A/HRC/27/37
Advance Edited Version Distr.: General 30 มิถุนายน 2557
ต้นฉบับเดิม: อังกฤษ
ฉบับแปลภาษาไทยโดยเครือข่ายพลเมืองเน็ต (เผยแพร่ 8 กันยายน 2557)

คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ สมัยประชุมที่ 27 วาระ 2 และ 3
รายงานประจำปีของข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติและ
รายงานของสำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติและ
เลขาธิการสหประชาชาติ

การส่งเสริมและคุ้มครองสิทธิมนุษยชน สิทธิพลเมือง การเมือง เศรษฐกิจ สังคมและวัฒนธรรม รวมทั้งสิทธิด้านการพัฒนา

สิทธิความเป็นส่วนตัวในยุคดิจิทัล

รายงานของสำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติ

สรุป

ในมติที่ 68/167 สมัชชาใหญ่แห่งสหประชาชาติร้องขอให้ข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติ ส่งมอบรายงานว่าด้วยการส่งเสริมและคุ้มครองสิทธิความเป็นส่วนตัว ในบริบทของการสอดแนมในประเทศและนอกประเทศ และ/หรือการดักจับข้อมูลสื่อสารแบบดิจิทัล และการเก็บข้อมูลส่วนบุคคล รวมทั้งกรณีที่เกิดขึ้นในวงกว้าง ทั้งนี้เพื่อการพิจารณาของคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติในสมัยประชุมที่ 27 และการพิจารณาของสมัชชาใหญ่สหประชาชาติในสมัยประชุมที่ 69 ทั้งนี้เพื่อให้รัฐภาคีได้พิจารณาความเห็นและข้อเสนอแนะต่าง ๆ รายงานฉบับนี้เป็นการส่งมอบตามคำร้องขอดังกล่าว โดยสำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติยังได้ส่งมอบรายงานฉบับนี้ให้กับที่ประชุมสมัยที่ 69 ของสมัชชาใหญ่สหประชาชาติ โดยเป็นไปตามคำร้องขอของสมัชชา

สารบัญ

I. อารัมภบท

1. เทคโนโลยีการสื่อสารแบบดิจิทัล อย่างเช่น การสื่อสารผ่านอินเทอร์เน็ต สมาร์ตโฟนและอุปกรณ์เชื่อมต่อไวไฟ กลายเป็นส่วนหนึ่งของชีวิตประจำวัน นวัตกรรมเทคโนโลยีการสื่อสารเช่นนี้นอกจากทำให้สามารถเข้าถึงข้อมูลและการสื่อสารแบบปัจจุบันได้อย่างรวดเร็วมากขึ้นแล้ว ยังมีส่วนสนับสนุนเสรีภาพในการแสดงออก การแลกเปลี่ยนความเห็นในระดับโลก และการมีส่วนร่วมด้านประชาธิปไตย เทคโนโลยีที่ทรงพลังเหล่านี้ยังเป็นเหตุให้ผู้พิทักษ์สิทธิมนุษยชนสามารถรณรงค์ได้หนักแน่นมากขึ้น เป็นเครื่องมือชนิดใหม่ที่ช่วยในการบันทึกข้อมูลและเปิดโปงการปฏิบัติไม่ชอบ ทำให้เกิดความหวังมากขึ้นต่อการเข้าถึงสิทธิมนุษยชนประการต่าง ๆ เนื่องจากชีวิตในรุ่นคนปัจจุบันมีส่วนเกี่ยวข้องกับโลกออนไลน์มากขึ้น อินเทอร์เน็ตจึงเป็นสิ่งที่แพร่หลายและใกล้ชิดกับเรามากยิ่งขึ้น

2. ในยุคดิจิทัล เทคโนโลยีการสื่อสารมีส่วนสนับสนุนศักยภาพของรัฐบาล วิสาหกิจและบุคคลในการสอดแนม ดักจับ และเก็บรวบรวมข้อมูล ตามที่ตั้งข้อสังเกตไว้โดยผู้รายงานพิเศษว่าด้วยสิทธิที่จะมีเสรีภาพในการแสดงออกและการแสดงความเห็น (Special Rapporteur on the right to freedom of expression and opinion) ความก้าวหน้าทางเทคโนโลยีส่งผลให้รัฐสามารถสอดแนมข้อมูลได้อย่างไม่มีข้อจำกัดในแง่ของขอบเขตและระยะเวลา ต้นทุนด้านเทคโนโลยีและที่จัดเก็บข้อมูลที่ลดลงทำให้อุปสรรคด้านการเงินหรือในทางปฏิบัติของการสอดแนมข้อมูลหมดไป ในปัจจุบันรัฐมีศักยภาพเพิ่มขึ้นมากในการสอดแนมข้อมูลหลายครั้งในเวลาเดียวกัน รุกล้ำความเป็นส่วนตัว มีเป้าหมายเฉพาะเจาะจงและเป็นไปอย่างกว้างขวางมากกว่าที่เคยเป็น[1] กล่าวอีกอย่างหนึ่ง พื้นฐานเทคโนโลยีที่เป็นปัจจัยหนุนเสริมสำคัญมากขึ้นต่อชีวิตทางการเมือง เศรษฐกิจและสังคมในระดับโลก ไม่เพียงจะตกเป็นเป้าหมายของการสอดแนมข้อมูลในวงกว้าง หากยังเป็นปัจจัยหนุนเสริมการสอดแนมดังกล่าว

3. มีการแสดงข้อกังวลอย่างลึกซึ้ง หลังจากมีการเปิดโปงข้อมูลเกี่ยวกับนโยบายและการปฏิบัติที่ใช้ประโยชน์จากจุดอ่อนของเทคโนโลยีการสื่อสารแบบดิจิทัล เพื่อทำการสอดแนมและดักจับข้อมูลทางอิเล็กทรอนิกส์ในหลายประเทศทั่วโลก ดังเราจะเห็นตัวอย่างการสอดแนมข้อมูลดิจิทัลอย่างเปิดเผยและปิดลับในเขตอำนาจศาลต่าง ๆ ที่เกิดขึ้นทั่วไปในโลก โดยรัฐได้หันมาใช้การสอดแนมข้อมูลในวงกว้างจนกลายเป็นนิสัยที่อันตราย แทนที่จะใช้เป็นมาตรการชั่วคราว มีรายงานว่ารัฐบาลข่มขู่จะห้ามไม่ให้บริษัทให้บริการด้านสื่อสารโทรคมนาคมและอุปกรณ์เชื่อมต่อแบบไร้สาย เว้นแต่บริษัทเหล่านี้จะยอมให้รัฐสามารถเข้าถึงช่องทางการสื่อสารของพวกเขาโดยตรง ต้องยอมให้รัฐดักจับสัญญาณจากสายไฟเบอร์ออปติกเพื่อการสอดแนมข้อมูล ทั้งยังบังคับให้บริษัทต้องเปิดเผยข้อมูลจำนวนมากของลูกค้าและพนักงานของตนอย่างเป็นระบบ นอกจากนั้น รัฐบางแห่งยังได้ใช้การสอดแนมเครือข่ายโทรคมนาคมเพื่อเล่นงานฝ่ายตรงข้ามทางการเมือง และ/หรือฝ่ายที่คัดค้านรัฐบาล มีรายงานว่าทางการในหลายรัฐมักจะบันทึกข้อมูลการสื่อสารทางโทรศัพท์ทุกครั้ง เพื่อเก็บข้อมูลไว้วิเคราะห์ ทั้งยังมีรายงานว่ารัฐบาลหลายแห่งได้ดักฟังข้อมูลการสื่อสารในการประชุมหรือกิจกรรมระดับโลก หน่วยงานในรัฐแห่งหนึ่งกำหนดให้มีการติดตั้งซอฟต์แวร์คัดกรองข้อมูลอยู่ในเครื่องคอมพิวเตอร์ที่ขายในประเทศ ทั้งนี้เพื่อจุดประสงค์ในการสอดแนมข้อมูล แม้แต่กลุ่มที่ไม่ใช่รัฐก็มีรายงานว่าได้มีการพัฒนาศักยภาพการสอดแนมข้อมูลดิจิทัลที่ทันสมัย เทคโนโลยีการสอดแนมข้อมูลในวงกว้างยังเข้าสู่ตลาดโลก ทำให้เกิดความเสี่ยงว่ารัฐบาลจะไม่สามารถควบคุมการสอดแนมข้อมูลดิจิทัลได้อีกต่อไป

4. มีการแสดงความกังวลมากขึ้นภายหลังมีการเปิดโปงในระหว่างปี 2556 และ 2557 ที่ชี้ว่า หน่วยงานความมั่นคงแห่งชาติ (National Security Agency) ในสหรัฐอเมริกา และหน่วยงานข่าวกรองกลาง (General Communications Headquarters) ในสหราชอาณาจักรและไอร์แลนด์เหนือ ได้ร่วมมือกันพัฒนาเทคโนโลยีซึ่งทำให้สามารถเข้าถึงจราจรด้านอินเทอร์เน็ตในระดับโลกเป็นส่วนใหญ่ ข้อมูลการติดต่อทางโทรศัพท์ในสหรัฐฯ การเข้าถึงบันทึกรายชื่อทางอิเล็กทรอนิกส์ของบุคคล และการสื่อสารข้อมูลดิจิทัลปริมาณมหาศาล มีรายงานว่า มีการติดตั้งเทคโนโลยีเหล่านี้ในเครือข่ายการสื่อสารข้ามประเทศ โดยเป็นผลมาจากกความร่วมมือด้านข่าวกรองเชิงยุทธศาสตร์ระหว่างรัฐบาล หน่วยงานควบคุมบริษัทเอกชนและสัญญาเชิงพาณิชย์

5. ผลจากข้อกังวลของรัฐภาคีและผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่มีต่อผลกระทบด้านลบของการสอดแนมข้อมูลด้านสิทธิมนุษยชนเหล่านี้ เป็นเหตุให้เมื่อเดือนธันวาคม 2556 สมัชชาใหญ่สหประชาชาติรับรองมติที่ 68/167 ว่าด้วยสิทธิ

---

[1] A/HRC/23/40, ย่อหน้า 33

ความเป็นส่วนตัวในยุคดิจิทัล โดยไม่มีการลงคะแนนเสียง ในมติที่มีการสนับสนุนร่วมกันโดยรัฐภาคี 57 แห่ง ทางสมัชชาใหญ่ยืนยันถึงสิทธิของคนที่ไม่ใช้อินเทอร์เน็ตซึ่งต้องได้รับการคุ้มครองเมื่ออยู่ในโครงข่ายอินเทอร์เน็ตด้วย และเรียกร้องให้รัฐทุกแห่งเคารพและคุ้มครองสิทธิความเป็นส่วนตัวในการสื่อสารแบบดิจิทัล ทั้งยังเรียกร้องให้รัฐต่าง ๆ ทบทวนขั้นตอนปฏิบัติ การปฏิบัติและกฎหมายที่เกี่ยวข้องกับการสอดแนมข้อมูลการสื่อสาร การดักจับ และการรวบรวมข้อมูลส่วนบุคคล โดยเน้นความจำเป็นที่รัฐต้องประกันให้มีการปฏิบัติตามพันธกรณีของกฎหมายสิทธิมนุษยชนระหว่างประเทศอย่างเต็มที่และเป็นผล

6. ในมติที่ 68/167 สมัชชาใหญ่สหประชาชาติยังร้องขอให้ข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติ ส่งมอบรายงานว่าด้วยการส่งเสริมและคุ้มครองสิทธิความเป็นส่วนตัว ในบริบทของการสอดแนมในประเทศและนอกประเทศและ/หรือการดักจับข้อมูลสื่อสารแบบดิจิทัล และการเก็บข้อมูลส่วนบุคคลรวมทั้งกรณีที่เกิดขึ้นในวงกว้าง ทั้งนี้เพื่อการพิจารณาของคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติในสมัยประชุมที่ 27 และการพิจารณาของสมัชชาใหญ่สหประชาชาติในสมัยประชุมที่ 69 ทั้งนี้เพื่อให้รัฐภาคีได้พิจารณาความเห็นและข้อเสนอแนะต่าง ๆ รายงานฉบับนี้เป็นการส่งมอบตามคำร้องขอดังกล่าว โดยสำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติยังได้ส่งมอบรายงานฉบับนี้ให้กับที่ประชุมสมัยที่ 69 ของสมัชชาใหญ่สหประชาชาติ โดยเป็นไปตามคำร้องขอของสมัชชา และเป็นไปตามมติที่ 68/167 สำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติยังจะส่งมอบรายงานฉบับนี้เพื่อการพิจารณาในสมัยประชุมที่ 69 ของสมัชชาใหญ่

II. ข้อมูลพื้นฐานและวิธีการ

7. เมื่อคำนึงถึงมติที่ 68/167 สำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติได้เข้าร่วมในกิจกรรมหลายครั้งและรวบรวมข้อมูลจากแหล่งต่าง ๆ ในวันที่ 24 กุมภาพันธ์ 2557 ข้าหลวงใหญ่ด้านสิทธิมนุษยชนได้กล่าวนำในการสัมมนาผู้ชำนาญการว่าด้วย “สิทธิความเป็นส่วนตัวในยุคดิจิทัล” ซึ่งเป็นการร่วมจัดโดยประเทศออสเตรีย บราซิล เยอรมนี ลิกเตนสไตน์ เม็กซิโก นอร์เวย์ และสวิตเซอร์แลนด์ โดยมีสถาบันกฎหมายมนุษยธรรมและสิทธิมนุษยชนระหว่างประเทศแห่งเจนีวา (Geneva Academy on International Humanitarian Law and Human Rights) เป็นผู้ประสานงาน

8. นับจากเดือนพฤศจิกายน 2556 ถึงมีนาคม 2557 สำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติร่วมมือกับมหาวิทยาลัยแห่งสหประชาชาติในการทำโครงการวิจัย ว่าด้วยการประยุกต์ใช้กฎหมายสิทธิมนุษยชนระหว่างประเทศสำหรับรัฐบาลในระดับประเทศ ทั้งนี้เพื่อกำกับดูแลการสอดแนมข้อมูลดิจิทัลของรัฐบาล สำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติรู้สึกขอบคุณทางมหาวิทยาลัย ซึ่งมีบทบาทอย่างสำคัญในการจัดเตรียมรายงานฉบับนี้โดยผ่านการทำโครงการวิจัยดังกล่าว

9. ในระหว่างการปรึกษาหารืออย่างเปิดเผยในวันที่ 27 กุมภาพันธ์ 2557 สำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติได้ส่งแบบสอบถามไปยังรัฐภาคี โดยผ่านผู้แทนการทูตถาวรซึ่งประจำอยู่ที่กรุงเจนีวาและนิวยอร์ก หน่วยงานระหว่างประเทศและภูมิภาค สถาบันสิทธิมนุษยชนแห่งชาติ องค์กรพัฒนาเอกชน และหน่วยงานธุรกิจ ในแบบสอบถามดังกล่าว สำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติต้องการรับฟังความเห็นต่อประเด็นที่จะมีอภิปรายโดยสมัชชาใหญ่สหประชาชาติในมติที่ 68/167 และมีการจัดทำหน้าเว็บเป็นการเฉพาะโดยสำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติ ทั้งนี้เพื่อเผยแพร่แบบสอบถามและแสดงความเห็นต่อการปรึกษาหารือกับสาธารณะ รวมทั้งเปิดโอกาสให้มีการเข้ามาแสดงความเห็น เราได้รับข้อมูลจากรัฐภาคี 29 แห่งในทุกภูมิภาค หน่วยงานระหว่างประเทศและ/หรือภูมิภาค 5 แห่ง สถาบันสิทธิมนุษยชนแห่งชาติ 3 แห่ง องค์กรพัฒนาเอกชน 16 แห่ง และหน่วยงานภาคเอกชนอีก 2 แห่ง[2]

10. จากข้อมูลที่ได้รับมาจำนวนมากทำให้ทราบรายละเอียดเกี่ยวกับกรอบกฎหมายระดับประเทศและมาตรการอื่น ๆ ที่มีการนำมาใช้เพื่อประกันการเคารพและการคุ้มครองสิทธิความเป็นส่วนตัวในยุคดิจิทัล รวมทั้งข้อเสนอในการจัดทำและดำเนินการตามมาตรการป้องกันในเชิงขั้นตอนปฏิบัติและการกำกับดูแลที่เป็นผล ข้อมูลที่ได้รับบางส่วนยังชี้ให้เห็นปัญหาท้าทายจากการปฏิบัติตามสิทธิความเป็นส่วนตัวในยุคดิจิทัล และให้ข้อเสนอแนะเกี่ยวกับมาตรการแก้ปัญหาในระดับสากล รวมทั้งการสนับสนุนให้คณะกรรมการสิทธิมนุษยชนปรับปรุงแก้ไขเอกสารความเห็นทั่วไปที่เกี่ยวข้อง โดย

[2] สามารถอ่านความเห็นที่ได้รับทั้งหมดที่ www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

เฉพาะที่เกี่ยวกับข้อ 17 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights-ICCPR) การพัฒนากลไกพิเศษภายใต้คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติที่มีอำนาจหน้าที่เกี่ยวกับสิทธิความเป็นส่วนตัว และ/หรือการมีส่วนร่วมกับกลไกพิเศษที่มีอยู่หรือมาตรการของบุคคลอื่นใดเพื่อแก้ปัญหาที่เกี่ยวข้องกับสิทธิความเป็นส่วนตัวในบริบทของการสอดแนมข้อมูลดิจิทัล และเพื่อเป็นการเสนอแนะแนวปฏิบัติที่ดี

11. จากคำร้องขอในมติสมัชชาใหญ่สหประชาชาติที่ 68/167 รายงานฉบับนี้จึงเสนอข้อพิจารณาและข้อเสนอแนะจากการประเมินข้อมูลเท่าที่มีอยู่ระหว่างการจัดทำรายงาน รวมทั้งการใช้ประโยชน์จากเอกสารมากมายที่ได้รับในระหว่างการขอข้อมูลของฝ่ายต่าง ๆ

III. ปัญหาเกี่ยวกับสิทธิความเป็นส่วนตัวในยุคดิจิทัล

12. จากที่กล่าวถึงโดยสมัชชาใหญ่สหประชาชาติในมติที่ 68/167 กฎหมายสิทธิมนุษยชนระหว่างประเทศกำหนดกรอบสากลที่สามารถใช้ประเมินการแทรกแซงสิทธิความเป็นส่วนตัวของบุคคลได้ ข้อ 12 ของปฏิญญาสากลว่าด้วยสิทธิมนุษยชนกำหนดไว้ว่า “บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว เคหสถาน หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น” กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองซึ่งจนถึงปัจจุบันมีรัฐ 167 แห่งให้สัตยาบันรับรอง กำหนดไว้ในข้อ 17 ว่า “บุคคลจะถูกแทรกแซงความเป็นส่วนตัว ครอบครัว เคหสถาน หรือการติดต่อสื่อสารโดยพลการหรือไม่ชอบด้วยกฎหมายมิได้ และจะถูกลบหลู่เกียรติและชื่อเสียงโดยไม่ชอบด้วยกฎหมายมิได้” ทั้งยังระบุต่อไปว่า “บุคคลทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายมิให้ถูกแทรกแซงหรือลบหลู่เช่นว่านั้น”

13. กฎบัตรสิทธิมนุษยชนระหว่างประเทศอื่น ๆ มีข้อบทที่คล้ายคลึงกัน กฎหมายระดับภูมิภาคและประเทศสะท้อนให้เห็นถึงสิทธิของประชาชนทุกคนที่จะได้รับการเคารพซึ่งชีวิตความเป็นส่วนตัวและครอบครัว เคหสถาน และการติดต่อสื่อสาร หรือสิทธิที่จะได้รับการยอมรับ และการเคารพต่อศักดิ์ศรีของตน บูรณภาพของตนหรือชื่อเสียงเกียรติยศของตน กล่าวอีกอย่างหนึ่ง เป็นการยอมรับอย่างเป็นสากลต่อความสำคัญขั้นพื้นฐานและความเกี่ยวข้องอย่างต่อเนื่องของสิทธิความเป็นส่วนตัว รวมทั้งความจำเป็นที่จะต้องดูแลให้มีการคุ้มครองสิทธิดังกล่าวทั้งในทางกฎหมายและในทางปฏิบัติ

14. แม้ว่ารายงานฉบับนี้มุ่งเน้นที่สิทธิความเป็นส่วนตัว แต่ควรเน้นว่าสิทธิอย่างอื่นย่อมอาจได้รับผลกระทบจากการสอดแนมข้อมูลในวงกว้าง การดักจับข้อมูลสื่อสารแบบดิจิทัลและการเก็บข้อมูลส่วนบุคคล ซึ่งรวมทั้งสิทธิที่จะมีเสรีภาพด้านความเห็นและการแสดงออก และสิทธิที่จะแสวงหา ได้รับ และถ่ายทอดข้อมูล เสรีภาพในการชุมนุมโดยสงบและการสมาคม และการมีชีวิตครอบครัว ซึ่งล้วนเป็นสิทธิที่เกี่ยวข้องอย่างใกล้ชิดกับสิทธิความเป็นส่วนตัว และมีการใช้สิทธิเหล่านี้มากขึ้นโดยผ่านสื่อดิจิทัล สิทธิอย่างอื่นไม่ว่าจะเป็นสิทธิด้านสุขภาพย่อมอาจได้รับผลกระทบจากการสอดแนมข้อมูลดิจิทัลเช่นเดียวกัน ตัวอย่างเช่น บุคคลอาจระวังที่จะแสวงหาหรือเผยแพร่ข้อมูลที่อ่อนไหวในเชิงสุขภาพ เนื่องจากกลัวว่าคนอื่นจะรู้ว่าตนเองเป็นใคร มีแนวโน้มที่น่าเชื่อถือว่าเทคโนโลยีดิจิทัลได้ถูกใช้เพื่อเก็บข้อมูล และเป็นเหตุให้บุคคลถูกทรมานและปฏิบัติอย่างโหดร้าย มีรายงานที่ชี้ว่าคำอธิบายข้อมูล (เมทาดาทา - metadata) ที่ได้มาจากการสอดแนมข้อมูลอิเล็กทรอนิกส์ ได้ถูกนำมาวิเคราะห์เพื่อจำแนกตำแหน่งที่เป็นเป้าหมายการโจมตีให้บุคคลเสียชีวิตโดยใช้อากาศยานไร้พลขับ การโจมตีในลักษณะเช่นนี้ทำให้เกิดข้อกังวลอย่างมากต่อไปเกี่ยวกับการปฏิบัติตามกฎหมายสิทธิมนุษยชนและมนุษยธรรมระหว่างประเทศ และการตรวจสอบการละเมิดใด ๆ ที่เกิดขึ้น ความเชื่อมโยงระหว่างการสอดแนมข้อมูลในวงกว้างกับผลกระทบด้านต่าง ๆ ที่มีต่อสิทธิมนุษยชนเป็นสิ่งที่ควรได้รับการศึกษาเพิ่มเติม แม้จะนอกเหนือจากขอบเขตของรายงานฉบับนี้ก็ตาม

ก. สิทธิที่จะได้รับการคุ้มครองจากการถูกแทรกแซงความเป็นส่วนตัว ครอบครัว เคหสถาน หรือการติดต่อสื่อสารโดยพลการหรือไม่ชอบด้วยกฎหมาย

15. ความเห็นที่ได้รับหลายประการเน้นย้ำว่า การสอดแนมข้อมูลการสื่อสารทางอิเล็กทรอนิกส์หากเป็นการกระทำในกรอบของกฎหมาย รวมทั้งกฎหมายสิทธิมนุษยชนระหว่างประเทศ อาจเป็นมาตรการที่จำเป็นและเป็นผล เพื่อสนับสนุนการบังคับใช้กฎหมายหรืองานข่าวกรองที่ชอบธรรม แต่การเปิดโปงข้อมูลเกี่ยวกับการสอดแนมข้อมูลดิจิทัลในวงกว้าง ทำให้เกิดคำถามว่ามาตรการเหล่านี้สอดคล้องกับมาตรฐานกฎหมายระหว่างประเทศหรือไม่ และจำเป็นต้องมีข้อ

ห้ามที่เข้มงวดมากขึ้นต่อการสอดแนม เพื่อคุ้มครองไม่ให้เกิดการละเมิดสิทธิมนุษยชนหรือไม่ โดยเฉพาะอย่างยิ่งมาตรการสอดแนมข้อมูลจะต้องไม่แทรกแซงความเป็นส่วนตัว ครอบครัว เคหสถาน หรือการติดต่อสื่อสาร โดยพลการหรือโดยไม่ชอบด้วยกฎหมาย รัฐบาลจะต้องดำเนินการอย่างเฉพาะเจาะจงเพื่อประกันให้มีการคุ้มครองทางกฎหมายเพื่อห้ามการแทรกแซงดังกล่าว

16. จากการพิจารณาความเห็นที่ได้รับหลายประการชี้ให้เห็นว่า เพื่อตอบคำถามเหล่านี้ เราจำเป็นต้องประเมินว่า อะไรที่ถือว่าเป็นการแทรกแซงความเป็นส่วนตัวในบริบทการสื่อสารแบบดิจิทัล และอะไรเป็นความหมายของคำว่า "โดยพลการและไม่ชอบด้วยกฎหมาย" และสิทธิของใครที่พึงได้รับการคุ้มครองตามกฎหมายสิทธิมนุษยชนระหว่างประเทศ และคุ้มครองในที่ใด เนื้อหาด้านล่างเป็นการตอบคำถามเหล่านี้ ซึ่งเน้นย้ำในหลายความเห็นที่เราได้รับ

1. การแทรกแซงความเป็นส่วนตัว

17. หน่วยงานตามสนธิสัญญาสิทธิมนุษยชนระหว่างประเทศและภูมิภาค ศาล คณะกรรมาธิการและผู้ชำนาญการอิสระ ต่างมีข้อชี้แนะเชิงปฏิบัติเกี่ยวกับขอบเขตและเนื้อหาที่เกี่ยวข้องกับสิทธิความเป็นส่วนตัว รวมทั้งได้กำหนดนิยามคำว่า "การแทรกแซง" ความเป็นส่วนตัวของบุคคล ในความเห็นทั่วไป ฉบับที่ 16 คณะกรรมการสิทธิมนุษยชนเน้นย้ำการปฏิบัติตามข้อ 17 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง ซึ่งกำหนดให้คุ้มครองบูรณภาพและการเก็บเป็นความลับของข้อมูลการติดต่อสื่อสารทั้งในทางนิตินัยและพฤตินัย "ข้อมูลการติดต่อสื่อสารควรส่งไปยังผู้รับโดยตรงโดยไม่มีการดักจับ และไม่ถูกเปิดออกดู หรือไม่ถูกอ่านเสียก่อน"[3]

18. มีข้อเสนอแนะว่า การส่งและการแลกเปลี่ยนข้อมูลส่วนบุคคลผ่านช่องทางอิเล็กทรอนิกส์ แสดงถึงการยอมประนีประนอมอย่างจงใจ กล่าวคือบุคคลสมัครใจที่จะส่งมอบข้อมูลเกี่ยวกับตนเองและความสัมพันธ์ของตน เพื่อแลกกับการเข้าถึงโลกดิจิทัลและให้ได้มาซึ่งสินค้า บริการ และข้อมูลสนเทศ แต่ก็มีคำถามอย่างจริงจังว่าผู้บริโภคตระหนักดีหรือไม่ว่าข้อมูลที่ตนแลกเปลี่ยนไปนั้นมีขอบเขตมากน้อยเพียงใด แลกเปลี่ยนโดยใช้ช่องทางใด และแลกเปลี่ยนกับใคร และจะมีการนำข้อมูลเหล่านั้นไปใช้ประโยชน์อย่างไร จากรายงานฉบับหนึ่ง "สัจธรรมของข้อมูลขนาดใหญ่ได้แก่ เมื่อมีการเก็บข้อมูลไว้แล้ว ย่อมเป็นเรื่องยากที่จะเก็บข้อมูลส่วนบุคคลของผู้ที่เกี่ยวข้องเป็นความลับ แม้จะมีความพยายามในการวิจัยเพื่อหาทางปกปิดข้อมูลส่วนบุคคลจากชุดข้อมูลขนาดใหญ่เหล่านี้ แต่ในขณะเดียวกันก็มีความพยายามที่ก้าวหน้ามากยิ่งกว่าที่หาทางจำแนกตัวตนของบุคคลที่เกี่ยวข้องกับข้อมูลที่เป็นความลับเช่นนี้ การลงทุนโดยภาพรวมในการส่งเสริมศักยภาพในการจำแนกผู้ที่เกี่ยวข้องกับข้อมูล ดูเหมือนจะมีมากกว่าการลงทุนในเทคโนโลยีเพื่อสนับสนุนความเป็นส่วนตัว" นอกจากนั้น ผู้เขียนรายงานยังมีข้อสังเกตว่า "การเน้นการควบคุมการจัดเก็บและรักษาข้อมูลส่วนบุคคลแม้จะเป็นเรื่องสำคัญ แต่อาจยังไม่เพียงพอที่จะคุ้มครองความเป็นส่วนตัวของบุคคลได้" ส่วนหนึ่งเป็นเพราะ "ข้อมูลขนาดใหญ่ส่งผลให้เกิดการพัฒนาการใช้ข้อมูลแบบใหม่ ซึ่งมีความไม่ชัดเจน และเหนือความคาดหมายมากขึ้น"[4]

19. ในทำนองเดียวกัน มีข้อเสนอแนะว่าการดักจับหรือการเก็บข้อมูลเกี่ยวกับการสื่อสาร โดยไม่ได้เป็นการดักจับหรือเก็บเนื้อหาการสื่อสาร ย่อมไม่อาจถือเป็นการแทรกแซงความเป็นส่วนตัวได้ แต่ความเห็นเช่นนี้ไม่เป็นที่ยอมรับเมื่อมองจากมุมของผู้สนับสนุนสิทธิความเป็นส่วนตัว การเก็บรวบรวมข้อมูลที่เรียกว่าเป็นคำอธิบายข้อมูลหรือเมทาดาทา (metadata) อาจทำให้บุคคลสามารถทราบถึงพฤติกรรม ความสัมพันธ์เชิงสังคม รสนิยมส่วนบุคคล และอัตลักษณ์ส่วนบุคคลได้ ซึ่งเป็นข้อมูลที่มีมากกว่าการวิเคราะห์จากเนื้อหาของการสื่อสารส่วนบุคคลนั้นเสียอีก ดังที่ศาลยุติธรรมแห่งสหภาพยุโรป (European Union Court of Justice) มีข้อสังเกตเมื่อเร็ว ๆ นี้ว่า การสื่อสารคำอธิบายข้อมูล "เมื่อพิจารณาโดยรวมแล้วย่อมทำให้บุคคลสามารถได้ข้อสรุปที่ชัดเจนมาก เกี่ยวกับชีวิตส่วนตัวของบุคคลที่ถูกเก็บข้อมูลมา"[5] จากความ

---

[3] บันทึกอย่างเป็นทางการของสมัชชาใหญ่สหประชาชาติ สมัยประชุมที่ 43, Supplement No. 40 (A/43/40), ภาคผนวก VI, ย่อหน้า 8

[4] สำนักงานบริหารประธานาธิบดีสหรัฐฯ, "ข้อมูลขนาดใหญ่: การฉวยโอกาสและการรักษาคุณค่า - Big Data: Seizing Opportunities, Preserving Values", พฤษภาคม 2557 (จาก http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf), น. 54

[5] ศาลยุติธรรมแห่งสหภาพยุโรป (Court of Justice of the European Union), คำพิพากษาในคดีร่วม (Judgment in Joined Cases) C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, คำพิพากษาวันที่ 8

ตระหนักต่อพัฒนาการในเรื่องนี้เป็นเหตุให้มีความพยายามปฏิรูปนโยบายและการปฏิบัติที่เป็นอยู่ ทั้งนี้เพื่อประกันให้มีการคุ้มครองความเป็นส่วนตัวที่เข้มแข็งมากขึ้น

20. มีความเห็นต่อไปว่าการดักจับข้อมูลการสื่อสารมีแนวโน้มจะเป็นการแทรกแซงความเป็นส่วนตัว และนอกจากนั้น การเก็บและรักษาข้อมูลการสื่อสารเหล่านี้ไว้ ย่อมถือเป็นการแทรกแซงความเป็นส่วนตัว ไม่ว่าจะมีการนำข้อมูลเหล่านั้นไปวิเคราะห์หรือใช้ประโยชน์หรือไม่ก็ตาม แม้แต่ความเป็นไปได้ที่จะมีการดักจับข้อมูลการสื่อสารยังถือว่าเป็นการแทรกแซงความเป็นส่วนตัว[6] โดยอาจส่งผลกระทบร้ายแรงต่อสิทธิประการต่าง ๆ รวมทั้งสิทธิที่จะแสดงออกและสมาคมอย่างเสรี การดำรงอยู่ของโครงการสอดแนมข้อมูลในวงกว้างจึงถือว่าเป็นการแทรกแซงความเป็นส่วนตัว เป็นความรับผิดชอบของรัฐที่จะต้องแสดงให้เห็นว่าการแทรกแซงดังกล่าว เกิดขึ้นโดยไม่มีลักษณะที่เป็นการกระทำโดยพลการหรือไม่ชอบด้วยกฎหมาย

2. "โดยพลการ" หรือ "ไม่ชอบด้วยกฎหมาย" หมายถึงอย่างไร?

21. ตามกฎหมายสิทธิมนุษยชนระหว่างประเทศ การแทรกแซงสิทธิความเป็นส่วนตัวของบุคคลกระทำได้เฉพาะเมื่อไม่เป็นการกระทำโดยพลการหรือไม่ชอบด้วยกฎหมาย ในความเห็นทั่วไป ฉบับที่ 16 คณะกรรมการสิทธิมนุษยชนอธิบายถึงคำว่า "ไม่ชอบด้วยกฎหมาย" ว่ามีนัยหมายถึงการแทรกแซงไม่อาจเกิดขึ้นได้เลย "ยกเว้นเป็นกรณีที่ได้รับอนุญาตตามกฎหมาย การแทรกแซงที่รัฐอนุญาตให้ใช้ได้ต้องเป็นไปบนพื้นฐานของกฎหมาย และตัวกฎหมายดังกล่าวต้องมีความสอดคล้องกับข้อบท เป้าหมาย และวัตถุประสงค์ของกติกานี้"[7] กล่าวอีกอย่างหนึ่ง การแทรกแซงที่กระทำได้ตามกฎหมายในประเทศก็อาจจะ "ไม่ชอบด้วยกฎหมาย" หากกฎหมายในประเทศมีเนื้อหาขัดกับข้อบทของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง ส่วนคำว่า "การแทรกแซงโดยพลการ" ยังอาจครอบคลุมถึงการแทรกแซงที่เป็นไปตามกฎหมาย ในการกล่าวถึงแนวคิดดังกล่าว คณะกรรมการฯ อธิบายว่า "แนวคิดนี้มีเป้าประสงค์เพื่อให้การคุ้มครอง กล่าวคือแม้แต่การแทรกแซงที่เป็นไปตามกฎหมาย ก็ควรสอดคล้องกับข้อบท เป้าหมาย และวัตถุประสงค์ของกติกานี้ และควรชอบด้วยเหตุผลเมื่อพิจารณาถึงพฤติการณ์ที่เกี่ยวข้องไม่ว่าในสถานการณ์ใด ๆ"[8] คณะกรรมการฯ ตีความว่า ความชอบด้วยเหตุผลสะท้อนให้เห็นว่า "การแทรกแซงความเป็นส่วนตัวใด ๆ ต้องมีสัดส่วนเหมาะสมกับผลลัพธ์ที่ต้องการ และต้องมีความจำเป็นเมื่อคำนึงถึงพฤติการณ์ของแต่ละคน"[9]

22. ที่แตกต่างจากข้อบทอื่น ๆ ของกติกานี้ ข้อ 17 ไม่ได้ระบุเงื่อนไขที่เป็นข้อจำกัดอย่างชัดเจน อย่างไรก็ดี เราสามารถหาข้อชี้แนะเกี่ยวกับนิยามของคำว่า "โดยพลการหรือไม่ชอบด้วยกฎหมาย" ได้จากหลักการไซราคูซาว่าด้วยการจำกัดและการลดทอนสิทธิของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights)[10] การปฏิบัติของคณะกรรมการสิทธิมนุษยชนซึ่งสะท้อนให้เห็นจากความเห็นทั่วไปฉบับที่ 16, 27, 29, 34, และ 31 เป็นต้น ข้อวินิจฉัยที่

เมษายน 2557, ย่อหน้า 26-27 และ 37 และโปรดดู สำนักงานบริหารประธานาธิบดีสหรัฐฯ, "Big Data and Privacy: A Technological Perspective" (จาก http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf) น. 19

[6] ดู ศาลสิทธิมนุษยชนแห่งยุโรป (European Court of Human Rights), Weber and Saravia, ย่อหน้า 78; Malone v. UK, ย่อหน้า 64

[7] บันทึกอย่างเป็นทางการของสมัชชาใหญ่สหประชาชาติ (โปรดดู เชิงอรรถ 3), ย่อหน้า 3

[8] อ้างแล้ว ย่อหน้า 4

[9] คำร้อง ฉบับที่ 488/1992, Toonan v Australia, ย่อหน้า 8.3; และดู คำร้อง ฉบับที่ 903/1999, ย่อหน้า 7.3, และ 1482/2006, ย่อหน้า 10.1 และ 10.2

[10] ดู E/CN.4/1985/4, ภาคผนวก

มีต่อคำร้องของบุคคล[11] และข้อสังเกตเชิงสรุป[12] กฎหมายที่เกิดจากการตัดสินคดีทั้งระดับภูมิภาคและประเทศ[13] และความเห็นของผู้ชำนาญการอิสระ[14] ตัวอย่างเช่น ในความเห็นทั่วไป ฉบับที่ 31 ว่าด้วยลักษณะทั่วไปของพันธกรณีด้านกฎหมายของรัฐภาคีที่มีต่อกติกา คณะกรรมการสิทธิมนุษยชนกำหนดว่า รัฐภาคีต้องงดเว้นจากการละเมิดสิทธิที่มีการรับรองในกติกานี้ และ "การจำกัดใด ๆ ซึ่งสิทธิ (เหล่านี้) กระทำได้เฉพาะเมื่อมีข้อบทที่เกี่ยวข้องในกติกานี้ กรณีที่มีการจำกัดสิทธิดังกล่าว รัฐต้องแสดงให้เห็นถึงความจำเป็น และต้องดำเนินมาตรการดังกล่าวโดยมีสัดส่วนเหมาะสมเพื่อบรรลุเป้าหมายอันควร และทั้งนี้เพื่อประกันให้มีการคุ้มครองสิทธิตามกติกานี้อย่างต่อเนื่องและอย่างเป็นผล"[15] คณะกรรมการฯ ยังเน้นต่อไปว่า "ไม่ว่าในพฤติการณ์ใด ๆ ไม่อนุญาตให้มีการจำกัดสิทธิหรืออ้างที่จะกำจัดสิทธิ หากการกระทำเช่นนั้นส่งผลกระทบต่อสารัตถะของสิทธิในกติกานี้"

23. แหล่งข้อมูลอย่างเป็นทางการเหล่านี้แสดงให้เห็นหลักการพื้นฐานว่าด้วยความชอบด้วยกฎหมาย ความจำเป็น และความได้สัดส่วน เป็นสาระสำคัญที่มีการเน้นย้ำจากการรับฟังความเห็นที่เราได้รับมา ตั้งแต่การจำกัดสิทธิความเป็นส่วนตัวที่ปรากฏอยู่ในข้อ 17 ต้องกระทำเมื่อมีกฎหมายอนุญาตเท่านั้น และกฎหมายดังกล่าวต้องสามารถเข้าถึงได้ ชัดเจน และเฉพาะเจาะจงอย่างเพียงพอ เพื่อช่วยให้บุคคลสามารถพิจารณาจากตัวบทและวินิจฉัยได้อย่างแน่นอนว่าใครเป็นผู้มีอำนาจในการสอดแนมข้อมูล และจะกระทำได้ภายใต้พฤติการณ์ใด การจำกัดสิทธิจะกระทำได้เท่าที่จำเป็นเพื่อเป้าหมายอันควร รวมทั้งได้สัดส่วนกับเป้าหมายและเป็นทางเลือกที่เป็นการละเมิดสิทธิน้อยสุด[16] นอกจากนั้น การจำกัดสิทธิใด ๆ (อย่างเช่น การแทรกแซงความเป็นส่วนตัวเพื่อเป้าประสงค์ในการคุ้มครองความมั่นคงแห่งชาติ หรือสิทธิที่จะมีชีวิตรอดของบุคคลอื่น) จะกระทำได้เมื่อมีการพิสูจน์ให้เห็นว่ามีโอกาสจะบรรลุเป้าหมายดังกล่าว เป็นภาระของทางการที่ต้องการจำกัดสิทธิเหล่านั้นที่จะต้องแสดงให้เห็นว่า การจำกัดสิทธิมีส่วนเชื่อมโยงกับเป้าหมายอันควร นอกจากนั้น การจำกัดสิทธิความเป็นส่วนตัวใด ๆ ต้องไม่กระทบต่อสารัตถะของสิทธิดังกล่าว และต้องสอดคล้องกับสิทธิมนุษยชนอื่น ๆ รวมทั้งข้อห้ามต่อการเลือกปฏิบัติ กรณีที่เป็นการจำกัดซึ่งไม่สอดคล้องกับหลักเกณฑ์เหล่านี้ ย่อมถือเป็นการจำกัดสิทธิที่ไม่ชอบด้วยกฎหมาย และ/หรือเป็นการแทรกแซงสิทธิความเป็นส่วนตัวโดยพลการ

24. รัฐบาลมักสร้างความชอบธรรมให้กับโครงการสอดแนมการสื่อสารข้อมูลดิจิทัล โดยอ้างเหตุผลด้านความมั่นคงแห่งชาติ รวมทั้งความเสี่ยงจากลัทธิก่อการร้าย ความเห็นที่เราได้รับมาหลายประการชี้ว่า เนื่องจากที่ผ่านมาเทคโนโลยีการสื่อสารแบบดิจิทัลอาจถูกใช้และได้ถูกใช้โดยบุคคลเพื่อวัตถุประสงค์ที่เป็นอาชญากรรม (รวมทั้งการได้มาซึ่งผู้ปฏิบัติงาน และการสนับสนุนเงินและการมอบหมายให้ปฏิบัติการก่อการร้าย) ด้วยเหตุดังกล่าว การสอดแนมข้อมูลการสื่อสารแบบดิจิทัลที่ชอบด้วยกฎหมายและมีเป้าหมายเฉพาะเจาะจง อาจเป็นมาตรการที่จำเป็นและเป็นผลสำหรับหน่วยงานด้านข่าวกรองและ/หรือหน่วยงานบังคับใช้กฎหมาย หากมีการปฏิบัติที่สอดคล้องกับกฎหมายระหว่างประเทศและในประเทศ การสอดแนมข้อมูลด้วยเหตุผลความมั่นคงแห่งชาติและเพื่อป้องกันลัทธิก่อการร้ายหรืออาชญากรรมอื่น ๆ อาจเป็น "เป้าหมายอันควร" เมื่อประเมินจากความเห็นที่สะท้อนในข้อ 17 ของกติกานี้ อย่างไรก็ดี ต้องมีการประเมินระดับของการแทรกแซง เปรียบเทียบกับความจำเป็นของมาตรการเพื่อให้บรรลุเป้าประสงค์ดังกล่าว กับผลประโยชน์ที่จะเกิดขึ้นจริงจากการปฏิบัติเช่นนั้น

---

[11] ตัวอย่างเช่น คำร้อง ฉบับที่ 903/1999, 2004, Van Hulst v. The Netherlands

[12] CCPR /C/USA/CO/4

[13] ตัวอย่างเช่น ศาลสิทธิมนุษยชนแห่งยุโรป, Uzun v. Germany, 2 กันยายน 2553 และ Weber and Soravia v. Germany, ย่อหน้า 4; และศาลสิทธิมนุษยชนแห่งทวีปอเมริกา (Inter-American Court of Human Rights), Escher v. Brazil, คำพิพากษา วันที่ 20 พฤศจิกายน 2552

[14] ดู A/HRC/13/37 และ A/HRC/23/40. และดู International Principles on the Application of Human Rights to Communications Surveillance, จาก https://en.necessaryandproportionate.org/text (ฉบับแปลภาษาไทย: หลักการระหว่างประเทศว่าด้วยการใช้หลักสิทธิมนุษยชนกับการสอดแนมการสื่อสาร https://th.necessaryandproportionate.org/text – ผู้แปล)

[15] CCPR/C/21/Rev.1/Add.13, ย่อหน้า 6

[16] CCPR/C/21/Rev.1/Add.9, ย่อหน้า 11 – 16. และดู A/HRC/14/46, ภาคผนวก, practice 20

25. ในการประเมินความจำเป็นของมาตรการ คณะกรรมการสิทธิมนุษยชนในความเห็นทั่วไป ฉบับที่ 27 ว่าด้วยข้อ 12 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง เน้นย้ำว่า “การจำกัดสิทธิดังกล่าวจะต้องไม่กระทบต่อสารัตถะของสิทธินั้น […] และต้องไม่ส่งผลกระทบต่อความสัมพันธ์ระหว่างสิทธิกับการจำกัด และระหว่างบรรทัดฐานกับข้อยกเว้น จนทำให้เป็นความสัมพันธ์แบบสลับข้างกัน”[17] คณะกรรมการฯ อธิบายต่อไปว่า “ยังไม่พอที่การจำกัดสิทธิอาจตอบสนองเป้าประสงค์ที่ชอบด้วยกฎหมาย หากยังต้องมีความจำเป็นเพื่อคุ้มครองเป้าประสงค์ดังกล่าวด้วย” นอกจากนั้น มาตรการดังกล่าวต้องมีสัดส่วนเหมาะสม “โดยเป็นกลไกที่มีการแทรกแซงน้อยสุดและยังอาจสามารถบรรลุผลลัพธ์ที่ต้องการได้”[18] กรณีที่มีเป้าหมายอันควรและมีมาตรการคุ้มครองสิทธิที่เหมาะสม รัฐอาจสามารถปฏิบัติการสอดแนมข้อมูลในเชิงรุกได้ เพียงแต่รัฐบาลมีภาระต้องพิสูจน์ให้เห็นว่าการแทรกแซงเช่นนั้นมีความจำเป็นและมีสัดส่วนเหมาะสมกับภารกิจที่ต้องการปฏิบัติ โครงการสอดแนมข้อมูลในวงกว้าง หรือ “เหวี่ยงแห” จึงอาจต้องถือว่าเป็นการกระทำโดยพลการ แม้จะมีเป้าหมายอันควร และแม้จะเป็นการนำมาปฏิบัติบนพื้นฐานของกรอบกฎหมายที่เข้าถึงได้ กล่าวอีกอย่างหนึ่ง การใช้มาตรการที่มีเป้าหมายเพียงเพื่อค้นหาเข็มบางเล่มในกองฟางอาจไม่เพียงพอ จำเป็นต้องมีการประเมินผลกระทบต่อกองฟางอันเนื่องมาจากการใช้มาตรการเหล่านั้น โดยคำนึงถึงอันตรายที่อาจจะเกิดขึ้นด้วย เพื่อตัดสินว่ามาตรการนั้นมีความจำเป็นและมีสัดส่วนเหมาะสมหรือไม่

26. ความกังวลว่าการเข้าถึงและการใช้ข้อมูลได้ถูกออกแบบเพื่อตอบสนองเป้าหมายตามกฎหมาย ทำให้เกิดคำถามเกี่ยวกับการพึ่งพามากขึ้นของรัฐบาลต่อหน่วยงานเอกชน เพื่อให้เก็บรักษาข้อมูลไว้ “เผื่อว่า” จะตอบสนองเป้าประสงค์ของรัฐบาล ทั้ง ๆ ที่ข้อบังคับให้เก็บรักษาข้อมูลของบุคคลที่สามไว้ดูเหมือนจะไม่จำเป็นหรือไม่มีสัดส่วนเหมาะสมเลย แต่ที่ผ่านมาหลายรัฐได้กำหนดข้อบังคับดังกล่าวเป็นส่วนหนึ่งของการสอดแนมข้อมูล กล่าวคือรัฐบาลกำหนดให้บริษัทโทรศัพท์และอินเทอร์เน็ตเก็บคำอธิบายข้อมูล (metadata) เกี่ยวกับการสื่อสารของลูกค้าและที่อยู่ของลูกค้าเอาไว้เพื่อประโยชน์ในการบังคับใช้กฎหมายและการเข้าถึงข้อมูลของหน่วยข่าวกรอง[19]

27. ปัจจัยหนึ่งที่ต้องคำนึงถึงเพื่อจำแนกความได้สัดส่วน ได้แก่ จะจัดการกับข้อมูลแบบเหวี่ยงแหอย่างไรและใครจะเป็นผู้เข้าถึงข้อมูลหลังจากจัดเก็บแล้ว กรอบกฎหมายระดับประเทศหลายแห่งไม่มี “ข้อจำกัดในการใช้งาน” แต่กลับอนุญาตให้เก็บข้อมูลเพื่อเป้าประสงค์ทางกฎหมายอย่างหนึ่ง แต่ในภายหลังนำข้อมูลนั้นไปใช้เพื่อเป้าประสงค์อย่างอื่น สภาพที่ขาดการจำกัดการใช้ข้อมูลอย่างเป็นผลเลวร้ายลงหลังจากเหตุการณ์ 11 กันยายน 2544 ทำให้เกิดเส้นแบ่งที่คลุมเครือเป็นอย่างมากระหว่างความยุติธรรมทางอาญากับการปกป้องความมั่นคงแห่งชาติ ส่งผลให้มีการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานบังคับใช้กฎหมาย หน่วยงานข่าวกรอง และหน่วยงานของรัฐอื่น ๆ ซึ่งเสี่ยงจะละเมิดข้อ 17 ของกติกานี้ เนื่องจากมาตรการสอดแนมข้อมูลที่อาจจำเป็นและได้สัดส่วนเหมาะสมเพื่อเป้าประสงค์ทางกฎหมายอย่างหนึ่งอาจไม่เป็นเช่นนั้นหากนำไปใช้เพื่อเป้าประสงค์อย่างอื่น จากการศึกษาการเข้าถึงข้อมูลของบุคคลที่สามของรัฐบาลทำให้เราพบว่า “ยิ่งหน่วยงานความมั่นคงแห่งชาติและหน่วยงานบังคับใช้กฎหมายสามารถเข้าถึงและใช้ประโยชน์ของภาคเอกชนได้ง่ายมากขึ้นเท่าไร ยิ่งส่งผลให้หน่วยงานเหล่านั้นมีเสรีภาพในการแลกเปลี่ยนข้อมูลมากยิ่งขึ้น และมีการนำไปใช้เพื่อเป้าประสงค์อื่น ๆ นอกเหนือจากเป้าประสงค์ที่กำหนดไว้ตอนที่เก็บข้อมูลเหล่านั้น และทำให้มาตรการคุ้มครองข้อมูล

---

[17] CCPR/C/21/Rev.1/Add.9, ย่อหน้า 11 – 16. และดู ศาลสิทธิมนุษยชนแห่งยุโรป, Handyside v. the United Kingdom, ย่อหน้า 48; and Klass v. Germany, ย่อหน้า 42

[18] CCPR/C/21/Rev.1/Add.9, ย่อหน้า 11 – 16

[19] ดู ความเห็นของพนักงานอัยการ Cruz Villalón ศาลยุติธรรมแห่งสหภาพยุโรปในคดีฟ้องร่วม เลขที่ C-293/12 และ C-594/12 ซึ่งชี้ว่ากฎหมายระเบียบ (Directive) ที่ 2006/24/EU (เกี่ยวกับการเก็บรักษาข้อมูลที่เกิดจากหรือผ่านกระบวนการการให้บริการการสื่อสารทางอิเล็กทรอนิกส์) เป็นคำสั่งที่ “โดยรวมแล้ว” ละเมิดธรรมนูญว่าด้วยสิทธิขั้นพื้นฐานของสหภาพยุโรป (Charter of Fundamental Rights of the European Union) ทั้งนี้เพราะไม่มีการจำกัดการเก็บรักษาข้อมูลอย่างเข้มงวด และโปรดดู CCPR/C/USA/CO/4, ย่อหน้า 22

แบบดั้งเดิมอ่อนแอลง"[20] ในรัฐหลายแห่ง ศาลได้อ้างเหตุผลดังกล่าวเพื่อยับยั้งกรอบกฎหมายที่อนุญาตให้แลกเปลี่ยนข้อมูล และมีข้อเสนอแนะว่าการจำกัดการใช้ประโยชน์ของข้อมูลเช่นนี้เป็นแนวปฏิบัติที่ดี เพื่อประกันให้รัฐปฏิบัติตามพันธกรณีของตนตามข้อ 17 ของกติกานี้อย่างเป็นผล[21] และกำหนดให้มีการลงโทษอย่างจริงจังหากมีการละเมิด

ข. การคุ้มครองตามกฎหมาย

28. ย่อหน้า 2 ของข้อ 17 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองกำหนดอย่างชัดเจนว่า บุคคลทุกคนมีสิทธิที่จะได้รับการคุ้มครองตามกฎหมายมิให้ถูกแทรกแซงความเป็นส่วนตัวโดยไม่ชอบด้วยกฎหมายหรือโดยพลการ ซึ่งหมายถึงว่า โครงการสอดแนมการสื่อสารใด ๆ ต้องดำเนินไปบนพื้นฐานกฎหมายที่เข้าถึงได้อย่างเปิดเผย และย่อมสอดคล้องกับกรอบตามรัฐธรรมนูญของตนและกฎหมายสิทธิมนุษยชนระหว่างประเทศ[22] "การเข้าถึงได้" ไม่ได้หมายถึงเฉพาะมีการตีพิมพ์เผยแพร่กฎหมาย แต่หมายถึงมีเนื้อหาชัดเจนมากพอที่จะช่วยให้บุคคลที่ได้รับผลกระทบควบคุมพฤติกรรมของตนเองได้ โดยตระหนักถึงผลลัพธ์ที่จะเกิดขึ้นจากการกระทำบางอย่างของตน รัฐต้องประกันว่า การแทรกแซงใด ๆ ต่อความเป็นส่วนตัว ครอบครัว เคหสถานหรือการติดต่อสื่อสาร ต้องเป็นไปตามกรอบกฎหมายที่ (ก) เข้าถึงได้อย่างเปิดเผย (ข) มีตัวบทซึ่งประกันให้มีการออกแบบการเก็บ เข้าถึง และใช้ประโยชน์จากข้อมูลการสื่อสารเพื่อตอบสนองเป้าประสงค์ที่ชอบด้วยกฎหมายอย่างชัดเจน (ค) มีเนื้อหาชัดเจนมากเพียงพอพร้อมกับกำหนดเงื่อนไขอย่างเฉพาะเจาะจงว่าการแทรกแซงดังกล่าวอาจเกิดขึ้นได้ในกรณีใด ต้องผ่านขั้นตอนการอนุมัติแบบใด บุคคลประเภทใดที่อาจตกเป็นเป้าหมายการสอดแนม ข้อจำกัดด้านระยะเวลาของการสอดแนม และการใช้และเก็บรักษาข้อมูล และ (ง) กำหนดมาตรการคุ้มครองที่เป็นผลเพื่อไม่ให้เกิดการปฏิบัติมิชอบ[23]

29. ในลำดับต่อมา ระเบียบลับและการตีความกฎหมายแบบลับ หรือกระทั่งการตีความของศาลแบบลับ ถือว่าไม่มีคุณสมบัติที่จำเป็นในฐานะเป็น "กฎหมาย"[24] ทั้งกฎหมายหรือระเบียบต้องไม่ให้อำนาจวินิจฉัยอย่างเกินขอบเขตกับหน่วยงานฝ่ายบริหาร ไม่ว่าจะเป็นหน่วยงานความมั่นคงและข่าวกรอง กล่าวคือในกฎหมายหรือระเบียบนั้นต้องมีตัวบทที่แสดงอย่างชัดเจนถึงขอบเขตและลักษณะการใช้อำนาจวินิจฉัยนั้น (ทั้งในตัวกฎหมายเอง หรือในแนวปฏิบัติที่มีผลบังคับใช้และมีการประกาศใช้) พร้อมกับแสดงความชอบด้วยเหตุผลที่ชัดเจน กฎหมายที่เข้าถึงได้แต่ไม่ทำให้เห็นผลลัพธ์ที่ชัดเจน ย่อมถือว่าบกพร่อง อำนาจการสอดแนมแบบปิดลับมักทำให้เกิดความเสี่ยงมากขึ้นต่อการใช้อำนาจวินิจฉัยโดยพลการ ซึ่งในกรณีเช่นนั้นจำเป็นต้องมีระเบียบที่เฉพาะเจาะจงเพื่อควบคุมการใช้อำนาจวินิจฉัยเช่นนั้น และให้มีการกำกับดูแลเพิ่มเติม รัฐหลายแห่งยังกำหนดให้กรอบกฎหมายในลักษณะเช่นนี้ต้องจัดทำขึ้นตามพื้นฐานกฎหมายที่ผ่านการพิจารณาของรัฐสภา แทนที่จะเป็นกฎหมายลูกที่ฝ่ายบริหารเป็นผู้ประกาศใช้ ข้อกำหนดดังกล่าวช่วยประกันว่ากรอบกฎหมายเช่นนี้ไม่เพียงจะเข้าถึงได้สำหรับประชาชนที่เกี่ยวข้องหลังมีการประกาศใช้ หากยังสามารถเข้าถึงได้ในช่วงที่มีการแก้ไขเพิ่มเติม ทั้งนี้โดยเป็นไปตามข้อ 25 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง[25]

30. ข้อกำหนดให้เข้าถึงได้ยังเกี่ยวข้องกับการประเมินแนวโน้มที่รัฐมักมอบหมายให้หน่วยงานอื่น ๆ สอดแนมข้อมูลแทน มีข้อมูลที่น่าเชื่อถือได้ว่า รัฐบาลบางแห่งใช้ประโยชน์อย่างเป็นระบบจากการเก็บและวิเคราะห์ข้อมูล โดยเลือกปฏิบัติการในเขตอำนาจที่มีมาตรการคุ้มครองความเป็นส่วนตัวอ่อนแอกว่า มีรายงานว่า รัฐบาลบางแห่งอาศัยช่องว่างของ

---

[20] Fred H. Cate, James X. Dempsey and Ira S. Rubinstein, "การเข้าถึงข้อมูลของภาคเอกชนอย่างเป็นระบบโดยรัฐบาล - Systematic government access to private- sector data", International Data Privacy Law, vol. 2, No. 4, 2012, น. 198

[21] ดู A/HRC/14/46, ภาคผนวก, practice 23

[22] ดู อ้างแล้ว ภาคผนวก

[23] CCPR /C/USA/CO/4, ย่อหน้า 22. และโปรดดู ศาลสิทธิมนุษยชนแห่งยุโรป, Malone v the United Kingdom, No. 8691/79, 2 สิงหาคม 2527, ย่อหน้า 67 และ 68; และ Weber and Saravia v Germany, คำร้องที่ 54934/00, 29 มิถุนายน 2549 ซึ่งศาลระบุมาตรการคุ้มครองขั้นต่ำที่ต้องกำหนดไว้ในกฎหมายระดับพระราชบัญญัติ

[24] ดู CCPR /C/USA/CO/4, ย่อหน้า 22

[25] และดู A/HRC/14/46

กฎหมายที่เชื่อมโยงกันเกี่ยวกับการประสานงานเพื่อการสอดแนมข้อมูล เพื่อใช้ประโยชน์จากเครือข่ายหน่วยข่าวกรองข้ามชาติ ทั้งนี้เพื่อเอาชนะข้อจำกัดในการคุ้มครองสิทธิในประเทศของรัฐบาล การปฏิบัติเช่นนี้ย่อมไม่สอดคล้องกับความชอบด้วยกฎหมาย ทั้งนี้เพราะดังที่ความเห็นซึ่งเราได้รับมาในรายงานฉบับนี้เสนอว่า จะทำให้บุคคลที่ได้รับผลกระทบไม่ตระหนักถึงการปฏิบัติงานของระบบสอดแนมข้อมูลที่ไม่ทราบผลลัพธ์ ซึ่งอาจเป็นการละเมิดสารัตถะของสิทธิที่ได้รับการคุ้มครองตามข้อ 17 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง และถูกห้ามไม่ให้ปฏิบัติตามข้อ 5 รัฐหลายแห่งไม่ได้ดำเนินมาตรการที่เป็นผลเพื่อคุ้มครองบุคคลในเขตอำนาจศาลของตน ให้ปลอดพ้นจากการสอดแนมข้อมูลอย่างผิดกฎหมายที่กระทำโดยสหรัฐฯ หรือหน่วยธุรกิจอื่น ๆ ซึ่งเท่ากับเป็นการละเมิดพันธกรณีด้านสิทธิมนุษยชนของตนเอง

ค. คุ้มครองใครและที่ไหน?

31. จากความเห็นที่ได้รับหลายประการ มีการกล่าวถึงการประยุกต์ใช้กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองนอกพรมแดนประเทศ แม้เป็นที่ชัดเจนว่าโครงการสอดแนมข้อมูลดิจิทัลที่ถูกเปิดโปงเมื่อเร็ว ๆ นี้ น่าจะกระตุ้นให้เกิดคำถามต่อพันธกรณีในพรมแดนของตนสำหรับรัฐซึ่งทำการสอดแนมข้อมูล แต่มีการแสดงข้อกังวลเพิ่มเติมเกี่ยวกับการสอดแนมข้อมูลและการดักจับข้อมูลการสื่อสารนอกพรมแดนของตน

32. ข้อ 2 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองกำหนดให้รัฐภาคีแต่ละรัฐแห่งกติกานี้รับที่จะเคารพและประกันแก่ปัจเจกบุคคลทั้งปวง ภายในดินแดนของตนและภายใต้เขตอำนาจของตน ในสิทธิทั้งหลายที่รับรองไว้ในกติกานี้ โดยปราศจากการแบ่งแยกใด ๆ อาทิ เชื้อชาติ ผิว เพศ ภาษา ศาสนา ความคิดเห็นทางการเมืองหรือความคิดเห็นอื่นใด เผ่าพันธุ์แห่งชาติหรือสังคม ทรัพย์สิน กำเนิด หรือสถานะอื่น ๆ คณะกรรมการสิทธิมนุษยชนในความเห็นทั่วไป ฉบับที่ 31 ยืนยันว่า รัฐภาคีต้องปฏิบัติตามข้อ 2 ย่อหน้า 1 เพื่อเคารพและประกันแก่ปัจเจกบุคคลทั้งปวง ภายในดินแดนของตนและภายใต้เขตอำนาจของตน ในสิทธิทั้งหลายที่รับรองไว้ในกติกานี้ ซึ่งหมายถึงว่า รัฐภาคีต้องเคารพและประกันให้บุคคลใด ๆ ในอำนาจหรือการควบคุมโดยปริยายของตนต้องได้รับสิทธิตามที่บัญญัติในกติกานี้ แม้ว่าบุคคลดังกล่าวจะมิได้อยู่ในพรมแดนของรัฐภาคีนั้น[26] เป็นการขยายสิทธิไปถึงบุคคลที่อยู่ภายใต้ “อำนาจ” ของรัฐ[27]

33. คณะกรรมการสิทธิมนุษยชนได้รับฟังหลักการเหล่านี้ และได้แสดงความเห็นในแนวนิติศาสตร์ตั้งแต่เริ่มต้นของตนว่า รัฐไม่อาจหลีกเลี่ยงพันธกรณีสิทธิมนุษยชนระหว่างประเทศ โดยดำเนินการภายนอกพรมแดนประเทศของตน โดยที่การดำเนินการนั้นเป็นข้อห้ามตามกฎหมาย “ในประเทศของตน”[28] จุดยืนเช่นนี้สอดคล้องกับความเห็นของศาลยุติธรรมระหว่างประเทศซึ่งยืนยันว่า กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองมีผลบังคับใช้ต่อการกระทำของรัฐ “ทั้งที่เป็นการใช้อำนาจนอกพรมแดนประเทศตนเอง”[29] ในทำนองเดียวกับข้อ 31 และ 32 ของอนุสัญญาเวียนนาว่าด้วยกฎหมายสนธิสัญญา (Vienna Convention on the Law of Treaties) แนวคิดเรื่อง “อำนาจ” และ “การควบคุมโดยปริยาย” เป็นปัจจัยบ่งชี้ว่ารัฐได้ใช้ “เขตอำนาจ” หรืออำนาจปกครองของตนอย่างไร โดยที่มาตรการคุ้มครองสิทธิมนุษยชนมีเป้าประสงค์เพื่อควบคุมมิให้มีการปฏิบัติมิชอบในการใช้อำนาจดังกล่าว รัฐจึงไม่อาจหลีกเลี่ยงความรับผิด

---

[26] CCPR/C/21/Rev.1/Add.13, ย่อหน้า 10

[27] ดู บันทึกอย่างเป็นทางการของสมัชชาใหญ่สหประชาชาติ สมัยประชุมที่ 39, Supplement No. 40 (A/36/40), ภาคผนวก XIX, ย่อหน้า 12.2; และโปรดดู ภาคผนวก XX. และดู CCPR/CO/78/ISR, ย่อหน้า 11; CCPR/CO/72/NET, ย่อหน้า 8; CCPR/CO/81/BEL, ย่อหน้า 6; และคณะกรรมการสิทธิมนุษยชนแห่งทวีปอเมริกา (Inter-American Commission of Human Rights), Coard และคณะ v. สหรัฐฯ, case No. 10.951, Report No. 109/99, 29 กันยายน 2542, ย่อหน้า 37, 39, 41 และ 43

[28] ดู บันทึกอย่างเป็นทางการของสมัชชาใหญ่สหประชาชาติ สมัยประชุมที่ 39 (โปรดดู เชิงอรรถ 27), ภาคผนวก XIX, ย่อหน้า 12.2-12.3, และภาคผนวก XX, ย่อหน้า 10.3

[29] ความเห็นเชิงให้คำปรึกษาของศาลยุติธรรมระหว่างประเทศเกี่ยวกับผลด้านกฎหมายของการสร้างกำแพงกั้นในเขตยึดครองปาเลสไตน์ (Occupied Palestinian Territory) 9 กรกฎาคม 2547 (A/ES-10/273 และ Corr.1), ย่อหน้า 107-111. และดู ศาลยุติธรรมระหว่างประเทศ, คดีเกี่ยวกับกิจกรรมการใช้อาวุธในดินแดนของคองโก (Democratic Republic of the Congo v. Uganda), คำพิพากษา 2548, น. 168

ชอบด้านสิทธิมนุษยชนของตน โดยงดเว้นจากการใช้อำนาจภายใต้ขอบเขตของกฎหมายได้ ข้อสรุปที่เป็นอย่างอื่นไม่เพียงทำลายหลักความเป็นสากลและสารัตถะของสิทธิซึ่งได้รับการคุ้มครองตามกฎหมายสิทธิมนุษยชนระหว่างประเทศเท่านั้น หากยังกลายเป็นแรงกระตุ้นเชิงโครงสร้างให้รัฐกระตุ้นให้รัฐแห่งอื่นทำหน้าที่สอดแนมข้อมูลแทนตน

34. ด้วยเหตุดังกล่าว การสอดแนมข้อมูลดิจิทัลอาจเกี่ยวข้องกับพันธกรณีด้านสิทธิมนุษยชนของรัฐ หากการสอดแนมเช่นนั้นเกี่ยวข้องกับการใช้อำนาจหรือการควบคุมโดยปริยายของรัฐ ที่กระทำต่อโครงสร้างพื้นฐานการสื่อสารแบบดิจิทัล หากพบว่าเกิดกรณีดังกล่าวขึ้น ตัวอย่างเช่นการดักจับข้อมูลโดยตรงหรือการล่วงล้ำเข้าไปในโครงสร้างพื้นฐานการสื่อสารนั้น ในทำนองเดียวกัน กรณีที่รัฐใช้อำนาจกำกับดูแลบุคคลที่สามซึ่งควบคุมข้อมูลในเชิงกายอยู่นั้น รัฐก็ต้องมีพันธกรณีตามกติกานี้เช่นกัน กรณีที่ประเทศหนึ่งประกาศเขตอำนาจเหนือข้อมูลของบริษัทเอกชน โดยอ้างว่าบริษัทดังกล่าวจดทะเบียนในประเทศ ในทำนองเดียวกันรัฐก็ต้องให้ความคุ้มครองด้านสิทธิมนุษยชนต่อบุคคลที่ถูกแทรกแซงความเป็นส่วนตัว ไม่ว่าบุคคลนั้นจะอยู่ในประเทศที่บริษัทดังกล่าวจดทะเบียนหรืออยู่ในประเทศอื่น หลักการเช่นนี้เป็นสิ่งที่ต้องกระทำไม่ว่าการประกาศเขตอำนาจนั้นจะชอบด้วยกฎหมายในเบื้องต้นหรือไม่ หรือเป็นการละเมิดอธิปไตยของรัฐอื่น

35. ข้อสรุปเช่นนี้มีความสำคัญเช่นเดียวกัน เมื่อพิจารณาถึงการอภิปรายที่กำลังเกิดขึ้นว่า “คนต่างชาติ” และ “พลเมือง” ควรสามารถเข้าถึงการคุ้มครองความเป็นส่วนตัวอย่างเท่าเทียมกัน เมื่อคำนึงถึงกรอบกำกับดูแลการสอดแนมข้อมูลด้านความมั่นคง ระบบกฎหมายหลายแห่งแยกแยะพันธกรณีที่ต้องปฏิบัติต่อคนชาติของตนหรือผู้ที่อาศัยอยู่ในดินแดนของรัฐ ออกจากผู้ที่ไม่ใช่คนชาติและผู้ที่อาศัยอยู่นอกประเทศ[30] หรืออาจกำหนดระดับการคุ้มครองที่ต่ำกว่าสำหรับการสื่อสารของคนต่างชาติหรือที่เกิดขึ้นนอกประเทศ หากมีความไม่ชัดเจนว่าเป็นข้อมูลต่างชาติหรือในประเทศ หน่วยข่าวกรองมักปฏิบัติราวกับข้อมูลนั้นเป็นของต่างชาติ (เนื่องจากการสื่อสารแบบดิจิทัลมักเกิดขึ้นโดยผ่านช่องทาง “นอกประเทศ”) และอนุญาตให้มีการเก็บและรักษาข้อมูลเหล่านั้นไว้ได้ ส่งผลให้เกิดความอ่อนแอหรือแทบจะไม่มีการคุ้มครองความเป็นส่วนตัวของคนต่างชาติและผู้ที่ไม่ใช่พลเมืองของตน เมื่อเปรียบเทียบกับพลเมืองของตน

36. กฎหมายสิทธิมนุษยชนระหว่างประเทศกำหนดอย่างชัดเจนเกี่ยวกับหลักการไม่เลือกปฏิบัติ ข้อ 26 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองกำหนดว่า “บุคคลทั้งปวงย่อมเสมอกันตามกฎหมาย และมีสิทธิที่จะได้รับความคุ้มครองอย่างไม่เลือกปฏิบัติตามกฎหมาย” และยังกำหนดด้วยว่า “ในกรณีนี้ กฎหมายจะต้องห้ามการเลือกปฏิบัติใด ๆ และต้องประกันการคุ้มครองบุคคลทุกคนอย่างเสมอภาคและเป็นผลจริงจังจากการเลือกปฏิบัติด้วยเหตุผลใด เช่น เชื้อชาติ ผิว เพศ ภาษา ศาสนา ความคิดเห็นทางการเมืองหรือความคิดเห็นอื่นใด เผ่าพันธุ์แห่งชาติหรือสังคม ทรัพย์สิน กำเนิด หรือสถานะอื่น ๆ” ข้อกำหนดเหล่านี้ควรพิจารณาไปพร้อมกับข้อ 17 ที่ระบุว่า “บุคคลจะต้องไม่ถูกแทรกแซงโดยพลการต่อความเป็นส่วนตัวของตน” และ “บุคคลทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายมิให้ถูกแทรกแซงหรือลบหลู่เช่นว่านั้น” รวมทั้งข้อ 2 ย่อหน้า 1 ด้วยเหตุดังกล่าว คณะกรรมการสิทธิมนุษยชนเน้นย้ำความสำคัญของ “มาตรการเพื่อประกันว่าการแทรกแซงสิทธิความเป็นส่วนตัวใด ๆ ต้องเป็นไปตามหลักการความชอบด้วยกฎหมาย ความได้สัดส่วน และความจำเป็น ไม่ว่าบุคคลที่ตกเป็นเป้าหมายการสอดแนมข้อมูลการสื่อสารโดยตรงจะมีสัญชาติหรืออยู่ในถิ่นที่อยู่ใด”[31]

ง. ขั้นตอนปฏิบัติเพื่อคุ้มครองและกำกับดูแลอย่างเป็นผล

37. ข้อ 17 ย่อหน้า 2 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองระบุว่า บุคคลทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายมิให้ถูกแทรกแซงหรือลบหลู่เช่นว่านั้น “ความคุ้มครองตามกฎหมาย” ต้องเป็นจริงขึ้นมาได้เมื่อมีขั้นตอนปฏิบัติเพื่อคุ้มครอง รวมทั้งมีโครงสร้างเชิงสถาบันที่เป็นผลและได้รับการอุดหนุนด้านทรัพยากรอย่างเพียงพอ แต่เป็นที่ชัดเจนว่า การขาดการกำกับดูแลอย่างเป็นผล ส่งผลให้เกิดความบกพร่องในการตรวจสอบการ

---

[30] ดูตัวอย่างเช่น ในสหรัฐฯ พระราชบัญญัติการสอดแนมข้อมูลต่างชาติ - Foreign Intelligence Surveillance Act S1881(a); ในสหราชอาณาจักร พระราชบัญญัติระเบียบว่าด้วยอำนาจการสอบสวน - Regulation of Investigatory Powers Act 2000, s8(4); ในนิวซีแลนด์ พระราชบัญญัติหน่วยงานความมั่นคงของรัฐบาล - Government Security Bureau Act 2003, s. 15A; ในออสเตรเลีย พระราชบัญญัติบริการด้านข่าวกรอง - Intelligence Services Act S. 9 และในแคนาดา พระราชบัญญัติการป้องกันประเทศ - National Defence Act, S. 273.64 (1)

[31] CCPR /C/USA/CO/4, ย่อหน้า 22

แทรกแซงสิทธิความเป็นส่วนตัวโดยพลการหรือไม่ชอบด้วยกฎหมายในโลกดิจิทัล การมีกลไกคุ้มครองภายในโดยไม่มีกลไกตรวจสอบที่เป็นอิสระจากภายนอก ก็ไม่สามารถป้องกันวิธีการสอดแนมข้อมูลอย่างไม่ชอบด้วยกฎหมายหรือโดยพลการเช่นกัน แม้ว่ามาตรการคุ้มครองอาจมีได้ในหลายรูปแบบ แต่การมีส่วนร่วมของหน่วยงานทุกแห่งของรัฐบาลที่ทำหน้าที่กำกับดูแลโครงการสอดแนม รวมทั้งหน่วยงานพลเรือนที่เป็นอิสระและมีหน้าที่กำกับดูแล เป็นปัจจัยสำคัญเพื่อประกันให้มีการคุ้มครองตามกฎหมายอย่างเป็นผล

38. บทบาทด้านตุลาการที่สอดคล้องกับมาตรฐานระหว่างประเทศในแง่ความเป็นอิสระ ความไม่ลำเอียง และความโปร่งใส อาจมีส่วนสนับสนุนให้ระบบการกำกับดูแลตามกฎหมายทำหน้าที่ได้ตามมาตรฐานขั้นต่ำตามข้อกำหนดของกฎหมายสิทธิมนุษยชนระหว่างประเทศ ในเวลาเดียวกัน เราไม่ควรมองว่าบทบาทด้านตุลาการในการกำกับดูแลเป็นยาวิเศษเพื่อแก้ปัญหา เพราะในหลายประเทศ การขอหมายจากศาลหรือการขอให้ศาลไต่สวนความชอบด้วยกฎหมายของกิจกรรมการสอดแนมข้อมูลดิจิทัลเพื่อแสวงหาข่าวกรอง และ/หรือการปฏิบัติหน้าที่ของหน่วยงานบังคับใช้กฎหมาย มีลักษณะเป็นเหมือนการประทับตรายางเพื่ออนุมัติเท่านั้นเอง จึงมีความสนใจมากขึ้นต่อแม่แบบผสมระหว่างการกำกับดูแลของกลไกฝ่ายบริหาร ตุลาการ และรัฐสภา ซึ่งสอดคล้องกับความเห็นหลายประการที่นำเสนอในรายงานฉบับนี้ โดยเฉพาะมีความสนใจเป็นพิเศษต่อการกำหนดให้มีตำแหน่ง “การรณรงค์เพื่อประโยชน์สาธารณะ” ภายในกระบวนการอนุมัติการสอดแนมข้อมูล เนื่องจากบุคคลที่สามอย่างเช่น ผู้ให้บริการอินเทอร์เน็ต มีบทบาทเพิ่มมากขึ้น เราจึงอาจจำเป็นต้องส่งเสริมให้หน่วยงานเหล่านี้มีส่วนร่วมในการอนุมัติมาตรการการสอดแนมข้อมูลที่ส่งผลกระทบต่อผลประโยชน์ของพวกเขา หรือเปิดโอกาสให้หน่วยงานเหล่านี้สามารถคัดค้านมาตรการที่เป็นอยู่ ดังที่แนวนิติศาสตร์ที่เกี่ยวข้องหลายแห่งให้ความสนับสนุนต่อการใช้ประโยชน์จากคำปรึกษา การติดตามและ/หรือการตรวจสอบของหน่วยงานอิสระ ซึ่งจะช่วยประกันให้มีการตรวจสอบอย่างเคร่งครัดต่อมาตรการที่นำมาใช้ตามระบบกฎหมายการสอดแนมข้อมูล คณะกรรมาธิการรัฐสภาก็อาจมีบทบาทสำคัญเช่นกัน อย่างไรก็ดี หน่วยงานเหล่านี้อาจไม่มีความเป็นอิสระ ไม่มีทรัพยากร หรือเจตจำนงที่จะเปิดโปงการปฏิบัติมิชอบ และอาจถูกควบคุมด้วยกลไกการกำกับดูแล แนวนิติศาสตร์ระดับภูมิภาคเน้นถึงประโยชน์ของหน่วยงานกำกับดูแลที่เป็นอิสระอย่างเต็มที่ โดยเฉพาะหน้าที่ในการติดตามตรวจสอบการปฏิบัติตามมาตรการการสอดแนมข้อมูลที่ได้รับอนุมัติ[32] ในปี 2552 ผู้รายงานพิเศษว่าด้วยการส่งเสริมและคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานในช่วงที่เผชิญหน้ากับปัญหาลัทธิก่อการร้าย จึงมีข้อเสนอแนะว่า “จะต้องไม่อนุญาตให้มีระบบสอดแนมข้อมูลอย่างเป็นความลับที่ไม่ถูกตรวจสอบโดยหน่วยงานกำกับดูแลที่เป็นอิสระ และการแทรกแซงใด ๆ ต้องได้รับอนุมัติจากหน่วยงานอิสระ”[33]

จ. สิทธิที่จะได้รับการเยียวยาอย่างเป็นผล

39. กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองกำหนดให้รัฐภาคีประกันให้ผู้เสียหายจากการละเมิดกติกานี้ได้รับการเยียวยาอย่างเป็นผล ข้อ 2 ย่อหน้า 3 (b) ยังกำหนดเพิ่มเติมว่า รัฐภาคีของกติกาจะต้อง “ประกันว่าบุคคลใดที่เรียกร้องการเยียวยาดังกล่าว ย่อมมีสิทธิจะได้รับการพิจารณาจากฝ่ายตุลาการ ฝ่ายบริหาร หรือฝ่ายนิติบัญญัติที่มีอำนาจ หรือจากหน่วยงานอื่นที่มีอำนาจตามที่กำหนดไว้ โดยระบบกฎหมายของรัฐ และจะพัฒนาหนทางการเยียวยาด้วยกระบวนการยุติธรรมทางศาล” รัฐยังจะต้องประกันให้มีหน่วยงานที่มีอำนาจเพื่อบังคับให้เกิดการเยียวยาตามที่ได้รับอนุญาต ดังที่คณะกรรมการสิทธิมนุษยชนเน้นย้ำในความเห็นทั่วไป ฉบับที่ 31 ว่า กรณีที่รัฐไม่สามารถสอบสวนตามข้อกล่าวหาว่ามีการละเมิด อาจส่งผลและโดยตัวของมันเองอาจเป็นการละเมิดอีกข้อหนึ่งต่อกติกานี้[34] นอกจากนั้น การทำให้การละเมิดอย่างต่อเนื่องยุติลงเป็นองค์ประกอบสำคัญของสิทธิที่จะได้รับการเยียวยาอย่างเป็นผล

40. การเยียวยาที่เป็นผลสำหรับการละเมิดความเป็นส่วนตัวที่เกิดจากการสอดแนมข้อมูลดิจิทัล จึงอาจปรากฏในหลายรูปแบบทั้งที่ผ่านศาล ด้านนิติบัญญัติ หรือบริหาร โดยการเยียวยาที่เป็นผลมักจะมีลักษณะร่วมกันบางประการ ประการแรก การเยียวยาเหล่านี้ต้องเป็นที่รับรู้และเข้าถึงได้โดยบุคคลทุกคนที่มีข้ออ้างว่าสิทธิของตนได้ถูกละเมิด การรับแจ้งข้อมูล (ทั้งกรณีที่มีระบบการสอดแนมข้อมูลโดยทั่วไปและมาตรการสอดแนมข้อมูลเป็นการเฉพาะ) และสิทธิการฟ้อง

---

[32] ดูตัวอย่างเช่น ศาลสิทธิมนุษยชนแห่งยุโรป, Ekimdzhiev v Bulgaria, คำร้องที่ 62540/00, 28 มิถุนายน 2550

[33] A/HRC/13/37, ย่อหน้า 62

[34] CCPR/C/21/Rev.1/Add. 13, ย่อหน้า 15

คดี (เพื่อคัดค้านการใช้มาตรการดังกล่าว) จึงเป็นประเด็นสำคัญในการจำแนกการเข้าถึงการเยียวยาที่เป็นผล รัฐได้ใช้วิธีการต่าง ๆ เพื่อรับแจ้งข้อมูล ในขณะที่บางรัฐกำหนดให้เป้าหมายการสอดแนมแจ้งข้อมูลย้อนหลัง หลังจากการสอบสวนสิ้นสุดลงแล้ว แต่ระบบกฎหมายหลายแห่งไม่เปิดให้มีการแจ้งข้อมูล และในบางระบบอาจกำหนดให้มีการแจ้งข้อมูลในลักษณะนี้กรณีที่เป็นคดีอาญา อย่างไรก็ดี ในทางปฏิบัติแล้ว ข้อจำกัดเช่นนี้มักจะถูกเพิกเฉย ในระดับประเทศมีแนวคิดแตกต่างกันในแง่ของสิทธิการฟ้องคดีผ่านศาล ศาลสิทธิมนุษยชนแห่งยุโรปเคยตัดสินว่า แม้ว่าการมีอยู่ของระบบกฎหมายการสอดแนมข้อมูลอาจแทรกแซงต่อความเป็นส่วนตัว แต่การยื่นคำร้องว่ากฎหมายเช่นนี้เป็นเหตุให้เกิดการละเมิดสิทธิสามารถกระทำได้ เฉพาะเมื่อมี “ความเป็นไปได้อย่างสมเหตุผล” ที่บุคคลได้ตกเป็นเป้าหมายของการสอดแนมข้อมูลที่ไม่ชอบด้วยกฎหมาย[35]

41. ประการที่สอง การเยียวยาที่เป็นผลต้องเกิดขึ้นพร้อมกับการสอบสวนโดยพลัน อย่างรอบด้านและอย่างไม่ลำเอียงต่อข้อกล่าวหาว่ามีการละเมิดเกิดขึ้น ทั้งนี้ย่อมเป็นผลมาจากการมีข้อกำหนดให้มี “หน่วยงานกำกับดูแลที่เป็นอิสระ […] ที่อยู่ใต้การกำกับดูแลของกระบวนการอันควรอย่างเหมาะสมและอยู่ใต้การกำกับดูแลของศาล และอยู่ภายในข้อจำกัดตามที่อนุญาตให้กระทำได้ตามสังคมประชาธิปไตย”[36] ประการที่สาม เพื่อให้การเยียวยาเป็นผล การเยียวยานั้นต้องสามารถยุติการละเมิดอย่างต่อเนื่องได้ ตัวอย่างเช่น สามารถสั่งการให้ลบข้อมูลหรือให้มีการชดใช้อย่างอื่น[37] หน่วยงานที่ให้การเยียวยาจะต้องสามารถ “เข้าถึงข้อมูลที่เกี่ยวข้องอย่างเต็มที่และไม่มีการขัดขวาง เข้าถึงทรัพยากรและความชำนาญที่จำเป็นต่อการสอบสวน และสามารถออกระเบียบที่มีผลผูกพันตามกฎหมาย”[38] ประการที่สี่ กรณีที่การละเมิดสิทธิมนุษยชนเพิ่มสูงขึ้นจนถึงระดับที่เป็นการละเมิดอย่างร้ายแรง การเยียวยาจากหน่วยงานอื่นยกเว้นศาลอาจไม่เพียงพอ โดยจำเป็นต้องมีการฟ้องคดีทางอาญาด้วย[39]

IV. ภาคธุรกิจจะมีบทบาทอย่างไร?

42. มีข้อมูลที่หนักแน่นว่ารัฐบาลได้พึ่งพาหน่วยงานเอกชนมากขึ้น เพื่อดำเนินการและสนับสนุนการสอดแนมข้อมูลดิจิทัล ในทุกทวีป รัฐบาลใช้ทั้งกลไกตามกฎหมายอย่างเป็นทางการและวิธีการแบบปิดลับเพื่อเข้าถึงเนื้อหา รวมทั้งคำอธิบายข้อมูล กระบวนการเช่นนี้เริ่มพัฒนาอย่างเป็นระบบมากขึ้น ในขณะที่บทบาทการให้บริการด้านโทรคมนาคมได้เปลี่ยนจากภาครัฐไปสู่ภาคเอกชนมากขึ้น ที่ผ่านมามี “การมอบหมายให้หน่วยงานด้านอินเทอร์เน็ตรับผิดชอบงานการบังคับใช้กฎหมายและทำหน้าที่กึ่งตุลาการ โดยอ้างว่าเป็น ‘การควบคุมตนเอง’ หรือ ‘ความร่วมมือ’[40] การกำหนดเป็น

---

[35] ดู Esbester v. the United Kingdom, คำร้องที่ 18601/91, มติของคณะกรรมาธิการ 2 เมษายน 2536; Redgrave v. the United Kingdom, คำร้องที่ 202711/92, มติของคณะกรรมาธิการ 1 กันยายน 2536; และ Matthews v. the United Kingdom, คำร้องที่ 28576/95, มติของคณะกรรมาธิการ 16 ตุลาคม 2539

[36] “แถลงการณ์ร่วมว่าด้วยโครงการสอดแนมและผลกระทบที่มีต่อเสรีภาพในการแสดงออก” ของผู้รายงานพิเศษว่าด้วยการส่งเสริมและการคุ้มครองสิทธิที่จะมีเสรีภาพด้านความเห็นและการแสดงออก และผู้รายงานพิเศษว่าด้วยเสรีภาพในการแสดงออกของคณะกรรมาธิการสิทธิมนุษยชนแห่งทวีปอเมริกา มิถุนายน 2556 (จาก www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1) ย่อหน้า 9

[37] ดูตัวอย่างเช่น ศาลสิทธิมนุษยชนแห่งยุโรป, Segersted-Wiber and others v. Sweden, คำร้องที่ 62332/00, 6 มิถุนายน 2549. และโปรดดู CCPR/C/21/Rev.1/Add. 13, ย่อหน้า 15-17

[38] A/HRC/14/46

[39] หลักการและแนวปฏิบัติขั้นพื้นฐานว่าด้วยสิทธิที่จะได้รับการเยียวยาและการชดใช้สำหรับผู้เสียหายจากการละเมิดกฎหมายสิทธิมนุษยชนระหว่างประเทศร้ายแรงและการละเมิดกฎหมายมนุษยธรรมระหว่างประเทศร้ายแรง (มติสมัชชาใหญ่แห่งสหประชาชาติที่ 60/147, ภาคผนวก)

[40] โปรดดู European Digital Rights, “การเปลี่ยนผ่านจาก ‘การควบคุมตนเอง’ ไปสู่การเซ็นเซอร์ของบรรษัท - The Slide from ’Self-Regulation’ to Corporate Censorship”, Brussels, มกราคม 2554 ที่ www.edri.org/files/EDRI_selfreg_final_20110124.pdf

กฎหมายเพื่อบังคับให้บริษัทพัฒนาโครงข่ายการสื่อสาร “แบบพร้อมสำหรับการดักฟัง” เป็นข้อกังวลอย่างมาก เพราะอย่างน้อยเป็นการทำให้เกิดโครงสร้างที่สนับสนุนมาตรการการสอดแนมในวงกว้าง

43. รัฐอาจมีเหตุผลอันควรในการกำหนดให้บริษัทเทคโนโลยีข้อมูลสนเทศและการสื่อสารต้องนำข้อมูลของผู้ใช้มามอบให้ อย่างไรก็ดี ในกรณีที่บริษัทมอบข้อมูลหรือข้อมูลเกี่ยวกับผู้ใช้ให้กับรัฐ โดยคำร้องขอนั้นขัดกับสิทธิความเป็นส่วนตัวตามกฎหมายระหว่างประเทศ หรือกรณีที่บริษัทขายเทคโนโลยีหรืออุปกรณ์เพื่อการสอดแนมในวงกว้างให้กับรัฐโดยไม่มีมาตรการคุ้มครองที่เหมาะสม หรือกรณีที่มีการนำข้อมูลนั้นไปใช้เพื่อการละเมิดสิทธิมนุษยชน มีความเสี่ยงว่าบริษัทดังกล่าวอาจมีส่วนร่วมในการปฏิบัติมิชอบด้านสิทธิมนุษยชน หลักปฏิบัติด้านธุรกิจและสิทธิมนุษยชน (Guiding Principles on Business and Human Rights) ซึ่งผ่านการรับรองของคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติในปี 2544 กำหนดมาตรฐานระดับโลกเพื่อป้องกันและแก้ปัญหาผลกระทบด้านสิทธิมนุษยชนที่เชื่อมโยงกับกิจกรรมด้านธุรกิจ ความรับผิดชอบในการเคารพสิทธิมนุษยชนมีผลบังคับใช้ต่อการดำเนินงานทุกขั้นตอนในระดับโลกของบริษัท ไม่ว่าผู้ใช้งานจะอยู่ในที่ใด และมีความเป็นอิสระไม่ว่ารัฐจะปฏิบัติตามพันธกรณีด้านสิทธิมนุษยชนของตนเองหรือไม่

44. ได้มีความพยายามที่สำคัญของหลายภาคส่วนของผู้มีส่วนได้ส่วนเสีย เพื่อให้เกิดความชัดเจนเกี่ยวกับการประยุกต์ใช้หลักการชี้นำกับภาคเทคโนโลยีการสื่อสารและข้อมูลสนเทศ ยกตัวอย่างเช่น วิสาหกิจที่ให้บริการด้านเนื้อหาหรือบริการอินเทอร์เน็ต หรือเป็นผู้ขายเทคโนโลยีและอุปกรณ์เพื่อการสื่อสารแบบดิจิทัล ควรจัดทำถ้อยแถลงด้านนโยบายที่ชัดเจนที่สะท้อนให้เห็นพันธกรณีของตนที่มีต่อการเคารพสิทธิมนุษยชนในการดำเนินงานทุกประการของบริษัท ทั้งยังควรกำหนดให้มีนโยบายการตรวจสอบที่เหมาะสมเพื่อจำแนก ประเมิน ป้องกัน และบรรเทาผลกระทบด้านลบ บริษัทควรประเมินว่าเงื่อนไขการให้บริการของตนหรือนโยบายการเก็บและแลกเปลี่ยนข้อมูลของลูกค้า จะส่งผลกระทบด้านลบต่อสิทธิมนุษยชนของลูกค้าหรือไม่และอย่างไร

45. กรณีที่วิสาหกิจได้รับคำร้องขอจากรัฐบาลเพื่อการเข้าถึงข้อมูล โดยเป็นคำร้องขอที่ไม่ชอบด้วยมาตรฐานสิทธิมนุษยชนระหว่างประเทศ เราคาดหวังว่าทางบริษัทจะตัดสินใจปฏิบัติตามหลักการสิทธิมนุษยชนให้มากสุดเท่าที่จะทำได้ และแสดงให้เราเห็นอย่างต่อเนื่องว่ามีความพยายามทำเช่นนั้น ทั้งนี้อาจหมายถึงการที่บริษัทตีความคำร้องขอของรัฐบาลให้แคบสุดเท่าที่จะเป็นไปได้ ขอให้รัฐบาลชี้แจงเกี่ยวกับขอบเขตและพื้นฐานด้านกฎหมายของคำร้องขอนั้น ขอให้มีการแสดงหมายจากศาลก่อนจะปฏิบัติตามคำร้องขอด้านข้อมูลของรัฐบาล และสื่อสารอย่างโปร่งใสเพื่อให้ผู้ใช้บริการทราบถึงความเสี่ยงและการปฏิบัติตามคำร้องขอของรัฐบาล มีตัวอย่างในเชิงบวกของอุตสาหกรรมที่ปฏิบัติเช่นนี้ ทั้งวิสาหกิจที่เป็นของเอกชนและกิจกรรมที่มีผู้มีส่วนได้ส่วนเสียหลายส่วน

46. องค์ประกอบสำคัญของการตรวจสอบด้านสิทธิมนุษยชนซึ่งมีการนิยามไว้ในหลักการชี้นำได้แก่ การปรึกษาหารืออย่างจริงจังกับผู้มีส่วนได้ส่วนเสียที่ได้รับผลกระทบ ในแง่ของบริษัทผู้ให้บริการเทคโนโลยีข้อมูลสนเทศและการสื่อสาร อาจหมายถึงการประกันให้ผู้ใช้บริการได้รับทราบอย่างจริงจังว่า ข้อมูลของตนได้ถูกเก็บ รักษา ใช้ประโยชน์ และอาจมีการแลกเปลี่ยนกับบุคคลอื่นใด ทั้งนี้เพื่อให้ผู้ใช้บริการสามารถแสดงข้อกังวลและตัดสินใจได้อย่างมีข้อมูล หลักการชี้นำกำหนดอย่างชัดเจนว่า หากวิสาหกิจพบว่าตนได้ก่อให้เกิดหรือมีส่วนทำให้เกิดผลกระทบร้ายแรงด้านสิทธิมนุษยชน วิสาหกิจเหล่านั้นย่อมมีความรับผิดชอบดูแลให้มีการเยียวยาตามมาตรการเยียวยาโดยตรง หรือร่วมมือในกระบวนการเยียวยาอันควร เพื่อให้เกิดการเยียวยาในขั้นตอนแรกสุด ทางวิสาหกิจควรกำหนดให้มีกลไกรับข้อร้องเรียนระดับปฏิบัติการ กลไกเช่นนี้อาจสำคัญอย่างยิ่งในประเทศที่มีความบกพร่องด้านการคุ้มครองสิทธิ หรือกรณีที่ไม่สามารถเข้าถึงการเยียวยาผ่านระบบศาลและระบบอื่น ๆ ได้ นอกจากองค์ประกอบเหล่านี้ ทั้งค่าชดเชยและการชดใช้ การเยียวยายังควรครอบคลุมข้อมูลว่ามีการนำข้อมูลไปแลกเปลี่ยนกับหน่วยงานของรัฐหรือไม่และอย่างไร

V. **สรุปและข้อเสนอแนะ**

47. กฎหมายสิทธิมนุษยชนระหว่างประเทศกำหนดกรอบอย่างชัดเจนและเป็นสากลเพื่อส่งเสริมและคุ้มครองสิทธิความเป็นส่วนตัว ทั้งที่เป็นการสอดแนมข้อมูลจากหน่วยงานในประเทศและต่างประเทศ การดักจับการสื่อสารแบบดิจิทัลและการรวบรวมข้อมูลส่วนบุคคล แต่จากการปฏิบัติหน้าที่ของรัฐหลายแห่งทำให้พบว่า กฎหมายและ/หรือการบังคับใช้กฎหมายในระดับประเทศยังมีความบกพร่อง มาตรการเชิงคุ้มครองก็อ่อนแอ และมีการกำกับดูแลที่ไม่เป็นผล ทั้งหมดทำให้ไม่สามารถตรวจสอบการแทรกแซงสิทธิความเป็นส่วนตัวโดยพลการหรือไม่ชอบด้วยกฎหมายได้

48. ในการแก้ปัญหาช่องว่างของการปฏิบัติตามสิทธิความเป็นส่วนตัว เรามีข้อสังเกตสองประการ ประการแรก ยังมีรายงานข้อมูลเกี่ยวกับนโยบายและการปฏิบัติเพื่อสอดแนมข้อมูลในประเทศและต่างประเทศอย่างต่อเนื่อง และมีการสอบสวนโดยมีเป้าหมายเพื่อรวบรวมข้อมูลเกี่ยวกับการสอดแนมทางอิเล็กทรอนิกส์และการเก็บและรักษาข้อมูลส่วนบุคคล รวมทั้งการประเมินผลกระทบต่อสิทธิมนุษยชน ศาลในระดับประเทศและภูมิภาคมีบทบาทในการตรวจสอบความชอบด้วยกฎหมายของนโยบายและมาตรการการสอดแนมทางอิเล็กทรอนิกส์ การประเมินนโยบายและการปฏิบัติด้านการสอดแนมโดยเปรียบเทียบกับกฎหมายสิทธิมนุษยชนระหว่างประเทศ ต้องมีการดัดแปลงให้เหมาะสมกับลักษณะของปัญหาที่เปลี่ยนแปลงไป ข้อสังเกตที่สองซึ่งเกี่ยวข้องกันเป็นเรื่องของการขาดความโปร่งใสอย่างมากของรัฐบาลในแง่นโยบาย กฎหมาย และการปฏิบัติด้านการสอดแนมข้อมูล ซึ่งเป็นอุปสรรคต่อความพยายามในการประเมินความสอดคล้องที่มีต่อกฎหมายสิทธิมนุษยชนระหว่างประเทศ และเพื่อประกันการตรวจสอบได้

49. การแก้ปัญหาที่เกี่ยวข้องกับสิทธิความเป็นส่วนตัวอย่างเป็นผลในบริบทเทคโนโลยีการสื่อสารสมัยใหม่จำเป็นต้องมีส่วนร่วมอย่างต่อเนื่องและเป็นเอกภาพของผู้มีส่วนได้ส่วนเสียหลายกลุ่ม โดยกระบวนการนี้ควรครอบคลุมการเจรจาของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทุกหน่วยงาน ทั้งรัฐภาคี ภาคประชาสังคม ชุมชน นักวิทยาศาสตร์และด้านเทคนิค ภาคธุรกิจ นักวิชาการและผู้ชำนาญการด้านสิทธิมนุษยชน ในขณะที่เทคโนโลยีการสื่อสารพัฒนามากขึ้น ความเป็นผู้นำเป็นปัจจัยสำคัญที่ประกันว่า จะมีการใช้เทคโนโลยีเหล่านี้เพื่อสนับสนุนการเข้าถึงสิทธิมนุษยชนที่ได้รับการรับรองตามกรอบกฎหมายระหว่างประเทศ

50. เมื่อคำนึงถึงข้อสังเกตข้างต้น จะทำให้เราเห็นความจำเป็นที่ชัดเจนและเร่งด่วนในการตรวจสอบว่า การปฏิบัติหน้าที่และนโยบายด้านการสอดแนมข้อมูลสอดคล้องกับกฎหมายสิทธิมนุษยชนระหว่างประเทศหรือไม่ รวมทั้งในแง่สิทธิความเป็นส่วนตัว โดยมีการจัดทำมาตรการคุ้มครองไม่ให้เกิดการปฏิบัติมิชอบอย่างเป็นผล สำหรับปัญหาเฉพาะหน้า รัฐควรทบทวนกฎหมาย นโยบาย และการปฏิบัติระดับชาติ เพื่อประกันให้มีการปฏิบัติตามกฎหมายสิทธิมนุษยชนระหว่างประเทศอย่างเต็มที่ กรณีที่ยังมีข้อบกพร่อง รัฐควรดำเนินมาตรการเพื่อแก้ปัญหานั้น รวมทั้งการนำกรอบกฎหมายที่ชัดเจน เฉพาะเจาะจง เข้าถึงได้ ครอบคลุม และไม่เลือกปฏิบัติมาใช้ และมีการดำเนินงานตามขั้นตอนเพื่อประกันให้มีระบบการกำกับดูแลและการปฏิบัติที่เป็นผลและเป็นอิสระ ทั้งนี้โดยคำนึงถึงสิทธิของผู้เสียหายที่จะได้รับการเยียวยาอย่างเป็นผล

51. ยังคงมีอุปสรรคเชิงปฏิบัติที่สำคัญหลายประการ ในแง่ของการส่งเสริมและคุ้มครองสิทธิความเป็นส่วนตัวในยุคดิจิทัล จากการพิจารณาในเบื้องต้นถึงประเด็นต่าง ๆ ที่นำเสนอในรายงานฉบับนี้ ทำให้เห็นความจำเป็นที่จะต้องมีการอภิปรายและการศึกษาในเชิงลึกเพิ่มเติม สำหรับประเด็นที่เกี่ยวข้องกับการคุ้มครองด้านกฎหมายอย่างเป็นผล การมีมาตรการคุ้มครองเชิงปฏิบัติ การกำกับดูแลอย่างเป็นผลและการเยียวยา การวิเคราะห์ในเชิงลึกต่อประเด็นปัญหานี้ จะช่วยให้เรามีแนวปฏิบัติเพิ่มเติม ซึ่งเป็นแนวปฏิบัติที่อยู่บนพื้นฐานของกฎหมายสิทธิมนุษยชนระหว่างประเทศ ในแง่หลักการความจำเป็น ความได้สัดส่วน และความชอบด้วยกฎหมาย เมื่อเปรียบเทียบกับการสอดแนมข้อมูลที่กระทำอยู่ การวิเคราะห์มาตรการเพื่อการกำกับดูแลที่เป็นผล เป็นอิสระและไม่ลำเอียง และมีมาตรการเยียวยา การวิเคราะห์เพิ่มเติมย่อมจะช่วยให้ภาคธุรกิจปฏิบัติตามความรับผิดชอบในการเคารพสิทธิมนุษยชนได้ รวมทั้งการตรวจสอบภายในและมาตรการบริหารจัดการความเสี่ยง รวมทั้งบทบาทในการให้การเยียวยาที่เป็นผล