Human Rights Lawyers Association

AMERICAN BAR ASSOCIATION
Rule of Law Initiative

ความเป็นส่วนตัวของข้อมูล: คู่มือสำหรับนักกฎหมายในยุคดิจิทัล

Data Privacy Playbook: Lawyer's Guide in the Digital Age

โดย สมาคมนักกฎหมายสิทธิมนุษยชน
ร่วมกับ เนติบัณฑิตยสภาแห่งสหรัฐอเมริกา

ความเป็นส่วนตัวของข้อมูล:
คู่มือสำหรับนักกฎหมายในยุคดิจิทัล

Data Privacy Playbook:

A Lawyer's Guide in the Digital Age

ชื่อหนังสือ ความเป็นส่วนตัวของข้อมูล: คู่มือสำหรับนักกฎหมาย
ในยุคดิจิทัล
Data Privacy Playbook: A Lawyer's Guide in
the Digital Age
จำนวนหน้า 239 หน้า
คณะผู้จัดทำ ผู้ช่วยศาสตราจารย์ ดร.ธีทัต ชวิศจินดา (หัวหน้าคณะทำงาน)
คุณฐิติรัตน์ ทิพย์สัมฤทธิ์กุล
คุณกุณฑิกา นุตจรัส
พิมพ์ครั้งที่ 1 สิงหาคม 2567
จำนวนพิมพ์ 200 เล่ม
จัดพิมพ์โดย สมาคมนักกฎหมายสิทธิมนุษยชน (สนส.)
Human Rights Lawyers Association (HRLA)
เลขที่ 109 ถนนสุทธิสารวินิจฉัย แขวงสามเสนนอก
เขตห้วยขวาง กรุงเทพมหานคร 10310
โทร 02 275 3954 เว็บไซต์ www.naksit.net
พิมพ์ที่ ห้างหุ้นส่วนจำกัด เยื่อไผ่ พริ้นติ้ง
เลขที่ 9/10 หมู่ที่ 3 ตำบลโพรงอากาศ อำเภอบางน้ำเปรี้ยว
จังหวัดฉะเชิงเทรา 2415

คำนำ

ในยุคที่เทคโนโลยีก้าวกระโดด ข้อมูลส่วนบุคคลของเราก็เปลี่ยนรูปแบบตาม จากแฟ้มกระดาษสู่ไฟล์ดิจิทัล ทั้งภาครัฐและเอกชนต่างใช้เทคโนโลยีจัดการข้อมูลเหล่านี้ แม้จะสะดวกรวดเร็ว แต่ก็แฝงไปด้วยความเสี่ยงที่หลายคนอาจมองข้าม

น่าเสียดายที่ความเข้าใจเรื่องความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลยังมีจำกัด ส่งผลให้หลายคนต้องเผชิญปัญหาโดยไม่จำเป็น ด้วยเหตุนี้ สมาคมนักกฎหมายสิทธิมนุษยชน โดยการสนับสนุนจากเนติบัณฑิตยสภาแห่งสหรัฐอเมริกา (American Bar Association: ABA) จึงได้จัดทำ **"ความเป็นส่วนตัวของข้อมูล: คู่มือสำหรับนักกฎหมายในยุคดิจิทัล"** ฉบับนี้ขึ้น

เราเชื่อว่าความรู้คือพลัง และคู่มือนี้จะเป็นเครื่องมือสำคัญในการสร้างสังคมที่ปลอดภัยและเคารพสิทธิความเป็นส่วนตัว

เชิญชวนทุกคนร่วมเป็นส่วนหนึ่งในการสร้างอนาคตที่ดีกว่า เริ่มต้นได้ง่าย ๆ เพียงเปิดหน้าถัดไป แล้วจะพบว่า การปกป้องตนเองในโลกดิจิทัลนั้นไม่ยากอย่างที่คิดและยังน่าค้นหาอีกด้วย!

ณัฐาศิริ เบิร์กแมน
นายกสมาคมนักกฎหมายสิทธิมนุษยชน

สารบัญ

ส่วนที่ 1
ความนำ: ผจญภัยในโลกความเป็นส่วนตัวทางดิจิทัล

ในยุคดิจิทัลที่ข้อมูลคือทองคำ คุณเคยสงสัยไหมว่าข้อมูลของเรามีความปลอดภัยแค่ไหน? เมื่อร่องรอยตัวตนของเราอาจปรากฏในโลกดิจิทัล ทุกคลิกอาจซ่อนปริศนา และทุกไลค์อาจเป็นหลักฐาน!

เตรียมตัวให้พร้อมเพราะเรากำลังจะร่วมออกเดินทางไปในดินแดนแห่ง “ความเป็นส่วนตัวของข้อมูล:คู่มือสำหรับนักกฎหมายในยุคดิจิทัล”

ทำไมต้องอ่านหนังสือเล่มนี้?

นี่ไม่ใช่ตำราที่น่าเบื่อ แต่เป็น **“คู่มือผจญภัย”** ที่จะพาคุณท่องไปในโลกของกฎหมายความเป็นส่วนตัวทางดิจิทัลและการคุ้มครองข้อมูลส่วนบุคคลแบบเข้าใจง่าย สนุก พร้อมใช้งานได้จริง

คู่มือฉบับนี้เกิดขึ้นจากความร่วมมือระหว่างสมาคมนักกฎหมายสิทธิมนุษยชน (Human Rights Lawyers Association: HRLA) โดยการสนับสนุนจากเนติบัณฑิตยสภาแห่งสหรัฐอเมริกา (American Bar Association: ABA) เพื่อให้พวกเราเหล่านักกฎหมายและผู้ปฏิบัติงานด้านกฎหมายเตรียมพร้อมรับมือกับปัญหาการละเมิดความเป็นส่วนตัวของข้อมูล และการคุ้มครองข้อมูลส่วนบุคคลในโลกไซเบอร์

เราจะได้อะไรจากหนังสือเล่มนี้?

1. เข้าใจกฎเกณฑ์การเล่นเกมในสนามดิจิทัล
2. วิเคราะห์คดีแบบมือโปร เชื่อมโยงทฤษฎีสู่โลกจริง
3. พัฒนาทักษะให้คำปรึกษาแบบเทพ ตอบโจทย์ลูกความยุค 4.0
4. มองทะลุอนาคต รู้เท่าทันเทรนด์กฎหมายดิจิทัล

สองขั้วของระบบกฎหมายความเป็นส่วนตัวในข้อมูล

รู้หรือไม่? เมื่อพูดถึงกฎหมายความเป็นส่วนตัวของข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล โลกของเราแบ่งออกเป็น 2 ขั้วใหญ่ๆ คือ ขั้วยุโรป (Comprehensive Approach) และขั้วอเมริกา (Sectoral Approach)

ขั้วยุโรป: เข้มงวด ครอบคลุม ดูแลทุกองคาพยพ เหมือนปราสาทที่มีกำแพงแกร่งล้อมรอบ ปกป้องทุกซอกทุกมุม

ขั้วอเมริกา: ยืดหยุ่น แยกส่วน ตามแต่ละภาคส่วน เปรียบเสมือนเมืองที่มีกฎระเบียบแตกต่างกันไปในแต่ละย่าน

Q: แล้วประเทศไทยของเราล่ะ อยู่ขั้วไหน?

A: ประเทศของเราค่อนข้างเอนเอียงไปทาง “ขั้วยุโรป” แต่ในโลกไร้พรมแดนแห่งนี้ ปัญหาการละเมิดข้อมูลส่วนบุคคลอาจไม่จำกัดอยู่แค่ในบ้านของเราเท่านั้นนะ

แต่ก็ไม่ต้องกังวล! เพราะหนังสือเล่มนี้จะพาคุณท่องไปทั้งสองขั้ว เพื่อให้เข้าใจภาพรวมของการคุ้มครองข้อมูลทั่วโลก

หนังสือเล่มนี้มีอะไรบ้าง?

ส่วนที่ 1 ความนำ: ผจญภัยในโลกความเป็นส่วนตัวทางดิจิทัล

เริ่มต้นตั้งศูนย์และปูพื้นฐานความเข้าใจ เหตุใดเรื่องนี้จึงสำคัญ ผู้อ่านจะได้อะไรจากหนังสือเล่มนี้ ข้อควรรู้เกี่ยวกับสองขั้วกฎหมาย และวิธีการอ่านให้สนุกและได้ประโยชน์

ส่วนที่ 2 ความลับที่ซ่อนอยู่ในโลกดิจิทัล: เปิดโปงทุกสิ่งที่คุณต้องรู้

เนื้อหาส่วนนี้มาตามคำเรียกร้องของหลายท่าน จากเอกสารฝึกอบรม Digital Privacy Training: Southeast Asia ที่ได้จัดขึ้นก่อนหน้านี้ เพื่อให้คุณได้เรียนรู้อย่างเต็มที่ แม้ว่าต้นฉบับจะเป็นเอกสารทางวิชาการที่อาจเข้าใจยาก แต่เราได้แปลและปรับเปลี่ยนเรียบเรียงใหม่ให้เป็นภาษาที่เข้าใจง่ายเหมือนกำลังอ่านนิยายสนุกๆ เล่มหนึ่ง โดยยังคงรักษาสาระสำคัญไว้อย่างครบถ้วน

เราจะพาคุณเดินทางผ่านเนื้อหา 4 ตอนที่น่าตื่นเต้น

ตอนที่ 1: ค้นพบสิทธิของคุณในโลกดิจิทัล ออกสำรวจดินแดนแห่งสิทธิดิจิทัล ที่คุณอาจไม่เคยรู้มาก่อน!

ตอนที่ 2: เจาะลึกกฎหมายความเป็นส่วนตัวทั่วโลก เปิดแผนที่กฎหมาย ท่องไปในโลกแห่งความเป็นส่วนตัวระดับสากล!

ตอนที่ 3: ประเด็นร้อนเรื่องความเป็นส่วนตัวยุคดิจิทัล ร่วมไขปริศนาและถกเถียงประเด็นเด็ดที่กำลังเป็นที่พูดถึง!

ตอนที่ 4: มุมมอง 5 ประเทศอาเซียนกับการจัดการความเป็นส่วนตัวในข้อมูล สำรวจวิธีการที่ประเทศเพื่อนบ้านรับมือกับความท้าทายด้านความเป็นส่วนตัว!

ส่วนที่ 3 เรื่องจริงจาก 13 คดีที่ควรรู้

เรียนรู้จากเรื่องจริง 13 คดีพิพาทที่เกิดขึ้นในสหรัฐอเมริกา สหภาพยุโรป สหราชอาณาจักร แคนาดา และออสเตรเลีย ที่จะทำให้คุณทึ้งอึ้ง ทึ่ง และแปลกใจ

จากการท้าทายของ Schrems ถึงความปลอดภัยไซเบอร์ เราจะเผชิญหน้ากับสิทธิที่จะถูกลืม ดาราปะทะปาปารัซซี่ 143 ล้านชีวิตที่ถูกเปิดเผย นายจ้างแอบดู และอีกมากมาย! แต่ละคดีถูกถอดรหัสมาเล่าในรูปแบบกรณีศึกษาสุดเข้าใจง่าย ชวนคิด ชวนวิเคราะห์ และหาทางออก โดยแต่ละคดีประกอบด้วย:

เรื่องราวชวนติดตาม: ภูมิหลังและข้อเท็จจริงของคดีที่อ่านแล้วไม่มีวันหลับ!

ประเด็นกฎหมายเด็ด: วิเคราะห์ประเด็นสำคัญ การยกข้อต่อสู้ และการปฏิเสธ แบบเข้าใจง่าย ไม่ต้องแปลซ้ำ!

คำตัดสินและเหตุผล: เจาะลึกคำตัดสินและเหตุผลทางกฎหมาย เข้าใจทั้งวิธีคิดและการให้เหตุผล!

คำถามชวนคิด: ฝึกวิเคราะห์จากหลากมุมมอง ทั้งโจทก์ จำเลย ผู้กำหนดนโยบาย และผู้เสียหาย ฝึกสมองให้แหลมคม!

คำแนะนำสำหรับทนายความ: เคล็ดลับการรับมือและเตรียมความพร้อมพร้อมใช้งานได้เลย!

แหล่งข้อมูลเพิ่มเติม: ทั้งภาษาไทยและอังกฤษ สำหรับผู้ที่ต้องการศึกษาเชิงลึก สร้างทักษะเพื่อการใช้งานและเรียนรู้ตลอดชีวิต!

คดีที่เราเลือกมานี้ ไม่เพียงแต่ให้ความรู้กฎหมายทั่ว ๆ ไป แต่จะพาคุณท่องไประบบกฎหมายที่หลายหลาก เห็นวิธีคิดที่แตกต่าง การปรับใช้และตีความกฎหมาย และการให้เหตุผลทางกฎหมายที่ชวนให้ติดตา เปรียบเสมือนประตูสู่การศึกษากฎหมายเปรียบเทียบที่จะช่วยให้เราเข้าใจเรื่องความเป็นส่วนตัวของข้อมูลและการคุ้มครองข้อมูลส่วนบุคคลในที่ต่าง ๆ

ที่สนุกยิ่งไปกว่านั้น เราจะได้เห็นว่ากฎหมายแต่ละแขนงเชื่อมโยงกันอย่างไร ทั้งกฎหมายอาญา แพ่ง แรงงาน การแข่งขันทางการค้า และอื่น ๆ อีกมากมาย เหมือนกำลังต่อจิ๊กซอว์ขนาดยักษ์ในโลกดิจิทัลที่ซับซ้อน เตรียมตัวให้พร้อม และเปิดโลกแห่งกฎหมายไปพร้อมกัน!

วิธีอ่านให้สนุก และได้ประโยชน์

1. เริ่มต้นจากบทนำและหลักการพื้นฐาน ค่อย ๆ อ่าน ซึมซับเนื้อหาและประเด็นต่าง ๆ อย่างใจเย็น ไม่จำเป็นต้องรีบร้อน

2. เมื่อถึงกรณีศึกษา ให้ลองนึกภาพตามว่าหากเจอเหตุการณ์แบบเดียวกัน คุณจะทำยังไง ?

3. ถ้าสงสัยอะไร ย้อนกลับไปดูหลักการได้เสมอ และค้นคว้าเพิ่มเติม ไม่ต้องอาย เพราะเราเองก็ทำแบบนี้เหมือนกัน

4. ลองคุยกับเพื่อน ๆ ว่าคิดเห็นยังไงกับเนื้อหาในแต่ละส่วน โดยเฉพาะจุดที่มีคลิป และกิจกรรมแนะนำ รวมถึงพูดคุยกันเกี่ยวกับข้อถกเถียงและคำถามในแต่ละคดี รับรองได้เลยว่าคุณจะได้มุมมองใหม่ ๆ อย่างแน่นอน

สุดท้ายนี้ หวังว่าคู่มือเล่มนี้ จะเป็นเพื่อนซี้คู่ใจ พาพวกเราผจญภัยไปในโลกกฎหมายดิจิทัล โลกที่มีความเปลี่ยนแปลงและความท้าทายใหม่ ๆ รออยู่ทุกวัน

พร้อมแล้วใช่ไหม? พลิกหน้าถัดไปได้เลย รับรองว่าโลกความเป็นส่วนตัวของข้อมูลและการคุ้มครองข้อมูล ... จะทำให้ตื่นเต้นยิ่งกว่าหนังสืบสวนซะอีก!

ส่วนที่ 2
ความลับที่ซ่อนอยู่ในโลกดิจิทัล: เปิดโปงทุกสิ่งที่คุณต้องรู้

เนื้อหาส่วนนี้จะพาคุณดำดิ่งสู่โลกแห่งความเป็นส่วนตัวและการคุ้มครองข้อมูล ผ่านมุมมองที่เข้าใจง่าย สนุก และน่าติดตาม

เราจะพาคุณเดินทางผ่านเนื้อหา 4 ตอนที่น่าตื่นเต้น

ตอนที่ 1 ค้นพบสิทธิของคุณในโลกดิจิทัล

ตอนที่ 2 เจาะลึกกฎหมายความเป็นส่วนตัวทั่วโลก: จากระดับโลกสู่ท้องถิ่น

ตอนที่ 3 ประเด็นร้อนเรื่องความเป็นส่วนตัวยุคดิจิทัล

ตอนที่ 4 มุมมอง 5 ประเทศอาเซียนกับการจัดการความเป็นส่วนตัวในข้อมูล

ไม่ว่าคุณจะเป็นใคร เป็นนักกฎหมาย นักกิจกรรม นักวิจัย ผู้กำหนดนโยบาย หรือเป็นเพียงผู้ใช้อินเทอร์เน็ตทั่วไป บทนี้มีคำตอบสำหรับทุกคำถามที่คุณอาจไม่เคยรู้

ถ้าพร้อมแล้ว มาเริ่มการผจญภัยกัน

ตอนที่ 1 ค้นพบสิทธิของคุณในโลกดิจิทัล

เคยตกใจไหม เมื่อแค่คุยเรื่องรองเท้าคู่ใหม่ แล้วโฆษณาก็โผล่มาในเฟซบุ๊กทันที? หรือแปลกใจที่แอปสุขภาพรู้ว่าคุณนอนกี่ชั่วโมง? นี่แหละโลกดิจิทัลที่เราอยู่!

มาเถอะ! เราจะพาคุณสำรวจความหมายของ “สิทธิความเป็นส่วนตัว” ในยุคที่ข้อมูลมีค่าเท่าทองคำ เรียนรู้วิธีปกป้องตัวในโลกออนไลน์ที่ดูเหมือนจะรู้ใจเราไปหมด

พร้อมไขปริศนาเบื้องหลังเทคโนโลยีที่ทั้งน่ารักและน่าขนลุกในเวลาเดียวกัน! คุณจะได้รู้ว่าโลกดิจิทัลที่ว่าวุ่นวายนี้ ทำงานยังไงกันแน่

สิ่งที่จะได้เรียนรู้:

1. รู้เท่าทันสิทธิของเรา: เข้าใจว่าความเป็นส่วนตัวไม่ใช่แค่เรื่องซ่อนความลับ แต่เป็นสิทธิมนุษยชนขั้นพื้นฐาน

2. แยกแยะให้ออก: รู้ความแตกต่างระหว่าง “ความเป็นส่วนตัวของข้อมูล” กับ “การคุ้มครองข้อมูล” (ไม่เหมือนกันนะ!)

3. เจาะลึกแนวคิดสำคัญ: ทำความรู้จักกับคำเท่ ๆ อย่าง “ความเป็นส่วนตัวแบบเครือข่าย” และ “ความเป็นส่วนตัวทางดิจิทัล”

4. รู้เท่าทันเทคโนโลยี: เข้าใจว่า AI, IoT, และ Blockchain เกี่ยวข้องกับความเป็นส่วนตัวของเรายังไง

พิเศษสุด! ดูวิดีโอสุดเจ๋งที่จะเปิดโลกทัศน์ใหม่ๆ เรียนรู้จากกรณีศึกษา และร่วมสนุกกับกิจกรรมที่จะทำให้เห็นภาพความเป็นส่วนตัวชัดเจนขึ้น

1. ความเป็นส่วนตัว: สมบัติล้ำค่าในยุคดิจิทัล

เคยรู้สึกไหมว่ามีใครกำลังแอบดูคุณอยู่ ในยุคดิจิทัลนี้ ความรู้สึกนั้นอาจเป็นจริง! ลองนึกภาพ: คุณกำลังเดินอยู่บนถนน จู่ ๆ มีคนแปลกหน้าเข้ามาถาม “คุณชื่ออะไร อยู่ที่ไหน ชอบอะไร?” คุณคงรู้สึกอึดอัดใช่ไหม แต่ในโลกออนไลน์ เรื่องแบบนี้เกิดขึ้นทุกวินาทีโดยที่คุณอาจไม่รู้ตัว!

ความเป็นส่วนตัวคืออะไร ทำไมต้องสนใจ มันคือสิทธิที่คุณจะควบคุมข้อมูลของตัวเองได้ ไม่ว่าจะเป็นชื่อ ที่อยู่ หรือความชอบส่วนตัว คุณอาจคิดว่า “ฉันไม่ได้ทำอะไรผิด จะกลัวทำไม?” แต่ลองคิดดู ถ้าทุกย่างก้าวถูกบันทึก ทุกการค้นหาถูกเก็บไว้ ทุกข้อความถูกอ่าน... คุณจะรู้สึกยังไง? นี่คือเหตุผลที่ต้องให้ความสนใจเรื่องความเป็นส่วนตัว

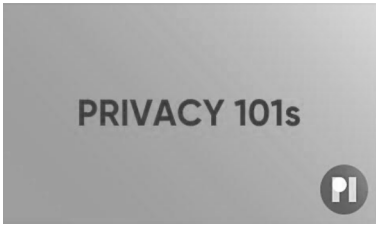
แต่สิ่งที่เป็นความท้าทายและความยากระดับโลกของเรื่องนี้ คือ แต่ละประเทศมองเรื่องความเป็นส่วนตัวไม่เหมือนกัน บางที่ถือว่าสำคัญมาก แต่บางที่กลับมองว่าไม่จำเป็น เหมือนกับการเล่นเกมที่กติกาเปลี่ยนไปเรื่อย ๆ ตามแต่ละด่าน นี่คือความยากในการสร้างกฎหมายคุ้มครองความเป็นส่วนตัวระดับโลก

เรื่องจริงที่อาจไม่เชื่อ ในจีน 78.2% ของคนออนไลน์เคยโดนขโมยข้อมูลส่วนตัว ตั้งแต่ชื่อยันเลขบัตรประชาชน ส่วนในเวียดนาม แฮกเกอร์เคยขโมยข้อมูลลูกค้า 2 ล้านคนจากแพลตฟอร์มเงินดิจิทัล แล้วเอาไปขายออนไลน์

อย่าลืมว่า ในโลกที่ข้อมูลคือพลัง การคุ้มครองข้อมูลของเราก็คือการปกป้องอิสรภาพของตัวเราเอง!

ประเด็นอภิปราย (15 นาที): เราเข้าใจสิทธิความเป็นส่วนตัวอย่างไร

มาร่วมกันสำรวจโลกความเป็นส่วนตัวในยุคดิจิทัลกัน! เริ่มด้วยการดูคลิปสั้น ๆ ที่จะเปิดมุมมองใหม่ จากนั้นแชร์ประสบการณ์สุดล้ำของ เคยโดนแอบดูข้อมูลไหม? มีอะไรในคลิปที่ทำให้เราอึ้ง? แล้วลองมองผ่านเลนส์วัฒนธรรมบ้านเรา สังคมไทยมองเรื่องนี้ยังไง? มีสำนวนไทยเด็ด ๆ เกี่ยวกับความเป็นส่วนตัวไหม? จับกลุ่มแล้วระดมไอเดียสุดครีเอทกัน



ที่มา: **"What Is Privacy? | Privacy International" (2015)**
https://youtu.be/zsboDBMq6vo

2. ประเภทของความเป็นส่วนตัว

ถ้าคุณนึกสงสัยว่าทำไมกฎหมายความเป็นส่วนตัวถึงซับซ้อนนัก? ไม่ต้องกังวล! เรามีเครื่องมือเจ๋ง ๆ ที่จะช่วยให้เข้าใจได้ง่ายขึ้น นั่นคือ **"4Ps"** ของความเป็นส่วนตัว

Q: แล้ว 4Ps คืออะไร?

A: **4Ps** คือคำ 4 คำ ได้แก่ 1) ผู้คน (People) 2) สถานที่ (Place) 3) แพลตฟอร์ม (Platform) และ 4) วัตถุประสงค์ (Purpose) เพื่อทำความเข้าใจ เราจะมาไล่พิจารณากันทีละคำ

1) ผู้คน (People): ใครบ้างที่เกี่ยวข้อง? พนักงาน ลูกค้า หรือแม้แต่เด็ก? กฎหมายความเป็นส่วนตัวมักจะเกี่ยวข้องกับคนที่ระบุตัวตนได้เท่านั้น! และอย่าลืม ข้อมูลแต่ละประเภทก็มีความสำคัญไม่เท่ากัน ชื่อ-นามสกุล อาจไม่เท่ากับข้อมูลชีวมิติ หรือที่อยู่ IP ของเรา

2) สถานที่ (Places): คิดว่ากฎหมายมีผลเฉพาะภายในประเทศ ไม่ข้ามเขต? คิดใหม่! บางกฎหมายมีอำนาจข้ามทวีปเลยนะ เช่น กฎหมายของแคลิฟอร์เนีย บราซิล หรือสหภาพยุโรป อาจส่งผลถึงเราโดยที่เราไม่รู้ตัว ดังนั้น รู้ไว้ว่าเราอยู่ที่ไหน ทำงานที่ไหน และอาจเดินทางไปไหนบ้าง เพื่อไม่ให้พลาดกฎเกณฑ์ต่าง ๆ

3) แพลตฟอร์ม (Platforms): โลกดิจิทัลไม่ได้มีแค่เว็บไซต์! ทุกวันนี้มีทั้งแอปพลิเคชันมือถือ อุปกรณ์ IoT และแม้แต่รถยนต์ที่เก็บข้อมูล แต่ละแพลตฟอร์มก็มีวิธีจัดการข้อมูลต่างกัน บางที่ใช้คุกกี้ บางที่ใช้เทคโนโลยีติดตาม ทำให้ชีวิตสะดวกขึ้น ทำให้เราต้องระวังความเป็นส่วนตัว!

4) วัตถุประสงค์ (Purposes): ทำไมเขาต้องเก็บข้อมูลเราเพื่อโฆษณา เพื่อรักษาโรค หรือเพื่อความปลอดภัย? แต่ละวัตถุประสงค์มีกฎเกณฑ์ไม่เหมือนกัน บางทีอาจทำให้มีภาระทางกฎหมายเพิ่มขึ้นโดยไม่รู้ตัว ดังนั้น ก่อนให้ข้อมูลใคร ถามตัวเองก่อนว่า “เขาจะเอาไปทำอะไร?”

หลัก 4Ps ในทางปฏิบัติ:

ลองนึกถึงร้านค้าเล็ก ๆ ในจาการ์ตาที่อยากก้าวสู่โลกออนไลน์ พวกเขาสร้างเว็บไซต์และเริ่มส่งอีเมลการตลาด แต่ลูกค้าไม่ได้มีแค่คนอินโดนีเซีย อาจมาจากเวียดนามหรือมาเลเซียด้วย นี่คือตัวอย่างที่ 4Ps ทำงานพร้อมกัน:

1) ผู้คน ได้แก่ ลูกค้าจากหลายประเทศ

2) สถานที่ ได้แก่ ร้านในอินโดนีเซียแต่ขายทั่วโลก

3) แพลตฟอร์ม ได้แก่ เว็บไซต์และอีเมล

4) วัตถุประสงค์ ได้แก่ การขายของและทำการตลาด

ทั้งหมดนี้ต้องอยู่ภายใต้นโยบายความเป็นส่วนตัวที่รัดกุม เพื่อให้ธุรกิจเติบโตอย่างปลอดภัยและถูกกฎหมาย ไม่ว่าลูกค้าจะอยู่มุมไหนของโลก

ประเภทของความเป็นส่วนตัว

ความเป็นส่วนตัวของเรามีถึง 4 แบบด้วยกัน เริ่มจากความเป็นส่วนตัวของร่างกาย นี่คือสิทธิที่จะปกป้องร่างกายเราจากการถูกล่วงล้ำโดยไม่ได้รับอนุญาต ไม่ว่าจะเป็นการตรวจ DNA การตรวจสารเสพติด หรือแม้แต่การเจาะเลือด ทุกอย่างต้องได้รับความยินยอมจากเราก่อน นอกจากนี้ ยังรวมถึงเรื่องละเอียดอ่อนอย่างการคุมกำเนิด การทำแท้ง หรือการรับเลี้ยงบุตรบุญธรรมด้วย

ต่อมาคือความเป็นส่วนตัวในการสื่อสาร เรามีสิทธิที่จะเลือกว่าจะคุยกับใคร ด้วยวิธีไหน ไม่ว่าจะเป็นจดหมาย โทรศัพท์ อีเมล หรือแชทในแอปต่าง ๆ ไม่มีใครมีสิทธิมาแอบดู แอบฟัง หรือดักข้อมูลของเราโดยไม่ได้รับอนุญาต

ประเภทที่สามคือความเป็นส่วนตัวของข้อมูล ในยุคดิจิทัล ข้อมูลของเราถูกใช้และแชร์ไปทั่ว แต่เราต้องมีสิทธิควบคุมว่าใครจะเก็บ ใช้ หรือแชร์ข้อมูลของเราได้บ้าง ไม่ว่าจะเป็นข้อมูลการเงิน ประวัติการรักษา หรือแม้แต่ประวัติการเข้าเว็บไซต์ต่าง ๆ

สุดท้าย คือความเป็นส่วนตัวในอาณาเขต ซึ่งไม่ได้หมายถึงแค่บ้านหรือที่ทำงานของเรา แต่รวมถึงพื้นที่ส่วนตัวในที่สาธารณะด้วย เราควรได้รับการปกป้องจากการถูกค้นตัว การถูกติดตามด้วยกล้องวงจรปิด หรือการถูกสอดรู้สอดเห็นโดยไม่จำเป็น

การรู้จักและเข้าใจสิทธิความเป็นส่วนตัวทั้ง 4 แบบนี้ จะช่วยให้เราสามารถปกป้องตัวเองได้ดีขึ้นในโลกที่ดูเหมือนจะไม่มีความลับอีกต่อไป จำไว้ว่าความเป็นส่วนตัวคือสิทธิของเรา และเราทุกคนมีหน้าที่ในการปกป้องมันไว้

ความเป็นส่วนตัวในสภาพแวดล้อมดิจิทัล

ความก้าวหน้าทางเทคโนโลยีได้เปลี่ยนแปลงภูมิทัศน์ของข้อมูลอย่างมีนัยสำคัญ การวิเคราะห์และจัดเก็บข้อมูลมีราคาถูกลงและทำได้ง่ายขึ้น อุปกรณ์อัจฉริยะและนาโนบอทในร่างกายมนุษย์เพิ่มการเชื่อมต่อดิจิทัล AI

และ IoT เปิดโอกาสให้รัฐบาลและบริษัทยักษ์ใหญ่สามารถรวบรวมข้อมูลเกี่ยวกับกิจกรรม พฤติกรรม และวิถีชีวิตของมนุษย์ในทุกด้าน การเข้าถึงข้อมูลขนาดใหญ่เป็นปัจจัยสำคัญในการแข่งขันทางธุรกิจ รัฐบาลทั่วโลกจึงออกกฎหมายเพื่อเพิ่มความปลอดภัยและการควบคุมข้อมูลส่วนบุคคล โดยมองว่าความเป็นส่วนตัวเป็นสิทธิมนุษยชนสำคัญ

ในความเป็นจริง ข้อมูลส่วนบุคคลมักถูกประมวลผลด้วยวิธีและวัตถุประสงค์หลายประการ ซึ่งบางส่วนไม่สามารถคาดหวังได้เมื่อได้รับความยินยอมจากเจ้าของข้อมูล ผู้ใช้มักไม่อ่านเงื่อนไขการใช้งานอย่างละเอียด แนวคิด ***"สิทธิที่จะอยู่ตามลำพัง"*** กำลังถูกท้าทายโดยเทคโนโลยีสมัยใหม่ เช่น เซ็นเซอร์ กล้องวงจรปิด และผู้ช่วยดิจิทัล เกิดแนวคิดใหม่ เช่น สิทธิในการคัดค้านการสร้างโปรไฟล์อัตโนมัติ ตัวอย่างที่เห็นได้ชัดคือการที่รัฐบาลหลายประเทศเริ่มใช้ระบบระบุตัวตนดิจิทัลแห่งชาติ ซึ่งรวบรวมข้อมูลส่วนบุคคลจำนวนมาก ก่อให้เกิดความกังวลด้านความเป็นส่วนตัว

แนวคิดความเป็นส่วนตัวแบบเครือข่าย

วาทกรรมความเป็นส่วนตัวในยุคดิจิทัลมักเน้นสิทธิของปัจเจกบุคคลในการควบคุมข้อมูล ***"ส่วนตัว"*** แต่ในความเป็นจริง การคุ้มครองความเป็นส่วนตัวต้องมองกว้างกว่าระดับบุคคล เนื่องจากข้อมูลมีความเชื่อมโยงกันอย่างซับซ้อน ตัวอย่างเช่น การตรวจ DNA อาจเปิดเผยข้อมูลของผู้อื่นที่มีความเกี่ยวข้องทางพันธุกรรม ข้อมูลการใช้โซเชียลมีเดียอาจเปิดเผยข้อมูลของเพื่อนและคนรู้จัก การพึ่งพาเพียงการควบคุมและความยินยอมของแต่ละคนจึงอาจไม่เพียงพอ จำเป็นต้องหาวิธีใหม่ในการดูแลความเป็นส่วนตัวที่คำนึงถึงลักษณะเครือข่ายของข้อมูล เช่น การพัฒนากฎหมายที่คุ้มครองความเป็นส่วนตัวในระดับกลุ่มหรือชุมชน และการสร้างความตระหนักรู้เกี่ยวกับผลกระทบของการแบ่งปันข้อมูลต่อบุคคลอื่น

อย่าลืมว่าในโลกดิจิทัล การปกป้องคุ้มครองความเป็นส่วนตัวไม่ใช่แค่เรื่องของตัวเราคนเดียว แต่เป็นความรับผิดชอบของทุกคน! เราต้องฉลาดในการใช้เทคโนโลยี และรู้จักปกป้องตัวเองและคนรอบข้าง

คำถามชวนคิด: คิดว่าเราควรทำอย่างไรเพื่อสร้างสมดุลระหว่างประโยชน์ของเทคโนโลยีและการปกป้องความเป็นส่วนตัว?

ประเด็นอภิปราย "พลังแห่งความเป็นส่วนตัวในยุคดิจิทัล"

ดูวิดีโอ The Guardian "อินเทอร์เน็ตรู้ที่อยู่คุณไหม?" แล้วอภิปรายว่าความเป็นส่วนตัวออนไลน์เปลี่ยนไปอย่างไร ส่งผลต่องานเรายังไง มีตัวอย่างในประเทศไหม แชร์ประสบการณ์ถูกละเมิดความเป็นส่วนตัวและวิธีป้องกัน สรุปประเด็นสำคัญร่วมกัน เตรียมพร้อมแลกเปลี่ยนไอเดียและรับฟังมุมมองใหม่ ๆ

ที่มา: **"The power of privacy (1/5): Does the internet know where you live?" (2015)** https://youtu.be/iA89GhyLao8

เมื่อชีวิตเราถูกแปลงเป็นข้อมูล

รู้หรือไม่ว่า ทุกการกระทำของเราในโลกออนไลน์กำลังถูกบันทึกเป็นข้อมูลนี่แหละคือ "Datafication" หรือการแปลงทุกสิ่งเป็นข้อมูลดิจิทัล!

ทุกการกด "ไลค์" บน Facebook ไม่ใช่แค่การแสดงความชื่นชอบ แต่มันบอกได้ว่าเราเป็นใคร ชอบอะไร ทุกก้าวที่เราเดิน ทุกที่ที่เราไปก็กำลังถูกติดตามด้วย GPS หรือแม้แต่การค้นหาบน Google ก็เผยความต้องการ

ของเรา เพราะในยุค IoT อุปกรณ์รอบตัวก็ส่งข้อมูลตลอดเวลา ทั้งข้อมูลในอีเมล พิกัดในรูปถ่าย AI ล้ำ ๆ วิเคราะห์พฤติกรรมอย่างละเอียด

Q: แล้วทำไมบริษัทใหญ่ถึงอยากได้ข้อมูลพวกนี้?

A: นั่นก็เพราะมันช่วยให้การตัดสินใจแม่นยำยิ่งขึ้น ไม่ว่าจะเป็นการตัดสินใจในการออกแบบการทำการตลาด วินิจฉัยโรค หรือแม้แต่ป้องกันอาชญากรรม! นี่เป็นเหตุผลที่ Netflix หรือ Amazon สร้างระบบปิด เพื่อควบคุมและสร้างมูลค่าจากข้อมูลเรา

ลองสังเกตดูว่าในชีวิตประจำวัน อะไรบ้างที่กลายเป็น “ข้อมูล” โดยที่เราไม่รู้ตัว แล้วเราจะรักษาความเป็นส่วนตัวได้ดีขึ้น!

ข้อมูลขนาดใหญ่: 4V ที่ต้องรู้!

คิดว่าข้อมูลเป็นแค่ตัวเลขไหม? หากใช่ คิดใหม่! ข้อมูลขนาดใหญ่มีมิติที่น่าทึ่งกว่านั้นมาก

1. ปริมาตร (Volume): มหาศาลจนคิดไม่ถึง! ข้อมูลมากมายมหาศาลจนเก็บในคอมธรรมดาไม่ไหว

2. ความหลากหลาย (Variety): ไม่ใช่แค่ตัวเลข! ทั้งข้อความ รูปภาพ วิดีโอ เสียง ทุกอย่างล้วนเป็นข้อมูลได้ทั้งหมด

3. ความเร็ว (Velocity): เร็วจี๋เหมือนสายฟ้า! ข้อมูลไหลเข้ามาแบบเรียลไทม์ ทันใจจริง ๆ

4. ความจริง (Veracity): จริงหรือปลอม? เราต้องแยกแยะให้ดีว่าข้อมูลไหนเชื่อถือได้

ข้อมูลส่วนบุคคลกับข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคล

ในยุคเศรษฐกิจดิจิทัล ข้อมูลส่วนบุคคลมีมูลค่ามหาศาล! บริษัทต่างแย่งชิงข้อมูลเพื่อสร้างบริการแบบเฉพาะตัว ทำให้เส้นแบ่งระหว่างผู้บริโภคและผู้ผลิตเลือนราง แต่ระวัง! การวิเคราะห์ข้อมูลขนาดใหญ่และ AI อาจส่งผลกระทบต่อกลุ่มเปราะบาง ด้วยเหตุนี้ GDPR จึงถูกสร้างขึ้นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูล แต่หลายประเทศยังตามไม่ทัน การสร้างสมดุลระหว่างธุรกิจและสิทธิมนุษยชนจึงยังคงเป็นความท้าทาย

รู้หรือไม่ ข้อมูลอ่อนไหวตาม GDPR รวมถึงเชื้อชาติ ศาสนา สุขภาพ และข้อมูลชีวภาพ! ระวังเมื่อใช้เทคโนโลยีไบโอเมตริกซ์ เช่น สแกนลายนิ้วมือ ม่านตา หรือใบหน้า เพราะหากถูกละเมิด จะยากต่อการกู้คืนหรือเปลี่ยนแปลง ต่างจากรหัสผ่านที่เปลี่ยนได้ง่าย

นอกจากนี้ AI ก็สร้างความท้าทายไม่แพ้กัน! การใช้ข้อมูลอ่อนไหวในอัลกอริทึมอาจนำไปสู่ข้อสรุปที่มีอคติ ส่งผลต่อความเท่าเทียมในการให้บริการ นักวิทยาศาสตร์จึงพัฒนา “ไบโอเมตริกที่ยกเลิกได้” และ “ขอบเขตความเป็นธรรมของอัลกอริทึม” เพื่อแก้ปัญหานี้

ผู้ประกอบวิชาชีพไม่ควรลืมว่าข้อมูลอาจไม่ใช่ข้อมูลส่วนบุคคลสำหรับผู้ควบคุม/ประมวลผลข้อมูลรายใดรายหนึ่ง แต่เมื่อโอนไปยังมือของผู้รับโอน ข้อมูลดังกล่าวจะกลายเป็นข้อมูลส่วนบุคคล (เนื่องจากผู้รับโอนเก็บข้อมูลอื่นซึ่งหากอ้างอิงถึงข้อมูลที่ถ่ายโอนจะกลายเป็นข้อมูลส่วนบุคคล หรือ ข้อมูลที่สามารถระบุตัวบุคคลได้) กล่าวโดยสรุป เจ้าของข้อมูลจะสามารถระบุตัวตนได้หากข้อมูลที่ถ่ายโอนถูกอ้างอิงถึงข้อมูลที่อยู่ในมือของผู้รับโอน นี่เป็นช่องโหว่ด้านกฎระเบียบอย่างหนึ่งที่ต้องปิดในเขตอำนาจศาลบางแห่ง และญี่ปุ่นก็เป็นหนึ่งในเขตอำนาจศาลในเอเชียที่ปิดช่องโหว่นี้

ข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคล

เคยสงสัยไหมว่าทำไมบางข้อมูลถึงแชร์กันได้อย่างเสรี แต่บางอย่างกลับถูกปกปิดอย่างมิดชิด เหมือนกับการที่เราสวมเสื้อผ้าออกจากบ้าน บางส่วนเราอยากให้โลกเห็น แต่บางส่วนเราก็อยากเก็บไว้เป็นความลับ

ในโลกของข้อมูล เราก็มี **“ตู้เสื้อผ้า”** แบบพิเศษ ที่เรียกว่า **“ชุดข้อมูลแบบผสม”** มีทั้งข้อมูลส่วนตัวที่เป็นเหมือนชุดชั้นในอันเป็นความลับ และข้อมูลทั่วไปที่เหมือนเสื้อผ้าที่เราใส่ออกไปเดินห้าง

ในโลกที่ข้อมูลไหลเวียนอย่างเสรี เราต้องเรียนรู้ที่จะสร้างสมดุล ระหว่างการแบ่งปันข้อมูลเพื่อพัฒนาเศรษฐกิจและนวัตกรรม กับการปกป้องความเป็นส่วนตัวของเรา เหมือนกับการเลือกเสื้อผ้าให้เหมาะกับกาลเทศะ บางครั้งเราอาจต้องเปิดเผยข้อมูลบางอย่างเพื่อประโยชน์ส่วนรวม แต่ก็ต้องระวังไม่ให้ละเมิดความเป็นส่วนตัวของใคร

3. แนวคิดการคุ้มครองข้อมูลส่วนบุคคล

กฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายที่มีจุดประสงค์เพื่อคุ้มครองสิทธิในข้อมูลส่วนตัวของประชาชน กฎหมายนี้มีบทบาทสำคัญในการควบคุมการดำเนินงานขององค์กรและรัฐบาล โดยมีเป้าหมายให้เจ้าของข้อมูลมีอำนาจควบคุมข้อมูลของตนเอง

กฎหมายนี้ครอบคลุมหลายประเด็น เริ่มจากการรับรองความเป็นส่วนตัวเป็นสิทธิมนุษยชนขั้นพื้นฐาน กำหนดแนวทางการจัดการและแบ่งปันข้อมูล รวมถึงสนับสนุนนวัตกรรมใหม่ เช่น แซนด์บ็อกซ์ข้อมูล ซึ่งเป็นพื้นที่ทดลองใช้ข้อมูลอย่างปลอดภัย

ปัจจุบัน กฎหมายคุ้มครองข้อมูลทั่วโลกมีความหลากหลาย GDPR ของสหภาพยุโรปเป็นตัวอย่างที่สำคัญ ให้สิทธิผู้ใช้ขอลบหรือโอนย้ายข้อมูล และสอบถามเหตุผลการเก็บข้อมูล หากละเมิด บริษัทอาจถูกปรับสูงถึง 4% ของยอดขายทั่วโลก

อย่างไรก็ตาม กว่า 30% ของประเทศทั่วโลก โดยเฉพาะประเทศกำลังพัฒนา ยังไม่มีกฎหมายคุ้มครองข้อมูล นอกจาก GDPR ยังมีกรอบการคุ้มครองข้อมูลอื่น ๆ เช่น APEC Privacy Framework และแนวทางของ OECD และอนุสัญญา 108+ ที่พยายามปกป้องข้อมูลของคุณเหมือนกัน

การคุ้มครองข้อมูลส่วนบุคคลยังคงเป็นประเด็นสำคัญที่ต้องพัฒนาต่อไป เพื่อรักษาสมดุลระหว่างประโยชน์ทางเศรษฐกิจและการปกป้องสิทธิของประชาชน

4. สิทธิตามรัฐธรรมนูญในการเรียกร้องข้อมูล

ในโลกที่ข้อมูลคืออำนาจ **“สิทธิตามรัฐธรรมนูญในการเรียกร้องข้อมูล”** หรือ **“habeas data”** ถือเป็นโล่ที่ใช้ปกป้องตัวเรา หลายประเทศในโลกได้รับรองสิทธินี้เอาไว้ภายใต้รัฐธรรมนูญเพื่อเป็นหลักประกันให้ประชาชนสามารถเข้าถึง ตรวจสอบ และแก้ไขข้อมูลส่วนตัวที่ถูกเก็บไว้โดยหน่วยงานรัฐหรือองค์กรต่าง ๆ ไม่เพียงเท่านั้น หากพบการละเมิด ก็ยังสามารถร้องเรียนต่อศาลได้ด้วยการใช้สิทธินี้เริ่มจากการรู้จักสิทธิของตนเอง ศึกษากฎหมายในประเทศ ตรวจสอบข้อมูลที่หน่วยงานเก็บไว้ และกล้าที่จะแก้ไขเมื่อพบข้อผิดพลาด ในบราซิล ประชาชนสามารถขอดูข้อมูลส่วนตัวจากหน่วยงานรัฐได้โดยตรง ส่วนฟิลิปปินส์มี “หมายเรียกร้องข้อมูล” เป็นเครื่องมือทางกฎหมายในการปกป้องสิทธิความเป็นส่วนตัว เมื่อทุกการกระทำถูกบันทึกเป็นข้อมูล สิทธินี้จึงเป็นเครื่องมือสำคัญในการควบคุมข้อมูลส่วนบุคคล สร้างความโปร่งใส และปกป้องความเป็นส่วนตัวในยุคดิจิทัล

กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) มาตรา 16 และ 17 วางหลักสำคัญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไว้ว่า การเก็บข้อมูลส่วนตัวต้องมีกฎหมายควบคุม ไม่ว่าจะเป็นรัฐหรือเอกชนที่เก็บ รัฐต้องมีมาตรการที่ดีเพื่อป้องกันไม่ให้ข้อมูลส่วนตัวรั่วไหลหรือถูกใช้ผิดวัตถุประสงค์ ทุกคนควรมีสิทธิรู้ว่าใครเก็บข้อมูลอะไรของตนไว้บ้างและเก็บไว้ทำไม และถ้าพบว่าข้อมูลผิดหรือถูกเก็บอย่างไม่ถูกกฎหมาย ทุกคนควรมีสิทธิขอแก้ไขหรือลบได้ หลักการนี้ช่วยให้เราควบคุมข้อมูลส่วนตัวของเราได้ดีขึ้นและป้องกันการละเมิดความเป็นส่วนตัว ในยุคที่ข้อมูลมีความสำคัญอย่างยิ่ง

การแยกการคุ้มครองข้อมูลเป็นสิทธิแยกขาดจากสิทธิอื่น

การคุ้มครองข้อมูลส่วนบุคคลกำลังกลายเป็นประเด็นร้อนในวงการกฎหมายและวิชาการ แม้จะเริ่มต้นจากแนวคิดเรื่องความเป็นส่วนตัว แต่ตอนนี้มันได้พัฒนาไปไกลกว่านั้นมาก! มันกลายเป็นหน้าที่ใหม่สำหรับทั้งรัฐและเอกชนที่ต้องให้เราควบคุมข้อมูลตัวเองได้ ไม่ว่าจะดู แก้ไข หรือยืนยันความถูกต้อง นอกจากนี้ ยังครอบคลุมสิทธิอื่นๆ เช่น สิทธิในการได้รับแจ้งสิทธิที่จะถูกลืม สิทธิในการเคลื่อนย้ายข้อมูล สิทธิในการคัดค้านการประมวลผล และสิทธิเกี่ยวกับการตัดสินใจอัตโนมัติและการจัดทำโปรไฟล์ ทำให้การคุ้มครองข้อมูลมีขอบเขตกว้างและซับซ้อนกว่าเพียงแค่ความเป็นส่วนตัว

แนวคิดนี้ได้รับการยอมรับเป็นสิทธิแยกต่างหากในกฎหมายและคำตัดสินของศาลในหลายประเทศทั่วโลก โดยสหภาพยุโรปรับรองเอาไว้ในกฎบัตรสิทธิขั้นพื้นฐาน มาตรา 8 ขณะที่ศาลฎีกาประเทศบราซิลก็ยอมรับแนวคิดนี้ และเมื่อเร็ว ๆ นี้ ศาลฎีกาประเทศอินเดียก็ยังยืนยันว่าความเป็นส่วนตัวเป็นสิทธิขั้นพื้นฐาน ในคดีระหว่างผู้พิพากษา K.S. Puttaswamy (เกษียณอายุ) กับสหภาพอินเดีย สะท้อนให้เห็นถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลในยุคดิจิทัล

5. หลักการสำคัญในการคุ้มครองข้อมูล

การคุ้มครองข้อมูลในปัจจุบันเน้นแนวทางแบบองค์รวม ผสมผสานมาตรการทางกฎหมาย การบริหาร และเทคนิคเข้าด้วยกัน หลายประเทศได้ออกกฎหมายคุ้มครองข้อมูลและความเป็นส่วนตัวที่ครอบคลุมทั้งภาครัฐและเอกชน โดยมีหลักการสำคัญดังนี้

1. จำกัดการใช้และรวบรวมข้อมูล: การเก็บและใช้ข้อมูลต้องชอบด้วยกฎหมาย ได้รับความยินยอม และมีวัตถุประสงค์ชัดเจน เช่น แอปสุขภาพต้องขออนุญาตก่อนเก็บข้อมูลการออกกำลังกาย พร้อมอธิบายวิธีการใช้ข้อมูล

2. เก็บข้อมูลเท่าที่จำเป็น: องค์กรควรเก็บเฉพาะข้อมูลที่จำเป็นจริง ๆ ไม่มากเกินไป ตัวอย่างเช่น ร้านค้าออนไลน์ควรเก็บเพียงชื่อ ที่อยู่ และข้อมูลการชำระเงิน โดยไม่จำเป็นต้องเก็บข้อมูลส่วนตัวอื่น เช่น วันเกิดหรืออาชีพ

3. ปฏิบัติตามกฎหมายและเปิดเผย: การจัดการข้อมูลต้องมีเหตุผลทางกฎหมายรองรับและดำเนินการอย่างโปร่งใส เช่น บริษัทประกันสุขภาพต้องแจ้งลูกค้าว่าจะเก็บข้อมูลสุขภาพเพื่อประเมินความเสี่ยงตามกฎหมายประกันภัย

4. ดำเนินการอย่างเป็นธรรม: การจัดการข้อมูลต้องเป็นธรรม ไม่เอาเปรียบหรือสร้างผลเสียแก่เจ้าของข้อมูล เช่น ธนาคารไม่ควรใช้ข้อมูลการใช้จ่ายของลูกค้าเพื่อปฏิเสธการให้สินเชื่อโดยไม่มีเหตุผลอันสมควร

5. โปร่งใส: องค์กรต้องเปิดเผยวิธีการใช้ข้อมูลอย่างชัดเจนตรงไปตรงมา ให้เจ้าของข้อมูลเข้าใจได้ง่าย เช่น เว็บไซต์ข่าวควรมีนโยบายความเป็นส่วนตัวที่อธิบายการใช้คุกกี้และการเก็บข้อมูลผู้อ่านอย่างละเอียดและเข้าใจง่าย

6. รักษาความถูกต้องและความทันสมัยของข้อมูล: องค์กรต้องดูแลให้ข้อมูลถูกต้อง เป็นปัจจุบัน และแก้ไขข้อผิดพลาดโดยเร็ว เช่น โรงพยาบาลต้องปรับปรุงประวัติการรักษาของผู้ป่วยให้เป็นปัจจุบันเสมอ และแก้ไขข้อมูลที่ผิดพลาดทันทีเมื่อพบ

7. จำกัดการเก็บข้อมูล: องค์กรไม่ควรเก็บข้อมูลไว้นานเกินจำเป็น และควรให้สิทธิผู้ใช้เลือกระยะเวลาการเก็บข้อมูลได้ เช่น บริษัท e-commerce ควรลบข้อมูลบัตรเครดิตของลูกค้าหลังจากทำธุรกรรมเสร็จ หรือให้ลูกค้าเลือกระยะเวลาการเก็บข้อมูล

เทคโนโลยีเพิ่มความเป็นส่วนตัวและความรับผิดชอบในการคุ้มครองข้อมูล

ในยุคดิจิทัล การคุ้มครองข้อมูลส่วนบุคคลต้องอาศัยเทคโนโลยีและความรับผิดชอบขององค์กร เทคโนโลยีเพิ่มความเป็นส่วนตัว (Privacy-enhancing technologies หรือ PETs) เป็นเครื่องมือสำคัญที่ช่วยปกป้องความเป็นส่วนตัว และคุ้มครองข้อมูลส่วนบุคคล เช่น การเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การปกปิดตัวตน (Anonymization) ลบข้อมูลที่สามารถระบุตัวบุคคลได้ การใช้นามแฝง (Pseudonymization) แทนที่ข้อมูลส่วนบุคคลด้วยรหัสที่ไม่สามารถระบุตัวตนได้โดยตรง ตลอดจนการใช้โทเค็นแทนตัวระบุที่ไม่ซ้ำกัน ช่วยลดการเก็บข้อมูลส่วนตัวที่ไม่จำเป็นและป้องกันการประมวลผลข้อมูลที่ไม่พึงประสงค์ในด้านความรับผิดชอบ

การประมวลผลข้อมูลส่วนบุคคลควรอยู่ภายใต้การกำกับดูแลของหน่วยงานอิสระที่ได้รับอนุญาต และการควบคุมโดยเจ้าของข้อมูลเอง แต่ละประเทศอาจมีรูปแบบการกำกับดูแลที่แตกต่างกัน อาจมีหน่วยงานกำกับดูแลหลายหน่วยงาน หรือแบ่งตามการจัดการข้อมูลขององค์กรภาครัฐหรือเอกชน นอกจากนี้ การโอนข้อมูลระหว่างประเทศก็เป็นประเด็นสำคัญ กฎหมายควรห้ามการโอนข้อมูลไปยังประเทศที่ไม่มีมาตรการคุ้มครองที่เพียงพอ (Equivalency) เพื่อป้องกันการนำข้อมูลไปใช้ในทางที่ไม่เหมาะสม

6. มาตรฐานสากลในโลกดิจิทัล:

เมื่อทุกประเทศถือไพ่คนละใบโลกข้อมูลนั้นซับซ้อนกว่าที่คิด! แต่ละประเทศมีกฎเกณฑ์ต่างกันไปในการคุ้มครองข้อมูล ทั้งเรื่องใครเข้าถึงได้ ใครรับผิดชอบ และใครต้องรับโทษ การบอกว่าใครเป็นเจ้าของข้อมูลนั้นยากยิ่งกว่าการชี้ว่าใครเป็นเจ้าของบ้านหรือรถยนต์เสียอีก! เหมือนร้านอาหารที่มีเมนูหลากหลายให้เลือก

สหภาพยุโรปเสิร์ฟเมนูเด็ดอย่าง GDPR ที่หลายประเทศนำไปเป็นแบบอย่าง โดยกฎหมายฉบับนี้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเข้มงวด ให้อำนาจผู้ใช้ในการควบคุมข้อมูลของตนเอง

ขณะที่ออสเตรเลียกับนิวซีแลนด์กลับคิดต่าง โดยมองว่าการเข้าถึงข้อมูลเป็นสิทธิของผู้บริโภค ไม่ใช่เรื่องความเป็นเจ้าของ เหมือนให้เราดูเมนูในร้านอาหาร แต่ไม่ได้ให้เราเป็นเจ้าของร้าน แนวคิดนี้เน้นการให้สิทธิผู้ใช้ในการเข้าถึงและแก้ไขข้อมูลของตนเอง แทนที่จะกำหนดความเป็นเจ้าของอย่างชัดเจน

แม้ว่าแนวคิดและหลักการคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศอาจแตกต่างกัน แต่ไม่ต้องกังวล เพราะประเทศทั่วโลกต่างเห็นพ้องกันเรื่องบทบาทหลัก ๆ ในวงจรชีวิตของข้อมูล เรียกว่าว่าอาจมีชื่อเรียกที่ต่างกันอยู่บ้าง ความรับผิดชอบก็อาจไม่เหมือนกันเสียทีเดียว แต่ก็มีเป้าหมายเดียวกันคือการปกป้องคุ้มครองข้อมูลและสิทธิของผู้ใช้ในยุคดิจิทัล!

เจ้าของข้อมูล: ตัวจริงหรือแค่นามธรรมในโลกดิจิทัล?

หากถามว่าใครคือเจ้าของข้อมูลในโลกดิจิทัล ภายใต้ GDPR ได้ตอบเอาไว้อย่างชัดเจนว่าผู้เป็นเจ้าของก็คือตัวคุณนั่นเอง! ทุกอย่างที่เกี่ยวกับคุณตั้งแต่รูปร่างหน้าตา DNA ความคิด ไปจนถึงฐานะ และวิถีชีวิต ข้อมูลไม่ว่าโดยทางตรง หรือทางอ้อมที่เชื่อมโยงกับตัวคุณต่างนำไปสู่การบ่งบอกตัวคุณ

ในโลกดิจิทัล ความเป็นเจ้าของข้อมูลนั้นซับซ้อน แม้ข้อมูลจะเกิดจากตัวคุณ แต่เมื่อคุณ **“ยินยอม”** ให้ผู้อื่นใช้ ความเป็นเจ้าของก็ของคุณอาจหลุดลอยไป อย่างไรก็ตาม ก็ไม่ได้หมายความว่าคุณจะไม่เหลือสิทธิใด ๆ เลยเพราะในความเป็นจริงคุณยังคงมีอำนาจอยู่บ้าง คล้ายกับเจ้าของบ้านที่ให้คนอื่นเช่า แม้ว่าขณะให้ผู้อื่นเช่า คุณจะไม่ได้ควบคุมทุกอย่าง แต่ก็ยังคงมีสิทธิสำคัญอยู่ เช่น สิทธิที่จะถูกลืม (ขอลบข้อมูลได้) สิทธิแก้ไขข้อมูลที่ผิด และสิทธิเข้าถึงข้อมูลว่าใครเก็บอะไรไว้บ้าง สิทธิเหล่านี้ทำให้คุณยังมีอำนาจบางส่วนเหนือข้อมูลของตนเอง แม้ไม่ใช่เจ้าของ 100% แต่ก็ยังดีกว่าไม่มีอะไรเลย ถูกไหมล่ะ?

7. สิทธิของเจ้าของข้อมูล

ลองนึกภาพว่าคุณเป็นซูเปอร์ฮีโร่ในโลกดิจิทัล! คุณมีชุดเกราะวิเศษที่ประกอบด้วยอาวุธหลากหลายชนิด แต่ละชิ้นคือสิทธิที่ช่วยปกป้องคุ้มครองข้อมูลส่วนตัวของคุณ! มีทั้งโล่แห่งการเข้าถึงที่ช่วยให้คุณรู้ว่าใครเก็บข้อมูลอะไรของคุณไว้บ้าง ดาบแห่งการแก้ไขที่ช่วยให้คุณปรับปรุงข้อมูลให้ถูกต้อง เวทมนตร์แห่งการลบที่ช่วยให้คุณลบข้อมูลที่ไม่ต้องการออกไป หรือกระเป๋าวิเศษแห่งการโอนย้ายที่ช่วยคุณย้ายข้อมูลไปไหนก็ได้ แถมยังมีพลังพิเศษอื่น ๆ อีกมากมาย!

ด้วยอาวุธเหล่านี้ จะทำให้คุณผจญภัยในโลกดิจิทัลอย่างมั่นใจ ปกป้องตัวตนของคุณจากภัยคุกคามต่างๆ และควบคุมการใช้ข้อมูลของคุณได้อย่างเต็มที่! มาดูกันดีกว่าว่าอาวุธแต่ละชิ้นมีพลังวิเศษอะไรบ้าง!

สิทธิที่จะได้รับแจ้ง: เคยรู้สึกเหมือนถูกแอบดูไหม? ไม่ต้องกังวลอีกต่อไป! สิทธินี้เหมือนไฟฉายที่ใช้ส่องทะลุความมืด ช่วยเปิดเผยทุกซอกทุกมุมของการจัดการข้อมูลของคุณ ลองนึกภาพว่าคุณกำลังเปิดตู้เสื้อผ้าขนาดยักษ์ที่ทุกลิ้นชักเต็มไปด้วยข้อมูลที่ต้องเปิดเผย – คำถามก็คือใครเป็นคนเก็บ แล้วจะเอาไปทำอะไร เก็บไว้นานแค่ไหน เอาไปแบ่งปันให้ใครบ้าง แม้แต่วิธีร้องเรียนก็ต้องบอก! เหมือนกับการได้แผนที่ขุมทรัพย์ข้อมูลของตัวคุณเอง ไม่มีอะไรต้องซ่อน ไม่มีอะไรต้องกลัว คุณจะรู้ทุกอย่างเกี่ยวกับข้อมูลของตัวคุณเอง

สิทธิที่จะเข้าถึงข้อมูล: ลองนึกภาพว่าคุณมีกุญแจวิเศษที่สามารถเปิดประตูทุกบานที่เก็บข้อมูลของคุณได้ เมื่ออยากรู้ว่าในห้องไหนเก็บอะไรไว้ก็สามารถเปิดดูได้เลย เมื่ออยากรู้ว่าใครเข้ามาในห้องบ้างก็ตรวจสอบได้ทันที สงสัยว่าจะเก็บของไว้ในห้องนานแค่ไหน ก็สามารถถามได้หมด นี่คือสิทธิที่ทำให้คุณเป็นเจ้าของข้อมูลอย่างแท้จริง คุณจะได้รู้ทุกอย่าง ตั้งแต่ว่าเขาเก็บอะไรของคุณไว้บ้าง เอาไปใช้ทำอะไร ใครได้เห็นบ้าง จะเก็บไว้นานแค่ไหน แถมยังรู้ด้วยว่าคุณมีสิทธิอะไรอีกบ้าง เช่น จะแก้ไขหรือลบได้ไหม เรียกว่าเป็นเจ้าของปราสาทแห่งข้อมูลที่รู้ทุกตารางนิ้ว

สิทธิที่จะถูกลืม: คุณเคยอายเรื่องในอดีตจนอยากให้โลกลืมไหม? สิทธินี้เหมือนยางลบวิเศษที่ลบรอยดินสอดิจิทัลของคุณได้ ให้ลองนึกภาพว่าอินเทอร์เน็ตเป็นเหมือนกระดานดำขนาดยักษ์ที่มีข้อมูลของคุณถูกขีดเขียนเต็มไปหมด สิทธินี้จะช่วยให้คุณสามารถขอลบข้อมูลที่คุณไม่อยากให้ใครเห็นออกไปได้ เช่น การขอให้ Google ลบลิงก์ที่โผล่มาเวลาใครค้นชื่อคุณ หรือขอลบโพสต์เก่า ๆ ที่คุณไม่อยากให้ใครเห็นอีก ในอินโดนีเซียถึงขนาดว่ามีกฎหมายที่อนุญาตให้คุณขอคำสั่งศาลเพื่อลบข้อมูลที่ทำลายชื่อเสียงคุณได้เลย อย่างไรก็ดี อย่าลืมว่าถ้าข้อมูลนั้นยังมีประโยชน์ต่อสาธารณะก็อาจจะลบไม่ได้

ที่ผ่านมา สิทธิที่จะถูกลืมต้องถูกท้าทายจากหลายประเทศทั่วโลก เพราะศาลในหลายประเทศมักไม่ค่อยเห็นด้วยกับการบังคับใช้สิทธินี้กับเครื่องมือค้นหา ยกตัวอย่างเช่นกรณีของญี่ปุ่น ที่บอก Google ว่าจะลบได้ก็ต่อเมื่อความเป็นส่วนตัวสำคัญกว่าการเปิดเผยข้อมูลมาก ๆ เท่านั้น ขณะที่บราซิลก็ไม่ยอมให้ลบผลการค้นหาตามใจชอบเช่นกัน ส่วนกรณีของประเทศจีน เคยมีคนขอลบประวัติการทำงาน แต่ศาลก็ปฏิเสธได้บอกว่าไม่ได้! เพราะนี่มันข้อมูลสำคัญ

เห็นไหมล่ะ? แม้แต่ในประเทศที่ต่างกัน ศาลก็มองคล้าย ๆ กัน ไม่ใช่ว่าอยากลบอะไรก็ลบได้ เพราะต้องชั่งน้ำหนักระหว่างความเป็นส่วนตัวกับประโยชน์สาธารณะก่อน แม้หลักคิดของสิทธิที่จะถูกลืมอาจฟังดูดี แต่ในโลกแห่งความจริงกลับไม่สามารถบังคับได้ง่ายเช่นนั้น

ตามหลักการสากล สิทธิที่จะถูกลืมจำกัดเพียงการขอให้เครื่องมือค้นหาลบลิงก์ที่ไม่ถูกต้องหรือล้าสมัยออกจากผลการค้นชื่อบุคคล โดยจำกัดเฉพาะระดับชื่อโดเมน การร้องขอต้องผ่านการพิจารณาจากศาลหรือองค์กรอิสระที่เชี่ยวชาญเข้าใจเรื่องเสรีภาพการแสดงออกและกฎหมายคุ้มครองข้อมูล ต้องพิจารณาชั่งน้ำหนักระหว่างสิทธิส่วนบุคคลกับประโยชน์สาธารณะ อย่างไรก็ตาม มีบางกรณีที่ข้อมูลสำคัญทางประวัติศาสตร์และยังมีคุณค่าต่อสาธารณะถูกลบออกไปภายใต้สิทธินี้ ซึ่งสะท้อนให้เห็นถึงความท้าทายในการรักษาสมดุลระหว่างการปกป้องคุ้มครองความเป็นส่วนตัวของบุคคลและการรักษาไว้ซึ่งข้อมูลที่มีคุณค่าต่อสังคม

สิทธิในการแก้ไข: นึกภาพว่าคุณมีปากกาวิเศษที่สามารถลบและเขียนข้อมูลในสมุดประวัติของคุณได้ หากเจอประวัติผิด ก็ลบทิ้งได้ อยากเพิ่มเติมข้อมูลให้สมบูรณ์ ก็เขียนได้เลย นี่คือสิทธิที่ทำให้คุณเป็นนักเขียนประวัติตัวเองอย่างแท้จริง คุณสามารถขอแก้ไขข้อมูลที่ไม่ถูกต้องหรือเติมเต็มส่วนที่ขาดหายได้ด้วยตัวคุณเอง แถมองค์กรที่เก็บข้อมูลยังต้องทำตามคำขอของคุณด้วยนะ! นี่คือสิทธิของคุณที่จะทำให้ประวัติในโลกดิจิทัลตรงกับความเป็นตัวคุณที่สุด

สิทธิในการโอนย้ายข้อมูล: นึกภาพว่าคุณมีกระเป๋าวิเศษที่บรรจุข้อมูลส่วนตัวของคุณทั้งหมดเอาไว้ เมื่อไรที่ต้องการย้ายข้อมูลดิจิทัลของคุณก็ทำได้ง่าย ๆ เพียงแค่คว้ากระเป๋าใบนี้แล้วเดินไปที่ใหม่ ข้อมูลทุกต่าง ๆ ที่คุณเคยให้ไว้ ไม่ว่าจะเป็นประวัติการค้นหา ตำแหน่งที่คุณเคยไป หรือแม้แต่ประวัติการเข้าชมเว็บไซต์สามารถย้ายไปไว้ที่อื่นได้แบบง่าย ๆ อย่างไรก็ดี ไม่ได้หมายความว่าทุกอย่างจะย้ายได้หมด โดยจำกัดแต่เฉพาะข้อมูลที่คุณให้ไว้ด้วยความเต็มใจหรือตามสัญญาเท่านั้น และต้องเป็นข้อมูลที่ถูกประมวลผลด้วยวิธีอัตโนมัติด้วย

สิทธิในการคัดค้านการประมวลผลข้อมูล: ให้ลองนึกภาพว่าคุณมีโล่วิเศษที่สามารถป้องกันไม่ให้ใครมายุ่งกับข้อมูลของคุณได้ คุณสามารถยกโล่ขึ้นมาพร้อมพูดว่า “หยุด!” กับการใช้ข้อมูลของคุณเมื่อไหร่ก็ได้ และจะใช้เพื่อป้องกันข้อมูลทั้งหมดหรือเลือกป้องกันเฉพาะบางส่วนก็ได้ แถมยังสามารถเลือกว่าจะป้องกันการใช้ข้อมูลเพื่อวัตถุประสงค์ไหนบ้าง เช่น ไม่ให้ใช้เพื่อการตลาด แต่ยอมให้ใช้เพื่อการวิจัยได้

แต่ก็ต้องระวัง เพราะในบางประเทศโล่ดังกล่าวก็ไม่อาจป้องกันการใช้ข้อมูลบางอย่างได้ เช่น ข้อมูลที่ใช้เพื่อการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ และที่เจ๋งสุดๆ คือ ถ้าเป็นเรื่องการตลาดทางตรง โล่จะแข็งแกร่งเป็นพิเศษ! ในอดีต อาจต้องคอยชูโล่ตลอดเวลา (opt-out) แต่ตอนนี้หลายประเทศในเอเชีย เช่น ฮ่องกงและเกาหลีใต้ สามารถเก็บโล่ไว้จนกว่าจะอนุญาต (opt-in) ให้ใครใช้ข้อมูล ถ้าใครฝ่าฝืน จะโดนปรับเงินก้อนโตเลยล่ะ!

สิทธิที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติและการทำโปรไฟล์: นึกภาพว่าคุณมีเวทมนตร์ป้องกันไม่ให้คอมพิวเตอร์ตัดสินชะตาชีวิตของคุณ แม้ว่าคอมพิวเตอร์จะพยายามวิเคราะห์ทุกอย่างเกี่ยวกับคุณ ไม่ว่าจะเป็นประสิทธิภาพในการทำงาน สถานะทางการเงิน สุขภาพ ความชอบส่วนตัว งานอดิเรก ความน่าเชื่อถือ พฤติกรรม หรือแม้แต่ตำแหน่งที่อยู่ของคุณ แต่ด้วยเวทมนตร์นี้ คุณสามารถป้องกันไม่ให้มันทำการตัดสินใจสำคัญ ๆ ที่ส่งผลกระทบอย่างมีนัยสำคัญต่อชีวิตคุณโดยอัตโนมัติได้

อย่างไรก็ตาม เวทมนตร์นี้อาจไม่ทำงานในบางสถานการณ์ เช่น เมื่อจำเป็นสำหรับการปฏิบัติตามสัญญา หรือกฎหมายอนุญาตให้ทำ หรือเมื่อเราให้การยินยอมโดยชัดแจ้ง แต่โดยทั่วไปเรามีสิทธิที่จะบอกว่า “ไม่!” ถ้าเราไม่ต้องการให้คอมพิวเตอร์ตัดสินใจแทนเราทุกเรื่อง ถูกไหมล่ะ?

สิทธิในการขอถอนความยินยอม: คิดดูสิ คุณมีปุ่มวิเศษที่สามารถถอนความยินยอมในการประมวลผลข้อมูลของคุณได้ตลอดเวลา เหมือนกับการกดปุ่ม “ยกเลิก” ในเกมที่คุณไม่อยากเล่นต่อแล้ว และการกดปุ่มนี้ควรจะง่ายพอ ๆ กับตอนที่คุณกดปุ่ม “ตกลง” โดยเฉพาะในโลกออนไลน์ ถ้าพวกเขาขอความยินยอมจากคุณทางอิเล็กทรอนิกส์ การถอนความยินยอมก็ควรทำได้ง่ายในลักษณะเดียวกัน และที่สำคัญ กระบวนการให้ความยินยอมจะต้องไม่รบกวนการใช้บริการของคุณโดยไม่จำเป็น พวกเขาต้องใช้วิธีที่เป็นมิตรกับผู้ใช้มากที่สุด อย่างในเวียดนาม กฎหมายกำหนดให้การให้ความยินยอมต้องเป็นไปโดยสมัครใจ โดยธุรกิจต้องแจ้งขอบเขตและวัตถุประสงค์การใช้ข้อมูลก่อนขอความยินยอม แม้ไม่มีรูปแบบเฉพาะสำหรับการอนุญาตประมวลผลข้อมูลส่วนบุคคล แต่ก็มีกฎเข้มงวดขึ้นสำหรับพาณิชย์อิเล็กทรอนิกส์และการสื่อสารการตลาด นี่แหละคือพลังที่ทำให้คุณควบคุมข้อมูลของตัวเองได้ตลอดเวลา!

สิทธิในการขอความช่วยเหลือและการเยียวยา: นึกภาพทีมซูเปอร์ฮีโร่ปกป้องข้อมูลของคุณ! เมื่อมีคนละเมิดสิทธิข้อมูลของคุณ คุณมีพลังเรียกทีมฮีโร่สุดเจ๋งนี้มาช่วยได้เลย:

1. กรรมาธิการด้านความเป็นส่วนตัว: ซูเปอร์ฮีโร่รับเรื่องร้องเรียนและสอบสวน

2. ศาล: ผู้พิพากษาผู้ทรงพลัง สั่งให้ผู้ละเมิดชดใช้ค่าเสียหายได้

3. หน่วยงานคุ้มครองข้อมูลส่วนบุคคล (DPA): ทีมนักสืบมืออาชีพมีอำนาจตรวจสอบและลงโทษผู้กระทำผิด

กฎหมายรับรองว่าคุณมีสิทธิได้รับการเยียวยาที่มีประสิทธิภาพจากผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล หากพวกเขาละเมิดสิทธิของคุณ และถ้า DPA ไม่จัดการข้อร้องเรียนของคุณ คุณยังมีสิทธิดำเนินการทางกฎหมายกับพวกเขาได้อีกด้วย แต่ถ้าทีมซูเปอร์ฮีโร่เหล่านี้ไม่ทำงาน หรือคุณรู้สึกว่าการต่อสู้นี้ใหญ่เกินกำลัง คุณยังมีพลังพิเศษอีกอย่าง สามารถรวมพลังกับคนอื่น ๆ ที่ถูกละเมิดเหมือนกัน หรือแม้แต่ขอให้ NGO ที่เชี่ยวชาญมาช่วยสู้แทนคุณได้

การเยียวยาแบบกลุ่มนี้เหมือนกับการรวมพลังของอเวนเจอร์สเลยใช่ไหมล่ะ ? มันเป็นเครื่องมือสำคัญในการต่อสู้กับผู้ละเมิดความเป็นส่วนตัว โดยเฉพาะเมื่อการดำเนินคดีอาจมีค่าใช้จ่ายสูงและซับซ้อนเกินไปสำหรับคน ๆ เดียว นี่แหละคือพลังที่ทำให้คุณมั่นใจได้ว่า ไม่ว่าใครจะมาละเมิดสิทธิข้อมูลของคุณ คุณก็มีทีมซูเปอร์ฮีโร่และพลังพิเศษที่จะปกป้องตัวเองได้เสมอ

8. ตัวละครสำคัญอีกหลายตัวในโลกข้อมูลดิจิทัล

คุณเคยสงสัยไหมว่า มีใครอีกบ้างที่เกี่ยวข้องในโลกข้อมูลดิจิทัล ในเรื่องนี้มีตัวละครสำคัญอีกหลายตัวที่คุณควรรู้จัก

ผู้ควบคุมข้อมูล เปรียบเสมือนผู้กำกับภาพยนตร์ข้อมูลของคุณ เขาตัดสินใจว่าจะเก็บข้อมูลอะไร เก็บไว้ทำไม และจะจัดการอย่างไร ไม่ว่าข้อมูลจะมาจากตัวคุณโดยตรงหรือจากที่อื่น เขาเป็นผู้รับผิดชอบสูงสุดในการดูแลความปลอดภัย ควบคุมการเข้าถึง และการแปลงข้อมูล บางทีคุณอาจได้ยินเขาถูกเรียกว่า “เจ้าของข้อมูล” แต่อย่าสับสนล่ะ คุณต่างหากที่เป็นเจ้าของข้อมูลตัวจริง!

ผู้ประมวลผลข้อมูล เปรียบเสมือนทีมงานเบื้องหลังที่ทำตามคำสั่งผู้กำกับ พวกเขาจัดการข้อมูลตามที่ผู้ควบคุมบอก อาจเป็นคนในบริษัทเดียวกันหรือเป็นบริษัทอื่นก็ได้ พวกเขาไม่ได้เป็นเจ้าของข้อมูล แต่มีสิทธิเข้าถึงเพื่อทำงานตามที่ได้รับมอบหมาย เช่น บริษัทที่รับจ้างวิเคราะห์ข้อมูลลูกค้าให้กับร้านค้าออนไลน์ บางครั้ง บริษัทเดียวอาจเล่นทั้งสองบทบาท เหมือนผู้กำกับที่ลงมาเล่นเองด้วย! แต่ไม่ว่าจะเป็นอย่างไร พวกเขาต้องทำตามกฎหมายและสัญญาที่ตกลงกันไว้อย่างเคร่งครัด เพื่อให้แน่ใจว่าข้อมูลของคุณจะปลอดภัย

ความแตกต่างระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

Artsy เป็นผู้ควบคุมข้อมูลที่เก็บรวบรวมข้อมูลการเข้าชมเว็บไซต์ของผู้ใช้ ซึ่งประกอบด้วยหน้าที่ผู้ใช้เข้าชม ลำดับการดูหน้าต่างๆ และระยะเวลาที่ใช้ในแต่ละหน้า Artsy กำหนดวัตถุประสงค์และวิธีการใช้ข้อมูลนี้ โดยใช้บริการ Google Analytics เป็นผู้ประมวลผลข้อมูลเพื่อวิเคราะห์ความนิยมของหน้าเว็บต่างๆ และพฤติกรรมการใช้งานของผู้เยี่ยมชม

ข้อมูลที่ได้จากการวิเคราะห์ช่วยให้ Artsy สามารถปรับปรุงการออกแบบเนื้อหาเว็บไซต์ ระบุหัวข้อที่ได้รับความสนใจ ค้นพบหัวข้อใหม่ๆ ที่อาจดึงดูดลูกค้า และพัฒนาเนื้อหาที่มีอยู่ให้ตรงกับความต้องการของผู้ใช้มากขึ้น การใช้ Google Analytics ในลักษณะนี้ ทำให้ Artsy สามารถปรับปรุงประสบการณ์การใช้งานเว็บไซต์และเนื้อหาให้ตอบสนองความต้องการของผู้ใช้ได้ดียิ่งขึ้น

ที่มา: https://digitalguardian.com/blog/data-controller-vs-data-processor-whats-difference

หน่วยงานคุ้มครองข้อมูล เคยสงสัยไหมว่าใครคอยดูแลและกำกับให้คนที่เล่นกับข้อมูลของคุณต้องทำตามกฎ นั่นแหละ! หน่วยงานคุ้มครองข้อมูลทีมซูเปอร์ฮีโร่ที่คอยปกป้องความลับของคุณนั่นเอง

นึกภาพว่าพวกเขาเป็นตำรวจข้อมูล คอยตรวจตราให้ทุกคนเล่นตามกติกา อาจเป็นหน่วยงานรัฐ หรือทีมฮีโร่หลายคนรวมกัน แต่ไม่ว่าจะเป็นใคร พวกเขาต้องทำงานอย่างอิสระ ไม่มีใครมาสั่งได้ ดังนั้น หากรู้สึกว่าใครมาแอบเก็บข้อมูล หรือใช้ประโยชน์จากข้อมูลของคุณโดยไม่ชอบ คุณก็สามารถบอกพวกเขาได้เลย ง่ายกว่าไปฟ้องศาลตั้งเยอะแถมถ้าจับได้ว่ามีคนทำผิดจริง พวกเขามีพลังสั่งให้แก้ไข ลบ หรือทำลายข้อมูลที่ไม่ถูกต้องได้ด้วย

เห็นไหมว่าคุณไม่ได้อยู่คนเดียวในโลกข้อมูลนี้ ยังมีซูเปอร์ฮีโร่ที่คอยช่วยคุณอยู่ ดังนั้น ถ้าใครมาเล่นงานข้อมูลของคุณ อย่าลืมเรียกพวกเขามาช่วยล่ะ!

9. กฎหมายจัดการข้อมูลข้ามแดน: 6 ระดับจากเสรีถึงเข้มงวด

OECD แบ่งระบบการคุ้มครองข้อมูลของประเทศต่าง ๆ ไว้ 6 แบบ โดยเรียงลำดับจากเบาไปหาหนัก

1. แบบไร้กฎ (หมวดหมู่ 0): ไม่มีกฎอะไรเลย ข้อมูลไหลไปไหนก็ได้ แต่ระวังนะ ประเทศอื่นอาจไม่อยากส่งข้อมูลมาให้!

2. แบบไหลเสรี (หมวดหมู่ 1): ไม่ห้ามส่งข้อมูลข้ามประเทศ แต่ถ้าใครเอาข้อมูลไปใช้ผิดๆ คนส่งต้องรับผิดชอบ

3-4. แบบมีเงื่อนไข (หมวดหมู่ 2, 3, 4): ต้องแน่ใจก่อนว่าประเทศที่จะส่งข้อมูลไปมีการป้องกันข้อมูลดีพอ ถ้าไม่ดีพอก็ต้องทำอะไรเพิ่มก่อนส่ง ยิ่งเลขมาก ยิ่งเข้มงวด! แต่ละแบบต่างกันที่วิธีประเมินความเพียงพอและใครเป็นคนประเมิน

5. แบบมีเงื่อนไขพิเศษ (หมวดหมู่ 5): ต้องให้หน่วยงานรัฐประเมินก่อนว่าประเทศปลายทางปลอดภัยพอ ถ้าไม่ผ่าน ต้องขออนุญาตเป็นกรณีพิเศษ

6. แบบเข้มสุด (หมวดหมู่ 6): ทุกครั้งที่จะส่งข้อมูลต้องให้เจ้าหน้าที่ตรวจก่อน ไม่มีข้อยกเว้นแต่ละแบบมีข้อดีข้อเสียต่างกัน บางแบบทำให้ส่งข้อมูลง่าย แต่อาจไม่ปลอดภัย บางแบบปลอดภัยมาก แต่อาจทำให้ธุรกิจทำงานยาก แล้วคุณคิดว่าแบบไหนเหมาะกับประเทศเราที่สุด? ต้องคิดให้ดีนะ เพราะมันเกี่ยวกับความเป็นส่วนตัวของเราทุกคนเลยล่ะ! แถมยังส่งผลต่อการทำธุรกิจระหว่างประเทศด้วย!

10. ความเป็นส่วนตัวในยุคของเทคโนโลยีเกิดใหม่

โลกดิจิทัลกำลังท้าทายความเป็นส่วนตัวของเราอย่างที่ไม่เคยมีมาก่อน ปัญญาประดิษฐ์ (AI) อินเทอร์เน็ตของสรรพสิ่ง (IoT) และนายหน้าข้อมูลกำลังรวบรวมและประมวลผลข้อมูลของเราในปริมาณมหาศาล ทุกครั้งที่เราใช้ ไม่มีวันหายไป AI ติดตามพฤติกรรมออนไลน์ของเรา สร้างโปรไฟล์ และใช้มันเพื่อโฆษณาแบบเจาะจง ทำให้เรารู้สึกเหมือนถูกสอดส่องตลอดเวลา

แต่ไม่ใช่แค่ความเป็นส่วนตัวเท่านั้นที่ถูกคุกคาม การละเมิดนี้ส่งผลกระทบต่อสิทธิอื่น ๆ ด้วย ทั้งเสรีภาพในการแสดงออกและการรวมกลุ่ม อัลกอริทึมของสื่อสังคมและเครื่องมือค้นหากำลังควบคุมสิ่งที่เราเห็นในโลกออนไลน์ ทั้งยังจำกัดมุมมองและความหลากหลายของข้อมูลที่เราเข้าถึง และแน่นอนว่านี่ไม่ใช่แค่เรื่องความสะดวกสบาย แต่เป็นเรื่องของอำนาจและการควบคุม

ความเป็นส่วนตัวไม่ใช่แค่ความสบายใจ แต่เป็นสิทธิขั้นพื้นฐานที่จำเป็นต่อศักดิ์ศรีความเป็นมนุษย์ เราต้องเรียกร้องให้มีกฎหมายและมาตรการที่เข้มแข็งในการคุ้มครองข้อมูลของเรา ไม่ใช่แค่ในประเทศเดียว แต่หมายถึงการคุ้มครองในระดับทั่วทุกมุมโลก เพราะในโลกดิจิทัลนั้นข้อมูลของเราไม่มีพรมแดน ถึงเวลาแล้วที่เราต้องยืนหยัดเพื่อสิทธิความเป็นส่วนตัวในข้อมูลของเรา ก่อนที่มันจะสายเกินไป

การทำให้ข้อมูลเป็นนิรนาม ไม่เท่ากับการปกป้องความเป็นส่วนตัว

ปกติแล้ว ความเป็นส่วนตัวของข้อมูลมักจะได้รับการปกป้องผ่านการทำให้ข้อมูลเป็นนิรนาม โดยการลบข้อมูลที่สามารถระบุตัวตนได้ เช่น ชื่อ เบอร์โทรศัพท์ และอีเมล ข้อมูลจะถูกปรับเปลี่ยนให้มีความแม่นยำน้อยลง และมีการเพิ่ม “สัญญาณรบกวน” เข้าไปในข้อมูล อย่างไรก็ตาม ผลการศึกษาจาก Nature Communications แสดงให้เห็นว่า การทำให้ข้อมูลเป็นนิรนามนั้นไม่ได้หมายถึงความเป็นส่วนตัวเสมอไป นักวิจัยได้พัฒนาแบบจำลอง Machine Learning ที่สามารถประมาณการว่า บุคคลสามารถถูกระบุตัวตนใหม่ได้อย่างไรจากชุดข้อมูลที่ถูกทำให้เป็นนิรนาม เพียงแค่ใส่รหัสไปรษณีย์ เพศ และวันเกิด

ที่มา: https://www.nature.com/articles/s41467-019-10933-3

AI นักสืบดิจิทัลที่รู้จักคุณดีกว่าตัวคุณเอง

คุณคิดว่ารู้จักตัวเองดีแค่ไหน? AI อาจรู้จักคุณดีกว่าที่คุณคิด! มันไม่ใช่แค่เครื่องมือธรรมดา แต่เป็นนักสืบดิจิทัลที่แสนฉลาด สามารถขุดคุ้ยชีวิตส่วนตัวของคุณได้ลึกซึ้งกว่าที่คุณคาดคิด มันรู้ว่าคุณชอบไปวัดไหน ดูทีวีรายการอะไร แม้กระทั่งรู้ว่าคุณนอนกี่โมง! มันสามารถจับกลุ่มคนตามความคิดทางการเมือง หรือแม้แต่คาดเดาสุขภาพกายและใจของคุณได้ มันไม่ได้แค่เก็บข้อมูลที่คุณให้ แต่สร้างข้อมูลใหม่เกี่ยวกับคุณ โดยเอาข้อมูลเล็กๆ น้อยๆ มาปะติดปะต่อจนได้ภาพใหญ่ของชีวิตคุณ ที่น่าตกใจคือ ข้อมูลสองส่วนที่ดูไม่เกี่ยวข้องกัน อาจ “ผสมพันธุ์” (breed) กัน และสร้างข้อมูลใหม่โดยที่คุณไม่รู้ตัว!

แต่นี่ไม่ใช่แค่เรื่องน่าตื่นเต้น มันน่ากลัวด้วย! การคาดเดาของ AI อาจกลายเป็นตัวตัดสินชะตาชีวิตของคุณและคนรอบตัวคุณด้วย เช่น การวิเคราะห์ DNA ของคุณอาจเปิดเผยความลับทางสุขภาพของทั้งครอบครัว!

AI กำลังเปลี่ยนการสอดส่องให้กลายเป็นภัยคุกคามร้ายแรงต่อเสรีภาพของเรา! ด้วยกล้องวงจรปิดและระบบจดจำใบหน้าที่แพร่หลาย รัฐบาลสามารถติดตามเราได้ 24/7 โดยไม่จำเป็นและไม่สมเหตุสมผล

ในสหรัฐฯ ผู้ใหญ่ครึ่งประเทศอยู่ในฐานข้อมูลจดจำใบหน้าของตำรวจแล้ว! นี่ไม่ใช่แค่เรื่องความเป็นส่วนตัว แต่คุกคามสิทธิขั้นพื้นฐานของเรา ทำให้เราไม่กล้าใช้เสรีภาพในการชุมนุม และอาจทำให้กลุ่มคนชายขอบถูกเล็งเป็นพิเศษ เราต้องลุกขึ้นมาเรียกร้องการควบคุมการใช้ AI ในการสอดส่อง ต้องการความโปร่งใสในการจัดเก็บข้อมูล และกฎหมายที่เข้มงวดในการคุ้มครองความเป็นส่วนตัว ก่อนที่เราจะพบว่าตัวเองกำลังอาศัยอยู่ในโลกที่ถูกจับตามองตลอดเวลาโดยไม่รู้ตัว! จำไว้ ความปลอดภัยไม่ควรแลกมาด้วยเสรีภาพ เราต้องหาจุดสมดุลก่อนที่จะสายเกินไป!

กิจกรรม: AI และสิทธิความเป็นส่วนตัว

ดูวิดีโอและหารือเกี่ยวกับผลกระทบที่เป็นไปได้ของ AI เกี่ยวกับสิทธิความเป็นส่วนตัว และพยายามตอบคำถามต่อไปนี้: อะไรคือผลกระทบต่อความเป็นส่วนตัวของเทคโนโลยีเกิดใหม่ เช่น อินเทอร์เน็ตของสรรพสิ่ง (IoT) และปัญญาประดิษฐ์ (AI) จะมีวิธีจัดการเชิงรุกอย่างไร (แทนที่จะเพียงตอบสนองต่อผลกระทบที่เกิดขึ้น) เทคโนโลยีเกิดใหม่เปลี่ยนแปลงไปอย่างไร แนวคิดเรื่องความเป็นส่วนตัวทางดิจิทัล (ถ้ามี)?

ที่มา: UNESCO
https://youtu.be/WGHPsquQmVo?list=PLPA_JE570-MHqtgHwYgJaMWcW_cq4ArPl

11. คำถามท้ายตอน

1) 4 Ps ของความเป็นส่วนตัวคือ:

a. สถานที่ วัตถุประสงค์ แพลตฟอร์ม ผู้คน

b. การคุ้มครอง วัตถุประสงค์ แพลตฟอร์ม และผู้คน

c. ราคา การป้องกัน ผู้คน แพลตฟอร์ม

d. ไม่มีข้อใดถูก

2) ความเป็นส่วนตัวในการสื่อสาร หมายถึง การปกป้องตัวตนทางกายภาพของผู้คนจากกระบวนการรุกราน เช่น การทดสอบทางพันธุกรรมและยา การตรวจค้นร่างกายอย่างละเอียด ผ่านช่องเปิดต่าง ๆ ของร่างกาย (Cavity Searches) การคุมกำเนิด การทำแท้ง และการรับเลี้ยงบุตรบุญธรรม

☐ จริง

☐ เท็จ

3) ความเป็นส่วนตัวของเครือข่ายเหมือนกับความเป็นส่วนตัวของข้อมูล

☐ จริง

☐ เท็จ

4) Datafication หมายถึง การแพร่กระจายของเครื่องมือที่ได้รับการปรับปรุงสำหรับการบูรณาการ การวิเคราะห์ และการแสดงรูปแบบข้อมูลเพื่อเป้าหมายของการตัดสินใจและการค้า

☐ จริง

☐ เท็จ

5) โปรดระบุหลักการคุ้มครองข้อมูลที่สำคัญ

6) โปรดระบุสิทธิของเจ้าของข้อมูล

ตอนที่ 2 เจาะลึกกฎหมายความเป็นส่วนตัวทั่วโลก

เคยสงสัยไหมว่าทำไมเว็บไซต์ทุกแห่งถึงมีป๊อปอัพให้ยอมรับคุกกี้ หรือทำไมบริษัทใหญ่ ๆ ถึงต้องจ่ายค่าปรับมหาศาลเมื่อเกิดการรั่วไหลข้อมูลลูกค้า นี่แหละคือโลกของกฎหมายความเป็นส่วนตัวที่ซับซ้อนแต่น่าสนใจ

เนื้อหาตอนนี้ เราจะพาคุณท่องโลกกว้างของกฎหมายและนโยบายความเป็นส่วนตัว ตั้งแต่ระดับโลกไปจนถึงกฎหมายในบ้านเรา เรียนรู้ว่าทำไม GDPR ถึงทำให้บริษัทเทคฯ ทั่วโลกต้องปวดหัว และทำไมสิงคโปร์ถึงได้ชื่อว่าเป็น “ศูนย์กลางข้อมูล” ของเอเชีย

สิ่งที่จะได้เรียนรู้:

1. รู้จักกฎหมายระดับโลก: เจาะลึก GDPR ที่ทำให้โลกต้องตื่นตัวเรื่องความเป็นส่วนตัว

2. สำรวจกฎหมายในภูมิภาค: ดูว่าเพื่อนบ้านในเอเชียตะวันออกเฉียงใต้เขาทำกันยังไง

3. เปรียบเทียบกฎหมายทั่วโลก: ดูความเหมือนและต่างของกฎหมายในสิงคโปร์ อังกฤษ และอเมริกา

4. รู้จักองค์กรสำคัญ: ทำความรู้จักกับ “ซูเปอร์ฮีโร่” ที่ปกป้องข้อมูลของเราในระดับสากล

พิเศษสุด! เรียนรู้ผ่านกรณีศึกษาสุดฮือฮาที่อาจทำให้คุณอึ้ง ร่วมสนุกกับกิจกรรมที่จะทำให้กฎหมายกลายเป็นเรื่องสนุก และชมวิดีโอที่จะทำให้คุณเข้าใจกฎหมายได้ง่ายขึ้นกว่าที่คิด!

เนื้อหาในคู่มือฉบับนี้ แปลมาจากเอกสารต้นฉบับของ The American Bar Association โดยผู้ที่สนใจสามารถศึกษารายละเอียดเพิ่มเติมได้ที่ https://www.americanbar.org/advocacy/global-programs/what-we-do/programs/defending-data-privacy-southeast-asia/

1. หลักการสากลและกรอบกติกาใหม่ในยุคดิจิทัล

ลองนึกภาพคุณกำลังคุยโทรศัพท์กับเพื่อนสนิท แล้วจู่ ๆ มีคนแปลกหน้ามาแอบฟัง คงจะรู้สึกอึดอัดใช่ไหมล่ะ? นั่นแหละ คือความสำคัญของ “ความเป็นส่วนตัว” ความเป็นส่วนตัวไม่ใช่แค่เรื่องของคุณหรือผม แต่เป็นเรื่องของทุกคนบนโลกใบนี้ ถึงขนาดที่องค์การสหประชาชาติต้องบรรจุเรื่องนี้ไว้ในเอกสารสำคัญระดับโลกถึงสองฉบับด้วยกัน

ฉบับแรก คือ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน หรือ UDHR ในข้อที่ 12 ระบุไว้ชัดเจนว่า:

> *“บุคคลใดจะถูกแทรกแซงความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสารโดยพลการไม่ได้ และจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น”*

ข้อความข้างต้นคือการประกาศอย่างชัดเจนว่าความเป็นส่วนตัวเป็นสิทธิขั้นพื้นฐานที่ทุกคนพึงมี

อีกฉบับหนึ่ง คือ **กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง** หรือ ICCPR ในข้อที่ 17 ซึ่งย้ำความสำคัญของความเป็นส่วนตัวอีกครั้ง โดยระบุว่า: 1) บุคคลจะถูกแทรกแซงความเป็นส่วนตัว ครอบครัว เคหสถาน หรือการติดต่อสื่อสารโดยพลการหรือไม่ชอบด้วยกฎหมายมิได้ และจะถูกลบหลู่เกียรติและชื่อเสียงโดยไม่ชอบด้วยกฎหมายมิได้ 2) บุคคลทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายมิให้ถูกแทรกแซงหรือลบหลู่เช่นว่านั้น

ทั้งสองเอกสารนี้เป็นเหมือน **“ธรรมนูญโลก”** ที่บอกว่าทุกคนมีสิทธิที่จะมีความเป็นส่วนตัว ไม่ว่าคุณจะอยู่ที่ไหนบนโลก ยังไงก็ควรได้รับการปกป้องความเป็นส่วนตัว

Q: แล้วทำไมความเป็นส่วนตัวถึงสำคัญนักหนา?

A: ให้ลองคิดดูว่า หากคุณไม่มีความเป็นส่วนตัวเลย ทุกอย่างที่ทำ ทุกคำพูด หรือแม้แต่ความคิดของคุณล้วนถูกสอดส่อง คุณจะกล้าแสดงความคิดเห็นหรือไม่ จะกล้าวิพากษ์วิจารณ์อะไรไหม นี่แหละที่ความเป็นส่วนตัวช่วยรักษาสมดุลระหว่างอำนาจรัฐกับสิทธิของประชาชน

ในยุคดิจิทัลแบบนี้ ความเป็นส่วนตัวยิ่งมีค่ามากขึ้นไปอีก ลองนึกดูทุกครั้งที่คุณท่องโลกโซเชียลมีเดีย ช้อปปิ้งออนไลน์ หรือแม้แต่เปิดแอปฯ ในมือถือ คุณกำลังทิ้งร่องรอยดิจิทัลเอาไว้ ถ้าไม่มีการคุ้มครองความเป็นส่วนตัว ข้อมูลพวกนี้อาจถูกนำไปใช้ในทางที่ไม่ถูกต้องได้

ประเทศในแถบเอเชียตะวันออกเฉียงใต้ก็ตระหนักถึงความสำคัญนี้ หลายประเทศได้ลงนามใน UDHR และสนธิสัญญาอื่น ๆ ที่เกี่ยวข้อง นอกจากนี้ ในปี 2012 สมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ หรืออาเซียน ยังได้ออกแถลงการณ์ยืนยันว่าจะเคารพและส่งเสริมสิทธิมนุษยชน รวมถึงความเป็นส่วนตัวด้วย

แต่ปัญหาใหญ่ก็คือ เทคโนโลยีได้เติบโตและพัฒนาเร็วเกินไป เพราะนับแต่ปี 1976 ที่มีการเซ็นสัญญาเรื่องสิทธิพลเมืองและสิทธิทางการเมืองระหว่างประเทศ โลกเราเปลี่ยนไปมาก ลองคิดดูสิ สมัยนั้นใครจะคิดว่าจะมี Facebook, Google, หรือ TikTok ดังนั้น จึงไม่แปลกเลยที่กฎหมายคุ้มครองความเป็นส่วนตัวไม่สามารถพัฒนาได้ทันความเปลี่ยนแปลง และมีช่องโหว่มากมาย เปรียบเสมือนเราเรากำลังใช้กฎหมายยุคโทรศัพท์บ้านมาควบคุมสมาร์ทโฟน 5G โดยเฉพาะเมื่อรัฐบาลหลายประเทศมีเครื่องมือดักฟังข้อมูลอิเล็กทรอนิกส์ที่ทันสมัย และโซเชียลมีเดียก็เติบโตแบบก้าวกระโดด ความเป็นส่วนตัวของเราจึงเสี่ยงมากขึ้นทุกวัน

แต่ก็ไม่ต้องตกใจไป เพราะหลายประเทศทั่วโลกต่างพยายามในการแก้ปัญหานี้อยู่ เช่น ในยุโรปมีอนุสัญญาพิเศษชื่อ “Convention 108” (อนุสัญญาคุ้มครองบุคคลจากการประมวลผลข้อมูลส่วนบุคคลอัตโนมัติ The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981) ที่ออกแบบมาเพื่อคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ แต่น่าเสียดายที่ยังไม่มีประเทศในเอเชียตะวันออกเฉียงใต้เข้าร่วม

คราวหน้าเวลาคุณโพสต์อะไรในโซเชียลมีเดีย หรือกดยอมรับนโยบายความเป็นส่วนตัวของแอปไหนสักอัน ลองคิดถึงเรื่องนี้ดู เพราะในโลกดิจิทัล การใช้ปลายนิ้วสัมผัสเพียงครั้งเดียวอาจส่งผลกระทบต่อเราได้มากกว่าที่เราคิด

2. ภาพรวมตราสารระหว่างประเทศที่สำคัญเกี่ยวกับสิทธิความเป็นส่วนตัว

ในทางกฎหมาย มีเอกสารและมาตรฐานระหว่างประเทศหลายฉบับที่กล่าวถึงสิทธิความเป็นส่วนตัว ไม่ว่าจะเป็นสนธิสัญญาระหว่างประเทศ มาตรฐานการคุ้มครองข้อมูลส่วนบุคคล หรือแนวทางปฏิบัติในการจัดการข้อมูล เรามาดูกันว่ามีอะไรบ้าง

- **ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (UDHR)** เป็นเอกสารสากลที่ประกาศโดยสมัชชาใหญ่แห่งสหประชาชาติเมื่อปี พ.ศ. 2491 (ค.ศ. 1948) มีเนื้อหาที่มุ่งคุ้มครองสิทธิมนุษยชนขั้นพื้นฐานและศักดิ์ศรีของมนุษย์ทั่วโลก ประกอบด้วยบทบัญญัติ 30 ข้อ ที่กล่าวถึงสิทธิพลเมือง การเมือง เศรษฐกิจ สังคม และวัฒนธรรม เช่น สิทธิในการมีชีวิต เสรีภาพ และความมั่นคง การห้ามการเป็นทาส และการทรมาน เป็นต้น
- **กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR)** เป็นสนธิสัญญาระหว่างประเทศที่ประกาศใช้เมื่อปี พ.ศ. 2509 (ค.ศ. 1966) มีผลบังคับใช้ในปี พ.ศ. 2519 (ค.ศ. 1976) มีวัตถุประสงค์เพื่อคุ้มครองสิทธิและเสรีภาพของบุคคลในด้านสิทธิพลเมืองและสิทธิทางการเมือง เช่น สิทธิในการแสดงออก สิทธิในการเลือกตั้ง สิทธิในความเป็นธรรมในกระบวนการยุติธรรม และการห้ามการกักขังโดยไม่ชอบด้วยกฎหมาย

- **อนุสัญญาระหว่างประเทศว่าด้วยการขจัดการเลือกปฏิบัติทางเชื้อชาติในทุกรูปแบบ (ICERD)** เป็นข้อตกลงระหว่างประเทศที่ประกาศใช้เมื่อปี พ.ศ. 2508 (ค.ศ. 1965) มีผลบังคับใช้ในปี พ.ศ. 2512 (ค.ศ. 1969) มีวัตถุประสงค์เพื่อขจัดการเลือกปฏิบัติทางเชื้อชาติ และส่งเสริมความเข้าใจและความเป็นหนึ่งเดียวกันระหว่างทุกเชื้อชาติ มุ่งเน้นการห้ามการเลือกปฏิบัติในทุกด้านของชีวิตสังคม เช่น การจ้างงาน การศึกษา และการให้บริการสาธารณะ
- **แนวทางของ OECD ว่าด้วยการคุ้มครองความเป็นส่วนตัวและการไหลเวียนข้อมูลข้ามพรมแดน** ถูกประกาศใช้ครั้งแรกในปี พ.ศ. 2523 (ค.ศ. 1980) และได้รับการปรับปรุงในปี พ.ศ. 2556 (ค.ศ. 2013) กำหนดหลักการสำหรับการจัดการข้อมูลส่วนบุคคลที่มีการส่งผ่านระหว่างประเทศ เพื่อรักษาสมดุลระหว่างการคุ้มครองข้อมูลและการส่งเสริมการค้าระหว่างประเทศ เช่น การเก็บข้อมูลอย่างยุติธรรมและถูกต้อง การใช้ข้อมูลอย่างเหมาะสม และการให้ความคุ้มครองสิทธิของบุคคลในการเข้าถึงและแก้ไขข้อมูลส่วนบุคคลของตนเอง
- **อนุสัญญาสภายุโรปว่าด้วยการคุ้มครองบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ** (อนุสัญญา 108/อนุสัญญา 108+) เป็นข้อตกลงระหว่างประเทศที่ประกาศใช ในปี พ.ศ. 2524 (ค.ศ. 1981) และได้รับการปรับปรุงในปี พศ.2561 (ค.ศ. 2018) เพื่อให้สอดคล้องกับความเปลี่ยนแปลงทางเทคโนโลยีและสังคม โดยมีวัตถุประสงค์เพื่อคุ้มครองสิทธิความ เป็นส่วนตัวของบุคคลในการประมวลผลข้อมูลส่วนบุคคล และกำหนดมาตรการเพื่อความปลอดภัยและความเป็นส่วนตัวในการจัดการข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ

- **แนวทางของสหประชาชาติเกี่ยวกับไฟล์ข้อมูลส่วนบุคคลทางคอมพิวเตอร์ (UN, 1990)** เป็นหลักการพื้นฐานที่กำหนดขึ้นในยุคเริ่มต้นของการใช้คอมพิวเตอร์อย่างแพร่หลาย โดยมุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคลในระบบคอมพิวเตอร์
- **มาตรฐานสากลว่าด้วยความเป็นส่วนตัวและการคุ้มครองข้อมูล (มติมาดริด)** เป็นข้อตกลงระหว่างประเทศที่กำหนดมาตรฐานสำหรับการคุ้มครองข้อมูลส่วนบุคคลในระดับสากล โดยครอบคลุมหลักการสำคัญเช่นความยินยอม ความโปร่งใส และสิทธิของเจ้าของข้อมูล
- **คำแนะนำ OECD เกี่ยวกับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยดิจิทัลเพื่อความเจริญรุ่งเรืองทางเศรษฐกิจและสังคม** มุ่งเน้นการสร้างความสมดุลระหว่างการใช้ประโยชน์จากเทคโนโลยีดิจิทัลและการรักษาความปลอดภัยของข้อมูล เพื่อส่งเสริมการพัฒนาทางเศรษฐกิจและสังคม
- **หลักการของสหประชาชาติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว (2018)** เป็นแนวทางล่าสุดที่ครอบคลุมประเด็นด้านความเป็นส่วนตัวในยุคดิจิทัล โดยเน้นย้ำความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลในบริบทของเทคโนโลยีสมัยใหม่
- **มติสมัชชาใหญ่แห่งสหประชาชาติว่าด้วยสิทธิความเป็นส่วนตัวในยุคดิจิทัล 2014** ยืนยันว่าสิทธิความเป็นส่วนตัวเป็นสิทธิมนุษยชนขั้นพื้นฐาน และเรียกร้องให้รัฐบาลทั่วโลกเคารพและคุ้มครองสิทธินี้ในบริบทของการสื่อสารดิจิทัล

นอกจากนี้ ยังมีเอกสารอื่นๆ เช่น รายงานของผู้รายงานพิเศษเรื่องการส่งเสริมและคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานขณะต่อต้านการก่อการร้าย 2014 มติสมัชชาใหญ่แห่งสหประชาชาติว่าด้วยสิทธิความเป็นส่วนตัวในยุคดิจิทัล 2020 ซึ่งกล่าวถึง “การแฮ็กและการใช้เทคโนโลยีไบโอเมตริกซ์อย่างผิดกฎหมาย” ว่าเป็น “การกระทำที่รุกล้ำละเมิดสิทธิความเป็นส่วนตัวเป็นอย่างมาก” ขัดขวางเสรีภาพในการแสดงออกและความคิดเห็น การชุมนุม และการสมาคมโดยสันติ และเสรีภาพในการนับถือศาสนาหรือความเชื่อ และ “อาจขัดแย้งกับหลักการของสังคมประชาธิปไตย รวมถึงเมื่อดำเนินการนอกอาณาเขตรัฐหรือในวงกว้าง” รายงานของข้าหลวงใหญ่สิทธิมนุษยชนแห่งสหประชาชาติประจำปี 2021 เรื่อง “สิทธิในความเป็นส่วนตัวในยุคดิจิทัล” ได้เรียกร้องให้มีการระงับการนำเทคโนโลยีจดจำใบหน้าไปใช้ในพื้นที่สาธารณะจนกว่ารัฐบาลจะสามารถแสดงให้เห็นได้ว่าไม่มีปัญหาสำคัญที่เกี่ยวข้องกับความถูกต้องหรือผลกระทบจากการเลือกปฏิบัติ และเทคโนโลยีเหล่านี้สอดคล้องกับมาตรฐานความเป็นส่วนตัวและการคุ้มครองข้อมูลที่เข้มแข็ง ตลอดจนเอกสารเรื่องความเป็นส่วนตัว จริยธรรม และการคุ้มครองข้อมูลของ UNSDG: คำแนะนำเกี่ยวกับข้อมูลขนาดใหญ่เพื่อการบรรลุผลสำเร็จของวาระปี 2030 และบทสรุปของสหประชาชาติเกี่ยวกับการคุ้มครองข้อมูลและนโยบายความเป็นส่วนตัว ซึ่งได้รวบรวมแนวปฏิบัติที่ดีและข้อเสนอแนะสำหรับการพัฒนานโยบายและกฎหมายเกี่ยวกับการคุ้มครองข้อมูลและความเป็นส่วนตัวในระดับประเทศและระหว่างประเทศ

3. การคุ้มครองข้อมูลเป็นส่วนหนึ่งของความเป็นส่วนตัวหรือเป็นสิทธิแยกต่างหาก

สิทธิความเป็นส่วนตัวและการคุ้มครองข้อมูลมีรากฐานจากปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 ที่กำหนดให้ความเป็นส่วนตัวเป็นสิทธิขั้นพื้นฐาน ปัจจุบันมีการเห็นพ้องในระดับนานาชาติว่าทั้งสองสิทธินี้เชื่อมโยงกัน ตัวอย่างเช่น ศาลฎีกาอินเดียในคดี Puttaswamy v. Union of India (2017) ยอมรับว่า “ความเป็นส่วนตัวด้านข้อมูล” เป็นส่วนสำคัญของสิทธิความเป็นส่วนตัว และเรียกร้องให้มีกฎหมายคุ้มครองข้อมูลที่เข้มแข็ง เช่นเดียวกับศาลสิทธิมนุษยชนแห่งยุโรปที่ในคดี Z v. Finland (1997) ชี้ว่า การคุ้มครองข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของการปกป้องชีวิตส่วนตัวภายใต้มาตรา 8 ของอนุสัญญายุโรป

กฎหมายคุ้มครองข้อมูลหลายฉบับทั่วโลก เช่น กฎหมายของยูกันดา (2019), ฟิลิปปินส์ (2012), และร่างกฎหมายของปากีสถาน (2019) รวมทั้งแนวปฏิบัติของ OECD และ APEC ต่างยึดหลักการคุ้มครองข้อมูลควบคู่ไปกับความเป็นส่วนตัว อย่างไรก็ตาม ในกฎบัตรสิทธิขั้นพื้นฐานของสหภาพยุโรป สิทธิในการคุ้มครองข้อมูลส่วนบุคคลถูกแยกออกมาเป็นสิทธิขั้นพื้นฐานต่างหากในมาตรา 8

โดยสรุป การคุ้มครองข้อมูลมักถูกมองว่าเป็นส่วนหนึ่งของสิทธิความเป็นส่วนตัว แต่ในบางกรณีอาจถูกพิจารณาเป็นสิทธิแยกต่างหาก ขึ้นอยู่กับบริบททางกฎหมายของแต่ละประเทศ

ประเด็นเสวนา: Digital Privacy ในฐานะสิทธิมนุษยชนที่ได้รับการยอมรับในระดับสากล

ดูวิดีโอและหารือเกี่ยวกับมิติสากลของสิทธิความเป็นส่วนตัวในสภาพแวดล้อมดิจิทัล สิ่งต่างๆ เปลี่ยนแปลงไปอย่างไรนับตั้งแต่ที่ UDHR และ ICCPR ถูกนำมาใช้? ข้อควรพิจารณาหลักที่คุณจะนำมาพิจารณาเมื่อพิจารณาสิทธิในความเป็นส่วนตัวในสภาพแวดล้อมดิจิทัลในปัจจุบันคืออะไร

ที่มา: https://www.youtube.com/watch?v=1TAHoAomKQg

4. หลักการความเป็นส่วนตัวและกรอบกติการะดับภูมิภาค

ภาพรวมของกรอบการทำงานที่สำคัญในภูมิภาคเอเชีย-แปซิฟิกและอาเซียน สามารถสรุปได้ ดังนี้

กรอบความร่วมมือด้านความเป็นส่วนตัวทางเศรษฐกิจเอเชีย-แปซิฟิก (APEC) กรอบการทำงานของ APEC ในเรื่องความเป็นส่วนตัว (จำลองตามแนวทางของ OECD) เน้นให้ประเทศสมาชิกใช้มาตรการที่สมเหตุสมผลเพื่อขจัดอุปสรรคที่ไม่จำเป็นต่อการไหลของข้อมูล และหลีกเลี่ยงการสร้างอุปสรรคใหม่ ๆ นอกจากนี้ ยังเป็นพื้นฐานสำหรับกฎความเป็นส่วนตัวข้ามพรมแดนหรือ Cross-Border Privacy Rules (CBPR)

กรอบการทำงานอาเซียนว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กรอบนี้มีวัตถุประสงค์เพื่อส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลในประเทศ

สมาชิกอาเซียน และสนับสนุนความร่วมมือระหว่างประเทศ โดยไม่มีพันธกรณีทางกฎหมาย แต่ส่งเสริมการนำหลักการความเป็นส่วนตัวไปใช้ในกฎหมายและข้อบังคับของแต่ละประเทศ พร้อมทั้งอำนวยความสะดวกในการไหลของข้อมูลอย่างเสรีระหว่างสมาชิก

ปฏิญญาสิทธิมนุษยชนอาเซียน (AHRD) มีผลใช้ในปี 2555 ระบุถึงสิทธิมนุษยชนขั้นพื้นฐานและเสรีภาพที่ประเทศสมาชิกอาเซียนให้คำมั่นจะเคารพและปกป้อง แม้ว่าปฏิญญานี้จะไม่มีกลไกบังคับใช้และมีการวิพากษ์วิจารณ์ว่าขาดมาตรฐานสิทธิมนุษยชนระหว่างประเทศ แต่ก็เป็นเอกสารสำคัญที่เน้นความสำคัญของสิทธิความเป็นส่วนตัวและความเท่าเทียมกันภายใต้กฎหมาย

กรอบอาเซียนว่าด้วยการกำกับดูแลข้อมูลดิจิทัล กรอบที่ได้รับความเห็นชอบในปี 2561 นี้กำหนดหลักการและความริเริ่มเพื่อเป็นแนวทางนโยบายและการกำกับดูแลการจัดการข้อมูลดิจิทัลในเศรษฐกิจดิจิทัลของประเทศสมาชิกอาเซียน

กรอบการจัดการข้อมูลอาเซียนและข้อสัญญาต้นแบบสำหรับกระแสข้อมูลข้ามพรมแดน (DMF และ MCCs) ในการประชุมรัฐมนตรีดิจิทัลอาเซียนครั้งที่ 1 ในปี 2564 มีการเห็นพ้องกันในกรอบการจัดการข้อมูลอาเซียน (DMF) และข้อสัญญาต้นแบบ (MCCs) สำหรับการไหลของข้อมูลข้ามพรมแดน DMF ช่วยองค์กรขนาดเล็กและขนาดกลาง (SMEs) ในการวางระบบการจัดการข้อมูลที่รวมเอาโครงสร้างการกำกับดูแลและการป้องกัน MCC ช่วยลดต้นทุนและเวลาในการเจรจาและการปฏิบัติตามกฎระเบียบ โดยเฉพาะสำหรับ SMEs และมั่นใจในความปลอดภัยของข้อมูลส่วนบุคคลในระหว่างการถ่ายโอนข้ามพรมแดน

กรอบการทำงานเหล่านี้สะท้อนให้เห็นถึงความพยายามของภูมิภาคเอเชีย-แปซิฟิกและอาเซียนในการปกป้องสิทธิความเป็นส่วนตัวและการ จัดการข้อมูลอย่างรอบคอบและปลอดภัย ในขณะเดียวกันก็ส่งเสริมการเติบโตของเศรษฐกิจดิจิทัลอย่างยั่งยืน

ประเด็นอภิปราย (10 นาที): การคุ้มครองข้อมูล: ผลกระทบระดับภูมิภาคสำหรับเอเชียตะวันออกเฉียงใต้

อ่านข้อความด้านล่างและหารือภายใต้สถานการณ์ใดที่การคุ้มครองข้อมูลและความเป็นส่วนตัวอาจมีความสำคัญในระดับภูมิภาคในเอเชียตะวันออกเฉียงใต้ และข้อควรพิจารณาสำคัญที่ต้องนำมาพิจารณาคืออะไร?

การคุ้มครองข้อมูลและความเป็นส่วนตัวในเอเชียตะวันออกเฉียงใต้มีความสำคัญอย่างมาก แต่ยังขาดความสอดคล้องกันในการพัฒนากฎหมาย ข้อกำหนดด้านการคุ้มครองข้อมูลของแต่ละประเทศสมาชิกอาเซียนมีความแตกต่างกัน เช่น สิงคโปร์มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ที่เข้มงวด แต่มีข้อยกเว้นสำหรับข้อมูลสาธารณะ ขณะที่อินโดนีเซียและไทยมีกรอบกฎหมายที่ยังไม่เข้มข้นนัก

นักกฎหมายและองค์กรภาคประชาสังคมร่วมพิจารณาสิ่งสำคัญเหล่านี้:

- ผู้ประมวลผลข้อมูลทำงานที่ไหน และรวบรวมข้อมูลใดบ้าง
- ข้อมูลทั้งหมดที่เก็บรวบรวมจำเป็นหรือไม่
- เจ้าของข้อมูลอยู่ที่ไหน
- ผู้ประมวลผลข้อมูลเก็บบันทึกประเภทใด ข้อมูลนี้อยู่ที่ไหน และข้อมูลถูกจัดเก็บอย่างไร (เช่น การประมวลผลแบบคลาวด์)
- กฎหมายคุ้มครองข้อมูลและความเป็นส่วนตัวในประเทศที่ผู้ประมวลผลข้อมูลดำเนินการอยู่มีอะไรบ้าง และเจ้าของข้อมูลอาศัยอยู่หรือไม่
- อะไรคือประเด็นที่แตกต่างกันของการเคลื่อนย้ายข้อมูลและสิทธิในข้อมูลส่วนบุคคลที่อาจเกิดขึ้นในการถ่ายโอนข้อมูลในระดับภูมิภาคข้ามพรมแดน เช่น การแจ้งเตือนด้านความปลอดภัยและการละเมิด

5. การผสานกรอบระหว่างประเทศและภูมิภาคสู่ระดับชาติ

ในส่วนนี้ เราจะสำรวจภาพรวมของกฎหมายและข้อบังคับด้านความเป็นส่วนตัวและการคุ้มครองข้อมูลระดับชาติที่สำคัญ ซึ่งได้ปรับใช้กรอบระหว่างประเทศและระดับภูมิภาค พร้อมยกตัวอย่างหน่วยงานกำกับดูแลที่ประสบความสำเร็จและบทเรียนสำคัญในการกำกับดูแลข้อมูลและความเป็นส่วนตัวดิจิทัลทั่วโลก

เริ่มต้นที่ยุโรป สหภาพยุโรปได้จัดทำกฎระเบียบหลายฉบับเพื่อการกำกับดูแลข้อมูลอย่างครอบคลุม เช่น ข้อบังคับคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป (General Data Protection Regulation: GDPR) ข้อกำหนด ePrivacy, Digital Services Act, และร่าง EU AI Act (ที่ตอนนี้ผ่านการพิจารณาแล้วและเตรียมบังคับใช้) รวมถึงร่าง EU Data Governance Act กฎหมายเหล่านี้มีเป้าหมายเพื่อปกป้องความเป็นส่วนตัวและสิทธิของผู้ใช้อินเทอร์เน็ตและผู้บริโภคออนไลน์

GDPR ถือเป็นจุดเปลี่ยนสำคัญที่เปลี่ยนแปลงการบริหารจัดการข้อมูลทั่วโลก มีผลบังคับใช้ตั้งแต่ 25 พฤษภาคม 2018 แทนที่กฎหมายเดิมปี 1995 โดยมอบอำนาจให้ผู้บริโภคควบคุมข้อมูลของตนเองอย่างไม่เคยมีมาก่อน พร้อมเสริมสร้างความโปร่งใสและปกป้องเสรีภาพออนไลน์ นอกจากนี้ ยังเพิ่มความพยายามด้านความปลอดภัยทางไซเบอร์ขององค์กร และสร้างความไว้วางใจในลูกค้า โดยป้องกันการรั่วไหลของข้อมูลในอนาคตด้วย

GDPR ครอบคลุมองค์กรทั้งในและนอกสหภาพยุโรปที่จัดการข้อมูลของคนในยุโรป รวมถึงธุรกิจเอเชียที่มีความเชื่อมโยงกับยุโรป องค์กรต้องปฏิบัติตามหลักการสำคัญ 6 ประการ ได้แก่ ปกป้องข้อมูลทุกขั้นตอน มีนโยบายที่เหมาะสม โปร่งใส รับผิดชอบ เคารพสิทธิของบุคคล และปฏิบัติตามกฎอย่างเคร่งครัด

การปฏิบัติตาม GDPR ไม่ใช่เพียงการทำตามรายการตรวจสอบ แต่ต้องจัดการข้อมูลอย่างรอบคอบและสร้างวัฒนธรรมองค์กรที่ใส่ใจความเป็นส่วนตัว องค์กรจำเป็นต้องปรับตัวทั้งด้านเทคนิค นโยบาย และวัฒนธรรม เพื่อให้สามารถปกป้องข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพตามที่ GDPR กำหนด

6. หลักการสำคัญของ GDPR

GDPR เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่มีหลักการสำคัญหลายประการ เริ่มจากความรับผิดชอบและการกำกับดูแล องค์กรต้องสามารถแสดงหลักฐานการปฏิบัติตาม GDPR ได้ โดยต้องบันทึกการประมวลผลข้อมูลอย่างละเอียด มีนโยบายคุ้มครองข้อมูล ประเมินผลกระทบสำหรับกิจกรรมเสี่ยงสูง และจัดอบรมพนักงาน

การประมวลผลข้อมูลต้องเป็นไปตามหลัก 6 ประการ คือ ชอบธรรม โปร่งใส มีวัตถุประสงค์ชัดเจน เก็บเฉพาะข้อมูลที่จำเป็น ข้อมูลต้องถูกต้องและเป็นปัจจุบัน และประมวลผลอย่างปลอดภัย นอกจากนี้ การประมวลผลต้องมีพื้นฐานทางกฎหมายรองรับ เช่น ได้รับความยินยอม ปฏิบัติตามสัญญา หรือเพื่อประโยชน์สาธารณะ

GDPR ให้ความสำคัญกับสิทธิของเจ้าของข้อมูล โดยกำหนดสิทธิต่าง ๆ เช่น สิทธิที่จะถูกลืม สิทธิคัดค้านการประมวลผล สิทธิโอนย้ายข้อมูล และสิทธิแก้ไขข้อมูลที่ไม่ถูกต้อง การขอความยินยอมต้องทำอย่างชัดเจน ใช้ภาษาเข้าใจง่าย และเจ้าของข้อมูลสามารถเพิกถอนได้ตลอดเวลา

ด้านความปลอดภัย องค์กรต้องใช้มาตรการป้องกันที่เหมาะสม และออกแบบระบบโดยคำนึงถึงความเป็นส่วนตัวตั้งแต่ต้น หากเกิดการละเมิดข้อมูลต้องรายงานภายใน 72 ชั่วโมง ความโปร่งใสเป็นอีกประเด็นสำคัญ โดยต้องแจ้งวิธีการ เหตุผล และผู้ประมวลผลข้อมูลอย่างชัดเจน

การโอนข้อมูลออกนอกสหภาพยุโรปทำได้เฉพาะกับประเทศที่มีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอ สุดท้าย องค์กรที่มีความเสี่ยงสูงหรือประมวลผลข้อมูลพิเศษต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (DPO) เพื่อให้คำแนะนำและตรวจสอบการปฏิบัติตาม GDPR

โดยสรุป GDPR กำหนดมาตรฐานสูงในการคุ้มครองข้อมูลส่วนบุคคล ทำให้องค์กรต้องปรับตัวอย่างมากเพื่อให้สอดคล้องกับกฎหมายนี้ ซึ่งครอบคลุมทั้งด้านเทคนิค นโยบาย และวัฒนธรรมองค์กร

ประเด็นอภิปราย (15 นาที): อ่านกรณีศึกษาและแลกเปลี่ยนความคิดเห็นว่ากฎหมายคุ้มครองข้อมูลในประเทศของตนเองเป็นอย่างไร เปรียบเทียบกับคดี GDPR ที่ยกมานี้

คดีดัง: Facebook โดนปรับเพราะทำผิด GDPR Meta บริษัทแม่ของ Facebook โดนปรับ 265 ล้านยูโร ในไอร์แลนด์ สาเหตุเพราะข้อมูลผู้ใช้หลุดไปอยู่ในฟอรัมแฮกเกอร์ ข้อมูลที่รั่วไหลมีทั้งชื่อเต็ม ข้อมูลติดต่อ วันเกิด และที่อยู่ ของคนใช้ Facebook ในปี 2018 -2019

Meta ยอมรับว่าต้นเหตุคือฟีเจอร์ค้นหาเพื่อนด้วยเบอร์โทรที่ไม่ปลอดภัยพอ Facebook ถูกปรับเพราะ “ไม่ได้ใช้การคุ้มครองข้อมูลโดยการออกแบบและโดยค่าเริ่มต้น” ตามที่ GDPR กำหนด หากฟีเจอร์นี้ถูกออกแบบให้ปลอดภัยกว่านี้ตั้งแต่แรก ก็อาจหลีกเลี่ยงค่าปรับได้

Google ก็โดนปรับเพราะทำผิด GDPR

เมื่อ 6 มกราคม 2022 Google โดนปรับ 90 ล้านยูโร ในฝรั่งเศส เหตุผลคือวิธีขอความยินยอมเรื่องคุกกี้ของ YouTube ไม่ถูกต้องตาม GDPR

ปัญหาคือ YouTube ให้กด “ยอมรับ” คุกกี้ง่าย ๆ แค่คลิกเดียว แต่ถ้าจะ “ปฏิเสธ” ต้องคลิกหลายที GDPR ระบุว่าการให้ความยินยอมต้อง “สมัครใจ” ถ้ายอมรับง่าย การปฏิเสธก็ต้องง่ายเท่ากัน

CNIL หน่วยงานคุ้มครองข้อมูลของฝรั่งเศสให้เหตุผลว่าที่ปรับหนักเพราะ YouTube มีผู้ใช้เยอะและ Google ก็ได้เงินมหาศาลจากเว็บนี้

นอกจากนี้ มีการยกประเด็นเรื่องเขตอำนาจศาลขึ้น โดย Google โต้แย้งว่า Google ดำเนินการในสหภาพยุโรปจากไอร์แลนด์ หน่วยงานกำกับดูแลของไอร์แลนด์ควรเป็นผู้ดูแลค่าปรับนี้ แต่ CNIL แย้งโดยบอกว่า การกำกับดูแลคุกกี้อยู่ภายใต้ข้อกำหนด ePrivacy เป็นหลักไม่ใช่ GDPR ดังนั้นหน่วยงานกำกับดูแลสามารถดำเนินการกับผู้ดำเนินการเว็บไซต์ในเขตอำนาจของตนได้โดยตรง ไม่ต้องส่งทุกอย่างกลับไปยัง “สถานประกอบการหลัก” ของบริษัท

GDPR เปลี่ยนโลกการค้าในเอเชียตะวันออกเฉียงใต้

เคยสงสัยไหมว่าทำไมเว็บไซต์ต่าง ๆ ถึงชอบถามเรื่องคุกกี้กันนักหนา? นั่นแหละคือผลพวงจาก GDPR กฎหมายคุ้มครองข้อมูลส่วนตัวของยุโรปที่ส่งผลกระเทือนไปทั่วโลก รวมถึงบ้านเราในเอเชียตะวันออกเฉียงใต้ โดย GDPR เป็นสาเหตุที่ทำให้บริษัทในเอเชียตะวันออกเฉียงใต้ต้องปวดหัวกันยกใหญ่ และต้องมานั่งทบทวนนโยบายความเป็นส่วนตัวกันใหม่หมด เพื่อให้สอดคล้องกับกฎการโอนข้อมูลข้ามประเทศของ GDPR

แต่ความปวดหัวดังกล่าวก็ไม่ใช่เรื่องร้าย แต่กลับกลายเป็นโอกาสให้หลายประเทศในภูมิภาคนี้ยกระดับกฎหมายคุ้มครองข้อมูลของตัวเองให้ทัดเทียมมาตรฐานโลก

คิดดูสิ ถ้าประเทศไหนได้รับการยอมรับว่ามีมาตรฐาน “เพียงพอ” ตาม GDPR ก็เหมือนได้ใบเบิกทางให้ข้อมูลไหลเวียนเข้าออกยุโรปได้อย่างเสรี โดยไม่ต้องกังวลเรื่องกฎระเบียบที่ยุ่งยาก โดยปัจจุบัน ในเอเชีย-แปซิฟิก มีแค่ญี่ปุ่น เกาหลีใต้ และนิวซีแลนด์เท่านั้นที่ได้ “ใบเบิกทาง” นี้ ขณะที่ประเทศอื่นในเอเชียตะวันออกเฉียงใต้กำลังวิ่งกันขาขวิดเพื่อปรับปรุงกฎหมายให้ได้มาตรฐานนี้

GDPR จึงเหมือนตัวเร่งปฏิกิริยาให้เกิดการเปลี่ยนแปลงครั้งใหญ่ในวงการคุ้มครองข้อมูลส่วนบุคคลของภูมิภาคเรา ใครที่ปรับตัวได้เร็วก็จะมีโอกาสชิงความได้เปรียบในตลาดโลกก่อนใครเพื่อน

ถึงตอนนี้ คงพอเห็นภาพแล้วว่า GDPR ไม่ใช่แค่กฎหมายของยุโรป แต่เป็นมาตรฐานใหม่ของโลกที่ทุกคนต้องปรับตัว รวมถึงเราชาวเอเชียตะวันออกเฉียงใต้ด้วย

7. กฎหมายคุ้มครองข้อมูลของประเทศสมาชิกอาเซียนหลัง GDPR

มาเลเซีย: กำลังแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ปี 2010 ให้เข้ากับ GDPR โดยเริ่มทบทวนตั้งแต่ปี 2018 แล้ว แต่ยังไม่เสร็จ

ฟิลิปปินส์: ทำการบ้านส่งทันเวลา มีกฎหมายความเป็นส่วนตัวของข้อมูลตั้งแต่ปี 2016 และปรับปรุงให้สอดคล้องกับ GDPR แล้ว นอกจากนี้ หน่วยงานกำกับดูแลก็ออกแนวทางใหม่ ๆ มาเรื่อย ๆ เพื่อให้ทันกับ GDPR

ไทย: มี PDPA ที่ให้การคุ้มครองคล้าย GDPR แต่ก็มีกลิ่นอายความเป็นไทยอยู่ เนื่องจากไทยเป็นคู่ค้าใหญ่อันดับ 3 ในอาเซียนของ EU เลยต้องปรับตัวให้ทัน แต่บริษัทต่าง ๆ ก็ต้องระวังเพราะการทำตาม GDPR เพียงอย่างเดียวก็ไม่พอ เพราะต้องดูกฎหมายไทยด้วย

อินโดนีเซีย: มาช้าแต่มาแรง ออกกฎหมายใหม่เอี่ยมเมื่อ 17 ตุลาคม 2022 โดยมีเนื้อหาสาระที่คล้ายกับ GDPR มาก ใช้คำศัพท์เหมือนกัน แต่เข้มกว่าในบางเรื่อง เช่น ต้องรายงานข้อมูลรั่วไหลภายใน 3 วัน (GDPR ให้ 72 ชั่วโมง) และขอบเขตการบังคับใช้กว้างกว่า GDPR อีก

เวียดนาม: เหมือนเด็กดื้อในห้อง ไม่ยอมทำตามใคร มีกฎหมายกระจัดกระจายหลายฉบับ แถมยังออกกฎไซเบอร์สุดเข้มในปี 2019 บังคับให้เก็บข้อมูลไว้ในประเทศ ต้องแปลข้อมูลเป็นภาษาเวียดนาม และบริษัทต่างชาติต้องตั้งสำนักงานในเวียดนาม แถมยังต้องเปิดเผยข้อมูลลูกค้าเมื่อรัฐบาลขอ

สิงคโปร์: ผู้นำด้านการคุ้มครองข้อมูลในเอเชียตะวันออกเฉียงใต้ เปรียบเสมือนเด็กเก่งประจำห้อง มีความโดดเด่นในฐานะประเทศที่มีประวัติการกำกับดูแลที่เข้มแข็ง มีการออกกฎหมายตั้งแต่ปี 2012 กำหนดให้ต้องขอความยินยอมในการเก็บข้อมูล ยกเว้นข้อมูลที่เปิดเผยต่อสาธารณะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 2012 ของสิงคโปร์มีความคล้ายคลึงกับ GDPR ในแง่ที่ทั้งสองกฎหมายต้องการความยินยอมจากผู้บริโภคสำหรับการสื่อสารทั้งหมดเกี่ยวกับการเก็บ ประมวลผล และเปิดเผยข้อมูล นอกจากนี้ สิงคโปร์ได้เผยแพร่เอกสารอภิปรายเพื่อกำหนดสิทธิในการโอนย้ายข้อมูล ซึ่งจะให้ผู้บริโภคมีอำนาจควบคุมการไหลของข้อมูลของตนระหว่างผู้ให้บริการมากขึ้น ล่าสุด สิงคโปร์ได้กำหนดให้หน่วยงานพัฒนาสื่อสารสนเทศ (IMDA) เป็นองค์กรกำกับดูแลในเรื่องนี้

สิงคโปร์ก้าวไกลในเวทีโลก เข้าร่วมระบบ APEC CBPR ในปี 2018 โดยเป็นประเทศที่สามต่อจากสหรัฐฯ และญี่ปุ่น ระบบนี้เป็นมาตรฐานความเป็นส่วนตัวข้ามพรมแดนของกลุ่มเอเปค ในฐานะตัวแทนรับผิดชอบ IMDA (หน่วยงานพัฒนาสื่อสารสนเทศ) จะทำหน้าที่ตรวจสอบอิสระจากบุคคลที่สาม เพื่อให้แน่ใจว่านโยบายและขั้นตอนด้านความเป็นส่วนตัวของบริษัทที่เข้าร่วมนั้น สอดคล้องกับ APEC CBPR และ Privacy Recognition for Processors: PRP (การรับรองด้านความเป็นส่วนตัวสำหรับผู้ประมวลผล) ก่อนที่จะให้การรับรอง

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ (PDPC) มีบทบาทอย่างมากในการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ตัวอย่างเช่น ในปี 2019 องค์กร 5 แห่งถูกปรับรวมทั้งสิ้น 117,000 ดอลลาร์สิงคโปร์ เนื่องจากละเมิดกฎความเป็นส่วนตัวของข้อมูล โดยไม่สามารถปกป้องข้อมูลส่วนบุคคลของลูกค้าและพนักงานได้ นอกจากนี้ มีกรณีบริษัท Horizon Fast Ferry ถูกปรับ 54,000 ดอลลาร์สิงคโปร์ เนื่องจากไม่ได้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล ไม่กำหนดและดำเนินการตามนโยบายและกระบวนการคุ้มครองข้อมูล และไม่ได้จัดให้มี “มาตรการรักษาความปลอดภัยที่เพียงพอ” เพื่อปกป้องข้อมูลส่วนบุคคลของผู้บริโภค

สิงคโปร์จัดการข้อมูลภาครัฐและเอกชนแยกกันอย่างชาญฉลาด ใช้ PSGA (พระราชบัญญัติการกำกับดูแลภาครัฐ) ควบคุมหน่วยงานรัฐส่วน PDPA ดูแลภาคเอกชน ที่เป็นเช่นนี้เพราะประชาชนคาดหวังต่างกัน รัฐต้องทำงานแบบบูรณาการ ส่วนเอกชนดูแลข้อมูลแยกกันไป แต่ที่เด็ดสุดคือ PSGA ไม่เล่นด้วย ถ้าเจ้าหน้าที่รัฐแอบเปิดเผยข้อมูล เอาไปใช้ส่วนตัว หรือพยายามสืบหาตัวตนจากข้อมูลไม่ระบุชื่อ มีสิทธิติดคุกเลยนะ! นี่แหละวิธีที่สิงคโปร์สร้างความเชื่อมั่นให้ประชาชน ว่าข้อมูลของพวกเขาจะปลอดภัย ไม่ว่าจะอยู่ในมือรัฐหรือเอกชน PSGA นี่แหละที่ทำให้การจัดการข้อมูลภาครัฐของสิงคโปร์แข็งแกร่งและน่าเชื่อถือ

สิงคโปร์ยกระดับการคุ้มครองข้อมูลด้วย “เครื่องหมายรับรองการคุ้มครองข้อมูล” หรือ DPTM ซึ่งเป็นเสมือนตราประทับรับรองว่าองค์กรนั้นดูแลข้อมูลส่วนบุคคลได้ดี พัฒนาโดย PDPC และ IMDA เครื่องหมายนี้มีความสำคัญในการรับรองคุณภาพ สร้างความเชื่อมั่น และแสดงการปฏิบัติตามกฎหมาย PDPA อย่างเคร่งครัด DPTM เปรียบเสมือนดาวทองที่บ่งบอกว่าองค์กรไหนเป็น “เด็กดี” ในเรื่องการดูแลข้อมูล ช่วยให้ประชาชนและหน่วยงานรัฐมั่นใจได้ว่าข้อมูลส่วนตัวจะปลอดภัยเมื่ออยู่ในมือขององค์กรที่มีเครื่องหมายนี้ นับเป็นอีกก้าวที่แสดงให้เห็นว่า สิงคโปร์ไม่ได้แค่ออกกฎหมาย แต่ยังสร้างระบบนิเวศที่ส่งเสริมการคุ้มครองข้อมูลอย่างจริงจัง

8. ท่องโลกกฎหมายคุ้มครองความเป็นส่วนตัวของข้อมูล

สหราชอาณาจักร: เข้มงวดเรื่องข้อมูลส่วนบุคคลไม่แพ้ใคร

สหราชอาณาจักรยกระดับการคุ้มครองข้อมูลส่วนบุคคลด้วยพระราชบัญญัติคุ้มครองข้อมูล 2018 ซึ่งนำ GDPR มาปรับใช้อย่างจริงจัง กฎหมายนี้วางกฎเกณฑ์เข้มงวดในการจัดการข้อมูลส่วนตัว ให้สิทธิประชาชนในการเข้าถึงและลบข้อมูลของตนเอง บังคับให้องค์กรต้องมีเจ้าหน้าที่คุ้มครองข้อมูล (DPO) และรายงานกิจกรรมบางอย่างต่อสำนักงานคณะกรรมการข้อมูลข่าวสาร (ICO) หากฝ่าฝืน โทษปรับรุนแรงรออยู่ สะท้อนให้เห็นว่าสหราชอาณาจักรให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคลอย่างจริงจัง ใครที่ต้องจัดการข้อมูลของชาวอังกฤษต้องระมัดระวังเป็นพิเศษ

สหรัฐอเมริกา: การคุ้มครองข้อมูลแบบ “แยกส่วน” ที่น่าจับตา

ขณะที่สหราชอาณาจักรยกระดับการคุ้มครองข้อมูลส่วนบุคคลด้วยพระราชบัญญัติคุ้มครองข้อมูล 2018 ซึ่งนำ GDPR มาปรับใช้อย่างจริงจัง กฎหมายนี้วางกฎเกณฑ์เข้มงวดในการจัดการข้อมูลส่วนตัว ให้สิทธิประชาชนในการเข้าถึงและลบข้อมูลของตนเอง บังคับให้องค์กรต้องมีเจ้าหน้าที่คุ้มครองข้อมูล (DPO) และรายงานกิจกรรมบางอย่างต่อสำนักงานคณะกรรมการข้อมูลข่าวสาร (ICO) หากฝ่าฝืน โทษปรับรุนแรงรออยู่ สะท้อนให้เห็นว่าสหราชอาณาจักรให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคลอย่างจริงจัง ใครที่ต้องจัดการข้อมูลของชาวอังกฤษต้องระมัดระวังเป็นพิเศษ

สหรัฐจัดการเรื่องความเป็นส่วนตัวของข้อมูลแบบ “แยกส่วน” ที่ไม่เหมือนใคร ไม่มีกฎหมายกลางแบบ GDPR แต่มีกฎเฉพาะสำหรับแต่ละด้าน เช่น ข้อมูลสุขภาพ การจ้างงาน หรือข้อมูลนักเรียน แต่ละรัฐก็มีกฎของตัวเอง ทำให้ภาพรวมดูซับซ้อน ไม่มีการคุ้มครองแบบครอบคลุมทั่วไปสำหรับการเก็บหรือใช้ข้อมูลโดยไม่ได้รับอนุญาต แต่มีคณะกรรมาธิการการค้าแห่งรัฐบาลกลาง (FTC) คอยจับตาดูบริษัทที่อาจหลอกลวงหรือใช้ข้อมูลอย่างไม่เป็นธรรม วิธีนี้ทำให้สหรัฐฯ ยืดหยุ่นในการจัดการข้อมูลแต่ละประเภท แต่ก็อาจทำให้เกิดช่องโหว่ในการคุ้มครองข้อมูลบางอย่างได้ ใครทำธุรกิจในสหรัฐฯ ต้องระวังให้ดี เพราะกฎอาจแตกต่างกันไปในแต่ละรัฐและแต่ละประเภทธุรกิจ

หลักการปฏิบัติด้านข้อมูลที่เป็นธรรม (FIPPs): รากฐานการคุ้มครองข้อมูลของสหรัฐฯ

ย้อนกลับไปปี 1973 สหรัฐฯ วางรากฐานการคุ้มครองข้อมูลด้วย FIPPs (The Fair Information Practice Principles) จากรายงานเรื่อง “การบันทึกคอมพิวเตอร์ และสิทธิของพลเมือง” หลักการนี้กลายเป็นแม่แบบสำคัญที่มีอิทธิพลต่อกฎหมายทั้งในระดับรัฐบาลกลาง รัฐ และแม้แต่ต่างประเทศ FIPPs เป็นเหมือน “คัมภีร์” ในการจัดการข้อมูลของรัฐบาล โดยเฉพาะข้อมูลส่วนบุคคล แม้เวลาจะผ่านไป ถ้อยคำอาจเปลี่ยน แต่แก่นแท้ยังคงอยู่ ใช้ได้กับทุกองค์กรภาครัฐ

สิ่งที่น่าทึ่งคือ หลักการที่คิดขึ้นตั้งแต่ยุค 70 ยังคงใช้ได้ดีในยุคดิจิทัล แสดงให้เห็นว่า FIPPs วางรากฐานที่แข็งแกร่งและยืดหยุ่นพอที่จะรับมือกับความเปลี่ยนแปลงทางเทคโนโลยี

ที่มา: https://www.fpc.gov/resources/fipps/

นอกจากนี้ สหรัฐฯ ยังมีกฎหมายอีกหลายฉบับที่คุ้มครองข้อมูลส่วนบุคคลในด้านต่างๆ แยกจากกัน มาดูกันว่าแต่ละฉบับมีอะไรบ้าง

กฎหมายคุ้มครองข้อมูลสุขภาพ (Health Insurance Portability and Accountability Act, HIPAA): ถ้าคุณไปหาหมอ ข้อมูลการรักษาของคุณจะถูกปกป้องโดย HIPAA โรงพยาบาลหรือคลินิกต้องรักษาความลับข้อมูลสุขภาพของคุณอย่างเคร่งครัด ไม่สามารถเปิดเผยให้ใครรู้ได้ถ้าคุณไม่อนุญาต

กฎหมายคุ้มครองความเป็นส่วนตัวออนไลน์ของเด็ก (Children's Online Privacy Protection Act, COPPA): เว็บไซต์หรือแอปที่มีกลุ่มเป้าหมายเป็นเด็กอายุต่ำกว่า 13 ปี ต้องระวังให้มาก! COPPA กำหนดให้ต้องขออนุญาตผู้ปกครองก่อนเก็บข้อมูลเด็ก และต้องให้ข้อมูลชัดเจนว่าจะเก็บอะไร ใช้ยังไง

กฎหมายคุ้มครองข้อมูลการศึกษา (Family Educational Rights and Privacy Act, FERPA): ถ้าคุณเป็นนักเรียนหรือผู้ปกครอง FERPA ให้สิทธิคุณเข้าถึงและแก้ไขบันทึกการศึกษาได้ โรงเรียนจะเปิดเผยข้อมูลเหล่านี้ให้คนอื่นไม่ได้ถ้าไม่ได้รับอนุญาตจากคุณ ยกเว้นในบางกรณีที่จำเป็น

กฎหมายคุ้มครองข้อมูลเครดิต (Fair Credit Reporting Act, FCRA): เคยสงสัยไหมว่าทำไมธนาคารถึงรู้ว่าควรให้คุณกู้เงินหรือไม่ เหตุผลก็เพราะว่า FCRA ควบคุมการใช้ข้อมูลเครดิตของคุณ ให้สิทธิคุณตรวจสอบรายงานเครดิตฟรีปีละครั้ง และแก้ไขข้อมูลที่ไม่ถูกต้องได้

กฎหมายคุ้มครองการสื่อสารทางอิเล็กทรอนิกส์ (Electronic Communications Privacy Act, ECPA): อีเมล ข้อความ และการโทรของคุณจะถูกแอบดูไม่ได้ เพราะ ECPA ทำหน้าที่ป้องกันการดักฟังหรือเข้าถึงการสื่อสารของคุณโดยไม่ได้รับอนุญาต แม้แต่รัฐบาลก็ต้องขออนุญาตศาลก่อนจะเข้าถึงข้อมูลเหล่านี้

กฎหมายคุ้มครองข้อมูลที่รัฐบาลถือครอง (Privacy Act of 1974): เมื่อคุณติดต่อกับหน่วยงานรัฐ ข้อมูลของคุณจะถูกปกป้องโดยกฎหมายนี้ คุณมีสิทธิรู้ว่ารัฐเก็บข้อมูลอะไรของคุณบ้าง แก้ไขได้ถ้าไม่ถูกต้อง และรัฐต้องขออนุญาตคุณก่อนจะเอาข้อมูลไปใช้นอกเหนือจากวัตถุประสงค์ที่เก็บ

นอกจากกฎหมายที่ได้ยกตัวอย่างไปข้างต้น หากดูกฎหมายระดับมลรัฐ ก็มีตัวอย่างกฎหมายที่น่าสนใจอีกหลายฉบับ เช่น

พระราชบัญญัติคุ้มครองความเป็นส่วนตัวของผู้บริโภคแคลิฟอร์เนีย (California Consumer Protection Act, CCPA): แคลิฟอร์เนียนำร่องกฎหมายคุ้มครองข้อมูลแบบ GDPR ในสหรัฐฯ CCPA ให้สิทธิชาวแคลิฟอร์เนียรู้ว่าใครเก็บข้อมูลอะไรของพวกเขาบ้าง และสามารถขอลบข้อมูลได้อีกด้วย ซึ่งนับเป็นก้าวสำคัญในการคุ้มครองความเป็นส่วนตัวของผู้บริโภคในยุคดิจิทัล

พระราชบัญญัติสิทธิความเป็นส่วนตัวแคลิฟอร์เนีย (California Privacy Rights Act, CPRA): เริ่มใช้ 1 มกราคม 2023 เป็นการอัพเกรด CCPA ให้แรงขึ้น เพิ่มสิทธิให้ชาวแคลิฟอร์เนียควบคุมข้อมูลตัวเองได้มากขึ้น และบีบให้บริษัทต่างๆ ต้องระมัดระวังในการจัดการข้อมูลลูกค้ามากขึ้น เรียกว่าเป็น “GDPR ฉบับอเมริกัน” ก็ว่าได้

จะเห็นได้ว่า แม้สหรัฐฯ จะไม่มีกฎหมายคุ้มครองข้อมูลกลางแบบรวมศูนย์เช่นยุโรป แต่ก็มีกฎหมายเฉพาะหลากหลายด้าน และมลรัฐแคลิฟอร์เนียก็กำลังนำร่องสร้างมาตรฐานใหม่ในการคุ้มครองข้อมูล ซึ่งอาจส่งผลให้รัฐอื่น ๆ หรือแม้แต่รัฐบาลกลางต้องพิจารณาออกกฎหมายในลักษณะเดียวกันในอนาคต

ประเด็นอภิปราย (10-15 นาที): ความเป็นส่วนตัวได้รับผลกระทบจากประเพณีทางกฎหมายและวัฒนธรรมหรือไม่?

อ่านข้อมูลเกี่ยวกับความแตกต่างและแนวทางการคุ้มครองความเป็นส่วนตัวระหว่างสหรัฐอเมริกาและสหภาพยุโรปด้านล่าง จากนั้นร่วมกันอภิปรายว่าโครงสร้างทางกฎหมายด้านความเป็นส่วนตัวในแต่ละเขตอำนาจศาลแตกต่างกันอย่างไร และอะไรคือปัจจัยสำคัญที่มีอิทธิพลต่อความแตกต่างเหล่านี้ ให้พิจารณาทั้งข้อดีและข้อเสียของแต่ละแนวทาง รวมถึงความเหมาะสมกับบริบทของประเทศตนเอง เพื่อให้เข้าใจถึงความหลากหลายในการคุ้มครองข้อมูลส่วนบุคคลในระดับโลก

สหภาพยุโรปและสหรัฐอเมริกามีแนวทางที่แตกต่างกันในการคุ้มครองข้อมูลส่วนบุคคล โดยสหภาพยุโรปถือว่าการคุ้มครองข้อมูลเป็นสิทธิขั้นพื้นฐาน ในขณะที่สหรัฐฯ เน้นการไม่แทรกแซงและให้ความสำคัญกับผลประโยชน์ทางการค้ามากกว่า อย่างไรก็ตาม เนื่องจากการละเมิดข้อมูลที่เกิดขึ้นอย่างต่อเนื่อง ทำให้แนวคิดของสหรัฐฯ เริ่มเปลี่ยนไปสู่การคุ้มครองบุคคลมากขึ้น แต่การปรับเปลี่ยนให้สอดคล้องกับแนวทางของสหภาพยุโรปอย่างสมบูรณ์ยังต้องใช้เวลา เนื่องจากความแตกต่างทางวัฒนธรรมพื้นฐานที่ฝังรากลึก

แอฟริกาใต้: ผู้นำการคุ้มครองข้อมูลส่วนบุคคลแห่งทวีปแอฟริกา

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Protection of Personal Information Act, POPI Act) ของแอฟริกาใต้: กฎหมายนี้เป็นเสมือนเสาหลักในการปกป้องความเป็นส่วนตัวของชาวแอฟริกาใต้ ทำให้สิทธิตามรัฐธรรมนูญกลายเป็นความจริง โดยวางกรอบชัดเจนว่าใครจะจัดการข้อมูลส่วนตัวของประชาชนได้อย่างไร ครอบคลุมทุกขั้นตอนตั้งแต่เก็บ ใช้ จนถึงลบข้อมูล โดย POPI Act ไม่ได้ทำตามใครแต่ก้าวทันโลก สอดคล้องกับมาตรฐานสากล แถมยังมีกฎพิเศษสำหรับเรื่องสำคัญ ๆ เช่น การตลาดตรง การตัดสินใจอัตโนมัติ และการส่งข้อมูลข้ามประเทศ ด้วยหลักการ 8 ข้อ POPI Act ทำให้แอฟริกาใต้มีที่ยืนในเวทีโลกด้านการคุ้มครองข้อมูล แสดงให้เห็นว่าประเทศกำลังพัฒนาก็สามารถมีกฎหมายทันสมัยที่คุ้มครองประชาชนในยุคดิจิทัลได้

หลักการสำคัญของ POPI Act

POPI Act ของแอฟริกาใต้วางหลักสำคัญ 8 ข้อในการจัดการข้อมูลส่วนบุคคล ได้แก่

1) ต้องทำอย่างถูกกฎหมายและมีจริยธรรม
2) ใช้ข้อมูลตามวัตถุประสงค์ที่ได้รับมาเท่านั้น
3) จำกัดการประมวลผลในอนาคตที่นอกเหนือจากขอบเขตเดิม
4) รับรองคุณภาพของข้อมูลให้ครบถ้วนและถูกต้อง
5) แจ้งเจ้าของข้อมูลและหน่วยงานกำกับดูแลเกี่ยวกับการประมวลผล
6) มีมาตรการรักษาความปลอดภัยที่เหมาะสม
7) ให้เจ้าของข้อมูลเข้าถึงและแก้ไขข้อมูลของตนได้ และ
8) ผู้ประมวลผลต้องรับผิดชอบในการปฏิบัติตามมาตรการเหล่านี้

หลักการนี้ครอบคลุมทุกขั้นตอนของการจัดการข้อมูล ตั้งแต่การเก็บรวบรวม ใช้งาน จนถึงการป้องกันการสูญหายหรือเข้าถึงโดยไม่ได้รับอนุญาต ทำให้การคุ้มครองข้อมูลส่วนบุคคลในแอฟริกาใต้มีความครอบคลุมและเข้มแข็ง

แต่แอฟริกาใต้ยังไม่หยุดแค่นี้! กำลังจะมีกฎใหม่เกี่ยวกับข้อมูลและคลาวด์ที่จะทำให้การคุ้มครองข้อมูลแน่นหนายิ่งขึ้น ขยายความหมาย “ข้อมูลส่วนตัว” ให้กว้างขึ้น ข้อมูลสำคัญๆ ต้องเก็บไว้ในประเทศเท่านั้น! รัฐบาลเองก็จะเก็บข้อมูลลับๆ ไว้ในที่ปลอดภัยสุดๆ แบบนี้ใครจะกล้าเล่นกับข้อมูลคนแอฟริกาใต้ล่ะ? นี่แหละ ประเทศกำลังพัฒนาที่ไม่ยอมตามหลังใครในเรื่องกฎหมายดิจิทัล!

บราซิล: ก้าวสำคัญสู่การคุ้มครองข้อมูลส่วนบุคคลแบบครอบคลุม บราซิลยกระดับการปกป้องข้อมูลประชาชนด้วยพระราชบัญญัติคุ้มครองข้อมูลทั่วไป (LGPD) ในปี 2018 กฎหมายนี้เป็นเสมือนร่มใหญ่ที่ครอบคลุมการจัดการข้อมูลส่วนบุคคลทั้งประเทศ แทนที่กฎหมายเก่าที่แยกส่วนและสร้างความสับสน LGPD ได้แรงบันดาลใจจาก GDPR ของยุโรป วางมาตรฐานชัดเจนในการเก็บใช้ และแชร์ข้อมูลส่วนตัว

จุดเด่นของ LGPD คือการห้ามเก็บและใช้ข้อมูลโดยไม่ได้รับความยินยอม ไม่ว่าจะเป็นหน่วยงานรัฐหรือเอกชน และห้ามใช้ข้อมูลเพื่อเลือกปฏิบัติอย่างไม่เป็นธรรม นี่เป็นก้าวใหญ่ของบราซิลในการรับรองสิทธิความเป็นส่วนตัวของประชาชน และทำให้บราซิลก้าวขึ้นมาเป็นผู้นำด้านการคุ้มครองข้อมูลในละตินอเมริกา

จีน: ยักษ์ใหญ่แห่งเอเชียกับการปฏิวัติกฎหมายคุ้มครองข้อมูล

จีนเขย่าวงการเทคโนโลยีด้วยกฎหมายคุ้มครองข้อมูล 2 ฉบับใหม่เอี่ยมที่ทำให้ทั้งบริษัทในและนอกจีนต้องปรับตัวกันขนานใหญ่

ฉบับแรก **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (The Personal Information Protection Law: PIPL)** เริ่มใช้เมื่อพฤศจิกายน 2021 ให้อำนาจประชาชนจีนควบคุมข้อมูลตัวเองมากขึ้น มีลักษณะคล้าย GDPR ของยุโรป ใครจะแตะต้องข้อมูลคนจีน ไม่ว่าจะอยู่ในหรือนอกจีน จะต้องระวังไว้ให้ดี เพราะกฎหมายกำหนดโทษเอาไว้หนักมาก ปรับได้ถึง 50 ล้านหยวน หรือ 5% ของรายได้ปีที่แล้ว (แล้วแต่อันไหนมากกว่า)

อีกฉบับ **กฎหมายความปลอดภัยของข้อมูล (Data Security Law: DSL)** เน้นเรื่องการจัดระดับความสำคัญของข้อมูล และควบคุมการส่งข้อมูลออกนอกประเทศ ทำให้บริษัทต่าง ๆ ต้องคิดหนักว่าจะเก็บ ใช้ และส่งข้อมูลอย่างไรให้ถูกกฎหมาย โดยจีนได้สร้างระบบป้องกันข้อมูลสุดเข้มงวด บังคับให้บริษัทจัดระดับความสำคัญของข้อมูลทางการค้า โดยดูจากผลกระทบต่อความมั่นคงและประโยชน์สาธารณะ ใครจะส่งข้อมูล “สำคัญ” ออกนอกจีน ต้องผ่านด่านหินสามขั้น: ตรวจสอบภายในก่อน ขออนุมัติจากสำนักงานบริหารไซเบอร์สเปซของจีน (Cyberspace Administration of China – CAC) ซึ่งหน้าที่ควบคุมทุกอย่างในโลกออนไลน์จีน ตั้งแต่เนื้อหาเว็บไซต์ ความปลอดภัยทางไซเบอร์ไปจนถึงการไหลเวียนของข้อมูลข้ามพรมแดน ภายใต้กฎหมาย DSL ใหม่ และอาจต้องผ่านหน่วยงานอื่นอีก ทำผิด? เตรียมเจอค่าปรับสาหัส!

DSL จึงเป็นเสมือนกำแพงดิจิทัลที่จีนสร้างขึ้น แสดงให้เห็นว่าจีนจริงจังแค่ไหนกับการควบคุมและคุ้มครองข้อมูลสำคัญ รวมถึงการกำกับดูแลการไหลเวียนของข้อมูลข้ามประเทศ ใครทำธุรกิจในจีน ต้องปรับตัวให้ทันกับกฎใหม่นี้ หากไม่อยากเจอปัญหาใหญ่ในการดำเนินธุรกิจ

ตัวอย่าง หน่วยงานกำกับดูแลความเป็นส่วนตัวและการป้องกันข้อมูล

DPI: ผู้พิทักษ์สิทธิดิจิทัลแห่งยุโรปเหนือ

หน่วยงานตรวจสอบการคุ้มครองข้อมูลของเอสโตเนีย (Estonian Data Protection Inspectorate: DPI) เป็นหน่วยงานที่ทำหน้าที่ตามกฎหมายสำคัญสามฉบับ ได้แก่ พระราชบัญญัติคุ้มครองข้อมูล พระราชบัญญัติข้อมูลข่าวสารสาธารณะ และพระราชบัญญัติการสื่อสารอิเล็กทรอนิกส์ ภารกิจหลักของ DPI คือการปกป้องสิทธิตามรัฐธรรมนูญของประชาชน ซึ่งรวมถึงสิทธิในการรับรู้กิจกรรมของรัฐ สิทธิความเป็นส่วนตัวของชีวิตครอบครัว และสิทธิในการเข้าถึงข้อมูลของตนเอง นอกจากนี้ DPI ยังมีบทบาทสำคัญในการให้ความรู้แก่ทุกภาคส่วนเกี่ยวกับการคุ้มครองข้อมูล มีอำนาจในการดำเนินคดีอาญาและลงโทษผู้ที่ละเมิดกฎหมาย รวมทั้งทำหน้าที่ประสานงานกับองค์กรระหว่างประเทศด้านการคุ้มครองข้อมูล ด้วยบทบาทที่หลากหลายนี้ DPI จึงเป็นทั้งผู้ปกป้อง ผู้ให้ความรู้ และผู้บังคับใช้กฎหมายด้านข้อมูลส่วนบุคคลของเอสโตเนีย ทำให้ประเทศนี้มีระบบการคุ้มครองข้อมูลที่เข้มแข็ง

หน่วยงานกำกับดูแลข้อมูลแอฟริกาใต้: ผู้พิทักษ์ความเป็นส่วนตัวแห่งแอฟริกา

หน่วยงานกำกับดูแลข้อมูลของแอฟริกาใต้ถูกจัดตั้งขึ้นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (POPI Act) เป็นองค์กรอิสระที่แต่งตั้งโดยประธานาธิบดีตามคำแนะนำของสภาแห่งชาติ ผ่านการเสนอชื่อจากคณะกรรมการที่มีตัวแทนจากทุกพรรคการเมือง หน่วยงานนี้รับผิดชอบโดยตรงต่อสภาแห่งชาติ และมีภารกิจหลักในการปกป้องสิทธิความเป็นส่วนตัวของประชาชนชาวแอฟริกาใต้

บทบาทของหน่วยงานนี้ครอบคลุมหลายด้าน ตั้งแต่การให้ความรู้แก่สาธารณชน การติดตามและบังคับใช้กฎหมาย การปรึกษาหารือกับผู้มีส่วนได้ส่วนเสีย การจัดการข้อร้องเรียน การทำวิจัย การออกหลักจรรยาบรรณและแนวทางปฏิบัติ ไปจนถึงการส่งเสริมความร่วมมือระหว่างประเทศ และการติดตามการใช้รหัสประจำตัวของเจ้าของข้อมูล ทั้งหมดนี้เพื่อสร้างระบบการคุ้มครองข้อมูลส่วนบุคคลที่แข็งแกร่งและครอบคลุมสำหรับแอฟริกาใต้

ICO: แชมเปี้ยนคุ้มครองข้อมูลแห่งสหราชอาณาจักร

สำนักงานคณะกรรมการข้อมูลข่าวสารแห่งสหราชอาณาจักร (Information Commissioner's Office: ICO) เป็นองค์กรอิสระที่ทำหน้าที่เป็นผู้พิทักษ์สิทธิด้านข้อมูลของชาวอังกฤษ โดยมีภารกิจสำคัญคือการสร้างสมดุลระหว่างความโปร่งใสของรัฐบาลและการปกป้องความเป็นส่วนตัวของประชาชน แม้จะได้รับเงินทุนจากกระทรวงดิจิทัล วัฒนธรรม สื่อ และกีฬา แต่ ICO ไม่ใช่หน่วยงานราชการ ทำให้สามารถทำงานได้อย่างอิสระและมีประสิทธิภาพ ด้วยทีมงานกว่า 500 คน ICO จัดการกับข้อร้องเรียนด้านข้อมูลนับหมื่นรายต่อปี

ICO ไม่ใช่เสือกระดาษ! บริษัทที่ละเมิดกฎอาจเจอค่าปรับหลายล้าน ในปี 2019/20 ICO ตอบคำถามเกี่ยวกับการคุ้มครองข้อมูลถึง 39,000 รายการ จัดการกับเรื่องการโทรและส่งข้อความรบกวนมากกว่า 102,000 ครั้ง และตอบคำขอข้อมูลเสรีภาพอีก 6,421 รายการ ICO จึงเป็นทั้งโล่และดาบในการปกป้องสิทธิด้านข้อมูลของชาวอังกฤษ ทำให้สหราชอาณาจักรเป็นหนึ่งในผู้นำด้านการคุ้มครองข้อมูลของโลก

9. ถอดบทเรียนจาก GDPR

ภายหลัง GDPR เริ่มบังคับใช้เมื่อวันที่ 25 พฤษภาคม 2561 ได้กลายเป็นจุดเปลี่ยนสำคัญในการคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรป โดยให้ความสำคัญกับสิทธิมนุษยชนในการปกป้องข้อมูล และเพิ่มอำนาจให้กับพลเมืองในการควบคุมข้อมูลส่วนบุคคลของตนเอง การบังคับใช้ GDPR ทำให้ประชาชนมีความเข้าใจเรื่องสิทธิในการเข้าถึงข้อมูลมากขึ้น และส่งผลให้หน่วยงานคุ้มครองข้อมูลได้รับการร้องเรียนจำนวนมาก ซึ่งสะท้อนถึงความสนใจและความตื่นตัวของสาธารณะในการปกป้องข้อมูลส่วนบุคคล

อย่างไรก็ตาม GDPR ยังเผชิญความท้าทายที่สำคัญ ธุรกิจขนาดเล็กพบว่า GDPR เพิ่มความซับซ้อนในการปฏิบัติตามกฎระเบียบ ขณะเดียวกันก็มีอุปสรรคในการแบ่งปันข้อมูลในอุตสาหกรรมดิจิทัล คณะกรรมาธิการยุโรปกำลังพิจารณามาตรการเพื่อลดอุปสรรคด้านนวัตกรรมที่อาจเกิดจากการบังคับใช้ GDPR แต่ยังต้องติดตามว่าการแก้ไขปัญหาจะมีประสิทธิภาพแค่ไหน การบังคับใช้ GDPR นั้นไม่ได้จำกัดอยู่แค่ในยุโรป แต่มีผลกระทบต่อองค์กรทั่วโลกที่จัดการกับข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรป ซึ่งรวมถึงธุรกิจในเอเชียตะวันออกเฉียงใต้ที่มีการเชื่อมโยงกับยุโรป การปฏิบัติตาม GDPR จึงเป็นกระบวนการที่ครอบคลุมและต้องการการปรับเปลี่ยนทั้งในด้านเทคนิค นโยบาย และวัฒนธรรมองค์กร

นอกจากนี้ยังมีข้อวิจารณ์เกี่ยวกับการบังคับใช้ GDPR ว่ากลไกการบังคับใช้อาจไม่เข้มแข็งพอในการจัดการกับพฤติกรรมที่ไม่ดีของบริษัทใหญ่ และการนำ GDPR ใช้ในประเทศกำลังพัฒนาที่มีปัญหาด้านการบังคับใช้กฎหมายอาจเป็นเรื่องท้าทาย โดยเฉพาะในแง่ของการรักษาสมดุลระหว่างการปกป้องข้อมูลและการสนับสนุนการพัฒนาเทคโนโลยีอย่างยั่งยืน

GDPR: ความท้าทายและผลกระทบที่ธุรกิจต้องรู้

การนำ GDPR มาใช้ได้สร้างความท้าทายใหญ่หลวง โดยเฉพาะต้นทุนการปฏิบัติตามกฎระเบียบที่สูง ซึ่งส่งผลกระทบหนักต่อธุรกิจขนาดกลางและขนาดย่อม ทั้งนี้ GDPR กำหนดข้อกำหนดที่เข้มงวดเกี่ยวกับการเก็บรวบรวม ประมวลผล และจัดเก็บข้อมูล รวมถึงต้องได้รับความยินยอมอย่างชัดแจ้งจากลูกค้า ธุรกิจต้องสามารถตอบสนองต่อคำขอเข้าถึง แก้ไข และลบข้อมูลได้ และห้ามเก็บข้อมูลไว้นานเกินความจำเป็น ส่งผลให้ต้นทุนการปฏิบัติตามกฎระเบียบเพิ่มสูงขึ้นและบีบให้หลายธุรกิจต้องปรับตัว

ข้อกำหนดใหม่เกี่ยวกับการขอความยินยอมแบบ opt-in ทำให้ธุรกิจไม่สามารถติดตามพฤติกรรมของลูกค้าหรือแบ่งปันข้อมูลกับบุคคลที่สามได้โดยไม่ขอความยินยอมอย่างชัดเจน ส่งผลให้ธุรกิจขนาดเล็กที่พึ่งพาข้อมูลในการให้บริการและโฆษณาต้องเก็บข้อมูลน้อยลง ตัวอย่างเช่น ข้อมูลผู้ใช้ในภาคการท่องเที่ยวออนไลน์ลดลง 12.5% หลังจาก GDPR มีผลบังคับใช้

นอกจากนี้ การแบ่งปันข้อมูลยังเป็นอีกหนึ่งข้อจำกัดที่สร้างความยุ่งยาก โดยธุรกิจต้องรับผิดชอบต่อการละเมิดความเป็นส่วนตัวของบุคคลที่สาม และตรวจสอบการปฏิบัติตาม GDPR ของผู้ที่รับข้อมูลไปใช้ การละเมิดอาจนำไปสู่ค่าปรับสูงถึง 20 ล้านยูโร หรือ 4% ของรายได้ทั่วโลก ทำให้เว็บไซต์ในสหภาพยุโรปลดการใช้เทคโนโลยีของบุคคลที่สาม เช่น คุกกี้ ลง 12.8% และบริษัทมักเลือกทำงานกับผู้ให้บริการเทคโนโลยีเว็บรายใหญ่แทน SMEs เนื่องจากสามารถปฏิบัติตามข้อกำหนดที่เข้มงวดของ GDPR ได้ดีกว่า

10. คำถามท้ายตอน

1) โปรดระบุหลักการความเป็นส่วนตัวระหว่างประเทศและกรอบการกำกับดูแลอย่างน้อย 3 ข้อ

2) โปรดระบุหลักการความเป็นส่วนตัวและกรอบการกำกับดูแลที่สำคัญระดับภูมิภาค (SEA)

3) GDPR ของสหภาพยุโรปไม่มีการเข้าถึงนอกอาณาเขต

☐ จริง

☐ เท็จ

4) สหรัฐอเมริกาไม่มีกฎระเบียบด้านความเป็นส่วนตัวในระดับรัฐบาลกลาง

☐ จริง

☐ เท็จ

5) โปรดระบุกฎหมายคุ้มครองข้อมูลที่สำคัญในประเทศจีน

6) ระบุหลักการ 7 ประการของพระราชบัญญัติคุ้มครองข้อมูลของสหราชอาณาจักรปี 2018

ตอนที่ 3 ประเด็นร้อนเรื่องความเป็นส่วนตัวยุคดิจิทัล

เคยสงสัยไหมว่าทำไมบางประเทศถึงแบนแอปดัง หรือทำไมบริษัทเทคยักษ์ใหญ่ถึงต้องเปลี่ยนนโยบายความเป็นส่วนตัวบ่อย ๆ นี่แหละคือโลกแห่งความเป็นส่วนตัวยุคดิจิทัลที่กำลังเปลี่ยนแปลงอย่างรวดเร็ว

ในตอนนี้ เราจะพาคุณดำดิ่งสู่ประเด็นร้อนแรงที่กำลังเขย่าวงการความเป็นส่วนตัวของข้อมูล ตั้งแต่นวัตกรรมล่าสุดไปจนถึงคดีดังที่เปลี่ยนโฉมหน้าของกฎหมาย เรียนรู้ว่าทำไม “แซนด์บ็อกซ์ข้อมูล” ถึงเป็นคำฮิตในวงการเทค และทำไม “ตราประทับความเป็นส่วนตัว” ถึงสำคัญกับธุรกิจยุคใหม่

สิ่งที่จะได้เรียนรู้:

1. รู้จักเทรนด์ใหม่: เจาะลึกนวัตกรรมล่าสุดในวงการความเป็นส่วนตัว
2. เข้าใจข้อจำกัด: รู้ว่าอะไรทำได้ อะไรทำไม่ได้ในโลกดิจิทัล
3. เรียนรู้จากคดีดัง: ดูกรณีศึกษาที่เปลี่ยนโฉมหน้ากฎหมายความเป็นส่วนตัว
4. มองภาพรวม: เข้าใจความเชื่อมโยงระหว่างความเป็นส่วนตัว ความปลอดภัยไซเบอร์ และอาชญากรรมออนไลน์

หลังจบตอนนี้ คุณจะกลายเป็น “ผู้เชี่ยวชาญด้านความเป็นส่วนตัวยุคใหม่” ที่พร้อมจะเข้าใจและรับมือกับความท้าทายในโลกดิจิทัลที่เปลี่ยนแปลงอย่างรวดเร็ว!

1. ข้อจำกัดทางกฎหมายด้านสิทธิความเป็นส่วนตัว: สมดุลระหว่างความมั่นคงและเสรีภาพส่วนบุคคล

คุณเคยนึกสงสัยไหมว่าทำไมบางครั้งรัฐบาลถึงสามารถ “แอบดู” ข้อมูลของเราได้? นี่คือเรื่องราวของความขัดแย้งระหว่างสิทธิส่วนบุคคลและความมั่นคงของชาติ

ในโลกที่ข้อมูลคือพลัง รัฐบาลมักอ้างเหตุผลด้านความปลอดภัยเพื่อเข้าถึงข้อมูลส่วนตัวของเรา แต่พวกเขาทำได้แค่ไหน? และอะไรคือกติกาที่พวกเขาต้องปฏิบัติตาม

เพราะสิทธิความเป็นส่วนตัว ไม่ใช่สิทธิเด็ดขาด!

แม้ว่าเราจะมีสิทธิในความเป็นส่วนตัว แต่นั่นไม่ได้หมายความว่าไม่มีใครสามารถละเมิดได้เลย รัฐบาลสามารถจำกัดสิทธินี้ได้ภายใต้เงื่อนไขบางประการ เช่น กรณีฉุกเฉิน หรือเป็นภัยคุกคามความมั่นคง อย่างไรก็ตาม การจำกัดสิทธินี้ต้องเป็นไปตามหลักเกณฑ์ที่เข้มงวดเราจะพาคุณไปสำรวจ:

- เงื่อนไขที่รัฐบาลต้องพิสูจน์เพื่อ “แอบดู” ข้อมูลของเรา
- มาตรฐานระดับโลกที่ควบคุมการกระทำของรัฐบาล
- วิธีที่เราสามารถปกป้องตัวเองจากการละเมิดสิทธิ

พร้อมแล้วหรือยังที่จะเรียนรู้วิธีรักษาสมดุลระหว่างความปลอดภัยและความเป็นส่วนตัว มาดูกันว่าคุณจะเป็นพลเมืองดิจิทัลที่ฉลาดและรู้เท่าทันได้อย่างไร!

เมื่อรัฐบาลต้องการจำกัดสิทธิความเป็นส่วนตัวของประชาชน ไม่ว่าจะผ่านกฎหมายใดก็ตาม จำเป็นที่จะต้องทำตามมาตรฐานสิทธิมนุษยชนระหว่างประเทศ ซึ่งกำหนดไว้ในเอกสารสำคัญของสหประชาชาติ เช่น มติว่าด้วยความเป็นส่วนตัวในยุคดิจิทัลปี 2014 รายงานของผู้รายงานพิเศษด้านการต่อต้านการก่อการร้าย และรายงานของสำนักงานข้าหลวงใหญ่สิทธิมนุษยชน กฎเกณฑ์เหล่านี้ครอบคลุมประเด็นต่าง ๆ อาทิ การคุ้มครองข้อมูล ความปลอดภัยทางไซเบอร์ อาชญากรรมทางไซเบอร์ และการสอดแนมทางดิจิทัล โดยมุ่งเน้นให้การจำกัดสิทธิต้องชอบด้วยกฎหมาย จำเป็น และได้สัดส่วน ทั้งนี้ เพื่อรักษาสมดุลระหว่างความมั่นคงของชาติและสิทธิส่วนบุคคลของประชาชน ช่วยให้มั่นใจว่าแม้ในยามฉุกเฉิน สิทธิพื้นฐานของประชาชนก็ยังได้รับการคุ้มครองอย่างเหมาะสม

กฎเหล็กที่พวกเขาต้องปฏิบัติตามอย่างเคร่งครัดเลยล่ะ มาดูกันว่ามีอะไรบ้าง!

เหตุผลต้องชัด ไม่ใช่อยากดูก็ดู! (วัตถุประสงค์ที่ชอบธรรม) รัฐบาลจะแอบดูข้อมูลของเราไม่ได้ถ้าไม่มีเหตุผลสำคัญจริง ๆ เช่น ป้องกันประเทศ รักษาความปลอดภัย หรือจับผู้ร้าย ไม่ใช่แค่อยากรู้ว่าเราชอบกินอะไรตอนดึก! และถ้าจะทำ ก็ต้องพิสูจน์ให้ได้ว่าจำเป็นจริง ๆ ไม่มีทางอื่นแล้ว

กฎหมายต้องชัด ไม่คลุมเครือ! (ชอบด้วยกฎหมาย) การจำกัดสิทธิของเราต้องมีกฎหมายรองรับชัดเจน ไม่ใช่แบบ “อาจจะ” หรือ “น่าจะ” และต้องปรับให้ทันสมัยด้วยนะ เพราะเทคโนโลยีมันพัฒนาไวมาก ยิ่งถ้ากฎหมายในประเทศขัดกับกฎหมายระหว่างประเทศ ก็อาจถือว่าผิดได้ด้วย! เห็นไหมล่ะ ไม่ใช่ว่าจะทำอะไรก็ได้

เท่าเทียม ไม่เลือกที่รักมักที่ชัง! (ไม่เลือกปฏิบัติ) กฎต้องใช้กับทุกคนเหมือนกันหมด ไม่ว่าจะรวยจนดำขาว หรือเป็นใคร ต้องไม่มีการเล่นพรรคเล่นพวกหรือกลั่นแกล้งกลุ่มไหนเป็นพิเศษ นี่แหละความยุติธรรม!

พอดี ๆ นะ อย่าให้มากไป! (จำเป็นและได้สัดส่วน) ถ้าจะละเมิดสิทธิเราก็ต้องทำแค่พอดี และต้องขออนุญาตศาลก่อนด้วย ไม่ใช่ว่าอยู่ ๆ ก็มาแอบดู แถมต้องเลือกวิธีที่รบกวนเราน้อยที่สุดด้วย

พิสูจน์ให้ได้ว่าจำเป็นจริง ๆ! (ภาระการพิสูจน์) รัฐบาลต้องพิสูจน์ให้ได้ว่าทำไมถึงต้องจำกัดสิทธิเรา มีหลักฐานอะไร และทำแล้วจะได้ผลจริง ๆ ไม่ใช่แค่คิดเอาเองว่าน่าจะดี

อย่างที่บอก สิทธิความเป็นส่วนตัวไม่ใช่สิทธิเด็ดขาด รัฐบาลหลายแห่งหยิบยกเหตุผลต่าง ๆ เพื่อจำกัดสิทธิความเป็นส่วนตัวได้ เริ่มจากความมั่นคงของชาติ (ความมั่นคงของชาติ) ความปลอดภัยของประชาชน (ความปลอดภัยสาธารณะ) อีกทั้งรัฐบาลยังอ้างว่าต้องดูแลเศรษฐกิจให้แข็งแรง (เสถียรภาพและความอยู่ดีมีสุขทางเศรษฐกิจของประเทศ) นอกจากนี้ ยังสามารถยกการปกป้องสิทธิและเสรีภาพของคนอื่น ๆ ด้วยนะ (การคุ้มครองสิทธิและเสรีภาพของผู้อื่น) หรือเพื่อป้องกันอาชญากรรมและความวุ่นวายในสังคม (การป้องกันความผิดปกติหรืออาชญากรรม) และสุดท้ายรัฐยังสามารถอ้างว่าต้องคุ้มครองสุขภาพและศีลธรรม

ของสังคมด้วย (การคุ้มครองสุขภาพหรือศีลธรรมอันดี) ดังนั้น จึงต้องคอยดูให้ดีว่ารัฐบาลจะไม่ยกเหตุผลเหล่านี้มาใช้อ้างเพื่อละเมิดความเป็นส่วนตัวเรามากจนเกินไป

2. แนวทางการประเมินกฎหมายความเป็นส่วนตัวในยุคดิจิทัล: มองผ่านแว่นสิทธิมนุษยชน

เมื่อรัฐบาลจะออกกฎหมายเกี่ยวกับความปลอดภัยทางไซเบอร์หรือการคุ้มครองข้อมูล พวกเขาควรใช้แนวคิดที่เรียกว่า “แนวทางสิทธิมนุษยชน” หรือ HRBA (Human Rights-Based Approach) มาเป็นหลักในการร่างกฎหมาย แนวคิดนี้เน้นให้สิทธิมนุษยชนเป็นหัวใจสำคัญของการกำหนดนโยบายและร่างกฎหมาย

หลักการสำคัญของ HRBA มีดังนี้:

1. ให้ประชาชนมีส่วนร่วม
2. รัฐบาลต้องรับผิดชอบและโปร่งใส
3. ไม่เลือกปฏิบัติและให้ความเท่าเทียม
4. ให้อำนาจแก่ประชาชน
5. ทุกอย่างต้องถูกต้องตามกฎหมาย

HRBA เป็นเครื่องมือสำคัญในการประเมินว่าข้อจำกัดที่รัฐบาลกำหนดต่อสิทธิความเป็นส่วนตัวนั้นชอบธรรม ชอบด้วยกฎหมาย สอดคล้องกับหลักการไม่เลือกปฏิบัติ และจำเป็นและได้สัดส่วน

นอกจากนี้ ยังควรใช้ **HRBA** ในการประเมินกฎระเบียบดิจิทัลระดับชาติโดยเทียบกับหลักการระหว่างประเทศว่าด้วยการประยุกต์ใช้สิทธิมนุษยชนกับการสอดแนม (International Principles on the Application of Human Rights to Communications Surveillance) ซึ่งมีประเด็นสำคัญดังนี้:

1. การอนุญาตล่วงหน้าโดยศาล ต้องมีผู้พิพากษาที่เชี่ยวชาญด้านเทคโนโลยีและสิทธิมนุษยชน

2. มีวัตถุประสงค์ชอบด้วยกฎหมาย เช่น ป้องกันการก่อการร้ายหรืออาชญากรรมร้ายแรง

3. เหตุผลอันสมควร ต้องมีภัยคุกคามระดับสูงและการสอดแนมมีโอกาสสูงที่จะได้หลักฐานสำคัญ

4. ความถูกต้องตามกฎหมาย ดำเนินการภายในขอบเขตที่กฎหมายกำหนด

5. ความจำเป็น ไม่มีวิธีอื่นที่ละเมิดความเป็นส่วนตัวน้อยกว่า

6. ได้สัดส่วน ขอบเขตและระยะเวลาต้องเหมาะสมกับภัยคุกคาม

7. การแจ้งเรื่อง ผู้ถูกสอดแนมต้องได้รับแจ้งโดยเร็วที่สุด

8. รายงานความโปร่งใส ต้องมีการเปิดเผยข้อมูลต่อสาธารณะ

9. การกำกับดูแลที่เป็นอิสระ ต้องมีกลไกการตรวจสอบที่เป็นอิสระ

ทั้งหมดนี้เพื่อให้แน่ใจว่า แม้รัฐบาลจะมีเหตุผลในการจำกัดสิทธิความเป็นส่วนตัว แต่ก็ยังต้องทำอย่างระมัดระวังและเคารพสิทธิมนุษยชนของประชาชน

3. นวัตกรรมการกำกับดูแลความเป็นส่วนตัวของข้อมูล

ในโลกที่เทคโนโลยีพัฒนาไปอย่างรวดเร็ว รัฐบาลทั่วโลกกำลังเผชิญความท้าทายในการออกกฎหมายให้ทันกับการเปลี่ยนแปลง โดยเฉพาะในเรื่องการดูแลข้อมูลและความเป็นส่วนตัว เพราะบริษัทเทคโนโลยีมีอำนาจควบคุมข้อมูลของเรามากขึ้นเรื่อย ๆ เพื่อแก้ปัญหานี้ หลายประเทศได้นำวิธีการใหม่ ๆ มาใช้ในการกำกับดูแลข้อมูล เช่น:

1. Data sandboxes: พื้นที่ทดลองใช้กฎใหม่ ๆ ก่อนนำไปใช้จริง เช่น สหราชอาณาจักร นอร์เวย์ แคนาดา สิงคโปร์ และโคลอมเบีย

2. Data trusts: องค์กรที่ดูแลข้อมูลแทนเจ้าของข้อมูล

3. Privacy seals: เครื่องหมายรับรองว่าองค์กรปกป้องความเป็นส่วนตัวได้ดี

4. Certification Schemes: โครงการรับรองมาตรฐาน การรับรองว่าองค์กรทำตามมาตรฐานการคุ้มครองข้อมูล

นอกจากนี้ ยังมีแนวคิดใหม่ๆ ที่น่าสนใจ เช่น สหกรณ์ข้อมูลที่สมาชิกเป็นเจ้าของร่วมกัน (Data cooperatives) พื้นที่แบ่งปันข้อมูลเพื่อประโยชน์ส่วนรวม (Data commons) และ ตลาดซื้อขายข้อมูล (Data marketplaces) วิธีการเหล่านี้ช่วยให้การกำกับดูแลข้อมูลยืดหยุ่นและตอบสนองต่อการเปลี่ยนแปลงได้ดีกว่า โดยไม่ต้องพึ่งพากฎระเบียบที่เข้มงวดตลอดเวลา

นักกฎหมายและองค์กรภาคประชาสังคมในเอเชียตะวันออกเฉียงใต้ควรรู้จักวิธีการเหล่านี้ เพราะมันอาจเป็นทางเลือกที่ดีในการคุ้มครองข้อมูลของประชาชนในยุคดิจิทัล

สิ่งสำคัญคือ เราต้องหาวิธีที่ทำให้การแบ่งปันและใช้ข้อมูลเป็นประชาธิปไตยมากขึ้น ให้ประชาชนมีอำนาจในการควบคุมข้อมูลของตัวเองมากขึ้น ไม่ใช่ปล่อยให้บริษัทใหญ่ๆ ควบคุมแต่เพียงผู้เดียว

ประเด็นอภิปราย (15 นาที): อ่านกรณีศึกษาด้านล่าง และอภิปรายว่ามีแนวทางการทดลองด้านการควบคุมดูแลข้อมูลที่คล้ายกันในเขตอำนาจหรือประเทศตนหรือไม่

นวัตกรรมการกำกับดูแล: การใช้ Regulatory Sandbox สำหรับข้อมูลเพื่อยกระดับกฎหมายคุ้มครองข้อมูลในสิงคโปร์ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ของสิงคโปร์ได้เปิดตัวแซนด์บ็อกซ์กฎระเบียบสำหรับข้อมูลในปี 2017 โดยดำเนินการร่วมกับหน่วยงานพัฒนาสื่อสารสนเทศ (Infocomm Media Development Authority: IMDA) และได้ร่วมมือกับบริษัทกว่า 30 แห่ง ภายในปี 2019 แซนด์บ็อกซ์นี้ประกอบด้วย 3 ขั้นตอน:

1. การมีส่วนร่วม: หารือกับองค์กรที่ใช้เทคโนโลยีใหม่ เช่น AI และบล็อกเชน เพื่อดูว่ากฎระเบียบการคุ้มครองข้อมูลถูกนำไปใช้อย่างไร

2. การให้คำแนะนำ: หากเทคโนโลยีใหม่สร้างช่องโหว่ในกฎระเบียบที่มีอยู่ ผู้กำกับดูแลสามารถออกคำแนะนำเฉพาะได้

3. การสร้างต้นแบบนโยบาย: ผู้กำกับดูแลร่วมมือกับภาคอุตสาหกรรมเพื่อสร้างนโยบายใหม่ที่แก้ไขช่องว่างที่พบ

ตัวอย่างเช่น องค์กรธุรกิจได้ระบุช่องว่างในการใช้ข้อมูลส่วนบุคคลเพื่อนวัตกรรมทางธุรกิจ ซึ่งนำไปสู่การร่วมกันร่างข้อเสนอนโยบายใหม่ระหว่าง PDPC กับคณะกรรมการที่นำโดยภาคเอกชน

ประโยชน์ที่ได้รับ: บริษัทได้รับความชัดเจนในการใช้เทคโนโลยีใหม่สำหรับประมวลผลข้อมูล และ PDPC มีความมั่นใจมากขึ้นในการปรับนโยบายคุ้มครองข้อมูลให้ทันสมัยและมีประสิทธิภาพ

ความเสี่ยง: การ “สร้างต้นแบบนโยบาย” อาจเอื้อประโยชน์ให้ภาคธุรกิจมากเกินไป เนื่องจากผู้กำกับดูแลทำหน้าที่แทนประชาชนและผู้ใช้ ทำให้การรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียอื่น ๆ เกิดขึ้นช้า ซึ่งอาจเสียเปรียบต่อผลประโยชน์ของกลุ่มที่ต้องการจำกัดการใช้ข้อมูลเพื่อปกป้องความเป็นส่วนตัว

ที่มา: Zee Kin, Y. (2019), Keynote Speech by Deputy Commissioner at AI and Commercial Law: Re-imagining Trust Governance and Private Law Rules, Singapore Management University Blog.

แซนด์บ็อกซ์ข้อมูลข้ามพรมแดน: ทางออกใหม่สู่การแลกเปลี่ยนข้อมูลระหว่างประเทศ

คุณอาจเคยสงสัยว่าทำไมการส่งข้อมูลข้ามประเทศถึงยุ่งยาก นั่นเป็นเพราะแต่ละประเทศมีกฎหมายและระเบียบที่แตกต่างกัน ทำให้การแลกเปลี่ยนข้อมูลเป็นเรื่องซับซ้อน แต่ตอนนี้มีแนวคิดใหม่ที่น่าสนใจมาก นั่นคือ “แซนด์บ็อกซ์กฎระเบียบข้อมูลข้ามพรมแดน”

Q: แล้ว “แซนด์บ็อกซ์” คืออะไร?

A: ให้ลองคิดว่ามันเหมือนกับสนามทดลองขนาดใหญ่ที่ประเทศต่าง ๆ สามารถมาร่วมกันทดสอบวิธีการแลกเปลี่ยนข้อมูลแบบใหม่ ๆ โดยไม่ต้องกังวลกับกฎระเบียบที่เข้มงวดมากเกินไป

ข้อดีของแซนด์บ็อกซ์คือมันช่วยลดความยุ่งยากในการส่งข้อมูลข้ามประเทศ ทำให้กฎระเบียบระหว่างประเทศสอดคล้องกันมากขึ้น และส่งเสริมความร่วมมือระหว่างผู้เชี่ยวชาญหลายสาขา

ในปี 2019 อาเซียนและ GSMA (สมาคมผู้ให้บริการมือถือระดับโลก) ได้เสนอไอเดียนี้ โดยเรียกว่า “ASEAN-GSMA Regulatory Pilot Space for Cross-Border Data Flows” โดยมีเป้าหมายให้ประเทศในเอเชีย-แปซิฟิกสามารถแลกเปลี่ยนข้อมูลกันได้สะดวกขึ้น

แนวคิดนี้สอดคล้องกับกลยุทธ์ของอาเซียนสองอย่าง ได้แก่ 1) กรอบการทำงานสำหรับการจำแนกข้อมูลอาเซียน (นำโดยอินโดนีเซีย) และ 2) กลไกการไหลเวียนข้อมูลข้ามพรมแดนของอาเซียน (นำโดยสิงคโปร์)

แม้ว่าแนวคิดนี้จะยังมีรายละเอียดที่ต้องปรับปรุง แต่ก็ถือเป็นก้าวสำคัญสู่การสร้างระบบแลกเปลี่ยนข้อมูลระหว่างประเทศที่ดีกว่าเดิม ในอนาคต เราอาจเห็นการแลกเปลี่ยนข้อมูลระหว่างประเทศที่ราบรื่นและปลอดภัยมากขึ้น ซึ่งจะส่งผลดีต่อทั้งธุรกิจและประชาชนทั่วไป

ตราประทับความเป็นส่วนตัว: ไม่ใช่ทุกอย่างที่ดูดีจะดีจริง

คุณเคยสังเกตเห็นสัญลักษณ์เล็ก ๆ บนเว็บไซต์ที่บอกว่า “รับรองความเป็นส่วนตัว” ไหม? นั่นแหละคือ “ตราประทับความเป็นส่วนตัว” (Privacy Seals) ที่เรากำลังจะพูดถึง มันเหมือนเครื่องหมายรับรองว่าเว็บไซต์หรือบริการนั้น ๆ ดูแลข้อมูลส่วนตัวของคุณตามมาตรฐานที่กำหนด เปรียบเสมือนเป็นเหมือนสัญญาณบอกว่า “เชื่อใจเราได้นะ!” อย่างไรก็ดี การได้รับการรับรองก็ไม่ได้หมายความว่ามันจะสวยหรูอย่างที่ว่า

เนื่องจากหลายตราประทับขาดความโปร่งใส ไม่บอกว่าใครเป็นสมาชิก หรือตรวจสอบยังไง บางบริษัทที่ให้ตราประทับก็หายตัวไปเฉย ๆ นอกจากนี้ ยังเคยมีกรณีฉ้อโกง เช่น TRUSTe ในสหรัฐฯ โดนปรับ 200,000 ดอลลาร์เพราะหลอกลวงผู้บริโภค ทำไมมันถึงไม่ได้ผล? ในประเทศที่กฎหมายคุ้มครองข้อมูลยังไม่เข้มแข็ง ตราประทับแบบนี้ก็ไม่ช่วยอะไรมาก มันควรเป็นแค่ตัวเสริม ไม่ใช่ตัวแทนกฎหมายจริง ๆ สุดท้ายแล้ว มันไม่ได้ช่วยคุ้มครองผู้บริโภคได้จริงแล้วเราควรทำยังไง? แทนที่จะหวังพึ่งตราประทับพวกนี้ เราควรผลักดันให้มีกฎหมายคุ้มครองข้อมูลที่เข้มแข็งและบังคับใช้จริงจัง นั่นแหละคือวิธีที่จะปกป้องความเป็นส่วนตัวของเราได้ดีที่สุด

อย่าเชื่อแค่เพราะเห็นตราประทับสวย ๆ แต่ต้องดูว่ากฎหมายและการบังคับใช้เป็นยังไงด้วย นั่นแหละสำคัญกว่า!

แผนการรับรองมาตรฐานความเป็นส่วนตัว: ทางเลือกใหม่ในการคุ้มครองข้อมูล

ในโลกธุรกิจปัจจุบัน บางบริษัทดูเหมือนจะใส่ใจเรื่องความเป็นส่วนตัวของลูกค้ามากเป็นพิเศษ นั่นอาจเป็นเพราะพวกเขาได้รับ “การรับรองมาตรฐานความเป็นส่วนตัว” นั่นเอง! แผนการรับรองมาตรฐานนี้เป็นวิธีที่รัฐบาลใช้กระตุ้นให้บริษัทต่างๆ ใส่ใจเรื่องความเป็นส่วนตัวของข้อมูลมากขึ้น โดยมอบสิ่งจูงใจบางอย่างให้

ตัวอย่างเช่น ในเกาหลีใต้ บริษัทที่ได้รับการรับรองอาจได้รับการลดหย่อนค่าปรับหรือผ่อนผันการลงโทษ หากเกิดปัญหาข้อมูลรั่วไหล ส่วนในสหภาพยุโรป กฎหมาย GDPR ก็สนับสนุนระบบการรับรองแบบนี้เช่นกัน โดยช่วยให้บริษัทสามารถแสดงว่าพวกเขาทำตามกฎหมายอย่างเคร่งครัด และช่วยให้ผู้บริโภคสามารถเลือกใช้บริการที่ปกป้องข้อมูลของพวกเขาได้ดีที่สุด

นอกจากนี้ ระบบนี้ยังอาจใช้ตรวจสอบมาตรฐานการจัดการข้อมูลใหม่ ๆ ในระดับสหภาพยุโรป และช่วยให้มั่นใจว่าการส่งข้อมูลระหว่างประเทศมีความปลอดภัยเพียงพอ อย่างไรก็ตาม เราไม่ควรเชื่อถือมันโดยไม่ตั้งคำถาม ต้องคอยดูด้วยว่าการรับรองนั้นมีความน่าเชื่อถือแค่ไหน และบริษัทปฏิบัติตามมาตรฐานจริงหรือไม่

ประเด็นการอภิปราย (15 นาที) อ่านข้อความที่ตัดตอนมาจาก Guardian เกี่ยวกับเรื่องอื้อฉาวของ TRUSTe และหารือเกี่ยวกับวิธีจัดการเรื่องนี้ในระบบกฎหมายของตนเอง

"TRUSTe ถูกปรับ 200,000 ดอลลาร์สำหรับตราประทับความปลอดภัยบนเว็บที่ทำให้เข้าใจผิด New York Times, Apple และเว็บไซต์ขนาดใหญ่อื่น ๆ ใช้ตราประทับการอนุมัติของบริษัท แต่ FTC วิพากษ์วิจารณ์การตรวจสอบของบริษัท

คณะกรรมาธิการการค้าแห่งสหพันธรัฐ (FTC) ของสหรัฐอเมริกาสั่งปรับ TRUSTe ในฐานะผู้ให้บริการการรับรองความเป็นส่วนตัวสำหรับธุรกิจออนไลน์ 200,000 ดอลลาร์ หลังจากที่ผู้ใช้ถูกชักจูงให้เชื่อว่ากำลังทำการตรวจสอบที่เหมาะสมกับผู้ที่ได้รับการอนุมัติ แม้ว่าจะมีการอ้างว่าทุกเว็บไซต์ แอป และบริการคลาวด์ที่ได้รับ TRUSTe Certified Privacy Seal จะต้องได้รับการประเมินใหม่ทุกปี แต่อย่างน้อย 1,000 กรณีไม่มีการประเมินให้เกิดขึ้นระหว่างปี 2549 ถึง 2556"

ที่มา: https://www.theguardian.com/technology/2014/nov/18/truste-fine-web-security-seals

แนวทางการกำกับดูแลข้อมูลแบบใหม่: กองทุนทรัสต์ข้อมูล

ในยุคที่ข้อมูลกลายเป็นทรัพยากรสำคัญ เราต้องหาวิธีจัดการที่ทั้งมีประสิทธิภาพและเป็นธรรม นี่คือที่มาของแนวคิด **"กองทุนทรัสต์ข้อมูล"** หรือ **Data Trusts** ตามคำจำกัดความของสถาบันOpen Data Institute มันคือ "โครงสร้างทางกฎหมายที่ให้การดูแลข้อมูลอย่างเป็นอิสระ" ว่าง่าย ๆ ก็คือการมีคนกลางที่เราเรียกว่า "ทรัสตี" มาช่วยดูแลและตัดสินใจเกี่ยวกับข้อมูลแทนเรา

กองทุนทรัสต์ข้อมูลทำงานโดยให้เจ้าของข้อมูล (อาจเป็นคนหรือองค์กร) มอบความไว้วางใจให้ทรัสตีดูแลข้อมูล ทรัสตีมีหน้าที่ตามกฎหมายต้องทำตามข้อตกลงที่วางไว้ ไม่เอาไปใช้เพื่อประโยชน์ส่วนตัว และสามารถรวมข้อมูลจากหลายแหล่ง รวมทั้งเจรจาเรื่องการเข้าถึงข้อมูลแทนกลุ่มเจ้าของได้ ข้อดีคือช่วยให้การจัดการข้อมูลมีความเป็นกลางและโปร่งใสมากขึ้น ปกป้องผลประโยชน์ของเจ้าของข้อมูลได้ดีกว่า และเพิ่มอำนาจต่อรองให้กับกลุ่มเล็ก ๆ เมื่อต้องเจรจากับบริษัทใหญ่

อย่างไรก็ตาม กฎหมายทรัสต์แบบนี้มีเฉพาะบางประเทศ เช่น อังกฤษ อเมริกา แคนาดา แต่ก็ไม่ต้องกังวล เพราะแนวคิดการมีตัวแทนดูแลผลประโยชน์แทนคนอื่นมีอยู่ทั่วไปในหลายประเทศ แม้จะไม่เรียกว่า "ทรัสต์" ก็ตาม

กองทุนทรัสต์ข้อมูลถือได้ว่าเป็นแนวคิดใหม่ที่น่าสนใจในการจัดการข้อมูลในยุคดิจิทัล โดยกำหนดหน้าที่ "ความไว้วางใจ" ให้กับองค์กรที่ดูแลข้อมูล ข้อดีคือ มันใช้โครงสร้างกฎหมายเอกชนที่มีอยู่แล้ว โดยไม่ต้องพึ่งรัฐบาลมากเกินไป และอาจช่วยปกป้องสิทธิของประชาชนได้ดีขึ้น

มีการทดลองใช้แนวคิดนี้ทั้งในภาครัฐและเอกชน เช่น ในการวิจัยทางการแพทย์ เพื่อจัดการข้อมูลผู้ป่วยอย่างรอบคอบ แต่ตัวอย่างที่น่าสนใจคือ "ทรัสต์ข้อมูลเมือง" ในโครงการ Sidewalk Labs ที่โตรอนโต แม้ว่าในที่สุดจะถูกยกเลิก แต่ก็แสดงให้เห็นถึงความพยายามในการใช้แนวคิดนี้กับข้อมูลในเมืองอัจฉริยะ

อย่างไรก็ตาม แนวคิดนี้ยังมีคำถามมากมายที่ยังไม่มีคำตอบ เช่น จะจัดการหรือทำให้ทรัสต์รับผิดชอบได้อย่างไร จะมีการแข่งขันระหว่างทรัสต์หรือไม่ ผู้เก็บข้อมูลสามารถเป็นทรัสตีที่น่าเชื่อถือได้หรือไม่ คำถามเหล่านี้แสดงให้เห็นว่า แม้จะเป็นแนวคิดที่น่าสนใจ แต่ก็ยังต้องการการศึกษาและพัฒนาอีกมากเพื่อให้เกิดความชัดเจนและการยอมรับในวงกว้าง

สหกรณ์ข้อมูล: พลังประชาชนในยุคดิจิทัล

สหกรณ์ข้อมูลเป็นแนวคิดใหม่ที่น่าตื่นเต้นในการจัดการข้อมูลแบบประชาธิปไตย แทนที่จะปล่อยให้บริษัทใหญ่ๆ ควบคุมข้อมูลของเรา สหกรณ์ข้อมูลให้อำนาจแก่ผู้ใช้ในการเป็นเจ้าของและควบคุมข้อมูลของตนเอง

ลองนึกภาพว่า แทนที่จะให้ Uber เป็นคนเก็บและใช้ข้อมูลของคนขับรถ คนขับรถสามารถรวมตัวกันเป็นสหกรณ์และจัดการข้อมูลของตัวเองได้ นี่คือสิ่งที่ Driver's Seat กำลังทำ พวกเขารวบรวมข้อมูลการขับรถและขายให้กับหน่วยงานท้องถิ่น โดยคนขับได้รับส่วนแบ่งรายได้ด้วย

ข้อดีของสหกรณ์ข้อมูลคือ:

1. ให้อำนาจแก่ผู้ใช้: เราเป็นเจ้าของและควบคุมข้อมูลของเราเอง
2. แบ่งปันผลประโยชน์: รายได้จากข้อมูลถูกแบ่งปันอย่างเป็นธรรม
3. ความโปร่งใส: ทุกคนรู้ว่าข้อมูลถูกใช้อย่างไร
4. ประชาธิปไตย: สมาชิกมีสิทธิออกเสียงในการตัดสินใจสำคัญ

แนวคิดนี้ไม่ได้จำกัดอยู่แค่การขนส่ง มีการนำไปใช้ในหลายอุตสาหกรรม เช่น ธนาคาร และการเกษตร นอกจากนี้ ยังมีนักพัฒนาซอฟต์แวร์หลายรายที่กำลังสร้างเครื่องมือเพื่อสนับสนุนสหกรณ์ข้อมูล

แม้ว่าสหกรณ์ข้อมูลจะเป็นแนวคิดใหม่และยังมีความท้าทายในการนำไปปฏิบัติ แต่มันเป็นก้าวสำคัญในการสร้างระบบเศรษฐกิจดิจิทัลที่เป็นธรรมและเป็นประชาธิปไตยมากขึ้น ในอนาคต เราอาจเห็นสหกรณ์ข้อมูลเป็นทางเลือกที่แข็งแกร่งสำหรับแพลตฟอร์มขนาดใหญ่ ให้อำนาจแก่ผู้ใช้ในการควบคุมข้อมูลและชะตากรรมดิจิทัลของตนเอง

คลังข้อมูลสาธารณะ: ข้อมูลเพื่อทุกคน

คลังข้อมูลสาธารณะ หรือ **Data Commons** เป็นแนวคิดที่น่าสนใจในการจัดการข้อมูลแบบเปิดกว้างและเป็นประชาธิปไตย ลองนึกภาพว่ามันเป็นเหมือนสวนสาธารณะของข้อมูล ที่ทุกคนสามารถเข้าไปใช้และมีส่วนร่วมได้

ข้อดีของคลังข้อมูลสาธารณะ คือ

1. ความเท่าเทียม: ทุกคนสามารถเข้าถึงข้อมูลได้ ไม่ว่าจะรวยหรือจน
2. การมีส่วนร่วมของชุมชน: ผู้คนสามารถร่วมกันสร้างและดูแลข้อมูล
3. ประโยชน์สาธารณะ: มุ่งเน้นการใช้ข้อมูลเพื่อประโยชน์ของส่วนรวม
4. ความยืดหยุ่น: สามารถปรับใช้ได้กับกฎหมายและระบบการปกครองที่หลากหลาย

ตัวอย่างที่เราคุ้นเคย เช่น Wikipedia สารานุกรมออนไลน์ที่ทุกคนสามารถแก้ไขได้ OpenStreetMap แผนที่ออนไลน์ที่ผู้ใช้สร้างขึ้นเอง และ Wikidata ฐานข้อมูลความรู้ที่มนุษย์และคอมพิวเตอร์อ่านได้

คลังข้อมูลสาธารณะไม่ได้เพิ่งเกิดขึ้น มันมีบทบาทสำคัญในการพัฒนาอินเทอร์เน็ตมาตั้งแต่ยุค 90 แล้ว และยังคงเติบโตอย่างต่อเนื่อง สิ่งสำคัญ คือ คลังข้อมูลสาธารณะต้องรับประกันความถูกต้องของข้อมูล ปกป้องความเป็นส่วนตัวของผู้ให้ข้อมูล และมีกฎการใช้งานที่ชัดเจน บางครั้งอาจต้องจำกัดการเข้าถึงบางส่วนเพื่อปกป้องข้อมูลที่ละเอียดอ่อน

แนวคิดนี้แสดงให้เห็นว่า เราสามารถสร้างระบบการจัดการข้อมูลที่เปิดกว้าง เป็นประโยชน์ต่อสาธารณะ และให้ทุกคนมีส่วนร่วมได้ ในยุคที่ข้อมูลมีความสำคัญมากขึ้นเรื่อย ๆ คลังข้อมูลสาธารณะอาจเป็นทางออกที่ช่วยให้เราใช้ประโยชน์จากข้อมูลได้อย่างทั่วถึงและเป็นธรรมมากขึ้น

การทำงานร่วมกันของข้อมูล พลังแห่งการแบ่งปันเพื่อประโยชน์ส่วนรวม

การทำงานร่วมกันของข้อมูล (Data Collaborative) เป็นแนวคิดใหม่ที่น่าสนใจในการจัดการและใช้ประโยชน์จากข้อมูลเพื่อสังคม โดยเป็นความร่วมมือระหว่างภาครัฐและเอกชนในการแบ่งปันข้อมูลเพื่อประโยชน์สาธารณะ แตกต่างจากการเปิดเผยข้อมูลทั่วไป เพราะรวมถึงการแบ่งปันข้อมูลที่อาจเป็นความลับหรือมีความละเอียดอ่อน เพื่อนำไปใช้ในการวิจัยหรือกำหนดนโยบาย

ตัวอย่างที่น่าสนใจ เช่น บริษัทเรียกรถส่วนตัวแบ่งปันข้อมูลการเดินทางเพื่อช่วยวางแผนระบบขนส่งของเมือง หรือองค์กรต่างๆ แบ่งปันข้อมูลให้สหประชาชาติเพื่อรับมือกับภัยพิบัติ นอกจากนี้ยังมีองค์กรอย่าง SharedStreets ที่พัฒนาซอฟต์แวร์เปิดสำหรับแลกเปลี่ยนข้อมูลด้านการขนส่ง และ BrightHive ที่ให้คำปรึกษาด้านกฎหมายและเครื่องมือสำหรับความร่วมมือด้านข้อมูล

การทำงานร่วมกันของข้อมูลทำหน้าที่เป็นผู้ดูแลข้อมูลที่รับผิดชอบเพื่อเพิ่มอำนาจให้กับสมาชิกหรือประชาชนในการแก้ปัญหาสังคม ภาคเอกชนมักเข้าร่วมด้วยเหตุผลด้านรายได้ การวิจัย การปฏิบัติตามกฎระเบียบ ชื่อเสียงหรือความรับผิดชอบต่อสังคม อย่างไรก็ตาม ยังมีข้อกังวลเรื่องความเป็นส่วนตัว ความยินยอม และ ‘อคติข้อมูลขนาดใหญ่’ ที่อาจเกิดขึ้นเมื่อนำข้อมูลไปใช้ในบริบทใหม่

แม้จะมีความท้าทาย แต่การทำงานร่วมกันของข้อมูลมีศักยภาพในการใช้พลังของข้อมูลเพื่อแก้ปัญหาสังคมที่ซับซ้อน โดยสร้างความร่วมมือระหว่างภาครัฐและเอกชน นำไปสู่นวัตกรรมและการพัฒนานโยบายที่ดีขึ้น ในอนาคต เราอาจเห็นรูปแบบนี้เป็นวิธีปกติในการใช้ข้อมูลเพื่อประโยชน์ส่วนรวม

ตลาดข้อมูล (Data Marketplace): การซื้อขายข้อมูลในยุคดิจิทัล

ตลาดข้อมูลเป็นแนวคิดที่น่าสนใจในการจัดการข้อมูลส่วนบุคคลในยุคดิจิทัล มันเป็นแพลตฟอร์มที่ให้ผู้ใช้สามารถขายหรือแลกเปลี่ยนข้อมูลของตนเองเพื่อรับบริการหรือผลประโยชน์อื่นๆ แนวคิดนี้เกิดจากความตระหนักว่าข้อมูลมี “มูลค่า” แต่ยังไม่มีวิธีที่ชัดเจนในการกำหนดราคาหรือควบคุมการเข้าถึงข้อมูล

ประเด็นสำคัญของตลาดข้อมูล:

1. การชดเชยให้ผู้ใช้: เหตุใดผู้ใช้ไม่ควรได้รับค่าตอบแทนจากข้อมูลที่พวกเขาสร้างบนแพลตฟอร์มใหญ่ๆ เช่น Facebook หรือ Instagram

2. ความโปร่งใส: จะสร้างระบบที่ทำงานร่วมกันได้ระหว่างหลายแพลตฟอร์มและแสดงให้เห็นชัดเจนว่าใครเป็นเจ้าของข้อมูลอะไรได้อย่างไร

3. อำนาจต่อรอง: ผู้ใช้สามารถรวมกลุ่มกันเพื่อเพิ่มอำนาจต่อรองได้เหมือนกับแนวคิด “สหภาพข้อมูล”

ตัวอย่างที่น่าสนใจ เช่น Streamr ตลาดที่ช่วยให้ธุรกิจและบุคคลสามารถรวบรวมและขายข้อมูลแบบเรียลไทม์อย่างมีจริยธรรม และ Data Union ในสหรัฐอเมริกา กลุ่มที่สนับสนุนให้ประชาชนมีสิทธิในการเป็นเจ้าของข้อมูลส่วนบุคคลของตนเอง

แนวคิดตลาดข้อมูลนี้เปิดโอกาสให้ผู้ใช้มีส่วนร่วมในการกำหนดมูลค่าและการใช้งานข้อมูลของตนเองมากขึ้น แทนที่จะปล่อยให้บริษัทใหญ่ ๆ เป็นผู้ควบคุมทั้งหมด อย่างไรก็ตาม ยังมีคำถามเกี่ยวกับความเป็นไปได้ในทางปฏิบัติ ความปลอดภัย และผลกระทบทางจริยธรรมที่ต้องพิจารณา

ในอนาคต เราอาจเห็นการพัฒนาของตลาดข้อมูลที่ให้ความสำคัญกับความโปร่งใส การควบคุมโดยผู้ใช้ และการแบ่งปันผลประโยชน์อย่างเป็นธรรม ซึ่งอาจเป็นการเปลี่ยนแปลงครั้งสำคัญในวิธีที่เราจัดการกับข้อมูลส่วนบุคคลในยุคดิจิทัล

4. ความท้าทายความปลอดภัยไซเบอร์ในเอเชียตะวันออกเฉียงใต้

เอเชียตะวันออกเฉียงใต้กำลังก้าวเข้าสู่ยุคเศรษฐกิจดิจิทัลอย่างรวดเร็ว โดยเฉพาะในปี 2022 ที่เทคโนโลยีอย่างเมตาเวิร์ส และ AI เข้ามามีบทบาทสำคัญ ส่งผลให้ธุรกิจออนไลน์และการเงินดิจิทัลเติบโตอย่างก้าวกระโดด มีการคาดการณ์ว่าเศรษฐกิจดิจิทัลของภูมิภาคนี้จะมีมูลค่าสูงถึง 1 ล้านล้านเหรียญสหรัฐภายในปี 2030 การใช้สมาร์ทโฟนในการซื้อขายสินค้าและบริการออนไลน์กลายเป็นเรื่องปกติ ทำให้ธุรกิจต่าง ๆ สนใจเก็บข้อมูลลูกค้าเพื่อนำไปใช้ประโยชน์ทางธุรกิจมากขึ้น

ในขณะเดียวกัน เราเห็นการเกิดขึ้นของ “ซูเปอร์แอป” อย่าง WeChat และ Alipay ที่ครองส่วนแบ่งตลาดการชำระเงินผ่านมือถือในเอเชียถึง 95% รวมถึงการขยายตัวของบริษัทอย่าง Grab และ Tencent ที่เริ่มต้นจากบริการเฉพาะทาง แต่ขยายขอบเขตจนกลายเป็นแพลตฟอร์มที่ให้บริการหลากหลาย ปรากฏการณ์นี้ทำให้เส้นแบ่งระหว่างอุตสาหกรรมต่าง ๆ เริ่มเลือนราง และเกิดการรวมศูนย์ของข้อมูลจำนวนมหาศาล

แต่การเติบโตอย่างรวดเร็วนี้ก็มาพร้อมกับความเสี่ยงด้านความปลอดภัยไซเบอร์ที่เพิ่มขึ้น เราได้เห็นการละเมิดข้อมูลขนาดใหญ่ในหลายประเทศ เช่น ในมาเลเซียที่ข้อมูลส่วนบุคคลของพลเมืองกว่า 13 ล้านคนถูกเปิดเผย ในอินโดนีเซียที่หมายเลขซิมการ์ดกว่า 1 พันล้านหมายเลข ถูกขโมยและนำไปขายในเว็บมืด และในสิงคโปร์ที่ข้อมูลบัญชีผู้ใช้จำนวนมากจากแพลตฟอร์ม Carousell ถูกลักลอบนำไปขาย

สถานการณ์เหล่านี้ชี้ให้เห็นถึงความจำเป็นเร่งด่วนในการพัฒนากฎหมายและมาตรการรักษาความปลอดภัยทางไซเบอร์ที่เข้มแข็ง เพื่อปกป้องข้อมูลส่วนบุคคลและสร้างความเชื่อมั่นในเศรษฐกิจดิจิทัลที่กำลังเติบโตอย่างรวดเร็วในภูมิภาคนี้

กิจกรรม: ดูวิดีโอ "การเปิดเผยการแฮ็ก: เคล็ดลับการค้า" และอภิปรายว่าความเป็นส่วนตัวและการคุ้มครองข้อมูลเกี่ยวข้องกับความปลอดภัยทางไซเบอร์และอาชญากรรมทางไซเบอร์อย่างไร

ที่มา: เดอะการ์เดียน, https://youtu.be/fbevmsPIYDk

กฎหมายคุ้มครองข้อมูล: เกราะป้องกันความเป็นส่วนตัวในยุคดิจิทัล

ในโลกยุคดิจิทัลที่ข้อมูลกลายเป็นทรัพย์สินล้ำค่า การปกป้องความเป็นส่วนตัวของเราจึงสำคัญกว่าที่เคย นี่คือเหตุผลที่กฎหมายคุ้มครองข้อมูลและความปลอดภัยทางไซเบอร์ถูกสร้างขึ้น พวกมันทำหน้าที่เหมือนเกราะป้องกันให้กับข้อมูลส่วนบุคคลของเรา ป้องกันไม่ให้ใครมาแอบดู ขโมย หรือทำลายได้โดยง่าย

กฎหมายเหล่านี้กำหนดมาตรการความปลอดภัยหลายอย่าง เช่น การเข้ารหัสข้อมูล การใช้นามแฝง การรักษาความลับของระบบ และการตรวจสอบความปลอดภัยอย่างสม่ำเสมอ นอกจากนี้ ยังมีแผนรับมือเหตุฉุกเฉิน เพื่อให้แน่ใจว่าข้อมูลของเราจะปลอดภัยแม้ในยามวิกฤต และถ้ามีอะไรผิดปกติเกิดขึ้น กฎหมายก็บังคับให้ผู้ดูแลระบบต้องแจ้งให้เราทราบทันที

ที่สำคัญ กฎหมายยังกำหนดบทลงโทษสำหรับผู้ที่ละเมิดความเป็นส่วนตัวของเรา ไม่ว่าจะเป็นคนดูแลระบบหรือบุคคลภายนอก นี่คือวิธีที่ช่วยให้เรารู้สึกปลอดภัยในการใช้ชีวิตในโลกดิจิทัล แต่ก็อย่าลืมว่า การป้องกันที่ดีที่สุดคือการระมัดระวังตัวของเราเอง กฎหมายอาจเป็นเกราะป้องกัน แต่เราต้องเป็นคนใช้มันอย่างชาญฉลาด

การแจ้งเตือนการละเมิดข้อมูลที่ได้รับคำสั่งจากกฎหมายในเอเชียตะวันออกเฉียงใต้

กฎหมายคุ้มครองข้อมูลในประเทศ SEA กำหนดภาระผูกพันด้านความปลอดภัยกับผู้ควบคุมข้อมูลและผู้ประมวลผลเพื่อคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูล อย่างไรก็ตาม ไม่ใช่ว่าทุกประเทศในเอเชียตะวันออกเฉียงใต้ เช่น มาเลเซีย จะกำหนดข้อกำหนดบังคับเพื่อแจ้งให้เจ้าหน้าที่และเจ้าของข้อมูลทราบถึงการละเมิดข้อมูลในทุกลักษณะ

ในสิงคโปร์ องค์กรต่างๆ ได้รับการกระตุ้นให้แจ้งให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ทราบถึงการละเมิดข้อมูลที่อาจก่อให้เกิดความกังวลของสาธารณชนหรือก่อให้เกิดอันตรายต่อกลุ่มบุคคล PDPC ได้ระบุความตั้งใจที่จะใช้กรอบการแจ้งเตือนการละเมิดข้อมูลที่จำเป็น

ในฟิลิปปินส์ ผู้กำกับดูแลจะต้องได้รับแจ้งภายใน 72 ชั่วโมงหลังจากได้รับข้อมูลหรือมีข้อสงสัยตามสมควรว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น นอกจากนี้ เจ้าของข้อมูลที่ได้รับผลกระทบจะต้องได้รับแจ้งเหตุการณ์ดังกล่าวภายใน 72 ชั่วโมง

ในประเทศไทย ผู้ควบคุมข้อมูลจะต้องรายงานสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงหลังจากทราบถึงการละเมิดข้อมูลที่อาจกระทบต่อสิทธิและเสรีภาพส่วนบุคคล การละเมิดข้อมูลที่ก่อให้เกิดอันตรายต่อสิทธิและเสรีภาพส่วนบุคคลจะต้องถูกรายงานไปยังเจ้าของข้อมูลโดยผู้ควบคุมข้อมูล

ในอินโดนีเซีย ไม่มีข้อกำหนดการแจ้งเตือนสำหรับการละเมิดข้อมูล อย่างไรก็ตาม ผู้ให้บริการระบบอิเล็กทรอนิกส์จะต้องแจ้งให้เจ้าของข้อมูลทราบถึงการละเมิดพร้อมเหตุผลของการฝ่าฝืนภายในสิบสี่วัน

ที่มา: https://www.financierworldwide.com/the-eu-gdprs-impact-on-asean-data-protection-law

การคุ้มครองผู้บริโภคในยุคเศรษฐกิจดิจิทัล

โลกออนไลน์ทุกวันนี้เต็มไปด้วยบริการฟรีที่น่าดึงดูด ไม่ว่าจะเป็นโซเชียลมีเดียอย่าง Facebook หรือเครื่องมือค้นหาอย่าง Google ที่กลายเป็นส่วนสำคัญของชีวิตประจำวันและระบบการค้าออนไลน์ แต่รู้หรือไม่ว่า ทุกครั้งที่เราใช้บริการเหล่านี้ เราก็กำลังแลกข้อมูลส่วนตัวของเราไปโดยไม่รู้ตัว

ธุรกิจต่าง ๆ ใช้ข้อมูลที่เราทิ้งไว้เพื่อโฆษณาสินค้าให้ตรงใจเรามากขึ้น พวกเขาเก็บข้อมูลส่วนตัว ตำแหน่งที่อยู่ ความชอบ ประวัติการค้นหา เครือข่ายสังคม รายชื่อติดต่อ และประวัติการซื้อขายของเรา ทำให้สามารถสร้างโฆษณาที่เฉพาะเจาะจงสำหรับแต่ละคนได้

เทคโนโลยีทำให้การช็อปปิ้งออนไลน์ง่ายขึ้นกว่าที่เคย ลองนึกภาพว่าคุณสามารถสั่งซื้อของด้วยเสียงผ่าน Alexa บนลำโพงอัจฉริยะ Echo ของ Amazon หรือแม้แต่เครื่องซักผ้าของคุณก็สามารถสั่งซื้อผงซักฟอกใหม่ให้โดยอัตโนมัติเมื่อใกล้หมด สะดวกจริงๆ แต่อย่าลืมว่า ความสะดวกสบายเหล่านี้มาพร้อมกับการเก็บข้อมูลของเราอย่างมหาศาล

ระบบการเงินก็เปลี่ยนไปมาก ด้วยบริการอย่าง PayPal และ Alipay ที่ทำให้การชำระเงินออนไลน์ง่ายและปลอดภัยขึ้น นอกจากนี้ ยังมีนวัตกรรม FinTech ที่ทำให้เกิดธนาคารเสมือน การให้สินเชื่อออนไลน์ และการระดมทุนผ่าน “คลาวด์”

ตัวอย่างที่น่าสนใจคือ WeChat ในจีน ที่รวมทุกอย่างไว้ในแอปเดียว ทั้งแชท จ่ายเงิน และช็อปปิ้ง ทำให้การใช้จ่ายง่ายขึ้นมาก แต่ก็ต้องแลกกับการให้ข้อมูลส่วนตัวของเรามากขึ้นเช่นกัน

ทุกครั้งที่เราใช้อินเทอร์เน็ต เราทิ้ง “รอยเท้าดิจิทัล” ไว้ ข้อมูลเหล่านี้ถูกนำไปใช้เพื่อปรับปรุงบริการ แต่บางครั้งก็ถูกใช้ในทางที่เราควบคุมไม่ได้ หลายคนมองว่าการให้ข้อมูลส่วนตัวเป็น “ความจำเป็นที่หลีกเลี่ยงไม่ได้” หากต้องการใช้บริการออนไลน์ โดยมักไม่สามารถเลือกได้ว่าจะให้ข้อมูลใดบ้าง และเมื่อให้ข้อมูลไปแล้ว ก็แทบไม่มีอำนาจควบคุมการใช้งานข้อมูลนั้นอีกต่อไป

การคุ้มครองข้อมูลและการกำกับดูแลที่เหมาะสมจึงเป็นสิ่งสำคัญในการปกป้องผู้บริโภคยุคดิจิทัล เราอาจใช้โปรแกรมตรวจสอบความน่าเชื่อถือของเว็บไซต์หรือแอปพลิเคชันก่อนให้ข้อมูล และควรศึกษาว่าข้อมูลของเราจะถูกนำไปใช้อย่างไร

การฉ้อโกงเว็บไซต์ COPYCAT

ในเดือนมีนาคม 2018 หลังจากการสอบสวนโดยทีมงาน eCrime มาตรฐานการค้าแห่งชาติของสหราชอาณาจักร มีผู้ถูกตัดสินว่ามีความผิดและถูกตัดสินจำคุก 6 รายจากเว็บไซต์ปฏิบัติการที่เลียนแบบเว็บไซต์อย่างเป็นทางการของหน่วยงานและหน่วยงานภาครัฐ 11 แห่ง ผลลัพธ์ของเครื่องมือค้นหายังได้รับการปรับเปลี่ยนเพื่อทำให้เว็บไซต์ดูเป็นของแท้มากขึ้น ผู้ฉ้อโกงจงใจหลอกลวงผู้บริโภคหลายแสนรายให้จ่ายเงินแพงเกินไปสำหรับบริการของรัฐบางรายการ รวมถึงหนังสือเดินทางเล่มใหม่หรือหนังสือเดินทางเล่มใหม่ ใบขับขี่และค่าธรรมเนียมความแออัดของลอนดอน

คนร้ายยังสร้างเว็บไซต์ที่เลียนแบบเว็บไซต์ขอวีซ่าอย่างเป็นทางการของประเทศอื่น ๆ (รวมถึงสหรัฐอเมริกาและตุรกี) ซึ่งนักเดินทางสามารถสมัครและชำระค่าวีซ่าอิเล็กทรอนิกส์เพื่อเยี่ยมชมประเทศเหล่านั้นได้ ในทุกกรณี ไซต์ต่าง ๆ เสนอมูลค่าเพิ่มเติมเพียงเล็กน้อยหรือไม่มีเลยให้กับผู้บริโภคที่ใช้งานไซต์เหล่านั้น เชื่อกันว่านอกจากผู้บริโภคในสหราชอาณาจักรแล้ว พลเมืองอินเดีย ตุรกี และสหรัฐอเมริกายังถูกฉ้อโกงอีกด้วย

ที่มา: NTS (2018), “Six sentenced for large copycat website fraud”, http://bit.ly/2p1gRFR.

กิจกรรม: ดูวิดีโอและอภิปรายว่าสิทธิของผู้บริโภคอาจเปลี่ยนแปลงไปอย่างไรในสภาพแวดล้อมดิจิทัล พวกเขายังอภิปรายว่าการคุ้มครองข้อมูลและความเป็นส่วนตัวเกี่ยวข้องกับสิทธิผู้บริโภคในขอบเขตดิจิทัลอย่างไร

สร้างโลกดิจิทัลที่ผู้บริโภคไว้วางใจได้ (Consumers International)

ที่มา: https://youtu.be/xRmj30iAMZM

5. ดิจิทัลเดือด: คดีระทึกบนเส้นด้ายความเป็นส่วนตัว

ส่วนนี้ให้ภาพรวมของคดีทางกฎหมายที่เกี่ยวข้องกับประเด็นการคุ้มครองข้อมูลและความเป็นส่วนตัวในโลกดิจิทัล

การเป็นสื่อกลางในการติดต่อกับรัฐและการสร้างความโปร่งใสในกิจการสาธารณะ

ในคดี Saket v. Union of India ศาลสูงบอมเบย์ตัดสินว่ากระทรวงข้อมูลข่าวสารและการประชาสัมพันธ์ละเมิดสิทธิความเป็นส่วนตัวของผู้ร้องโดยการเผยแพร่ข้อมูลส่วนบุคคลของผู้ร้องบนเว็บไซต์ของกระทรวงฯ เพื่อตอบสนองต่อคำขอข้อมูล ศาลวินิจฉัยว่าการเผยแพร่ข้อมูลดังกล่าวเป็นการกระทำที่ไม่สมควรและก่อให้เกิดความเสียหายต่อผู้ร้อง อีกทั้งยังอาจส่งผลให้ผู้ร้องรายอื่นในอนาคตไม่กล้ายื่นคำขอภายใต้พระราชบัญญัติสิทธิในข้อมูลข่าวสาร (the Right to Information Act) ค.ศ. 2005 เนื่องจากเกรงว่าข้อมูลส่วนบุคคลของตนจะถูกเปิดเผยในลักษณะเดียวกัน

ระบบระบุตัวตนสาธารณะ

ในปี 2021 ศาลสูงเคนยาได้ตัดสินคดี Nubian Rights Forum and Others v. The Attorney General of Kenya โดยประกาศว่าระบบ NIIMS (National Integrated Identity Management System) ซึ่งเป็นระบบระบุตัวตนดิจิทัลแห่งชาติ เป็นสิ่งที่ไม่ชอบด้วยกฎหมาย ศาลระบุว่าก่อนนำระบบนี้มาใช้ ควรมีการประเมินผลกระทบด้านการคุ้มครองข้อมูลและสร้างกรอบการกำกับดูแลที่เหมาะสม เพื่อลดความกังวลเกี่ยวกับการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล

แพลตฟอร์มออนไลน์และความเป็นส่วนตัวทางดิจิทัล Meta ถูกปรับเป็นเงินทั้งสิ้น 390 ล้านยูโรโดยคณะกรรมการคุ้มครองข้อมูลของไอร์แลนด์ (Data Protection Commission: DPC) หลังจากที่หน่วยงานด้านข้อมูลของสหภาพยุโรปปฏิเสธข้อโต้แย้งของบริษัทที่ว่า ผู้ใช้ยินยอมที่จะรับโฆษณาตามข้อมูลส่วนบุคคลของพวกเขาเมื่อยอมรับข้อกำหนดและเงื่อนไขของแพลตฟอร์มโซเชียลมีเดีย การรวบรวมโปรไฟล์ผู้ใช้ตามกิจกรรมออนไลน์เป็นหัวใจสำคัญของโมเดลธุรกิจของ Facebook และ Instagra ช่วยให้ผู้ลงโฆษณาสามารถกำหนดเป้าหมายผู้ใช้ตามปัจจัยต่างๆ เช่น ความสนใจ พฤติกรรมผู้บริโภค และภูมิศาสตร์

ในตอนแรก DPC สนับสนุนจุดยืนทางกฎหมายของ Meta ที่ว่า “สัญญา” ไม่ได้ละเมิด GDPR ของสหภาพยุโรป แต่ต่อมาได้ประกาศว่าจำเป็นต้องปฏิบัติตามคำแนะนำของคณะกรรมการคุ้มครองข้อมูลแห่งยุโรป ซึ่งประกอบด้วยหน่วยงานด้านความเป็นส่วนตัวของสหภาพยุโรปทั้งหมด

กลุ่มนักเคลื่อนไหวด้านความเป็นส่วนตัว Noyb (ย่อมาจาก “none of your business” แปลว่า “ไม่ใช่ธุรกิจของคุณ”) ซึ่งกระตุ้นให้มีการพิจารณาคดีโดยการยื่นเรื่องร้องเรียนต่อ Meta อธิบายว่า คำตัดสินดังกล่าวเป็นผลกระทบทางการเงิน “สำคัญ” ต่อบริษัท ซึ่งขึ้นอยู่กับการโฆษณาสำหรับ 98% ของรายได้ 118 พันล้านดอลลาร์ในปี 2021 นับจากนี้ไป ผู้ใช้ Facebook และ Instagram ในสหภาพยุโรปจะต้องได้รับการขอให้ยินยอมให้ใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการโฆษณา เจ้าของข้อมูลจะต้องได้รับตัวเลือก “ใช่หรือไม่ใช” และสามารถเปลี่ยนใจได้ตลอดเวลา การตัดสินใจนี้ใช้กับผู้ลงโฆษณารายอื่นที่ต้องได้รับความยินยอมด้วย

การละเมิดการคุ้มครองข้อมูลโดยนายหน้าข้อมูล

Privacy International ยื่นเรื่องร้องเรียนต่อนายหน้าข้อมูลเจ็ดราย (Acxiom, Oracle), บริษัทเทคโนโลยีโฆษณา (Criteo, Quantcast, Tapad) และหน่วยงานอ้างอิงเครดิต (Equifax, Experian) กับหน่วยงานคุ้มครองข้อมูลในฝรั่งเศส ไอร์แลนด์ และสหราชอาณาจักร โดยมีวัตถุประสงค์คือ “เปลี่ยนพฤติกรรมของนายหน้าข้อมูล บริษัท AdTech และหน่วยงานจัดอันดับเครดิตโดยการจำกัดการติดตาม และการแบ่งปันข้อมูลส่วนบุคคล ซึ่งจะช่วยปรับปรุงการปกป้องความเป็นส่วนตัวสำหรับผู้คนทั่วยุโรป”

การใช้เทคโนโลยีจดจำใบหน้าโดยหน่วยงานบังคับใช้กฎหมายและหน่วยงานตุลาการ

StraLi (หน่วยงานคลังสมองในการดำเนินคดีเชิงกลยุทธ์ของอิตาลี) กำลังเตรียมกลยุทธ์เพื่อท้าทายการใช้เทคโนโลยีการจดจำใบหน้าโดยหน่วยงานบังคับใช้กฎหมายและหน่วยงานตุลาการในอิตาลี แผนการฟ้องคดีคือ จะยกเว้นกฎหมายที่ประกาศใช้เมื่อเดือนธันวาคม พ.ศ. 2564 กฎหมายนี้ระงับการติดตั้งและการใช้เทคโนโลยีการจดจำใบหน้าในพื้นที่สาธารณะโดยทั้งภาครัฐและเอกชน โดยได้รับการยกเว้นให้ใช้ต่อไปในกรณีการป้องกัน สืบสวน ตรวจจับ และการดำเนินคดีอาญา

การใช้ข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐ

ศาลสูงแห่งมลายาที่กัวลาลัมเปอร์ตัดสินว่า อธิบดีกรมสรรพากรภายในประเทศ (Director General of Inland Revenue: DGIR) ไม่สามารถใช้บทบัญญัติของพระราชบัญญัติภาษีเงินได้ปี 1967 (Income Tax Act: ITA) เพื่อหลีกเลี่ยงการคุ้มครองที่ได้รับจาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2553 (Personal Data Protection Act: PDPA) เพื่อดำเนินการสำรวจประมงเพื่อเก็บข้อมูลส่วนบุคคลของลูกค้าที่ถือครอง โดยธุรกิจที่ดำเนินกิจการในฐานะผู้ใช้ข้อมูล บริษัทผู้เสียภาษีได้จัดทำโปรแกรมสมาชิกให้กับลูกค้า (customer loyalty program) โดยกำหนดให้ลูกค้าที่เข้าร่วมต้องเปิดเผยข้อมูลส่วนบุคคลแก่บริษัท ทำให้บริษัทกลายเป็นผู้ใช้ข้อมูลตาม PDPA DGIR ได้ขอเข้าถึงข้อมูลส่วนบุคคลทั้งหมดที่บริษัทเก็บไว้ โดยมีเป้าหมายที่จะเก็บข้อมูลนี้ไว้ในคลังข้อมูลของตนและใช้เพื่อขยายฐานภาษีของ IRB ในอนาคต การร้องขอนี้ไม่ได้เกี่ยวข้องกับการตรวจสอบหรือสอบสวนบุคคลใดโดยเฉพาะ แต่เป็นความต้องการครอบคลุมฐานข้อมูลลูกค้าทั้งหมดของบริษัท ซึ่งสะท้อนให้เห็นถึงประเด็นสำคัญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการใช้อำนาจของหน่วยงานภาษี

บริษัทปฏิเสธที่จะให้ข้อมูลส่วนบุคคลของลูกค้าตามที่ DGIR ร้องขอ โดยอ้างว่าอำนาจของ DGIR ในการเรียกร้องข้อมูล ตลอดจนเป้าหมายในการสืบสวนและรวบรวมของ DGIR ไม่สามารถแทนที่การป้องกันที่ PDPA กำหนดไว้ได้ DGIR จึงขอคำยืนยันจากกรรมาธิการคุ้มครองข้อมูลส่วนบุคคล/รองกรรมาธิการคุ้มครองข้อมูลส่วนบุคคล (“กรรมาธิการ PDP”) ว่าอำนาจของ DGIR ภายใต้ ITA อาจเข้ามาแทนที่การคุ้มครองที่ PDPA กำหนดไว้เพื่ออนุญาตให้มีการสำรวจประมงเพื่อเก็บข้อมูลส่วนบุคคล บริษัทคัดค้านจุดยืนของ DGIR โดยเขียนจดหมายถึงกรรมาธิการ PDP ในที่สุด กรรมาธิการ PDP ก็เห็นด้วยกับ DGIR และออกคำตัดสินโดยระบุว่า DGIR สามารถใช้ ITA เพื่อหลีกเลี่ยงการคุ้มครองที่ PDPA กำหนดในการส่งคำขอแบบครอบคลุมดังกล่าวสำหรับข้อมูลส่วนบุคคลจากผู้เสียภาษี (นั่นคือ ลูกค้า) โดยไม่ได้รับความยินยอมจากพวกเขา (“คำวินิจฉัยของกรรมาธิการ PDP”)

บริษัทยื่นพิจารณาคดีในศาลสูงโดยฟ้องร้องกรรมาธิการ PDP และ DGIR เพื่อยกเลิกคำตัดสินของกรรมาธิการ PDP โดยอ้างว่าตนละเมิดมาตรการป้องกันของ PDPA ศาลสูงเห็นด้วยกับบริษัทและอนุญาตให้มีการอุทธรณ์เพื่อตรวจสอบการพิจารณาคดี ดังนั้นจึงทำให้คำตัดสินของกรรมาธิการ PDP เป็นโมฆะ เหนือสิ่งอื่นใด ศาลสูงตัดสินว่า DGIR ผูกพันตามบทบัญญัติของ PDPA ที่จะคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ ศาลยังระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้องซึ่งจะต้องทำให้เสร็จสิ้นก่อนที่ DGIR จะขอข้อมูลส่วนบุคคลจากบริษัท

สิทธิของเจ้าของข้อมูลในการไม่อยู่ภายใต้การตัดสินใจโดยการประมวลผลอัตโนมัติเพียงอย่างเดียว

กรณีหนึ่งของ Uber ล่าสุดอาศัยเฉพาะมาตรา 22 GDPR ซึ่งระบุว่าบุคคล “มีสิทธิที่จะไม่อยู่ภายใต้การตัดสินใจโดยอาศัยการประมวลผลอัตโนมัติเพียงอย่างเดียว รวมถึงการจัดทำโปรไฟล์ ซึ่งก่อให้เกิดผลทางกฎหมายที่เกี่ยวข้องกับเจ้าของข้อมูล หรือส่งผลกระทบอย่างมีนัยสำคัญต่อเจ้าของข้อมูลในทำนองเดียวกัน” ผู้สมัครขอให้ศาลแขวงอัมสเตอร์ดัมวิเคราะห์ Mastermind ซึ่งเป็นโปรแกรมตรวจจับการฉ้อโกงที่ซับซ้อนของ Uber ผู้ขับขี่ Uber ในสหราชอาณาจักรและโปรตุเกสอ้างว่า พวกเขาถูกไล่ออกโดยอัลกอริทึมต่อต้าน

การฉ้อโกงของบริษัท โดยใช้มาตรการป้องกัน GDPR ต่อการตัดสินใจแบบอัตโนมัติ ผู้สมัครอ้างว่าอัลกอริทึมที่ Uber ใช้นั้นเป็นแบบอัตโนมัติทั้งหมด (ไม่มีการแทรกแซงของมนุษย์) และส่งผลให้งานของพวกเขากับ Uber สิ้นสุดลง โดยไม่ให้โอกาสพวกเขาในการท้าทายการตัดสินใจ

วัตถุประสงค์ที่ระบุไว้ของ Mastermind คือการช่วยเหลือ Uber ในการตรวจสอบแพลตฟอร์มของตนอย่างมีประสิทธิภาพ คดีดังกล่าวอ้างว่า Uber ล้มเหลวในการแสดงให้เห็นว่าพนักงานมีความรู้เพียงพอเกี่ยวกับข้อมูลที่ป้อนเข้าระบบเพื่อสู้กับการฉ้อโกงอย่าง Mastermind เพื่อจะได้คาดการณ์ผลลัพธ์ หรืออธิบายการตัดสินของอัลกอริทึม นอกจากนี้ยังระบุด้วยว่า Uber จำเป็นต้องให้ข้อมูลที่แม่นยำแก่ผู้ขับขี่เกี่ยวกับการละเมิดที่ถูกกล่าวหาตามคำร้องเรียน จดหมายแจ้งการปิดใช้งานของ Uber ส่วนใหญ่เป็นจดหมายทั่วไปและละเว้นข้อมูลเกี่ยวกับการฉ้อโกงที่ถูกกล่าวหา นอกจากนี้ ผู้ขับขี่ไม่ได้รับโอกาสปฏิเสธข้อกล่าวหาดังกล่าว

ศาลแขวงในอัมสเตอร์ดัมสั่งให้ Uber คืนสถานะผู้ขับขี่ที่ถูกอัลกอริทึมของบริษัทยุติการทำงานอย่างไม่ถูกต้อง นอกจากนี้ยังสั่งให้ Uber ชดเชยความเสียหายให้กับผู้ขับขี่มากกว่า 100,000 ยูโร

การจัดทำโพรไฟล์โดยการตัดสินใจอัตโนมัติ (Automated Decision Making - ADM)

ในปี 2018 หน่วยงานคุ้มครองข้อมูลส่วนบุคคลของอิตาลี (Garante) พบว่าผู้ควบคุมข้อมูลแห่งหนึ่งละเมิดกฎหมายคุ้มครองข้อมูลของประเทศโดยเสนออัตราค่าบริการแบบส่วนตัวให้กับลูกค้าบริการแบ่งปันรถยนต์ตามพฤติกรรมและลักษณะที่สังเกตได้ ในกระบวนการทางปกครอง จำเลยโต้แย้งว่าไม่มีการ “จัดหมวดหมู่” ผู้ใช้บริการ เนื่องจากข้อมูลที่ใช้กำหนดค่าธรรมเนียมไม่ได้เชื่อมโยงกับบุคคลโดยตรง อย่างไรก็ตาม หน่วยงานคุ้มครองข้อมูลปฏิเสธข้อโต้แย้งนี้ โดยพบว่ามีการประมวลผลข้อมูลส่วนบุคคลอย่างชัดเจน เป็นการประมวลผลแบบอัตโนมัติทั้งหมด และมีวัตถุประสงค์เพื่อ กำหนดโปรไฟล์หรือบุคลิกของบุคคล หรือวิเคราะห์พฤติกรรมหรือทางเลือกในการบริโภค ในเดือนพฤศจิกายน 2021 ศาลฎีกาอิตาลี (Corte Suprema de Cassazione) ยืนยันคำตัดสินนี้ ส่งผลให้มีการปรับทางปกครอง 60,000 ยูโร ในกระบวนการอุทธรณ์

ศาลฎีกาเห็นด้วยกับ Garante เนื่องจากวินิจฉัยว่าการประมวลผลข้อมูลส่วนบุคคลโดยใช้อัลกอริทึมเพื่อกำหนดอัตราส่วนบุคคลถือเป็นการทำโปรไฟล์ แม้ว่าข้อมูลนั้นจะไม่ถูกเก็บไว้โดยผู้ควบคุมหรือไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ก็ตาม

6. การฟ้องคดีเชิงยุทธศาสตร์ความเป็นส่วนตัว

การฟ้องคดีเชิงยุทธศาสตร์ หรือที่เรียกว่าการดำเนินคดีแบบหวังสร้างผลกระทบ เป็นวิธีการที่น่าสนใจในการผลักดันการเปลี่ยนแปลงทางสังคม โดยเฉพาะในประเด็นความเป็นส่วนตัวทางดิจิทัล แทนที่จะเป็นเพียงการชนะคดีในศาล วิธีการนี้มุ่งหวังที่จะสร้างผลกระทบในวงกว้างต่อสังคมและนโยบาย

จุดเด่นของการฟ้องคดีเชิงยุทธศาสตร์ คือ สร้างความตระหนักรู้ให้สาธารณชน ส่งเสริมสิทธิของกลุ่มชายขอบ กดดันให้รัฐบาลแก้ไขกฎหมาย และผลักดันการคุ้มครองสิทธิความเป็นส่วนตัวและการคุ้มครองข้อมูล

ในด้านความเป็นส่วนตัวทางดิจิทัล การฟ้องคดีเชิงยุทธศาสตร์มักมุ่งเน้นที่การจำกัดสิทธิความเป็นส่วนตัวที่ไม่เป็นธรรม การเข้าถึงข้อมูล เสรีภาพในการแสดงออก การชุมนุม และการสมาคมในสภาพแวดล้อมดิจิทัล

ตัวอย่างน่าสนใจคือคดี Amabhungane Center for Investigative Journalism NPC and Others v. Minister of Justice and Correctional Services and Others ในแอฟริกาใต้ ที่ท้าทายกฎหมายสอดแนมของประเทศ โดยหวังจะนำไปสู่การปฏิรูปกฎหมายทั้งระบบ

อย่างไรก็ตาม การฟ้องคดีเชิงยุทธศาสตร์ก็มีความท้าทาย เพราะค่าใช้จ่ายสูงผลลัพธ์ไม่แน่นอน และอาจส่งผลเสียต่อชื่อเสียงหากไม่ประสบความสำเร็จ

การจะประสบความสำเร็จได้ ต้องอาศัยความร่วมมือจากหลายฝ่าย ทั้งทนายความ นักเคลื่อนไหวด้านสิทธิมนุษยชน นักวิชาการ องค์กรภาคประชาสังคม และผู้เชี่ยวชาญในด้านต่าง ๆ

แม้จะมีความเสี่ยง แต่หากทำสำเร็จ การฟ้องคดีเชิงยุทธศาสตร์สามารถนำประเด็นสำคัญเข้าสู่การรับรู้ของสาธารณชน และนำไปสู่การเปลี่ยนแปลงกฎหมายและสังคมในวงกว้าง โดยเฉพาะในยุคที่ความเป็นส่วนตัวทางดิจิทัลกำลังเป็นประเด็นร้อนแรง วิธีการนี้จึงเป็นเครื่องมือสำคัญในการปกป้องสิทธิของประชาชนในโลกออนไลน์ตัวอย่างการฟ้องคดีเชิงยุทธศาสตร์ความเป็นส่วนตัวที่ประสบความสำเร็จ

ตัวอย่าง การฟ้องคดีเชิงยุทธศาสตร์ความเป็นส่วนตัวที่ประสบความสำเร็จ

ศาลรัฐธรรมนูญของแอฟริกาใต้พบว่าบทบัญญัติหลายประการของพระราชบัญญัติข้อมูลที่เกี่ยวข้อง (RICA) ขัดต่อรัฐธรรมนูญ นอกจากนี้ยังพบว่ารัฐ (ศูนย์สื่อสารแห่งชาติ) มีความผิดในการดำเนินการสอดแนมมวลชนและสกัดกั้นสัญญาณจากต่างประเทศโดยผิดกฎหมาย ศูนย์ Amabhungane ยื่นฟ้องคดีนี้ในข้อหาวารสารศาสตร์เชิงสืบสวน ในปี 2017 โดยโต้แย้งรัฐธรรมนูญของ RICA

ในประเทศเคนยา ศาลสูงประกาศว่ากระบวนการรวบรวมและเผยแพร่ข้อมูลของระบบ ID ไบโอเมตริกซ์ Huduma นั้นขัดต่อรัฐธรรมนูญ ศาลเห็นว่าพระราชบัญญัติคุ้มครองข้อมูลปี 2019 ควรมีผลย้อนหลังกับการเปิดตัวระบบของรัฐบาลที่เริ่มในปี 2020

ในเดือนเมษายน 2018 สมาคมบล็อกเกอร์แห่งเคนยา (BAKE) ได้ยื่นคำร้องคัดค้านพระราชบัญญัติการใช้คอมพิวเตอร์ในทางที่ผิดและอาชญากรรมทางคอมพิวเตอร์ปี 2018 โดยอ้างว่าละเมิด ละเมิด และคุกคามเสรีภาพขั้นพื้นฐานที่รับรองโดย Bill of Rights ของเคนยาปี 2010 ถูกท้าทายเนื่องจากฝ่าฝืนหลักประกันตามรัฐธรรมนูญเกี่ยวกับเสรีภาพในการแสดงความคิดเห็น เสรีภาพในการแสดงออก เสรีภาพสื่อ ความปลอดภัยของบุคคล สิทธิในความเป็นส่วนตัว สิทธิในทรัพย์สิน และสิทธิในการได้รับการพิจารณาคดีอย่างยุติธรรม ในคำพิพากษาที่ออกเมื่อวันที่ 29 พฤษภาคม 2561 ผู้พิพากษารับรองคำร้องของ BAKE เป็นเรื่องเร่งด่วน และสั่งให้ผู้ถูกร้องต้องตอบกลับอย่างรวดเร็ว มีคำสั่งระงับการใช้บังคับชั่วคราว ในที่สุดมาตรการชั่วคราวนี้ ก็ถูกยกเลิก

และปฏิเสธโดยศาลสูง ซึ่งถือว่าพระราชบัญญัติทั้งหมดถูกต้องตามกฎหมาย นอกจากนี้ ศาลยังตัดสินว่าพระราชบัญญัติ 26 มาตราที่ BAKE โต้แย้งนั้นเป็นรัฐธรรมนูญ แม้ว่ามาตรการชั่วคราวเดิมที่ระงับการกระทำดังกล่าวถือเป็นก้าวไปในทิศทางที่ถูกต้อง แต่คำตัดสินของศาลสูงที่จะสนับสนุนกฎหมายดังกล่าวถือเป็นอุปสรรคสำหรับการเคลื่อนไหวด้านสิทธิดิจิทัลในเคนยา

กิจกรรม: อ่านข้อความด้านล่างว่าเทคโนโลยีการจดจำใบหน้าสามารถละเมิดสิทธิความเป็นส่วนตัวและดูวิดีโอได้อย่างไร หารือเกี่ยวกับเทคโนโลยีการจดจำใบหน้าและความเสี่ยงที่สามารถดำเนินคดีภายใต้กฎหมายคุ้มครองข้อมูลและความเป็นส่วนตัว

เดือนพฤษภาคมปี 2020 สหภาพเสรีภาพพลเรือนอเมริกัน (ACLU) ได้ยื่นฟ้อง ในนามขององค์กรที่เป็นตัวแทนของเหยื่อการละเมิดในครอบครัว ผู้อพยพผิดกฎหมาย และผู้ให้บริการทางเพศ องค์กรดังกล่าวกล่าวหาว่า Clearview ซึ่งเป็นบริษัทเทคโนโลยีที่พัฒนาเทคโนโลยีการจดจำใบหน้า ฝ่าฝืนกฎหมาย Biometric Information Privacy Act (BIPA) ของรัฐอิลลินอยส์ ซึ่งเป็นกฎหมายของรัฐที่ป้องกันไม่ให้ธุรกิจเชิงพาณิชย์ใช้ประโยชน์จากตัวระบุทางกายภาพของพลเมือง รวมถึงการทำแผนที่ใบหน้าด้วยคอมพิวเตอร์โดยไม่ได้รับความยินยอม

คำร้องเรียนถูกยื่นต่อศาลรัฐอิลลินอยส์ในชิคาโก หลังจากที่นิวยอร์กไทมส์เปิดเผยเมื่อเดือนมกราคม 2020 ว่า Clearview กำลังพัฒนาระบบติดตามและเฝ้าระวังที่ใช้ตัวระบุไบโอเมตริกซ์ เทคโนโลยีการจดจำใบหน้าทำให้ Clearview สามารถพิมพ์ใบหน้าได้มากกว่า 3 พันล้านใบหน้าจากภาพถ่ายบนเว็บ

การเข้าถึงข้อมูลนี้จัดทำโดย Clearview ให้กับองค์กรเอกชน ผู้รวบรวม และองค์กรบังคับใช้กฎหมายของรัฐบาลกลาง รัฐ และท้องถิ่น ธุรกิจยืนยันว่าการใช้ฐานข้อมูลขนาดใหญ่นี้สามารถระบุบุคคลได้ทันทีด้วยความแม่นยำที่ไม่มีใครเทียบได้ ช่วยให้สามารถสอดแนมอเมริกันจากระยะไกลได้ภายใต้ปฏิบัติการที่เป็นความลับ

BIPA กำหนดว่าธุรกิจที่รวบรวม จับภาพ หรือได้รับข้อมูลระบุตัวตนทางชีวมิติจากผู้อยู่อาศัยในรัฐอิลลินอยส์ เช่น ลายนิ้วมือ ใบหน้า หรือการสแกนม่านตา จะต้องแจ้งให้บุคคลนั้นทราบก่อน และได้รับความยินยอมเป็นลายลักษณ์อักษร เนื่องจากข้อเท็จจริงที่ว่าการบังคับให้ได้มาซึ่งตัวระบุไบโอเมตริกซ์ที่ไม่เปลี่ยนรูปนั้นก่อให้เกิดอันตรายต่อความปลอดภัย ความเป็นส่วนตัว และความปลอดภัยของบุคคลมากกว่า

การจับตัวระบุอื่นๆ เช่น ชื่อและที่อยู่ และการบันทึกใบหน้าของบุคคล ซึ่งเทียบได้กับการสร้างโปรไฟล์ DNA ของพวกเขาจากสารพันธุกรรมที่หลั่งลงบนขวดน้ำอย่างหลีกเลี่ยงไม่ได้ แต่แตกต่างจากการตีพิมพ์หรือการส่งภาพถ่าย ถือเป็นพฤติกรรม ไม่ใช่คำพูด และอยู่ภายใต้กฎหมายอย่างชอบธรรม Clearview ไม่ปฏิบัติตาม BIPA ซึ่งลิดรอนสิทธิความเป็นส่วนตัวของพลเมืองอิลลินอยส์หลายคน

คดีนี้เป็นคดีแรกที่มุ่งเน้นไปที่ความเสียหายที่เทคโนโลยีของ Clearview จะก่อให้เกิดต่อผู้รอดชีวิตจากการล่วงละเมิดทางเพศและในบ้าน ผู้อพยพที่ไม่มีเอกสาร ชุมชนคนผิวสี และสมาชิกของประชากรกลุ่มเปราะบางอื่นๆ สมาชิก ลูกค้า และผู้เข้าร่วมโปรแกรมขององค์กรโจทก์ถูกพิมพ์ใบหน้าโดย Clearview โดยไม่ได้รับความยินยอม และต้องเผชิญกับผลกระทบร้ายแรงที่สุดจากโปรแกรมติดตามตรวจสอบที่ไม่มีใครเทียบได้ของ Clearview

11 พฤษภาคม 2022 หลังจากที่ทั้งสองฝ่ายเจรจาข้อตกลงยุติคดี ศาลได้อนุมัติคำสั่งยินยอมให้ยกฟ้องเรื่องนี้ องค์ประกอบพื้นฐานของข้อตกลงดังกล่าวได้ห้ามการดำเนินงานของ Clearview ไม่เพียงแต่ในรัฐอิลลินอยส์เท่านั้น แต่ยังทั่วทั้งสหรัฐอเมริกา โดยห้ามไม่ให้ Clearview เข้าถึงฐานข้อมูล faceprint ขององค์กรเอกชนอย่างถาวร นอกจากนี้ บริษัทถูกห้ามเป็นเวลาห้าปีในการขายการเข้าถึงฐานข้อมูลของบริษัทให้กับหน่วยงานใดๆ ในรัฐอิลลินอยส์ รวมถึงหน่วยงานของรัฐและเทศบาล

ที่มา: https://youtu.be/s44EFtBoRxY

ที่มา: https://youtu.be/cc0dqW2HCRc

7. คำถามท้ายตอน

อ่านเนื้อหาในตอนที่ 1, 2 และ 3 และร่างประเด็นข้อเท็จจริง และกฎหมายที่สำคัญ (3 ชั่วโมง)

ในปี 2020 บีเจ (“โจทก์”) ถูกจับกุมและถูกตั้งข้อหาทางอาญาในข้อหาลหุโทษ 2 คดี แต่ไม่เคยถูกดำเนินคดีเลย ต่อจากนั้นบีเจร้องขอให้ลบประวัติอาชญากรรมของเขา ซึ่งหมายความว่าบันทึกอย่างเป็นทางการถูกทำลายหรือไม่สามารถเข้าถึงได้ อย่างไรก็ตาม เหตุการณ์เหล่านี้ได้รับการรายงานโดยหนังสือพิมพ์ท้องถิ่นในหน้ารายงานข่าวเกี่ยวกับตำรวจ และทำให้ยังคงมีข้อมูลออนไลน์ผ่านการค้นหาของ Google ซึ่งโจทก์ต้องการลบออก บีเจได้ยื่นฟ้อง Media Inc. ซึ่งเป็นสื่อมวลชนของมาเลเซียซึ่งมีสำนักงานใหญ่ในกรุงกัวลาลัมเปอร์ (“จำเลย”) จำเลยยื่นคำร้องให้ยกฟ้อง คุณในฐานะผู้พิพากษาต้องตัดสินใจว่าโจทก์มีสิทธิที่จะถูกลืมหรือไม่ คุณจะตัดสินคดีอย่างไร โปรดอธิบาย

ตอนที่ 4 มุมมอง 5 ประเทศอาเซียนกับการจัดการความเป็นส่วนตัว

เคยสงสัยไหมว่าทำไมแอปพลิเคชันบางตัวถึงใช้ได้ในไทย แต่ใช้ไม่ได้ในเวียดนาม? หรือทำไมบริษัทใหญ่ๆ ถึงต้องมีเซิร์ฟเวอร์แยกสำหรับแต่ละประเทศในอาเซียน?

เนื้อหาตอนนี้จะพาคุณทัวร์กฎหมาย 5 ประเทศอาเซียน ดูว่าแต่ละประเทศมีวิธีปกป้องข้อมูลประชาชนแตกต่างกันอย่างไร เรียนรู้ว่าทำไมอินโดนีเซียถึงได้ชื่อว่าเข้มงวดเรื่องโซเชียลมีเดีย และทำไมฟิลิปปินส์ถึงได้ฉายา “ศูนย์กลาง BPO” ของภูมิภาค

สิ่งที่จะได้เรียนรู้:

1. เจาะลึก 5 ประเทศ: ดูว่าแต่ละประเทศมีกฎหมายและนโยบายอะไรบ้าง
2. รู้จักสิทธิของคุณ: เข้าใจว่าคุณมีสิทธิอะไรบ้างในแต่ละประเทศ
3. เรียนรู้จากคดีดัง: ดูกรณีศึกษาที่ทำให้เกิดการเปลี่ยนแปลงในแต่ละประเทศ
4. เข้าใจความแตกต่าง: เปรียบเทียบจุดเด่นจุดด้อยของแต่ละประเทศ

หลังจบตอนนี้ คุณอาจจะกลายเป็น **“ผู้เชี่ยวชาญกฎหมายข้อมูลส่วนบุคคลอาเซียน”** ที่พร้อมจะเข้าใจความซับซ้อนของกฎหมายในภูมิภาค และรู้วิธีปกป้องสิทธิของตัวเองไม่ว่าจะอยู่ที่ไหนในอาเซียน

กฎหมายคุ้มครองข้อมูลส่วนบุคคลในอาเซียน: เปรียบเทียบ 5 ประเทศ

ในส่วนนี้จะพาทุกคนไปสำรวจกฎหมายคุ้มครองข้อมูลส่วนบุคคลใน 5 ประเทศอาเซียนเพื่อให้เห็นว่าแต่ละประเทศมีกฎหมายที่เหมือนหรือต่างกันอย่างไร

1. อินโดนีเซีย: ยักษ์ใหญ่แห่งข้อมูลกับความท้าทายในการบังคับใช้

สิทธิความเป็นส่วนตัวในอินโดนีเซีย: เมื่อรัฐธรรมนูญไม่พูดตรง ๆ

คุณเคยสงสัยไหมว่าความเป็นส่วนตัวของคุณในอินโดนีเซียได้รับการคุ้มครองอย่างไร? เรื่องนี้น่าสนใจมาก เพราะแม้แต่รัฐธรรมนูญของประเทศก็ยังไม่ได้พูดถึง **“ความเป็นส่วนตัว”** ตรง ๆ

แต่อย่าเพิ่งตกใจไป เพราะมีมาตราลับ ๆ ที่ช่วยคุ้มครองเราอยู่ คือ

• มาตรา 28(g) พูดถึงสิทธิที่จะมี “ศักดิ์ศรี” และ “รู้สึกปลอดภัย” (ฟังดูคุ้นๆ กับความเป็นส่วนตัวไหมล่ะ?) และ

• มาตรา 28(f) บอกว่าเรามีสิทธิสื่อสารและรับข้อมูล (แต่ไม่ได้บอกว่าใครจะแอบดูได้ไหมนะ)

รัฐธรรมนูญอินโดนีเซีย มาตรา 28 (g) ระบุว่า *“ทุกคนมีสิทธิที่จะได้รับการคุ้มครองตนเอง ครอบครัว เกียรติยศ ศักดิ์ศรี และทรัพย์สิน ภายใต้การควบคุมของตน และมีสิทธิที่จะรู้สึกปลอดภัยและได้รับการคุ้มครองจากภัยคุกคามความกลัวในการทำหรือไม่ทำบางสิ่ง ซึ่งเป็นสิทธิมนุษยชน”* และมาตรา *28(f) ระบุว่า “ทุกคนมีสิทธิในการสื่อสารและได้รับข้อมูล เพื่อพัฒนาตนเองและสภาพแวดล้อมทางสังคม รวมทั้งมีสิทธิในการแสวงหา ได้รับ ครอบครอง เก็บรักษา ประมวลผล และส่งต่อข้อมูลโดยใช้ทุกประเภทของช่องทางที่มีอยู่”*

แม้ว่ามาตราเหล่านี้ไม่ได้ใช้คำว่า “ความเป็นส่วนตัว” โดยตรง แต่ก็สามารถตีความได้ว่าให้การคุ้มครองสิทธิความเป็นส่วนตัวในทางอ้อม โดยเฉพาะอย่างยิ่งการกล่าวถึงศักดิ์ศรี ความปลอดภัย และสิทธิในการสื่อสารและจัดการข้อมูล

นอกจากนี้ อินโดนีเซียยังเข้าร่วมสนธิสัญญาสิทธิมนุษยชนระดับโลกหลายฉบับ เช่น UDHR, ICCPR และปฏิญญาสิทธิมนุษยชนอาเซียน เรียกว่าเป็นการเซ็นสัญญาคุ้มครองความเป็นส่วนตัวแบบอ้อมๆ นั่นเอง

เมื่อความเป็นส่วนตัวมาถึงยุคดิจิทัล อินโดนีเซียเพิ่งออกกฎหมายใหม่เอี่ยมชื่อ Personal Data Protection (PDP) ที่จะมาคุ้มครองข้อมูลส่วนตัวโดยเฉพาะ กฎหมายนี้จะเริ่มใช้จริงๆ ในเดือนตุลาคม 2024 โดยอิงมาจาก GDPR ของสหภาพยุโรป (เรียกว่าเอาของดีมาใช้เลยทีเดียว!)

ก่อนหน้านี้ การคุ้มครองข้อมูลในอินโดนีเซียเหมือนจิ๊กซอว์ที่กระจัดกระจาย มีกฎเล็กกฎน้อยอยู่ในกฎหมายหลายฉบับ แต่ตอนนี้ PDP จะมารวมทุกอย่างเข้าด้วยกัน

แล้ว PDP คุ้มครองใครบ้าง ? กฎหมายนี้ครอบคลุมกว้างมาก ไม่ว่าคุณจะเป็นคนธรรมดาอย่างเราๆ หรือบริษัทใหญ่โต หรือหน่วยงานรัฐ (แม้แต่ NGO ที่ได้เงินจากรัฐก็รวมอยู่ด้วย) หรือบริษัทต่างชาติที่เก็บข้อมูลคนอินโดนีเซีย เรียกว่าใครก็ตามที่ยุ่งกับข้อมูลส่วนตัวของคนอินโดนีเซีย ต้องระวังตัวกัน

ความเป็นส่วนตัวออนไลน์ในอินโดนีเซีย: จากวิกฤตสู่การปฏิรูป

อินโดนีเซียเผชิญกับปัญหาการรั่วไหลของข้อมูลครั้งใหญ่หลายครั้งในปี 2021 ไม่ว่าจะเป็นการละเมิดข้อมูลประกันสุขภาพแห่งชาติ การรั่วไหลของบัตรแจ้งเตือนสุขภาพอิเล็กทรอนิกส์ และการโจมตีเว็บไซต์ของหน่วยงานไซเบอร์และการเข้ารหัสแห่งชาติ

แต่เรื่องที่ทำให้ทุกคนตกใจที่สุดคือ การที่แฮกเกอร์นามว่า Bjorka ขายข้อมูลซิมการ์ดถึง 3 พันล้านรายการ! (มากกว่าประชากรอินโดนีเซียซะอีก) Bjorka ไม่หยุดแค่นั้น เขายังเปิดเผยบันทึกการสื่อสารลับระหว่างประธานาธิบดีและหน่วยข่าวกรอง และข้อมูลติดต่อและประวัติการฉีดวัคซีนของนักการเมืองดัง

เหตุการณ์เหล่านี้ชี้ให้เห็นว่าความปลอดภัยทางไซเบอร์ของอินโดนีเซียยังไม่แข็งแกร่งพอ แต่ก็มีข่าวดี ในปี 2022 อินโดนีเซียออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDP) ฉบับใหม่ เพื่อสร้างกรอบการทำงานที่ครอบคลุมมากขึ้น อย่างไรก็ตาม ยังไม่มีกฎเกณฑ์เฉพาะเกี่ยวกับคุกกี้และข้อมูลตำแหน่ง ตราบใดที่ไม่สามารถระบุตัวตนได้ ก็ยังใช้งานได้อยู่

ทั้งหมดนี้แสดงให้เห็นว่าอินโดนีเซียกำลังพยายามปรับปรุงความปลอดภัยทางไซเบอร์ แต่ก็ยังมีอีกหลายอย่างที่ต้องทำเพื่อปกป้องข้อมูลของประชาชน โดยเฉพาะเมื่อเศรษฐกิจดิจิทัลของประเทศคาดว่าจะเติบโตถึง 146 พันล้านดอลลาร์ในปี 2568!

คุณคิดว่าอินโดนีเซียควรทำอะไรเพิ่มเติมเพื่อปกป้องความเป็นส่วนตัวออนไลน์ของประชาชน ?

การคุ้มครองข้อมูลส่วนบุคคล: PDP อินโดนีเซีย

กฎหมาย PDP ของอินโดนีเซียครอบคลุมทุกขั้นตอนการจัดการข้อมูลส่วนบุคคล ตั้งแต่การรวบรวม วิเคราะห์ จัดเก็บ แก้ไข เผยแพร่ ไปจนถึงการลบทิ้ง โดยมีความคล้ายคลึงกับ GDPR ของสหภาพยุโรป กฎหมายนี้วางหลักการสำคัญในการประมวลผลข้อมูล 6 ประการ ได้แก่ ความยินยอม ภาระผูกพันตามสัญญา ภาระผูกพันทางกฎหมาย ผลประโยชน์สำคัญสาธารณประโยชน์ และประโยชน์โดยชอบด้วยกฎหมาย

ในแง่การปฏิบัติ กฎหมายเน้นย้ำให้การเก็บรวบรวมข้อมูลต้องทำอย่างมีจริยธรรมและถูกกฎหมาย โดยได้รับความยินยอมจากเจ้าของข้อมูล การประมวลผลต้องทำตามวัตถุประสงค์ที่กำหนดและคุ้มครองสิทธิของเจ้าของข้อมูล ข้อมูลที่เก็บต้องถูกต้อง ครบถ้วน และเป็นปัจจุบัน พร้อมทั้งมีการรักษาความปลอดภัยจากการใช้งานที่ไม่ได้รับอนุญาต

ก่อนการประมวลผล ต้องแจ้งวัตถุประสงค์และกิจกรรมที่เกี่ยวข้องให้เจ้าของข้อมูลทราบ และเมื่อหมดความจำเป็น ข้อมูลต้องถูกทำลายหรือลบทิ้ง เว้นแต่จะมีกฎหมายกำหนดให้เก็บรักษาไว้ ทั้งหมดนี้ดำเนินการด้วยความรับผิดชอบและโปร่งใส เพื่อสร้างความเชื่อมั่นในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนอินโดนีเซีย ในยุคที่ข้อมูลดิจิทัลมีความสำคัญมากขึ้นเรื่อย ๆ

กฎหมาย PDP อินโดนีเซีย คุ้มครองข้อมูลส่วนบุคคลแบบเข้มข้น

PDP ของอินโดนีเซียไม่ได้แค่วางหลักการกว้างๆ แต่ยังมีข้อกำหนดที่ละเอียดและเข้มงวดสำหรับผู้ควบคุมข้อมูล โดยมีจุดเด่นสำคัญดังนี้:

1. การบันทึกข้อมูล: ผู้ควบคุมข้อมูลต้องเก็บบันทึกการประมวลผลอย่างละเอียด ยกเว้นภาคการเงินที่มีข้อยกเว้นพิเศษ

2. เทคโนโลยีจดจำใบหน้า: มีข้อกำหนดพิเศษสำหรับการใช้เทคโนโลยีนี้เพื่อป้องกันการละเมิดความเป็นส่วนตัว

3. ข้อมูลส่วนบุคคลเฉพาะ: มีการคุ้มครองเป็นพิเศษสำหรับข้อมูลประเภทนี้ ซึ่งรวมถึงข้อมูลของเด็กและข้อมูลทางการเงิน

4. การตอบสนองต่อคำขอ: องค์กรต้องตอบสนองต่อคำขอของเจ้าของข้อมูล เช่น การขอเข้าถึง แก้ไข หรือจำกัดข้อมูล ภายในเวลาเพียง 72 ชั่วโมง

ความแตกต่างระหว่างกฎหมาย PDP และ GDPR

แม้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDP) ของอินโดนีเซียจะได้แรงบันดาลใจมาจาก GDPR ของสหภาพยุโรป แต่ก็มีการปรับแต่งให้เหมาะสมกับสภาพแวดล้อมของประเทศ ความแตกต่างที่สำคัญมีดังนี้:

1. การยกเว้นภาคการเงิน: PDP ไม่ครอบคลุมภาคการเงินซึ่งต่างจาก GDPR ที่บังคับใช้กับทุกภาคส่วน

2. การบันทึกข้อมูลที่ละเอียดยิ่งขึ้น: PDP กำหนดให้บันทึกกิจกรรมการประมวลผลข้อมูลอย่างละเอียด มากกว่าที่ GDPR กำหนด

3. การควบคุมเทคโนโลยีจดจำใบหน้า: PDP มีข้อกำหนดเฉพาะสำหรับเทคโนโลยีนี้ ในขณะที่ GDPR ไม่ได้กล่าวถึงโดยตรง

4. นิยามข้อมูลละเอียดอ่อน: PDP รวมข้อมูลทางการเงินและข้อมูลของเด็กเป็นข้อมูลละเอียดอ่อน ต่างจาก GDPR

5. ระยะเวลาตอบสนองต่อคำขอ: PDP กำหนดให้ตอบสนองภายใน 72 ชั่วโมง ซึ่งเร็วกว่า GDPR ที่ให้เวลา 1 เดือน

ความแตกต่างเหล่านี้แสดงให้เห็นว่าอินโดนีเซียไม่ได้เพียงแค่คัดลอก GDPR มาใช้ แต่ได้พิจารณาถึงความต้องการเฉพาะของประเทศ โดยเน้นการคุ้มครองสิทธิของประชาชนในยุคดิจิทัลอย่างเข้มแข็ง และตอบสนองต่อความท้าทายด้านความปลอดภัยของข้อมูลที่เกิดขึ้นในประเทศ

กิจกรรม: อภิปรายว่ากฎหมาย PDP ควบคุมเทคโนโลยีการจดจำใบหน้าและผลกระทบต่อการคุ้มครองข้อมูลอย่างไร พวกเขาจะทำอะไรที่แตกต่างออกไปหากพวกเขาเป็นผู้ควบคุม?

มาตรา 17 ของกฎหมาย PDP กำหนดว่าผู้ควบคุมที่ใช้เทคโนโลยีการจดจำใบหน้าหรือติดตั้งอุปกรณ์ประมวลผลข้อมูลภาพในพื้นที่สาธารณะสามารถทำได้เพียงเพื่อความปลอดภัย การหลีกเลี่ยงภัยพิบัติ หรือการวิเคราะห์ข้อมูลการจราจรเท่านั้น นอกจากนี้ องค์กรจะต้องแจ้งให้สาธารณชนทราบว่ามีการใช้งานเทคโนโลยีนี้ในพื้นที่ที่พวกเขาวางอุปกรณ์ไว้ อย่างไรก็ตาม กฎเหล่านี้ใช้ไม่ได้กับการบังคับใช้กฎหมายหรือการป้องกันการกระทำผิดทางอาญา

ที่มา: https://fpf.org/blog/indonesias-personal-data-protection-bill-overview-key-takeaways-and-context/

นโยบายและความริเริ่มของภาคส่วนต่าง ๆ

อินโดนีเซียไม่ได้พึ่งพาเพียงกฎหมาย PDP เท่านั้น แต่ยังมีการคุ้มครองข้อมูลส่วนบุคคลในภาคส่วนเฉพาะอีกด้วย โดยเฉพาะในภาคโทรคมนาคมและภาคข้อมูลสาธารณะ ในภาคโทรคมนาคม กฎหมายฉบับที่ 36 ปี 1999 (แก้ไขในปี 2020) ให้ความคุ้มครองข้อมูลที่ส่งผ่านเครือข่ายโทรคมนาคมทุกประเภท โดยผู้ให้บริการมีหน้าที่รักษาความลับของข้อมูลที่ผู้ใช้ส่งหรือรับผ่านเครือข่าย

ส่วนในภาคข้อมูลสาธารณะ กฎหมายฉบับที่ 14 ปี 2551 ห้ามองค์กรสาธารณะเปิดเผยข้อมูลที่เกี่ยวข้องกับสิทธิส่วนบุคคล โดยเฉพาะข้อมูลอ่อนไหว เช่น ประวัติครอบครัว ประวัติทางการแพทย์และจิตวิทยา ข้อมูลทางการเงิน บันทึกการประเมินความสามารถ และประวัติการศึกษา การมีกฎหมายเฉพาะสำหรับแต่ละภาคส่วนนี้สะท้อนให้เห็นถึงความพยายามของอินโดนีเซียในการสร้างระบบคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมและเข้มแข็ง โดยคำนึงถึงลักษณะเฉพาะของแต่ละภาคส่วนและความสำคัญของความเป็นส่วนตัวในยุคดิจิทัล

ในภาคการธนาคารและตลาดทุนของอินโดนีเซีย การคุ้มครองข้อมูลส่วนบุคคลได้รับความสำคัญเป็นพิเศษ กฎหมายการธนาคารฉบับที่ 7 ปี 1992 (แก้ไขล่าสุดในปี 2020) และกฎหมายตลาดทุนฉบับที่ 8 ปี 1995 เป็นเสาหลักในการควบคุมความเป็นส่วนตัวของข้อมูลในภาคส่วนนี้ โดยครอบคลุมทั้งข้อมูลส่วนบุคคลและข้อมูลธุรกิจ

หนึ่งในมาตรการสำคัญคือ การกำหนดให้หน่วยงานบริการทางการเงินต้องได้รับการอนุมัติล่วงหน้าก่อนที่จะถ่ายโอนข้อมูลลูกค้า ไม่ว่าจะเป็นการจัดตั้งศูนย์ข้อมูลหรือการประมวลผลข้อมูลนอกประเทศอินโดนีเซีย ซึ่งสะท้อนถึงความระมัดระวังในการปกป้องข้อมูลทางการเงินของประชาชน

เมื่อกฎหมาย PDP มีผลบังคับใช้ กฎหมายเหล่านี้จะยังคงมีผลเฉพาะในส่วนที่สอดคล้องกับ PDP เท่านั้น นอกจากนี้ ยังมีการคาดการณ์ว่าจะมีการออกกฎระเบียบเพิ่มเติมเพื่อให้สอดคล้องกับ PDP

การกำกับดูแล การตรวจสอบ และถ่วงดุล

การกำกับดูแลการสอดแนมของรัฐ แม้อินโดนีเซียจะมีความก้าวหน้าในการคุ้มครองข้อมูลส่วนบุคคลในหลายภาคส่วน แต่ยังมีช่องว่างสำคัญในการควบคุมการสอดแนมของรัฐ ปัจจุบัน ไม่มีหน่วยงานกำกับดูแลเฉพาะหรือหลักเกณฑ์ที่ชัดเจนสำหรับการอนุญาตให้สอดแนม แต่ละหน่วยงานสามารถเริ่มการเฝ้าระวังได้ตามดุลยพินิจ โดยไม่มีข้อจำกัดด้านระยะเวลาที่ชัดเจน การติดตามสามารถขยายเวลาได้จาก 30 วันเป็น 6 เดือน และอาจต่อเวลาได้อีกโดยไม่มีกำหนด นอกจากนี้ ในกรณีฉุกเฉิน รัฐบาลสามารถตรวจสอบการสื่อสารได้โดยไม่ต้องขออนุญาตศาล

สถานการณ์นี้ส่งผลให้ประชาชนขาดความโปร่งใสและการเข้าถึงกระบวนการยุติธรรมที่เหมาะสม ซึ่งอาจนำไปสู่การละเมิดสิทธิความเป็นส่วนตัวโดยไม่จำเป็น เพื่อแก้ไขปัญหานี้ อินโดนีเซียจำเป็นต้องปรับปรุงกฎหมาย โดยจัดตั้งหน่วยงานกำกับดูแลอิสระ กำหนดหลักเกณฑ์ที่ชัดเจนสำหรับการอนุญาตให้สอดแนม กำหนดข้อจำกัดด้านระยะเวลาที่เหมาะสม และเพิ่มการตรวจสอบทางกฎหมายสำหรับการใช้อำนาจในกรณีฉุกเฉิน การปรับปรุงเหล่านี้จะช่วยสร้างสมดุลที่ดีขึ้นระหว่างความมั่นคงของชาติและการคุ้มครองสิทธิความเป็นส่วนตัวของประชาชน ซึ่งเป็นสิ่งสำคัญในการรักษาความไว้วางใจของสาธารณชนและส่งเสริมหลักนิติธรรมในยุคดิจิทัล

อินโดนีเซียมีกรอบกฎหมายที่ซับซ้อนเกี่ยวกับการสอดแนมและการคุ้มครองความเป็นส่วนตัว โดยมีการผสมผสานระหว่างการรับรองสิทธิและการให้อำนาจแก่รัฐ

กฤษฎีกาของสภาที่ปรึกษาปี 1998 (TAP MPR) เลขที่ 17/MPR/1998 (The 1998 Decree of the Consultative Assembly (TAP MPR) No. 17/MPR/1998) คุ้มครองเสรีภาพในการแสดงออก การสมาคม และการสื่อสาร แต่ไม่ได้รับรองความเป็นส่วนตัวอย่างชัดแจ้งว่าเป็นสิทธิ และภายใต้กฎหมายฉบับที่ 39 ปี 1999 อินโดนีเซียมีหน้าที่เคารพและปฏิบัติตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชนและสนธิสัญญาสิทธิมนุษยชนระหว่างประเทศอื่ นๆ ซึ่งขยายออกไปแล้วจะรับประกันสิทธิในความเป็นส่วนตัวของมาตรา 12

กฎหมายโทรคมนาคมฉบับที่ 36 ปี 1999 ให้อำนาจรัฐในการควบคุมภาคการสื่อสารอย่างกว้างขวาง โดยกำหนดให้ผู้ให้บริการต้องบันทึกการใช้บริการและอาจต้องเปิดเผยข้อมูลเพื่อกระบวนการยุติธรรมทางอาญา กฎกระทรวงปี 2549 ยังอำนวยความสะดวกในการเข้าถึงเครือข่ายโทรคมนาคมโดยหน่วยงานบังคับใช้กฎหมายโดยตรง

กฎหมายว่าด้วยข้อมูลและธุรกรรมทางอิเล็กทรอนิกส์ (The Electronic Information and TrAactions: EIT) พยายามสร้างสมดุลโดยกำหนดให้รัฐบาลออกกฎระเบียบควบคุมการดักฟัง และห้ามการใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

กฎหมายข่าวกรองแห่งรัฐอินโดนีเซียปี 2011 เป็นอีกหนึ่งบทบัญญัติสำคัญที่ส่งผลกระทบต่อความสมดุลระหว่างความมั่นคงของชาติและสิทธิส่วนบุคคลของประชาชน กฎหมายนี้ให้อำนาจอย่างกว้างขวางแก่สำนักข่าวกรองแห่งรัฐอินโดนีเซีย (BIN) ในการดำเนินการเพื่อปกป้องผลประโยชน์และความมั่นคงของชาติ ประเด็นสำคัญของกฎหมายนี้ ได้แก่

1. ขอบเขตอำนาจที่กว้างขวาง BIN ได้รับอำนาจในการป้องกันและต่อสู้กับ “ความพยายาม การทำงาน กิจกรรมข่าวกรอง และ/หรือฝ่ายตรงข้าม” ที่อาจเป็นภัยต่อชาติ

2. การตรวจสอบการสื่อสาร อำนาจนี้อาจรวมถึงการตรวจสอบการสื่อสารของประชาชน ซึ่งสร้างความกังวลเกี่ยวกับการละเมิดความเป็นส่วนตัว

3. การคัดค้านจากภาคประชาสังคม กลุ่มประชาสังคมในอินโดนีเซียได้แสดงความไม่เห็นด้วยกับมาตรการเหล่านี้ สะท้อนถึงความกังวลของสาธารณชนต่อการใช้อำนาจที่อาจเกินขอบเขต

4. การประกาศใช้ท่ามกลางการคัดค้าน แม้จะมีเสียงคัดค้านแต่กฎหมายนี้ก็ยังถูกประกาศใช้ ซึ่งอาจบ่งชี้ถึงความไม่สมดุลระหว่างอำนาจรัฐและเสียงของประชาชน

ความพยายามในการปรับปรุงกฎหมายเกี่ยวกับการสอดแนมและความเป็นส่วนตัวในอินโดนีเซีย ตั้งแต่ปี 2557 เป็นต้นมา อินโดนีเซียได้แสดงให้เห็นถึงความพยายามอย่างต่อเนื่องในการปรับปรุงกรอบกฎหมายเกี่ยวกับการสอดแนมและความเป็นส่วนตัว รัฐสภาได้เสนอร่างกฎหมายหลายฉบับ เช่น ร่างพระราชบัญญัติว่าด้วยกระบวนการสกัดกั้น การให้ความช่วยเหลือทางกฎหมายร่วมกัน และการคุ้มครองข้อมูลส่วนบุคคลในระบบอิเล็กทรอนิกส์ ซึ่งได้รับการรับรองในปี 2559

กฎระเบียบของรัฐบาล 82 ได้กำหนดมาตรฐานสำหรับผู้ดำเนินการระบบอิเล็กทรอนิกส์ โดยกำหนดให้ต้องจ้างผู้เชี่ยวชาญที่มีคุณสมบัติเหมาะสม ซึ่งครอบคลุมทั้งบุคคล หน่วยงานรัฐ และองค์กรธุรกิจที่เกี่ยวข้องกับระบบอิเล็กทรอนิกส์

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (MCIT) มีบทบาทสำคัญในการกำหนดนโยบายด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ ในขณะที่กรมไปรษณีย์และโทรคมนาคม (DGPT) รับผิดชอบด้านการออกใบอนุญาตและการกำกับดูแล นอกจากนี้ ยังมีหน่วยงานกำกับดูแลโทรคมนาคมที่มีหน้าที่สร้างนโยบายการกำกับดูแลผ่านการมีส่วนร่วมของสาธารณะ

ในปี 2559 มีการแก้ไขกฎหมายว่าด้วยข้อมูลอิเล็กทรอนิกส์และธุรกรรมเพื่อรวมสิทธิที่จะถูกลืม โดยกำหนดให้ผู้ดำเนินการระบบอิเล็กทรอนิกส์ต้องลบข้อมูลที่ไม่จำเป็นตามคำขอที่ได้รับอนุมัติจากศาล

ความพยายามเหล่านี้แสดงให้เห็นถึงความตั้งใจของอินโดนีเซียในการปรับปรุงกฎหมายให้ทันสมัยและสอดคล้องกับความท้าทายด้านความเป็นส่วนตัวในยุคดิจิทัล อย่างไรก็ตาม ยังคงมีความท้าทายในการสร้างสมดุลระหว่างการคุ้มครองความเป็นส่วนตัวและความต้องการด้านความมั่นคงของรัฐ

คดี Tokopedia: จุดเปลี่ยนการคุ้มครองข้อมูลในอินโดนีเซีย

ปี 2020 เกิดเหตุการณ์ที่เขย่าวงการเทคโนโลยีอินโดนีเซีย เมื่อ Tokopedia ยักษ์ใหญ่อีคอมเมิร์ซของประเทศ ถูกฟ้องร้องในคดีละเมิดข้อมูลครั้งใหญ่ที่ส่งผลกระทบต่อผู้ใช้กว่า 15 ล้านคน!

ชุมชนผู้บริโภคชาวอินโดนีเซีย (KKI) ไม่รอช้า พวกเขายื่นฟ้อง Tokopedia และกระทรวงการสื่อสารฯ (MCI) ต่อศาล เรียกร้องให้เพิกถอนใบอนุญาตของ Tokopedia และปรับเงินมหาศาลถึง 100 พันล้านรูเปียห์

คดีนี้ไม่ใช่แค่เรื่องของ Tokopedia แต่เป็นการทดสอบครั้งสำคัญของระบบกฎหมายอินโดนีเซียในการรับมือกับภัยคุกคามทางไซเบอร์ มันเป็นสัญญาณเตือนว่าถึงเวลาแล้วที่ต้องจริงจังกับการปกป้องข้อมูลส่วนบุคคลในยุคดิจิทัล

ผลของคดีนี้อาจเปลี่ยนโฉมหน้าการคุ้มครองข้อมูลในอินโดนีเซีย บริษัทเทคโนโลยีอาจต้องยกระดับมาตรการรักษาความปลอดภัย ในขณะที่ภาครัฐอาจต้องเข้มงวดกับการกำกับดูแลมากขึ้น

2. มาเลเซีย: เสือแห่งอาเซียนผู้พิทักษ์ข้อมูลดิจิทัล

สิทธิความเป็นส่วนตัวในมาเลเซีย: เมื่อกฎหมายยังตามไม่ทันโลกดิจิทัล

เริ่มจากรัฐธรรมนูญที่ไม่ได้พูดถึงสิทธิความเป็นส่วนตัวตรงๆ แต่ศาลก็พยายามตีความให้เป็นส่วนหนึ่งของ “สิทธิในชีวิตและเสรีภาพ” ตามมาตรา 5(1) แถมยังอนุญาตให้ฟ้องร้องทางแพ่งในกรณีละเมิดความเป็นส่วนตัวได้ด้วย แต่นั่นก็ยังไม่พอ

ปัญหาใหญ่อยู่ที่กฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ที่มีช่องโหว่เยอะแยะ เพราะไม่ครอบคลุมหน่วยงานรัฐ แปลว่ารัฐเข้าถึงข้อมูลเราได้ง่าย ๆ และยังติดตามการเคลื่อนไหวของประชาชนได้อีกต่างหาก และไม่พูดถึงความเป็นส่วนตัวทางอินเทอร์เน็ตโดยตรง ทั้งเรื่องคุกกี้และข้อมูลตำแหน่งทั้งที่เราใช้เน็ตกันทุกวัน! แถมคนมาเลเซียเองก็ยังไม่ค่อยรู้วิธีปกป้องข้อมูลตัวเอง โดยเฉพาะตอนสมัครบริการออนไลน์หรือล็อกอินเข้าระบบต่างๆ เรียกว่าเสี่ยงโดนขโมยข้อมูลแบบไม่รู้ตัวเลยทีเดียว

อย่างไรก็ตาม ยังมีแสงสว่างปลายอุโมงค์อยู่บ้าง แม้ PDPA จะไม่พูดถึงความเป็นส่วนตัวทางอินเทอร์เน็ตโดยตรง แต่การประมวลผลข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์ใดๆ ในมาเลเซียก็ยังอยู่ภายใต้บังคับของ PDPA อยู่ดี

เมื่อข้อมูลส่วนตัวกลายเป็นสินค้า ในช่วงไม่กี่ปีที่ผ่านมา มาเลเซียเจอปัญหาการรั่วไหลของข้อมูลครั้งใหญ่หลายครั้ง แต่ที่ทำเอาทุกคนตาค้าง คือกรณีล่าสุด มีคนนำฐานข้อมูลขนาด 160 เมกะไบต์มาขายในตลาดมืดออนไลน์ ฐานข้อมูลนี้มีข้อมูลส่วนตัวของชาวมาเลเซียถึง 22.5 ล้านคน ครอบคลุมผู้ใหญ่ชาวมาเลเซียทุกคนที่เกิดระหว่างปี 1940 ถึง 2004 ที่น่ากลัวไปกว่านั้นคือ ผู้ขายอ้างว่าได้ข้อมูลนี้มาจาก MyIdentity API ซึ่งเป็นระบบของรัฐบาล! และนี่ไม่ใช่ครั้งแรก เพราะปีก่อนหน้านี้ก็มีการขายข้อมูลชาวมาเลเซียอีก 4 ล้านคนด้วย

เหตุการณ์นี้ชี้ให้เห็นว่าระบบรักษาความปลอดภัยข้อมูลของมาเลเซียยังมีช่องโหว่ใหญ่ แฮกเกอร์และอาชญากรไซเบอร์มองเห็นโอกาสทางธุรกิจจากข้อมูลส่วนตัวของประชาชน และประชาชนมาเลเซียกำลังเสี่ยงต่อการถูกละเมิดความเป็นส่วนตัวและอาชญากรรมทางการเงิน

กฎหมายคุ้มครองข้อมูลฉบับใหม่กำลังมา ย้อนกลับไปปี 2010 มาเลเซียเริ่มต้นด้วยการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ PDPA แต่พอใช้ไปสักพัก ก็เจอปัญหาเยอะ เลยต้องปรับปรุงใหม่ ปี 2020 มาเลเซียจัดรับฟังความเห็นจากประชาชน มีเรื่องที่ต้องแก้ตั้ง 22 ข้อ! แต่สุดท้ายก็เลือกมา 5 ข้อสำคัญที่สุด ตั้งใจว่าจะเสนอแก้กฎหมายในปี 2022 แต่มีการยุบสภาซะก่อน

ตอนนี้แม้จะยังไม่รู้ว่ากฎหมายใหม่จะเสร็จเมื่อไหร่ แต่อย่างน้อยก็เห็นว่ามาเลเซียกำลังพยายามปกป้องข้อมูลของประชาชนจริง ๆ

สิ่งที่น่าติดตามคือ กฎหมายใหม่จะช่วยป้องกันการรั่วไหลของข้อมูลได้ดีขึ้นไหม? จะรับมือกับภัยคุกคามทางไซเบอร์ยังไง? แม้จะต้องรอให้การเมืองนิ่งก่อน แต่นี่ก็เป็นสัญญาณที่ดีว่ามาเลเซียพร้อมปรับตัวเพื่อปกป้องประชาชนในยุคดิจิทัลแล้ว! เตรียมตัวรอชมกฎหมายใหม่กันได้เลย!

การคุ้มครองข้อมูลส่วนบุคคล: PDPA มาเลเซีย

มาเลเซียไม่เล่นเมื่อพูดถึงการคุ้มครองข้อมูลส่วนบุคคล โดยมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ที่วางกฎเกณฑ์ต่าง ๆ ชัดเจน เช่น ต้องขอความยินยอมก่อนใช้ข้อมูลใดๆ และต้องบันทึกไว้ด้วย สำหรับเด็กอายุต่ำกว่า 18 ปี ต้องขอความยินยอมจากผู้ปกครอง นอกจากนี้ยังมีหลักการคุ้มครองข้อมูลถึง 7 ข้อที่ผู้ใช้ข้อมูลต้องปฏิบัติตาม แสดงให้เห็นถึงความจริงจังในการสร้างความโปร่งใสและปกป้องสิทธิของเจ้าของข้อมูล โดยเฉพาะเด็กและเยาวชน

ขอบเขตการบังคับใช้ PDPA มาเลเซีย โดยปกติจะใช้เฉพาะในมาเลเซีย แต่ก็มีข้อยกเว้นสำหรับข้อมูลที่จะนำมาใช้ในประเทศ นอกจากนี้ยังครอบคลุมทั้งองค์กรในมาเลเซียและต่างชาติที่ใช้อุปกรณ์ในมาเลเซียประมวลผลข้อมูล (แต่ไม่รวมการส่งผ่าน)

PDPA ให้ความสำคัญกับทุกขั้นตอนการจัดการข้อมูล ตั้งแต่เก็บ ใช้ แก้ไข ส่งต่อ ไปจนถึงทำลาย แต่ก็มีข้อยกเว้น เช่น ข้อมูลที่ใช้โดยรัฐบาล หรือเพื่อกิจการส่วนตัวและครอบครัว

ทั้งนี้ PDPA มาเลเซียได้กำหนดนิยามครอบคลุมทุกมิติของข้อมูลส่วนบุคคลโดยนิยาม “การประมวลผล” อย่างกว้าง ตั้งแต่เก็บ ค้นคืน ใช้ ส่งต่อ ไปจนถึงทำลายข้อมูล แต่ก็มีข้อยกเว้น เช่น ข้อมูลที่ใช้โดยรัฐบาล หรือเพื่อกิจการส่วนตัวและครอบครัว

ที่น่าสนใจคือ PDPA ยังเพิ่มความรับผิดชอบให้ผู้เก็บข้อมูลด้วย ต้องแจ้งเหตุผลในการเก็บข้อมูล และเก็บบันทึกการเปิดเผยข้อมูลให้บุคคลที่สาม แถมในปี 2015 ยังมีการออกมาตรฐานเพิ่มเติม ครอบคลุมทั้งความปลอดภัย การเก็บรักษา และความถูกต้องของข้อมูล ทั้งในรูปแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์

เรามาลุ้นกันว่ามาเลเซียจะรับมือกับความท้าทายในยุคดิจิทัลได้ยังไง! ใครจะรู้ บางทีพวกเขาอาจจะกลายเป็นผู้นำด้านการคุ้มครองข้อมูลในภูมิภาคก็ได้! แต่ก็ต้องดูกันต่อไปว่าการปรับปรุงกฎหมายจะทันกับการเปลี่ยนแปลงของเทคโนโลยีหรือไม่ และจะสามารถคุ้มครองสิทธิของประชาชนได้อย่างมีประสิทธิภาพจริงหรือ

นโยบายและความริเริ่มของภาคส่วนต่าง ๆ

กล้องวงจรปิดและคลาวด์คอมพิวติ้ง ในปี 2014 มาเลเซียพยายามร่างแนวทางการใช้กล้องวงจรปิดให้สอดคล้องกับ PDPA เพื่อกำหนดมาตรฐานการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ใช้กล้องวงจรปิด แต่... ยังไม่เสร็จ! เรียกว่าตั้งใจดี แต่ยังไม่ถึงฝั่ง ทำให้ตอนนี้ยังไม่มีกฎชัด ๆ ว่าควรใช้กล้องวงจรปิดยังไงให้ไม่ละเมิดสิทธิส่วนบุคคล

ส่วนเรื่องคลาวด์คอมพิวติ้ง มาเลเซียจริงจังกว่า! มีมาตรฐาน PDP ที่วางกฎไว้ชัดเจน: อยากส่งข้อมูลขึ้น “เมฆ”? ต้องขออนุญาตเป็นลายลักษณ์อักษรก่อน, ส่งข้อมูลที่ไร ต้องจดบันทึกไว้ทุกครั้ง และต้องทำตามกฎหมายทั้งของมาเลเซียและประเทศที่ส่งข้อมูลไป

ความปลอดภัยไซเบอร์ ศึกไซเบอร์มาเลเซีย เมื่อแฮกเกอร์ท้าชนรัฐบาล ปี 2022 มาเลเซียสะเทือน! ข้อมูลลับของประชาชนหลุดจาฐานข้อมูลรัฐบาล เหมือนฝันร้ายที่กลายเป็นจริง เหตุการณ์นี้ไม่เพียงแต่สร้างความตื่นตระหนก แต่ยังนำไปสู่การตรวจสอบระบบคุ้มครองข้อมูลและความปลอดภัยทางไซเบอร์ของประเทศอย่างเข้มข้น

รัฐบาลมาเลเซียได้ประกาศแผนออกกฎหมายใหม่ ตั้งเป้าจะเสนอร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อรัฐสภาภายในมีนาคม 2023 กฎหมายนี้จะเป็นกรอบหลักในการควบคุมปัญหาความปลอดภัยทางไซเบอร์ของประเทศ และไม่ใช่แค่รัฐบาลที่ตื่นตัว ธนาคารกลางก็เข้าร่วมวงด้วย โดยเผยแพร่ร่างแนวทางการประเมินความเสี่ยงเทคโนโลยีคลาวด์ (CTRAG) เพื่อรับฟังความคิดเห็นสาธารณะ มุ่งเน้นการให้คำแนะนำแก่สถาบันการเงินในการระบุความเสี่ยงและพิจารณากลไกควบคุมเมื่อใช้บริการคลาวด์

มาเลเซียไม่ได้แค่ป้องกัน แต่ยังวางกฎเหล็กในการเข้าถึงข้อมูลด้วย หน่วยงานกำกับดูแลต้องปฏิบัติตามข้อกำหนดอย่างน้อยหนึ่งข้อ เช่น ได้รับอนุญาตจากเจ้าของข้อมูล หรือมีหมายศาล ก่อนจะเข้าถึงข้อมูลส่วนบุคคลได้ นอกจากนี้ ยังมีกฎพิเศษสำหรับข้อมูลที่อยู่ภายใต้กฎหมายต่างประเทศ ต้องได้รับคำสั่งศาลถึงที่สุดจากศาลในเขตอำนาจนั้นๆ ก่อน ถึงจะเปิดเผยได้ แสดงให้เห็นถึงความซับซ้อนในการจัดการข้อมูลข้ามพรมแดน

อีกทั้ง มาเลเซียยังมีพระราชบัญญัติความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญา (MACMA) ที่กำกับดูแลการร้องขอเปิดเผยข้อมูลจาหน่วยงานบังคับใช้กฎหมายต่างประเทศ แต่น่าเสียดายที่มีข้อมูลสถิติเปิดเผยน้อยมากเกี่ยวกับการให้ความช่วยเหลือจริง

แม้มาเลเซียจะพยายามอย่างหนักเพื่อปกป้องข้อมูลประชาชน แต่โลกไซเบอร์เปลี่ยนแปลงเร็วเกินคาด มาเลเซียจะตามทันไหม? และจะเกิดอะไรขึ้นต่อไป? นี่คือศึกไซเบอร์ที่ต้องจับตามองกันต่อไป!

การกำกับดูแล การตรวจสอบ และถ่วงดุล

ศึกไซเบอร์มาเลเซีย: เมื่อผู้พิทักษ์กลายเป็นผู้ล่า

มาเลเซียกำลังเผชิญวิกฤตศรัทธาครั้งใหญ่! ในขณะที่รัฐบาลประกาศแผนปกป้องคุ้มครองข้อมูลประชาชน กลับถูกกล่าวหาว่าเป็น “ผู้ล่า” เสียเอง!

เรื่องช็อกโลก! เอกสารรั่วไหลเผยว่ารัฐบาลมาเลเซียซื้อบริการสปายแวร์จากบริษัท ทีมแฮ็ก” ผู้เชี่ยวชาญด้านการสอดแนม ซึ่งมีชื่อเสียงในการให้บริการระบบสอดแนมแก่รัฐบาลทั่วโลก นี่เป็นหลักฐานชิ้นสำคัญที่แสดงให้เห็นว่ารัฐบาลอาจกำลังละเมิดสิทธิความเป็นส่วนตัวของประชาชนอย่างจงใจ

แต่นั่นยังไม่พอ! ในปี 2013 รัฐบาลแก้ไขพระราชบัญญัติการกระทำความผิดด้านการรักษาความปลอดภัย (SOSMA) ให้ตัวเองมีอำนาจดักฟังการสื่อสารและติดตามผู้ต้องขังด้วยกำไลข้อเท้าอิเล็กทรอนิกส์ ภายใต้พระราชบัญญัติป้องกันการก่อการร้าย (PoTA) เป็นการเพิ่มอำนาจการสอดส่องประชาชนอย่างชัดเจน

กฎหมายมาเลเซียยังให้อำนาจหน่วยงานบังคับใช้กฎหมายแบบไม่อั้น! มาตรา 116 ของประมวลกฎหมายวิธีพิจารณาความอาญา (CPC) ให้อำนาจอัยการสูงสุดสกัดกั้นการสื่อสารได้ถ้าเชื่อว่าเกี่ยวข้องกับอาชญากรรม โดยไม่ต้องขออนุญาตศาล! และมาตรา 81 ของพระราชบัญญัติภาษีเงินได้ปี 1976 (ITA) ก็ให้อำนาจคล้ายกัน

ที่น่าตกใจยิ่งกว่าคือ PDPA ที่ควรจะปกป้องข้อมูลประชาชน กลับมีข้อยกเว้นให้เปิดเผยข้อมูลได้ถ้าอ้างว่าเพื่อป้องกันและตรวจจับอาชญากรรม ทำให้เกิดช่องโหว่ใหญ่ในการคุ้มครองข้อมูลส่วนบุคคล

คำถามใหญ่ คือ ใครจะคุ้มครองประชาชนจากผู้คุ้มครอง ? มาเลเซียกำลังเดินบนเส้นบาง ๆ ระหว่างความมั่นคงของชาติและสิทธิส่วนบุคคล ศึกไซเบอร์ครั้งนี้ไม่ใช่แค่ระหว่างรัฐกับแฮกเกอร์อีกต่อไป แต่เป็นการต่อสู้ระหว่างรัฐกับประชาชนของตัวเอง! และผลลัพธ์จะเป็นอย่างไร ? เราต้องติดตามกันต่อไป ในมหากาพย์ไซเบอร์ที่กำลังเขย่าประเทศมาเลเซีย

คดีและการฟ้องคดีความเป็นส่วนตัวออนไลน์

มาเลเซียกำลังเผชิญความท้าทายครั้งใหญ่ในการปกป้องคุ้มครองสิทธิความเป็นส่วนตัวของประชาชนในยุคดิจิทัล แต่กฎหมาย PDPA ที่ควรจะเป็นเกราะป้องกัน กลับมีช่องโหว่ที่น่ากังวล

จุดอ่อนสำคัญของ PDPA คือไม่ได้ให้สิทธิประชาชนฟ้องร้องผู้ละเมิดข้อมูลส่วนตัวได้โดยตรง อย่างไรก็ตาม ยังมีช่องทางอื่นให้ดำเนินคดี เช่น ฟ้องเรื่องผิดสัญญารักษาความปลอดภัยข้อมูล หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

ที่น่าสนใจคือ ศาลมาเลเซียโดยทั่วไปไม่ยอมรับหลักการละเมิดความเป็นส่วนตัว มีเพียงบางกรณีเท่านั้นที่ศาลตัดสินว่ามีการละเมิด เช่น กรณีแพทย์เปิดเผยข้อมูลผู้ป่วย นอกจากนี้ PDPA ยังจำกัดขอบเขตเฉพาะเรื่องข้อมูลส่วนตัว ไม่ครอบคลุมสิทธิความเป็นส่วนตัวในภาพรวม

อย่างไรก็ตาม มีพัฒนาการที่น่าจับตามองเมื่อธันวาคม 2021 ศาลสูงตัดสินคดี Genting Malaysia Berhad ซึ่งเป็นครั้งแรกที่ท้าทายอำนาจรัฐในการขอข้อมูลส่วนตัวภายใต้ PDPA คำตัดสินนี้วางขอบเขตให้หน่วยงานรัฐในการเก็บข้อมูล นับเป็นก้าวสำคัญในการคุ้มครองสิทธิประชาชน

ประเด็นสำคัญคือ มาเลเซียจะปรับปรุงกฎหมายให้เข้มแข็งขึ้นได้อย่างไร? PDPA จะพัฒนาเป็นเครื่องมือที่มีประสิทธิภาพในการปกป้องประชาชน หรือจะยังคงมีช่องโหว่ให้เกิดการละเมิดสิทธิต่อไป?

การพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลของมาเลเซียจึงเป็นเรื่องที่น่าติดตาม เพราะไม่เพียงแต่เกี่ยวข้องกับเทคโนโลยี แต่ยังเป็นการต่อสู้เพื่อสิทธิขั้นพื้นฐานของประชาชนในยุคดิจิทัล

3. ฟิลิปปินส์: ความพยามของหมู่เกาะกับภัยคุกคามไซเบอร์

ข้อมูลส่วนตัวในยุคดิจิทัล: ฟิลิปปินส์บนเส้นด้ายแห่งความเสี่ยง

ฟิลิปปินส์กำลังเผชิญหน้ากับความท้าทายครั้งใหญ่ในการรักษาความลับของประชาชน! ในขณะที่เศรษฐกิจดิจิทัลพุ่งทะยานสู่อันดับหนึ่งของอาเซียน ภัยคุกคามทางไซเบอร์ก็กำลังคืบคลานเข้ามาอย่างน่าหวาดหวั่

ลองคิดดู ชาวฟิลิปปินส์ใช้เวลาออนไลน์มากที่สุดในโลก! แถมยังมีประชากรวัยหนุ่มสาว อินเทอร์เน็ตเข้าถึงง่าย และมือถือแทบจะมากกว่าคน นี่คือสวรรค์ของนักการตลาดดิจิทัล... แต่ก็เป็นสนามเด็กเล่นของเหล่าแฮกเกอร์เช่นกัน

เพียงปีเดียว การโจมตีทางไซเบอร์พุ่งกระฉูด! แรนซัมแวร์เพิ่ม 30% ภัยคุกคามต่อบริษัทเอกชนเพิ่ม 49% ฟิชชิ่งพุ่ง 200% และคดีฉ้อโกงออนไลน์เพิ่ม 37% แต่ที่น่าตกใจที่สุดคือการแฮ็กระบบของคณะกรรมการการเลือกตั้ง ทำให้ข้อมูลผู้มีสิทธิเลือกตั้งรั่วไหลถึง 60 กิกะไบต์!

แต่ฟิลิปปินส์ไม่ได้นิ่งนอนใจ พวกเขามีพระราชบัญญัติความเป็นส่วนตัวของข้อมูลตั้งแต่ปี 2012 และจัดตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแห่งชาติในปี 2016 เพื่อกำกับดูแลการใช้ข้อมูลส่วนบุคคลและลงโทษผู้ละเมิด

การคุ้มครองข้อมูลส่วนบุคคล: DPA ฟิลิปปินส์

ในปี 2012 ฟิลิปปินส์ได้เปิดศักราชใหม่แห่งการคุ้มครองข้อมูลส่วนบุคคล ด้วยการประกาศใช้พระราชบัญญัติความเป็นส่วนตัวของข้อมูล (Data Privacy Act of 2012) หรือที่รู้จักกันในชื่อรัฐบัญญัติที่ 10173 นับเป็นกฎหมายฉบับแรกของประเทศที่ครอบคลุมการคุ้มครองข้อมูลส่วนบุคคลอย่างรอบด้าน

เพื่อให้กฎหมายมีเขี้ยวเล็บในการบังคับใช้ ในต้นปี 2016 รัฐบาลฟิลิปปินส์ได้จัดตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแห่งชาติ (The National Privacy Commission: NPC) ขึ้น โดย NPC ได้ออกกฎและระเบียบการดำเนินการของรัฐบัญญัติที่ 10173 (Implementing Rules and Regulations: IRR) ซึ่งระบุรายละเอียดมาตรฐานที่ทั้งบุคคลและองค์กรต้องปฏิบัติตามในการประมวลผลข้อมูลส่วนบุคคล

IRR ไม่เพียงแต่กำหนดแนวทางปฏิบัติ แต่ยังระบุบทลงโทษสำหรับผู้ที่ละเมิดพระราชบัญญัติด้วย ทำให้กฎหมายนี้มีทั้งการป้องกันและการลงโทษ เป็นการสร้างระบบนิเวศที่ปลอดภัยสำหรับข้อมูลส่วนบุคคลของชาวฟิลิปปินส์

DPA ฟิลิปปินส์ ครอบคลุมแต่มีข้อยกเว้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของฟิลิปปินส์มีขอบเขตกว้างขวาง ครอบคลุมการจัดการข้อมูลส่วนบุคคลทุกรูปแบบ ไม่ว่าจะเป็นของบุคคลธรรมดาหรือนิติบุคคล แต่กฎหมายนี้ก็มีข้อยกเว้นที่น่าสนใจ

ประการแรก ข้อมูลที่เผยแพร่เพื่อประโยชน์สาธารณะไม่อยู่ภายใต้กฎหมายนี้ รวมถึงข้อมูลที่ใช้ในงานสื่อ ศิลปะ วรรณกรรม และการวิจัยเพื่อสาธารณะ นี่เป็นการปกป้องเสรีภาพในการแสดงออกและการทำงานของสื่อมวลชน

หน่วยงานรัฐก็ได้รับยกเว้นสำหรับข้อมูลที่จำเป็นในการปฏิบัติหน้าที่ ส่วนสถาบันการเงินก็มีข้อยกเว้นภายใต้กฎหมายเฉพาะ เช่น Republic Act No. 9510 ว่าด้วยการจัดตั้งระบบข้อมูลเครดิต ปี 2008 และ Republic Act No. 9160 ว่าด้วยการต่อต้านการฟอกเงิน ปี 2001

ที่น่าสนใจคือ ข้อมูลส่วนบุคคลที่มาจากต่างประเทศและเข้ามาตามกฎหมายของประเทศนั้น ก็ไม่อยู่ภายใต้กฎหมายนี้เช่นกัน

สำหรับสื่อสิ่งพิมพ์ แม้จะต้องปฏิบัติตามกฎหมายนี้ แต่ก็ได้รับการคุ้มครองในการไม่ต้องเปิดเผยแหล่งข่าวลับ

ข้อยกเว้นเหล่านี้สร้างความสมดุลระหว่างการคุ้มครองข้อมูลส่วนบุคคลและการรักษาเสรีภาพในด้านต่างๆ แต่ก็อาจเป็นช่องว่างให้เกิดการตีความและการใช้ประโยชน์ในทางที่ผิดได้ การบังคับใช้กฎหมายนี้จึงต้องอาศัยความรอบคอบและการพิจารณาอย่างรอบด้าน

สิทธิต่าง ๆ ของเจ้าของข้อมูลภายใต้ DPA เจ้าของข้อมูลมีสิทธิต่าง ๆ ที่สำคัญตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของฟิลิปปินส์

อันดับแรกคือสิทธิที่จะได้รับแจ้งเมื่อมีการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเอง โดยเจ้าของข้อมูลจะได้รับข้อมูลที่ชัดเจนและโปร่งใสเกี่ยวกับการใช้ข้อมูลของพวกเขา

นอกจากนี้ เจ้าของข้อมูลยังมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเองอย่างสมเหตุสมผล ซึ่งหมายความว่าพวกเขาสามารถทราบได้ว่าใครบ้างที่สามารถเข้าถึงข้อมูลส่วนบุคคลของตน เช่น ตัวตนของผู้ควบคุมข้อมูล (PIC) หรือผู้ประมวลผลข้อมูล (PIP)

สิทธิในการแก้ไขข้อมูลก็เป็นสิทธิที่สำคัญ เจ้าของข้อมูลสามารถโต้แย้งความไม่ถูกต้องหรือข้อผิดพลาดในข้อมูลส่วนบุคคลและขอให้ผู้ควบคุมข้อมูลแก้ไขให้ถูกต้องภายในระยะเวลาอันสมควร

ในกรณีที่เจ้าของข้อมูลต้องการลบข้อมูล พวกเขามีสิทธิในการระงับ เพิกถอน หรือสั่งการบล็อก การลบ หรือการทำลายข้อมูลส่วนบุคคลออกจากระบบการจัดเก็บของผู้ควบคุมข้อมูลได้

หากเจ้าของข้อมูลไม่ต้องการให้ข้อมูลส่วนบุคคลของตนถูกประมวลผล พวกเขามีสิทธิในการคัดค้านหรือไม่เข้าร่วมการประมวลผลข้อมูล รวมถึงการตลาดทางตรง การประมวลผลแบบอัตโนมัติ และการจัดทำโปรไฟล์

นอกจากนี้ เจ้าของข้อมูลยังมีสิทธิในการเคลื่อนย้ายข้อมูล สามารถขอสำเนาข้อมูลส่วนบุคคลของตนจากผู้ควบคุมข้อมูลในรูปแบบอิเล็กทรอนิกส์หรือโครงสร้างที่ใช้โดยทั่วไปเพื่อการใช้งานต่อไปได้

สิทธิที่จะไม่อยู่ภายใต้การตัดสินใจโดยอัตโนมัติเป็นอีกสิทธิหนึ่งที่เจ้าของข้อมูลมี เจ้าของข้อมูลสามารถคัดค้านการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติได้

สุดท้าย สิทธิอื่น ๆ ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของฟิลิปปินส์รวมถึงสิทธิในการชดเชยความสูญเสียที่เกิดขึ้นเนื่องจากการใช้ข้อมูลส่วนบุคคลที่ไม่ถูกต้อง ไม่สมบูรณ์ ล้าสมัย เป็นเท็จ ได้มาอย่างผิดกฎหมาย หรือไม่ได้รับอนุญาต และสิทธิในการยื่นเรื่องร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (NPC)

การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในฟิลิปปินส์

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแห่งชาติ (NPC) ของฟิลิปปินส์ได้ออกประกาศฉบับที่ 2022-01 ซึ่งกล่าวถึงค่าปรับทางปกครองสำหรับการละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดย NPC มีสิทธิกำหนดค่าปรับสำหรับการละเมิดร้ายแรงได้ตั้งแต่ 0.5% ถึง 3% ของรายได้รวมประจำปี หรือ 0.25% ถึง 2% ของรายได้สุทธิประจำปีของผู้ควบคุมหรือผู้ประมวลผลข้อมูล

นอกจากนี้ การละเมิดอื่น ๆ เช่น การไม่ลงทะเบียนข้อมูลที่แท้จริง ระบบประมวลผลข้อมูล หรือข้อมูลเกี่ยวกับการตัดสินใจอัตโนมัติ อาจถูกปรับสูงสุดถึง 200,000 เปโซ (ประมาณ 4,000 ดอลลาร์สหรัฐ) หรือ 50,000 เปโซ (ประมาณ 1,000 ดอลลาร์สหรัฐ) ขึ้นอยู่กับลักษณะของการละเมิด

กิจกรรม: ทบทวนมาตรการบังคับใช้ในการคุ้มครองข้อมูลและความปลอดภัยทางไซเบอร์ที่กล่าวถึงข้างต้น และหารือว่าค่าปรับและบทลงโทษสามารถทำหน้าที่เป็นแรงจูงใจตามความเป็นจริงสำหรับบริษัทดิจิทัลในการปฏิบัติตามข้อกำหนดการประมวลผลข้อมูลและความปลอดภัยทางไซเบอร์หรือไม่ ค่าปรับสูงพอที่จะขัดขวางและทำให้บริษัทดิจิทัลปฏิบัติตามกฎหมายได้หรือไม่?

นโยบายและการริเริ่มของภาคส่วนต่าง ๆ

การคุ้มครองผู้บริโภค ในปี 2008 กระทรวงการค้าและอุตสาหกรรม, กระทรวงเกษตร, และกระทรวงสาธารณสุขของฟิลิปปินส์ได้ออกคำสั่งทางปกครองร่วม DTI-DOH-DA หมายเลข 01 เพื่อดำเนินการตามพระราชบัญญัติผู้บริโภค (พระราชบัญญัติสาธารณรัฐหมายเลข 7394) และพระราชบัญญัติอีคอมเมิร์ซ (พระราชบัญญัติสาธารณรัฐหมายเลข 8792) คำสั่งนี้มีจุดประสงค์เพื่อปกป้องผู้บริโภคในการทำธุรกรรมออนไลน์ รวมถึงการซื้อสินค้าและบริการ และใช้กับผู้ค้าปลีกและผู้ขายทั้งในประเทศและต่างประเทศที่เกี่ยวข้องกับอีคอมเมิร์ซ

คำสั่งนี้กำหนดให้ผู้ค้าปลีก, ผู้ขาย, ผู้จัดจำหน่าย, ซัพพลายเออร์, และผู้ผลิตที่เข้าร่วมในการค้าอิเล็กทรอนิกส์ต้องหลีกเลี่ยงการโฆษณาที่ฉ้อโกง หลอกลวง หรือทำให้เข้าใจผิดจัดเตรียมข้อมูลที่ยุติธรรม ถูกต้อง โปร่งใส และเข้าถึงได้ฟรี โดยให้รายละเอียดเกี่ยวกับลักษณะ คุณภาพ และปริมาณของสินค้าหรือบริการที่ขายให้ข้อมูลที่เพียงพอสำหรับผู้บริโภคในการตัดสินใจว่าจะเข้าร่วมในการทำธุรกรรมหรือไม่ และให้ข้อมูลที่ช่วยให้ผู้บริโภคสามารถเก็บบันทึกข้อมูลเกี่ยวกับสินค้าและบริการที่ขายได้อย่างเพียงพอ

นอกจากนี้ เจ้าของข้อมูลยังต้องได้รับข้อมูลที่ชัดเจนเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของตนเพื่อวัตถุประสงค์ทางการตลาดทางตรง และมีสิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนเพื่อวัตถุประสงค์ทางการตลาดทางตรง

ในปี 2022 NPC และหน่วยงานภาครัฐอื่น ๆ ยังได้เผยแพร่คำสั่งบริหารร่วมหมายเลข 2022-01 ซึ่งเป็นแนวปฏิบัติสำหรับธุรกิจออนไลน์ เพื่อย้ำถึงกฎหมายและข้อบังคับที่ใช้บังคับกับธุรกิจและผู้บริโภคออนไลน์ แนวปฏิบัตินี้กำหนดหน้าที่ของผู้ขายออนไลน์ ผู้ค้า และผู้ค้าปลีกอิเล็กทรอนิกส์ภายใต้ DPA และพยายามรับประกันการปกป้องความเป็นส่วนตัว ความโปร่งใส และความได้สัดส่วนในการรวบรวมและประมวลผลข้อมูล

การกำกับดูแล การตรวจสอบ และถ่วงดุล

การเฝ้าระวังกลายเป็นประเด็นที่น่ากังวลมากขึ้นในฟิลิปปินส์ แม้ว่ารัฐธรรมนูญจะรับรองความเป็นส่วนตัวในการสื่อสาร แต่ประธานาธิบดีได้ลงนามในพระราชบัญญัติต่อต้านการก่อการร้ายปี 2020 ซึ่งแทนที่พระราชบัญญัติความมั่นคงของมนุษย์ปี 2007 กฎหมายใหม่นี้ขยายคำนิยามของการก่อการร้ายและให้อำนาจเจ้าหน้าที่ในการเฝ้าระวังบุคคลที่สงสัยว่าก่อการร้ายเป็นเวลา 60 วัน และขยายเวลาได้อีก 30 วัน นอกจากนี้ ผู้ที่สงสัยว่าช่วยเหลือกลุ่มก่อการร้ายก็อาจถูกติดตามด้วย กลุ่มภาคประชาสังคมกังวลว่ากฎหมายนี้อาจถูกใช้เพื่อเฝ้าติดตามผู้วิจารณ์รัฐบาล โดยเฉพาะองค์กรฝ่ายซ้ายที่มักถูกเรียกว่าเป็นองค์กรก่อการร้าย ศาลฎีกาได้รับคำร้อง 37 ฉบับที่ท้าทายกฎหมายนี้ และในเดือนธันวาคม 2021 ศาลได้ยืนยันความชอบด้วยกฎหมายของพระราชบัญญัติโดยยกเลิกเพียงบางส่วนที่คำนิยามการก่อการร้ายอย่างกว้างขวางเกินไป

รัฐบาลฟิลิปปินส์ยังเพิ่มขีดความสามารถในการติดตามช่องทางสื่อสังคมออนไลน์ โดยในเดือนมกราคม 2019 กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (DICT) ได้มอบสัญญาให้บริษัท Integrated Computer Systems, Inc. และ Verint Systems, Ltd. เพื่อพัฒนาระบบจัดการความปลอดภัยทางไซเบอร์ (CMS) ที่รวมถึงการติดตามสื่อสังคมออนไลน์แบบเกือบเรียลไทม์ แม้ในช่วงเลือกตั้ง เพื่อค้นหาข้อมูลบิดเบือนและภัยคุกคามอื่น ๆ

ในเดือนกุมภาพันธ์ 2022 รัฐสภาผ่านกฎหมายลงทะเบียนซิมการ์ดฉบับใหม่ กำหนดให้ต้องลงทะเบียนซิมการ์ดก่อนการขายและเปิดใช้งาน และให้ผู้ให้บริการบัญชีสื่อสังคมออนไลน์ต้องขอชื่อจริงและหมายเลขโทรศัพท์จากผู้ลงทะเบียน แต่ไม่ได้กำหนดบทลงโทษสำหรับการไม่ปฏิบัติตาม อย่างไรก็ตาม ผู้ที่ใช้ข้อมูลเท็จในการสร้างโปรไฟล์สื่อสังคมออนไลน์จะถูกจำคุกอย่างน้อย 6 ปี หรือปรับ 200,000 เปโซ (ประมาณ 3,800 ดอลลาร์สหรัฐ) หรือทั้งจำทั้งปรับ ผู้สนับสนุนร่างกฎหมายกล่าวว่าการลงทะเบียนนี้จำเป็นเพื่อต่อสู้กับ การใช้โทรลล์ คำพูดสร้างความเกลียดชัง และการหมิ่นประมาท แต่ในเดือนเมษายน 2022 ประธานาธิบดีดูเตอร์เตได้ปฏิเสธมาตรการนี้เนื่องจากข้อกำหนดที่บังคับให้ลงทะเบียนบัญชีสื่อสังคมออนไลน์ ซึ่งเขาเห็นว่าอาจนำไปสู่การแทรกแซงและการตรวจสอบจากรัฐบาล กลุ่มต่าง ๆ เช่น Foundation for Media

Alternatives, Democracy.net.ph และสหภาพผู้เชี่ยวชาญคอมพิวเตอร์ ได้ออกความเห็นเรียกร้องให้ประธานาธิบดีคัดค้านมาตรการนี้เนื่องจากอันตรายที่อาจเกิดขึ้นต่อเสรีภาพในการแสดงออกและสิทธิความเป็นส่วนตัว

คดีและการฟ้องคดีความเป็นส่วนตัวออนไลน์

ในคดี Cadajas v. People of the Philippines (GR No. 247348, 2021) ศาลฎีกาฟิลิปปินส์ตัดสินว่า สิทธิในความเป็นส่วนตัวภายใต้รัฐธรรมนูญไม่สามารถบังคับใช้ได้ในกรณีที่ภาพหน้าจอถูกเก็บรวบรวมโดยบุคคลธรรมดาไม่ใช่เจ้าหน้าที่ของรัฐ กฎหมายที่เกี่ยวข้องคือประมวลกฎหมายแพ่งของฟิลิปปินส์ (พระราชบัญญัติสาธารณรัฐหมายเลข 386) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (DPA) ซึ่งอนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อนได้ในกรณีที่จำเป็นต่อการพิจารณาความรับผิดทางอาญาของเจ้าของข้อมูล และเพื่อปกป้องสิทธิทางกฎหมายในการดำเนินคดีในศาล

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแห่งชาติ (NPC) ได้ออกความเห็นเชิงแนะนำฉบับที่ 2018-084 ซึ่งระบุว่า การติดตามพฤติกรรมของพนักงานบนคอมพิวเตอร์ของบริษัทอาจเป็นไปได้ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (DPA) หากเป็นไปตามเงื่อนไขในมาตรา 12 และ/หรือ 13 ของกฎหมายนี้ ความเห็นนี้ชี้แจงว่า “การเฝ้าระวังลับ” ถือเป็นสิ่งที่ไม่พึงประสงค์ นายจ้างต้องอธิบายการดำเนินการติดตามให้พนักงานทราบอย่างชัดเจน รวมถึงวัตถุประสงค์ ขอบเขต วิธีการ มาตรการรักษาความปลอดภัย และขั้นตอนการแก้ไขกรณีละเมิดสิทธิของพนักงาน ข้อมูลที่ได้รับจากการติดตามจะต้องตอบสนองวัตถุประสงค์โดยตรงและสอดคล้องกับความต้องการและเป้าหมายขององค์กรอย่างชัดเจน แนวทางนี้มีจุดมุ่งหมายเพื่อสร้างสมดุลระหว่างความต้องการของนายจ้างในการติดตามการใช้ทรัพยากรของบริษัทกับการคุ้มครองสิทธิความเป็นส่วนตัวของพนักงาน

กิจกรรม: อ่านข้อเท็จจริงของคดีและหารือว่าพวกเขาเห็นด้วยกับเหตุผลของศาลหรือไม่ และเพราะเหตุใด

ในคำพิพากษาปี 2565 ศาลฎีกาฟิลิปปินส์ตัดสินว่าภาพและข้อมูลอื่น ๆ ที่ได้จากบัญชีแอปพลิเคชันส่งข้อความของบุคคลสามารถใช้เป็นหลักฐานในคดีอาญาได้ โดยปฏิเสธข้อกล่าวอ้างของจำเลยว่าเป็นการละเมิดสิทธิความเป็นส่วนตัว

คดีนี้ชื่อ Cadajas v. People (2564) เกี่ยวกับบุคคลที่ถูกตัดสินว่ามีความผิดฐานครอบครองสื่อลามกอนาจารเด็ก ผู้ปกครองของเด็กได้นำภาพและบทสนทนาจากบัญชี Facebook Messenger ของจำเลยมาเป็นหลักฐาน โดยพบว่าจำเลยได้ให้เด็กเข้าถึงบัญชีของตน

จำเลยโต้แย้งว่าหลักฐานดังกล่าวได้มาโดยละเมิดสิทธิความเป็นส่วนตัวของตน จึงไม่ควรรับฟังเป็นพยานหลักฐาน แต่ศาลไม่เห็นด้วย

ศาลได้อภิปรายเกี่ยวกับสิทธิความเป็นส่วนตัว โดยเน้นที่ความเป็นส่วนตัวของข้อมูล โดยวินิจฉัยว่าสิทธิตามรัฐธรรมนูนคุ้มครองบุคคลจากการล่วงละเมิดของรัฐเท่านั้น ไม่ใช่จากบุคคลอื่น ในกรณีหลังจะใช้ประมวลกฎหมายแพ่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และกฎหมายอื่นที่เกี่ยวข้อง

ศาลให้เหตุผลว่า การประมวลผลข้อมูลส่วนบุคคลในคดีนี้ชอบด้วยกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ด้วยเหตุผลสองประการ: (1) เกี่ยวข้องกับการพิจารณาความรับผิดทางอาญาของจำเลย และ (2) จำเป็นต่อการคุ้มครองสิทธิและผลประโยชน์ตามกฎหมายของบุคคลในกระบวนการยุติธรรม

ท้ายที่สุด ศาลได้นำหลักการ “ความคาดหวังที่สมเหตุสมผลในความเป็นส่วนตัว” มาพิจารณา และสรุปว่าในคดีนี้ไม่มีการละเมิดความเป็นส่วนตัว

ที่มา: https://www.ateneo.edu/news/2022/07/11/the-cadajas-case-and-data-privacy

4. ประเทศไทย: ก้าวใหม่ PDPA สู่มาตรฐานสากล

สิทธิในความเป็นส่วนตัวในระบบกฎหมายของประเทศไทย

ในระบบกฎหมายของประเทศไทย สิทธิในความเป็นส่วนตัวได้รับการยอมรับและคุ้มครองอย่างต่อเนื่อง โดยการรับรองสิทธินี้มีอยู่ในรัฐธรรมนูญ ซึ่งหมายความว่าทุกคนมีสิทธิได้รับการคุ้มครองจากการใช้ข้อมูลส่วนบุคคลโดยไม่ชอบธรรม การละเมิดสิทธิในความเป็นส่วนตัวที่กำหนดในรัฐธรรมนูญ ซึ่งส่งผลให้เกิดความเสียหายต่อผู้อื่น ถือเป็นการละเมิดตามประมวลกฎหมายแพ่งและพาณิชย์ อย่างไรก็ตาม ยังไม่มีคำพิพากษาของศาลที่ตีความบทบัญญัติของรัฐธรรมนูญในลักษณะนี้อย่างชัดเจน

นอกจากนี้ ประเทศไทยได้ให้สัตยาบันต่อกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) โดยไม่มีข้อสงวนในมาตรา 17 ซึ่งเกี่ยวข้องกับสิทธิในความเป็นส่วนตัว และมาตรา 19 เกี่ยวกับเสรีภาพในการแสดงออก อีกทั้ง ประเทศไทยยังได้ร่วมกับประเทศสมาชิกอาเซียนอื่น ๆ รับรองปฏิญญาอาเซียนว่าด้วยสิทธิมนุษยชนในปี 2012 ซึ่งรับรองสิทธิในความเป็นส่วนตัวไว้ในมาตรา 21

PDPA ประเทศไทย

การคุ้มครองข้อมูล สภานิติบัญญัติแห่งชาติของไทยได้ผ่านพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act 2022: PDPA) มีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน 2565 นับเป็นกฎหมายฉบับแรกที่ควบคุมการเก็บรวบรวม ใช้ เปิดเผย และโอนข้อมูลส่วนบุคคลข้ามประเทศอย่างครอบคลุม

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ก่อตั้งขึ้นในปี 2022 และได้จัดการรับฟังความคิดเห็นสาธารณะหลายครั้งเกี่ยวกับกฎหมายลำดับรองซึ่งบางฉบับได้รับการประกาศใช้แล้ว ขณะที่บางฉบับยังอยู่ระหว่างการพิจารณา PDPC ได้ออกกฎระเบียบย่อยและคำแนะนำภายใต้ PDPA อย่างเป็นทางการ ส่วนร่างกฎระเบียบอื่นๆ ยังอยู่ในระหว่างการพิจารณา

หลักการของ PDPA ได้รับอิทธิพลจาก GDPR ของสหภาพยุโรป แต่มีความแตกต่างบางประการ PDPA เน้นสิทธิของเจ้าของข้อมูลในการควบคุมการรวบรวม จัดเก็บ ประมวลผล และเผยแพร่ข้อมูลส่วนบุคคล กำหนดเหตุผลทางกฎหมายสำหรับการประมวลผลข้อมูล และระบุภาระผูกพันของผู้ควบคุมและผู้ประมวลผลข้อมูล แม้จะนำองค์ประกอบจาก GDPR มาใช้ แต่ PDPA มีแนวทางที่แตกต่างโดยเฉพาะในเรื่องความยินยอม

PDPA ใช้กับทุกองค์กรที่รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในประเทศไทย หรือของผู้มีถิ่นที่อยู่ในประเทศไทย ขอบเขตนอกอาณาเขตของ PDPA ทำให้เกิดความรับผิดชอบเพิ่มขึ้นในการคุ้มครองข้อมูลของประเทศไทย โดยรวมการประมวลผลทั้งหมดที่เกี่ยวข้องกับเจ้าของข้อมูลที่อยู่ในประเทศไทย

ฐานทางกฎหมายสำหรับการรวบรวมและการประมวลผลข้อมูล การเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูล เว้นแต่มีเหตุผลทางกฎหมายอื่น เช่น การทำสัญญา ข้อกำหนดทางกฎหมาย หรือผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูล

PDPA แยกแยะฐานทางกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลที่ละเอียดอ่อน โดยข้อมูลส่วนบุคคลที่ละเอียดอ่อนต้องได้รับความยินยอมอย่างชัดแจ้งในการเก็บ ใช้ และเปิดเผย การขอความยินยอมต้องทำเป็นลายลักษณ์อักษรหรือทางอิเล็กทรอนิกส์ แยกจากข้อความอื่น ใช้ภาษาที่เข้าใจง่าย และไม่หลอกลวง เจ้าของข้อมูลต้องให้ความยินยอมโดยสมัครใจและไม่เป็นเงื่อนไขในการทำสัญญา

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถกำหนดรูปแบบและคำแถลงสำหรับการขอความยินยอมได้ อย่างไรก็ตาม การปฏิบัติตามกฎหมายผ่านแบบฟอร์มที่กำหนดอาจทำได้ยาก เนื่องจากผู้ควบคุมข้อมูลอาจออกแบบกระบวนการขอและประเมินความยินยอมของตนเอง

ความยินยอมและการแจ้งเตือนตาม PDPA การให้ความยินยอมของเจ้าของข้อมูลต้องชัดเจนและแสดงออกอย่างเป็นรูปธรรม เช่น การติ๊กถูกในช่องการชี้สองครั้งบนหน้าจอ หรือการปัดหน้าจอเพื่อยินยอม เจ้าของข้อมูลมีสิทธิในการปฏิเสธหรือเพิกถอนความยินยอมได้ตลอดเวลา และเมื่อมีการปฏิเสธหรือเพิกถอน ผู้ควบคุมข้อมูลต้องหยุดการประมวลผลข้อมูลทันที

ก่อนหรือขณะเก็บรวบรวมข้อมูล ผู้ควบคุมข้อมูลต้องแจ้งเจ้าของข้อมูลเกี่ยวกับการเก็บข้อมูลส่วนบุคคลหรือข้อมูลส่วนบุคคลที่ละเอียดอ่อน ข้อมูลที่ต้องแจ้งให้ทราบรวมถึงกลุ่มบุคคลหรือหน่วยงานที่จะได้รับข้อมูล และวัตถุประสงค์ในการเก็บรวบรวมข้อมูล ธุรกิจขนาดกลางและขนาดย่อม (SMEs) ก็ต้องปฏิบัติตาม PDPA แม้ว่าจะไม่มีข้อยกเว้นสำหรับธุรกิจประเภทนี้ (หมายเหตุผู้แปล: อาจมีข้อยกเว้นตามประกาศ)

ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลมีความรับผิดชอบที่แตกต่างกัน โดยทั่วไป ผู้ประมวลผลข้อมูลจะมีหน้าที่น้อยกว่าผู้ควบคุมข้อมูล แต่หากผู้ประมวลผลข้อมูลไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล อาจถูกถือเป็นผู้ควบคุมข้อมูลได้

การกำกับดูแล การตรวจสอบ และถ่วงดุล

จากข้อมูลของ Freedom House (2021) ระบุว่ารัฐบาลไทยติดตามการสื่อสารส่วนตัวและโซเชียลมีเดียเป็นประจำ โดยมีการกำกับดูแลที่จำกัด ระบบกฎที่ซับซ้อนมุ่งควบคุมการสื่อสารทางอินเทอร์เน็ตและขาดกรอบกฎหมายที่ชัดเจนในการกำหนดความรับผิดชอบและความโปร่งใสของรัฐบาล

มาตรา 4(2) ของ PDPA ยกเว้นข้อมูลที่รวบรวมภายใต้พระราชบัญญัติความปลอดภัยทางไซเบอร์จากการคุ้มครองภายใต้ PDPA พระราชบัญญัติความปลอดภัยทางไซเบอร์ให้สิทธิแก่รัฐบาลในการเข้าถึงข้อมูลส่วนบุคคลอย่างกว้างขวาง โดยไม่ต้องมีการควบคุมดูแลจากศาล สำหรับ “ความเสี่ยงระดับวิกฤติ” เจ้าหน้าที่สามารถเข้าถึงและดึงข้อมูลจากระบบคอมพิวเตอร์ได้โดยไม่จำเป็นต้องแจ้งเจ้าของข้อมูล และไม่มีการป้องกันความเป็นส่วนตัวที่ชัดเจน

พระราชบัญญัติข่าวกรองแห่งชาติปี 2019 ให้อำนาจแก่สำนักข่าวกรองแห่งชาติในการรวบรวมข้อมูลที่อาจส่งผลต่อ “ความมั่นคงของชาติ” โดยสามารถใช้วิธีการต่างๆ รวมถึงเทคโนโลยีเพื่อรวบรวมข้อมูล นายกรัฐมนตรีรับผิดชอบในการบังคับใช้กฎหมายนี้

เพื่อรับมือกับการแพร่ระบาดของไวรัสโควิด-19 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) เปิดตัวแอปพลิเคชันติดตามบุคคลที่เดินทางกลับประเทศไทย แอปนี้จำเป็นต้องกรอกข้อมูลส่วนบุคคล แม้จะมีการเก็บข้อมูลอย่างชัดเจนจนสิ้นสุดการกักกัน แต่การขาดความชัดเจนเกี่ยวกับการใช้ข้อมูลทำให้เกิดประเด็นด้านสิทธิความเป็นส่วนตัว แอปพลิเคชัน เช่น หมอชนะ และไทยชนะ มีข้อวิจารณ์เกี่ยวกับช่องโหว่ในนโยบายความเป็นส่วนตัวและขาดความเปิดกว้าง

ผู้ให้บริการต้องปฏิบัติตามมาตรา 15 ของพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ (CCA) ซึ่งอาจเสี่ยงต่อการถูกปรับตามมาตรา 14 หากไม่ควบคุมหรืออนุญาตให้เจ้าหน้าที่เข้าถึงข้อมูลของผู้ใช้ CCA 2007 กำหนดให้ผู้ให้บริการเก็บข้อมูลการรับส่งข้อมูลคอมพิวเตอร์ได้นานถึงสองปี และต้องเก็บข้อมูลที่ช่วยระบุตัวตนผู้ใช้ไว้ไม่น้อยกว่า 90 วัน

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) กำหนดให้สถานที่ที่ให้บริการ Wi-Fi สาธารณะต้องบันทึกข้อมูลผู้ใช้เพื่อป้องกันการเผยแพร่ข้อมูลอันเป็นเท็จ

มาตรา 4 ของ PDPA ยกเว้นการดำเนินการของหน่วยงานรัฐที่เกี่ยวข้องกับความมั่นคงของชาติและการรักษาความปลอดภัยทางไซเบอร์ รวมถึงสภาผู้แทนราษฎรและคณะกรรมการที่จัดตั้งขึ้น

มติคณะรัฐมนตรีปี 2555 ให้คณะกรรมการสอบสวนพิเศษ (DSI) มีอำนาจในการสกัดกั้นการสนทนาออนไลน์และรับข้อมูลส่วนบุคคลโดยไม่ต้องมีหมายศาล

พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 อนุญาตให้สำนักข่าวกรองแห่งชาติสั่งให้ผู้ให้บริการจัดหาเนื้อหาที่ร้องขอ แม้จะเป็นข้อมูลส่วนบุคคล ข้อมูลรั่วไหลเมื่อเดือนมิถุนายน 2563 ระบุว่ารัฐบาลใช้การวิเคราะห์ข้อมูลขนาดใหญ่เพื่อติดตามการแพร่กระจายของไวรัส รวมถึงการเข้าถึงข้อมูลตำแหน่งจากผู้ให้บริการโทรคมนาคม

กิจกรรม: อภิปรายว่า COVID19 ส่งผลกระทบต่อความเป็นส่วนตัวของข้อมูลของพลเมืองอย่างไร จากการที่หน่วยงานสาธารณะได้เริ่มปรับใช้แอปบนอุปกรณ์เคลื่อนที่เพื่อติดตามความเคลื่อนไหวของประชาชน อภิปรายว่าการแพร่ระบาดของโควิด 19 มีอิทธิพลต่อแนวการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยหรือไม่ อย่างไร และทนายความและองค์กรภาคประชาสังคมจะต่อสู้กับแนวโน้มนี้ได้อย่างไร

ในปี 2561 กสทช. ได้กำหนดให้ผู้ให้บริการโทรศัพท์มือถือทุกรายต้องรวบรวมลายนิ้วมือหรือสแกนใบหน้าจากผู้ลงทะเบียนซิมการ์ดใหม่ ข้อมูลทั้งหมดจะถูกส่งไปยังที่เก็บข้อมูลกลางของ กสทช. ผู้ใช้ซิมการ์ดใหม่ต้องดำเนินการตามขั้นตอนนี้ ส่วนผู้ใช้ซิมการ์ดเดิมจะต้องลงทะเบียนใหม่ ข้อกำหนดนี้ได้รับการบังคับใช้อย่างเข้มงวดในจังหวัดชายแดนภาคใต้ของประเทศไทย รวมถึงจังหวัดยะลา ปัตตานี นราธิวาส และ 3 อำเภอในจังหวัดสงขลา ตั้งแต่ปี 2562 ผู้ที่ไม่ลงทะเบียนซิมการ์ดด้วยการสแกนใบหน้าไม่สามารถใช้บริการโทรศัพท์มือถือได้ ข้อบังคับนี้ส่งผลให้โทรศัพท์จำนวนหนึ่งถูกระงับการให้บริการในเดือนเมษายน 2563 โดยองค์กรภาคประชาสังคมและผู้สนับสนุนสิทธิมนุษยชนได้แสดงความกังวลเกี่ยวกับผลกระทบต่อความเป็นส่วนตัวและเสรีภาพ รวมถึงการรวบรวมข้อมูลในชุมชนมุสลิมในท้องถิ่น

ตามมาตรา 18(7) ของพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ (CCA) ที่แก้ไขเพิ่มเติม รัฐบาลสามารถสั่งให้ทำลายมาตรการการเข้ารหัสและถอดรหัสข้อมูลคอมพิวเตอร์ได้โดยไม่ต้องมีหมายศาล ข้อกำหนดเหล่านี้อาจเป็นอันตรายต่อการคุ้มครองข้อมูลและสิทธิความเป็นส่วนตัวในสภาพแวดล้อมดิจิทัล

นโยบายและการริเริ่มของภาคส่วนต่าง ๆ

ความปลอดภัยทางไซเบอร์ในปี 2562 ประเทศไทยได้ออกพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSA) โดยมีวัตถุประสงค์หลักในการรับประกันความมั่นคงของชาติในโลกไซเบอร์ ผ่านการจัดการฐานข้อมูลและข้อมูลจากภาครัฐและเชิงพาณิชย์ พระราชบัญญัตินี้กำหนดให้มีการจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กพช.) นำโดยนายกรัฐมนตรี ซึ่งจะกำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์และกำกับดูแลการดำเนินการ การเพิ่มกรอบมาตรฐานหลักเกณฑ์ด้านความปลอดภัยภายในสิ้นปี 2566 จะครอบคลุมองค์กร 120 แห่งที่เชื่อมโยงกับโครงสร้างพื้นฐานข้อมูลที่สำคัญ (CII) เพิ่มขึ้นจากข้อกำหนดปัจจุบันขององค์กร 60 แห่ง

โทรคมนาคม คณะกรรมการกิจการโทรคมนาคมแห่งชาติได้ออกประกาศเกี่ยวกับมาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลผู้ใช้โทรคมนาคม ซึ่งกำหนดข้อกำหนดให้ผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมต้องรวบรวม ประมวลผล และรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการ

ข้อมูลเครดิตบูโร พระราชบัญญัติธุรกิจข้อมูลเครดิต พ.ศ. 2545 มีวัตถุประสงค์ในการควบคุมบริษัทข้อมูลเครดิตและธุรกรรมข้อมูลเครดิต การปกป้องสิทธิของเจ้าของข้อมูล และการมอบข้อมูลที่เชื่อถือได้ให้กับผู้ประมวลผลข้อมูลเครดิต

การคุ้มครองเด็ก พระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 กำหนดการคุ้มครองข้อมูลของเด็กอายุต่ำกว่า 18 ปี และข้อมูลของผู้ปกครอง

สาธารณสุข พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 กำหนดการคุ้มครองข้อมูลสุขภาพส่วนบุคคล โดยห้ามการเปิดเผยข้อมูลที่อาจก่อให้เกิดความเสียหายต่อเจ้าของข้อมูล เว้นแต่จะได้รับความยินยอมหรือมีข้อยกเว้นอื่น ๆ

การธนาคารและการชำระเงินทางอิเล็กทรอนิกส์ พระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560 ให้อำนาจธนาคารแห่งประเทศไทยในการออกประกาศกำหนดหลักเกณฑ์ในการให้บริการระบบการชำระเงินและการควบคุมในส่วนที่เกี่ยวข้องกับการเก็บรักษาและการเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการ

ประกันภัย ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ว่าด้วยหลักเกณฑ์และวิธีการคุ้มครองข้อมูลส่วนบุคคลในธุรกิจประกันภัย ระบุให้องค์กร ตัวแทน และนายหน้าต้องมีการจัดการข้อมูล ระบบจัดเก็บและป้องกันข้อมูลตามกฎหมายว่าด้วยการคุ้มครองข้อมูล

เจ้าหน้าที่รัฐบาล ข้อมูลส่วนบุคคลของบุคคลที่อยู่ภายใต้การควบคุมของหน่วยงานของรัฐได้รับการคุ้มครองภายใต้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

5. เวียดนาม: มังกรดิจิทัลกับการรักษาความมั่นคงของชาติ

สิทธิความเป็นส่วนตัว พัฒนาการและความท้าทายของเวียดนามในเวียดนาม ความเป็นส่วนตัวถือเป็นสิทธิมนุษยชนที่สำคัญและได้รับการรับรองในรัฐธรรมนูญของประเทศ ข้อมูลส่วนบุคคลได้รับการคุ้มครองโดยกฎหมายที่หลากหลาย ซึ่งมุ่งหวังที่จะรักษาความเป็นส่วนตัวและความปลอดภัยของบุคคลในยุคดิจิทัล

พระราชบัญญัติความปลอดภัยทางไซเบอร์ (CSA) ซึ่งมีผลใช้บังคับตั้งแต่ปี 2562 เป็นกฎหมายหลักที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในเวียดนาม กฎหมายนี้กำหนดให้มีข้อกำหนดสำคัญ เช่น การรับความยินยอมจากบุคคลก่อนที่จะรวบรวม ประมวลผล หรือถ่ายโอนข้อมูลส่วนบุคคล โดยองค์กรต้องใช้มาตรการด้านเทคนิคและองค์กรที่เหมาะสมเพื่อปกป้องข้อมูลจากการเข้าถึง การเปิดเผย การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต นอกจากนี้ ยังมีข้อกำหนดเกี่ยวกับการลดขนาดข้อมูล โดยระบุว่าองค์กรต้องรวบรวมและประมวลผลข้อมูลส่วนบุคคลให้น้อยที่สุดเท่าที่จำเป็นเพื่อวัตถุประสงค์ที่ตั้งใจไว้

ในเดือนกุมภาพันธ์ พ.ศ. 2564 กระทรวงความมั่นคงสาธารณะ (MPS) ได้ยื่นร่างพระราชกฤษฎีกาคุ้มครองข้อมูลส่วนบุคคลเพื่อขอความคิดเห็นจากสาธารณะ ร่างกฎหมายนี้มีข้อกำหนดเกี่ยวกับการจำกัดวัตถุประสงค์ การรักษาความปลอดภัยของข้อมูล การแจ้งเตือนการละเมิด ข้อมูล และการโอนย้ายข้อมูล

ข้ามพรมแดน โดยระบุว่าองค์กรต้องได้รับความยินยอมจากบุคคลก่อนการถ่ายโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สาม และข้อมูลจะต้องถูกถ่ายโอนไปยังประเทศที่มีกฎหมายคุ้มครองข้อมูลเพียงพอหรือมีการป้องกันที่เหมาะสม

อย่างไรก็ตาม การละเมิดข้อมูลยังคงเป็นปัญหาสำคัญในเวียดนาม ตัวอย่างที่เด่นชัด ได้แก่ การรั่วไหลของข้อมูลจาก Vietnam Airlines ในปี 2016 ซึ่งแฮกเกอร์ขโมยข้อมูลส่วนบุคคลของลูกค้ามากกว่า 400,000 ราย, การละเมิดข้อมูลจาก Mobile World ในปี 2018 ซึ่งเปิดเผยข้อมูลของลูกค้าประมาณ 31 ล้านราย, และการละเมิดข้อมูลจาก VNG Corporation ในปีเดียวกันที่เปิดเผยข้อมูลส่วนบุคคลของผู้ใช้แพลตฟอร์มเกมออนไลน์ประมาณ 163 ล้านคน โดยรวมแล้ว การคุ้มครองข้อมูลในเวียดนามกำลังอยู่ในช่วงพัฒนา และอาจมีช่องว่างในกรอบทางกฎหมายปัจจุบัน ซึ่งต้องการการปรับปรุงเพื่อให้สามารถตอบสนองต่อความท้าทายใหม่ๆ ที่เกิดจากสภาพแวดล้อมออนไลน์ที่มีการรั่วไหลและการละเมิดข้อมูลอย่างแพร่หลาย

การคุ้มครองข้อมูลส่วนบุคคลในเวียดนาม: CSA เวียดนาม

การคุ้มครองข้อมูลส่วนบุคคลในเวียดนามเป็นไปตามพระราชบัญญัติความปลอดภัยทางไซเบอร์ (CSA) ซึ่งมีผลใช้บังคับตั้งแต่ปี 2562 เป็นกฎหมายหลักที่ควบคุมการคุ้มครองข้อมูลส่วนบุคคลในประเทศ โดยกำหนดให้ข้อมูลส่วนบุคคลคือข้อมูลที่สามารถใช้ระบุตัวตนได้ทั้งโดยตรงและโดยอ้อม

บทบัญญัติสำคัญของ CSA รวมถึง

• **ความยินยอม** องค์กรต้องได้รับความยินยอมอย่างชัดเจนจากบุคคลก่อนที่จะรวบรวม ประมวลผล หรือถ่ายโอนข้อมูลส่วนบุคคล

• **ข้อจำกัดด้านวัตถุประสงค์** ข้อมูลส่วนบุคคลต้องถูกรวบรวมและประมวลผลเพื่อวัตถุประสงค์เฉพาะที่ถูกต้องตามกฎหมายเท่านั้น และต้องไม่ใช้ข้อมูลเพื่อวัตถุประสงค์อื่นโดยไม่ได้รับความยินยอมจากบุคคล

• **การลดขนาดข้อมูล** องค์กรต้องจำกัดการรวบรวมและประมวลผลข้อมูลให้เหลือน้อยที่สุดที่จำเป็นต่อการบรรลุวัตถุประสงค์ที่ตั้งไว้

• **การรักษาความปลอดภัย** ต้องใช้มาตรการด้านเทคนิคและองค์กรที่เหมาะสมเพื่อปกป้องข้อมูลจากการเข้าถึง การเปิดเผย การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต

• **การแจ้งเตือน** องค์กรต้องแจ้งให้บุคคลทราบโดยทันทีถึงการละเมิดข้อมูลส่วนบุคคลที่อาจเสี่ยงต่อสิทธิและเสรีภาพของตน

• **การโอนย้าย** การถ่ายโอนข้อมูลไปยังบุคคลที่สามต้องได้รับความยินยอมจากบุคคล และข้อมูลจะต้องถูกถ่ายโอนไปยังประเทศที่มีกฎหมายคุ้มครองข้อมูลที่เพียงพอหรือมีการป้องกันที่เหมาะสม

นอกจากนี้ ยังมีร่างพระราชกฤษฎีกาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ออกมาให้สาธารณชนแสดงความคิดเห็นตั้งแต่ปี 2564 ซึ่งคาดว่าจะช่วยเสริมสร้างกรอบการคุ้มครองข้อมูลส่วนบุคคลให้มีความเข้มแข็งยิ่งขึ้น

ขอบเขตการคุ้มครองข้อมูลส่วนบุคคลในเวียดนาม: ครอบคลุมทั้งองค์กรและบุคคล กฎหมายว่าด้วยความปลอดภัยทางไซเบอร์ในเวียดนามมีขอบเขตการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมองค์กร สถาบัน บุคคลที่จัดการข้อมูลส่วนบุคคล (ผู้ประมวลผลข้อมูล) และบุคคลธรรมดาที่ระบุหรือระบุได้จากข้อมูลส่วนบุคคลของตน (เจ้าของข้อมูล) โดยไม่มีการแยกแยะระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

หลักการสำคัญของการคุ้มครองข้อมูลในเวียดนาม ประกอบด้วย

• องค์กรและบุคคลที่เกี่ยวข้อง การคุ้มครองข้อมูลส่วนบุคคลใช้กับทุกองค์กร สถาบัน และบุคคลที่มีการจัดการข้อมูลส่วนบุคคล โดยไม่คำนึงถึงประเภทขององค์กรหรือรูปแบบการดำเนินงาน

• การจัดการข้อมูล ไม่มีความแตกต่างระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลภายใต้กฎหมายของเวียดนาม ทุกฝ่ายที่มีบทบาทในการจัดการข้อมูลต้องปฏิบัติตามข้อกำหนดของกฎหมายอย่างเท่าเทียมกัน

• การปกป้องคุ้มครองเจ้าของข้อมูล เจ้าของข้อมูล ซึ่งหมายถึงบุคคลธรรมดาที่สามารถระบุหรือระบุได้จากข้อมูลส่วนบุคคลของตนเอง จะได้รับสิทธิเสรีภาพตามกฎหมายในการควบคุมการรวบรวม การประมวลผล และการถ่ายโอนข้อมูลส่วนบุคคลของตนการไม่มีการแยกแยะระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลทำให้ทุกฝ่ายที่มีการจัดการข้อมูลต้องรับผิดชอบต่อการปฏิบัติตามมาตรฐานการคุ้มครองข้อมูลที่กำหนดไว้ ซึ่งช่วยเสริมสร้างความปลอดภัยและความเป็นส่วนตัวของข้อมูลในระดับที่สอดคล้องกันทั่วทั้งระบบ

ข้อมูลที่ได้รับการคุ้มครอง ในเวียดนาม ข้อมูลส่วนบุคคลหมายถึงข้อมูลใด ๆ ที่สามารถระบุเจ้าของได้ ซึ่งรวมถึงข้อมูลเกี่ยวกับชีวิตส่วนตัว ความลับส่วนตัวหรือครอบครัว และการสื่อสารส่วนบุคคล เช่น จดหมายที่เป็นลายลักษณ์อักษรและการสนทนาทางโทรศัพท์ ระบบกฎหมายของเวียดนามไม่แยกแยะข้อมูลส่วนบุคคลทั่วไปจากข้อมูลส่วนบุคคลที่ละเอียดอ่อน อย่างไรก็ตาม ข้อมูลบางประเภท เช่น ข้อมูลทางการเงินและบันทึกทางการแพทย์ ได้รับการจัดประเภทเป็นความลับของรัฐและมีการรักษาความปลอดภัยที่เข้มงวดยิ่งขึ้น เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและการใช้ที่ไม่เหมาะสม

หน่วยงานคุ้มครองข้อมูล เวียดนามยังไม่มีหน่วยงานคุ้มครองข้อมูลระดับชาติที่เดียว แต่มีหลายหน่วยงานรัฐบาลที่ได้รับมอบหมายให้ดูแลข้อมูลและการคุ้มครองข้อมูลในบางด้าน รวมถึง:

- กระทรวงสารสนเทศและการสื่อสาร (MIC) มีบทบาทในการกำหนดนโยบายและข้อกำหนดทางเทคนิคในการคุ้มครองข้อมูล
- กระทรวงความมั่นคงสาธารณะ (MPS) รับผิดชอบในการสอบสวนการละเมิดข้อมูลและเหตุการณ์ทางไซเบอร์
- ทีมตอบสนองเหตุฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์ของเวียดนาม/ศูนย์ประสานงาน (VNCERT/CC) จัดการเหตุการณ์ด้านความปลอดภัยทางไซเบอร์และเป็นส่วนหนึ่งของ Authority of Information Security (AIS) ซึ่งจัดการโดย MIC

หน่วยงานเหล่านี้มีอำนาจในการตรวจสอบการละเมิดข้อมูลและจัดการกับเหตุการณ์ทางไซเบอร์ แต่ไม่ได้มีหน้าที่ในการค้นพบความผิดทางแพ่ง

ความเป็นส่วนตัวออนไลน์และการคุ้มครองข้อมูล ในด้านความเป็นส่วนตัวออนไลน์ คุกกี้และข้อมูลตำแหน่งถูกมองว่าเป็นเครื่องมือที่เก็บข้อมูลส่วนบุคคลของผู้ใช้ เช่น ความสนใจ เว็บไซต์ที่เยี่ยมชม และพื้นที่ที่มักจะเดินทางไป เนื่องจากข้อมูลเหล่านี้สามารถเปิดเผยรายละเอียดชีวิตส่วนตัวของผู้ใช้ได้ กฎเกณฑ์การคุ้มครองข้อมูลในเวียดนามจึงรวมถึงการจัดการคุกกี้และข้อมูลตำแหน่ง ผู้ให้บริการไซเบอร์สเปซจะต้องได้รับความยินยอมล่วงหน้าจากผู้ใช้ก่อนที่จะเปิดใช้งานเทคโนโลยีเหล่านี้เพื่อให้สอดคล้องกับข้อกำหนดการคุ้มครองข้อมูลส่วนบุคคล

กิจกรรม: หารือถึงประโยชน์และความท้าทายของการปฏิบัติตามโมเดลการคุ้มครองข้อมูลและความปลอดภัยทางไซเบอร์ของจีน แทนที่จะเป็น GDPR สิ่งนี้จะส่งผลกระทบต่อการถ่ายโอนข้อมูลข้ามพรมแดนกับประเทศเพื่อนบ้านอย่างไร

กฎหมายความปลอดภัยทางไซเบอร์ของเวียดนามแตกต่างจากกฎหมายความปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลของประเทศอื่น ๆ ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ซึ่งได้รับอิทธิพลจาก GDPR ของสหภาพยุโรป กฎหมายความปลอดภัยทางไซเบอร์ของเวียดนามมีความคล้ายคลึงกับกฎหมายความปลอดภัยทางไซเบอร์ของจีนที่ประกาศใช้ในปี 2560 กฎหมายนี้มุ่งเน้นไปที่การให้ความสามารถแก่รัฐบาลในการควบคุมการไหลของข้อมูล ในขณะที่กฎหมายความปลอดภัยของข้อมูลเครือข่ายปกป้องสิทธิความเป็นส่วนตัวของข้อมูลของแต่ละบุคคล

ที่มา: https://www.dlapiperdataprotection.com/index.html?t=law&c=VN

การบังคับใช้และบทลงโทษ การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในเวียดนามมีทั้งบทลงโทษทางปกครองและทางอาญาที่แตกต่างกันขึ้นอยู่กับลักษณะและความรุนแรงของการละเมิด

บทลงโทษทางปกครอง

• การปรับทางปกครอง การเก็บข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตอาจทำให้ถูกปรับตั้งแต่ 10 ล้านดองถึง 20 ล้านดอง

• บทลงโทษสำหรับการละเมิดซ้ำ ร่างกฎหมายใหม่ที่กำลังพิจารณาจะกำหนดให้มีการปรับสูงสุดถึง 5% ของรายได้ หากองค์กรฝ่าฝืนกฎหมายซ้ำมากกว่า 3 ครั้ง

• การถ่ายโอนข้อมูลข้ามประเทศและการคุ้มครองในด้านการตลาดและโฆษณา มีข้อกำหนดใหม่เกี่ยวกับการป้องกันข้อมูลส่วนบุคคลที่นำไปใช้สร้างรายได้ และความรับผิดชอบในการรักษาความปลอดภัยของข้อมูล

บทลงโทษทางอาญา การใช้ข้อมูลโดยผิดกฎหมาย และการใช้ข้อมูลส่วนบุคคลในลักษณะที่ผิดกฎหมาย อาจถูกปรับตั้งแต่ 30 ล้านดองถึง 1 พันล้านดอง หรืออาจถูกจำคุกสูงสุด 7 ปี

ปัจจุบัน หน่วยงานที่รับผิดชอบด้านความปลอดภัยไซเบอร์ในเวียดนามกำลังยกร่างกฎหมายที่กำหนดบทลงโทษทางปกครองที่ชัดเจนมากขึ้น ซึ่งจะรวมถึงมาตรการการลงโทษที่เข้มงวดสำหรับการละเมิดกฎหมายความปลอดภัยไซเบอร์และการคุ้มครองข้อมูล โดยคาดว่ากฎหมายฉบับนี้จะประกาศใช้ในเร็ว ๆ นี้

กิจกรรม: ทบทวนมาตรการบังคับใช้ในการคุ้มครองข้อมูลและความปลอดภัยทางไซเบอร์ที่กล่าวถึงข้างต้น และหารือว่าค่าปรับและบทลงโทษสามารถทำหน้าที่เป็นแรงจูงใจตามความเป็นจริงสำหรับบริษัทดิจิทัลในการปฏิบัติตามข้อกำหนดการประมวลผลข้อมูลและความปลอดภัยทางไซเบอร์หรือไม่ ค่าปรับสูงพอที่จะขัดขวางและทำให้บริษัทดิจิทัลปฏิบัติตามกฎหมายได้หรือไม่?

การเก็บข้อมูลภายในประเทศ (Data Localization) รัฐบาลเวียดนามได้ออกกฎหมายใหม่เพื่อเพิ่มความเข้มงวดด้านความปลอดภัยไซเบอร์ โดยกำหนดให้บริษัทเทคโนโลยีต้องเก็บข้อมูลลูกค้าไว้ภายในประเทศและตั้งสำนักงานในประเทศ กฎหมายนี้มีผลบังคับใช้ตั้งแต่เดือนตุลาคม ปี 2022 โดยครอบคลุมบริษัทโซเชียลมีเดียอย่าง Google และ Facebook รวมถึงผู้ให้บริการโทรคมนาคม ข้อมูลของผู้ใช้อินเทอร์เน็ตทุกคน รวมถึงข้อมูลทางการเงิน ข้อมูลชีวภาพ ข้อมูลเชื้อชาติ ความเชื่อทางการเมือง และข้อมูลอื่น ๆ ที่ผู้ใช้อินเทอร์เน็ตสร้างขึ้นต้องถูกเก็บไว้ภายในประเทศ นอกจากนี้ บริษัทเทคโนโลยีต่างชาติต้องทำการประเมินความปลอดภัยก่อนถ่ายโอนข้อมูลข้ามประเทศ และต้องทำให้บริการไซเบอร์ของตนเองเป็นไปตามมาตรฐาน **“การประกันคุณภาพ”** ก่อนที่จะเปิดตัวในตลาดภายในประเทศ

กิจกรรม: อ่านข้อความด้านบน และอภิปรายว่าข้อกำหนดการแปลข้อมูลจะส่งผลกระทบต่อเศรษฐกิจดิจิทัลของเวียดนามอย่างไร อะไรคือข้อดีและข้อเสียที่สำคัญของการเก็บข้อมูลภายในประเทศ (Data Localization) สำหรับเศรษฐกิจดิจิทัลของประเทศ?

การยกเว้นการคุ้มครองข้อมูลให้กับหน่วยงานของรัฐ

ในเวียดนาม หน่วยงานที่เกี่ยวข้องมีสิทธิเพิ่มเติมในการจัดการและปกป้องข้อมูลอิเล็กทรอนิกส์เพื่อรักษาความมั่นคงทางไซเบอร์ ซึ่งรวมถึงการรวบรวมข้อมูลเกี่ยวกับกิจกรรมออนไลน์ที่อาจเป็นภัยต่อความมั่นคงแห่งชาติหรือความปลอดภัยสาธารณะ และการจัดการข้อมูลที่ผิดกฎหมายโดยการลบหรือขอเข้าถึงข้อมูลที่เป็นการละเมิดสิทธิผู้อื่นหรือเป็นภัยต่อความมั่นคง นอกจากนี้ยังสามารถระงับหรือหยุดการให้บริการเครือข่ายข้อมูลหรือการสร้างและใช้งานเครือข่ายโทรคมนาคมหรืออินเทอร์เน็ตได้ คณะทำงานด้านความปลอดภัยไซเบอร์ยังมีอำนาจในการบังคับให้ผู้ให้บริการโทรคมนาคมและอินเทอร์เน็ตเปิดเผยข้อมูลเกี่ยวกับกิจกรรมผิดกฎหมาย และสามารถสั่งให้ลบข้อมูลเท็จหรือเนื้อหาที่เป็นภัยภายใน 24 ชั่วโมงหลังได้รับคำสั่ง

อย่างไรก็ตาม กฎหมายความปลอดภัยทางไซเบอร์ของเวียดนามมีข้อกำหนดที่อาจละเมิดสิทธิมนุษยชน โดยเฉพาะการตรวจสอบตัวตนของผู้ใช้และการมอบข้อมูลส่วนบุคคลให้กับรัฐบาล ซึ่งขัดกับสิทธิความเป็นส่วนตัวตามรัฐธรรมนูญ นอกจากนี้ การลบหรือแบนเนื้อหาที่ถือว่าเป็น “อันตราย” โดยเกณฑ์ที่ไม่ชัดเจนยังขัดแย้งกับเสรีภาพในการแสดงออก การเข้ารหัสข้อมูลก็มีข้อกำหนดให้ผู้ใช้ต้องเปิดเผยข้อมูลเกี่ยวกับกุญแจเข้ารหัสและร่วมมือกับหน่วยงานรัฐในการป้องกันการใช้ผลิตภัณฑ์เข้ารหัสอย่างผิดกฎหมาย ซึ่งสร้างความกังวลเกี่ยวกับการละเมิดสิทธิมนุษยชนและการควบคุมที่เข้มงวดเกินไป

นอกจากนี้ ในเวียดนาม ผู้ใช้ผลิตภัณฑ์เข้ารหัสต้องให้ความร่วมมือกับรัฐบาลตามกฎหมาย โดยมีข้อกำหนดให้เปิดเผยข้อมูลเกี่ยวกับกุญแจเข้ารหัสเมื่อถูกเรียกร้อง และร่วมมือกับหน่วยงานรัฐในการป้องกันการใช้ผลิตภัณฑ์เข้ารหัสในทางที่ผิดกฎหมาย นอกจากนี้ ผู้ใช้ยังต้องแจ้งผลิตภัณฑ์เข้ารหัสที่ไม่ได้รับการอนุญาตจากผู้ประกอบการที่ได้รับใบอนุญาตให้กับคณะกรรมการเข้ารหัสของรัฐบาล เพื่อตรวจสอบและจัดการตามข้อกำหนดของกฎหมาย ความร่วมมือดังกล่าวมีเป้าหมายในการควบคุมและป้องกันการใช้เทคโนโลยีเข้ารหัสในทางที่เป็นภัยหรือผิดกฎหมาย

นโยบายและการริเริ่มของภาคส่วนต่าง ๆ

นอกเหนือจากกฎหมายว่าด้วยความปลอดภัยทางไซเบอร์ เวียดนามยังมีหลายกฎหมายและข้อบังคับที่มุ่งเน้นการปกป้องความเป็นส่วนตัวและข้อมูลในอาณาจักรดิจิทัล:

กฎหมายว่าด้วยเทคโนโลยีสารสนเทศ กำหนดกรอบสิทธิและภาระหน้าที่ขององค์กร หน่วยงาน และบุคคลที่เกี่ยวข้องกับการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศ รวมถึงการรวบรวม การใช้ การจัดเก็บ และการจัดหาข้อมูลส่วนบุคคลในสภาพแวดล้อมเครือข่าย

กฎหมายว่าด้วยการคุ้มครองผู้บริโภค คุ้มครองสิทธิความเป็นส่วนตัวของผู้บริโภคในด้านการตลาด การโฆษณา การรวบรวม และการใช้ข้อมูลส่วนบุคคล

กฎหมายว่าด้วยบันทึกการพิจารณาคดี ควบคุมการรวบรวม การใช้ และการเปิดเผยประวัติอาชญากรรมและบันทึกการพิจารณาคดีอื่น ๆ

กฎหมายว่าด้วยการต่อต้านการทุจริต มีบทบัญญัติที่เกี่ยวข้องกับการคุ้มครองตัวตนของผู้แจ้งเบาะแสและการรักษาความลับของการสอบสวนการต่อต้านการทุจริต

มาตรา 38 ของประมวลกฎหมายแพ่ง ควบคุมการรวบรวม การจัดเก็บ การประมวลผล การใช้ การเปิดเผย และการเผยแพร่ข้อมูลที่สามารถระบุตัวบุคคลได้

กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ควบคุมธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐและภาคการค้า ห้ามการใช้ แจกจ่าย หรือเผยแพร่ข้อมูลเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่ได้รับความยินยอม

กฎหมายว่าด้วยโทรคมนาคม ควบคุมกิจกรรมโทรคมนาคมและสิทธิและความรับผิดชอบของผู้ทำงานในอุตสาหกรรมนี้ กำหนดให้องค์กรโทรคมนาคมต้องไม่เปิดเผยข้อมูลของผู้ใช้ปลายทางโดยไม่ได้รับความยินยอมจากผู้ใช้ปลายทางหรือคำขอที่ถูกต้องตามกฎหมายจากหน่วยงานที่มีอำนาจ รัฐบาลกำลังร่างกฎหมายโทรคมนาคมใหม่เพื่อควบคุมบริการโทรคมนาคมแบบ over-the-top (OTT) และบริการโทรคมนาคมแบบคลาวด์

ทบทวนและประยุกต์

อ่านข้อความด้านล่างและอภิปรายวิธีการและเหตุผลในการคุ้มครองข้อมูลส่วนบุคคลในเมตาเวิร์ส ความเป็นส่วนตัวจะเปลี่ยนไปอย่างไรเมื่อเราเริ่มใช้อวตารดิจิทัล (digital avatars) สำหรับกิจกรรมในแต่ละวัน

เมตาเวิร์สคืออะไร? อาณาจักรเสมือนจริง 3 มิติที่แชร์ ดื่มด่ำ และถาวรที่เดียว ซึ่งผู้คนอาจได้สัมผัสกับชีวิตในแบบที่พวกเขาไม่สามารถทำได้ในโลกแห่งความเป็นจริงคือสิ่งที่หลายคนในอุตสาหกรรมคอมพิวเตอร์เรียกว่า “เมตาเวิร์ส” ความเป็นจริงเสมือนซึ่งโดดเด่นด้วยโลกเสมือนจริงที่คงอยู่ซึ่งยังคงมีอยู่ แม้ว่าคุณจะไม่ได้เล่นอยู่ก็ตาม และความเป็นจริงเสริมซึ่งรวมเอาองค์ประกอบของโลกดิจิทัลและโลกกายภาพเข้าด้วยกัน เป็นสองตัวอย่างของเทคโนโลยีที่บริษัทต่างๆ โดยทั่วไปอ้างถึงเมื่อพวกเขาพูดคุยกัน “เมตาเวิร์ส” ยักษ์ใหญ่ด้านดิจิทัลอย่าง Microsoft และ Meta ไม่ใช่กลุ่มเดียวที่พัฒนาเทคโนโลยีสำหรับการเชื่อมต่อกับโลกเสมือนจริง ธุรกิจขนาดเล็กและสตาร์ทอัพจำนวนมาก รวมถึงบริษัทสำคัญ ๆ หลายแห่ง เช่น Nvidia, Unity, Roblox และแม้แต่ Snap กำลังสร้างโครงสร้างพื้นฐานที่จำเป็นเพื่อพัฒนาโลกเสมือนจริงที่ดีขึ้น ซึ่งคล้ายกับประสบการณ์ในโลกแห่งความเป็นจริงของเรามากขึ้น

ที่มา: https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know

Milieu ซึ่งเป็นแพลตฟอร์มรวบรวมโปรไฟล์ผู้บริโภค ได้ทำการสำรวจความคิดเห็นที่เผยให้เห็นถึงความกระตือรือร้นของเอเชียตะวันออกเฉียงใต้ในการนำเมตาเวิร์สมาใช้ การศึกษาผู้ตอบแบบสอบถาม 6,000 รายจาก 6 ประเทศสมาชิกอาเซียน ได้แก่ มาเลเซีย ฟิลิปปินส์ ไทย อินโดนีเซีย สิงคโปร์ และเวียดนาม เปิดเผยว่าผู้ตอบแบบสอบถามส่วนใหญ่ (72%) ชอบใช้เมตาเวิร์สในการติดต่อรายวัน

อย่างไรก็ตาม ผู้ตอบแบบสอบถามส่วนใหญ่ (60%) มีความกังวลเกี่ยวกับความปลอดภัยของข้อมูลและความเป็นส่วนตัวเมื่อเข้าถึง metaverse ตามการสำรวจ มาเลเซียทำประตูแรกด้วยคะแนน 70% ตามด้วยสิงคโปร์และอินโดนีเซียอย่างละ 63% ฟิลิปปินส์ 60% ไทย 55% และเวียดนาม 47%

แม้จะมีการจัดอันดับดัชนีโดยรวมสูงสุดในกลุ่มประเทศเอเชียตะวันออกเฉียงใต้ (79.22 จาก 100 โดยรวมและ 100 ที่ไร้ที่ติในด้านตัวบ่งชี้ ‘การคุ้มครองข้อมูลส่วนบุคคล’) อาชญากรรมทางไซเบอร์ยังคงเป็นอันตรายต่อข้อมูลส่วนบุคคลของชาวมาเลเซีย ในปี 2021 เหตุการณ์ที่ต้องสงสัยในการขายข้อมูลส่วนบุคคลของชาวมาเลเซียจำนวน 4 ล้านคนจาก myIDENTITY ถือเป็นเหตุการณ์ที่น่าประหลาดที่สุด สิงคโปร์ ซึ่งตามมาเป็นอันดับสองรองจากมาเลเซีย (คะแนน 71.43 จากคะแนนรวมและ 100 คะแนนจากตัวบ่งชี้ “การคุ้มครองข้อมูลส่วนบุคคล”) ก็ตกอยู่ในอันตรายจากการละเมิดข้อมูลเช่นเดียวกัน ซึ่งรวมถึงการถ่ายโอนข้อมูลในปี 2021 ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของผู้ใช้ Fullerton Health ชาวสิงคโปร์จำนวน 400,000 คน

สถานการณ์เลวร้ายยิ่งขึ้นในอินโดนีเซีย ซึ่งเป็นประเทศในเอเชียตะวันออกเฉียงใต้ที่มีอัตราการเจาะอินเทอร์เน็ตสูงสุด (91%) โดยได้คะแนน 38.96 จากคะแนนรวม และ 25 คะแนนจากตัวบ่งชี้การคุ้มครองข้อมูลส่วนบุคคล แม้ว่าจะเผยแพร่สู่สาธารณะแล้วก็ตาม ข้อมูลที่ควบคุมโดยสถาบันของรัฐในระดับชาติถึงระดับท้องถิ่นก็ยังมีความเสี่ยงที่จะเกิดการรั่วไหล การขายข้อมูลส่วนบุคคลที่ต้องสงสัยทางออนไลน์ของชาวอินโดนีเซีย 279 คนจากฐานข้อมูลสำนักงานประกันสังคม (BPJS) เป็นหนึ่งในกรณีการละเมิดข้อมูลที่ร้ายแรงที่สุดในปี 2564 SAFENet ยังเน้นย้ำถึงเหตุการณ์สองเหตุการณ์ในระดับท้องถิ่น รวมถึงการเปิดเผยข้อมูลส่วนบุคคล ของครู 815 คนในเขต Tangerang และนักกีฬามากกว่า 1,000 คนในสำนักงานเยาวชนและกีฬาประจำจังหวัด Riau

ก่อนที่จะกระโดดข้ามกลุ่มนวัตกรรมที่ขับเคลื่อนด้วยดิจิทัล เจ้าหน้าที่และผู้มีส่วนได้ส่วนเสียอื่นๆ จะต้องจัดลำดับความสำคัญของความยืดหยุ่นทางไซเบอร์และความปลอดภัยของข้อมูลของผู้อยู่อาศัยในทันที แม้ว่าภูมิภาคจะตื่นเต้นกับการเปลี่ยนแปลงดังกล่าวก็ตาม

ที่มา: https://fulcrum.sg/the-metaverse-and-the-importance-of-personal-data-protection-in-southeast-asia/

กิจกรรม: แบ่งกลุ่มออกเป็น 2 หรือ 3 กลุ่ม แต่ละกลุ่มกลับไปที่ตอนที่ 3 และพยายามใช้ “แนวทางที่อิงสิทธิมนุษยชน (HRBA) เพื่อประเมินผลกระทบของกฎระเบียบเกี่ยวกับสิทธิความเป็นส่วนตัวในสภาพแวดล้อมดิจิทัล” โดยดูที่ “ส่วนการกำกับดูแล การตรวจสอบ และถ่วงดุล” สำหรับเขตอำนาจศาลที่เกี่ยวข้อง และพิจารณาว่าองค์ประกอบอะไร (ถ้ามี) ที่ขาดหายไปในเขตอำนาจศาลของตนมีอะไรบ้าง โดยพิจารณาจากดังนี้ :

การอนุญาตล่วงหน้าของการสอดแนมโดยหน่วยงานตุลาการที่มีอำนาจ: มีผู้พิพากษาที่เชี่ยวชาญด้านเทคโนโลยีดิจิทัลและสิทธิมนุษยชนที่สามารถประเมินและอนุมัติคำขอสอดแนมจากการสอบสวนหน่วยงานของรัฐได้หรือไม่?

จุดมุ่งหมายที่ชอบด้วยกฎหมาย: กฎหมายกำหนดวัตถุประสงค์ทางกฎหมายบางประการในการสอดแนม เช่น การป้องกันการก่อการร้ายหรืออาชญากรรมร้ายแรง โดยมีโทษจำคุกตั้งแต่ 10 ปีขึ้นไปหรือไม่

เหตุอันสมควร: ผู้พิพากษามีอำนาจในการพิจารณาว่ามีภัยคุกคามในระดับสูงต่อวัตถุประสงค์ที่ชอบด้วยกฎหมายหรือไม่ และมีความเป็นไปได้สูงที่การสอดแนมจะสร้างหลักฐานที่กำจัดภัยคุกคามนั้นได้หรือไม่

ความถูกต้องตามกฎหมาย: การเฝ้าระวังดำเนินการเฉพาะภายในข้อจำกัดและโดยหน่วยงานที่กฎหมายกำหนดหรือไม่ กฎหมายกำหนดให้การสอดแนมอื่น ๆ ผิดกฎหมายและกำหนดบทลงโทษหรือไม่?

ความจำเป็น: ผู้พิพากษาได้รับอนุญาตให้พิจารณาว่าจำเป็นต้องมีการตรวจสอบเพื่อรักษาความปลอดภัยของหลักฐานหรือไม่ และไม่มีวิธีอื่นที่รุกล้ำน้อยกว่าแต่สามารถบรรลุวัตถุประสงค์ที่ชอบด้วยกฎหมายได้หรือไม่

สัดส่วน: ผู้พิพากษามีอำนาจในการพิจารณาว่าการเฝ้าระวังที่เสนอนั้นมีขอบเขตจำกัดหรือไม่ และระยะเวลาเป็นสัดส่วนกับหลักฐานที่จำเป็นในการกำจัดภัยคุกคามหรือไม่

การแจ้งเตือน: กฎหมายกำหนดให้ผู้ถูกสอดแนมได้รับคำแนะนำให้ทำการสอดแนมโดยเร็วที่สุดเพื่อให้มีโอกาสอุทธรณ์ทางกฎหมายและดำเนินคดีตามกำหนดหรือไม่?

รายงานความโปร่งใส: รายงานความโปร่งใสประจำปีเปิดเผยต่อสาธารณะเกี่ยวกับจำนวนคำขอติดตาม การให้เหตุผล และการอนุญาตหรือไม่

การกำกับดูแลที่เป็นอิสระ: แนวทางปฏิบัติด้านการเฝ้าระวังมีกลไกการติดตามสาธารณะเพื่อรับประกันความรับผิดชอบและความโปร่งใสหรือไม่?

ส่วนที่ 3
เรื่องจริงจาก 13 คดีที่ควรรู้

เคยสงสัยหรือไม่ว่าในโลกที่ทุกคลิกของเราถูกบันทึก ทุกการกดไลค์ถูกวิเคราะห์ แล้วความเป็นส่วนตัวของเราหลงเหลืออยู่แค่ไหน?

เตรียมตัวให้พร้อม เพราะคุณกำลังจะได้พบกับ 13 คดีที่เขย่าโลกความเป็นส่วนตัวในยุคดิจิทัลเพราะในยุคที่เทคโนโลยีเปลี่ยนแปลงไปอย่างรวดเร็วเกินกว่าที่กฎหมายจะสามารถไล่ตามได้ทัน การเรียนรู้จากคำพิพากษาและคดีที่สำคัญถือเป็นกุญแจสำคัญที่จะช่วยให้ทนายความและผู้ปฏิบัติงานด้านกฎหมายสามารถเข้าใจภูมิทัศน์ทางกฎหมายที่ซับซ้อนเช่นทุกวันนี้ได้ดียิ่งขึ้น

เรื่องเล่าในแต่ละคดีในส่วนนี้ไม่ได้เป็นเพียงแค่ตัวอักษรในหนังสือหรือตำรา แต่เป็นเรื่องราวที่มีชีวิตที่จะชวนให้คิด และท้าทายความเข้าใจของเราเกี่ยวกับความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลในโลกดิจิทัล

แต่ละคดีจะพาพวกเราดำดิ่งลงไปในรายละเอียด ตั้งแต่ภูมิหลัง สถานการณ์ที่น่าติดตาม ข้อกฎหมาย และคำถามท้าทายชวนคิด รวมถึงคำแนะนำสุดล้ำค่าสำหรับทนายความและผู้ปฏิบัติงานด้านกฎหมาย นอกจากนี้ ยังรวมถึงแหล่งข้อมูลเพิ่มเติมสำหรับผู้ที่สนใจ และที่พลาดไม่ได้ ได้แก่ ตอนท้ายของแต่ละคดีที่จะพาพวกเราศึกษาและสำรวจคำตัดสิน เหตุผลทางกฎหมาย และบทวิเคราะห์ที่จะช่วยเปิดมุมมองใหม่ให้แก่ทุกคน

กรณีศึกษาที่ 1 : การท้าทายของ Schrems

นักศึกษาผู้เขย่าโลกที่ทำให้ข้อตกลง Safe Harbor ระหว่าง EU-US ต้องพังทลาย

ศาล/เขตอำนาจ ศาลยุติธรรมแห่งสหภาพยุโรป (CJEU)

ปี 2015

การอ้างอิง Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015]

ภูมิหลัง

ในช่วงต้นทศวรรษ 2010 เมื่อแพลตฟอร์มโซเชียลมีเดียขยายการเข้าถึงทั่วโลก คำถามเกี่ยวกับการโอนข้อมูลระหว่างประเทศและการคุ้มครองความเป็นส่วนตัวได้กลายเป็นประเด็นสำคัญ กรณีศึกษาที่จะศึกษานี้เป็นการปรับเปลี่ยนภูมิทัศน์ของการคุ้มครองข้อมูลทั่วโลก

สถานการณ์

นายแม็กซิมิเลียน เชร์มส์ (Maximilian Schrems) นักศึกษากฎหมายชาวออสเตรียวัยหนุ่มกังวลเกี่ยวกับความเป็นส่วนตัวของข้อมูลส่วนบุคคลของเขาบนแพลตฟอร์มโซเชียลมีเดีย โดยเฉพาะอย่างยิ่ง Facebook ความกังวลของเขาเพิ่มขึ้น หลังจากเกิดเหตุการณ์การเปิดเผยข้อมูลของ Edward Snowden เกี่ยวกับโครงการการสอดแนมขนาดใหญ่ในสหรัฐอเมริกา

นายเชร์มส์ คิดว่าตัวเองในฐานะนักกฎหมายต้องทำบางสิ่งบางอย่าง เขาได้ตัดสินใจยื่นเรื่องร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูลไอริช (Irish Data Protection Commissioner - DPC) กับ Facebook Ireland ซึ่งเป็นผู้ดูแลการประมวลผลข้อมูลทั้งหมดของ Facebook สำหรับผู้ใช้นอกสหรัฐอเมริกาและแคนาดา

นายเชร์มส์ ได้ตั้งประเด็นร้องเรียนว่า Facebook Ireland กำลังโอนข้อมูลส่วนบุคคลของเขาไปยังเซิร์ฟเวอร์ที่ตั้งอยู่ในสหรัฐอเมริกา โดยตัวเขาเชื่อว่ากฎหมายและแนวปฏิบัติของสหรัฐฯ ไม่ได้ให้การคุ้มครองที่เพียงพอต่อการสอดแนมโดยหน่วยงานของรัฐ ด้วยเหตุนี้ นายเชร์มส์ จึงขอให้ DPC ของไอร์แลนด์สั่งห้าม Facebook Ireland โอนข้อมูลส่วนบุคคลของเขาไปยังสหรัฐอเมริกา โดยในขณะที่มีการร้องเรียนกันนั้น การโอนข้อมูลระหว่างสหภาพยุโรปและสหรัฐอเมริกาอยู่ภายใต้ข้อตกลง “Safe Harbor” ซึ่งข้อตกลงดังกล่าวเกิดขึ้นเพื่อประกันว่าบริษัทที่โอนข้อมูลจากสหภาพยุโรปไปยังสหรัฐอเมริกาได้ให้การคุ้มครองที่เพียงพอสำหรับข้อมูลของพลเมืองยุโรป

ภายหลังการร้องเรียน คณะกรรมการคุ้มครองข้อมูลของไอร์แลนด์ได้ปฏิเสธข้อร้องเรียนของนายเซร็มส์ ในตอนแรก โดยอ้างว่า 1) ข้อตกลง Safe Harbor ได้รับการอนุมัติจากคณะกรรมาธิการยุโรป รับประกันการคุ้มครองที่เพียงพอสำหรับข้อมูลที่โอนไปยังสหรัฐอเมริกาแล้ว และ 2) DPC ไม่มีอำนาจในการสอบสวนหรือระงับการโอนข้อมูลเหล่านี้

นายเซร็มส์ ไม่ย่อท้อ ได้อุทธรณ์คำตัดสินต่อศาลสูงไอร์แลนด์ ศาลตระหนักถึงความซับซ้อนและความสำคัญของประเด็นนี้ จึงส่งคำถามหลายข้อไปยังศาลยุติธรรมแห่งสหภาพยุโรป (CJEU) เพื่อขอคำชี้แจง โดยศาลยุติธรรมแห่งสหภาพยุโรป ถูกขอให้พิจารณาใน 2 เรื่อง คือ

1. ความถูกต้องของข้อตกลง Safe Harbor ในแง่ของกฎบัตรว่าด้วยสิทธิขั้นพื้นฐานของสหภาพยุโรป

2. อำนาจของหน่วยงานคุ้มครองข้อมูลแห่งชาติในการสอบสวนและระงับการโอนข้อมูล แม้จะอยู่ภายใต้ข้อตกลงทั่วทั้งสหภาพยุโรปคำถามสำคัญ

สำหรับการวิเคราะห์

1. ควรสร้างความสมดุลระหว่างผลประโยชน์ด้านความมั่นคงของชาติและสิทธิความเป็นส่วนตัวของบุคคลอย่างไรในบริบทของการโอนข้อมูลระหว่างประเทศหรือไม่ อย่างไร ?

2. ระดับการคุ้มครองใดที่ควรถือว่า “เพียงพอ” สำหรับข้อมูลส่วนบุคคลที่ถูกโอนระหว่างประเทศ ?

3. อะไรคือผลกระทบที่อาจเกิดขึ้นทางเศรษฐกิจและการทูตหากยกเลิกข้อตกลง Safe Harbor ?

4. คดีนี้ส่งผลกระทบต่ออนาคตของบริการอินเทอร์เน็ตทั่วโลกและการไหลเวียนของข้อมูลระหว่างประเทศอย่างไร ?

5. หากท่านเป็นทนายความของ Facebook ไอร์แลนด์ ท่านจะโต้แย้งอย่างไรเพื่อชี้ว่าข้อตกลง Safe Harbor ให้การคุ้มครองข้อมูลที่เพียงพอโดยคำนึงถึงความแตกต่างระหว่างระบบกฎหมายของสหภาพยุโรปและสหรัฐอเมริกาแล้ว

คำแนะนำสำหรับทนายความ

ประเด็นการโอนข้อมูลระหว่างประเทศเป็นประเด็นที่สำคัญที่ส่งผลต่อทางปฏิบัติทางการค้าระหว่างประเทศ ซึ่งมีการยกขึ้นอ้างในฐานะอุปสรรคทางการค้าที่มิใช่ภาษี ทนายความควรศึกษาและทำความเข้าใจการโอนข้อมูลระหว่างประเทศอย่างละเอียด นอกจากนี้ พิจารณามาตรา 28 และมาตรา 29 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 ผลกระทบของคำตัดสินต่อลูกความ โดยเฉพาะลูกความที่ดำเนินธุรกิจข้ามพรมแดน

กฎหมายที่เกี่ยวข้อง

1. EU Data Protection Directive 95/46/EC (กฎหมายคุ้มครองข้อมูลของสหภาพยุโรป 95/46/EC) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่ออกในปี 1995 มีจุดประสงค์เพื่อกำหนดกรอบการคุ้มครองข้อมูลส่วนบุคคลในประเทศสมาชิก EU โดยกำหนดหลักการสำคัญเกี่ยวกับการเก็บรวบรวม ประมวลผล และใช้ข้อมูลส่วนบุคคล รวมถึงสิทธิของเจ้าของข้อมูล ต่อมากฎหมายนี้ถูกแทนที่โดย General Data Protection Regulation (GDPR) มีผลบังคับใช้เมื่อวันที่ 25 พฤษภาคม 2018 เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ที่มีความครอบคลุมและเข้มงวดมากขึ้น

2. EU-US Safe Harbor Agreement (ข้อตกลง Safe Harbor ระหว่างสหภาพยุโรปกับสหรัฐอเมริกา) เป็นข้อตกลงระหว่าง สหภาพยุโรปกับสหรัฐอเมริกา ที่จัดทำขึ้นในปี 2000 เพื่อให้บริษัทในสหรัฐฯ สามารถรับและประมวลผลข้อมูลส่วนบุคคลจาก EU ได้โดยไม่ละเมิดกฎหมายคุ้มครองข้อมูลของ EU โดยกำหนดมาตรฐานการคุ้มครองข้อมูลที่บริษัทสหรัฐฯ ต้องปฏิบัติตาม

3. EU Charter of Fundamental Rights (กฎบัตรว่าด้วยสิทธิขั้นพื้นฐานของสหภาพยุโรป) เป็นกฎบัตรที่รับรองสิทธิขั้นพื้นฐานของพลเมือง EU ซึ่งมีผลบังคับใช้ในปี 2009 โดยครอบคลุมสิทธิด้านต่าง ๆ รวมถึงสิทธิในการคุ้มครองข้อมูลส่วนบุคคล เสรีภาพในการแสดงออก และสิทธิในความเป็นส่วนตัว ซึ่งเป็นพื้นฐานสำคัญของกฎหมายคุ้มครองข้อมูลของ EU

แหล่งข้อมูล

1. คำตัดสินของ CJEU ในคดี Schrems I (Case C-362/14)
2. EU Data Protection Directive 95/46/EC
3. แนวทางของ Article 29 Working Party เกี่ยวกับการโอนข้อมูลระหว่างประเทศ

เอกสารแนะนำเพิ่มเติม

วรรณรัชชา ทรัพย์รดาพัดชา (2558). ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศกับสหภาพยุโรป: ศึกษาผลกระทบของคดีคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดี C-362/14 ต่อโครงการเซฟฮาร์เบอร์ (Safe Harbour). มหาวิทยาลัยธรรมศาสตร์.

Kuner, C. (2017). Reality and Illusion in EU Data TrAfer Regulation Post Schrems. German Law Journal, 18(4), 881-918.

Bignami, F. & Resta, G. (2018). TrAatlantic Privacy Regulation: Conflict and Cooperation. Law and Contemporary Problems, 81(4), 101-134.

คำตัดสิน

ศาลยุติธรรมแห่งสหภาพยุโรปตัดสินว่า กรรมาธิการคุ้มครองข้อมูลประเทศไอร์แลนด์มีอำนาจตรวจสอบการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม แม้จะมีการตัดสินของคณะกรรมาธิการยุโรปแล้วว่าประเทศนั้นมีการคุ้มครองข้อมูลที่เพียงพอก็ตาม คดีชี้ให้เห็นว่ากฎหมายของสหรัฐอเมริกาไม่ได้มีการคุ้มครองข้อมูลของพลเมืองยุโรปที่เพียงพอ การสอดแนมของรัฐบาลสหรัฐอเมริกาเป็นการละเมิดสิทธิขั้นพื้นฐานของพลเมืองสหภาพยุโรป ประเทศสหรัฐอเมริกาไม่สามารถรับโอนข้อมูลส่วนบุคคลโดยใช้ข้อตกลง Safe Harbor ได้อีก

ผลของคำพิพากษาเป็นการวางหลักเกณฑ์ใหม่ในการพิจารณาระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (adequate level of protection) ทำให้ประเทศต่าง ๆ ต้องกลับมาพิจารณากฎหมายคุ้มครองข้อมูลส่วนบุคคลภายในประเทศตน คดีนี้ถือเป็นจุดเปลี่ยนสำคัญในกฎหมายคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศ โดยเฉพาะการตรวจสอบอย่างเข้มงวดเรื่องการโอนข้อมูลระหว่างสหภาพยุโรปและสหรัฐอเมริกาและนำไปสู่การเจรจาข้อตกลงใหม่ในเวลาต่อมา

กรณีศึกษาที่ 2: การท้าทายครั้งที่สองของ Schrems

เกราะคุ้มกันข้อมูลที่พังทลาย: Schrems II กับวิกฤตการโอนข้อมูลข้ามทวีป

ศาล/เขตอำนาจ ศาลยุติธรรมแห่งสหภาพยุโรป (CJEU)

ปี 2020

การอ้างอิง Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems [2020]

ภูมิหลัง

หลังจากชัยชนะในคดี Schrems I ที่นำไปสู่การยกเลิกข้อตกลง Safe Harbor ระหว่างสหภาพยุโรปและสหรัฐอเมริกา นายแม็กซิมิเลียน เชร์มส์ นักกฎหมายและนักเคลื่อนไหวด้านความเป็นส่วนตัวยังคงติดตามประเด็นการโอนข้อมูลระหว่างประเทศอย่างใกล้ชิด กรณีศึกษานี้จะเน้นที่คดี Schrems II ซึ่งท้าทายกลไกการโอนข้อมูลที่ใช้แทนที่ Safe Harbor

สถานการณ์

นายแม็กซิมิเลียน เชร์มส์ ได้ยื่นเรื่องร้องเรียนต่อกรรมาธิการคุ้มครองข้อมูลของไอร์แลนด์ (Irish Data Protection Commissioner - DPC) อีกครั้งเกี่ยวกับการโอนข้อมูลส่วนบุคคลของเขาจาก Facebook ไอร์แลนด์ไปยังสหรัฐอเมริกา โดยครั้งนี้ นายเชร์มส์ มีข้อกังวล คือ 1) การโอนข้อมูลส่วนบุคคลของเขาจาก Facebook ไอร์แลนด์ไปยังสหรัฐอเมริกาอยู่ภายใต้ข้อสัญญามาตรฐาน (Standard Contractual Clauses - SCCs) และข้อตกลง EU-US Privacy Shield 2) นายเชร์มส์เชื่อว่าหน่วยงานความมั่นคงของสหรัฐอเมริกาอาจละเมิดสิทธิความเป็นส่วนตัวของเขา และ 3) นายเขาต้องการให้มีการตรวจสอบความชอบด้วยกฎหมายของการโอนข้อมูลภายใต้กลไกเหล่านี้

การโอนข้อมูลระหว่างสหภาพยุโรปและสหรัฐอเมริกาในครั้งนี้ อยู่ภายใต้ข้อสัญญามาตรฐาน (SCCs): ชุดของข้อกำหนดและเงื่อนไขมาตรฐานที่ได้รับการรับรองโดยคณะกรรมาธิการยุโรป ใช้เพื่อให้องค์กรสามารถปฏิบัติตามข้อกำหนดการคุ้มครองข้อมูลของสหภาพยุโรปเมื่อมีการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม และข้อตกลง EU-US Privacy Shield: กรอบการทำงานที่ออกแบบมาเพื่อให้บริษัทในยุโรปและสหรัฐอเมริกาสามารถปฏิบัติตามข้อกำหนดการคุ้มครองข้อมูลเมื่อโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปไปยังสหรัฐอเมริกา

ภายหลังได้รับคำร้อง กรรมาธิการคุ้มครองข้อมูลของไอร์แลนด์ได้นำคดีขึ้นสู่ศาลสูงไอร์แลนด์ โดยศาลสูงไอร์แลนด์ได้ส่งคำถามไปยังศาลยุติธรรมแห่งสหภาพยุโรป (CJEU) เพื่อขอคำชี้แจง โดยศาลยุติธรรมแห่งสหภาพยุโรป ถูกขอให้พิจารณา 3 ประเด็น คือ

1. ความสมบูรณ์ของข้อสัญญามาตรฐาน (SCCs) ในการคุ้มครองข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรป

2. ความชอบด้วยกฎหมายของข้อตกลง EU-US Privacy Shield และ

3. ระดับการคุ้มครองข้อมูลที่จำเป็นเมื่อโอนข้อมูลไปยังประเทศที่สาม โดยเฉพาะในกรณีที่หน่วยงานรัฐมีอำนาจในการเข้าถึงข้อมูลอย่างกว้างขวาง

คำถามสำคัญสำหรับการวิเคราะห์

1. ข้อสัญญามาตรฐาน (SCCs) สามารถให้การคุ้มครองที่เพียงพอสำหรับข้อมูลส่วนบุคคลที่โอนไปยังประเทศที่สามได้จริงหรือไม่? มีข้อจำกัดอย่างไร?

2. ในยุคที่การเฝ้าระวังโดยรัฐเป็นเรื่องปกติ จะสามารถสร้างสมดุลระหว่างความมั่นคงของชาติและสิทธิความเป็นส่วนตัวของพลเมืองได้อย่างไร?

3. การตัดสินใจของ CJEU ในคดีนี้อาจส่งผลกระทบต่อการค้าและความร่วมมือระหว่างสหภาพยุโรปและสหรัฐอเมริกาอย่างไร?

4. หากข้อตกลง EU-US Privacy Shield ถูกยกเลิก จะมีทางเลือกอื่นใดสำหรับการโอนข้อมูลระหว่างสหภาพยุโรปและสหรัฐอเมริกา?

5. บริษัทเทคโนโลยีขนาดใหญ่ที่ให้บริการข้ามพรมแดนควรปรับตัวอย่างไรเพื่อให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลที่แตกต่างกันในแต่ละภูมิภาค?

6. หากท่านเป็นที่ปรึกษากฎหมายให้กับบริษัทที่ต้องโอนข้อมูลระหว่างสหภาพยุโรป และสหรัฐอเมริกา ท่านจะให้คำแนะนำมาตรการเพิ่มเติมอะไรนอกเหนือจาก Standard Contractual Clauses เพื่อให้มั่นใจว่าการโอนข้อมูลเป็นไปตามมาตรฐานของ GDPR?

คำแนะนำสำหรับทนายความ

ทำความเข้าใจข้อตกลงการโอนข้อมูลระหว่างประเทศของลูกความ พิจารณาการใช้มาตรการเสริมเพื่อเพิ่มการคุ้มครองข้อมูลในการโอนข้อมูลไปยังประเทศที่สาม และติดตามการพัฒนากฎระเบียบใหม่สำหรับการโอนข้อมูลระหว่างสหภาพยุโรปและสหรัฐอเมริกา ตลอดจนประเทศอื่น ๆ

ในบริบทของประเทศไทย พิจารณามาตรา 28 และมาตรา 29 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566

กฎหมายที่เกี่ยวข้อง

1. EU Data Protection Directive 95/46/EC (กฎหมายคุ้มครองข้อมูลของสหภาพยุโรป 95/46/EC) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่ออกในปี 1995 มีจุดประสงค์เพื่อกำหนดกรอบการคุ้มครองข้อมูลส่วนบุคคลในประเทศสมาชิก EU โดยกำหนดหลักการสำคัญเกี่ยวกับการเก็บรวบรวม ประมวลผล และใช้ข้อมูลส่วนบุคคล รวมถึงสิทธิของเจ้าของข้อมูล ต่อมากฎหมายนี้ถูกแทนที่โดย General Data Protection Regulation (GDPR) มีผลบังคับใช้เมื่อวันที่ 25 พฤษภาคม 2018 เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ที่มีความครอบคลุมและเข้มงวดมากขึ้น

2. EU Charter of Fundamental Rights (กฎบัตรว่าด้วยสิทธิขั้นพื้นฐานของสหภาพยุโรป) เป็นกฎบัตรที่รับรองสิทธิขั้นพื้นฐานของพลเมือง EU ซึ่งมีผลบังคับใช้ในปี 2009 โดยครอบคลุมสิทธิด้านต่างๆ รวมถึงสิทธิในการคุ้มครองข้อมูลส่วนบุคคล เสรีภาพในการแสดงออก และสิทธิในความเป็นส่วนตัว ซึ่งเป็นพื้นฐานสำคัญของกฎหมายคุ้มครองข้อมูลของ EU

แหล่งข้อมูล

1. คำตัดสินของ CJEU ในคดี Schrems II (Case C-311/18)
2. แนวทางของ European Data Protection Board เกี่ยวกับมาตรการเสริมสำหรับการโอนข้อมูล
3. GDPR Chapter V เกี่ยวกับการโอนข้อมูลไปยังประเทศที่สาม

เอกสารแนะนำเพิ่มเติม

Kuner, C. (2020). The Schrems II Judgment of the Court of Justice and the future of data trAfer regulation. European Law Blog. https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-trAfer-regulation/

Christakis, T. (2020). After Schrems II: Uncertainties on the Legal Basis for Data TrAfers and Constitutional Implications for Europe. European Law Blog. https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-trAfers-and-con stitutional-implications-for-europe/

Propp, K., & Swire, P. (2020). After Schrems II: A Proposal to Meet the Individual Redress Challenge. Georgia Tech Scheller College of Business Research Paper, (3680148).

คำตัดสิน

ศาลยุติธรรมแห่งสหภาพยุโรปยืนยันความถูกต้องของคำตัดสินในคดี Schrems I โดยชี้ว่า ข้อตกลง Safe Harbor ไม่สามารถใช้เป็นฐานในการโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปไปยังสหรัฐอเมริกาได้ การโอนข้อมูลส่วนบุคคลไปยังประเทศนอกสหภาพยุโรป (รวมถึงสหรัฐอเมริกา) จะทำได้ภายใต้เงื่อนไขบางประการ เช่น การใช้ข้อสัญญามาตรฐาน อย่างไรก็ตาม ศาลยุติธรรมแห่งสหภาพยุโรปได้กำหนดให้ผู้ควบคุมข้อมูล (data controller) ต้องประเมินกฎหมาย และแนวปฏิบัติของประเทศปลายทาง (ประเทศที่รับข้อมูล) เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลได้รับการคุ้มครองอย่างเพียงพอ หากกฎหมายและแนวปฏิบัติของประเทศปลายทางไม่ได้มีการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลจะต้องดำเนินการเพิ่มเติม เช่น การใช้มาตรการคุ้มครองทางเทคนิคเพิ่มเติม หรือยกเลิกการโอนข้อมูล

เหตุผลทางกฎหมายในคดีนี้ กฎหมายของสหรัฐอเมริกาไม่ได้ให้การคุ้มครองที่เพียงพอแก่ข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรป และพลเมืองสหภาพยุโรปไม่มีสิทธิในการดำเนินคดีในศาลสหรัฐอเมริกาเกี่ยวกับการใช้ข้อมูลของพวกเขา ซึ่งขัดกับหลักการพื้นฐานของสิทธิขั้นพื้นฐานของสหภาพยุโรป ผลกระทบจากคดี ส่งผลให้มีการยกเลิก EU-US Privacy Shield ทำให้การโอนข้อมูลระหว่างสหภาพยุโรปและสหรัฐอเมริกาต้องหาวิธีการทางกฎหมายใหม่ องค์กรต่างๆ ต้องประเมินการใช้ SCCs เป็นรายกรณี และอาจต้องใช้มาตรการเสริมเพื่อให้แน่ใจว่ามีการคุ้มครองข้อมูลที่เพียงพอ ทำให้เกิดความซับซ้อนและภาระในการปฏิบัติตามกฎหมาย สำหรับองค์กรที่โอนข้อมูลระหว่างประเทศ

กรณีศึกษาที่ 3: สิทธิที่จะถูกลืม

ลบรอยดิจิทัล: Google Spain กับการกำเนิด “สิทธิที่จะถูกลืม”

ศาล/เขตอำนาจ ศาลยุติธรรมแห่งสหภาพยุโรป (CJEU)

ปี 2014

การอ้างอิง Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014]

ภูมิหลัง

การค้นหาข้อมูลออนไลน์กลายเป็นส่วนสำคัญของชีวิตประจำวัน แต่การที่ข้อมูลส่วนบุคคลปรากฏในผลการค้นหาอาจส่งผลกระทบต่อชีวิตของบุคคลได้ในระยะยาว กรณีศึกษานี้จะพิจารณาคดีสำคัญที่นำไปสู่แนวคิดเรื่อง “สิทธิที่จะถูกลืม” ในสหภาพยุโรป

สถานการณ์

มาริโอ กอนซาเลซ (Mario Costeja González) พลเมืองชาวสเปน ได้ทำการค้นหาชื่อของตนเองบน Google และพบว่าผลการค้นหาแสดงลิงก์ไปยังบทความหนังสือพิมพ์เก่าจากปี 1998 โดยบทความดังกล่าวเสนอข่าวเกี่ยวกับการขายทอดตลาดทรัพย์สินของเขาเพื่อชำระหนี้ประกันสังคม เมื่อนายกอนซาเลซ เห็นข้อมูลดังกล่าวจึงได้ยื่นเรื่องร้องเรียนต่อหน่วยงานคุ้มครองข้อมูลของสเปน [Agencia Española de Protección de Datos (AEPD)] โดยตั้งประเด็นว่า ข้อมูลที่ปรากฏในผลการค้นหาไม่มีความเกี่ยวข้องและล้าสมัยแล้ว เนื่องจากตัวเขาได้ชำระหนี้เรียบร้อยเป็นเวลาหลายปีแล้ว ต้องการให้ Google Spain ลบหรือซ่อนข้อมูลดังกล่าวจากผลการค้นหา

AEPD ได้พิจารณาคำร้องเรียน และมีคำสั่งให้ Google Spain ลบข้อมูลดังกล่าวออกจากผลการค้นหา

บริษัท Google Spain ไม่เห็นด้วยกับคำสั่งของ AEPD จึงได้นำคดีขึ้นสู่ศาลแห่งชาติสเปน ศาลแห่งชาติสเปนตระหนักถึงความซับซ้อนและความสำคัญของประเด็นนี้ จึงได้ส่งคำถามต่อไปยังศาลยุติธรรมแห่งสหภาพยุโรป (CJEU) เพื่อขอคำชี้แจง โดยมีประเด็นพิจารณา 3 เรื่อง คือ

1. ขอบเขตการบังคับใช้กฎหมายคุ้มครองข้อมูลของสหภาพยุโรปกับผู้ให้บริการค้นหาข้อมูล

2. ความรับผิดชอบของผู้ให้บริการค้นหาข้อมูลต่อเนื้อหาที่ปรากฏในผลการค้นหา

3. สิทธิของบุคคลในการขอให้ลบหรือแก้ไขข้อมูลส่วนบุคคลที่ปรากฏในผลการค้นหา

คำถามสำคัญสำหรับการวิเคราะห์

1. ควรมีแนวทางการสร้างสมดุลระหว่างสิทธิในการเข้าถึงข้อมูลและสิทธิในความเป็นส่วนตัวอย่างไร?

2. ผู้ให้บริการค้นหาข้อมูลควรมีความรับผิดชอบมากน้อยเพียงใดต่อเนื้อหาที่ปรากฏในผลการค้นหา?

3. อะไรคือเกณฑ์ที่เหมาะสมในการพิจารณาว่าข้อมูลใด “ไม่เกี่ยวข้อง” หรือ “ล้าสมัย” จนสมควรถูกลบออกจากผลการค้นหา?

4. การรับรอง “สิทธิที่จะถูกลืม” อาจส่งผลกระทบต่อเสรีภาพในการแสดงออกและสิทธิในการรับรู้ข้อมูลข่าวสารหรือไม่ อย่างไร?

5. การบังคับใช้ “สิทธิที่จะถูกลืม” ในระดับโลกจะมีความท้าทายอย่างไร โดยเฉพาะอย่างยิ่งเมื่อพิจารณาถึงความแตกต่างทางกฎหมายและวัฒนธรรมในแต่ละประเทศ?

คำแนะนำสำหรับทนายความ

ควรทำความเข้าใจความหมาย ขอบเขตและข้อจำกัดของสิทธิที่จะถูกลืม พิจารณากฎหมายไทย มาตรา 33 สิทธิที่จะลบข้อมูล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และติดตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. .... เตรียมพร้อมให้คำแนะนำแก่ลูกความเกี่ยวกับการจัดการคำขอลบข้อมูล ตลอดจนพิจารณาแนวทางการตีความ และการพิจารณาผลกระทบของคำตัดสินที่ส่งผลต่อเสรีภาพในการแสดงออกและสิทธิในการเข้าถึงข้อมูล

กฎหมายที่เกี่ยวข้อง

1. EU Data Protection Directive 95/46/EC (กฎหมายคุ้มครองข้อมูลของสหภาพยุโรป 95/46/EC) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่ออกในปี 1995 มีจุดประสงค์เพื่อกำหนดกรอบการคุ้มครองข้อมูลส่วนบุคคลในประเทศสมาชิก EU ต่อมากฎหมายนี้ถูกแทนที่โดย General Data Protection Regulation (GDPR) มีผลบังคับใช้เมื่อวันที่ 25 พฤษภาคม 2018

2. EU Charter of Fundamental Rights (กฎบัตรว่าด้วยสิทธิขั้นพื้นฐานของสหภาพยุโรป) เป็นกฎบัตรที่รับรองสิทธิขั้นพื้นฐานของพลเมือง EU ซึ่งมีผลบังคับใช้ในปี 2009 โดยครอบคลุมสิทธิด้านต่างๆ รวมถึงสิทธิในการคุ้มครองข้อมูลส่วนบุคคล เสรีภาพในการแสดงออก และสิทธิในความเป็นส่วนตัว ซึ่งเป็นพื้นฐานสำคัญของกฎหมายคุ้มครองข้อมูลของ EU

แหล่งข้อมูล

1. คำตัดสินของ CJEU ในคดี Google Spain (Case C-131/12)
2. แนวทางของ Article 29 Working Party เกี่ยวกับการปฏิบัติตามคำตัดสิน Google Spain
3. GDPR Article 17 เกี่ยวกับสิทธิในการลบข้อมูล

เอกสารแนะนำเพิ่มเติม

ชยาภรณ์ มั่นสกุล (2565). ปัญหาการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. จุฬาลงกรณ์มหาวิทยาลัย.

Frantziou, E. (2014). Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos. Human Rights Law Review, 14(4), 761-777.

Lynskey, O. (2015). Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez. Modern Law Review, 78(3), 522-534.

คำตัดสิน

ศาลยุติธรรมแห่งสหภาพยุโรปตัดสินว่า เครื่องมือค้นหาอย่าง Google ถือเป็นผู้ควบคุมข้อมูล (Data Controller) ภายใต้กฎหมายคุ้มครองข้อมูลของสหภาพยุโรป ดังนั้น บุคคลมีสิทธิร้องขอให้เครื่องมือค้นหาลบลิงก์ที่เกี่ยวข้องกับชื่อของตนออกจากผลการค้นหา หากข้อมูลนั้นไม่เพียงพอ ไม่เกี่ยวข้อง หรือเกินความจำเป็น (หลักการ Data minimization) โดยเหตุผลทางกฎหมายในคดีนี้ คือ การพิจารณาว่าการประมวลผลข้อมูลโดยเครื่องมือค้นหา อาจส่งผลกระทบอย่างมีนัยสำคัญต่อสิทธิขั้นพื้นฐานในความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล ด้วยเหตุนี้ จึงได้ชั่งน้ำหนักระหว่างสิทธิความเป็นส่วนตัวของบุคคลกับผลประโยชน์ทางเศรษฐกิจของผู้ให้บริการเครื่องมือค้นหา และสิทธิในการเข้าถึงข้อมูลของสาธารณชน อย่างไรก็ตาม ในบางกรณี สิทธิความเป็นส่วนตัวของบุคคลอาจมีน้ำหนักมากกว่าประโยชน์สาธารณะในการเข้าถึงข้อมูลได้

คดีนี้เป็นจุดเริ่มต้นสำคัญในการกำหนด “สิทธิที่จะถูกลืม” ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป และส่งผลกระทบอย่างยิ่งต่อการทำงานของเครื่องมือสืบค้น และการจัดการข้อมูลส่วนบุคคลออนไลน์ กล่าวอีกนัยหนึ่ง ผลจากคดีเป็นการเพิ่มภาระให้กับผู้ให้บริการเครื่องมือค้นหาในการจัดการคำขอ และต้องชั่งน้ำหนักระหว่างสิทธิส่วนบุคคลกับประโยชน์สาธารณะ นำไปสู่ข้อถกเถียงเกี่ยวกับการตีความขอบเขตของสิทธิที่จะถูกลืม และผลกระทบต่อเสรีภาพในการแสดงออกและการเข้าถึงข้อมูล

กรณีศึกษาที่ 4: ขอบเขตทางภูมิศาสตร์ของสิทธิที่จะถูกลืม

	สิทธิที่จะถูกลืมไร้พรมแดน: Google v CNIL และขอบเขตของการลบข้อมูลทั่วโลก
ศาล/เขตอำนาจ	ศาลยุติธรรมแห่งสหภาพยุโรป (CJEU)
ปี	2019
การอ้างอิง	Case C-507/17 Google LLC v Commission nationale de l'informatique et des libertés (CNIL) [2019]

ภูมิหลัง

สิทธิที่จะถูกลืม (Right to be Forgotten) เป็นหนึ่งในหลักการสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) อย่างไรก็ตาม การตีความและการบังคับใช้สิทธินี้ในยุคอินเทอร์เน็ตที่ไร้พรมแดนนี้ไม่ง่าย และมีความท้าทายทางกฎหมายและเทคโนโลยี กรณีพิพาทระหว่าง CNIL (Commission nationale de l'informatique et des libertés) ซึ่งเป็นหน่วยงานคุ้มครองข้อมูลของฝรั่งเศส และ Google เป็นตัวอย่างสำคัญของความซับซ้อนในประเด็นนี้

สถานการณ์

CNIL ได้มีคำสั่งให้ Google ลบลิงก์ที่เกี่ยวข้องกับบุคคลออกจากผลการค้นหาทั่วโลก (global de-listing) ตามสิทธิที่จะถูกลืมที่ GDPR ได้กำหนดไว้ โดย CNIL สั่งให้ Google ลบลิงก์ที่เกี่ยวข้องกับบุคคลออกจากผลการค้นหาทั่วโลก โดยการลบต้องมีผลในทุกเวอร์ชั่นของ Google Search ทั่วโลก ภายหลังได้รับคำสั่ง Google ไม่เห็นด้วย โดยเห็นว่าการลบข้อมูลจะส่งผลกระทบต่อรายได้และทางปฏิบัติของตนในฐานะ search engine เบอร์หนึ่งของโลก จึงได้ปฏิเสธคำสั่งของ CNIL และเสนอที่จะลบลิงก์เฉพาะในเวอร์ชั่นยุโรปของ Google Search เท่านั้น Google ได้ยกข้อต่อสู้ ดังนี้

1. สิทธิที่จะถูกลืมควรจำกัดเฉพาะในเขตอำนาจของสหภาพยุโรป ไม่ใช่ทั่วโลก

2. การบังคับใช้ทั่วโลกเป็นการละเมิดกฎหมายและสิทธิของประเทศอื่น

3. การลบข้อมูลทั่วโลกอาจกระทบต่อสิทธิในการเข้าถึงข้อมูลของผู้ใช้นอกสหภาพยุโรป

4. ควรสร้างสมดุลระหว่างสิทธิความเป็นส่วนตัวกับสิทธิในการรับรู้ข้อมูล

5. CNIL ไม่มีอำนาจในการบังคับใช้กฎหมายยุโรปนอกเขตสหภาพยุโรป

6. การบังคับใช้กฎหมายนี้จะกระทบและขัดต่อกฎหมายท้องถิ่นในบางประเทศ

7. ผลของการลบอาจนำไปสู่การสกัดกั้นและการปิดกั้นข้อมูลในวงกว้าง และอาจกระทบต่อหลักความเป็นกลางของอินเทอร์เน็ตและการไหลเวียนของข้อมูล

CNIL ได้มีคำสั่งปรับ Google ที่ไม่ยอมปฏิบัติตามคำสั่ง จำนวน 100,000 ยูโร

Google ยื่นอุทธรณ์คำสั่งต่อสภาแห่งรัฐฝรั่งเศส (ซึ่งสภาแห่งรัฐฝรั่งเศสยังทำหน้าที่เป็นศาลปกครองสูงสุดด้วย นอกเหนือจากการให้คำปรึกษาทางกฎหมายแก่รัฐบาล) สภาแห่งรัฐฝรั่งเศสจึงส่งคำถามต่อไปยังศาลยุติธรรมแห่งสหภาพยุโรป (CJEU) เพื่อตีความขอบเขตทางภูมิศาสตร์ของการลบลิงก์หรือสิทธิที่จะถูกลืม โดยมีประเด็นต้องพิจารณา คือ

1. ขอบเขตทางภูมิศาสตร์ของการบังคับใช้สิทธิที่จะถูกลืม

2. ความขัดแย้งระหว่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปกับกฎหมายของประเทศอื่น

3. ความสมดุลระหว่างสิทธิความเป็นส่วนตัวและสิทธิในการเข้าถึงข้อมูล

4. อำนาจของหน่วยงานกำกับดูแลระดับประเทศในการบังคับใช้กฎหมายนอกเขตอำนาจ และ

5. ผลกระทบของการลบข้อมูลทั่วโลกต่อการไหลเวียนของข้อมูลและความเป็นกลางของอินเทอร์เน็ต

คำถามสำคัญสำหรับการวิเคราะห์

1. สิทธิที่จะถูกลืมควรมีขอบเขตทางภูมิศาสตร์เพียงใด? ควรจำกัดเฉพาะในเขตอำนาจของสหภาพยุโรป หรือควรบังคับใช้ทั่วโลก?

2. การบังคับใช้สิทธิที่จะถูกลืมทั่วโลกจะส่งผลกระทบต่อสิทธิในการเข้าถึงข้อมูลของผู้ใช้นอกสหภาพยุโรปอย่างไร?

3. หน่วยงานกำกับดูแลระดับประเทศ เช่น CNIL ควรมีอำนาจในการสั่งการให้บริษัทเทคโนโลยีดำเนินการนอกเขตอำนาจของตนหรือไม่?

4. เราจะสร้างสมดุลระหว่างการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความเป็นกลางของอินเทอร์เน็ตได้อย่างไร?

5. จะมีทางเลือกอื่นในการคุ้มครองสิทธิความเป็นส่วนตัวของบุคคลโดยไม่ต้องลบข้อมูลทั่วโลกหรือไม่? (เช่น การใช้เทคโนโลยีในการจำกัดการเข้าถึงข้อมูลตามภูมิภาค)

6. ในฐานะทนายความของ Google ท่านจะเสนอแนวทางปฏิบัติอย่างไรในการจัดการคำขอลบข้อมูลที่สามารถตอบสนองต่อกฎหมายสหภาพยุโรป โดยไม่ส่งผลกระทบต่อการเข้าถึงข้อมูลในประเทศอื่น ๆ?

คำแนะนำสำหรับทนายความ

ทำความเข้าใจความหมายและขอบเขตทางภูมิศาสตร์ของ GDPR ขอบเขตการบังคับใช้กฎหมายเชิงพื้นที่ การชั่งน้ำหนักระหว่างสิทธิในการลบข้อมูลกับการเข้าถึงข้อมูลในเขตอำนาจศาลที่แตกต่างกัน ศึกษาแนวคิดกฎหมายเกี่ยวกับถิ่นที่อยู่ของข้อมูล (Data localization) ซึ่งกล่าวถึงการจัดเก็บและประมวลผลข้อมูลในประเทศโดยห้ามส่งข้อมูลบางประเภทออกไปยังต่างประเทศ หลักความจำเป็นและได้สัดส่วน และการบังคับใช้กฎหมายคุ้มครองข้อมูลข้ามพรมแดน

กฎหมายที่เกี่ยวข้อง

1. General Data Protection Regulation (GDPR) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เข้มงวดของสหภาพยุโรป มีผลบังคับใช้ตั้งแต่ปี 2018 ครอบคลุมองค์กรทั้งในและนอก EU ที่จัดการข้อมูลของพลเมือง EU โดยกำหนดหลักการสำคัญในการประมวลผลข้อมูล เช่น ความโปร่งใส การจำกัดวัตถุประสงค์และความปลอดภัย รวมทั้งเพิ่มสิทธิให้กับเจ้าของข้อมูล เช่น สิทธิในการลบข้อมูลและการโอนย้ายข้อมูล กำหนดให้ต้องขอความยินยอมอย่างชัดเจน มีการแจ้งเตือนการละเมิดข้อมูลภายใน 72 ชั่วโมง และกำหนดบทลงโทษที่รุนแรงสำหรับการละเมิด GDPR ส่งผลให้องค์กรต่าง ๆ ต้องปรับปรุงนโยบายและแนวปฏิบัติในการจัดการข้อมูลส่วนบุคคลอย่างมีนัยสำคัญ

2. EU Charter of Fundamental Rights (กฎบัตรว่าด้วยสิทธิขั้นพื้นฐานของสหภาพยุโรป) เป็นกฎบัตรที่รับรองสิทธิขั้นพื้นฐานของพลเมือง EU ซึ่งมีผลบังคับใช้ในปี 2009 โดยครอบคลุมสิทธิด้านต่างๆ รวมถึงสิทธิในการคุ้มครองข้อมูลส่วนบุคคล เสรีภาพในการแสดงออก และสิทธิในความเป็นส่วนตัว ซึ่งเป็นพื้นฐานสำคัญของกฎหมายคุ้มครองข้อมูลของ EU

3. French Data Protection Act หรือ “Loi Informatique et Libertés” คือกฎหมายคุ้มครองข้อมูลส่วนบุคคลของฝรั่งเศสที่มีมาตั้งแต่ปี 1978 และได้รับการปรับปรุงให้สอดคล้องกับ GDPR โดยกำหนดหลักเกณฑ์การจัดการข้อมูลส่วนบุคคล รับรองสิทธิของเจ้าของข้อมูล จัดตั้งหน่วยงานกำกับดูแล CNIL และกำหนดบทลงโทษสำหรับการละเมิด เพื่อคุ้มครองสิทธิและเสรีภาพด้านข้อมูลส่วนบุคคลของประชาชนฝรั่งเศส

แหล่งข้อมูล

1. คำตัดสินของ CJEU ในคดี Google LLC v CNIL (Case C-507/17)
2. GDPR Article 17 เกี่ยวกับสิทธิในการลบข้อมูล
3. แนวทางของ European Data Protection Board เกี่ยวกับการบังคับใช้สิทธิที่จะถูกลืม

เอกสารแนะนำเพิ่มเติม

Kuner, C. (2019). The Internet and the Global Reach of EU Law. In EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law (Collected Courses of the Academy of European Law). Oxford University Press.

Woods, A. K. (2018). Litigating Data Sovereignty. Yale Law Journal, 128, 328-406.

คำตัดสิน

ศาลยุติธรรมแห่งสหภาพยุโรป ตัดสินว่า กฎหมายสหภาพยุโรปไม่ได้กำหนดให้ต้องลบลิงก์ทั่วโลก ผู้ให้บริการเครื่องมือค้นหาข้อมูลต้องลบลิงก์ในเวอร์ชั่นของสหภาพยุโรปเท่านั้น ศาลได้พยายามสร้างสมดุลระหว่างการคุ้มครองสิทธิความเป็นส่วนตัวของพลเมืองยุโรปกับการเคารพอธิปไตยทางกฎหมายของประเทศอื่น ศาลชี้ให้เห็นว่า GDPR ไม่ได้มีผลบังคับใช้นอกเขตสหภาพยุโรปแต่อย่างใด การตีความของศาลเป็นการจำกัดขอบเขตทางภูมิศาสตร์ของสิทธิที่จะถูกลืมภายใต้กฎหมาย สร้างความชัดเจนสำหรับผู้ให้บริการเครื่องมือค้นหาเกี่ยวกับขอบเขตของการลบลิงก์ โดยยังเปิดโอกาสให้หน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลสามารถพิจารณาการลบลิงก์ทั่วโลกเป็นรายกรณีได้

คดีนี้ได้กำหนดขอบเขตทางภูมิศาสตร์ของการบังคับใช้กฎหมายคุ้มครองข้อมูลของสหภาพยุโรป โดยเฉพาะในบริบทของอินเทอร์เน็ตที่ไร้พรมแดน และเน้นย้ำถึงความท้าทายในการบังคับใช้กฎหมายคุ้มครองข้อมูลในยุคดิจิทัล

กรณีศึกษาที่ 5: ความเจ็บปวดที่มองไม่เห็น

Vidal-Hall กับการชดเชยความเสียหายทางจิตใจในโลกดิจิทัล

ศาล/เขตอำนาจ	ศาลอุทธรณ์แห่งสหราชอาณาจักรและเวลส์
ปี	2015
การอ้างอิง	Vidal-Hall & Ors v Google Inc [2015] EWCA Civ 311

ภูมิหลัง

การเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลโดยบริษัทเทคโนโลยีขนาดใหญ่เป็นประเด็นที่ได้รับความสนใจอย่างมาก คดี Vidal-Hall v. Google เป็นตัวอย่างสำคัญที่ท้าทายข้อกฎหมายเกี่ยวกับแนวปฏิบัติด้านความเป็นส่วนตัวของบริษัทเทคโนโลยี

สถานการณ์

กลุ่มผู้ใช้ Apple Safari ในสหราชอาณาจักร นำโดย Judith Vidal-Hall ได้ยื่นฟ้อง Google เป็นจำเลยในข้อหาละเมิดพระราชบัญญัติคุ้มครองข้อมูล (Data Protection Act) และการใช้ข้อมูลส่วนตัวในทางที่ผิด (misuse of private information) โดยโจทก์มีข้อกล่าวหาหลัก ดังนี้

1. Google ได้หลีกเลี่ยงการตั้งค่าความเป็นส่วนตัวของเบราว์เซอร์ Safari

2. Google ติดตามและรวบรวมข้อมูลการท่องเว็บไซต์ของกลุ่มโจทก์โดยไม่ได้รับความยินยอม

3. Google ใช้ข้อมูลที่รวบรวมได้เพื่อมุ่งผลโฆษณาแบบเจาะจงพฤติกรรม (targeted advertising)

4. การกระทำของ Google ก่อให้เกิดความเครียดทางจิตใจแก่โจทก์ โจทก์ได้ร้องขอค่าเสียหายสำหรับความเครียดทางจิตใจที่เกิดขึ้นจากการละเมิดความเป็นส่วนตัว

ศาลชั้นต้นได้ตัดสินว่า โจทก์ไม่สามารถเรียกร้องค่าเสียหายได้ เนื่องจากไม่มีความเสียหายที่เป็นตัวเงิน (pecuniary loss)

ภายหลังทราบคำตัดสิน โจทก์ไม่พอใจคำตัดสินของศาลชั้นต้น จึงยื่นอุทธรณ์ไปยังศาลอุทธรณ์ โดยมีประเด็นพิจารณา 4 ประเด็น คือ 1. การตีความพระราชบัญญัติคุ้มครองข้อมูล (Data Protection Act) ในบริบทของการเก็บข้อมูลออนไลน์ 2. การพิจารณาว่าความเครียดทางจิตใจสามารถถือเป็นความเสียหายที่เรียกร้องค่าชดเชยได้หรือไม่ 3. ขอบเขตของความรับผิดชอบของบริษัทเทคโนโลยีในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้ และ 4. การพิจารณาความยินยอมในบริบทของการเก็บข้อมูลออนไลน์

คำถามสำคัญสำหรับการวิเคราะห์

1. การเก็บข้อมูลโดยไม่ได้รับความยินยอมควรถือเป็นการละเมิดความเป็นส่วนตัวที่ร้ายแรงเพียงใด?

2. ความเสียหายทางจิตใจที่เกิดจากการละเมิดความเป็นส่วนตัวควรได้รับการชดเชยทางกฎหมายหรือไม่ อย่างไร?

3. บริษัทเทคโนโลยีควรมีมาตรการอะไรบ้างในการป้องกันการละเมิดความเป็นส่วนตัวของผู้ใช้?

4. การตั้งค่าความเป็นส่วนตัวของเบราว์เซอร์ควรถือเป็นการแสดงความยินยอมหรือไม่ยินยอมในการเก็บข้อมูลหรือไม่?

5. ผลการตัดสินคดีนี้ส่งผลกระทบต่อแนวปฏิบัติด้านความเป็นส่วนตัวและการโฆษณาออนไลน์อย่างไร?

6. ในฐานะทนายความของผู้ใช้อินเทอร์เน็ต ท่านจะมีวิธีการประเมินและพิสูจน์ความเสียหายที่ไม่ใช่ทางการเงินอย่างไร ในกรณีที่มีการละเมิดความเป็นส่วนตัวออนไลน์

คำแนะนำสำหรับทนายความ

ความยากของการฟ้องคดีละเมิดและการเรียกค่าเสียหายจากการละเมิดข้อมูลส่วนบุคคล คือ การกำหนดค่าเสียหาย ซึ่งแนวคิดระบบกฎหมายละเมิดเดิมการเรียกค่าเสียหายตั้งอยู่บนพื้นฐานของค่าเสียหายที่เกิดขึ้นจริงที่ฝ่ายโจทก์มีหน้าที่ต้องพิสูจน์ความเสียหายที่เป็นรูปธรรมให้ได้ อย่างไรก็ดี ในคดีละเมิดความเป็นส่วนตัวและข้อมูลส่วนบุคคลนั้น ไม่ได้ตั้งอยู่บนแนวคิดดังกล่าว แต่มุ่งเน้นที่การคุ้มครองสิทธิพื้นฐานมากกว่าการชดเชยความเสียหายทางวัตถุ โดยความเสียหาย อาจรวมถึงความเสียหายทางจิตใจ ที่ไม่เพียงแต่เป็นความเสียหายที่เป็นตัวเงิน และอาจมีการกำหนดค่าเสียหายเชิงลงโทษได้ด้วยเพื่อป้องปรามการกระทำความผิดในอนาคต มีกลไกพิเศษในการคำนวณค่าเสียหาย เช่น การกำหนดค่าเสียหายขั้นต่ำ และในบางประเทศอาจมีการอนุญาตให้มีการฟ้องคดีแบบกลุ่ม

ความท้าทายในบริบทไทย โปรดพิจารณาเปรียบเทียบ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หมวด 6 ความรับผิดทางแพ่ง มาตรา 77 และ 78 ซึ่งจะเป็นเรื่องท้าทายของศาลและทางปฏิบัติของไทย และการฟ้องคดีแบบกลุ่ม

กฎหมายที่เกี่ยวข้อง

1. UK Data Protection Act 1998 หรือพระราชบัญญัติคุ้มครองข้อมูลของสหราชอาณาจักร ปี 1998 เป็นกฎหมายหลักที่กำกับดูแลการจัดการข้อมูลส่วนบุคคลในสหราชอาณาจักรก่อนถูกแทนที่ในปี 2018 กฎหมายนี้กำหนดหลักการสำคัญในการเก็บรวบรวม ประมวลผล และใช้ข้อมูลส่วนบุคคล รวมถึงสิทธิของเจ้าของข้อมูลและหน้าที่ของผู้ควบคุมข้อมูล มีการจัดตั้ง Information Commissioner's Office (ICO) เป็นหน่วยงานกำกับดูแล และกำหนดบทลงโทษสำหรับการละเมิด แม้จะถูกแทนที่แล้ว แต่กฎหมายนี้มีความสำคัญในการวางรากฐานการคุ้มครองข้อมูลส่วนบุคคลในสหราชอาณาจักร และเป็นพื้นฐานสำหรับการพัฒนากฎหมายคุ้มครองข้อมูลในยุคต่อมา

2. EU Data Protection Directive 95/46/EC (ข้อกำหนดการคุ้มครองข้อมูลของสหภาพยุโรป 95/46/EC) เป็นกรอบกฎหมายหลักของสหภาพยุโรปที่วางรากฐานการคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรป มีผลบังคับใช้ในปี 1995 ก่อนที่จะถูกแทนที่ด้วย GDPR ในปี 2018 ซึ่งมีความครอบคลุมและเข้มงวดมากขึ้น

3. หลักการละเมิดการใช้ข้อมูลส่วนตัวในทางที่ผิด (UK Misuse of Private Information Tort) เป็นหลักกฎหมายที่พัฒนาขึ้นในระบบกฎหมายคอมมอนลอว์ของสหราชอาณาจักร เพื่อคุ้มครองสิทธิความเป็นส่วนตัวของบุคคล หลักการนี้ให้สิทธิแก่บุคคล ในการฟ้องร้องเมื่อมีการใช้หรือเปิดเผยข้อมูลส่วนตัวของตนโดยไม่ได้รับอนุญาตหรือในทางที่ผิด โดยศาลจะพิจารณาว่าข้อมูลนั้นมีลักษณะเป็นส่วนตัวหรือไม่ และการเปิดเผยหรือใช้ข้อมูลนั้นชอบด้วยกฎหมายหรือเป็นประโยชน์ต่อสาธารณะหรือไม่ หลักการนี้มีความสำคัญในการให้ความคุ้มครองเพิ่มเติมนอกเหนือจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีอยู่

แหล่งข้อมูล

1. คำตัดสินของศาลอุทธรณ์ในคดี Vidal-Hall v Google Inc [2015] EWCA Civ 311

2. พระราชบัญญัติคุ้มครองข้อมูลของสหราชอาณาจักร ปี 1998 (UK Data Protection Act 1998)

3. แนวทางของ Information Commissioner's Office (ICO) เกี่ยวกับการชดเชยความเสียหายในคดีคุ้มครองข้อมูล

เอกสารแนะนำเพิ่มเติม

O'Dell, E. (2017). Compensation for breach of the general data protection regulation. Dublin ULJ, 40, 97.

Eaton v. Boc Group Plc & Ors [2015] UKSC 243 (UK Supreme Court case on damages in privacy cases) Available at: https://www.supremecourt.uk/cases/docs/uksc-2013-0243-judgment.pdf

Benjamin C. Zipursky and John C. P. Goldberg. A Tort for the Digital Age: False Light Invasion of Privacy Reconsidered (October 3, 2023). Fordham Law Legal Studies Research Paper No. 4591188

คำตัดสิน

คดีนี้ศาลอุทธรณ์ของอังกฤษและเวลส์ตัดสินว่า คำว่า “ความเสียหาย” ตามพระราชบัญญัติคุ้มครองข้อมูลของสหราชอาณาจักร ควรตีความให้รวมถึงความเสียหายที่ไม่ใช่ตัวเงิน ด้วยเหตุนี้ โจทก์ผู้ร้องจึงสามารถเรียกร้องค่าเสียหายสำหรับความเครียดทางจิตใจได้ แม้จะไม่มีความเสียหายทางการเงินก็ตาม เนื่องจากการใช้ข้อมูลส่วนบุคคลในทางที่มิชอบถือเป็นการละเมิด ศาลได้ตีความให้สอดคล้องกับเจตนารมณ์ของ EU Data Protection Directive ศาลเห็นว่าการจำกัดการเรียกร้องค่าเสียหายเฉพาะกรณีที่มีความเสียหายเป็นตัวเงินจะทำให้สิทธิในการคุ้มครองข้อมูลส่วนบุคคลไม่มีประสิทธิภาพ จะเห็นได้ว่า การยอมรับว่าการใช้ข้อมูลส่วนบุคคลในทางที่ผิดเป็นการละเมิดและเรียกค่าเสียหายได้สะท้อนถึงพัฒนาการของกฎหมายละเมิดและการคุ้มครองความเป็นส่วนตัวในยุคดิจิทัล

ผลกระทบของคดีส่งผลต่อการพิจารณาขอบเขตการเรียกร้องค่าเสียหายในคดีคุ้มครองข้อมูล โดยรวมถึงความเสียหายที่ไม่ใช่ตัวเงิน ถือเป็นการเปิดโอกาสให้มีการฟ้องร้องคดีคุ้มครองข้อมูลมากขึ้น เนื่องจากผู้เสียหายไม่จำเป็นต้องพิสูจน์ความเสียหายที่เป็นตัวเงิน แนวทางการตีความเช่นว่าได้สร้างบรรทัดฐานใหม่ในการพิจารณาคดีเกี่ยวกับการละเมิดความเป็นส่วนตัวและการคุ้มครองข้อมูลของสหราชอาณาจักร ทำให้บริษัทเทคโนโลยีต้องระมัดระวังมากขึ้นในการจัดการข้อมูลส่วนบุคคลของผู้ใช้

กรณีศึกษาที่ 6: ดาราปะทะปาปารัซซี่

คดี Campbell และการชั่งน้ำหนักระหว่างความเป็นส่วนตัวกับเสรีภาพสื่อ

ศาล/เขตอำนาจ สภาขุนนาง (The House of Lords) สหราชอาณาจักร

ปี 2004

การอ้างอิง Campbell v MGN Ltd [2004] UKHL 22

ภูมิหลัง

ในโลกที่ข่าวสารแพร่กระจายอย่างรวดเร็ว ความสมดุลระหว่างสิทธิความเป็นส่วนตัวของบุคคลและเสรีภาพของสื่อในการรายงานข่าวเป็นประเด็นที่ซับซ้อน โดยเฉพาะอย่างยิ่งเมื่อเกี่ยวข้องกับบุคคลสาธารณะ คดี Naomi Campbell v. Mirror Group Newspapers เป็นตัวอย่างสำคัญที่แสดงให้เห็นถึงความท้าทายในการสร้างสมดุลระหว่างสิทธิเหล่านี้

สถานการณ์

นาโอมิ แคมเบล (Naomi Campbell) นางแบบชื่อดังระดับโลก ยื่นฟ้องหนังสือพิมพ์ Daily Mirror (ภายใต้การดำเนินงานของ Mirror Group Newspapers (MGN) Ltd) หลังจากที่หนังสือพิมพ์ได้ตีพิมพ์บทความและภาพถ่ายเกี่ยวกับการเข้ารับการบำบัดการติดยาเสพติดของเธอ โดยโจทก์ (นาโอมิ แคมเบล) มีข้อกล่าวหา คือ 1. การตีพิมพ์บทความและภาพถ่ายเป็นการละเมิดความเป็นส่วนตัว และ 2. ข้อมูลเกี่ยวกับการบำบัดยาเสพติดเป็นข้อมูลส่วนบุคคลที่ละเอียดอ่อนและไม่ควรถูกเปิดเผยต่อสาธารณะ

ทางฝ่ายจำเลย (Mirror Group Newspapers) ได้แสดงข้อโต้แย้ง คือ 1.โจทก์เป็นนางแบบและบุคคลสาธารณะ ซึ่งมีอิทธิพลต่อสังคม โดยเฉพาะในวงการแฟชั่น จึงควรคาดหวังความเป็นส่วนตัวที่น้อยกว่าบุคคลทั่วไป 2. การเปิดเผยข้อมูลเกี่ยวกับการบำบัดยาเสพติดของโจทก์เป็นไปเพื่อประโยชน์สาธารณะ 3. โจทก์เคยปฏิเสธการใช้ยาเสพติดในที่สาธารณะ การเปิดเผยความจริงจึงเป็นการแก้ไขข้อมูลที่เป็นเท็จ 4. การรายงานข่าวเป็นการใช้เสรีภาพในการแสดงออกและเสรีภาพของสื่อ และ 5. การรายงานข่าวไม่ได้มีเจตนาร้ายหรือทำลายชื่อเสียงของโจทก์คดีนี้ได้นำไปสู่การพิจารณาประเด็นทางกฎหมายที่สำคัญ 4 ประเด็น คือ

1. ขอบเขตของสิทธิความเป็นส่วนตัวของบุคคลสาธารณะ
2. การชั่งน้ำหนักระหว่างสิทธิความเป็นส่วนตัวและเสรีภาพของสื่อ
3. การตีความ “ประโยชน์สาธารณะ” ในบริบทของการรายงานข่าวเกี่ยวกับชีวิตส่วนตัวของบุคคลสาธารณะ
4. ความรับผิดชอบของสื่อในการรายงานข้อมูลส่วนบุคคลที่ละเอียดอ่อน

คำถามสำคัญสำหรับการวิเคราะห์

1. บุคคลสาธารณะควรมีสิทธิความเป็นส่วนตัวมากน้อยเพียงใด? มีความแตกต่างระหว่างความเป็นส่วนตัวของบุคคลสาธารณะและบุคคลทั่วไปหรือไม่?

2. อะไรคือเกณฑ์ในการพิจารณาว่าการเปิดเผยข้อมูลส่วนบุคคลเป็นไปเพื่อ “ประโยชน์สาธารณะ”?

3. การที่บุคคลสาธารณะเคยให้ข้อมูลที่เป็นเท็จต่อสาธารณะควรเป็นเหตุผลที่เพียงพอสำหรับสื่อในการเปิดเผยความจริงหรือไม่?

4. ในกรณีที่เกี่ยวข้องกับปัญหาสุขภาพหรือการบำบัดรักษา ควรมีการพิจารณาเป็นพิเศษหรือไม่?

5. การรายงานข่าวเกี่ยวกับชีวิตส่วนตัวของบุคคลสาธารณะส่งผลต่อสังคมอย่างไร? มีประโยชน์หรือโทษอย่างไร?

6. หากศาลตัดสินให้สื่อมีความผิด จะส่งผลกระทบต่อเสรีภาพของสื่อและการรายงานข่าวในอนาคตอย่างไร?

7. ในยุคดิจิทัลที่ข้อมูลแพร่กระจายอย่างรวดเร็ว ควรมีการปรับปรุงกฎหมายหรือแนวปฏิบัติเกี่ยวกับการคุ้มครอง

8. ในฐานะทนายความของนาโอมิ แคมเบล ท่านจะเสนอแนวทางอะไรในการกำหนดขอบเขตความเป็นส่วนตัวสำหรับบุคคลสาธารณะโดยยังคงรักษาสมดุลกับเสรีภาพของสื่อ?

คำแนะนำสำหรับทนายความ

พิจารณาการชั่งน้ำหนักระหว่างสิทธิความเป็นส่วนตัวและเสรีภาพในการแสดงออก ศึกษาพัฒนาการของกฎหมายละเมิดการใช้ข้อมูลส่วนตัวในทางที่ผิด ศึกษาแนวคิดกฎหมายละเมิดของไทย เสรีภาพสื่อ และแนวทางการตีความคดีของศาลไทยว่าด้วยเรื่องการคุ้มครองบุคคลสาธารณะ และติดตามร่างพระราชบัญญัติส่งเสริมจริยธรรมและมาตรฐานวิชาชีพสื่อมวลชน พ.ศ. ....

ในบริบทที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล พิจารณาประวัติการใช้ยาเสพติดในฐานะข้อมูลสุขภาพซึ่งเป็นข้อมูลอ่อนไหว และข้อยกเว้น “Journalistic exemption clause” ตามมาตรา 4 (4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กฎหมายที่เกี่ยวข้อง

1. European Convention on Human Rights, Articles 8 and 10 (อนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน มาตรา 8: สิทธิในการเคารพชีวิตส่วนตัวและครอบครัว และมาตรา 10: เสรีภาพในการแสดงออก) อนุสัญญานี้เป็นกฎหมายระหว่างประเทศที่สำคัญในการคุ้มครองสิทธิมนุษยชนในยุโรป โดยมาตรา 8 รับรองสิทธิในการเคารพชีวิตส่วนตัวและครอบครัว ซึ่งครอบคลุมถึงการคุ้มครองข้อมูลส่วนบุคคล ในขณะที่มาตรา 10 รับรองเสรีภาพในการแสดงออก ทั้งสองมาตรานี้มักถูกนำมาชั่งน้ำหนักเพื่อหาจุดสมดุลระหว่างการคุ้มครองความเป็นส่วนตัวและเสรีภาพในการแสดงออก โดยเฉพาะในกรณีที่เกี่ยวข้องกับการเปิดเผยข้อมูลส่วนบุคคล

2. UK Human Rights Act 1998 หรือ พระราชบัญญัติสิทธิมนุษยชนของสหราชอาณาจักร ปี 1998 กฎหมายนี้นำหลักการของอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชนมาบังคับใช้ในระบบกฎหมายของสหราชอาณาจักร ทำให้ประชาชนสามารถอ้างสิทธิตามอนุสัญญาในศาลภายในประเทศได้ รวมถึงสิทธิในความเป็นส่วนตัวและเสรีภาพในการแสดงออก กฎหมายนี้กำหนดให้ศาลและหน่วยงานของรัฐต้องตีความและใช้กฎหมายให้สอดคล้องกับสิทธิที่รับรองไว้ในอนุสัญญา

3. หลักกฎหมายจารีตประเพณีว่าด้วยการละเมิดความไว้วางใจ (Common Law of Breach of Confidence) หลักกฎหมายนี้เป็นส่วนหนึ่งของระบบคอมมอนลอว์ที่ให้การคุ้มครองข้อมูลที่เป็นความลับ โดยกำหนดว่าหากข้อมูลถูกเปิดเผยภายใต้สถานการณ์ที่สร้างหน้าที่ในการรักษาความลับ การเปิดเผยข้อมูลนั้นโดยไม่ได้รับอนุญาตถือเป็นการละเมิด หลักการนี้ได้รับการพัฒนาให้ครอบคลุมการคุ้มครองข้อมูลส่วนบุคคลมากขึ้น และเป็นพื้นฐานสำคัญในการพัฒนากฎหมายคุ้มครองความเป็นส่วนตัวในระบบกฎหมายอังกฤษ

แหล่งข้อมูล

1. คำตัดสินของสภาขุนนางในคดี Campbell v MGN Ltd [2004] UKHL 22

2. European Convention on Human Rights (Articles 8 and 10)

3. แนวทางของ Independent Press Standards Organization (IPSO) เกี่ยวกับความเป็นส่วนตัว

เอกสารแนะนำเพิ่มเติม

พรรัตน์ แสนทวีสุข (2562). ปัญหาการใช้เสรีภาพของสื่อมวลชนกับการละเมิดสิทธิส่วนบุคคลของบุคคลสาธารณะ. มหาวิทยาลัยธรรมศาสตร์.

ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, ปิยะบุตร บุญอร่ามเรือง, พรรษาสิริ กุหลาบ และชวิน อุ่นภัทร. (2565). คู่มือมาตรฐานและแนวปฏิบัติสำหรับงานข่าวและสื่อสารมวลชน (Professional Journalism Ethics Toolkit 1.0). ศูนย์บริการวิชาการแห่งจุฬาลงกรณ์มหาวิทยาลัย. https://www.law.chula.ac.th/wp-content/uploads/2022/08/Professional-Journalism-Ethics-Toolkit-1.0-Jul2022.pdf

Wong, B. (2020). The journalism exception in UK data protection law. Journal of Media Law, 12(2), 216-236.

คำตัดสิน

ศาลได้ตัดสินด้วยเสียงข้างมากว่า การเปิดเผยรายละเอียดเกี่ยวกับการบำบัดยาเสพติด เป็นการละเมิดความเป็นส่วนตัวของนาโอมิ แคมเบล ดังนั้น โจทก์มีสิทธิได้รับค่าเสียหายแม้ว่าโจทก์จะเป็นบุคคลสาธารณะ แต่โจทก์ก็ยังคงมีสิทธิในความเป็นส่วนตัวในบางสถานการณ์ การเปิดเผยรายละเอียดเกี่ยวกับการบำบัดไม่ได้เป็นประโยชน์ต่อสาธารณะอย่างแท้จริง ในคดีนี้ ศาลต้องชั่งน้ำหนักระหว่างสิทธิในความเป็นส่วนตัวตามมาตรา 8 ของอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (ECHR) กับเสรีภาพในการแสดงออกตามมาตรา 10

ผลกระทบจากคำตัดสินนำไปสู่การพัฒนาการเรื่องละเมิด “การใช้ข้อมูลส่วนตัวในทางที่ผิด” ในกฎหมายอังกฤษ โดยจะเห็นได้ว่าเป็นการคุ้มครองความเป็นส่วนตัวของบุคคลสาธารณะในบางสถานการณ์ ศาลได้พิจารณาถึงความได้สัดส่วน กำหนดแนวทางการชั่งน้ำหนักระหว่างความเป็นส่วนตัวและเสรีภาพในการแสดงออก ความสำคัญของคดีนี้ถือได้ว่าเป็นหมุดหมายสำคัญในการพัฒนากฎหมายความเป็นส่วนตัวในสหราชอาณาจักร โดยเฉพาะในบริบทของบุคคลสาธารณะและสื่อมวลชน สะท้อนถึงการเปลี่ยนแปลงทัศนคติทางสังคมและกฎหมายต่อความเป็นส่วนตัว และการปรับสมดุลระหว่างสิทธิส่วนบุคคลกับประโยชน์สาธารณะ

กรณีศึกษาที่ 7: 143 ล้านชีวิตที่ถูกเปิดเผย

การรั่วไหลข้อมูลของ Equifax: บทเรียนด้านความปลอดภัยข้อมูล

ศาล/เขตอำนาจ คณะกรรมาธิการการค้าของรัฐบาลกลาง

ปี 2019

การอ้างอิง Federal Trade Commission v. Equifax Inc., (N.D. Ga. Jul. 22, 2019)

ภูมิหลัง

ในยุคดิจิทัล ข้อมูลส่วนบุคคลกลายเป็นสินทรัพย์ที่มีค่าและเป็นเป้าหมายสำคัญของอาชญากรไซเบอร์ กรณีการรั่วไหลข้อมูลของ Equifax ในปี 2017 เป็นหนึ่งในเหตุการณ์ละเมิดข้อมูลที่ใหญ่ที่สุดในประวัติศาสตร์ ส่งผลกระทบต่อผู้บริโภคจำนวนมหาศาลและสร้างความเสียหายอย่างกว้างขวาง

สถานการณ์

Equifax Inc. บริษัทรายงานเครดิตผู้บริโภครายใหญ่ของสหรัฐอเมริกา ประสบกับเหตุการณ์การละเมิดข้อมูลครั้งใหญ่ระหว่างเดือนพฤษภาคมถึงกรกฎาคม 2017 โดยข้อมูลส่วนบุคคลของผู้บริโภคชาวอเมริกันประมาณ 147 ล้านคนรั่วไหล ข้อมูลที่รั่วไหลประกอบด้วย หมายเลขประกันสังคม วันเดือนปีเกิด ที่อยู่ และหมายเลขบัตรเครดิต (ในบางกรณี)

จากการสอบข้อเท็จจริงพบสาเหตุของการรั่วไหลข้อมูล คือพบช่องโหว่ในซอฟต์แวร์ Apache Struts ที่ใช้ในเว็บแอปพลิเคชันของบริษัท บริษัทตรวจพบการโจมตีก่อนหน้าหลายเดือน แต่ไม่ได้ดำเนินการแก้ไขอย่างทันท่วงที และบริษัทไม่ได้ติดตั้งแพตช์ความปลอดภัยที่จำเป็น นอกจากนี้ ยังพบข้อบกพร่องด้านความปลอดภัย คือ บริษัทขาดการวางมาตรการการเข้ารหัสข้อมูลที่เหมาะสม ระบบตรวจสอบไม่มีประสิทธิภาพเพียงพอ และขาดระบบเฝ้าระวังที่มีประสิทธิภาพ

ผลของเหตุการณ์ดังกล่าวจึงนำไปสู่การฟ้องร้องจำนวนมาก และมีการตกลงเรียกค่าชดเชยและค่าเสียหายให้กับผู้ได้รับผลกระทบ คดีนี้มีประเด็นพิจารณา คือ

1. ความรับผิดชอบขององค์กรในการปกป้องข้อมูลส่วนบุคคลของลูกค้า
2. ความสำคัญของการตอบสนองต่อภัยคุกคามด้านความปลอดภัยอย่างรวดเร็ว
3. ความจำเป็นในการมีระบบรักษาความปลอดภัยข้อมูลที่ครอบคลุมและทันสมัย และ
4. ผลกระทบทางกฎหมายและการเงินจากการละเมิดข้อมูลขนาดใหญ่

คำถามสำคัญสำหรับการวิเคราะห์

1. องค์กรควรมีมาตรการอะไรบ้างในการป้องกันการรั่วไหลของข้อมูลในลักษณะนี้?

2. ความรับผิดชอบในการรักษาความปลอดภัยข้อมูลควรตกอยู่กับใครบ้าง? (องค์กร, ผู้พัฒนาซอฟต์แวร์, ผู้บริโภค)

3. ระบบการแจ้งเตือนและการตอบสนองต่อภัยคุกคามด้านความปลอดภัยที่มีประสิทธิภาพควรมีลักษณะอย่างไร?

4. การชดเชยที่เหมาะสมสำหรับผู้ได้รับผลกระทบจากการรั่วไหลข้อมูลควรมีลักษณะอย่างไร?

5. กฎหมายและข้อบังคับเกี่ยวกับการรักษาความปลอดภัยข้อมูลควรได้รับการปรับปรุงอย่างไรเพื่อป้องกันเหตุการณ์ในลักษณะนี้?

6. บทเรียนสำคัญที่องค์กรอื่นๆ สามารถเรียนรู้จากกรณีของ Equifax มีอะไรบ้าง?

7. ในฐานะผู้บริโภค เราสามารถปกป้องตัวเองจากผลกระทบของการรั่วไหลข้อมูลในลักษณะนี้ได้อย่างไร?

8. ในฐานะทนายความของผู้บริโภคหรือกลุ่มผู้บริโภค ท่านจะมีเสนอวิธีการชดเชยแบบใดที่นอกเหนือจากค่าชดเชยทางการเงินเพื่อแก้ไขผลกระทบระยะยาวของการละเมิดข้อมูล?

คำแนะนำสำหรับทนายความ

ควรทำความเข้าใจกฎระเบียบด้านความปลอดภัยของข้อมูล โดยเฉพาะอย่างยิ่งมาตรการรักษาความปลอดภัยข้อมูลที่เหมาะสม และพิจารณาการชดเชยค่าเสียหายในวงกว้างต่อการดำเนินธุรกิจของลูกความ ทั้งนี้ ในบริบทของกฎหมายคุ้มครองข้อมูลส่วนบุคคล ให้ทำความเข้าใจบทบาทหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือ โดยมิชอบ โดยดูประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูล

ซึ่งกล่าวถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) ตลอดจนแนวทางการบริหารความเสี่ยง การรับมือกรณีเกิดการรั่วไหลของข้อมูล และหน้าที่ที่ต้องดำเนินการตามที่กฎหมายกำหนด

กฎหมายที่เกี่ยวข้อง

1. Federal Trade Commission Act 1914 กฎหมายหลักของสหรัฐอเมริกาที่ให้อำนาจแก่ Federal Trade Commission (FTC) ในการคุ้มครองผู้บริโภคและส่งเสริมการแข่งขันทางการค้า กฎหมายนี้ห้ามการปฏิบัติทางการค้าที่ไม่เป็นธรรมหรือหลอกลวง รวมถึงการปฏิบัติที่เกี่ยวข้องกับความเป็นส่วนตัวและความปลอดภัยของข้อมูล

2. Gramm-Leach-Bliley Act 1999 กฎหมายที่กำหนดให้สถาบันการเงินต้องอธิบายวิธีการแบ่งปันและคุ้มครองข้อมูลส่วนบุคคลของลูกค้า กฎหมายนี้กำหนดให้สถาบันการเงินต้องแจ้งนโยบายความเป็นส่วนตัวแก่ลูกค้า และให้สิทธิลูกค้าในการจำกัดการแบ่งปันข้อมูลบางอย่าง

3. Fair Credit Reporting Act 1970 กฎหมายที่ควบคุมการรวบรวม เผยแพร่ และใช้ข้อมูลเครดิตของผู้บริโภค กฎหมายนี้กำหนดมาตรฐานความถูกต้อง ความเป็นธรรม และความเป็นส่วนตัวของข้อมูลในรายงานเครดิตผู้บริโภค รวมทั้งให้สิทธิแก่ผู้บริโภคในการเข้าถึงและแก้ไขข้อมูลเครดิตของตน

4. กฎหมายทั้งสามฉบับข้างต้นมีบทบาทสำคัญในการกำกับดูแลการคุ้มครองข้อมูลและความเป็นส่วนตัวของผู้บริโภคในสหรัฐอเมริกา โดยเฉพาะในภาคการเงินและการค้าในกรณีของการละเมิดข้อมูลขนาดใหญ่ เช่น กรณี Equifax กฎหมายเหล่านี้เป็นพื้นฐานสำคัญในการดำเนินคดีและกำหนดบทลงโทษ

แหล่งข้อมูล

1. รายละเอียดการตกลงชดเชยของ Equifax จาก Federal Trade Commission

2. รายงานการสอบสวนของ U.S. Government Accountability Office เกี่ยวกับการละเมิดข้อมูล

3. Equifaxแนวทางปฏิบัติด้านความปลอดภัยของข้อมูลจาก National Institute of Standards and Technology (NIST)

เอกสารแนะนำเพิ่มเติม

Solove, D. J., & Hartzog, W. (2014). The FTC and the New Common Law of Privacy. Columbia Law Review, 114(3), 583-676.

McGeveran, W. (2019). The Duty of Data Security. Minnesota Law Review, 103, 1135-1210.

คำตัดสิน

Equifax ได้ทำข้อตกลงกับคณะกรรมาธิการการค้าของรัฐบาลกลาง FTC, สำนักงานคุ้มครองทางการเงินผู้บริโภค (Consumer Financial Protection Bureau (CFPB)) โดยตกลงจ่ายค่าชดเชยรวมมูลค่าสูงถึง 425 ล้านดอลลาร์สหรัฐ สำหรับผู้บริโภคที่ได้รับผลกระทบ ค่าปรับจำนวน 175 ล้านดอลลาร์สหรัฐให้กับรัฐต่างๆ และค่าปรับจำนวน 100 ล้านดอลลาร์สหรัฐให้กับ CFPB พร้อมให้คำมั่นต้องปรับปรุงมาตรการรักษาความปลอดภัยข้อมูลอย่างมีนัยสำคัญ เนื่องจากEquifax ล้มเหลวในการรักษาความปลอดภัยข้อมูลผู้บริโภคอย่างเพียงพอ และบริษัทไม่ได้แก้ไขช่องโหว่ด้านความปลอดภัยที่ทราบอยู่แล้วจนนำไปสู่การละเมิดข้อมูล ส่งผลกระทบต่อผู้บริโภคจำนวนมากทำให้เจ้าของข้อมูลเสี่ยงต่อการถูกขโมยข้อมูลและการฉ้อโกง

การละเมิดข้อมูลที่เกิดขึ้นเป็นการละเมิดข้อมูลที่ใหญ่ที่สุดในประวัติศาสตร์สหรัฐอเมริกา ผลของการทำข้อตกลงได้สร้างบรรทัดฐานใหม่สำหรับความรับผิดชอบของบริษัทในกรณีการละเมิดข้อมูล กระตุ้นให้บริษัทต่าง ๆ ให้ความสำคัญกับการรักษาความปลอดภัยข้อมูลมากขึ้นและเพิ่มความตระหนักของสาธารณชนเกี่ยวกับความเสี่ยงด้านความปลอดภัยของข้อมูลมากขึ้น คดีนี้ยังได้เน้นย้ำถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค และความจำเป็นในการมีมาตรการรักษาความปลอดภัยที่เข้มงวด คดีนี้ส่งผลให้เกิดการเปลี่ยนแปลงในวิธีการที่บริษัทต่าง ๆ จัดการกับข้อมูลผู้บริโภค และการเตรียมพร้อมรับมือกับการละเมิดข้อมูล

กรณีศึกษาที่ 8: ห้าพันล้านดอลลาร์กับการปฏิวัติความเป็นส่วนตัว

บทลงโทษ Facebook: ความรับผิดชอบของแพลตฟอร์มโซเชียลมีเดีย

ศาล/เขตอำนาจ คณะกรรมาธิการการค้าของรัฐบาลกลาง

ปี 2019

การอ้างอิง United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. filed Jul. 24, 2019)

ภูมิหลัง

ข้อมูลส่วนบุคคลกลายเป็นสินทรัพย์ที่มีมูลค่า การคุ้มครองความเป็นส่วนตัวของผู้ใช้บริการออนไลน์เป็นประเด็นที่ได้รับความสนใจอย่างมาก กรณีพิพาทระหว่างคณะกรรมาธิการการค้าของรัฐบาลกลางสหรัฐอเมริกา (Federal Trade Commission - FTC) และ Facebook นี้ เป็นตัวอย่างสำคัญที่ชี้ให้เห็นบทบาทของหน่วยงานของรัฐกับความพยายามกำกับดูแลบริษัทเทคโนโลยีขนาดใหญ่

สถานการณ์

FTC ได้ฟ้องร้อง Facebook ด้วยข้อกล่าวหาว่าละเมิดข้อตกลงที่ทำไว้กับ FTC เมื่อปี 2012 เกี่ยวกับการคุ้มครองความเป็นส่วนตัวของผู้ใช้ โดย FTC ตั้งข้อกล่าวหา Facebook ว่าละเมิดข้อตกลง Consent Order ปี 2012 โดยใช้ข้อมูลผู้ใช้ในทางที่ผิด เนื่องจากมีข้อมูลผู้ใช้ Facebook จำนวน 87 ล้านคนรั่วไหลเข้าสู่มือบริษัทเอกชนชื่อ เคมบริดจ์ อะนาไลติก้า (Cambridge Analytica) ซึ่งเป็นบริษัทที่ปรึกษาการเมืองบริติช ใช้การทำเหมืองข้อมูล การเป็นนายหน้าข้อมูล และวิเคราะห์ข้อมูลร่วมกับการสื่อสารยุทธศาสตร์สำหรับการเลือกตั้ง โดยบริษัทได้นำข้อมูลมาใช้ช่วยทำแคมเปญหาเสียงของโดนัลด์ ทรัมป์ จากพรรครีพับบลิกัน ในปี 2016 จนพลิกสถานการณ์แซงชนะฮิลลารี่ คลินตัน จากพรรคเดโมแครต และชนะเลือกตั้งในที่สุด

Facebook ได้โต้แย้งข้อกล่าวหา โดยยืนยันว่า ตนได้ปฏิบัติตามคำสั่งข้อตกลง Consent Order ปี 2012 อย่างเคร่งครัด โดยแสดงหลักฐานการปรับปรุงนโยบายและการปฏิบัติด้านความเป็นส่วนตัวตามข้อกำหนด ทั้งนี้ การใช้ข้อมูลในทางที่ผิดโดย Cambridge Analytica เป็นการกระทำของบุคคลที่สาม Facebook ไม่ได้จงใจหรือรู้เห็นกับการกระทำของ Cambridge Analytica แต่อย่างใด และ Facebook ไม่มีเจตนาละเมิดข้อมูลผู้ใช้หรือฝ่าฝืนข้อตกลง

เมื่อมีการต่อสู้และโต้แย้ง จึงมีประเด็นสำคัญให้พิจารณา ดังนี้

1. ขอบเขตความรับผิดชอบของแพลตฟอร์มโซเชียลมีเดียต่อการใช้ข้อมูลผู้ใช้โดยบุคคลที่สาม

2. ประสิทธิภาพของข้อตกลงระหว่างหน่วยงานกำกับดูแลและบริษัทเทคโนโลยี

3. ความสมดุลระหว่างนวัตกรรมทางธุรกิจและการคุ้มครองความเป็นส่วนตัวของผู้ใช้

4. ความท้าทายในการกำกับดูแลบริษัทเทคโนโลยีข้ามชาติ

คำถามสำคัญสำหรับการวิเคราะห์

1. แพลตฟอร์มโซเชียลมีเดียควรมีความรับผิดชอบมากน้อยเพียงใดต่อการใช้ข้อมูลผู้ใช้โดยบุคคลที่สาม?

2. การกำกับดูแลตนเอง (self-regulation) ของบริษัทมีเทคโนโลยีเพียงพอหรือไม่? หรือควรมีการกำกับดูแลจากภายนอกที่เข้มงวดมากขึ้น?

3. ผู้ใช้บริการควรมีบทบาทอย่างไรในการปกป้องคุ้มครองข้อมูลส่วนบุคคลของตนเอง?

4. กรณี Cambridge Analytica สะท้อนให้เห็นถึงความเสี่ยงอะไรบ้างในการใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการเมือง?

5. หากศาลตัดสินให้ Facebook มีความผิด ท่านคิดว่าควรมีบทลงโทษอย่างไรจึงจะเหมาะสมและมีประสิทธิภาพในการป้องกันการละเมิดในอนาคต?

6. การสร้างสมดุลระหว่างการส่งเสริมนวัตกรรมทางเทคโนโลยีและการคุ้มครองสิทธิของผู้ใช้ ควรทำอย่างไร?

7. หากท่านเป็นที่ปรึกษากฎหมายของ Facebook ท่านจะเสนอโครงสร้างการกำกับดูแลความเป็นส่วนตัวแบบใดที่สามารถตอบสนองข้อกังวลของคณะกรรมาธิการการค้าของรัฐบาลกลาง โดยยังคงรักษาความยืดหยุ่นในการพัฒนานวัตกรรมของบริษัท?

คำแนะนำสำหรับทนายความ

ศึกษาการบังคับใช้กฎหมายของคณะกรรมาธิการการค้าของรัฐบาลกลางสหรัฐอเมริกา และทำความเข้าใจเกี่ยวกับข้อกำหนดด้านความเป็นส่วนตัวสำหรับแพลตฟอร์มโซเชียลมีเดีย การกำหนดนโยบายความเป็นส่วนตัว และการบริหารความเสี่ยงข้อมูลกรณีที่มีบุคคลที่สามเข้ามาเกี่ยวข้อง หรือมีการส่งต่อข้อมูลส่วนบุคคล ซึ่งเรื่องดังกล่าว เชื่อมโยงกับแนวคิดและวิธีการการบริหารความเสี่ยงข้อมูล กับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

กฎหมายที่เกี่ยวข้อง

1. Federal Trade Commission Act 1914 กฎหมายหลักของสหรัฐอเมริกาที่ให้อำนาจแก่ Federal Trade Commission (FTC) ในการคุ้มครองผู้บริโภคและส่งเสริมการแข่งขันทางการค้า กฎหมายนี้ห้ามการปฏิบัติทางการค้าที่ไม่เป็นธรรมหรือหลอกลวง รวมถึงการปฏิบัติที่เกี่ยวข้องกับความเป็นส่วนตัวและความปลอดภัยของข้อมูล

2. FTC's 2012 Consent Order with Facebook เป็นข้อตกลงระหว่างคณะกรรมาธิการการค้าของรัฐบาลกลางกับ Facebook เพื่อแก้ไขข้อกังวลด้านความเป็นส่วนตัว โดยกำหนดให้ Facebook ต้องขอความยินยอมจากผู้ใช้ก่อนทำการเปลี่ยนแปลงการตั้งค่าความเป็นส่วนตัว ห้าม Facebook ให้ข้อมูลเท็จเกี่ยวกับความเป็นส่วนตัวหรือความปลอดภัยของข้อมูลผู้ใช้ และกำหนดให้มีการตรวจสอบความเป็นส่วนตัวโดยบุคคลที่สามทุก 2 ปี โดยความตกลงนี้มีผลบังคับใช้เป็นเวลา 20 ปี

3. Children's Online Privacy Protection Act 1998 (COPPA) หรือพระราชบัญญัติคุ้มครองความเป็นส่วนตัวออนไลน์ของเด็ก มีวัตถุประสงค์เพื่อคุ้มครองความเป็นส่วนตัวของเด็กอายุต่ำกว่า 13 ปี ในสหรัฐอเมริกา เนื่องจากระบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกา มีลักษณะการแยกระหว่างกฎหมายกลางและกฎหมายระดับมลรัฐ อีกทั้งยังแยกตามประเด็น หรือ sectoral approach ในกรณีของการคุ้มครองความเป็นส่วนตัวของเด็กนั้น COPPA คือกฎหมายกลางที่ใช้กับทุกมลรัฐ โดยกำหนดให้เว็บไซต์และ

แอปพลิเคชันต้องได้รับความยินยอมจากผู้ปกครองก่อนเก็บข้อมูลส่วนบุคคลของเด็ก มีการควบคุมวิธีการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลของเด็ก และกำหนดให้เว็บไซต์ต้องมีนโยบายความเป็นส่วนตัวที่ชัดเจนและให้ผู้ปกครองสามารถตรวจสอบข้อมูลของบุตรหลานได้ ในกรณีของเด็กอายุต่ำกว่า 13 ปี มีบัญชี Facebook จึงอยู่ภายใต้กฎหมายดังกล่าว

แหล่งข้อมูล

1. รายละเอียดข้อตกลงระหว่าง FTC และ Facebook
2. รายงานการสอบสวนของ U.S. Senate เกี่ยวกับกรณี Cambridge Analytica

เอกสารแนะนำเพิ่มเติม

Hoofnagle, C. J., et al. (2019). The FTC can rise to the privacy challenge, but not without help from Congress. Brookings Institution. https://www.brookings.edu/articles/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press.

คำตัดสิน

Facebook ได้ขอทำข้อตกลงกับคณะกรรมาธิการการค้าของรัฐบาลกลาง โดยยอมจ่ายค่าปรับจำนวน 5 พันล้านดอลลาร์สหรัฐ ซึ่งเป็นค่าปรับที่สูงที่สุดที่คณะกรรมาธิการการค้าของรัฐบาลกลางเคยกำหนดในคดีการละเมิดความเป็นส่วนตัวของผู้บริโภค พร้อมทั้งเสนอการปรับโครงสร้างการกำกับดูแลด้านความเป็นส่วนตัวของบริษัท และจัดทำข้อกำหนดใหม่เกี่ยวกับการรายงานและการตรวจสอบด้านความเป็นส่วนตัว การทำข้อตกลงดังกล่าวสะท้อนว่า Facebook ได้ละเมิดข้อตกลงปี 2012 โดยไม่แจ้งผู้ใช้อย่างชัดเจนว่าข้อมูลของผู้ใช้จะถูกเปิดเผยต่อแอปพลิเคชันของบุคคลที่สาม โดยพบว่าบริษัทใช้หมายเลขโทรศัพท์ที่ผู้ใช้ให้ไว้ในการโฆษณาโดยไม่ได้รับอนุญาต (เดิมบริษัทขอข้อมูลหมายเลขโทรศัพท์ของผู้ใช้มาไว้เพื่อวัตถุประสงค์ในการรักษาความปลอดภัยเท่านั้น) และ Facebook ไม่ได้ตรวจสอบอย่างเพียงพอว่าแอปพลิเคชันของบุคคลที่สามปฏิบัติตามนโยบายความเป็นส่วนตัวของบริษัทหรือไม่

คดีนี้ได้สร้างบรรทัดฐานสำหรับความรับผิดชอบด้านความเป็นส่วนตัวของบริษัทเทคโนโลยีขนาดใหญ่ที่จะต้องเพิ่มการตรวจสอบและการกำกับดูแลการปฏิบัติด้านความเป็นส่วนตัว และกระตุ้นให้บริษัทเทคโนโลยีอื่น ๆ ทบทวนและปรับปรุงนโยบายความเป็นส่วนตัวของตนตาม รวมถึงเพิ่มความตระหนักของสาธารณชนเกี่ยวกับการใช้ข้อมูลส่วนบุคคลโดยแพลตฟอร์มโซเชียลมีเดีย และเน้นย้ำความจริงจังของหน่วยงานกำกับดูแลในการจัดการกับการละเมิดความเป็นส่วนตัวของผู้บริโภคในสหรัฐอเมริกา โดยสัญญาณที่ชัดเจนเรื่องความคาดหวังที่สูงในเรื่องความโปร่งใส และความรับผิดชอบจากบริษัทเทคโนโลยีขนาดใหญ่ในการจัดการข้อมูลผู้ใช้ คดีนี้มีอิทธิพลอย่างมากต่อการพัฒนานโยบายและแนวปฏิบัติด้านความเป็นส่วนตัวในอุตสาหกรรมเทคโนโลยี

กรณีศึกษาที่ 9: เมื่อนายจ้างแอบดู

Bărbulescu กับความเป็นส่วนตัวในที่ทำงาน

ศาล/เขตอำนาจ ศาลสิทธิมนุษยชนยุโรป

ปี 2017

การอ้างอิง Bărbulescu v Romania [2017] ECHR 742

ภูมิหลัง

เส้นแบ่งระหว่างชีวิตส่วนตัวและชีวิตการทำงานมักไม่ชัดเจน การใช้เทคโนโลยีการสื่อสารในที่ทำงานก่อให้เกิดคำถามเกี่ยวกับขอบเขตของความเป็นส่วนตัวที่พนักงานควรได้รับ และสิทธิของนายจ้างในการตรวจสอบการใช้ทรัพยากรของบริษัท คดี Bărbulescu v. Romania จะเป็นตัวอย่างสำคัญที่ช่วยให้เห็นความท้าทายทางกฎหมายและการสร้างสมดุลระหว่างสิทธิที่ว่าทนายความที่สนใจมิติทับซ้อนระหว่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกฎหมายแรงงานไม่ควรพลาด

สถานการณ์

นาย Bogdan Mihai Bărbulescu ถูกไล่ออกจากงานเนื่องจากมีพฤติกรรมใช้บัญชี Yahoo Messenger ของบริษัทเพื่อวัตถุประสงค์ส่วนตัว โดยนายจ้างได้ตรวจสอบประวัติการสื่อสารของเขาโดยไม่ได้แจ้งให้ทราบล่วงหน้า นาย Bărbulescu ไม่พอใจจึงได้ยื่นฟ้องนายจ้างต่อศาลโรมาเนียข้อหาละเมิดความเป็นส่วนตัว ผลปรากฏว่า นาย Bărbulescu แพ้คดีในทุกชั้นศาลของโรมาเนีย และเป็นที่มาของการร้องต่อศาลสิทธิมนุษยชนยุโรป (ECtHR) ให้พิจารณา

ในการสู้คดี บริษัทในฐานะนายจ้างให้เหตุผลว่า บริษัทมีนโยบายห้ามใช้อุปกรณ์และการสื่อสารของบริษัทเพื่อวัตถุประสงค์ส่วนตัว ซึ่งตัวนาย Bărbulescu ได้รับทราบและยอมรับนโยบายนี้ ทั้งนี้ การตรวจสอบการสื่อสารของพนักงานเป็นสิ่งจำเป็นเพื่อยืนยันว่าพนักงานได้ปฏิบัติตามนโยบายและทำงานอย่างมีประสิทธิภาพ อีกทั้ง การตรวจสอบยังมีความสำคัญต่อการรักษาความปลอดภัยของข้อมูลและความลับทางธุรกิจ โดยในการตรวจสอบจำกัดเฉพาะบัญชี Yahoo Messenger ที่สร้างขึ้นเพื่อวัตถุประสงค์ทางธุรกิจเท่านั้น ไม่ได้ตรวจสอบข้อมูลส่วนตัวของพนักงานแต่อย่างใด

นอกจากนี้ ทางบริษัทยังกล่าวอีกว่า พนักงานไม่ควรคาดหวังความเป็นส่วนตัวจากการใช้ทรัพยากรของบริษัทในเวลางาน อีกทั้ง บริษัทมีนโยบายระบุการแจ้งเตือนล่วงหน้าอยู่แล้วว่าการสื่อสารอาจถูกตรวจสอบได้ การที่นาย Bărbulescu ถูกตรวจสอบและถูกเลิกจ้าง เป็นเรื่องที่ชอบด้วยกฎหมาย ได้สัดส่วนกับการละเมิดนโยบายของบริษัท เพราะการกระทำของ Bărbulescu ส่งผลกระทบต่อประสิทธิภาพการทำงานและความน่าเชื่อถือ การเลิกจ้างเป็นไปตามขั้นตอนทางกฎหมายเพื่อปกป้องผลประโยชน์ทางธุรกิจของบริษัท โดยนโยบายและการปฏิบัติดังกล่าวก็ใช้กับพนักงานทุกคนอย่างเท่าเทียม ไม่มีการเลือกปฏิบัติกับพนักงานคนใดคนหนึ่ง อีกทั้งยังสอดคล้องกับแนวปฏิบัติมาตรฐานทั่วไปในอุตสาหกรรมของธุรกิจประเภทเดียวกัน

จากข้อเท็จจริง มีประเด็นชวนพิจารณา 6 ประเด็นหลัก คือ

1. ขอบเขตของความเป็นส่วนตัวในที่ทำงาน

2. สิทธิของนายจ้างในการตรวจสอบการใช้ทรัพยากรของบริษัท

3. ความสมดุลระหว่างการคุ้มครองผลประโยชน์ทางธุรกิจและสิทธิของพนักงาน

4. ความเพียงพอของการแจ้งเตือนเกี่ยวกับนโยบายการตรวจสอบ

5. ผลกระทบของการใช้เทคโนโลยีการสื่อสารในที่ทำงานต่อความเป็นส่วนตัว และ

6. ความเหมาะสมของการลงโทษสำหรับการละเมิดนโยบายการใช้ทรัพยากรของบริษัท

คำถามสำคัญสำหรับการวิเคราะห์

1. พนักงานควรคาดหวังความเป็นส่วนตัวในการใช้ทรัพยากรการสื่อสารของบริษัทมากน้อยเพียงใด?

2. นายจ้างควรมีขอบเขตในการตรวจสอบการสื่อสารของพนักงานอย่างไร? มีวิธีการใดที่สามารถสร้างสมดุลระหว่างความจำเป็นทางธุรกิจและสิทธิความเป็นส่วนตัวของพนักงาน?

3. การแจ้งเตือนล่วงหน้าเกี่ยวกับนโยบายการตรวจสอบเพียงพอที่จะทำให้การตรวจสอบนั้นชอบธรรมหรือไม่? ควรมีมาตรการเพิ่มเติมอย่างไร?

4. การใช้ทรัพยากรของบริษัทเพื่อวัตถุประสงค์ส่วนตัวในระดับใดที่ควรถือว่าเป็นการละเมิดร้ายแรงจนถึงขั้นเลิกจ้างหรือไม่?

5. การตัดสินของ ECtHR ในคดีนี้จะส่งผลกระทบต่อแนวปฏิบัติด้านการบริหารทรัพยากรบุคคลและนโยบายการใช้เทคโนโลยีในที่ทำงานอย่างไร?

6. หากท่านเป็นที่ปรึกษากฎหมายให้กับบริษัท ท่านจะร่างนโยบายการตรวจสอบการสื่อสารของพนักงานอย่างไรให้สอดคล้องกับคำตัดสินนี้ โดยยังคงปกป้องผลประโยชน์ของนายจ้าง?

คำแนะนำสำหรับทนายความ

คดีนี้เป็นการพิจารณาความสมดุลระหว่างสิทธิของนายจ้างและลูกจ้างในกรณีการใช้เทคโนโลยีการสื่อสาร ซึ่งประเด็นแห่งคดีเป็นการชั่งน้ำหนักสิทธิความเป็นส่วนตัวในที่ทำงานกับกฎหมายแรงงาน แม้นายจ้างจะได้ยกข้อต่อสู้เรื่องการจัดทำประกาศหรือนโยบายความเป็นส่วนตัว แต่ก็ยังอาจถูกพิจารณาเรื่องความไม่ได้สัดส่วนเรื่องนโยบายการตรวจสอบและความชอบด้วยกฎหมายของการตรวจสอบการสื่อสาร บริบทของคดีเป็นกลุ่มสหภาพยุโรปซึ่งให้ความสำคัญกับการคุ้มครองสิทธิมนุษยชน

ศึกษา ทบทวน และปรับปรุงนโยบายการตรวจสอบการสื่อสารของพนักงานของลูกความ จัดทำนโยบายของบริษัทว่าด้วยความเป็นส่วนตัวที่ชัดเจน โปร่งใส และพัฒนาแนวทางการแจ้งเตือนแก่พนักงานเกี่ยวกับการตรวจสอบการสื่อสารที่อาจเกิดขึ้น และกรณีการเลิกจ้างต้องพิจารณาสัดส่วนความรุนแรงของการกระทำกับการเลิกจ้าง เพื่อหลีกเลี่ยงการเลิกจ้างไม่เป็นธรรม

กฎหมายที่เกี่ยวข้อง

1. European Convention on Human Rights (Article 8) หรืออนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (มาตรา 8) เป็นบทบัญญัติสำคัญที่รับรองสิทธิในการเคารพชีวิตส่วนตัวและครอบครัว ที่อยู่อาศัย และการติดต่อสื่อสาร โดยคุ้มครองบุคคลจากการแทรกแซงที่ไม่ชอบด้วยกฎหมายในชีวิตส่วนตัว ครอบคลุมทั้งความเป็นส่วนตัวทางกายภาพและจิตใจ รวมถึงการคุ้มครองข้อมูลส่วนบุคคล อย่างไรก็ตาม สิทธินี้ไม่ใช่สิทธิเด็ดขาดและอาจถูกจำกัดได้ภายใต้เงื่อนไขที่กำหนด เช่น เพื่อความมั่นคงของชาติหรือความปลอดภัยสาธารณะ

2. Romanian Labour Code หรือประมวลกฎหมายแรงงานของโรมาเนีย เป็นกฎหมายแรงงานของโรมาเนีย กำหนดสิทธิและหน้าที่ของนายจ้างและลูกจ้างในโรมาเนีย ครอบคลุมเรื่องสัญญาจ้างงาน เงื่อนไขการทำงาน และการเลิกจ้าง และมีบทบัญญัติเกี่ยวกับการคุ้มครองสิทธิของพนักงาน รวมถึงสิทธิความเป็นส่วนตัว

3. EU Working Party 29 Opinion on data processing at work หรือความเห็นคณะทำงานมาตรา 29 แห่งสหภาพยุโรปเกี่ยวกับการประมวลผลข้อมูลในที่ทำงาน เป็นแนวทางที่ออกโดยคณะทำงานผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลของสหภาพยุโรป ให้คำแนะนำเกี่ยวกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลในบริบทของการจ้างงาน ครอบคลุมประเด็นต่าง ๆ เช่น การตรวจสอบอีเมลและการใช้อินเทอร์เน็ตของพนักงาน การใช้กล้องวงจรปิด และการประมวลผลข้อมูลชีวภาพ โดยเน้นย้ำหลักความโปร่งใส ความได้สัดส่วน และความจำเป็นในการประมวลผลข้อมูลของพนักงาน

แหล่งข้อมูล

1. คำตัดสินของ ECtHR ในคดี Bărbulescu v Romania [2017] ECHR 742

2. แนวทางของ European Data Protection Board เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลในบริบทการจ้างงาน

3. รายงานของ International Labour Organization เกี่ยวกับความเป็นส่วนตัวในที่ทำงาน

เอกสารแนะนำเพิ่มเติม

ปิยะบุตร บุญอร่ามเรือง และคณะ. (2563). Thailand Data Protection Guidelines 3.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. (การตรวจสอบลูกจ้างดูหน้า 457-467) https://www.law.chula.ac.th/wp-content/uploads/2020/12/TDPG3.0-C5-20201208.pdf

Hendrickx, F. (2019). Privacy 4.0 at work: Regulating employment, technology and automation. Comparative Labor Law & Policy Journal, 41(1), 147-172.

Mantouvalou, V. (2019). New Technologies at Work: The Human Rights Implications. Comparative Labor Law & Policy Journal, 41(1), 1-32.

คำตัดสิน

ศาลสิทธิมนุษยชนยุโรป (ECtHR) ตัดสินว่ามีการละเมิดมาตรา 8 (สิทธิในการเคารพชีวิตส่วนตัวและครอบครัว) ของอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (ECHR) โดยศาลให้เหตุผลว่าหน่วยงานในประเทศไม่ได้คุ้มครองสิทธิของนาย Bărbulescu อย่างเพียงพอ ไม่มีการแจ้งเตือนล่วงหน้าเกี่ยวกับขอบเขตและลักษณะของการตรวจสอบการสื่อสาร ไม่ได้พิจารณาถึงความรุนแรงของผลกระทบจากการตรวจสอบและการเลิกจ้างที่ตามมา และไม่ได้ตรวจสอบว่ามีวิธีการอื่นที่รุนแรงน้อยกว่าในการบรรลุวัตถุประสงค์ของนายจ้างหรือไม่

ผลของคำพิพากษาส่งผลให้เกิดการกำหนดแนวทางสำหรับการคุ้มครองความเป็นส่วนตัวในที่ทำงาน และเน้นย้ำความสำคัญของการแจ้งให้พนักงานทราบล่วงหน้าเกี่ยวกับนโยบายการตรวจสอบ นอกจากนี้ยังกำหนดให้นายจ้างต้องมีเหตุผลที่ชอบธรรมและใช้วิธีการที่ได้สัดส่วนในการตรวจสอบ และส่งเสริมให้มีการสร้างสมดุลระหว่างผลประโยชน์ของนายจ้างและสิทธิของลูกจ้าง

คดีนี้เน้นให้เห็นความสำคัญในการกำหนดขอบเขตของความเป็นส่วนตัวในที่ทำงานในยุคดิจิทัล โดยเฉพาะในบริบทของการใช้เทคโนโลยีการสื่อสาร คำตัดสินเหมือนเป็นการเตือนว่าแม้ในสภาพแวดล้อมการทำงาน ลูกจ้างยังคงมีสิทธิที่จะคาดหวังความเป็นส่วนตัวในระดับหนึ่ง และนายจ้างต้องดำเนินการอย่างโปร่งใสและได้สัดส่วนในการตรวจสอบการสื่อสารของพนักงาน นอกจากนี้ ยังเน้นย้ำถึงความสำคัญของการมีนโยบายที่ชัดเจนและการสื่อสารที่มีประสิทธิภาพเกี่ยวกับการใช้เทคโนโลยีในที่ทำงาน

กรณีศึกษาที่ 10:ความเป็นส่วนตัวเบื้องหลัง IP Address

คดี Spencer และความลับออนไลน์ที่ไม่มีอีกต่อไป

ศาล/เขตอำนาจ ศาลสูงแห่งแคนาดา

ปี 2014

การอ้างอิง R v Spencer, 2014 SCC 43

ภูมิหลัง

การสืบสวนอาชญากรรมทางอินเทอร์เน็ตมักเผชิญกับความท้าทายในการสร้างสมดุลระหว่างประสิทธิภาพในการบังคับใช้กฎหมายและการคุ้มครองสิทธิความเป็นส่วนตัวของพลเมือง คดี R v. Spencer จะชวนให้ทนายความอาญาคิดวิเคราะห์ และแสดงให้เห็นถึงความซับซ้อนของเรื่องในบริบทของกฎหมายแคนาดา

สถานการณ์

ตำรวจแคนาดากำลังสืบสวนการแชร์ภาพอนาจารเด็กทางอินเทอร์เน็ต และได้รับที่อยู่ IP address ที่เกี่ยวข้องกับการกระทำผิด โดยระหว่างการสืบสวน ตำรวจได้ขอข้อมูลผู้สมัครใช้บริการจากผู้ให้บริการอินเทอร์เน็ต (ISP) โดยไม่มีหมายศาล ผู้ให้บริการอินเทอร์เน็ตรายหนึ่งได้ให้ข้อมูลแก่ตำรวจ และเป็นที่มานำไปสู่การระบุตัวนาย Spencer ภายหลัง ตำรวจใช้ข้อมูลนี้เพื่อขอหมายค้นบ้านของ Spencer และพบหลักฐานการครอบครองสื่อลามกอนาจารเด็กของนาย Spencer

นาย Spencer ให้เหตุผลโต้แย้งว่า ตนมีความคาดหวังความเป็นส่วนตัวที่สมเหตุสมผลในข้อมูลในฐานะผู้สมัครใช้บริการอินเทอร์เน็ต เพราะตัวข้อมูลนี้เชื่อมโยงกับกิจกรรมออนไลน์ส่วนตัว การที่ตำรวจขอข้อมูลจาก ISP โดยไม่มีหมายศาลเป็นการค้นที่ไม่ชอบด้วยกฎหมาย ละเมิดสิทธิตามกฎบัตรสิทธิและเสรีภาพแห่งแคนาดา (มาตรา 8) อีกทั้ง กฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (PIPEA, 2000) ไม่ได้ให้อำนาจตำรวจในการขอข้อมูลโดยไม่มีหมายศาลแต่อย่างใด

นอกจากนี้ นาย Spencer ยังต่อสู้อีกว่า การที่ตนยินยอมให้ ISP เก็บข้อมูล ไม่ได้หมายถึงการยินยอมให้เปิดเผยข้อมูลต่อเจ้าหน้าที่ การให้ความยินยอมดังกล่าวไม่ใช่การสละสิทธิความเป็นส่วนตัวจากการใช้บริการอินเทอร์เน็ต ด้วยเหตุนี้ นาย Spencer จึงขอให้ตัดพยานหลักฐานที่ได้มาโดยไม่ชอบด้วยกฎหมายนี้ เพราะหากรับฟังจะทำให้กระบวนการยุติธรรมเสื่อมเสีย พร้อมกับโต้แย้ง

ว่าการขอข้อมูลโดยไม่มีหมายศาลไม่ได้สัดส่วนกับวัตถุประสงค์ของการสืบสวนคดี เนื่องจากมีวิธีการอื่นหรือทางเลือกอื่นที่กระทบสิทธิของตนน้อยกว่า อีกทั้งไม่มีสถานการณ์ฉุกเฉินที่จำเป็นที่ตำรวจต้องขอข้อมูลโดยไม่มีหมายศาล การกระทำของตำรวจเช่นว่า เป็นการกระทำที่กระทบต่อสิทธิความเป็นส่วนตัวของพลเมืองในวงกว้าง ชี้ให้เห็นถึงความเสี่ยงของการสอดแนมทางอินเทอร์เน็ตโดยรัฐ จึงขอให้ศาลตีความกฎหมายให้สอดคล้องกับความเป็นจริงในยุคดิจิทัลและการคุ้มครองความเป็นส่วนตัวออนไลน์

เหตุผลข้อหักล้างนำมาสู่การตั้งประเด็นพิจารณาข้อกฎหมาย คือ

1. ขอบเขตของความเป็นส่วนตัวออนไลน์และความคาดหวังที่สมเหตุสมผลในความเป็นส่วนตัว

2. ความจำเป็นของหมายศาลในการขอข้อมูลจากผู้ให้บริการอินเทอร์เน็ต

3. การตีความกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบริบทของการสืบสวนทางอาญา

4. ความสมดุลระหว่างประสิทธิภาพในการบังคับใช้กฎหมายและการคุ้มครองสิทธิความเป็นส่วนตัว

5. การใช้หลักความได้สัดส่วนในการพิจารณาความชอบด้วยกฎหมายของการสืบสวน และ

6. ผลกระทบของการตัดสินคดีต่อการคุ้มครองความเป็นส่วนตัวออนไลน์และการสืบสวนอาชญากรรมทางอินเทอร์เน็ต

คำถามสำคัญสำหรับการวิเคราะห์

1. การขอข้อมูลจากผู้ให้บริการอินเทอร์เน็ตโดยไม่มีหมายศาลควรถือว่าเป็นการค้นที่ไม่ชอบด้วยกฎหมายหรือไม่? ภายใต้เงื่อนไขใดบ้าง?

2. ควรมีการปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างไร เพื่อให้สอดคล้องกับความท้าทายในการสืบสวนอาชญากรรมทางอินเทอร์เน็ต?

3. การยินยอมให้ผู้ให้บริการอินเทอร์เน็ตเก็บข้อมูลควรถือว่าเป็นการยินยอมให้เปิดเผยข้อมูลต่อเจ้าหน้าที่หรือไม่ เพราะเหตุใด?

4. ในกรณีของอาชญากรรมร้ายแรง เช่น การแชร์ภาพอนาจารเด็ก ควรมีข้อยกเว้นในการขอข้อมูลโดยไม่ต้องมีหมายศาลหรือไม่?

5. จะสร้างสมดุลระหว่างการคุ้มครองเด็กจากการถูกล่วงละเมิดทางอินเทอร์เน็ตและการคุ้มครองสิทธิความเป็นส่วนตัวของผู้ใช้อินเทอร์เน็ตทั่วไปได้อย่างไร?

6. การตีความกฎหมายในยุคดิจิทัลควรคำนึงถึงปัจจัยใดบ้างเพื่อให้สอดคล้องกับความเป็นจริงของเทคโนโลยีและการใช้งานอินเทอร์เน็ต?

7. ในฐานะที่ปรึกษากฎหมายของตำรวจ ท่านจะเสนอแนวทางอะไรในการขอข้อมูลจากผู้ให้บริการอินเทอร์เน็ตที่สามารถสมดุลระหว่างความจำเป็นในการสืบสวนอาชญากรรมกับการคุ้มครองความเป็นส่วนตัวของผู้ใช้อินเทอร์เน็ต?

คำแนะนำสำหรับทนายความ

ศึกษาแนวทางการตีความหลักความคาดหวังที่สมเหตุสมผลเกี่ยวกับความเป็นส่วนตัวในบริบทดิจิทัล (reasonable expectation of privacy) พิจารณาผลกระทบของคำตัดสินต่อการสืบสวนอาชญากรรมทางอินเทอร์เน็ต และเตรียมพร้อมให้คำแนะนำแก่ผู้ให้บริการอินเทอร์เน็ตเกี่ยวกับการเปิดเผยข้อมูลผู้ใช้ โดยเฉพาะประเด็นเรื่องการขอหมาย หรือกรณีการเข้าถึงหรือค้นข้อมูลโดยไม่ต้องมีหมายศาล

กฎหมายที่เกี่ยวข้อง

1. Canadian Charter of Rights and Freedoms (Section 8) หรือกฎบัตรสิทธิและเสรีภาพแห่งแคนาดา (มาตรา 8) กำหนดเรื่องการคุ้มครองจากการค้นและยึดโดยไม่สมเหตุสมผล และความคาดหวังที่สมเหตุสมผลในเรื่องความเป็นส่วนตัว

2. Criminal Code of Canada หรือประมวลกฎหมายอาญาแคนาดา กำหนดความผิดทางอาญาและบทลงโทษ รวมถึงบทบัญญัติเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์และการละเมิดความเป็นส่วนตัว

3. Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA)) หรือพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ เป็นกฎหมายหลักของประเทศแคนาดาที่ควบคุมการจัดการข้อมูลส่วนบุคคลในภาคเอกชน มีผลบังคับใช้ตั้งแต่ปี 2000 กฎหมายนี้กำหนด

หลักการพื้นฐานในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยมุ่งเน้นการให้ความยินยอมของเจ้าของข้อมูล ความโปร่งใส และความรับผิดชอบขององค์กร PIPEDA ยังกำหนดสิทธิของเจ้าของข้อมูลในการเข้าถึงและแก้ไขข้อมูลของตน รวมถึงการร้องเรียนต่อ Privacy Commissioner of Canada หากมีการละเมิด นอกจากนี้ ยังครอบคลุมการรับรองความถูกต้องของเอกสารอิเล็กทรอนิกส์ ทำให้เป็นกฎหมายที่มีความสำคัญทั้งในด้านการคุ้มครองข้อมูลส่วนบุคคลและการส่งเสริมธุรกรรมอิเล็กทรอนิกส์ในแคนาดา

แหล่งข้อมูล

1. คำตัดสินของศาลฎีกาแคนาดาในคดี R v Spencer, 2014 SCC 43
2. Personal Information Protection and Electronic Documents Act (PIPEDA)
3. แนวทางของ Office of the Privacy Commissioner of Canada เกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลแก่หน่วยงานบังคับใช้กฎหมาย

เอกสารแนะนำเพิ่มเติม

Wilkins, R. G. (1987). Defining the reasonable expectation of privacy: an emerging tripartite analysis. Vand. L. Rev., 40, 1077.

Winn, P. (2009). Katz and the origins of the reasonable expectation of privacy test. McGeorge L. Rev., 40, 1.

Austin, L. M. (2015). Enough About Me: Why Privacy is About Power, Not Consent (or Harm). In A. Sarat (ed.), A World Without Privacy: What Law Can and Should Do? Cambridge University Press.

Bailey, J. (2018). Framed by Technology: Canadian Privacy Law Through the Lens of Predictive Analytics. Ottawa Law Review, 49(2), 311-350.

คำตัดสิน

ศาลฎีกาแคนาดาตัดสินว่า บุคคลมีการคาดหวังความเป็นส่วนตัวที่สมเหตุสมผลในข้อมูลผู้สมัครใช้บริการอินเทอร์เน็ต โดยการขอข้อมูลจากผู้ให้บริการอินเทอร์เน็ต (ISP) โดยไม่มีหมายศาลเป็นการค้นที่ไม่ชอบด้วยกฎหมาย เป็นการละเมิดกฎบัตรสิทธิและเสรีภาพแห่งแคนาดา (มาตรา 8) อย่างไรก็ตาม หลักฐานที่ได้มาไม่ถูกตัดออกจากการพิจารณาคดี เนื่องจากการยอมรับหลักฐานจะไม่ทำให้การดำเนินคดีเสียหาย

ในคดีนี้จะเห็นได้ว่า ข้อมูลผู้สมัครใช้บริการเชื่อมโยงกับข้อมูลส่วนบุคคลที่ละเอียดอ่อน รวมถึงกิจกรรมออนไลน์ของบุคคล เป็นข้อมูลส่วนบุคคลที่ได้รับการคุ้มครอง ดังนั้น การเปิดเผยข้อมูลนี้โดยไม่มีหมายศาล ถือเป็นการละเมิดความคาดหวังความเป็นส่วนตัวที่สมเหตุสมผล แม้กฎหมายจะอนุญาตให้ผู้ให้บริการอินเทอร์เน็ตเปิดเผยข้อมูลโดยสมัครใจ แต่ทั้งนี้กฎหมายไม่ได้อนุญาตให้ตำรวจขอข้อมูลโดยไม่มีหมายศาล ผลของคดีทำให้เกิดเกิดการเพิ่มการคุ้มครองความเป็นส่วนตัวของข้อมูลออนไลน์ในแคนาดา ทำให้เจ้าหน้าที่ต้องขอหมายศาลก่อนขอข้อมูลผู้สมัครใช้บริการจากผู้ให้บริการอินเทอร์เน็ต อีกทั้งยังส่งผลต่อวิธีการสืบสวนอาชญากรรมทางอินเทอร์เน็ตของเจ้าหน้าที่ และกระตุ้นให้มีการทบทวนกฎหมายและนโยบายเกี่ยวกับการเข้าถึงข้อมูลออนไลน์

คดีนี้สะท้อนการคุ้มครองความเป็นส่วนตัวทางดิจิทัลในแคนาดากับผู้บังคับใช้กฎหมาย โดยยอมรับว่าข้อมูลผู้สมัครใช้บริการอินเทอร์เน็ตมีความละเอียดอ่อน และควรได้รับการคุ้มครองภายใต้กฎหมาย คำตัดสินสะท้อนถึงการปรับตัวของระบบกฎหมายให้เข้ากับความท้าทายด้านความเป็นส่วนตัวในยุคดิจิทัล และเน้นย้ำความสำคัญของการสร้างสมดุลระหว่างการบังคับใช้กฎหมายกับสิทธิความเป็นส่วนตัวของพลเมือง นอกจากนี้ยังส่งผลกระทบต่อการปฏิบัติงานของเจ้าหน้าที่บังคับใช้กฎหมายและผู้ให้บริการอินเทอร์เน็ตในการจัดการกับข้อมูลส่วนบุคคลของผู้ใช้อินเทอร์เน็ต

กรณีศึกษาที่ 11:ลิงก์อันตราย

	ABC v Google กับความรับผิดจากการแชร์เนื้อหาหมิ่นประมาท
ศาล/เขตอำนาจ	ศาลสูงแห่งออสเตรเลีย
ปี	2019
การอ้างอิง	ABC v Google LLC (Australia, 2019) หมายเหตุ คดีนี้มักถูกอ้างอิงเป็น “ABC v Google LLC” แต่ชื่อที่ถูกต้องคือ Trkulja v Google LLC [2018] HCA 25

ภูมิหลัง

เครื่องมือค้นหาออนไลน์เป็นช่องทางหลักในการเข้าถึงข้อมูล แต่การทำงานอัตโนมัติของระบบเหล่านี้อาจนำไปสู่การเผยแพร่ข้อมูลที่ไม่ถูกต้องหรือเป็นการหมิ่นประมาท คดี Trkulja v. Google เป็นตัวอย่างที่แสดงให้เห็นถึงการปฏิรูปกฎหมายละเมิด และการกำหนดความรับผิดชอบของแพลตฟอร์มดิจิทัลต่อเนื้อหาที่ปรากฏในผลการค้นหา

สถานการณ์

Milorad Trkulja ฟ้อง Google ในข้อหาหมิ่นประมาท โดยอ้างว่าผลการค้นหาของ Google ได้เชื่อมโยงชื่อและรูปภาพของเขากับอาชญากรในเมลเบิร์น โดยโจทก์ (Trkulja) ได้กล่าวหา Google ว่าเป็นผู้เผยแพร่เนื้อหาจึงต้องรับผิดในข้อหาหมิ่นประมาทจากการแสดงผลการค้นหา เนื่องจากผลการค้นหาสร้างความเสียหายต่อชื่อเสียงของโจทก์

Google โต้แย้งว่า ตนเป็นเพียงตัวกลางที่แสดงผลการค้นหา ไม่ใช่ผู้เผยแพร่เนื้อหา โดยอ้างข้อยกเว้นเรื่องความรู้เท่าไม่ถึงการณ์ (Innocent dissemination) เนื่องจากไม่ทราบถึงลักษณะหมิ่นประมาทของเนื้อหา (ในบริบทของอินเทอร์เน็ตคือ mechanical distributor) Google ไม่สามารถตรวจสอบความถูกต้องของทุกเนื้อหาที่ปรากฏในผลการค้นหาได้ สิ่งที่ทำได้คือจัดให้มีกระบวนการรับแจ้งและนำเนื้อหาที่มีการละเมิดออกเมื่อได้รับแจ้งเท่านั้น

Google ยังอ้างถึงความสำคัญของการคุ้มครองเสรีภาพในการแสดงออกและการเข้าถึงข้อมูล โดยชี้ให้เห็นผลกระทบต่อการแสดงความคิดเห็นออนไลน์หากต้องรับผิดชอบทุกเนื้อหา การเรียกร้องกำหนดให้ตัวกลางแสดงผลการสืบค้นต้องรับผิดชอบต่อทุกการค้นหาเป็นภาระที่ไม่ได้สัดส่วน วิธีคิดเรื่องนี้ไม่ควรใช้มาตรฐานสื่อดั้งเดิมในการพิจารณาความรับผิดของเครื่องมือค้นหาอย่าง Google ยังได้อ้างประโยชน์สาธารณะในการเข้าถึงข้อมูล และขอให้ศาลพิจารณาโดยสร้างความสมดุลระหว่างการคุ้มครองชื่อเสียงและการส่งเสริมนวัตกรรม

คดีนี้ ศาลอุทธรณ์มีคำสั่งยกฟ้องศาลล่าง ประเด็นพิจารณาสำคัญมีดังนี้

1. ขอบเขตความรับผิดชอบของเครื่องมือค้นหาออนไลน์ต่อเนื้อหาที่ปรากฏในผลการค้นหา

2. การตีความกฎหมายหมิ่นประมาทในบริบทของเทคโนโลยีดิจิทัล

3. ความสมดุลระหว่างการคุ้มครองชื่อเสียงบุคคลและการส่งเสริมนวัตกรรมทางเทคโนโลยี

4. การอ้างหลัก “ความรู้เท่าไม่ถึงการณ์” ในกรณีของแพลตฟอร์มดิจิทัล

5. ความเหมาะสมของการใช้มาตรฐานสื่อดั้งเดิมกับสื่อดิจิทัล

6. ผลกระทบของการตัดสินคดีต่อเสรีภาพในการแสดงออกและการเข้าถึงข้อมูลออนไลน์

คำถามสำคัญสำหรับการวิเคราะห์

1. เครื่องมือค้นหาออนไลน์ควรถือว่าเป็น “ผู้เผยแพร่” เนื้อหาหรือเป็นเพียง “ตัวกลาง” ในทางกฎหมาย?

2. ควรมีการปรับปรุงกฎหมายหมิ่นประมาทอย่างไรเพื่อให้สอดคล้องกับความท้าทายในยุคดิจิทัล?

3. การอ้าง “ความรู้เท่าไม่ถึงการณ์” ควรมีขอบเขตอย่างไรสำหรับแพลตฟอร์มดิจิทัลที่ใช้ระบบอัตโนมัติ?

4. จะสร้างสมดุลระหว่างการคุ้มครองชื่อเสียงของบุคคลและการส่งเสริมนวัตกรรมทางเทคโนโลยีได้อย่างไร?

5. กระบวนการ “แจ้งและนำออก” (notice and takedown) เพียงพอที่จะคุ้มครองสิทธิของบุคคลที่ได้รับผลกระทบจากข้อมูลที่ไม่ถูกต้องหรือเป็นการหมิ่นประมาทหรือไม่?

6. การตัดสินคดีนี้จะส่งผลกระทบต่อการพัฒนาและการใช้งานเทคโนโลยีการค้นหาข้อมูลในอนาคตอย่างไร?

7. ควรมีมาตรฐานความรับผิดชอบที่แตกต่างกันระหว่างสื่อดั้งเดิมและแพลตฟอร์มดิจิทัลหรือไม่ อย่างไร?

8. การคุ้มครองเสรีภาพในการแสดงออกและการเข้าถึงข้อมูลควรมีขอบเขตอย่างไรในกรณีที่อาจมีการหมิ่นประมาทเกิดขึ้น?

9. หากท่านเป็นทนายความของ Google ท่านจะเสนอแนวทางอะไรในการจัดการผลการค้นหาที่อาจเป็นการหมิ่นประมาท โดยยังคงรักษาความเป็นกลางและประสิทธิภาพของเครื่องมือค้นหา?

คำแนะนำสำหรับทนายความ

เข้าใจแนวคิดการกำหนดความรับผิดของเครื่องมือค้นหาในกฎหมายหมิ่นประมาทของออสเตรเลีย ซึ่งนำไปสู่การทำความเข้าใจแนวคิดการปฏิรูปกฎหมายละเมิดของออสเตรเลีย กรณีความรับผิดของบุคคลที่สาม (สื่อใหม่) จากการเผยแพร่ข้อมูลที่กระทบต่อชื่อเสียงบุคคลบนแพลตฟอร์ม คดีลักษณะนี้มีความสัมพันธ์กับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในเรื่องหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลในการขอลบข้อมูลส่วนบุคคล และการดำเนินคดีหมิ่นประมาทออนไลน์ ซึ่งทนายความจำเป็นต้องจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลให้ชัดเจนแก่ลูกความ มีมุมมองการบริหารความเสี่ยงข้อมูล และแนวทางการประเมินความเสี่ยงด้านการหมิ่นประมาทสำหรับการแสดงผลการค้นหาโดยระบบอัตโนมัติ

กฎหมายที่เกี่ยวข้อง

1. Australian Defamation Act 2005 หรือพระราชบัญญัติหมิ่นประมาทออสเตรเลีย ค.ศ. 2005 เป็นกฎหมายหมิ่นประมาทของออสเตรเลียที่มีการปรับปรุงให้เป็นมาตรฐานเดียวกันทั่วประเทศ ครอบคลุมการหมิ่นประมาทโดยสื่อ ทั้งสื่อดั้งเดิมและสื่อออนไลน์ โดยแต่ละรัฐและเขตปกครองได้นำไปปรับใช้ กฎหมายฉบับนี้กำหนดองค์ประกอบของการหมิ่นประมาท ข้อต่อสู้ และการเยียวยา โดยมุ่งสร้างสมดุลระหว่างการคุ้มครองชื่อเสียงของบุคคลและเสรีภาพในการแสดงออก กฎหมายนี้มีผลกระทบสำคัญต่อสื่อมวลชนและการสื่อสารสาธารณะในออสเตรเลีย และได้รับการปรับปรุงเพื่อรองรับความท้าทายในยุคดิจิทัล

8. การคุ้มครองเสรีภาพในการแสดงออกและการเข้าถึงข้อมูลควรมีขอบเขตอย่างไรในกรณีที่อาจมีการหมิ่นประมาทเกิดขึ้น?

9. หากท่านเป็นทนายความของ Google ท่านจะเสนอแนวทางอะไรในการจัดการผลการค้นหาที่อาจเป็นการหมิ่นประมาท โดยยังคงรักษาความเป็นกลางและประสิทธิภาพของเครื่องมือค้นหา?

คำแนะนำสำหรับทนายความ

เข้าใจแนวคิดการกำหนดความรับผิดของเครื่องมือค้นหาในกฎหมายหมิ่นประมาทของออสเตรเลีย ซึ่งนำไปสู่การทำความเข้าใจแนวคิดการปฏิรูปกฎหมายละเมิดของออสเตรเลีย กรณีความรับผิดของบุคคลที่สาม (สื่อใหม่) จากการเผยแพร่ข้อมูลที่กระทบต่อชื่อเสียงบุคคลบนแพลตฟอร์ม คดีลักษณะนี้มีความสัมพันธ์กับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในเรื่องหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลในการขอลบข้อมูลส่วนบุคคล และการดำเนินคดีหมิ่นประมาทออนไลน์ ซึ่งทนายความจำเป็นต้องจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลให้ชัดเจนแก่ลูกความ มีมุมมองการบริหารความเสี่ยงข้อมูล และแนวทางการประเมินความเสี่ยงด้านการหมิ่นประมาทสำหรับการแสดงผลการค้นหาโดยระบบอัตโนมัติ

กฎหมายที่เกี่ยวข้อง

1. Australian Defamation Act 2005 หรือพระราชบัญญัติหมิ่นประมาทออสเตรเลีย ค.ศ. 2005 เป็นกฎหมายหมิ่นประมาทของออสเตรเลียที่มีการปรับปรุงให้เป็นมาตรฐานเดียวกันทั่วประเทศ ครอบคลุมการหมิ่นประมาทโดยสื่อ ทั้งสื่อดั้งเดิมและสื่อออนไลน์ โดยแต่ละรัฐและเขตปกครองได้นำไปปรับใช้ กฎหมายฉบับนี้กำหนดองค์ประกอบของการหมิ่นประมาท ข้อต่อสู้ และการเยียวยา โดยมุ่งสร้างสมดุลระหว่างการคุ้มครองชื่อเสียงของบุคคลและเสรีภาพในการแสดงออก กฎหมายนี้มีผลกระทบสำคัญต่อสื่อมวลชนและการสื่อสารสาธารณะในออสเตรเลีย และได้รับการปรับปรุงเพื่อรองรับความท้าทายในยุคดิจิทัล

2. Privacy Act 1988 หรือ หรือพระราชบัญญัติความเป็นส่วนตัว 1988 ของออสเตรเลีย เป็นกฎหมายหลักที่ควบคุมการจัดการข้อมูลส่วนบุคคลในประเทศ กฎหมายนี้กำหนดหลักการความเป็นส่วนตัวของออสเตรเลีย (Australian Privacy Principles - APPs) ซึ่งเป็นมาตรฐานในการเก็บรวบรวม ใช้ เปิดเผย และจัดการข้อมูลส่วนบุคคล ครอบคลุมทั้งหน่วยงานรัฐบาลและองค์กรเอกชนที่มีรายได้เกินเกณฑ์ที่กำหนด กฎหมายนี้ให้สิทธิแก่บุคคลในการเข้าถึงและแก้ไขข้อมูลของตน กำหนดหน้าที่ขององค์กรในการรักษาความปลอดภัยของข้อมูล และให้อำนาจแก่ Office of the Australian Information Commissioner (OAIC) ในการตรวจสอบและบังคับใช้กฎหมาย นอกจากนี้ยังมีบทบัญญัติเฉพาะเกี่ยวกับการรายงานการละเมิดข้อมูลและการคุ้มครองข้อมูลสุขภาพ ทำให้เป็นเครื่องมือสำคัญในการคุ้มครองความเป็นส่วนตัวของประชาชนออสเตรเลีย

3. กฎหมายทั้งสองฉบับของออสเตรเลียเป็นกฎหมายที่มีบทบาทสำคัญในการกำหนดกรอบทางกฎหมายสำหรับการสื่อสาร การคุ้มครองชื่อเสียง และความเป็นส่วนตัว โดยเฉพาะในบริบทของสื่อดิจิทัลและออนไลน์ในออสเตรเลีย

แหล่งข้อมูล

1. คำตัดสินของศาลสูงออสเตรเลียในคดี Trkulja v Google LLC [2018] HCA 25

2. Australian Defamation Act 2005

3. แนวทางของ Australian Competition and Consumer Commission เกี่ยวกับแพลตฟอร์มดิจิทัล

เอกสารแนะนำเพิ่มเติม

Kohl, U. (2017). Google: The Rise and Rise of Online Intermediaries in the Governance of the Internet and Beyond. International Journal of Law and In formation Technology, 25(2), 85-106.

Rolph, D. (2019). Publication, Innocent Dissemination and the Internet after Trkulja. Sydney Law Review, 41(4), 635-654.

Svantesson, D. J. B. (2020). Internet & Jurisdiction Global Status Report 2019. Internet & Jurisdiction Policy Network.

คำตัดสิน

ศาลสูงออสเตรเลียตัดสินว่า Google อาจมีความรับผิดในฐานะผู้เผยแพร่เนื้อหาที่หมิ่นประมาท คดีนี้ไม่ควรถูกยกฟ้องในขั้นตอนแรก และควรดำเนินการต่อไป โดยหากมีการพิจารณาคดีต่อ โจทก์ Trkulja มีโอกาสที่สมเหตุสมผลที่จะชนะคดี

ศาลให้เหตุผลทางกฎหมายโดยมองว่าเครื่องมือค้นหาสามารถถือเป็น “ผู้เผยแพร่” ตามกฎหมายหมิ่นประมาทได้ เมื่อมีการแสดงผลการค้นหาที่เชื่อมโยงบุคคลกับเนื้อหาที่อาจเป็นการหมิ่นประมาท ศาลเห็นว่าการยกฟ้องในขั้นตอนแรกควรทำเฉพาะในกรณีที่คดีไม่มีโอกาสชนะอย่างชัดเจน โดยต้องพิจารณาบริบททั้งหมดของผลการค้นหา ไม่ใช่เพียงลิงก์หรือข้อความสั้น ๆ เท่านั้น

ในบริบทของกฎหมายหมิ่นประมาทออสเตรเลีย ผลกระทบจากการตีความดังกล่าวได้เพิ่มความเสี่ยงทางกฎหมายสำหรับเครื่องมือค้นหาในออสเตรเลีย ส่งผลให้มีการฟ้องร้องคดีหมิ่นประมาทต่อเครื่องมือค้นหามากขึ้น ซึ่งกระตุ้นให้ผู้ให้บริการเครื่องมือค้นหาต้องระมัดระวังมากขึ้นในการจัดการกับคำร้องขอลบเนื้อหา อย่างไรก็ดี ในอีกแง่หนึ่ง ผลของคำพิพากษาส่งผลต่อการจำกัดการเข้าถึงข้อมูลในออสเตรเลีย คดีนี้ถือเป็นจุดเปลี่ยนสำคัญในการตีความกฎหมายหมิ่นประมาทในยุคดิจิทัลของออสเตรเลีย โดยเฉพาะในส่วนที่เกี่ยวข้องกับเครื่องมือค้นหาออนไลน์ โดยคำตัดสินแสดงให้เห็นถึงความท้าทายในการสร้างสมดุลระหว่างเสรีภาพในการแสดงออก และการคุ้มครองชื่อเสียงของบุคคลในโลกออนไลน์ นอกจากนี้ คดียังเน้นย้ำให้เห็นความซับซ้อนของการกำหนดความรับผิดชอบสำหรับเนื้อหาออนไลน์ โดยเฉพาะเมื่อเกี่ยวข้องกับระบบอัตโนมัติอย่างเครื่องมือค้นหา คดีนี้ได้ส่งผลกระทบต่อการพัฒนากฎหมายและนโยบายที่เกี่ยวข้องกับความรับผิดของแพลตฟอร์มดิจิทัลในอนาคตของออสเตรเลีย

กรณีศึกษาที่ 12:ลายนิ้วมือมีราคา

	ลายนิ้วมือมีราคา: Rooney และมูลค่าของข้อมูลชีวภาพ
ศาล/เขตอำนาจ	ศาลอุทธรณ์สหรัฐภาค 7
ปี	2019
การอ้างอิง	Rooney v Arcelor Mittal USA LLC (US, 2019) หมายเหตุ คดีนี้มักถูกอ้างอิงเป็น “Rooney v Arcelor Mittal USA LLC” คดีมีประเด็นคล้ายกันคือ Bryant v. Compass Group USA, Inc., 958 F.3d 617 (7th Cir. 2020)

ภูมิหลัง

พระราชบัญญัติความเป็นส่วนตัวของข้อมูลชีวภาพ (Biometric Information Privacy Act - BIPA) ของรัฐอิลลินอยส์เป็นกฎหมายที่มีจุดมุ่งหมายในการคุ้มครองข้อมูลชีวภาพของบุคคล เช่น ลายนิ้วมือ การสแกนม่านตา หรือการจดจำใบหน้า กฎหมายนี้กำหนดให้องค์กรต้องปฏิบัติตามข้อกำหนดเฉพาะในการเก็บ ใช้ และเก็บรักษาข้อมูลชีวภาพ คดีที่เกี่ยวข้องกับ BIPA แสดงให้เห็นถึงความท้าทายในการบังคับใช้กฎหมายนี้ในสภาพแวดล้อมที่เทคโนโลยีชีวภาพกำลังได้รับความนิยมมากขึ้น

สถานการณ์

คดีที่ 1: พนักงาน v. Arcelor Mittal USA LLC พนักงานของ Arcelor Mittal USA LLC เป็นโจทก์ยื่นฟ้องบริษัทภายใต้ BIPA โดยกล่าวหาว่าบริษัทเก็บและใช้ข้อมูลชีวภาพของพนักงาน และบริษัทไม่ปฏิบัติตามข้อกำหนดของ BIPA ในการเก็บและใช้ข้อมูลชีวภาพ

คดีที่ 2: Bryant v. Compass Group USA, Inc. นาย Bryant ยื่นฟ้องบริษัท Compass Group USA, Inc. โดยกล่าวหาว่าบริษัทติดตั้งเครื่องขายอาหารอัตโนมัติที่ใช้ลายนิ้วมือในการชำระเงิน โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรก่อนเก็บข้อมูลชีวภาพ อีกทั้ง บริษัทไม่เปิดเผยนโยบายการเก็บรักษาข้อมูล การกระทำดังกล่าวละเมิดกฎหมาย BIPA

ทั้งสองคดี มีประเด็นพิจารณาสำคัญ คือ ขอบเขตของความยินยอมในการเก็บและใช้ข้อมูลชีวภาพ ความรับผิดชอบขององค์กรในการเปิดเผยนโยบายการเก็บรักษาข้อมูลชีวภาพ ความแตกต่างระหว่างการใช้ข้อมูลชีวภาพในบริบทของการจ้างงานและการให้บริการ ผลกระทบของการละเมิด BIPA ต่อสิทธิความเป็นส่วนตัวของบุคคล และความท้าทายในการบังคับใช้ BIPA ในยุคที่เทคโนโลยีชีวภาพกำลังแพร่หลาย

คำถามสำคัญสำหรับการวิเคราะห์

1. การขอความยินยอมในการเก็บและใช้ข้อมูลชีวภาพควรมีลักษณะอย่างไรจึงจะถือว่าเพียงพอตามกฎหมาย BIPA?

2. บริษัทควรมีแนวปฏิบัติอย่างไรในการเปิดเผยนโยบายการเก็บรักษาข้อมูลชีวภาพให้สอดคล้องกับ BIPA?

3. มีความแตกต่างในการพิจารณาการละเมิด BIPA ระหว่างกรณีการจ้างงานและการให้บริการหรือไม่? อย่างไร?

4. ในกรณีที่มีการละเมิด BIPA การเยียวยาที่เหมาะสมควรมีลักษณะอย่างไร?

5. การละเมิดกฎหมายคุ้มครองข้อมูลชีวภาพ ควรถือเป็นความเสียหายที่เป็นรูปธรรมโดยไม่ต้องพิสูจน์ความเสียหายที่เกิดขึ้นจริงหรือไม่?

6. การให้ความรู้แก่ประชาชนเกี่ยวกับสิทธิตาม BIPA และความเสี่ยงของการใช้ข้อมูลชีวภาพควรทำอย่างไร ?

7. ในอนาคต เมื่อการใช้ข้อมูลชีวภาพกลายเป็นเรื่องปกติในชีวิตประจำวัน กฎหมายและนโยบายควรปรับตัวอย่างไรเพื่อสร้างสมดุลระหว่างนวัตกรรมและการคุ้มครองความเป็นส่วนตัว ?

คำแนะนำสำหรับทนายความ

ทำความเข้าใจแนวคิดการคุ้มครองข้อมูลส่วนบุคคลประเภทข้อมูลอ่อนไหว เช่น กรณีข้อมูลชีวภาพ ศึกษาแนวทางการตีความกฎหมายคุ้มครองความเป็นส่วนตัวของข้อมูลชีวภาพแห่งรัฐอิลลินอยส์ เปรียบเทียบกับเรื่องการคุ้มครองข้อมูลชีวภาพตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและประเทศอื่นๆ เพื่อใช้เป็นกรอบในการทำความเข้าใจกฎหมายไทยว่าด้วยการคุ้มครองข้อมูลสุขภาพ และข้อมูลชีวภาพพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ตลอดจนระเบียบกระทรวงสาธารณสุขเรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

คดีนี้เกิดขึ้นที่สหรัฐอเมริกา มีการยื่นฟ้องคดีแบบกลุ่มกับกรณีการละเมิดข้อมูลส่วนบุคคลประเภทอ่อนไหว ซึ่งในกรณีของประเทศไทยจะต้องพิจารณาข้อจำกัด แนวปฏิบัติ หรือการผลักดันแนวทางการใช้สิทธิการฟ้องคดีแบบกลุ่มในการละเมิดข้อมูลส่วนบุคคล

กฎหมายที่เกี่ยวข้อง

1. Illinois Biometric Information Privacy Act (BIPA) – 2008 หรือพระราชบัญญัติความเป็นส่วนตัวของข้อมูลชีวมิติแห่งรัฐอิลลินอยส์ (BIPA) ปี 2008 เป็นกฎหมายระดับรัฐฉบับแรกในสหรัฐอเมริกาที่ให้การคุ้มครองข้อมูลชีวภาพอย่างเข้มงวด กฎหมายนี้กำหนดให้องค์กรต้องได้รับความยินยอมเป็นลายลักษณ์อักษรก่อนเก็บรวบรวมหรือใช้ข้อมูลชีวภาพ เช่น ลายนิ้วมือ การสแกนม่านตา หรือการจดจำใบหน้า นอกจากนี้ยังกำหนดให้องค์กรต้องเปิดเผยวัตถุประสงค์และระยะเวลาในการเก็บข้อมูล รวมถึงมีนโยบายการทำลายข้อมูลที่ชัดเจน BIPA ให้สิทธิแก่บุคคลในการฟ้องร้ององค์กรที่ละเมิดกฎหมายนี้ โดยกำหนดค่าเสียหายที่สูง ส่งผลให้เกิดคดีฟ้องร้องจำนวนมากและมีอิทธิพลต่อการพัฒนากฎหมายคุ้มครองข้อมูลชีวมิติในรัฐอื่น ๆ และระดับประเทศ

2. มาตรา 3 แห่งรัฐธรรมนูญสหรัฐอเมริกา (Article III of the US Constitution – 1788) กำหนดอำนาจของฝ่ายตุลาการ โดยระบุเงื่อนไขในการฟ้องร้องคดีในสหรัฐอเมริกา รวมถึงหลักการ “standing” (สิทธิในการฟ้องคดี)

3. Federal Rules of Civil Procedure - 1938 หรือกฎหมายวิธีพิจารณาความแพ่งของศาล (มีการแก้ไขเพิ่มเติมหลายครั้ง) กำหนดกระบวนการและขั้นตอนในการดำเนินคดีแพ่งในศาลสหรัฐอเมริกา รวมถึงกฎเกณฑ์เกี่ยวกับการฟ้องคดีแบบกลุ่ม (class action)

แหล่งข้อมูล

1. คำตัดสินของศาลอุทธรณ์สหรัฐฯ ภาค 7 ในคดี Bryant v. Compass Group USA, Inc., 958 F.3d 617 (7th Cir. 2020)

2. Illinois Biometric Information Privacy Act (BIPA)

3. แนวทางของ Federal Trade Commission เกี่ยวกับการใช้ข้อมูลชีวภาพ

เอกสารแนะนำเพิ่มเติม

แสงระวี วิปุลาคม และสราวุธ ปิติยาศักดิ์. (2021). ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลประเภทข้อมูลชีวภาพ. วารสารสุโขทัยธรรมาธิราช, 34 (2), 36-59.

Kugler, M. B. (2018). From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms. UC Irvine Law Review, 10, 107-152.

Citron, D. K. (2019). A Poor Mother's Right to Privacy: A Review. Boston University Law Review, 98, 1139-1190.

คำตัดสิน

ศาลอุทธรณ์สหรัฐฯ ภาค 7 ได้ตัดสินว่า นาย Bryant มีสิทธิฟ้องคดีสำหรับการละเมิดข้อมูล กฎหมายคุ้มครองความเป็นส่วนตัวของข้อมูลชีวภาพแห่งรัฐอิลลินอยส์ โดยศาลให้เหตุผลว่าการไม่ให้ข้อมูลที่กำหนดโดยกฎหมาย BIPA ก่อนเก็บข้อมูลชีวภาพ ถือได้ว่าเป็นความเสียหายที่เป็นรูปธรรม เนื่องจากกฎหมาย BIPA ได้รับรองสิทธิตามกฎหมายในการควบคุมข้อมูลชีวภาพ และการละเมิดสิทธินี้เป็นมากกว่าเพียงการละเมิดกระบวนการ การไม่เปิดเผยนโยบายจึงถือเป็นความเสียหายต่อสาธารณะมากกว่าความเสียหายส่วนบุคคล

ผลกระทบจากคำพิพากษา ส่งผลให้เกิดการขยายขอบเขตการมีสิทธิฟ้องในคดีความเป็นส่วนตัวของข้อมูลชีวภาพ และเพิ่มความเสี่ยงทางกฎหมายสำหรับบริษัทที่มีการประมวลผลข้อมูลและใช้เทคโนโลยีชีวภาพ เกิดการกระตุ้นให้บริษัทต่าง ๆ ปฏิบัติตาม BIPA อย่างเคร่งครัด โดยเฉพาะในเรื่องการขอความยินยอม และนำไปสู่การฟ้องร้องคดีแบบกลุ่ม (class action) เพิ่มขึ้นภายใต้กฎหมาย BIPA

คดีนี้มีความสำคัญในแง่ของการตีความกฎหมายความเป็นส่วนตัวของข้อมูลชีวภาพในสหรัฐอเมริกา โดยเฉพาะในเรื่องของการมีสิทธิฟ้อง คำพิพากษาได้แสดงให้เห็นถึงแนวโน้มของศาลในการให้ความสำคัญกับสิทธิความเป็นส่วนตัวของข้อมูลชีวภาพ และการยอมรับว่าการละเมิดสิทธิเหล่านี้สามารถก่อให้เกิดความเสียหายที่เป็นรูปธรรมได้ แม้จะไม่มีความเสียหายทางการเงินที่ชัดเจนก็ตาม นอกจากนี้ยังส่งผลให้บริษัทต่าง ๆ ต้องให้ความสำคัญกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลชีวภาพ อย่างเคร่งครัดมากขึ้น เพื่อหลีกเลี่ยงความเสี่ยงทางกฎหมายที่อาจเกิดขึ้น

กรณีศึกษาที่ 13:ความปลอดภัยไซเบอร์ไม่ใช่ทางเลือก

	FTC ปะทะ Wyndham การกำกับดูแลความปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลผู้บริโภค
ศาล/เขตอำนาจ	คณะกรรมาธิการการค้าของรัฐบาลกลาง
ปี	2015
การอ้างอิง	FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015)

ภูมิหลัง

การรักษาความปลอดภัยของข้อมูลลูกค้าเป็นความท้าทายสำคัญสำหรับธุรกิจทุกประเภท คดี FTC v. Wyndham Worldwide Corp. เป็นตัวอย่างคดีที่เกิดขึ้นในสหรัฐอเมริกาโดยจะชี้ให้เห็นถึงความซับซ้อนของการกำกับดูแลความปลอดภัยทางไซเบอร์ และบทบาทของหน่วยงานรัฐในการคุ้มครองผู้บริโภค

สถานการณ์

บริษัท Wyndham Worldwide Corp. ดำเนินธุรกิจด้านการโรงแรมและการท่องเที่ยว ประสบเหตุการณ์ละเมิดข้อมูลสามครั้งระหว่างปี 2008-2009 โดยข้อมูลบัตรเครดิตของลูกค้ากว่า 619,000 รายถูกขโมยไป คณะกรรมาธิการการค้าของรัฐบาลกลาง (FTC) ได้ฟ้องร้องบริษัท Wyndham Worldwide Corp. โดยกล่าวหาว่า บริษัทมีการปฏิบัติทางการค้าที่ไม่เป็นธรรมและหลอกลวง และบริษัทไม่ได้ใช้มาตรการรักษาความปลอดภัยที่สมเหตุสมผล

บริษัทโต้แย้งข้อกล่าวหา โดยแย้งว่า FTC ไม่มีอำนาจในการกำกับดูแลการปฏิบัติด้านความปลอดภัยทางไซเบอร์ โดยมาตรา 5 ของกฎหมายว่าด้วยคณะกรรมาธิการการค้าของรัฐบาลกลางไม่ครอบคลุมถึงความปลอดภัยของข้อมูล อีกทั้ง กรณีของบริษัทไม่เข้าข่ายความหมาย “การค้าที่ไม่เป็นธรรม” ตามมาตรา 5 แต่อย่างใด ที่ผ่านมา บริษัทได้ดำเนินการตามมาตรฐานความปลอดภัยที่เป็นที่ยอมรับในอุตสาหกรรมแล้ว และได้มีความพยายามในการรักษาความปลอดภัยของข้อมูลมาโดยตลอด บริษัทยังให้เหตุผลว่า การโจมตีทางไซเบอร์ในปัจจุบันมีความซับซ้อนและความก้าวหน้ามากขึ้น แม้แต่องค์กรที่มีการรักษาความปลอดภัยที่ดีก็สามารถถูกโจมตีได้ บริษัทไม่ได้มีเจตนาที่จะสร้างความเสียหายแก่ผู้บริโภคแต่อย่างใด

ข้อโต้แย้งของบริษัทนำไปสู่ประเด็นพิจารณา ดังต่อไปนี้

1. ขอบเขตอำนาจของ FTC ในการกำกับดูแลความปลอดภัยทางไซเบอร์

2. การตีความ “การปฏิบัติที่ไม่เป็นธรรม” ในบริบทของความปลอดภัยข้อมูล

3. มาตรฐานความปลอดภัยที่เหมาะสมสำหรับการคุ้มครองข้อมูลผู้บริโภค

4. ความรับผิดชอบของบริษัทในกรณีที่เกิดการละเมิดข้อมูล

5. บทบาทของหน่วยงานรัฐในการส่งเสริมความปลอดภัยทางไซเบอร์

6. ความสมดุลระหว่างการส่งเสริมนวัตกรรมทางธุรกิจและการคุ้มครองผู้บริโภค

คำถามสำคัญสำหรับการวิเคราะห์

1. FTC ควรมีอำนาจในการกำกับดูแลการปฏิบัติด้านความปลอดภัยทางไซเบอร์ของบริษัทเอกชนหรือไม่ ภายใต้เงื่อนไขใด?

2. อะไรคือมาตรฐานในการพิจารณาว่าบริษัทได้ใช้มาตรการรักษาความปลอดภัยที่ “เหมาะสม” แล้ว?

3. การเกิดเหตุละเมิดข้อมูลซ้ำ ๆ ควรถือเป็นหลักฐานของการละเลยด้านความปลอดภัยหรือไม่? หรือเป็นเพียงผลของภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้น?

4. บริษัทควรมีหน้าที่ในการเปิดเผยข้อมูลเกี่ยวกับการละเมิดความปลอดภัยแก่ผู้บริโภคและหน่วยงานกำกับดูแลอย่างไร?

5. เหตุผลทางกฎหมายอะไรที่ใช้ในการสนับสนุนว่า “การไม่มีมาตรการรักษาความปลอดภัยข้อมูลที่เหมาะสม คือ การปฏิบัติที่ไม่เป็นธรรมต่อผู้บริโภค”

6. การลงโทษที่เหมาะสมสำหรับบริษัทที่ละเลยการรักษาความปลอดภัยของข้อมูลลูกค้าควรเป็นอย่างไร?

7. หากท่านเป็นที่ปรึกษากฎหมายให้กับบริษัท หรือโรงแรม ท่านจะเสนอแนวทางปฏิบัติด้านความปลอดภัยทางไซเบอร์อย่างไร โดยยังคงคำนึงถึงความเป็นไปได้ในทางปฏิบัติและต้นทุน ?

คำแนะนำสำหรับทนายความ

ทำความเข้าใจแนวคิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล นอกเหนือจากมุมการคุ้มครองสิทธิของเจ้าของข้อมูล คือมุมความมั่นคงปลอดภัยข้อมูล (Data security) โดยเฉพาะแนวคิดความมั่นคงปลอดภัยไซเบอร์ ในส่วนที่เกี่ยวข้องกับกฎหมายไทย ควรทำความเข้าใจพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)

ในส่วนที่เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ให้พิจารณาทำความเข้าใจประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 โดยเฉพาะอย่างยิ่ง นิยาม “ความมั่นคงปลอดภัย ที่หมายรวมแนวคิดการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ และรายละเอียดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ที่กฎหมายกำหนดไว้เป็นการเฉพาะ (มาตรา 4) เช่น การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมทั้งมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ตลอดจนมาตรการทางกายภาพ (physical measures) ที่จำเป็น โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เป็นต้น

กฎหมายที่เกี่ยวข้อง

1. Federal Trade Commission Act 1914 (FTC Act) หรือกฎหมายว่าด้วยคณะกรรมาธิการการค้าของรัฐบาลกลาง มาตรา 5 ของสหรัฐอเมริกา เป็นกฎหมายพื้นฐานสำคัญในการคุ้มครองผู้บริโภคของสหรัฐอเมริกา โดยห้ามการปฏิบัติทางการค้าที่ไม่เป็นธรรมหรือหลอกลวง และให้อำนาจแก่คณะกรรมาธิการการค้าของรัฐบาลกลาง (FTC) ในการบังคับใช้กฎหมาย FTC มีบทบาทสำคัญในการตรวจสอบและดำเนินการกับธุรกิจที่ละเมิดกฎหมายนี้ ทำให้เกิดสภาพแวดล้อมทางการค้าที่เป็นธรรมและโปร่งใสมากขึ้นสำหรับผู้บริโภค

2. Gramm-Leach-Bliley Act – 1999 กฎหมายฉบับนี้มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าในภาคการเงิน โดยกำหนดให้สถาบันการเงินต้องมีมาตรการคุ้มครองข้อมูลของลูกค้า พัฒนานโยบายความเป็นส่วนตัว และแจ้งให้ลูกค้าทราบเกี่ยวกับวิธีการจัดการข้อมูลของพวกเขา กฎหมายนี้เป็นการตอบสนองต่อความกังวลที่เพิ่มขึ้นเกี่ยวกับความเป็นส่วนตัวของข้อมูลในยุคดิจิทัล และช่วยสร้างความไว้วางใจระหว่างสถาบันการเงินและลูกค้า

3. Fair Credit Reporting Act 1970 หรือกฎหมายว่าด้วยการรายงานเครดิตที่เป็นธรรม กฎหมายนี้เป็นกฎหมายควบคุมการใช้และการเผยแพร่ข้อมูลเครดิตของผู้บริโภค โดยให้สิทธิแก่ผู้บริโภคในการเข้าถึงและแก้ไขข้อมูลเครดิตของตนเอง นอกจากนี้ยังกำหนดมาตรฐานสำหรับความถูกต้องและความเป็นส่วนตัวของข้อมูลเครดิต กฎหมายนี้มีความสำคัญอย่างยิ่งในการป้องกันการใช้ข้อมูลเครดิตอย่างไม่เป็นธรรมและช่วยให้ผู้บริโภคสามารถตรวจสอบและรักษาสถานะทางการเงินของตนได้อย่างมีประสิทธิภาพ

แหล่งข้อมูล

1. คำตัดสินของศาลอุทธรณ์สหรัฐฯ ภาค 3 ในคดี FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015)

2. กฎหมายว่าด้วยคณะกรรมาธิการการค้าของรัฐบาลกลาง

3. แนวทางปฏิบัติด้านความปลอดภัยของข้อมูลจาก FTC

เอกสารแนะนำเพิ่มเติม

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

Stegmaier, M., & Bartnick, W. (2013). Physics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements. George Mason Law Review, 20(3), 673-720.

Hartzog, W., & Solove, D. J. (2015). The Scope and Potential of FTC Data Protection. George Washington Law Review, 83(6), 2230-2300.McGeveran, W. (2019). The Duty of Data Security. Minnesota Law Review, 103, 1135-1210.

คำตัดสิน

ศาลอุทธรณ์สหรัฐฯ ภาค 3 ตัดสินว่า คณะกรรมาธิการการค้าของรัฐบาลกลางมีอำนาจในการควบคุมดูแลการปฏิบัติด้านความปลอดภัยทางไซเบอร์ภายใต้ มาตรา 5 ตามกฎหมายคณะกรรมาธิการการค้าของรัฐบาลกลาง โดยศาลให้เหตุผลว่า การปฏิบัติด้านความปลอดภัยที่ไม่เพียงพอ ถือเป็น “การปฏิบัติที่ไม่เป็นธรรม” แล้ว โดยศาลเห็นว่า บริษัท Wyndham ได้รับการแจ้งเตือนอย่างเพียงพอแล้วว่าการปฏิบัติของบริษัทอาจละเมิดกฎหมายของ FTC ได้ เหตุผลทางกฎหมายในคดีนี้เริ่มจากกฎหมายคณะกรรมาธิการการค้าของรัฐบาลกลาง ให้อำนาจ FTC ในการป้องกัน “การปฏิบัติที่ไม่เป็นธรรม” ซึ่งรวมถึงการปฏิบัติที่ก่อให้เกิดความเสียหายต่อผู้บริโภค ดังนั้น การละเมิดข้อมูลที่เกิดจากการรักษาความปลอดภัยที่ไม่เพียงพอสามารถก่อให้เกิดความเสียหายที่สำคัญต่อผู้บริโภค และถือเป็นการปฏิบัติที่ไม่เป็นธรรมได้

คดีนี้เน้นย้ำบทบาทของ FTC ในการควบคุมดูแลความปลอดภัยทางไซเบอร์ในสหรัฐอเมริกา โดยยืนยันว่า FTC มีอำนาจในการดำเนินการกับบริษัทที่ไม่คุ้มครองครองข้อมูลลูกค้าอย่างเพียงพอ ซึ่งเป็นการเสริมสร้างกลไกการคุ้มครองผู้บริโภคในยุคดิจิทัล คำตัดสินแสดงให้เห็นถึงความคาดหวังที่สูงขึ้นในเรื่องการรักษาความปลอดภัยทางไซเบอร์ของภาคธุรกิจ และกระตุ้นให้บริษัทต่างๆ ให้ความสำคัญกับการลงทุนในระบบรักษาความปลอดภัย และการปฏิบัติตามแนวทางที่ FTC กำหนด

ตารางสรุปสาระสำคัญของกรณีศึกษา

ชื่อคดี	ความสำคัญของคดี	ประเด็นสำคัญ
1. Schrems I	การตรวจสอบกลไกการโอนข้อมูลระหว่างประเทศ	การยกเลิกข้อตกลง Safe Harbor ระหว่างสหภาพยุโรปและสหรัฐอเมริกา
2. Schrems II	การโอนข้อมูลส่วนบุคคลไปยังสหรัฐอเมริกา กับข้อสัญญามาตรฐาน (Standard Contractual Clauses – SCCs) และการกำหนดมาตรการป้องกันเพิ่มเติม	การยกเลิก EU-US Privacy Shield
3. Google Spain v AEPD	ขอบเขตการตีความสิทธิที่จะถูกลืม	การใช้เครื่องมือช่วยสืบค้น (search engine) กับคำขอใช้สิทธิลบข้อมูลของเจ้าของข้อมูล
4. Google LLC v CNIL	ขอบเขตทางภูมิศาสตร์ของสิทธิที่จะถูกลืม	ข้อจำกัดการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลนอกสหภาพยุโรป

ชื่อคดี	ความสำคัญของคดี	ประเด็นสำคัญ
5. Vidal-Hall v Google Inc	ความเสียหายที่ไม่ใช่วัตถุเป็นเหตุผลในการเรียกร้องค่าชดเชยในคดีละเมิดข้อมูลได้	การฟ้องเรียกร้องค่าเสียหายทางจิตใจโดยไม่ต้องมีความเสียหายที่เป็นตัวเงิน
6. Campbell v MGN Ltd	พัฒนาการคดีละเมิดว่าด้วยการใช้ข้อมูลส่วนตัวในทางที่ผิด	การสร้างสมดุลระหว่างสิทธิความเป็นส่วนตัวกับเสรีภาพในการแสดงออกและเสรีภาพสื่อ
7. Equifax Data Breach Settlement	การชดใช้ค่าเสียหายคดีละเมิดข้อมูลที่ใหญ่ที่สุดในประวัติศาสตร์	การกำหนดมาตรการความปลอดภัยทางไซเบอร์แก่ลูกค้า
8. FTC v Facebook	ค่าปรับ 5 พันล้านดอลลาร์จากการละเมิดความเป็นส่วนตัว	คำแนะนำเกี่ยวกับการตั้งค่าโปรแกรมความเป็นส่วนตัวและการปฏิบัติตามกฎระเบียบ
9. Bărbulescu v Romania	ความสมดุลระหว่างผลประโยชน์ของนายจ้างกับสิทธิความเป็นส่วนตัวของพนักงาน	ความเป็นส่วนตัวของพนักงานในสถานที่ทำงาน

ชื่อคดี	ความสำคัญของคดี	ประเด็นสำคัญ
10. R v Spencer	ความคาดหวังที่สมเหตุสมผลของความเป็นส่วนตัว	ความเป็นส่วนตัวในข้อมูลของผู้สมัครใช้บริการ ISP
11. ABC v Google LLC	ความรับผิดที่อาจเกิดขึ้นจากการแชร์และเชื่อมโยงเนื้อหา	ความรับผิดจากกรณีการเชื่อมโยงลิงก์ไปยังเนื้อหาที่เป็นการหมิ่นประมาท
12. Rooney v ArcelorMittal USA LLC	ความเสียหายจากการละเมิดข้อมูลชีวภาพ ไม่จำเป็นต้องมีความเสียหายที่เป็นรูปธรรมตาม BIPA	สิทธิฟ้องคดีความเป็นส่วนตัว กรณีข้อมูลอ่อนไหวประเภทข้อมูลชีวภาพ
13. FTC v Wyndham Worldwide Corp.	มาตรการความปลอดภัยทางไซเบอร์ที่ไม่เหมาะสมในฐานะการปฏิบัติที่ไม่เป็นธรรม	FTC กับการบังคับใช้มาตรการรักษาความปลอดภัยที่สมเหตุสมผล

จดบันทึก

จดบันทึก

จดบันทึก

จดบันทึก

จดบันทึก

จดบันทึก

จดบันทึก

โดย สมาคมนักกฎหมายสิทธิมนุษยชน
ร่วมกับ เนติบัณฑิตยสภาแห่งสหรัฐอเมริกา