แถลงการณ์สถานการณ์ด้านสิทธิในความเป็นอยู่ส่วนตัว

แถลงต่อการประชุมปรึกษาหารือระดับชาติเพื่อจัดทำรายงานทบทวนสถานการณ์สิทธิมนุษยชนของประเทศไทยรอบที่ 2 (22 ธันวาคม 2558) จัดโดยกระทรวงยุติธรรม[1]

1. แถลงการณ์นี้รายงานสถานการณ์ด้านสิทธิในความเป็นอยู่ส่วนตัว ซึ่งครอบคลุมประเด็นกฎหมาย โครงสร้างองค์กรอิสระ และข้อเสนอแนะสำหรับประเทศไทย ข้อมูลในคำแถลงนี้นำมาจากรายงานที่จัดทำโดย เครือข่ายพลเมืองเน็ต (Thai Netizen Network) ไพรเวซีอินเทอร์เนชันแนล (Privacy International)[2] และมูลนิธิศูนย์คุ้มครองสิทธิด้านเอดส์ (Foundation for AIDS Rights - FAR)[3]

2. ผม อาทิตย์ สุริยะวงศ์กุล นักวิจัยจากเครือข่ายพลเมืองเน็ต เป็นผู้อ่านแถลงการณ์ฉบับนี้ เครือข่ายพลเมืองเน็ตดำเนินงานภายใต้มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง ซึ่งเป็นองค์กรที่ทำงานเพื่อสนับสนุนสิทธิพลเมือง การมีส่วนร่วมในนโยบายด้านสารสนเทศและการสื่อสาร และช่วยเหลือการทำงานของนักปกป้องสิทธิมนุษยชนในยุคดิจิทัล

3. ข้อเสนอแนะในคำแถลงการณ์นี้มาจากการประชุมปรึกษาหารือและเวทีว่าด้วยนโยบายอินเทอร์เน็ต สิทธิพลเมือง และสิทธิในการพัฒนา ร่วมกับผู้มีส่วนได้ส่วนเสีย มาอย่างต่อเนื่องทั้งในระดับสากล ระดับภูมิภาค และระดับประเทศ เช่น เวทีการอภิบาลอินเทอร์เน็ตของสหประชาชาติ (2553-2558)[4], เวทีระดับภูมิภาคเอเชียแปซิฟิกว่าด้วยการอภิบาลอินเทอร์เน็ต (2553, 2555, 2557, 2558)[5], การประชุมว่าด้วยเทคโนโลยีและสิทธิพลเมือง (2555-2556)[6][7], สัมมนาสาธารณะ “บริการออนไลน์ไทยปลอดภัยแค่ไหน?: มาตรการทางกฎหมายและทางเทคโนโลยีที่เกี่ยวกับการจัดเก็บและการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย” (2557)[8][9], เวทีประชาสังคมไทยว่าด้วยการ

---

1 กระทรวงยุติธรรม โดยกรมคุ้มครองสิทธิฯ จัดประชุมรายงานสถานการณ์สิทธิมนุษยชนแห่งประเทศไทย ตามกลไก Universal Periodic Review (UPR) http://www.rlpd.go.th/rlpdnew/index.php/component/content/article?id=4488

2 The Right to Privacy – Stakeholder submission to Universal Periodic Review 2nd cycle on Thailand https://thainetizen.org/docs/right-to-privacy-stakeholder-submission-upr-thailand-2016/

3 ข้อมูลจากรายงานภายในของมูลนิธิศูนย์คุ้มครองสิทธิด้านเอดส์ ซึ่งผู้เขียนแถลงการณ์ได้รับระหว่างการประชุม

4 http://www.intgovforum.org/

5 http://www.aprigf.asia/

6 https://thainetizen.org/2012/07/technology-civil-rights-conf-31-july/

7 https://thainetizen.org/2013/09/tech-civil-rights-conf-2013-online-privacy-communications-surveillance/

8 https://thainetizen.org/2014/12/research-seminar-thai-online-security/

9 ถกหนัก กฎหมายดักฟัง นักกฎหมายเตือนต้องเจาะจง ชั่งน้ำหนักสาธารณะ VS บุคคล

อภิบาลอินเทอร์เน็ต (ก.พ. 2558)[10], เวทีระดับชาติว่าด้วยการอภิบาลอินเทอร์เน็ตของไทย (ก.ค. 2558)[11], และ Asia Regional Consultation on the World Summit on the Information Society+10 Review (ก.ย. 2558)[12]

สิทธิในความเป็นอยู่ส่วนตัว

4. สิทธิในความเป็นอยู่ส่วนตัวเป็นสิทธิมนุษยชนขั้นพื้นฐาน และเป็นหัวใจในการปกป้องศักดิ์ศรีความเป็นมนุษย์และเป็นรากฐานของสังคมประชาธิปไตยทุกแห่ง

5. สิทธิในความเป็นอยู่ส่วนตัวยังสนับสนุนและส่งเสริมสิทธิอื่นๆ เช่น เสรีภาพในการแสดงออก การเข้าถึงข้อมูลข่าวสาร และการรวมตัวสมาคม Martin Scheinin ผู้รายงานพิเศษของสหประชาชาติว่าด้วยสิทธิมนุษยชนและการต่อต้านการก่อการร้ายกล่าวว่า สิทธิในความเป็นส่วนตัวตั้งอยู่บนหลักการที่ว่า บุคคลควรมีพื้นที่สำหรับการพัฒนาอย่างเป็นอิสระ สำหรับการแลกเปลี่ยน และสำหรับเสรีภาพ เป็น “ปริมณฑลส่วนตัว” ที่อาจมีการติดต่อหรือไม่ติดต่อกับผู้อื่น ปราศจากการถูกรัฐแทรกแซงโดยพลการและจากการรบกวนโดยบุคคลที่ไม่ได้รับเชิญ[13]

6. กิจกรรมที่จำกัดสิทธิในความเป็นอยู่ส่วนตัว เช่น การสอดส่องตรวจตราและการปิดกั้นเนื้อหา จะสมเหตุผลก็ต่อเมื่อมันถูกประกาศเป็นกฎหมายอยู่แล้ว มีความจำเป็นอันหลีกเลี่ยงไม่ได้เพื่อที่จะบรรลุเป้าประสงค์ที่ชอบธรรม และทำไปตามสัดส่วนที่สมควรกับเป้าประสงค์ที่ต้องการ

7. นวัตกรรมในเทคโนโลยีสารสนเทศ ทำให้การเก็บ บันทึก ประมวลผล และกระจายข้อมูลส่วนบุคคลในรูปแบบที่ไม่เคยมีใครจินตนาการได้มาก่อน สามารถทำได้ ข้อวินิจัยลำดับที่ 16 ในปี 2531 ของคณะกรรมการสิทธิมนุษยชนแห่งสหประชาชาติ ระบุว่าสิทธิในความเป็นอยู่ส่วนตัว ได้พัฒนามาสู่จุดที่พันธกรณีของรัฐที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องที่สำคัญอย่างยิ่งยวด[14]

8. ประเทศไทยให้สัตยาบันในกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) โดยไม่ได้

---

https://thainetizen.org/2014/12/seminar-surveillance-law/

10 https://igf.in.th/csdig2015/

11 https://igf.in.th/

12 http://wsis10.asia/

13 Martin Scheinin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamentalfreedoms while countering terrorism, 2009, A/HRC/17/34 http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A.HRC.10.3.pdf

14 Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home andcorrespondence, and protection of honour and reputation (art. 17).

กำหนดข้อยกเว้นในข้อ 17 และข้อ 19 ว่าด้วยสิทธิในความเป็นอยู่ส่วนตัวและเสรีภาพในการแสดงออกตามลำดับ กติกาข้อ 17 กล่าวว่า “บุคคลจะถูกแทรกแซงความเป็นส่วนตัว ครอบครัว เคหสถาน หรือการติดต่อสื่อสารโดยพลการหรือไม่ชอบด้วยกฎหมายมิได้ และจะถูกลบหลู่เกียรติและชื่อเสียงโดยไม่ชอบด้วยกฎหมายมิได้”

9. เช่นเดียวกับรัฐสมาชิกอาเซียนอื่นๆ ประเทศไทยเป็นภาคีปฏิญญาอาเซียนว่าด้วยสิทธิมนุษยชน ตั้งแต่วันที่ 18 พฤศจิกายน 2555 ซึ่งข้อ 21 ระบุว่า “บุคคลทุกคนมีสิทธิที่จะเป็นอิสระจากการแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร ซึ่งรวมถึงข้อมูลส่วนบุคคล หรือการดูหมิ่นเกียรติและชื่อเสียงของบุคคลนั้น บุคคลทุกคนมีสิทธิที่จะได้รับการคุ้มครองทางกฎหมายจากการแทรกแซงหรือการดูหมิ่นดังกล่าว”

การประเมินผลโดยสรุปของการดำเนินการตามข้อเสนอแนะในการทบทวนครั้งที่ 1

10. ไม่มีการกล่าวถึงสิทธิในความเป็นอยู่ส่วนตัว การสอดส่อง และการคุ้มครองข้อมูลส่วนบุคคล โดยชัดแจ้งในรายงานจากประเทศไทยในการทบทวนครั้งที่ 1[15]

11. ประเด็นที่เกี่ยวข้องกับสิทธิในความเป็นอยู่ส่วนตัวที่ถูกพูดถึงโดยผู้มีส่วนได้ส่วนเสีย เป็นประเด็นที่สัมพันธ์กับสิทธิเด็กที่ตกเป็นเหยื่อ และการสมรสในวัยเยาว์ของเด็กผู้หญิง[16]

ประเด็นปัญหา

12. แม้ประเทศไทยจะมีกฎหมายอยู่หลายฉบับที่ให้อำนาจกับเจ้าหน้าที่รัฐในการค้นตัวบุคคล เคหสถาน และดักรับข้อมูลการสื่อสาร[17] และกฎหมายที่รัฐบังคับให้หน่วยงานในหลายกิจการมีหน้าที่ต้องจัดเก็บข้อมูลของประชาชน[18] ครอบคลุมกิจกรรมในชีวิตของประชาชนในแทบทุกมิติ แต่ประเทศไทยยังไม่มีกฎหมายคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวหรือกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปเลย[19] กฎหมายคุ้มครองข้อมูลส่วน

---

15 A/HRC/WG.6/12/THA/1

16 A/HRC/WG.6/12/THA/3, para 40

17 เช่น ประมวลกฎหมายวิธีพิจารณาความอาญา, มาตรา 6 และมาตรา 9 ในกฎอัยการศึก, พ.ร.บ.การสอบสวนคดีพิเศษ พ.ศ. 2552, พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, พ.ร.บ.ป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, และพ.ร.บ.ป้องกันและปราบปรามยาเสพติด พ.ศ. 2519

18 เช่น พ.ร.บ.การประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545, พ.ร.บ.ประกอบกิจการโทรคมนาคม พ.ศ 2544, พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, และประกาศกสทช. เรื่อง การจัดเก็บข้อมูลและรายละเอียดเกี่ยวกับผู้ใช้บริการโทรศัพท์เคลื่อนที่ในลักษณะที่เรียกเก็บเงินล่วงหน้า พ.ศ. 2558

19 กิจการบางประเภทมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะสำหรับกิจการประเภทนั้น เช่น ข้อมูลส่วนบุคคลในกิจการโทรคมนาคม ถูกคุ้มครองโดย ประกาศกทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม พ.ศ. 2549 และข้อมูลสุขภาพ ถูกคุ้มครองโดย พ.ร.บ.สุขภาพแห่งชาติ พ.ศ. 2550

บุคคลที่ครอบคุลมที่สุดของประเทศไทยในขณะนี้ คือ พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งคุ้มครองเฉพาะข้อมูลส่วนบุคคลที่อยู่ในความดูแลของหน่วยงานของรัฐ ในขณะที่โลกสมัยใหม่ บริการสาธาณะถูกให้บริการโดยเอกชนเป็นจำนวนมากขึ้นโดยลำดับ ตัวอย่างเช่น กิจการการสื่อสาร อินเทอร์เน็ต และขนส่งมวลชน

13. ในเรื่องของการค้นตัวและค้นสถานที่ มีความเป็นห่วงในเรื่องของการตั้งเข้าค้นหรือตั้งด่านค้นและตรวจปัสสาวะเพื่อตรวจหายาเสพติดที่ไม่มีการกำกับดูแลอย่างเพียงพอ จนนำไปสู่การใช้อำนาจโดยมิชอบโดยผู้บังคับใช้กฎหมาย มูลนิธิศูนย์คุ้มครองสิทธิด้านเอดส์ระบุผลการศึกษาที่พบว่า ร้อยละ 48 ของผู้ใช้ยาเสพติดด้วยวิธีการฉีด (PWID) เคยถูก “ยัดยา” โดยตำรวจ และร้อยละ 48 ของกลุ่มดังกล่าวเคยจ่ายเงินสินบนเพื่อหลีกเลี่ยงการถูกจับ

14. นอกจากนี้ ตั้งแต่การรัฐประหารเมื่อวันที่ 22 พฤษภาคม 2557 เมื่อมีการจับกุมผู้ร่วมชุมนุม เจ้าหน้าที่รัฐได้เริ่มยึดคอมพิวเตอร์และอุปกรณ์การสื่อสารไปจากผู้ที่ถูกจับกุม จนการยึดอุปกรณ์ไปตรวจค้นข้อมูลและการขอรหัสผ่านเพื่อเข้าถึงข้อมูลส่วนบุคคลกลายเป็นหลักปฏิบัติทั่วไป[20]

15. ความพยายามของเจ้าหน้าที่ในการเข้าถึงอุปกรณ์สื่อสารและข้อมูลส่วนบุคคลของนักกิจกรรม ยังขยายขอบเขตไปสู่การคุกคามทนายความของนักกิจกรรมอีกด้วย กลางดึกวันที่ 26 มิถุนายน 2558 จนถึงช่วงเย็นของวันที่ 27 มิถุนายน 2558 รถยนต์ส่วนตัวของทนายความประจำศูนย์ทนายความเพื่อสิทธิมนุษยชนถูกกักไว้หน้าศาลทหาร หลังเจ้าหน้าที่ตำรวจและทหารพยายามเข้าค้นรถคันดังกล่าว ตั้งแต่กลางดึกวันที่ 26 มิ.ย. โดยมีเป้าหมายคือโทรศัพท์มือถือและอุปกรณ์คอมพิวเตอร์ที่อยู่ในรถ ซึ่งจำนวนหนึ่งเป็นของนักศึกษาและนักกิจกรรมต้านรัฐประหารบางส่วนที่ถูกจับในวันที่ 26 มิถุนายน ในคดีฝืนคำสั่งหัวหน้า คสช. และประมวลกฎหมายอาญามาตรา 116[21] อย่างไรก็ตาม กลุ่มทนายยืนยันปฏิเสธไม่ให้ค้นรถเนื่องจากเจ้าหน้าที่ไม่มีหมายค้น เจ้าหน้าที่จึงล็อกล้อรถและนำแผงเหล็กมากั้นโดยรอบ ไม่ให้มีการเข้าออกหรือเปิดเข้าไปในรถได้ และพยายามให้กลุ่มทนายสิทธิกลับไปก่อน แต่กลุ่มทนายยืนยันขอเฝ้ารถถึงเช้าจนกว่าจะมีความชัดเจนเรื่องอำนาจการค้น

16. การค้นข้อมูลโดยไม่มีหมายค้น ยังนำไปสู่การไม่ปฏิบัติตามหลักการเก็บรักษาข้อมูลและพยานหลักฐานทางอิเล็กทรอนิกส์ โดยในช่วงบ่ายของวันที่ 27 มิถุนายน 2558 หลังตำรวจพร้อมเจ้าหน้าที่กองพิสูจน์หลักฐานนำหมายค้นของศาลอาญา มายังรถของทนายความเพื่อขอตรวจค้นรถ ตามคำยืนยันของทนายความว่าการตรวจค้น

---

20 มีรายงานถึงการบังคับให้ผู้ร่วมชุมที่ถูกจับกุม บอกรหัสผ่านของโทรศัพท์ รหัสผ่านของบัญชีอีเมล และรหัสผ่านของบัญชีสื่อสังคมออนไลน์ นักกิจกรรมที่เชียงใหม่รายหนึ่งให้ข้อมูลว่าระหว่างที่ถูกควบคุมตัวโดยเจ้าหน้าที่ทหาร เจ้าหน้าที่ได้ขอรหัสผ่านเฟซบุ๊กไปจากเขา หลังจากนั้นเมื่อถูกปล่อยตัว เขาเปลี่ยนรหัสผ่านใหม่ ต่อมาเจ้าหน้าที่ได้โทรศัพท์หาเขา ต่อว่าทำไมถึงเปลี่ยนรหัสผ่าน

21 https://tlhr2014.wordpress.com/2015/07/01/%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%A1%E0%B8%A7%E0%B8%A5%E0%B8%AA%E0%B8%96%E0%B8%B2%E0%B8%99%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%93%E0%B9%8C-%E0%B8%82%E0%B8%9A%E0%B8%A7%E0%B8%99%E0%B8%81%E0%B8%B2%E0%B8%A3/

จะต้องมีหมายค้น ระหว่างการตรวจค้นยังไม่สิ้นสุด เจ้าหน้าที่ตำรวจ 2 นายได้นำโทรศัพท์มือถือที่พบทั้งหมด 5 เครื่อง ขึ้นมอเตอร์ไซค์ไปจากจุดตรวจค้น โดยไม่ได้ปิดผนึกซองเก็บพยานหลักฐานและไม่ได้ทำบันทึกการยึด ขณะที่พนักงานพิสูจน์หลักฐานยังสับสนอยู่ว่าเกิดอะไรขึ้น ท่ามกลางการทักท้วงของทนายและผู้อยู่ในเหตุการณ์ ก่อนที่อีกประมาณ 12 นาทีถัดมา เจ้าหน้าที่ตำรวจรายดังกล่าวจะนั่งรถกระบะของตำรวจนำโทรศัพท์กลับมาคืนให้พนักงานพิสูจน์หลักฐาน และยอมรับว่าได้ทำผิดขั้นตอน แต่ยืนยันว่าไม่ได้เปิดเครื่องหรือแก้ไขข้อมูลภายในเครื่องแต่อย่างใด

17. การขอรหัสผ่านโทรศัพท์ บัญชีอีเมล และสื่อสังคมออนไลน์จากผู้ถูกจับกุม การยึดอุปกรณ์ และการจัดเก็บพยานหลักฐานที่เป็นอุปกรณ์สื่อสารอย่างผิดหลักการ ทำให้มีความเป็นห่วงถึงความน่าเชื่อถือของหลักฐานพยานต่างๆ ที่เจ้าหน้าที่ใช้ดำเนินคดี ไม่ว่าจะเป็นกรณีผู้ชุมนุมหรือกรณีประชาชนทั่วไป โดยเฉพาะกับหลักฐานข้อความการสื่อสารที่ถูกเผยแพร่ภายใต้ชื่อบัญชีของผู้ถูกจับกุม

18. สำหรับการเข้าถึงข้อมูลหรือสอดแนมการสื่อสารเพื่อประโยชน์ในการบังคับใช้กฎหมาย ประเทศไทยยังไม่มีมาตรฐานในทางกฎหมายที่ใช้เป็นการทั่วไปเพื่อกำกับการเข้าถึงข้อมูลส่วนบุคคล ทำให้พบความไม่สม่ำเสมอในกลไกการตรวจสอบการใช้อำนาจ เช่น มีเงื่อนไขการขอคำสั่งศาล ความเฉพาะเจาะจงของคำร้องต่อศาล ระยะเวลาที่เข้าถึงข้อมูลได้ เงื่อนไขการขอขยายระยะเวลาเข้าถึงข้อมูล และระยะเวลาสูงสุดที่สามารถเข้าถึงข้อมูลได้แตกต่างกัน ทั้งที่ข้อมูลที่เข้าถึงอาจเป็นข้อมูลชนิดเดียวกัน[22][23]

กฎหมาย/ร่างกฎหมาย	มาตรา	ใช้คำสั่ง/หมายศาล?	คำร้องเจาะจง?	ระบุระยะเวลา?
(ร่าง) มั่นคงปลอดภัยไซเบอร์	35	ไม่ระบุ	ไม่ระบุ	ไม่ระบุ
(ร่าง) สิ่งยั่วยุพฤติกรรมอันตราย	16	ใช้	ไม่เจาะจง	ไม่ระบุ
(ร่าง) วิธีพิจารณาความอาญา	131/2	ใช้	เจาะจง	15 วัน (x4 คราว รวมไม่เกิน 90 วัน)
คอมพิวเตอร์	18	แล้วแต่กรณี	ไม่เจาะจง	ไม่ระบุ
สอบสวนคดีพิเศษ	25	ใช้	เจาะจง	90 วัน (ไม่มีเพดาน)

22 ใน พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 18, พ.ร.บ.การสอบสวนคดีพิเศษ มาตรา 25, ร่าง พ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรา 35, ร่าง พ.ร.บ.ป้องกันและปราบปรามสิ่งยั่วยุพฤติกรรมอันตราย มาตรา 16, ร่าง พ.ร.บ.แก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความอาญา (เข้าถึงข้อมูลข่าวสารของผู้ต้องสงสัย) มาตรา 131/2

23 http://ilaw.or.th/node/3400

19. เมื่อ วันที่ 15 ธันวาคม 2557 กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ออกคำสั่งที่ 163/2557 แต่งตั้งคณะทำงานทดสอบระบบเฝ้าติดตามสื่อออนไลน์ ซึ่งประกอบด้วยกรรมการ 39 คน ในจำนวนนี้เป็นตำรวจและฝ่ายความมั่นคง 30 คน เพื่อจัดหาและทดสอบอุปกรณ์ที่สามารถตรวจสอบและปิดกั้นเว็บไซต์ที่มีการเข้ารหัสป้องกันข้อมูล (SSL: Secure Socket Layer) และประสานทางเทคนิคกับผู้ให้บริการอินเทอร์เน็ตภายในประเทศและที่เชื่อมต่อกับต่างประเทศโดยตรง (International Internet Gateway) ในการทดสอบระบบเฝ้าติดตามสื่อออนไลน์ การติดตั้งระบบดังกล่าวจะทำให้เจ้าหน้าที่มีความสามารถในการดูข้อมูลทุกอย่างที่ส่งผ่านสื่อออนไลน์ได้[24] รายงานโดยวารสารเทเลคอมเอเชียระบุแหล่งข่าวที่เป็นผู้ให้บริการเครือข่ายที่ใช้บริการของ กสท โทรคมนาคม ระบุว่า กสท โทรคมนาคม อาจเกี่ยวข้องกับการใช้ใบอนุญาตการเข้ารหัส SSL ปลอม. ในเดือนมกราคม 2558 มีรายงานว่าผู้ให้บริการอินเทอร์เน็ตภายในประเทศถูกร้องขอจากกระทรวงไอซีทีให้ติดตั้งอุปกรณ์ที่สามารถดูรหัสผ่านของผู้ใช้เฟซบุ๊กได้

20. คำสั่งของกระทรวงไอซีทีดังกล่าว สอดคล้องกับโครงการ “ซิงเกิลเกตเวย์” ซึ่งถูกเสนอขึ้นมาโดยปลัดกระทรวงไอซีทีในสัปดาห์แรกหลังการรัฐประหารเมื่อเดือนพฤษภาคม 2557 และเป็นข่าวใหญ่อีกครั้งในเดือนกันยายน 2558 โครงการซิงเกิลเกตเวย์ดังกล่าว มีสาระสำคัญคือเพื่อให้สามารถตรวจสอบและปิดกั้นข้อมูลจากต่างประเทศได้ โดยไม่จำเป็นต้องร้องขอให้ผู้ให้บริการเป็นผู้ทำให้ ความกังวลในเรื่องนี้คือ วิธีดังกล่าวสามารถลัดขั้นตอนการขออนุญาตจากศาล ทำให้เป็นไปได้ที่จะใช้อำนาจในทางที่ผิดได้ในทันที โดยไม่มีการบันทึกประวัติเป็นลายลักษณ์อักษร ทำให้เอาผิดกับผู้ใช้อำนาจในทางที่ผิดย้อนหลังได้ยาก

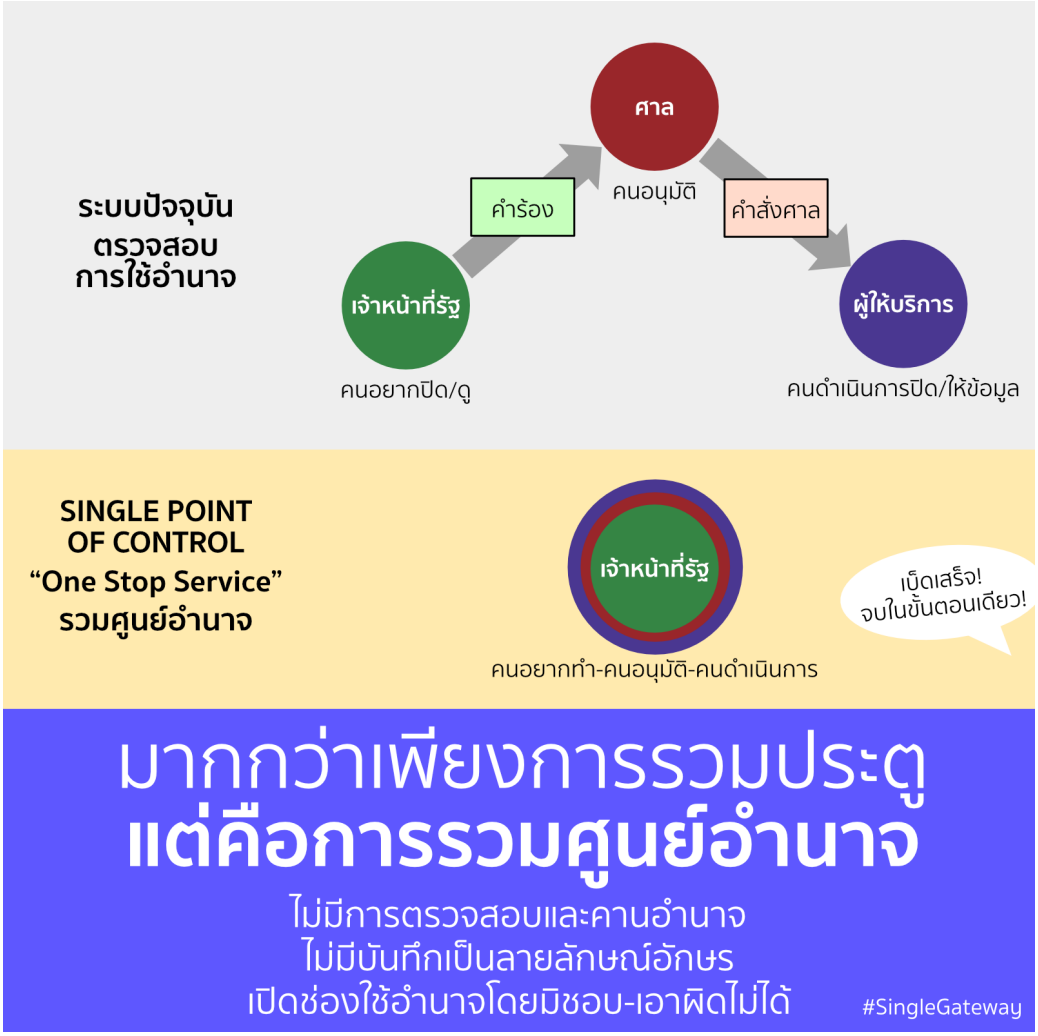
21. ความต้องการในการเข้าถึงข้อมูลการสื่อสารของประชาชน โดยไม่จำเป็นต้องผ่านการตรวจสอบการใช้อำนาจที่เหมาะสม ยังปรากฏผ่านการตรวจพบการใช้และสั่งซื้อซอฟต์แวร์ที่ชื่อว่า Remote Control System (RCS) ในประเทศไทย RCS เป็นซอฟต์แวร์ที่ผลิตโดยบริษัท Hacking Team ซึ่งสามารถฝังตัวลงในคอมพิวเตอร์และโทรศัพท์มือถือ เพื่อจัดเก็บข้อมูลโดยผู้ใช้ไม่รู้ตัว RCS และเนื่องจากเป็นการจัดเก็บที่ตัวอุปกรณ์ก่อนที่ข้อมูลจะถูกเข้ารหัสและส่งออกไปนอกอุปกรณ์ ทำให้การเข้ารหัสข้อมูลไม่มีประโยชน์ RCS ยังสามารถควบคุมการทำงานของอุปกรณ์ได้จากระยะไกล[25] ศูนย์วิจัย Citizen Lab ของมหาวิทยาลัยโทรอนโร ประเทศแคนาดา ตรวจพบการใช้ Remote Control System (RCS) ในประเทศไทย[26]

---

24 https://www.facebook.com/thainetizen/photos/a.10150109699603130.289409.116319678129/10153052852963130/

25 https://thainetizen.org/2015/07/surveillance-trends-challenges-and-opportunities-in-asia-pacific/

26 Marczak, Bi., Guarnieri, C., Marquis-Boire, M, and Scott-Railton, J., Mapping Hacking Team's “Untraceable” Spyware, TheCitizenLab, University of Toronto, February 2014. Available at: https://citizenlab.org/wp-content/uploads/2015/03/Mapping-Hacking-Team%E2%80%99s-_Untraceable_-Spyware.pdf



22. จากเอกสารของ Hacking Team ที่หลุดรั่วออกมา ในเดือนกันยายน 2555 ตัวแทนของ Hacking Team เข้าพบเจ้าหน้าที่รัฐบาลไทย ซึ่งรวมถึงเจ้าหน้าที่จากสำนักนายกรัฐมนตรี สำนักงานข่าวกรองแห่งชาติ กอ.รมน. กระทรวงกลาโหม กองทัพบก และกรมราชทัณฑ์[27] หกเดือนหลังจากนั้น สำนักงานความมั่นคงแห่งชาติ สอบถาม Hacking Team อย่างเจาะจงว่า สามารถดักฟัง LINE, WeChat, และ WhatsApp ได้หรือยัง[28] ในเดือนเมษายน 2557 มีอีเมลยืนยันว่าผลิตภัณฑ์ของ Hacking Team สามารถดักฟังแอปเหล่านั้นได้แล้ว[29] ในเดือนมิถุนายน 2558 มีการแลกเปลี่ยนอีเมลและเอกสารยืนยันว่าผลิตภัณฑ์ Remote Control System Galileo ถูกสั่งซื้อแล้ว และกำลังจะถูกจัดส่งมายังประเทศไทย[30]

---

27 Wikileaks files published 8 July 2015, Hacking Team, Thailand Project. Available at:https://wikileaks.org/hackingteam/emails/emailid/445474

28 Wikileaks files published 8 July 2015, Hacking Team: LH for Thailand National Security Council. Available at: https://wikileaks.org/hackingteam/emails/emailid/445665

29 Wikileaks files published 8 July 2015, Hacking Team: Japanese Messaging App Line Gian Traction Abroad. Available at: https://wikileaks.org/hackingteam/emails/emailid/11249

30 Wikileaks files published 8 July 2015, RE: (Draft) End User Statement. Available at:See also: TIKIT Delivery Preparation, Available at https://ht.transparencytoolkit.org/FAE%20DiskStation/5.%20SWAP/TIKIT

23. ร่างพ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มาตรา 35 ให้อำนาจเจ้าหน้าที่เข้าถึงข้อมูลได้โดยไม่มีการกล่าวถึงกลไกการตรวจสอบการใช้อำนาจ ส่วนมาตรา 33 และ 34 ซึ่งให้อำนาจสำนักงานความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีอำนาจในการสั่งการให้หน่วยงานรัฐ เอกชน และบุคคล กระทำการหรือไม่กระทำการใดๆ ก็ได้ในประการที่จะเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ก็เป็นการให้อำนาจที่กว้างขวางเช่นเดียวกับกฎหมายอัยการศึก แต่ในร่างปัจจุบันไม่มีกล่าวถึงการตรวจสอบการใช้อำนาจเลย

24. ที่น่าตกใจยิ่งกว่า คือในร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล[31] กำหนดให้สำนักงานความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นสำนักงานเลขานุการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ทั้งที่ลักษณะงานนั้นมีความขัดแย้งกันอยู่ คืองานด้านหนึ่งมีโอกาสละเมิดสิทธิเสรีภาพสูง ในขณะอีกด้านหนึ่งต้องทำหน้าที่คุ้มครองสิทธิ ทำให้มีความกังวลว่าคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในโครงสร้างนี้ ซึ่งอยู่ใต้กระทรวงอีกหนึ่งด้วย จะทำหน้าที่ปกป้องสิทธิเสรีภาพได้เพียงใด โดยเฉพาะถ้าการละเมิดนั้นมาจากรัฐ

25. เช่นเดียวกับ ร่างพ.ร.บ.กสทช. ที่เตรียมเสนอสู่สภานิติบัญญัติแห่งชาติ ที่มีการปรับโครงสร้างคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ จากปัจจุบันที่เป็นองค์กรกำกับอิสระ มาเป็นองค์กรที่จะมีนายกรัฐมนตรีนั่งเป็นประธานกรรมการ กสทช.เป็นองค์กรกำกับกิจการสื่อและการสื่อสาร มีอำนาจออกใบอนุญาตและยึดใบอนุญาตสื่อ กำหนดมาตรฐานเนื้อหา มีหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่ส่งผ่านทางโทรคมนาคม ทำให้มีความเป็นห่วงถึงการแทรกแซงจากฝ่ายการเมือง ที่จะกระทบต่อเสรีภาพสื่อและการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวทางการสื่อสาร

%20%28Thailand%29/TIKIT_Delivery_Preparation.txt, Delivery Certificate https://ht.transparencytoolkit.org/FAE%20DiskStation/5.%20SWAP/TIKIT%20%28Thailand%29/TIKIT_Delivery_Certificate.pdf

31 http://ictlawcenter.etda.or.th/de_laws/detail/de-laws-data-privacy-act

ข้อเสนอแนะ

26. จัดให้มีการอบรมถึงการปฏิบัติที่ถูกต้องตามหลักสิทธิมนุษยชนอย่างต่อเนื่องให้กับผู้บังคับใช้กฎหมาย เช่น เจ้าหน้าที่ ณ ด่านตรวจค้น เจ้าหน้าที่ตามพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เจ้าหน้าที่ตามพ.ร.บ.การสอบสวนคดีพิเศษ และจะต้องมีระบบการตรวจสอบภายในที่มีประสิทธิภาพเพื่อป้องกันการใช้อำนาจในทางมิชอบ การละเมิดโดยเจ้าหน้าที่จะต้องได้รับการจัดการอย่างเคร่งครัด การออกนโยบายมาตรการหรือข้อปฏิบัติใดๆ โดยหน่วยงานบังคับใช้กฎหมาย ที่อาจกระทบกับสิทธิในความเป็นอยู่ส่วนตัวของประชาชน จะต้องผ่านการปรึกษาหารือร่วมกับคณะกรรมการสิทธิมนุษยชนแห่งชาติและคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

27. ทบทวนและปรับปรุงกฎหมายที่เกี่ยวกับการดักฟัง ดักรับ และจัดเก็บข้อมูลให้มีความสม่ำเสมอกัน ยกเลิกข้อกฎหมายที่ซ้ำซ้อน (สำหรับการเข้าถึงข้อมูลในคดีที่เป็นความผิดอาญา ให้อ้างอิงตามประมวลกฎหมายวิธีพิจารณาความอาญาที่จะมีการแก้ไขเพิ่มเติมใหม่ ไม่ต้องกำหนดซ้ำอีก) และปรับปรุงข้อกฎหมายให้ได้มาตรฐานสิทธิมนุษยชนระหว่างประเทศ โดยพิจารณาตามหลักการระหว่างประเทศว่าด้วยการใช้หลักสิทธิมนุษยชนกับการสอดแนมการสื่อสาร (International Principles on the Application of Human Rights to Communications Surveillance)[32] และรายงานของสำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติว่าด้วย “สิทธิความเป็นส่วนตัวในยุคดิจิทัล” (The Right to Privacy in the Digital Age) (A/HRC/27/37)[33]

28. ทำให้แน่ใจได้ว่า การดักฟังดักรับข้อมูลทุกอย่าง จะถูกใช้ก็ต่อเมื่อมีการอนุญาตจากฝ่ายตุลาการ และทำตามหลักความชอบด้วยกฎหมาย ความชอบธรรม ความได้สัดส่วน และความจำเป็น ไม่ว่าผู้ถูกสอดแนมนั้นจะมีสัญชาติใดหรืออยู่ที่แห่งใด

29. เร่งออกข้อปฏิบัติว่าด้วยการปฏิบัติกับข้อมูลส่วนบุคคลในหลักฐานทางนิติวิทยาศาสตร์ เช่น รหัสพันธุกรรม หลักฐานทางอิเล็กทรอนิกส์ ข้อมูลการสื่อสาร

30. แก้ไขร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต้องเป็นองค์กรกำกับที่เป็นอิสระ (Independent Regulatory Agency) ที่ไม่ขึ้นกับฝ่ายการเมือง ฝ่ายราชการ และฝ่ายความมั่นคง เนื่องจากหน้าที่ส่วนหนึ่งของคณะกรรมการดังกล่าวจะต้องตรวจสอบการใช้อำนาจของรัฐ และให้กรรมการทั้งหมดทำงานเต็มเวลาให้กับคณะกรรมการ เพื่อทำงานได้อย่างมีประสิทธิภาพและหลีกเลี่ยงผลประโยชน์ทับซ้อน

31. ส่งเสริมการศึกษาด้านการอ่านออกเขียนได้ด้านสื่อและสารสนเทศ (Media and Information Literacy) ที่

32 https://th.necessaryandproportionate.org/text

33 https://thainetizen.org/docs/un-right-to-privacy-in-digital-age/

เน้นทักษะด้านการตรวจสอบข้อมูล การปกป้องความเป็นส่วนตัวและข้อมูลส่วนบุคคลของตัวเอง และการรักษาความมั่นคงปลอดภัยของตัวเอง

32. เชิญ ผู้รายงานพิเศษว่าด้วยสิทธิในความเป็นอยู่ส่วนตัว[34] มาเยือนประเทศไทย ภายในปี 2561

33. เชิญ ผู้รายงานพิเศษว่าด้วยการส่งเสริมและปกป้องสิทธิมนุษยชนและเสรีภาพพื้นฐานในขณะต่อต้านการก่อการร้าย[35] มาเยือนประเทศไทย ภายในปี 2562

34. เชิญ ผู้รายงานพิเศษว่าด้วยการส่งเสริมและปกป้องสิทธิที่จะมีเสรีภาพในความคิดเห็นและการแสดงออก[36] มาเยือนประเทศไทย ภายในปี 2562

34 Special Rapporteur on the right to privacy http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

35 Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism http://www.ohchr.org/EN/Issues/Terrorism/Pages/SRTerrorismIndex.aspx

36 Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression http://www.ohchr.org/EN/ISSUES/FREEDOMOPINION/Pages/OpinionIndex.aspx