



ดร.สุพล พรหมมาพันธ์

ผู้ช่วยคณบดีฝ่ายวิชาการ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม เชี่ยวชาญเรื่องระบบข้อมูลสารสนเทศ การวางกลยุทธ์การใช้เทคโนโลยีสารสนเทศ การสื่อสาร รวมถึงกลยุทธ์ออนไลน์

การเก็บข้อมูลชีวมาตรของหน่วยงานรัฐ กับความเสี่ยงที่อาจมีการละเมิดสิทธิส่วนบุคคล และผลกระทบต่อความมั่นคงของประเทศ

■ เก็บประเด็นสำคัญจากเวทีเสวนา การเก็บข้อมูลชีวมาตร (Biometrics) ของหน่วยงานรัฐกับการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ ผู้เชี่ยวชาญชี้ประเด็นที่บวกลบ ความมั่นคงของประเทศ และละเมิดสิทธิส่วนบุคคล

เมื่อกรกฎาคม พ.ศ.2562 ที่ผ่านมา สมาคมความมั่นคงปลอดภัยสารสนเทศ และ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม ร่วมกันจัดเสวนาประชาชน เรื่อง การเก็บข้อมูลชีวมาตร (Biometrics) ของหน่วยงานรัฐกับการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ โดยมีผู้ร่วมเสวนา คือ ปริญญา หอมเอนก ประธานและผู้ก่อตั้ง, ACIS Professional Center Co., Ltd. (ACIS), นพ.สุธี ทวีรัตน์ กรรมการสมาคมความมั่นคงปลอดภัยสารสนเทศ, พล.อ.บรรเจิด เทียนทองดี, พล.อ.เจิตวุธ คราประยูร, และ พ.ต.อ.ญาณพล ยั่งยืน ณ ห้อง

พัชรกิติยาภา อาคารเฉลิมพระบารมี 50 ปี ซอยศูนย์วิจัย ถ.เพชรบุรีตัดใหม่ กรุงเทพฯ

อ.ปริญญา หอมเอนก กล่าวว่า ในประเทศไทย พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ปี 2562 ประกาศใช้แล้ว เมื่อวันที่ 24 พฤษภาคม พ.ศ.2562 ถ้าเป็นข้อมูลอีเมล Facebook รั่วไหล ยังสามารถแก้ไขได้ด้วยการเปลี่ยน Password แต่ถ้าเป็นข้อมูลเหล่านี้รั่วไหลแล้วจะอย่างไร เช่น ลายพิมพ์นิ้วมือ ผ่ามือ ใบหน้า จอตา (Retina) ม่านตา (Iris) ลายเซ็น ดีเอ็นเอ เสีย เป็นต้น ซึ่งข้อมูลเหล่านี้รั่วไหลแล้วไม่สามารถนำกลับมาได้ แก้ไขได้ยาก

อ.ปริญญา ยังได้กล่าวถึงกระบวนการในการเข้าถึงเทคโนโลยีการเก็บข้อมูลมี 3 รูปแบบที่มีความแตกต่างกัน รูปแบบแรก คือ การระบุตัวตน (Identification) หมายถึงการระบุตัวตนว่า คุณเป็นใคร ซึ่งเป็นการระบุตัวตนผ่านชื่อผู้ใช้ (Username) ความปลอดภัยของหมายเลขไอดี (Security ID) สมาร์ทการ์ด (Smart Card) และพีไอวี (PIV)

รูปแบบที่สอง การตรวจสอบรับรอง (Authentication) เป็นการพิสูจน์ตรวจสอบว่าคุณเป็นใคร ผ่านชื่อผู้ใช้/คำสั่งผสมรหัสผ่าน (Username/Password Combo), หรือ PIN, OTP หรือการเก็บข้อมูลทางชีวมาตร (Biometrics Data) ซึ่งเป็นลักษณะเฉพาะของแต่ละบุคคล หรือ อัตลักษณ์ เช่น ลายพิมพ์นิ้วมือ ม่านตา ใบหน้า เป็นต้น ปัจจุบันมีการใช้ไบโอเมทริกซ์กันอย่างแพร่หลาย เช่น การสแกนลายพิมพ์นิ้วมือเพื่อปลดล็อกปุ่มโทรศัพท์, การสแกนใบหน้าเข้าทำงาน

และรูปแบบที่สาม การอนุญาต (Authorization) หมายถึง การได้รับอนุญาตจากผู้ที่เป็นเจ้าของข้อมูล ในการเก็บข้อมูลความเป็นส่วนตัวของประชาชนนั้น หน่วยงานของรัฐต้องมีการรับรองความปลอดภัยที่แน่นอนยิ่งขึ้นว่า ข้อมูลเหล่านั้นต้องไม่รั่วไหล

ความจริงแล้วการเก็บข้อมูลสามารถทำได้ แต่เราไม่รู้ว่า ผู้เก็บข้อมูลของเราไปขายหรือเปล่า สรุปประเด็นเป็น 2 ข้อ คือ (1) ปัจจุบันเทคโนโลยีไปไกลมาก ที่เรียกว่า Disruptive Technologies for Value Economy ต้องรู้เท่าทัน (2) เรื่องของการจัดเก็บข้อมูลของคนต้องดูว่าเขาเอาไปทำอะไร เมื่อคุณเก็บข้อมูลไปแล้วมีการรักษาความปลอดภัยที่ดีหรือไม่

การจัดเก็บข้อมูลต้องให้ความสำคัญกับเรื่อง Privacy ด้วย การจัดเก็บข้อมูล “ถ้าเก็บข้อมูลเพื่อความมั่นคงของประเทศสามารถทำได้ แต่คุณต้องไม่ให้ข้อมูลรั่วไหลนะ ถ้าไม่จริงจริงอย่าเก็บดีกว่า” ถ้าคุณเก็บข้อมูลของใครแล้ว ควรลบทิ้ง พ.ร.บ.ความมั่นคงไซเบอร์ห้ามลบ, พ.ร.บ.ข้อมูลส่วนบุคคล ห้ามรั่ว ถ้าข้อมูลรั่ว มีคนจะเล่นงานคุณ

นพ.สุธี ทวีรัตน์ กล่าวว่า มี 2 เรื่องหลัก คือ

(1).หนังสือเดินทาง (Passport) รุ่นใหม่ของประเทศไทย โดยกระทรวงการต่างประเทศ ซึ่งแต่เดิมมีการเก็บข้อมูลทั้งภาพถ่าย และลายพิมพ์นิ้วมือ 10 นิ้ว แต่ต่อไปนี้จะมีการเก็บข้อมูลชีวมาตรม่านตาด้วย

ซึ่งทางกระทรวงฯ ได้ให้เหตุผลว่า การเก็บข้อมูลชีวมาตรดังกล่าวเป็นคุณลักษณะความปลอดภัยสูงสุดในการป้องกันการปลอมแปลงหนังสือเดินทาง ซึ่งแตกต่างจากประเทศอื่น เช่น สหรัฐอเมริกาเก็บเฉพาะข้อมูลภาพถ่ายอย่างเดียว ไม่ให้เก็บลายพิมพ์นิ้วมือ ในสหภาพยุโรป เก็บเฉพาะภาพถ่ายและลายพิมพ์นิ้วมือเพียง 2 นิ้ว เช่น ประเทศเยอรมนีมีการเก็บม่านตา ส่วนประเทศเนเธอร์แลนด์เก็บลายพิมพ์นิ้วมือ เป็นต้น

สำนักงานตรวจคนเข้าเมือง (ตม.) เวลามีคนเดินทางไปต่างประเทศเขาจะดำเนินการตรวจ 2 เรื่อง คือ (1) ตรวจเอกสาร โดยเอา Passport มาสแกน เพื่อให้รู้ว่าคนนี่คือใคร (Identification) (2) ระบบอิเล็กทรอนิกส์ (Chip) คือการนำเอาข้อมูลในเอกสารมาตรวจสอบว่าตรงกันไหม ซึ่งเป็นการยืนยันตัวตนที่แน่นอน (Authentication)

ตอนนี้ใครจะไปทำหนังสือเดินทาง จะต้องถูกเก็บ 3 อย่าง คือ (1) รูปถ่าย (2) ลายพิมพ์นิ้วมือ และ (3) ม่านตา ซึ่งคนที่มาจัดเก็บข้อมูลนั้นเป็นบริษัทเอกชนที่มีการเข้ามาประมูลงานได้จากภาครัฐและได้ไปในราคาถูกๆ ซึ่งเอกชนเหล่านี้ในแต่ละปีมีการเปลี่ยนแปลงไปแล้วแต่ใครจะประมูลได้ ซึ่งตรงนี้ข้อมูลคนทำหนังสือเดินทางอาจรั่วไหล และอาจถูกสวมรอยได้

(2). การลงทะเบียนซิมโทรศัพท์ด้วยวิธีอัตลักษณ์ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) มีนโยบายการให้ลงทะเบียนซิมโทรศัพท์ทั้งการตรวจสอบใบหน้า และสแกนลายพิมพ์นิ้วมือทั่วประเทศ เมื่อเก็บข้อมูลเหล่านี้ไปแล้ว มันใจได้อย่างไรว่าข้อมูลไม่รั่วไหล แม้กระทั่งข้อมูลบัตรประชาชนของบุคคลสำคัญหลายคนถูกนำไปลงทะเบียนซ้ำกันหลายครั้ง ต่อไปอาจมีผลกระทบต่อการใช้เลือกตั้ง เมื่อก่อนมีการใช้บัตรประชาชนใน

การเลือกตั้ง แต่ต่อไปจะมีการใช้ e-Vote ในการเลือกตั้ง เมื่อข้อมูลถูกนำไปเก็บไว้ในฐานข้อมูล ถ้าข้อมูลเหล่านั้นถูกแฮกจะเกิดอะไรขึ้นกับผลการเลือกตั้ง

สรุป คือ รัฐอยากควบคุมข้อมูลส่วนบุคคล, บริษัทธุรกิจ อยากได้ข้อมูลของลูกค้า ข้อมูลส่วนบุคคลในโลกออนไลน์ถูกนำไปวิเคราะห์หาผลประโยชน์ ควรมีการปกป้องข้อมูลด้วยวิธีการที่ปลอดภัยด้วย

โดยสรุปแล้ว เวทีเสวนาประชาชนอันประกอบด้วย มีความเห็นที่น่าสนใจหลายประการ อาทิ การจัดเก็บข้อมูลชีวมาตรนั้นมีทั้งข้อดี และข้อเสีย สำหรับข้อดี คือ เมื่อเกิดปัญหาอาชญากรรมขึ้น การจัดเก็บข้อมูลส่วนบุคคลเอาไว้ในการทำบัตรประชาชนก็ถือว่ายังมีประโยชน์ แต่ไม่ใช่เก็บข้อมูลทุกอย่างรหัสผ่าน (Password) อีเมล เมื่อถูกแฮกไปก็ยังสามารถเปลี่ยนได้ แต่ม่านตาเปลี่ยนไม่ได้ การเก็บข้อมูลของหน่วยงานรัฐควรต้องมีการออกแบบให้ชัดเจนว่าจะเก็บข้อมูลอะไรบ้าง ไม่ใช่เก็บทุกอย่าง

เพราะตอนนี้ ทำบัตรประชาชน, ทำหนังสือเดินทาง, ทำใบขับขี่ ก็เก็บข้อมูลกันหมดทั้งรูปถ่าย ลายพิมพ์นิ้วมือ ใบหน้า ม่านตา ต่อไปอาจมีการเก็บถึงเรื่องดีเอ็นเอ (DNA) ด้วย เพราะอาจเสี่ยงต่อการละเมิดสิทธิส่วนบุคคล ต้องบอกประชาชนให้ชัดเจนว่า มีความจำเป็นอะไรต้องเก็บข้อมูลชีวมาตรเหล่านี้ ถ้าพลาดข้อมูลรั่วไหลเพียง 1% ย่อมมีผลเสียส่งผลกระทบต่อประชาชน

ท้ายสุด นพ.สุธี ทวีรัตน์ ได้มีข้อเสนอแนะในการเสวนา ครั้งนี้ คือ (1).รัฐควรจะหลีกเลี่ยงการบังคับเก็บข้อมูลชีวมาตรของประชาชนเกินเท่าที่จำเป็นจริงๆ (2).รัฐควรจะต้องกำกับดูแลมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ และคุ้มครองข้อมูลส่วนบุคคลของข้อมูลชีวมาตร อย่างมีธรรมาภิบาลเปิดเผย โปร่งใส (3).รัฐไม่ควรจะยอมให้เอกชน เข้ามาบริหารจัดการฐานข้อมูลชีวมาตร และ (4).รัฐต้องมีมาตรการเยียวยาแก้ไขเจ้าของข้อมูลที่เกิดการรั่วไหล ทั้งหมดทั้งหมดนี้ หากทางรัฐได้เห็นความสำคัญเหล่านี้ จึงนับได้ว่าจะเป็นประโยชน์ต่อประชาชน และประเทศชาติโดยแท้จริง