บทที่ 1

บทนำ

1.1. ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้กับการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลายนั้น อาจถูกแทรกแซงลบกวนความเป็นส่วนตัวของผู้ใช้บริการที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ได้ เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐานที่สำคัญตามรัฐธรรมนูญในความเป็นส่วนตัว (Right to privacy) ของประชาชนที่ได้รับการคุ้มครองตามมาตร 36 บุคคลย่อมมีเสรีภาพในการติดต่อสื่อสารถึงกันไม่ว่าในทางใด ๆ การตรวจ การกัก หรือการเปิดเผยข้อมูลที่บุคคลสื่อสารถึงกัน รวมทั้งการกระทำด้วยประการใด ๆ เพื่อให้ล่วงรู้ หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันจะกระทำมิได้ เว้นแต่จะมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ ดังนั้น บุคคลย่อมมีสิทธิได้รับการคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตนตามบทบัญญัติของกฎหมาย[1] อันทำให้ประชาชนมีความเชื่อมั่นเนื่องจากมีการพัฒนาทางเทคโนโลยีทำให้ผู้ประกอบกิจการพาณิชย์อิเล็กทรอนิกส์ทั้งหลายสามารถเก็บรวบรวมข้อมูลส่วนบุคคลไว้ในฐานข้อมูล และอาจเฝ้าติดตามพฤติกรรมในการใช้บริการในเว็บไซต์ โดยที่ผู้ใช้บริการก็ไม่อาจทราบ

จากปัญหาดังกล่าว การนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้ขอความยินยอม หรือแม้ว่าจะให้ความยินยม แต่อาจนำไปใช้เกินขอบเขตที่ให้ความยินยอมไว้ อาจส่งผลกระทบโดยตรงต่อสิทธิส่วนบุคคลของผู้บริโภคและขาดความเชื่อมั่นในการทำธุรกรรมผ่านทางระบบอิเล็กทรอนิกส์ อาจส่งผลกระทบอย่างต่อเนื่องในภาคธุรกิจอิเล็กทรอนิกส์ภายในประเทศไม่เติบโตเท่าที่ควร ด้วยเหตุนี้ ผู้ประกอบกิจการทางพาณิชย์อิเล็กทรอนิกส์จำเป็นจะต้องทำให้เกิดความเชื่อมั่นในเรื่องการให้ความคุ้มครองความเป็นส่วนตัวข้อมูลส่วนบุคคล โดยวิธีการผ่านระบบอิเล็กทรอนิกส์สามารถดำเนินการได้ กล่าวคือ การขอความยินยอม การจัดทำนโยบายความเป็นส่วนตัวเป็นลายลักษณ์อักษรชัดเจน ให้เจ้าของข้อมูลสามารถเข้าถึง หรือแก้ไขเปลี่ยนแปลง หากข้อมูลดังกล่าวไม่ถูกต้องครบถ้วนหรือไม่เป็นปัจจุบัน รวมทั้งทำลายข้อมูลส่วนบุคคลเมื่อหมดวัตถุประสงค์ หรือสิทธิที่จะถูกลืม

---

[1] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560. มาตรา 36.

(Right to be forgotten) เช่น คดี Google Spain[2] ประเด็นโจทก์ทำการขายทรัพย์สินเพื่อชำระหนี้ ถูกบันทึกในไม่กี่บรรทัดในหนังสือพิมพ์ท้องถิ่น และได้ทำการจัดเก็บระบบข้อมูลไว้ในระบบออนไลน์ แต่เมื่อใส่คำค้นหาเป็นชื่อของโจทก์ลงใน Google Search กลับปรากฏว่าลิงค์ถูกเชื่อมโยงไปยังข้อมูลในหนังสือพิมพ์ฉบับดังกล่าวถูกบันทึกไว้เป็นเวลา 16 ปี โดยศาลยุติธรรมของสหภาพยุโรปมีคำสั่งให้ Google ลบข้อมูลส่วนตัวของโจทก์ออกจากระบบการค้นหา โดยจำเลยสามารถทำการลบลิงค์ออกจากฐานระบบอินเทอร์เน็ตของจำเลยได้ เพื่อให้ข้อมูลของโจทก์ถูกลืมจากระบบในไม่ช้า ศาลได้ชี้แจงว่าผู้บริโภคสมควรได้รับสิทธิ์ที่เรียกว่า “สิทธิที่จะถูกลืม” จึงควรต้องตระหนักถึงความเป็นส่วนตัว (Privacy policy)

เมื่อเปรียบเทียบกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พุทธศักราช 2540 โดยให้ความคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานรัฐเท่านั้นที่ได้รับการคุ้มครอง แต่มิได้ให้ความคุ้มครองข้อมูลข่าวสารที่อยู่ในหน่วยงานเอกชน หรือของบุคคลไว้แต่อย่างไร ซึ่งความสัมพันธ์ระหว่างสิทธิส่วนความเป็นส่วนตัวและเสรีภาพในการเคลื่อนไหวข้อมูลข่าวสารต่าง ๆ ต้องเป็นไปในทิศทางเดียว เพื่อมิให้เกิดการละเมิดสิทธิความเป็นอยู่ส่วนตัวและข้อมูลส่วนบุคคล อันตั้งอยู่บนพื้นฐานความสัมพันธ์ระหว่างปัจเจกชน (Individual) กับสังคมส่วนรวม

โดยสหภาพยุโรปในปี 2018 ได้ออกหลักเกณฑ์ Regulation (EU) 2018/1725 หรือ “จีดีพีอาร์” (GDPR) ใหม่ โดยมีการประกาศใช้กฎหมาย (General data protection regulation: GDPR) หรือ “กลไกการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป” หรือ “กฎหมายคุ้มครองข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรป” ในการประมวลผลข้อมูลส่วนบุคคลและการโอนข้อมูลโดยคำนึงถึงสนธิสัญญาการจัดตั้งประชาคมสหภาพยุโรปของประเทศสมาชิกขึ้น[3] ซึ่งปัจจุบันการทำนิติกรรมทางพาณิชย์จะต้องมีการติดต่อระหว่างประเทศ โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Data protection directive) ของเดิมที่มีการบังคับใช้มาตั้งแต่ปี 1995 เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค โดยเฉพาะในธุรกิจบริการทางอินเทอร์เน็ต[4] สิทธิของบุคคลใดบุคคลหนึ่งที่

---

[2] Homo Digitalis. (2018). ***The case Google Spain v AEPD and Mario Costeja Gonzalez of the Court of Justice of the European Union: A brief critical analysis***. (ออนไลน์).เข้าถึงได้จาก: https://www.homodigitalis.gr/en/posts/2900. [2562, 21 ธันวาคม]

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1), and in particular Article 25(6) thereof,

[4] ข่าวคมชัดลึก. (2561). ***จุดอันตราย “ไทย- ยุโรป” ธุรกิจข้อมูลส่วนบุคคล***. (ออนไลน์). เข้าถึงได้จาก: http://www.komchadluek.net/news/scoop/331794. [2562,15 กรกฎาคม].

จะทำการใด ๆ ได้ โดยปราศจากการแทรกแซงจากภายนอก รวมทั้งการปลอดจากการสอดส่องเฝ้ามองจากสังคม หรือบุคคลอื่น สิทธิในความเป็นส่วนตัวยังรวมถึงสิทธิที่จะมีความลับ (Secret) ในการดำเนินชีวิตของบุคคลนั้น หรือถูกเผยแพร่ความรู้ที่ได้จากข้อมูลส่วนบุคคลนั้น

เมื่อสิทธิความเป็นส่วนตัว (Right to privacy) แบ่งเป็นด้านลบ (Negative right) และรวมถึงด้านบวก (Positive right) จากสิทธิมนุษยชนมักจะเริ่มจากสิทธิด้านลบ (Negative right) จะมาก่อน กล่าวคือ การไม่ถูกแทรกแซงจากอำนาจที่เหนือกว่า หรือไม่ถูกแทรกแซงจากอำนาจรัฐ ก็คือ สิทธิที่จะอยู่คนเดียว (Right to be let alone)[5] หรือขอมีชีวิตเป็นส่วนตัว และในความเป็นส่วนตัวนี้เป็นสิทธิที่ได้รับการรับรองมาตั้งแต่สงครามโลกครั้งที่ 2 คือ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights)[6] ซึ่งถูกรับรองต่อ ๆ ไปในสนธิสัญญาตามกฎหมายระหว่างประเทศต่าง ๆ ส่วนสิทธิด้านบวก (Positive right) สิทธิในการควบคุมการไหลเวียนของข้อมูลของตน โดยบุคคลอื่นมีหน้าที่จะต้องดำเนินการลบการกระทำนั้น ๆ ไม่ใช่การกระทำซึ่งเจ้าของข้อมูลส่วนบุคคลสามารถควบคุมแก้ไขข้อมูลของตน หากไม่ถูกต้องและไม่เป็นปัจจุบัน[7]

สหรัฐอเมริกาได้ประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ (Biometric Information Privacy Act 2008: BIPA)ในสามมลรัฐแรกแก่ข้อมูลไบโอเมตริกซ์ เช่น ลายนิ้วมือ ม่านตาใบหน้า เพื่อจัดการกับกระบวนการเข้า – ออกและการตอกบัตรแทนที่จะใช้บัตรประจำตัวของพนักงานแบบเดิม ๆ โดยบัญญัติคำนิยามศัพท์ “ข้อมูลที่มีความอ่อนไหว” (Biometrics information) และจำแนกประเภทออกจากข้อมูลส่วนบุคคลทั่วไปที่ต้องขอความยินก่อน เช่น

กรณีคดี Rosenbach v. Six Flags Entertainment Corporation[8] และคดี Facebook[9] โดยได้มีการรวบรวมลายนิ้วมือของผู้เยาว์โดยไม่แจ้งล่วงหน้าเป็นลายลักษณ์อักษรให้โจทก์ทราบและไม่ได้รับความยินยอมจากเจ้าของข้อมูลเป็นลายลักษณ์อักษรล่วงหน้า ด้วยเหตุละเมิดเช่นนี้เพียงแค่แสดงให้ศาลเห็นว่า “อาจได้รับผบกระทบ” ก็เป็นการเพียงพอที่จะนำมาฟ้องขึ้นสู่ศาล แม้ว่าบุคคลนั้น

---

[5] ไทยพับลิก้า สามัญดิจิทัล. (2015). ***กฎหมายกับความเป็นส่วนตัวในโลกดิจิทัล*** (ออนไลน์). เข้าถึงได้จาก: https://thaipublica.org/2015/10/big-data-4/. [2562,15 กรกฎาคม].

[6] Draft Committee. (2491). ***ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน***. (ออนไลน์). เข้าถึงได้จาก: http://unicode.org/udhr/d/udhr_tha.html. [2562,15 กรกฎาคม].

[7] Gregory Norton. (2019). ***What are positive rights and negative rights?*** (ออนไลน์). เข้าถึงได้จาก: https://www.quora.com/What-are-positive-rights-and-negative-rights. [2562,15 กรกฎาคม].

[8] Illinois Official Reports Supreme Court. (2019). ***Rosebush v. Six Flags Entertainment Corp., 2019 IL 123186.*** pp. 3-5

[9] Court of Justice of the European Union. (2019). Judgment in Case C-40/17Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV. pp. 1-2

จะไม่ได้รับอันตราย หรือผลกระทบที่ร้ายแรงจากการละเมิดนั้นก็ตาม อันเป็นสิทธิภายใต้บทบัญญัติ (BIPA)

สหพันธ์สาธารณรัฐเยอรมนี (Bundesdatenschutzgesetz : BDSG) ได้มีการยกเลิกกฎหมายฉบับก่อนเพื่อให้สอดคล้องกับการป้องกันข้อมูลทั่วไปของสหภาพยุโรป (GDPR) ใหม่ โดยให้การคุ้มครองข้อมูลไบโอเมตริกซ์อย่างเข้มงวด สำหรับข้อมูลที่มีความละเอียดอ่อนเป็นข้อมูลลับเฉพาะของบุคคลนั้น ในการเก็บ รวบรวม เปิดเผย ใช้ หรือทำลายที่ต้องได้รับความยินยอนก่อน โดยเฉพาะอย่างยิ่งระยะเวลาในการเก็บรักษาข้อมูลจะต้องเป็นไปตามหลัก (Right to be forgotten) หากไม่มีการแจ้งระยะเวลาเก็บข้อมูลส่วนบุคคลผู้ควบคุมจะต้องคำนึงถึงภายในระยะเวลาที่เหมาะสม แต่ไม่เกิน 2 สัปดาห์ ประการสำคัญบทบัญญัติของ (BDSG) จะต้องไม่ขัดกับกฎหมายของสหภาพยุโรป

สาธารณรัฐสิงคโปร์ (Personal Data Protection Act 2012: PDPA) โดยวางหลักไว้ว่า ข้อมูลใดก็ตามที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคลที่สามารถเชื่อมโยงถึงสิ่งบ่งบอกลักษณะอื่นใดที่ทำให้รู้ตัวผู้นั้นได้ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้อง ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลทราบเสียก่อน เจ้าของข้อมูลมีสิทธิในการเข้าถึงข้อมูลของตนและกำหนดให้องค์กรต่าง ๆ หรือผู้ควบคุมข้อมูลส่วนบุคคลต้องแก้ไขข้อมูลส่วนบุคคลโดยเร็วเท่าที่จะสามารถกระทำได้ และส่งการแก้ไขข้อมูลส่วนบุคคลนั้นให้เจ้าของข้อมูลนั้นทราบ แต่มิได้บัญญัติการคุ้มครองข้อมูลไบโอเมตริกซ์ไว้แต่อย่างใด

ปัญหาดังกล่าวนี้ อาจทวีความรุนแรงมากขึ้น โดยบุคคลที่อยู่ในข่ายอาจถูกละเมิดสิทธิจะมีวิธีปกป้องสิทธิของตนอย่างไรกับกระบวนการ “จัดเก็บข้อมูล” ไม่ว่าจะผ่านการพิมพ์ออกมาเก็บใส่แฟ้มแบบสมัยก่อน หรือการรวบรวมข้อมูลในจำนวนมหาศาล (Big data) ไว้ในระบบฐานข้อมูลออนไลน์ ซึ่งข้อมูลส่วนบุคคลเหล่านั้นมีทั้งข้อมูลทั่วไปและข้อมูลไบโอเมตริกซ์ที่สามารถเรียกใช้ได้ง่ายไม่ว่าจะผ่านฮาร์ดแวร์ ซอฟต์แวร์ หรือระบบคลาวด์ แม้ว่าปัจจุบันจะได้ประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 แล้วก็ตาม แต่เนื่องจากปัญหาทางกฎหมายบางประการในให้ความคุ้มครองความเป็นส่วนตัวของข้อมูลไบโอเมตริกซ์และการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัติฉบับนี้ จะต้องคำนึงถึงความก้าวหน้าทางเทคโนโลยีที่สามารถเชื่อมโยงข้อมูลส่วนบุคคลหลายชุดเข้าด้วยกัน เพื่อป้องกันความเสี่ยงในการละเมิดสิทธิในความเป็นส่วนตัวของข้อมูลบุคคลที่ถูกบันทึกไว้ในฐานระบบออนไลน์ ควรถูกจดจำในระบบออนไลน์น้อยที่สุดและมีสิทธิที่จะถูกลืม (Right to be forgotten) ผู้วิจัยจึงได้ศึกษามาตรการทางกฎหมายเกี่ยวกับความเป็นส่วนตัวของข้อมูลไบโอเมตริกซ์ของต่างประเทศต่อไป

1.2 วัตถุประสงค์ของการวิจัย

1.2.1. เพื่อศึกษาแนวความคิดกับทฤษฎีเกี่ยวกับกับมาตรการคุ้มครองความเป็นส่วนตัวในข้อมูลไบโอเมตริกซ์ภายใต้กฎหมายไทย

1.2.2. เพื่อศึกษาเกี่ยวกับความยินและการถอนความยินยอมในการใช้ข้อมูลไบโอเมตริกซ์ (Biometrics)

1.2.3. เพื่อศึกษาเกี่ยวกับมาตรการในการบังคับใช้กฎหมายโดยเฉพาะอย่างยิ่งระยะเวลาในการเก็บรักษาข้อมูลที่เป็นไปตามหลักสิทธิที่จะถูกลืม (Right to be forgotten)

1.2.4. เพื่อศึกษาหาแนวทางในการแก้ไขปัญหาความเป็นส่วนตัวในข้อมูลไบโอเมตริกซ์ (Biometrics)

1.3 สมมติฐานของการวิจัย

การศึกษาของวิทยานิพนธ์ฉบับนี้ ตั้งอยู่บนสมมติฐานอันเกี่ยวกับมาตรการเพื่อความมั่นคงปลอดภัยในการคุ้มครองข้อมูลส่วนบุคคล การเก็บ รวบรวม เปิดเผย ใช้ หรือ ทำลายข้อมูลไบโอเมตริกซ์ ดังนั้น ข้อยกเว้นในการเผยแพร่ข้อมูลไบโอเมตริกซ์ โดยการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัติ พุทธศักราช 2562 จึงต้องคำนึงถึงความเสี่ยงในการเข้าถึงข้อมูลไบโอเมตริกซ์ได้มีมาตรการป้องกันและการทำลายข้อมูลเมื่อหมดวัตถุประสงค์เพื่อมิให้เข้าถึงข้อมูลส่วนบุคคลภายหลังการลบข้อมูล หรือสิทธิที่จะถูกลืม (Right to be forgotten) รวมทั้งฐานระบบของเทคโนโลยีในปัจจุบันและอนาคต

1.4 ขอบเขตของการศึกษา

ศึกษาวิจัยเกี่ยวกับปัญหาและมาตรการคุ้มครองความเป็นส่วนตัวในข้อมูลไบโอเมตริกซ์ (Biometrics) โดยศึกษาวิเคราะห์มาตรการทางกฎหมายของสหภาพยุโรป สหรัฐอเมริกา สหพันธ์สาธารณรัฐเยอรมนี สาธารณรัฐสิงคโปร์และกฎหมายภายของประเทศไทย ได้แก่ รัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2560 ประมวลกฎหมายแพ่งและพาณิชย์พุทธศักราช 2561 ประมวลกฎหมายอาญา พระราชบัญญัติข้อมูลข่าวสาร พุทธศักราช 2540 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พุทธศักราช 2544 แก้ไขเพิ่มเติม (ฉบับที่ 4) พุทธศักราช 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พุทธศักราช 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพุทธศักราช 2562 รวมทั้งเอกสารต่าง ๆ เช่น บทบัญญัติของกฎหมาย กฎ ระเบียบข้อบังคับ ตำรา บทความ รายการวิจัย และกฎหมาต่างประเทศ เป็นต้น

1.5 วิธีการดำเนินการศึกษา

การศึกษาวิจัยเอกสาร (Documentary research) โดยทำการสืบค้นค้นคว้าวิจัยวิเคราะห์ข้อมูลในส่วนประเด็นที่เกี่ยวกับมาตรการความมั่นคงปลอดภัยข้อมูลส่วนบุคคล คำจำกัดความ การเก็บรักษา การรวบรวมใช้ เปิดเผย หรือทำลายข้อมูลส่วนบุคค จากบทบัญญัติของกฎหมายข้อบังคับตามพระราชบัญญัติและหรือกฎหมายอื่น ๆ ทั้งในประเทศไทยและของต่างประเทศ ได้แก่ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 และRegulation (EU) 2016/679 (General Data Protection Regulation) of 27 April 2016 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 Biometric Information Privacy Act 2008 (BIPA) Federal Data Protection Act 2018 (BDSG) Personal Data Protection Act 2012 (PDPA) รวมทั้งบทความทางวิชาการ ผลงานวิจัยของนักวิชาการ ตำราของนักวิชาการในสายงานวิชาการต่าง ๆ ในส่วนที่เกี่ยวกับความเป็นส่วนตัวของข้อมูลไบโอเมตริกซ์ในปัจจุบันและข้อเสนอแนะ

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ทำให้ทราบถึงแนวความคิดเกี่ยวกับกับมาตรการคุ้มครองความเป็นส่วนตัวในข้อมูลไบโอเมตริกซ์ ภายใต้กฎหมายไทย

1.6.2 ทำให้ทราบถึงความยินและการถอนความยินยอมในการใช้ข้อมูลไบโอเมตริกซ์ (Biometrics)

1.6.3 ทำให้ทราบถึง มาตรการในการบังคับใช้กฎหมายโดยเฉพาะอย่างยิ่งระยะเวลาในการเก็บรักษาข้อมูลที่เป็นไปตามหลักสิทธิที่จะถูกลืม (Right to be forgotten)

1.6.4 ทำให้ทราบถึงแนวทางในการแก้ไขปัญหาความเป็นส่วนตัวในข้อมูลไบโอเมตริกซ์ (Biometrics)

1.7 นิยามคำศัพท์เฉพาะ

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

“ไบโอเมตริกซ์” (Biometrics) หรือ ตัววัดชีวมาตร หมายถึง การนำค่าคุณลักษณะเฉพาะของบุคคลที่เป็นเอกลักษณ์ หรือ พฤติกรรมบางอย่างของบุคคลที่มีชีวิต หรือนำมาผนวกเข้ากับหลักการทางสถิติและเทคโนโลยีทางการแพทย์ในการตรวจสอบจำแนกสิ่งมีชีวิต โดยนำมาเทียบวัดจากคุณลักษณะเฉพาะของบุคคลนั้น ๆ เพื่อจดจำลักษณะของแต่ละบุคคลไว้ในระบบอิเล็กทรอนิกส์

“Consent” แทนคำว่า หลักการความยินยอม การยินยอม ยินยอม ความยินยอม ให้ความยินยอม ให้คำยินยอม โดยผู้วิจัยได้ใช้คำดังกล่าวนี้แทนในบางบริบทซึ่งมีความหมายเช่นเดียวกัน