

มาตรการทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรม อิเล็กทรอนิกส์ : ศึกษากรณีการใช้คุกกี้บนอินเทอร์เน็ต

Legal Measures on Privacy Protection in Electronic Transaction : Case Study of Internet Cookies¹

ภารวี ปุณเสรีพิพัฒน์²

Parawee Poonserepipat

บทคัดย่อ

การละเมิดข้อมูลส่วนบุคคลโดยใช้เทคโนโลยีอย่างคุกกี้ (cookie) ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นเป็นปัญหาสำคัญที่ทั่วโลกตระหนักถึงและให้ความสนใจ กฎหมายจึงมีบทบาทสำคัญและมีความจำเป็นในการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์ให้มีประสิทธิภาพและครอบคลุมมากยิ่งขึ้น บทความวิจัยนี้มีวัตถุประสงค์เพื่อที่จะหาคำตอบว่ามาตรการทางกฎหมายของประเทศไทย ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้นเพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์หรือไม่ ผลการวิจัยพบว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้นเป็นการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป ไม่ได้แยกบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ไว้ต่างหาก อย่างไรก็ตามมาตรการทางกฎหมายของต่างประเทศ จึงส่งผลถึงประสิทธิภาพในการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ที่ยังไม่ชัดเจนและครอบคลุมเพียงพอ ข้อเสนอแนะของการวิจัยจึงเห็นว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลดังกล่าวควรมีการแยกประเภทเพื่อคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์เป็นการเฉพาะ

คำสำคัญ : ข้อมูลส่วนบุคคล, คุกกี้, ธุรกรรมอิเล็กทรอนิกส์, การคุ้มครองข้อมูลส่วนบุคคล

¹ บทความนี้ปรับปรุงจากวิทยานิพนธ์ เรื่อง “มาตรการทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ : ศึกษากรณีการใช้คุกกี้บนอินเทอร์เน็ต” ตามหลักสูตรนิติศาสตรมหาบัณฑิต มหาวิทยาลัยกรุงเทพ

² นักศึกษาหลักสูตรนิติศาสตรมหาบัณฑิต บัณฑิตวิทยาลัย มหาวิทยาลัยกรุงเทพ ปัจจุบันตำแหน่ง นิติกรปฏิบัติการ กองนิติการ สำนักงานประกันสังคม



Abstract

An invasion of data privacy by using cookies technology for collecting personal data was an important problem which had been concerned by almost all countries. Data Protection Law, therefore, played an important role to protect personal data used in electronic transactions. This study aimed to find out whether the Draft law on Personal Data Protection of Thailand was sufficient to protect personal data used in electronic transactions. The research revealed that the Draft law on Personal Data Protection of Thailand, unlike that in other countries, didn't have a specific provision regarding the protection of personal data used in electronic transactions. It had only provisions which aimed to protect personal data in general. Such law, thus, was unclear, inefficient and insufficient to protect personal data, especially personal data used in electronic transactions. To resolve such problem, the author recommended that the Draft law on Personal Data Protection of Thailand should have a specific provision for the protection of personal data used in electronic transactions.

Keywords : Personal Data, Cookies, Electronic Transaction, Protection of Personal Data

1. บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) ถือเป็นสิทธิมนุษยชนขั้นพื้นฐานประเภทหนึ่งที่นานาประเทศให้ความสำคัญ โดยการคุ้มครองข้อมูลส่วนบุคคลนั้นถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว (Right of Privacy) เนื่องจากความเป็นอยู่ส่วนตัวนั้นย่อมหมายถึงความรวมถึง ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) และความเป็นส่วนตัวในเคหสถาน (Territorial Privacy) ซึ่งการคุ้มครองข้อมูลส่วนบุคคลนั้นถือได้ว่าเป็นความเป็นส่วนตัวเกี่ยวกับข้อมูลนั่นเอง โดยสิทธิดังกล่าวมีการรับรองไว้อย่างชัดเจนในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ข้อ 12³ นอกจากนี้รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 มาตรา 35⁴ ก็ได้บัญญัติให้ความคุ้มครองรับรองสิทธิความเป็นอยู่ส่วนตัวไว้เช่นกัน

ในสังคมยุคข้อมูลข่าวสารอย่างปัจจุบัน บรรดาความเป็นส่วนตัวทั้งหมดดังกล่าว ความเป็นส่วนตัวเกี่ยวกับข้อมูล เป็นเรื่องที่ประเทศส่วนใหญ่ให้ความสำคัญเป็นอย่างมาก ทั้งนี้เนื่องจากความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศที่เป็นไปอย่างรวดเร็ว การรับรู้ข้อมูลข่าวสารต่างๆ เป็นเรื่องที่สะดวกสบายมากขึ้น เมื่ออินเทอร์เน็ตได้เข้ามาเป็นสื่อที่มีบทบาทสำคัญในการติดต่อสื่อสารระหว่างกันและเป็นสื่อที่ได้รับความนิยมอย่างแพร่หลาย ทำให้แทบทุกกิจกรรมที่เกิดขึ้นล้วนแต่มีความเกี่ยวข้องกับอินเทอร์เน็ตทั้งสิ้น ส่งผลให้ธุรกิจและธุรกรรมต่างๆ บนอินเทอร์เน็ตเกิดขึ้นมากมาย ในแต่ละวันข้อมูลนับล้านถูกส่งผ่านเครือข่าย เพื่ออำนวยความสะดวกให้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ต่างๆ อย่างไรก็ตาม ในทางกลับกันเมื่อข้อมูลต่างๆ สามารถเข้าถึงได้ง่าย จึงอาจมีการนำข้อมูลเหล่านี้ไปใช้โดยละเมิดต่อบุคคลอื่น โดยอาจทำให้เกิดความเสียหายหรือสูญเสียของข้อมูล หรืออาจถูกนำข้อมูลไปใช้ในทางที่ผิด ไม่ว่าจะเป็นโดยเจตนาหรือไม่เจตนาก็ตาม

³ มาตรา 12 บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือจะถูกกลั่นแกล้งหรือข่มขู่และชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการแทรกแซงสิทธิหรือการกลั่นแกล้งดังกล่าว

⁴ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 มาตรา 35 สิทธิความเป็นส่วนตัวย่อมได้รับความคุ้มครองสิทธิของบุคคลในครอบครัวเกียรติยศ ชื่อเสียง ตลอดจนความเป็นส่วนตัวย่อมได้รับความคุ้มครองการกล่าวหรือโฆษณาแพร่หลาย ซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียงหรือความเป็นส่วนตัวจะกระทำได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ

ความก้าวหน้าของสังคมยุคข้อมูลข่าวสารถูกแสดงลักษณะพิเศษโดยการนำเข้ามาซึ่งบริการอิเล็กทรอนิกส์ใหม่ๆ ที่มีอยู่ ไปจนถึงประเภทของเทคโนโลยีและอุปกรณ์ที่หลากหลาย ซึ่งบริการเหล่านี้มีความสามารถในการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลที่เยอะมาก ตัวอย่างของหนึ่งในเทคโนโลยีที่สำคัญมากในการทำงานของอินเทอร์เน็ต ซึ่งเป็นที่รู้จักกันแพร่หลายในชื่อของคุกกี้ (Cookie) คุกกี้ หมายถึง ไฟล์ที่ทางเว็บไซต์ต่างๆ สร้างขึ้นมาในเครื่องคอมพิวเตอร์ของผู้เยี่ยมชมเว็บไซต์นั้นๆ โดยคุกกี้จะมีวัตถุประสงค์ในการเก็บข้อมูล ตรวจสอบ จากผู้ที่เรียกใช้งานเว็บไซต์นั้น โดยไฟล์คุกกี้จะมีลักษณะเป็น Text File ในการเก็บข้อมูลต่างๆ และเป็นไฟล์ขนาดเล็ก ทั้งนี้ เว็บไซต์ต่างๆ ที่ขายสินค้าหรือให้บริการโฆษณา มักนิยมใช้โปรแกรมคุกกี้ดังกล่าว เช่น เว็บไซต์ Amazon.com หรือเว็บไซต์ eBay.com ซึ่งใช้เพื่อติดตามความเคลื่อนไหวของผู้ใช้งานแต่ละบุคคลบนเว็บไซต์ต่างๆ โดยสามารถใช้เพื่อเก็บข้อมูลซึ่งผู้ใช้แต่ละบุคคลได้ไว้ในเว็บไซต์ อย่างเช่น ชื่อ, ที่อยู่ หมายเลขบัตรเครดิต และอื่นๆ ปัญหาที่เกิดขึ้นจากการเก็บและการใช้ข้อมูลส่วนบุคคลโดยผู้ให้บริการดังกล่าวนี้ คือ เก็บข้อมูลข่าวสารเกี่ยวกับบุคคลโดยผู้ให้บริการเพื่อใช้ประโยชน์ในทางการค้าของตนเองหรือเพื่อเปิดเผยแก่บุคคลภายนอกโดยได้รับผลประโยชน์ตอบแทนโดยที่เจ้าของข้อมูลเหล่านั้นไม่อนุญาตหรือไม่เคยได้ให้ความยินยอมไว้ ซึ่งฐานข้อมูลเหล่านี้เรียกว่าเป็นฐานข้อมูลที่มีความสำคัญทางเศรษฐกิจ เพราะสิ่งเหล่านี้สามารถชี้วัดแนวโน้มความต้องการโดยรวมในสินค้าอุปโภคและบริโภค ซึ่งเป็นประโยชน์สำหรับการวางแผนการตลาด วางแผนการผลิตสินค้า ซึ่งข้อมูลเหล่านี้เป็นที่ต้องการของผู้ประกอบธุรกิจการค้ามาก แต่อย่างไรก็ดีการเก็บข้อมูลข่าวสารประเภทนี้ก่อให้เกิดความเสี่ยงต่อสิทธิในความเป็นอยู่ส่วนตัวของบุคคลมาก เนื่องจากฐานข้อมูลทางคอมพิวเตอร์เหล่านี้สามารถถูกเผยแพร่ ถูกขโมย หรือถูกสำเนา นำไปใช้ได้อย่างรวดเร็วและไม่จำกัด ดังนั้น กรอบของกฎหมายจึงจำเป็นที่จะต้องคุ้มครองสิทธิความเป็นส่วนตัวขั้นพื้นฐานของแต่ละบุคคลและข้อมูลส่วนบุคคลของพวกเขา โดยในขณะเดียวกันก็ต้องให้ความใส่ใจต่อผลประโยชน์ที่สอดคล้องกับกฎหมายของรัฐบาลและธุรกิจทั้งหลาย

ทั้งนี้ สหภาพยุโรปได้มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลไว้ โดยในวันที่ 12 กรกฎาคม ปี ค.ศ. 2002 EU ได้นำ Directive 2002/58/EC ซึ่งเกี่ยวข้องกับกระบวนการของข้อมูลส่วนบุคคล และการคุ้มครองความเป็นส่วนตัวในภาคส่วนของการติดต่อสื่อสารทางอิเล็กทรอนิกส์ มาใช้บังคับ Directive นี้เป็นส่วนหนึ่งของส่วนประกอบทั้งหมดของ 5 Directive ใหม่ ซึ่งมีจุดประสงค์ที่จะปฏิรูปกฎหมายและกรอบของการควบคุมของบริการการติดต่อสื่อสารทางอิเล็กทรอนิกส์ใน EU Directive นี้ยกเลิกและแทนที่ Directive 97/66/EC ของ EU ลงวันที่ 15 ธันวาคม ปี ค.ศ. 1997 ซึ่งเกี่ยวข้องกับกระบวนการของข้อมูลส่วนบุคคล และการคุ้มครองความเป็นส่วนตัวในส่วนของการสื่อสารทางไกลโดยใช้เทคโนโลยี (โทรคมนาคม)⁵ ต่อมาภายหลัง EU ได้มี

⁵ Debussere, F., (2005), *The EU E-Privacy Directive : A Monstrous Attempt to Starve the Cookie Monster?*, Retrieved April 16, 2012, from http://www.law.kuleuven.be/icri/publications/657_FredericDebussereCookies.pdf.

การพัฒนาต่อจาก Directive 2002/58/EC ดังกล่าวมาเป็น The Privacy and Electronic Communications (EC Directive) Regulation 2003 ซึ่งมีผลบังคับใช้เมื่อวันที่ 11 ธันวาคม ปี ค.ศ. 2003 และล่าสุด EU ได้ออก The Privacy and Electronic Communications (EC Directive) Regulation 2011 ซึ่งเป็นการแก้ไขเพิ่มเติมของ The Privacy and Electronic Communications (EC Directive) Regulation 2003 โดยมีผลบังคับใช้ไปเมื่อวันที่ 26 พฤษภาคม ปี ค.ศ. 2011

สำหรับในสหรัฐอเมริกา มีคดีที่เกิดขึ้นฟ้องบริษัทและองค์กรที่ใช้เทคโนโลยีคุกนี้เพื่อรวบรวมข้อมูลเกี่ยวกับผู้ใช้อินเทอร์เน็ต ตัวอย่างของคดีที่มีชื่อเสียงรู้จักกันทั่วไป ได้แก่ คดีของบริษัทโฆษณา DoubleClick⁶ ซึ่งทำการเก็บรวบรวมและวิเคราะห์ข้อมูลจำนวนมหาศาลเกี่ยวกับผู้ใช้อินเทอร์เน็ต โดยวางคุกไว้บน hard drive ของผู้ใช้บริการแต่ละคนซึ่งเข้าไปเยี่ยมชมเว็บไซต์ใดเว็บไซต์หนึ่ง ใน 11,000 เว็บไซต์ในเครือของ DoubleClick โดยที่ผู้ใช้บริการไม่รู้ตัว ซึ่งนั่นทำให้ DoubleClick สามารถติดตามข้อมูลเกี่ยวกับพฤติกรรมของผู้ใช้แต่ละคนในการเยี่ยมชมเว็บไซต์ต่างๆ หลังจากนั้นในสหรัฐอเมริกาก็ยังมีความเกี่ยวกับการใช้คุกก็ตามมาอีกมากมาย หนึ่งในคดีที่น่าสนใจล่าสุดเป็นคดีของบริษัทโฆษณา InterClick⁷ ทั้งนี้ ในส่วนของกฎหมายของสหรัฐอเมริกาที่เกี่ยวข้องกับการคุ้มครองความเป็นส่วนตัวหรือข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์นั้น จะมีปรากฏอยู่ใน The Computer Fraud and Abuse Act (1994) 18 USC § 1030—Fraud and related activity in connection with computers ซึ่งเป็นกฎหมายระดับรัฐบาลกลาง หรือ Federal Statute, Electronic Communications Privacy Act of 1986 (ECPA) และล่าสุดสหรัฐอเมริกาได้ออก The Consumer Privacy Bill of Rights ซึ่งมีแนวทางที่จะคุ้มครองผู้ใช้บริการออนไลน์จากการติดตามของเว็บไซต์โดยที่ผู้ใช้บริการไม่รู้ตัว

จะเห็นได้ว่าการให้ความคุ้มครองข้อมูลส่วนบุคคลเพื่อคุ้มครองสิทธิความเป็นส่วนตัวนั้นเป็นเรื่องที่มีความสำคัญที่ทุกประเทศทั่วโลกได้ตระหนักถึง เพราะเป็นสิ่งที่บุคคลอื่นสามารถจะนำไปใช้หาประโยชน์จากข้อมูลส่วนบุคคลของเราได้ในรูปแบบต่างๆ โดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในระบบคอมพิวเตอร์ ซึ่งสามารถประมวลผล และเผยแพร่ถึงบุคคลจำนวนมากได้โดยง่าย สะดวก และรวดเร็ว โดยอาศัยเทคโนโลยีสารสนเทศอันทันสมัย ในยุคปัจจุบันการละเมิดข้อมูลส่วนบุคคลจึงสามารถกระทำได้อย่างง่ายดายมากขึ้น และเอาผิดกับบุคคลที่ล่วงละเมิดสิทธิของบุคคลอื่นได้ยากลำบากมากขึ้น ฉะนั้นแล้วเราจึงต้องหันมาตระหนักถึงปัญหาดังกล่าวและหาแนวทางมาตรการเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล เมื่อสังคมไทยในปัจจุบันก็เป็นเช่นเดียวกับประเทศทั้งหลายในโลกที่ตกอยู่ท่ามกลางเครื่องคอมพิวเตอร์ ทำให้ต้องตั้งคำถามว่ากฎหมายไทยที่เกี่ยวข้องในเรื่องการคุ้มครองข้อมูลส่วนบุคคลเพียงพอที่จะให้

⁶ DoubleClick, Inc. Privacy Litigation, 154 F.Supp.2d 497 (S.D.N.Y.2001).

⁷ Sonal Bose v. Interclick, Inc. (2012) Case No. 10 Civ. 9183 (DAB).

ความคุ้มครองหรือไม่ โดยเฉพาะอย่างยิ่งข้อมูลประเภทที่ถูกจัดเก็บในระบบคอมพิวเตอร์ที่ใช้ในการดำเนินธุรกรรมอิเล็กทรอนิกส์ดังกล่าว

1.2 ปัญหาของการวิจัย

1) การใช้โปรแกรมคุกกี้นในระบบคอมพิวเตอร์ส่งผลต่อความปลอดภัยของข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์อย่างไร

2) การคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ในการทำธุรกรรมอิเล็กทรอนิกส์มีความแตกต่างจากการคุ้มครองข้อมูลส่วนบุคคลทั่วไปหรือไม่ อย่างไร

3) ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... เพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ในการดำเนินธุรกรรมอิเล็กทรอนิกส์หรือไม่

1.3 วัตถุประสงค์ของการวิจัย

1) เพื่อศึกษาถึงแนวคิดของการคุ้มครองข้อมูลส่วนบุคคลในยุคของอินเทอร์เน็ต

2) เพื่อศึกษาถึงความหมาย ประเภท ลักษณะการทำงานและรูปแบบการจัดเก็บข้อมูลของโปรแกรมคุกกี้นในระบบคอมพิวเตอร์รวมถึงประโยชน์ของการทำคุกกี้นับธุรกรรมอิเล็กทรอนิกส์

3) เพื่อศึกษาถึงปัญหาที่เกิดขึ้นเกี่ยวกับความปลอดภัยของข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์รวมทั้งแนวคิดและความจำเป็นในการมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ในการทำธุรกรรมอิเล็กทรอนิกส์

4) เพื่อศึกษาถึงมาตรการทางกฎหมายของสหภาพยุโรป และประเทศสหรัฐอเมริกาในการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ว่ามีบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ในแนวทางใด

5) เพื่อศึกษาและวิเคราะห์ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ว่าเพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ในการดำเนินธุรกรรมอิเล็กทรอนิกส์หรือไม่โดยศึกษาในเชิงเปรียบเทียบมาตรการทางกฎหมายของสหภาพยุโรป และประเทศสหรัฐอเมริกา

1.4 สมมติฐานของการวิจัย

การใช้คุกกี้นเก็บรวบรวมข้อมูลของผู้ใช้บริการคอมพิวเตอร์ในการดำเนินธุรกรรมอิเล็กทรอนิกส์นั้น สุ่มเสี่ยงให้เกิดการละเมิดข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในระบบคอมพิวเตอร์ได้ง่าย ความคุ้มครองทางกฎหมายของข้อมูลส่วนบุคคลในการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายไทยนั้นยังไม่ชัดเจนแน่นอน เนื่องจากไม่มีกฎหมายเฉพาะที่บังคับใช้ สำหรับในส่วน of ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ที่ถูกกำหนดให้เป็นกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลนั้น เป็นการบัญญัติการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบกว้างๆ ไม่ได้มีการบัญญัติแยกชัดเจนถึงข้อมูลที่ถูกเก็บรวบรวมไว้ในระบบคอมพิวเตอร์ในการ

ดำเนินธุรกรรมทางอิเล็กทรอนิกส์ เนื่องจากข้อมูลส่วนบุคคลนั้นถูกจัดเก็บไว้ในสื่อที่หลากหลาย ส่งผลให้ข้อมูลที่ถูกจัดเก็บในระบบคอมพิวเตอร์นั้นยังไม่มีมาตรการทางกฎหมายคุ้มครองที่ชัดเจนแน่นอนและมีประสิทธิภาพ

1.5 วิธีการดำเนินการวิจัย

เป็นการวิจัยเชิงเอกสาร โดยมีการค้นคว้าจากตำรากฎหมาย บทความ วารสาร เอกสารทางวิชาการทั้งของประเทศไทยและต่างประเทศ วิทยานิพนธ์ ตำบทยกฎหมายทั้งของประเทศไทยและต่างประเทศที่เกี่ยวข้อง ตลอดจนข้อมูลที่ค้นคว้าได้จากเว็บไซต์ต่างๆ บนอินเทอร์เน็ต

1.6 ขอบเขตของการวิจัย

การศึกษานี้เป็นการศึกษาถึงรูปแบบการจัดเก็บข้อมูลของโปรแกรมคุกกี้ในระบบคอมพิวเตอร์ และลักษณะของการละเมิดข้อมูลส่วนบุคคลที่จัดเก็บในระบบคอมพิวเตอร์ในการดำเนินธุรกรรมอิเล็กทรอนิกส์ นอกจากนี้ยังศึกษาถึงหลักเกณฑ์และมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (EU) ตาม The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 และประเทศสหรัฐอเมริกา ตาม The Computer Fraud and Abuse Act (1994) 18 USC § 1030–Fraud and related activity in connection with computers, Electronic Communications Privacy Act of 1986 (ECPA) และ The Consumer Privacy Bill of Rights โดยนำมาวิเคราะห์เปรียบเทียบกับร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...ของประเทศไทยในประเด็นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระบบคอมพิวเตอร์ในการดำเนินธุรกรรมอิเล็กทรอนิกส์ เพื่อให้ทราบถึงหลักเกณฑ์ แนวทางปฏิบัติ และปัญหา เพื่อนำมาพัฒนากฎหมายของประเทศไทยต่อไป

1.7 ประโยชน์ที่คาดว่าจะได้รับ

- 1) ทำให้เข้าใจถึงความหมาย ประเภท ลักษณะการทำงานและรูปแบบการจัดเก็บข้อมูลของโปรแกรมคุกกี้ในระบบคอมพิวเตอร์รวมถึงประโยชน์ของการทำคุกกี้กับธุรกรรมอิเล็กทรอนิกส์
- 2) ทำให้เห็นถึงสภาพปัญหาที่เกิดขึ้นเกี่ยวกับความปลอดภัยของข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์ รวมทั้งแนวคิดและความจำเป็นในการมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ในการทำธุรกรรมอิเล็กทรอนิกส์
- 3) ทำให้เห็นแนวทางในมาตรการทางกฎหมายของสหภาพยุโรป และประเทศสหรัฐอเมริกาในการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์
- 4) ทำให้ทราบถึงมาตรการทางกฎหมายตามที่บัญญัติไว้ในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...ของประเทศไทยรวมทั้งข้อบกพร่องของร่างพระราชบัญญัตินี้ดังกล่าว และแนวทางในการแก้ไขปรับปรุง

2. การทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดของการคุ้มครองสิทธิส่วนบุคคล

“สิทธิความเป็นส่วนตัว” (Right of Privacy) เป็นหนึ่งในสิทธิมนุษยชน และเป็นสิทธิขั้นพื้นฐานของมนุษย์ที่ได้รับการรับรองไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 (Universal Declaration of Human Right 1948) ว่าต้องได้รับการคุ้มครองตามกฎหมาย แนวคิดในการคุ้มครองสิทธิความเป็นส่วนตัวได้เกิดขึ้นมานานและหลากหลาย แนวคิดหนึ่งที่ได้รับการยอมรับและมีการอ้างอิงถึงอย่างแพร่หลาย คือ แนวคิดของ Samuel D. Warren และ Louis D. Brandeis ในปี ค.ศ. 1980 ที่ได้ให้ความหมายคำว่า “Privacy” ในรูปของวลีสั้นๆ ว่า “สิทธิที่จะอยู่ตามลำพัง” หรือ “Right to be let alone”⁸

ถึงแม้ว่า “ความเป็นส่วนตัว” จะมีความหมายเป็นหลายประการ กล่าวคือ ความเป็นส่วนตัวในข้อมูลข่าวสารส่วนบุคคล (Information Privacy) ความเป็นส่วนตัวในอาณาเขต หรือสถานที่ของตนเอง (Territorial Privacy) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) แต่ความเป็นส่วนตัวที่นานาประเทศต่างให้ความสำคัญอย่างมากในสังคมยุคใหม่ คือ “ความเป็นส่วนตัวในข้อมูลส่วนบุคคล” เนื่องจากการพัฒนาการทางคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งเทคโนโลยีอินเทอร์เน็ตที่ได้ส่งผลให้การติดต่อสื่อสาร การเผยแพร่ข้อมูลต่างๆ สามารถเคลื่อนย้ายและเชื่อมโยงกันได้โดยไม่จำกัดเวลาและสถานที่อีกต่อไป ทำให้การประมวลผล จัดเก็บ หรือการเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้โดยง่าย สะดวก และรวดเร็ว ในทางตรงกันข้ามจึงอาจมีการนำประโยชน์จากเทคโนโลยีเหล่านี้ไปใช้ในการละเมิดต่อบุคคลอื่นได้เช่นกัน เนื่องด้วยข้อมูลส่วนบุคคลนั้น บางส่วนสามารถนำไปใช้ในการหาประโยชน์ได้ ดังนั้น การจัดเก็บข้อมูลจึงจำเป็นต้องระมัดระวังในเรื่องความปลอดภัยในการจัดเก็บข้อมูล เพราะอาจมีผู้ที่ไม่ประสงค์ดีนำข้อมูลส่วนตัวของผู้อื่นไปหาประโยชน์โดยมิชอบ ซึ่งนับว่าเป็นปัญหาที่เกิดจากความก้าวหน้าทางเทคโนโลยีที่รุกราล้ำความเป็นส่วนตัวที่ยากแก่การหลีกเลี่ยงและป้องกัน จากผลกระทบที่เกิดขึ้นทำให้หลายประเทศทั่วโลกเกิดแนวคิดในการให้ความคุ้มครองข้อมูลส่วนบุคคลอย่างจริงจัง ซึ่งการให้ความคุ้มครองของแต่ละประเทศนั้นอาจมีรูปแบบที่แตกต่างกัน หรือวิธีการอื่นๆ เพื่อป้องกันมิให้เกิดการละเมิดข้อมูลส่วนบุคคลหรือนำข้อมูลส่วนบุคคลไปใช้ในทางมิชอบ ดังนั้น ในหลายประเทศจึงตระหนักถึงความสำคัญและความจำเป็นในการตรากฎหมายหรือมีแนวทางเพื่อให้การคุ้มครองสิทธิความเป็นส่วนตัวในข้อมูลข่าวสารส่วนบุคคลของประชาชน ไม่ว่าจะเป็นระดับองค์กรต่างประเทศหรือระดับรัฐก็ตาม เช่น

⁸ กิตติพงศ์ กมลธรรมวงศ์, (2549), “การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย: ปัญหาและแนวทางการแก้ไข,” (นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์), 19.

OECD สหภาพยุโรป สหรัฐอเมริกา หรือแม้แต่ประเทศไทยเองก็ตาม โดยมีเหตุผลสำคัญเพื่อวางหลักประกันในการคุ้มครองข้อมูลส่วนบุคคลอันเป็นสิทธิขั้นพื้นฐานประการหนึ่ง และเพื่อสนับสนุนหรือส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์

การคุ้มครองข้อมูลส่วนบุคคลนั้น หากพิจารณาถึงพัฒนาทางความคิด ก็จะพบว่าได้เติบโตและก้าวหน้า จนได้รับการยอมรับและกลายเป็นหลักกฎหมายสากลซึ่งใช้บังคับกันในระหว่างประเทศมานานแล้ว บทบัญญัติในกฎหมายระหว่างประเทศที่กล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลที่เป็นแม่บทหลักในทางระหว่างประเทศปัจจุบันนั้น อาจกล่าวได้ว่ามีที่มาจาก ปฎิญญาสากลว่าด้วยสิทธิมนุษยชนของสหประชาชาติที่ได้ประกาศไว้เมื่อวันที่ 10 ธันวาคม ค.ศ. 1948 ซึ่งได้กล่าวรับรองไว้ในมาตรา 12⁹ ว่า

“มาตรา 12 บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือจะถูกลบลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการแทรกแซงสิทธิหรือการลบลู่ดังกล่าวนี้”

สิทธิมนุษยชนขั้นพื้นฐานในปฎิญญาสากลฉบับนี้มีความหมายกว้างขวางครอบคลุมถึงสิทธิอื่นๆ ไม่ว่าจะเป็น ความเป็นส่วนตัวในข้อมูลข่าวสารส่วนบุคคล (Information Privacy) ความเป็นส่วนตัวในอาณาเขตหรือสถานที่ของตนเอง (Territorial Privacy) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) ซึ่งความเป็นส่วนตัวเหล่านี้ได้กลายเป็นหลักการพื้นฐานที่ได้รับการยอมรับกันทั่วไป

การพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคลในระบบกฎหมายไทยต้องเริ่มต้นจากการศึกษาวิเคราะห์จากบทบัญญัติของรัฐธรรมนูญเป็นหลัก ในฐานะที่เป็นกฎหมายสูงสุดที่มีความสำคัญในการรับรองและสร้างหลักประกันคุ้มครองไว้ซึ่งสิทธิเสรีภาพของบุคคลต่างๆ ซึ่งข้อมูลส่วนบุคคลนั้นก็ถือเป็นสิทธิเสรีภาพขั้นพื้นฐานประการหนึ่ง เมื่อพิจารณาถึงบทบัญญัติเรื่องการคุ้มครองข้อมูลส่วนบุคคล ภายใต้กรอบความคุ้มครองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ฉบับปัจจุบัน มาตราหลักที่สำคัญปรากฏอยู่ในส่วนที่ 3 ว่าด้วยสิทธิและเสรีภาพส่วนบุคคล มาตรา 35 ซึ่งบัญญัติไว้ว่า

“สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง

การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว จะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

⁹ No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ”

จากบทบัญญัติดังกล่าวจะพบว่ารัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 นั้นได้คุ้มครองข้อมูลส่วนบุคคลไม่ให้ถูกละเมิดไว้ในวรรคท้ายของมาตรา 35 โดยแยกการคุ้มครองข้อมูลส่วนบุคคลออกมาอย่างชัดเจนจากการคุ้มครองสิทธิและเสรีภาพส่วนบุคคลในลักษณะอื่นๆ ซึ่งเป็นการบัญญัติขึ้นเพิ่มเติมจากรัฐธรรมนูญฉบับก่อนๆ ที่ยังมีได้มีการบัญญัติแยกการคุ้มครองข้อมูลส่วนบุคคลออกมาจากสิทธิเสรีภาพอื่นๆ อย่างชัดเจน

2.2 ปัญหาที่เกิดขึ้นเกี่ยวกับความปลอดภัยของข้อมูลส่วนบุคคลในการจัดเก็บคุกกี้บนการดำเนินธุรกรรมอิเล็กทรอนิกส์

คุกกี้นั้นถูกสร้างขึ้นมาเพื่อช่วยอำนวยความสะดวกให้กับผู้ใช้ในการเข้าไปยังเว็บไซต์ที่ชื่นชอบโดยที่ไม่ต้องเสียเวลาในการที่หาสิ่งที่ต้องการทุกครั้งที่ใช้เข้ามาซึ่งจะทำให้เสียเวลาในค้นหาข้อมูลอีกครั้ง เช่นเมื่อผู้ใช้ได้เข้าไปที่เว็บไซต์หนึ่งเป็นครั้งแรก ผู้ใช้อาจจะถูกขอร้องให้ใส่ชื่อ, ข้อมูลส่วนบุคคล หรือข้อมูลเกี่ยวกับการเงินเพื่อเว็บไซต์นั้นจะได้นำมาใช้อีกครั้งเมื่อผู้ใช้เข้ามาที่เว็บไซต์นั้นอีกครั้งในอนาคต โดยที่เว็บไซต์นั้นก็จะทำการสร้างคุกกี้ซึ่งบรรจุข้อมูลเหล่านั้นลงไปบนเครื่องคอมพิวเตอร์ของผู้ใช้ และหากว่าผู้ใช้ได้กลับมาที่เว็บไซต์นั้นอีกก็จะมีการร้องขอข้อมูลเหล่านั้นมาตรวจสอบว่าผู้ใช้เป็นใครและได้รับอนุญาตให้เข้ามาที่เว็บไซต์นั้นหรือไม่ แต่อย่างไรก็ดี คุกกี้เองก็เป็นเทคโนโลยีที่ใช้ในการรุกร้าความเป็นส่วนตัว ซึ่งมีความสามารถที่จะติดตามการใช้อินเทอร์เน็ตของบุคคล โดยเว็บไซต์ส่วนใหญ่มักใช้คุกกี้ ในการติดตามพฤติกรรมการใช้งานอินเทอร์เน็ตของผู้ใช้ และใช้เพื่อเก็บข้อมูลซึ่งผู้ใช้แต่ละบุคคลได้ไว้ในเว็บไซต์ อย่างเช่น ชื่อ, ที่อยู่ หมายเลขบัตรเครดิต และอื่นๆ ทั้งนี้เพื่อนำข้อมูลที่ได้จากคุกกี้ไปใช้ทางการตลาดเพื่อศึกษาพฤติกรรมของผู้บริโภค หรือเพื่อนำเสนอโฆษณาสินค้าที่ตรงกับผู้บริโภค หรือเพื่อนำมาพัฒนาเว็บไซต์ หรือแม้กระทั่งนำข้อมูลที่ได้ดังกล่าวไปขายให้แก่บุคคลที่สาม เป็นต้น

ทั้งนี้ จากรูปแบบการละเมิดข้อมูลส่วนบุคคลข้างต้น จะเห็นได้ว่ารูปแบบในการจัดเก็บข้อมูลนั้น มีทั้งในแบบที่เจ้าของข้อมูลทราบและไม่ทราบ

รูปแบบการจัดเก็บข้อมูลแบบที่เจ้าของข้อมูลทราบนั้น อาจกล่าวได้ว่าเป็นกรณีที่เว็บไซต์แจ้งให้เจ้าของข้อมูลทราบก่อนมีการเก็บรวบรวมข้อมูลผ่านทางหน้าเว็บไซต์ ในรูปแบบของ “นโยบายการคุ้มครองข้อมูลส่วนบุคคล” (Privacy Policy) ยกตัวอย่างเช่น นโยบายความเป็นส่วนตัวของ Google โดย Privacy Policy คือ สิ่งที่บอกให้เหล่าผู้ให้บริการเว็บไซต์ได้ทราบถึงแนวปฏิบัติของเว็บไซต์ต่อข้อมูลส่วนบุคคลของผู้ใช้บริการ ดังนั้น สาระสำคัญที่กำหนดไว้ใน Privacy Policy จึงต้องเป็นสาระสำคัญเกี่ยวกับการดำเนินการใดๆ ของเจ้าของเว็บไซต์ต่อข้อมูลส่วนบุคคลของผู้เข้ามาใช้บริการนั่นเอง

สำหรับรูปแบบการจัดเก็บข้อมูลแบบที่เจ้าของข้อมูลไม่ทราบนั้นจะเป็นกรณีที่เว็บไซต์ต่างๆ ใช้โปรแกรมเพื่อเก็บรวบรวมข้อมูลต่างๆ ของผู้เข้าชมเว็บไซต์ โดยที่ผู้เข้าชมเว็บไซต์หรือเจ้าของ

ข้อมูลนั้นไม่ทราบ โดยโปรแกรมดังกล่าว ได้แก่ คุกกี้ (cookie) ซึ่งเป็นไฟล์ตัวหนังสือขนาดเล็กของ web server ที่ส่งไปตัวอยู่บน hard drive ของคอมพิวเตอร์ของผู้เข้าชมเว็บไซต์ คุกกี้จะเก็บข้อมูลต่างๆ ที่เกิดจากกิจกรรมที่ได้ทำขึ้นบนเว็บไซต์ โดยที่ผู้เข้าชมเว็บไซต์อาจจะทราบหรือไม่ทราบว่ามีการเก็บข้อมูลโดยคุกกี้จากการแจ้งให้ทราบล่วงหน้าถึงนโยบายการใช้คุกกี้ของเว็บไซต์ต่างๆ เช่น นโยบายการใช้คุกกี้ของเว็บไซต์ eBay

โดยส่วนใหญ่เว็บไซต์บนอินเทอร์เน็ต ทั้งที่เป็นเว็บไซต์ e-commerce และไม่ใช่เว็บไซต์ e-commerce ต่างนิยมใช้คุกกี้ในการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้งานเว็บไซต์ดังกล่าว ซึ่งเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์อย่างมาก อย่างคดีที่เกิดขึ้นของเว็บไซต์ชื่อดังในประเทศที่มักถูกฟ้องคดีในเรื่องการใช้คุกกี้เพื่อติดตามพฤติกรรมหรือการใช้งานอินเทอร์เน็ตของลูกค้า ยกตัวอย่างเช่น เว็บไซต์ e-commerce ชื่อดังอย่าง Amazon.com¹⁰ ที่ถูกฟ้องคดีในนามกลุ่มบุคคล ขอให้หลีกเลี่ยงการติดตั้งความเป็นส่วนตัวใน Web-browser ของผู้ใช้ เพื่อเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้ และแชร์ข้อมูลดังกล่าวให้กับบริษัทอื่นๆ

คดีความที่ฟ้องในนามกลุ่มบุคคลของ Amazon.com นั้น กล่าวหาว่าผู้ค้าปลีกออนไลน์ใช้เล่ห์เหลี่ยมหลอกลวงให้ Microsoft's Internet Explorer คิดว่าเว็บไซต์ e-commerce “มีการคุ้มครองความเป็นส่วนตัวมากกว่าความเป็นจริง” และใช้วิธีการอันตรายฉลาด-Flash cookies—เพื่อเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ใช้แม้ว่าพวกเขาจะตั้ง browser เพื่อบล็อกคุกกี้แล้วก็ตาม การฟ้องคดีในนามกลุ่มบุคคลกล่าวหาว่า Amazon ได้จัดเว็บไซต์เพื่อหลอก Internet Explorer และทำให้ลูกค้าหลงผิดในนโยบายความเป็นส่วนตัวของ Amazon ที่เผยแพร่ออนไลน์

“เป็นเวลาหลายปีแล้วที่ Amazon ได้นำข้อมูลส่วนบุคคลของผู้เข้าเยี่ยมชมเว็บไซต์ไปโดยที่ Amazon ไม่มีสิทธิที่จะทำเช่นนั้น Amazon ใช้ซอฟต์แวร์คุ้มครองความเป็นส่วนตัวบนคอมพิวเตอร์ของผู้ใช้งานในทางที่ผิด โดยใช้ซอฟต์แวร์เพื่อวัตถุประสงค์ของ Amazon ในการเก็บรวบรวมข้อมูลส่วนบุคคลมากกว่าที่ Amazon มีสิทธิที่จะทำหรือมากกว่าที่ผู้ใช้งานให้ความยินยอมในการเก็บ” คดีที่ฟ้องในนามกลุ่มบุคคลได้กล่าวไว้

การที่บริษัทหลายบริษัทใช้ Flash cookies เพื่อหลีกเลี่ยงการติดตั้งความเป็นส่วนตัวของผู้ใช้และเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต กลายเป็นรากฐานในการฟ้องร้องในนามกลุ่มบุคคลหลายคดีในช่วงที่ผ่านมา (Interclick Class Action Lawsuit และ Quantcast & Clearspring Class Action Settlement) อย่างไรก็ตาม บริษัทจำนวนมากเหล่านี้เป็นเครือข่ายบริษัทโฆษณา ไม่ใช่เว็บไซต์ e-commerce

¹⁰ Case No. C11-366RSL. NICOLE DEL VECCHIO, et al., V. AMAZON.COM, INC., UNITED STATES DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT SEATTLE, 1st of June, 2012.

“Amazon อ้างไว้ในการแจ้งเตือนล่วงหน้าเรื่องความเป็นส่วนตัวว่า Amazon จะไม่แชร์ข้อมูลของผู้ใช้กับบุคคลที่สามเพื่อวัตถุประสงค์ในการโฆษณา แต่อันที่จริง Amazon เป็นเว็บไซต์ที่ยอมให้มีการโฆษณาของบุคคลที่สามในนามของ Amazon ต่างหาก” การฟ้องคดีในนามกลุ่มบุคคลกล่าว “โดยแท้จริงแล้ว Amazon แชร์ข้อมูลส่วนตัวที่ระบุตัวตนของผู้ใช้กับบุคคลที่สามเพื่อให้บุคคลที่สามสามารถไปใช้งานต่อไปได้และไม่เปิดเผยข้อเท็จจริงนี้กับผู้บริโภค”

คดีที่ฟ้องในนามกลุ่มบุคคล กับ Amazon.com Flash cookie นี่เป็นการฟ้องในนามของผู้ใดก็ตามที่เคยใช้ Internet Explorer เวอร์ชัน 6, 7 หรือ 8—และมีการติดตั้งความเป็นส่วนตัวอย่างสูง—เข้าเยี่ยมชมเว็บไซต์ Amazon.com เพื่อซื้อสินค้าที่นั่น การฟ้องร้องนี้มุ่งหวังจะได้รับคำสั่งศาลเพื่อยุติการนำข้อมูลส่วนบุคคลไปแชร์และเรียกร้องค่าเสียหายที่เป็นตัวเงิน ซึ่งคาดว่าจะมีผู้ใช้ที่เข้าข่ายถูกละเมิดโดย Amazon หลายล้านราย¹¹ หรืออย่างเว็บไซต์สังคมออนไลน์ยอดนิยมอย่าง Facebook¹² โดย Facebook อาจจะกำลังติดตามกิจกรรมออนไลน์ของคุณ แม้ว่า คุณจะออกจากการทำงานในเว็บไซต์เครือข่ายสังคมแล้วก็ตาม นี่เป็นการกล่าวอ้างตามที่มีการฟ้องคดีในนามกลุ่มบุคคลซึ่งยื่นฟ้องโดยสำนักงานทนายความยักษ์ใหญ่ 2 แห่ง

คำฟ้องกล่าวหาว่า Facebook ติดตั้งคุกกี้— (ไฟล์ขนาดเล็กที่อนุญาตให้เว็บไซต์จดจำ preferences ของผู้ใช้, ข้อมูลการใช้อินเทอร์เน็ต และอื่นๆ) บนคอมพิวเตอร์ของผู้ใช้ ซึ่งจะติดตามการใช้อินเทอร์เน็ตของผู้ใช้อย่างต่อเนื่องหลังจากที่พวกเขาได้ออกจาก Facebook แล้ว

นั่นไม่เข้ากันกับเงื่อนไขในการใช้งานของ Facebook ซึ่งได้กล่าวไว้ว่า “เมื่อคุณออกจาก Facebook เราจะลบคุกกี้ซึ่งระบุบัญชีผู้ใช้ของคุณออก” นอกจากนี้ การกระทำของ Facebook อาจฝ่าฝืน Federal Wiretap Act และ Stored Electronic Communications Act ตามคำฟ้องอย่างเป็นทางการอีกด้วย¹³ หรือในเว็บไซต์ชื่อดังอย่าง Google¹⁴ มีการยื่นฟ้องคดีในนามกลุ่มบุคคล กับ Google โดยกล่าวหาว่า Google ได้ใส่ code เข้าไปใน Google Ads ทำให้ Google สามารถติดตั้งคุกกี้ติดตามบน iPhones, iPads และคอมพิวเตอร์ Mac การฟ้องคดีในนามกลุ่มบุคคลของมลรัฐอ้างว่า Google ได้ทำการฝ่าฝืน Wiretap Act, Computer Fraud and Abuse Act และ Stored Electronics Communication Act

¹¹ O'Donnell, M., (2011), *Amazon.com Flash Cookie Class Action Lawsuit*, Retrieved May 26, 2012, from <http://www.topclassactions.com/lawsuit-settlements/lawsuit-news/1061-amazoncom-flash-cookie-class-action-lawsuit->

¹² MDL No.2314 – IN RE: Facebook internet tracking litigation.

¹³ Koebler, J., (2012), *Lawsuit Says Facebook Tracks Users After Logging Out*, Retrieved May 26, 2012, from <http://www.usnews.com/news/articles/2012/02/23/lawsuit-says-facebook-tracks-users-after-logging-out>

¹⁴ MDL No.2358 –IN RE: Google Inc. cookie placement consumer privacy litigation.

คดีนั้นกล่าวหาว่า Google ติดตั้งคุกกี้ติดตามบนสินค้าของ Apple เพื่อที่จะเก็บเกี่ยวข้อมูลเกี่ยวกับการค้นหาอินเทอร์เน็ต และเป็นการกระทำที่ลูกค้าไม่รู้หรือไม่ได้อนุญาต

ผู้นำโจทก์ในคดีกล่าวอ้างเพิ่มเติมว่า Google นั้นเจตนาที่จะดักจับการติดต่อสื่อสารทางอิเล็กทรอนิกส์เหล่านี้และเจตนาเปิดเผยข้อมูลที่ได้มา สร้างความเสียหายต่อตัวเขาและสมาชิกคนอื่นๆ ในกลุ่ม

ตามคดี การกระทำที่ถูกล่ามหาของ Google ถูกพบในเดือนกุมภาพันธ์ เมื่อ the Wall Street Journal รายงานว่า นักวิจัยของมหาวิทยาลัย Stanford ได้ค้นพบว่า Google ใส่ code เข้าไปใน Google Ads เพื่อที่จะหลีกเลี่ยงการติดตั้งความเป็นส่วนตัวของ web browser ของ Apple ซึ่งบล็อกคุกกี้ของบุคคลที่สาม (third-party cookies) บทความนั้นกล่าวว่า Google ติดตั้งคุกกี้บนอุปกรณ์ของ Apple เพื่อที่จะติดตามกิจกรรมการซื้อขายบนอินเทอร์เน็ตของพวกเขา คดีดังกล่าวยังกล่าวอ้างเพิ่มเติมอีกว่า Google ได้ให้คำแนะนำการใช้ browser สำหรับอุปกรณ์ Apple บนเว็บไซต์ของ Google โดยระบุว่า การติดตั้ง browser ตาม default จะบล็อกคุกกี้ของบุคคลที่สามทั้งหมด ตั้งแต่มีบทความของ the Wall Street Journal นี้ออกมา Google จึงได้ลบคำแนะนำดังกล่าวออกจากหน้าเว็บเพจของ Google

“Google ยอมรับว่าใช้ code ที่ออกแบบมาเพื่อให้แน่ใจว่าอุปกรณ์ของ Apple ที่ใช้ browser Safari สามารถเข้าใช้งาน Google ได้ และผลที่ตามมาคือ คุกกี้ติดตามจะถูกติดตั้งบน browser Safari ในอุปกรณ์ของ Apple ด้วย” คดีได้กล่าวไว้โดยคดีดังกล่าวมุ่งหวังที่จะได้รับการชดเชยค่าเสียหายที่แท้จริง, กำไรของ Google หรือค่าชดเชยขั้นต่ำตามกฎหมาย \$1,000 ต่อคน, ค่าเสียหายในเชิงลงโทษ, ค่าทนายความ และค่าฤชาธรรมเนียมศาล¹⁵ เป็นต้น

3. ผลการวิจัย

จากการศึกษาถึงลักษณะ รูปแบบ และวิธีการของการละเมิดข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์ โดยใช้เทคโนโลยี อย่างเช่น คุกกี้ นั้น จะเห็นได้ว่ามีลักษณะรูปแบบ และวิธีการเฉพาะที่แตกต่างจากการละเมิดข้อมูลส่วนบุคคลทั่วไป ข้อแตกต่างที่เห็นได้ชัดคือ ลักษณะของการติดตามพฤติกรรมการใช้งานอินเทอร์เน็ตของผู้บริโภค โดยใช้เทคโนโลยีอย่างคุกกี้เข้ามาช่วยในการเก็บข้อมูล ซึ่งจะไม่พบในการละเมิดข้อมูลส่วนบุคคลที่ไม่อยู่ในระบบคอมพิวเตอร์ เนื่องด้วยเทคโนโลยีที่ทันสมัยทำให้เกิดการติดต่อสื่อสารกันได้อย่างกว้างขวางไร้พรมแดน สามารถติดต่อทำธุรกรรมกันได้จากทุกที่ทั่วทุกมุมโลกด้วยวิธีที่หลากหลาย การละเมิดข้อมูลส่วนบุคคล

¹⁵ Google Facing Wire Tap Class Action over Cookies on Apple Devices, Retrieved May 26, 2012, from <http://www.lawyersandsettlements.com/case/google-wire-tap-class-action-cookies-on-apple.html>.

ในการดำเนินธุรกรรมอิเล็กทรอนิกส์จึงเกิดขึ้นได้ง่าย รวดเร็ว และยากแก่การคุ้มครอง นอกจากนั้น ปัญหาที่เกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ก็ซับซ้อนและมีลักษณะเฉพาะกว่าปัญหาที่เกิดขึ้นกับการละเมิดข้อมูลส่วนบุคคลโดยทั่วไปด้วย

การศึกษานี้จึงเน้นศึกษาถึงกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยที่มีอยู่ในปัจจุบัน กล่าวคือ ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... เปรียบเทียบกับมาตรการทางกฎหมายของสหภาพยุโรป (EU) คือ Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 และมาตรการทางกฎหมายของประเทศสหรัฐอเมริกา คือ The Consumer Privacy Bill of Rights ที่มุ่งเน้นคุ้มครองผู้ใช้บริการ ในการดำเนินธุรกรรมอิเล็กทรอนิกส์โดยเฉพาะ เพื่อเปรียบเทียบให้เห็นถึงข้อแตกต่างและความเหมาะสมในการนำมาปรับใช้ให้สอดคล้องกับลักษณะ รูปแบบ และวิธีการของการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นบนธุรกรรมอิเล็กทรอนิกส์ให้มากที่สุด

3.1 การคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ในกฎหมายต่างประเทศ

3.1.1 มาตรการทางกฎหมายของสหภาพยุโรป (EU)

จากการศึกษามาตรการทางกฎหมายของสหภาพยุโรป (EU) ตาม Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 พบว่ามาตรการดังกล่าวครอบคลุมถึงการใช้คุกกี้และเทคโนโลยีอื่นที่คล้ายกันสำหรับเก็บข้อมูล และการเข้าถึงข้อมูลที่ถูกเก็บไว้บนอุปกรณ์ของผู้ใช้ อย่างเช่น คอมพิวเตอร์หรือมือถือ ข้อบังคับในเรื่องนี้ถูกออกแบบมาเพื่อที่จะคุ้มครองความเป็นส่วนตัวส่วนตัวของผู้ใช้อินเทอร์เน็ต แม้ว่าข้อมูลที่ถูกเก็บไป จะไม่สามารถระบุตัวผู้ใช้ได้ นี่ไม่ใช่ข้อบังคับที่ออกแบบมาเพื่อจำกัดการใช้เทคโนโลยีดังกล่าว แต่ใช้สำหรับป้องกันไม่ให้มีการเก็บข้อมูลบนคอมพิวเตอร์ของผู้ใช้ และป้องกันไม่ให้นำข้อมูลนั้น มาใช้ โดยที่ผู้ใช้ไม่อนุญาตและไม่ยินยอม¹⁶

ตาม Directive มีบทบัญญัติในส่วนที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคลในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ที่สำคัญ ดังนี้

ใน Directive ตามข้อ 5 ได้มีการบัญญัติถึงความปลอดภัยของบริการติดต่อสื่อสารทางอิเล็กทรอนิกส์สาธารณะ โดยกำหนดให้ผู้ให้บริการติดต่อสื่อสารทางอิเล็กทรอนิกส์สาธารณะ (“ผู้ให้บริการ”) จะต้องปฏิบัติตามมาตรการทางเทคนิคและการจัดการที่เหมาะสมเพื่อที่จะปกป้องความปลอดภัยของบริการนั้น ซึ่งมาตรการดังกล่าวที่อ้างถึงนั้น อย่างน้อยที่สุด ต้อง

¹⁶ Information Commissioner's Office (ico.), (2012), *Guidance on the rules on use of cookies and similar technologies*, Retrieved May 26, 2012, from http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/-/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx.

1) ทำให้แน่ใจว่าข้อมูลส่วนบุคคลสามารถเข้าถึงได้เพียงโดยบุคคลที่ได้รับอนุญาตด้วยวัตถุประสงค์ที่ได้รับอำนาจโดยชอบด้วยกฎหมาย ;

2) ปกป้องข้อมูลส่วนบุคคลที่ถูกเก็บหรือส่งผ่านจากความเสียหายโดยไม่ได้ตั้งใจหรือโดยไม่ชอบด้วยกฎหมาย, การสูญหาย หรือการเปลี่ยนแปลงแก้ไขโดยไม่ได้ตั้งใจ และการเก็บข้อมูลโดยไม่ได้รับอนุญาตหรือโดยไม่ชอบด้วยกฎหมาย, การดำเนินการ, การเข้าถึง หรือการเปิดเผย ; และ

3) ทำให้แน่ใจถึงการนำนโยบายความปลอดภัยเกี่ยวกับการจัดการของข้อมูลส่วนบุคคลไปปฏิบัติใช้ให้เกิดผล

ทั้งนี้หากมีการดำเนินการตามมาตรการดังกล่าวแล้ว ยังพบความเสี่ยงต่อความปลอดภัยของบริการติดต่อสื่อสารทางอิเล็กทรอนิกส์สาธารณะ ผู้ให้บริการจะต้องแจ้งให้ผู้รับบริการทราบเกี่ยวกับ

(1) ลักษณะของความเสี่ยงนั้น

(2) มาตรการที่เหมาะสมใดๆ ที่ผู้รับบริการสามารถใช้เพื่อป้องกันความเสี่ยงนั้น และ

(3) ค่าใช้จ่ายที่จะเกิดขึ้นหากผู้รับบริการใช้มาตรการนั้น

ในส่วนของการละเมิดข้อมูลส่วนบุคคลถูกกำหนดไว้ในข้อ 5A ของ Directive นี้ โดยหากมีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ผู้ให้บริการจะต้องแจ้งการละเมิดนั้นต่อกรรมาธิการข้อมูลข่าวสารโดยเร็ว ซึ่งการแจ้งดังกล่าว อย่างน้อยที่สุดจะต้องมีการอธิบายถึง

(1) ลักษณะของการละเมิด

(2) ผลที่ตามมาของการละเมิด ; และ

(3) มาตรการที่ผู้ให้บริการเอามาใช้ หรือเสนอเพื่อที่จะจัดการปัญหาการละเมิดดังกล่าว

และหากการละเมิดข้อมูลส่วนบุคคลดังกล่าวนั้นอาจส่งผลร้ายต่อข้อมูลส่วนบุคคลหรือความเป็นส่วนตัวของผู้รับบริการหรือผู้ใช้ ผู้ให้บริการจะต้องแจ้งการละเมิดนั้นต่อผู้รับบริการหรือผู้ใช้ที่เกี่ยวข้องโดยเร็วโดยการแจ้งดังกล่าวอย่างน้อยที่สุดจะต้องมี

(1) คำอธิบายถึงลักษณะของการละเมิด ;

(2) ข้อมูลเกี่ยวกับผู้ที่ลูกค้าจะติดต่อได้ในองค์กรของผู้ให้บริการ ซึ่งผู้ให้บริการสามารถขอข้อมูลเพิ่มเติมได้ ; และ

(3) การแนะนำมาตรการที่จะช่วยให้ผู้รับบริการลดผลกระทบทางลบของการละเมิดดังกล่าว

ทั้งนี้ อาจไม่จำเป็นต้องมีการแจ้งดังกล่าว ถ้าผู้ให้บริการมีการพิสูจน์จนเป็นที่พอใจแก่กรรมาธิการข้อมูลข่าวสารว่า

(1) ผู้ให้บริการได้ใช้มาตรการป้องกันทางเทคโนโลยีที่เหมาะสม ซึ่งทำให้ผู้ที่ไม่ได้รับอนุญาตไม่สามารถเข้าถึงข้อมูลได้, และ

(2) มาตรการเหล่านั้นถูกใช้กับข้อมูลที่เกี่ยวข้องในการละเมิดนั้น

ในส่วนของการตรวจสอบการละเมิดข้อมูลส่วนบุคคลตาม Directive นี้ นั้น จะปรากฏอยู่ในข้อ 5B ซึ่งให้อำนาจกรรมการข้อมูลข่าวสารในการตรวจสอบการปฏิบัติตามข้อกำหนดในข้อ 5A ของผู้ให้บริการ โดยการบังคับใช้ Directive นี้ถูกบัญญัติไว้ในข้อ 5C ซึ่งให้อำนาจกรรมการข้อมูลข่าวสารในการที่จะลงโทษปรับเป็นจำนวนเงินที่แน่นอน หากผู้ให้บริการไม่ปฏิบัติตามข้อกำหนดแห่งกฎหมายในการแจ้งตามข้อ 5A

บทบัญญัติในเรื่องการรักษาความลับของการติดต่อสื่อสารตาม Directive นี้ปรากฏอยู่ในข้อ 6 โดยกำหนดไว้ว่าบุคคลจะต้องไม่เก็บ หรือเข้าถึงข้อมูลที่เก็บไว้ในเครื่องของผู้รับบริการหรือผู้ใช้ เว้นแต่ผู้รับบริการหรือผู้ใช้เครื่องนั้น

(1) ได้รับข้อมูลเกี่ยวกับวัตถุประสงค์ของการเก็บหรือการเข้าถึงข้อมูลอย่างชัดเจนและครอบคลุม และ

(2) ได้รับความยินยอมจากผู้รับบริการหรือผู้ใช้

โดยมาตรานี้จะไม่นำไปใช้กับการเก็บทางเทคนิค หรือการเข้าถึงข้อมูล

(1) สำหรับวัตถุประสงค์ในการดำเนินการส่งผ่านข้อมูลบนเครือข่ายการติดต่อสื่อสารทางอิเล็กทรอนิกส์เท่านั้น หรือ

(2) ในกรณีที่การเก็บหรือการเข้าถึงข้อมูลจำเป็นอย่างยิ่งในการให้ข้อมูลบริการสังคม ซึ่งถูกร้องขอโดยผู้รับบริการหรือผู้ใช้

ในส่วนที่เกี่ยวข้องกับการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้นั้น ปรากฏอยู่ในข้อ 29A ซึ่งกำหนดให้ ผู้ให้บริการติดต่อสื่อสารต้องสร้างและรักษาขั้นตอนภายในสำหรับตอบสนองต่อคำร้องขอในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้ อีกทั้งผู้ให้บริการติดต่อสื่อสารจะต้องจัดหาข้อมูลตามที่กรรมการข้อมูลข่าวสารร้องขอเกี่ยวกับ

(1) ขั้นตอนเหล่านั้น;

(2) จำนวนของคำร้องขอที่ได้รับ;

(3) การให้เหตุผลที่สอดคล้องกฎหมายสำหรับคำร้องขอ; และ

(4) การตอบสนองต่อคำร้องขอของผู้ให้บริการติดต่อสื่อสาร

3.1.2 มาตรการทางกฎหมายของประเทศสหรัฐอเมริกา

เมื่อพิจารณาถึงระบบการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในประเทศสหรัฐอเมริกานั้น จะเห็นได้ว่ามีลักษณะเฉพาะสำคัญที่เป็นระบบกฎหมายเฉพาะเรื่อง (Sectoral laws) ประเทศสหรัฐอเมริกาไม่มีกฎหมายแม่บทหรือกฎหมายกลางวางหลักเกณฑ์เป็นการทั่วไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ระบบการคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาจึงมีบทบัญญัติที่ใช้คุ้มครองความเป็นส่วนตัวที่แยกเป็นส่วนๆ กล่าวคือ การคุ้มครองความเป็นส่วนตัวจะกระจัดกระจายอยู่ในบทบัญญัติ กฎเกณฑ์ ข้อบังคับหลายๆ ฉบับที่จำกัดเฉพาะเรื่องที่บทบัญญัตินั้นมีวัตถุประสงค์มุ่งคุ้มครอง ในขณะที่ EU ใช้ระบบที่ใช้กฎหมายแม่บทเป็นกฎหมายกลางในการให้ความคุ้มครองข้อมูลส่วนบุคคล

ทั้งนี้เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาที่มีจำนวนมากมายหลายฉบับตามแต่ลักษณะของข้อมูลส่วนบุคคลนั้น ดังนั้นในการวิจัยนี้จึงขอเสนอเฉพาะหลักการสำคัญที่ปรากฏใน The Computer Fraud and Abuse Act (1994) (CFAA) และ Electronic Communications Privacy Act of 1986 (ECPA) ซึ่งเป็นกฎหมายในระดับสหพันธรัฐ และ The Consumer Privacy Bill of Rights

โดยรายละเอียดสำคัญของ The Consumer Privacy Bill of Rights และกฎหมายทั้งสองฉบับมีดังต่อไปนี้

– The Computer Fraud and Abuse Act (1994) (CFAA)

18 USC § 1030–Fraud and related activity in connection with computers

18 USC § 1030–FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS ว่าด้วยการฉ้อฉลและกิจกรรมที่เกี่ยวข้องกับคอมพิวเตอร์

Computer Fraud and Abuse Act (“CFAA”)

CFAA (18 U.S.C. § 1030) เป็นกฎหมายอาญาของประเทศสหรัฐอเมริกาที่เกี่ยวข้องกับคอมพิวเตอร์ โดยห้ามการบุกรุกคอมพิวเตอร์ ซึ่งส่วนใหญ่แล้วมักเกี่ยวข้องกับการเข้าถึงคอมพิวเตอร์ “โดยไม่ได้รับอนุญาต” หรือ “เกินกว่าที่ได้รับอนุญาต” รวมทั้งผลที่ตามมา อย่างเช่น ได้รับข้อมูลส่วนบุคคลหรือเป็นเหตุให้เกิดความเสียหาย CFAA เป็นบทบัญญัติที่รับมือกับการแฮกคอมพิวเตอร์ ความเสียหายหรือความสูญเสียที่บุคคลได้รับจากการกระทำที่ถูกล่ามโซ่ อาจฟ้องร้องเป็นคดีได้ ถ้าการกระทำผิดตามที่กล่าวหาเป็นสาเหตุให้เกิด “ความสูญเสียแก่บุคคลหนึ่งหรือมากกว่าในช่วงระยะเวลา 1 ปี มีผลรวมมูลค่าอย่างน้อยที่สุด \$5,000” การเยียวยาภายใต้ CFAA ถูก “จำกัดเพียงค่าเสียหายทางเศรษฐกิจ” และการบรรเทาทุกข์อย่างยุติธรรม

– Electronic Communications Privacy Act of 1986 (ECPA)

Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§ 2510–22) หรือที่รู้จักกันในชื่อ Wiretap Act กล่าวถึงบทบัญญัติสำหรับการเข้าถึง, การใช้, การเปิดเผย, การดักจับ และการคุ้มครองความเป็นส่วนตัวของการติดต่อสื่อสารทางอิเล็กทรอนิกส์ กฎหมายนี้ประกาศใช้ในปี ค.ศ. 1986 และครอบคลุมรูปแบบที่หลากหลายในการติดต่อสื่อสารทั้งโดยใช้สายและทางอิเล็กทรอนิกส์ ตามกฎหมายอเมริกา “การสื่อสารทางอิเล็กทรอนิกส์” หมายถึง การส่งผ่านสัญลักษณ์, สัญญาณ, ตัวอักษร, รูปภาพ, เสียง, ข้อมูล หรือข่าวกรองในลักษณะใดก็ตามที่มีการส่งผ่านทั้งหมดหรือบางส่วนโดยสาย, วิทยุ, แม่เหล็กไฟฟ้า, รูปภาพอิเล็กทรอนิกส์ หรือระบบรูปภาพทางสายตา ซึ่งส่งผลกระทบต่อการค้าระหว่างมลรัฐหรือต่างประเทศ” ECPA ห้ามการเข้าถึงและการเปิดเผย content ในการติดต่อสื่อสาร โดยไม่ชอบด้วยกฎหมาย นอกจากนั้น กฎหมายยังห้ามไม่ให้รัฐบาลร้องขอให้ผู้ให้บริการเปิดเผยการติดต่อสื่อสารทางอิเล็กทรอนิกส์โดยปราศจากกระบวนการที่เหมาะสม

– Consumer Privacy Bill of Rights 2012

The Consumer Privacy Bill of Right ถูกเสนอขึ้นโดยรัฐบาลของบารัค โอบามา ในเดือนมกราคม ปี ค.ศ. 2012 โดยสิทธิดังกล่าวนี้ให้ความเข้าใจที่ชัดเจนแก่ผู้บริโภค ในการจัดการกับข้อมูลส่วนบุคคลของพวกเขา และในขณะเดียวกันก็กำหนดหลักการสำหรับบริษัท ในการใช้ข้อมูลส่วนบุคคล

The Consumer Privacy Bill of Right (บทบัญญัติว่าด้วยสิทธิพื้นฐานของพลเมือง เกี่ยวกับความเป็นส่วนตัวของผู้บริโภค) นั้นมีหลักการซึ่งอธิบายได้พอสังเขป ดังนี้

The Consumer Privacy Bill of Rights นั้นนำไปใช้บังคับกับข้อมูลส่วนบุคคล ซึ่งหมายถึง ข้อมูลใดๆ ก็ตาม และการรวบรวมข้อมูลที่เกี่ยวข้องกับข้อมูลของแต่ละบุคคล ข้อมูลส่วนบุคคล อาจรวมถึงข้อมูลในคอมพิวเตอร์หรืออุปกรณ์อื่นๆ ของบุคคล รัฐบาลสนับสนุนการออกกฎหมาย ของสหพันธรัฐที่ยึดหลักการ The Consumer Privacy Bill of Rights แม้ว่าจะไม่มีการออกกฎหมาย รัฐบาลก็ใช้กระบวนการที่คำนึงถึงผู้มีส่วนได้ส่วนเสียทั้งหมด ซึ่งยึดสิทธิในเรื่องข้อมูลส่วนบุคคลนี้ เป็นแม่แบบของจรรยาบรรณ จรรยาบรรณนี้ถูกบังคับใช้โดยคณะกรรมการการค้าของสหพันธรัฐ องค์ประกอบเหล่านี้ ได้แก่ The Consumer Privacy Bill of Rights จรรยาบรรณ และการบังคับ ใช้ที่เคร่งครัดจะช่วยเพิ่มความสามารถในการทำงานร่วมกันระหว่างกฎหมายคุ้มครองข้อมูล ส่วนบุคคลของสหรัฐอเมริกาและกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศคู่ค้า

1) การควบคุมของแต่ละบุคคล : ผู้บริโภคมีสิทธิที่จะควบคุมข้อมูลส่วนบุคคลที่บริษัท เก็บรวบรวมจากพวกเขาและควบคุมวิธีการใช้ข้อมูลนั้น บริษัทควรจะให้บุคคลสามารถควบคุม ข้อมูลส่วนตัวที่ผู้บริโภคได้แชร์ให้กับผู้อื่นได้ และรวมไปถึงวิธีการที่บริษัทจัดเก็บข้อมูล, นำไปใช้ หรือเปิดเผยข้อมูลส่วนบุคคล บริษัทควรเปิดโอกาสให้บุคคลเข้าถึงทางเลือกดังกล่าวข้างต้น โดยจัดกลไกที่ใช้งานและเข้าถึงได้ง่ายให้กับผู้บริโภค กลไกนี้จะต้องแสดงระดับ, ขอบเขต และ ความอ่อนไหวของข้อมูลส่วนบุคคลที่พวกเขาเก็บรวบรวม, นำไปใช้ หรือเปิดเผย เช่นเดียว กับ ความอ่อนไหวของการนำข้อมูลส่วนบุคคลไปใช้ บริษัทควรเสนอทางเลือกที่ชัดเจนและเข้าใจง่าย ไม่ซับซ้อนให้กับผู้บริโภค ทั้งนี้ต้องเสนอทางเลือกบ่อยครั้ง ด้วยวิธีการที่เป็นประโยชน์ต่อการตัดสินใจ ของผู้บริโภคในเรื่องการเก็บรวบรวมข้อมูลส่วนบุคคล, การนำไปใช้ และการเปิดเผย บริษัทควรให้ ผู้บริโภคสามารถถอนคืนหรือจำกัดความยินยอม โดยวิธีการถอนคืนหรือจำกัดความยินยอม ต้องเข้าถึงได้ง่ายและสะดวกเหมือนวิธีการให้ความยินยอมในครั้งแรก

2) ความโปร่งใส : ผู้บริโภคมีสิทธิที่จะได้รับข้อมูลเกี่ยวกับความเป็นส่วนตัวและวิธีปฏิบัติ เพื่อความปลอดภัยที่สามารถเข้าใจและเข้าถึงได้โดยง่าย บริษัทควรให้คำอธิบายที่ชัดเจนว่าข้อมูล ส่วนตัวอะไรบ้างที่พวกเขาเก็บรวบรวม, ทำไมพวกเขาถึงต้องการข้อมูลเหล่านั้น, พวกเขาจะนำ ข้อมูลนั้นไปใช้อย่างไร, เมื่อไหร่ที่พวกเขาจะลบข้อมูลหรือยุติการใช้ข้อมูลนั้น และทำไมพวกเขา ถึงแชร์ข้อมูลส่วนบุคคลดังกล่าวให้แก่บุคคลที่สาม ทั้งนี้ คำอธิบายเหล่านี้จะต้องถูกนำเสนอให้กับ ผู้บริโภคในพื้นที่และเวลาที่เป็นประโยชน์มากที่สุดในการที่ผู้บริโภคจะทำความเข้าใจเกี่ยวกับ ความเสี่ยงในการเผยแพร่ข้อมูลส่วนบุคคล และความสามารถในการควบคุมของแต่ละบุคคล

3) การให้ความเคารพต่อบริบท : ผู้บริโภคมีสิทธิที่จะคาดหวังให้บริษัทเก็บรวบรวม, นำไปใช้และเปิดเผยข้อมูลส่วนบุคคลด้วยวิธีการที่สอดคล้องกับบริบทที่ผู้บริโภคได้ให้ข้อมูลนั้นไป บริษัทควรจำกัดการใช้และการเปิดเผยข้อมูลส่วนบุคคลให้อยู่ภายใต้วัตถุประสงค์ที่สอดคล้องกับความสัมพันธ์ระหว่างบริษัทกับผู้บริโภค และบริบทแรกเริ่มที่ผู้บริโภคเปิดเผยข้อมูลนั้น เว้นแต่กฎหมายจะกำหนดไว้เป็นอย่างอื่น ถ้าบริษัทจะใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นๆ พวกเขาควร会增加 “ความโปร่งใส” และ “การควบคุมของแต่ละบุคคล” ให้สูงขึ้นโดยแจ้งวัตถุประสงค์อื่นนั้นให้เห็นได้เด่นชัดและง่ายต่อการดำเนินการของผู้บริโภคให้แจ้งขณะที่มีการเก็บรวบรวมข้อมูล ถ้าหลังจากที่บริษัทเก็บรวบรวมข้อมูลส่วนบุคคลแล้ว บริษัทตัดสินใจที่จะใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่ไม่สอดคล้องกับบริบทในตอนแรกที่ข้อมูลถูกเก็บ พวกเขาต้องจัดมาตรการด้าน “ความโปร่งใส” และ “ทางเลือกของแต่ละบุคคล” ให้มีความเข้มงวดมากยิ่งขึ้น อายุและความชำนาญด้านเทคโนโลยีของผู้บริโภคเป็นองค์ประกอบสำคัญของบริบท บริษัทควรปฏิบัติตามหน้าที่ภายใต้หลักการนี้ในแนวทางที่เหมาะสมกับอายุและความชำนาญด้านเทคโนโลยีของผู้บริโภค โดยเฉพาะ หลักการใน The Consumer Privacy Bill of Rights ให้ความสำคัญเป็นพิเศษกับการป้องกันข้อมูลส่วนบุคคลที่ได้รับจากเด็กและวัยรุ่นมากกว่าผู้ใหญ่

4) ความปลอดภัย : ผู้บริโภคมีสิทธิที่จะได้รับการจัดการข้อมูลส่วนบุคคลที่ปลอดภัยและมีความรับผิดชอบ บริษัทควรประเมินความเป็นส่วนตัวและความเสี่ยงด้านความปลอดภัยไปพร้อมกับวิธีปฏิบัติในการจัดการข้อมูลของบริษัท โดยต้องมีมาตรการที่เหมาะสมในการควบคุมความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลส่วนบุคคลของผู้บริโภค อย่างเช่น การสูญหาย, การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต, การใช้, การทำลาย หรือการแก้ไขเปลี่ยนแปลง และการเปิดเผยที่ไม่เหมาะสม

5) การเข้าถึงและความแม่นยำ : ผู้บริโภคมีสิทธิที่จะเข้าถึงและแก้ไขข้อมูลส่วนบุคคลในรูปแบบที่ใช้งานง่าย และด้วยวิธีการที่เหมาะสมกับความอ่อนไหวของข้อมูล และความเสี่ยงต่อผลกระทบด้านลบต่อผู้บริโภคในกรณีที่ข้อมูลนั้นไม่ถูกต้องหรือคลาดเคลื่อน บริษัทควรมีมาตรการที่เหมาะสมเพื่อให้สามารถมั่นใจได้ว่าบริษัทได้เก็บข้อมูลส่วนบุคคลที่ถูกต้องแม่นยำ บริษัทควรให้ผู้บริโภคสามารถเข้าถึงข้อมูลส่วนบุคคลที่บริษัทได้เก็บรวบรวม และให้ผู้บริโภคสามารถแก้ไขข้อมูลที่ผิด, ลบข้อมูล หรือจำกัดการใช้ข้อมูลได้ บริษัทที่จัดการข้อมูลส่วนบุคคลควรตีความหลักการข้อนี้ไปในทางที่สอดคล้องกับเสรีภาพในการแสดงออกและเสรีภาพสื่อในการที่จะพิจารณาว่าควรใช้มาตรการใดเพื่อรักษาความถูกต้องแม่นยำของข้อมูล และเพื่อให้ผู้บริโภคเข้าถึงข้อมูล, สามารถที่จะแก้ไข, ลบข้อมูล หรือจำกัดการใช้ข้อมูล บริษัทอาจพิจารณาจากระดับ, ขอบเขต และความอ่อนไหวของข้อมูลส่วนบุคคลที่พวกเขาเก็บรวบรวมไว้ และความเป็นไปได้ที่ว่าการใช้ข้อมูลนั้นอาจทำให้เกิดความเสียหายต่อทรัพย์สิน, ร่างกาย หรือความเสียหายอื่นๆ

6) การเก็บรวบรวมที่เฉพาะเจาะจง : ผู้บริโภคมีสิทธิที่จะจำกัดข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวม บริษัทควรเก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะที่ต้องใช้ เพื่อให้บรรลุวัตถุประสงค์

ตามที่ระบุไว้ภายใต้หลักการ “การให้ความเคารพต่อสิทธิ” เท่านั้น บริษัทควรกำจัดหรือยุติการใช้ข้อมูลทันทีที่บริษัทไม่ต้องใช้ข้อมูลนั้นอีกต่อไป เว้นเสียแต่ว่ากฎหมายจะบัญญัติหน้าที่ไว้เป็นอย่างอื่น ไมเช่นนั้น บริษัทควรเปิดเผยอย่างปลอดภัยและระบุตัวข้อมูลส่วนบุคคลครั้งหนึ่งที่พวกเขาไม่ต้องการมันอีกต่อไป

7) ความรับผิดชอบ : ผู้บริโภคมีสิทธิที่จะให้บริษัทจัดการข้อมูลส่วนบุคคลโดยมาตรการที่เหมาะสมเพื่อให้มั่นใจได้ว่าบริษัทนั้นปฏิบัติตาม The Consumer Privacy Bill of Rights บริษัทควรให้ผู้บริโภคและหน่วยงานที่กำกับดูแลบังคับใช้กฎหมายสามารถตรวจสอบบริษัทได้ว่าบริษัทได้ปฏิบัติตามหลักการเหล่านี้หรือไม่ นอกจากนี้บริษัทควรจะควบคุมดูแลลูกจ้างให้ปฏิบัติตามหลักการเหล่านี้เช่นกัน เพื่อให้บรรลุวัตถุประสงค์ดังกล่าว บริษัทควรฝึกอบรมพนักงานเพื่อให้สามารถจัดการกับข้อมูลส่วนบุคคลได้อย่างเหมาะสมและสอดคล้องกันกับหลักการนี้ และต้องประเมินผลการดำเนินงานในด้านนี้เป็นประจำในโอกาสอันเหมาะสม บริษัทควรจัดการให้มีการตรวจสอบในทุกๆ ด้าน บริษัทที่เปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลที่สาม อย่างน้อยที่สุดควรทำให้มั่นใจได้ว่าบุคคลที่สามนั้นอยู่ภายใต้บังคับความรับผิดชอบตามสัญญาซึ่งยึดตามหลักการนี้ เว้นแต่กฎหมายจะกำหนดไว้เป็นอย่างอื่น

8) ทั้งนี้ เมื่อพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ของประเทศไทย เปรียบเทียบกับมาตรการทางกฎหมายในต่างประเทศ กล่าวคือ ตามมาตรการทางกฎหมายของสหภาพยุโรป (EU) คือ Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 และมาตรการคุ้มครองข้อมูลส่วนบุคคลออนไลน์ในประเทศสหรัฐอเมริกา คือ The Consumer Privacy Bill of Rights จะเห็นได้ว่ามีประเด็นให้นำมาวิเคราะห์อยู่ 5 ประเด็น ดังนี้

8.1) การบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์

ประเด็นหลักประเด็นแรกจะเห็นได้ว่าการคุ้มครองข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ของประเทศไทยนั้น เป็นการบัญญัติการคุ้มครองข้อมูลส่วนบุคคลในฐานะเป็นกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลทั่วไป โดยไม่ได้จำแนกประเภทของการจัดเก็บข้อมูล ซึ่งต่างจากมาตรการทางกฎหมายในต่างประเทศที่จะแยกประเภทของการคุ้มครองข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์ออกมาจากบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลในลักษณะอื่นอย่างชัดเจน อย่างเช่นตามมาตรการทางกฎหมายของสหภาพยุโรป (EU) คือ Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 ที่บัญญัติถึงการคุ้มครองข้อมูลส่วนบุคคลในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ และตาม The Consumer Privacy Bill of Rights ซึ่งเป็นมาตรการหลักในการคุ้มครองข้อมูลส่วนบุคคลออนไลน์ในประเทศสหรัฐอเมริกา ซึ่งนั่นทำให้ข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ได้รับการคุ้มครองโดยมีหลักการที่ชัดเจนและครอบคลุมเฉพาะเรื่องสำหรับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยนั้นจะเห็นได้ว่าไม่ได้บัญญัติ

แยกประเภทของการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ออกมาจากการคุ้มครองข้อมูลส่วนบุคคลในลักษณะอื่นๆ โดยรวมเข้าไว้เป็นกฎหมายกลางฉบับเดียว คือ ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้น ย่อมส่งผลให้มาตรการทางกฎหมายที่จะนำไปใช้เพื่อคุ้มครองข้อมูลส่วนบุคคลนั้นไม่สอดคล้องกับรูปแบบ ลักษณะ และวิธีการของการละเมิดข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์ซึ่งแตกต่างไปจากการละเมิดข้อมูลส่วนบุคคลที่ถูกจัดเก็บในลักษณะอื่น และย่อมส่งผลไปถึงการกำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการเก็บรวบรวมและดูแลข้อมูลส่วนบุคคล

8.2) การให้ความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ประเด็นในเรื่องนี้นั้นเมื่อศึกษาตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย จะพบว่าในบางมาตรา อย่างเช่นมาตรา 23, มาตรา 25, มาตรา 26, มาตรา 28, มาตรา 30 และมาตรา 31 ได้บัญญัติถึง “การได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล” ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งเมื่อพิจารณาเปรียบเทียบกับมาตรการทางกฎหมายในต่างประเทศดังกล่าวแล้วจะเห็นได้ว่าการบัญญัติถึง การได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลไว้เช่นเดียวกัน แต่ได้บัญญัติไว้ในลักษณะของ “การได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล” ดังนั้น ในประเด็นนี้จึงทำให้เห็นถึงปัญหาในการบังคับใช้กับกรณีของการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ เนื่องจากการได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลนั้น หากเป็นการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ซึ่งเกิดขึ้นในระบบคอมพิวเตอร์ หรือการติดต่อสื่อสารทางอิเล็กทรอนิกส์แล้ว ผู้ควบคุมข้อมูลส่วนบุคคลจะขอความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคลได้อย่างไร หรือหากเป็นการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลบนหน้าเว็บเพจ จะถือว่าเป็นการได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคลหรือไม่ ซึ่งยังเป็นปัญหาที่คลุมเครือและต้องมีการตีความอยู่

8.3) การแจ้งต่อเจ้าของข้อมูลส่วนบุคคลถึงการเก็บรวบรวมข้อมูล

ในประเด็นนี้จากการศึกษาจะพบว่าตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ในร่างมาตรา 16 ได้กำหนดถึงรายละเอียดที่ต้องแจ้งให้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่จะดำเนินการเก็บรวบรวม ซึ่งรายละเอียดดังกล่าวประกอบไปด้วย

- 1) ชื่อ สถานที่ทำการ และสถานภาพของผู้ควบคุมข้อมูลส่วนบุคคลว่าเป็นบุคคลหรือนิติบุคคล และเป็นผู้ควบคุมข้อมูลส่วนบุคคลเชิงธุรกิจหรือการพาณิชย์ ตามมาตรา 34 หรือไม่
 - 2) วัตถุประสงค์ของการเก็บรวบรวมตามหลักเกณฑ์และวิธีการที่กำหนดไว้ในมาตรา 18
 - 3) ประเภทของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมว่าเป็นข้อมูลส่วนบุคคลตามมาตรา 23 หรือไม่
 - 4) กำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล
 - 5) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 41
- รายละเอียดอื่นตามที่คณะกรรมการประกาศกำหนด

ทั้งนี้ เมื่อพิจารณาเปรียบเทียบกับ Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 และ The Consumer Privacy Bill of Rights จะพบว่ามาตรการทางกฎหมายในต่างประเทศดังกล่าวนี้มีประเด็นการแจ้งแก่เจ้าของข้อมูล ที่เพิ่มเติมจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย โดยได้กำหนดให้ผู้ควบคุม ข้อมูลส่วนบุคคลต้องแจ้งแก่เจ้าของข้อมูลว่าข้อมูลส่วนบุคคลอะไรบ้างที่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องการเก็บรวบรวม รวมทั้งแจ้งถึงการแชร์ข้อมูลดังกล่าวให้แก่บุคคลที่สามด้วยว่ามีหรือไม่อย่างไร ซึ่งหากพิจารณาตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแล้วก็จะพบว่าไม่ได้มีการบัญญัติ ถึงการแจ้งเกี่ยวกับการแชร์ข้อมูลดังกล่าวให้แก่บุคคลที่สามด้วยว่ามีหรือไม่อย่างไร และในประเด็น เรื่องประเภทของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมนั้นตามร่างพระราชบัญญัติดังกล่าว ในมาตรา 16 (3) ได้กล่าวถึง การแจ้งถึงประเภทของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมว่าเป็น ข้อมูลส่วนบุคคลตามมาตรา 23 หรือไม่ ซึ่งไม่ชัดเจนว่าหากมิใช่ข้อมูลส่วนบุคคลตามมาตรา 23 (ข้อมูลที่มีความอ่อนไหว) แล้ว ผู้ควบคุมข้อมูลส่วนบุคคลนั้นจำเป็นต้องแจ้งแก่เจ้าของข้อมูลหรือไม่ว่าพวกเขาจะทำการเก็บรวบรวมข้อมูลส่วนตัวอะไรของเจ้าของข้อมูลบ้าง

8.4 มาตรการในการคุ้มครองข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์

จากการศึกษาถึงมาตรการในการคุ้มครองข้อมูลส่วนบุคคลในการดำเนินธุรกรรม อิเล็กทรอนิกส์ของประเทศไทยตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 32 นั้นพบว่ามาตราดังกล่าวได้มีการกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีระบบรักษา ความมั่นคงปลอดภัยให้แก่ข้อมูลส่วนบุคคล ซึ่งโดยหลักการตามร่างดังกล่าวสอดคล้องกับกฎหมาย คุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปและสหรัฐอเมริกา แต่ในประเด็นเรื่องการวางหลักเกณฑ์ ในการรักษาความมั่นคงปลอดภัยที่ระบุถึง

1) การเข้าถึงและการใช้งานสารสนเทศ อุปกรณ์ ระบบ และสถานที่

2) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพ พร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการ ทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

8.5 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

จะเห็นได้ว่ายังอธิบายไม่ชัดเจนว่าหลักเกณฑ์ในการรักษาความมั่นคงปลอดภัยตามร่าง พระราชบัญญัตินี้จะสามารถสร้างความมั่นใจในการรักษาความมั่นคงปลอดภัยของข้อมูล ส่วนบุคคลให้กับผู้ใช้งานได้อย่างไร โดยเมื่อเปรียบเทียบกับ Privacy and Electronic Communi- cations (EC Directive) (Amendment) Regulations 2011 ในข้อ 5 แล้วจะพบว่าได้มีการวาง หลักเกณฑ์มาตรการในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่ชัดเจน โดยกำหนดให้ผู้ให้ บริการติดต่อสื่อสารทางอิเล็กทรอนิกส์สาธารณะ (“ผู้ให้บริการ”) จะต้องมีการวาง มาตรการทางเทคนิค และการจัดการที่เหมาะสมเพื่อที่จะปกป้องความปลอดภัยของบริการนั้นซึ่งมาตราดังกล่าว ที่อ้างถึงนั้น อย่างน้อยที่สุดต้อง

1) ทำให้แน่ใจว่าข้อมูลส่วนบุคคลสามารถเข้าถึงได้เพียงโดยบุคคลที่ได้รับอนุญาต ด้วยวัตถุประสงค์ที่ได้รับอำนาจโดยชอบด้วยกฎหมาย ;

2) ปกป้องข้อมูลส่วนบุคคลที่ถูกเก็บหรือส่งผ่านจากความเสียหายโดยไม่ได้ตั้งใจหรือโดยไม่ชอบด้วยกฎหมาย, การสูญหาย หรือการเปลี่ยนแปลงแก้ไขโดยไม่ได้ตั้งใจ และการเก็บข้อมูลโดยไม่ได้รับอนุญาตหรือโดยไม่ชอบด้วยกฎหมาย, การดำเนินการ, การเข้าถึง หรือการเปิดเผย; และ

3) ทำให้แน่ใจถึงการนำนโยบายความปลอดภัยเกี่ยวกับการจัดการของข้อมูลส่วนบุคคลไปปฏิบัติให้เกิดผล

4. บทสรุปและข้อเสนอแนะ

4.1 บทสรุป

จากการวิเคราะห์กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... เปรียบเทียบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (EU) และสหรัฐอเมริกา อาจสรุปข้อวิเคราะห์ออกมาได้ดังนี้

ประเด็นแรก เรื่องการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลบนรัฐธรรมนูญอิเล็กทรอนิกส์ โดยตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยไม่ได้มีการแยกประเภทของการคุ้มครองข้อมูลส่วนบุคคลบนรัฐธรรมนูญอิเล็กทรอนิกส์ออกจากการคุ้มครองข้อมูลส่วนบุคคลโดยทั่วไปดังเช่นอย่างในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและสหรัฐอเมริกา ซึ่งแม้ว่าโดยหลักการแล้วการคุ้มครองข้อมูลส่วนบุคคลบนรัฐธรรมนูญอิเล็กทรอนิกส์จะไม่แตกต่างจากการคุ้มครองข้อมูลส่วนบุคคลโดยทั่วไปก็ตาม แต่ด้วยลักษณะ รูปแบบ และวิธีการในการละเมิดข้อมูลส่วนบุคคลบนรัฐธรรมนูญอิเล็กทรอนิกส์ที่มีความซับซ้อนและแตกต่างไปจากการละเมิดข้อมูลส่วนบุคคลในลักษณะทั่วไป จึงเห็นได้ว่ามาตรการทางกฎหมายของสหภาพยุโรปและสหรัฐอเมริกาในการคุ้มครองข้อมูลส่วนบุคคลบนการดำเนินธุรกรรมอิเล็กทรอนิกส์จะกำหนดหน้าที่ให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลบนรัฐธรรมนูญอิเล็กทรอนิกส์มากกว่าผู้ควบคุมข้อมูลส่วนบุคคลโดยทั่วไป

ประเด็นที่สอง เรื่องการให้ความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในประเด็นนี้จะเห็นได้ว่าตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของ泰นั้นได้มีการกล่าวถึง “การได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล” ในขณะที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและสหรัฐอเมริกา บัญญัติถึง “การได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล” เท่านั้น ด้วยเหตุนี้จึงอาจเกิดปัญหาในการตีความคำว่า “การได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล” ในการดำเนินธุรกรรมอิเล็กทรอนิกส์ว่า การได้รับความยินยอมแบบใดจึงจะเรียกได้ว่าเป็นการได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล

ประเด็นที่สาม เรื่องการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลถึงการเก็บรวบรวมข้อมูล ในประเด็นนี้จะเห็นได้ว่าตามกฎหมายข้อมูลส่วนบุคคลส่วนบุคคลของสหภาพยุโรปและสหรัฐอเมริกาได้กำหนดให้มีการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับเรื่องของข้อมูลส่วนบุคคลอะไรบ้างที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องการเก็บรวบรวม และการแชร์ข้อมูลดังกล่าวให้แก่บุคคลที่สามด้วยว่ามีหรือไม่อย่างไร แต่สำหรับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยนั้นไม่ได้มีบทบัญญัติให้แจ้งแก่เจ้าของข้อมูลส่วนบุคคลในประเด็นดังกล่าวด้วย

ประเด็นที่สี่ เรื่องมาตรการในการคุ้มครองข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์ในประเด็นนี้จะพบว่าแม้ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยจะมีหลักการในการรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและสหรัฐอเมริกาก็ตาม แต่ในประเด็นเรื่องการวางหลักเกณฑ์ในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลนั้นจะเห็นได้ว่าหลักเกณฑ์ดังกล่าวไม่สามารถอธิบายให้เห็นได้ว่าจะสามารถรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลส่วนบุคคลได้อย่างไร

โดยสรุปแล้วผลการวิจัยจากการศึกษาค้นคว้าและการวิเคราะห์ข้อมูลในบทต่างๆ ก่อนหน้านี้สามารถตอบปัญหาของการวิจัยทั้ง 3 ข้อได้ดังนี้

1) การใช้โปรแกรมคุกกี้นั้นในระบบคอมพิวเตอร์นั้นเป็นเทคโนโลยีที่เข้ามาช่วยในการเก็บรวบรวมข้อมูล ซึ่งสามารถเก็บข้อมูลได้อย่างมหาศาลและต่อเนื่องโดยที่บางครั้งเจ้าของข้อมูลส่วนบุคคลยังไม่ทันรู้ตัวด้วยซ้ำ ซึ่งนั่นย่อมส่งผลกระทบต่อความปลอดภัยของข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์ ด้วยเหตุที่ข้อมูลส่วนบุคคลเหล่านั้นอาจถูกนำไปใช้โดยที่ไม่ได้รับอนุญาตจากเจ้าของข้อมูลส่วนบุคคลและโดยที่เจ้าของข้อมูลส่วนบุคคลไม่รู้ตัว

2) การละเมิดข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์ โดยการใช้เทคโนโลยีอย่างคุกกี้มีรูปแบบ วิธีการ และลักษณะเฉพาะที่แตกต่างไปจากการละเมิดข้อมูลส่วนบุคคลทั่วไป ที่เห็นได้ชัดเจนคือในเรื่องของการติดตามพฤติกรรมการใช้งานอินเทอร์เน็ตของผู้บริโภค โดยการใช้เทคโนโลยีอย่างคุกกี้เข้ามาช่วยในการเก็บข้อมูล ซึ่งลักษณะเช่นนี้จะไม่พบในการละเมิดข้อมูลส่วนบุคคลทั่วไป การใช้โปรแกรมคุกกี้นี้จึงทำให้เกิดปัญหาสู่ความเสี่ยงในเรื่องการละเมิดข้อมูลส่วนบุคคลในการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ ด้วยลักษณะเฉพาะของการละเมิดข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ที่แตกต่างไปจากการการละเมิดข้อมูลส่วนบุคคลทั่วไปในรูปแบบเดิม ส่งผลให้ปัญหาที่เกิดจากการละเมิดข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์มีความแตกต่างและซับซ้อนกว่าปัญหาที่เกิดกับการละเมิดข้อมูลส่วนบุคคลโดยทั่วไป ด้วยเหตุนี้การคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ในการทำธุรกรรมอิเล็กทรอนิกส์จึงย่อมมีความแตกต่างจากการคุ้มครองข้อมูลส่วนบุคคลทั่วไป

3) เมื่อเทคโนโลยีคอมพิวเตอร์ได้เข้ามาเป็นส่วนหนึ่งในชีวิตประจำวันของคนทั่วโลก มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์นั้น

จึงเป็นส่วนสำคัญในการสร้างความเชื่อมั่นของผู้บริโภคในการทำธุรกรรมทางอิเล็กทรอนิกส์ และภาพรวมในการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย โดยเมื่อวิเคราะห์กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... เปรียบเทียบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (EU) และสหรัฐอเมริกาแล้วจะพบว่ากฎหมายของไทยยังไม่มีกรอบการประกอบและการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ นอกจากการคุ้มครองข้อมูลส่วนบุคคลโดยทั่วไป ซึ่งทำให้เกิดความไม่ชัดเจนในการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ เนื่องจากบทบัญญัติในกฎหมายไทยจะบัญญัติในลักษณะกว้างๆ เพื่อคุ้มครองข้อมูลส่วนบุคคลทั่วไป ไม่เจาะประเด็นให้ครอบคลุมไปถึงการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ ซึ่งทำให้เกิดปัญหาในการตีความและการบังคับใช้กฎหมายตามมาด้วย

4.2 ข้อเสนอแนะ

จากการศึกษาผู้วิจัยเห็นว่า ยังคงมีประเด็นที่ควรแก้ไขร่างกฎหมายดังกล่าวให้สมบูรณ์ขึ้น เพื่อให้เกิดการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ได้อย่างสมบูรณ์ ดังนี้

1) เนื่องด้วยความก้าวหน้าเทคโนโลยีในการเก็บรวบรวมข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์นั้นมีการพัฒนาอย่างต่อเนื่องอยู่ตลอดเวลา และมีวิธีการหรือรูปแบบในการละเมิดข้อมูลส่วนบุคคลที่มีลักษณะเฉพาะ ข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในระบบคอมพิวเตอร์นั้นจึงย่อมมีความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลได้ง่าย ไม่ว่าจะเป็นการสูญหาย การถูกแก้ไขเปลี่ยนแปลง การดักจับข้อมูล การเข้าถึงข้อมูล การแชร์ข้อมูลไปยังบุคคลที่สาม ซึ่งสามารถทำได้อย่างรวดเร็วและง่ายดายมากกว่าข้อมูลที่ถูกจัดเก็บในรูปแบบอื่น และการติดตามพฤติกรรมของผู้บริโภค ซึ่งจะไม่ปรากฏในการละเมิดข้อมูลส่วนบุคคลที่ถูกจัดเก็บในรูปแบบอื่น การรักษาความปลอดภัยของข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์จึงเป็นสิ่งสำคัญ ดังนั้นในประเด็นเรื่องการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์จึงเห็นควรที่จะให้มีการแยกประเภทของการคุ้มครองข้อมูลส่วนบุคคลในการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ออกมาต่างหากจากบทบัญญัติการคุ้มครองข้อมูลส่วนบุคคลในลักษณะอื่นๆ โดยหากเป็นกรณีของข้อมูลส่วนบุคคลในการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ก็ควรมีข้อบังคับหรือกฎเกณฑ์เพิ่มเติมพิเศษในการคุ้มครองไว้ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

2) ในประเด็นเรื่องการให้ความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ที่บัญญัติถึง “การได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล” ดังกล่าว ในประเด็นปัญหานี้เห็นควรที่จะบัญญัติโดยใช้คำว่า “ความยินยอม” อย่างในมาตรการทางกฎหมายของต่างประเทศ เพื่อไม่ให้เกิดปัญหาในทางปฏิบัติหรือการตีความและสามารถนำไปปฏิบัติใช้ได้จริง

3) ในประเด็นเรื่องการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลถึงการเก็บรวบรวมข้อมูล เห็นว่าควรกำหนดหลักเกณฑ์ในการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลเพิ่มเติมในประเด็นเรื่องข้อมูลส่วนบุคคลอะไรบ้างที่ผู้ควบคุมข้อมูลส่วนบุคคลจะดำเนินการเก็บรวบรวม และประเด็นในเรื่องของการแชร์ข้อมูลดังกล่าวให้แก่บุคคลที่สามด้วยว่ามีหรือไม่อย่างไร

4) ในประเด็นเรื่องมาตรการในการคุ้มครองข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์นั้น เห็นควรจะต้องกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ในการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ มีมาตรการทางเทคนิคและการจัดการที่เหมาะสมและสูงกว่ามาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในรูปแบบอื่นเพื่อที่จะปกป้องความปลอดภัยของข้อมูลส่วนบุคคลนั้นจากเทคโนโลยีการละเมิดข้อมูลส่วนบุคคลในระบบคอมพิวเตอร์ ซึ่งมาตรการดังกล่าวอย่างน้อยที่สุดต้องทำให้แน่ใจว่าข้อมูลส่วนบุคคลสามารถเข้าถึงได้เพียงโดยบุคคลที่ได้รับอนุญาตป้องกันข้อมูลส่วนบุคคลจากการสูญหาย ทำลาย หรือเปลี่ยนแปลงแก้ไข และต้องทำให้เจ้าของข้อมูลส่วนบุคคลแน่ใจถึงการนำนโยบายความปลอดภัยเกี่ยวกับการจัดการของข้อมูลส่วนบุคคลไปปฏิบัติใช้ให้เกิดผล โดยควรกำหนดเป็นหลักเกณฑ์ที่ชัดเจนและสามารถนำไปปฏิบัติได้จริง

บรรณานุกรม

- กิตติพงศ์ กมลธรรมวงศ์. (2549). “การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข.” วิทยานิพนธ์ปริญญาโทมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.
- นาวิก นำเสียง. (2549). **ความเป็นส่วนตัวบนโลกอินเทอร์เน็ต**. สืบค้นเมื่อ 17 เมษายน 2555, จาก http://www.navik.net/articles_contents.php?id=42&cs=2&ca=7&do=.
- ปกรณ์ มงคลประสิทธิ์. (2551). “การคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลในการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ : กรณีศึกษาตามร่างพระราชบัญญัติข้อมูลส่วนบุคคล.” วิทยานิพนธ์ปริญญาโทมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง.
- วิชานันต์ ดัชชานนท์, วิวัฒน์พงศ์ พรหมโยธา และ ศตวรรษ กาสะลง. (ม.ป.ป.). **COMPUTER SECURITY**. สืบค้นเมื่อ 21 มีนาคม 2555, จาก <http://std.kku.ac.th/4830205646/COMPUTER%20SECURITY2.pdf>.
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (ม.ป.ป.). **การซื้อสินค้าออนไลน์ ข้อมูลส่วนตัวนั้นสำคัญไฉน**. สืบค้นเมื่อ 22 มีนาคม 2555, จาก <http://www.etda.or.th/main/contents/display/244>.
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (ม.ป.ป.). **Security Tips**. สืบค้นเมื่อ 20 เมษายน 2555, จาก <http://www.etda.or.th/main/contents/display/61>.
- สุชินทร์ ฬิรายันนท์. (2550). “การกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล.” วิทยานิพนธ์วิชาเอกนโยบายสาธารณะ มหาวิทยาลัยศรีนครินทรวิโรฒ.
- Debussere, F. (2005). **The EU E-Privacy Directive : A Monstrous Attempt to Starve the Cookie Monster?**. Retrieved April 16, 2012, from <https://www.law.kuleuven.be/icri/publications/657FredericDebussereCookies.pdf>.
- DoubleClick, Inc. (n.d.). **Privacy Litigation**. Retrieved April 17, 2012, from <http://cyber.law.harvard.edu/is02/readings/doubleclick.html>.
- O'Donnell, M. (2011). **Amazon.com Flash Cookie Class Action Lawsuit**. Retrieved May 26, 2012, from <http://www.topclassactions.com/lawsuit-settlements/lawsuit-news/1061-amazoncom-flash-cookie-class-action-lawsuit->.
- Eckler, M. (2011). **An Introduction to Flash Cookies; How to Manage Them**. Retrieved April 12, 2012, from <http://www.practicalecommerce.com/articles/2653-An-Introduction-to-Flash-Cookies-How-to-Manage-Them>.
- Google Facing Wire Tap Class Action over Cookies on Apple Devices. (n.d.). Retrieved

- May 26, 2012, from <http://www.lawyersandsettlements.com/case/google-wire-tap-class-action-cookies-on-apple.html>.
- Greeley, B. (2012). **The Consumer Privacy Bill of Right : Are We the Consumers, Or Are We the Product?**. Retrieved April 20, 2012, from <http://www.businessweek.com/articles/2012-02-23/the-consumer-privacy-bill-of-rights-are-we-the-consumers-or-are-we-the-product>.
- Information Commissioner's Office (ico.). (2012). **Guidance on the rules on use of cookies and similar technologies**. Retrieved May 28, 2012, from http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/~media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx.
- Koebler, J. (2012). **Lawsuit Says Facebook Tracks Users After Logging Out**. Retrieved May 26, 2012, from <http://www.usnews.com/news/articles/2012/02/23/lawsuit-says-facebook-tracks-users-after-logging-out>.
- Persistent Cookie Description**. (n.d.). Retrieved April 14, 2012, from <http://www.cookiecontroller.com/persistent-cookie.html>.
- Session Cookies and what is a session cookies used**. (n.d.). Retrieved April 14, 2012, from <http://www.cookiecontroller.com/session-cookie.html>.
- Super Cookie Description**. (n.d.). Retrieved April 14, 2012, from <http://www.cookiecontroller.com/super-cookie.html>.
- Third Party Cookie Description**. (n.d.). Retrieved April 14, 2012, from <http://www.cookiecontroller.com/third-party-cookie.html>.
- Tirtea, R., Castelluccia, C., and Ikonomou, D. (2011). **Bittersweet cookies. Some security and privacy considerations**. Retrived April 16, 2012, from <http://www.enisa.europa.eu/activities/identity-and-trust/library/pp/cookies>.
- What are Cookies and what is a Cookie used for**. (n.d.). Retrieved April 14, 2012, from <http://www.cookiecontroller.com/what-are-cookies.html>
- Zombie Cookie Description**. (n.d.). Retrieved April 14, 2012, from <http://www.cookiecontroller.com/zombie-cookie.html>.