

ศาลยุติธรรมกับการรักษาคุณภาพระหว่างเสรีภาพในการสื่อสาร
กับการรักษาความมั่นคงบนสังคมออนไลน์

โดย

นายพงษ์เดช วานิชกิตติกุล
เลขาธิการประธานศาลฎีกา
สำนักประธานศาลฎีกา

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 56
ประจำปีการศึกษา พุทธศักราช 2556 - 2557

บทคัดย่อ

เรื่อง ศาลยุติธรรมกับการรักษาคุณภาพระหว่างเสรีภาพในการสื่อสารกับการรักษา
ความมั่นคงบนสังคมออนไลน์

ลักษณะวิชา การเมือง

ผู้วิจัย นายพงษ์เดช วานิชกิตติกุล

หลักสูตร วปอ. รุ่นที่ 56

หลายทศวรรษที่ผ่านมาเทคโนโลยีสารสนเทศได้พัฒนาอย่างรวดเร็วและยังมีแนวโน้มที่จะพัฒนาต่อไปอีกมาก ทำให้การติดต่อสื่อสาร ซึ่งเป็นสิทธิขั้นพื้นฐานของมนุษย์ ในยุคปัจจุบันเป็นไปด้วยความสะดวก รวดเร็ว ประหยัด กว้างขวางและครอบคลุมพื้นที่ทั่วโลก ในขณะเดียวกันการใช้เทคโนโลยีสารสนเทศในปัจจุบันก็ส่งผลในทางลบและกระทบต่อความมั่นคงของประเทศได้ เช่น การส่งข้อมูลอันเป็นเท็จเพื่อปลุกกระแสความเกลียดชังในกลุ่มคน ใช้ข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ชอบ เจาะระบบข้อมูลของรัฐ เป็นต้น

การใช้เทคโนโลยีสารสนเทศเพื่อการสื่อสารระหว่างบุคคลจึงอาจถูกตรวจสอบโดยรัฐเพื่อรักษาความมั่นคงปลอดภัยของรัฐ แต่มาตรการที่ควบคุมต้องถูกต้อง เหมาะสม และเป็นธรรม ในงานวิจัยฉบับนี้มุ่งศึกษาวิธีการรักษาคุณภาพของสิทธิในการสื่อสารของบุคคลและการรักษาความมั่นคงของประเทศ โดยเสนอให้ศาลยุติธรรมเป็นผู้ควบคุมดูแลพนักงานเจ้าหน้าที่ที่จะเข้าไปค้นหาข้อมูลต่าง ๆ โดยไม่ให้กระทบกับข้อมูลส่วนบุคคลและความเป็นส่วนตัวของประชาชน

คำนำ

ปัจจุบันเทคโนโลยีสารสนเทศได้พัฒนาไปอย่างรวดเร็ว ช่วยให้การติดต่อสื่อสารระหว่างบุคคลเป็นไปได้อย่างสะดวก รวดเร็ว และประหยัด และยังเกิดรูปแบบของการติดต่อสื่อสารกันมากมายหลากหลายรูปแบบ รูปแบบหนึ่งที่ประชาชนใช้งานกันมากและเป็นที่ยอมรับหลายคือ การส่งข้อความในกลุ่ม ที่เรียกว่า โครงข่ายสังคมออนไลน์ (Social Network) ในขณะที่การติดต่อสื่อสารกันในรูปแบบนี้เพิ่มมากขึ้นและมีโปรแกรมสนทนาลักษณะนี้มากมาย ปัญหาที่เกิดขึ้นจากโครงข่ายสังคมออนไลน์ก็เพิ่มขึ้น ไม่ว่าจะเป็นข้อมูลหรือข่าวสารที่เป็นเท็จ การใช้สังคมออนไลน์หมิ่นประมาทผู้อื่น การนำข้อมูลส่วนบุคคลของผู้อื่น ไปใช้แสวงหาประโยชน์โดยไม่ชอบ หรือใช้สื่อสังคมออนไลน์ปลุกกระดมให้เกิดการชุมนุม ซึ่งสามารถนำไปสู่ปัญหาที่กระทบต่อความมั่นคงของประเทศได้ งานวิจัยเรื่อง “สาละยุดิธรรมกับการรักษาคุณภาพระหว่างเสรีภาพในการสื่อสารกับการรักษาความมั่นคงบนสังคมออนไลน์” เขียนขึ้นเพื่อแสดงให้เห็นปัญหาที่เกิดจากการใช้สื่อสารสนเทศสมัยใหม่กับความมั่นคงของประเทศ และเสนอแนะแนวทางที่จะรักษาคุณภาพของสิทธิขั้นพื้นฐานของประชาชนกับการปฏิบัติหน้าที่ของเจ้าพนักงานในการรักษาความมั่นคงของประเทศ

(นายพงษ์เดช วานิชกิตติกุล)

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร

หลักสูตร วปอ. รุ่นที่ 56

ผู้วิจัย

สารบัญ

	หน้า
บทคัดย่อ	ก
คำนำ	ข
กิตติกรรมประกาศ	ค
สารบัญ	ง
สารบัญแผนภาพ	ฉ
บทที่ 1 บทนำ	1
ความเป็นมาและความสำคัญของปัญหา	1
วัตถุประสงค์ของการวิจัย	3
ขอบเขตของการวิจัย	3
วิธีดำเนินการวิจัย	3
ประโยชน์ที่ได้รับจากการวิจัย	3
บทที่ 2 แนวคิด และหลักการของเสรีภาพในการสื่อสาร	4
หลักสากลที่รับรองและคุ้มครองเสรีภาพในการสื่อสาร	4
ความสัมพันธ์กับสิทธิในความเป็นส่วนตัว	9
หลักความคุ้มครองเสรีภาพในการสื่อสาร	13
ความคุ้มครองตามประมวลกฎหมายแพ่งและพาณิชย์ และประมวลกฎหมายอาญา	14
ความคุ้มครองตามกฎหมายอื่น ๆ	15
บทที่ 3 ข้อจำกัด และวิวัฒนาการของการสื่อสารในส่วนที่เกี่ยวข้อง	
ความมั่นคงของชาติ	19
ข้อจำกัดตามหลักสากล	20
ข้อจำกัดตามกฎหมาย	23
วิวัฒนาการของการสื่อสาร	30
วิธีปฏิบัติของหน่วยงานที่เกี่ยวข้อง	38

สารบัญ (ต่อ)

	หน้า
บทที่ 4 การควบคุมเสรีภาพในการสื่อสารของประเทศสหรัฐอเมริกา	42
พระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ ค.ศ. 1978	42
กฎหมายที่เกี่ยวข้องและวิธีดำเนินการตรวจสอบโดยศาล	49
บทที่ 5 สรุป และข้อเสนอแนะ	58
สรุป	58
ข้อเสนอแนะ	60
บรรณานุกรม	62
ประวัติย่อผู้วิจัย	65

สารบัญแผนภาพ

แผนภาพที่		หน้า
3-1	ตัวอย่างเว็บไซต์ที่ใช้งานโปรโตคอล HTTPS ซึ่งการเชื่อมต่อจะมีการรับข้อมูลไปรับรองอิเล็กทรอนิกส์ เพื่อให้แอปพลิเคชันฝั่งผู้ใช้งานพิจารณาความถูกต้องก่อนจะใช้งานต่อไป	36
3-2	ขั้นตอนการทำงานของโปรโตคอล HTTPS	37

บทที่ 1

บทนำ

ความเป็นมาและความสำคัญของปัญหา

อินเทอร์เน็ตเป็นระบบเครือข่ายของการเชื่อมโยงคอมพิวเตอร์ ที่มีผู้ใช้งานจำนวนมาก จากทั่วทุกมุม โลก เป็นช่องทางหนึ่งที่สำคัญในปัจจุบันที่คนใช้ในการติดต่อสื่อสารระหว่างกัน ด้วยความสะดวกและรวดเร็วในการใช้งานประกอบกับไม่มีข้อจำกัดด้านพื้นที่ อินเทอร์เน็ตจึงเติบโตขึ้นอย่างรวดเร็วในทุกประเทศทั่วโลก

ประเทศไทยเริ่มมีการใช้อินเทอร์เน็ตตั้งแต่ปี 2530 โดยเริ่มต้นจากการใช้งานของสถาบันการศึกษา และขยายตัวออกไปสู่ภาคธุรกิจในปี 2537 ความต้องการมีมากขึ้น จึงมีการให้บริการเชิงพาณิชย์ขึ้น ในรูปแบบของผู้ให้บริการอินเทอร์เน็ตที่มีการเรียกเก็บค่าใช้บริการที่เรียกว่า Internet Service Provider (ISP) จนกระทั่งการใช้งานอินเทอร์เน็ตของคนไทย เริ่มเข้ามาสู่การใช้งานเพื่อติดต่อสื่อสารกันมากขึ้นในปัจจุบัน ทั้งนี้เป็นผลมาจากการพัฒนาในสิ่งต่อไปนี้

1. การพัฒนาอย่างรวดเร็วของเทคโนโลยีสารสนเทศ เป็นการส่งเสริมและกระตุ้นให้ใช้อินเทอร์เน็ตเพื่อติดต่อสื่อสารระหว่างกัน เพิ่มมากขึ้นอย่างรวดเร็วในคนทุกเพศทุกวัย
2. การพัฒนาโทรศัพท์เคลื่อนที่ ให้สามารถตอบสนองความต้องการของคนในการติดต่อสื่อสารระหว่างกัน โดยสามารถส่งข้อความร่วมกับรูปภาพและเสียง
3. การคิดค้นและพัฒนาแอปพลิเคชันต่าง ๆ เพื่อนำมาใช้งานร่วมกับคอมพิวเตอร์ และ โทรศัพท์เคลื่อนที่

จนในปัจจุบันกล่าวได้ว่า คนไทยมีการใช้อินเทอร์เน็ตเพื่อติดต่อสื่อสารกันมากที่สุดประเทศหนึ่งในโลก โดยมีการประยุกต์คอมพิวเตอร์และเทคโนโลยีสารสนเทศสมัยใหม่มาใช้เพื่อติดต่อสื่อสารกันในรูปแบบต่าง ๆ เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) การสนทนาและแสดงความคิดเห็นในหน้าเว็บบอร์ด (Webboard) และการติดตามข่าวสาร เป็นต้น

รูปแบบของการติดต่อสื่อสารกันบนโลกออนไลน์ได้มีการเปลี่ยนแปลงครั้งใหญ่ อีกครั้งหนึ่ง เมื่อเกิดการคิดค้นรูปแบบของการติดต่อสื่อสารกันบนอินเทอร์เน็ต เมื่อมีการสร้างนวัตกรรมที่ให้คุณคนสามารถสร้างเครือข่ายเพื่อติดต่อสื่อสารระหว่างบุคคลและระหว่างกลุ่ม เรียกว่า เครือข่ายสังคมออนไลน์ (Social Network หรือ Social Media) เช่น Twitter Facebook Whatsapp หรือ Line เป็นต้น

เครือข่ายสังคมออนไลน์ เป็นเว็บพื้นฐานในการบริการให้แต่ละบุคคลสามารถสร้างเครือข่ายของตนเองอย่างเป็นระบบ สามารถสร้างบัญชีรายชื่อของกลุ่มผู้ติดต่อที่สามารถติดต่อสื่อสาร และแลกเปลี่ยนความเห็นหรือสิ่งที่สนใจเหมือน ๆ กันได้ ซึ่งมีลักษณะ 3 ประการ ดังนี้

1. เป็นพื้นที่ที่มีการสื่อสาร 2 ทาง โดยไม่มีข้อจำกัดเรื่องเวลาและสถานที่ ขอให้ให้มีเครื่องมือและอุปกรณ์ที่จะสามารถเข้าสู่อินเทอร์เน็ตได้เท่านั้น
2. เป็นพื้นที่ที่ไม่อาจมีการควบคุมหรือปิดกั้นได้อย่างสมบูรณ์
3. เป็นพื้นที่ของคนชั้นกลาง เพราะราคาโดยเฉลี่ยของอุปกรณ์หรือเครื่องมือที่จะติดต่อสื่อสารกันบนอินเทอร์เน็ตประมาณ 30,000 บาท

การใช้วิธีการสื่อสารออนไลน์ก่อให้เกิดการแลกเปลี่ยนข้อมูลข่าวสารกันได้อย่างสะดวกรวดเร็ว และรับรู้ในวงกว้างภายในระยะเวลาอันสั้น ซึ่งบ่อยครั้งที่ก่อให้เกิดปรากฏการณ์ของการรวมตัวกันของกลุ่มที่มีความคิดเห็นเหมือนหรือคล้ายคลึงกัน ก่อให้เกิดปรากฏการณ์ที่เรียกว่า ฟลัชชันวัยพริบตา (Flash mob) หรือในบางกรณีอาจเกิดการแพร่กระจายของข้อมูลข่าวสารที่เป็นเท็จหรือขัดต่อความเป็นจริง ก่อให้เกิดความตระหนกตกใจแก่ประชาชน ก่อให้เกิดความสับสนวุ่นวายในบ้านเมืองได้

การเกิดฟลัชชันวัยพริบตาอาจเป็นไปได้ในด้านบวกหรือลบต่อสังคมโดยรวมก็ได้ หรือการเกิดข่าวลือทางการเมืองที่สร้างความสับสนวุ่นวายในประเทศอย่างมาก จนฝ่ายปกครองเกิดแนวคิดที่จะตรวจสอบข้อมูลการใช้อินเทอร์เน็ตของบุคคลบนโลกออนไลน์ในลักษณะของการสุ่ม โดยที่ไม่จำเป็นต้องมีเหตุตามกฎหมายก่อนที่จะใช้อำนาจในการป้องกันและคุ้มครองความสงบเรียบร้อยหรือความมั่นคงของประเทศก่อนแต่อย่างใด ซึ่งการกระทำดังกล่าวถูกมองว่าเป็นการละเมิดสิทธิเสรีภาพส่วนบุคคลที่ได้รับการคุ้มครองตามกฎหมาย

ในกรณีดังกล่าว เคยเกิดกรณีที่นาย เอ็ดเวิร์ด สโนว์เดน (Edward Snowden) ได้เปิดเผยข้อมูลว่า ทางการของสหรัฐอเมริกาได้ใช้อำนาจตามกฎหมายให้ผู้ใช้บริการอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์เปิดเผยข้อมูลการใช้อินเทอร์เน็ตในการติดต่อสื่อสารกัน จนเกิดการวิพากษ์วิจารณ์การกระทำดังกล่าวของทางการสหรัฐอเมริกา และเกิดคำถามถึงความเหมาะสมและขอบเขตของการใช้อำนาจ

วัตถุประสงค์ของการวิจัย

งานวิจัยฉบับนี้จึงต้องการ

1. ศึกษาแนวคิด ของการคุ้มครองเสรีภาพในการสื่อสารระหว่างกันของบุคคลตามกฎหมาย
2. ศึกษาแนวคิด ในการแทรกแซงเสรีภาพในการสื่อสารของบุคคลเพื่อรักษาความมั่นคงของรัฐ
3. ศึกษาบทบาทของศาลยุติธรรม ในการรักษาดุลยภาพระหว่างเสรีภาพส่วนบุคคล และการรักษาความมั่นคงของประเทศ

ขอบเขตของการวิจัย

ศึกษากรณีของการใช้สังคมออนไลน์ในประเทศไทย เปรียบเทียบกับแนวคิด และวิธีปฏิบัติของประเทศสหรัฐอเมริกา

วิธีดำเนินการวิจัย

ศึกษาวิจัยในเชิงคุณภาพ (Qualitative Research) โดยการศึกษาแนวคิด ทฤษฎี ข้อเท็จจริง และกฎหมายต่าง ๆ ค้นคว้าและรวบรวมข้อมูลจากเอกสาร บทความ หนังสือ รายงานวิจัยวิทยานิพนธ์ ข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้อง ทั้งภาษาไทยและภาษาต่างประเทศ เพื่อนำข้อมูลที่ได้มาวิเคราะห์ ประเด็นปัญหาและเสนอแนวทางการแก้ไขอย่างเหมาะสม ซึ่งจะทำให้ศาลยุติธรรมเป็นตัวกลางในการรักษาดุลยภาพระหว่างเสรีภาพในการสื่อสารกับการรักษาความมั่นคงบนสังคมออนไลน์

ประโยชน์ที่ได้รับจากการวิจัย

1. ได้ทราบแนวคิดของการคุ้มครองเสรีภาพในการสื่อสาร
2. ได้ทราบเงื่อนไขและพฤติการณ์ที่เหมาะสมในกรณีที่รัฐจะแทรกแซงเสรีภาพในการสื่อสารของบุคคล
3. ได้ทราบบทบาทของศาลยุติธรรมในการรักษาดุลยภาพระหว่างเสรีภาพในการสื่อสารและการรักษาความมั่นคงของประเทศ

บทที่ 2

แนวคิดและหลักการของเสรีภาพในการสื่อสาร

หลักสากลที่รับรองและคุ้มครองเสรีภาพในการสื่อสาร

ระยะเวลาหลายทศวรรษที่ผ่านมา มนุษย์เริ่มมีความตื่นตัวเกี่ยวกับแนวความคิดว่าด้วยสิทธิมนุษยชนเพิ่มมากขึ้นจนเกิดการเรียกร้องสิทธิต่าง ๆ มากมาย และกลายเป็นกระแสความคิดที่ได้รับการยอมรับ เพราะเป็นเรื่องสิทธิตามธรรมชาติหรืออาจจะกล่าวได้ว่าเป็นสิทธิที่ติดตัวมนุษย์มาตั้งแต่เกิด จึงมีการนำแนวคิดนี้ไปใช้อย่างหลากหลาย ทั้งนี้ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ข้อ 1 กล่าวว่า “มนุษย์ทั้งปวงเกิดมามีอิสระและเสมอภาคกันในศักดิ์ศรีและสิทธิต่างในตน มีเหตุผลและมีโนธรรมและควรปฏิบัติต่อกันด้วยจิตวิญญาณแห่งภราดรภาพ”¹

สำหรับเสรีภาพในการสื่อสารนั้น อดีตเราอาศัยหลักเกณฑ์สำหรับวิธีการเดิม ๆ มาพิจารณาว่ากรณีใดเป็นการรุกรานการสื่อสาร (Invasiveness of Communication) ซึ่งหลักเกณฑ์เหล่านั้นไม่เหมาะสมแก่สถานการณ์ในปัจจุบัน เนื่องจากเดิมเราเชื่อว่าเนื้อหาของ การสื่อสารที่สำคัญ และควรค่าแก่การได้รับความคุ้มครอง เพราะอาจมีการนำเอาข้อมูลที่เป็นความลับออกมาเปิดเผย แต่เป็นที่ประจักษ์ชัดแล้วปัจจุบันว่าข้อมูลอื่นที่แม้ไม่ได้เป็นตัวเนื้อหาโดยตรงกลับเผยให้เห็นตัวตนของบุคคลได้มากกว่า และควรค่าแก่การได้รับความคุ้มครองไม่แพ้กัน

¹ กระทรวงการต่างประเทศ และ UN Country Team Thailand. ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน. (กรุงเทพมหานคร: กรมองค์การระหว่างประเทศ กระทรวงการต่างประเทศ, 2551). หน้า 20.

ทุกวันนี้ข้อมูลแต่ละชนิดไม่ว่าจะเป็นข้อมูลเดียวหรือหลายข้อมูลที่น่ามารวมกันแสดงให้เห็นรูปพรรณของบุคคล พฤติกรรม กลุ่มสังคมที่คบหา ลักษณะทางกายภาพ ประวัติทางการแพทย์ เชื้อชาติ สีผิว รสนิยมทางเพศ พื้นเพของชาติพันธุ์ มุมมอง หรือสามารถกำหนดแผนของตำแหน่งที่ตั้ง ความเคลื่อนไหว หรือการปฏิสัมพันธ์ในแต่ละช่วงเวลาของบุคคลหนึ่งหรือหลายบุคคลในบริเวณเขตพื้นที่ที่กำหนด เช่น ในการชุมนุมหรือในเหตุการณ์ทางการเมืองอื่น ๆ ดังนั้นข้อมูลทุกอย่างที่มี แสดงให้เห็น เป็นผลมาจาก หรือเกี่ยวข้องกับการติดต่อสื่อสารของบุคคล ซึ่งไม่มีปรากฏหรือหาได้ง่ายในที่สาธารณะอยู่แล้ว ควรเป็นข้อมูลที่ได้ความคุ้มครองสูงสุดตามกฎหมาย

1. ความหมายของสิทธิ เสรีภาพ และเสรีภาพในการสื่อสาร

สิทธิ (Right) คือ ประโยชน์ที่กฎหมายรับรองและคุ้มครองให้แก่บุคคลในอันที่จะกระทำการเกี่ยวกับทรัพย์สินหรือบุคคลอื่น เช่น สิทธิในทรัพย์สิน สิทธิในชีวิตและร่างกาย เป็นต้น

เสรีภาพ (Liberty) คือ ภาวะของมนุษย์ที่ไม่ตกภายใต้การครอบงำของผู้อื่น มีอิสระที่จะกระทำการหรืองดเว้นกระทำการ เช่น เสรีภาพในการติดต่อสื่อสาร เสรีภาพในการเดินทาง เป็นต้น

การสื่อสาร (Communication) เป็นพื้นฐานสำคัญของมนุษย์ซึ่งอยู่ร่วมกันเป็นสังคม กล่าวคือ เมื่อมีการอยู่ร่วมกัน มนุษย์ย่อมต้องมีปฏิสัมพันธ์ต่อกัน การให้และการรับความหมาย การถ่ายทอด และการรับสาร อันเป็นการแสดงความรู้สึก ความต้องการ หรือแลกเปลี่ยนข้อมูลข่าวสาร จากบุคคลหนึ่งไปยังอีกบุคคลหนึ่ง รวมถึง กิจกรรม การมีปฏิสัมพันธ์ และการทำธุรกรรม ที่ส่งผ่านสื่ออิเล็กทรอนิกส์ เป็นต้นว่า เนื้อหาการสื่อสาร การระบุตัวบุคคลคู่สนทนา ข้อมูลที่สามารถค้นหาตำแหน่งสถานที่ ซึ่งรวมถึงหมายเลขประจำเครื่องคอมพิวเตอร์ ช่วงเวลาและการเข้าถึงอุปกรณ์ที่ใช้ติดต่อสื่อสารนั้น

เสรีภาพในการสื่อสาร (Freedom of communication) หมายถึง เงื่อนไขของบุคคลที่จะสื่อสารโดยไม่ขึ้นต่อผู้หนึ่งผู้ใด และเป็นอำนาจหรือมีอำนาจที่จะสื่อสารหรือไม่สื่อสารก็ได้ การสื่อสารโดยผ่านเครือข่ายในรูปแบบต่าง ๆ รัฐบาลหรือเจ้าหน้าที่ของรัฐจะเข้าไปขัดขวางไปตรวจ ไปกัก ไปเผยแพร่ หรือไปดักฟังไม่ได้ เว้นแต่มีกฎหมายให้ทำได้เพื่อรักษาความมั่นคง เพื่อรักษาความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน² จึงถือว่าเสรีภาพในการสื่อสารเป็นสิทธิมนุษยชนขั้นพื้นฐานอย่างหนึ่งในอันที่จะต้องได้รับการคุ้มครอง ทั้งยังเกี่ยวกับสิทธิ

² เกรียงไกร เจริญธนาวัฒน์. “สิทธิของผู้เล่นเกมออนไลน์”. (ออนไลน์). เข้าถึงได้จาก : <http://www.pub-law.net/publaw/view.aspx?ID=609,2547>.

อันชอบธรรมที่จะดำรงความเชื่อของตนไว้ด้วยการสื่อสารถ่ายทอดความคิดความเชื่อของตนออกไป ซึ่งหมายความว่าต้องเข้าถึงทรัพยากรด้านการสื่อสารได้อย่างเสมอภาคเท่าเทียมกันอีกด้วย

2. หลักสากลเกี่ยวข้องกับเสรีภาพในการสื่อสาร

แนวคิดเกี่ยวกับเสรีภาพในการสื่อสารพัฒนาขึ้นจากการที่นักวิชาการอเมริกันและนักวิชาการตะวันตกกลุ่มหนึ่งซึ่งเชื่อว่าสิทธิในการสื่อสารเป็นสิทธิมนุษยชนขั้นพื้นฐาน สิทธินี้ไม่ได้มีอยู่โดด ๆ แต่ต้องอยู่ร่วมกับแนวความคิดในเรื่องความรับผิดชอบ ความเสมอภาค การสนทนาหลายฝ่าย การมีส่วนร่วม การโต้ตอบ และการพัฒนาการเข้าถึงข้อมูลข่าวสารและสื่อ³ อันเป็นสิทธิที่มีการรับรองไว้ในกฎหมายระหว่างประเทศที่สำคัญสองฉบับ คือ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights) และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant of Civil and Political Rights) ซึ่งประเทศไทยได้รับรองเป็นภาคีของทั้งสองฉบับ โดยร่วมรับรองปฏิญญาสากลว่าด้วยสิทธิมนุษยชน เมื่อวันที่ 10 ธันวาคม พ.ศ. 2491 และเข้าเป็นภาคีของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง เมื่อ 29 ตุลาคม พ.ศ. 2539

2.1 ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights) เมื่อวันที่ 10 ธันวาคม พ.ศ. 2491 ที่ประชุมสมัชชาสหประชาชาติ สมัยสามัญสมัยที่ 3⁴ ได้มีข้อมติรับรองปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ซึ่งมีเจตนารมณ์เพื่อรับรองและคุ้มครองสิทธิมนุษยชนของประชาชนทั่วโลกอย่างแท้จริง ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนดังกล่าว จึงถือว่าเป็นเอกสารที่มีความสำคัญอย่างยิ่งต่อการวางรากฐานด้านสิทธิมนุษยชนระหว่างประเทศอันเป็นมาตรฐานสากลที่ประเทศสมาชิกสหประชาชาติได้ร่วมกันจัดทำขึ้น นอกจากนี้ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนดังกล่าวยังเป็นพื้นฐานของการตรากฎหมายและการทำข้อตกลงระหว่างประเทศด้านสิทธิมนุษยชนฉบับต่าง ๆ ในระยะเวลาต่อมาด้วย โดยเฉพาะอย่างยิ่งอนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน

³ อุบลรัตน์ ศิริยุวศักดิ์. “สิทธิในการสื่อสารของประชาชนกับสิทธิมนุษยชน : วาทกรรมการต่อสู้ในเวทีสากล”. (ออนไลน์). เข้าถึงได้จาก : <http://www.freedom.comarts.chula.ac.th/articles/CRSU04.pdf>, 2544.

⁴ การประชุมดังกล่าวได้จัดขึ้น ณ กรุงปารีส ประเทศสาธารณรัฐฝรั่งเศส และปฏิญญาสากลว่าด้วยสิทธิมนุษยชนดังกล่าวได้รับการประกาศในราชกิจจานุเบกษาของประเทศสาธารณรัฐฝรั่งเศส (le Journal Officiel) เมื่อวันที่ 19 กุมภาพันธ์ ค.ศ. 1949

ทั้งนี้ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน มีวัตถุประสงค์และหลักการทั่วไปเกี่ยวกับมาตรการด้านสิทธิมนุษยชน แต่ไม่มีพันธะผูกพันในแง่ของกฎหมายระหว่างประเทศ อันประกอบด้วยการรับรองสิทธิมนุษยชนในด้านต่าง ๆ จำนวน 30 ข้อ ซึ่งสามารถนำมาจัดกลุ่มได้เป็น 4 กลุ่ม คือ

1. สิทธิมนุษยชนเบื้องต้น
2. สิทธิพลเมืองและสิทธิทางการเมือง
3. สิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม
4. หน้าที่ความรับผิดชอบของทุกคนต่อระเบียบสังคม และการรับรอง

สิทธิมนุษยชนและเสรีภาพพื้นฐานระหว่างประเทศ

โดยมีบทบัญญัติที่เกี่ยวข้องกับเสรีภาพในการสื่อสาร คือ ข้อ 12 บัญญัติว่า “บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกหลอกลวงหรือขู่ข่มขู่และชื่อเสียงมิได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการหลอกลวงดังกล่าวนี้”⁵ และ

ข้อ 19 บัญญัติว่า “ทุกคนมีสิทธิในอิสรภาพแห่งความเห็นและการแสดงออก ทั้งนี้ สิทธินี้รวมถึงอิสรภาพที่จะถือเอาความเห็นโดยปราศจากการแทรกแซงและที่จะแสวงหา รับ และส่งข้อมูลข่าวสารและข้อคิดผ่านสื่อใด และโดยไม่คำนึงถึงพรมแดน” กล่าวคือมนุษย์ทุกคนมีสิทธิและเสรีภาพในการแสดงออกซึ่งความคิดเห็น รับ และส่งข้อมูลข่าวสารใด ๆ โดยปราศจากการแทรกแซง เช่น การปิดกั้นการสื่อสารไม่ว่าทางโทรศัพท์ โทรทัศน์ หรืออินเทอร์เน็ต การแทรกแซงสื่อ และการดักฟังทางโทรศัพท์ เป็นต้น

2.2 กติการะหว่างประเทศ ว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant of Civil and Political Rights หรือ ICCPR) เป็นสนธิสัญญาพหุภาคีซึ่งสมัชชาใหญ่แห่งสหประชาชาติได้ให้การรับรองเมื่อวันที่ 16 ธันวาคม พ.ศ. 2509 และมีผลใช้บังคับเมื่อ 23 มีนาคม พ.ศ. 2519 สนธิสัญญานี้ให้คำมั่นสัญญาว่าภาคีจะเคารพสิทธิพลเมืองและสิทธิทางการเมืองของบุคคล ซึ่งรวมถึงสิทธิในชีวิต เสรีภาพในศาสนา เสรีภาพในการพูด เสรีภาพในการรวมตัว สิทธิเลือกตั้ง และสิทธิในการได้รับการพิจารณาความอย่างยุติธรรม

⁵ กระทรวงการต่างประเทศ และ UN Country Team Thailand. ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน. (กรุงเทพมหานคร: กรมองค์การระหว่างประเทศ กระทรวงการต่างประเทศ, 2551). หน้า 23.

กติการะหว่างประเทศฯ นี้เป็นส่วนหนึ่งของ "International Bill of Human Rights" ร่วมกับปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights) และกติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม (International Covenant on Economic, Social and Cultural Rights หรือ ICESCR) โดยมีการติดตามตรวจสอบโดยคณะกรรมการสิทธิมนุษยชน (Human Rights Committee) ซึ่งตั้งขึ้นอย่างถาวร เพื่อพิจารณา รายงานตามกำหนดเวลาที่ส่งเข้ามาโดยรัฐสมาชิกตามข้อตกลงในสนธิสัญญา สมาชิกของคณะกรรมการสิทธิมนุษยชนนั้นจะคัดเลือกโดยรัฐสมาชิก แต่ไม่ได้เป็นตัวแทนของรัฐใด ๆ ทั้งนี้ บทบัญญัติที่เกี่ยวข้องกับเสรีภาพในการสื่อสาร คือ ข้อ 19 ซึ่งบัญญัติว่า

“1. บุคคลทุกคนมีสิทธิที่จะถือความเห็นใดก็ได้โดยปราศจากการแทรกแซง

2. บุคคลทุกคนมีสิทธิในเสรีภาพแห่งการแสดงออก สิทธินี้รวมถึงเสรีภาพที่จะแสวงหา รับและเผยแพร่ข้อมูลข่าวสารและความคิดทุกประเภท โดยไม่คำนึงถึงพรมแดน ทั้งนี้ ไม่ว่าด้วยวาจาเป็นลายลักษณ์อักษรหรือการตีพิมพ์ในรูปของศิลปะ หรือโดยอาศัยสื่อประการอื่น ตามที่ตนเลือก

3. การใช้สิทธิตามที่บัญญัติในวรรคสองของข้อนี้ ต้องมีหน้าที่และความรับผิดชอบพิเศษควบคู่ไปด้วย การใช้สิทธิดังกล่าวอาจมีข้อจำกัดในบางเรื่อง แต่ทั้งนี้ข้อจำกัดนั้น ต้องบัญญัติไว้ในกฎหมายและจำเป็นต่อ

3.1 การเคารพในสิทธิหรือชื่อเสียงของบุคคลอื่น

3.2 การรักษาความมั่นคงของชาติ หรือความสงบเรียบร้อย หรือการสาธารณสุข หรือศีลธรรมของประชาชน”

แม้ว่ากติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองจะให้การรับรองเสรีภาพในการสื่อสารไว้ก็ตาม แต่เสรีภาพดังกล่าวก็อาจถูกจำกัดได้ด้วยเงื่อนไขสำคัญสามประการ คือ เมื่อเป็นการเคารพต่อสิทธิหรือชื่อเสียงของบุคคลอื่น เพื่อการรักษาความมั่นคงของชาติ หรือความสงบเรียบร้อย หรือการสาธารณสุข หรือศีลธรรมของประชาชน และการจำกัดสิทธิดังกล่าวต้องมีการบัญญัติเป็นกฎหมาย

ความสัมพันธ์กับสิทธิในความเป็นส่วนตัว

1. ความหมายของสิทธิในความเป็นส่วนตัว

สิทธิในความเป็นส่วนตัว หรือสิทธิส่วนบุคคล (Right to privacy) หมายถึง สิทธิของบุคคลที่ประกอบไปด้วย สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว ซึ่งเป็นสถานะที่บุคคลจะรอดพ้นจากการสังเกต การรู้เห็น การสืบความลับ การรบกวนต่าง ๆ และความมีสันโดษไม่ติดต่อสัมพันธ์กับสังคม โดยขอบเขตที่ควรได้รับการคุ้มครองและการเคารพในสิทธิส่วนบุคคลก็คือการดำรงชีวิตอย่างเป็นอิสระ มีการพัฒนาบุคลิกลักษณะตามที่ต้องการ สิทธิที่จะแสวงหาความสุขในชีวิตตามวิถีทางที่อาจเป็นไปได้และเป็นความพอใจทราบเท่าที่ไม่ขัดต่อกฎหมาย ไม่ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชนและไม่เป็นการล่วงละเมิดสิทธิเสรีภาพของผู้อื่น⁶

นอกจากนี้ที่ประชุม International Commission of Jurists หรือ ICJ ได้ให้ความหมายไว้ในการประชุมเมื่อปี ค.ศ. 1967 ที่กรุงสต็อกโฮล์ม ประเทศสวีเดน ว่าเป็น “สิทธิที่จะอยู่โดยลำพังโดยมีการรบกวนการแทรกแซงในระดับที่น้อยที่สุด” ซึ่งมีการขยายความว่า หมายถึง สิทธิของปัจเจกชนที่จะดำเนินชีวิตโดยได้รับการคุ้มครองจากการแทรกแซงต่าง ๆ เช่น การแทรกแซงในชีวิตความเป็นส่วนตัว ครอบครัว และเคหะสถาน การแทรกแซงการติดต่อสื่อสารระหว่างกัน เป็นต้น⁷

จากความหมายข้างต้น สิทธิในความเป็นส่วนตัว จึงเป็นสิทธิขั้นพื้นฐานของมนุษย์ และเป็นสิ่งสำคัญของการดำรงไว้ซึ่งสังคมประชาธิปไตยเป็นสาระแห่งศักดิ์ศรีความเป็นมนุษย์และยังส่งเสริมสิทธิอื่น ๆ ด้วย การใดที่มีลักษณะจำกัดสิทธิในความเป็นส่วนตัว ซึ่งรวมถึงการติดต่อสื่อสาร สามารถกระทำได้ต่อเมื่อมีบทบัญญัติของกฎหมายและเป็นเรื่องที่ต้องกระทำเพื่อบรรลุวัตถุประสงค์ที่ชอบด้วยกฎหมายและได้สัดส่วนกับเป้าประสงค์นั้น

⁶ เกรียงไกร เจริญชนาวัดน์. เรื่องเดิม.

⁷ วีรพงษ์ บึงไกร. “การเปิดเผยข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540”. (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย, 2543). หน้า 14.

จึงอาจกล่าวได้ว่า ขอบเขตที่บุคคลควรได้รับการคุ้มครองและการเคารพในสิทธิความเป็นส่วนตัวก็คือการดำรงชีวิตอย่างเป็นอิสระ มีสิทธิที่จะแสวงหาความสุขในชีวิตตามความพอใจตราบเท่าที่ไม่ขัดต่อกฎหมาย ความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และไม่เป็นการล่วงละเมิดสิทธิเสรีภาพของผู้อื่น และการจำกัดสิทธิเช่นว่านั้นจะกระทำได้อีกเมื่อมีบทบัญญัติแห่งกฎหมายให้อำนาจไว้เท่านั้น

2. หลักสากลที่รับรองและคุ้มครองสิทธิในความเป็นส่วนตัวของบุคคลธรรมดา⁸

โดยที่สิทธิในความเป็นส่วนตัวของบุคคลเป็นสิทธิมนุษยชนประการหนึ่งนี้เอง การศึกษาเกี่ยวกับสิทธิในความเป็นส่วนตัวนั้น จึงจำเป็นที่จะต้องศึกษาสิทธิในความเป็นส่วนตัวที่ได้รับการรับรองและคุ้มครองตามข้อตกลงระหว่างประเทศและกฎหมายต่างๆ อันเป็นหลักสากล โดยเฉพาะอย่างยิ่งปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights) และอนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน (European Convention for the Protection of Human Rights and Fundamental Freedoms) ดังนี้

2.1 ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights)

สิทธิในความเป็นส่วนตัวของบุคคลได้รับการรับรองและคุ้มครองในฐานะเป็นสิทธิมนุษยชนไว้ในข้อ 12 บัญญัติว่า “บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกกลบหลู่เกียรติยศและชื่อเสียงมิได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการกลบหลู่ดังกล่าวนี้”⁹

⁸ บรรเจิด สิงคะเนติ, นนทวัชร นวตระกูลพิสุทธิ์ และเรวดี ขวัญทองยิ้ม. “รายงานการศึกษาวิจัยฉบับสมบูรณ์ เรื่อง ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy)”. (เอกสารวิจัย, สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ) หน้า 1 – 5.

⁹ Article 12

No one shall be subjected to arbitrary interference with his privacy family, home or correspondence, nor to attacks upon his honour and reputation, Everyone has the right to the protection of the law against such interference or attacks.

2.2 อนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน (European Convention for the Protection of Human Rights and Fundamental Freedoms)

อนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานเป็นข้อตกลงที่คณะกรรมการแห่งยุโรปได้จัดทำขึ้นเพื่อใช้บังคับในระหว่างประเทศต่างๆ ในสหภาพยุโรปโดยรับแนวความคิดมาจากปฏิญญาสากลว่าด้วยสิทธิมนุษยชน โดยมีเจตนารมณ์เพื่อคุ้มครองและพัฒนาสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานในระหว่างประเทศภาคีสมาชิก และกำหนดหลักการเบื้องต้นที่มุ่งหมายเพื่อสร้างหลักประกันสิทธิบางประการที่กำหนดไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชนเป็นการเฉพาะ

อนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานก็ได้รับรองและคุ้มครองสิทธิในความเป็นส่วนตัวของบุคคลไว้โดยชัดแจ้งในข้อ 8 ว่า

“1. บุคคลทุกคนมีสิทธิได้รับการเคารพในชีวิตส่วนตัวและครอบครัวที่อยู่อาศัยและการสื่อสาร

2. การแทรกแซงการใช้สิทธิในชีวิตส่วนตัวของบุคคลโดยองค์กรของรัฐจะกระทำได้อีกเฉพาะแต่เมื่อมีกฎหมายบัญญัติให้กระทำได้ และการแทรกแซงดังกล่าวเป็นมาตรการที่จำเป็นในสังคมประชาธิปไตยต่อความปลอดภัยแห่งชาติ ความมั่นคงของรัฐ ประโยชน์ทางเศรษฐกิจของประเทศ การรักษาความสงบเรียบร้อยและการป้องกันการกระทำคามผิดทางอาญา การคุ้มครองสุขภาพหรือจิตใจ หรือการคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น”¹⁰

¹⁰ Article 8 – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

2.3 Data Protection Directive (European Union)

ในปี ค.ศ. 1995 สหภาพยุโรปได้ออกหลักเกณฑ์ฉบับหนึ่งว่า Directive 95/46/EC of the Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data เพื่อผลักดันให้กฎหมายในกลุ่มประเทศสมาชิกมีความสอดคล้องกันในการให้หลักประกันที่ดีเพียงพอต่อการคุ้มครองความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของพลเมืองของสหภาพยุโรปและเพื่อให้การส่งผ่านข้อมูลส่วนบุคคลภายในประเทศสมาชิกเป็นไปได้โดยเสรี ปราศจากข้อจำกัดที่เกิดจากความแตกต่างกันของกฎหมายหรือกฎเกณฑ์ภายในของประเทศต่าง ๆ¹¹

Data Protection Directive มีวัตถุประสงค์เพื่อให้ประเทศสมาชิกของสหภาพยุโรปมีแนวทางการบัญญัติกฎหมายที่สอดคล้องกัน และเพื่อให้มีการส่งผ่านข้อมูลส่วนบุคคลภายในประเทศสมาชิก โดยมีขอบเขตการบังคับใช้ถึงการประมวลผลข้อมูลโดยวิธีการปกติ (Manual) และการประมวลผลข้อมูลโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอัตโนมัติ (Electronic or Automatic) ทั้งนี้ หลักเกณฑ์ดังกล่าวมีสาระสำคัญ ดังนี้

1. การรักษาคุณภาพของข้อมูล
 2. มาตรฐานของการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย
 3. การประมวลผลข้อมูลพิเศษ
 4. สิทธิในการได้รับแจ้งข้อมูลต่างๆ ของเจ้าของข้อมูล
 5. สิทธิในการเข้าถึงข้อมูลของเจ้าของข้อมูล
 6. สิทธิในการคัดค้านการประมวลผลข้อมูลของเจ้าของข้อมูล
 7. การรักษาความปลอดภัยในการประมวลผลข้อมูล
 8. การส่งผ่านข้อมูลส่วนบุคคลไปยังประเทศที่สาม
3. ความสัมพันธ์ของเสรีภาพในการสื่อสารกับสิทธิในความเป็นส่วนตัว

เสรีภาพในการสื่อสารและสิทธิในความเป็นส่วนตัวเป็นสิ่งที่อยู่ควบคู่กัน กล่าวคือ เมื่อกฎหมายรับรองและคุ้มครองให้แก่บุคคลในสิทธิในความเป็นส่วนตัว ไม่ว่าจะ เป็นความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลหรือข้อมูลส่วนตัว ความเป็นส่วนตัวเกี่ยวกับเนื้อตัวร่างกาย ความเป็นส่วนตัวในการอยู่หรือพักอาศัย และความเป็นส่วนตัวในการติดต่อสื่อสาร แล้ว บุคคลย่อมมีเสรีภาพที่จะสามารถกระทำการใด ๆ トラบเท่าที่ไม่ขัดหรือแย้งต่อกฎหมาย หรือความสงบ

¹¹ ไพโรจน์ วายุภาพ. “กฎหมายคุ้มครองข้อมูลส่วนบุคคล”. (เอกสารประกอบการบรรยาย).

เรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การติดต่อสื่อสาร ไม่ว่าจะเป็นทางโทรศัพท์ โทรสาร จดหมายจดหมายอิเล็กทรอนิกส์ หรือเครือข่ายสังคมออนไลน์ (Social network) ซึ่งการกระทำต่าง ๆ เหล่านี้ต้องปราศจากการแทรกแซงของบุคคลอื่น หรือก็คือบุคคลย่อมมีเสรีภาพในการสื่อสารนั่นเอง การแทรกแซงนี้ หมายความว่ารวมถึง การแทรกแซงการติดต่อสื่อสารระหว่างกัน การสืบความลับ การสอดรู้สอดเห็น การติดตามเฝ้าดู การรบกวน การเปิดเผยข้อมูลข่าวสาร และการใช้งานในทางที่มีขอบซึ่งการติดต่อสื่อสารส่วนบุคคล เช่น การสอดแนม หรือการดักฟัง เป็นต้น ดังนั้น เพื่อให้การรับรองและคุ้มครองสิทธิในความเป็นส่วนตัวและเสรีภาพในการสื่อสาร จึงต้องมีการบัญญัติกฎหมายต่าง ๆ ออกมาบังคับใช้แก่บุคคล โดยอาจจะเป็นรัฐธรรมนูญซึ่งบัญญัติรับรองสิทธิและเสรีภาพที่บุคคลพึงมี หรือในรูปของกฎหมายแพ่ง กฎหมายอาญา รวมถึงพระราชบัญญัติต่าง ๆ ซึ่งเป็นบทบัญญัติคุ้มครองสิทธิและเสรีภาพ นอกจากนี้ การจะจำกัดสิทธิและเสรีภาพดังกล่าวยังไม่สามารถกระทำได้ เว้นแต่จะโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เฉพาะและเท่าที่จำเป็น

หลักความคุ้มครองเสรีภาพในการสื่อสาร

ปัญหาว่ารัฐตรวจสอบการสื่อสารอันเป็นการรุกรานรบกวนข้อมูลที่ได้รับ ความคุ้มครองหรือไม่ ควรพิจารณาด้วยปัจจัย ดังนี้

1. ความชอบด้วยกฎหมาย (Legality) การจำกัดสิทธิความเป็นส่วนตัวกระทำได้ต่อเมื่อมีกฎหมายบัญญัติไว้ และรัฐต้องไม่ใช่มาตรการใดๆ ที่เป็นการสอดเข้าไปรบกวนสิทธิดังกล่าวโดยปราศจากกฎหมายที่ออกโดยฝ่ายนิติบัญญัติซึ่งมีปรากฏแก่สาธารณชนอยู่ก่อนแล้วในขณะนั้น โดยต้องมีความชัดเจนและแน่นอนเพียงพอให้บุคคลได้ทราบและคาดเห็นถึงการบังคับใช้ซึ่งกฎหมายฉบับดังกล่าว นอกจากนี้ บนความเปลี่ยนแปลงของเทคโนโลยี กฎหมายที่จำกัดสิทธิความเป็นส่วนตัวนั้นควรมีการชำระแก้ไขในแต่ละช่วงเวลาโดยผ่านกระบวนการออกกฎหมายของฝ่ายนิติบัญญัติ

2. ความจำเป็น (Necessity) กฎหมายที่อนุญาตให้มีการตรวจสอบการสื่อสารโดยรัฐต้องจำกัดการตรวจสอบเท่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ที่ชอบด้วยกฎหมาย โดยไม่ว่าวิธีเดียวหรือหลายวิธี ต้องเป็นการละเมิดสิทธิมนุษยชนให้น้อยที่สุด รัฐเป็นผู้รับผิดชอบในการพิสูจน์และให้เหตุผลความจำเป็นดังกล่าวต่อองค์กรที่ใช้อำนาจตุลาการหรือกระบวนการตรากฎหมายของฝ่ายนิติบัญญัติ

3. ความเหมาะสมเพียงพอ (Adequacy) การตรวจสอบการสื่อสารต้องกระทำด้วยความเหมาะสมเพื่อให้บรรลุวัตถุประสงค์ที่ชอบด้วยกฎหมายดังที่ได้กำหนดไว้

4. ความได้สัดส่วน (Proportionality) การตรวจสอบการสื่อสารถือว่าเป็นการกระทำที่รุกรานสิทธิความเป็นส่วนตัวและเสรีภาพในการแสดงความคิดเห็นและการแสดงออก ถือเป็นการคุกคามรากฐานของสังคมประชาธิปไตย คำวินิจฉัยชี้ขาดในเรื่องที่เกี่ยวกับการตรวจสอบการสื่อสารจะต้องปรากฏว่าประโยชน์ที่ได้รับจากการตรวจสอบนั้นมีน้ำหนักเหนือความเสียหายที่กระทบต่อสิทธิหรือประโยชน์อื่นของบุคคล โดยคำนึงถึงผลกระทบที่เกิดจากข้อมูล ประกอบความเสียหายจากการล่วงละเมิดสิทธิส่วนบุคคล

ความคุ้มครองตามประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญา

1. ประมวลกฎหมายแพ่งและพาณิชย์

การคุ้มครองเสรีภาพในการสื่อสารตามประมวลกฎหมายแพ่งและพาณิชย์ ปรากฏอยู่ในมาตรา 420 บัญญัติว่า “ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่น โดยผิดกฎหมาย ให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่า ผู้นั้นทำละเมิด จำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น” ซึ่งเป็นกฎหมายที่มีลักษณะในการเยียวยาความเสียหายที่เกิดขึ้นแก่บุคคลผู้ถูกละเมิดเสรีภาพในการสื่อสาร

นอกจากนี้ หากมีการนำข้อมูลที่ได้จากการละเมิดเสรีภาพในการสื่อสารของบุคคลอื่น ไปเปิดเผยต่อบุคคลที่สาม ก็อาจจะเข้าลักษณะเป็นการหมิ่นประมาท ตามมาตรา 423 ซึ่งบัญญัติว่า “ผู้ใดกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนต่อความจริงเป็นที่เสียหายแก่ชื่อเสียงหรือเกียรติคุณของบุคคลอื่นก็ดี หรือเป็นที่เสียหายแก่ทางมาหาได้หรือทางเจริญของเขา โดยประการอื่นก็ดี ท่านว่าผู้นั้นจะต้องใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อความเสียหายอย่างใด ๆ อันเกิดแต่การนั้น แม้ทั้งเมื่อตนมิได้รู้ว่าข้อความนั้นไม่จริง แต่หากว่าควรจะได้รู้” อีกด้วย

2. ประมวลกฎหมายอาญา

ประมวลกฎหมายอาญาเป็นกฎหมายว่าด้วยความผิดและโทษ¹² มีการห้ามไม่ให้กระทำการอย่างใด ๆ และสภาพบังคับทางอาญา มิได้บัญญัติถึงการกระทำความผิดเกี่ยวกับเสรีภาพในการสื่อสารไว้โดยตรง แต่หากมีการนำข้อมูลใด ๆ ของบุคคลอื่นออกเปิดเผยและน่าจะเกิดความ

¹² แสวง บุญเฉลิมวิภาส, หลักกฎหมายอาญา. (กรุงเทพมหานคร: โรงพิมพ์เดือนตุลา, 2539). หน้า 11.

เสียหายต่อบุคคลใด ก็อาจมีความผิดตามมาตรา 322 ถึง 324 ซึ่งเป็นบทบัญญัติเกี่ยวกับความผิดฐานเปิดเผยข้อมูลในการติดต่อสื่อสารส่วนบุคคลและความผิดฐานเปิดเผยความลับ โดยพนักงานหรือบุคคลที่ได้รับข้อมูลนั้นมาในทางประกอบวิชาชีพ เช่น แพทย์ เภสัชกร ทนายความ ผู้สอบบัญชี เป็นต้น

นอกจากนี้ มาตรา 163 อันเป็นความผิดต่อตำแหน่งหน้าที่ราชการ บัญญัติว่า “ผู้ใดเป็นเจ้าของงาน มีหน้าที่ในการไปรษณีย์ โทรเลข หรือโทรศัพท ุกระทำอันมิชอบด้วยหน้าที่ดังต่อไปนี้

1. เปิด หรือยอมให้ผู้อื่นเปิด จดหมายหรือสิ่งอื่นที่ส่งทางไปรษณีย์โทรเลข หรือโทรศัพท ุกระทำอันมิชอบด้วยหน้าที่ดังต่อไปนี้
2. ทำให้เสียหาย ทำลาย ทำให้สูญหาย หรือยอมให้ผู้อื่นทำให้เสียหาย ทำลาย หรือทำให้สูญหาย ซึ่งจดหมายหรือสิ่งอื่นที่ส่งทางไปรษณีย์ หรือโทรเลข
3. กัก ส่งให้ผิดทาง หรือส่งให้แก่บุคคลซึ่งรู้ว่ามิใช่เป็นผู้ควรรับ ซึ่งจดหมาย หรือสิ่งอื่นที่ส่งทางไปรษณีย์หรือโทรเลข หรือ
4. เปิดเผยข้อความที่ส่งทางไปรษณีย์ ทางโทรเลขหรือทางโทรศัพท ุต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรานี้เป็นบทบัญญัติซึ่งกำหนดโทษแก่เจ้าพนักงานผู้มีหน้าที่ในการไปรษณีย์ โทรเลข หรือโทรศัพท เช่น พนักงานไปรษณีย์¹³ พนักงานขององค์การโทรศัพท¹⁴ ซึ่งกระทำ ความผิดต่อเสรีภาพในการสื่อสารของบุคคลเกี่ยวกับจดหมาย ไปรษณีย์โทรเลข หรือโทรศัพท

ความคุ้มครองตามกฎหมายอื่น

นอกจากการคุ้มครองเสรีภาพในการสื่อสารตามประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญาแล้ว ยังมีพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ.2544 และประกาศคณะปฏิรูปการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข ฉบับที่ 21 เรื่อง ห้ามการดักฟังทางโทรศัพทหรือเครื่องมือสื่อสารใด ซึ่งเป็นกฎหมายเฉพาะที่คุ้มครองเสรีภาพในการสื่อสาร โดยเฉพาะการคุ้มครองเรื่องการดักฟัง และเปิดเผยข้อมูลของบุคคลใด

¹³ พระราชบัญญัติไปรษณีย์ พ.ศ. 2477 มาตรา 4

¹⁴ พระราชบัญญัติองค์การโทรศัพทแห่งประเทศไทย พ.ศ. 2497 มาตรา 4

1. พระราชบัญญัติการประกอบกิจการ โทรคมนาคม พ.ศ. 2544

พระราชบัญญัติการประกอบกิจการ โทรคมนาคม พ.ศ. 2544 เป็นกฎหมายว่าด้วยการประกอบกิจการ โทรคมนาคม การจัดสรรคลื่นความถี่ และการกำกับกิจการ วิทยุกระจายเสียง วิทยุโทรทัศน์ และโทรคมนาคม ซึ่งมีบทบัญญัติให้การคุ้มครองเสรีภาพในการ สื่อสารของบุคคลในมาตรา 74 ซึ่งหากมีการดักฟัง หรือเปิดเผยข้อมูลข่าวสารที่มีการสื่อสารทาง โทรคมนาคม¹⁵ โดยไม่ชอบด้วยกฎหมาย ย่อมมีความผิดตามมาตรา

2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้การเข้าถึงข้อมูลโดยมิชอบเป็นความผิด แม้ว่าผู้กระทำจะมีได้มีมูลเหตุจงใจเพื่อก่อให้เกิด ความเสียหายก็ตาม โดยมีมาตรการคุ้มครองการเข้าถึงข้อมูลทางอิเล็กทรอนิกส์เกี่ยวกับคอมพิวเตอร์ ดังนี้

¹⁵ โทรคมนาคม (Telecommunications) เป็นการส่งสารสนเทศในรูปแบบของตัวอักษร ภาพและเสียงโดยใช้คลื่นแม่เหล็กไฟฟ้าหรือการติดต่อสื่อสารจากที่หนึ่งไปยังอีกที่หนึ่งโดยใช้ พลังงานไฟฟ้าให้ไหลไปตามสายเคเบิลทองแดง เคเบิลเส้นใยแสง หรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้า ในการส่งสัญญาณไปในบรรยากาศ เช่น การส่งวิทยุ โทรทัศน์ การส่งคลื่นไมโครเวฟ และการส่ง สัญญาณผ่านดาวเทียม โดยจุดที่ส่งข่าวสารกับจุดรับจะอยู่ห่างไกลกัน และข่าวสารที่ส่งจะ เฉพาะเจาะจงผู้รับคนใดคนหนึ่งหรือส่งให้ผู้รับทั่วไปก็ได้

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้ให้คำจำกัดความอย่างเป็นทางการครั้งแรกต่อคำว่าโทรคมนาคมในปี พ.ศ.๒๔๙๕(ค.ศ.1932)ว่า “การสื่อสารใดๆ ไม่ว่าจะด้วยโทรเลขหรือโทรศัพท์ เพื่อส่งสัญลักษณ์ สัญญาณ ข้อความ ภาพและ เสียงใดๆ ทางสายส่งคลื่นวิทยุ หรือระบบอื่นๆ หรือกระบวนการส่งสัญญาณทางไฟฟ้าหรือการ มองเห็นต่าง ๆ

ต่อมาในภายหลังไอทียู (ITU) ได้ปรับเปลี่ยนคำนิยามใหม่เป็น “การส่งแพร่กระจาย หรือการรับสัญลักษณ์ สัญญาณ ข้อความ ภาพและเสียงใดๆหรือหมายถึงกระบวนการที่คิดค้นขึ้น เพื่อการใช้งานคุณสมบัติปกติของสายส่งคลื่นวิทยุ การมองเห็น หรือระบบทางแม่เหล็กไฟฟ้า

Anton A. Huurdeman, The World Wide History of Telecommunications, John Wiley & Sons, New Jersey, 2003 อ้างถึงใน ปิยนาด บุญนาค และคณะ. “รายงานผลการวิจัยเรื่อง พระมหากษัตริย์กับการสื่อสารโทรคมนาคม”. หน้า 14 – 15.

มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา 8 ผู้ใดกระทำความผิดด้วยประการใด โดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

กฎหมายฉบับนี้ ให้นิยามความหมายของข้อมูลคอมพิวเตอร์ไว้ว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย และข้อมูลตามกฎหมายฉบับนี้ยังหมายความรวมถึง ข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งเป็นข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น¹⁶ ทั้งนี้ กฎหมายฉบับนี้ได้บัญญัติให้การเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของบุคคลอื่นหรือกระทำการดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ ต้องมีกฎหมายให้อำนาจกระทำเท่านั้น หากผู้ใดเข้าถึงหรือดักจับข้อมูลไว้โดยมิชอบ ย่อมมีโทษจำคุกหรือปรับ หรือทั้งจำทั้งปรับ

¹⁶ มาตรา 3 ในพระราชบัญญัตินี้

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

3. ประกาศคณะปฏิรูปการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข ฉบับที่ 21

ประกาศคณะปฏิรูปการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข ฉบับที่ 21 เรื่อง ห้ามการดักฟังทางโทรศัพท์หรือเครื่องมือสื่อสารใด เพื่อคุ้มครองเสรีภาพในการสื่อสารถึงกันโดยชอบด้วยกฎหมายและเพื่อให้เกิดความเป็นระเบียบเรียบร้อยและรักษาความสงบของประเทศ เนื่องจากการลักลอบดักฟัง ใ้ประโยชน์ และเปิดเผยข้อความที่มีการติดต่อสื่อสารทางโทรศัพท์หรือเครื่องมือสื่อสารอื่น โดยมีชอบด้วยกฎหมาย เป็นการละเมิดสิทธิและเสรีภาพของบุคคล โดยมีสาระสำคัญ คือ ห้ามมิให้มีการดักฟังหรือเปิดเผยข้อความที่มีการติดต่อทางโทรศัพท์หรือเครื่องมือสื่อสารอื่นใด และกำหนดบทลงโทษกรณีกระทำการฝ่าฝืนประกาศฯ เอาไว้ แต่ประกาศฯ ดังกล่าวก็มีข้อยกเว้นให้สามารถดักฟังหรือเปิดเผยข้อความได้เมื่อมีกฎหมายให้อำนาจไว้โดยชอบ เช่น พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 มาตรา 14 จัตวา พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 พระราชบัญญัติป้องกันและปราบปรามการค้าย พ.ศ. 2551 มาตรา 30 เป็นต้น ซึ่งกฎหมายต่าง ๆ เหล่านี้ให้อำนาจแก่เจ้าพนักงานหรือเจ้าหน้าที่ของรัฐสามารถดักฟังโทรศัพท์หรือเครื่องมือสื่อสารอื่นใดได้เมื่อมีเหตุจำเป็นตามที่พระราชบัญญัตินี้ดังกล่าวกำหนดไว้

บทที่ 3

ข้อจำกัดและวิวัฒนาการของการสื่อสารใน ส่วนที่เกี่ยวกับความมั่นคงของชาติ

ปัจจุบันการใช้งานอินเทอร์เน็ตเพื่อการติดต่อสื่อสารกันมีแนวโน้มเพิ่มมากขึ้นอย่างต่อเนื่อง มีการขยายตัวของกลุ่มผู้ใช้อินเทอร์เน็ต ทั้งผ่านทางคอมพิวเตอร์ หรือ โทรศัพท์มือถือ (Smartphone) โดยการเชื่อมต่ออินเทอร์เน็ต ไม่ว่าจะเป็นระบบ ADSL¹⁷ WIFI¹⁸ หรือ 3G¹⁹ และมีการ

¹⁷ ADSL ย่อมาจาก Asymmetric Digital Subscribers Line คือเทคโนโลยีการสื่อสารข้อมูลความเร็วสูงแบบใหม่ ซึ่งทำให้สามารถเชื่อมต่ออินเทอร์เน็ตและเครือข่ายระยะไกลได้ด้วยความเร็วสูง โดยใช้คู่สายโทรศัพท์ธรรมดา ถือเป็นเทคโนโลยีของโมเด็ม (Modem) แบบใหม่ ที่เปลี่ยนสายโทรศัพท์ที่ทำจากทองแดงเป็นเส้นสัญญาณนำส่งข้อมูลความเร็วสูง

¹⁸ WIFI เป็นเทคโนโลยีที่ได้รับความนิยมที่ช่วยให้อุปกรณ์อิเล็กทรอนิกส์ในการแลกเปลี่ยนข้อมูลหรือการเชื่อมต่ออินเทอร์เน็ตแบบไร้สายโดยใช้คลื่นวิทยุ

คำ ๆ นี้เป็นเครื่องหมายการค้าของ Wi-Fi Alliance ที่ได้ให้คำนิยามของวายฟายว่า หมายถึง ชุดผลิตภัณฑ์ใด ๆ ที่สามารถทำงานได้ตามมาตรฐานเครือข่ายคอมพิวเตอร์แบบไร้สาย (แลนไร้สาย) ซึ่งอยู่บนมาตรฐาน IEEE 802.11 อย่างไรก็ตามเนื่องจากแลนไร้สายที่ทันสมัยส่วนใหญ่จะขึ้นอยู่กับมาตรฐานเหล่านี้ คำว่า "วายฟาย" จึงถูกนำมาใช้ในภาษาอังกฤษทั่วไปโดยเป็นคำพ้องสำหรับ "แลนไร้สาย"

¹⁹ ระบบ 3G หรือ Third Generation ซึ่งเป็นเทคโนโลยีการสื่อสารในยุคที่ 3 จุดเด่นที่สุดของ 3G นั้นเป็นเรื่องของความเร็วในการเชื่อมต่อและการรับส่งข้อมูล โดยเน้นการเชื่อมต่อแบบไร้สายด้วยความเร็วสูงทำให้ประสิทธิภาพในการรับส่งข้อมูลต่าง ๆ รวดเร็วมากขึ้น พร้อมทั้งสามารถใช้ บริการมัลติมีเดีย (Multimedia) ได้อย่างสมบูรณ์แบบ และมีประสิทธิภาพมากยิ่งขึ้น เช่น การรับส่ง ข้อมูลที่มีขนาดใหญ่ การใช้บริการ Video/Call Conference Download เพลง ดู TV Streaming ต่าง ๆ ซึ่งถ้าเปรียบเทียบกับเทคโนโลยี 2G กับ 3G แล้ว 3G มีช่องสัญญาณความถี่ และความจุในการรับส่งข้อมูลที่มากกว่า

นำเทคโนโลยีการติดต่อสื่อสาร โดยผ่านเครือข่ายอินเทอร์เน็ต ที่เรียกว่า เครือข่ายสังคมออนไลน์ (Social Network) เช่น Twitter Facebook Whatsapp และ Line เป็นต้น ซึ่งโปรแกรมเหล่านี้สามารถติดต่อสื่อสารกันได้โดยผ่านทางข้อความ (Message) ข้อความเสียง (Audio message หรือ Voice message) วิดีโอ (Video clip) เสียง (Call) หรือวิดีโอคอล (Video Call) จึงได้มีการบัญญัติกฎหมายออกมาคุ้มครองเสรีภาพในการสื่อสาร เพื่อป้องกันมิให้บุคคลหนึ่งบุคคลใด หรือกลุ่มบุคคล หน่วยงาน องค์กร ไม่ว่าจะ เป็นของเอกชนหรือรัฐ เข้าแทรกแซงเสรีภาพในการสื่อสารได้

แต่ทั้งนี้ การนำเทคโนโลยีต่าง ๆ มาใช้ แม้จะก่อให้เกิดความสะดวกสบาย และมีความสามารถเผยแพร่ข้อมูลข่าวสารได้อย่างรวดเร็ว แต่เมื่อมีผู้ใช้งานเป็นจำนวนมาก และข้อมูลข่าวสารที่เผยแพร่ไปอย่างง่ายและรวดเร็ว ย่อมเป็นดาบสองคมซึ่งอาจจะมีการกระจายข้อมูลที่ไม่ถูกต้องหรือผิดเพี้ยนไปจากความเป็นจริง จนก่อให้เกิดความวิตกกังวลของประชาชนทั่วไปที่ได้รับข่าวสารเช่นนั้น อีกทั้ง การติดต่อสื่อสารผ่านทางเครือข่ายสังคมออนไลน์ ยังสามารถใช้ในการกระทำความผิดต่าง ๆ ซึ่งอาจส่งผลกระทบต่อความมั่นคงของชาติ เช่นเดียวกับการติดต่อสื่อสารผ่านจดหมาย หรือโทรศัพท์ธรรมดาอีกด้วย กฎหมายที่บัญญัติให้การรับรองและคุ้มครองเสรีภาพในการสื่อสาร จึงมีบทบัญญัติยกเว้น อันเป็นข้อจำกัดของเสรีภาพในการสื่อสารไว้ โดยมีวัตถุประสงค์เพื่อประโยชน์ในการคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น หรือเพื่อประโยชน์แห่งความมั่นคงของชาติ ดังนี้

ข้อจำกัดตามหลักสากล

ตามที่คุณเขียนได้กล่าวมาแล้วในบทที่ 2 ถึงหลักสากลที่เกี่ยวข้องกับเสรีภาพในการสื่อสาร อันเป็นสิทธิและเสรีภาพที่มีการรับรองไว้ในกฎหมายระหว่างประเทศหลายฉบับ ซึ่งล้วนมีจุดประสงค์สำคัญเช่นเดียวกัน คือ เพื่อคุ้มครองสิทธิและเสรีภาพในการติดต่อสื่อสารของบุคคล และถือว่าสิทธิและเสรีภาพดังกล่าวเป็นสิทธิขั้นพื้นฐานที่มนุษย์ทุกคนพึงมี

ทั้งนี้ สิทธิและเสรีภาพในการสื่อสาร แม้จะได้รับการคุ้มครองอย่างเต็มที่ แต่สิทธิและเสรีภาพดังกล่าวย่อมต้องมีข้อจำกัดบางประการ ซึ่งกฎหมายระหว่างประเทศล้วนแต่อาศัยหลักการอย่างเดียวกันในการจำกัดสิทธิและเสรีภาพ ดังนี้

1. อนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน (European Convention for the Protection of Human Rights and Fundamental Freedoms)²⁰

อนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานได้รับรองและคุ้มครองสิทธิและเสรีภาพในการสื่อสารไว้โดยชัดแจ้งในข้อ 8 ของอนุสัญญา ความว่า

“1. บุคคลทุกคนมีสิทธิได้รับการเคารพในชีวิตส่วนตัวและครอบครัว ที่อยู่อาศัย และการสื่อสาร

2. การแทรกแซงการใช้สิทธิในชีวิตส่วนตัวของบุคคลโดยองค์กรของรัฐจะกระทำได้อีกเฉพาะแต่เมื่อมีกฎหมายบัญญัติให้กระทำได้ และการแทรกแซงดังกล่าวเป็นมาตรการที่จำเป็นในสังคมประชาธิปไตยต่อความปลอดภัยแห่งชาติ ความมั่นคงของรัฐ ประโยชน์ทางเศรษฐกิจของประเทศ การรักษาความสงบเรียบร้อยและการป้องกันการกระทำความผิดทางอาญา การคุ้มครองสุขภาพหรือจิตใจ หรือการคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น”

บทบัญญัติดังกล่าว แม้จะให้การรับรองและคุ้มครองสิทธิและเสรีภาพในการสื่อสารของบุคคลก็ตาม แต่ก็มีบทบัญญัติข้อจำกัดหรือข้อยกเว้นไว้ใน ข้อ 8 (2) กล่าวคือ เป็นการบัญญัติว่าเจ้าหน้าที่ของรัฐจะกระทำการใด ๆ ที่เป็นการขัดต่อสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานของมนุษย์ได้ ก็แต่เฉพาะมีกฎหมายบัญญัติให้กระทำได้ และการแทรกแซงดังกล่าวเป็นมาตรการที่จำเป็นต่อความปลอดภัยแห่งชาติ ความมั่นคงของรัฐ ประโยชน์ทางเศรษฐกิจของประเทศ การรักษาความสงบเรียบร้อยและการป้องกันการกระทำความผิดทางอาญา การคุ้มครองสุขภาพหรือจิตใจ หรือการคุ้มครองสิทธิและเสรีภาพของบุคคลอื่นเท่านั้น

ดังนั้น หากไม่มีกฎหมายให้อำนาจเจ้าหน้าที่ของรัฐกระทำการแทรกแซงเสรีภาพในการสื่อสาร และการแทรกแซงดังกล่าวมิได้เป็นไปเพื่อวัตถุประสงค์ดังกล่าวข้างต้นแล้วย่อมไม่สามารถกระทำการใด ๆ เพื่อแทรกแซงเสรีภาพในการสื่อสารของบุคคลได้

²⁰ อนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน ลงนามเมื่อวันที่ 4 พฤศจิกายน ค.ศ. 1950 และมีผลใช้บังคับเมื่อวันที่ 3 กันยายน ค.ศ. 1953

2. Data Protection Directive (European Union)²¹

Data Protection Directive เป็นบทบัญญัติที่ประกันสิทธิขั้นพื้นฐานของประชาชนที่สหภาพยุโรปได้กำหนดให้ประเทศสมาชิกให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เทียบเท่ากันในยุโรป โดยใช้นุสสัญญาของคณะมนตรีแห่งยุโรปเป็นแนวทางในการร่างกฎหมาย ทั้งนี้เพื่อให้กฎหมายอยู่ในลักษณะเป็นเอกบุรุษทั่วทั้งยุโรป Directive ของสหภาพยุโรปได้กำหนดให้รัฐสมาชิกอนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลภายใต้หลักทั่วไป ดังนี้

1. ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล
2. การประมวลผลจะทำได้เท่าที่จำเป็นในการทำนิติกรรมสัญญาใด ๆ ของผู้เป็นเจ้าของข้อมูลเท่านั้น
3. การประมวลผลจะต้องอยู่ภายใต้กรอบของกฎหมาย
4. การประมวลผลจะต้องกระทำเพื่อปกป้องผลประโยชน์สำคัญของผู้เป็นเจ้าของข้อมูล
5. การประมวลผลจำเป็นที่จะต้องกระทำเพื่อผลประโยชน์ของสาธารณะ หรือในการดำเนินงานของหน่วยงานของรัฐที่ได้รับมอบหมายให้เป็นผู้ควบคุมข้อมูล หรือเปิดเผยข้อมูลต่อบุคคลที่สาม
6. การประมวลผลที่จำเป็นและอยู่ภายใต้กรอบของกฎหมายจะต้องไม่กระทบต่อผลประโยชน์ หรือสิทธิขั้นพื้นฐานของผู้เป็นเจ้าของข้อมูลนอกจากหลักเกณฑ์ทั่วไปข้างต้น

Directive ของสหภาพยุโรปยังได้ให้ความสำคัญเกี่ยวกับความลับและความมั่นคง รวมถึงข้อยกเว้นในการเปิดเผยข้อมูลกรณีที่มีได้นำข้อมูลไปใช้ประโยชน์สาธารณะ แต่นำไปใช้เพื่อประโยชน์ส่วนตัว และกำหนดเกี่ยวกับเรื่องความเสียหายที่เกิดขึ้นต่อ ผู้เป็นเจ้าของข้อมูล เมื่อมีการประมวลผลโดยไม่ชอบด้วยกฎหมาย และการเปิดเผยข้อมูลจะต้องไม่ละเมิดต่อความมั่นคงของรัฐ

จากหลักสากลดังกล่าวข้างต้น อาจจะกล่าวโดยสรุปได้ว่า การจะแทรกแซงเสรีภาพในการสื่อสารของบุคคล ซึ่งมีกฎหมายให้การรับรองและคุ้มครองเสรีภาพในการสื่อสารไว้แล้ว จะกระทำมิได้ ยกเว้นแต่เข้าองค์ประกอบของข้อจำกัด ดังต่อไปนี้

²¹ เฉลิมชัย กักเกียรติกุล. “การคุ้มครองข้อมูลส่วนบุคคลในกิจการโทรคมนาคมของสหภาพยุโรป”. (ออนไลน์). เข้าถึงได้จาก : <http://chalemchai-nbtc.blogspot.com/2013/06/privacy-jewish-law-classical-greece.html>.

1. การแทรกแซงเสรีภาพในการสื่อสารจะต้องกระทำโดยรัฐ หรือเจ้าหน้าที่ของรัฐ

2. จะต้องมีความจำเป็นที่อำนาจรัฐ หรือเจ้าหน้าที่ของรัฐ กระทำการอย่างใดอย่างหนึ่ง หรือหลายอย่างประกอบกัน เพื่อให้ได้มาซึ่งข้อมูลข่าวสารจากการแทรกแซงนั้น และ

3. การแทรกแซงเสรีภาพในการสื่อสารจะต้องกระทำไปเพื่อความปลอดภัยแห่งชาติ ความมั่นคงของรัฐ ประโยชน์ทางเศรษฐกิจของประเทศ การรักษาความสงบเรียบร้อยและการป้องกันการกระทำความผิดทางอาญา การคุ้มครองสุขภาพหรือจิตใจ หรือการคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น และกระทำได้เท่าที่จำเป็นเท่านั้น

ข้อจำกัดตามกฎหมาย

ที่ผ่านมา ประเทศไทยมีการบัญญัติให้การรับรองและคุ้มครองเสรีภาพในการสื่อสารไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย ตั้งแต่ปี พ.ศ. 2540 เป็นต้นมา โดยมีข้อจำกัดว่า การจำกัดสิทธิและเสรีภาพของบุคคลที่รัฐธรรมนูญรับรองไว้ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย ซึ่งต้องไม่กระทบกระเทือนสาระสำคัญของสิทธิและเสรีภาพนั้น และเป็นไปเพื่อรักษาความมั่นคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ซึ่งเป็นข้อจำกัดเช่นเดียวกับหลักสากลที่กล่าวมาแล้ว

ทั้งนี้ ประเทศไทยมีการบัญญัติกฎหมายให้อำนาจรัฐในการแทรกแซงเสรีภาพในการสื่อสาร เช่น การตรวจสอบข้อความในจดหมาย การดักฟังทางโทรศัพท์ และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ เพื่อหาข้อมูลข่าวสารในการรักษาความมั่นคงและความสงบเรียบร้อยของรัฐ ดังนี้

1. ข้อจำกัดตามประมวลกฎหมายวิธีพิจารณาความอาญา

ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 105 บัญญัติว่า

“จดหมาย ไปรษณียบัตร โทรเลข สิ่งพิมพ์หรือเอกสารอื่น ซึ่งส่งทางไปรษณีย์ และโทรเลข จากหรือถึงผู้ต้องหาหรือจำเลยและยังมิได้ส่ง ถ้าเจ้าหน้าที่ต้องการเพื่อประโยชน์แห่งการสอบสวนได้ส่วนมูลฟ้อง พิเคราะห์ หรือการกระทำอย่างอื่นตามประมวลกฎหมายนี้ ให้ขอคำสั่งจากศาลถึงเจ้าหน้าที่ ไปรษณีย์โทรเลขให้ส่งเอกสารนั้นมา ...”

มาตรานี้เป็นการบัญญัติให้อำนาจแก่เจ้าหน้าที่ให้ได้มาซึ่งจดหมายไปรษณียบัตร โทรเลข สิ่งพิมพ์หรือเอกสาร ในกรณีที่มีการส่งทางไปรษณีย์ และโทรเลข จากหรือถึงผู้ต้องหาหรือจำเลย และกรณียังมีได้ส่ง เพื่อประโยชน์ในการสอบสวน ใต้สวนมูลฟ้อง พิจารณา หรือการกระทำอย่างอื่นตามประมวลกฎหมายวิธีพิจารณาความอาญา โดยเจ้าหน้าที่ต้องขอคำสั่งจากศาลให้ส่งเอกสารเหล่านั้นมา

2. ข้อจำกัดตามพระราชบัญญัติที่เกี่ยวข้อง

2.1 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46 บัญญัติว่า

“ในกรณีที่มีพยานหลักฐานตามสมควรว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน พนักงานเจ้าหน้าที่ซึ่งเลขานุการมอบหมายเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลแพ่ง เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชี ข้อมูลทางการสื่อสาร หรือข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็”

ในกรณีตามวรรคหนึ่ง ศาลจะสั่งอนุญาตให้พนักงานเจ้าหน้าที่ผู้ยื่นคำขอ ดำเนินการ โดยใช้เครื่องมือหรืออุปกรณ์ใด ๆ ตามที่เห็นสมควรก็ได้ แต่ทั้งนี้ให้อนุญาตได้คราวละไม่เกินเก้าสิบวัน

เมื่อศาลได้สั่งอนุญาตตามความในวรรคหนึ่งหรือวรรคสองแล้ว ผู้เกี่ยวข้องกับบัญชี ข้อมูลทางการสื่อสาร หรือข้อมูลคอมพิวเตอร์ตามคำสั่งดังกล่าว จะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้”

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 บัญญัติให้อำนาจเจ้าหน้าที่ของรัฐสามารถเข้าถึงบัญชี ข้อมูลทางการสื่อสาร หรือข้อมูลคอมพิวเตอร์ เพื่อให้ได้มาซึ่งข้อมูลดังกล่าว ในกรณีที่มีเหตุอันควรเชื่อได้ว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน โดยเจ้าหน้าที่ซึ่งเลขานุการคณะกรรมการป้องกันและปราบปรามการฟอกเงินมอบหมายเป็นหนังสือ จะยื่นคำขอฝ่ายเดียวต่อศาลแพ่ง เพื่อมีคำสั่งอนุญาตให้เจ้าหน้าที่นั้นดำเนินการ ศาลจะสั่งอนุญาตให้เจ้าหน้าที่ผู้ยื่นคำขอได้คราวละไม่เกินเก้าสิบวัน หากศาลได้สั่งอนุญาตแล้ว ผู้เกี่ยวข้องกับบัญชีข้อมูลทางการสื่อสาร หรือข้อมูลคอมพิวเตอร์ตามคำสั่งดังกล่าว จะต้องให้ความร่วมมือเพื่อให้เป็นไปตามบทบัญญัติของกฎหมายดังกล่าว โดยประเภทความผิดที่ศาลจะอนุญาตให้มีการเข้าถึงข้อมูลได้นั้นสามารถกระทำได้เพียงบัญชีลูกค้าของ

สถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือ เครื่องคอมพิวเตอร์ ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน ซึ่งเกี่ยวกับมูลฐานความผิด 9 มูลฐาน ตามมาตรา 3 แห่งพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ดังนี้

1. ความผิดเกี่ยวกับยาเสพติดตามกฎหมายว่าด้วยการป้องกันและปราบปรามยาเสพติดหรือกฎหมายว่าด้วยมาตรการในการปราบปรามผู้กระทำความผิดเกี่ยวกับยาเสพติด

2. ความผิดเกี่ยวกับเพศตามประมวลกฎหมายอาญา เฉพาะที่เกี่ยวกับการเป็นธุระจัดหา ล่อไป หรือพาไปเพื่อการอนาจารหญิงและเด็ก เพื่อสนองความใคร่ของผู้อื่นและความผิดฐานพรากเด็กและผู้เยาว์ ความผิดตามกฎหมายว่าด้วยมาตรการในการป้องกันและปราบปรามการค้าหญิงและเด็ก หรือความผิดตามกฎหมายว่าด้วยการป้องกันและปราบปรามการค้าประเวณีเฉพาะที่เกี่ยวกับการเป็นธุระจัดหา ล่อไปหรือชักพาไปเพื่อให้บุคคลนั้นกระทำการค้าประเวณี หรือความผิดเกี่ยวกับการเป็นเจ้าของกิจการการค้าประเวณี ผู้ดูแลหรือผู้จัดการกิจการการค้าประเวณี หรือสถานการค้าประเวณี หรือเป็นผู้ควบคุมผู้กระทำการค้าประเวณีในสถานการค้าประเวณี

3. ความผิดเกี่ยวกับการฉ้อโกงประชาชนตามประมวลกฎหมายอาญา หรือความผิดตามกฎหมายว่าด้วยการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน

4. ความผิดเกี่ยวกับการชักยอกหรือฉ้อโกงหรือประทุษร้ายต่อทรัพย์หรือกระทำโดยทุจริตตามกฎหมายว่าด้วยการธนาคารพาณิชย์ กฎหมายว่าด้วยการประกอบธุรกิจเงินทุน ธุรกิจหลักทรัพย์ และธุรกิจเครดิตฟองซิเออร์ หรือกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ซึ่งกระทำโดย กรรมการ ผู้จัดการ หรือบุคคลใด ซึ่งรับผิดชอบหรือมีประโยชน์เกี่ยวข้องในการดำเนินงานของสถาบันการเงิน นั้น

5. ความผิดต่อตำแหน่งหน้าที่ราชการ หรือความผิดต่อตำแหน่งหน้าที่ในการยุติธรรมตามประมวลกฎหมายอาญา ความผิดตามกฎหมายว่าด้วยความผิดของพนักงานในองค์การหรือหน่วยงานของรัฐ หรือความผิดต่อตำแหน่งหน้าที่หรือทุจริตต่อหน้าที่ตามกฎหมายอื่น

6. ความผิดเกี่ยวกับการกรรโชก หรือรีดเอาทรัพย์ที่กระทำโดยอ้างอำนาจอั้งยี่ หรือช่องโจรตามประมวลกฎหมายอาญา

7. ความผิดเกี่ยวกับการลักลอบหนีศุลกากรตามกฎหมายว่าด้วยศุลกากร

8. ความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

9. ความผิดเกี่ยวกับการพนันตามกฎหมายว่าด้วยการพนัน เฉพาะความผิดเกี่ยวกับการเป็นผู้จัดให้มีการเล่นการพนัน โดยไม่ได้รับอนุญาต และมีจำนวนผู้เข้าเล่นหรือเข้าพนันในการเล่นแต่ละครั้งเกินกว่าหนึ่งร้อยคน หรือมีวงเงินในการกระทำความผิดรวมกันมีมูลค่าเกินกว่าสิบล้านบาทขึ้นไป

10. ความผิดเกี่ยวกับการเป็นสมาชิกอั้งยี่ตามประมวลกฎหมายอาญา หรือการมีส่วนร่วมในองค์กรอาชญากรรมที่มีกฎหมายกำหนดเป็นความผิด

11. ความผิดเกี่ยวกับการรับของโจรตามประมวลกฎหมายอาญา เฉพาะที่เกี่ยวกับการช่วยจำหน่ายซื้อ รับจำนำ หรือรับไว้ด้วยประการใดซึ่งทรัพย์สินที่ได้มาโดยการกระทำความผิดอันมีลักษณะเป็นการค้า

12. ความผิดเกี่ยวกับการปลอมหรือการแปลงเงินตรา ดวงตรา แสตมป์ และตั๋วตามประมวลกฎหมายอาญาอันมีลักษณะเป็นการค้า

13. ความผิดเกี่ยวกับการค้าตามประมวลกฎหมายอาญาเฉพาะที่เกี่ยวกับการปลอม หรือการละเมิดทรัพย์สินทางปัญญาของสินค้า หรือความผิดตามกฎหมายที่เกี่ยวกับการคุ้มครองทรัพย์สินทางปัญญาอันมีลักษณะเป็นการค้า

14. ความผิดเกี่ยวกับการปลอมเอกสารสิทธิ บัตรอิเล็กทรอนิกส์ หรือหนังสือเดินทางตามประมวลกฎหมายอาญาอันมีลักษณะเป็นปกติธุระหรือเพื่อการค้า

15. ความผิดเกี่ยวกับทรัพยากรธรรมชาติหรือสิ่งแวดล้อม โดยการใช้อยึดถือ หรือครอบครองทรัพยากรธรรมชาติหรือกระบวนการแสวงหาประโยชน์จากทรัพยากรธรรมชาติ โดยมีขอบด้วยกฎหมายอันมีลักษณะเป็นการค้า

16. ความผิดเกี่ยวกับการประทุษร้ายต่อชีวิตหรือร่างกายจนเป็นเหตุให้เกิดอันตรายสาหัสตามประมวลกฎหมายอาญา เพื่อให้ได้ประโยชน์ซึ่งทรัพย์สิน

17. ความผิดเกี่ยวกับการหน่วงเหนี่ยวหรือกักขังผู้อื่นตามประมวลกฎหมายอาญาเฉพาะกรณีเพื่อเรียกหรือรับผลประโยชน์หรือเพื่อต่อรองให้ได้รับผลประโยชน์อย่างใดอย่างหนึ่ง

18. ความผิดเกี่ยวกับการลักทรัพย์ กรรโชก ริดเอาทรัพย์ ชิงทรัพย์ ปล้นทรัพย์ น้อโกง หรือข่มขู่ ตามประมวลกฎหมายอาญาอันมีลักษณะเป็นปกติธุระ

19. ความผิดเกี่ยวกับการกระทำอันเป็นโจรสลัดตามกฎหมายว่าด้วยการป้องกันและปราบปรามการกระทำอันเป็นโจรสลัด

20. ความผิดเกี่ยวกับการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขาย
หลักทรัพย์ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์

21. ความผิดเกี่ยวกับอาวุธหรือเครื่องมืออุปกรณ์ของอาวุธที่ใช้หรือ
อาจนำไปใช้ในการรบหรือการสงครามตามกฎหมายว่าด้วยการควบคุมยุทโธปกรณ์”

3. พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไข
เพิ่มเติม ฉบับที่ 4 พ.ศ. 2545

พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม
ฉบับที่ 4 พ.ศ. 2545 มาตรา 14 จัตวา บัญญัติว่า

“ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทาง
ไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่อ
อิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการ
กระทำความผิดเกี่ยวกับยาเสพติด เจ้าพนักงานซึ่งได้รับอนุมัติจากเลขาธิการเป็นหนังสือ จะยื่นคำ
ขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้เจ้าพนักงานได้มาซึ่งข้อมูลข่าวสาร
ดังกล่าวได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญา พิจารณาถึง
ผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

1. มีเหตุอันควรเชื่อว่ามีกระทำความผิดหรือจะมีการกระทำความผิด
เกี่ยวกับยาเสพติด

2. มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิด
เกี่ยวกับยาเสพติดจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

3. ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้...”

มาตรานี้เป็นการบัญญัติให้อำนาจเจ้าหน้าที่ในการได้มาซึ่งข้อมูลข่าวสารใน
กรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใด ซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์
คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยี
สารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด โดย
เจ้าหน้าที่ต้องได้รับอนุมัติจากเลขาธิการคณะกรรมการป้องกันและปราบปรามยาเสพติดเป็น
หนังสือ จึงจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญา เพื่อมีคำสั่งอนุญาตให้ใช้มาตรการ
ดังกล่าวได้

4. พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551

พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 มาตรา 30 บัญญัติว่า

“ในกรณีที่มีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์หรือสื่อสารสนเทศอื่นใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานค้ามนุษย์ พนักงานเจ้าหน้าที่ซึ่งได้รับอนุมัติเป็นหนังสือจากผู้บัญชาการตำรวจแห่งชาติ อธิบดีกรมสอบสวนคดีพิเศษ หรือผู้ว่าราชการจังหวัด แล้วแต่กรณี จะยื่นคำขอฝ่ายเดียวต่อศาลอาญาหรือศาลจังหวัดที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ได้มาซึ่งเอกสาร หรือข้อมูลข่าวสารดังกล่าวก็ได้ ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่กำหนดในข้อบังคับประธานศาลฎีกา

การอนุญาตตามวรรคหนึ่ง ให้ศาลพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็น ดังต่อไปนี้

1. มีเหตุอันควรเชื่อว่าจะมีการกระทำความผิดหรือจะมีการกระทำความผิดฐานค้ามนุษย์
2. มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดฐานค้ามนุษย์จากการเข้าถึงข้อมูลข่าวสารดังกล่าว
3. ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้ ...”

มาตรานี้เป็นการบัญญัติให้อำนาจแก่เจ้าหน้าที่ได้มาซึ่งเอกสาร หรือข้อมูลข่าวสารในกรณีที่มีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารนั้น ซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศอื่นใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดฐานค้ามนุษย์เท่านั้น

5. พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 บัญญัติว่า

“ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ พนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือจะยื่นคำขอขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญา เพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้

การอนุญาตตามวรรคหนึ่งให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาถึงผลกระทบ ต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

1. มีเหตุอันควรเชื่อว่าจะมีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ

2. มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

3. ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้ ...”

มาตรานี้เป็นการบัญญัติให้อำนาจแก่เจ้าหน้าที่ได้มาซึ่งเอกสาร หรือข้อมูลข่าวสารในกรณีที่มีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารนั้น ซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศอื่นใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ เท่านั้น

จะเห็นได้ว่า การที่เจ้าหน้าที่ของรัฐ จะกระทำการใด ๆ เพื่อแทรกแซงเสรีภาพในการสื่อสารของบุคคล หรือเพื่อให้ได้มาซึ่งข้อมูลข่าวสารของบุคคล จะต้องมีความหมายให้อำนาจกระทำไว้ และกฎหมายดังกล่าวจะต้องเป็นกฎหมายในระดับพระราชบัญญัติหรือเทียบเท่า ประกอบกับต้องมีวัตถุประสงค์ในการรักษาความมั่นคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น เพื่อประโยชน์แห่งการสอบสวนคดีอาญา (ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 105) เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน (พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46) เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด (พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 มาตรา 14) หรือเพื่อประโยชน์ในการกระทำความผิดฐานค้ามนุษย์ (พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 มาตรา 30) เป็นต้น

แต่ทั้งนี้ เพื่อมิให้การแทรกแซงเสรีภาพในการสื่อสารของบุคคลถูกกระทำไปโดยไม่มีขอบเขตจำกัด กฎหมายจึงกำหนดให้มีองค์กรกลางมีอำนาจในการอนุญาตและตรวจสอบการกระทำดังกล่าว ได้แก่ ศาลนั่นเอง

วิวัฒนาการของการสื่อสาร

การสื่อสารเป็นกระบวนการสำคัญและเป็นพฤติกรรมพื้นฐานของมนุษย์ โดยมนุษย์ได้พัฒนาการสื่อสารให้มีความสลับซับซ้อนมากยิ่งขึ้น เริ่มต้นจากการสื่อสารอย่างง่าย ได้แก่ การสนทนา มนุษย์ใช้เครื่องมือหลายประเภทสำหรับการสื่อสารเริ่มตั้งแต่สัญลักษณ์ ภาษา จนถึงการนำวิทยาการสมัยใหม่ที่เรียกว่าการสื่อสารโทรคมนาคมเข้ามาเสริมสร้างการติดต่อสื่อสาร การสื่อสารโทรคมนาคมจึงเป็นนวัตกรรมที่พัฒนาขึ้นจากกระบวนการเรียนรู้ในด้านการสื่อสารของมนุษยชาติ

1. ยุคแรกเริ่ม

การสื่อสารภายในประเทศไทยในยุคนี้ เป็นระยะก่อนการตั้งกรมไปรษณีย์โทรเลข มีหลายแบบตามจารีต คือ หากเป็นหนังสือชาวบ้านทั่วไป อาจใช้คนของตนนำไป หรืออาจฝากคนรู้จักหรือพ่อค้าที่จะนำไปยังจุดหมายปลายทางของหนังสือนั้น หรือส่งบอกต่อ ๆ กันไปด้วยวาจา แต่ถ้าเป็นหนังสือของทางราชการที่เรียกว่า ใบบอก (บอก) ท้องบัตรท้องตรา (คำสั่ง) ที่ส่งถึงหัวเมืองต่าง ๆ นั้น ให้ทางราชการส่งต่อ ๆ กันไปตามระยะทาง โดยชนิดของพาหนะก็เป็นไปตามลักษณะภูมิประเทศ เช่น ช้าง ม้า เรือ เรือแพ หรือหากเป็นหนังสือราชการปกติ (ไม่เร่งด่วน) คณะกรรมการเมืองก็จัดคนเดินส่งต่อ ๆ กันไป แต่ถ้าเป็นหนังสือเร่งด่วน รัฐบาลดำเนินการแต่งตั้งข้าหลวงให้เชิญไปจากกรุง (เมืองหลวง) เมื่อข้าหลวงไปถึงเมืองใด กรรมการเมืองนั้นก็จะต้องจัดพาหนะส่งข้าหลวงต่อไป

2. ยุคที่สอง

การสื่อสารในยุคที่สองนี้ เป็นระยะที่ความเจริญก้าวหน้าทางการสื่อสารโทรคมนาคมของไทยปรากฏชัด ตั้งแต่รัชสมัยพระบาทสมเด็จพระจอมเกล้าเจ้าอยู่หัว รัชกาลที่ 4 จากการที่ไทยเปิดประตูการค้าและรับวิทยาการสมัยใหม่เข้ามาปรับปรุงประเทศ ขณะเดียวกันก็ทรงตระหนักถึงความสำคัญของการสื่อสารให้ความเข้าใจถึงการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้น โดยทรงริเริ่มการใช้สิ่งพิมพ์สื่อสารสู่มวลชนอย่างกว้างขวาง และเริ่มใช้ไปรษณีย์โดยผ่านกงสุลอังกฤษ เพื่อติดต่อกับต่างประเทศ ทั้งยังเกิดการเจรจาเรื่องการขอวางสายโทรเลขจากประเทศต่าง ๆ อันทำให้พระองค์ต้องทรงตระหนักถึงการริเริ่มดำเนินการเกี่ยวกับกิจการสื่อสาร โทรคมนาคมสมัยใหม่ เพื่อมิให้เกิดการแทรกแซงจากภายนอก

การวางรากฐานกิจการสื่อสารโทรคมนาคมไทย ปรากฏอย่างเป็นรูปธรรมในสมัยรัชกาลที่ 5 โดยพระองค์มีพระบรมราชโองการ โปรดเกล้าฯ ให้เปิดการไปรษณีย์ขึ้นภายในพระนครเป็นการทดลองก่อนจนกิจการไปรษณีย์เริ่มขยายตัวจนกลายมาเป็นบริษัทไปรษณีย์ไทยในปัจจุบัน และเริ่มสร้างทางสายโทรเลขขึ้นเป็นครั้งแรก นอกจากนี้ยังมีการริเริ่มกิจการโทรศัพท์

เครื่องโทรศัพท์ที่ได้นำเข้ามาใช้ในประเทศไทยครั้งแรกได้นำเข้ามาทดลองใช้ระหว่างกรุงเทพกับสมุทรปราการจนแพร่หลายจนถึงปัจจุบันภายใต้การควบคุมของบริษัท ทีโอที จำกัด (มหาชน)

3. ยุคที่สาม

ในปี พ.ศ. 2530 ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ได้ริเริ่มโครงการเครือข่ายคอมพิวเตอร์ระหว่างมหาวิทยาลัยขึ้น เพื่อเชื่อมโยงศูนย์คอมพิวเตอร์ของหลายมหาวิทยาลัยเข้าด้วยกันด้วยระบบสื่อสาร ในปีเดียวกันมีการใช้จดหมายอิเล็กทรอนิกส์ในประเทศไทย เป็นครั้งแรกระบบการสื่อสารผ่านอินเทอร์เน็ตจึงพัฒนาเรื่อยมาจนถึงปี พ.ศ. 2538 ซึ่งเป็นปีแห่งเทคโนโลยีสารสนเทศ ที่การสื่อสารแห่งประเทศไทยอนุญาตให้เปิดบริการอินเทอร์เน็ตเชิงพาณิชย์ จนพัฒนาสู่การติดต่อสื่อสารผ่านเครือข่ายสังคมออนไลน์ อาทิ Facebook Twitter WhatsApp และ Line เป็นต้น

4. ยุคปัจจุบัน

ปัจจุบันเป็นยุคที่การติดต่อสื่อสารเป็นไปในรูปแบบของเครือข่ายสังคมออนไลน์ (Social Network) เป็นเครือข่ายของสังคม แต่จะเน้นเครือข่ายที่มีอยู่บนโลกออนไลน์ ซึ่งเครือข่ายนี้สามารถขยายกว้างออกไปได้อย่างอิสระไร้พรมแดน เชื่อมกันด้วยสายสัมพันธ์ของคนที่มีลักษณะคล้ายคลึงกันด้วยเรื่องใดเรื่องหนึ่ง จนทำให้เครือข่ายมีลักษณะใหญ่และเข้มแข็งขึ้น โดยมีจุดเริ่มต้นจาก Blog²² ซึ่งเป็นชื่อเรียกสั้น ๆ ของ Web log ซึ่งมาจากคำว่า “Web” เวิลด์ไวด์เว็บ (www) เป็นบริการอย่างหนึ่งในอินเทอร์เน็ต รวมทั้งคำว่า “log” ที่เป็นเสมือนบันทึกหรือรายละเอียดข้อมูลที่เก็บไว้²³ ดังนั้น Blog จึงเป็นแอปพลิเคชันบนเว็บที่ใช้เก็บบันทึกเรื่องราวหรือเนื้อหาให้คนอื่นเข้ามาเยี่ยมชม ซึ่งเว็บบล็อกส่วนใหญ่จะไม่เพียงแต่ให้บันทึกเนื้อหาที่เป็นข้อความเท่านั้น แต่ยังสามารถใส่รูป ใส่เพลง และมีลูกเล่นต่าง ๆ เพื่อให้ตกแต่งได้อีกมากมาย ด้วยเหตุนี้จึงทำให้บล็อกเป็นที่นิยมกันมากขึ้นอย่างรวดเร็วในกลุ่มผู้ใช้อินเทอร์เน็ต

²² เว็บบล็อกจัดเป็นเว็บไซต์ประเภท Social Network หรือเครือข่ายสังคมออนไลน์โดยจะมี Blogger ทำหน้าที่เขียนบันทึก หรือเล่าเหตุการณ์ที่ต้องการให้คนอื่นอ่านได้รับรู้ แสดงถึงความเป็นตัวเองโดยนำเสนอมุมมอง แนวความคิด ความสนใจส่วนตัว เข้าไปในบล็อกนั้น ๆ โดยให้ผู้อ่านสามารถแสดงความคิดเห็น (comment) ได้ตอบกันในบล็อกของตนเองได้

²³ ศรีนลิน พิมพ์ประเสริฐ. สนุกเล่น เป็นเร็ว facebook & twitter. (กรุงเทพมหานคร: โปรวิชั่น, 2552). หน้า 16 – 17.

นอกจากจะใช้เป็นสื่อกลางของการติดต่อสื่อสารของสมาชิกในกลุ่มแล้ว บรรดาเว็บ Social Network ทั้งหลายยังเข้ามามีบทบาทในชีวิตประจำวันของหลาย ๆ คนเพิ่มขึ้น ทำให้เรารู้สึกว่าเทคโนโลยีเหล่านี้เริ่มเข้ามาเป็นส่วนหนึ่งของชีวิตไปแล้ว ทั้งนี้ประโยชน์ของเว็บ Social Network ก็ยังนำไปประยุกต์ใช้และสร้างประโยชน์กับอีกหลากหลายเรื่อง เช่น การทำโฆษณาบนเว็บบล็อกต่าง ๆ ซึ่งถือเป็นการลงทุนที่ต่ำแต่ได้ผลตอบแทนที่คุ้มค่า โดยจะเป็นการก้าวจากยุค E – commerce ไปสู่ยุค Social commerce และปัจจุบันเว็บ Social Network ยังเป็นศูนย์กลางสำหรับประชาชนในการแสดงความคิดเห็นทั้งด้าน การเมือง สังคม เศรษฐกิจ สิ่งแวดล้อม ฯลฯ อีกมากมาย ซึ่งนับเป็นการก้าวไปสู่สังคมแห่งการเรียนรู้ และสังคมแห่งการพัฒนา โดยอยู่บนพื้นฐานของเทคโนโลยีที่ทุกคนเข้าถึงได้บนโลก Social Network

4.1 ประวัติความเป็นมา

4.1.1 Facebook

Facebook เป็นอีกหนึ่งเว็บในสังคม Social Network ที่เปิดให้ทุกคนได้ร่วมกันแบ่งปันความคิดเห็น แร่ความรู้ และนำเสนอชีวิตประจำวัน (Life style) ของตัวเอง เริ่มก่อตั้งโดยมาร์ก ซักเคอร์เบิร์ก (Mark Elliot Zuckerberg) นักศึกษามหาวิทยาลัยฮาร์วาร์ด มีจุดเริ่มต้นมาจาก Facemash.com เว็บไซต์โหวตรูปนักศึกษาฮาร์วาร์ดว่าใครได้รับความนิยมชมชอบมากหรือน้อย แต่ต้องถูกมหาวิทยาลัยระงับการใช้ ด้วยข้อหาว่าโปรเจกต์ของซักเคอร์เบิร์กละเมิดนโยบายการใช้งานอินเทอร์เน็ตที่มหาวิทยาลัยกำหนดไว้ และเป็นภัยต่อระบบความปลอดภัยคอมพิวเตอร์ของมหาวิทยาลัย เวลาผ่านไปไม่นาน Facebook ก็กลับมาเป็นที่รู้จักในนามบริการออนไลน์ที่ทำให้ผู้ใช้แบ่งปันข้อมูลกับเพื่อนที่อยู่ในสังคมเดียวกันแบบรวดเร็วทันใจและเข้าถึงทั้งข้อมูลเพิ่มภาพถ่ายเมื่อครั้งไปเที่ยว ภาพยนตร์ที่ชอบและประวัติส่วนตัว และยังสามารถทำกิจกรรมอื่น ๆ ผ่านแอปพลิเคชันเสริม (Applications) ที่มีอยู่อย่างมากมาย ต่างจากเว็บไซต์ชุมชนออนไลน์อื่นตรงที่ Facebook เป็นชุมชนในโลกที่มีตัวตนอยู่จริง ใช้ชื่อ Email เดียวกัน และต้องการทำความรู้จักคนอื่น ๆ ในสังคมเดียวกัน

4.1.2 Twitter

Twitter ก่อตั้งขึ้น โดยบริษัท Obvious Corp เมื่อปี ค.ศ.2006 ที่เมืองซานฟรานซิสโก ประเทศสหรัฐอเมริกา พัฒนาขึ้นโดย Evan Williams และ Meg Hourihan Evan Williams คำว่า Twitter มาจากรากศัพท์คำว่า tweet ที่แปลว่า เสียงนกกริ่ง ในช่วงแรกมีผู้เล่นเพียงกลุ่มเล็ก ๆ เท่านั้น ทำให้การใช้งานค่อนข้างเงียบเหงา จนมาเมื่อกลางปี ค.ศ. 2008 กระแสการใช้ Twitter ได้กลับมามีบทบาทอีกครั้งจากการประโคมข่าวของ CNN (ข่าว Breaking News) เรื่องเหตุการณ์แผ่นดินไหวที่มณฑลเสฉวน โดยที่เด็กหญิงชาวจีนได้ Tweet ข้อความแผ่นดินไหว

ไว้บน Twitter หลังจากนั้นก็มีผู้เล่นคนอื่น ๆ นำข้อความนั้น Retweet²⁴ ต่อ ๆ กันออกไปอย่างรวดเร็ว หลังจากนั้นเป็นต้นมาได้มีการยกย่องให้ Twitter เป็นเหยี่ยวข่าวที่เร็วที่สุดในโลก และทำให้ผู้คนทั่วโลกต่างเข้าไปสมัครเล่น Twitter แพร่หลายเพิ่มขึ้น

Twitter เป็น Social Network ขนาดเล็ก เรียกว่า Microblogging มีคุณสมบัติคล้ายกับบล็อกทั่วไป ที่ให้บริการเพื่อการติดต่อสื่อสารระหว่าง เพื่อน ครอบครัวและเพื่อนร่วมงาน สามารถเชื่อมต่อเป็นเครือข่าย และแลกเปลี่ยนข้อมูลได้อย่างรวดเร็ว แบบ Real Time แต่จะสามารถส่งข้อความได้เพียง 140 ตัวอักษรเท่านั้น นอกจากนี้ยังสามารถโพสภาพถ่าย วิดีโอ และไฟล์ต่าง ๆ ได้ด้วย โดยมีเว็บไซต์ที่ให้บริการฝากรูปภาพจากนั้นก็แนบมาเป็นลิงค์เพื่อให้บุคคลอื่นคลิกเข้าไปดูจากเว็บไซต์แทน Twitter จะเน้นที่ข้อความมากกว่ารูปภาพหรือวิดีโอ จึงทำให้อัพเดทข้อความใหม่ ๆ ได้อย่างรวดเร็ว อัพเดทข่าวสารที่ทันต่อเหตุการณ์ปัจจุบัน

ด้วยคุณสมบัติของ Twitter ที่สามารถอัพเดทข้อความใหม่ ๆ ได้อย่างรวดเร็ว และทันต่อเหตุการณ์ปัจจุบัน จึงมีการนำ Twitter มาใช้อย่างแพร่หลาย เพื่อแลกเปลี่ยนข้อมูลข่าวสาร เช่น

1. Twitter กับการเมือง ข่าวการปะทะคารมกันระหว่างนายกรัฐมนตรีอภิสิทธิ์ เวชชาชีวะ กับอดีตนายกรัฐมนตรีทักษิณ ชินวัตร ปลุกกระแสผู้ใช้ Twitter กลับมาเล่นอีกครั้ง การตอบโต้กันไปมาทางการเมืองของไทยทำให้ Twitter โด่งดังชั่วข้ามคืนจากรายงานข่าวทาง TV รวมถึงขึ้นหน้าหนึ่งของหนังสือพิมพ์หลายฉบับและวิทยุด้วย นอกจากนี้ยังมีนักการเมืองหลายท่านที่มี Twitter เพื่อโพสข้อความประชาสัมพันธ์เกี่ยวกับภารกิจของแต่ละคนด้วย

2. Twitter กับคนดัง เมื่อ Ashton Kutcher ดาราตลกจาก Hollywood หนุ่มหล่อคนนี้ทำควอลกับ CNN ว่าใครจะมีผู้เข้าติดตาม Follower ถึง 1 ล้านคนก่อนกัน ผลออกมาคือ Ashton Kutcher เป็นฝ่ายชนะขาด โดยมีผู้ติดตามถึงหนึ่งล้านคนภายในเวลาอันรวดเร็ว ซึ่งปรากฏการณ์ครั้งนี้ทำให้มีผู้รู้จัก Twitter มากขึ้นด้วย

²⁴ Retweet เป็นการอ้างอิงข้อความ Tweet ของบุคคลอื่น เพื่อไม่ให้สาระสำคัญขาดหายไป จึงต้องเก็บข้อความเอาไว้ด้วย โดยข้อความที่ส่งต่อจะสามารถส่งไปถึงเพื่อน ๆ อีกมากมาย ทั้งของคุณเอง และเพื่อนของผู้รับด้วย เรื่องเดียวกัน. หน้า 254.

ส่วนคนดังในเมืองไทยก็มีคนดังหลายคน เช่น ู้ดดี มีลินทจินดา @Woodytalk พิธีกรรายการทอล์คโชว์ที่มีประเด็นฮือฮาให้ติดตามเสมอ พัชรศรี เบญจมาศ @kalamare พิธีกรสาวสวยหรือผู้ประกาศข่าวช่อง 3 และคนดังอื่น ๆ อีกมากมาย

ที่น่าสนใจคือนักแสดงหรือคนดังหลาย ๆ คนที่นิยมใช้มือถือท่องอินเทอร์เน็ต ได้นำมือถือมาถ่ายภาพแล้วอัปโหลดภาพถ่ายให้เหล่าแฟนคลับ (Followers) ของเค้าได้ร่วมติดตามความเคลื่อนไหวของเธอและเขาอย่างใกล้ชิดขึ้นด้วย

3. Twitter กับการตลาด Twitter กลายเป็นอาวุธทางการตลาดไปแล้ว Twitter ถือเป็นเครื่องมือในการประชาสัมพันธ์ข่าวสารเพิ่มขึ้นอีกทาง ของหน่วยงาน บริษัทเจ้าของผลิตภัณฑ์ ธุรกิจวงการบันเทิง รวมถึงวงการไอทีและการสื่อสาร และวงการอื่น ๆ อีกมากได้เริ่มหันหน้ามาใช้ Twitter ในการโปรโมทสินค้า หรือนำเสนอเรื่องราวที่แตกต่างกันออกไป เช่น

@Dellthailand ผู้ผลิตคอมพิวเตอร์ Dell ประเทศไทย อัปเดตข้อมูล และประชาสัมพันธ์ผลิตภัณฑ์ใหม่ ๆ สามารถรับข่าวสารได้ก่อนใคร

@ktnews หนังสือพิมพ์กรุงเทพธุรกิจ นำเสนอข่าวสาร และบทความทุกชั่วโมง

@Centralnews ประกาศ ประชาสัมพันธ์เกี่ยวกับนิทรรศการ และกิจกรรมรับส่วนลดต่าง ๆ

4.1.3 WhatsApp

WhatsApp คือ โปรแกรมส่งข้อความ รูปภาพ เสียง และวิดีโอสำหรับโทรศัพท์มือถือไปยังเพื่อนของเราได้ไม่จำกัด และไม่มีค่าบริการในการส่งข้อความ สามารถทำงานข้ามระบบปฏิบัติการ Android Windows Phone iOS และ BlackBerry ได้ หากมีโปรแกรม WhatsApp เหมือนกัน การใช้งาน WhatsApp จะต้องมี การเชื่อมต่อผ่าน WiFi 3G หรือ GPRS/EDGE เป็นความคิดริเริ่มของ Brian Acton ชาวอเมริกัน และ Jan Koum ชาวยูเครน

คุณสมบัติที่โดดเด่นของ WhatsApp คือ ตอบรับข้อความได้รวดเร็ว พร้อมระบบเตือน (Push Notifications) สามารถเก็บข้อความที่สนทนาครั้งก่อน ๆ เซฟรูปภาพที่อีกฝ่ายส่งมาไว้ในเครื่องให้อัตโนมัติ สามารถสนทนากับเพื่อน ๆ ได้แม้จะใช้งานโทรศัพท์มือถือต่างระบบกัน เพราะ WhatsApp ใช้เบอร์โทรศัพท์ในการเชื่อมต่อ ทั้งยังสามารถส่งข้อความ รูปภาพ วิดีโอและคลิปเสียงต่าง ๆ ได้อย่างรวดเร็ว และสามารถสร้างกลุ่มเพื่อใช้งานสำหรับพูดคุยกันเฉพาะกลุ่มได้

4.1.4 Line

Line เป็นแอปพลิเคชันหรือโปรแกรมส่งข้อความ ออกแบบโดย บริษัท Naver Japan Corporation พัฒนาโดยบริษัท NHN Japan Inc. บริษัทของทีมงานเกาหลีและ ญี่ปุ่นเปิดตัววันที่ 23 มิถุนายน พ.ศ. 2554 หลังเหตุการณ์แผ่นดินไหว สึนามิ และ โรงไฟฟ้าพลังงานนิวเคลียร์รั่วไหล เมื่อวันที่ 11 มีนาคม พ.ศ. 2554 ช่วงนั้นการติดต่อทางโทรศัพท์ และสัญญาณมือถือขัดข้องหมด แต่ไลน์ใช้ระบบเชื่อมต่อผ่าน GPRS/EDGE, Wi-Fi หรือ 3G ได้ ทั้งไม่มีค่าใช้จ่ายในการสนทนาหรือส่งข้อมูลในรูปแบบต่าง ๆ เช่น ภาพ เสียง วิดีโอ จึงเข้ามาทดแทนในสถานการณ์ยากลำบากได้เป็นอย่างดี ทั้งได้รับความนิยมในพื้นที่อื่น ๆ ด้วยซึ่งไลน์สามารถใช้งานได้ทั้งโทรศัพท์มือถือที่มีระบบปฏิบัติการ ไอโอเอส (iOS) แอนดรอยด์ (Android) วินโดวส์โฟน (Window Phone) รวมถึงคอมพิวเตอร์ส่วนบุคคล (Personal Computer หรือ PC) และ แมคโอเอส (Mac OS)

คุณสมบัติสำคัญของไลน์ คือ มีฟังก์ชันการใช้งานที่หลากหลาย เช่น การสนทนาทางข้อความทั้งแบบส่วนตัวและกลุ่ม การแชร์พิกัดสถานที่ การคุยผ่านเสียง การคุยผ่านวิดีโอ การส่งคลิปวิดีโอ การส่งไฟล์เสียง การส่งสติ๊กเกอร์ รวมถึงแอปพลิเคชันยังรองรับการใช้งานได้ทั้งบนโทรศัพท์สมาร์ทโฟนและคอมพิวเตอร์ ซึ่งส่วนใหญ่เป็นบริการที่ไม่เสียค่าใช้จ่าย

4.2 ลักษณะการรับส่งข้อมูลของแอปพลิเคชัน

แอปพลิเคชันรับส่งข้อมูลบนโพรโทคอล HTTPS โดยการทำงานของ โพรโทคอล HTTPS สามารถแบ่งออกเป็น 2 ส่วนประกอบหลักๆ คือ การตรวจสอบใบรับรองอิเล็กทรอนิกส์ (Certificate) ของผู้ให้บริการ ดังจะเห็นจากตัวอย่างในรูปที่ 1 เป็นตัวอย่างการเข้าใช้งานเว็บไซต์ของธนาคารกสิกรไทย ที่มีการทำงานในโหมดเข้ารหัสลับข้อมูลและรับส่งผ่านโพรโทคอล HTTPS ซึ่งส่วนประกอบสำคัญในขั้นตอนการทำงานของ HTTPS คือข้อมูลใบรับรองอิเล็กทรอนิกส์ หรือที่เรียกว่า Certificate ซึ่งสามารถแสดงข้อมูลใบรับรองของเซิร์ฟเวอร์ที่เราเชื่อมต่ออยู่ได้

แผนภาพที่ 3-1 แสดงตัวอย่างเว็บไซต์ที่ใช้งานโพรโทคอล HTTPS ซึ่งการเชื่อมต่อจะมีการรับข้อมูลใบรับรองอิเล็กทรอนิกส์ เพื่อให้แอปพลิเคชันฝั่งผู้ใช้งานพิจารณาความถูกต้องก่อนจะใช้งานต่อไป



และอีกส่วนประกอบสำคัญคือการเข้ารหัสลับข้อมูลที่มีการรับส่งอยู่กับเซิร์ฟเวอร์ที่ให้บริการปลายทาง รูปแบบคือจะมีกุญแจ ที่สำคัญ 2 ชนิด คือ

1. กุญแจเซสชัน (Session key) เป็นกุญแจที่ใช้เข้ารหัสลับข้อมูลแบบ Symmetric Key ใช้กุญแจเพียงดอกเดียว นำมาใช้สำหรับเข้ารหัสลับและถอดรหัสลับข้อมูลที่รับส่งระหว่างแอปพลิเคชัน ฝั่งผู้ใช้งานและเครื่องเซิร์ฟเวอร์

2. กุญแจคู่ เป็นกุญแจที่ใช้เข้ารหัสลับข้อมูลแบบ Asymmetric Key ประกอบไปด้วยกุญแจ 2 ส่วนคือกุญแจสาธารณะ (Public key) และกุญแจส่วนตัว (Private key) ของเครื่องเซิร์ฟเวอร์ที่ให้บริการ นำมาใช้เข้ารหัสลับและถอดรหัสลับกุญแจเซสชันในข้อที่ 1

การทำงานของโพรโทคอล HTTPS สามารถสรุปเป็นขั้นตอนได้ ดังนี้

ขั้นตอนที่ 1 ผู้ใช้งานมีการเชื่อมต่อไปยังเซิร์ฟเวอร์ของผู้ให้บริการเพื่อขอให้เริ่มการเชื่อมต่อด้วยโพรโทคอล HTTPS

ขั้นตอนที่ 2 เครื่องเซิร์ฟเวอร์ที่ให้บริการจะทำการส่งข้อมูลใบรับรองอิเล็กทรอนิกส์ (Certificate) ของผู้ให้บริการกลับมายังแอปพลิเคชันในฝั่งผู้ใช้งานเพื่อตรวจสอบ หากเป็นใบรับรองอิเล็กทรอนิกส์ที่แอปพลิเคชันนั้นเชื่อถือและรู้จักอยู่แล้ว ก็จะสามารทำงานในลำดับถัดไปทันที แต่ถ้าในทางตรงกันข้าม ถ้าแอปพลิเคชันไม่สามารถตรวจสอบ

ใบรับรองอิเล็กทรอนิกส์ได้ว่าจะมีความน่าเชื่อถือหรือไม่ ก็จะขึ้นอยู่กับการบริหารจัดการของแอปพลิเคชันนั้นๆว่าจะเป็นอย่างไต่อไป เช่น แอปพลิเคชันนั้นยอมให้ดำเนินการต่อได้ หรือแอปพลิเคชันนั้นตั้งยกเลิกการเชื่อมต่อ เป็นต้น

ขั้นตอนที่ 3 แอปพลิเคชันในฝั่งผู้ใช้งานจะสร้างกุญแจเซสชัน (Session key) ที่ใช้ในการเข้ารหัสลับและถอดรหัสลับข้อมูล จากนั้นทำการเข้ารหัสลับกุญแจเซสชันด้วยกุญแจสาธารณะ (Public key) ซึ่งเป็นข้อมูลที่ได้มาจากใบรับรองอิเล็กทรอนิกส์ในขั้นตอนที่ 2 จากนั้นแอปพลิเคชันจะส่งข้อมูลที่เข้ารหัสลับกลับไปยังเครื่องเซิร์ฟเวอร์ ที่ให้บริการ โดยเซิร์ฟเวอร์ที่ให้บริการจะทำการถอดรหัสลับข้อมูลด้วยกุญแจส่วนตัว (Private key) ผลลัพธ์สุดท้ายคือเครื่องเซิร์ฟเวอร์ที่ให้บริการจะได้รับกุญแจเซสชัน (Session key) เพื่อนำมาใช้ในงานในขั้นตอนต่อไป

ขั้นตอนที่ 4 การรับส่งข้อมูลระหว่างผู้ใช้งานกับเซิร์ฟเวอร์ที่ให้บริการ จะผ่านการเข้ารหัสลับและถอดรหัสลับข้อมูลด้วยกุญแจเซสชันที่ได้จากขั้นตอนที่ 3 ตลอดเวลา เช่น ผู้ใช้งานส่งคำขอการเข้าถึงหน้าเว็บไซต์ ซึ่งเนื้อหาต่างๆที่ใช้ทำการเรียกไปยังเซิร์ฟเวอร์ที่ให้บริการเว็บไซต์นั้น จะถูกเข้ารหัสลับข้อมูลที่ฝั่งแอปพลิเคชันของผู้ใช้งาน ด้วยกุญแจเซสชันที่สร้างขึ้นในขั้นตอนที่ 3 และข้อมูลดังกล่าวจะถูกถอดรหัสลับออกด้วยกุญแจเซสชันตัวเดิมในฝั่งเซิร์ฟเวอร์ที่ให้บริการเว็บไซต์ เช่นกัน

แผนภาพที่ 3-2 ขั้นตอนการทำงานของโปรโตคอล HTTPS



วิธีปฏิบัติของหน่วยงานที่เกี่ยวข้อง

การตรวจสอบและแทรกแซงการสื่อสารบนเครือข่ายสังคมออนไลน์ของบุคคล เพื่อให้ได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์นั้น เป็นอำนาจของฝ่ายบริหารหรือเจ้าหน้าที่รัฐซึ่งจะกระทำได้อีกต่อเมื่อมีกฎหมายให้อำนาจไว้ โดยมีฝ่ายตุลาการหรือศาลเป็นผู้มีอำนาจตรวจสอบความชอบด้วยกฎหมายของการกระทำดังกล่าวอีกชั้นหนึ่ง ดังนั้น หน่วยงานที่เกี่ยวข้องในการตรวจสอบและแทรกแซงเสรีภาพในการสื่อสาร จึงประกอบด้วย 2 องค์กรหลัก คือ

1. ฝ่ายบริหาร ได้แก่ เจ้าหน้าที่รัฐ
2. ฝ่ายตุลาการ ได้แก่ ศาล

โดยทั่วไปแล้ว กฎหมายแต่ละฉบับซึ่งให้อำนาจฝ่ายบริหารหรือเจ้าหน้าที่รัฐตรวจสอบและแทรกแซงเสรีภาพในการสื่อสารจะกำหนดกระบวนการหรือขั้นตอนให้แก่เจ้าหน้าที่รัฐต้องปฏิบัติตามซึ่งอาจจะมีรายละเอียดปลีกย่อยแตกต่างกัน ขึ้นอยู่กับว่าเป็นกฎหมายฉบับใด มีวัตถุประสงค์หรือจุดมุ่งหมายในการคุ้มครองอะไร แต่ทั้งนี้ กฎหมายแต่ละฉบับก็จะมีหลักการสำคัญของขั้นตอน ดังต่อไปนี้

1. การขออนุญาต

การที่เจ้าหน้าที่จะดำเนินการใด ๆ เพื่อตรวจสอบและแทรกแซงเสรีภาพในการสื่อสารนั้น จะต้องดำเนินการขออนุญาต โดยผ่านการตรวจสอบตั้งแต่ผู้บังคับบัญชาของตนเองไปจนถึงผู้บังคับบัญชาซึ่งเป็นหัวหน้าหน่วยงานหรือองค์กรของรัฐตามลำดับชั้น และต้องได้รับการอนุมัติเป็นหนังสือจากผู้บังคับบัญชาดังกล่าวเสียก่อน

ในการนี้ เจ้าหน้าที่ต้องมีหน้าที่ในการนำเสนอข้อมูลหรือหลักฐานประกอบการขออนุญาตต่อผู้บังคับบัญชาเพื่อพิจารณาอนุมัติด้วย

2. การยื่นคำขอต่อศาล

เมื่อเจ้าหน้าที่ได้ขออนุญาต และผู้บังคับบัญชาหรือหัวหน้าหน่วยงานหรือองค์กรของรัฐได้ใช้ดุลพินิจและพิจารณาอนุมัติแล้ว เจ้าหน้าที่จะต้องยื่นคำร้องดังกล่าวเป็นคำขอฝ่ายเดียวต่อศาลเพื่อมีคำสั่งอนุญาตให้เจ้าหน้าที่กระทำการใด ๆ เพื่อให้ได้มาซึ่งเอกสาร หรือข้อมูลข่าวสาร

ศาลจะทำการพิจารณาคำร้องจากพยานหลักฐาน โดยคำนึงถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใด ประกอบกับเหตุผลและความจำเป็น กล่าวคือ ต้องมีเหตุอันควรเชื่อว่ามี การกระทำความผิด และจะได้ข้อมูลข่าวสารซึ่งเกี่ยวข้องกับการกระทำความผิดนั้น อีกทั้งยังต้องไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าวิธีการนี้ได้ ซึ่งหากศาลพิจารณาแล้วเห็นว่าไม่เข้าเงื่อนไขทั้งสามประการนี้ ศาลมีอำนาจยกคำร้องดังกล่าวได้

เจ้าหน้าที่มีภาระการพิสูจน์เพื่อแสดงให้ศาลเห็นว่า ในการที่จะแสวงหาข้อมูลที่มีเหตุอันควรเชื่อได้ว่า หากไม่ใช้มาตรการตรวจสอบและแทรกแซงเพื่อให้ได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ตามที่กฎหมายให้อำนาจแล้ว เจ้าหน้าที่จะไม่สามารถแสวงหาข้อมูล เพื่อใช้เป็นพยานหลักฐานนำตัวผู้กระทำความผิดมาลงโทษได้

3. ระยะเวลา

การอนุญาตให้เจ้าหน้าที่ตรวจสอบและแทรกแซงเสรีภาพในการสื่อสารนั้น ศาลจะสั่งอนุญาตได้คราวละไม่เกิน ๕๐ วัน โดยจะกำหนดเงื่อนไขใด ๆ ก็ได้ และไม่ได้จำกัดว่าจะขออนุญาตได้กี่คราวหรือไม่เกินกี่คราว ดังนั้นเจ้าหน้าที่จึงสามารถขออนุญาตได้ไม่จำกัดจำนวนครั้ง แต่อย่างไรก็ตาม หากเจ้าหน้าที่ไม่สามารถเข้าถึงข้อมูลได้ในคราวแรก การขออนุญาตในการใช้มาตรการดังกล่าวในคราวต่อไป จำเป็นต้องมีข้อมูลเสนอต่อศาลเป็นจำนวนมากกว่าเดิมหรือภาระการพิสูจน์ของเจ้าหน้าที่ต่อศาลย่อมมีมากกว่าการขออนุญาตให้คราวก่อน ๆ เพื่อให้ศาลเห็นว่ามีเหตุอันควรที่ศาลจะมีคำสั่งอนุญาตให้ใช้การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์

4. การเก็บรักษาและการใช้ประโยชน์

การเก็บรักษาและการใช้ประโยชน์บรรดาเอกสารหรือข้อมูลข่าวสารที่ได้มาจากการตรวจสอบและแทรกแซงเสรีภาพในการสื่อสารของเจ้าหน้าที่นั้น ให้เก็บรักษาและใช้ประโยชน์ในการสืบสวนและใช้เป็นพยานหลักฐานในการดำเนินคดีความผิดที่กำหนดไว้เป็นการเฉพาะในกฎหมายแต่ละฉบับซึ่งให้อำนาจเจ้าหน้าที่ในการใช้กระบวนการตรวจสอบและแทรกแซงดังกล่าวเท่านั้น

ทั้งนี้ กระบวนการต่าง ๆ ที่เกี่ยวข้องภายในหน่วยงานซึ่งมีอำนาจตรวจสอบและแทรกแซงการติดต่อสื่อสาร ขึ้นอยู่กับระเบียบและวิธีปฏิบัติราชการภายในหน่วยงานนั้น เช่น สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด ซึ่งมีขั้นตอนการได้มา การใช้ประโยชน์ และการเก็บรักษาข้อมูลข่าวสาร ดังนี้

เจ้าพนักงานต้องมีคำขออนุมัติเข้าถึงข้อมูลข่าวสาร พร้อมด้วยรายละเอียดเกี่ยวกับพฤติกรรมและข้อมูลที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับยาเสพติด เพื่อยื่นต่อเลขานุการพิจารณา ซึ่งการกระทำความผิดต้องมีพฤติกรรมเกี่ยวกับการกระทำความผิดตามกฎหมายว่าด้วยมาตรการในการปราบปรามผู้กระทำความผิดเกี่ยวกับยาเสพติด และมีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดและไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้²⁵ ต่อเลขานุการเพื่อพิจารณาและอาจเรียกเจ้าพนักงานผู้ยื่นคำขอหรือผู้เกี่ยวข้องมาให้ถ้อยคำหรือส่งพยานหลักฐานเพื่อประกอบการพิจารณาก็ได้²⁶

เมื่อเลขานุการอนุมัติแล้ว ให้เจ้าพนักงานร่วมกับผู้ประสานงานยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญา และรายงานผลการพิจารณาของอธิบดีผู้พิพากษาศาลอาญาให้เลขานุการทราบโดยเร็ว²⁷ และหากศาลมีคำสั่งอนุมัติและเจ้าหน้าที่ได้ข้อมูลมาแล้วต้องรายงานให้ผู้บังคับบัญชาทราบทุกครั้ง²⁸ และรายงานผลการปฏิบัติการให้ศาลทราบด้วย

เจ้าหน้าที่ต้องบันทึกข้อมูลข่าวสารที่ได้ดำเนินการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ ขณะที่ดำเนินการใช้มาตรการดังกล่าวไว้ด้วย โดยไม่ให้มีการเปลี่ยนแปลงหรือแก้ไขได้โดยง่าย หลังจากนั้นเจ้าหน้าที่ต้องทำการถอดถ้อยคำหรือเสียงของบุคคลหรือการสนทนาระหว่างบุคคลที่ได้มาโดยการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์เป็นลายลักษณ์อักษร หากข้อมูลข่าวสารดังกล่าวเป็นภาษาต่างประเทศหรือรหัสที่จำเป็นต้องแปลความหมาย โดยเจ้าหน้าที่จะทำการแปลเองหรือให้ผู้เชี่ยวชาญดำเนินการแปลความหมายข้อมูลข่าวสารที่ได้มานั้นก็ได้ ทั้งนี้ การบันทึกข้อมูลข่าวสารต้องมีรายละเอียดเกี่ยวกับวันเดือนปีและเวลาในการบันทึกตามลำดับ

ในขั้นต้นสุดท้ายเจ้าหน้าที่ต้องทำการสรุปหรือประมวลผลข้อมูลจากสิ่งที่บันทึกข้อมูลข่าวสารและบันทึกถ้อยคำที่ได้จัดทำไว้เป็นลายลักษณ์อักษรอีกครั้งหนึ่ง เพื่อที่จะส่ง

²⁵ ระเบียบคณะกรรมการป้องกันและปราบปรามยาเสพติดว่าด้วยการได้มา การใช้ประโยชน์และการเก็บรักษาข้อมูลข่าวสาร พ.ศ. 2545 ข้อ 9

²⁶ ระเบียบคณะกรรมการป้องกันและปราบปรามยาเสพติดว่าด้วยการได้มา การใช้ประโยชน์และการเก็บรักษาข้อมูลข่าวสาร พ.ศ. 2545 ข้อ 10

²⁷ ระเบียบคณะกรรมการป้องกันและปราบปรามยาเสพติดว่าด้วยการได้มา การใช้ประโยชน์และการเก็บรักษาข้อมูลข่าวสาร พ.ศ. 2545 ข้อ 12

²⁸ ระเบียบคณะกรรมการป้องกันและปราบปรามยาเสพติดว่าด้วยการแต่งตั้งการปฏิบัติหน้าที่และการกำกับดูแลการปฏิบัติหน้าที่ของเจ้าพนักงาน ป.ป.ส. พ.ศ. 2545

บันทึกถ้อยคำที่ทำเป็นลายลักษณ์อักษรดังกล่าว รวมทั้งรายงานบันทึกข้อมูลข่าวสาร สิ่งที่บันทึกข้อมูลข่าวสาร ต่อศาลภายในเจ็ดวันนับแต่ยุติการใช้มาตรการดังกล่าว โดยให้ปิดผนึกประทับตรา “ลับ” และลงลายมือชื่อกำกับไว้ด้วย²⁹ เมื่อเสร็จสิ้นการใช้ประโยชน์จากข้อมูลข่าวสารแล้ว ให้ทำลายข้อมูลข่าวสารที่เก็บรักษาไว้ โดยเจ้าหน้าที่ต้องระบุประเภท ลักษณะและวิธีการที่จะทำลาย แล้วรายงานให้ศาลและผู้บังคับบัญชาของคนทราบ³⁰

²⁹ ระเบียบคณะกรรมการป้องกันและปราบปรามยาเสพติดว่าด้วยการได้มา การใช้ประโยชน์และการเก็บรักษาข้อมูลข่าวสาร พ.ศ. พ.ศ. 2545 ข้อ 15

³⁰ ระเบียบคณะกรรมการป้องกันและปราบปรามยาเสพติดว่าด้วยการได้มา การใช้ประโยชน์และการเก็บรักษาข้อมูลข่าวสาร พ.ศ. 2545 ข้อ 21

บทที่ 4

การควบคุมเสรีภาพในการสื่อสารของประเทศสหรัฐอเมริกา

พระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ ค.ศ. 1978 (Foreign Intelligence Surveillance Act of 1978 หรือ FISA)³¹

พระราชบัญญัติฉบับนี้เป็นกฎหมายระดับสหพันธรัฐ ที่กล่าวถึงขั้นตอนในการร้องขอ สอดแนมทางอิเล็กทรอนิกส์และการรวบรวมข้อมูลลับระหว่างใช้อำนาจนอกประเทศ (Foreign Powers) และเจ้าหน้าที่ของผู้มีอำนาจดังกล่าว (Agents of foreign Powers) ซึ่งอาจรวมถึงชาวอเมริกัน หรือผู้มีถิ่นที่อยู่ถาวรในสหรัฐอเมริกาที่ถูกสงสัยว่าก่อวินาศกรรมหรือก่อการร้าย กฎหมายฉบับนี้ไม่ใช่บังคับนอกประเทศสหรัฐอเมริกา และมีการแก้ไขเพิ่มเติมหลายครั้งนับแต่เกิดเหตุการณ์โจมตีเมื่อวันที่ 11 กันยายน พ.ศ. 2544

1. ประวัติความเป็นมา

เดิกรัฐบาลสหรัฐฯ มีอิสระอย่างมากในการดักฟังโทรศัพท์ หากเป็นการสืบสวน สอบสวนเพื่อบังคับให้เป็นไปตามกฎหมาย จนกระทั่งศาลฎีกามีคำตัดสินเกี่ยวกับประเด็นนี้เมื่อปี ค.ศ. 1967 และพระราชบัญญัติดักฟังโทรศัพท์ (Wiretap Act) ผ่านการอนุมัติโดยรัฐสภาในปี ค.ศ. 1968 อย่างไรก็ตามยังไม่มีคดีที่มีปัญหาเรื่องความชอบด้วยกฎหมายของการตรวจค้นและดักฟังโทรศัพท์ในประเด็นที่เกี่ยวข้องกับเรื่องความมั่นคงของประเทศจนถึงศตวรรษที่ 70

ปี ค.ศ. 1972 ศาลฎีกาวินิจฉัยถึงประเด็นการดักฟังโทรศัพท์ในคดีความมั่นคงของประเทศที่กลุ่มชาวอเมริกันผู้ต่อต้านสงครามเวียดนามพากันเดือดดาลต่อการกระทำของสำนักงานข่าวกรองกลาง (Central Intelligence Agency หรือ CIA) ที่เจ้าหน้าที่สืบสวนรวบรวมพยานหลักฐานโดยใช้วิธีดักฟังโทรศัพท์โดยไม่ได้รับอนุญาต ฝ่ายเจ้าหน้าที่อ้างว่าประธานาธิบดีมีอำนาจอนุญาตให้สอดแนมโดยไม่ต้องได้รับอนุญาตจากศาลหากเป็นเรื่องความมั่นคงแห่งชาติ

³¹ Federal Judicial Center. “History of the Federal Judiciary”. (ออนไลน์). เข้าถึงได้

จาก : http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html.

ในคดีดังกล่าวศาลวินิจฉัยว่า รัฐบาลไม่ได้มีอำนาจโดยไม่มีข้อจำกัดเพียงเพราะอ้างว่าเป็นเรื่องความมั่นคงของชาติ โดยเฉพาะเป็นการสอดแนมภัยคุกคามที่เกิดอยู่ภายในประเทศ ซึ่งหมายถึง ภัยคุกคามอันเกิดจากชาวอเมริกัน หรือผู้มีถิ่นพำนักถาวรโดยชอบ อย่างไรก็ตามคดีนี้ยังทิ้งประเด็นไว้ต่อว่าถ้าเป็นภัยคุกคามจากนอกประเทศต้องได้รับอนุญาตจากศาลหรือไม่

หลังจากคำวินิจฉัยดังกล่าว มีการเปิดเผยออกมาว่าในช่วงปี ค.ศ. 1960 ถึงต้นปี ค.ศ. 1970 รัฐบาลเข้าสอดแนมโดยไม่ได้รับอนุญาตจากศาล รัฐสภาได้ตัดสินใจวางกรอบทางกฎหมายเพื่อควบคุมการสืบราชการลับที่เกี่ยวกับต่างชาติ ดังนั้นพระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ (Foreign Intelligence Surveillance Act of 1978 หรือ FISA) จึงถูกเสนอขึ้น โดยวุฒิสภา Ted Kennedy เมื่อวันที่ 18 พฤษภาคม ค.ศ. 1977 ในสมัยประธานาธิบดี Carter ในปี ค.ศ. 1978 โดยได้รับการสนับสนุนจากวุฒิสภา 9 คน

พระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ ค.ศ. 1978 ถูกบัญญัติขึ้นและมีการปรับปรุงแก้ไขโดยสร้างกระบวนการร้องขอให้ออกหมายสำหรับการสืบราชการลับที่เกี่ยวกับต่างชาติ เพื่อให้การสอดแนมเช่นนั้นต้องผ่านการตรวจสอบของศาลก่อน โดยที่พระราชบัญญัติฉบับดังกล่าวอนุญาตให้มีการสอดแนมภายในประเทศโดยไม่ต้องขออนุญาตจากศาลในระยะเวลาสูงสุดไม่เกิน 1 ปี เว้นแต่เป็นการสอดแนมเนื้อหาการติดต่อสื่อสารที่มีฝ่ายหนึ่งเป็นชาวอเมริกัน เช่นนี้ต้องขออนุญาตศาลภายใน 72 ชั่วโมง นับแต่เริ่มสอดแนม

2. ขอบเขตและข้อจำกัด

พระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ ค.ศ. 1978 ประสงค์ให้รัฐบาลต้องได้รับอนุญาตจากศาลแม้จะเป็นการสืบสวนที่เกี่ยวกับภัยคุกคามต่อความมั่นคงภายในที่มาจากต่างประเทศ ซึ่งกระบวนการจะแตกต่างจากการบังคับใช้กฎหมายโดยทั่วไป วัตถุประสงค์ของการสอดแนมต้องเป็นไปเพื่อรวบรวมข้อมูลความลับของต่างชาติ และที่สำคัญที่สุด มาตรฐานความน่าจะเป็น (Probable Cause Standard) ยังแตกต่างกัน แทนที่จะแสดงว่ามีความเป็นไปได้ว่าการกระทำผิดกำลังเกิดขึ้น ได้เกิดขึ้นแล้ว หรือกำลังจะเกิดขึ้น รัฐบาลต้องแสดงให้เห็นว่าเป้าหมายการสอดแนมนั้นเป็นผู้ใช้อำนาจนอกประเทศ (Foreign Power) หรือเจ้าหน้าที่ของผู้มีอำนาจนอกประเทศ (Agent of a foreign power) รัฐบาลไม่จำเป็นต้องเปิดเผยแก่เป้าหมายว่าเป้าหมายถูกสอดแนม และบุคคลผู้ปฏิบัติการตามหมายจะถูกห้ามให้ข้อมูลเกี่ยวกับการปฏิบัติการดังกล่าว (Gag Order) เว้นแต่กับทนายความของตัวเอง

ผู้ใช้อำนาจนอกประเทศ (Foreign Power) หมายความว่าให้นิยามไว้กว้าง ๆ เท่านั้น โดยไม่มีการเสนอเป็นประเด็นให้ศาลวินิจฉัย จึงไม่อาจบอกได้ว่าคำนิยามเหล่านั้นจะถูกแปลความ กว้างหรือแคบเพียงใด ทั้งนี้ ตามพระราชบัญญัติฉบับดังกล่าว “ผู้ใช้อำนาจนอกประเทศ” หมายความว่ารวมถึง³²

1. รัฐบาลต่างชาติหรือองค์ประกอบส่วนใดของรัฐบาลต่างชาติ (Any foreign government or component of a foreign government) ไม่ว่าจะได้รับการรับรองจากสหประชาชาติหรือไม่ก็ตาม

2. กลุ่มย่อย (Fraction) ที่อยู่ในรัฐต่างชาติรัฐเดียวหรือหลายรัฐ หรือองค์กรทางการเมืองที่มีฐานอยู่ต่างประเทศ ที่ไม่มีชาวอเมริกันเข้าร่วมเป็นองค์ประกอบสำคัญ (is not substantially composed of)

3. หน่วยงานใด (Any entity) เช่น องค์กรทางการเมืองหรือธุรกิจ ที่ถูกกำกับควบคุมโดยรัฐบาลต่างชาติ

4. กลุ่มใดที่เกี่ยวข้องหรือเตรียมการก่อการร้ายข้ามชาติ (International Terrorism)³³

³² Foreign Intelligence Surveillance Act Sec. 101. (a)

³³ Foreign Intelligence Surveillance Act Sec. 101. (c)

การก่อร้ายข้ามชาติถูกให้คำนิยามไว้กว้าง ๆ ว่าเป็นกิจกรรมซึ่ง

1. ใช้ความรุนแรงหรือเป็นอันตรายต่อมนุษยชาติ อันเป็นความผิดอาญาตามกฎหมาย สหรัฐฯ

2. จะเป็นความผิดเช่นนั้นหากกระทำในสหรัฐฯ หรือสร้างอิทธิพลต่อนโยบายของรัฐ ด้วยวิธีการข่มขู่หรือบังคับ หรือให้มีผลกระทบต่อการทำงานของรัฐบาล ด้วยการลอบสังหารหรือลักพาตัว และ

3. เกิดขึ้นนอกภายนอกสหรัฐฯทั้งสิ้น หรือนอกดินแดนของประเทศ ในแง่ที่ว่า การก่อการร้ายเกิดขึ้นสำเร็จได้อย่างไร บุคคลที่ถูกข่มขู่บังคับ หรือสถานที่ปฏิบัติงานของผู้ก่อการร้าย

สำหรับ เจ้าหน้าที่ของผู้ใช้อำนาจนอกประเทศ (Agent of a foreign power) หมายความว่ารวมถึง³⁴

1. บุคคลที่ไม่ใช่ชาวอเมริกัน ซึ่งเป็นเจ้าหน้าที่หรือลูกจ้างของผู้ใช้อำนาจนอกประเทศ
2. บุคคลที่ไม่ใช่ชาวอเมริกัน ซึ่งเกี่ยวข้องกับกระทำความผิดหรือสายลับในสหรัฐ ในนามของผู้ใช้อำนาจนอกประเทศ หรือชาวอเมริกันที่กระทำการเช่นนั้นและอาจเป็นการละเมิดต่อกฎหมาย
3. บุคคลใดที่ไม่ใช่ชาวอเมริกัน และเข้าเกี่ยวข้องกับการสืบราชการลับ การเป็นสายลับ (Clandestine Intelligence Activities or Spying) หรือชาวอเมริกันที่กระทำในลักษณะเดียวกันและอาจเป็นการล่วงละเมิดต่อกฎหมาย

และข้อมูลลับของต่างชาติ (Foreign Intelligence Information) หมายความว่า ข้อมูลที่จำเป็นแก่การปกป้องสหรัฐอเมริกาจากการโจมตี การก่อวินาศกรรม หรือการก่อการร้ายที่มีความร้ายแรงซึ่งมีอยู่จริงหรือมีความเป็นไปได้ว่าจะเกิดขึ้น³⁵ พระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติให้อำนาจการสอดแนมทางอิเล็กทรอนิกส์และการตรวจค้นทางกายภาพ (electronic surveillance and physical searches) โดยไม่ต้องขออนุญาตจากศาล ยกเว้น ในกรณีที่เกี่ยวข้องกับการก่อการร้ายสากล และมีเงื่อนไขจำกัดการบังคับใช้ต่อชาวอเมริกัน พลเมือง ชาวต่างด้าวที่มีถิ่นพำนักถาวรโดยชอบ และบริษัทที่จัดตั้งขึ้นในสหรัฐอเมริกา

กล่าวโดยสรุป วัตถุประสงค์สำคัญของการสอดแนมทางอิเล็กทรอนิกส์ต้องเป็นไปเพื่อให้ได้ข้อมูลลับที่อยู่ในสหรัฐอเมริกาของผู้ใช้อำนาจนอกประเทศ เช่น สายลับของศัตรู หรือบุคคลที่มีความเกี่ยวข้องกับกลุ่มก่อการร้ายสากล โดยฝ่ายรัฐบาลต้องพิสูจน์ให้ได้ว่ามีความเป็นไปได้ (Probable cause) ว่าเป้าหมายของการสอดแนมอาศัยผู้ใช้อำนาจนอกประเทศหรือเป็นเจ้าหน้าที่ที่อาศัยอำนาจจากผู้ใช้อำนาจนอกประเทศ

3. บทมาตรา

พระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ กำหนดให้ศาลเป็นผู้พิจารณาเป็นการลับ เพื่อออกคำสั่งอนุญาตหรือปฏิเสธคำร้องขอของเจ้าหน้าที่ จากรายงานที่ปรากฏในปี ค.ศ. 1980 ศาลอนุญาตตามคำร้องขอทั้งสิ้น 322 ฉบับ จำนวนคำร้องที่ได้รับอนุญาตสูงเพิ่มขึ้นเรื่อย ๆ จนถึง 2,224 ฉบับในปี ค.ศ. 2006

³⁴ Foreign Intelligence Surveillance Act Sec. 101. (b)

³⁵ Foreign Intelligence Surveillance Act Sec. 101. (e)

ในช่วงระหว่างปี ค.ศ. 1979 - 2006 จากจำนวนคำร้องทั้งหมด 22,990 ฉบับที่ยื่นต่อศาล มีคำร้องที่ศาลอนุญาตไปทั้งสิ้น 22,985 ฉบับ มีเพียง 5 ฉบับเท่านั้นที่ศาลไม่อนุญาต

ในหมวดย่อยของพระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติบัญญัติเนื้อหาสำคัญไว้ในเรื่อง

1. การสอดแนมทางอิเล็กทรอนิกส์ (Electronic surveillance)³⁶ กล่าวโดยทั่วไปกฎหมายฉบับนี้อุญาตให้มีการสอดแนมได้ใน 2 รูปแบบ

1. แบบที่ไม่ต้องได้รับอนุญาตจากศาล โดยประธานาธิบดีเป็นผู้อนุมัติผ่านทางอัยการสูงสุด ทั้งนี้การสอดแนมนั้นต้องมีระยะเวลา 1 ปี กระทำเพื่อให้ได้ข้อมูลลับของต่างชาติของผู้ใช้อำนาจนอกประเทศที่เป็นเป้าหมาย โดยไม่มีแนวโน้มว่ามีเนื้อหาการติดต่อสื่อสารที่ฝ่ายหนึ่งเป็นชาวอเมริกัน อัยการสูงสุดมีหน้าที่ยื่นคำรับรองปิดผนึกต่อศาลที่ทำหน้าที่ตรวจสอบงานข่าวกรองต่างชาติ (Foreign Intelligence Surveillance Court) ว่าเป็นการสอดแนมที่ครบตามเงื่อนไขที่กฎหมายบัญญัติข้างต้น และยังต้องรายงานเสนอต่อรัฐสภาด้านงานข่าวกรอง (House Permanent Select Committee on Intelligence และ The Senate Select Committee on Intelligence) อีกด้วย ตามที่พระราชบัญญัติฉบับนี้จำกัดการสอดแนมโดยไม่ต้องได้รับอนุญาตจากศาลได้เฉพาะที่เกี่ยวข้องกับผู้ใช้อำนาจนอกประเทศที่กล่าวถึงในมาตรา 1802 (a) (1) (A) เท่านั้น ดังนั้นการสอดแนมที่ไม่ต้องขออนุญาตศาลข้างต้นจึงไม่ใช้กับกรณีอื่น เช่น กลุ่มที่เกี่ยวข้องกับการก่อการร้ายสากลหรือการเตรียมการกระทำเช่นนั้น องค์การทางการเมืองที่มีฐานอยู่ต่างประเทศและไม่มีชาวอเมริกันเป็นผู้มีส่วนประกอบสำคัญ หรือหน่วยงานที่อยู่ในการกำกับหรือควบคุมของรัฐต่างชาติ

บุคคลใดก็ตามที่เกี่ยวข้องกับการสอดแนมทางอิเล็กทรอนิกส์โดยฝ่าฝืนต่อกฎหมายนี้มีโทษในทางอาญาและความรับผิดชอบทางแพ่ง

ประธานาธิบดีโดยผ่านอัยการสูงสุดมีอำนาจสอดแนมทางอิเล็กทรอนิกส์โดยไม่ต้องขออนุญาตศาลเพื่อให้ได้มาซึ่งข้อมูลลับต่างชาติในช่วงเวลาไม่เกิน 15 วันตามปฏิทิน นับแต่วันที่รัฐสภาประกาศภาวะสงคราม

2. แบบที่ต้องขออนุญาตศาล กรณีนี้ให้รัฐบาลยื่นคำร้องขออนุญาตสอดแนมอิเล็กทรอนิกส์ต่อศาล FISA ศาลจะอนุญาตตามขอได้ต่อเมื่อมีเหตุความเป็นไปได้ว่าเป้าหมายที่ต้องการสอดแนมเป็นผู้ใช้อำนาจนอกประเทศหรือเป็นเจ้าหน้าที่ของผู้นั้น

³⁶ Foreign Intelligence Surveillance Act Sec. 101. (f)

2. การตรวจค้นทางกายภาพ (Physical searches)

พระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ ให้อำนาจตรวจค้นที่ดิน ข้อมูล วัตถุ ทรัพย์สิน ที่ผู้ใช้อำนาจนอกประเทศใช้โดยเฉพาะ ส่วนองค์ประกอบและขั้นตอนในการขอเกือบจะเหมือนกับการขอสอดแนมทางอิเล็กทรอนิกส์

ศาลตรวจสอบข้อมูลลับของต่างชาติ (Foreign Intelligence Surveillance Court)

พระราชบัญญัตินี้จัดตั้งศาลที่ทำหน้าที่ตรวจสอบงานข่าวกรองต่างชาติ มีชื่อว่า Foreign Intelligence Surveillance Court หรือ FISC เพื่อพิจารณาคำร้องขอสอดแนมของเจ้าหน้าที่ตำรวจที่กระทำต่อผู้ต้องสงสัยซึ่งเป็นสายลับต่างชาติในสหรัฐอเมริกา ศาลนี้ตั้งอยู่ในอาคารสำนักงานใหญ่ของกระทรวงยุติธรรม ประกอบไปด้วยผู้พิพากษา 11 คน ที่อธิบดีศาลฎีกาสหรัฐแต่งตั้ง มีระยะเวลาดำรงตำแหน่ง 7 ปี

ศาลตรวจสอบข้อมูลลับของต่างชาติ จะดำเนินกระบวนการพิจารณาในลักษณะฝ่ายเดียว ไม่มีคู่กรณีอีกฝ่าย โดยฟังพยานหลักฐานทั้งหมดตามที่กระทรวงยุติธรรมเสนอต่อศาล ไม่มีบทมาตรใดที่กล่าวถึงการให้ข้อมูลเกี่ยวกับการพิจารณาหรือการจัดเก็บข้อมูล

กรณีศาลยกคำร้อง ผู้ยื่นคำร้องอาจอุทธรณ์ไปยังศาลพิเศษชั้นอุทธรณ์ มีชื่อว่า Foreign Intelligence Surveillance Court of Review ศาลชั้นอุทธรณ์นี้ประกอบด้วยองค์คณะผู้พิพากษา 3 คน และนับแต่ก่อตั้งมา ศาลชั้นอุทธรณ์ดังกล่าวพิจารณาคดีอุทธรณ์เพียง 2 ครั้ง ในปี ค.ศ. 2002 และ 2008

4. การเยียวยาผู้ใช้กรณีมีการกระทำละเมิด (Remedies for violations)

ผู้สอดแนมอิเล็กทรอนิกส์หรือตรวจค้นทางกายภาพฝ่าฝืนพระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ อาจต้องโทษทางอาญาและมีความรับผิดชอบแก่ผู้ฝ่าฝืนต้องรับโทษทางอาญาต่อเมื่อมีเจตนาสอดแนมโดยไม่ได้รับอนุญาต หรือเปิดเผยหรือใช้ข้อมูลที่ตนรู้หรือมีเหตุอันควรรู้ว่าข้อมูลนั้นได้รับมาจากการสอดแนมโดยไม่ได้รับอนุญาต มีระวางโทษจำคุกสูงสุด 7 ปี หรือปรับสูงสุด 10,000 ดอลลาร์ หรือทั้งจำทั้งปรับ ทั้งนี้กฎหมายเปิดช่องให้เจ้าหน้าที่ที่ถูกฟ้องนำสืบพิสูจน์ให้พ้นผิดได้ หากเป็นการกระทำตามหน้าที่โดยคำสั่งศาลที่ชอบด้วยกฎหมาย แต่ข้อพิสูจน์นี้ไม่ให้ใช้กับกรณีที่เจ้าหน้าที่ผู้นั้นปฏิบัติตามคำสั่งของประธานาธิบดี

5. Lone wolf amendment

ในปี ค.ศ. 2004 มีการแก้ไข พระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ โดยเพิ่มเติม Lone wolf ได้แก่ บุคคลที่ไม่ใช่ชาวอเมริกัน แต่มีความเกี่ยวข้องกับก่อการร้ายสากล หรือการเตรียมการกระทำเช่นนั้น ให้ถือว่าเป็นเจ้าหน้าที่ของผู้ใช้อำนาจนอกประเทศ โดยผู้ร้องขอไม่ต้องแสดงให้เห็นว่าบุคคลผู้นั้นมีความเกี่ยวข้องกับต่างชาติหรือกลุ่มต่างชาตินั้นอย่างไร

6. ปัญหาเรื่องความชอบด้วยรัฐธรรมนูญ

6.1 ยุคก่อนพระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ

ในปี ค.ศ. 1967 ศาลฎีกาสหรัฐวินิจฉัยในคดี Katz V. United states (1967) ว่ารัฐธรรมนูญฉบับแก้ไข (ฉบับที่ 4) (Fourth Amendment) คุ้มครองประชาชนจากการตรวจค้นและยึดโดยมิชอบเพื่อปกป้องสิทธิความเป็นส่วนตัวซึ่งคาดหมายได้ตามสมควร (reasonable expectation of privacy) ในคดีดังกล่าวไม่ได้กล่าวถึงประเด็นเรื่องความมั่นคงของชาติ ไม่นานหลังจากนั้นในปี ค.ศ.1972 ศาลฎีกาสหรัฐวินิจฉัยในคดี United States V. US District Court (1972) ว่าเจ้าหน้าที่รัฐจะต้องขออนุญาตจากศาลก่อนจึงจะเริ่มสอดแนมทางอิเล็กทรอนิกส์ได้ แม้จะมีประเด็นเรื่องความมั่นคงภายในเข้ามาเกี่ยวข้องก็ตาม แต่คดีนี้ก็ไม่ได้กล่าวถึงกรณีที่เกี่ยวข้องกับการกระทำของผู้ใช้อำนาจนอกประเทศหรือเจ้าหน้าที่ของผู้มีอำนาจดังกล่าว ต่อมาศาลฎีกาสหรัฐมีคำวินิจฉัยเกี่ยวกับการดักฟังโทรศัพท์โดยไม่ได้รับอนุญาตในคดี United States V. Brown (1973) และคดี United States V. Butenko (1974) วินิจฉัยว่ารัฐสามารถกระทำได้หากเป็นไปเพื่อรวบรวมข้อมูลลับของต่างชาติ ส่วนในคดี Zweibon V. Mitchell (1975) วินิจฉัยว่าการสอดแนมองค์กรในประเทศที่ไม่ได้รับอนุญาตจากศาลไม่ชอบด้วยเหตุผลและขัดต่อรัฐธรรมนูญ

6.2 ยุคหลังพระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ

มีคดีน้อยมากที่วินิจฉัยเรื่องความชอบด้วยรัฐธรรมนูญของพระราชบัญญัติฉบับนี้ ในคดี United States V. Duggan (1988) จำเลยเป็นชาวไอแลนด์และเป็นสมาชิกกลุ่มแบ่งแยกดินแดน ไอแลนด์ถูกศาลพิพากษาว่ามีความผิดฐานขนส่งระเบิดและอาวุธปืนทางทะเลจำนวนมาก ศาลวินิจฉัยว่าประเด็นความมั่นคงของชาติเป็นข้อพิจารณาเรื่องการปฏิบัติที่แตกต่างกันระหว่างพลเมืองชาวอเมริกาและคนต่างด้าวที่ไม่มีถิ่นพำนักในสหรัฐอเมริกา

คดี United States V. Nicholson (1997) ศาลวินิจฉัยว่า FISA ไม่ขัดต่อหลักการ Due process ของ Fifth Amendment ไม่ขัดต่อหลักการ Equal protection, Separation of powers และ Right to counsel ของ Sixth Amendment

มีข้อสนใจในคดี In re Sealed Case (2002) ที่นอกจากศาลพิเศษชั้นอุทธรณ์ States Foreign Intelligence Surveillance Court of Review จะตัดสินว่า FISA ชอบด้วยรัฐธรรมนูญแล้ว ยังมีส่วนที่วินิจฉัยกลับคำสั่งของศาลตรวจสอบข้อมูลลับของต่างชาติ ว่าการที่ศาลอนุญาตให้สอดแนมแต่ไปกำหนดเงื่อนไขจำกัดห้ามมิให้เจ้าหน้าที่นำพยานหลักฐานที่รวบรวมมาได้มาเป็นส่วนหนึ่งของการฟ้องคดีอาญาเป็นการมิชอบ โดยเฉพาะศาลไปวินิจฉัยถึงประเด็นว่าพระราชบัญญัติฉบับนี้ไม่ได้เป็นการจำกัดอำนาจของประธานาธิบดีที่มีอยู่เดิมตามรัฐธรรมนูญในการค้นหาข้อมูลลับของต่างชาติ

กฎหมายที่เกี่ยวข้องและวิธีดำเนินการตรวจสอบโดยศาล

1. หลักการทั่วไป

หากรัฐต้องการเข้าถึงหรือใช้ข้อมูลที่ได้รับจากการคุ้มครอง ซึ่งรัฐได้มาจากการตรวจสอบและแทรกแซงการสื่อสาร อันเกี่ยวพันกับความมั่นคงของชาติ จะต้องมืองค์กรคอยถ่วงดุลและตรวจสอบการใช้อำนาจดังกล่าวอย่างถูกต้อง เพื่อมิให้เป็นการล่วงละเมิดสิทธิและเสรีภาพของประชาชน ซึ่งต้องเป็นอิสระแยกจากหน่วยงานที่เป็นผู้ตรวจสอบการสื่อสาร มีความเชี่ยวชาญในประเด็นที่เกี่ยวข้องและสามารถที่จะวินิจฉัยในเรื่องความชอบด้วยกฎหมายของการตรวจสอบการสื่อสาร เทคนิคที่ใช้และหลักสิทธิมนุษยชนและ มีทรัพยากรที่เพียงพอต่อการปฏิบัติหน้าที่ซึ่งได้รับมอบหมาย องค์กรดังกล่าวคือ ศาลยุติธรรม

ทั้งนี้ การตรวจสอบและแทรกแซงการสื่อสารจะต้องปรากฏต่อศาลว่า

1. มีความเป็นไปได้สูงว่าจะมีการกระทำความผิดซึ่งเกี่ยวพันกับความมั่นคงของชาติเกิดขึ้น
2. ต้องมีการเข้าถึงข้อมูลที่ได้รับจากการคุ้มครองจึงจะได้มาซึ่งพยานหลักฐานแห่งการกระทำความผิดดังกล่าว
3. ไม่สามารถหาวิธีการอื่นที่เป็นการรุกรานรบกวนเสรีภาพในการสื่อสารได้น้อยกว่านี้ได้อีก
4. การเข้าถึงข้อมูลต้องจำกัดตามสมควรอยู่เท่าที่เกี่ยวข้องกับอาชญากรรมที่มีการกล่าวอ้าง และข้อมูลที่ได้รับรวบรวมมาได้ต้องถูกทำลายหรือส่งคืนโดยทันที และ
5. การเข้าถึงข้อมูลให้กระทำโดยหน่วยงานที่ตั้งขึ้นพิเศษและให้มีการใช้ข้อมูลได้ภายในขอบเขตวัตถุประสงค์ที่ได้รับอนุญาต

2. กฎหมายที่เกี่ยวข้อง

การแทรกแซงเสรีภาพในการสื่อสารของบุคคล จำต้องมีบทบัญญัติของกฎหมายให้อำนาจต่าง ๆ แก่เจ้าหน้าที่รัฐ เพื่อให้ได้มาซึ่งข้อมูลข่าวสาร แต่การให้อำนาจทั้งหลายนั้น ต้องมีการควบคุมและตรวจสอบ หรือใช้หลักการตรวจสอบและถ่วงดุลอำนาจระหว่างองค์กร³⁷ เพื่อตรวจสอบการใช้อำนาจของรัฐในการแสวงหาข้อมูลข่าวสาร อันเกิดจากการแทรกแซงการสื่อสาร

³⁷ สุขศักดิ์ ลิขสิทธิ์วัฒนกุล. “อำนาจรัฐกับการดักฟังทางโทรศัพท์”. การเสวนาทางวิชาการ เมื่อวันที่ 2 กุมภาพันธ์ 2539 ห้องประชุม 112 คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ วารสารนิติศาสตร์, ปีที่ 26, ฉบับที่ 3 (กันยายน 2539), น. 657.

ซึ่งกระทบต่อสิทธิและเสรีภาพของบุคคลโดยตรง ทั้งนี้ กฎหมายหลายฉบับให้อำนาจศาลยุติธรรม ดำเนินการตรวจสอบความชอบด้วยกฎหมาย เมื่อรัฐหรือเจ้าหน้าที่ของรัฐจำเป็นต้องใช้มาตรการ แทรกแซงเสรีภาพในการสื่อสารหรือการตรวจสอบการสื่อสาร ดังนี้

2.1 ประมวลกฎหมายวิธีพิจารณาความอาญา

ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 105 บัญญัติว่า

“จดหมาย ไปรษณียบัตร โทรเลข สิ่งพิมพ์หรือเอกสารอื่น ซึ่งส่งทางไปรษณีย์ และโทรเลข จากหรือถึงผู้ต้องหาหรือจำเลยและยังมีได้ส่ง ถ้าเจ้าหน้าที่ต้องการเพื่อประโยชน์แห่ง การสอบสวนได้สวนมูลฟ้อง พิจารณา หรือการกระทำอย่างอื่นตามประมวลกฎหมายนี้ ให้ขอคำสั่ง จากศาลถึงเจ้าหน้าที่ ไปรษณีย์โทรเลขให้ส่งเอกสารนั้นมา ...”

บทบัญญัติดังกล่าว กำหนดให้เจ้าหน้าที่ต้องขออนุญาตต่อศาล เพื่อให้ศาลมี คำสั่งถึงเจ้าหน้าที่ไปรษณีย์ โทรเลขให้ส่งจดหมาย ไปรษณียบัตร โทรเลข สิ่งพิมพ์หรือเอกสารอื่น ซึ่งส่งทางไปรษณีย์และโทรเลข จากหรือถึงผู้ต้องหาหรือจำเลยและยังมีได้ส่ง

2.2 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542

มาตรา 46 บัญญัติว่า

“ในกรณีที่มีพยานหลักฐานตามสมควรว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ ในการกระทำความผิดฐานฟอกเงิน พนักงานเจ้าหน้าที่ซึ่งเลขาธิการมอบหมายเป็นหนังสือจะยื่นคำ ขอฝ่ายเดียวต่อศาลแพ่ง เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชี ข้อมูลทางการสื่อสาร หรือข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็”

ในกรณีตามวรรคหนึ่ง ศาลจะสั่งอนุญาตให้พนักงานเจ้าหน้าที่ผู้ยื่นคำขอ ดำเนินการ โดยใช้เครื่องมือหรืออุปกรณ์ใด ๆ ตามที่เห็นสมควรก็ได้ แต่ทั้งนี้ให้อนุญาตได้คราวละ ไม่เกินเก้าสิบวันเมื่อศาลได้สั่งอนุญาตตามความในวรรคหนึ่งหรือวรรคสองแล้ว ผู้เกี่ยวข้องกับ บัญชี ข้อมูลทางการสื่อสาร หรือข้อมูลคอมพิวเตอร์ตามคำสั่งดังกล่าว จะต้องให้ความร่วมมือ เพื่อให้เป็นไปตามความในมาตรานี้”

พระราชบัญญัตินี้มิได้กำหนดหลักเกณฑ์ หรือเงื่อนไข เพื่อประกอบการ พิจารณาสั่งของศาล ดังเช่นพระราชบัญญัติอื่น ๆ

2.3 พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม ฉบับที่ 4 พ.ศ. 2545

มาตรา 14 จัตวา บัญญัติว่า

“ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด เจ้าพนักงานซึ่งได้รับอนุมัติจากเลขาธิการเป็นหนังสือ จะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้เจ้าพนักงานได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญา พิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

1. มีเหตุอันควรเชื่อว่าจะมีการกระทำความผิดหรือจะมีการกระทำความผิดเกี่ยวกับยาเสพติด
2. มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดเกี่ยวกับยาเสพติดจากการเข้าถึงข้อมูลข่าวสารดังกล่าว
3. ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้...”

2.4 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 บัญญัติว่า

“ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ พนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญา เพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

1. มีเหตุอันควรเชื่อว่าจะมีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ
2. มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว
3. ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้ ...”

2.5 พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551

มาตรา 30 บัญญัติว่า

“ในกรณีที่มีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อสารสนเทศอื่นใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานค้ามนุษย์ พนักงานเจ้าหน้าที่ซึ่งได้รับอนุมัติเป็นหนังสือจากผู้บัญชาการตำรวจแห่งชาติ อธิบดีกรมสอบสวนคดีพิเศษ หรือผู้ว่าราชการจังหวัด แล้วแต่กรณี จะยื่นคำขอฝ่ายเดียวต่อศาลอาญาหรือศาลจังหวัดที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ได้มาซึ่งเอกสาร หรือข้อมูลข่าวสารดังกล่าวก็ได้ ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่กำหนดในข้อบังคับประธานศาลฎีกา

การอนุญาตตามวรรคหนึ่ง ให้ศาลพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็น ดังต่อไปนี้

1. มีเหตุอันควรเชื่อว่าจะมีการกระทำความผิดหรือจะมีการกระทำความผิดฐานค้ามนุษย์
2. มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดฐานค้ามนุษย์จากการเข้าถึงข้อมูลข่าวสารดังกล่าว
3. ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้ ...”

พระราชบัญญัตินี้ให้อำนาจประธานศาลฎีกาออกข้อบังคับประธานศาลฎีกาเพื่อกำหนดหลักเกณฑ์และวิธีการ เกี่ยวกับการยื่นคำขอ และการพิจารณาสั่งอนุญาตของศาล

3. วิธีการดำเนินการตรวจสอบโดยศาล

3.1 ประมวลกฎหมายวิธีพิจารณาความอาญา

เมื่อศาลได้รับคำร้องของเจ้าหน้าที่ตามมาตรา 105 ศาลจะต้องพิจารณาว่า การได้มาซึ่งจดหมาย ไปรษณียบัตร โทรเลข สิ่งพิมพ์หรือเอกสารอื่น ตามคำร้องขอของเจ้าหน้าที่นั้น เป็นไปเพื่อประโยชน์แห่งการสอบสวน ใ้สวนมูลฟ้อง พิจารณาหรือการกระทำอย่างอื่นตามประมวลกฎหมายนี้หรือไม่ หากตามคำร้องปรากฏว่าเป็นไปเพื่อการนั้น ก็ให้ศาลมีคำสั่งไปถึงเจ้าหน้าที่ไปรษณีย์โทรเลขส่งเอกสารนั้นมาให้แก่ศาล

3.2 พระราชบัญญัติอื่น

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม ฉบับที่ 4 พ.ศ. 2545 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และพระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551

มีบทบัญญัติที่เกี่ยวข้องกับการตรวจสอบและแทรกแซงเสรีภาพในการสื่อสาร โดยอาศัยหลักการอย่างเดียวกัน ดังนี้

1. มีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อสารสนเทศอื่นใด ถูกใช้หรืออาจถูกใช้

2. เพื่อประโยชน์ในการกระทำความผิดตามพระราชบัญญัตินั้นกำหนด ได้แก่ การกระทำความผิดฐานฟอกเงิน การกระทำความผิดเกี่ยวกับยาเสพติด การกระทำความผิดที่เป็นคดีพิเศษ และการกระทำความผิดฐานค้ามนุษย์ ซึ่งความผิดต่าง ๆ เหล่านี้เป็นความผิดอันเกี่ยวกับความมั่นคงของชาติ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชน

หากเข้าเหตุดังกล่าวข้างต้น เจ้าหน้าที่ของรัฐซึ่งต้องใช้มาตรการตรวจสอบและแทรกแซงเสรีภาพในการสื่อสารต้องขออนุญาตต่อศาลก่อน

3.2.1 การดำเนินการตรวจสอบก่อนมีคำสั่ง

เมื่อเจ้าหน้าที่ได้ขออนุญาต และผู้บังคับบัญชาหรือหัวหน้าหน่วยงานหรือองค์กรของรัฐได้ใช้ดุลพินิจและพิจารณาอนุมัติแล้ว เจ้าหน้าที่จะต้องยื่นคำร้องดังกล่าวเป็นคำขอฝ่ายเดียวต่อศาลเพื่อมีคำสั่งอนุญาตให้เจ้าหน้าที่กระทำการใด ๆ เพื่อให้ได้มาซึ่งเอกสาร หรือข้อมูลข่าวสาร โดยเจ้าหน้าที่รัฐจะต้องนำสำนวนทั้งหลายไปประกอบการพิจารณาขออนุญาต

ศาลจะทำการพิจารณาคำร้องจากพยานหลักฐานที่เสนอโดยเจ้าหน้าที่ของรัฐ โดยคำนึงถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็น กล่าวคือ มีเหตุอันควรเชื่อว่าจะมีการกระทำความผิดหรือจะมีการกระทำความผิดตามพระราชบัญญัตินั้น ๆ มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดจากการเข้าถึงข้อมูลข่าวสารดังกล่าว และไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้ หากศาลตรวจสอบแล้วไม่ปรากฏว่ามีเหตุอันควรสงสัย ศาลก็จะมีคำสั่งไม่อนุญาต แต่ถ้าพิจารณาจากพยานหลักฐานแล้วมีเหตุอันควรสงสัยจริง เพียงแต่พยานหลักฐานยังไม่เพียงพอ จึงต้องอาศัยพยานหลักฐานอื่นเพิ่มเติมมากกว่านั้น และเห็นว่าไม่มีวิธีการอื่นใดแล้ว ศาลก็อนุญาตให้ใช้มาตรการตรวจสอบและแทรกแซงการสื่อสารได้

ศาลต้องพิจารณาให้ได้ความตามหลักเกณฑ์ดังกล่าว และเจ้าหน้าที่มีภาระการพิสูจน์เพื่อแสดงให้เห็นว่า ในการที่จะแสวงหาข้อมูลที่มีเหตุอันควรเชื่อได้ว่า หากไม่ใช้มาตรการตรวจสอบและแทรกแซงเพื่อให้ได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ตามที่กฎหมายให้อำนาจแล้ว เจ้าหน้าที่จะไม่สามารถแสวงหาข้อมูล เพื่อใช้เป็นพยานหลักฐานนำตัวผู้กระทำความผิด

มาลงโทษได้ ซึ่งหากศาลพิจารณาแล้วเห็นว่าไม่เข้าหลักเกณฑ์ทั้งสามประการนี้ ศาลมีอำนาจยกคำร้องดังกล่าวได้

3.2.2 การดำเนินการตรวจสอบหลังมีคำสั่ง

หลังจากศาลมีคำสั่งให้เจ้าหน้าที่ของรัฐดำเนินการอย่างใด เพื่อให้ได้มาซึ่งเอกสาร หรือข้อมูลข่าวสาร ซึ่งเชื่อได้ว่าเพื่อประโยชน์ในการกระทำความผิด ได้ดำเนินการตรวจสอบและแทรกแซงการสื่อสาร เพื่อรวบรวมพยานหลักฐาน อันเป็นประโยชน์ต่อการสืบสวนสอบสวนแล้ว กฎหมายบัญญัติว่าภายหลังศาลมีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือมีพฤติการณ์เปลี่ยนแปลงไป ให้ศาลมีอำนาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร กล่าวคือ ในการขออนุญาตใช้มาตรการอย่างใดเพื่อให้ได้มาซึ่งเอกสารหรือข้อมูลข่าวสารเพื่อประโยชน์ในการกระทำความผิด การอนุญาตนั้น ศาลจะสามารถสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวัน โดยจะกำหนดเงื่อนไขอย่างใดก็ได้ ซึ่งภายหลังพ้นกำหนดเก้าสิบวันแล้ว เจ้าหน้าที่ของรัฐต้องการที่จะขออนุญาตศาลเพื่อใช้มาตรการดังกล่าวต่อ ศาลจะต้องพิจารณาว่า ในการขออนุญาตใช้มาตรการนั้นครั้งแรก เจ้าหน้าที่ของรัฐผู้ขออนุญาต สามารถหาพยานหลักฐาน เอกสาร หรือข้อมูล เพื่อใช้ในการกระทำความผิด จากการใช้มาตรการดังกล่าวหรือไม่อย่างไร ซึ่งหากศาลเห็นว่า การดำเนินการตามมาตรการดังกล่าวของเจ้าหน้าที่รัฐในครั้งแรกไม่สามารถหาพยานหลักฐาน เอกสาร หรือข้อมูลได้ เจ้าหน้าที่ของรัฐก็จำเป็นต้องหาพยานหลักฐานแจ้งต่อศาลว่ามีเหตุจำเป็นซึ่งจะต้องใช้มาตรการดังกล่าวอยู่ ดังเช่นที่ศาลขออนุญาตศาลในครั้งแรก แต่พยานหลักฐานในครั้งต่อมาศาลควรพิจารณาว่ามีน้ำหนักมากกว่าการแสดงพยานหลักฐานในครั้งแรก ว่ามีเหตุจำเป็นที่จะต้องใช้มาตรการดังกล่าวจริง ซึ่งหากศาลเห็นว่าเป็นการไร้ประโยชน์ที่จะใช้มาตรการดังกล่าว หรือไม่มีเหตุจำเป็น ประกอบกับพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใด และเหตุผลความจำเป็นแล้ว ศาลมีอำนาจเปลี่ยนแปลงคำสั่ง หรือสั่งไม่อนุญาตให้เจ้าหน้าที่ของรัฐใช้มาตรการดังกล่าวต่อไปก็ได้

กรณีที่มีการดำเนินการตามมาตรการในครั้งแรกสามารถหาพยานหลักฐาน เอกสาร หรือข้อมูลได้ และเจ้าหน้าที่ของรัฐประสงค์จะใช้มาตรการดังกล่าวต่อ เจ้าหน้าที่ของรัฐจะต้องแจ้งให้ศาลทราบ เพื่อขออนุญาต ศาลจะต้องพิจารณาจากข้อเท็จจริง เหตุผลความจำเป็นหรือพฤติการณ์ หากไม่ปรากฏว่ามีความจำเป็นหรือพฤติการณ์เปลี่ยนแปลงไป ศาลก็มีคำสั่งอนุญาต หรือไม่อนุญาตได้ตามที่เห็นสมควร หากว่าศาลเห็นสมควรอนุญาต ก็อาจจะเปลี่ยนแปลงคำสั่งดังกล่าว เช่น เปลี่ยนแปลงวิธีการดำเนินการ จากมาตรการดักฟังทางโทรศัพท์ เป็นแจ้งให้บุคคลส่งเอกสารหรือข้อมูลใดต่อศาล เป็นต้น

4. ปัญหาจากกฎหมายที่เกี่ยวข้องและวิธีดำเนินการตรวจสอบโดยศาล

4.1 ปัญหาจากบทบัญญัติแห่งกฎหมาย

ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 105 ให้อำนาจศาลมีคำสั่งหากเจ้าหน้าที่รัฐต้องการตรวจสอบจดหมาย ไปรษณียบัตร โทรเลข สิ่งพิมพ์หรือเอกสารอื่น ซึ่งส่งทางไปรษณีย์และโทรเลข จากหรือถึงผู้ต้องหาหรือจำเลยและยังมีได้ส่ง แต่หากเป็นกรณีของการใช้เครือข่ายสังคมออนไลน์ จะเข้าหลักเกณฑ์ตามมาตรานี้หรือไม่ ตัวอย่างกรณี กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) จะทำการตรวจสอบและออกกฎหมายในการควบคุมการใช้ Line โดยลำพังตนเอง ไม่ผ่านการตรวจสอบของศาลยุติธรรม³⁸ นั้น

มีปัญหาว่า จากกรณีดังกล่าว หากมีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางเครือข่ายสังคมออนไลน์ เช่น Line Whatsapp Twitter และ Facebook ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดอันเกี่ยวกับความมั่นคงของชาติ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชน หรือเพื่อหาพยานหลักฐาน อันเป็นประโยชน์แห่งการสอบสวน ไล่สวนมูลฟ้อง พิจารณา หรือการกระทำอย่างอื่นตามประมวลกฎหมายวิธีพิจารณาความอาญา หรือกฎหมายอื่น เจ้าหน้าที่รัฐผู้ทำการตรวจสอบจะต้องขออนุญาตต่อศาลหรือไม่

ประการแรก ต้องพิจารณาเสียก่อนว่า การติดต่อสื่อสารผ่านทางเครือข่ายสังคมออนไลน์ เช่น Line Whatsapp Twitter และ Facebook นั้น ถือได้ว่าเป็นสิ่งพิมพ์หรือเอกสารอื่นหรือไม่ หากพิจารณาจากประมวลกฎหมายอาญา มาตรา 1 (7) เอกสาร หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข พัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพหรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น จะเห็นได้ว่า การติดต่อสื่อสารผ่านทางเครือข่ายสังคมออนไลน์ เช่น Line Whatsapp Twitter และ Facebook จะเป็นในรูปแบบของตัวอักษรหรือข้อความ จึงถือว่าเป็นเอกสารตามประมวลกฎหมายอาญา ดังนั้น จึงเป็นเอกสารอื่นตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 105 ด้วย

³⁸ ทีมข่าวไทยรัฐออนไลน์. “สถานาย ท้วง ปอท. สอบแชทไลน์ ไม่ผ่านศาลผิด”.

(ออนไลน์). เข้าถึงได้จาก : <http://www.thairath.co.th/content/363656>, 2556.

ประการที่สอง มาตรา 105 กำหนดว่า การส่งนั้น ต้องส่งทางไปรษณีย์และโทรเลข ซึ่งระบบการทำงานของเครือข่ายสังคมออนไลน์นั้น ไม่ได้มีการส่งทางไปรษณีย์หรือโทรเลข แต่เป็นการส่งข้อมูลผ่านระบบที่เรียกว่า Network จึงไม่เข้าเงื่อนไขดังกล่าวที่เจ้าหน้าที่รัฐจะต้องขออนุญาตต่อศาล เพื่อให้ศาลมีคำสั่ง

ดังนั้น หากเป็นกรณีเจ้าหน้าที่ของรัฐจะทำการตรวจสอบการใช้งานผ่านเครือข่ายสังคมออนไลน์ ย่อมไม่จำเป็นต้องขอคำสั่งจากศาล ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 105

ส่วนกรณีตามพระราชบัญญัติต่าง ๆ ให้อำนาจเจ้าหน้าที่รัฐตรวจสอบและแทรกแซง เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อสารสนเทศอื่นใด ซึ่งครอบคลุมถึงเครือข่ายสังคมออนไลน์ที่เป็นรูปแบบของการส่งข้อมูลข่าวสารทางคอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อสารสนเทศอื่นใดอยู่แล้ว ดังนั้น หากเจ้าหน้าที่ของรัฐต้องการตรวจสอบหรือแทรกแซงการติดต่อสื่อสารผ่านเครือข่ายสังคมออนไลน์ โดยอาศัยอำนาจตามพระราชบัญญัติที่เกี่ยวข้อง ย่อมต้องร้องขอต่อศาล เพื่อให้ศาลมีคำสั่งอนุญาต

4.2 ปัญหาเกี่ยวกับการดำเนินการตรวจสอบโดยศาล

4.2.1 หลักเกณฑ์และวิธีการเกี่ยวกับการออกคำสั่ง

การดำเนินการตรวจสอบโดยศาล ยังไม่มีหลักเกณฑ์การพิจารณาอย่างชัดเจน ในกรณีของการพิจารณาพยานหลักฐานของศาลก่อนมีคำสั่งอนุญาต กฎหมายที่เกี่ยวข้องก็มิได้บัญญัติถึงการรับฟังพยานหลักฐานเพื่อประกอบการพิจารณาแต่อย่างใด กฎหมายบัญญัติเพียงให้ศาลพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นเท่านั้น จึงอาจเกิดปัญหาเกี่ยวกับมาตรฐานในการพิจารณาพยานหลักฐานว่าต้องมีน้ำหนักมากเพียงใด ซึ่งแตกต่างกันไปตามแต่ดุลพินิจของศาล ทั้งยังไม่มีวิธีการ รูปแบบ และขั้นตอนในการขออนุญาตเพื่อใช้มาตรการตรวจสอบและแทรกแซงการสื่อสารของหน่วยงานต่าง ๆ หรือเจ้าหน้าที่รัฐ

นอกจากนี้ พระราชบัญญัติป้องกันและปราบปรามการค้ำมนุษย์ พ.ศ. 2551 กำหนดการให้ยื่นคำขอฝ่ายเดียวต่อศาลอาญาหรือศาลจังหวัดที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ได้มาซึ่งเอกสาร หรือข้อมูลข่าวสารดังกล่าวก็ได้ เป็นไปตามหลักเกณฑ์และวิธีการที่กำหนดในข้อบังคับประธานศาลฎีกา ซึ่งปัจจุบันยังไม่มีการออกข้อบังคับของประธานศาลฎีกาเพื่อให้เป็นไปตามบทบัญญัติแห่งมาตรานี้แต่อย่างใด

ผู้เขียนเห็นว่า การได้มาซึ่งเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด อันกระทบต่อสิทธิและเสรีภาพในการสื่อสาร จะกระทำมิได้เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย ถึงแม้ว่าจะมีกฎหมายให้อำนาจไว้ก็ต้องมีองค์การคอยตรวจสอบ โดยศาลเป็นองค์กรซึ่งกฎหมายบัญญัติให้อำนาจในการพิจารณาอนุญาต ดังนั้น เพื่อให้การออกคำสั่งของศาลเป็นไปอย่างเหมาะสม เป็นหลักประกันการคุ้มครองสิทธิและเสรีภาพของประชาชน จึงควรมีหลักเกณฑ์มาตรฐานในการพิจารณาพยานหลักฐานของศาลก่อนมีคำสั่ง และวิธีการเกี่ยวกับการออกคำสั่งไว้เพื่อถือปฏิบัติเป็นแนวเดียวกัน

4.2.2 เขตอำนาจศาล

เนื่องจากมีกฎหมายที่เกี่ยวข้องหลายฉบับ และกฎหมายแต่ละฉบับที่วัตถุประสงค์แตกต่างกันไป รวมถึงศาลซึ่งมีอำนาจพิจารณาสั่งก็แตกต่างกันไปด้วย กฎหมายบางฉบับให้อำนาจแก่ศาลแพ่ง บางฉบับให้อำนาจศาลอาญา บางฉบับให้อำนาจแก่ศาลจังหวัดซึ่งมีเขตอำนาจ

ผู้เขียนเห็นว่า ในคดีที่เกี่ยวข้องกับความมั่นคงของชาติ ควรให้ศาลเพียงศาลเดียวมีอำนาจพิจารณาสั่งอนุญาต เพื่อให้การพิจารณาเป็นไปในแนวทางเดียวกัน คือ ศาลอาญา

4.2.3 การดำเนินการตรวจสอบหลังมีคำสั่ง

กฎหมายมิได้บัญญัติถึงการตรวจสอบภายหลังจากที่ศาลมีคำสั่งอนุญาต ให้เจ้าหน้าที่ของรัฐใช้มาตรการตรวจสอบและแทรกแซงการสื่อสารของบุคคล ดังนั้น ศาลจึงไม่อาจทราบได้เลยว่าเจ้าหน้าที่ของรัฐกระทำไปอยู่ภายในขอบเขตวิธีการซึ่งศาลกำหนดหรือไม่ เว้นแต่มีคู่ความโต้แย้งขึ้นมาในศาล ซึ่งกฎหมายควรมีบทบัญญัติให้อำนาจศาลในการติดตามตรวจสอบภายหลังจากอนุญาตไปแล้ว ประกอบกับให้เจ้าหน้าที่รัฐมีหน้าที่รายงานและแจ้งผลการตรวจสอบให้ศาลทราบเป็นระยะ รวมถึงวิธีการที่ใช้ไปด้วย

อีกทั้ง ศาลควรตรวจสอบว่าพยานหลักฐานที่ได้มาเป็นพยานหลักฐานที่เกี่ยวข้องกับคดี อันได้มาเพื่อประโยชน์เกี่ยวกับความมั่นคงของชาติ ในคดีที่ถูกฟ้องหรือไม่ หากการตรวจสอบและแทรกแซงการสื่อสารของเจ้าหน้าที่รัฐทำให้ได้มาซึ่งพยานหลักฐานอื่นที่ไม่เกี่ยวข้องแก่คดี ศาลต้องพิจารณาถึงความชอบด้วยพยานหลักฐานดังกล่าว

บทที่ 5

สรุป และข้อเสนอแนะ

สรุป

เมื่อมีการใช้อินเทอร์เน็ตกันอย่างแพร่หลาย จนกระทั่งมีการพัฒนาของเทคโนโลยีสารสนเทศในด้านการติดต่อสื่อสารที่เรียกว่า เครือข่ายสังคมออนไลน์ จนกระทั่งมีผู้ใช้งานเป็นจำนวนมาก และอาจกล่าวได้ว่าปัจจุบันนี้เครือข่ายสังคมออนไลน์กลายเป็นส่วนหนึ่งในชีวิตประจำวันของมนุษย์ไปแล้ว ซึ่งการติดต่อสื่อสารผ่านเครือข่ายสังคมออนไลน์ก่อให้เกิดการแลกเปลี่ยนข้อมูลข่าวสารกันได้อย่างสะดวก รวดเร็ว และรับรู้ในวงกว้างภายในระยะเวลาอันสั้น จนอาจก่อให้เกิดปรากฏการณ์ฝูงชนชั่วพริบตา ซึ่งข้อมูลข่าวสารที่กระจายออกไปอย่างกว้างขวางนี้ แม้ว่าจะเป็นข้อมูลจริงหรือเท็จก็ตามแต่ ย่อมก็ให้เกิดความตื่นตระหนกตกใจแก่ประชาชน และก่อให้เกิดความสับสนวุ่นวายในบ้านเมืองได้ จนฝ่ายปกครองเกิดแนวความคิดที่จะตรวจสอบข้อมูลการใช้อินเทอร์เน็ตของบุคคลบนโลกออนไลน์ โดยไม่จำเป็นต้องมีเหตุตามกฎหมายก่อนที่จะใช้อำนาจดังกล่าวแต่อย่างใด ซึ่งการกระทำเช่นว่านั้นถูกมองว่าเป็นการละเมิดสิทธิและเสรีภาพส่วนบุคคลที่ได้รับการรับรองและคุ้มครองตามกฎหมาย ไม่ว่าจะเป็นหลักกฎหมายระหว่างประเทศ เช่น ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน กติการะหว่างประเทศ ว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง อนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน หรือกฎหมายภายในประเทศ เช่น รัฐธรรมนูญ ประมวลกฎหมายอาญา ประมวลกฎหมายแพ่งและพาณิชย์ และพระราชบัญญัติต่าง ๆ เป็นต้น

การตรวจสอบและแทรกแซงการสื่อสารและข้อมูลหาที่กระทำโดยรัฐมีเพิ่มสูงขึ้นมาก โดยไม่มีการตรวจสอบอย่างพอเพียง โดยเฉพาะข้อมูลการใช้อุปกรณ์นั้นหากนำมาประเมินวิเคราะห์ย่อมสามารถสร้างแฟ้มประวัติชีวิตส่วนตัวของบุคคล ทั้งเรื่องประวัติทางการแพทย์ทัศนคติด้านการเมืองและศาสนา การคบหาสมาคม การมีปฏิสัมพันธ์ ความสนใจ สิ่งเหล่านี้เผยให้เห็นรายละเอียดความเป็นส่วนตัวได้มากกว่าเนื้อหาของสื่อสาร แม้ว่าโอกาสที่เอาจริงเอาจังชีวิตความเป็นส่วนตัวจะมีความเป็นไปได้สูงและส่งผลกระทบต่ออันน่ากลัว แต่ฝ่ายนิติบัญญัติและผู้มีหน้าที่วางนโยบายกลับมีมาตรการป้องกันในระดับต่ำโดยไม่ได้มีการกำหนดขอบเขตให้แก่หน่วยงานต่าง ๆ ว่าสามารถใช้เผยแพร่ ส่งต่อ และเก็บรักษาข้อมูลได้แค่ไหน เพียงใดบ้าง

ทุกครั้งที่เกิดการพัฒนาเทคนิคด้านการตรวจสอบการสื่อสารใหม่ ๆ ขึ้นหรือมีการขยายขอบเขตของเทคนิคเดิมที่มี รัฐควรคำนึงว่าข้อมูลที่รัฐต้องการตรวจสอบนั้นเป็นข้อมูลที่ได้รับ ความคุ้มครองหรือไม่ ซึ่งกฎหมายต่าง ๆ ที่เกี่ยวข้องและให้ความคุ้มครองเสรีภาพในการสื่อสารนั้น มีข้อจำกัดเสรีภาพบางประการอยู่ เพื่อจำกัดสิทธิและเสรีภาพของประชาชน และเปิดช่องให้รัฐ สามารถเข้าตรวจสอบและแทรกแซงการสื่อสารได้ โดยมีวัตถุประสงค์เพื่อความมั่นคงของรัฐ แต่ ทั้งนี้ การตรวจสอบและแทรกแซงการสื่อสาร แม้จะเป็นไปเพื่อความมั่นคงของรัฐ แต่หากให้อำนาจแก่รัฐหรือเจ้าหน้าที่รัฐมากเกินไป ย่อมเป็นการใช้อำนาจอย่างไม่มีความชอบเขต และอาจจะกระทบต่อสาระสำคัญของสิทธิและเสรีภาพในการสื่อสารของประชาชนมากเกินไป ดังนั้น จึงควรมีหน่วยงานซึ่งคอยตรวจสอบความชอบด้วยการกระทำของรัฐหรือเจ้าหน้าที่รัฐ และเป็นการถ่วงดุลอำนาจของรัฐอีกทางหนึ่งด้วย

สำหรับประเทศสหรัฐอเมริกาก็มีกฎหมายที่เกี่ยวข้องกับการตรวจสอบและแทรกแซงเสรีภาพในการสื่อสารของประชาชน คือ พระราชบัญญัติว่าด้วยการตรวจสอบข้อมูลลับของต่างชาติ ค.ศ. 1978 (Foreign Intelligence Surveillance Act of 1978 หรือ FISA) ที่ให้อำนาจแก่รัฐหรือหน่วยงานของรัฐ เพื่อรวบรวมข้อมูล สอดแนม การติดต่อสื่อสารของบุคคล เพื่อการสืบสวนที่เกี่ยวกับภัยคุกคามต่อความมั่นคงภายในที่มาจากต่างประเทศ โดยมีองค์กรตุลาการ หรือ ศาล FISA เป็นผู้มีอำนาจตรวจสอบ และอนุญาตให้เจ้าหน้าที่รัฐดำเนินการเพื่อได้มาซึ่งข้อมูลความลับของต่างชาติที่จะแสดงว่ามีความเป็นไปได้ว่ามีการกระทำผิดกำลังเกิดขึ้น ได้เกิดขึ้นแล้ว หรือกำลังจะเกิดขึ้น

ทั้งนี้ ประเทศไทยก็มีบทบัญญัติที่เกี่ยวข้องอยู่ตามพระราชบัญญัติต่าง ๆ เช่น พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม ฉบับที่ 4 พ.ศ. 2545 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และพระราชบัญญัติป้องกันและปราบปรามการค้ำมนุษย์ พ.ศ. 2551 เป็นต้น ซึ่งพระราชบัญญัติเหล่านี้ให้อำนาจในการตรวจสอบรัฐหรือเจ้าหน้าที่ของรัฐคือองค์กรที่ใช้อำนาจตุลาการ หรือศาล โดยรัฐหรือเจ้าหน้าที่ของรัฐควรเสนอเรื่องให้องค์กรตุลาการหรือศาล พิจารณาผ่านกลไกตรวจสอบตามบทบัญญัติแห่งกฎหมาย การพิจารณาว่าข้อมูลใดเป็นข้อมูลที่ได้รับ ความคุ้มครองต้องเกี่ยวพันกับปัจจัยด้านรูปแบบ ขอบเขต และระยะเวลา ของการตรวจสอบ การสื่อสารด้วย

ข้อเสนอแนะ

ผู้เขียนจึงเห็นว่า ปัจจุบันประเทศไทยยังไม่มีกฎหมายเฉพาะที่เกี่ยวกับการตรวจสอบและแทรกแซงการสื่อสารของบุคคล มีเพียงพระราชบัญญัติต่าง ๆ ซึ่งให้อำนาจเจ้าหน้าที่รัฐไว้เพื่อประโยชน์ในการรวบรวมพยานหลักฐานพิสูจน์ความผิดของผู้ถูกตรวจสอบ จึงควรมีบทบัญญัติแห่งกฎหมายโดยเฉพาะ เพื่อให้อำนาจเจ้าหน้าที่รัฐเกี่ยวกับการตรวจสอบและแทรกแซงการสื่อสารในกรณีที่มีเหตุจำเป็น เพื่อรักษาความมั่นคงของรัฐหรือความสงบเรียบร้อยของประชาชน และมีบทบัญญัติว่าด้วยการตรวจสอบและถ่วงดุลโดยศาลยุติธรรม มีรูปแบบ ดังนี้

1. ศาลที่มีอำนาจอนุญาต

การที่เจ้าหน้าที่จะดำเนินการใด ๆ เพื่อตรวจสอบและแทรกแซงการสื่อสาร จะต้องขออนุญาตต่อศาลอาญา เพื่อให้อธิบดีผู้พิพากษาศาลอาญาพิจารณา และมีคำสั่งอนุญาตหรือไม่ อนุญาตตามที่เห็นสมควร

2. ผู้ร้องขอให้ใช้มาตรการตรวจสอบการสื่อสาร

ผู้ร้องขอให้ใช้มาตรการตรวจสอบการสื่อสาร ควรเป็นเจ้าหน้าที่ของรัฐ เช่น พนักงานฝ่ายปกครอง ตำรวจ หรือเจ้าพนักงานอื่นตามกฎหมาย และจะต้องเป็นผู้มีอำนาจหน้าที่เกี่ยวข้องกับการสืบสวนหรือสอบสวนคดีที่ร้องขออนุญาตใช้มาตรการตรวจสอบการสื่อสาร เพื่อให้ได้มาซึ่งข้อมูลข่าวสาร

3. รายละเอียดแห่งคำร้องและเอกสารประกอบ

คำร้องขอ ต้องมีรายละเอียดเกี่ยวกับตัวบุคคลผู้ต้องถูกตรวจสอบ และต้องระบุเหตุที่จะขออนุญาตใช้มาตรการตรวจสอบนั้น ใส่ซองปิดผนึกประทับตรา “ลับ” เพื่อยื่นต่อศาล

4. การเสนอพยานหลักฐานในการอนุญาต

ผู้ร้องขอต้องเสนอพยานหลักฐานเพื่อแสดงให้เห็นว่า ในการที่จะแสวงหาข้อมูลที่มีเหตุอันควรเชื่อได้ว่า หากไม่ใช้มาตรการตรวจสอบและแทรกแซงเพื่อให้ได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ตามที่กฎหมายให้อำนาจแล้ว เจ้าหน้าที่จะไม่สามารถแสวงหาข้อมูล เพื่อใช้เป็นพยานหลักฐานนำตัวผู้กระทำความผิดมาลงโทษได้

5. การพิจารณาสั่งของศาล

ศาลต้องพิจารณาคำร้องจากพยานหลักฐานซึ่งเจ้าหน้าที่ผู้ร้องขอเสนอ โดยคำนึงถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใด ประกอบกับเหตุผลและความจำเป็น กล่าวคือ ต้องมีเหตุอันควรเชื่อว่ามีกระทำความผิด และจะได้ข้อมูลข่าวสารซึ่งเกี่ยวข้องกับการกระทำความผิด

นั้น อีกทั้งยังต้องไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าวิธีการนี้ได้ ซึ่งหากศาลพิจารณาแล้วเห็นว่าไม่เข้าเงื่อนไขทั้งสามประการนี้ ศาลมีอำนาจยกคำร้องดังกล่าวได้

คำสั่งของศาลในการอนุญาตหรือยกคำร้อง จะต้องระบุเหตุผลให้ครบถ้วนและชัดเจน

อนึ่ง การรับฟังพยานหลักฐานเพื่อพิจารณาอนุญาตไม่จำเป็นต้องถือเคร่งครัดเช่นเดียวกับการรับฟังพยานหลักฐานที่ใช้พิสูจน์ความผิดของจำเลย

6. ระยะเวลา

การอนุญาตให้เจ้าหน้าที่ตรวจสอบและแทรกแซงเสรีภาพในการสื่อสารนั้น ศาลจะสั่งอนุญาตได้คราวละไม่เกิน 90 วัน โดยจะกำหนดเงื่อนไขใด ๆ ก็ได้ และไม่ได้จำกัดว่าจะขออนุญาตได้กี่คราวหรือไม่เกินกี่คราว

7. การใช้และการเก็บรักษา

การเก็บรักษาและการใช้ประโยชน์บรรดาเอกสารหรือข้อมูลข่าวสารที่ได้มาจากการตรวจสอบและแทรกแซงเสรีภาพในการสื่อสารของเจ้าหน้าที่นั้น ให้เก็บรักษาและใช้ประโยชน์ในการสืบสวนและใช้เป็นพยานหลักฐานในการดำเนินคดีซึ่งขออนุญาตเท่านั้น

บรรณานุกรม

ภาษาไทย

หนังสือ

การต่างประเทศ , กระทรวง และ UN Country Team Thailand. ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน.

กรุงเทพมหานคร : กรมองค์ระหว่างประเทศ กระทรวงการต่างประเทศ, 2551.

ณัฐวสา นัทรไพฑูรย์. การค้นและยึดคอมพิวเตอร์และการได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์

ในการสอบสวนคดีอาญา. กรุงเทพมหานคร : สำนักงานอัยการสูงสุด, 2545.

ปวีณา มีปိုင်. Facebook & Twitter. กรุงเทพมหานคร: บริษัทโปรวิชั่น จำกัด, 2554.

ศรินลิน พิมพ์ประเสริฐ. สนุกเล่น เป็นเร็ว facebook & twitter. กรุงเทพมหานคร: บริษัทโปรวิชั่น

จำกัด, 2552.

แสวง บุญเฉลิมวิภาส. หลักกฎหมายอาญา. กรุงเทพมหานคร : โรงพิมพ์เดือนตุลา, 2539.

วารสารและหนังสือพิมพ์

สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. “อำนาจรัฐกับการดักฟังทางโทรศัพท์”, วารสารนิติศาสตร์. ปีที่ 26

(ฉบับที่ 3), กันยายน 2539. 657.

วิทยานิพนธ์ รายงานการวิจัย เอกสารวิจัยส่วนบุคคล

กิตติมา ประคุณดี. “การดักฟังทางโทรศัพท์โดยเจ้าพนักงาน”. นิติศาสตรมหาบัณฑิต. จุฬาลงกรณ์

มหาวิทยาลัย, 2533.

ชนชัย นักสอน. “การตรวจสอบและถ่วงดุลการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทาง

อิเล็กทรอนิกส์ ตามมาตรา 25 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547”.

นิติศาสตรมหาบัณฑิต. สาขากฎหมายอาญา. มหาวิทยาลัยธรรมศาสตร์, 2552.

บรรเจิด สิงคะเนติ , นนทวัชร นวตระกูลพิสุทธิ์ และ เรวดี ขวัญทองยิ้ม. “รายงานการศึกษาวิจัย

ฉบับสมบูรณ์ เรื่อง ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิ

ในความเป็นอยู่ส่วนตัว (Right to privacy)”. เอกสารวิจัย, สำนักงานคณะกรรมการ

สิทธิมนุษยชนแห่งชาติ.

วีรพงษ์ บิ่งไกร. “การเปิดเผยข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ

พ.ศ. 2540”. นิติศาสตรมหาบัณฑิต. จุฬาลงกรณ์มหาวิทยาลัย, 2543.

กฎหมาย

ประกาศคณะปฏิรูปการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข
ฉบับที่ 21 เรื่อง ห้ามการดักฟังทาง โทรศัพท์หรือเครื่องมือสื่อสารใด

ประมวลกฎหมายแพ่งและพาณิชย์

ประมวลกฎหมายวิธีพิจารณาความอาญา

ประมวลกฎหมายอาญา

พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547

พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542

พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519

พระราชบัญญัติไประณีย์ พ.ศ. 2477

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติองค์การโทรศัพท์แห่งประเทศไทย พ.ศ. 2497

ระเบียบคณะกรรมการป้องกันและปราบปรามยาเสพติดว่าด้วยการได้มา การใช้ประโยชน์และการ
เก็บรักษาข้อมูลข่าวสาร พ.ศ. 2545

Foreign Intelligence Surveillance Act

เอกสารไม่ตีพิมพ์

ไพโรจน์ วายุกาพ. “กฎหมายคุ้มครองข้อมูลส่วนบุคคล”. เอกสารประกอบการบรรยาย.

ฐานข้อมูลอิเล็กทรอนิกส์

เกรียงไกร เจริญธนาวัฒน์. “สิทธิของผู้เล่นเกมออนไลน์”. (ออนไลน์). <http://www.pub-law.net/publaw/view.aspx?ID=609>. 2547

เฉลิมชัย กักเกียรติกุล. “การคุ้มครองข้อมูลส่วนบุคคลในกิจการโทรคมนาคมของสหภาพยุโรป”.
(ออนไลน์). เข้าถึงได้จาก : <http://chalermchai-nbtc.blogspot.com/2013/06/privacy-jewish-law-classical-greece.html>.

อุบลรัตน์ ศิริยุวศักดิ์. “สิทธิในการสื่อสารของประชาชนกับสิทธิมนุษยชน : มาตรการต่อสู้ใน
เวทีสากล”. (ออนไลน์). [http://www.freedom.commarts.chula.ac.th/articles/CRSU04.
pdf](http://www.freedom.commarts.chula.ac.th/articles/CRSU04.pdf),.2544.

Federal Judicial Center. “History of the Federal Judiciary”. (ออนไลน์).

http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html.

<http://www.mindphp.com/คู่มือ/73-คืออะไร/2163-ads1-คืออะไร.html>

<http://th.wikipedia.org/wiki/วายฟาย>

<http://lovelovelover77.wordpress.com/ประวัติของ-3g/>

<http://www.trachoo.com/ประวัติwhatsapp>

<https://www.thaicert.or.th/สพธอ>

<https://www.thaicert.or.th/สพธอ/line>

ประวัติย่อผู้วิจัย

ชื่อ	นายพงษ์เดช วานิชกิตติกูล
วัน เดือน ปี เกิด	15 ตุลาคม 2507
การศึกษา	<ul style="list-style-type: none"> - นิติศาสตร์บัณฑิต มหาวิทยาลัยธรรมศาสตร์ - เนติบัณฑิตไทย - LL.M. The American University
ประวัติการทำงาน	<ul style="list-style-type: none"> - นิติกร บริษัทตรีเพชรอีซูซุเซลส์ จำกัด - นิติกร กองรายได้ สำนักงานการคลัง ศาลาว่าการกรุงเทพมหานคร - ผู้ช่วยผู้พิพากษา - ผู้พิพากษาศาลจังหวัดชัยนาท - ผู้ช่วยผู้พิพากษาศาลอุทธรณ์ - ผู้พิพากษาประจำกระทรวงช่วยทำงานในตำแหน่งรองเลขาธิการส่งเสริมงานตุลาการ - ผู้พิพากษาหัวหน้าศาลช่วยทำงานในตำแหน่งผู้ช่วยผู้พิพากษาศาลฎีกา - ผู้พิพากษาหัวหน้าศาลประจำสำนักงานเลขานุการคณะกรรมการวินิจฉัยชี้ขาดอำนาจหน้าที่ระหว่าง - ผู้พิพากษาหัวหน้าศาลประจำสำนักประธานศาลฎีกา - เลขานุการศาลอุทธรณ์ภาค 8 - เลขานุการศาลอุทธรณ์ - ผู้พิพากษาหัวหน้าศาลประจำสำนักประธานศาลฎีกา - ผู้พิพากษาศาลอุทธรณ์ประจำสำนักประธานศาลฎีกา - รองเลขานุการศาลฎีกา
ตำแหน่งปัจจุบัน	เลขาธิการประธานศาลฎีกา

สรุปย่อ

ลักษณะวิชาการ การเมือง

เรื่อง ศาลยุติธรรมกับการรักษาคุณภาพระหว่างเสรีภาพในการสื่อสาร
กับการรักษาความมั่นคงบนสังคมออนไลน์

ผู้วิจัย นายพงษ์เดช วานิชกิตติกูล หลักสูตร วปอ. รุ่นที่ 56

ตำแหน่ง เลขานุการประธานศาลฎีกา

ความเป็นมาและความสำคัญของปัญหา

อินเทอร์เน็ตเป็นระบบเครือข่ายของการเชื่อมโยงคอมพิวเตอร์ ที่มีผู้ใช้งานจำนวนมาก จากทั่วทุกมุม โลก เป็นช่องทางหนึ่งที่สำคัญในปัจจุบันที่คนใช้ในการติดต่อสื่อสารระหว่างกัน ด้วยความสะดวกและรวดเร็วในการใช้งาน ประกอบกับไม่มีข้อจำกัดด้านพื้นที่ อินเทอร์เน็ต จึงเติบโตขึ้นอย่างรวดเร็วในทุกประเทศทั่วโลก

ประเทศไทยเริ่มมีการใช้อินเทอร์เน็ตตั้งแต่ปี 2530 โดยเริ่มต้นจากการใช้งานของ สถาบันการศึกษา และขยายตัวออกไปสู่ภาคธุรกิจในปี 2537 ความต้องการมีมากขึ้น จึงมีการ ให้บริการเชิงพาณิชย์ขึ้นในรูปแบบของผู้ให้บริการอินเทอร์เน็ตที่มีการเรียกเก็บค่าใช้บริการที่ เรียกว่า Internet Service Provider (ISP) จนกระทั่งการใช้งานอินเทอร์เน็ตของคนไทย เริ่มเข้ามาสู่ การใช้งานเพื่อติดต่อสื่อสารกันมากขึ้นในปัจจุบัน ทั้งนี้เป็นผลมาจากการพัฒนาในสิ่งต่อไปนี้

1. การพัฒนาอย่างรวดเร็วของเทคโนโลยีสารสนเทศ เป็นการส่งเสริมและกระตุ้น ให้การใช้อินเทอร์เน็ตเพื่อติดต่อสื่อสารระหว่างกัน เพิ่มมากขึ้นอย่างรวดเร็วในคนทุกเพศทุกวัย
2. การพัฒนาโทรศัพท์เคลื่อนที่ ให้สามารถตอบสนองความต้องการของคนในการ ติดต่อสื่อสารระหว่างกัน โดยสามารถส่งข้อความร่วมกับรูปภาพและเสียง
3. การคิดค้นและพัฒนาแอปพลิเคชันต่าง ๆ เพื่อนำมาใช้งานร่วมกับคอมพิวเตอร์ และโทรศัพท์เคลื่อนที่

จนในปัจจุบันกล่าวได้ว่า คนไทยมีการใช้อินเทอร์เน็ตเพื่อติดต่อสื่อสารกันมาก ที่สุดประเทศหนึ่งในโลก โดยมีการประยุกต์คอมพิวเตอร์และเทคโนโลยีสารสนเทศสมัยใหม่มาใช้ เพื่อติดต่อสื่อสารกันในรูปแบบต่าง ๆ เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) การสนทนาและแสดง ความคิดเห็นในหน้าเว็บบอร์ด (Webboard) และการติดตามข่าวสาร เป็นต้น

รูปแบบของการติดต่อสื่อสารกันบนโลกออนไลน์ได้มีการเปลี่ยนแปลงครั้งใหญ่ อีกครั้งหนึ่ง เมื่อเกิดการคิดค้นรูปแบบของการติดต่อสื่อสารกันบนอินเทอร์เน็ต เมื่อมีการสร้างนวัตกรรมที่ให้คุณคนสามารถสร้างเครือข่ายเพื่อติดต่อสื่อสารระหว่างบุคคลและระหว่างกลุ่ม เรียกว่า เครือข่ายสังคมออนไลน์ (Social Network หรือ Social Media) เช่น Twitter Facebook Whatsapp หรือ Line เป็นต้น

เครือข่ายสังคมออนไลน์ เป็นเว็บพื้นฐานในการบริการให้แต่ละบุคคลสามารถสร้างเครือข่ายของตนเองอย่างเป็นระบบ สามารถสร้างบัญชีรายชื่อของกลุ่มผู้ติดต่อที่สามารถติดต่อสื่อสาร และแลกเปลี่ยนความเห็นหรือสิ่งที่สนใจเหมือน ๆ กันได้ ซึ่งมีลักษณะ 3 ประการ ดังนี้

1. เป็นพื้นที่ที่มีการสื่อสาร 2 ทาง โดยไม่มีข้อจำกัดเรื่องเวลาและสถานที่ ขอให้ให้มีเครื่องมือและอุปกรณ์ที่จะสามารถเข้าสู่อินเทอร์เน็ตได้เท่านั้น
2. เป็นพื้นที่ที่ไม่อาจมีการควบคุมหรือปิดกั้นได้อย่างสมบูรณ์
3. เป็นพื้นที่ของคนชั้นกลาง เพราะราคาโดยเฉลี่ยของอุปกรณ์หรือเครื่องมือที่จะติดต่อสื่อสารกันบนอินเทอร์เน็ตประมาณ 30,000 บาท

การใช้วิธีการสื่อสารออนไลน์ก่อให้เกิดการแลกเปลี่ยนข้อมูลข่าวสารกันได้อย่างสะดวกรวดเร็ว และรับรู้ในวงกว้างภายในระยะเวลาอันสั้น ซึ่งบ่อยครั้งที่ก่อให้เกิดปรากฏการณ์ของการรวมตัวกันของกลุ่มที่มีความคิดเห็นเหมือนหรือคล้ายคลึงกัน ก่อให้เกิดปรากฏการณ์ที่เรียกว่า ผุ่ชนชั่วพริบตา (Flash mob) หรือในบางกรณีอาจเกิดการแพร่กระจายของข้อมูลข่าวสารที่เป็นเท็จหรือขัดต่อความเป็นจริง ก่อให้เกิดความตระหนกตกใจแก่ประชาชน ก่อให้เกิดความสับสนวุ่นวายในบ้านเมืองได้

การเกิดผุ่ชนชั่วพริบตาอาจเป็นไปได้ในด้านบวกหรือลบต่อสังคมโดยรวมก็ได้ หรือการเกิดข่าวลือทางการเมืองที่สร้างความสับสนวุ่นวายในประเทศอย่างมาก จนฝ่ายปกครองเกิดแนวคิดที่จะตรวจสอบข้อมูลการใช้อินเทอร์เน็ตของบุคคลบนโลกออนไลน์ในลักษณะของการสุ่ม โดยที่ไม่จำเป็นต้องมีเหตุตามกฎหมายก่อนที่จะใช้อำนาจในการป้องกันและคุ้มครองความสงบเรียบร้อยหรือความมั่นคงของประเทศก่อนแต่อย่างใด ซึ่งการกระทำดังกล่าวถูกมองว่าเป็นการละเมิดสิทธิเสรีภาพส่วนบุคคลที่ได้รับการคุ้มครองตามกฎหมาย

ในกรณีดังกล่าว เคยเกิดกรณีที่นาย เอ็ดเวิร์ด สโนว์เดน (Edward Snowden) ได้เปิดเผยข้อมูลว่า ทางการของสหรัฐอเมริกาได้ใช้อำนาจตามกฎหมายให้ผู้ใช้บริการอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์เปิดเผยข้อมูลการใช้อินเทอร์เน็ตในการติดต่อสื่อสารกัน จนเกิดการวิพากษ์วิจารณ์การกระทำดังกล่าวของทางการสหรัฐอเมริกา และเกิดคำถามถึงความเหมาะสมและขอบเขตของการใช้อำนาจ

วัตถุประสงค์ของการวิจัย

งานวิจัยฉบับนี้จึงต้องการ

1. ศึกษาแนวคิด ของการคุ้มครองเสรีภาพในการสื่อสารระหว่างกันของบุคคลตาม
กฎหมาย
2. ศึกษาแนวคิด ในการแทรกแซงเสรีภาพในการสื่อสารของบุคคลเพื่อรักษาความ
มั่นคงของรัฐ
3. ศึกษาบทบาทของศาลยุติธรรม ในการรักษาดุลยภาพระหว่างเสรีภาพส่วน
บุคคล และการรักษาความมั่นคงของประเทศ

ขอบเขตของการวิจัย

ศึกษากรณีของการใช้สังคมออนไลน์ในประเทศไทย เปรียบเทียบกับแนวคิด
และวิธีปฏิบัติของประเทศสหรัฐอเมริกา

วิธีดำเนินการวิจัย

ศึกษาวิจัยในเชิงคุณภาพ (Qualitative Research) โดยการศึกษานำแนวคิด ทฤษฎี ข้อเท็จจริง
และกฎหมายต่าง ๆ ค้นคว้าและรวบรวมข้อมูลจากเอกสาร บทความ หนังสือ รายงานวิจัยวิทยานิพนธ์
ข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้อง ทั้งภาษาไทยและภาษาต่างประเทศ เพื่อนำข้อมูลที่ได้มาวิเคราะห์
ประเด็นปัญหาและเสนอแนวทางการแก้ไขอย่างเหมาะสม ซึ่งจะทำให้ศาลยุติธรรมเป็นตัวกลางใน
การรักษาดุลยภาพระหว่างเสรีภาพในการสื่อสารกับการรักษาความมั่นคงบนสังคมออนไลน์

ประโยชน์ที่ได้รับจากการวิจัย

1. ได้ทราบแนวคิดของการคุ้มครองเสรีภาพในการสื่อสาร
2. ได้ทราบเงื่อนไขและพฤติการณ์ที่เหมาะสมในกรณีที่รัฐจะแทรกแซงเสรีภาพ
ในการสื่อสารของบุคคล
3. ได้ทราบบทบาทของศาลยุติธรรมในการรักษาดุลยภาพระหว่างเสรีภาพในการ
สื่อสารและการรักษาความมั่นคงของประเทศ