องค์การสหประชาชาติ A/HRC/23/40

สมัชชาใหญ่แห่งสหประชาชาติ

การแจกจ่าย: ทั่วไป

17 เมษายน 2556

ภาษาเดิม: อังกฤษ

(Unofficial Thai Translation)

คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ

สมัยประชุมที่ 23

วาระที่ 3

การส่งเสริมและคุ้มครองสิทธิมนุษยชน สิทธิพลเมือง

การเมือง เศรษฐกิจ สังคมและวัฒนธรรม

รวมทั้งสิทธิด้านการพัฒนา

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*

รายงานของผู้รายงานพิเศษว่าด้วยการส่งเสริมและคุ้มครองสิทธิและเสรีภาพด้านความเห็นและการแสดงออก แฟรงค์ ลารัว+

สรุป

รายงานฉบับนี้ส่งมอบให้ตามมติของคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติที่ 16/4 เป็นการวิเคราะห์ผลกระทบของการสอดแนมการสื่อสารโดยรัฐต่อการใช้สิทธิมนุษยชนเพื่อเข้าถึงความเป็นส่วนตัวและเสรีภาพด้านความเห็นและการแสดงออก เมื่อคำนึงถึงผลกระทบจากความก้าวหน้าด้านเทคโนโลยีที่สำคัญด้านการสื่อสาร รายงานเน้นย้ำถึงความจำเป็นเร่งด่วนที่จะต้องศึกษาวิธีการใหม่ ๆ ในการสอดแนมข้อมูล และการแก้ไขเพิ่มเติมกฎหมายในประเทศที่ควบคุมการปฏิบัติดังกล่าวให้สอดคล้องกับมาตรฐานสิทธิมนุษยชน

* การส่งมอบล่าช้า

+ ฉบับภาษาไทยอย่างไม่เป็นทางการโดยเครือข่ายพลเมืองเน็ต แปลโดย พิภพ อุดมอิทธิพงศ์ เผยแพร่ครั้งแรก 19 พ.ย. 2556 (ปรับปรุงคำแปล 23 พ.ย. 2556)
https://thainetizen.org/docs/a-hrc-23-40-surveillance-of-communications/
ดาวน์โหลดต้นฉบับภาษาอังกฤษได้ที่ http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

สารบัญ

I. อารัมภบท

1. รายงานฉบับนี้เป็นการวิเคราะห์ผลกระทบของการสอดแนมการสื่อสารโดยรัฐต่อการใช้สิทธิมนุษยชนเพื่อเข้าถึงความเป็นส่วนตัวและเสรีภาพด้านความเห็นและการแสดงออก เมื่อคำนึงถึงผลกระทบจากความก้าวหน้าด้านเทคโนโลยีที่สำคัญด้านการสื่อสาร รายงานเน้นย้ำถึงความจำเป็นเร่งด่วนที่จะต้องศึกษาวิธีการใหม่ ๆ ในการสอดแนมข้อมูล และการแก้ไขเพิ่มเติมกฎหมายในประเทศที่ควบคุมการปฏิบัติดังกล่าวให้สอดคล้องกับมาตรฐานสิทธิมนุษยชน

2. นวัตกรรมด้านเทคโนโลยีได้เพิ่มโอกาสด้านการสื่อสาร และการคุ้มครองการแสดงออกอย่างเสรีและการแสดงความเห็น ทำให้สามารถปกปิดตัวตน มีการแลกเปลี่ยนข้อมูลอย่างรวดเร็ว และมีการสานเสวนาข้ามวัฒนธรรม ในขณะเดียวกัน การเปลี่ยนแปลงด้านเทคโนโลยีเพิ่มโอกาสที่รัฐจะสอดแนมและแทรกแซงการสื่อสารอย่างเป็นส่วนตัวของบุคคลเช่นกัน

3. ข้อกังวลเกี่ยวกับความมั่นคงของชาติและการก่ออาชญากรรม อาจเป็นเหตุผลสนับสนุนข้อยกเว้นให้สามารถใช้เทคโนโลยีการสอดแนมการสื่อสารได้ในบางกรณี อย่างไรก็ดี ยังมีข้อบกพร่องด้านกฎหมายระดับประเทศที่ควบคุมบทบาทที่จำเป็น ชอบด้วยกฎหมายและมีสัดส่วนเหมาะสมของรัฐในการสอดแนมการสื่อสาร หรือไม่มีกฎหมายเช่นนั้นอยู่เลย กรอบกฎหมายในประเทศที่บกพร่องเป็นผลให้มีการละเมิดสิทธิการสื่อสารอย่างเป็นส่วนตัวโดยพลการและไม่ชอบด้วยกฎหมาย และยังคุกคามต่อการคุ้มครองสิทธิที่จะมีเสรีภาพด้านความเห็นและการแสดงออก

4. ในรายงานฉบับก่อนหน้า (A/HRC/17/27 และ A/66/290) ผู้รายงานพิเศษได้วิเคราะห์ผลกระทบด้านอินเทอร์เน็ตซึ่งไม่เคยเป็นมาก่อน โดยเป็นการเพิ่มโอกาสที่บุคคลจะใช้สิทธิที่จะมีเสรีภาพด้านความเห็นและการแสดงออก เขาได้แสดงข้อกังวลเกี่ยวกับมาตรการในหลายระดับของรัฐที่ใช้เพื่อป้องกันและควบคุมกระแสข้อมูลทางอินเทอร์เน็ต และเน้นย้ำถึงข้อบกพร่องในการคุ้มครองสิทธิความเป็นส่วนตัวทางอินเทอร์เน็ต

5. จากการวิเคราะห์ดังกล่าว เป็นเหตุให้รายงานฉบับนี้มีเป้าหมายเพื่อจำแนกความเสี่ยงที่มีต่อสิทธิมนุษยชน โดยเป็นผลมาจากวิธีการและรูปแบบการสอดแนมการสื่อสารสมัยใหม่ รวมทั้งผลกระทบต่อสิทธิความเป็นส่วนตัวและ เสรีภาพด้านความเห็นและการแสดงออก

6. คำศัพท์ต่อไปนี้ได้ถูกนำมาใช้ในรายงานฉบับนี้เพื่ออธิบายถึงรูปแบบทั่วไปของการสอดแนมการสื่อสาร:

(a) การสอดแนมการสื่อสาร: การติดตาม ดักรับ เก็บข้อมูล รักษาข้อมูล และกักข้อมูลที่มีการสื่อสาร ส่งต่อ หรือสร้างขึ้นมาในโครงข่ายการสื่อสาร

(b) ข้อมูลการสื่อสาร: ข้อมูลเกี่ยวกับการสื่อสารของบุคคล (อีเมล โทรศัพท์ และการส่งและรับข้อความสั้น ข้อความและสิ่งที่เขียนทางสื่อสังคมออนไลน์) เกี่ยวกับอัตลักษณ์ของบุคคล ข้อมูลด้านเครือข่าย ที่อยู่ เว็บไซต์ที่เข้าเยี่ยมชม หนังสือและเอกสารอื่น ๆ ที่อ่าน รับชมหรือรับฟัง ข้อมูลเกี่ยวกับการสืบค้น ข้อมูลที่นำไปใช้ประโยชน์ การปฏิสัมพันธ์ (จุดเริ่มต้นและจุดสิ้นสุดของการสื่อสาร คนที่มีปฏิสัมพันธ์ด้วย เพื่อน ครอบครัว คนที่คุ้นเคย) และช่วงเวลาและตำแหน่งของบุคคล รวมทั้งจุดที่อยู่ใกล้เคียงกับบุคคลอื่น)

(c) การกรองเนื้อหาอินเทอร์เน็ต: การติดตามเนื้อหาในอินเทอร์เน็ตในระบบอัตโนมัติหรือระบบที่ทำขึ้นเป็นการเฉพาะ (รวมทั้งเนื้อหาในเว็บไซต์ เว็บบล็อก และแหล่งข้อมูลของสื่อออนไลน์ รวมทั้งอีเมล) ทั้งนี้เพื่อจำกัดหรือห้ามการส่งต่อข้อความ ภาพ เว็บไซต์ เครือข่าย โปรโตคอล บริการหรือกิจกรรมอื่นใด

II. กิจกรรมของผู้รายงานพิเศษ

7. ในระหว่างการรายงาน ผู้รายงานพิเศษได้เข้าร่วมกิจกรรมระหว่างประเทศและในประเทศหลายครั้งที่เกี่ยวข้องกับประเด็นที่ทำการศึกษาในรายงานที่ผ่านมา รวมทั้งเสรีภาพในการแสดงออกทางอินเทอร์เน็ต การป้องกันถ้อยคำที่สร้างความเกลียดชัง (hate speech) และการคุ้มครองผู้สื่อข่าว เขาให้ความสนใจเป็นพิเศษต่อกิจกรรมระดับชาติเพื่อส่งเสริมการคุ้มครองผู้สื่อข่าว ด้วยเหตุดังกล่าว เขาจึงเข้าร่วมประชุมเพื่อจัดทำมาตรการเหล่านั้น ทั้งในบราซิล โคลอมเบีย ฮอนดูรัส และเม็กซิโก เขายังได้เข้าร่วมในการประชุมระหว่างหน่วยงานแห่งสหประชาชาติว่าด้วยความปลอดภัยของผู้สื่อข่าวและปัญหาการลอยนวลพ้นผิด (“United Nations Inter-Agency Meeting on the Safety of Journalists and the Issues of Impunity”) ซึ่งจัดขึ้นเมื่อเดือนพฤศจิกายน 2555 ที่กรุงเวียนนา

8. รายงานฉบับสุดท้ายที่เขานำเสนอต่อสมัชชาใหญ่แห่งสหประชาชาติ เน้นการป้องกันถ้อยคำที่แสดงความเกลียดชังและการยุยงให้เกิดความเกลียดชัง[1] และมีการพูดถึงประเด็นดังกล่าวอีกในการประชุมนอกรอบของสมัชชาใหญ่แห่งสหประชาชาติ ซึ่งเป็นกิจกรรมที่จัดร่วมกันระหว่างผู้รายงานพิเศษกับที่ปรึกษาพิเศษด้านการป้องกันการสังหารล้างเผ่าพันธุ์มนุษย์ (Special Adviser on the Prevention of Genocide) ในเดือนกุมภาพันธ์ 2556 ในเดือนเดียวกัน เขายังได้กล่าวถึงประเด็นนี้อีกในการเปิดตัวแผนปฏิบัติการราบัตว่าด้วยการห้ามการส่งเสริมความเกลียดชังเกี่ยวกับชาติ เชื้อชาติ หรือศาสนาที่ถือว่าเป็นการยุยงให้เกิดการเลือกปฏิบัติ ความเกลียดชัง หรือความรุนแรง (“Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence”) ที่กรุงเจนีวา และในการประชุมเวทีระดับโลกของพันธมิตรด้านอารยธรรมแห่งสหประชาชาติครั้งที่ 5 (the Fifth United Nations Alliance of Civilizations Global Forum) ที่กรุงเวียนนา

9. ผู้รายงานพิเศษได้เดินทางไปยังประเทศฮอนดูรัสระหว่างวันที่ 7-14 สิงหาคม 2555 ข้อมูลการค้นพบและข้อเสนอแนะจากการเดินทางครั้งนั้นมีอยู่ในภาคผนวกของรายงานฉบับนี้ (A/HRC/20/40/Add.1) เขาได้รับเชิญจากรัฐบาลอินโดนีเซียให้ไปเยือนประเทศในเดือนมกราคม 2556 แต่เป็นที่น่าเสียดายว่า ทางรัฐบาลอินโดนีเซียแจ้งให้เลื่อนการเดินทาง และที่ผ่านมายังไม่มีการกำหนดช่วงเวลาใหม่ของการมาเยือนประเทศ

10. ในการจัดเตรียมรายงานฉบับนี้ ผู้รายงานพิเศษได้แก้ไขการศึกษาที่เกี่ยวข้องและปรึกษาหารือกับผู้เชี่ยวชาญในประเด็นการสอดแนมการสื่อสาร ในเดือนธันวาคม 2555 เขาได้เข้าร่วมการสัมมนาเชิงปฏิบัติการว่าด้วยการสอดแนมด้านอิเล็กทรอนิกส์และสิทธิมนุษยชน (Workshop on Electronic Surveillance and Human Rights) ซึ่งจัดขึ้นโดยมูลนิธิ Electronic Frontier Foundation ในเดือนกุมภาพันธ์ 2556 เขาได้จัดการประชุมปรึกษาหารือผู้เชี่ยวชาญเพื่อจัดเตรียมรายงานฉบับนี้ โดยมีขึ้นคู่ขนานไปกับกิจกรรมระหว่างการประชุมสุดยอดระดับโลกว่าด้วยสังคมสารสนเทศ (“World Summit on the Information Society+10 Meeting”) ที่มีขึ้นที่สำนักงานองค์การเพื่อการศึกษา วิทยาศาสตร์และวัฒนธรรมแห่งสหประชาชาติ (UN Educational, Scientific and Cultural Organization – UNESCO) กรุงปารีส และยังได้เข้าร่วมอภิปรายในเวทีเปิดการประชุมด้วย

III. การพัฒนาเทคโนโลยีการสอดแนม

11. นวัตกรรมด้านเทคโนโลยีได้เพิ่มโอกาสด้านการสื่อสาร และการคุ้มครองการแสดงออกอย่างเสรีและการแสดงความเห็น ทำให้สามารถปกปิดตัวตน มีการแลกเปลี่ยนข้อมูลอย่างรวดเร็ว และมีการสานเสวนาข้ามวัฒนธรรม ในขณะเดียวกัน การเปลี่ยนแปลงด้านเทคโนโลยีเพิ่มโอกาสที่รัฐจะสอดแนมและแทรกแซงการสื่อสารอย่างเป็นส่วนตัวของบุคคลเช่นกัน

12. นับแต่เริ่มมีการพัฒนารูปแบบการสื่อสารทางไกลเป็นครั้งแรก รัฐได้พยายามดักรับและติดตามการสื่อสารส่วนบุคคล เพื่อผลในการบังคับใช้กฎหมายและประโยชน์เกี่ยวกับความมั่นคงของชาติ การสื่อสารเหล่านี้เป็นผลทำให้มีการเปิดเผยข้อมูลส่วนตัวและเกี่ยวข้องกับ

[1] A/67/357

บุคคลเป็นการเฉพาะ รวมทั้งการกระทำในอดีตหรืออนาคตของบุคคลหรือของกลุ่มก็ตาม การสื่อสารเป็นแหล่งข้อมูลที่มีคุณค่า ช่วยให้รัฐป้องกันหรือฟ้องร้องดำเนินคดีกรณีที่เกิดอาชญากรรมร้ายแรง หรือใช้เพื่อป้องกันไม่ให้เกิดภัยฉุกเฉินต่อความมั่นคงของชาติได้

13. นวัตกรรมด้านเทคโนโลยีในช่วงศตวรรษที่ 20 ได้เปลี่ยนแปลงแบบแผนและส่งผลกระทบต่อการสอดแนมการสื่อสาร ประชาชนสามารถสื่อสารผ่านช่องทางต่าง ๆ ได้มากขึ้น และบ่อยครั้งขึ้น การเปลี่ยนแปลงจากระบบโทรศัพท์พื้นฐานไปสู่การสื่อสารแบบเคลื่อนที่และการลดลงของค่าใช้จ่ายด้านบริการการสื่อสาร ส่งผลให้มีการเติบโตของการใช้โทรศัพท์เป็นอย่างมาก การเกิดขึ้นของอินเทอร์เน็ตทำให้เกิดเครื่องมือใหม่ ๆ และมีการนำไปใช้เพื่อการสื่อสารโดยไม่มีค่าใช้จ่าย หรือมีค่าใช้จ่ายในระดับที่เหมาะสม ความก้าวหน้าเหล่านี้ทำให้ความเชื่อมโยงกันมีเพิ่มมากขึ้น สนับสนุนการแลกเปลี่ยนด้านข้อมูลและแนวคิดทั่วโลก และเพิ่มโอกาสสำหรับการเติบโตทางเศรษฐกิจและการเปลี่ยนแปลงทางสังคม

14. ในขณะที่เทคโนโลยีการสื่อสารพัฒนาไป วิธีการที่รัฐใช้เพื่อสอดส่องการสื่อสารส่วนบุคคลก็พัฒนาไปเช่นกัน การใช้โทรศัพท์มากขึ้นส่งผลให้มีการดักฟังมากขึ้น โดยมีการต่อสายจากโทรศัพท์เพื่อดักฟังข้อมูลการสนทนาเป็นการส่วนตัว จากการทดแทนเครือข่ายโทรศัพท์แบบอนาล็อกด้วยระบบไฟเบอร์ออพติกและดิจิทัลในช่วงปลายทศวรรษ 1990 เป็นเหตุให้รัฐออกแบบเครือข่ายเทคโนโลยีใหม่ โดยมีการติดตั้งระบบเพื่อดักรับข้อมูล (“backdoors”) ทำให้รัฐสามารถสอดแนมข้อมูล เป็นเหตุให้ระบบเครือข่ายโทรศัพท์สมัยใหม่เข้าถึงได้และถูกควบคุม

15. เทคโนโลยีที่มีพลวัตสูงเช่นนี้ไม่เพียงเปลี่ยนแบบแผนการสอดแนม แต่ยังเปลี่ยน “ข้อมูล” ที่ถูกสอดแนมด้วย ระบบอินเทอร์เน็ตทำให้เกิดโอกาสที่หลากหลายในการสื่อสารและแลกเปลี่ยนข้อมูล ทั้งยังสนับสนุนให้บุคคลสามารถผลิตข้อมูลด้านธุรกรรมจำนวนมาก เราเรียกข้อมูลเหล่านี้ว่าข้อมูลการสื่อสารหรือเมทาดาทา (metadata; ข้อมูลอธิบายข้อมูล) ซึ่งครอบคลุมข้อมูลส่วนบุคคล ตำแหน่งที่ตั้ง และการใช้บริการอินเทอร์เน็ต มีระบบบันทึกข้อมูลที่เกี่ยวข้องรวมทั้งอีเมลและข้อความที่ส่งหรือรับ ข้อมูลการสื่อสารเป็นข้อมูลที่จัดเก็บได้ เข้าถึงได้ และสืบค้นได้ และการเปิดเผยและใช้ประโยชน์ของข้อมูลเหล่านี้โดยรัฐ มักเป็นไปโดยขาดการควบคุมกำกับ การวิเคราะห์ข้อมูลเหล่านี้มีลักษณะเผยให้เห็นข้อมูลที่เป็นส่วนตัวอย่างมากและเป็นการรุกล้ำความเป็นส่วนตัว โดยเฉพาะกรณีที่นำข้อมูลมารวมกันและสะสมไว้ด้วยกัน เป็นเหตุให้รัฐพึ่งพาข้อมูลเหล่านี้มากขึ้นในการสนับสนุนการบังคับใช้กฎหมายหรือการสืบสวนเกี่ยวกับความมั่นคงของชาติ รัฐยังบังคับให้มีการเก็บรักษาและกักข้อมูลการสื่อสารเอาไว้ เพื่อช่วยให้สอดแนมย้อนหลังได้

16. การเปลี่ยนแปลงด้านเทคโนโลยีเกิดขึ้นควบคู่ไปกับการเปลี่ยนแปลงด้านทัศนคติต่อการสอดแนมการสื่อสาร ตอนที่เริ่มมีการดักฟังโทรศัพท์อย่างเป็นทางการในสหรัฐฯ การดักฟังจะเกิดขึ้นเฉพาะกรณีที่จำกัด และศาลมักไม่อนุญาตให้ทำเช่นนั้น[2] โดยถือว่าเป็นภัยคุกคามร้ายแรงต่อสิทธิความเป็นส่วนตัว มีการจำกัดการใช้เฉพาะการสอบสวนและฟ้องร้องคดีที่ร้ายแรงสุดเท่านั้น แต่เมื่อเวลาผ่านไปรัฐได้ขยายอำนาจในการปฏิบัติการสอดแนม ทำให้ข้อยกเว้นมีน้อยลง และเพิ่มเหตุผลที่ชอบธรรมสำหรับการสอดแนมเช่นนั้น

17. ในหลายประเทศ ที่ผ่านมาไม่มีการทบทวนและปรับปรุงกฎหมายและการปฏิบัติเพื่อให้สามารถรับมือกับภัยคุกคามและความท้าทายจากการสอดแนมการสื่อสารในโลกยุคดิจิทัลได้ มีการประยุกต์แนวคิดการเข้าถึงจดหมายโต้ตอบแบบทั่วไปให้เป็นส่วนหนึ่งของกฎหมาย เพื่ออนุญาตให้สามารถเข้าถึงข้อมูลในคอมพิวเตอร์ส่วนบุคคลและข้อมูลและเทคโนโลยีการสื่อสารอื่น ๆ โดยไม่คำนึงว่าการใช้เครื่องมือและการนำหลักกฎหมายไปใช้มากขึ้นเช่นนี้จะส่งผลกระทบต่อสิทธิของบุคคลอย่างไร ในเวลาเดียวกัน เนื่องจากไม่มีกฎหมายเพื่อกำกับดูแลการสอดแนมการสื่อสารระดับโลกและโครงสร้างการแลกเปลี่ยนข้อมูล เป็นเหตุให้เกิดการสอดแนมเฉพาะกิจที่อยู่นอกเหนือการกำกับดูแลของหน่วยงานอิสระ ในปัจจุบัน ในหลายรัฐ การเข้าถึงข้อมูลการสื่อสารอยู่ภายใต้อำนาจของหน่วยงานสาธารณะมากมาย และ

[2] ในการไต่สวนความชอบด้วยกฎหมายกรณีการดักฟัง ผู้พิพากษา Brandeis ศาลสูงสุดแห่งสหรัฐอเมริกาได้เขียนคำสั่งแสดงความไม่เห็นด้วยและประณาม โดยมีข้อสังเกตว่าการดักฟังเป็น “วิธีการล่วงล้ำความเป็นส่วนตัวที่ลึกซึ้งและกว้างขวาง” ซึ่งไม่ชอบด้วยเหตุผลใด ๆ ตามรัฐธรรมนูญ รวมทั้งมีการทำนายไว้อย่างแม่นยำ โดยผู้พิพากษาผู้ทรงเกียรติได้ทำนายไว้ว่า “สักวันหนึ่งรัฐบาลจะสามารถพัฒนาวิธีการทำสำเนาเอกสารมาแสดงต่อศาล โดยไม่ต้องนำเอกสารนั้นออกมาจากตู้เก็บ ทำให้รัฐสามารถนำข้อมูลที่เป็นเรื่องส่วนตัวในครัวเรือนมาเปิดเผยต่อคณะลูกขุนได้ ความก้าวหน้าเรื่องการหยั่งรู้และศาสตร์ที่เกี่ยวข้องอาจทำให้เกิดวิธีการค้นหาความเชื่อ ความคิดและอารมณ์ความรู้สึกที่ยังไม่มีการแสดงออกได้” คดี Olmstead v. United States, 277 U.S. 438 (1928)

ตอบสนองจุดประสงค์ที่หลากหลาย โดยมักไม่จำเป็นต้องขออำนาจศาลและไม่มีการกำกับดูแลอย่างเป็นอิสระ นอกจากนั้น รัฐยังมักใช้แบบแผนการสอดแนมข้อมูลที่ส่งผลกระทบข้ามพรมแดนประเทศ

18. กลไกสิทธิมนุษยชนยังตรวจสอบผลกระทบด้านสิทธิมนุษยชนของอินเทอร์เน็ตและเทคโนโลยีสมัยใหม่ด้าน การสอดแนมการสื่อสารและการเข้าถึงข้อมูลการสื่อสาร ได้ช้าเกินไปทั้งสองด้าน ในขณะเดียวกัน ที่ผ่านมาคณะมนตรีสิทธิมนุษยชน ผู้มีอำนาจหน้าที่ตามกลไกพิเศษ (special procedures) และหน่วยงานกำกับดูแลสนธิสัญญาสิทธิมนุษยชน ยังไม่สามารถพิจารณาได้อย่างรอบด้านถึงผลลัพธ์ของการขยายอำนาจและการปฏิบัติด้านการสอดแนมของรัฐมากขึ้นในแง่ผลกระทบที่มีต่อสิทธิความเป็นส่วนตัวและเสรีภาพด้านความเห็นและการแสดงออก รายงานฉบับนี้พยายามที่จะแก้ไขปัญหาดังกล่าว

IV. กรอบสิทธิมนุษยชนระหว่างประเทศ

19. สิทธิที่จะมีเสรีภาพด้านความเห็นและการแสดงออกเป็นสิทธิที่ได้รับการประกันตามข้อ 19 ของปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights – UDHR) และกติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม (International Covenant on Economic, Social and Cultural Rights – ICESCR) ซึ่งยืนยันว่าบุคคลทุกคนมีสิทธิในการมีความเห็นโดยต้องไม่ถูกแทรกแซง มีสิทธิที่จะแสวงหา ได้รับ และเผยแพร่ข้อมูลและแนวคิดใด ๆ โดยผ่านสื่อชนิดต่าง ๆ และโดยไม่มีขอบเขต ในระดับภูมิภาค สิทธิดังกล่าวได้รับการคุ้มครองตามกฎบัตรสิทธิมนุษยชนและสิทธิประชาชนแห่งแอฟริกา (African Charter on Human and Peoples' Rights) (ข้อ 9) อนุสัญญาสิทธิมนุษยชนแห่งอเมริกา (American Convention on Human Rights) (ข้อ 13) และอนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานแห่งยุโรป (European Convention for the Protection of Human Rights and Fundamental Freedoms) (ข้อ 10)

20. ทั้งในระดับระหว่างประเทศและภูมิภาค ความเป็นส่วนตัวถือได้ว่าเป็นสิทธิมนุษยชนขั้นพื้นฐานอย่างเป็นเอกฉันท์ สิทธิความเป็นส่วนตัวได้รับการรับรองตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (ข้อ 12) กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ข้อ 17) อนุสัญญาว่าด้วยสิทธิเด็ก (Convention on the Rights of the Child – CRC) (ข้อ 16) และอนุสัญญาว่าด้วยการคุ้มครองสิทธิของคนงานอพยพและสมาชิกครอบครัว (International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families – ICRMW) (ข้อ 14). ในระดับภูมิภาค สิทธิความเป็นส่วนตัวได้รับการคุ้มครองตามอนุสัญญาสิทธิมนุษยชนแห่งยุโรป (European Convention on Human Rights) (ข้อ 8) และอนุสัญญาสิทธิมนุษยชนแห่งอเมริกา (American Convention on Human Rights) (ข้อ 11)

21. แม้จะมีการยอมรับพันธกรณีในการคุ้มครองความเป็นส่วนตัวอย่างกว้างขวาง แต่ที่ผ่านมากลไกคุ้มครองสิทธิมนุษยชนระหว่างประเทศยังไม่ได้กำหนดเนื้อหาของสิทธิดังกล่าวที่ครอบคลุม แม้จะมีการบรรจุสิทธิความเป็นส่วนตัวเป็นส่วนหนึ่งของกฎบัตรสิทธิมนุษยชนข้างต้น แต่เนื่องจากไม่กำหนดเนื้อหาที่ชัดเจนของสิทธิดังกล่าว ทำให้เกิดอุปสรรคในการนำไปปฏิบัติและการบังคับใช้[3] เนื่องจากสิทธิความเป็นส่วนตัวเป็นสิทธิที่อาจถูกจำกัดได้ การตีความสิทธิดังกล่าวจึงต้องอยู่บนพื้นฐานการกำหนดเนื้อหาว่าครอบคลุมความเป็นส่วนตัวมากน้อยเพียงใด ทั้งนี้เพื่อจำแนกว่าเนื้อหาส่วนใดที่ถือว่าเป็นไปเพื่อประโยชน์ของสาธารณะ การเปลี่ยนแปลงอย่างรวดเร็วและกว้างขวางของเทคโนโลยีการสื่อสารและข้อมูลในช่วงหลายทศวรรษที่ผ่านมา ยังส่งผลกระทบต่อความเข้าใจของเราที่มีต่อพรมแดนระหว่างความเป็นส่วนตัวและสาธารณะ

22. ความเป็นส่วนตัวอาจจำแนกตามสมมติฐานที่ว่า บุคคลควรมีพื้นที่ของการพัฒนา การปฏิสังสรรค์และอิสรภาพที่เป็นของตนเอง เป็น "พื้นที่ส่วนตัว" ที่อาจมีการปฏิสังสรรค์กับบุคคลอื่นหรือไม่ก็ได้ ปลอดจากการแทรกแซงของรัฐและการแทรกแซงที่ไม่คาดหมายและ

[3] UNESCO, การสำรวจความเห็นระดับโลกเกี่ยวกับความเป็นส่วนตัวทางอินเทอร์เน็ตและเสรีภาพในการแสดงออก 2555, น. 51

เกินกว่าเหตุของบุคคลอื่นที่ไม่ได้รับเชิญ[4] สิทธิความเป็นส่วนตัวยังหมายถึงความสามารถของบุคคลในการจำแนกว่าใครควรเป็นผู้เก็บรักษาข้อมูลเกี่ยวกับตัวพวกเขา และจะมีการนำข้อมูลนั้นไปใช้อย่างไร

23. เพื่อส่งเสริมให้บุคคลใช้สิทธิความเป็นส่วนตัวด้านการสื่อสารได้ พวกเขาต้องมั่นใจได้ว่าการสื่อสารเหล่านี้เป็นไปอย่างเป็นส่วนตัว ปลอดภัย และไม่ปรากฏชื่อบุคคลตามที่ต้องการได้ ความเป็นส่วนตัวของการสื่อสารหมายถึงการที่บุคคลสามารถแลกเปลี่ยนข้อมูลและแนวคิดในพื้นที่ที่สมาชิกคนอื่นในสังคม ภาคเอกชน และรัฐเข้าไม่ถึง ความปลอดภัยด้านการสื่อสารหมายถึงการที่บุคคลสามารถตรวจสอบได้ว่า ข้อมูลการสื่อสารไปถึงเฉพาะเป้าหมายของการรับข้อมูลที่ตนเองกำหนดเท่านั้น โดยปราศจากการแทรกแซงหรือการแก้ไข และข้อมูลที่ได้รับก็ปลอดจากการแทรกแซงเช่นเดียวกัน การสื่อสารอย่างปกปิดชื่อเป็นหนึ่งในความก้าวหน้าที่สำคัญสุดของอินเทอร์เน็ต ช่วยให้บุคคลสามารถแสดงความเห็นอย่างเสรีโดยไม่ต้องกลัวว่าจะถูกตอบโต้หรือถูกประณาม

A. ความสัมพันธ์ระหว่างสิทธิความเป็นส่วนตัวกับเสรีภาพด้านความเห็นและการแสดงออก

24. เรามักเข้าใจว่าสิทธิความเป็นส่วนตัวเป็นข้อกำหนดสำคัญที่นำไปสู่การปฏิบัติตามสิทธิที่จะมีเสรีภาพด้านการแสดงออก การแทรกแซงอย่างไม่เหมาะสมต่อความเป็นส่วนตัวของบุคคล อาจนำไปสู่การจำกัดการคิดค้นและแลกเปลี่ยนแนวคิดทั้งโดยทางตรงและทางอ้อม การจำกัดไม่ให้มีการปกปิดชื่อในระหว่างการสื่อสารมีผลกระทบร้ายแรงต่อเหยื่อของความรุนแรงและการปฏิบัติมิชอบในทุกรูปแบบ เป็นเหตุให้พวกเขาไม่กล้าจะรายงานข้อมูลเนื่องจากกลัวว่าจะตกเป็นเหยื่อซ้ำสอง ด้วยเหตุดังกล่าว ข้อ 17 ของกติกา ICCPR จึงกล่าวถึงการคุ้มครองให้ “การแลกเปลี่ยนข้อมูล” ปลอดจากการแทรกแซง ซึ่งตามเงื่อนไขดังกล่าวอาจตีความได้ว่าครอบคลุมรูปแบบการสื่อสารทุกประเภททั้งออนไลน์และออฟไลน์[5] ดังที่ผู้รายงานพิเศษมีข้อสังเกตในรายงานฉบับที่ผ่านมาว่า[6] สิทธิการแลกเปลี่ยนข้อมูลอย่างเป็นส่วนตัวทำให้รัฐมีพันธกรณีอย่างรอบด้านที่จะต้องประกันให้มีการส่งอีเมลและการสื่อสารออนไลน์รูปแบบอื่น ๆ ไปยังบุคคลที่ต้องการ โดยปลอดจากการแทรกแซง หรือการตรวจสอบของหน่วยงานของรัฐหรือบุคคลที่สาม[7]

25. คณะกรรมการสิทธิมนุษยชนวิเคราะห์เนื้อหาของสิทธิความเป็นส่วนตัว (ข้อ 17) ในความเห็นทั่วไป (General Comment) ฉบับที่ 16 (2531) โดยระบุว่าข้อ 17 มีเป้าหมายเพื่อคุ้มครองบุคคลจากการแทรกแซงที่ไม่ชอบด้วยกฎหมายและโดยพลการต่อความเป็นส่วนตัว ครอบครัว บ้าน หรือการแลกเปลี่ยนข้อมูล และกรอบกฎหมายในประเทศต้องกำหนดให้มีการคุ้มครองสิทธิดังกล่าว ข้อบัญญัติดังกล่าวกำหนดให้มีพันธกรณีเพื่อคุ้มครองความเป็นส่วนตัวในการสื่อสาร เป็นการเน้นย้ำว่า “ข้อมูลในการสนทนาควรส่งไปยังผู้รับโดยตรง โดยปราศจากการดักรับและไม่ให้มีการเปิดข้อมูลหรืออ่านข้อมูลนั้น” “การสอดแนมทั้งในทางอิเล็กทรอนิกส์หรือช่องทางอื่น การดักรับรูปแบบการสื่อสารทั้งทางโทรศัพท์ โทรภาพ และอื่น ๆ การดักฟังและบันทึกบทสนทนาทางโทรศัพท์ ควรเป็นสิ่งต้องห้าม[8] ความเห็นทั่วไปดังกล่าวยังระบุด้วยว่า “การรวบรวมและเก็บรักษาข้อมูลส่วนบุคคลในคอมพิวเตอร์ ธนาคารข้อมูลและอุปกรณ์อื่นใด ไม่ว่าเป็นการกระทำของหน่วยงานของรัฐหรือหน่วยงานหรือบุคคลเอกชน ต้องอยู่ภายใต้การกำกับดูแลตามกฎหมาย”[9] ในช่วงที่มีการรับรองความเห็นทั่วไปฉบับนี้ เรายังมีความเข้าใจน้อยมากเกี่ยวกับผลกระทบจากความก้าวหน้าของเทคโนโลยีด้านข้อมูลและการสื่อสารที่มีต่อสิทธิความเป็นส่วนตัว

[4] Lord Lester and D. Pannick (บรรณาธิการ) Human Rights Law and Practice. London, Butterworth, 2004, ย่อหน้า 4.82

[5] ICCPR commentary, น.401

[6] A/HRC/17/23

[7] ICCPR commentary, น.401

[8] Centre for Civil and Political Rights (CCPR) General Comment No. 16. (General Comments), น.8

[9] อ้างแล้ว, น.10

26. ในความเห็นทั่วไป ฉบับที่ 34 (2554) ว่าด้วยสิทธิที่จะมีเสรีภาพด้านการแสดงออก คณะกรรมการสิทธิมนุษยชนระบุว่า รัฐภาคีควรคำนึงถึงว่าการพัฒนาด้านเทคโนโลยีด้านข้อมูลและการสื่อสาร ส่งผลให้เกิดการเปลี่ยนแปลงการปฏิบัติด้านการสื่อสารเป็นอย่างมาก คณะกรรมการยังเรียกร้องให้รัฐภาคีปฏิบัติตามขั้นตอนทั้งหมดที่จำเป็นเพื่อสนับสนุนให้สื่อใหม่มีความเป็นอิสระ ความเห็นทั่วไปฉบับดังกล่าวยังวิเคราะห์ความสัมพันธ์ระหว่างการคุ้มครองความเป็นส่วนตัวกับเสรีภาพในการแสดงออก และมีข้อเสนอแนะให้รัฐภาคีเคารพองค์ประกอบของสิทธิที่จะมีเสรีภาพในการแสดงออก ซึ่งครอบคลุมกรณีที่ผู้สื่อข่าวมีเอกสิทธิในระดับหนึ่งที่จะปกปิดแหล่งข้อมูล[10]

27. ความตึงเครียดระหว่างสิทธิความเป็นส่วนตัวกับสิทธิที่จะมีเสรีภาพด้านการแสดงออกเกิดขึ้น ในกรณีที่มีการเผยแพร่ข้อมูลที่ถือว่าเป็นเรื่องส่วนตัวผ่านสื่อ ในกรณีดังกล่าว ข้อ 19(3) กำหนดให้มีการจำกัดเสรีภาพในการแสดงออกและด้านข้อมูล ทั้งนี้เพื่อคุ้มครองสิทธิของบุคคลอื่น อย่างไรก็ดี เช่นเดียวกับข้อจำกัดสิทธิที่จะมีเสรีภาพด้านการแสดงออกซึ่งสามารถกระทำได้ (โปรดดูด้านล่าง) เราจำเป็นต้องปฏิบัติตามหลักความได้สัดส่วนอย่างเคร่งครัด ไม่เช่นนั้นแล้วจะทำให้เกิดความเสี่ยงต่อการสกัดกั้นเสรีภาพในการแสดงออกนั้น โดยเฉพาะอย่างยิ่งในด้านการเมือง เราต้องไม่อนุญาตให้มีการวิจารณ์โจมตีชื่อเสียงที่ดีงามของนักการเมืองในทุกกรณี เนื่องจากเสรีภาพในการแสดงออกและด้านข้อมูลย่อมสูญเสียความสำคัญไป ในกรณีที่นำไปใช้เป็นส่วนหนึ่งของการแสดงความเห็นทางการเมือง[11] การรณรงค์ให้เกิดความโปร่งใสและต่อสู้กับการทุจริต ตามแนวนิติศาสตร์ระหว่างประเทศและระดับภูมิภาคสะท้อนว่า ในกรณีที่เกิดความขัดแย้งระหว่างความเป็นส่วนตัวกับเสรีภาพในการแสดงออก ให้คำนึงถึงผลประโยชน์โดยรวมของสาธารณะสำหรับเนื้อหาที่ต้องการรายงาน[12]

B. การจำกัดที่เป็นไปได้กรณีความเป็นส่วนตัวและเสรีภาพในการแสดงออก

28. กรอบตามข้อ 17 ของกติกา ICCPR อนุญาตให้มีการจำกัดเท่าที่จำเป็น ที่ชอบด้วยกฎหมายและมีสัดส่วนเหมาะสมกรณีของสิทธิความเป็นส่วนตัว ทั้งนี้ตามวิธีการจำกัดที่ได้รับอนุญาต ตรงข้ามกับข้อบัญญัติในข้อ 19 ย่อหน้า 3 ซึ่งกำหนดองค์ประกอบของการจำกัดสิทธิที่สามารถกระทำได้[13] ผู้จัดทำร่างข้อ 17 ไม่ได้ระบุเงื่อนไขการจำกัดสิทธิเอาไว้ แม้จะมีการใช้ถ้อยคำแตกต่างกันไปบ้าง แต่เป็นที่เข้าใจว่าข้อ 17 ของกติกาฉบับนี้ควรได้รับการตีความว่าครอบคลุมข้อจำกัดที่กระทำได้ ซึ่งมีการอธิบายไว้แล้วในความเห็นทั่วไปฉบับอื่นของคณะกรรมการสิทธิมนุษยชน[14]

29. ด้วยเหตุดังกล่าว ผู้รายงานพิเศษมีจุดยืนว่า สิทธิความเป็นส่วนตัวก็ควรอยู่ภายใต้เงื่อนไขที่ถูกจำกัดได้ เช่นเดียวกับสิทธิที่จะมีเสรีภาพในการเดินทาง ซึ่งอธิบายไว้อย่างชัดเจนตามความเห็นทั่วไปฉบับที่ 27[15] หลักเกณฑ์ตามที่ระบุไว้ในความเห็นดังกล่าวครอบคลุมองค์ประกอบดังต่อไปนี้:

(a) การจำกัดใด ๆ ที่กระทำได้ตามกฎหมาย (ย่อหน้า 11-12)

(b) สารัตถะของสิทธิมนุษยชนต้องไม่ถูกจำกัด (ย่อหน้า 13)

(c) การจำกัดต้องเป็นไปเท่าที่จำเป็นในสังคมประชาธิปไตย (ย่อหน้า 11)

---

[10] CCPR General Comment No. 34

[11] Nowak, Manfred, United Nations Covenant on Civil and Political Rights: CCPR Commentary (1993), น.462

[12] UNESCO, การสำรวจความเห็นระดับโลกเกี่ยวกับความเป็นส่วนตัวทางอินเทอร์เน็ตและเสรีภาพในการแสดงออก 2555, น. 53 และ 99

[13] สิทธิที่อาจถูกจำกัดได้ตามข้อ 12(3) ได้แก่ สิทธิที่จะมีอิสรภาพในการเดินทางและเสรีภาพในการเลือกถิ่นที่อยู่อาศัย ข้อ 18(3) สิทธิที่จะมีเสรีภาพทางความคิดมโนธรรมสำนึกและศาสนา ข้อ 21 สิทธิในการชุมนุมอย่างสงบและข้อ 22(2) สิทธิที่จะมีเสรีภาพในการสมาคม

[14] อ้างแล้ว

[15] และโปรดดู CCPR General Comment No. 34

(d) การใช้ดุลพินิจใด ๆ ในการจำกัดสิทธิดังกล่าว ต้องมีขอบเขต (ย่อหน้า 13)

(e) การจำกัดที่สามารถกระทำได้ ต้องไม่เป็นไปเพียงเพื่อตอบสนองเป้าหมายที่ชอบด้วยกฎหมายเพียงส่วนใดส่วนหนึ่งเท่านั้น หากต้องเป็นสิ่งจำเป็นเพื่อให้บรรลุเป้าหมายสูงสุด (ย่อหน้า 14)

(f) มาตรการที่ใช้จำกัดสิทธิต้องสอดคล้องกับหลักความได้สัดส่วน โดยต้องมีความเหมาะสมต่อการบรรลุหน้าที่ในการคุ้มครอง ต้องเป็นกฎหมายที่มีการล่วงล้ำความเป็นส่วนตัวน้อยสุดเพื่อให้บรรลุผลลัพธ์ที่ต้องการ และต้องได้สัดส่วนเมื่อเปรียบเทียบกับผลประโยชน์ที่จะได้รับการคุ้มครอง (ย่อหน้า 14-15)

C. การพิจารณาล่าสุดของกลไกสิทธิมนุษยชนเพื่อคุ้มครองสิทธิมนุษยชน

30. ในรายงานฉบับก่อนหน้านี้ ผู้รายงานพิเศษได้ประเมินผลกระทบของอินเทอร์เน็ตต่อการบรรลุสิทธิที่จะมีเสรีภาพด้านความเห็นและการแสดงออก (A/HRC/17/27 และ A/66/290) โดยเขามีข้อสังเกตว่า แม้ผู้ใช้งานอินเทอร์เน็ตจะปกปิดตัวตนได้ในระดับหนึ่งระหว่างการใช้งาน แต่รัฐและภาคเอกชนสามารถเข้าถึงเทคโนโลยีใหม่ ๆ เพื่อติดตามและเก็บข้อมูลการสื่อสารและกิจกรรมอื่น ๆ ของบุคคลได้ เทคโนโลยีเช่นนั้นมีศักยภาพในการละเมิดสิทธิความเป็นส่วนตัว ทำลายความมั่นใจและความรู้สึกปลอดภัยในการใช้งานอินเทอร์เน็ตและสกัดกั้นการแลกเปลี่ยนข้อมูลและความเห็นอย่างเสรีทางอินเทอร์เน็ต ผู้รายงานพิเศษกระตุ้นให้รัฐนำกฎหมายคุ้มครองความเป็นส่วนตัวและข้อมูลที่เป็นผลมาใช้โดยให้สอดคล้องกับมาตรฐานสิทธิมนุษยชน และให้นำมาตรการใด ๆ ที่เหมาะสมมาใช้เพื่อประกันว่าบุคคลสามารถแสดงความเห็นได้โดยสามารถปกปิดตัวตนในทางอินเทอร์เน็ต[16]

31. ผู้มีอำนาจหน้าที่ตามกลไกพิเศษอื่น ๆ ได้พิจารณาประเด็นการแทรกแซงสิทธิความเป็นส่วนตัวเช่นกัน ผู้รายงานพิเศษว่าด้วยการส่งเสริมและคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานในระหว่างการต่อต้านการก่อการร้าย ได้ศึกษาพัฒนาการของการสอดแนมและเทคโนโลยีซึ่งส่งผลกระทบอย่างมากต่อสิทธิความเป็นส่วนตัว และได้ถูกใช้เพื่อสร้างความชอบธรรมให้กับการต่อต้านการก่อการร้าย[17] ผู้รายงานพิเศษเน้นย้ำว่า มาตรการเหล่านี้ไม่เพียงนำไปสู่การละเมิดสิทธิความเป็นส่วนตัว แต่ยังมีผลกระทบต่อสิทธิตามกระบวนการอันควรตามกฎหมาย และสิทธิที่จะมีเสรีภาพในการเดินทาง เสรีภาพในการสมาคมและเสรีภาพในการแสดงออก เขากระตุ้นรัฐบาลให้พิจารณาโดยละเอียดว่า นโยบายการสอดแนมของตนสอดคล้องกับหลักความได้สัดส่วนและความจำเป็นหรือไม่ เป็นไปตามมาตรฐานสิทธิมนุษยชนระหว่างประเทศหรือไม่ และมีการนำมาตรการใดมาใช้เพื่อป้องกันไม่ให้เกิดการละเมิดเช่นนั้น ผู้รายงานพิเศษยังเรียกร้องให้นำกฎหมายการคุ้มครองข้อมูลและความเป็นส่วนตัวที่รอบด้านมาใช้ และให้จัดตั้งหน่วยงานกำกับดูแลที่เป็นอิสระเพื่อให้มีอำนาจหน้าที่ในการทบทวนการใช้เทคนิคการสอดแนมที่ล่วงล้ำความเป็นส่วนตัว และการนำข้อมูลส่วนบุคคลไปใช้งาน เขายังเรียกร้องให้มีการวิจัยและพัฒนาทรัพยากรเพื่อสนับสนุนเทคโนโลยีที่ส่งเสริมความเป็นส่วนตัว

32. เมื่อเร็ว ๆ นี้กลไกคุ้มครองสิทธิมนุษยชนอื่น ๆ ยังให้ความสำคัญกับผลกระทบของการสอดแนมการสื่อสารที่มีต่อการคุ้มครองสิทธิความเป็นส่วนตัวและเสรีภาพในการแสดงออก ตัวอย่างเช่น คณะกรรมการสิทธิมนุษยชนแสดงข้อกังวลต่อข้อกล่าวหาว่ารัฐติดตามการใช้งานอินเทอร์เน็ตและปิดกั้นการเข้าถึงเว็บไซต์บางแห่ง[18] และมีข้อเสนอแนะให้ทบทวนกฎหมายซึ่งให้อำนาจอย่างกว้างขวางต่อรัฐบาลในการ

[16] A/HRC/17/27, น.22

[17] A/HRC/13/37

[18] CCPR/C/IRN/CO/3

สอดแนมการสื่อสารทางอิเล็กทรอนิกส์[19] กลไกทบทวนสถานการณ์ด้านสิทธิมนุษยชนตามวาระ (Universal Periodic Review) ยังมีข้อเสนอแนะเพื่อประกันว่ากฎหมายเกี่ยวกับอินเทอร์เน็ตและเทคโนโลยีการสื่อสารอื่น ๆ สอดคล้องกับพันธกรณีด้านสิทธิมนุษยชน[20]

V. วิธีการสอดแนมการสื่อสาร

33. เทคโนโลยีและโครงสร้างการสอดแนมสมัยใหม่ซึ่งช่วยให้รัฐรุกล้ำพื้นที่ชีวิตส่วนบุคคลได้ ทำให้มีโอกาสจะเกิดความพร่าเลือนของเส้นแบ่งระหว่างพื้นที่ส่วนบุคคลกับสาธารณะ สนับสนุนให้มีการติดตามบุคคลในลักษณะที่เป็นการรุกล้ำความเป็นส่วนตัวโดยพลการ ทำให้ผู้ถูกติดตามไม่ทราบด้วยซ้ำว่าตนเองตกเป็นเป้าของการสอดแนม ไม่ต้องพูดถึงการคิดที่จะขอให้ทบทวนการสอดแนมดังกล่าว ความก้าวหน้าด้านเทคโนโลยีทำให้ประสิทธิภาพของรัฐในการสอดแนมไม่ถูกจำกัดด้วยขนาดหรือระยะเวลาอีกต่อไป ต้นทุนด้านเทคโนโลยีและการจัดเก็บข้อมูลที่ลดลงทำให้อุปสรรคด้านการเงินหรือเชิงปฏิบัติต่อการสอดแนมลดน้อยลง ด้วยเหตุดังกล่าว รัฐจึงมีศักยภาพมากขึ้นในการสอดแนมหลายครั้งพร้อม ๆ กัน ในลักษณะที่เป็นการรุกล้ำความเป็นส่วนตัว เฉพาะเจาะจง และในวงกว้างมากกว่าที่เคยเป็นมา

A. การสอดแนมการสื่อสารอย่างเจาะจงเป้าหมาย

34. รัฐสามารถเข้าถึงเทคนิคและเทคโนโลยีต่าง ๆ มากมายในการสอดแนมการสื่อสาร โดยเลือกการสอดแนมการสื่อสารของบุคคลบางคน การดักรับข้อมูลโดยทันทีระหว่างการรับฟัง ทำให้รัฐสามารถรับฟังและบันทึกการสนทนาทางโทรศัพท์ของบุคคลใดก็ได้ที่ใช้โทรศัพท์พื้นฐานหรือโทรศัพท์มือถือ ทั้งนี้โดยใช้คุณลักษณะการดักฟังซึ่งเป็นเงื่อนไขที่กำหนดให้โครงข่ายการสื่อสารทุกแห่งต้องมี เพื่อตอบสนองความต้องการในการสอดแนมของรัฐ[21] ทำให้รัฐสามารถระบุตำแหน่งที่ตั้งของบุคคล สามารถอ่านและบันทึกข้อความสั้น การติดตั้งเครื่องดักฟังทางสายอินเทอร์เน็ตในบางตำแหน่งหรือการเลือกกระทำกับบางบุคคล ทำให้หน่วยงานของรัฐสามารถติดตามกิจกรรมทางออนไลน์ของบุคคลได้ รวมทั้งข้อมูลเกี่ยวกับการเข้าชมเว็บไซต์ต่าง ๆ

35. การเข้าถึงข้อมูล อีเมลและข้อความของบุคคลที่ถูกจัดเก็บไว้ นอกเหนือจากข้อมูลการสื่อสารที่เกี่ยวข้องอื่น ๆ เป็นสิ่งที่สามารถทำได้ผ่านบริษัทอินเทอร์เน็ตและผู้ให้บริการด้านอินเทอร์เน็ต ความริเริ่มของหน่วยงานกำหนดมาตรฐานของยุโรป สถาบันมาตรฐานการสื่อสารแห่งยุโรป (European Telecommunications Standards Institute) ในการบังคับผู้ให้บริการกลุ่มเมฆ (cloud providers)[22] ทั้งนี้เพื่อให้มี “ศักยภาพการดักฟังข้อมูลที่ชอบด้วยกฎหมาย” ในส่วนของเทคโนโลยีฝากข้อมูลทางอินเทอร์เน็ต ซึ่งช่วยให้หน่วยงานของรัฐสามารถเข้าถึงเนื้อหาที่ผู้ให้บริการจัดเก็บไว้ได้โดยตรง รวมทั้งอีเมล ข้อความสั้น และข้อความเสียง ทั้งหมดทำให้เกิดข้อกังวล[23]

36. รัฐสามารถติดตามการเดินทางของโทรศัพท์มือถือบางเครื่อง สามารถจำแนกบุคคลทุกคนที่มีโทรศัพท์มือถืออยู่ภายในเขตที่กำหนด และสามารถดักฟังเสียงสนทนาและข้อความสั้นผ่านหลายวิธีการ รัฐบางแห่งได้ใช้อุปกรณ์ดักรับที่เรียกว่า International Mobile Subscriber Identity (IMSI) catcher เพื่อดักรับตัวเลขที่ระบุตัวตนของผู้ใช้งานจากสัญญาณในอากาศ โดยสามารถติดตั้งเป็นการชั่วคราวในบางจุดได้ (อย่างเช่นในพื้นที่ที่มีการประท้วงหรือเดินขบวน) หรือสามารถติดตั้งอย่างถาวร (อย่างเช่นที่สนามบินและจุดข้ามแดน) เครื่อง

[19] CCPR/C/SWE/CO/6

[20] A/HRC/14/10

[21] โปรดดู อย่างเช่น พระราชบัญญัติการบังคับใช้กฎหมายเพื่อช่วยเหลือด้านการสื่อสารแห่งสหรัฐฯ พ.ศ. 2537 (United States Communications Assistance for Law Enforcement Act 1994) (สหรัฐฯ); พระราชบัญญัติการสื่อสาร พ.ศ. 2540 (Telecommunications Act 1997), Part 15 (ออสเตรเลีย); พระราชบัญญัติควบคุมอำนาจการสอบสวน พ.ศ. 2543 (Regulation of Investigatory Powers Act 2000), ss12-14 (สหราชอาณาจักร); พระราชบัญญัติการสื่อสาร (อำนาจในการดักฟัง) พ.ศ. 2547 (Telecommunications (Interception Capability) Act 2004)

[22] ผู้ให้บริการกลุ่มเมฆ (cloud provider) เป็นลักษณะการให้พื้นที่เพื่อจัดเก็บข้อมูลทางอินเทอร์เน็ต

[23] ETSI DTR 101 567 VO.0.5 (2012-14), Draft Technical Report: Lawful Interception (LI); Cloud/Virtual Services (CLI)

ดักรับสัญญาณเหล่านี้ทำหน้าที่คล้ายกับสถานีส่งสัญญาณโทรศัพท์มือถือ มีการส่งและรับสัญญาณมือถือเพื่อคัดแยกข้อมูลตัวเลขระบุตัวตนของผู้ใช้หรือ subscriber identification module (SIM) และหมายเลขโทรศัพท์มือถือทุกเครื่องซึ่งอยู่ภายในพื้นที่

37. รัฐยังได้พัฒนาซอฟต์แวร์มากขึ้นเพื่อใช้ในการแทรกซึมเข้าไปยังคอมพิวเตอร์ โทรศัพท์มือถือหรืออุปกรณ์ดิจิทัลอื่น ๆ ของบุคคล[24] ซอฟต์แวร์ที่มีลักษณะรุกล้ำความเป็นส่วนตัวรวมทั้งการใช้ “โทรจัน” (หรือที่เรียกว่าสปายแวร์หรือมัลแวร์) สามารถใช้เพื่อเปิดไมโครโฟนหรือกล้องถ่ายรูปบนโทรศัพท์ สามารถติดตามการใช้ประโยชน์จากโทรศัพท์ และสามารถเข้าถึง เปลี่ยนแปลง หรือลบข้อมูลที่ถูกเก็บไว้ในอุปกรณ์สื่อสาร ซอฟต์แวร์ดังกล่าวช่วยให้รัฐสามารถควบคุมอุปกรณ์ที่ถูกแทรกซึมได้อย่างเต็มที่ และโดยที่ผู้ถูกสอดแนมไม่ทราบเรื่องนี้เลย

B. การสอดแนมการสื่อสารในวงกว้าง

38. ต้นทุนและอุปสรรคในการสอดแนมในวงกว้างเริ่มน้อยลงอย่างรวดเร็ว เทคโนโลยีสมัยใหม่ส่งเสริมให้มีการดักรับข้อมูล การติดตามและการวิเคราะห์การสื่อสารอย่างกว้างขวาง ในทุกวันนี้ รัฐบางแห่งสามารถติดตามและบันทึกการสื่อสารทางอินเทอร์เน็ตและโทรศัพท์ได้ในระดับประเทศ ทั้งนี้โดยการติดอุปกรณ์ดักรับข้อมูลที่เคเบิลเส้นใยนำแสง (ไฟเบอร์ออปติก) ซึ่งเป็นช่องทางหลักของการส่งข้อมูลการสื่อสารแบบดิจิทัล และการติดตั้งอุปกรณ์วิเคราะห์คำศัพท์ เสียง และคำพูด ทำให้รัฐแทบจะสามารถควบคุมการสื่อสารทางไกลและออนไลน์ได้ทั้งหมด มีรายงานว่าประเทศต่าง ๆ อย่างเช่น รัฐบาลอียิปต์และลิเบียได้นำระบบดักรับข้อมูลดังกล่าวมาใช้ในช่วงก่อนจะเกิดเหตุการณ์อาหรับสปริง[25]

39. ในรัฐหลายแห่ง การบังคับให้เก็บรักษาข้อมูลส่งผลให้มีการเก็บข้อมูลการสื่อสารจำนวนมหาศาล ซึ่งสามารถนำมาคัดกรองและวิเคราะห์ได้ในภายหลัง เทคโนโลยีนี้ช่วยให้รัฐสามารถสแกนโทรศัพท์และข้อความเพื่อจำแนกการใช้คำบางคำ การใช้เสียง หรือวลี หรือการกรองข้อมูลการใช้งานอินเทอร์เน็ตเพื่อจำแนกว่าบุคคลดังกล่าวได้เข้าเยี่ยมชมเว็บไซต์ หรือได้ใช้ประโยชน์จากข้อมูลทางอินเทอร์เน็ตใดบ้าง มีการคิดค้น “กล่องดำ” (“Black boxes”) เพื่อตรวจค้นข้อมูลที่ส่งผ่านอินเทอร์เน็ต ทั้งนี้เพื่อกรองและถอดรหัสข้อมูลทุกประการที่เกี่ยวข้องกับการใช้งานอินเทอร์เน็ต เป็นวิธีการที่เรียกว่า “deep-packet inspection” ซึ่งทำให้รัฐได้ข้อมูลลึกกว่าแค่ข้อมูลการเข้าเยี่ยมชมเว็บไซต์ต่าง ๆ แต่ยังรวมถึงการวิเคราะห์เนื้อหาในเว็บไซต์เหล่านั้นด้วย ยกตัวอย่างเช่น มีรายงานว่ารัฐที่เผชิญกับการลุกฮือของประชาชนในช่วงที่ผ่านมาในตะวันออกกลางและแอฟริกาเหนือ มักใช้วิธีการกรองข้อมูลแบบ deep-packed inspection[26]

40. เครื่องมืออีกอย่างหนึ่งที่รัฐสมัยใหม่นำมาใช้ได้แก่การติดตามข้อมูลทางสื่อสังคมออนไลน์ รัฐมีศักยภาพในการติดตามการใช้งานสื่อสังคมออนไลน์ เว็บบล็อก และสื่ออื่น ๆ สามารถทำแผนที่ความเชื่อมโยงและความสัมพันธ์ ความคิดเห็นและการสมาคม และแม้แต่ตำแหน่งที่อยู่ รัฐยังสามารถใช้เทคโนโลยีการวิเคราะห์ข้อมูลที่ทันสมัยมากเพื่อจัดการกับข้อมูลหรือข้อมูลการสื่อสารของสาธารณะซึ่งทางผู้ให้บริการส่งมอบให้ ในระดับพื้นฐาน รัฐยังมีช่องทางการได้มาซึ่งชื่อผู้ใช้งานและรหัสที่ใช้งานในสื่อสังคมออนไลน์ อย่างเช่น เฟซบุ๊ก[27]

C. การเข้าถึงข้อมูลการสื่อสาร

41. นอกเหนือจากการดักรับและติดตามเนื้อหาการสื่อสารของบุคคล รัฐยังอาจพยายามเข้าถึงข้อมูลการสื่อสารที่จัดเก็บไว้โดยผู้ให้บริการและบริษัทอินเทอร์เน็ต เนื่องจากภาคเอกชนเก็บสะสมข้อมูลจำนวนมากในหลายด้าน ซึ่งอาจเผยให้เห็นข้อมูลที่อ่อนไหวเกี่ยวกับวิถี

[24] Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixi Hawtin, and Natalia Torres, การสำรวจความเห็นระดับโลกเกี่ยวกับความเป็นส่วนตัวทางอินเทอร์เน็ตและเสรีภาพในการแสดงออก, UNESCO Series on Internet Freedom (2012), น. 41

[25] รัฐสภายุโรป, Directorate-General for External Policies, Policy Department, After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy (2012), น. 9-10

[26] Mendel และคณะ, อ้างแล้ว, น. 43

[27] รัฐสภายุโรป, อ้างแล้ว, น. 6

ชีวิตประจำวันของบุคคล โดยบุคคลทั่วไปและธุรกิจอาจเลือกใช้บริการเพื่อเก็บข้อมูลการสื่อสารเหล่านั้นไว้ ทั้งในรูปของวอยซ์เมล อีเมล และเอกสาร การเข้าถึงข้อมูลการสื่อสารเหล่านี้เป็นเทคนิคการสอดแนมที่มีค่ามากขึ้นที่รัฐนำมาใช้

42. ข้อมูลการสื่อสารที่ผู้ให้บริการจัดเก็บไว้ รวมทั้งบริษัทอินเทอร์เน็ตขนาดใหญ่ อาจเป็นข้อมูลที่รัฐนำมาใช้เพื่อปะติดปะต่อเป็นข้อมูลพื้นฐานส่วนบุคคล บันทึกการติดต่อและการสื่อสารที่ดูเหมือนไม่มีความเสี่ยงใด ๆ แต่เมื่อสามารถเข้าถึงและวิเคราะห์ได้ อาจทำให้สามารถจัดทำประวัติความเป็นมาและข้อมูลเกี่ยวกับชีวิตส่วนตัวของบุคคลได้ ไม่ว่าจะเป็นข้อมูลเกี่ยวกับการรักษาพยาบาล ความเห็นและ/หรือการเข้าเป็นสมาชิกกลุ่มการเมืองและศาสนา การมีปฏิสัมพันธ์และความสนใจ โดยสามารถให้รายละเอียดเป็นอย่างมาก หรือให้รายละเอียดที่ลึกซึ้งยิ่งขึ้นเมื่อเปรียบเทียบเฉพาะการวิเคราะห์เนื้อหาการสื่อสารเพียงอย่างเดียว[28] การนำข้อมูลเกี่ยวกับความสัมพันธ์ ตำแหน่งที่อยู่ อัตลักษณ์และกิจกรรมต่าง ๆ มารวมกัน ทำให้รัฐสามารถติดตามการเคลื่อนไหวของบุคคล และการดำเนินงานในหลายพื้นที่ ตั้งแต่จุดที่มีการเดินทางไปจนถึงสถานศึกษา หนังสือที่อ่าน และบุคคลที่เขามีปฏิสัมพันธ์ด้วย

43. ตัวอย่างการเข้าถึงข้อมูลการสื่อสารโดยรัฐมีเพิ่มมากขึ้นอย่างรวดเร็ว ในช่วงสามปีที่กูเกิลรายงานจำนวนการร้องขอข้อมูลการสื่อสาร ปรากฏว่าในช่วงเวลานั้นจำนวนการร้องขอข้อมูลเพิ่มขึ้นเกือบสองเท่า จาก 12,539 ในช่วงหกเดือนหลังของปี 2552 เป็น 21,389 ในช่วงหกเดือนหลังของปี 2555[29] ในสหราชอาณาจักร เจ้าพนักงานมีอำนาจในการอนุมัติการร้องขอข้อมูลการสื่อสารด้วยตนเอง มีรายงานว่าทางการได้มีคำสั่งร้องขอข้อมูลเช่นนั้นประมาณ 500,000 ครั้งต่อปี[30] ในสาธารณรัฐเกาหลี ซึ่งมีประชากรเกือบ 50 ล้านคน มีคำร้องขอข้อมูลประมาณ 37 ล้านครั้งตามรายงานข่าวในทุกปี[31]

D. การกรองเนื้อหาอินเทอร์เน็ตและการเซ็นเซอร์

44. ความก้าวหน้าด้านเทคโนโลยีไม่เพียงส่งเสริมให้มีการดักรับและเข้าถึงการสื่อสารเฉพาะบางกรณี หากยังช่วยให้รัฐสามารถคัดกรองการใช้งานอินเทอร์เน็ตได้ในระดับประเทศ ในหลายประเทศ มีการกรองเนื้อหาทางอินเทอร์เน็ตโดยอ้างว่าเพื่อสนับสนุนความสามัคคีในสังคม หรือเพื่อขจัดการใช้ถ้อยคำที่แสดงความเกลียดชัง แต่แท้จริงแล้วเป็นการใช้เพื่อขจัดคนที่เห็นต่างจากรัฐ ทำให้คนที่วิพากษ์วิจารณ์หรือเคลื่อนไหวต้องหยุดทำงาน

45. เทคโนโลยีการกรองเนื้อหาอินเทอร์เน็ตที่กล่าวถึงข้างต้น ยังสนับสนุนให้มีการติดตามการดำเนินงานของเว็บไซต์ ทำให้รัฐสามารถตรวจสอบภาพต้องห้าม คำพูด แอดเดรสของเว็บไซต์หรือเนื้อหาอื่น ๆ และสามารถเซ็นเซอร์หรือดัดแปลงแก้ไขเนื้อหาเหล่านั้นได้ รัฐสามารถใช้เทคโนโลยีดังกล่าวเพื่อตรวจสอบการใช้ถ้อยคำและวลีบางอย่าง ทั้งนี้เพื่อเซ็นเซอร์หรือควบคุมการใช้งานคำพูดเหล่านั้น หรือเพื่อจำแนกบุคคลที่ใช้คำดังกล่าว ในประเทศที่มีการเข้าถึงอินเทอร์เน็ตค่อนข้างสูง มีรายงานว่ารัฐใช้การกรองเนื้อหาอินเทอร์เน็ตเพื่อเซ็นเซอร์เนื้อหาและการสื่อสารของเว็บไซต์ และสนับสนุนให้มีการสอดแนมข้อมูลของผู้พิทักษ์สิทธิมนุษยชนและนักเคลื่อนไหว[32]

---

[28] Alberto Escudero-Pascual and Gus Hosein, “Questioning lawful access to traffic data”, Communications of the ACM, Volume 47 Issue 3, มีนาคม 2547, น. 77–82

[29] โปรดดู http://www.google.com/transparencyreport/userdatarequests/

[30] โปรดดู http://www.intelligencecommissioners.com/docs/0496.pdf

[31] Money Today, 23 ตุลาคม 2555, อ้างถึงการเปิดโปงข้อมูลโดยคณะกรรมาธิการการสื่อสารแห่งเกาหลีที่มีต่อคณะกรรมการตรวจสอบบัญชีแห่งชาติประจำปี 2556 กรณีสมาชิกรัฐสภา Yoo Seung-Hui (Korean Communication Commission for the Annual National Audit of 2013 to Assemblywoman Yoo Seung-Hui), http://www.mt.co.kr/view/mtview.php?type=1&no=2012102309430241764&outlink=1

[32] รัฐสภายุโรป, Directorate-General for External Policies, Policy Department, After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy (2012), น. 12

46. นอกจากการใช้เทคโนโลยีเพื่อสนับสนุนการกรองเนื้อหาและการเซ็นเซอร์แล้ว รัฐหลายแห่งยังใช้เจ้าหน้าที่ทำการกรองเนื้อหาอินเทอร์เน็ต มีการจัดตั้งทีมเจ้าหน้าที่และผู้ตรวจเพื่อทำหน้าที่สอดส่องดูแลเนื้อหาตามเว็บไซต์ สื่อสังคมออนไลน์ เว็บบล็อก และสื่อรูปแบบอื่น ๆ ในรัฐบางแห่ง “หน่วยตำรวจไซเบอร์” (“cyber police forces”) ได้รับมอบหมายให้คอยตรวจตราและควบคุมเนื้อหาในอินเทอร์เน็ต ค้นหาเว็บไซต์และจุดสำคัญภายในเว็บไซต์ต่าง (โดยเฉพาะตามกระดานสนทนาออนไลน์) ทั้งนี้เพื่อหาทางปิดกั้นหรือสั่งให้เว็บไซต์หยุดดำเนินการ ในกรณีที่นำเสนอเนื้อหาที่ไม่ผ่านความเห็นชอบของรัฐบาล รวมทั้งการวิพากษ์วิจารณ์ผู้นำประเทศ ยังมีการมอบหมายให้ผู้ให้บริการเอกชนแบบรับภาระการตรวจตราดังกล่าวด้วย รวมทั้งบริษัทที่ให้บริการสืบค้นข้อมูลและสื่อสังคมออนไลน์ โดยรัฐได้ออกกฎหมายขยายความรับผิดต่อเนื้อหาต้องห้ามจากผู้ที่โพสต์เป็นคนแรกให้ครอบคลุมไปถึงหน่วยงานที่เป็นสื่อกลางด้วย

E. การห้ามไม่ให้ปกปิดชื่อ

47. หนึ่งในความก้าวหน้าสำคัญสุดซึ่งเป็นผลมาจากพัฒนาการของอินเทอร์เน็ต ได้แก่ การที่ผู้ใช้งานสามารถเข้าถึงและเผยแพร่ข้อมูลโดยไม่ต้องเปิดเผยชื่อ และการสื่อสารอย่างเป็นความลับโดยบุคคลอื่นไม่ทราบว่าเราเป็นใคร เดิมเราสามารถทำแบบนั้นได้เนื่องจากไม่มี “ชั้นข้อมูลเกี่ยวกับเอกลักษณ์บุคคล” (“identity layer”) แต่เดิมเราไม่มีทางทราบว่าใครเป็นผู้ทำการสื่อสาร ใครเป็นเจ้าของอีเมล หรือเป็นการใช้งานจากคอมพิวเตอร์เครื่องไหน อย่างไรก็ดี รัฐได้อ้างเรื่องความมั่นคงและการบังคับใช้กฎหมาย และค่อย ๆ ปิดกั้นโอกาสการสื่อสารโดยการปกปิดชื่อ ในรัฐหลายแห่ง บุคคลต้องแจ้งชื่อของตนเองในการใช้อินเทอร์เน็ตคาเฟ่ และมีการบันทึกข้อมูลการทำธุรกรรมในคอมพิวเตอร์สาธารณะที่ใช้ ในเวลาต่อมาเริ่มมีการบังคับให้ต้องแสดงตัวบุคคลและจดทะเบียนในการซื้อซิมการ์ดหรือโทรศัพท์มือถือ หรือในการเข้าเยี่ยมชมเว็บไซต์ที่สำคัญบางแห่ง หรือในการโพสต์ความเห็นในเว็บไซต์หรือเว็บบล็อกต่าง ๆ

48. การห้ามไม่ให้ปกปิดชื่อช่วยสนับสนุนการสอดแนมการสื่อสารโดยรัฐ โดยช่วยให้สามารถจำแนกตัวบุคคลที่เข้าถึงหรือเผยแพร่เนื้อหาต้องห้ามได้ง่ายขึ้น ทำให้บุคคลเสี่ยงต่อการสอดแนมรูปแบบอื่น ๆ ของรัฐ

49. ด้วยเหตุดังกล่าว การห้ามไม่ให้ปกปิดชื่อย่อมส่งผลสะเทือนอย่างรุนแรง ปิดกั้นการแสดงข้อมูลและความเห็นอย่างเสรี ทั้งยังอาจส่งผลให้บุคคลปลีกตัวออกจากแวดวงสังคมออนไลน์ ปิดกั้นการใช้สิทธิในการแสดงออกและสิทธิด้านข้อมูล ทำให้ปัญหาความไม่เท่าเทียมทางสังคมรุนแรงขึ้น นอกจากนั้น การห้ามไม่ให้ปกปิดชื่อยังเปิดโอกาสให้ภาคเอกชนเก็บและรวบรวมข้อมูลจำนวนมหาศาล ทำให้เกิดภาระและความรับผิดชอบมากมายต่อบรรษัท ซึ่งต้องหาทางคุ้มครองความเป็นส่วนตัวและความปลอดภัยของข้อมูลเหล่านั้น

VI. ข้อกังวลเกี่ยวกับมาตรฐานกฎหมายในประเทศ

50. โดยทั่วไปแล้ว กฎหมายมักตามไม่ทันการเปลี่ยนแปลงทางเทคโนโลยี ในรัฐส่วนใหญ่มักไม่มีมาตรฐานกฎหมาย หรือมีแต่มีข้อบกพร่องในแง่การจัดการกับการสอดแนมการสื่อสารและสภาพแวดล้อมสมัยใหม่ ส่งผลให้รัฐสามารถสร้างความชอบธรรมให้กับการใช้เทคโนโลยีสมัยใหม่ได้มากขึ้นภายใต้กรอบกฎหมายแบบเดิม และโดยไม่ตระหนักว่าตนเองมีศักยภาพเพิ่มขึ้นมากมาย มากกว่าที่คาดการณ์ไว้ตามกรอบดังกล่าว ในหลายประเทศ จึงมีการอ้างข้อบัญญัติที่คลุมเครือและกว้างขวางเพื่อสร้างความชอบธรรมและแทรกแซงการใช้เทคนิคที่ล่วงล้ำความเป็นส่วนตัวอย่างรุนแรง หากปราศจากกฎหมายที่อนุญาตให้ใช้เทคโนโลยีและเทคนิคนั้นอย่างชัดเจน และหากไม่มีการกำหนดขอบเขตการใช้งาน จะทำให้บุคคลไม่สามารถคาดการณ์ หรือไม่รู้ตัวด้วยซ้ำว่ามีการใช้กฎหมายดังกล่าว ในเวลาเดียวกัน มีการนำกฎหมายมาใช้เพื่อขยายข้อยกเว้นด้านความมั่นคงของรัฐ ทั้งนี้เพื่อสร้างความชอบธรรมให้กับเทคนิคการสอดแนมที่รุกล้ำความเป็นส่วนตัว โดยขาดการกำกับดูแลของหน่วยงานอิสระ

51. มาตรฐานกฎหมายที่บกพร่องทำให้บุคคลเกิดความเสี่ยงมากขึ้นที่จะถูกละเมิดสิทธิมนุษยชน ไม่ว่าจะเป็นสิทธิความเป็นส่วนตัวและสิทธิที่จะมีเสรีภาพด้านการแสดงออก ทั้งยังส่งผลกระทบร้ายแรงต่อกลุ่มบุคคลบางกลุ่ม อย่างเช่น สมาชิกของพรรคการเมืองบางแห่ง นักสหภาพแรงงาน หรือชนกลุ่มน้อยในประเทศ ชนกลุ่มน้อยด้านชาติพันธุ์และภาษา ทำให้พวกเขาเสี่ยงมากขึ้นที่จะถูกสอดแนมการสื่อสารจากรัฐ หากไม่มีมาตรการคุ้มครองด้านกฎหมายที่เข้มแข็ง ผู้สื่อข่าว ผู้พิทักษ์สิทธิมนุษยชน และนักเคลื่อนไหวด้านการเมืองย่อมเสี่ยงที่จะถูกสอดแนมโดยพลการ

52. ที่ผ่านมามีการเก็บข้อมูลอย่างเป็นระบบเกี่ยวกับการสอดแนมผู้พิทักษ์สิทธิมนุษยชนในหลายประเทศ โดยผู้พิทักษ์สิทธิมนุษยชนและนักเคลื่อนไหวทางการเมืองรายงานข้อมูลว่ามีการดักฟังโทรศัพท์และดักรับอีเมลของพวกเขา และมีการติดตามการเดินทางของพวกเขา ผู้สื่อข่าวมักเสี่ยงที่จะตกเป็นเป้าของการสอดแนมการสื่อสาร เนื่องจากต้องพึ่งพาการสื่อสารทางอินเทอร์เน็ตมาก เพื่อให้สามารถรับและติดตามข้อมูลจากแหล่งข้อมูลที่ปิดลับ รวมทั้งคนในองค์กรที่ต้องการเปิดโปงความลับที่เป็นประโยชน์ต่อสาธารณะ ผู้สื่อข่าวต้องสามารถสื่อสารได้อย่างเป็นส่วนตัว ปลอดภัย และมีการปกปิดชื่อ โครงสร้างการสอดแนมที่ขยายตัวมากขึ้น และไม่ถูกจำกัดตามกระบวนการอันควรตามกฎหมายหรือการกำกับดูแลของศาล ทำให้ความพยายามในการคุ้มครองแหล่งข้อมูลเป็นไปได้ยาก แม้แต่การใช้การสอดแนมแบบแคบ ๆ ไม่โปร่งใส และไม่มีการบันทึกข้อมูล ยังอาจส่งผลกระทบรุนแรง และไม่มีการบันทึกข้อมูลการสอดแนมในพื้นที่สาธารณะ และไม่มีการถ่วงดุลตรวจสอบเพื่อป้องกันการสอดแนมอย่างมิชอบ

53. ย่อหน้าต่อไปนี้อธิบายถึงข้อกังวลพื้นฐานเกี่ยวกับกฎหมายที่อนุญาตให้รัฐสอดแนมการสื่อสาร ในสภาพแวดล้อมที่คุกคามต่อสิทธิที่จะมีเสรีภาพในการแสดงออกและความเป็นส่วนตัว

A. การขาดการกำกับดูแลจากศาล

54. โดยทั่วไปแล้ว การใช้อำนาจเพื่อสอดแนมการสื่อสารต้องได้รับความเห็นชอบจากศาล แต่ที่ผ่านมาเริ่มมีการผ่อนคลายหลักเกณฑ์ดังกล่าวมากขึ้น หรือยกเลิกหลักเกณฑ์ดังกล่าวไปเลย ในบางประเทศ รัฐมนตรี ตัวแทนที่ได้รับมอบหมายหรือคณะกรรมการมีอำนาจสั่งการให้ดักฟังการสื่อสารได้ ตัวอย่างเช่นในสหราชอาณาจักร รัฐมนตรีกระทรวงการต่างประเทศสามารถอนุมัติให้มีการดักฟังข้อมูลการสื่อสารได้[33] ในซิมบับเว รัฐมนตรีคมนาคมและการสื่อสารมีอำนาจดักรับข้อมูลการสื่อสารได้[34] และในปัจจุบันยังมีการอนุญาตการสอดแนมการสื่อสารในวงกว้างและโดยไม่เลือกเป้าหมายมากขึ้น ทั้งนี้โดยไม่มีเงื่อนไขบังคับให้เจ้าพนักงานผู้ใช้กฎหมายต้องจำแนกข้อเท็จจริงเพื่อการสอดแนมเป็นรายกรณี

55. รัฐหลายแห่งไม่กำหนดให้หน่วยงานที่บังคับใช้กฎหมายต้องคอยรายงานต่อศาลอย่างต่อเนื่อง ภายหลังได้รับหมายศาลให้ดักรับข้อมูลได้แล้ว ตามพระราชบัญญัติป้องกันการก่อการร้าย พ.ศ. 2555 (Kenyan Prevention of Terrorism Act) ของเคนยา การดักฟังการสื่อสารสามารถทำได้ในช่วงระยะเวลาไม่จำกัด โดยหน่วยงานที่บังคับใช้กฎหมายไม่จำเป็นต้องรายงานให้ศาลทราบ หรือไม่ต้องขอขยายระยะเวลาการใช้หมายศาล รัฐบางแห่งกำหนดข้อจำกัดในการปฏิบัติตามคำสั่งอนุญาต แต่เปิดโอกาสให้หน่วยงานที่บังคับใช้กฎหมายสามารถต่ออายุคำสั่งได้หลายครั้งและไม่จำกัดจำนวน

56. แม้ในกรณีที่กฎหมายกำหนดให้ต้องขออำนาจศาล แต่ก็มักเป็นการทำพอเป็นพิธี โดยมักมีการอนุญาตตามคำขอของหน่วยงานที่บังคับใช้กฎหมาย โดยเฉพาะกรณีที่หลักเกณฑ์การยื่นคำร้องมีอยู่น้อย ตัวอย่างเช่น พระราชบัญญัติกำกับดูแลและดักรับการสื่อสาร พ.ศ. 2553 (Regulation of Interception of Communications Act) ของยูกันดากำหนดเพียงให้หน่วยงานที่บังคับใช้กฎหมายแสดง “เหตุผลที่เหมาะสม” เพื่ออนุญาตให้การดักรับข้อมูล ในกรณีดังกล่าว ทางหน่วยงานมีภาระพิสูจน์เพื่อแสดงถึงความจำเป็นของการสอดแนมน้อยมาก แม้ว่าการสอดแนมเช่นนั้นอาจส่งผลกระทบรุนแรงต่อการสอบสวน การเลือกปฏิบัติ หรือการละเมิดสิทธิมนุษยชน ในประเทศอื่น ๆ ระบบกฎหมายที่ซับซ้อนอนุญาตให้มีการเข้าถึงและการสอดแนมการสื่อสารตามพฤติการณ์ที่แตกต่างกันไป ตัวอย่างเช่น ในอินโดนีเซีย พระราชบัญญัติวัตถุออกฤทธิ์ทางจิตประสาท พระราชบัญญัติยาเสพติด พระราชบัญญัติข้อมูลและธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติการสื่อสาร และพระราชบัญญัติการทุจริต ต่างมีองค์ประกอบของการสอดแนมข้อมูล ในสหราชอาณาจักร กว่า 200 หน่วยงานรวมทั้งตำรวจและศาลมีอำนาจในการร้องขอข้อมูลการสื่อสาร ทั้งนี้โดยเป็นไปตามพระราชบัญญัติควบคุมอำนาจในการสอบสวน พ.ศ. 2543 (Regulation of Investigatory Powers Act) ส่งผลให้บุคคลทั่วไปไม่สามารถคาดการณ์ได้ว่าจะถูกหน่วยงานของรัฐใดสอดแนม และได้ถูกสอดแนมเมื่อใด

[33] มาตรา 5, พระราชบัญญัติควบคุมอำนาจในการสอบสวน พ.ศ. 2543 (Regulation of Investigatory Powers Act 2000)

[34] มาตรา 5, พระราชบัญญัติการดักรับการสื่อสาร พ.ศ. 2549 (Interception of Communications Act 2006)

57. ในรัฐหลายแห่ง ผู้ให้บริการมักถูกบังคับให้ต้องดัดแปลงโครงสร้างพื้นฐานเพื่อเปิดโอกาสให้มีการสอดแนมข้อมูลโดยตรง ปิดโอกาสการกำกับดูแลจากศาลไป ตัวอย่างเช่น ในปี 2555 กระทรวงยุติธรรมและเทคโนโลยีข้อมูลและการสื่อสารของโคลอมเบียได้ออกพระราชกฤษฎีกากำหนดให้ผู้ให้บริการด้านการสื่อสารต้องจัดทำโครงข่ายซึ่งเปิดโอกาสให้ตำรวจสามารถเข้าถึงข้อมูลการสื่อสารโดยตรง โดยไม่จำเป็นต้องมีคำสั่งจากสำนักงานอัยการสูงสุด[35] พระราชบัญญัติกำกับดูแลและดักรับการสื่อสาร พ.ศ. 2553 ที่กล่าวถึงข้างต้นกำหนดให้มีการจัดตั้งศูนย์ควบคุม และกำหนดให้ผู้ให้บริการมีอำนาจหน้าที่ในการดูแลให้มีการส่งมอบข้อมูลการสื่อสารที่ถูกดักรับให้กับศูนย์ควบคุม (มาตรา 8(1)(f)) รัฐบาลอินเดียกำลังเสนอให้ติดตั้งระบบควบคุมจากส่วนกลาง (Centralized Monitoring System) ซึ่งจะหันเหทิศทางของข้อมูลการสื่อสารเข้ามาสู่รัฐบาลส่วนกลางทั้งหมด เปิดโอกาสให้หน่วยงานความมั่นคงไม่จำเป็นต้องติดต่อขอความร่วมมือจากผู้ให้บริการ[36] โครงสร้างเช่นนี้ทำให้การสอดแนมการสื่อสารอยู่นอกเหนืออำนาจศาล และเปิดโอกาสให้มีการสอดแนมข้อมูลโดยขาดการควบคุมและทำได้อย่างเป็นความลับ ทำให้ขาดความโปร่งใสหรือการตรวจสอบได้ต่อการดำเนินงานของรัฐ

B. ข้อยกเว้นด้านความมั่นคงของชาติ

58. คำนิยามที่กำกวมและไม่ชัดเจนของ “ความมั่นคงของชาติ” ได้สร้างความชอบธรรมให้กับการดักฟังและการเข้าถึงข้อมูลการสื่อสารในหลายประเทศ ตัวอย่างเช่นในอินเดีย พระราชบัญญัติเทคโนโลยีข้อมูลข่าวสาร พ.ศ. 2551 (Information Technology Act) อนุญาตให้มีการดักฟังการสื่อสารเพื่อประโยชน์ต่อ “ความเป็นเอกราช ความสมบูรณ์ของประเทศ หรือการป้องกันประเทศอินเดีย เพื่อความสัมพันธ์ฉันท์มิตรกับประเทศอื่น เพื่อความสงบเรียบร้อยของสาธารณะ และเพื่อการสอบสวนการกระทำความผิดใด ๆ” (มาตรา 69)

59. ในหลายกรณี หน่วยงานข่าวกรองแห่งชาติมักมีข้อยกเว้นอย่างกว้าง ๆ ทำให้ไม่จำเป็นต้องขอหมายศาล ตัวอย่างเช่น ในสหรัฐฯ พระราชบัญญัติการสอดแนมข่าวกรองของต่างประเทศ (Foreign Intelligence Surveillance Act) ให้อำนาจหน่วยงานความมั่นคงแห่งชาติ (National Security Agency) ในการดักฟังการสื่อสารโดยไม่ต้องขอหมายศาล กรณีที่ฝ่ายหนึ่งฝ่ายใดอยู่นอกประเทศสหรัฐฯ และมีความเชื่อได้ว่าฝ่ายหนึ่งฝ่ายใดเป็นสมาชิกของกลุ่มก่อการร้ายตามการจัดประเภทของรัฐ กฎหมายเยอรมนีอนุญาตให้หน่วยข่าวกรองของรัฐสามารถติดตั้งอุปกรณ์เพื่อดักฟังการสื่อสารภายในและระหว่างประเทศอย่างอัตโนมัติ ทั้งนี้เพื่อจุดประสงค์ในการคุ้มครองระบอบประชาธิปไตยเสรี และการคุ้มครองการดำรงอยู่หรือความมั่นคงของรัฐ[37] ในสวีเดน พระราชบัญญัติข้อมูลด้านสัญญาณเพื่อภารกิจป้องกันประเทศ (Law on Signals Intelligence in Defense Operations) ให้อำนาจหน่วยข่าวกรองสวีเดนในการดักรับข้อมูลโดยไม่ต้องขอหมายหรือขออำนาจจากศาล กรณีที่เป็นการดักฟังโทรศัพท์และข้อมูลทางอินเทอร์เน็ตที่เกิดขึ้นภายในพรมแดนประเทศสวีเดน ในสาธารณรัฐแทนซาเนีย พระราชบัญญัติข่าวกรองและบริการด้านความมั่นคง พ.ศ. 2539 (Intelligence and Security Service Act) อนุญาตให้หน่วยข่าวกรองของประเทศสามารถสอบสวนคดี และสอบปากคำบุคคลหรือการค้นตัว กรณีที่มีเหตุผลเชื่อได้ว่าเป็นบุคคลที่มีความเสี่ยง หรือเป็นต้นเหตุให้เกิดความเสี่ยง หรือเป็นภัยคุกคามต่อความมั่นคงของชาติ

60. การอ้างแนวคิดที่คลุมเครือเกี่ยวกับความมั่นคงของชาติเพื่อสร้างความชอบธรรมให้กับข้อจำกัดที่เป็นอุปสรรคต่อการเข้าถึงสิทธิมนุษยชน นับเป็นข้อกังวลร้ายแรง[38] แนวคิดดังกล่าวได้รับการกำหนดไว้อย่างหลวม ๆ ทำให้เสี่ยงที่รัฐจะบิดเบือน และใช้เพื่อสร้างความชอบธรรมให้กับการดำเนินงานที่มีเป้าหมายเป็นกลุ่มเสี่ยง อย่างเช่น ผู้พิทักษ์สิทธิมนุษยชน ผู้สื่อข่าวหรือนักเคลื่อนไหว ทั้งยังทำหน้าที่ให้อำนาจในการปกปิดข้อมูลการสอบสวน หรือการบังคับใช้กฎหมายเป็นความลับทั้งที่ไม่จำเป็น ซึ่งย่อมทำลายหลักการความโปร่งใสและการตรวจสอบได้

[35] Ministries of Justice and ICTs Decree 1704 มีที่มาจากประมวลกฎหมายวิธีพิจารณาความอาญา พ.ศ. 2547 (Criminal Procedure Code)

[36] รายงานประจำปี 2554-2555 กรมการสื่อสาร (Department of Communications) รัฐบาลอินเดีย น. 58 - http://www.dot.gov.in/annualreport/AR%20Englsih%2011-12.pdf

[37] กฎหมาย G-10

[38] มติของคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติด้านการต่อต้านการก่อการร้าย

C. การเข้าถึงข้อมูลการสื่อสารที่ขาดการควบคุม

61. การเข้าถึงข้อมูลการสื่อสารที่จัดเก็บไว้โดยผู้ให้บริการในประเทศ มักเป็นไปตามอำนาจตามกฎหมาย หรือเป็นไปตามเงื่อนไขการจดทะเบียนของบริษัท ส่งผลให้รัฐมักจะมีอำนาจที่ไม่จำกัดในการเข้าถึงข้อมูลการสื่อสารโดยแทบไม่มีการกำกับดูแลหรือการควบคุม ตัวอย่างเช่น กฎหมายในปี 2555 ของบราซิลเกี่ยวกับการฟอกเงินให้อำนาจตำรวจในการเข้าถึงข้อมูลการจดทะเบียนของผู้ให้บริการด้านอินเทอร์เน็ตและการสื่อสาร โดยไม่ต้องขอหมายศาล[39] ในระดับสากล การอนุญาตให้เข้าถึงข้อมูลการสื่อสารมักอยู่ใต้การกำกับดูแลของสนธิสัญญาความช่วยเหลือในคดีอาญา (Mutual Legal Assistance Treaties) ซึ่งเป็นข้อตกลงระดับทวิภาคี อย่างไรก็ดี ความร่วมมือในบางส่วนมักเกิดขึ้นนอกกรอบกฎหมาย โดยเป็นความร่วมมืออย่างสมัครใจของผู้ให้บริการหรือบริษัทอินเทอร์เน็ตเอง ด้วยเหตุดังกล่าว รัฐหลายแห่งจึงสามารถเข้าถึงข้อมูลการสื่อสาร โดยไม่จำเป็นต้องขออำนาจจากหน่วยงานอิสระและมีการกำกับดูแลที่จำกัด

D. การสอดแนมนอกเหนือจากกฎหมาย

62. ศักยภาพในการสอดแนมหลายประการตามที่ระบุไว้ข้างต้น อยู่นอกกรอบกฎหมายที่มีผลบังคับใช้ แต่ก็มีรัฐหลายแห่งนำมาตรการเหล่านั้นมาใช้ ซอฟต์แวร์ที่รุกล้ำความเป็นส่วนตัวอย่างมาก อย่างเช่น การใช้โทรจัน หรือการดักรับข้อมูลจำนวนมาก ถือเป็นข้อท้าทายอย่างมากต่อแนวคิดทั่วไปเกี่ยวกับการสอดแนม เนื่องจากวิธีการสอดแนมเช่นนี้ไม่สอดคล้องกับกฎหมายที่มีอยู่ในแง่การสอดแนมและการเข้าถึงข้อมูลส่วนบุคคล การสอดแนมเช่นนี้ไม่เพียงเป็นวิธีการใหม่ แต่ยังเป็นการสอดแนมในรูปแบบใหม่ จากมุมมองทางสิทธิมนุษยชน การใช้เทคโนโลยีเช่นนี้ทำให้เกิดปัญหาอย่างมาก ตัวอย่างเช่น การใช้โทรจันไม่เพียงทำให้รัฐสามารถเข้าถึงอุปกรณ์การสื่อสาร หากยังทำให้รัฐสามารถเปลี่ยนแปลงข้อมูลที่อยู่ในอุปกรณ์ได้โดยพลการและเพื่อจุดประสงค์บางอย่าง การทำเช่นนี้ส่งผลคุกคามไม่เพียงต่อสิทธิความเป็นส่วนตัวและสิทธิที่จะได้รับความเป็นธรรมในขั้นตอนปฏิบัติในแง่การใช้อุปกรณ์ตามกระบวนการกฎหมาย เทคโนโลยีการดักรับข้อมูลในวงกว้างทำให้ละเลยต่อข้อพิจารณาเรื่องการใช้งานตามสัดส่วน ทำให้เกิดการสอดแนมข้อมูลอย่างไม่เลือกเป้าหมาย เป็นเหตุให้รัฐสามารถทำสำเนาและติดตามการสื่อสารใด ๆ ในประเทศหรือพื้นที่ใด ๆ โดยไม่จำเป็นต้องขออำนาจจากหน่วยงานใดสำหรับการดักรับข้อมูลแต่ละครั้ง

63. รัฐบาลมักไม่ยอมรับว่าใช้เทคโนโลยีเหล่านี้เพื่อสอดแนมข้อมูล หรือแย้งว่าเทคโนโลยีเหล่านี้ได้ถูกนำมาใช้อย่างชอบด้วยกฎหมายภายใต้ขอบเขตอำนาจของกฎหมายการสอดแนมข้อมูลที่มีอยู่ แม้จะเป็นที่ชัดเจนว่า รัฐหลายแห่งใช้ซอฟต์แวร์ที่รุกล้ำความเป็นส่วนตัวอย่างมาก เช่น เทคโนโลยีโทรจัน แต่ที่ผ่านมาไม่เคยมีการถกเถียงเกี่ยวกับพื้นฐานกฎหมายเพื่อสนับสนุนการใช้งานเทคโนโลยีดังกล่าวในรัฐแห่งนั้น ยกเว้นในเยอรมนี ซึ่งในกรณีนั้น ทางรัฐนอร์ทไรน์-เวสท์ฟาเลียได้ผ่านกฎหมายในปี 2549 ให้อำนาจใน “การเข้าถึงระบบเทคโนโลยีข้อมูลอย่างเป็นความลับ” (§ 5.2 ข้อ 11, พระราชบัญญัติคุ้มครองรัฐธรรมนูญแห่งรัฐนอร์ทไรน์-เวสท์ฟาเลีย - North Rhine-Westphalia Constitution Protection Act) ซึ่งถือว่าเป็นการดักข้อมูลเชิงเทคนิค ทั้งนี้โดยใช้โปรแกรมสอดแนมข้อมูล หรือการใช้ประโยชน์จากช่องว่างในระบบความปลอดภัยทางคอมพิวเตอร์ ในเดือนกุมภาพันธ์ 2551 ศาลรัฐธรรมนูญแห่งสหพันธรัฐเยอรมนีได้ยกเลิกกฎหมายดังกล่าว โดยมีคำสั่งว่ามาตรการดังกล่าวจะสอดคล้องตามหลักสิทธิมนุษยชน หากเป็นการดำเนินงานโดยขออำนาจและได้รับการพิจารณาจากศาล และอาจกระทำได้เพียงในสถานการณ์ที่เกิดอันตรายอย่างเป็นรูปธรรมต่อผลประโยชน์ด้านกฎหมายที่สำคัญ[40]

[39] Brazilian Federal Law 12683/2012 มาตรา 17-B. จาก http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm

[40] เป็นภาษาเยอรมัน BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 -67),

http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

E. การใช้กฎหมายการสอดแนมข้อมูลนอกอาณาเขต

64. เนื่องจากในปัจจุบันมีการไหลเวียนของข้อมูลข้ามพรมแดนมากขึ้น และข้อมูลการสื่อสารส่วนใหญ่มักจัดเก็บไว้กับผู้ให้บริการในต่างประเทศ รัฐหลายแห่งจึงเริ่มนำกฎหมายที่ให้อำนาจตนเองในการสอดแนมข้อมูลนอกอาณาเขต หรือการดักรับข้อมูลการสื่อสารในเขตอำนาจของต่างประเทศ ทำให้เกิดข้อกังวลอย่างมากในแง่การละเมิดสิทธิมนุษยชนนอกอาณาเขตและการที่บุคคลไม่ทราบว่าตนเองตกเป็นเป้าการสอดแนมจากต่างชาติ ส่งผลกระทบต่อการขอให้ศาลทบทวนการสอดแนมข้อมูลจากต่างชาติ หรือการร้องขอการเยียวยา ตัวอย่างเช่นในแอฟริกาใต้ พระราชบัญญัติแก้ไขเพิ่มเติมกฎหมายข่าวกรองทั่วไป (General Intelligence Laws Amendment Bill) เปิดโอกาสให้มีการสอดแนมการสื่อสารนอกอาณาเขตของแอฟริกาใต้ หรือการสื่อสารที่ผ่านเข้ามาในแอฟริกาใต้[41] ในเดือนตุลาคม 2555 กระทรวงยุติธรรมและความมั่นคงของเนเธอร์แลนด์เสนอต่อรัฐสภาให้แก้ไขกฎหมาย ทั้งนี้เพื่ออนุญาตให้ตำรวจสามารถเจาะระบบคอมพิวเตอร์และโทรศัพท์มือถือทั้งภายในประเทศและภายนอกประเทศ ทั้งนี้เพื่อติดตั้งสปายแวร์ เพื่อการค้นหาและทำลายข้อมูล[42] ในเดือนธันวาคม 2555 สภานิติบัญญัติแห่งปากีสถานได้ผ่านพระราชบัญญัติการพิจารณาคดีที่เป็นธรรม พ.ศ. 2555 (Fair Trial Act) ซึ่งในย่อหน้า 31 กำหนดให้สามารถปฏิบัติตามคำสั่งศาลเพื่อสอดแนมข้อมูลในเขตอำนาจของต่างประเทศได้ ในปลายเดือนดังกล่าว สหรัฐฯ ได้รื้อฟื้นเพื่อใช้พระราชบัญญัติแก้ไขเพิ่มเติมการสอดแนมข้อมูลในต่างประเทศ พ.ศ. 2551 (Foreign Intelligence Surveillance Amendment Act) ซึ่งขยายอำนาจของรัฐบาลในการสอดแนมข้อมูลบุคคลที่ไม่ใช่พลเมืองอเมริกันและอยู่นอกประเทศสหรัฐฯ (§1881a) รวมทั้งบุคคลต่างชาติใด ๆ ซึ่งมีการสื่อสารโดยผ่านบริการเก็บข้อมูลทางอินเทอร์เน็ตและตั้งอยู่ในสหรัฐฯ (เช่นบริการของกูเกิลและบริษัทอินเทอร์เน็ตขนาดใหญ่อื่น ๆ)[43] และในปี 2555 สถาบันมาตรฐานการสื่อสารแห่งยุโรป (European Telecommunications Standards Institute) กำหนดร่างมาตรฐานเพื่อให้รัฐบาลในยุโรปสามารถดักรับข้อมูลในบริการรับฝากข้อมูลทางอินเทอร์เน็ตในต่างประเทศ[44] พัฒนาการเหล่านี้สะท้อนให้เห็นแนวโน้มที่น่าตกใจต่อการขยายอำนาจการสอดแนมข้อมูลนอกเหนือพรมแดนประเทศ ทำให้เกิดความเสี่ยงมากขึ้นว่าจะเกิดข้อตกลงความร่วมมือระหว่างหน่วยงานที่บังคับใช้กฎหมายและหน่วยงานความมั่นคงของรัฐ เพื่อหลีกเลี่ยงการปฏิบัติตามข้อจำกัดของกฎหมายในประเทศ

F. การบังคับให้เก็บข้อมูล

65. เพื่อเพิ่มโอกาสเข้าถึงข้อมูลการสื่อสารที่ถูกเก็บรักษาไว้ รัฐบางแห่งกำหนดเป็นกฎหมายให้ผู้ให้บริการอินเทอร์เน็ตและการสื่อสาร (เรียกโดยรวมว่า “ผู้ให้บริการการสื่อสาร”) ต้องเก็บและรักษาเนื้อหาและข้อมูลการสื่อสารของผู้ใช้งานอินเทอร์เน็ตเอาไว้ กฎหมายดังกล่าวอนุญาตให้เก็บข้อมูลที่ผ่านมาเกี่ยวกับอีเมล ข้อความ ตำแหน่ง การปฏิสัมพันธ์กับเพื่อนและครอบครัว ฯลฯ ไว้ได้

66. ในการให้บริการกับผู้ใช้งาน ผู้ให้บริการการสื่อสารจะกำหนดที่อยู่ไอพีให้กับอุปกรณ์หรือเครือข่ายของผู้สมัครใช้งาน[45] ซึ่งจะมีการเปลี่ยนแปลงตามเวลา ข้อมูลเกี่ยวกับไอพีแอดเดรสสามารถใช้เพื่อจำแนกบุคคลและที่อยู่ของบุคคล และติดตามการเคลื่อนไหวทางอินเทอร์เน็ตได้ กฎหมายที่บังคับให้ต้องเก็บรักษาข้อมูลส่งผลให้ผู้ให้บริการการสื่อสารต้องเก็บข้อมูลเกี่ยวกับการจัดสรรไอพีแอดเดรสไว้ช่วง

[41] มาตรา 1. c. General Intelligence Laws Amendment Bill. จาก http://www.parliament.gov.za/live/commonrepository/Processed/20111201/385713_1.pdf

[42] โปรดดู http://www.edri.org/edrigram/number10.20/dutch-proposal-state-spyware

[43] โปรดดู รัฐสภายุโรป Directorate-General for Internal Policies Policy Department C: Citizens Rights and Constitutional Affairs, Fighting crime and protecting privacy in the cloud: study, 2012

[44] Draft ESTI DTR 101 567 Lawful Interception (LI) Vo.1.0 (2012 - 05); Cloud/Virtual Services (CLI) จาก www.3gp.org

[45] ที่อยู่ไอพีหรือไอพีแอดเดรส (IP address) เป็นรหัสตัวเลขที่จำแนกคอมพิวเตอร์และอุปกรณ์อื่น ๆ ที่เชื่อมต่อกับระบบอินเทอร์เน็ต

เวลาหนึ่ง ทำให้รัฐมีโอกาสมากขึ้นในการร้องขอให้ผู้ให้บริการการสื่อสารจำแนกตัวบุคคลที่ได้รับไอพีแอดเดรสดังกล่าวในช่วงเวลาใดช่วงเวลาหนึ่ง รัฐบางแห่งยังพยายามบังคับให้ผู้ให้บริการเก็บและรักษาข้อมูลซึ่งปรกติไม่ได้เก็บเอาไว้ด้วย

67. กฎหมายที่บังคับให้ต้องเก็บรักษาข้อมูลระดับประเทศเป็นการล่วงล้ำความเป็นส่วนตัวและทำให้เกิดค่าใช้จ่าย คุกคามต่อสิทธิความเป็นส่วนตัวและการแสดงออกอย่างเสรี การบังคับให้ผู้ให้บริการการสื่อสารต้องจัดทำฐานข้อมูลขนาดใหญ่เกี่ยวกับบุคคลที่มีการสื่อสารผ่านโทรศัพท์หรืออินเทอร์เน็ต ระยะเวลาของติดต่อ และตำแหน่งของผู้ใช้งาน และบังคับให้เก็บข้อมูลนั้นไว้ (บางครั้งเป็นเวลาหลายปี) เป็นเหตุให้กฎหมายบังคับให้เก็บข้อมูลเพิ่มโอกาสให้กับรัฐในการสอดแนมข้อมูลอย่างมาก ทำให้ขอบเขตการละเมิดสิทธิมนุษยชนเพิ่มขึ้นไปด้วย ฐานข้อมูลของข้อมูลการสื่อสารยังเสี่ยงต่อการจารกรรม การฉ้อโกงและการเปิดเผยข้อมูลโดยไม่ตั้งใจ

G. กฎหมายบังคับให้เปิดเผยตัวตน

68. ในรัฐหลายแห่ง มีกฎหมายกำหนดให้ต้องแจ้งข้อมูลส่วนบุคคลระหว่างใช้งานอินเทอร์เน็ตคาเฟ่ กฎหมายเช่นนี้เป็นปัญหามากในประเทศที่อัตราการครอบครองคอมพิวเตอร์ส่วนบุคคลมีน้อย และประชาชนต้องพึ่งพาคอมพิวเตอร์สาธารณะเป็นส่วนใหญ่ ตัวอย่างเช่นในอินเดีย ระเบียบว่าด้วยเทคโนโลยีข้อมูลสนเทศ (แนวปฏิบัติสำหรับอินเทอร์เน็ตคาเฟ่) พ.ศ. 2554 กำหนดให้เจ้าของอินเทอร์เน็ตคาเฟ่ต้องขอเอกสารแสดงความเป็นตัวตนของบุคคลที่เข้ามาใช้บริการ และต้องเก็บไว้เป็นหลักฐานเป็นเวลาอย่างน้อยหนึ่งปี (ข้อ 4(2)) โดยอินเทอร์เน็ตคาเฟ่ต้องเก็บข้อมูลการใช้งานซึ่งประกอบด้วยช่วงเวลาการล็อกอินและข้อมูลที่จำแนกเครื่องคอมพิวเตอร์ที่ใช้งานไว้เป็นอย่างน้อยหนึ่งปี (ข้อ 5(1) และ 5(2)) เก็บและรักษาฐานข้อมูลสำรองของข้อมูลการใช้งานกรณีที่มีการเข้าถึงหรือการล็อกอินของผู้ใช้งานใด ๆ เป็นเวลาอย่างน้อยหนึ่งปี (ข้อ 5(4))

69. ในปัจจุบันรัฐหลายแห่งยังกำหนดให้บุคคลใช้ชื่อจริงเวลาใช้งานอินเทอร์เน็ต และต้องให้ข้อมูลส่วนบุคคลอย่างเป็นทางการเพื่อการจำแนกตัวผู้ใช้งาน ในสาธารณรัฐเกาหลี พระราชบัญญัติการสื่อสารข้อมูล (Information Communications Law) ซึ่งนำมาใช้เมื่อปี 2550 กำหนดให้ผู้ใช้งานต้องลงทะเบียนด้วยชื่อจริงก่อนเข้าไปยังเว็บไซต์ที่มีผู้เยี่ยมชมกว่า 100,000 คนต่อวัน ทั้งนี้เพื่อลดการใช้อิทธิพลข่มขู่และการใช้ถ้อยคำที่แสดงความเกลียดชังทางอินเทอร์เน็ต เมื่อเร็ว ๆ นี้ศาลรัฐธรรมนูญได้ยกเลิกคำสั่งดังกล่าวด้วยเหตุผลว่าเป็นการจำกัดเสรีภาพในการพูดและเป็นการบั่นทอนประชาธิปไตย[46] เมื่อเร็ว ๆ นี้จีนได้นำข้อวินิจฉัยเพื่อสนับสนุนและคุ้มครองข้อมูลทางอินเทอร์เน็ต (Decision to Strengthen the Protection of Online Information) มาใช้ โดยกำหนดให้พระราชบัญญัติการสื่อสารและอินเทอร์เน็ตต้องเก็บข้อมูลส่วนบุคคลของผู้ใช้งานตอนที่ล็อกอินเพื่อใช้อินเทอร์เน็ต ตอนที่ใช้โทรศัพท์พื้นฐานหรือบริการโทรศัพท์มือถือ ผู้ให้บริการซึ่งอนุญาตให้ผู้ใช้งานสามารถโพสต์ข้อความได้ จะต้องสามารถเชื่อมโยงชื่อที่ปรากฏบนจอกับชื่อจริงของผู้ใช้งานได้ ข้อกำหนดให้ลงทะเบียนด้วยชื่อจริงเปิดโอกาสให้ทางการสามารถจำแนกตัวผู้โพสต์ข้อความได้อย่างง่ายดาย และสามารถเชื่อมโยงข้อมูลในระบบเคลื่อนที่กับบุคคลได้ ทำให้การแสดงออกโดยการปกปิดชื่อสูญหายไป[47]

70. อีกมาตรการหนึ่งที่ใช้เพื่อป้องกันการปกปิดชื่อในระหว่างการสื่อสาร คือการนำนโยบายที่กำหนดให้มีการลงทะเบียนซิมการ์ดโดยใช้ชื่อจริงของผู้สมัคร หรือใช้บัตรประชาชน เป็นนโยบายที่มีการนำมาใช้มากขึ้นเรื่อย ๆ ใน 48 ประเทศในแอฟริกา มีกฎหมายกำหนดให้บุคคลต้องลงทะเบียนด้วยข้อมูลส่วนบุคคลกับผู้ให้บริการ ก่อนที่จะมีการเปิดใช้งานซิมการ์ดแบบเติมเงิน ซึ่งมีรายงานข่าวว่าการทำเช่นนั้นทำให้ต้องมีการเก็บฐานข้อมูลผู้ใช้งานขนาดใหญ่ ปิดกั้นโอกาสในการสื่อสารด้วยการปกปิดชื่อ ทำให้มีการติดตามตำแหน่งของผู้ใช้งานได้ และทำให้ขั้นตอนการสอดแนมการสื่อสารรวบรัดเกินไป[48] เมื่อไม่มีกฎหมายคุ้มครองข้อมูล เป็นเหตุให้หน่วยราชการนำข้อมูลจากซิมของผู้ใช้งานมาใช้ประโยชน์ และมีการเปรียบเทียบกับฐานข้อมูลของเอกชนและรัฐอื่น ๆ ทำให้รัฐสามารถทำประวัติอย่างละเอียดของบุคคลแต่ละ

[46] คำวินิจฉัยของศาลรัฐธรรมนูญ 2553 (Constitutional Court Decision 2010) Hun-Ma47 (“Real names” decision), 23 สิงหาคม 2555 โปรดดูสรุปอย่างเป็นทางการของคำวินิจฉัยของศาลที่เว็บไซต์ของศาล http://www.ccourt.go.kr/home/bpm/sentence01_list.jsp ภาษาเกาหลีเท่านั้น

[47] “จีนเพิ่มความเข้มงวดในการคุ้มครองข้อมูลทางอินเทอร์เน็ต” (“China to Strengthen Internet Information Protection”) - http://www.ebeijing.gov.cn/BeijingInformation/BeijingNewsUpdate/t1292298.htm

คนได้ ประชาชนยังมีความเสี่ยงที่จะถูกกีดกันจากการใช้บริการโทรศัพท์มือถือ (ซึ่งจะทำให้มีการสื่อสาร และยังทำให้สามารถเข้าถึงบริการด้านการเงิน) ในกรณีที่ไม่สามารถหรือไม่ประสงค์จะแจ้งข้อมูลส่วนบุคคลในการลงทะเบียน

H. ข้อจำกัดต่อการเข้ารหัสและกฎหมายบังคับให้เปิดเผยกุญแจ

71. ความปลอดภัยและการปกปิดตัวตนในการสื่อสาร ยังได้รับผลกระทบจากกฎหมายที่จำกัดการใช้เครื่องมือเพื่อรักษาความเป็นส่วนตัว ซึ่งเป็นเครื่องมือที่ใช้เพื่อคุ้มครองการสื่อสาร อย่างเช่น การเข้ารหัสข้อมูลได้ รัฐหลายแห่งได้นำกฎหมายบังคับให้บุคคลถอดรหัสข้อมูลตามคำสั่งของทางการได้ พระราชบัญญัติการควบคุมการดักฟังการสื่อสารและการเผยแพร่ข้อมูลเกี่ยวกับการสื่อสาร (Regulation of Interception of Communications and Provisions of Communication-Related Information Act) พ.ศ. 2545 ของแอฟริกาใต้กำหนดให้บุคคลที่มีกุญแจถอดรหัสต้องให้ความช่วยเหลือในการถอดรหัสข้อมูล[49] ฟินแลนด์ก็มีกฎหมายในลักษณะเดียวกัน (มาตรา 4(4)(a) พระราชบัญญัติมาตรการเชิงบังคับ 2530/450) (Coercive Measures Act 1987/450) เบลเยียม (มาตรา 9 พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ลงวันที่ 28 พฤศจิกายน 2543) และออสเตรเลีย (มาตรา 12 และ 28 พระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. 2544

VII. บทบาทและความรับผิดชอบของภาคเอกชน

72. พัฒนาการที่สำคัญของเทคโนโลยีทำให้เกิดรูปแบบการสื่อสารแบบใหม่ที่มีพลวัต โดยเฉพาะในภาคเอกชน ด้วยเหตุดังกล่าว การเปลี่ยนแปลงวิธีการสื่อสาร รับและส่งต่อข้อมูลของเรา จึงเป็นผลมาจากงานวิจัยและนวัตกรรมของบรรษัท

73. ภาคเอกชนยังมีบทบาทสำคัญในการสนับสนุนการสอดแนมข้อมูลบุคคลโดยรัฐในหลายรูปแบบ บรรษัทต้องกระทำตามข้อกำหนดของรัฐที่ระบุว่าเครือข่ายดิจิทัลและโครงสร้างการสื่อสาร ต้องได้รับการออกแบบเพื่อรองรับการแทรกแซงของรัฐ ข้อกำหนดดังกล่าวมีการรับรองเป็นครั้งแรกโดยรัฐต่าง ๆ ในช่วงทศวรรษ 1990 และกำลังกลายเป็นกฎบังคับสำหรับผู้ให้บริการการสื่อสารทุกหน่วยงาน รัฐได้นำกฎหมายที่กำหนดให้ผู้ให้บริการการสื่อสารต้องเปิดโอกาสให้รัฐเข้าถึงข้อมูลการสื่อสารได้โดยตรง หรือทำการดัดแปลงโครงสร้างพื้นฐานเพื่อสนับสนุนการรุกล้ำความเป็นส่วนตัวรูปแบบใหม่ของรัฐ

74. ในการจัดทำและนำเทคโนโลยีและเครื่องมือสื่อสารใหม่มาใช้ในบางพื้นที่ บรรษัทได้ยินยอมใช้มาตรการเพื่อสนับสนุนการสอดแนมของรัฐ ในรูปแบบพื้นฐาน ความร่วมมือดังกล่าวอยู่ในรูปการตัดสินใจว่าบรรษัทจะเข้ามาเก็บและวิเคราะห์ข้อมูลซึ่งจะทำให้กลายเป็นแหล่งพักขนาดใหญ่ของข้อมูลส่วนบุคคล ซึ่งรัฐสามารถเรียกดูเมื่อไรก็ได้ บรรษัทยังกำหนดมาตรการที่ช่วยให้รัฐเข้าถึงหรือรุกล้ำความเป็นส่วนตัว เก็บข้อมูลที่ถูกเปิดเผยไว้เป็นจำนวนมาก หรือจำกัดการใช้การเข้ารหัสและเทคนิคอื่น ๆ เพื่อจำกัดการเข้าถึงข้อมูลโดยบริษัทและรัฐบาล ภาคเอกชนยังมักล้มเหลวในการใช้เทคโนโลยีเพื่อส่งเสริมความเป็นส่วนตัวและนำมาใช้น้อยลง ซึ่งทำให้เป็นมาตรการรักษาความปลอดภัยที่มีคุณภาพต่ำ

75. ในกรณีร้ายแรงสุด ภาคเอกชนได้มีส่วนร่วมในการจัดทำเทคโนโลยีที่สนับสนุนให้มีการสอดแนมข้อมูลในวงกว้างหรือรุกล้ำความเป็นส่วนตัวซึ่งขัดกับมาตรฐานกฎหมายที่เป็นอยู่[50] ส่วนบรรษัทได้พัฒนาอุตสาหกรรมระดับโลกที่เน้นการแลกเปลี่ยนเทคโนโลยีการสอดแนม

[48] Kevin P. Donovan and Aaron K. Martin, “The Rise of African SIM Registration: Mobility, Identity, Surveillance and Resistance,” Information Systems and Innovation Group Working Paper Series, no. 186, London School of Economics and Political Science (2555)

[49] มาตรา 29. South African Regulation of Interception of Communications and Provisions of Communication - Related Information Act 2002. จาก http://www.dac.gov.za/acts/Regulation%20of%20Interception%20of%20Communications%20Act.pdf

[50] ตัวอย่างของเทคโนโลยีการสอดแนมข้อมูลที่ออกแบบโดยภาคเอกชนแล้วมีการนำมาใช้ในลิเบีย บาห์เรน สาธารณรัฐอาหรับซีเรีย อียิปต์และตูนีเซีย โปรดดู รัฐสภายุโรป, Directorate-General for External Policies, Policy Department, After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy (2555), น. 9-10

ข้อมูล โดยมักมีการขายเทคโนโลยีเหล่านี้ให้กับประเทศที่มีความเสี่ยงอย่างยิ่งว่าจะถูกนำไปใช้เพื่อละเมิดสิทธิมนุษยชน โดยเฉพาะผู้พิทักษ์สิทธิมนุษยชน ผู้สื่อข่าวหรือกลุ่มเสี่ยงอื่น ๆ อุตสาหกรรมดังกล่าวแทบไม่อยู่ภายใต้การควบคุมใด ๆ เนื่องจากรัฐไม่สามารถตามทันพัฒนาการด้านเทคโนโลยีและการเมืองได้

76. พันธกรณีด้านสิทธิมนุษยชนของรัฐกำหนดให้ต้องมีการเคารพและส่งเสริมสิทธิที่จะมีเสรีภาพในการแสดงออกและความเป็นส่วนตัว นอกจากนั้น ยังต้องคุ้มครองบุคคลจากการละเมิดสิทธิมนุษยชนที่เป็นผลจากการกระทำของบรรษัท และรัฐควรทำหน้าที่กำกับดูแลอย่างเพียงพอเพื่อปฏิบัติตามพันธกรณีด้านสิทธิมนุษยชนระหว่างประเทศ ในกรณีที่รัฐต้องเข้าไปทำสัญญา หรือออกกฎหมายเพื่อบรรษัท ซึ่งอาจส่งผลกระทบต่อการเข้าถึงสิทธิมนุษยชน[51] พันธกรณีด้านสิทธิมนุษยชนในแง่ดังกล่าวยังมีผลบังคับใช้กรณีที่บรรษัทดำเนินงานในต่างประเทศ[52]

77. รัฐต้องประกันว่าภาคเอกชนปฏิบัติหน้าที่อย่างเป็นอิสระ ในลักษณะที่ส่งเสริมสิทธิมนุษยชนของบุคคล ในเวลาเดียวกัน จะต้องไม่อนุญาตให้บรรษัทเข้าร่วมในกิจกรรมที่เป็นการละเมิดสิทธิมนุษยชน และรัฐมีความรับผิดชอบต้องตรวจสอบบรรษัทหากเกิดกรณีดังกล่าวขึ้น

VIII. ข้อสรุปและข้อเสนอแนะ

78. เทคนิคและเทคโนโลยีการสื่อสารได้พัฒนาไปอย่างมาก เปลี่ยนแปลงวิธีการสอดแนมการสื่อสารของรัฐ ด้วยเหตุดังกล่าว รัฐจะต้องเปลี่ยนแปลงความเข้าใจและปรับระเบียบด้านการสอดแนมการสื่อสารให้เข้ากับยุคสมัย และเปลี่ยนแปลงแนวปฏิบัติเพื่อประกันว่ามีการเคารพและคุ้มครองสิทธิมนุษยชนของบุคคล

79. รัฐยังไม่สามารถประกันให้บุคคลค้นหาและได้รับ หรือแสดงความเห็นได้อย่างเสรี หากไม่มีการเคารพคุ้มครอง และส่งเสริมสิทธิความเป็นส่วนตัวของพวกเขา ความเป็นส่วนตัวและเสรีภาพในการแสดงออกเชื่อมโยงกันและพึ่งพากัน การละเมิดสิทธิใดสิทธิหนึ่งอาจเป็นทั้งเหตุและผลของการละเมิดสิทธิอีกด้านหนึ่ง หากไม่มีกฎหมายและมาตรฐานด้านกฎหมายที่เพียงพอเพื่อประกันความเป็นส่วนตัว ความปลอดภัย และการปกปิดตัวตนในระหว่างการสื่อสาร ย่อมเป็นเหตุให้ผู้สื่อข่าว ผู้พิทักษ์สิทธิมนุษยชน และผู้เปิดโปงข้อมูลไม่สามารถมั่นใจได้ว่า การสื่อสารของพวกเขาจะไม่ถูกตรวจสอบจากรัฐ

80. เพื่อปฏิบัติตามพันธกรณีด้านสิทธิมนุษยชน รัฐต้องประกันว่าสิทธิที่จะมีเสรีภาพในการแสดงออกและความเป็นส่วนตัว เป็นหัวใจของกรอบกำหนดการสอดแนมการสื่อสาร ด้วยเหตุดังกล่าว ผู้รายงานพิเศษจึงมีข้อเสนอแนะดังต่อไปนี้

[51] หลักการที่เป็นแนวปฏิบัติด้านธุรกิจและสิทธิมนุษยชน: การปฏิบัติตามกรอบของหลักการที่ 5 ขององค์การสหประชาชาติว่าด้วย “การคุ้มครอง การเคารพ และการเยียวยา” (Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework, Principle 5)

[52] คณะกรรมการสิทธิมนุษยชน, Concluding Observations, เยอรมนี, ธันวาคม 2555

A. การปรับปรุงและพัฒนากฎหมายและมาตรฐานกฎหมาย

81. ควรถือว่าการสอดแนมการสื่อสารเป็นพฤติการณ์ที่รุกล้ำความเป็นส่วนตัวอย่างมาก และเสี่ยงที่จะเป็นการแทรกแซงสิทธิที่จะมีเสรีภาพในการแสดงออกและความเป็นส่วนตัว และคุกคามพื้นฐานของสังคมประชาธิปไตย กฎหมายต้องกำหนดว่า การสอดแนมการสื่อสารของรัฐสามารถกระทำได้เฉพาะกรณีที่เป็นข้อยกเว้นมากสุดเท่านั้น และเฉพาะเมื่อมีการกำกับดูแลจากหน่วยงานศาลที่เป็นอิสระ กฎหมายต้องกำหนดให้มีหลักประกันที่ระบุรายละเอียดขอบเขต และระยะเวลาที่อนุญาตให้ใช้มาตรการดังกล่าวได้ หลักเกณฑ์ให้อนุญาต หน่วยงานที่มีอำนาจซึ่งสามารถอนุมัติ ดำเนินการ และกำกับดูแล และการเยียวยาที่เป็นไปตามกฎหมายในประเทศ

82. บุคคลควรมีสิทธิตามกฎหมายที่จะได้รับแจ้งกรณีที่ถูกสอดแนมการสื่อสาร หรือกรณีที่รัฐเข้าถึงข้อมูลการสื่อสารของตน แม้การแจ้งล่วงหน้าหรือการแจ้งในระหว่างการสอดแนม อาจส่งผลกระทบต่อประสิทธิภาพของการสอดแนมข้อมูล แต่บุคคลก็ควรได้รับแจ้งเมื่อการสอดแนมสิ้นสุดลงแล้ว และให้มีช่องทางเข้าถึงการเยียวยาในแง่ของการใช้มาตรการสอดแนมการสื่อสารและผลที่เกิดขึ้น

(a) กรอบกฎหมายต้องประกันว่ามาตรการสอดแนมการสื่อสาร:

(b) เป็นไปตามที่กฎหมายบัญญัติ ชัดเจนตามมาตรฐานที่กำหนด และมีความแม่นยำเพียงพอเพื่อประกันว่าบุคคลได้รับแจ้งล่วงหน้า และเล็งเห็นผลจากการใช้มาตรการดังกล่าว

(c) เป็นสิ่งที่จำเป็นอย่างเคร่งครัดและพิสูจน์ได้เพื่อบรรลุเป้าหมายที่ชอบด้วยกฎหมาย และ

83. สอดคล้องกับหลักความได้สัดส่วน และจะต้องไม่นำมาใช้ในกรณีที่มีเทคนิคที่รุกล้ำความเป็นส่วนตัวน้อยกว่า หรือกรณีที่ยังไม่นำมาตรการอื่นมาใช้จนหมดสิ้น

84. รัฐควรลงโทษการสอดแนมที่ไม่ชอบด้วยกฎหมายที่กระทำโดยหน่วยงานของรัฐหรือเอกชน กฎหมายดังกล่าวต้องไม่ถูกใช้เพื่อปราบปรามผู้เปิดโปงข้อมูล หรือเพื่อปิดกั้นไม่ให้บุคคลเปิดโปงข้อมูลการละเมิดสิทธิมนุษยชน และต้องไม่กระทบต่อการกำกับดูแลที่ชอบด้วยกฎหมายของประชาชนต่อการปฏิบัติงานของรัฐ

85. ควรมีการกำกับดูแลอย่างเพียงพอกรณีที่ภาคเอกชนส่งมอบข้อมูลการสื่อสารให้กับรัฐ ทั้งนี้เพื่อประกันว่ามีการให้ความสำคัญเป็นลำดับแรกกับสิทธิมนุษยชนของบุคคลเสมอ การพยายามเข้าถึงข้อมูลการสื่อสารที่เก็บรักษาไว้โดยบรรษัทในประเทศ ให้กระทำได้ในกรณีที่ได้ลองใช้เทคนิคอื่นที่เป็นการรุกล้ำความเป็นส่วนตัวน้อยกว่านี้จนหมดสิ้นแล้ว

86. ควรมีหน่วยงานอิสระ อย่างเช่น ศาลหรือกลไกกำกับดูแลทำหน้าที่ติดตามการส่งมอบข้อมูลการสื่อสารให้กับรัฐ ในระดับสากล รัฐควรออกกฎหมายความร่วมมือทางอาญาเพื่อควบคุมการเข้าถึงข้อมูลการสื่อสารที่เก็บรักษาไว้โดยบรรษัทต่างชาติ

87. เทคนิคและการปฏิบัติเพื่อการสอดแนมข้อมูลที่นำมาใช้โดยขัดกับหลักนิติธรรม ต้องได้รับการแก้ไขให้อยู่ภายใต้การควบคุมตามกฎหมาย การใช้มาตรการนอกกฎหมายเช่นนี้ ทำลายหลักการพื้นฐานของประชาธิปไตย และมีแนวโน้มส่งผลกระทบด้านลบต่อการเมืองและสังคม

B. สนับสนุนการสื่อสารอย่างเป็นส่วนตัว ปลอดภัย และมีการปกปิดชื่อ

88. รัฐควรงดเว้นจากการบังคับให้เปิดเผยข้อมูลส่วนบุคคลก่อนการเข้าถึงการสื่อสาร ไม่ว่าจะเป็นบริการอินเทอร์เน็ต อินเทอร์เน็ตคาเฟ่หรือโทรศัพท์มือถือ

89. บุคคลควรมีเสรีภาพในการใช้เทคโนโลยีใดก็ตามเพื่อคุ้มครองความปลอดภัยของการสื่อสารของตนเอง รัฐไม่ควรแทรกแซงการใช้เทคโนโลยีการเข้ารหัส หรือไม่บังคับให้ต้องส่งมอบคีย์ที่ใช้ในการเข้ารหัส

90. รัฐไม่ควรเก็บรักษา หรือกำหนดให้ต้องเก็บรักษาข้อมูลใดเพื่อประโยชน์ในการสอดแนมเท่านั้น

C. การเพิ่มโอกาสการเข้าถึงข้อมูลของสาธารณะ การเพิ่มความเข้าใจและความตระหนักรู้ถึงภัยคุกคามต่อความเป็นส่วนตัว

91. รัฐควรดำเนินการอย่างโปร่งใสจนเต็มที่ ในแง่ของการใช้และขอบเขตของเทคนิคและอำนาจในการสอดแนมการสื่อสาร โดยอย่างน้อยควรตีพิมพ์เผยแพร่ข้อมูลโดยรวมของจำนวนการร้องขอข้อมูลที่อนุมัติและปฏิเสธ การแยกประเภทคำร้องขอตามรายชื่อผู้ให้บริการ และตามการสอบสวนและจุดประสงค์การใช้งาน

92. รัฐควรสนับสนุนให้บุคคลมีข้อมูลอย่างเพียงพอ เพื่อช่วยให้เข้าใจอย่างเต็มที่ถึงขอบเขต ลักษณะ และการใช้กฎหมายเพื่ออนุญาตให้มีการสอดแนมการสื่อสาร รัฐควรสนับสนุนให้ผู้ให้บริการตีพิมพ์เผยแพร่ขั้นตอนปฏิบัติที่นำมาใช้เมื่อรัฐทำหน้าที่สอดแนมการสื่อสาร ปฏิบัติตามขั้นตอนที่กำหนด และตีพิมพ์เผยแพร่คำร้องขอตามการสอดแนมการสื่อสารของรัฐ

93. รัฐควรจัดตั้งกลไกกำกับดูแลที่เป็นอิสระ เพื่อประกันให้การสอดแนมการสื่อสารของรัฐมีความโปร่งใสและตรวจสอบได้

94. รัฐควรสร้างความตระหนักรู้ต่อสาธารณะเกี่ยวกับการใช้เทคโนโลยีการสื่อสารใหม่ ๆ เพื่อสนับสนุนให้บุคคลสามารถประเมิน บริหารจัดการ ลดผลกระทบ และตัดสินใจอย่างมีความรู้เกี่ยวกับความเสี่ยงเนื่องจากการสื่อสาร

D. ควบคุมการใช้ประโยชน์เชิงพาณิชย์ของเทคโนโลยีการสอดแนมข้อมูล

95. รัฐควรประกันว่าข้อมูลการสื่อสารที่เก็บรวบรวมไว้โดยบรรษัทจากการให้บริการเป็นไปตามมาตรฐานการคุ้มครองข้อมูลขั้นสูงสุด

96. รัฐต้องงดเว้นจากการบังคับให้ภาคเอกชนใช้มาตรการที่ส่งผลกระทบต่อความเป็นส่วนตัว ความปลอดภัย และการปกปิดชื่อตนเองในการใช้บริการการสื่อสาร รวมทั้งการกำหนดให้มีการพัฒนาความสามารถในการดักรับข้อมูลเพื่อประโยชน์ด้านการสอดแนมของรัฐ หรือการห้ามการเข้ารหัสข้อมูล

97. รัฐต้องใช้มาตรการเพื่อป้องกันการใช้ประโยชน์เชิงพาณิชย์ของเทคโนโลยีการสอดแนมข้อมูล โดยให้ความใส่ใจกับการทำวิจัย การพัฒนา การค้า การส่งออก และการใช้เทคโนโลยีเหล่านี้ โดยคำนึงถึงศักยภาพที่ถูกใช้เพื่อการละเมิดสิทธิมนุษยชนอย่างเป็นระบบ

E. ส่งเสริมการประเมินพันธกรณีด้านสิทธิมนุษยชนระหว่างประเทศที่เกี่ยวข้อง

98. เป็นสิ่งที่จำเป็นอย่างยิ่งที่จะต้องส่งเสริมความเข้าใจในระหว่างประเทศเกี่ยวกับการคุ้มครองสิทธิความเป็นส่วนตัว เมื่อคำนึงถึงพัฒนาการของเทคโนโลยีที่เป็นอยู่ คณะกรรมการสิทธิมนุษยชนควรพิจารณาออก “ความเห็นทั่วไป” ฉบับใหม่ว่าด้วยสิทธิความเป็นส่วนตัวเพื่อทดแทนความเห็นทั่วไป ฉบับที่ 16 (2531)

99. กลไกสิทธิมนุษยชนควรประเมินเพิ่มเติมถึงพันธกรณีของภาคเอกชนในการจัดทำและการขายเทคโนโลยีการสอดแนม