ความคิดเห็นต่อร่างพ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. … (รับฟังความคิดเห็นระหว่างวันที่ 27 กันยายน 2561 - 12 ตุลาคม 2561)[1]

เครือข่ายพลเมืองเน็ต 12 ตุลาคม 2561

1. ขอบเขตและเงื่อนไขการใช้อำนาจตามกฎหมายไม่มีความชัดเจน ไม่มีกลไกตรวจสอบการใช้อำนาจ

- ร่างกฎหมายฉบับนี้จะให้อำนาจพิเศษจำนวนมากกับเจ้าหน้าที่รัฐและหน่วยงานของรัฐ ซึ่งจะมีผลกระทบต่อประชาชนทุกคน กฎหมายลักษณะนี้โดยปกติจำเป็นต้องมีการกำหนดขอบเขตและเงื่อนไขการใช้อำนาจอย่างเคร่งครัด เช่น ขอบเขตพื้นที่ (territorial scope) ขอบเขตเวลา (temporal scope) ขอบเขตในแง่ลักษณะของกิจกรรมหรือสิ่งที่จะเข้าข่ายให้สามารถใช้อำนาจได้ (material scope) รวมถึงพิจารณากลไกที่จะตรวจสอบการใช้อำนาจ
- **อย่างไรก็ตาม ร่างกฎหมายฉบับนี้ แทบไม่มีการกำหนดขอบเขตอำนาจเลย และกลไกตรวจสอบการใช้อำนาจมีเพียงอนุมาตราเดียว คือมาตรา 58 (4) ซึ่งเป็นเพียงการพิจารณายืดระยะเวลาหลังจากที่พนักงานเจ้าหน้าที่ได้ยึดอุปกรณ์ไปแล้วสามสิบวัน (การยึดในตอนแรกนั้นสามารถทำได้ทันทีโดยไม่ต้องขอศาล) ส่วนบทกำหนดโทษสำหรับสำนักงานหรือพนักงานเจ้าหน้าที่นั้น ไม่มีเลย**

2. จำเป็นต้องแบ่งประเภทของข้อมูลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ชัดเจน กำหนดเกณฑ์การเข้าถึงข้อมูลประเภทต่างๆ รวมถึงกำหนดประเภทข้อมูลที่มีความอ่อนไหวและห้ามเข้าถึง

- ร่างพ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ ให้อำนาจสำนักงาน เลขาธิการ และพนักงานเจ้าหน้าที่ ในการเข้าถึงข้อมูลอย่างกว้างขวาง ทั้งการรวบรวมข้อมูลโดยตัวสำนักงานเอง (มาตรา 53) การขอข้อมูล เรียกให้บุคคลมาให้ข้อมูลกับพนักงานเจ้าหน้าที่ เข้าไปในสถานประกอบการตรวจสอบสถานที่ ตรวจสอบคอมพิวเตอร์ และยึดอุปกรณ์เพื่อรวบรวมข้อมูล (มาตรา 54, 57 และ 58) การขอให้หน่วยงานรัฐและเอกชนให้ข้อมูลกับสำนักงาน (มาตรา 55)
- อย่างไรก็ตาม ในร่างกฎหมายไม่ได้มีการกำหนดว่า “ข้อมูล” ดังกล่าวครอบคลุมถึงข้อมูลประเภทใด ลักษณะใดบ้าง ทำให้ไม่สามารถกำหนดหลักเกณฑ์การเข้าถึงข้อมูลที่เหมาะสมกับข้อมูลที่มีลักษณะต่างๆ กัน มีเพียงมาตราเดียวที่จำแนกข้อมูลออกเป็นประเภทย่อยๆ คือมาตรา 46 ที่แบ่ง

[1] http://www.lawamendment.go.th/index.php/laws-independent-entity/item/1306-2018-09-27-07-35-21

ข้อมูลเป็น 3 ประเภทคือ 1) ข้อมูลการออกแบบระบบฯ 2) ข้อมูลการทำงานของระบบฯ และ 3) ข้อมูลอื่นใด อย่างไรก็ตาม เมื่อมีการกล่าวถึง “ข้อมูล” ในมาตราอื่นๆ ก็ไม่ปรากฏว่ามีการอ้างอิงนิยามหรือการจำแนกตามมาตรา 46 แต่อย่างใด

- **เสนอให้พิจารณาข้อมูลเป็น 5 ประเภท คือ**
    - 1) **ข้อมูลที่ถูกใช้เพื่อคุกคามระบบหรือทำให้ระบบมีความเสี่ยงจากภัยคุกคาม และ**
    - 2) **ข้อมูลที่ถูกเก็บรักษาอยู่ในระบบ ซึ่งเป็นข้อมูลของผู้ให้บริการและเป็นข้อมูลเกี่ยวกับการทำงานของระบบ (อาจแบ่งย่อยได้อีกตามข้อมูลประเภทที่** (1) **และ** (2) **ของมาตรา** 46)
    - 3) **ข้อมูลที่ถูกเก็บรักษาอยู่ในระบบ ซึ่งเป็นข้อมูลของผู้ให้บริการและไม่ใช่ข้อมูลเกี่ยวกับการทำงานของระบบ**
    - 4) **ข้อมูลที่ถูกเก็บรักษาอยู่ในระบบ ซึ่งเป็นข้อมูลของผู้ใช้บริการและไม่ใช่ข้อมูลส่วนบุคคล**
    - 5) **ข้อมูลที่ถูกเก็บรักษาอยู่ในระบบ ซึ่งเป็นข้อมูลของผู้ใช้บริการและเป็นข้อมูลส่วนบุคคล**
- ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ สำนักงาน เลขาธิการ และพนักงานเจ้าหน้าที่ ควรเน้นการเข้าถึงข้อมูลประเภทที่ 1 เป็นหลัก และอาจมีข้อมูลประเภทที่ 2 สนับสนุน โดยหลีกเลี่ยงการเข้าถึงข้อมูลที่ถูกเก็บรักษาอยู่ในระบบในประเภทอื่นๆ ซึ่งอาจมีข้อมูลความลับทางการค้าและข้อมูลส่วนบุคคล
- **การดำเนินการใดที่อาจกระทบต่อข้อมูลที่ไม่ใช่ข้อมูลเกี่ยวกับการทำงานของระบบ (ประเภทที่** 3) **ข้อมูลของผู้ใช้บริการ (ประเภทที่** 4) **และข้อมูลส่วนบุคคล (ประเภทที่** 5) **จะต้องคำนึงถึงหลักความจำเป็นและความได้สัดส่วนของมาตรการ ภายใต้หลักการการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวในรัฐธรรมนูญและการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้อง**
- **หลักเกณฑ์และเงื่อนไขในการเข้าถึงข้อมูลประเภทที่** 3, 4, **และ** 5 **จะต้องเข้มงวดกว่าประเภทที่** 1 **และ** 2

3. กลไกคุ้มครองข้อมูลส่วนบุคคลในกิจกรรมที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

- **ร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. … ฉบับรับฟังความคิดเห็นเดือนกันยายน** 2561[2] ซึ่งจะเข้าสู่การพิจารณาของสภานิติบัญญัติแห่งชาติในเวลาไล่เลี่ยกับร่างกฎหมายฉบับนี้ ใน**มาตรา** 4 (2) ระบุว่า *“[พระราชบัญญัตินี้ไม่ใช้บังคับแก่] การดำเนินการของหน่วยงานรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐหรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงินหรือนิติวิทยาศาสตร์”*

[2] http://lawamendment.go.th/index.php/component/k2/item/1297-5-20-2561

- การยกเว้นดังกล่าวจะทำให้ ข้อมูลส่วนบุคคลที่สำนักงาน เลขาธิการ และพนักงานเจ้าหน้าที่ ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ สามารถเข้าถึงได้ ไม่ได้รับการคุ้มครองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล[3] เท่ากับประชาชนจะขาดกลไกหลักสำหรับการคุ้มครองข้อมูลของตัวเองไปในทันที – *โดยเฉพาะถ้าพิจารณาว่าข้อมูลส่วนบุคคลจำนวนมากในปัจจุบันอยู่ในรูปแบบอิเล็กทรอนิกส์และถูกเก็บรวบรวมโดยหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ซึ่งตามมาตรา 43 สามารถรวมถึง ธนาคาร สถานพยาบาล ผู้ให้บริการโทรศัพท์ ผู้ให้บริการการอินเทอร์เน็ต และไปรษณีย์) หมายความว่า รัฐจะสามารถเข้าถึงข้อมูลส่วนบุคคลของประชาชนซึ่งอยู่ในระบบของหน่วยงานเหล่านี้ได้ โดยประชาชนไม่มีกลไกคุ้มครองตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลเลย*
- นอกจากนี้ยังมีข้อสังเกตว่า ในขณะที่พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ จะมีผลบังคับใช้ในทันที แต่พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลจะมีผลบังคับใช้หลังประกาศในราชกิจจานุเบกษา 180 วัน (ตามร่างปัจจุบัน – และมีบางข้อเสนอขอขยายเป็น 2-3 ปี)
- **เสนอให้ระบุให้ชัดเจน ในร่างพ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ ว่า กิจการและกิจกรรมทั้งหมดภายใต้พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์จะอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคล และให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้ก่อนจึงจะบังคับใช้กฎหมายความการรักษามั่นคงปลอดภัยไซเบอร์ได้**

4. เงื่อนไขและการตรวจสอบการใช้อำนาจของเจ้าหน้าที่ กรณีเข้าถึงและตรวจข้อมูล อุปกรณ์ สถานที่ และสั่งการผู้ครอบครองระบบ

- **เสนอให้**

  ในการปฏิบัติการตามมาตรา 54, 55, 56, 57, และ 58 ให้สำนักงาน เลขาธิการ และพนักงานเจ้าหน้าที่ ยื่นคำร้องโดยระบุเหตุผล ผลกระทบต่อเจ้าของข้อมูลหรืออุปกรณ์ และความจำเป็น ต่ออธิบดีผู้พิพากษาศาลแพ่งเพื่อขอคำสั่งศาลในการปฏิบัติการตามหน้าที่และอำนาจ

  การพิจารณาออกคำสั่งศาลดังกล่าวให้อธิบดีผู้พิพากษาศาลสั่งอนุญาตโดยกำหนดเงื่อนไขการใช้อำนาจใด ๆ ก็ได้ โดยให้อธิบดีผู้พิพากษาศาลพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคล สิทธิในข้อมูลส่วนบุคคล หรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

  (1) มีเหตุอันควรเชื่อว่ามีภัยคุกคามหรือจะมีภัยคุกคามที่จะกระทบต่อความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

[3] คณะทำงานของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ให้ความเห็นในทางเดียวกันระหว่างตอบข้อซักถามเมื่อวันที่ 11 ตุลาคม 2561 ว่า หากร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 4 (2) เขียนเช่นนั้น ข้อมูลส่วนบุคคลที่พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ให้อำนาจรัฐสามารถเข้าถึงได้ จะไม่ถูกคุ้มครองด้วยพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (เวทีรับฟังความคิดเห็น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ 11 ต.ค. 2561)

(2) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารที่สามารถใช้ยับยั้งภัยคุกคามความมั่นคงปลอดภัยไซเบอร์แห่งชาติดังกล่าวได้
(3) มาตรการตามคำร้อง และขอบเขตและระยะเวลาของมาตรการดังกล่าว ได้สัดส่วนกับขนาดและความร้ายแรงของภัยคุกคาม และพนักงานเจ้าหน้าที่ที่ยื่นคำร้องสามารถจำกัดการดำเนินมาตรการให้อยู่ในขอบเขตและระยะเวลาตามที่ร้องขอได้
(4) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

ภายหลังที่ศาลมีคำสั่ง หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุ หรือพฤติการณ์เปลี่ยนแปลงไป หรือภัยคุกคามต่อความมั่นคงปลอดภัยไซเบอร์แห่งชาติตามคำร้องได้สิ้นสุดลง อธิบดีผู้พิพากษาศาลอาจเปลี่ยนแปลงคำสั่งได้ตามที่เห็นสมควร

ในกรณีจำเป็นเร่งด่วนซึ่งปรากฏอย่างชัดแจ้งว่าหากไม่ดำเนินการในทันทีจะเกิดความเสียหายต่อความมั่นคงปลอดภัยไซเบอร์แห่งชาติอย่างร้ายแรง ให้พนักงานเจ้าหน้าที่โดยอนุมัติของคณะกรรมการ ดำเนินการไปก่อนเฉพาะเท่าที่จำเป็น แล้วรายงานให้อธิบดีผู้พิพากษาศาลทราบโดยเร็วภายในยี่สิบสี่ชั่วโมง

การดำเนินมาตรการตามให้เป็นไปตามหลักเกณฑ์และเงื่อนไขที่คณะกรรมการกำหนด โดยให้รายงานผลการดำเนินมาตรการต่ออธิบดีผู้พิพากษาศาลทุกสิบห้าวัน

บรรดาข้อมูลข่าวสารที่ได้มา ให้เก็บรักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับภัยคุกคามต่อความมั่นคงปลอดภัยไซเบอร์แห่งชาติซึ่งได้รับอนุญาตและให้ใช้ประโยชน์ในการรักษาหรือยับยั้งภัยคุกคามหรือใช้เป็นพยานหลักฐานถึงภัยคุกคามดังกล่าวเท่านั้น ส่วนข้อมูลข่าวสารอื่นให้ทำลายเสียทั้งสิ้น และให้แจ้งถึงการทำลายดังกล่าวกับอธิบดีผู้พิพากษาศาลหรือผู้พิพากษาหัวหน้าศาลจังหวัดทราบ