การคุ้มครองข้อมูลส่วนบุคคลในภาคธุรกิจธนาคาร

Personal data protection issues in the banking sector

เอกณัท สุชาติพันธุ์[1] และ ประพันธ์พงษ์ ขำอ่อน[2]

[1]หลักสูตรนิติศาสตรมหาบัณฑิต กลุ่มวิชากฎหมายตลาดทุน การเงิน และภาษี
มหาวิทยาลัยหอการค้าไทย, Eknat25@hotmail.com
[2]อาจารย์ประจำ คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย prapanpong_khu@utcc.ac.th

---

บทคัดย่อ

กฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีบทบัญญัติคุ้มครองถึงข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ และศึกษาแนวทางการให้ความ คุ้มครองความเป็นส่วนตัวของ เนื่องจากในปัจจุบันเทคโนโลยีต่าง ๆโดยเฉพาะอย่างยิ่งอินเตอร์เน็ตได้ก้าวเข้ามาเป็นส่วนสำคัญ ในชีวิตของทุกคนในทุกเพศทุกวัย ไม่ว่าจะเป็นการติดต่อสื่อสาร การสืบค้นข้อมูล หรือพาณิชย์ อิเล็กทรอนิกส์ โดยเฉพาะในภาคธุรกิจธนาคารที่มีการเก็บรวบรวมข้อมูลของลูกค้าเป็นจำนวนมากจากจำนวนผู้มาใช้บริการ ทำให้การคุ้มครองข้อมูลส่วนบุคคลในธุรกิจนี้จึงมีความจำเป็นอย่างมาก ข้อมูลจะไม่สามารถเปิดเผยข้อมูลได้ นอกจากกรณีที่ธนาคารจำเป็นต้องปฏิบัติตามกฎหมาย ธนาคารจึงต้องดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลต่อไป

คำสำคัญ: ข้อมูลส่วนบุคคล, ความเป็นส่วนตัว, ธนาคาร

ABSTRACT

Personal Information Protection Law Which has provisions to protect personal information in electronic form and study guidelines for Protect the privacy of Due to the current technology In particular, the Internet has entered into an important part. In the life of everyone in all ages Whether it is communication Searching for information or electronic commerce Especially in the business sector, banks that collect large amounts of customer information from the number of users Thus protecting personal information in this business is very necessary Information cannot be disclosed. In addition to the case that the bank needs to comply with the law Therefore, the bank must continue to comply with the Personal Data Protection Act

Keywords: personal information, privacy, bank

1.บทนำ

ธุรกิจธนาคารเป็นภาคธุรกิจเอกชนขนาดใหญ่ที่มีบทบาทต่อการดำเนินเศรษฐกิจของประเทศตั้งแต่อดีตจนถึงปัจจุบัน ฐานลูกค้าของธนาคารจึงมีฐานลูกค้าเป็นจำนวนมากไม่ว่าจะเป็นลูกค้าประเภทบุคคลธรรมดา ลูกค้าองค์กรธุรกิจทั้งในประเทศและต่างประเทศ ทำให้ธนาคารเป็นองค์กรธุรกิจที่มีฐานข้อมูลขนาดใหญ่ ซึ่งบางทีข้อมูลของลูกค้าได้ถูกเปิดเผยจากการปฏิบัติงานของตัวธนาคารเองหรือเกิดจากความผิดพลาดของระบบธนาคารเอง ทำให้

เจ้าของข้อมูลได้รับความเสียหายจากการกระทำดังกล่าว บทความฉบับนี้จะขอกล่าวถึงประเด็นสำคัญในการคุ้มครองข้อมูลส่วนบุคคลในภาคธุรกิจธนาคาร

ก่อนที่ประเทศไทยจะมีพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ใช้บังคับ ธนาคารมีกฎหมายเฉพาะภาคส่วนใช้บังคับ คือ พระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ.2551 ซึ่งพระราชบัญญัติฉบับนี้ได้มีบทบัญญัติเกี่ยวกับการได้มาซึ่งความลับของสถาบันการเงินไว้ในหมวด 8 บทกำหนดโทษ มาตรา 155 โดยเหตุที่เป็นผู้มีอำนาจในการจัดการหรือเป็นพนักงานและได้เปิดเผยความลับโดยการกระทำดังกล่าวนั้นทำให้เกิดความเสียหายแก่บุคคลอื่น หรือประชาชน ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ แต่มาตรา 155 มีวรรคท้ายบัญญัติไว้อีกว่า ความในวรรคหนึ่งมิให้ใช้บังคับกับการเปิดเผยตามกรณีในมาตรา 154 วรรคสอง ตั้งแต่อนุมาตรา 1 ถึง อนุมาตรา 10 และ

ในส่วนของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งเป็นกฎหมายกลางที่ใช้บังคับกับทุกภาคส่วนธุรกิจไม่ว่าจะเป็นหน่วยงานของภาครัฐหรือเอกชน ในส่วนที่เกี่ยวกับภาคธุรกิจธนาคารนั้นได้มีข้อยกเว้นไว้ในมาตรา 4 ของพระราชบัญญัติฉบับนี้ ถ้าการเปิดเผยนั้นเป็นการเปิดเผยนั้นใช้สำหรับการดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

นอกจากธนาคารต้องมีการปฏิบัติตามพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ.2551 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 แล้ว ธนาคาแต่ละธนาคารมีแนวนโยบายการคุ้มครองข้อมูลส่วนบุคคลของแต่ละธนาคารที่จัดทำขึ้นมาเพื่อคุ้มครองเจ้าของข้อมูลอีกทางหนึ่ง และมีประกาศของธนาคารแห่งประเทศไทย ที่ สนส. 19/2560 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน ที่ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสารและการจัดเก็บข้อมูลระบบงานและสื่อบันทึกข้อมูลต่าง ๆ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยได้ให้ความหมายข้อมูลส่วนบุคคล ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

Personal Data Protection Act 2012 ของประเทศสาธรณรัฐสิงค์โปร์ ได้ให้ความหมายของ “ข้อมูลส่วนบุคคล หมายถึง ข้อมูลไม่ว่าจะเป็นจริงหรือไม่เกี่ยวกับบุคคลที่สามารถระบุได้

(a) จากข้อมูลนั้น หรือ

(b) จากข้อมูลนั้นและข้อมูลอื่น ๆ ที่องค์กรมีหรือน่าจะมีโอกาสที่เข้าถึงได้

Personal Data Protection Act 2010 ของประเทศสหพันธรัฐมาเลเซีย ได้ให้ควาหมายของ

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใด ๆ ที่เกี่ยวกับการทำธุรกรรมเชิงพาณิชย์ซึ่ง

(a) กำลังประมวลผลทั้งหมดหรือบางส่วนด้วยการทำงานของอุปกรณ์โดยอัตโนมัติ ในการตอบสนองต่อคำแนะนำที่ได้รับเพื่อไปถึงจุดประสงค์นั้น

(b) บันทึกด้วยความตั้งใจว่าควรดำเนินการทั้งหมดหรือบางส่วนด้วยอุปกรณ์ หรือ

(c) ถูกบันทึกเป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูลที่เกี่ยวข้องหรือด้วยความตั้งใจว่าควรเป็นส่วนหนึ่งของระบบการจัดเก็บ

ประเภทของข้อมูลส่วนบุคคล

ความคุ้มครองข้อมูลส่วนบุคคลแบ่งความคุ้มครองข้อมูลออกเป็น 2 ประเภท คือ ข้อมูลทั่วไป (Non-Sensitive Data) และข้อมูลประเภทที่มีความอ่อนไหว (Sensitive Data) โดยข้อมูลทั้ง 2 ประเภทมีรายละเอียดดังต่อไปนี้

(1) ข้อมูลทั่วไป (Non-Sensitive Data) คือ ข้อมูลเกี่ยวกับผู้เป็นเจ้าของข้อมูลซึ่งสามารถบ่งชี้เฉพาะเจาะจงไปยังเจ้าของข้อมูลได้ เช่น ชื่อ ที่อยู่ อาชีพ อายุ เบอร์โทรศัพท์ การศึกษา สถานภาพในการสมรส ตำแหน่งหน้าที่ทางการงาน หรือลักษณะทางกายภาพของบุคคล เป็นต้น ข้อมูลประเภทดังกล่าวเป็นข้อมูลซึ่งมิได้มีความละเอียดอ่อนจนอาจนำมาสู่ปัญหาต่าง ๆ ได้ จึงทำให้ข้อมูลดังกล่าวเป็นข้อมูลที่อาจเก็บรวบรวม เปิดเผย หรือใช้ได้ ทั้งนี้ภายใต้หลักเกณฑ์ที่กฎหมายกำหนดไว้

(2) ข้อมูลที่มีความอ่อนไหว (Sensitive Data) คือ ข้อมูลของบุคคลซึ่งถือเป็นเรื่องเฉพาะตัวของบุคคล เป็นข้อมูลซึ่งมีความละเอียดอ่อนสูง กล่าวคือข้อมูลดังกล่าวเป็นข้อมูลซึ่งหากมีการเปิดเผยอาจก่อให้เกิดผลกระทบที่ไม่พึงประสงค์ตามมา เช่น กระทบต่อความรู้สึกของเจ้าของข้อมูลหรือประชาชนทั่วไป เป็นข้อมูลที่ก่อให้เกิดความขัดแย้งได้ ก่อให้เกิดผลกระทบต่อชื่อเสียงหรือเกียรติคุณของเจ้าของข้อมูล หรือเป้นข้อมูลซึ่งหากมีการเปิดเผยอาจก่อให้เกิดการตั้งข้อรังเกียจหรือเลือกปฏิบัติหรือเกิดอันตรายต่อเจ้าของข้อมูล โดยประเภทข้อมูลเจ้าของข้อมูลมีวัตถุประสงค์ที่จะเก็บข้อมูลประเภทนี้ไว้เป็นความลับ หรือ ไม่ประสงค์ให้มีการเปิดเผยข้อมูล เช่น ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อเกี่ยวกับลัทธิ ศาสนา พฤติกรรมทางเพศ ประวัติสุขภาพ ประวัติอาชาญกรรม หรือ สถานะทางการเงิน เป็นต้น

1) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับต่ำ (Low-Sensitive) ข้อมูลประเภทนี้เป็นข้อมูลที่ความเกี่ยวข้องกับบุคคลเป้นข้อมูลที่มีความอ่อนไหวเนื่องจากข้อมูลเหล่านี้อาจช่วยทำให้ได้มาซึ่งข้อมูลที่มีระดับความอ่อนไหวสูงขึ้น

2) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับปานกลาง (Moderate-Sensitivity) ข้อมูลประเภทนี้เป็นข้อมูลที่มีความอ่อนไหวมา ในแง่ที่มีโอกาสที่จะก่อให้เกิดความเสียหายเมื่อข้อมูลถูกนำเอาไปใช้ในทางที่ผิดอยู่ในระดับสูง ข้อมูลประเภทนี้ครอบคลุมถึงข้อมูลประเภทที่เกี่ยวกับความคิดเห็นของบุคคล ซึ่งมีความครอบคลุมในทุกเรื่องของชีวิต ข้อมูลที่มีความอ่อนไหวระดับปานกลางนี้มีความสำคัญเช่นกันกับข้อมูลที่มีความอ่อนไหวระดับสูงและไม่ควรเก็บไว้โดยสิ้นเชิง

3) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับสูง (High-Sensitivity) ข้อมูลประเภทนี้ ได้แก่ ข้อมูลรายละเอียดส่วนตัวของบุคคลในส่วนที่เกี่ยวข้องกับประวัติทางการแพทย์ พฤติกรรมทางเพศ หรือข้อที่จริงด้านอื่น ๆ ในชีวิตของบุคคล ซึ่งสามารถกล่าวได้ว่าเป็นเรื่องส่วนตัวหรือลับเฉพาะ ข้อมูลประเภทนี้มีความอ่อนไหวสูงนี้จึงมีความสำคัญและไม่ควรถูกเก็บรวบรวมไว้โดยสิ้นเชิง

Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and development หรือ OECD) ได้ออกแนวปฏิบัติ OECD Guidelines Governing the Protection pf Privacy and Transborder Flows of Personal Data มีขึ้นเพื่อทำหน้าที่ในการดูแลการส่งข้อมูลระหว่างประเทศ การคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองสิทธิความเป็นส่วนตัว จุดเริ่มต้นของแนวปฏิบัติดังกล่าวเกิดจากความไม่เท่าเทียมกันของ

บทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในประเทศต่าง OECD จึงได้จัดทำแนวปฏิบัติขั้นต้นของหลักการดังกล่าวเพื่อให้ประเทศสมาชิกได้นำไปเป็นแนวทางปฏิบัติ แนวปฏิบัติดังกล่าวใช้บังคับได้ทั้งหน่วยงานของรัฐและเอกชน แนวปฏิบัติดังกล่าวมีหลักการที่สำคัญ ดังนี้

(1) หลักการเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด (Collection Limitation Principle)

หลักการดังกล่าวกำหนดให้มีการจำกัดการเก็บรวบรวมข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลดังกล่าวต้องได้มาโดยวิธีที่ชอบด้วยกฎหมาย และได้มาภายใต้ความยินยอมหรือความรับรู้ของเจ้าของข้อมูลส่วนบุคคล

(2) หลักคุณภาพของข้อมูล (Data Quality Principle)

หลักการดังกล่าวกำหนดให้ข้อมูลส่วนบุคคลนั้นต้องเกี่ยวข้องกับวัตถุประสงค์ในการจัดเก็บรวบรวมข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลนั้นต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบัน

(3) หลักการกำหนดวัตถประสงค์ (Purpose Specification Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลในเวลาที่จัดเก็บรวบรวมข้อมูลนั้นและการนำข้อมูลส่วนบุคคลที่จัดเก็บนั้นไปใช้ต้องเป็นไปเพียงเพื่อให้บรรลุวัตถุประสงค์ที่ได้แจ้งไว้ หรือ หากผู้ควบคุมข้อมูลส่วนบุคคลต้องการใช้ข้อมูลส่วนบุคคลนั้นเพื่อวัตถุประสงค์อื่นซึ่งไม่ขัดต่อวัตถุประสงค์ที่ได้แจ้งไว้ในขณะทำการเก็บรวบรวมต้องมีการแจ้งวัตถุประสงค์ที่เปลี่ยนแปลงไปให้เจ้าของข้อมูลทราบ

(4) หลักการใช้ข้อมูลส่วนบุคคลอย่างจำกัด (Use Limitation Principle)

หลักการดังกล่าวกำหนดห้ามมิให้ผู้เก็บรวบรวมข้อมูลส่วนบุคคลทำการเปิดเผยข้อมูลส่วนบุคคล ทำให้บุคคลอื่นสามารถใช้ได้ หรือใช้เพื่อวัตถุประสงค์อื่นนอกจากวัตถุประสงค์ที่ได้แจ้งไว้ขณะเก็บรวบรวมข้อมูล เว้นแต่

1. ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือ
2. เป็นการปฏิบัติตามบทบัญญัติกฎหมาย

(5) หลักการรักษาความปลอดภัย (Security Safeguards Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องมีหลักเกณฑ์ในการรักษาความปลอดภัยที่เหมาะสมแก่ข้อมูลส่วนบุคคลเพื่อป้องกันความเสียหายที่เกิดจากการสูญหาย การเข้าถึงโดยมิได้รับอนุญาต การทำลาย การใช้ การเปลี่ยนแปลง หรือการเปิดเผยข้อมูลส่วนบุคคลดังกล่าว

(6) หลักการเปิดเผย (Openness Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการทั่วไปเกี่ยวกับการเปิดเผยถึงการนำไปใช้ แนวทางปฏิบัติ และนโยบายเกี่ยวกับข้อมูลส่วนบุคคล การเปิดเผยดังกล่าวต้องแสดงถึงความมีอยู่ของข้อมูลส่วนบุคคล ลักษณะของข้อมูลส่วนบุคคล และวัตถุประสงค์ในการนำข้อมูลไปใช้ รวมถึงชื่อของผู้เก็บรวบรวมข้อมูลส่วนบุคคลและที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคลและที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล

(7) หลักการมีส่วนร่วมของปัจเจกบุคคล (Individual Participation Principle)

ภายใต้หลักการดังกล่าวปัจเจกบุคคลมีสิทธิ

a) ได้รับการบอกกล่าวจากผู้ควบคุมข้อมูลส่วนบุคคลเพื่อยืนยันถึงการมีอยู่ซึ่งข้อมูลส่วนบุคคลของปัจเจกบุคคลนั้น

b) ได้รับการแจ้งถึงข้อมูลส่วนบุคคลของตนโดย

- ภายในระยะเวลาพอสมควร
- มีค่าใช้จ่ายไม่เกินสมควร
- โดยวิธีการที่เหมาะสม
- ในรูปแบบซึ่งเจ้าของข้อมูลสามารถเข้าใจได้

c) ได้รับการแจ้งถึงเหตุผลหากการร้องขอตามข้อ a) และข้อ b) ถูกปฏิเสธ และมีสิทธิในการอุทธรณ์การปฏิเสธดังกล่าว

d) มีสิทธิคัดค้านข้อมูลส่วนบุคคลเกี่ยวกับตน หากคคำคัดค้านมีเหตุผลเจ้าของข้อมูลมีสิทธิขอให้ลบข้อมูล ทำให้สมบูรณ์ แก้ไขหรือปรับปรุงข้อมูลนั้น

เจ้าของข้อมูลมีสิทธิขอให้ลบข้อมูล ทำให้สมบูรณ์ แก้ไขหรือปรับปรุงข้อมูลนั้น

(8) หลักความเชื่อถือได้ (Accountability Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลต้องปฏิบัติตามหลักการข้อ (1) ถึงข้อ (7) โดยผู้ควบคุมข้อมูลต้องจัดให้มีแผนในการจัดการเกี่ยวกับความเป็นส่วนตัวซึ่งมีลักษณะ 6 ประการ คือ

1. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องจัดให้มีแนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของตน

2. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องเหมาะสมต่อโครงสร้าง ขนาด ปริมาณและความอ่อนไหวของการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคล

3. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องกำหนดให้มีมาตรการป้องกันที่เหมาะสมโดยพิจารณาจากการประเมินความเสี่ยงในด้านความเป็นส่วนตัว

4. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องถูกรวมอยู่ในโครงสร้างการกำกับดุแลและจัดให้มีองค์กรกับดูแลภายใน

5. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องระบุถึงแผนการจัดการในกรณีที่เหตุฉุกเฉิน

6. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องได้รับการปรับปรุงให้เป็นไปตามการตรวจสอบและการประเมินผู้ควบคุมข้อมูลส่วนบุคคลต้องสามารถแสดงแผนในการจัดการความเป็นส่วนตัวให้แก่หน่วยงานที่กำกับดูแลได้ ทั้งต้องแจ้งแก่หน่วยงานที่มีหน้าที่กำกับดูแลหากมีการฝ่าฝืนความปลอดภัยอย่างมีนัยสำคัญซึ่งกระทบต่อข้อมูลส่วนบุคคล และหากการฝ่าฝืนนั้นอาจก่อให้เกิดผลร้ายต่อเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งแก่เจ้าของข้อมูลที่อาจได้รับความเสียหายด้วย

2.วัตถุประสงค์การวิจัย

เพื่อศึกษาแนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

3.การดำเนินการวิจัย

เป็นการวิจัยเชิงคุณภาพโดยการศึกษาค้นคว้าวิยานิพนธ์ เอกสาร ตำรา ทั้งของประเทศไทยและต่างประเทศ

4.ผลการวิจัย

ในเรื่องการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยได้นำต้นร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปมาเป็นต้นแบบในการร่างกฎหมาย GDPR ของสหภาพยุโรป โดยหลักการสำคัญ ๆ ของ GDPR ไม่ว่าจะเป็นเรื่องการคุ้มครองข้อมูล การเปิดเผยข้อมูล การโอนข้อมูล สิทธิที่จะลบข้อมูล ได้นำมาบัญญัติไว้ทั้งหมดในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย อาจจะไม่ได้เทียบเท่ากับกฎหมาย GDPR แต่ก็เทียบเคียง ส่วนพระราชบัญญัติคุ้มครองของไทยใช้กับทุกภาคส่วนไม่ได้แบ่งแยกภาคธุรกิจและประเทศไทยยังไม่ได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเฉพาะภาคธุรกิจธนาคารโดยเฉพาะ

5.สรุปและอภิปรายผล

จากการศึกษาพบว่าประเทศไทยยังไม่ได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะในภาคธุรกิจธนาคาร จึงควรนำต้นแบบของต่างประเทศมาต้นแบบในการร่าง

6.ข้อเสนอแนะ

ให้นำกฎหมายของสิงค์โปร์มาเป็นต้นแบบในการร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

เอกสารอ้างอิง

ดาวัลย์ ขาวสนิท มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล : ศึกษาเฉพาะกรณีด้านการเงินการธนาคารของธนาคารพาณิชย์ วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์

ธาริณี มณีรอด. (2559). ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล. วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์

ธนัท สุวรรณปริญญา. (2550). ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์ กรณีศึกษา : การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Polocy) ของธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย สารนิพนธ์ปริญญานิติศาสตรมหาบัณฑิต บัณฑิตวิทยาลัย มหาวิทยาลัยกรุงเทพ

รองศาสตราจารย์คณาธิป ทองรวีวงศ์. (2559). รายงานวิจัยฉบับสมบูรณ์ เรื่อง การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน. กรุงเทพมหานคร : สำนักงานเลขาธิการสภาผู้แทนราษฎร