

International Principles on the Application of Human Rights to Communications Surveillance

หลักการระหว่างประเทศ ว่าด้วยการใช้หลักสิทธิมนุษยชน กับการสอดแนมการสื่อสาร*

ฉบับสุดท้ายวันที่ 10 กรกฎาคม 2556

ในขณะที่เทคโนโลยีที่อำนวยความสะดวกให้รัฐทำการสอดแนมการสื่อสารมีความก้าวหน้ามากขึ้น รัฐต่าง ๆ กลับล้มเหลวในการทำให้แน่ใจว่ากฎหมายและระเบียบเกี่ยวกับการสอดแนมการสื่อสารนั้นสอดคล้องกับหลักสิทธิมนุษยชนสากลและให้การคุ้มครองอย่างเพียงพอต่อสิทธิความเป็นส่วนตัวและเสรีภาพในการแสดงออก เอกสารฉบับนี้พยายามอธิบายว่าจะนำกฎหมายสิทธิมนุษยชนสากลมาใช้กับสภาพแวดล้อมดิจิทัลในปัจจุบันได้อย่างไร โดยเฉพาะในขณะที่เทคโนโลยีและเทคนิคการสอดแนมการสื่อสารมีการเปลี่ยนแปลงและมีเพิ่มมากขึ้น กลุ่มภาคประชาสังคม ภาคอุตสาหกรรม ภาครัฐ และกลุ่มอื่น ๆ สามารถยึดหลักการเหล่านี้เป็นกรอบในการประเมินว่า กฎหมายและการปฏิบัติเกี่ยวกับการสอดแนมการสื่อสารที่มีอยู่ในปัจจุบันหรือที่กำลังจะมีขึ้น สอดคล้องกับหลักสิทธิมนุษยชนหรือไม่

หลักการเหล่านี้เป็นผลมาจากการปรึกษาหารือระดับสากลกับบรรดากลุ่มภาคประชาสังคม ภาคอุตสาหกรรม และผู้ชำนาญการระหว่างประเทศด้านกฎหมาย นโยบาย และเทคโนโลยีการสอดแนมการสื่อสาร

*ฉบับภาษาไทยโดยเครือข่ายพลเมืองเน็ต แปลโดย ทิภาพ อุดมอิทธิพงศ์ และ อาทิตย์ สุริยะวงศ์กุล เผยแพร่ครั้งแรก 23 พ.ย. 2556 ปรับปรุง 28 ม.ค. 2557 ดูต้นฉบับภาษาอังกฤษและคำแปลภาษาอื่น ๆ ได้ที่ <https://necessaryandproportionate.org/>

อาร์มภพ

ความเป็นส่วนตัวเป็นสิทธิมนุษยชนขั้นพื้นฐาน และเป็นหัวใจในการดำรงสังคมประชาธิปไตย เป็นสิ่งสำคัญสำหรับศักดิ์ศรีของมนุษย์ และหนุนเสริมสิทธิอื่น ๆ อย่างเช่น เสรีภาพในการแสดงออกและในข้อมูลข่าวสาร และเสรีภาพในการสมาคม ทั้งยังเป็นที่ยอมรับในกฎหมายสิทธิมนุษยชนระหว่างประเทศ¹ กิจกรรมที่จำกัดสิทธิความเป็นส่วนตัว รวมทั้งการสอดแนมการสื่อสาร จะสมเหตุสมผลให้กระทำได้ก็ต่อเมื่อมีกฎหมายรองรับไว้แล้ว มีความจำเป็นต่อการบรรลุเป้าหมายที่ชอบธรรม และการกระทำดังกล่าวได้สัดส่วนที่เหมาะสมกับเป้าหมายที่ต้องการ²

ในสมัยที่อินเทอร์เน็ตยังไม่แพร่หลายสู่สาธารณะ หลักกฎหมายที่มั่นคงและภาวะด้านการจัดการที่ตามมากับการจับตาดูตามการสื่อสาร ได้สร้างข้อจำกัดในการสอดแนมการสื่อสารของรัฐ ในช่วงไม่กี่ทศวรรษที่ผ่านมา อุปสรรคด้านการจัดการต่อการสอดแนมเหล่านั้นได้ลดลง ในขณะที่การนำหลักกฎหมายมาใช้ในบริบทเทคโนโลยีสมัยใหม่เริ่มเป็นที่ไม่ชัดเจน ความแพร่หลายของเนื้อหาการสื่อสารดิจิทัลและข้อมูลเกี่ยวกับการสื่อสาร หรือ “เมตาดาตาของการสื่อสาร” (communications metadata) ซึ่งหมายถึงข้อมูลเกี่ยวกับการสื่อสารหรือการใช้เครื่องมืออิเล็กทรอนิกส์ของบุคคล ประกอบกับต้นทุนที่ต่ำลงของการจัดเก็บและการวิเคราะห์ทำเหมืองข้อมูลขนาดใหญ่ และการจัดส่งจัดหาเนื้อหาส่วนบุคคลผ่านผู้ให้บริการที่เป็นบุคคลที่สาม ล้วนทำให้การสอดแนมของรัฐเกิดขึ้นได้อย่างกว้างขวางอย่างไม่เคยเป็นมาก่อน³ ในขณะเดียวกัน การพัฒนาแนวคิดเกี่ยวกับกฎหมายสิทธิมนุษยชนที่มีอยู่ในปัจจุบันนั้น ไม่สอดคล้องกับศักยภาพของรัฐในการสอดแนมการสื่อสารในยุคสมัย

¹ข้อ 12 ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights) ข้อ 14 อนุสัญญาแห่งสหประชาชาติว่าด้วยคนงานข้ามชาติ (United Nations Convention on Migrant Workers) ข้อ 16 อนุสัญญาแห่งสหประชาชาติว่าด้วยการคุ้มครองเด็ก (UN Convention of the Protection of the Child) ข้อ 17 กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights – ICCPR); อนุสัญญาระดับภูมิภาค ได้แก่ข้อ 10 กฎบัตรว่าด้วยการคุ้มครองสิทธิและสวัสดิภาพของเด็กแห่งแอฟริกา (African Charter on the Rights and Welfare of the Child) ข้อ 11 อนุสัญญาว่าด้วยสิทธิมนุษยชนแห่งอเมริกา (American Convention on Human Rights) ข้อ 4 หลักการว่าด้วยเสรีภาพในการแสดงออกของสหภาพแอฟริกา (African Union Principles on Freedom of Expression) ข้อ 5 ปฏิญญาว่าด้วยสิทธิและหน้าที่ของมนุษย์แห่งอเมริกา (American Declaration of the Rights and Duties of Man) ข้อ 21 กฎบัตรสิทธิมนุษยชนแห่งอาหรับ (Arab Charter on Human Rights) และข้อ 18 อนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานแห่งยุโรป (European Convention for the Protection of Human Rights and Fundamental Freedoms); หลักการว่าด้วยความมั่นคงแห่งชาติ การแสดงออกอย่างเสรี และการเข้าถึงข้อมูลสนเทศโจฮันเนสเบิร์ก (Johannesburg Principles on National Security, Free Expression and Access to Information) หลักการว่าด้วยเสรีภาพในการแสดงออกและความเท่าเทียมแคมเดน (Camden Principles on Freedom of Expression and Equality)

²ข้อ 29 ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน; ความเห็นทั่วไป (General Comment) ข้อ 27 รับรองโดยคณะกรรมการสิทธิมนุษยชน (Human Rights Committee) ตามข้อ 40 ย่อหน้า 4 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง, CCPR/C/21/Rev.1/Add.9, 2 พฤศจิกายน 2542; และโปรดดู Martin Scheinin, “รายงานของผู้รายงานพิเศษว่าด้วยการส่งเสริมและการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานในระหว่างการต่อต้านการก่อการร้าย” (“Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism”) 2552, A/HRC/17/34

ใหม่ที่กำลังเปลี่ยนแปลง ไม่สอดคล้องกับศักยภาพของรัฐในการผนวกรวมและจัดระบบข้อมูลด้วยเทคนิคการสอดแนมแบบต่าง ๆ หรือไม่สอดคล้องกับความอ่อนไหวที่เพิ่มมากขึ้นของข้อมูลที่มีให้เข้าถึง

ความถี่ของรัฐในการหาทางเข้าถึงทั้งเนื้อหาการสื่อสารและเมทาเดตาของการสื่อสารเพิ่มขึ้นอย่างน่าตกใจ โดยปราศจากการตรวจสอบอย่างเหมาะสม⁴ เมื่อถูกเข้าถึงและวิเคราะห์ เมทาเดตาอาจถูกนำมาสร้างประวัติชีวิตของบุคคล ซึ่งรวมถึงสภาพความเจ็บป่วยและการรักษาพยาบาล มุมมองทางการเมืองและศาสนา การสมาคม การติดต่อปฏิสัมพันธ์และความสนใจ ข้อมูลเมทาเดตาเปิดเผยรายละเอียดต่าง ๆ ของบุคคลมากพอที่รายละเอียดของบุคคลที่จะสามารถสังเกตเห็นได้จากเนื้อหาของการสื่อสาร หรืออาจจะเปิดเผยมากกว่าเสียด้วยซ้ำ⁵ แม้จะมีความสามารถอย่างมหาศาลในการรุกรานล้ำเข้ามาในชีวิตบุคคล และส่งผลกระทบต่อความสัมพันธ์ทางการเมืองและการสมาคมอื่น ๆ แต่เครื่องมือทางกฎหมายและนโยบายมักให้การคุ้มครองเมทาเดตาของการสื่อสารต่ำกว่าปกติ และไม่มีข้อกำหนดข้อจำกัดอย่างเพียงพอว่าหน่วยงานต่าง ๆ จะนำข้อมูลเหล่านี้ไปใช้ได้อย่างไรบ้าง รวมถึงว่าเมทาเดตาจะถูกทำเหมืองข้อมูล แบ่งปันส่งต่อ และเก็บรักษาอย่างไร

ในการที่รัฐจะสามารถปฏิบัติตามพันธกรณีด้านสิทธิมนุษยชนสากลที่เกี่ยวข้องกับการสอดแนมการสื่อสารได้ รัฐต้องปฏิบัติตามหลักการที่กำหนดไว้ด้านล่างนี้ หลักการเหล่านี้มีผลบังคับใช้ต่อการสอดแนมทั้งที่เกิดขึ้นภายในรัฐหรือนอกอาณาเขตของรัฐ ทั้งยังมีผลบังคับใช้ไม่ว่าเป้าประสงค์ของการสอดแนมจะเป็นอะไร ไม่ว่าจะเพื่อการบังคับใช้กฎหมาย ความมั่นคงแห่งชาติ หรือเพื่อเป้าประสงค์การควบคุมอื่นใด ทั้งยังมีผลบังคับใช้ต่อพันธกรณีที่รัฐจะต้องเคารพและปฏิบัติตามสิทธิส่วนบุคคล

⁴ข้อมูลเมทาเดตาของการสื่อสาร (communications metadata) อาจประกอบด้วยข้อมูลเกี่ยวกับอัตลักษณ์ของเรา (ข้อมูลของผู้สมัคร ข้อมูลของอุปกรณ์ที่ใช้) การปฏิสัมพันธ์ (แหล่งที่มาและที่ไปของการสื่อสาร โดยเฉพาะข้อมูลที่แสดงว่ามีการเข้าชมเว็บไซต์อะไรบ้าง อ่านหนังสือและเอกสารใดบ้าง มีการติดต่อกับบุคคลใดบ้าง มีเพื่อน ครอบครัว คนรู้จักเป็นใครบ้าง ประวัติการค้นหาข้อมูล และข้อมูลที่เคยถูกใช้งาน) และข้อมูลเกี่ยวกับตำแหน่งที่ตั้ง (สถานที่และเวลา ความใกล้ชิดกับบุคคลอื่น ๆ) โดยสรุป ข้อมูลเมทาเดตาเป็นกุญแจเปิดเผยกิจกรรมแทบจะทุกอย่างในชีวิตสมัยใหม่ มันเผยให้เห็นสภาพจิตใจ ความสนใจ ความตั้งใจ และความนึกคิดข้างในที่สุดของเรา

⁵ยกตัวอย่างเช่น เฉพาะในสหราชอาณาจักร ปัจจุบันมีการร้องขอข้อมูลเมทาเดตาประมาณ 500,000 ครั้งทุกปี โดยเป็นการร้องขอข้อมูลและการอนุมัติโดยหน่วยงานผู้บังคับใช้กฎหมายเอง ซึ่งสามารถให้อนุญาตคำขออนุญาตของตนเองเพื่อเข้าถึงข้อมูลของผู้ให้บริการ ในเวลาเดียวกัน ข้อมูลจากรายงานความโปร่งใส (Transparency Report) ของกูเกิลแสดงให้เห็นว่ามีการขอข้อมูลเกี่ยวกับผู้ใช้งาน เฉพาะในสหรัฐอเมริกา เพิ่มจาก 8,888 ครั้งในปี 2553 เป็น 12,271 ครั้งในปี 2554 ในเกาหลี ทุกปีจะมีการร้องขอข้อมูลเกี่ยวกับผู้สมัคร/ผู้โพสต์ข้อความประมาณ 6 ล้านครั้ง และการร้องขอข้อมูลเมทาเดตาของการสื่อสารในรูปแบบอื่น ๆ อีกประมาณ 30 ล้านครั้ง ทุกปีระหว่างปี 2554-2555 โดยได้รับอนุญาตและมีการดำเนินการตามคำร้องเกือบทั้งหมด ข้อมูลสำหรับปี 2555 ปรากฏที่ [http://www.kcc.go.kr/user.do?](http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586)

[mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586](http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586)

⁶โปรดดู อย่างเช่น การพิจารณารายงานของ Sandy Petland, 'Reality Mining', ในวารสาร MIT's Technology Review, 2551 ที่ <http://www2.technologyreview.com/article/409598/tr10-reality-mining/> และโปรดดู 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

และพันธกรณีที่จะต้องคุ้มครองสิทธิของบุคคลเพื่อไม่ให้ถูกละเมิดโดยหน่วยงานที่ไม่ใช่รัฐ รวมทั้ง บรรษัท ภาคเอกชนก็มีความรับผิดชอบเท่าเทียมกันในการเคารพสิทธิมนุษยชน โดยเฉพาะอย่างยิ่ง เมื่อคำนึงถึงบทบาทสำคัญที่ภาคเอกชนมีในการออกแบบ พัฒนา และเผยแพร่เทคโนโลยี การทำให้ การสื่อสารเป็นไปได้และจัดการสื่อสาร และ ในกรณีที่ถูกบังคับ การให้ความร่วมมือกับกิจการ สอดแนมของรัฐ อย่างไรก็ตาม ขอบเขตของหลักการฉบับนี้จำกัดอยู่เฉพาะพันธกรณีของรัฐเท่านั้น

เทคโนโลยีและนิยามที่เปลี่ยนแปลงไป

“การสอดแนมการสื่อสาร” ในบริบทสมัยใหม่ประกอบด้วย การติดตาม การตรวจจับ การ ค้นหา การวิเคราะห์ การใช้ การเก็บรักษา การคงสถานะไว้ การแทรกแซง หรือการเข้าถึงข้อมูลซึ่ง ครอบคลุม สะท้อน เป็นผลมาจาก หรือเกี่ยวข้องกับการสื่อสารของบุคคลในอดีต ปัจจุบัน หรือ อนาคต “การสื่อสาร” ครอบคลุมถึงกิจกรรม ปฏิสัมพันธ์ และธุรกรรมที่ส่งผ่านสื่ออิเล็กทรอนิกส์ เช่น เนื้อหาของการสื่อสาร ข้อมูลส่วนบุคคลเกี่ยวกับฝ่ายที่เกี่ยวข้องในการสื่อสาร ข้อมูลเพื่อการค้นหา ตำแหน่ง รวมทั้งข้อมูลที่อยู่ไอพี (IP address) เวลาและระยะเวลาของการสื่อสาร และตัวบ่งชี้ อุปกรณ์การสื่อสารที่ใช้ในการสื่อสาร

ดังที่ปฏิบัติต่อกันมา การประเมินความรุกร้าของการสอดแนมการสื่อสารนั้น ทำไปบนพื้นฐาน ของการจำแนกประเภทที่คนคิดขึ้นมาเองและถูกกำหนดตามแบบแผนตายตัว กรอบกฎหมายที่มีอยู่ จำแนกระหว่างสิ่งที่เป็น “เนื้อหา” หรือ “ไม่เป็นเนื้อหา” “ข้อมูลของผู้สมัครใช้งาน” หรือ “เมทาตา ทา” ข้อมูลที่เก็บกักไว้ หรือ ข้อมูลที่อยู่ระหว่างการจัดส่ง ข้อมูลซึ่งเก็บไว้ที่บ้าน หรือ ข้อมูลที่ถูกเก็บ ไว้โดยผู้ให้บริการที่เป็นบุคคลที่สาม⁷ อย่างไรก็ตาม วิธีการแบ่งเหล่านี้ดูจะไม่เหมาะสมอีกต่อไป สำหรับการวัดระดับการแทรกแซงที่การสอดแนมการสื่อสารมีต่อชีวิตส่วนตัวและการสมาคมของ บุคคล แม้จะเป็นที่ยอมรับกันมานานว่า เนื้อหาการสื่อสารสมควรได้รับการคุ้มครองอย่างยิ่งใน กฎหมาย เนื่องจากอาจเผยให้เห็นข้อมูลที่อ่อนไหว แต่ตอนนี้เป็นที่ชัดเจนว่าข้อมูลอื่นที่ถูกส่งไป ระหว่างการสื่อสาร อย่างเช่น เมทาตาทาและข้อมูลส่วนที่ไม่ใช่เนื้อหาในรูปแบบอื่น ก็อาจเปิดเผยราย ละเอียดเกี่ยวกับบุคคลได้มากกว่าตัวเนื้อหาเองด้วยซ้ำ ดังนั้นข้อมูลที่ไม่ใช่เนื้อหาจึงสมควรได้รับการ คุ้มครองดุจเดียวกัน ในปัจจุบัน ข้อมูลประเภทต่าง ๆ เหล่านี้ ไม่ว่าจะอยู่แยกเดี่ยวหรือวิเคราะห์รวม

⁶รายงานของผู้รายงานพิเศษว่าด้วยการส่งเสริมและการคุ้มครองสิทธิที่จะมีเสรีภาพในความคิดเห็นและการแสดงออก (Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression), Frank La Rue, 16 พฤษภาคม 2554 ที่ http://www.2ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

⁷“ผู้คนเปิดเผยหมายเลขโทรศัพท์ที่พวกเขาโทรหรือส่งข้อความ ให้กับผู้ให้บริการโทรศัพท์มือถือ เปิดเผยตัวชี้แหล่งอินเทอร์เน็ต (URL) ที่พวกเขาเข้าชมและที่อยู่อีเมลที่พวกเขาติดต่อด้วย ให้กับผู้ให้บริการอินเทอร์เน็ต และเปิดเผยถึงหนังสือ ของชำ และยาที่พวกเขาซื้อ ให้กับผู้ขายปลีกทางอินเทอร์เน็ต ... ศาลไม่เชื่อว่าข้อมูลทั้งหมดที่มีการเปิดเผยโดยสมัครใจให้กับสมาชิกบางคนในพื้นที่ สาธารณะเพื่อจุดประสงค์เฉพาะอย่าง ไม่ควรได้รับการคุ้มครองตามข้อแก้ไขรัฐธรรมนูญครั้งที่ 4 (Fourth Amendment) เพียงเพราะ เหตุผลนั้นเพียงอย่างเดียว” United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2555) (Sotomayor, J., พิพากษาขึ้น)

กัน ล้วนเผยให้เห็นอัตลักษณ์ พฤติกรรม การสมาคม สภาพทางร่างกายและการรักษาพยาบาล เชื้อชาติ สีผิว รสนิยมทางเพศ ขาดิกำเนิด หรือทัศนคติของบุคคล หรือทำให้สามารถสร้างแผนที่บอกตำแหน่ง ความเคลื่อนไหว หรือปฏิสัมพันธ์ในช่วงเวลาหนึ่งของบุคคลดังกล่าว^๑ หรือของทุกคนในตำแหน่งที่กำหนด รวมถึงบริเวณการประชุมประท้วงหรือเหตุการณ์ทางการเมืองอื่น ๆ ด้วยเหตุดังกล่าว ข้อมูลทุกชนิดซึ่งรวมเอา สะท้อน เป็นผลมาจาก หรือเกี่ยวข้องกับการสื่อสารของบุคคล ซึ่งประชาชนทั่วไปไม่สามารถได้มาโดยทันทีและไม่สามารถเข้าถึงได้โดยง่าย จึงควรถือเป็น “ข้อมูลที่ได้รับการคุ้มครอง” และควรได้รับการคุ้มครองตามกฎหมายในระดับสูงสุด

ในการประเมินความรุกร้าของการสอดแนมการสื่อสารของรัฐ เราจำเป็นต้องพิจารณาทั้งสองสิ่งคือ ศักยภาพของการสอดแนมว่าสามารถเปิดเผยข้อมูลที่ได้รับการคุ้มครองเพียงใด และเป้าประสงค์ว่าข้อมูลดังกล่าวที่รัฐค้นหาไปเพื่ออะไร การสอดแนมการสื่อสารที่อาจนำไปสู่การเปิดเผยข้อมูลที่ได้รับการคุ้มครอง ซึ่งอาจทำให้บุคคลเสี่ยงที่จะถูกสอบสวน ถูกเลือกปฏิบัติ หรือถูกละเมิดสิทธิมนุษยชน ย่อมถือได้ว่าเป็นการละเมิดอย่างร้ายแรงต่อสิทธิในความเป็นส่วนตัวของบุคคล ทั้งยังส่งผลกระทบต่อการใช้สิทธิขั้นพื้นฐานอื่น ๆ รวมทั้งสิทธิในการแสดงออกอย่างเสรี การสมาคม และการเข้าร่วมกิจกรรมทางการเมือง ทั้งนี้เพราะการเข้าถึงสิทธิต่าง ๆ ดังกล่าวจะเกิดขึ้นได้ก็ต่อเมื่อบุคคลสามารถสื่อสารโดยปลอดจากความกลัวอันเกิดจากการสอดแนมของรัฐ การประเมินตัดสินโดยใช้ทั้งลักษณะและศักยภาพของการนำข้อมูลไปใช้จึงเป็นสิ่งจำเป็นสำหรับกรณีแต่ละกรณีเป็นการเฉพาะ

ในการนำเทคนิคการสอดแนมการสื่อสารแบบใหม่มาใช้ หรือในการขยายขอบเขตของเทคนิคที่มีอยู่ รัฐควรดูแลให้แน่ใจว่าข้อมูลเหล่านั้นถูกจัดได้ว่าเป็น “ข้อมูลที่ได้รับการคุ้มครอง” หรือไม่ ก่อนเริ่มค้นหาข้อมูลดังกล่าว และควรดำเนินการภายใต้การกำกับดูแลของศาล หรือกลไกกำกับดูแลตามระบอบประชาธิปไตย ในการพิจารณาว่าข้อมูลที่ได้มาจากการสอดแนมการสื่อสารนั้น อยู่ในระดับที่เป็น “ข้อมูลที่ได้รับการคุ้มครอง” หรือไม่ เราจำเป็นต้องคำนึงถึงรูปแบบรวมทั้งขอบเขตและระยะเวลาของการสอดแนมนั้นด้วย ทั้งนี้เนื่องจากการติดตามที่มีขอบเขตกว้างขวางหรือเป็นระบบสามารถเผยให้เห็นข้อมูลส่วนบุคคลที่มีรายละเอียดมากกว่าข้อมูลที่แยกเป็นส่วน ๆ การติดตามดังกล่าวสามารถยกระดับการสอดแนมข้อมูลที่ไม่ได้รับการคุ้มครองไปสู่ระดับที่เป็นการรุกร้าซึ่งจำเป็นต้องอยู่ใต้การคุ้มครองที่เข้มงวด^๑

^๑ “การติดตามระยะสั้นถึงการเคลื่อนไหวของบุคคลในถนนหนทางสาธารณะ สอดคล้องกับความคาดหวังเกี่ยวกับความเป็นส่วนตัว” แต่ “การใช้การติดตามระยะยาวด้วยระบบกำหนดตำแหน่งบนโลก (GPS) ในการสืบสวนความผิดส่วนใหญ่ ขัดกับความคาดหวังเกี่ยวกับความเป็นส่วนตัว” *United States v. Jones*, 565 U.S., 132 S. Ct. 945, 964 (2555) (Alito, J. พิพากษาอื่น)

^๑ “การสอดแนมระยะยาวเผยให้เห็นข้อมูลประเภทที่ไม่อาจหาได้จากการสอดแนมระยะสั้น อย่างเช่น สิ่งที่คุณคลิกกระทำซ้ำ ๆ สิ่งที่เขาไม่ทำ และสิ่งที่เขาเข้าพวก ข้อมูลประเภทเหล่านี้เผยให้เห็นเรื่องราวของคุณมากกว่าการเก็บข้อมูลแยกเป็นครั้ง ๆ ไป การที่คุณไปโบสถ์ โรงยิม บาร์เหล้า หรือป้อนการพนันบ่อยครั้ง เล่าเรื่องที่คุณไปครั้งเดียวแต่ละครั้งไม่ได้เล่า เช่นเดียวกับการที่คุณไม่ไปยังสถานที่เหล่านี้เลยในช่วงเวลาหนึ่งเดือนก็เล่าเรื่องอีกเรื่อง ข้อมูลการเคลื่อนไหวของคุณที่เป็นลำดับติดต่อกันยังสามารถเผยให้เห็นเรื่องราว

การตัดสินใจว่ารัฐสามารถทำการสอดแนมการสื่อสารได้หรือไม่ ถ้าการสอดแนมดังกล่าว
แทรกแซงข้อมูลที่ได้รับการคุ้มครอง จำเป็นต้องพิจารณาตามแนวของหลักการดังต่อไปนี้

หลักการ

ความชอบด้วยกฎหมาย

การจำกัดสิทธิความเป็นส่วนตัวต้องมีกฎหมายรองรับ รัฐต้องไม่รับรองหรือปฏิบัติตาม
มาตรการที่แทรกแซงสิทธิความเป็นส่วนตัวโดยปราศจากข้อกฎหมายรองรับ โดยข้อกฎหมายดังกล่าว
ต้องมีอยู่แล้ว สาธารณะสามารถเข้าถึงได้ และสอดคล้องกับมาตรฐานว่าด้วยความชัดเจนและความ
เที่ยงตรง ที่เพียงพอจะประกันได้ว่าบุคคลจะได้รับแจ้งล่วงหน้าถึงการใช้อกฎหมายและเล็งเห็นผลที่จะ
เกิดขึ้นจากการใช้อกฎหมายได้ เมื่อพิจารณาถึงอัตราการเปลี่ยนแปลงของเทคโนโลยีที่เป็นอยู่ กฎหมาย
ที่จำกัดสิทธิความเป็นส่วนตัวควรได้รับการทบทวนเป็นระยะ ทั้งนี้โดยผ่านกระบวนการนิติบัญญัติหรือ
การกำกับดูแลอย่างมีส่วนร่วม

เป้าหมายที่ชอบธรรม

กฎหมายควรอนุญาตให้การสอดแนมการสื่อสารทำได้เฉพาะโดยหน่วยงานของรัฐที่ถูกระบุ
อย่างเจาะจง เพื่อบรรลุเป้าหมายที่ชอบธรรมซึ่งสอดคล้องกับประโยชน์ในทางกฎหมายที่สำคัญและมี
ความจำเป็นต่อสังคมประชาธิปไตย ไม่ควรนำมาตรการใด ๆ มาใช้ในลักษณะที่เป็นการเลือกปฏิบัติ
บนฐานของเชื้อชาติ สีผิว เพศ ภาษา ศาสนา ความเห็นทางการเมืองหรือความเห็นอื่น ๆ ถิ่นกำเนิด
ทางชนชาติหรือสังคม ทรัพย์สิน การเกิด หรือสถานภาพอื่นใด

ที่ลึกซึ้งยิ่งไปกว่านั้น อย่างเช่น การเดินทางไปคลินิกสูตินรีเวชเพียงครั้งเดียวแทบไม่ให้อะไรเกี่ยวกับผู้หญิงคนหนึ่ง แต่ถ้าเป็นการ
เดินทางไปคลินิกสูตินรีเวชและอีกไม่กี่สัปดาห์ต่อมาจะมีการเดินทางไปยังร้านขายของสำหรับเด็ก ย่อมบอกเล่าเรื่องราวที่แตกต่างไป*
การที่บุคคลทราบถึงการเดินทางทั้งหมดของอีกบุคคลหนึ่ง ย่อมทำให้สามารถอนุมานได้ว่าบุคคลดังกล่าวเป็นคนที่ไปโบสถ์ประจำทุก
สัปดาห์หรือไม่ เป็นคนดื่มหนักหรือไม่ เป็นคนที่ชอบไปโรงยิมเป็นประจำหรือไม่ เป็นสามีที่ซื่อสัตย์หรือไม่ เป็นคนไขนอกที่ต้องเข้ารับ
การรักษาพยาบาลหรือไม่ เป็นสมาชิกของกลุ่มบุคคลหรือกลุ่มการเมืองใดหรือไม่ – และไม่รู้ข้อเท็จจริงเช่นนั้นของบุคคลดังกล่าว
เพียงเรื่องเดียว แต่ยั้งรู้ข้อเท็จจริงเช่นนั้นทุกเรื่อง” U.S. v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.)p. 562; U.S. v. Jones,
565 U.S. ___, (2555), Alito, J., พิพากษายืน “มากไปกว่านั้น ข้อมูลสาธารณะยังอาจอยู่ในขอบเขตของชีวิตส่วนตัวได้ กรณีที่มันถูก
รวบรวมและจัดเก็บอย่างเป็นระบบลงเพิ่มข้อมูลโดยหน่วยงานของรัฐ โดยเฉพาะอย่างยิ่งกรณีที่เป็นข้อมูลเกี่ยวกับอดีตที่ย้อนกลับไป
ไกลมากของบุคคล...ตามความเห็นของศาล ข้อมูลลักษณะดังกล่าว หากถูกรวบรวมและจัดเก็บอย่างเป็นระบบลงเพิ่มข้อมูลโดยเจ้า
พนักงานของรัฐ ย่อมอยู่ในขอบเขต ‘ชีวิตส่วนตัว’ ตามเป้าประสงค์ในมาตรา 8(1) ของอนุสัญญาดังกล่าว” (Rotaru v. Romania,
[2000] ECHR 28341/95, ย่อหน้า 43-44

ความจำเป็น

กฎหมายซึ่งอนุญาตให้รัฐสอดแนมการสื่อสาร ต้องจำกัดการสอดแนมไว้อย่างเข้มงวดและต้องสามารถพิสูจน์ให้เห็นได้ว่าการสอดแนมเป็นสิ่งจำเป็นเพื่อบรรลุเป้าหมายที่ชอบธรรม การสอดแนมการสื่อสารจะทำได้ก็ต่อเมื่อมันเป็นหนทางเดียวที่จะบรรลุเป้าหมายที่ชอบธรรมได้ หรือในกรณีที่มีหนทางอื่น มันต้องเป็นหนทางที่น่าจะละเมิดสิทธิมนุษยชนน้อยสุด ภาระพิสูจน์เหตุผลเพื่อการสอดแนมดังกล่าว ทั้งในกระบวนการทางศาลและกระบวนการนิติบัญญัติ ต้องตกเป็นของรัฐ

ความเพียงพอ

การสอดแนมการสื่อสารแต่ละครั้งที่ได้รับอนุญาตให้กระทำได้ตามกฎหมาย ต้องมีความเหมาะสมเพื่อให้บรรลุเป้าหมายที่ชอบธรรมได้ตามที่ระบุไว้อย่างเจาะจง

ความได้สัดส่วน

การสอดแนมการสื่อสารควรถือเป็นการกระทำที่มีความรุกร้าเป็นอย่างมาก มันแทรกแซงสิทธิความเป็นส่วนตัวและเสรีภาพในความคิดเห็นและการแสดงออก ซึ่งเป็นการคุกคามรากฐานของสังคมประชาธิปไตย การตัดสินใจใด ๆ เกี่ยวกับการสอดแนมการสื่อสาร ต้องกระทำโดยซึ่งนำหนักประโยชน์ที่เล็งเห็นว่าจะได้รับ เปรียบเทียบกับโทษที่อาจเกิดกับสิทธิของบุคคลและผลประโยชน์อื่น ๆ และควรคำนึงถึงความอ่อนไหวของข้อมูลและความร้ายแรงของการละเมิดสิทธิความเป็นส่วนตัว

กล่าวอย่างเจาะจง หลักการนี้กำหนดว่า หากรัฐพยายามหาหนทางเข้าถึงหรือใช้ข้อมูลที่ได้รับ การคุ้มครอง ผ่านการสอดแนมการสื่อสารในบริบทของการสอบสวนทางอาญา รัฐจะต้องพิสูจน์ยืนยันต่อหน่วยงานตุลาการที่มีความรู้ความสามารถ เป็นอิสระ และไม่ลำเอียงได้ว่า

1. มีความเป็นไปได้สูงว่าอาชญากรรมร้ายแรงได้เกิดขึ้นแล้วหรือกำลังจะเกิด
2. พยานหลักฐานของอาชญากรรมดังกล่าว จะสามารถได้มาด้วยการเข้าถึงข้อมูลที่ได้รับ การคุ้มครองที่ระบุ
3. ได้ใช้วิธีการสอบสวนอื่น ๆ ที่รุกร้าความเป็นส่วนตัวน้อยกว่านี้จนไม่เหลือวิธีที่ใช้ได้แล้ว
4. การเข้าถึงข้อมูลจะจำกัดอยู่เฉพาะส่วนที่เกี่ยวข้องโดยชอบกับอาชญากรรมตามที่มีการกล่าวหา และข้อมูลส่วนเกินที่ได้รับมาจะต้องถูกทำลายหรือถูกส่งกลับโดยทันที และ
5. ข้อมูลจะถูกเข้าถึงโดยหน่วยงานเฉพาะตามที่ระบุไว้ และจะถูกใช้สำหรับเป้าประสงค์เฉพาะตามที่ได้รับอนุญาตเท่านั้น

กรณีที่รัฐพยายามหาหนทางเข้าถึงข้อมูลที่ได้รับการคุ้มครอง ผ่านการสอดแนมการสื่อสาร สำหรับเป้าประสงค์ที่จะไม่เป็นเหตุให้บุคคลเสี่ยงต่อการถูกฟ้องคดีอาญา การถูกสอบสวน การถูกเลือกปฏิบัติ หรือการถูกละเมิดสิทธิมนุษยชน รัฐจะต้องพิสูจน์ยืนยันต่อหน่วยงานตุลาการที่เป็นอิสระ ไม่ลำเอียง และมีความรู้ความสามารถได้ว่า

1. ได้พิจารณาวิธีการสอบสวนอื่น ๆ ที่รุกรานความเป็นส่วนตัวส่วนตนน้อยกว่านี้แล้ว
2. การเข้าถึงข้อมูลจะจำกัดอยู่เฉพาะส่วนที่เกี่ยวข้องโดยชอบ และข้อมูลส่วนเกินที่ได้รับมา จะต้องถูกทำลายหรือถูกส่งกลับไปยังบุคคลที่ได้รับผลกระทบโดยทันที และ
3. ข้อมูลจะถูกเข้าถึงโดยหน่วยงานเฉพาะตามที่ระบุไว้ และจะถูกใช้สำหรับเป้าประสงค์เฉพาะตามที่ได้รับอนุญาตเท่านั้น

หน่วยงานตุลาการที่มีความรู้ความสามารถ

การตัดสินใจเกี่ยวกับการสอดแนมการสื่อสารต้องอยู่ใต้การวินิจฉัยของหน่วยงานตุลาการที่มีความรู้ความสามารถ ไม่ลำเอียง และเป็นอิสระ โดยหน่วยงานดังกล่าวจะต้อง

1. แยกออกจากหน่วยงานที่ทำการสอดแนมการสื่อสาร
2. มีประสบการณ์ในประเด็นที่เกี่ยวข้องและมีความรู้ความสามารถเพียงพอสำหรับการวินิจฉัยเกี่ยวกับความชอบด้วยกฎหมายของการสอดแนมการสื่อสาร เทคโนโลยีที่ใช้ และสิทธิมนุษยชน และ
3. มีทรัพยากรเพียงพอในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

กระบวนการอันควรตามกฎหมาย

กระบวนการอันควรตามกฎหมายกำหนดให้รัฐต้องเคารพและประกันสิทธิมนุษยชนของบุคคล โดยดูแลให้มั่นใจได้ว่า ขั้นตอนปฏิบัติที่ถูกต้องตามกฎหมายที่กำกับดูแลการแทรกแซงสิทธิมนุษยชน ถูกแจกแจงอย่างชัดเจนในกฎหมาย มีการปฏิบัติตามอย่างสม่ำเสมอ และเป็นข้อมูลที่ประชาชนทั่วไปรับทราบ กล่าวอย่างเจาะจง ในการตัดสินใจเกี่ยวกับสิทธิมนุษยชนของบุคคล บุคคลทุกคนย่อมมีสิทธิเข้าถึงการพิจารณาคดีอย่างเป็นธรรมและอย่างเปิดเผยต่อสาธารณะภายในระยะเวลาที่เหมาะสม โดยหน่วยงานตุลาการที่เป็นอิสระ มีความรู้ความสามารถ และไม่ลำเอียง ที่จัดตั้งขึ้นตามกฎหมาย¹⁰ เว้นแต่กรณีเร่งด่วนฉุกเฉิน กล่าวคือเมื่อมีภัยเฉพาะหน้าซึ่งจะทำให้เกิดอันตรายต่อชีวิตมนุษย์ ในกรณีเช่น

¹⁰คำว่า “กระบวนการอันควรตามกฎหมาย” (due process) มักใช้แทนกันกับคำว่า “ความเป็นธรรมในขั้นตอนปฏิบัติ” (procedural fairness) และ “ความยุติธรรมตามธรรมชาติ (natural justice)” ซึ่งมีการกล่าวถึงอย่างละเอียดในข้อ 6(1) ของอนุสัญญาว่าด้วยสิทธิมนุษยชนแห่งยุโรป (European Convention for Human Rights) และข้อ 8 ของอนุสัญญาว่าด้วยสิทธิมนุษยชนแห่งอเมริกา (American Convention on Human Rights)

นั้น จำเป็นต้องมีการขออนุมัติย้อนหลังภายในระยะเวลาที่เหมาะสม การอ้างเพียงความเสี่ยงว่าอาจมีการหลบหนีหรือการทำลายพยานหลักฐาน ไม่อาจถือเป็นเหตุผลที่เพียงพอสำหรับการลงมือปฏิบัติก่อนแล้วขออนุมัติย้อนหลัง

การแจ้งให้ผู้ใช้ทราบ

บุคคลพึงได้รับแจ้งข้อวินิจฉัยที่อนุญาตให้ทำการสอดแนมการสื่อสาร การแจ้งดังกล่าวต้องใช้เวลาและข้อมูลมากพอที่บุคคลจะสามารถอุทธรณ์คำวินิจฉัยได้ บุคคลควรสามารถเข้าถึงเอกสารหลักฐานที่ใช้เพื่อสนับสนุนการขออนุมัติดังกล่าว การชะลอการแจ้งออกไปจะกระทำได้เฉพาะในสถานการณ์ดังนี้

1. การแจ้งให้ทราบอาจส่งผลกระทบต่อเป้าประสงค์ของการสอดแนมที่ได้รับอนุมัติ หรือมีภัยเฉพาะหน้าซึ่งจะทำให้เกิดอันตรายต่อชีวิตมนุษย์ หรือ
2. ในขณะที่อนุมัติให้สอดแนมได้ หน่วยงานตุลาการที่มีความรู้ความสามารถยังอนุมัติให้ชะลอการแจ้งให้ทราบถึงการสอดแนมดังกล่าวได้ด้วย และ
3. บุคคลผู้ได้รับผลกระทบได้รับแจ้งทันทีที่ภัยผ่านพ้นไปแล้ว หรือภายในระยะเวลาที่เหมาะสมที่สามารถปฏิบัติได้ แล้วแต่ว่าเวลาใดจะถึงก่อน และจะต้องมีการแจ้งโดยทันทีเมื่อการสอดแนมการสื่อสารเสร็จสมบูรณ์แล้วไม่ว่าในสภาพการณ์ใด พันธกรณีในการแจ้งให้ทราบเป็นภาระของรัฐ แต่ในกรณีที่รัฐไม่แจ้งให้ทราบ ผู้ให้บริการการสื่อสารย่อมมีอิสระที่จะแจ้งให้บุคคลที่เกี่ยวข้องกับการสอดแนมการสื่อสารดังกล่าวได้ทราบ โดยสมัครใจ หรือเมื่อมีการร้องขอ

ความโปร่งใส

รัฐควรมีความโปร่งใสเกี่ยวกับการใช้และขอบเขตของการสอดแนมการสื่อสารทั้งในเรื่องเทคนิคและอำนาจ โดยอย่างน้อยควรตีพิมพ์เผยแพร่ข้อมูลภาพรวมเกี่ยวกับจำนวนการร้องขอที่ได้ อนุมัติและปฏิเสธ ข้อมูลการร้องขอที่จำแนกตามผู้ให้บริการแต่ละรายและตามประเภทและเป้าประสงค์ของการสอบสวน รัฐควรจัดหาข้อมูลให้บุคคลอย่างเพียงพอเพื่อช่วยให้เข้าใจอย่างเต็มที่ถึงขอบเขต ลักษณะ และการบังคับใช้กฎหมายที่อนุญาตให้มีการสอดแนมการสื่อสาร รัฐยังควรทำให้ผู้ให้บริการสามารถเผยแพร่ขั้นตอนปฏิบัติที่ตัวผู้ให้บริการจะใช้ในกรณีต้องอยู่เกี่ยวกับการสอดแนมการสื่อสารโดยรัฐ สามารถยึดถือขั้นตอนปฏิบัติดังกล่าว และสามารถเผยแพร่ประวัติการสอดแนมการสื่อสารโดยรัฐได้

การตรวจสอบโดยสาธารณะ

รัฐควรกำหนดให้มีกลไกตรวจสอบที่เป็นอิสระเพื่อประกันความโปร่งใสและความพร้อมรับผิดของการสอดแนมการสื่อสาร¹¹ กลไกตรวจสอบควรมีอำนาจในการเข้าถึงข้อมูลทุกอย่างที่อาจเกี่ยวข้องกับการปฏิบัติงานของรัฐ และหากเหมาะสมควรมีอำนาจในการเข้าถึงข้อมูลที่เป็นความลับหรือที่ถูกปกปิด กลไกตรวจสอบควรมีอำนาจในการประเมินว่ารัฐได้ใช้อำนาจตามกฎหมายอย่างชอบธรรมหรือไม่ มีอำนาจประเมินว่ารัฐได้ตีพิมพ์เผยแพร่ข้อมูลการใช้และขอบเขตของเทคนิคและอำนาจเกี่ยวกับการสอดแนมการสื่อสารอย่างโปร่งใสและอย่างแม่นยำหรือไม่ และมีอำนาจตีพิมพ์เผยแพร่รายงานตามกำหนดเวลาและข้อมูลอื่นที่เกี่ยวข้องกับการสอดแนมการสื่อสาร กลไกตรวจสอบที่เป็นอิสระนี้ควรกำหนดให้มีความคู่ไปกับการตรวจสอบใด ๆ ที่มีอยู่แล้วโดยหน่วยงานอื่นของรัฐ

ความคงสภาพของการสื่อสารและระบบ

เพื่อเป็นการประกันความคงสภาพ ความมั่นคงปลอดภัย และความเป็นส่วนตัวของระบบการสื่อสาร และเป็นการยอมรับข้อเท็จจริงที่ว่า ในแทบทุกครั้งที่มีการผ่านระดับความมั่นคงปลอดภัยลงเพื่อบรรลุเป้าประสงค์ของรัฐ ระดับความมั่นคงปลอดภัยโดยทั่วไปก็จะลดลงตามไปด้วย รัฐไม่ควรบังคับให้ผู้ให้บริการหรือผู้ขายฮาร์ดแวร์หรือซอฟต์แวร์ใส่ความสามารถในการสอดแนมหรือการติดตามลงในระบบของพวกเขา และไม่ควรมันบังคับให้รวบรวมหรือรักษาข้อมูลใด ๆ ที่เป็นไปเพื่อเป้าประสงค์ในการสอดแนมของรัฐเท่านั้น การรักษาหรือรวบรวมข้อมูลเอาไว้ก่อนไม่ควรถูกกำหนดเป็นหน้าที่ของผู้ให้บริการ บุคคลมีสิทธิแสดงออกถึงความคิดเห็นของพวกเขาโดยไม่ระบุชื่อ รัฐจึงควรงดเว้นจากการบังคับให้มีการระบุตัวตนผู้ใช้ โดยห้ามกำหนดเป็นเงื่อนไขก่อนการให้บริการ¹²

หลักประกันสำหรับความร่วมมือระหว่างประเทศ

เพื่อตอบสนองต่อการเปลี่ยนแปลงในการไหลของข้อมูลและการเปลี่ยนแปลงของเทคโนโลยีและบริการด้านการสื่อสาร รัฐอาจต้องขอความช่วยเหลือจากผู้ให้บริการจากนอกประเทศ ดังนั้นแล้วสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันทางกฎหมาย (mutual legal assistance treaties – MLATs) และความตกลงอื่นใดที่รัฐได้เข้าเป็นภาคี ควรประกันว่า ในกรณีที่เกิดกฎหมายของรัฐมากกว่าหนึ่งแห่งมีผลบังคับใช้ต่อการสอดแนมการสื่อสาร รัฐจะต้องเลือกปฏิบัติตามมาตรฐานการคุ้มครอง

¹¹ คณะกรรมการการคุ้มครองการสื่อสารแห่งสหราชอาณาจักร (UK Interception of Communications Commissioner) หรือไอซีไอ (ICO) เป็นตัวอย่างหนึ่งของกลไกตรวจสอบลักษณะดังกล่าว ไอซีไอตีพิมพ์รายงานซึ่งมีข้อมูลภาพรวมจำนวนหนึ่ง แต่ไม่ได้ให้ข้อมูลที่เพียงพอสำหรับการตรวจสอบโดยละเอียดถึงประเภทของคำร้อง ขอบเขตของการร้องขอเพื่อเข้าถึงข้อมูล เป้าประสงค์ของการร้องขอ และการวิเคราะห์ข้อมูลที่เกี่ยวข้อง โปรดดู <http://www.iocco-uk.info/sections.asp?sectionID=2&type=top>

¹² รายงานของผู้รายงานพิเศษว่าด้วยการส่งเสริมและการคุ้มครองสิทธิที่จะมีเสรีภาพในความคิดเห็นและการแสดงออก, Frank La Rue, 16 พฤษภาคม 2554, A/HRC/17/27, ย่อหน้า 84

บุคคลในระดับที่สูงกว่าเสมอ ในกรณีที่รัฐขอความช่วยเหลือเพื่อเป้าหมายในการบังคับใช้กฎหมาย ควรมีการนำหลักความผิดอาญาสองรัฐ (Dual Criminality) มาใช้ รัฐไม่อาจหลีกเลี่ยงการปฏิบัติตามข้อจำกัดของกฎหมายในประเทศที่ว่าด้วยการสอดแนมการสื่อสาร โดยใช้กระบวนการช่วยเหลือซึ่งกันและกันทางกฎหมายและคำร้องขอจากต่างประเทศเพื่อให้ได้รับข้อมูลที่ได้รับการคุ้มครอง กระบวนการช่วยเหลือซึ่งกันและกันทางกฎหมายและความตกลงอื่น ๆ ควรมีการจัดทำเป็นเอกสารอย่างชัดเจน มีการเผยแพร่ต่อสาธารณะ และอยู่ภายใต้หลักประกันเพื่อความเป็นธรรมในขั้นตอนปฏิบัติ

หลักประกันเพื่อป้องกันการเข้าถึงโดยมิชอบด้วยกฎหมาย

รัฐควรกำหนดกฎหมายเพื่อเอาผิดทางอาญากับการสอดแนมการสื่อสารที่ไม่ชอบด้วยกฎหมาย ทั้งที่กระทำโดยรัฐและเอกชน กฎหมายดังกล่าวควรกำหนดบทลงโทษทั้งทางแพ่งและอาญาอย่างเพียงพอและอย่างมีนัยสำคัญ กำหนดความคุ้มครองให้กับผู้เปิดเผยความไม่ชอบมาพากล และกำหนดช่องทางเยียวยาสำหรับบุคคลผู้ได้รับผลกระทบ กฎหมายต่าง ๆ ควรระบุเงื่อนไขด้วยว่าข้อมูลใด ๆ ที่ได้มาในลักษณะที่ไม่สอดคล้องกับหลักการทั้งหมดนี้ ย่อมไม่สามารถนำมาใช้เป็นพยานหลักฐานในศาลหรือกระบวนการยุติธรรมใด ๆ ได้ เช่นเดียวกับพยานหลักฐานซึ่งเป็นผลพวงมาจากข้อมูลดังกล่าว รัฐควรกำหนดกฎหมายด้วยว่าข้อมูลใด ๆ ที่ได้มาจากการสอดแนมการสื่อสาร ภายหลังจากที่ถูกใช้ตามเป้าประสงค์ของการค้นหาข้อมูลดังกล่าวแล้ว ข้อมูลเหล่านั้นจะต้องถูกทำลายหรือถูกส่งกลับไปยังบุคคลที่เกี่ยวข้อง

ผู้ลงนาม

Access, Article 19, Arab Digital Expression Foundation, Australia Privacy Foundation, Association for Progressive Communications, Bolo Bhi. Chaos Computer Club, Center for Internet & Society-India, Center for Technology and Society at Fundação Getulio Vargas, ContingenteMX, Digitale Gesellschaft, Digital Courage, Electronic Frontier Foundation, Human Rights Watch, International Federation of Library Associations and Institutions, La Quadrature du Net, European Digital Rights, Fundación Vía Libre, OpenMedia.ca, Open Rights Group, Pen International, Reporters Without Borders, Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, SHARE Foundation and Privacy International. ดูรายชื่อผู้ลงนามในหลักการนี้ทั้งหมด (องค์กรผู้เชี่ยวชาญ นักวิชาการ บุคคลสำคัญ เจ้าหน้าที่ที่มาจากการเลือกตั้ง และพรรคการเมือง) ได้ที่ <https://necessaryandproportionate.org/signatories>