเกี่ยวกับแผนงานการสอดส่องที่กำลังดำเนินการอยู่ เพื่อให้มีการตรวจสอบโดยสาธารณะ[129]

เป็นสิ่งสำคัญที่ผู้ที่ตกอยู่ภายใต้การสอดส่องควรได้รับแจ้งและอธิบายให้ทราบ บุคคลจำเป็นต้องรู้ว่าตนถูกสอดส่องเพื่อที่จะร้องเรียนและรับการเยียวยาสำหรับการสอดส่องที่ไม่เป็นไปตามกฎหมาย และพวกเขาควรได้รับแจ้งถึงขั้นตอนในการยื่นคำร้องหากต้องการทำเช่นนั้น เป็นที่เข้าใจว่าบางครั้งอาจไม่สามารถแจ้งให้บุคคลทราบได้ว่าพวกเขาอยู่ภายใต้การสอดส่อง เนื่องจากการทำเช่นนี้อาจเป็นอันตรายต่อการสอดส่องเอง อย่างไรก็ตาม ผู้เชี่ยวชาญด้านสิทธิมนุษยชนแนะนำว่าผู้ถูกสอดส่องควรได้รับแจ้งถึงการตัดสินใจอนุญาตให้มีการสอดส่อง

---

[127] A/HRC/27/37, para. 40.

[128] A/69/397, para 50.

[129] A/HRC/28/39, para 51.

ของตนทันทีที่การแจ้งเตือนดังกล่าวจะไม่กระทบต่อวัตถุประสงค์ของการสอดส่องอย่างร้ายแรง[130] แต่หากรัฐไม่จัดให้มีการแจ้งให้ทราบ ก็ควรมีกฎเกณฑ์ฟ้องร้องท้าทายระบอบการสอดส่องอย่างลับ ๆ[131]

หน่วยงานที่ตรวจสอบการละเมิดจะต้องสามารถสั่งให้ยกเลิกการสอดส่องและลบข้อมูลและห้ามการใช้งานโดยการออกคำสั่งที่มีผลผูกพัน[132]

นอกจากนี้ จำเป็นต้องประกันว่ากฎเกณฑ์ที่เกี่ยวข้องกับเขตอำนาจศาล หลักฐาน ความทันเวลา และเงื่อนไขเกณฑ์พื้นฐานอื่น ๆ เหมาะสมสำหรับวัตถุประสงค์ในยุคดิจิทัล เช่น ควรประกันว่าศาลสามารถยอมรับและประเมินผลการวิเคราะห์ทางนิติเวชของผู้เชี่ยวชาญทางเทคนิคเพื่อเป็นหลักฐาน[133]

5.4 สิทธิในความเป็นส่วนตัวและการสอดส่องการสื่อสารทางดิจิทัลในประเทศไทย

5.4.1 หลักประกันการคุ้มครองรัฐธรรมนูญและกฎหมาย

1) รัฐธรรมนูญ

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 รับรองสิทธิในความเป็นส่วนตัวของการสื่อสารไว้ในมาตรา 32 และ 33 ดังนี้

มาตรา 33 บุคคลย่อมมีเสรีภาพในเคหสถาน

การเข้าไปในเคหสถานโดยปราศจากความยินยอมของผู้ครอบครอง หรือการค้นเคหสถานหรือที่รโหฐานจะกระทำมิได้ เว้นแต่มีคำสั่งหรือหมายของศาลหรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ

มาตรา 36 บุคคลย่อมมีเสรีภาพในการติดต่อสื่อสารถึงกันไม่ว่าในทางใด ๆ

การตรวจ การกัก หรือการเปิดเผยข้อมูลที่บุคคลสื่อสารถึงกัน รวมทั้งการกระทำด้วยประการใด ๆ เพื่อให้ล่วงรู้หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันจะกระทำมิได้ เว้นแต่มีคำสั่งหรือหมายของศาลหรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ

---

[130] A/HRC/41/35, para 50. ; A/HRC/28/39, para 51. ; A/HRC/23/40, para 82; Weber and Saravia v. Germany, para 135; Zakharov v. Russia,para 287.

[131] Zakharov v. Russia, paras. 171, 298.

[132] A/HRC/14/46 ; A/HRC/27/37, para 39.

[133] A/HRC/41/35, para 55.

2) กฎหมายระดับพระราชบัญญัติ

พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553 และที่แก้ไขเพิ่ม

มาตรา 27 ให้ กสทช. มีอำนาจหน้าที่ ดังต่อไปนี้

(13) คุ้มครองสิทธิและเสรีภาพของประชาชนมิให้ถูกเอาเปรียบจากผู้ประกอบกิจการและคุ้มครองสิทธิในความเป็นส่วนตัวและเสรีภาพของบุคคลในการสื่อสารถึงกันโดยทางโทรคมนาคมและส่งเสริมสิทธิเสรีภาพและความเสมอภาคของประชาชนในการเข้าถึงและใช้ประโยชน์คลื่นความถี่ที่ใช้ในกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม

มาตรา 32 เพื่อประโยชน์ในการคุ้มครองสิทธิในความเป็นส่วนตัวและเสรีภาพของบุคคลในการสื่อสารถึงกันโดยทางโทรคมนาคม ให้ กสทช. มีอำนาจกำหนดมาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม

ในกรณีที่มีการกระทำความผิดโดยการดักรับไว้ ใช้ประโยชน์ หรือเปิดเผยข้อความข่าวสารหรือข้อมูลอื่นใดที่มีการสื่อสารทางโทรคมนาคมโดยไม่ชอบด้วยกฎหมาย ให้ถือว่า กสทช. เป็นผู้เสียหายตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีที่ผู้ได้รับใบอนุญาตประกอบกิจการโทรคมนาคมเป็นผู้กระทำความผิดตามวรรคสอง หรือรู้ว่ามีการกระทำความผิดตามวรรคสอง แต่เพิกเฉยหรือไม่ดำเนินการตามกฎหมายภายในเวลาอันสมควร ให้ กสทช. มีอำนาจสั่งพักใช้หรือเพิกถอนใบอนุญาตประกอบกิจการโทรคมนาคมได้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ประเทศไทยมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีผลบังคับใช้อย่างเต็มรูปแบบเมื่อเดือนมิถุนายน 2565 ที่ผ่านมา กฎหมายฉบับนี้วางกรอบสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งมีต้นแบบมาจากข้อบังคับในกฎหมายของสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูล (General Data Protection Regulation 2016/679 : GDPR)

อย่างไรก็ดี พระราชบัญญัตินี้กำหนดข้อยกเว้นการบังคับใช้สำหรับกิจกรรมบางประเภทและสำหรับกิจการของภาครัฐบางส่วนไว้ในมาตรา 4 รวมถึงการยกเว้นการดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ

มาตรา 4 พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา 4 กำหนดยกเว้นสำหรับหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงดังกล่าว โดยกฎหมายไม่ได้กำหนดนิยามว่าหมายถึงหน่วยงานใดบ้าง ทำให้อาจมีการตีความข้อยกเว้นอย่างกว้างขวาง มีข้อสังเกตด้วยว่า การกำหนดข้อยกเว้นในลักษณะที่กว้างขวางดังกล่าว อาจนำไปสู่การเปิดช่องให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลหรือสอดส่องโดยวิธีนอกกฎหมายหรือไม่ เพราะหากเป็นการใช้อำนาจตามกฎหมายของหน่วยงาน ก็ย่อมสามารถทำได้ตามข้อยกเว้นที่ไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอยู่แล้ว (เช่น มาตรา 24, 25) ดังนั้น ในมุมมองเบื้องต้นของผู้วิจัย การกำหนดให้หน่วยงานที่มีหน้าที่ในการรักษาความมั่นคงอยู่ภายใต้การคุ้มครองของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ย่อมทำให้มีหลักประกันในการคุ้มครองสิทธิให้กับประชาชน โดยเฉพาะการประกันว่าการสอดส่องนอกกฎหมายสามารถทำได้ยากขึ้นและช่วยให้การดำเนินการสอดส่องมีความโปร่งใสและอยู่ภายใต้หลักความรับผิดชอบมากขึ้นด้วย

5.4.2 กรอบกฎหมายที่ให้อำนาจสอดส่องการสื่อสารทางดิจิทัล

เมื่อพิจารณากรอบกฎหมายของไทยแล้ว อาจจำแนกประเภทกฎหมายที่อำนาจการสอดส่องดังนี้

การสอดส่องในสถานการณ์พิเศษ

มีกฎหมาย 3 ฉบับ ที่ให้อำนาจในการสอดส่องในสถานการณ์พิเศษด้านความมั่นคง ได้แก่ พระราชบัญญัติกฎอัยการศึก พระพุทธศักราช 2457 (ประกาศกฎอัยการศึกษา) พระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 (ประกาศสถานการณ์ฉุกเฉินร้ายแรง)

<u>1) พระราชบัญญัติกฎอัยการศึก พระพุทธศักราช 2457 (กฎอัยการศึก)</u>

มาตรา 8 เมื่อประกาศใช้กฎอัยการศึกในตำบลใด, เมืองใด, มณฑลใด, เจ้าหน้าที่ฝ่ายทหารมีอำนาจเต็มที่จะตรวจค้น, ที่จะเกณฑ์, ที่จะห้าม, ที่จะยึด, ที่จะเข้าอาศัย, ที่จะทำลายหรือเปลี่ยนแปลงสถานที่, และที่จะขับไล่

มาตรา 9 การตรวจค้นนั้น ให้มีอำนาจที่จะตรวจค้น ดังต่อไปนี้

(2) ที่จะตรวจข่าวสาร จดหมาย โทรเลข หีบ ห่อ หรือสิ่งอื่นใดที่ส่งหรือมีไปมาถึงกันในเขตที่ประกาศใช้กฎอัยการศึก

มาตรา 16 ความเสียหายซึ่งอาจบังเกิดขึ้นอย่างหนึ่งอย่างใด ในเรื่องอำนาจของเจ้าหน้าที่ฝ่ายทหาร ตามที่ได้กล่าวมาแล้วในมาตรา 8 และมาตรา 15 บุคคลหรือบริษัทใด ๆ จะร้องขอค่าเสียหายหรือค่าปรับอย่างหนึ่งอย่างใด แก่เจ้าหน้าที่ฝ่ายทหารไม่ได้เลย เพราะอำนาจทั้งปวงที่เจ้าหน้าที่ฝ่ายทหารได้ปฏิบัติและดำเนินการตามกฎอัยการศึกนี้ เป็นการสำหรับป้องกันพระมหากษัตริย์ ชาติ ศาสนา ด้วยกำลังทหารให้ดำรงคงอยู่ในความเจริญรุ่งเรืองเป็นอิสรภาพและสงบเรียบร้อยปราศจากราชศัตรูภายนอกและภายใน

<u>2) พระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 (พ.ร.บ.ฉุกเฉินฯ)</u>

มาตรา 11 ในกรณีที่สถานการณ์ฉุกเฉินมีการก่อการร้าย การใช้กำลังประทุษร้ายต่อชีวิต ร่างกาย หรือทรัพย์สิน หรือมีเหตุอันควรเชื่อได้ว่ามีการกระทำที่มีความรุนแรงกระทบต่อความมั่นคงของรัฐ ความปลอดภัยในชีวิตหรือทรัพย์สินของรัฐหรือบุคคล และมีความจำเป็นที่จะต้องเร่งแก้ไขปัญหาให้ยุติได้อย่างมีประสิทธิภาพและทันท่วงที ให้นายกรัฐมนตรีโดยความเห็นชอบของคณะรัฐมนตรีมีอำนาจประกาศให้สถานการณ์ฉุกเฉินนั้นเป็นสถานการณ์ที่มีความร้ายแรง และให้นำความในมาตรา 5 และมาตรา 6 วรรคสอง มาใช้บังคับโดยอนุโลม

เมื่อมีประกาศตามวรรคหนึ่งแล้ว นอกจากอำนาจตามมาตรา 7 มาตรา 8 มาตรา 9 และมาตรา 11 ให้นายกรัฐมนตรีมีอำนาจดังต่อไปนี้ด้วย

(5) ประกาศให้พนักงานเจ้าหน้าที่มีอำนาจออกคำสั่งตรวจสอบจดหมาย หนังสือ สิ่งพิมพ์ โทรเลข โทรศัพท์ หรือการสื่อสารด้วยวิธีการอื่นใด ตลอดจนการสั่งระงับหรือยับยั้งการติดต่อหรือการสื่อสารใด เพื่อป้องกันหรือระงับเหตุการณ์ร้ายแรง โดยต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยการสอบสวนคดีพิเศษโดยอนุโลม

มาตรา 16 ข้อกำหนด ประกาศ คำสั่ง หรือการกระทำตามพระราชกำหนดนี้ไม่อยู่ในบังคับของกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง และกฎหมายว่าด้วยการจัดตั้งศาลปกครองและวิธีพิจารณาคดีปกครอง

มาตรา 17 พนักงานเจ้าหน้าที่และผู้มีอำนาจหน้าที่เช่นเดียวกับพนักงานเจ้าหน้าที่ตามพระราชกำหนดนี้ไม่ต้องรับผิดทั้งทางแพ่ง ทางอาญา หรือทางวินัย เนื่องจากการปฏิบัติหน้าที่ในการระงับหรือป้องกันการกระทำผิดกฎหมาย หากเป็นการกระทำที่สุจริต ไม่เลือกปฏิบัติ และไม่

เกินสมควรแก่เหตุหรือไม่เกินกว่ากรณีจำเป็น แต่ไม่ตัดสิทธิผู้ได้รับความเสียหายที่จะเรียกร้องค่าเสียหายจากทางราชการตามกฎหมายว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่

การสอดส่องเพื่อวัตถุประสงค์ในการบังคับใช้กฎหมาย

มีกฎหมาย 6 ฉบับที่ให้อำนาจในการสอดส่องข้อมูลและการสื่อสาร เพื่อวัตถุประสงค์ในการบังคับใช้กฎหมายและการดำเนินคดี ซึ่งกฎหมายเหล่านั้นมุ่งจัดการความผิดที่แตกต่างกันไป ดังนี้

1) พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 (พ.ร.บ. ฟอกเงินฯ)

มาตรา 46 ในกรณีที่มีพยานหลักฐานตามสมควรว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน พนักงานเจ้าหน้าที่ซึ่งเลขาธิการมอบหมายเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลแพ่ง เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชี ข้อมูลทางการสื่อสาร หรือข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็ได้

ในกรณีตามวรรคหนึ่ง ศาลจะสั่งอนุญาตให้พนักงานเจ้าหน้าที่ผู้ยื่นคำขอดำเนินการโดยใช้เครื่องมือหรืออุปกรณ์ใด ๆ ตามที่เห็นสมควรก็ได้ แต่ทั้งนี้ให้อนุญาตได้คราวละไม่เกินเก้าสิบวัน

เมื่อศาลได้สั่งอนุญาตตามความในวรรคหนึ่งหรือวรรคสองแล้ว ผู้เกี่ยวข้องกับบัญชีข้อมูลทางการสื่อสาร หรือข้อมูลคอมพิวเตอร์ตามคำสั่งดังกล่าว จะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้

2. พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 เพิ่มโดยพระราชบัญญัติป้องกันและปราบปรามยาเสพติด (ฉบับที่ 4) พ.ศ. 2545 (พ.ร.บ. ปราบปรามยาเสพติดฯ) มาตรา 14 จัตวา

3. พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 (พ.ร.บ. การสอบสวนคดีพิเศษ) มาตรา 25

4. พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 (พ.ร.บ.ค้ามนุษย์ฯ) มาตรา 30

5. พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 (พ.ร.บ.อาชญากรรมข้ามชาติฯ) มาตรา 17

โดยกฎหมายลำดับที่ 2 – 5 มีรูปแบบการเขียนกฎหมายทำนองเดียวกัน จึงขอยกมาเฉพาะรูปแบบการเขียน ดังนี้

มาตรา.....ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิด (.....ความผิดตามกฎหมายแต่ละฉบับ..) (...พนักงานเจ้าหน้าที่ที่รับผิดชอบกฎหมายแต่ละฉบับ...) ซึ่งได้รับอนุมัติจาก (...หัวหน้าหน่วยงานที่สังกัด เช่น อธิบดี...เลขาธิการ.. ผู้ว่าราชการจังหวัด...ผู้บัญชาการตำรวจแห่งชาติ...อัยการสูงสุด.. ขึ้นอยู่กับกฎหมายแต่ละฉบับกำหนด) เป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญา (พ.ร.บ.ค้ามนุษย์ฯ ให้ยื่นต่อศาลอาญาหรือศาลจังหวัดที่มีเขตอำนาจ) เพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

(1) มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิด (.....ความผิดตามกฎหมายแต่ละฉบับ..)

(2) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิด (.....ความผิดตามกฎหมายแต่ละฉบับ..) จากการเข้าถึงข้อมูลข่าวสารดังกล่าว

(3) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวันโดยกำหนดเงื่อนไขใด ๆ ก็ได้ และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อพนักงานสอบสวนคดีพิเศษได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

บรรดาข้อมูลข่าวสารที่ได้มาตามวรรคหนึ่ง ให้เก็บรักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษซึ่งได้รับอนุญาตตามวรรคหนึ่ง และให้ใช้ประโยชน์ในการสืบสวนหรือใช้เป็นพยานหลักฐานเฉพาะในการดำเนินคดีพิเศษดังกล่าวเท่านั้น ส่วนข้อมูลข่าวสารอื่นให้ทำลายเสียทั้งสิ้น ทั้งนี้ ตามข้อบังคับที่ (.....ส่วนใหญ่จะเป็นคณะกรรมการตามกฎหมายนั้น ๆ..หรือรัฐมนตรี...หรืออัยการสูงสุด..) กำหนด

6. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

มาตรา 18 ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดหรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวนอาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริงดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่รีบรวบรวมข้อเท็จจริงและหลักฐานแล้วแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (1) (2) และ (3) ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงานเจ้าหน้าที่กำหนดซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่ ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดระยะเวลาที่ต้องดำเนินการที่เหมาะสมกับประเภทของผู้ให้บริการก็ได้

มาตรา 19 การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) และ (8) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

<u>ข้อสังเกต</u>

1) การสั่งให้ผู้ให้บริการส่งมอบข้อมูลจราจรทางคอมพิวเตอร์ที่เก็บรักษาไว้ เพื่อประโยชน์ในการสืบสวนและสอบสวนนั้น ตาม พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 19 ไม่ได้กำหนดให้ต้องขอต่อศาลก่อน

2) พ.ร.บ.คอมพิวเตอร์ฯ กำหนดอำนาจของพนักงานเจ้าหน้าที่ในการสั่งให้ผู้ให้บริการส่งมอบข้อมูลจราจรทางคอมพิวเตอร์ไว้ค่อนข้างกว้าง ซึ่งนอกจากจะเพื่อประโยชน์ในการสืบสวนและสอบสวนความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ แล้ว ยังมีความผิดอาญาตามกฎหมายอื่นอีก

ข้อกำหนดของกฎหมายดังกล่าว จึงอาจเปิดช่องให้มีการใช้ข้อมูลที่ผู้บริการเก็บรักษาไว้นั้น ในวัตถุประสงค์ในการสอดส่องได้

การสอดส่องเพื่องานข่าวกรองหรือเชิงป้องกัน

พบว่ามีกฎหมายที่ให้อำนาจการสอดส่องเพื่องานข่าวกรองหรือเชิงป้องกันอย่างน้อย 2 ฉบับ

<u>1) พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 (พ.ร.บ.ข่าวกรองฯ)</u>

มาตรา 6 เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามมาตรา 5 สำนักข่าวกรองแห่งชาติอาจสั่งให้หน่วยงานของรัฐหรือบุคคลใดส่งข้อมูลหรือเอกสารที่มีผลกระทบต่อความมั่นคงแห่งชาติ

ภายในระยะเวลาที่ผู้อำนวยการกำหนด หากหน่วยงานของรัฐหรือบุคคลดังกล่าวไม่ส่งข้อมูลหรือเอกสารภายในกำหนดเวลาโดยไม่มีเหตุอันสมควร ให้สำนักข่าวกรองแห่งชาติรายงานต่อนายกรัฐมนตรีเพื่อพิจารณาสั่งการตามที่เห็นสมควรต่อไป

ในกรณีที่มีความจำเป็นต้องได้มาซึ่งข้อมูลหรือเอกสารอันเกี่ยวกับการข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการสื่อสาร หรือการรักษาความปลอดภัยฝ่ายพลเรือน สำนักข่าวกรองแห่งชาติอาจดำเนินการด้วยวิธีการใด ๆ รวมทั้งอาจใช้เครื่องมืออิเล็กทรอนิกส์ เครื่องมือทางวิทยาศาสตร์ เครื่องโทรคมนาคม หรือเทคโนโลยีอื่นใด เพื่อให้ได้มาซึ่งข้อมูลหรือเอกสารดังกล่าวได้ ทั้งนี้ หลักเกณฑ์ วิธีการ และเงื่อนไขในการดำเนินการให้เป็นไปตามระเบียบที่ผู้อำนวยการกำหนดโดยความเห็นชอบของนายกรัฐมนตรี โดยระเบียบดังกล่าวอย่างน้อยต้องกำหนดให้มีการบันทึกรายละเอียดขั้นตอนการดำเนินการโดยเจ้าหน้าที่ผู้รับผิดชอบ เหตุผลความจำเป็น วิธีการ บุคคลที่ได้รับผลกระทบหรืออาจได้รับผลกระทบ และระยะเวลาในการดำเนินการ รวมทั้งวิธีการป้องกัน แก้ไข และเยียวยาผลกระทบต่อบุคคลภายนอกที่ไม่เกี่ยวข้อง

การดำเนินการตามมาตรานี้ หากได้กระทำตามหน้าที่และอำนาจโดยสุจริตตามสมควรแก่เหตุแล้ว และเป็นไปเพื่อประโยชน์ด้านความมั่นคงหรือการป้องกันภัยสาธารณะ ให้ถือว่าเป็นการกระทำโดยชอบด้วยกฎหมาย

ทั้งนี้ การดำเนินการเป็นไปตามระเบียบสำนักข่าวกรองแห่งชาติว่าด้วยการได้มาซึ่งข้อมูลหรือเอกสารอันเกี่ยวกับการข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการสื่อสาร หรือการรักษาความปลอดภัยฝ่ายพลเรือน พ.ศ. 2563 ซึ่งมีประเด็นที่น่าสนใจดังนี้

- การปฏิบัติการข่าวกรอง อาจดำเนินการได้ทั้งโดยทางลับ และทางเปิด โดยบุคคล หรือโดยใช้เครื่องมือทางเทคนิค
- วัตถุประสงค์ของงานข่าวกรอง คือ เพื่อให้ได้มาซึ่งข้อมูล หลักฐานในการป้องกัน ยับยั้ง หรือจัดการภัยคุกคามอันอาจกระทบต่อความมั่นคงแห่งชาติ หรือเพื่อรักษาไว้ซึ่งผลประโยชน์แห่งชาติ ซึ่ง “ภัยคุกคาม” ในที่นี้หมายถึง ระเบียบกำหนดนิยามว่าหมายถึง ภัยจากการจารกรรม การบ่อนทำลาย การก่อวินาศกรรม การก่อการร้าย รวมถึงภัยทางไซเบอร์ อาชญากรรมข้ามชาติ หรือภัยอื่นใดอันมีลักษณะของความเคลื่อนไหวหรือพฤติกรรมที่อาจส่งผลกระทบต่อความมั่นคงหรือผลประโยชน์แห่งรัฐ
- การปฏิบัติการข่าวกรองต้องคำนึงถึงผลกระทบต่อการปฏิบัติงานซึ่งมีลักษณะเป็นความลับและความสมดุลระหว่างประโยชน์ด้านความมั่นคงของชาติกับสิทธิ

เสรีภาพของบุคคลเป็นสำคัญ และต้องระมัดระวังมิให้การปฏิบัติหน้าที่ส่งผลกระทบต่อสิทธิหรือเสรีภาพของบุคคลจนเกินสมควร

- อำนาจในการอนุญาตปฏิบัติการข่าวกรองเป็นอำนาจของผู้อำนวยการสำนักข่าวกรองแห่งชาติหรือรองผู้อำนวยการซึ่งผู้อำนวยการมอบหมายมีอำนาจอนุญาต
- การขออนุญาตต้องทำเป็นหนังสือ และมีรายละเอียดตามที่กำหนด เช่น การบรรยายเกี่ยวกับข่าวกรองที่ประสงค์จะขออนุญาต ซึ่งรวมถึงขั้นตอนการดำเนินการ ระยะเวลาและวิธีการในการดำเนินการ ข้อมูลของเป้าหมายที่จะดำเนินการต่อ เหตุจำเป็นที่ต้องปฏิบัติการข่าวกรอง การปฏิบัติการข่าวกรองที่กระทบสิทธิเสรีภาพของประชาชนอย่างน้อยที่สุด บุคคลที่ได้รับผลกระทบหรืออาจได้รับผลกระทบ วิธีจัดเก็บและทำลายข้อมูล เป็นต้น ทั้งนี้ หากเป็นกรณีเร่งด่วน อาจปฏิบัติการไปพรางก่อนเท่าที่จำเป็นแล้วรีบรายงานผู้บังคับบัญชา
- การพิจารณาอนุญาติปฏิบัติการข่าวกรอง ต้องมีเหตุควรเชื่อได้ว่าการปฏิบัติการข่าวกรองนั้นจะเป็นไปเพื่อทราบถึงความมุ่งหมาย กำลังความสามารถ และความเคลื่อนไหว รวมทั้งวิถีทางของบุคคลกลุ่มบุคคล หรือองค์กรใดทั้งภายในประเทศ และต่างประเทศ ที่อาจกระทำการเป็นภัยคุกคาม หรือมีพฤติการณ์เป็นภัยคุกคาม หรือเพื่อต่อต้านการกระทำของบุคคล กลุ่มบุคคล หรือองค์กรใด ที่มุ่งหมายจะให้ได้ไปซึ่งความลับของชาติ หรือทำลายความมั่นคงแห่งชาติ
- ผู้ได้รับผลกระทบหรือได้รับความเสียหายต่อร่างกาย ทรัพย์สิ ความเป็นส่วนตัว หรือด้านอื่นๆ จากการปฏิบัติการข่าวกรอง มีสิทธิร้องเรียนต่อคณะกรรมการ ณะกรรมการพิจารณาเยียวยาผลกระทบจากการปฏิบัติการข่าวกรอง ประกอบด้วย รองผู้อำนวยการสำนักงานข่าวกรองแห่งชาติซึ่งผู้อำนวยการมอบหมายเป็นประธานกรรมการ ผู้บังคับบัญชาระดับผู้อำนวยการกองขึ้นไปซึ่งผู้อำนวยการสำนักงานข่าวกรองแห่งชาติแต่งตั้งอีกไม่เกินห้าคนเป็นกรรมการ
- การเก็บรักษาข้อมูล ให้ผู้บังคับบัญชาเป็นนายทะเบียน หน้าที่ในการควบคุมเก็บรักษาทะเบียนข้อมูล เอกสาร หรือหลักฐานเกี่ยวกับการปฏิบัติการข่าวกรอง
- ข้อมูลเมื่อหมดความจำเป็นแล้ว ให้ส่งนายทะเบียนเพื่อทำลาย

- เจ้าหน้าที่ที่กระทำการโดยจงใจหรือประมาทเลินเล่ออย่างร้ายแรงนอกวัตถุประสงค์ในการปฏิบัติการข่าวกรองตามที่ได้รับมอบหมาย เพื่อแสงหาประโยชน์อันมิชอบสำหรับตนเองหรือผู้อื่น ย่อมไม่ได้รับการคุ้มครองตามกฎหมาย

2) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (พ.ร.บ.ความมั่นคงไซเบอร์ฯ)

มาตรา 66 ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ในเรื่องดังต่อไปนี้

(2) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนาหรือสกัดคัดกรองข้อมูลสารสนเทศ หรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้อง หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

ในการดำเนินการตาม (2) (3) และ (4) ให้ กกม. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉิน และให้ศาลพิจารณาไต่สวนโดยเร็ว

มาตรา 68 ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ คณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้โดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากการดำเนินการดังกล่าว ให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว

ในกรณีร้ายแรงหรือวิกฤติเพื่อประโยชน์ในการป้องกัน ประเมินผล รับมือ ปราบปราม ระงับ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการโดยความเห็นชอบของคณะกรรมการหรือ กกม. มีอำนาจขอข้อมูลที่เป็นปัจจุบันและต่อเนื่องจากผู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ โดยผู้นั้นต้องให้ความร่วมมือและให้ความสะดวกแก่คณะกรรมการหรือ กกม. โดยเร็ว

ตารางที่ 5.1 สรุปของเขตการใช้อำนาจสอดส่องตามกฎหมายฉบับต่าง ๆ ของประเทศไทย

กฎหมาย	เงื่อนไข/วัตถุประสงค์	วิธีการ	เกณฑ์ในการพิจารณา	กลไกตรวจสอบ/การเยียวยา
กฎอัยการศึก	เมื่อประกาศใช้กฎอัยการศึก	ตรวจ/เข้าถึงข้อมูลการสื่อสารด้วยตัวเอง		● ไม่ได้อนุญาตโดยกลไกตุลาการ ● มีข้อจำกัดเรื่องการเข้าถึงการเยียวยา
พ.ร.บ.ฉุกเฉินฯ	เมื่อประกาศสถานการณ์ฉุกเฉินที่มีความร้ายแรง เพื่อป้องกันหรือระงับเหตุการณ์ร้ายแรง	ออกคำสั่งให้ตรวจสอบการสื่อสาร	ตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายการสอบสวนคดีพิเศษ	● อนุญาตโดยศาล ● มีข้อจำกัดความรับผิดของเจ้าหน้าที่ ● เรียกร้องค่าเสียหายได้ตามกฎหมายว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่
พ.ร.บ. ฟอกเงินฯ	เพื่อดำเนินคดีความผิดฐานฟอกเงิน	เข้าถึงข้อมูลคอมพิวเตอร์	● มีพยานหลักฐานตามสมควร	อนุญาตโดยศาลแพ่ง
พ.ร.บ. ปราบปรามยาเสพติดฯ	เพื่อดำเนินคดีเกี่ยวกับยาเสพติด	ให้ได้มาซึ่งข้อมูลข่าวสารที่ส่งทางคอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสารสื่อ	● อาศัยเหตุอันควรเชื่อ ● มีการกำหนดหลักเกณฑ์การพิจารณาสำหรับศาล	อนุญาตโดยศาล
พ.ร.บ.ค้ามนุษย์ฯ	เพื่อดำเนินคดีความผิดฐานค้ามนุษย์			

กฎหมาย	เงื่อนไข/วัตถุประสงค์	วิธีการ	เกณฑ์ในการพิจารณา	กลไกตรวจสอบ/การเยียวยา
พ.ร.บ.อาชญากรรมข้ามชาติฯ	เพื่อดำเนินคดีความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ	อิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด	● มีหลักประกันการตรวจสอบอื่น ๆ เช่น การรายงาน	
พ.ร.บ. การสอบสวนคดีพิเศษ	เพื่อดำเนินคดีพิเศษ			
พ.ร.บ. คอมพิวเตอร์ฯ	เพื่อดำเนินคดีความผิดตาม พ.ร.บ. คอมพิวเตอร์ฯ และความผิดอาญาตามกฎหมายอื่นที่เกี่ยวข้อง	สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่เก็บรักษาไว้	● อาศัยเหตุอันควรเชื่อ ● แต่กำหนดให้คำร้องต้องระบุรายละเอียดต่าง ๆ รวมถึงเหตุที่ต้องใช้อำนาจ ● มีหลักประกันการตรวจสอบอื่น ๆ เช่น การรายงาน	ไม่ต้องได้รับอนุญาตจากศาล
		● ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ฯ ● ถอดรหัสลับของข้อมูลคอมพิวเตอร์		อนุญาตโดยศาล
พ.ร.บ.ข่าวกรองฯ	เพื่องานข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการสื่อสาร หรือการรักษาความปลอดภัยฝ่ายพลเรือน	ดำเนินการด้วยวิธีการใด ๆ รวมทั้งอาจใช้เครื่องมืออิเล็กทรอนิกส์ เครื่องมือทางวิทยาศาสตร์ เครื่อง	ไม่ได้กำหนดในกฎหมายหลัก แต่กำหนดในระเบียบ	● ไม่ต้องขออนุญาตจากศาล ● แต่อนุญาตโดยผู้อำนวยการสำนักงานข่าวกรองแห่งชาติ

กฎหมาย	เงื่อนไข/วัตถุประสงค์	วิธีการ	เกณฑ์ในการพิจารณา	กลไกตรวจสอบ/การเยียวยา
		โทรคมนาคม หรือเทคโนโลยีอื่นใด เพื่อให้ได้มาซึ่งข้อมูลหรือเอกสาร		● มีข้อจำกัดความรับผิดของเจ้าหน้าที่ทั้งทางแพ่ง ทางอาญา หรือทางวินัย
พ.ร.บ.ความมั่นคงไซเบอร์ฯ	เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์	อาศัยเหตุอันควรเชื่อ	อนุญาตโดยศาลที่มีเขตอำนาจ
	กรณีที่เป็นเหตุจำเป็นเร่งด่วนและเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ			ไม่ต้องยื่นคำร้องต่อศาล แต่ให้แจ้งรายละเอียดการดำเนินการต่อศาลในภายหลัง

5.5 สรุปส่งท้าย

จากการศึกษากรอบหลักการสิทธิมนุษยชนที่ปรากฏตามกฎหมายสิทธิมนุษยชนระหว่างประเทศ โดยเฉพาะ ICCPR และแนวทางการตีความโดยผู้เชี่ยวชาญด้านสิทธิมนุษยชน พบว่า ความเป็นส่วนตัวของการสื่อสาร ถือเป็นหนึ่งในประเด็นสิทธิในความปเนส่วนตัวที่ถูกรับรองตามข้อ 17 ของ ICCPR ซึ่งห้ามมิให้มีการแทรกแซงสิทธิดังกล่าวโดยไม่ชอบด้วยกฎหมายหรือโดยพลการ ดังนั้น การสอดส่องการสื่อสาร โดยหลักแล้วจึงเป็นสิ่งต้องห้าม เว้นแต่เป็นไปตามบททดสอบสามส่วน คือ ความชอบด้วยกฎหมาย (กำหนดโดยกฎหมาย) มีวัตถุประสงค์ที่ชอบธรรม (เช่น เพื่อดำเนินกระบวนการยุติธรรมทางอาญา) และมีความจำเป็นและได้สัดส่วน (กระทบสิทธิน้อยที่สุด กำหนดเป้าหมายเฉพาะเจาะจง/เป็นรายกรณี) ตลอดจนมีกลไกกำกับดูแลที่อิสระในการอนุญาตและกำกับดูแลการดำเนินมาตรการ ซึ่งโดยหลักแล้วกลไกดังกล่าวจะเป็นองค์กรที่ใช้อำนาจตุลาการซึ่งมีความเป็นอิสระ เป็นกลาง และมีอำนาจตามกฎหมาย อย่างไรก็ดี มีคำแนะนำว่ากลไกการตรวจสอบของฝ่ายบริหาร นิติบัญญัติ และสาธารณะอื่น ๆ ก็มีความจำเป็นเช่นกัน นอกจากนี้ เมื่อการสอดส่องนำไปสู่การละเมิดสิทธิมนุษยชน โดยเฉพาะสิทธิในความเป็นส่วนตัว ผู้ได้รับผลกระทบต้อได้รับการเยียวยาที่มีประสิทธิผล ซึ่งเพื่อให้การเยียวยาเป็นไปได้และมีประสิทธิผล การดำเนินการสอดส่องต้องโปร่งใส รวมถึงการแจ้งต่อผู้ที่ตกเป็นเป้าหมายหลังจากการใช้มาตรการเสร็จสิ้นแล้ว ตลอดจนมีการรายงานการใช้มาตรการต่อสาธารณะอย่างต่อเนื่อง

จากกรอบหลักการข้างต้น ผู้วิจัยได้นำมาเป็นกรอบในการศึกษากฎหมายภายในของประเทศไทย ซึ่งพบว่า

กรอบรัฐธรรมนูญของไทยให้การคุ้มครองสิทธิในความเป็นส่วนตัวและการติดต่อสื่อสารไว่อย่างชัดเจน (มาตรา 33 และ 35)

ประเทศไทยมีกฎหมายระดับพระราชบัญญัติที่ให้การคุ้มครองความเป็นส่วนตัวในการสื่อสารและข้อมูล อย่างน้อย 2 ฉบับ คือ พ.ร.บ. กสทช.ฯ (มาตรา 27 (13) และ 32) ที่อำนาจ กสทช. ในการคุ้มครองความเป็นส่วนตัวของประชาชนจากการถูกละเมิดโดยการประกอบกิจการโทรคมนาคม และประเทศไทยมีกฎหมายเฉพาะในการคุ้มครองข้อมูลส่วนบุคคล (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562) แต่กฎหมายดังกล่าวยกเว้นไม่นำมาใช้กับหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งนอกจากเพื่อการบังคับใช้กฎหมายแล้ว การสอดส่องมักอยู่บนพื้นฐานของเหตุผลด้านความมั่นคง โดยเฉพาะหน่วยงานด้านข่าวกรอง

ประเทศไทยมีกฎหมายหลายฉบับที่ให้อำนาจรัฐในการสอดส่องการสื่อสารและรวบรวมข้อมูลของประชาชน ด้วยวัตถุประสงค์และขอบเขตที่แตกต่างกันไป โดยผู้วิจัยจำแนกได้เป็น 4 ประเภท ดังนี้

<u>กฎหมายที่ให้อำนาจสอดส่องในสถานการณ์พิเศษ</u> ได้แก่ กฎอัยการศึก ซึ่งไม่มีหลักประกันการตรวจสอบการใช้อำนาจและจำกัดการเข้าถึงการเยียวยาความเสียหายอันเกิดจากการใช้อำนาจของเจ้าหน้าที่ทหาร

ส่วนกฎหมายอีกฉบับคือ พ.ร.ก. ฉุกเฉินฯ แม้จะกำหนดให้ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยการสอบสวนคดีพิเศษ ซึ่งมีหลักประกันเชิงกระบวนการที่ค่อนข้างดี แต่ขอบเขตของการบังคับใช้ตาม พ.ร.ก. ฉุกเฉินฯ นั้น กำหนดให้ใช้อำนาจเพื่อป้องกันและระงับ “เหตุการณ์ร้ายแรง” ซึ่งไม่มีนิยามและตีความได้กว้างขวาง

<u>กฎหมายที่ให้อำนาจสอดส่องเพื่อวัตถุประสงค์ในการบังคับใช้กฎหมายหรือการดำเนินคดี</u>

กฎหมายส่วนใหญ่กำหนดหลักประกันการคุ้มครองสิทธิไว้คล้ายกัน แม้จะมีรายละเอียดแตกต่างกันบ้างก็ตาม และข้อกำหนดทางกฎหมายค่อนข้างสอดคล้องกับกรอบหลักการสิทธิความเป็นส่วนตัวในมิติการสอดส่องการสื่อสาร กล่าวคือ

ความชอบด้วยกฎหมาย : มีการกำหนดอำนาจการสอดส่องโดยกฎหมายอย่างชัดเจน แน่นอน คาดหมายได้ อย่างไรก็ดี มีกฎหมายบางฉบับที่ให้อำนาจการสอดส่องสำหรับขอบเขตของความผิดที่ค่อนข้างกว้าง โดยเฉพาะ พ.ร.บ. การสอบสวนคดีพิเศษฯ ซึ่งคดีพิเศษนั้นกินความครอบคลุมความผิดตามกฎหมายกว่า 20 ฉบับ และสามารถพิจารณาเพิ่มคดีพิเศษได้อีกในภายหลัง นอกจากนี้ยังมี พ.ร.บ. คอมพิวเตอร์ฯ ซึ่งนอกจากจะใช้กับความผิดตาม พ.ร.บ. คอมพิวเตอร์ฯ โดยตรงแล้ว ยังอาจใช้กับความผิดทางอาญาตามกฎหมายอื่นที่เกี่ยวข้องกับคอมพิวเตอร์ด้วย

วัตถุประสงค์ที่ชอบธรรม : กฎหมายที่ให้อำนาจสอดส่อง จำนวนหนึ่งมีวัตถุประสงค์เพื่อจัดการกับคดีอาญาที่ร้ายแรง เช่น ค้ามนุษย์ องค์กรอาชญากรรมข้ามชาติ เป็นต้น ซึ่งอาจถือว่าเป็นวัตถุประสงค์ที่ชอบธรรม แต่มีกฎหมายบางฉบับดังที่กล่าวไปแล้วว่าสามารถนำไปใช้กับขอบเขตความผิดที่ค่อนข้างกว้าง เช่น พ.ร.บ. การสอบสวนคดีพิเศษฯ และ พ.ร.บ. คอมพิวเตอร์ฯ

ความจำเป็นและได้สัดส่วน : กฎหมายทุกฉบับกำหนดเงื่อนไขของการใช้อำนาจสอดส่องไว้ กล่าวคือ การใช้อำนาจสอดส่องต้องอาศัยความสงสัยหรือความเชื่อล่วงหน้าว่ากระทำความผิด และถูกใช้โดยกำหนดเป้าหมายเป็นรายกรณี โดยผ่านการอนุญาตจากกลไกตุลาการ และกฎหมายหลายฉบับ (4 ฉบับ) มีการกำหนดเกณฑ์การพิจารณาตามหลักความจำเป็นและได้สัดส่วน และมีการกำหนดระยะเวลาการใช้มาตรการไว้ แม้อาจจะนานถึง 90 วันก็ตาม อีกทั้ง กฎหมายยังกำหนดให้ศาลมีอำนาจกำหนดเงื่อนไขการใช้อำนาจสอดส่องได้ สามารถเปลี่ยนแปลงคำสั่งได้เมื่อพฤติการณ์เปลี่ยนไป และกำหนดให้เจ้าหน้าที่ผู้ใช้อำนาจสอดส่องต้องรายงานการดำเนินการต่อศาล ตลอดจนมีการกำหนดเงื่อนไขของเก็บรักษาข้อมูลเท่าที่จำเป็น และทำลายข้อมูลส่วนที่ไม่เกี่ยวข้อง

<u>กฎหมายที่ให้อำนาจสอดส่องเพื่อวัตถุประสงค์ด้านข่าวกรองหรือเชิงป้องกัน</u>

ความน่ากังวลของกฎหมายในส่วนนี้ โดยเฉพาะพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 คือ กฎหมายแม่บทไม่ได้กำหนดอย่างชัดเจนเกี่ยวกับขอบเขตการใช้อำนาจ และไม่ได้กำหนดให้อำนาจตรวจสอบแก่กลไกที่เป็นอิสระ โดยรายละเอียดหลักเกณฑ์ วิธีการ และเงื่อนไขถูกนำไปกำหนดในกฎหมายลำดับรอง ซึ่งประเด็นนี้

อาจไม่สอดคล้องกับบททดสอบของความชอบด้วยกฎหมาย ในเรื่องความชัดเจน แน่นอน คาดหมายได้ และเปิดเผยต่อสาธารณะ

เมื่อพิจารณาจากเนื้อหาในระเบียบแล้ว พบว่า ระเบียบระบุเกี่ยวกับการปฏิบัติการข่าวกรองแบบลับ และกำหนดให้ผู้อำนวยการสำนักงานข่าวกรองซึ่งเป็นหัวหน้าหน่วยงานนั้นเองเป็นผู้มีอำนาจอนุญาตให้ดำเนินการปฏิบัติการข่าวกรอง ซึ่งรวมถึงการสอดส่องด้วย และการกำกับดูแลการดำเนินการส่วนใหญ่อยู่ภายใต้ผู้บังคับบัญชาภายในหน่วยงาน ดังนั้น กฎเกณฑ์เหล่านี้จึงไม่สอดคล้องกับกรอบหลักการสำหรับการอนุญาตให้สอดส่องที่ถูกยอมรับตามหลักการสิทธิมนุษยชนสากล

ข้อสังเกต

ประเด็นเรื่องการสอดส่องแบบลับและการกลไกรตรวจสอบถ่วงดุลจากภายนอกที่เป็นอิสระโดยเฉพาะฝ่ายตุลาการนั้น ย่อมทำให้ยากยิ่งขึ้นที่จะตรวจสอบว่าการใช้มาตรการสอดส่องเหล่านั้นดำเนินการสอดคล้องกับกฎเกณฑ์ทางกฎหมายที่กำหนดไว้หรือไม่ อีกทั้ง การสอดส่องแบบปิดลับและไม่โปร่งใส ย่อมทำให้ผู้ได้รับผลกระทบยากที่จะเข้าถึงการเยียวยา เพราะไม่รู้ว่าหน่วยงานใดต้องรับผิดชอบ ดังตัวอย่างที่มีการรายงานเมื่อไม่นานมานี้ คือ กรณีการใช้สปายแวร์ที่ชื่อเพกาซัส (Pegasus) เพื่อเจาะโทรศัพท์ล่วงข้อมูลของนักปกป้องสิทธิมนุษยชน นักกิจกรรมทางการเมือง และนักการเมืองฝ่ายตรงข้าม โดยแม้จะมีข้อมูลบ่งชี้ว่าสปายแวร์ตัวนี้พัฒนาโดยบริษัท NSO Group ซึ่งขายให้รัฐบาลเท่านั้น[361] แต่ก็ยากสำหรับผู้ได้รับผลกระทบในการหาหลักฐานว่าหน่วยงานของรัฐใดใช้สปายแวร์ตัวนี้เพื่อสอดส่องพวกเขา เพราะที่ผ่านมารัฐเองไม่เคยโปร่งใสเกี่ยวกับการซื้อและการใช้เทคโนโลยีสอดส่องเหล่านี้ และระบอบการสอดส่องตามกฎหมายของไทย แม้กฎหมายหลายฉบับจะมีหลักประกันเชิงกระบวนการที่ดี แต่สิ่งที่ขาดไปคือหลักประกันความโปร่งใสในการใช้มาตรการสอดส่องตามกฎหมายเหล่านั้น กฎหมายไทยไม่ได้กำหนดให้ต้องมีการแจ้งมาตรการสอดส่องแก่ผู้ที่ตกเป็นเป้าหมาย ไม่มีกำหนดให้การรายงานต่อสาธารณะหรือรัฐสภาเกี่ยวกับมาตรการสอดส่องที่ถูกใช้ ดังนั้น ข้อท้าทายเหล่านี้จะต้องมีการหารือในวงกว้างต่อไปเพื่อให้มาตราการสอดส่องการสื่อสารของไทยเป็นไปตามความคาดหวังของกรอบสิทธิมนุษยชนสากลมากที่สุด

[361] iLaw, ปรสิตติดโทรศัพท์ : การส่งเพกาซัสติดตามนักการเมืองก้าวหน้า-ก้าวไกล, 21 กรกฎาคม 2565, https://freedom.ilaw.or.th/node/1090

บทที่ 6

บทสรุปและข้อเสนอแนะ

ส่วนนี้เป็นการนำเสนอบทสรุปตามวัตถุประสงค์การวิจัยที่กำหนดไว้ ได้แก่ การศึกษากรอบสิทธิมนุษยชนระหว่างประเทศในการส่งเสริมและคุ้มครองสิทธิมนุษยชนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์ (สิทธิดิจิทัล) และวิเคราะห์สถานการณ์ของประเทศไทย โดยเน้นประเด็นสิทธิทางอินเทอร์เน็ต เสรีภาพในการแสดงออก และสิทธิในความเป็นส่วนตัว พร้อมทั้งจัดทำข้อเสนอแนะในการส่งเสริมและคุ้มครองสิทธิดังกล่าว ดังนี้

6.1 ว่าด้วยกรอบสิทธิมนุษยชนในยุคดิจิทัล

ประเด็นสิทธิมนุษยชนกับเทคโนโลยีดิจิทัลได้รับความสนใจมากขึ้น โดยเฉพาะหลังจากมีการตั้งคำถามต่อกลไกการกำกับดูแลหรืออภิบาลอินเทอร์เน็ต (Internet Governance) ในระดับโลก ประกอบกับประเด็นข้อท้าทายใหม่ ๆ ที่เป็นผลมาจากพลังของอินเทอร์เน็ต โดยเฉพาะคุณสมบัติที่เปิดกว้างทั่วโลกและข้ามพรมแดน ทำให้เกิดข้อท้าทายต่อแนวคิดและกฎระเบียบแบบเดิม โดยเฉพาะแนวคิดเกี่ยวกับชาติ ตัวตนและความเป็นพลเมือง ทำให้เกิดแนวคิด “ตัวตนดิจิทัล (The Digital persona)” และชาติดิจิทัล (The Digital Nation) หรือชาติไซเบอร์ (cybernation) ซึ่งสิ่งเหล่านี้นำไปสู่คำถามเกี่ยวกับหลักการสิทธิมนุษยชนสำหรับพื้นที่หรือสภาพแวดล้อมดิจิทัล

กรอบสิทธิมนุษยชนที่ใช้อยู่ในปัจจุบัน เกิดขึ้นภายหลังการจัดทำปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights - UDHR) ในปี ค.ศ. 1948 หรือ พ.ศ. 2491 หรือเมื่อเกือบ 80 ปีที่แล้ว ซึ่งในขณะนั้นเทคโนโลยียังไม่ได้พัฒนาก้าวหน้ามากนัก เมื่อกับปัจจุบันที่เทคโนโลยีก้าวล้ำไปมาก ซึ่งความก้าวหน้าดังกล่าวเป็นทั้งพลังในการส่งเสริมและคุ้มครองสิทธิมนุษยชน แต่อีกด้านก็เป็นเหมือนหลุมดำที่นำไปสู่การละเมิดสิทธิมนุษยชน ทั้งโดยปัจเจก บริษัท และรัฐ

แม้ที่ผ่านมา จะมีการหารือเกี่ยวกับประเด็นสิทธิมนุษยชนกับเทคโนโลยี หรือสิทธิมนุษยชนในยุคดิจิทัลค่อนข้างมาก โดยเฉพาะในระดับของสหประชาชาติ อย่างไรก็ดี ไม่ได้มีการเปลี่ยนแปลงหรือมีการนำไปสู่การจัดทำตราสารใหม่ที่รองรับสิทธิมนุษยชนในยุคอินเทอร์เน็ตหรือยุคดิจิทัลเป็นการเฉพาะ สิ่งที่คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติและสมัชชาใหญ่แห่งสหประชาชาติช่วยวางเป็นกรอบของสิทธิมนุษยชนในยุคดิจิทัลก็คือการยืนยันว่า *“สิทธิมนุษยชนที่มีอยู่บนพื้นที่ออฟไลน์ ย่อมมีผลบังคับใช้กับพื้นที่ออนไลน์ด้วย”* ซึ่งโดยทั่วไปเป็นการพิจารณาในบริบทของเสรีภาพในการแสดงออกและสิทธิในความเป็นส่วนตัว

ภาคส่วนต่าง ๆ มีความพยายามในการพัฒนากรอบหลักการที่เฉพาะเจาะจงมากขึ้นสำหรับสิทธิมนุษยชนในสภาพแวดล้อมทางอินเทอร์เน็ตหรือดิจิทัล โดยจากการสำรวจของผู้วิจัยพบว่า มีเอกสารที่ระบุถึงสิทธิอินเทอร์เน็ตและดิจิทัลทั้งโดยตรงและอ้อมมากกว่า 40 ฉบับ ซึ่งส่วนใหญ่เป็นการริเริ่มของภาคประชาสังคมและเวทีของผู้มีส่วนได้เสียหลายฝ่าย รวมถึงกลไกระหว่างรัฐบาลระดับภูมิภาค โดยเฉพาะในภูมิภาคยุโรป และมีรัฐบาลบางแห่งที่พยายามรับรองสิทธิเหล่านี้ในกฎหมายระดับประเทศของตน เช่น บราซิล สเปน เป็นต้น

เอกสารเหล่านั้นกล่าวถึง “สิทธิในอินเทอร์เน็ต (Internet Rights)” และในระยะหลัง ๆ โดยเฉพาะนับตั้งแต่ปี 2557 (ค.ศ. 2014) เริ่มมีการใช้คำว่า “สิทธิดิจิทัล (Digital Rights) มากขึ้น[362]

อย่างไรก็ดี ไม่มีการให้คำนิยาม “สิทธิดิจิทัล” ที่ถูกยอมรับร่วมกันในทางสากล การกำหนดนิยามและขอบเขตสิทธิมนุษยชนสิทธิดิจิทัลนั้น ขึ้นอยู่กับมุมมองและความสนใจของแต่ละองค์กรที่ทำงานเกี่ยวข้องกับประเด็นสิทธิมนุษยชนกับเทคโนโลยีดิจิทัล

เมื่อพิจารณาลงไปในรายละเอียดของเนื้อหาที่ปรากฏในเอกสารฉบับต่าง ๆ พบว่า ส่วนใหญ่ไม่ได้สร้างสิทธิขึ้นมาใหม่ แต่เป็นการกล่าวถึงแนวทางการปรับใช้กรอบหลักการที่มีอยู่แล้วในตราสารสิทธิมนุษยชนระหว่างประเทศให้เข้ากันได้กับบริบทหรือสภาพแวดล้อมดิจิทัลหรืออินเทอร์เน็ต โดยเฉพาะประเด็นเสรีภาพในการแสดงออกและความเป็นส่วนตัว ซึ่งมีการพูดถึงมากในแทบทุกเอกสารที่รวบรวมมา

กล่าวโดยสรุป การกล่าวถึงสิทธิมนุษยชนในยุคดิจิทัล หรือบางครั้งเรียกว่า “สิทธิดิจิทัล” นั้น หมายถึงการปรับใช้กรอบหลักการสิทธิมนุษยชนที่ปรากฏในตราสารสิทธิมนุษยชนระหว่างประเทศให้เข้ากับสภาพแวดล้อมทางดิจิทัลหรืออินเทอร์เน็ต

6.2 สิทธิดิจิทัลในประเทศไทย : ความก้าวหน้า ข้อท้าทายและข้อเสนอแนะ

ในส่วนนี้จะพิจารณาใน 3 ประเด็นหลัก คือ สิทธิทางอินเทอรเน็ต เสรีภาพในการแสดงออก และสิทธิในความเป็นส่วนตัว ทั้งนี้ แม้จะพิจารณาเป็นรายประเด็น แต่ผู้วิจัยไม่ได้แยกสิทธิเหล่านั้นออกจากกัน เพราะตระหนักดีว่าหลักการพื้นฐานของสิทธิมนุษยชนนั้น สิทธิต่าง ๆ ล้วนเชื่อมโยงและสัมพันธ์กัน และแบ่งแยกจากกันไม่ได้

[362] โปรดดู เช่น Charter of Digital Rights (2014) ของ European Digital Rights (EDRi), Carta de derechos digitales (Charter for Digital Rights, 2021) ของรัฐบาลสเปน และ European Declaration on Digital Rights and Principles for the Digital Decade (2022) ที่เสนอโดย European Commission, European Union (EU) เป็นต้น

6.2.1 สิทธิในการเข้าถึงอินเทอร์เน็ต

สถานการณ์

ประเทศไทยยังไม่ได้รับรองให้อินเทอร์เน็ตเป็นสิทธิมนุษยชนหรือสิทธิพลเมืองอย่างชัดเจน แต่จากเนื้อหาของรัฐธรรมนูญ กฎหมาย โดยเฉพาะพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์และกิจการโทรคมนาคม พ.ศ. 2553 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 และ (ฉบับที่ 3) พ.ศ. 2562 (ต่อไปนี้เรียก พ.ร.บ. กสทช.ฯ) และพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 และนโยบายระดับชาติที่เกี่ยวข้อง รวมถึงยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 – 2580) แผนแม่บทภายใต้ยุทธศาสตร์ชาติ แผนปฏิรูปประเทศ แผนแม่บทกิจการโทรคมนาคม ฉบับที่ 2 (พ.ศ. 2562 - 2566) และนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 – 2580) นั้น เป็นกรอบให้หน่วยงานของรัฐ โดยเฉพาะ กสทช. และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ในฐานะหน่วยงานหลักที่มีหน้าที่ในการกำกับดูแลและดำเนินการด้านอินเทอร์เน็ต ในการดำเนินการต่าง ๆ เพื่อประกันการเข้าถึงอินเทอร์เน็ตสำหรับทุกคน โดยมีคุณภาพและราคาไม่แพง

ซึ่งที่ผ่านมาหน่วยงานที่รับผิดชอบก็ดำเนินโครงการต่าง ๆ รวมถึงการปรับปรุงโครงสร้างพื้นฐานทางอินเทอร์เน็ต เพื่อเอื้ออำนวยให้ทุกคนสามารถเข้าถึงอินเทอร์เน็ตได้ และที่ผ่านมาสถานการณ์ผู้ใช้อินเทอร์เน็ตในประเทศไทยก็มีอัตราเพิ่มขึ้นต่อเนื่อง และในแง่ของคุณภาพนั้นก็ค่อนข้างดี

อย่างไรก็ดี ในแง่การเข้าถึง อาจจะยังมีข้อท้าทายในการส่งเสริมการเข้าถึงของประชาชนบางกลุ่ม โดยเฉพาะกลุ่มผู้สูงอายุที่มีอัตราการใช้อินเทอร์เน็ตต่ำกว่ากลุ่มอื่น

และยังมีข้อท้าทายเรื่องราคาหรือความสามารถในการจ่ายได้ (Affordability) โดยเฉพาะราคาของบริการบรอดแบนด์ประจำที่ ซึ่งแม้จะมีแนวโน้มลดลงระหว่างปี 2561 – 2563 แต่ก็ยังสูงกว่าเป้าหมายที่ Broadband Commission กำหนดคือ 2 เปอร์เซ็นต์ของรายได้รวมประชาชาติ (GNI) ต่อเดือนต่อหัว และยังสูงกว่าค่าเฉลี่ยของภูมิภาคเอเชีย-แปรซิฟิก ในปี 2564 ที่มีค่าเฉลี่ยอยู่ที่ 3.08 % ของรายได้มวลรวมประชาชาติ (GNI) ต่อเดือนต่อหัว

นอกจากนี้ ข้าทายทายประการสำคัญ คือ ประเด็นเรื่องของความรู้หรือทักษะในการใช้งาน แม้ประเทศไทยจะให้ความสำคัญกับประเด็นดังกล่าวทั้งในระดับนโยบาย และในระดับของการดำเนินการ ซึ่งก็พบว่ามีหลากหลายหน่วยงานทั้งภาครัฐ ภาคเอกชนภาคประชาสังคม ได้ดำเนินการตามบทบาทหน้าที่ของตนเพื่อส่งเสริมการรู้ดิจิทัล (Digital Literacy) แต่จากข้อมูลการสำรวจที่ผ่าน ๆ พบว่า ทักษะดิจิทัลของประชาชนไทยส่วนใหญ่ยังจำกัดอยู่ในระดับพื้นฐาน (การเข้าใช้งาน การอ่าน การเขียน การโพสต์ข้อความ การแสดงความเห็น) และระดับกลาง (การส่งต่อข้อมูล) เท่านั้นและยังขาดความตระหนักรู้ในการปกป้องตรวจสอบข้อมูลก่อนเชื่อและส่งต่อไปยังผู้อื่น

ข้อเสนอแนะ

1) ในประเด็นการรับรองสิทธิอินเทอร์เน็ต แม้สิทธิทางอินเทอร์เน็ตยังไม่ถูกรับรองอย่างชัดเจนในระดับสากลว่าเป็นสิทธิมนุษยชน ซึ่งในทางการบังคับใช้ได้มีการตีความสิทธิดังกล่าวฐานะตัวเปิดใช้สิทธิมนุษยชนอื่น ๆ โดยเฉพาะเสรีภาพในการแสดงออก อย่างไรก็ดี มีบางรัฐที่มีการรับรองในกฎหมายให้อินเทอร์เน็ตเป็นสิทธิ ดังนั้น สำหรับประเทศไทย จำเป็นต้องมีการหารืออย่างกว้างขวางระหว่างผู้มีส่วนได้เสียหลายฝ่าย ว่าจำเป็นต้องมีการกำหนดให้อินเทอร์เน็ตเป็นสิทธิพลเมืองหรือไม่ เพราะการรับรองอย่างชัดเจนทางรัฐธรรมนูญหรือกฎหมายนั้นย่อมหมายถึงการมีหลักประกันการคุ้มครองที่หนักแน่นและมั่นคงยิ่งขึ้น อีกทั้งการรับรองให้อินเทอร์เน็ตเป็นสิทธิจะทำให้เกิดพันธะผูกพันแก่รัฐมากขึ้น กล่าวคือ รัฐย่อมมีพันธกรณีในเชิงบวกที่จะต้องทำให้สิทธิทางอินเทอร์เน็ตนั้นบรรลุผล ในแง่นี้จะเกี่ยวข้องกับการประกันโครงสร้างพื้นฐานที่ครอบคลุม เพื่อให้ทุกคนเข้าถึงได้ในราคาไม่แพงและมีคุณภาพ ซึ่งเป็นสิ่งที่รัฐบาลไทยดำเนินการได้ดีอยู่แล้วในช่วงระยะเวลาที่ผ่านมา ส่วนอีกมิติหนึ่งคือรัฐจะเกิดพันธกรณีในการที่จะต้องเคารพและคุ้มครองสิทธิเพื่อไม่ให้มีการตัดการเชื่อมต่ออินเทอร์เน็ต ซึ่งประเด็นนี้จะมีเกี่ยวพันกับเสรีภาพในการแสดงออกในพื้นที่ออนไลน์ด้วย

ทั้งนี้ ในมุมมองของงานวิจัยชิ้นนี้ เห็นว่าประเทศไทยควรมีการกำหนดให้อินเทอร์เน็ตเป็นสิทธิพลเมืองอย่างชัดเจนในรัฐธรรมนูญหรือกฎหมาย เพราะปัจจุบันอินเทอร์เน็ตเป็นเหมือนกับปัจจัยสำคัญในการดำรงชีวิตของประชาชน และเป็นประตูสู่การใช้สิทธิมนุษยชนอื่น ๆ จึงมีความสำคัญอย่างยิ่งที่จะประกันสิทธิทางอินเทอร์เน็ตอย่างชัดเจน เพื่อให้เกิดการดำเนินการส่งเสริมสิทธิที่ต่อเนื่องและมีหลักประกันการคุ้มครองที่หนักแน่นยิ่งขึ้น

2) จำเป็นต้องมีการลดช่องว่างในแง่ของความสามารถของผู้ใช้อินเทอร์เน็ต โดยควรขยายการดำเนินการเกี่ยวกับการส่งเสริมการรู้และทักษะดิจิทัลให้แพร่หลายมากขึ้น โดยเฉพาะในกลุ่มผู้สูงอายุและกลุ่มเสี่ยงอื่น ๆ รวมถึงกลุ่มชาติพันธุ์และผู้ที่อาศัยในชนบทห่างไกล นอกจากนี้ ควรพิจารณาการกำหนดให้การรู้ดิจิทัลหลักสูตรที่ทกคนต้องได้เรียนทั้งในและนอกระบบ

3) แม้ราคาค่าการบริการอินเทอร์เน็ตอยู่ในระดับที่ไม่แพงมากนัก โดยเฉพาะบอร์ดแบนด์มือถือ แต่ก็มีความจำเป็นที่หน่วยงานกำกับดูแลต้องควบคุมและรักษาการแข่งขันในตลาดที่มีความเสรีและป้องกันการผูกขาดต่อไป

4) ในการกำกับดูแลอินเทอร์เน็ตนั้น รัฐควรนำแนวทางการกำกับอยู่แลบนพื้นฐานสิทธิมนุษยชน แนวทางการมีส่วนร่วม และแนวทางผู้มีส่วนได้ส่วนเสียหลายฝ่ายมาใช้ให้มากขึ้น โดยให้การสนับสนุนให้มีการใช้แนวทางดังกล่าวทั้งในระดับนโยบายและการติดตามตรวจสอบการดำเนินการอินเทอร์เน็ตในประเทศไทย ซึ่งบาทของของผู้มีส่วนได้เสียเสียภาคประชาสังคมในปัจจุบันยังน้อย เช่น ในการแก้ไข พ.ร.บ. กสทช. ฉบับที่ 2 พ.ศ. 2560 ซึ่งปรับปรุงกระบวนการสรรหาและองค์ประกอบนั้น ได้ลดทอนความหลากหลายในกระบวนการสรรหา

ภาคประชาสังคมและองค์กรวิชาชีพต่าง ๆ ถูกตัดออกและให้เหลือเพียงฝ่ายตุลาการและองค์กรอิสระบางแห่งเท่านั้น นอกจากนี้ ยังมีข้อสังเกตเพิ่มเติมเกี่ยวกับสัดส่วนของ กสทช. ไม่ได้สะท้อนความหลากหลายทางเพศ ซึ่งที่ กสทช. ทุกชุดที่ผ่านมา รวมถึงชุดปัจจุบัน ล้วนประกอบด้วยเพศชายเกือบ 100 เปอร์เซ็นต์

6.2.2 เสรีภาพในการแสดงออกและการจำกัดเนื้อหาทางออนไลน์

ข้อ 19 ของ ICCPR ได้รับรองสิทธิที่จะมีความคิดเห็นโดยปราศจากการแทรกแซง ซึ่งถือว่าเป็นสิทธิสัมบูรณ์หรือเด็ดขาด (Absolute) ซึ่งไม่สามารถจำกัดได้ และรับรองสิทธิในเสรีภาพแห่งการแสดงออก ซึ่งอาจถูกจำกัดได้ภายใต้เงื่อนไข ข้อ 19 (3) ของ ICCPR กล่าวคือ ต้องประกอบด้วยเงื่อนไข 3 ประการ ได้แก่ (การทดสอบสามส่วน)

1) ความชอบด้วยกฎหมาย (Legality) การจำกัดต้องเป็นไปตามที่มีกฎหมายบัญญัติไว้ ซึ่งกฎหมายนี้ต้องออกด้วยกระบวนการที่ชอบธรรม ชัดเจน คาดหมายได้ เปิดเผยต่อสาธารณะ และไม่เลือกปฏิบัติ

2) ความชอบธรรม (Legitimacy) การจำกัดต้องจำเป็นเพื่อวัตถุประสงค์หรือเป้าหมายที่ชอบธรรมตามที่กำหนดไว้ในข้อ 19 (3) ของ ICCPR ได้แก่ การคุ้มครองสิทธิหรือชื่อเสียงของบุคคล การรักษาความมั่นคงของชาติ ความสงบเรียบร้อยสาธารณะ การสาธารณะสุขและศีลธรรมของประชาชน รวมถึงการปิดกั้นภาพลามกอนาจารของเด็ก เป็นต้น ตลอดจนการจำกัดภายใต้เงื่อนไขข้อ 20 ของ ICCPR ในกรณีที่เนื้อหานั้นเป็นการโฆษณาชวนเชื่อเพื่อการสงคราม หรือการสนับสนุนให้เกิดความเกลียดชังในชาติเผ่าพันธุ์ หรือศาสนา ซึ่งยุยงให้เกิดการเลือกปฏิบัติ การเป็นปฏิปักษ์ หรือการใช้ความรุนแรง

3) ความจำเป็น (necessity) และได้สัดส่วน (proportionality) ต้องพิสูจน์ให้เห็นว่าการจำกัดนั้นจำเป็นในการปกป้องวัตถุประสงค์หรือเป้าหมายที่ชอบธรรมข้างต้น และต้องจำกัดให้น้อยที่สุดเท่าที่เป็นไปได้เพื่อบรรลุวัตถุประสงค์หรือเป้าหมายดังกล่าว รวมถึงมาตรการใด ๆ ในการจำกัดสิทธิต้องไม่เป็นการเลือกปฏิบัติ

การใช้ข้อจำกัดดังกล่าว เป็นหน้าที่ของรัฐที่จะต้องแสดงให้เห็นความเชื่อมโยงโดยตรงและทันทีระหว่างการแสดงออกกับความเป็นไปได้หรือการเกิดขึ้นของภัยคุกคาม และการอนุญาตให้ใช้ข้อจำกัดต้องดำเนินการโดยหน่วยงานตุลาการที่มีอำนาจหรือเป็นอิสระ ไม่ควรมอบหมายมาตรการการปิดกั้นให้กับหน่วยงานเอกชนโดยไม่ผ่านกระบวนการพิจารณาโดยหน่วยงานตุลาการหรือหน่วยงานที่เป็นอิสระ

<u>สถานการณ์ของประเทศไทย</u>

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้รับรองเสรีภาพในการแสดงออกไว้ค่อนข้างสอดคล้องกับข้อ 19 ของ ICCPR อย่างไรก็ดี สิทธิในการมีความคิดเห็นโดยปราศจากการแทรกแซงรัฐธรรมนูญได้รับรองไว้ในส่วนเดียวกับเสรีภาพในการแสดงออก ทำให้ถูกตีความว่าเป็นสิทธิที่ถูกจำกัดได้

ซึ่งแตกต่างจากข้อ 19 ของ ICCPR ที่สิทธิที่จะมีความคิดเห็นนั้น จำกัดไม่ได้ ดังนั้น ประเด็นนี้อาจจะต้องทำให้ชัดเจนขึ้นในอนาคต

การใช้อำนาจของรัฐในการจำกัดเนื้อหาทางออนไลน์นั้น หลายครั้งมักกระทบต่อเสรีภาพในการแสดงออกและเสรีภาพแสดงออก ประเทศไทยถูกประเมินจากองค์กร Freedom House ซึ่งเป็นองค์กรอิสระตรวจสอบเสรีภาพและประชาธิปไตยทั่วโลก โดยถูกจัดอันดับให้อยู่ในกลุ่มประเทศที่ไร้เสรีภาพทางอินเทอร์เน็ต (Not Free) มาเป็นเวลากว่า 5 ปีติดต่อกัน (2560 – 2564) ซึ่งเป็นผลมาจากการจำกัดเนื้อหาบนอินเทอร์เน็ต (Limits on Content) และการละเมิดสิทธิผู้ใช้งานอินเทอร์เน็ต (Violations of User Rights)

เมื่อพิจารณาจากสถานการณ์การจำกัดเนื้อหาทางออนไลน์ ซึ่งเชื่อมโยงกับเสรีภาพในการแสดงออกนั้น พบว่า มีทั้งการพัฒนาในเชิงบวกและสิ่งที่ยังน่ากังวล โดยพัฒนาการเชิงบวกนั้น เกิดจากการที่ศาลได้วางบรรทัดฐานเกี่ยวกับการพิจารณาปิดกั้นเนื้อหาทางออนไลน์ โดยนับตั้งแต่ปี 2564 เป็นต้นมาศาลได้วางแนวปฏิบัติที่ชัดเจนในเรื่องการไต่สวนคัดค้านการขอปิดกั้นเว็บไซต์ และศาลได้แสดงเห็นถึงความพยายามในการนำหลักสิทธิมนุษยชนเป็นส่วนหนึ่งในการพิจารณาปิดกั้นเนื้อหาด้วย

สำหรับประเด็นที่ยังน่ากังวลนั้น เกี่ยวกับการฟ้องคดีเกี่ยวกับการเผยแพร่เนื้อหาหรือการแสดงออกทางออนไลน์ที่ยังมีแนวโน้มเพิ่มขึ้น โดยเฉพาะภายใต้สถานการณ์ความขัดแย้งทางการเมืองในช่วงหลายปีที่ผ่านมา ซึ่งเมื่อพิจารณาตามกรอบของการจำกัดเสรีภาพในการแสดงออกแล้ว (การทดสอบสามส่วน) พบว่า ยังมีข้อท้าทายที่สำคัญในการจำกัดเนื้อหาทางออนไลน์ ดังนี้

1) ความชอบด้วยกฎหมาย

ตามหลักความชอบด้วยกฎหมาย เรียกร้องให้รัฐจำกัดเนื้อหาทางออนไลน์บนพื้นฐานของกฎหมายที่ชัดเจน แน่นอน คาดหมายได้ และไม่เลือกปฏิบัติ อย่างไรก็ดี พบว่า กฎหมายที่ถูกนำมาใช้จำกัดเนื้อหาทางออนไลน์ในประเทศไทย ไม่ว่าจะโดยการปิดกั้นเนื้อหา หรือการดำเนินคดีกับการเผยแพร่เนื้อหานั้น กฎหมายหลายฉบับยังมีถ้อยคำที่คลุมเครือ ตัวอย่างได้แก่ พ.ร.บ. คอมพิวเตอร์ฯ เช่น คำว่า ข้อมูลฯ “บิดเบือน” “ปลอม” “เท็จ” "ความสงบเรียบร้อยของประชาชน" และประมวลกฎหมายอาญา มาตรา 112 (หมิ่นประมาทพระมหากษัตริย์) เช่น “แสดงความอาฆาตมาดร้าย” ซึ่งถ้อยคำเหล่านี้ไม่มีการนิยามความหมายไว้อย่างชัดเจนว่ามีขอบเขตแค่ไหน จึงอาจทำให้มีความเสี่ยงที่จะถูกนำมาใช้ละเมิดเสรีภาพภาพในการแสดงออกเกินสมควร

2) วัตถุประสงค์ที่ชอบธรรม

สำหรับการแสดงออกที่ก่อให้เกิดความผิดภายใต้กฎหมายระหว่างประเทศ ซึ่งอาจสามารถออกกฎหมายทางอาญาเพื่อจำกัดได้อย่างชัดแจ้งนั้น ได้แก่ 1) สื่อลามกที่เกี่ยวกับเด็ก (Child pornography) 2) การยุยงโดยตรงและโดยสาธารณะให้กระทำการฆ่าล้างเผ่าพันธุ์ 3) การโฆษณาชวนเชื่อเพื่อการสงคราม และการสนับสนุน

ให้เกิดความเกลียดชังในชาติ เผ่าพันธุ์ หรือศาสนา ซึ่งยุยงให้เกิดการเลือกปฏิบัติ การเป็นปฏิปักษ์ หรือการใช้ความรุนแรง และ 4) การยุยงให้เกิดการก่อการร้าย (Incitement to terrorism) อย่างไรก็ดี การจำกัดเนื้อหาเหล่านั้นต้องปฏิบัติตามเกณฑ์การทดสอบสามส่วนของข้อจำกัดสิทธิในเสรีภาพในการแสดงออก

ส่วนเนื้อหาอื่นนอกจากนี้ ต้องพิจารณาตามหลักเกณฑ์ของข้อ 19 (3) ของ ICCPR และเนื้อหาซึ่งปรากฏจากข้อเสนอแนะของกลไกสิทธิมนุษยชนระหว่างประเทศว่าไม่ควรถูกจำกัด ได้แก่

- การอภิปรายเกี่ยวกับนโยบายรัฐบาลและทางการเมือง รวมถึงการวิพากษ์วิจารณ์รัฐบาล หรือระบบสังคมการเมืองที่ดำเนินการโดยรัฐบาล การรายงานเกี่ยวกับสิทธิมนุษยชน กิจกรรมของรัฐบาล และการทุจริตในรัฐบาล กิจกรรมทางการเมือง สันติภาพ ประชาธิปไตย และการแสดงความเห็นเกี่ยวกับศาสนาหรือความเชื่อ
- กฎหมายสิทธิมนุษยชนระหว่างประเทศถูกออกแบบขึ้นเพื่อคุ้มครองบุคคล ไม่ใช่ค่านิยม หรือสถาบันที่เป็นนามธรรม เช่น อัตลักษณ์ประจำชาติ ศาสนา สัญลักษณ์ของรัฐ สถาบันหรือผู้แทนของรัฐ เช่น ประมุขแห่งรัฐ[363]
- การแสดงออกในเรื่องที่เป็นสาธารณประโยชน์ รวมถึงการวิพากษ์วิจารณ์รัฐบาลและผู้นำทางการเมืองและคำพูดของนักการเมือง และบุคคลสาธารณะอื่น ๆ
- การจำกัดเพียงเพราะ “ข้อมูลเท็จ (misinformation)” และ “ความจริงที่บิดเบือน (distorted truth)” ถือเป็นข้อจำกัดที่ไม่ชอบธรรมตามข้อ 19 (3)[364]
- กฎหมายหมิ่นประมาท ซึ่งกำหนดขึ้นเพื่อปกป้องชื่อเสียงของบุคคลนั้น อาจได้รับอนุญาตตามข้อ 19 (3) แต่มีคำแนะนำจากกลไกสิทธิมนุษยชนแห่งสหประชาชาติว่ากฎหมายหมิ่นประมาทไม่ควรเป็นความผิดทางอาญา

มีกฎหมายบางฉบับที่อาจไม่สอดคล้องกับวัตถุประสงค์ในข้อ 19 (3) ของ ICCPR และไม่ถูกจำกัดโดยเฉพาะ พ.ร.บ. คอมพิวเตอร์ฯ มาตรา 14 ที่กำหนดโทษทางอาญาสำหรับการจัดการข้อมูลเท็จ ปลอม หรือบิดเบือน ภายใต้กฎหมายที่คลุมเครือ และประมวลกฎหมายอาญา มาตรา 116 ซึ่งแม้จะอ้างวัตถุประสงค์เรื่องการรักษาความมั่นคง แต่ไม่มีขอบเขตเกี่ยวกับความมั่นคงที่ชัดเจน และบ่อยครั้งกฎหมายถูกนำมาใช้เพื่อรักษาความมั่นคงของรัฐบาล ซึ่งไม่สอดคล้องกับวัตถุประสงค์ในการรักษาความมั่นคงที่ระบุในข้อ 19 (3) ของ ICCPR ที่มุ่งใช้กับความมั่นคงที่คุกคามความอยู่รอดของชาติ ไม่ใช่การปกป้องรัฐบาลจากการถูกวิพากษ์วิจารณ์ สภาพดังกล่าวสะท้อนให้เห็นความคลุมเครือของวัตถุประสงค์ของกฎหมายดังกล่าว จึงจำเป็นต้องมีการทบทวนแก้ไขหรือยกเลิก

---

[363]CCPR General comment No. 34 (2011), para. 38. ; A/HRC/7/14, 28 February 2008, para 40.

[364] David Kaye, A/71/373, 6 September 2016, para. 27.

3) ความจำเป็นและได้สัดส่วน

กฎหมายอาญาบางฉบับที่ถูกนำมาใช้ยังคงกำหนดอัตราโทษจำคุกไว้ค่อนข้างสูง โดยเฉพาะประมวลกฎหมายอาญา มาตรา 112 ที่กำหนดระวางโทษจำคุกขั้นต่ำตั้งแต่ 3 ปีจนถึงขั้นสูง 15 ปี ซึ่งอาจจะเป็นโทษที่สูงเกินไปเมื่อเทียบกับลักษณะของการกระทำซึ่งเป็นการแสดงออกต่อสถาบันทางการเมืองในระบอบประชาธิปไตย

นอกจากนี้ กฎหมายหมิ่นประมาทของไทยยังคงเป็นความผิดอาญาและมีโทษจำคุก 1 ปี สำหรับการหมิ่นประมาททั่วไป และ 2 ปี สำหรับการหมิ่นประมาทโดยการโฆษณา ซึ่งกลไกสิทธิมนุษยชนแห่งสหประชาชาติได้แนะนำบ่อยครั้งให้ลดทอนความเป็นอาชญากรรมของความผิดฐานดังกล่าว โดยเฉพาะการยกเลิกโทษจำคุก เพราะถือว่าไม่ได้สัดส่วนสำหรับการจำกัดเสรีภาพในการแสดงออกตามข้อ 19 (3) ของ ICCPR

<u>ข้อเสนอแนะ</u>

1) รัฐควรพิจารณาทบทวนแก้ไขกฎหมายที่บังคับใช้ในการจำกัดเนื้อหาทางออนไลน์ เช่น พ.ร.บ. คอมพิวเตอร์ ฯ มาตรา 14 ประมวลกฎหมายอาญา มาตรา 112 มาตรา 116 และมาตรา 326, 328 (หมิ่นประมาท) ให้สอดคล้องกับการทดสอบสามส่วนสำหรับการจำกัดเสรีภาพในการแสดงออกตามข้อ 19 (3) ของ ICCPR กล่าวคือ การทำให้กฎหมายมีความชัดเจนและคาดหมายได้มากขึ้น และทำให้การลงโทษตามกฎหมายได้สัดส่วนมากขึ้น รวมถึงพิจารณายกเลิกโทษจำคุกของกฎหมายเหล่านี้ โดยเฉพาะในความผิดฐานหมิ่นประมาท

2) ในการพิจารณาจัดทำกฎหมายและนโยบายในการจำกัดเนื้อหาทางออนไลน์ ไม่ว่าจะเป็นการจัดการกับเนื้อหาที่สร้างความเกลียดชัง (Hate speech) หรือข่าวปลอม (Fake news) ข้อมูลบิดเบือน (Disinformation) รัฐควรนำการทดสอบสามส่วนสำหรับการจำกัดเสรีภาพในการแสดงออกตามข้อ 19 (3) และเงื่อนไขภายใต้ข้อ 20 ของ ICCPR มาเป็นกรอบในการพิจารณา ทั้งนี้ การสร้างกฎหมาย Hate speech ควรใช้เฉพาะในกรณีที่เข้าเงื่อนไขข้อ 20 ของ ICCPR เท่านั้น กล่าวคือ เป็นการแสดงออกที่สนับสนุนให้เกิดความเกลียดชังในชาติเผ่าพันธุ์ หรือศาสนา ซึ่งยั่วยุให้เกิดการเลือกปฏิบัติ การเป็นปฏิปักษ์ หรือการใช้ความรุนแรง ทั้งนี้ ในการพิจารณากำหนดขอบเขตของกฎหมาย นโยบายหรือมาตรการในการจัดการกับเนื้อหาที่เป็นอันตรายหรือไม่พึงประสงค์ดังกล่าว ควรนำ Rabat Plan of Action มาใช้เป็นแนวทาง

อย่างไรก็ดี แนวทางที่กลไกสิทธิมนุษยชนแห่งสหประชาชาติแนะนำสำหรับการจัดการปัญหาเหล่านี้ คือ การเปิดกว้างสำหรับการแสดงออกและส่งเสริมการสนทนาอย่างอดทนอดกั้น รวมถึงประกันความหลากหลายของเนื้อหาและสื่อ และเน้นการจัดการที่ปัญหารากเหง้าความเกลียดชัง

3) ในการส่งเสริมให้ประชาชนเข้าถึงข้อมูลข่าวสารเป็นพันธกรณีของรัฐในด้านเสรีภาพในการแสดงออกเช่นกัน และถือเป็นแนวทางเชิงบวกและสร้างสรรค์ในการจัดการกับเนื้อหาที่เป็นอันตรายและไม่พึง

ประสงค์ต่าง ๆ อย่างไรก็ดี รัฐควรใช้มาตรการด้านข้อมูลข่าวสาร โดยเฉพาะสิ่งที่เรียกว่าปฏิบัติการข้อมูลข่าวสาร (Information Operation: IO) อย่างโปร่งใสและพร้อมรับการตรวจสอบ เน้นวัตถุประสงค์ในการส่งเสริมสิทธิของประชาชนในการเข้าถึงข้อมูลข่าวสาร และที่สำคัญรัฐต้องไม่เข้าไปดำเนินการ ให้การสนับสนุน ส่งเสริมหรือเผยแพร่ข้อความที่รู้หรือมีเหตุอันควรรู้ว่าเป็นเท็จ หรือโฆษณาชวนเชื่อ หรือสร้างความเกลียดชังเสียเอง ไม่ว่าทั้งโดยจงใจหรือประมาท[365]

4) เพื่อประกันความโปร่งใสในการจัดการเนื้อหา โดยเฉพาะการปิดกั้นเว็บไซต์ รัฐบาลควรเผยแพร่รายชื่อไซต์ที่ถูกปิดกั้น วิธีการปิดกั้นและเหตุผลที่ชอบธรรมของการปิดกั้นเนื้อหาดังกล่าว

6.2.3 สิทธิในความเป็นส่วนตัวในยุคดิจิทัล

สิทธิในความเป็นส่วนตัว (Right to privacy) ถูกรับรองไว้ในข้อ 17 ของ ICCPR และเช่นเดียวกับเสรีภาพในการแสดงออก สิทธิในความส่วนตัวอาจถูกจำกัดหรือแทรกแซงได้ แต่การจำกัดต้องเป็นไปตามการทดสอบสามส่วนเช่นเดียวกับเสรีภาพในการแสดงออกดังกล่าวไว้แล้ว และต้องถูกตรวจสอบโดยกลไกที่อิสระ โดยเฉพาะศาลและมีการดำเนินการที่ความโปร่งใส

<u>สถานการณ์ของประเทศไทย</u>

สิทธิในความเป็นส่วนตัว ถูกรับรองสิทธิไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 33 และ 36 และมีการคุ้มครองในกฎหมายระดับพระราชบัญญัติอย่างน้อย 2 ฉบับ คือ พ.ร.บ. กสทช.ฯ (มาตรา 27 (13) และ 32) ที่อำนาจ กสทช. ในการปกป้องความเป็นส่วนตัวของประชาชนจากการถูกละเมิดโดยการประกอบกิจการโทรคมนาคม และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เน้นการคุ้มครองข้อมูลส่วนบุคคลทั้งทางออฟไลน์และออนไลน์ อย่างไรก็ดี กฎหมายฉบับนี้ยกเว้นไม่นำมาใช้กับหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งเป็นหนึ่งในประเด็นข้อท้าทายสำหรับการคุ้มครองสิทธิความเป็นส่วนตัวในมิติของการสอดส่อง

ประเทศไทยมีกฎหมายหลายฉบับที่ให้อำนาจรัฐในการสอดส่องการสื่อสารและรวบรวมข้อมูลของประชาชนโดยตรงภายใต้วัตถุประสงค์และขอบเขตที่แตกต่างกันไป โดยจำแนกได้ ดังนี้

<u>กฎหมายที่ให้อำนาจสอดส่องในสถานการณ์พิเศษ</u> ได้แก่ กฎอัยการศึก ซึ่งไม่มีหลักประกันการตรวจสอบการใช้อำนาจและจำกัดการเข้าถึงการเยียวยาความเสียหาย ส่วนกฎหมายอีกฉบับ คือ พ.ร.ก. ฉุกเฉินฯ แม้จะกำหนดให้ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยการสอบสวนคดีพิเศษ แต่ขอบเขตของ พ.ร.ก.ฉุกเฉินฯ นั้น ระบุให้ใช้มาตรการตรวจสอบการสื่อสารด้วยวิธีการอื่นใด เพื่อป้องกันหรือระงับเหตุการณ์ร้ายแรง ซึ่งคำว่า “เหตุการณ์ร้ายแรง” ไม่มีนิยามชัดเจน จึงอาจถูกตีความนำไปใช้ได้กว้างขวาง

---

[365] Joint declaration, 2017 ; A/HRC/RES/12/16, A/HRC/RES/26/13, A/HRC/RES/32/13 ; A/74/486

<u>กฎหมายที่ให้อำนาจสอดส่องเพื่อวัตถุประสงค์ในการบังคับใช้กฎหมายหรือการดำเนินคดี</u>
มีกฎหมายอย่างน้อย 6 ฉบับที่ให้อำนาจรัฐโดยตรงในการสอดส่องด้วยการเข้าถึงข้อมูลการสื่อสาร ได้แก่

- พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46
- พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 เพิ่มโดยพระราชบัญญัติป้องกันและปราบปรามยาเสพติด (ฉบับที่ 4) พ.ศ. 2545 มาตรา 14 จัตวา
- พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25
- พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 มาตรา 30
- พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 17

กฎหมายข้างต้นส่วนใหญ่กำหนดหลักประกันการคุ้มครองสิทธิไว้คล้ายกัน แม้จะมีรายละเอียดแตกต่างกันบ้างก็ตาม และข้อกำหนดทางกฎหมายค่อนข้างสอดคล้องกับกรอบสิทธิความเป็นส่วนตัวในมิติการสอดส่องการสื่อสาร กล่าวคือ

ความชอบด้วยกฎหมาย : มีการกำหนดอำนาจการสอดส่องโดยกฎหมายอย่างชัดเจน แน่นอน คาดหมายได้ อย่างไรก็ดี อาจจะมีกฎหมายบางฉบับที่ให้อำนาจการสอดส่องสำหรับขอบเขตของความผิดที่ค่อนข้างกว้าง โดยเฉพาะ พ.ร.บ. การสอบสวนคดีพิเศษฯ ซึ่งคดีพิเศษนั้นกินความครอบคลุมความผิดตามกฎหมายกว่า 20 ฉบับและสามารถพิจารณาเพิ่มคดีพิเศษได้อีกในภายหลัง นอกจากนี้ยังมี พ.ร.บ. คอมพิวเตอร์ฯ ซึ่งนอกจากจะใช้กับความผิดตาม พ.ร.บ. คอมพิวเตอร์ฯ โดยตรงแล้ว ยังอาจใช้กับความผิดทางอาญาตามกฎหมายอื่นที่เกี่ยวข้องกับคอมพิวเตอร์ด้วย ซึ่งประเด็นนี้จะเชื่อมโยงกับประเด็นวัตถุประสงค์ที่ชอบธรรมดังจะกล่าวต่อไป

วัตถุประสงค์ที่ชอบธรรม : กฎหมายที่ให้อำนาจสอดส่อง จำนวนหนึ่งมีวัตถุประสงค์เพื่อจัดการกับคดีอาญาที่ร้ายแรง เช่น ค้ามนุษย์ องค์กรอาชญากรรมข้ามชาติ เป็นต้น แต่มีกฎหมายบางฉบับที่สามารถนำไปใช้กับขอบเขตความผิดที่ค่อนข้างกว้าง เช่น พ.ร.บ. การสอบสวนคดีพิเศษฯ และ พ.ร.บ. คอมพิวเตอร์ฯ ซึ่งการกำหนดขอบเขตของกฎหมายเพื่อเปิดช่องให้ใช้อำนาจสอดส่องสำหรับฐานความผิดที่กว้างขวางดังกล่าวไปแล้วอาจสุ่มเสี่ยงที่จะนำไปสู่การใช้อำนาจสอดส่องในความผิดที่ใช่อาชญากรรมร้ายแรง เช่น ความผิดที่เกี่ยวข้องกับการแสดงออกทางการเมืองดังกล่าวไปในหัวข้อก่อนหน้านี้ ซึ่งหากเป็นเช่นนั้นย่อมถือว่ากฎหมายดังกล่าวมีวัตถุประสงค์ที่ไม่ชอบธรรม เพราะหากพิจารณาตามคำแนะนำของกลไกสิทธิมนุษยชนแห่งสหประชาชาติแล้ว การสอดส่องที่ถือเป็นมาตรการที่ล่วงล้ำสิทธิมนุษยชนอย่างยิ่งนั้น ควรถูกใช้อย่างจำกัดเฉพาะอาชญากรรมร้ายแรงเท่านั้น

ความจำเป็นและได้สัดส่วน : กฎหมายทุกฉบับกำหนดเงื่อนไขของการใช้อำนาจสอดส่องไว้กล่าวคือ การใช้อำนาจต้องอาศัยอันควรเชื่อล่วงหน้าว่ามีการกระทำความผิด และถูกใช้โดยกำหนดเป้าหมายเป็นรายกรณี โดยผ่านการอนุญาตจากกลไกตุลาการ

นอกจากนี้ กฎหมายหลายฉบับ (4 ฉบับ) มีการกำหนดเกณฑ์การพิจารณาตามหลักความจำเป็นและได้สัดส่วน และมีการกำหนดระยะเวลาการใช้มาตรการไว้ แม้อาจจะอนุญาตได้คราวละยานานถึง 90 วันก็ตาม และกฎหมายยังกำหนดให้ศาลสามารถเปลี่ยนแปลงคำสั่งได้เมื่อพฤติการณ์เปลี่ยนไป ตลอดจนกำหนดเงื่อนไขของเก็บรักษาข้อมูลเท่าที่จำเป็น และกฎหมายกำหนดให้เข้าถึงข้อมูลและเก็บรักษาข้อมูลเท่าที่จำเป็นและทำลายข้อมูลส่วนที่ไม่เกี่ยวข้อง ซึ่งแสดงให้เห็นว่ากฎหมายมีการกำหนดหลักประกันการคุ้มครองไว้ระดับหนึ่ง

<u>กฎหมายที่ให้อำนาจสอดส่องเพื่อวัตถุประสงค์ด้านข่าวกรองหรือเชิงป้องกัน</u>

สิ่งที่น่ากังวลของกฎหมายในส่วนนี้ โดยเฉพาะพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 คือ กฎหมายแม่บทไม่ได้กำหนดอย่างชัดเจนเกี่ยวกับขอบเขตการใช้อำนาจ โดยรายละเอียดหลักเกณฑ์ วิธีการ และเงื่อนไขถูกนำไปกำหนดในกฎหมายลำดับรอง ซึ่งประเด็นนี้อาจไม่สอดคล้องกับบททดสอบของความชอบด้วยกฎหมาย ในเรื่องความชัดเจน แน่นอน คาดหมายได้ และเปิดเผยต่อสาธารณะ นอกจากนี้ ประเด็นสำคัญคือ กฎหมายฉบับนี้ไม่ได้กำหนดหลักประกันการตรวจสอบโดยกลไกที่เป็นอิสระ โดยเฉพาะกลไกศาล

เมื่อพิจารณาจากเนื้อหาในระเบียบแล้ว พบว่า ระเบียบกำหนดให้ผู้อำนวยการสำนักงานข่าวกรองแห่งชาติ ซึ่งเป็นหัวหน้าหน่วยงานนั้นเองเป็นผู้มีอำนาจอนุญาตให้ดำเนินการปฏิบัติการข่าวกรองซึ่งรวมถึงการสอดส่องด้วย และการกำกับดูแลการดำเนินการส่วนใหญ่อยู่ภายใต้ผู้บังคับบัญชาภายในหน่วยงาน อีกทั้ง ระเบียบยังระบุถึงการดำเนินการใช้มาตรการแบบลับได้ด้วย ดังนั้น กฎเกณฑ์เหล่านี้จึงไม่สอดคล้องกับกรอบหลักการสำหรับการอนุญาตให้สอดส่องที่ถูกยอมรับตามกรอบหลักการสิทธิมนุษยชนสากลสำหรับการสอดส่อง

ประเด็นเรื่องการสอดส่องแบบลับและการขาดการตรวจสอบถ่วงดุลจากภายนอกที่เป็นอิสระโดยเฉพาะฝ่ายตุลาการนั้น ทำให้มีความยากลำบากในการตรวจสอบว่าการใช้มาตรการสอดส่องเหล่านั้นสอดคล้องกับกฎเกณฑ์ทางกฎหมายที่กำหนดไว้หรือไม่ อีกทั้ง การสอดส่องแบบปิดลับและไม่โปร่งใส ย่อมทำให้ผู้ได้รับผลกระทบยากที่จะแสวงหาการเยียวยา เพราะพวกเขาไม่รู้ว่าหน่วยงานใดต้องรับผิดชอบ ดังตัวอย่างที่มีการรายงานเมื่อไม่นานมานี้ ในประเด็นการใช้สปายแวร์ที่เพกาซัส (Pegasus) เพื่อเจาะโทรศัพท์ล่วงข้อมูลของนักปกป้องสิทธิมนุษยชน นักกิจกรรมทางการเมือง และนักการเมืองฝ่ายตรงข้าม ซึ่งแม้จะมีข้อมูลบ่งชี้ว่าสปายแวร์ตัวนี้เฉพาะรัฐบาลเท่านั้นที่ใช้ แต่ก็ยากสำหรับผู้ได้รับผลกระทบที่จะหาหลักฐานหรือพิสูจน์ว่าหน่วยงานของรัฐใดรับผิดชอบดำเนินการ ดังนั้น ในการใช้มาตรการสอดส่อง จึงจำเป็นต้องมีความโปร่งใสมากขึ้น โดยเฉพาะการซื้อและการใช้เทคโนโลยีสอดส่องเหล่านี้มาใช้ การกำหนดให้ต้องแจ้งมาตรการสอดส่องแก่ผู้ที่ตกเป็นเป้าหมาย

กำหนดให้การรายงานต่อสาธารณะหรือรัฐสภาเกี่ยวกับการจัดหาและการใช้มาตรการสอดส่อง ซึ่งข้อท้าทายเหล่านี้จะต้องมีการหารือในวงกว้างต่อไปเพื่อให้มาตราการสอดแนมการสื่อสารของไทยเป็นไปตามความคาดหวังของกรอบสิทธิมนุษยชนสากลมาที่สุด

ข้อเสนอแนะ

1) รัฐในฐานะที่มีพันธกรณีที่ต้องเคารพและคุ้มครองสิทธิมนุษยชน ควรประกันว่ากรอบกฎหมายที่ให้อำนาจสอดส่องนั้นเป็นไปตามหลักการของพันธกรณีสิทธิมนุษยชนระหว่างประเทศ กล่าวคือ เป็นไปตามบทการสอบสามส่วนของการจำกัดสิทธิ ตลอดจนกำหนดให้การใช้อำนาจสอดส่องต้องผ่านการตรวจสอบและอนุญาตโดยกลไกที่เป็นอิสระ เป็นกลางและมีอำนาจตามกฎหมาย โดยเฉพาะฝ่ายตุลาการ ในแง่นี้ จึงจำเป็นต้องมีการทบทวนแก้ไขกฎหมายบางฉบับให้สอดคล้องกับกรอบหลักการดังกล่าว โดยเฉพาะพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 ทั้งนี้ ในการปรับปรุงกฎหมายอาจดูแนวทางเพิ่มเติมจากหลักการระหว่างประเทศว่าด้วยการใช้หลักสิทธิมนุษยชนกับการสอดแนมการสื่อสาร (International Principles on the Application of Human Rights to Communications Surveillance) ซึ่งพัฒนาโดยองค์กรภาคประชาสังคมและผู้เชี่ยวชาญด้านสิทธิมนุษยชนระดับนานาชาติ มาเป็นกรอบแนวทางในการปรับปรุงกฎหมาย

2) รัฐต้องประกันความโปร่งใสของการใช้มาตรการสอดส่อง เพื่อให้สามารถตรวจสอบได้มากขึ้นและเพื่อประกันว่าผู้ได้รับผลกระทบจะสามารถเข้าถึงการเยียวยาอย่างมีประสิทธิผล สำหรับทางเลือกของการสร้างหลักประกันความโปร่งใสนั้น อย่างน้อยรัฐควรเปิดเผยเกี่ยวกับการจัดหาเทคโนโลยีการสอดส่องต่อสาธารณะโดยเฉพาะผ่านกลไกรัฐสภา เพื่อให้ตรวจสอบความจำเป็นและประเมินผลกระทบของเทคโนโลยีดังกล่าวอย่างรอบครอบและพิจารณาเกี่ยวกับการแจ้งการสอดส่องแก่ผู้ตกเป็นเป้าหมาย อย่างน้อยภายหลังจากการสอดส่องจบลงแล้ว

3) หลีกเลี่ยงการใช้เทคโนโลยีการจดจำใบหน้า (Face Recognition) ซึ่งเป็นส่วนหนึ่งของมาตรการสอดส่องในวงกว้าง ประกอบกับเทคโนโลยีดังกล่าวสามารถก่อผลกระทบต่อสิทธิมนุษยชนอย่างมีนัยยะสำคัญ ทั้งต่อสิทธิในความเป็นส่วนตัว สิทธิในการไม่ถูกเลือกปฏิบัติ และเสรีภาพในการแสดงออก

6.3 ข้อเสนอแนะในภาพรวม

ข้อเสนอแนะต่อรัฐ

โดยทั่วไปแล้ว รัฐเป็นผู้มีหน้าที่ตามกฎหมายสิทธิมนุษยชนระหว่างประเทศในการที่เคารพ (respect) โดยต้องไม่ใช้เครื่องมือทางเทคโนโลยีไปล่วงล้ำหรือละเมิดสิทธิมนุษยชนเสียเอง ต้องให้การคุ้มครอง (protect) โดยการป้องกันไม่ให้มีการละเมิดสิทธิมนุษยชนโดยบุคคลต่าง ๆ ผ่านการใช้เทคโนโลยี รวมถึงควรมีการจัดตั้งหรือสร้างความเข็มแข็งให้กลไกที่เป็นอิสระเพื่อประกันว่าบุคคลที่ได้รับผลกระทบหรือถูกละเมิดจะสามารถ

เข้าถึงกระบวนการยุติธรรมและการเยียวยาได้อย่างมีประสิทธิผล นอกจากนี้ รัฐมีพันธกรณีในการเติมเต็ม (fulfill) เพื่อให้ประชาชนได้รับสิทธิมนุษยชนขั้นพื้นฐานตามที่กำหนดไว้ในกฎหมายระหว่างประเทศ รวมถึงการส่งเสริมให้ทุกคนเข้าถึงเทคโนโลยีที่มีคุณภาพและเท่าเทียมกัน

โดยคำนึงถึงพันธกรณีในการเคารพและคุ้มครองบุคคลจากการละเมิดสิทธิมนุษยชนดังกล่าวในการออกแบบกฎหมาย นโยบาย หรือแนวทางการดำเนินการใด ๆ ในบริบทของเทคโนโลยี รวมถึงอินเทอร์เน็ต รัฐควรให้ความสำคัญกับแนวทางสิทธิมนุษยชน (Human Rights Based Approach) ซึ่งเรียกร้องให้รัฐมีความโปร่งใสในการตัดสินใจ (Transparency) มีหลักประกันความรับผิดชอบ (Accountability) มีหลักประกันว่าเทคโนโลยีใหม่จะสร้างความเท่าเทียมและไม่เลือกปฏิบัติในการใช้งาน (Non-discrimination and equality) และให้ความสำคัญกับการมีส่วนร่วม (Participatory) โดยประกันว่าเสียงของทุกคนที่ได้รับผลกระทบจากเทคโนโลยีใหม่จะถูกรับฟัง และสุดท้าย รัฐต้องให้ความสำคัญกับการเสริมสร้างศักยภาพให้ประชาชน (Empowerment) โดยทำให้ประชาชนทุกคนเข้าใจถึงผลกระทบของเทคโนโลยีใหม่ที่มีต่อชีวิตของตน และมีความรู้และเข้าถึงกระบวนการตรวจสอบและ/หรือการเยียวยาเมื่อมีการละเมิดเกิดขึ้น

ข้อเสนอแนะต่อภาคธุรกิจ

ภาคธุรกิจเทคโนโลยีมีบทบาทสำคัญในยุคดิจิทัลและบทบาทดังกล่าวอาจส่งผลกระทบต่อสิทธิมนุษยชนได้ทั้งในเชิงบวกและลบ บริษัทเทคโนโลยีจึงควรให้ความสำคัญกับมิติสิทธิมนุษยชนในการดำเนินงานของตนเช่นกัน โดยควรพิจารณานำหลักการชี้แนะของสหประชาชาติว่าด้วยธุรกิจกับสิทธิมนุษยชน (UNGP) มาปรับเข้ากับการประกอบกิจการของบริษัท

สำหรับแนวทางเกี่ยวกับการปรับใช้หลักการ UNGP ในบริบทของภาคธุรกิจเทคโนโลยีนั้น อาจดูเพิ่มเติมได้จากเอกสารดังต่อไปนี้[366]

- **The UN Guiding Principles in the Age of Technology** ภายใต้โครงการ B-Tech ของสำนักงานข้าหลวงใหญ่สิทธิมนุษยชนแห่งสหประชาชาติ (UNOHCHR)
- **ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights** ของคณะกรรมาธิการยุโรป (European Commission) ซึ่งพัฒนาโดย Shift and Institute for Human Rights and Business (IHRB)
- **The Practical Application of the UNGPs in the Technology Sector** โดย Global Network Initiative ซึ่งจัดทำขึ้นเพื่อส่งให้ข้าหลวงใหญ่สิทธิมนุษยชนแห่งสหประชาชาติเกี่ยวกับการประยุกต์ใช้ UNGPs ในภาคเทคโนโลยี

[366]โปรดดูคำแนะนำเพิ่มเติมจาก Business for Social Responsibility (BSR), Applying the UNGPs to Technology: Our Point of View

ข้อเสนอแนะต่อคณะกรรมการสิทธิมนุษยชนแห่งชาติ

เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงไปเรื่อง ๆ และอย่างรวดเร็ว ซึ่งส่งผลทั้งในแง่บวกและลบต่อสิทธิมนุษยชน คณะกรรมการสิทธิมนุษยชนแห่งชาติ จึงควรให้ความสำคัญกับการสร้างและเผยแพร่องค์ความรู้ในประเด็นเทคโนโลยีกับสิทธิมนุษยชนอย่างจริงจริงและต่อเนื่อง เพราะยังมีอีกหลายประเด็นที่จำเป็นจะต้องทำความเข้าใจและต้องการองค์ความรู้ โดยเฉพาะประเด็นสิทธิมนุษยชนที่เกี่ยวข้องกับระบบอัตโนมัติต่าง ๆ ที่มีแนวโน้มในการนำมาใช้มากขึ้น ทั้งนี้ ในการดำเนินการในเรื่องนี้นั้น ควรให้ความสำคัญกับการแนวทางสหวิทยาการและการมีส่วนร่วมข้ามภาคส่วน เพื่อเชื่อมประสานองค์ความรู้ด้านสิทธิมนุษยชนและเทคโนโลยีเข้าด้วยกัน

บรรณานุกรม

เอกสารภาษาไทย

งานวิจัย หนังสือ บทความ

คณาธิป ทองรวีวงศ์. (2559). ย้อนเหตุการณ์ “สอดส่องการสื่อสาร” ปี 2558 และแนวโน้มความเป็นส่วนตัวออนไลน์ปี 2559. เครือข่ายพลเมืองเน็ต มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง (Thainetizen).

เคอร์บาลิจา, โจวาน. (2558). เปิดประตูสู่การอภิบาลอินเทอร์เน็ต. กรุงเทพฯ : มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง (Thainetizen)

พิรงรอง รามสูต รณะนันทน์ และ นิธิมา คณานิธินันท์. (2547). รายงานวิจัยเรื่อง การกำกับดูแลเนื้อหาอินเทอร์เน็ต. โครงการ “การปฏิรูประบบสื่อ: การกำกับดูแลเนื้อหาโดยรัฐ การกำกับดูแลตนเอง และสื่อภาคประชาชน”. สำนักงานกองทุนสนับสนุนการวิจัย (สกว.).

ศุภณัฐ เพิ่มพูนวิวัฒน์, ศรัณยุ หมั้นทรัพย์ และ จารุวรรณ แก้วมะโน. (2564). รายงานวิจัย เรื่อง ความเป็นพลเมือง: บทสำรวจสถานะความเป็นพลเมืองกับการรู้ดิจิทัล. สำนักส่งเสริมการเมืองภาคพลเมือง สถาบันพระปกเกล้า.

เอมิลี่ ประดิจิต และอนันยา รามานี. (2562). พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย: สู่กฎหมายที่มีมนุษย์เป็นศูนย์กลาง เพื่อคุ้มครองเสรีภาพและความเป็นส่วนตัวออนไลน์ พร้อมกับแก้ไขปัญหาภัยคุกคามทางไซเบอร์. มูลนิธิมานุษยะ

รายงานของหน่วยงาน

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2561). ผู้นำการเปลี่ยนแปลงดิจิทัล กิจกรรมสร้างการรับรู้ประโยชน์เน็ตประชารัฐ รอบที่ 3.

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. รายงานผลการดำเนินงานตามนโยบายรัฐบาลประจำปี.

คณะกรรมการสิทธิมนุษยชนแห่งชาติ. (2563). รายงานผลการประเมินสถานการณ์ด้านสิทธิมนุษยชนของประเทศไทย ปี 2563.-- กรุงเทพฯ : สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ.

คณะกรรมการสิทธิมนุษยชนแห่งชาติ. (2564). รายงานผลการประเมินสถานการณ์ด้านสิทธิมนุษยชนของประเทศไทย ปี 2564.-- กรุงเทพฯ : สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ.

โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). (2553). สรุปสถานการณ์การควบคุมและปิดกั้นสื่อออนไลน์ พ.ศ.2550 – 2553.

โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). (2556). สถิติการปิดกั้นเว็บไซต์ในประเทศไทย นับตั้งแต่ปี 2550-2556.

โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). (2557). สถิติการปิดกั้นเว็บไซต์ในประเทศไทย นับตั้งแต่ปี 2556-2557.

โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). (2558). “ยุยงปลุกปั่น” ตามมาตรา 116 ข้อหาเพื่อประโยชน์ทางการเมืองในยุครัฐบาลคสช.

โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). (2560). มาตรา 116: เมื่อข้อหา “ยุยงปลุกปั่น” ถูกใช้เป็นเครื่องมือปิดกั้นการแสดงออก.

โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). (2561). พ.ร.บ.คอมพิวเตอร์ฯ 2560: กฎหมายใหม่แต่ยังถูกใช้ปิดปากเหมือนเดิม.

โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). (4 มีนาคม 2562). ตารางคดี "ปิดปาก" ประชาชนด้วย พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14 (2).

โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). (2563). เปิดคำสั่งศาล ให้เว็บ Change.org "ฆ่าไม่ตาย" กลับมาใช้งานได้.

โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). (2564). ศาลอาญากลับคำสั่ง ไม่ให้บล็อค คลิป "วัคซีนพระราชทาน" ของคณะก้าวหน้า.

โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). (2565). ปรสิตติดโทรศัพท์ : การส่งเพกาซัสติดตามนักการเมืองก้าวหน้า-ก้าวไกล.

โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). (2565). ขั้นตอน วิธีการสั่ง "บล็อคเว็บ" ตามพ.ร.บ. คอมพิวเตอร์ฯ และช่องทางการคัดค้าน.

ศูนย์ทนายความเพื่อสิทธิมนุษยชน. (2562). รู้จักข้อหา “ยุยงปลุกปั่น” เครื่องมือจัดการประชาชนยุค คสช..

ศูนย์ทนายความเพื่อสิทธิมนุษยชน. (2563). คดีความเปลี่ยนชีวิตของ ‘ดนัย’ ศิลปินกราฟิตี้ ผู้โพสต์ไม่พบ จนท. คัดกรองที่สุวรรณภูมิ.

ศูนย์ทนายความเพื่อสิทธิมนุษยชน. (2564). สันติบาลไปหา นร.ม.ปลาย ข่มขู่ให้ลบโพสต์เกี่ยวกับสถาบันกษัตริย์อ้างเจตนาดี.

ศูนย์ทนายความเพื่อสิทธิมนุษยชน. (4 กันยายน 2565). กันยายน 65: จำนวนผู้ถูกดำเนินคดีทางการเมืองยอดรวมอย่างน้อย 1,860 คน ใน 1,139 คดี.

สมาคมนักกฎหมายสิทธิมนุษยชน. (2562). รายงานข้อเสนอแนะต่อการคุ้มครองผู้ใช้สิทธิและเสรีภาพเพื่อการมีส่วนร่วมในประเด็นสาธารณะจากการถูกฟ้องคดี.

สมาคมนักกฎหมายสิทธิมนุษยชน. (2564). สถานการณ์การฟ้องคดีปิดปากในประเทศไทย : มีกลไกกลั่นกรองแล้วแต่ทำไมแนวโน้มคดียังสูงขึ้นต่อเนื่อง.

สำนักงาน กสทช. (2564). รายงานอัตราค่าบริการโทรคมนาคมประจำปี 2564.

สำนักงาน กสทช. (2564). รายงานสภาพตลาดโทรคมนาคมของประเทศไทย ประจำไตรมาสที่ 3 ปี 2564.

สำนักงาน กสทช.. (2565). รายงานข้อมูลการกำกับดูแลกิจการโทรคมนาคม ไตรมาส 1 ปี 2565.

สำนักงานสถิติแห่งชาติ. (2564). รายงานตัวชี้วัด ITU โครงการสำรวจ ICTครัวเรือน 2564.

สำนักเลขาธิการคณะรัฐมนตรี. รายงานผลการดำเนินงานของรัฐบาล พลเอกประยุทธ จันทร์โอชา.

เอกสารภาษาอังกฤษ

ข้อมติสมัชชาใหญ่แห่งสหประชาชาติ

United Nation General Assembly. (1993). Vienna Declaration and Programme of Action. (A/CONF.157/23)

United Nation General Assembly. (2005). United Nation General Assembly resolution 60/147 Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law. (A/RES/60/147).

United Nation General Assembly. (2014). United Nation General Assembly Resolution 68/167. The right to privacy in the digital age. (A/RES/68/167)

United Nation General Assembly. (2015). United Nation General Assembly Resolution 69/166. The right to privacy in the digital age. (A/RES/69/166)

United Nation General Assembly. (2017). United Nation General Assembly Resolution 71/199. The right to privacy in the digital age. (A/RES/71/199)

United Nation General Assembly. (2019). United Nation General Assembly Resolution 73/1979. The right to privacy in the digital age. (A/RES/73/179)

ข้อมติคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ

United Nations Human Rights Council. (2009). Human Rights Council Resolution 12/16 Freedom of opinion and expression. (A/HRC/RES/12/16)

United Nations Human Rights Council. (2011). Human Rights Council Resolution 17/4 Human rights and transnational corporations and other business enterprises. (A/HRC/RES/17/4)

United Nations Human Rights Council. (2011). United Nations Guiding Principles on Business and Human Rights (UNGPs)

United Nations Human Rights Council. (2012). Human Rights Council Resolution 20/8. The promotion, protection and enjoyment of human rights on the Internet. (A/HRC/RES/20/8)

United Nations Human Rights Council. (2013). Human Rights Council Resolution 23/2. The role of freedom of opinion and expression in women's empowerment. (A/HRC/RES/23/2)

United Nations Human Rights Council. (2014). Human Rights Council Resolution 26/13 The promotion, protection and enjoyment of human rights on the Internet. (A/HRC/RES/26/13)

United Nations Human Rights Council. (2015). Human Rights Council Resolution 28/16. The right to privacy in the digital age. (A/HRC/RES/28/16)

United Nations Human Rights Council. (2016). Human Rights Council Resolution 32/13. The promotion, protection and enjoyment of human rights on the Internet. (A/HRC/RES/32/13)

United Nations Human Rights Council. (2017). Human Rights Council Resolution 34/7. The right to privacy in the digital age. (A/HRC/RES/34/7)

United Nations Human Rights Council. (2018). Human Rights Council Resolution 38/7. The promotion, protection and enjoyment of human rights on the Internet. (A/HRC/RES/38/7)

United Nations Human Rights Council. (2019). Human Rights Council Resolution 41/11 New and emerging digital technologies and human rights. (A/HRC/RES/41/11)

United Nations Human Rights Council. (2020). Human Rights Council Resolution 44/12 Freedom of opinion and expression. (A/HRC/RES/44/12)

ความเห็นทั่วไปของคณะกรรมการสิทธิมนุษยชนแห่งสหประชาชาติ

United Nation Human Rights Committee. (1993). General Comment No. 22: Freedom of Thought, Conscience or Religion. CCPR/C/21/Rev.1/Add.4. (CCPR General Comment No. 22)

United Nation Human Rights Committee. (1996). General Comment No. 25: The right to participate in public affairs, voting rights and the right of equal access to public service. CCPR/C/21/Rev.1/Add.7. (CCPR General Comment No. 25)

United Nation Human Rights Committee. (2011). General Comment No. 16: Article 17 (Right to Privacy). (CCPR General Comment No. 16)

United Nation Human Rights Committee. (2004). General Comment No. 31 : The Nature of the General Legal Obligation Imposed on States Parties to the Covenant. CCPR/C/21/Rev.1/Add.13. (CCPR General Comment No. 31)

United Nation Human Rights Committee. (2011). General Comment No. 34 : Article 19, Freedoms of opinion and expression. CCPR/C/GC/34. (CCPR General Comment No. 34)

รายงานของกระบวนการพิเศษภายใต้คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. (2011). The right to freedom of opinion and expression exercised through the Internet. (A/66/290)

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. (2011). Key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet. (A/HRC/17/27)

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. (2012). Hate speech and incitement to hatred. (A/67/357)

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. (2013). The implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression. (A/HRC/23/40)

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. (2013). The right to access information. (A/68/362)

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. (2015). The use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age. (A/HRC/29/32).

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. (2016). Freedom of expression, states and the private sector in the digital age. (A/HRC/32/38).

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. (2016). Contemporary challenges to freedom of expression. (A/71/373).

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. (2017). The role of digital access providers. (A/HRC/35/22).

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. (2018). Artificial Intelligence technologies and implications for the information environment. (A/73/348).

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. (2018). Online content regulation. (A/HRC/38/35).

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. (2018). Overview of submission received in preparation of the Report of the Special Rapporteur (A/HRC/38/35). (A/HRC/38/35/Add.1).

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. (2019). Online hate speech. (A/74/486).

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. (2019). Surveillance and human rights. (A/HRC/41/35).

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan. (2021). Disinformation and freedom of opinion and expression. (A/HRC/47/25).

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan. (2022). Disinformation and freedom of opinion and expression during armed conflicts. (A/77/288).

UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheini. (2009). the protection of the right to privacy in the fight against terrorism. (A/HRC/13/37)

UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheini. (2010). Compilation of good practices on legal and institutional frameworks and measures that ensure respect for

human rights by intelligence agencies while countering terrorism, including on their oversight. (A/HRC/14/46)

UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson. (2012). Framework principles for securing the human rights of victims of terrorism. (A/HRC/20/14)

UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson. (2014). Counter terrorism and mass digital surveillance. (A/69/397)

UN Special Rapporteur on the right to privacy, Joseph A. Cannataci. (2017). Governmental surveillance activities from a national and international perspective. (A/HRC/34/60)

UN Special Rapporteur on the right to privacy, Joseph A. Cannataci. (2018). Security and Surveillance. (A/HRC/37/62)

UN Special Rapporteur on the right to privacy, Joseph A. Cannataci. (2018). Big Data and Open Data. (A/73/438)

UN Special Rapporteur on the right to privacy, Joseph A. Cannataci. (2019). Privacy, technology and other human rights from a gender perspective. (A/HRC/40/63)

UN Special Rapporteur on the right to privacy, Joseph A. Cannataci,. (2020). Data protection and surveillance in relation to COVID-19. (A/75/147)

UN Special Rapporteur on the right to privacy, Joseph A. Cannataci,. (2021). Artificial intelligence and privacy, and children's privacy. (A/HRC/46/37)

UN Special Rapporteur on the right to privacy, Joseph A. Cannataci,. (2021). How pandemics can be managed with respect to the right to privacy. (A/76/220)

UN Special Rapporteur on the sale of children, Maud de Boer-Buquicchio. (2014). child prostitution and child pornography. (A/HRC/28/56)

UN Special Rapporteur on violence against women. (2018). Online violence against women and girls. (A/HRC/38/47)

คำแถลงร่วมของผู้เชี่ยวชาญด้านเสรีภาพในการแสดงออก (Joint Declaration)

UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media and OAS Special Rapporteur on Freedom of Expression, London. (2002). Joint Declaration on Freedom of Expression and the Administration of Justice, Commercialisation and Freedom of Expression and Criminal Defamation. (Joint Declaration, 2002).

UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media and OAS Special Rapporteur on Freedom of Expression. (2004). Joint declaration on access to information. (Joint declaration, 2004).

UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media and OAS Special Rapporteur on Freedom of Expression. (2005). Joint declaration on the internet and anti-terrorism measures. (Joint Declarations, 2005). Available at: https://www.osce.org/fom/27455

UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information. (2011). Joint declaration on freedom of expression and the internet. (Joint Declaration, 2011).

UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information. (2014). Joint Declaration on Universality and the Right to Freedom of Expression. (Joint Declaration, 2014).

UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information. (2017). Joint declaration on freedom of expression and “fake news”, disinformation and propaganda. (Joint declaration, 2017).

UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information. (2018). Joint Declaration on Media Independence and Diversity in the Digital Age. (Joint Declaration, 2018).

เอกสารอื่นในวงงานขององค์กรสหประชาชาติ

Gagliardone, Iginio, et al.. (2015). Countering online hate speech. UNESCO.

Human Rights Council Advisory Committee. (2021). Possible impacts, opportunities and challenges of new and emerging digital technologies with regard to the promotion and protection of human rights. (A/HRC/47/52)

Ireton, Cherilyn [editor] and Posetti, Julie [editor]. (2018). Journalism, fake news & disinformation: handbook for journalism education and training. UNESCO.

Kalina Bontcheva and Julie Posetti (eds.). (2020). Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression. UNESCO Broadband Commission Report.

Mendel, Toby, et al.. (2012). Global survey on Internet privacy and freedom of expression. Paris: UN, UNESCO.

UN Commission on Human Rights. (1984). The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights. (E/CN.4/1985/4)

United Nations. (2020). United Nations Strategy and Plan of Action on Hate Speech : Detailed Guidance on Implementation for United Nations Field Presences.

United Nations High Commissioner for Human Rights (OHCHR). (2012). The corporate responsibility to respect human rights: an interpretive guide.

United Nations High Commissioner for Human Rights (OHCHR). (2013). Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (Rabat Plan of Action). ใน A/HRC/22/17/Add.4, Appendix.)

United Nations High Commissioner for Human Rights (OHCHR). (2014). The right to privacy in the digital age (focus on surveillance). (A/HRC/27/37)

United Nations High Commissioner for Human Rights (OHCHR). (2014). Summary of the Human Rights Council panel discussion on the right to privacy in the digital age. (A/HRC/28/39)

United Nations High Commissioner for Human Rights (OHCHR). (2018). The right to privacy in the digital age. (A/HRC/39/29)

United Nations High Commissioner for Human Rights (OHCHR). (2021). The right to privacy in the digital age : Artificial Intelligence (AI). (A/HRC/48/31)

United Nations High Commissioner for Human Rights (OHCHR). (2020). The UN Guiding Principles in the Age of Technology : A B-Tech Foundational Paper.

United Nations High Commissioner for Human Rights (OHCHR). (8 February 2021). “Thailand: UN experts alarmed by rise in use of lèse-majesté laws”.

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2011). UNESCO ICT Competency Framework for Teachers.

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2022). The Training Manual for Judges on International Standards on Freedom of Opinion and Expression.

United Nation Human Rights Committee. (2014). Concluding observations on the fourth periodic report of the United States of America. CCPR/C/USA/CO/4.

United Nation Human Rights Committee. (2015). Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland. CCPR/C/GBR/CO/7.

United Nation Human Rights Committee. (2017). Concluding observations on Thailand. CCPR/C/THA/CO/2.

United Nations Human Rights Council. (2021). Universal Periodic Review – Thailand, Third Cycle.

United Nation Thailand. (2020). Remarks of Secretary-General to the UN Human Rights Council on “The Highest Aspiration: A Call to Action for Human Rights”.

Working Group on Internet Governance (WGIG). (2015). Report of the Working Group on Internet Governance.

World Summit on the Information Society (WSIS). (2003). Geneva Declaration of Principles, Building the Information Society: a global challenge in the new Millennium. (WSIS-03/GENEVA/DOC/4-E)

World Summit on the Information Society (WSIS). (2005). Tunis Agenda for The Information Society. (WSIS-05/TUNIS/DOC/6(Rev. 1)-E)

คดีภายใต้ศาลสิทธิมนุษยชนแห่งยุโรป

European Court of Human Rights. (1990). Kruslin v. France. (Application no. 11801/85). 24 April 1990.

European Court of Human Rights. (2006). Weber and Saravia v. Germany. (Application no. 54934/00). 29 June 2006.

European Court of Human Rights. (2010). Uzun v. Germany. (Application No. 35623/05). 2 September 2010.

European Court of Human Rights (2010). Kennedy v. United Kingdom. (Application No. 26839/05). 18 May 2010.

European Court of Human Rights. (2015). Roman Zakharov v. Russia. (Application no. 47143/06). 4 December 2015.

European Court of Human Rights. (2019). Catt v. the United Kingdom. (Application No. 43514/15). 24 January 2019

เอกสารที่จัดทำโดยองค์กรระหว่างรัฐบาลระดับภูมิภาค ภาควิชาการ ภาเอกชน และภาคประชาสังคม

ACCESSNOW. (28 APRIL 2022). Internet shutdowns in 2021: the return of digital authoritarianism.

ARTICLE 19. (1996). The Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

ARTICLE 19. (2009). The Camden Principles on Freedom of Expression and Equality.

ARTICLE 19. (2012). International standards: Right to information.

ARTICLE 19. (2015). “Hate Speech” Explained: A Toolkit.

ARTICLE 19. (2016). Freedom of Expression Unfiltered: How Blocking and Filtering Affect Free Speech.

Asia-Europe Foundation (ASEF). (2012). Human Rights and Information and Communication Technology. Proceedings of the 12th Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights, 27 – 29 June 2012, Seoul, Republic of Korea

Association for Progressive Communications (APC). (2017). Unshackling expression: A study on laws criminalising expression online in Asia.

Association for Progressive Communications (APC). (2018). Content regulation in the digital age: Submission to the United Nations Special Rapporteur on the right to freedom of opinion and expression.

Association for Progressive Communications (APC). (2020) .APC Internet Rights Charter.

Association for Progressive Communications (APC) and Derechos Digitales. (2022). Internet shutdowns and human rights.

Bill Marczak and others. (2018). "Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries". Citizen Lab.

Center for Democracy and Technology. (2017). Mixed Messages? The Limits of Automated Media Content Analysis.

Citizen Lab. (2014). Information Controls during Thailand's 2014 Coup.

Commission on Science and Technology for Development (2015). Mapping of international Internet public : policy issues. (E/CN.16/2015/CRP.2)

Council of Europe, Committee of Ministers. (2003). Declaration on Freedom of Communication on the Internet.

Electronic Frontier Foundation and a coalition of NGOs. (2014). International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles" or "13 Principles").

Gill, Lex and Redeker, Dennis and Gasser. (2015). Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights. Berkman Center Research Publication No. 2015-15.

Global Network Initiative (GNI). (2017). GNI Principles on Freedom of Expression and Privacy.

Global Network Initiative (GNI). (2022). GNI Submission to the High Commissioner Report on the Practical Application of the UNGPs in the Technology Sector.

ICANN. (2013). "Montevideo Statement on the Future of Internet Cooperation".

Internet Rights and Principles Dynamic Coalition. (2011). The Charter of Human Rights and Principles for the Internet.

International Telecommunication Union (ITU). (2022). Global Connectivity Report 2022.

Johan Eriksson and Giampiero Giacomello. (2009). “Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State”. International Studies Review, Volume 11, Issue 1, March 2009.

Jonathan McCully. (2019). Digital rights are *all* human rights, not just civil and political.

Josh A. Goldstein, et al.. (2020). Cheerleading Without Fans: A Low-Impact Domestic Information Operation by the Royal Thai Army.

Jun-E. (2019) "Exploring the Nexus Between Technologies and Human Rights: Opportunities and Challenges in Southeast Asia".

Klaus Stoll and Sam Lanfranco. (2019). Internet Governance and the Universal Declaration of Human Rights, Part 1: Foundations.

Manushya Foundation, et al. (2021). Digital Rights in Thailand: Joint Submission to the UN Universal Periodic Review (UPR) to Thailand's Third UPR Cycle 39th Session of the UPR Working Group.

Media Legal Defence Initiative. (2018). Mapping Digital Rights and Online Freedom of Expression in East, West and Southern Africa

Open Observatory of Network Interference (OONI). (2017). The State of Internet Censorship in Thailand.

Perset, K. (2010). "The Economic and Social Role of Internet Intermediaries". OECD Digital Economy Papers, No. 171. OECD Publishing.

Privacy International. “Privacy and Human Rights: An International Survey of Privacy Laws and Practice”.

Privacy International. (2017). “Who’s That Knocking at My Door? Understanding Surveillance in Thailand”.

Shift and Institute for Human Rights and Business (IHRB). (2011). ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights. European Commission.

Simon Kemp. (2022). “Digital 2022: Thailand”.

Samuel D. Warren and Louis D. Brandeis. (1890). The Right to Privacy. Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.

Twitter Blog. (8 October 2020). Disclosing networks to our state-linked information operations archive.

ข้อมูลจากสื่อ/ข่าว

ฐานเศรษฐกิจ. (25 กรกฎาคม 2562). Facebook ลบเพจและบัญชีผู้ใช้ 'ป่วน' ในไทยกว่า 20 ราย.

เดอะแสตนดาร์ด. (23 สิงหาคม 2564). Twitter เผย ‘10 แฮชแท็ก’ ยอดนิยมของไทยช่วงครึ่งปีแรก 2021 มาครบทั้งเรื่องสังคมและวัฒนธรรม เช่น โควิด-19, น้าค่อม, ย้ายประเทศกันเถอะ, อแมนด้า และ แบมแบม เป็นต้น.

เดอะแสตนดาร์ด. (6 พฤศจิกายน 2563). Twitter ประเทศไทยแจงกรณีแอ็กเคานต์ เยาวชนปลดแอก และฟอร์ด ทัตเทพ ถูกระงับ เหตุละเมิดกฎการบิดเบือนระบบ สแปม.

เดอะแสตนดาร์ด. (4 มีนาคม 2564). Facebook ลบ 185 บัญชีและกลุ่มที่เกี่ยวข้องกับปฏิบัติการ IO ของกองทัพไทย.

โตมร ศุขปรีชา. (28 ธันวาคม 2563). โซเชียลเน็ตเวิร์ก : เชื่อมต่อคนห่างไกลหรือมหันตภัยแห่งยุค. The 101.

ไทยพีบีเอส. (9 ตุลาคม 2555). “ล่าแม่มด – เซ็กส์ - ความรุนแรง ภัยเงียบออนไลน์ที่สังคมไทยต้องรู้ให้เท่าทัน”.

ไทยพีบีเอส. (28 พฤษภาคม 2557). คสช.แถลง ไม่ได้สั่งปิดเฟซบุ๊ก.

ไทยพีบีเอส (27 กุมภาพันธ์ 2562). ศาลปกครอง เพิกถอนคำสั่ง กสทช. จอดำ "วอยซ์ ทีวี".

ไทยรัฐออนไลน์. (31 กรกฎาคม 2561). ธนาธร เข้าให้ข้อมูล ปอท. คดีไลฟ์สด พาดพิง คสช. ดูดอดีต ส.ส.

ไทยรัฐออนไลน์. (20 กรกฎาคม 2563). โซเชียลแชร์ความเห็น ติดแฮชแท็ก ถ้าการเมืองดี จะเห็น-ไม่เห็นอะไรในประเทศไทย.

บีบีซีไทย. (24 กันยายน 2563). เฟซบุ๊ก: กระทรวงดิจิทัลฯ แจ้งความดำเนินคดีเฟซบุ๊ก-ทวิตเตอร์ ไม่ปิดการเข้าถึงเพจผิดกฎหมาย.

บีบีซีไทย. (1 ธันวาคม 2563). ไอโอ : คณะก้าวหน้าเปิดโปงข้อมูลเครือข่ายปฏิบัติการข่าวสารกองทัพ ด้านเอกชนแถลงโต้ชี้ข้อมูลบิดเบือน.

ประชาไท. (21 ตุลาคม 2563). ด่วน! ศาลอาญายกเลิกคำร้องปิดวอยซ์ทีวี รวมทั้ง 'เยาวชนปลดแอก' ด้วย.

มติชนออนไลน์. (9 ตุลาคม 2563). ‘ทบ.’ โต้ ‘ทวิตเตอร์’ กองทัพไม่มีบัญชีไอโอโจมตีฝ่ายค้าน มีแค่บัญชีใช้ประชาสัมพันธ์.

วอยซ์ออนไลน์. (4 มกราคม 2564). เพลง 'ปฏิรูป' กลุ่ม R.A.D. ถูกปิดกั้นการเข้าถึงใน YOUTUBE.

สปริงนิวส์. (6 พฤศจิกายน 2563). ทวิตเตอร์ "เยาวชนปลดแอก-ฟอร์ด-เจมส์" กลับมาใช้งานได้ตามปกติแล้ว.

สำนักข่าวไทย. (24 สิงหาคม 2563). บช.น. ชี้แจงกรณีใช้รถตัดสัญญาณในพื้นที่ชุมนุม.

สำนักข่าวอิศรา. (7 กันยายน 2561). 'ฮิวแมนไรท์' ร้องไทยหยุดดำเนินคดี 12 มือโพสต์ข้อมูลสาวอังกฤษอ้างถูกข่มขืนบนเกาะเต่า.

สำนักงานศาลยุติธรรม. เพจเฟ็ซบุ๊ค “สื่อศาล”. เผยแพร่ 26 กรกฎาคม 2564.

สำนักงานศาลยุติธรรม. ศาลอาญาวางแนวปฏิบัติพิจารณาคำร้องปิดเว็บ เน้นไต่สวน 2 ฝ่ายให้โอกาสคัดค้านควบคู่ทำเร็วแจ้งไต่สวนไม่เกิน 7 วัน มองความมั่นคงมิติตุลาการสร้างกระบวนพิจารณาเป็นธรรม สังคมศรัทธาเชื่อใจ ไม่มุ่งแค่ปราบปราม.

BBC. (8 March 2010.). “Is access to the internet a fundamental human right?”.

BBC. (16 October 2020). “Thailand blocks Change.org as petition against king gains traction”.

Cerf, Vint (2012). Internet Access is not a Human Right. New York Times.

Prachatai. (9 October 2020). “YouTube locally blocks speech about monarchy reform at Thai government’s request”.

The Nation. (12 June 2014). Telenor must comply with martial law: NBTC.

The Nation. (15 June 2014). Telenor Group apologises for saying dtac ordered to block Facebook.

TNW. (9 June 2014). Telenor says Thailand's recent Facebook outage was ordered by the government.

Wats, J. (2013). "Amazon v the Amazon: internet retailer in domain name battle". The Guardian.

แหล่งข้อมูลออนไลน์อื่น

โครงการศึกษากฎหมายและมาตรการป้องกันการดำเนินคดีเชิงยุทธศาสตร์เพื่อระงับการมีส่วนร่วมของสาธารณะในบริบทธุรกิจกับสิทธิมนุษยชน, ข้อมูลการฟ้องคดีปิดปาก (SLAPPs) โดยภาคธุรกิจ

ไทยรัฐ และ DTAC. Cyberbullying

ภาพรวมเอกสารที่กล่าวถึงสิทธิดิจิทัล รวบรวมโดยโครงการวิจัยนี้

สำนักงาน กสทช. สรุปสถิติที่น่าสนใจในกิจการโทรคมนาคม ปี 2564.

Bangkok Post. การระบาดของ "ข่าวปลอม" ในสถานการณ์ Covid-19.

Broadband Commission for Sustainable Development, ITU, UNESCO. MAKE BROADBAND AFFORDABLE.

Freedom House. (2022). Thailand Freedom on the Net.

International Telecommunication Union (ITU). ITU-D ICT Statistics : Data and analytics: taking the pulse of the information society.

Google Transparency Report, Government Requests to Remove Content, "Requests: Thailand," https://transparencyreport.google.com/government-removals/government-requests/TH

Meta Transparency Cente, https://transparency.fb.com/data/content-restrictions/country/TH/

OOKLA. Thailand Median Speeds August 2022.

OOKLA 5G MAP

The Economist Intelligence Unit. The Inclusive Internet Index 2021.

Twitter Transparency, https://transparency.twitter.com/en/reports/countries/th.html

United Nations High Commissioner for Human Rights (OHCHR), B-Tech Project

United Nations. Hate speech

สัมภาษณ์

พรเพ็ญ คงขจรเกียรติ, ผู้อำนวยการมูลนิธิผสานวัฒนธรรม, สัมภาษณ์วันที่ 13 กรกฎาคม 2564, ผ่านระบบอิเล็กทรอนิกส์ (ZOOM)

โสภณ หนูรัตน์. หัวหน้าฝ่ายคุ้มครองและพิทักษ์สิทธิ์ผู้บริโภค สภาองค์กรของผู้บริโภค, สัมภาษณ์วันที่ 18 กรกฎาคม 2564, ผ่านระบบอิเล็กทรอนิกส์ (ZOOM)

อานนท์ ชวาลาวัณย์, หัวหน้าศูนย์ข้อมูลกฎหมายและคดีเสรีภาพ โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw), สัมภาษณ์วันที่ 21 กรกฎาคม 2564, ผ่านระบบอิเล็กทรอนิกส์ (ZOOM)

นพพล อาชามาส , หัวหน้าฝ่ายข้อมูลฯ ศูนย์ทนายความเพื่อสิทธิมนุษยชน, สัมภาษณ์วันที่ 23 กรกฎาคม 2564, ผ่านระบบอิเล็กทรอนิกส์ (ZOOM)

สฤณี อาชวานันทกุล, เครือข่ายพลเมืองเน็ต (Thai Netizen Network) สัมภาษณ์วันที่ 5 สิงหาคม 2564 , ผ่านระบบอิเล็กทรอนิกส์ (ZOOM)

สุภิญญา กลางณรงค์, ผู้ร่วมก่อตั้งโครงการโคแฟค (Cofact) ประเทศประเทศไทย, สัมภาษณ์วันที่ 17 สิงหาคม 2564, ผ่านระบบอิเล็กทรอนิกส์ (ZOOM)

วาสนา เกล้านพรัตน์, ผู้อำนวยการศูนย์พิทักษ์สิทธิเด็ก สัมภาษณ์วันที่ 3 ธันวาคม 2564, ผ่านระบบอิเล็กทรอนิกส์ (ZOOM)

ภาคผนวก

ภาคผนวก ก

สรุปการประชุมกลุ่มย่อย (Focus Group)
โครงการศึกษาวิจัยเพื่อพัฒนาข้อเสนอแนะในการส่งเสริมและคุ้มครองสิทธิมนุษยชน
กรณีการดำเนินการด้านเทคโนโลยีสารสนเทศและการสื่อสารออนไลน์
(หน่วยงานภาครัฐ)
วันที่ 31 มีนาคม 2565 เวลา 09.30 – 12.00 น. ผ่านระบบอิเล็กทรอนิกส์ (ZOOM)

โดยมีตัวแทนหน่วยงานรัฐที่เกี่ยวข้องเข้าร่วมประมาณ 30 คน ได้แก่ ตัวแทนสำนักงาน กสทช., กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ, สำนักงานกองทุนพัฒนาสื่อปลอดภัยและสร้างสรรค์, สำนักงานศาลยุติธรรม, สำนักงานอัยการสูงสุด, สำนักงานคณะกรรมการคุ้มครองผู้บริโภค, กรมคุ้มครองสิทธิและเสรีภาพ กระทรวงยุติธรรม, กรมกิจการเด็กและเยาวชน กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์, สถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ, สำนักงานตำรวจแห่งชาติ, สำนักงานสภาความมั่นคงแห่งชาติ, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC NSTDA), สำนักงานปลัดกระทรวงศึกษาธิการ กระทรวงศึกษาธิการ และสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

กองทุนสื่อปลอดภัยและสร้างสรรค์

- กองทุนสื่อปลอดภัย จัดตั้งปี 2558 ให้ทุนปีแรก 2560 เป็นต้นมา โดยปี 2563 เปิดรับ 4 ประเด็น คือ (1) การส่งเสริมกลไกเฝ้าระวัง เท่าทัน (2) การบุลลี่ออนไลน์ (3) การรับมือข่าวปลอม และ (4) การรู้เท่าทันสื่อ และในปี 2564 เปิดรับประเด็นโทษและความเสี่ยงของสื่อออนไลน์ 7 โครงการ (งบประมาณรวม 10 ล้านบาท) และปี 2565 มีเสนอโครงการ ใน 5 ประเด็น คือ (1) ชีวิตวิถีใหม่ กับสังคมดิจิทัล (2) พหุวัฒนธรรม ความหลากหลาย (3) ความเท่าทันรู้ทัน (4) สามัคคีปรองดอง (5) รับมือข่าวลวง ข่าวปลอม
- มีการทำงานกับสื่อมวลชน ผ่านการฝึกอบรมการตรวจสอบข่าว Fact-checking

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

- ทำงาน 5 ภูมิภาค ในเรื่องข่าวปลอม ทำเรื่องการรับรู้ และตรวจสอบข่าวปลอม โดยเน้น การรู้เท่าทันข่าวปลอม
- โครงการ Net ประชารัฐ ในโซนหมู่บ้าน (24,700 หมู่บ้าน) ที่ DE รับผิดชอบ คือเป็นชุมชนห่างไกล ไม่มีศักยภาพเชิงพาณิชย์ ประสาน บริษัทโทรมนาคมแห่งชาติ ดำเนินการเสร็จสิ้นในปี 2564 และจะมีการประสาน

เชื่อมใช้ ขยายไปที่เอกชนรายย่อยช่วยสนับสนุนการทำงาน และทำเป็น Open Access และเน้นค่าใช้จ่ายที่ไม่สูง (affordable) มีการแจ้งให้ผู้ใหญ่บ้านหรือหน่วยพื้นที่ เชื่อมต่อกับเน็ตประชารัฐ ดำเนินการติดตั้งเสร็จสิ้นแล้ว

- ยอดคนเข้าใช้งานเน็ตประชารัฐ 10,873,305 ล้านคน (ณ วันที่ 31 มีนาคม 2565)
- มติ ครม. 1 กุมภาพันธ์ 2565 เห็นชอบร่างการดำเนินการข่าวปลอม ปัจจุบัน อยู่ระหว่างการแจ้งเวียนขอความเห็นในการปรับปรุงของแต่ละหน่วยงานที่เกี่ยวข้อง

สำนักงานปลัดกระทรวงศึกษาธิการ

- ศธ. ทำการอบรมในโรงเรียน เสริมสร้างความรู้เรื่องการรังแกออนไลน์ และในโรงเรียน เพื่อให้รับมือกับการแก้ไขปัญหาได้ มีการณรงค์ สร้างความเข้าใจการแกล้งรังแกเด็ก

กสทช.

- กสทช, รับผิดชอบเน็ตประชารัฐพื้นที่โซน C+ จำนวน 3,900 หมู่บ้าน และพื้นที่ 15,7320 หมู่บ้าน โดยแบ่งเป็นหน่วยให้บริการทั้ง WiFi โรงเรียน อปท. และอื่น ๆ
- การอบรมให้ความรู้ ด้านการพัฒนา สื่อดิจิทัล การอบรม 8 หลักสูตร สำหรับ 8 กลุ่ม อาทิ ประชาชนทั่วไป ผู้สูงอายุ ครู/นักเรียน พิการ ด้อยโอกาสและรายได้น้อย และอื่น ๆ

NECTEC

- การดูแลศูนย์เฉพาะทาง คนพิการ ทั้ง hard และ software โดยใช้ competencies ทั้งเสียง การได้ยิน และเทคโนโลยีที่เกี่ยวข้องมาช่วย
- สิทธิที่เกี่ยวข้องกับ FEO ทำระบบ e-voting ใช้ในระบบเข้าไปที่โรงเรียนเอกชน และโรงเรียนสาธิต มศว. ประสานมิตร เป็นจุดทดลอง ดูการเข้าถึงสิทธิและเสียง
- ในเรื่อง information security มีระบบการยืนยันตัวตน หลาย ๆ factors อาทิ เข้าผ่าน username + password และ authentic ผ่านมือถือ และมีระบบ check-in ตาม location based ด้วย
- การพัฒนา AI โดยพัฒนา Responsible AI (จริยธรรม AI) โดยใช้พื้นฐาน 16 ด้าน อาทิ ความเท่าเทียม เชื่อถือได้ ความเป็นส่วนตัว ความมั่นคง ความครอบคลุม และตรวจสอบได้ โดยทุกอย่างที่เกี่ยวกับ data มีการจัดแบ่งข้อมูลส่วนบุคคลที่อ่อนไหว โดยใช้เทคโนโลยีจัดแยก มีเรื่องการเข้ารหัส และการปกป้องข้อมูล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- พรบ. คุ้มครองข้อมูลส่วนบุคคลฯ เน้นมาตรการ มาตรฐาน ความปลอดภัย การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล การทำกิจกรรมใด ๆ ต้องมีมาตรฐาน เพื่อให้การใช้ไม่ผิดแปลกไปจากวัตถุประสงค์ในการใช้ หรือรวบรวม โดยมีเรื่องความปลอดภัยด้วย
- การใช้บังคับครอบคลุมผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล โดยเฉพาะในราชอาณาจักรไทย แต่นอกราชอาณาจักร เป็นการเสนอสินค้า หรือข้อมูล หรือการเฝ้าระวังการติดตาม
- ใน พรบ. กล่าวถึง การเก็บรวบรวม การใช้ข้อมูลส่วนบุคคล เพื่อประโยชน์ส่วนตน ดังนั้น ตีความว่าหากเจ้าของข้อมูล post ใน FB เอง จะถือเป็นเรื่องของเจ้าของข้อมูล
- ส่วนระบบ AI หากมีการนำข้อมูลไปใช้ ต้องแจ้งให้เจ้าของข้อมูลทราบว่า จะไม่มีผลกระทบใด ๆ ต่อเจ้าของข้อมูล
- ระยะเริ่มต้นของการบังคับใช้กฎหมาย การเก็บข้อมูลจะมีการแจ้ง เรื่องวัตถุประสงค์ของการใช้ข้อมูลกับเจ้าของข้อมูล และขอรับ consent จากเจ้าของข้อมูล / ผู้นำข้อมูลไปประมวลผล คือ ผู้ควบคุมข้อมูล ต้องแจ้งเจ้าของข้อมูล และมาตราที่เกี่ยวข้อง รวมถึงการนำข้อมูลมาใช้ต้องพิจารณาความอ่อนไหวเพิ่มเติม

สภาความมั่นคงแห่งชาติ

- การทำยุทธศาสตร์ความมั่นคงปี 25660-2565 ยุทธที่ 6 การเสริมสร้างการใช้งาน cyberspace และการปลูกฝังการใช้งาน เครือข่าย มีกระทรวงดิจิทัลฯ และอื่น ๆ รับผิดชอบหลัก
- สมช. ให้ความสำคัญกับเรื่องความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน โดยขอให้หน่วยต่าง ๆ พิจารณาความมั่นคงด้านนี้ด้วย
- มีการทำงานเรื่องการส่งเสริม media/digital literacy / cyber bullying/ hate speech มีกระทรวงดิจิทัลฯ สธ. อว. วธ. ศธ. เข้ามาส่งเสริมความรู้ / แผนกำลังเสนอ ครม. และขับเคลื่อนต่อไป จะเป็นภูมิคุ้นกันระยะยาว
- สมช. กำลังยกร่างแผนความมั่นคง (ระดับ 2) ปี 2566 เป็นต้นไป เน้นความมั่นคงชาติ และของมนุษย์และสิทธิมนุษยชนเป็นพื้นฐาน การดำเนินการด้านต่าง ๆ นำเรื่องสิทธิมนุษยชน เป็นพื้นฐานดำเนินงาน การปรับปรุงกฎหมายให้ทันสมัยมากขึ้น รวมถึง cyber bullying เป็นเรื่องที่เกี่ยวกับเสรีภาพทาง ออนไลน์ การแสดงความเห็น ความปลอดภัย และการคุกคามต่าง ๆ เป็นการดูเรื่องทัศนคติ และการมองมิติความมั่นคงแบบองค์รวม โดยมิได้หมายถึงมิติด้านหนึ่งด้านใดเท่านั้น เป็นสร้าง mindset ที่ทำให้เห็นความแตกต่างหลากหลาย

สำนักงานคณะกรรมการความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (สกมช.)

- ดูแลภาพรวมนโยบาย และ พรบ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีการกำกับ ประสานหน่วยงาน 7 ด้าน ทำหน้าที่ดูแล ทั้งการติดตาม การละเมิด การแฮ็ก การขาย การค้า โดยจะติดตามและประสานกับหน่วยงานที่เกี่ยวข้องต่อไป

- กรณีการโจมตี ณ ปัจจุบัน เป็นการล้วงข้อมูล การนำข้อมูลไปขายต่อ เพื่อได้มาซึ่งเงิน (สกุลดิจิทัล) ข้อมูลที่รั่วไหล คือ ข้อมูลสุขภาพ การเงิน เป็นส่วนที่ล่อแหลม แต่การดูแลครอบคลุมทั้ง 7 ด้าน โดยยังไม่เห็นการแฮ็กข้อมูลความมั่นคงในประเทศไทย พบแต่ข้อมูลลูกค้า นักเรียนที่จะเข้าสอบ
- สกมช. สนับสนุนการทำให้บริการของรัฐมีความปลอดภัย อาทิ หมอพร้อม ซึ่งมีการลงทะเบียน ID ต่าง ๆ ตรงนี้ทาง สกมช. จะเน้นเป็นพิเศษ
- ในช่วงสถานการณ์ COVID สกมช. ขอให้ช่วยกันสร้างความตระหนักรู้ การรักษาความปลอดภัย ข้อมูล และความเป็นส่วนบุคคล ซึ่งขอให้คำนึงถึงการรักษาความปลอดภัย และความลับของข้อมูลด้วย

สำนักงานศาลยุติธรรม

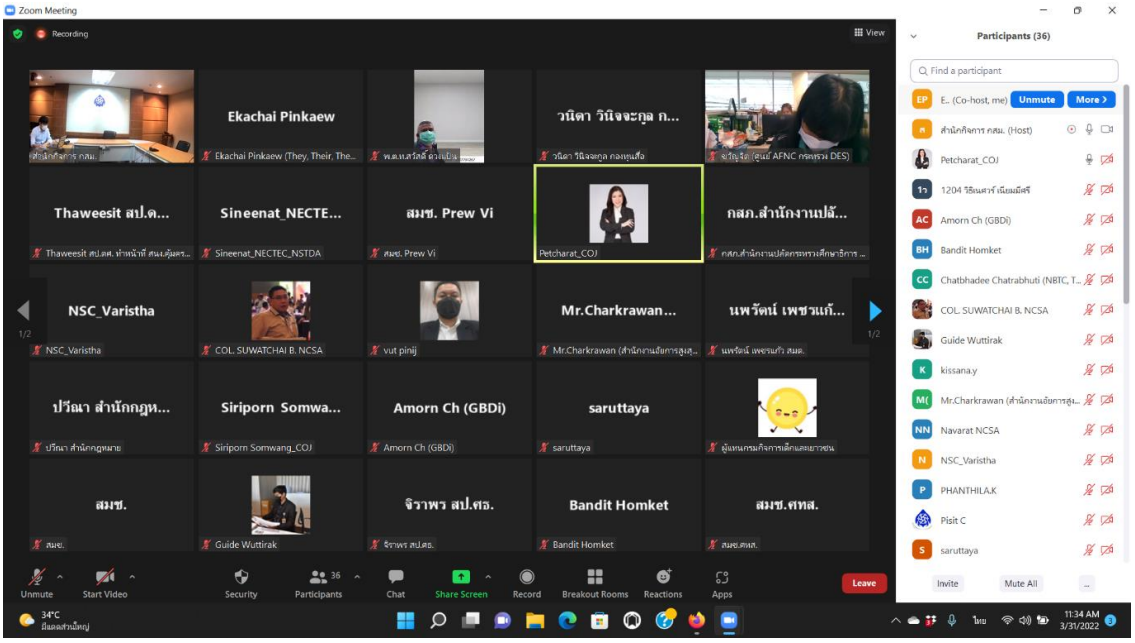
- การทำระบบของศาล มีการใช้ดิจิทัลครอบคลุมทั้งคดีอาญา คดีค้ามนุษย์ โดยเป็นไปตามคำแนะนำของ ปธ.ศาลฎีกา
- นโยบายหลัก ๆ ของสำนักงานศาลยุติธรรม เน้นการคุ้มครองสิทธิของผู้บริโภค ทำให้ง่ายต่อการเข้าถึงกระบวนการยุติธรรม ในส่วนของอาญา ไม่มีการเน้นมากนัก แต่มีการเผยแพร่ความรู้ ทั้งการอบรม fake news กับศาล หรือหน่วยงานภายนอก สร้างความร่วมมือต่าง ๆ
- การคุ้มครองสิทธิของประชาชน มีเรื่องคดีฉ้อโกง cyber bullying และ hate speech จำนวนมาก โดยส่วนใหญ่ต้องการค่าสินไหมทดแทน หรือการขอโทษ
- เมตาเวิร์ส สำนักงานศาล กำลังศึกษา และมีเรื่องของกฎหมาย อาทิ ทรัพย์สินทางปัญญาด้วย
- นำระบบระบบอิเล็กทรอนิกส์มาใช้เพื่อให้เข้าถึงกระบวนการยุติธรรมได้ง่ายขึ้น ตั้งแต่ปี 2542 ทำ e-court จนเป็น smart-court เน้น easy access to justice แต่เป็นด้านคดีแพ่งเป็นหลัก
- ช่วงสถานการณ์ COVID-19 ศาลนำระบบเทคโนโลยีมาใช้ การติดตามผลคดีออนไลน์ tracking system โดยดูความคืบหน้า การขอคัดสำเนาเอกสาร และทำได้ในทุกศาลทั่วประเทศ
- ส่วนการนำ AI มาใช้ สำนักงานศาลยุติธรรม กำลังพิจารณา โดยเห็นว่า (1) ระบบ AI ใช้ใน chatbot ก่อน ในการทำ SMART AI แต่ AI ยังไม่สามารถนำมาใช้ในการประมวลผล (อาทิ การประกันตัว หรืออื่น ๆ) และการพิจารณาพิพากษา ยังต้องใช้การทำงานของผู้พิพากษาจริง ๆ

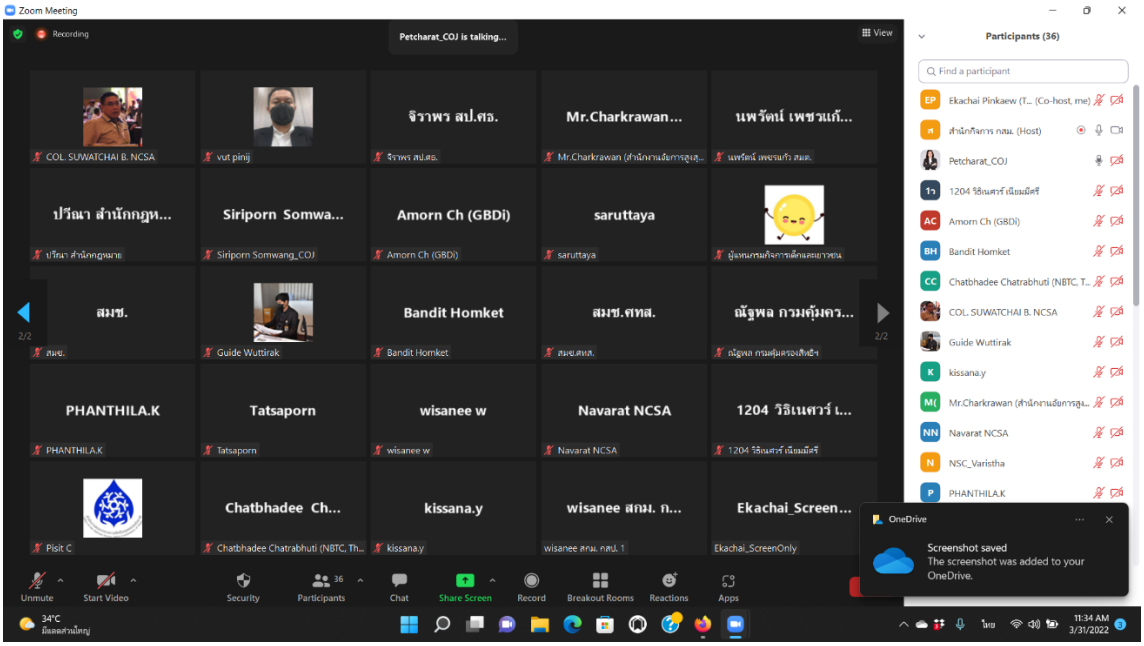
กรมคุ้มครองสิทธิและเสรีภาพ กระทรวงยุติธรรม

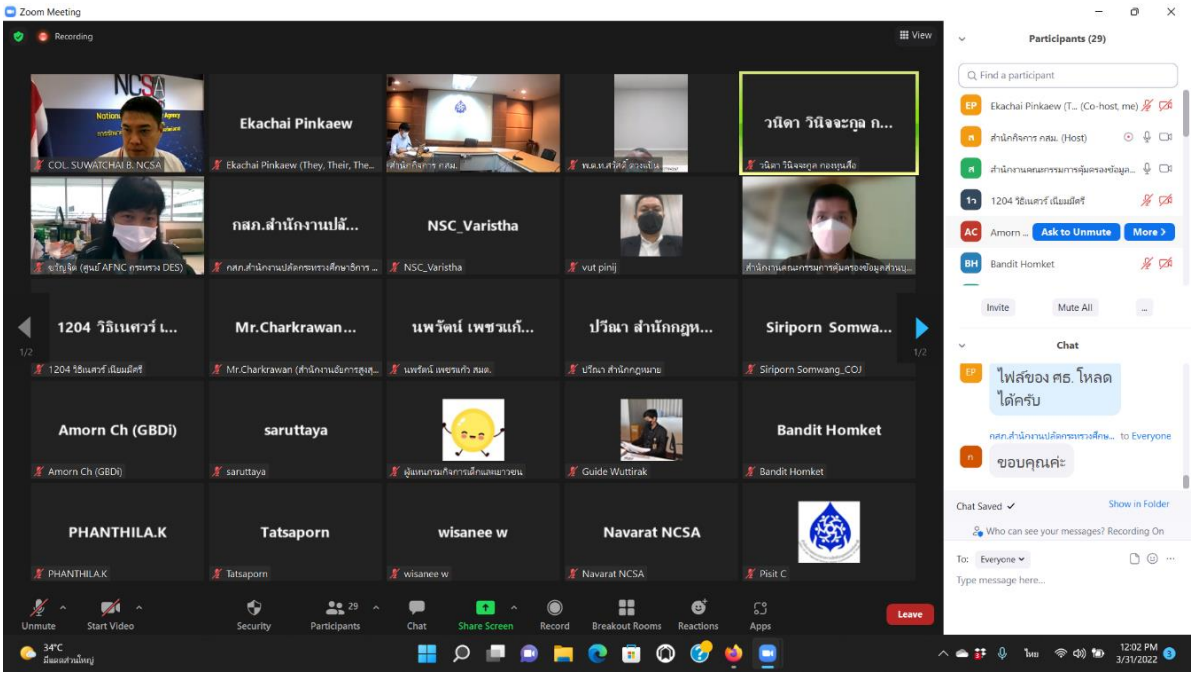
- งานให้การช่วยเหลือ ส่งเสริม และคุ้มครองเยียวยา ตั้งแต่ต้นน้ำ การมุ่งเน้นทำให้การละเมิดสิทธิมนุษยชนในสังคมไทยลดลง โดยใช้แผนสิทธิมนุษยชน ฉบับที่ 4 และแผนปฏิบัติการระดับชาติว่าด้วยธุรกิจกับสิทธิมนุษยชน
- การนำระบบดิจิทัลมาใช้การช่วยเหลือดูแลเหยื่อ การเชื่อมโยงประสานกับหน่วยงานต่าง ๆ การทำให้ระบบที่มีอยู่เชื่อมโยงกับหน่วยงานภาครัฐ ภาคเอกชน และการเชื่อมโยงระบบกับตำรวจ ประกันภัย หรือภาคธุรกิจ

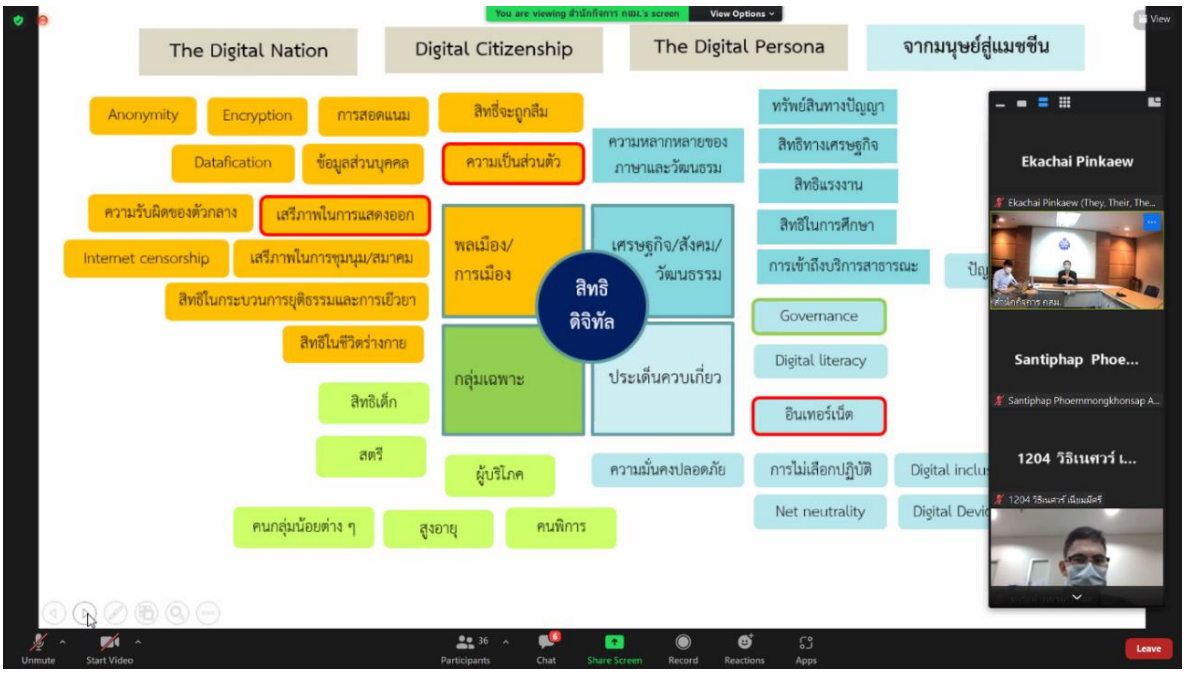
ต่าง ๆ โดยกรมคุ้มครองสิทธิฯ มีระบบการรองรับ การส่งเสริมสิทธิ การเก็บข้อมูล และข้อมูลในการช่วยเหลือเป็นส่วนที่จะเกิดขึ้นในอนาคต

- ส่วน Hate Speech กรมฯ ยังไม่ได้ทำโดยตรง แต่ ยธ. มีการตั้งคณะกรรมการดูแล มีรองปลัดกระทรวงยุติธรรมเป็นประธาน และมีผู้แทนหน่วยงานต่าง ๆ เข้ามาสนับสนุนการทำงาน




Zoom Meeting
Recording
Petcharat_COJ is talking...
View
Participants (36)
Find a participant
COL. SUWATCHAI B. NCSA
vut pinij
จิราพร สป.ศธ.
Mr.Charkrawan...
นพรัตน์ เพชรแก้...
ปรีณา สำนักกฎหม...
Siriporn Somwa...
Amorn Ch (GBDi)
saruttaya
สมช.
Guide Wuttirak
Bandit Homket
สมช.ศทส.
ณัฐพล กรมคุ้มครอ...
PHANTHILA.K
Tatsaporn
wisanee w
Navarat NCSA
1204 วิริเนตวร์ เ...
Pisit C
Chatbhadee Ch...
kissana.y
wisanee สคม. ก...
Ekachai_Screen...
OneDrive
Screenshot saved
The screenshot was added to your OneDrive.
Unmute
Start Video
Security
Participants
Chat
Share Screen
Record
Breakout Rooms
Reactions
Apps
34°C
11:34 AM
3/31/2022


Zoom Meeting
Recording
View
Participants (29)
Find a participant
COL. SUWATCHAI B. NCSA
Ekachai Pinkaew
Ekachai Pinkaew (They, Their, The...
วนิดา วินิจจะกุล ก...
กสภ.สำนักงานปลั...
NSC_Varistha
vut pinij
1204 วิริเนตวร์ เ...
Mr.Charkrawan...
นพรัตน์ เพชรแก้...
ปรีณา สำนักกฎหม...
Siriporn Somwa...
Amorn Ch (GBDi)
saruttaya
Bandit Homket
PHANTHILA.K
Tatsaporn
wisanee w
Navarat NCSA
Pisit C
Ask to Unmute
More
Invite
Mute All
Chat
ไฟล์ของ ศธ. โหลดได้ครับ
ขอบคุณค่ะ
Chat Saved
Show in Folder
Who can see your messages? Recording On
To: Everyone
Type message here...
Leave
Unmute
Start Video
Security
Participants
Chat
Share Screen
Record
Breakout Rooms
Reactions
Apps
34°C
12:02 PM
3/31/2022


You are viewing สำนักกิจการ กสม.'s screen
View Options
The Digital Nation
Digital Citizenship
The Digital Persona
จากมนุษย์สู่แมชชีน
Anonymity
Encryption
การสอดแนม
สิทธิ์จะถูกลืม
Datafication
ข้อมูลส่วนบุคคล
ความเป็นส่วนตัว
ความรับผิดของตัวกลาง
เสรีภาพในการแสดงออก
Internet censorship
เสรีภาพในการชุมนุม/สมาคม
สิทธิในกระบวนการยุติธรรมและการเยียวยา
สิทธิในชีวิตร่างกาย
สิทธิเด็ก
สตรี
ผู้บริโภค
คนกลุ่มน้อยต่าง ๆ
สูงอายุ
คนพิการ
พลเมือง/การเมือง
เศรษฐกิจ/สังคม/วัฒนธรรม
สิทธิดิจิทัล
กลุ่มเฉพาะ
ประเด็นควบเกี่ยว
ความหลากหลายของภาษาและวัฒนธรรม
ความมั่นคงปลอดภัย
ทรัพย์สินทางปัญญา
สิทธิทางเศรษฐกิจ
สิทธิแรงงาน
สิทธิในการศึกษา
การเข้าถึงบริการสาธารณะ
Governance
Digital literacy
อินเทอร์เน็ต
การไม่เลือกปฏิบัติ
Net neutrality
Ekachai Pinkaew
Ekachai Pinkaew (They, Their, The...
Santiphap Phoe...
Santiphap Phoemmongkhonsap A...
1204 วิธิเนศวร์ เ...
Unmute
Start Video
Participants
Chat
Share Screen
Record
Reactions
Apps
Leave

ประวัติผู้วิจัย

ชื่อนักวิจัย (ภาษาไทย) บัณฑิต หอมเกษ

(ภาษาอังกฤษ) Bandit Homket

ตำแหน่งปัจจุบัน นักวิชาการสิทธิมนุษยชนปฏิบัติการ

สังกัด กลุ่มงานวิจัยสิทธิมนุษยชน

สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

กรุงเทพมหานคร

ติดต่อ bandit.nhrc@gmail.com

ประวัติการศึกษา

ปริญญาตรี **:** นิติศาสตร์บัณฑิต มหาวิทยาลัยมหาสารคาม

ปริญญาโท : ศิลปศาสตรมหาบัณฑิต (สิทธิมนุษยชนและสันติศึกษา)

มหาวิทยาลัยมหิดล

สาขาวิชาการที่สนใจ สิทธิมนุษยชน, กฎหมาย, กระบวนการยุติธรรม

ผลงานที่ผ่านมา

การต่อสู้เหนือพื้นที่ป่า : การต่อสู้และต่อรองของชุมชนชาติพันธุ์กะเหรี่ยงเพื่อสิทธิการจัดการพื้นที่ป่าในบริบทการผลักดันให้กลุ่มป่าแก่งกระจานเป็นมรดกโลก (วิทยานิพนธ์)

การต่อสู้ของกลุ่มชาติพันธุ์กะเหรี่ยงเพื่อสิทธิในที่ดินและทรัพยากรธรรมชาติในพื้นที่อุทยานแห่งชาติแก่งกระจาน (บทความนำเสนอในการประชุมเสนอผลงานวิจัยระดับชาติ มหาวิทยาลัยสุโขทัยธรรมาธิราช ครั้งที่ 11 ปี 2564)