บทที่ 2
วิวัฒนาการ และแนวคิดพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคล ของเด็กจากการใช้งานบนเครือข่ายอินเตอร์เน็ต

การคุ้มครองข้อมูลส่วนบุคคลของเด็กมีวัตถุประสงค์ของความคุ้มครองแบ่งได้เป็น 2 ด้าน ด้านหนึ่งเป็นการคุ้มครองสิทธิในข้อมูลส่วนบุคคล ซึ่งจัดได้ว่าเป็นวัตถุแห่งสิทธิในความเป็นส่วนตัวและอีกด้านหนึ่งเป็นการคุ้มครองเด็กซึ่งยอมรับกันเป็นสากลว่าเป็นผู้ซึ่งยังอ่อนด้อยทั้งด้านร่างกายและจิตใจ ประกอบกับวุฒิภาวะและประสบการณ์ที่ยังไม่เพียงพอทำให้การตัดสินใจไม่อาจกระทำได้อย่างผู้ใหญ่และตกเป็นเหยื่อของการถูกหลอกลวงหรือเอาเปรียบได้ง่าย แนวคิดและความคุ้มครองในอดีตนั้นมีวิวัฒนาการความคุ้มครองทั้ง 2 ด้าน แยกออกจากกันก่อนจะมีการผสานวิวัฒนาการความคุ้มครองทั้ง 2 ด้านเข้าด้วยกันในเวลาต่อมาโดยมีปัจจัยการพัฒนาระบบคอมพิวเตอร์ เทคโนโลยีสารสนเทศและเครือข่ายอินเตอร์เน็ตเป็นตัวเร่งให้เกิดการผสานของวิวัฒนาการความคุ้มครองทั้ง 2 ด้าน ให้ไปด้วยกันอย่างชัดเจนในการศึกษาถึงมาตรการของการคุ้มครองข้อมูลส่วนบุคคลของเด็กจากการใช้งานบนเครือข่ายอินเตอร์เน็ต จึงจำเป็นต้องมีความเข้าใจถึงลักษณะการทำงานและวิวัฒนาการของเครือข่ายอินเตอร์เน็ตและพื้นฐานแนวความคิดของสิทธิความเป็นส่วนตัวกับการคุ้มครองข้อมูลส่วนบุคคล กับแนวความคิดในเรื่องการคุ้มครองเด็กทั้งในระดับสากลและที่เกิดขึ้นภายในประเทศไทย เพื่อให้เข้าใจถึงความเป็นมาและแนวโน้มการพัฒนาต่อไปในอนาคต

2.1 วิวัฒนาการของการใช้งานเครือข่ายอินเตอร์เน็ต

การพัฒนาทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศทำให้เกิดวิวัฒนาการของเทคโนโลยีการสื่อสารเชื่อมโยงเครือข่ายของผู้ใช้คอมพิวเตอร์ซึ่งอยู่คนละแห่งผ่านระบบการสื่อสารที่เรียกว่าระบบอินเตอร์เน็ต

อินเตอร์เน็ตมีลักษณะเป็นเครือข่ายขนาดใหญ่ที่เชื่อมโยงกลุ่มเครือข่ายคอมพิวเตอร์ขนาดเล็กหลาย ๆ กลุ่มเข้าด้วยกัน จึงอาจกล่าวได้ว่าอินเตอร์เน็ตนั้นเป็นเครือข่ายขนาดใหญ่ของกลุ่มเครือข่ายท้องที่ (Local Area Networks) หลายกลุ่มที่มีอยู่ทั่วทุกแห่ง เครือข่ายบางกลุ่มมีลักษณะปิดไม่ได้เชื่อมโยงกับคอมพิวเตอร์หรือเครือข่ายอื่น อย่างไรก็ตามหลายเครือข่ายมีการ

เชื่อมโยงกันเพื่อให้คอมพิวเตอร์แต่ละเครื่องสามารถที่จะเชื่อมโยงกับเครือข่ายต่าง ๆ เพื่อสื่อสารไปยังคอมพิวเตอร์ในเครือข่ายอื่นจนเกิดเป็นโครงข่ายไปทั่วโลก[1]

อินเตอร์เน็ตเป็นสื่อกลางในการสื่อสารที่มีลักษณะระหว่างประเทศเป็นสื่อกลางที่เปิดให้ประชาชนทั่วไปสามารถเข้าสู่ระบบอินเตอร์เน็ตเพื่อสื่อสารแลกเปลี่ยนข้อมูลซึ่งกันและกัน โดยการสื่อสารดังกล่าวอาจเกิดขึ้นในลักษณะทันทีและสามารถเชื่อมโยงไปยังบุคคลใดบุคคลหนึ่งโดยเฉพาะเจาะจงหรือกลุ่มบุคคลในวงกว้างที่มีความสนใจในเรื่องใดเรื่องหนึ่งหรือไปยังทุกคนทั่วโลกก็ได้[2]

วิวัฒนาการของอินเตอร์เน็ตเริ่มต้นขึ้นในช่วงยุคปี ค.ศ. 1960-1969 โดยมีการพัฒนาให้คอมพิวเตอร์สามารถใช้แบ่งปันข้อมูลจากการค้นคว้าวิจัยทางวิทยาศาสตร์และทางการทหาร ในปี ค.ศ. 1962 นักวิทยาศาสตร์ของสถาบัน MIT เริ่มใช้ระบบเครือข่ายคอมพิวเตอร์ในครั้งแรก และถูกพัฒนาต่อไปโดยหน่วยงานวิจัยเพื่อป้องกันประเทศของสหรัฐอเมริกา (Defense Advanced Research Projects Agency หรือ DARPA) ในช่วงปลายปีเดียวกันมีการพัฒนาระบบอินเตอร์เน็ตเพื่อใช้เครือข่ายสื่อสารแพคเกตสวิตช์ซิ่ง (Packet Switching) เป็นพื้นฐานการทำงานของการเชื่อมโยงทางอินเตอร์เน็ต ในปี ค.ศ. 1965 มีการเชื่อมโยงคอมพิวเตอร์ระหว่างรัฐแมสซาชูเซทส์และคอมพิวเตอร์ของมลรัฐแคลิฟอร์เนียเป็นครั้งแรกโดยผ่านทางสายโทรศัพท์ซึ่งแสดงให้เห็นถึงความเป็นไปได้ในการเชื่อมโยงกันในวงกว้าง ต่อมามีการเปลี่ยนแปลงชื่อของหน่วยงาน DARPA เป็นหน่วยงานชื่อ Advanced Research Projects Agency หรือ ARPA และมีการทำสัญญากับเอกชนเพื่อพัฒนาระบบเครือข่ายสำหรับการเชื่อมโยงของหน่วยงานดังกล่าว ทำให้อินเตอร์เน็ตถูกรู้จักมากขึ้นในชื่อว่า ARPANET[3]

ระบบ ARPANET ถูกใช้ครั้งแรกในปี ค.ศ. 1969 โดย ARPA เสนอให้จัดทำสัญญาเพื่อเชื่อมโยงระบบคอมพิวเตอร์ของมหาวิทยาลัยในเขตตะวันตกเฉียงใต้ของมหาวิทยาลัย 4 แห่ง ได้แก่ มหาวิทยาลัยแห่งมลรัฐแคลิฟอร์เนีย (ลอสแองเจลิส) สถาบันวิจัยสแตนฟอร์ด มหาวิทยาลัยแห่งมลรัฐแคลิฟอร์เนีย (ซานตาบาบารา) และมหาวิทยาลัยแห่งมลรัฐยูท่าห์ หลังจากนั้นจึงเพิ่มเติมสถาบันวิจัยและมหาวิทยาลัยอื่นอีกหลายแห่งในเวลาต่อมา รวมทั้งองค์การวิจัย NASA ซึ่งเข้าร่วมในเดือนกุมภาพันธ์ ค.ศ. 1971 จนเกิดเป็นระบบเครือข่าย ARPANET[4] ในปี ค.ศ. 1981 มีจำนวน

---

[1] คำอธิบายความหมายของอินเตอร์เน็ตในคดี ACLU v Reno 929F Supp 824, 830-845 (ED Pa 1996).

[2] แหล่งเดิม.

[3] Walt Howe. (n.d.). *An anecdotal history of the people and communities that brought about the Internet and the Web.* Retrieved January 25, 2015, from http://www.walthowe.com/navnet/history.html

[4] แหล่งเดิม.

คอมพิวเตอร์ไม่ถึง 300 เครื่อง เชื่อมโยงอยู่ในอินเตอร์เน็ต แต่มีการขยายเพิ่มเติมจนกระทั่งในปี ค.ศ. 1993 มีคอมพิวเตอร์มากกว่า 1 ล้านเครื่องที่เชื่อมโยงกัน คอมพิวเตอร์บางเครื่องหรือบางเครือข่ายมีรัฐบาลหรือสถาบันของรัฐเป็นผู้ใช้งาน บางส่วนใช้งานโดยกลุ่มองค์กรการกุศล และอีกจำนวนมากใช้งานโดยเอกชน การใช้งานอินเตอร์เน็ตโดยภาพรวมในลักษณะเช่นนี้จึงก่อให้เกิดสื่อกลางในการสื่อสารของโลกหรือที่เรียกว่าโลกไซเบอร์ (Cyberspace) ซึ่งเชื่อมโยงประชาชน สถาบัน บริษัทและรัฐบาลทั่วโลกเข้าด้วยกัน

ในช่วงกลางของทศวรรษที่ 1990 อินเตอร์เน็ตมีผลกระทบต่อการค้าและวัฒนธรรมเป็นอย่างมากรวมทั้งการเกิดขึ้นของระบบสื่อสารแบบเกือบจะทันที เช่น ไปรษณีย์อิเล็กทรอนิกส์ (Electronic Mail) การส่งข้อความ (Instant Messaging) ระบบโทรศัพท์ผ่านอินเตอร์เน็ต (Voice over Internet Protocol (VoIP) ระบบวีดีโอคอลและระบบโครงข่าย World Wide Web ซึ่งส่งผลให้เกิดเวทีสำหรับการสนทนาแลกเปลี่ยน เกิดเว็บไซต์ที่ให้บริการบันทึกข้อมูลส่วนตัว (Blog) เกิดเครือข่ายทางสังคม (Social Networking) เว็บไซต์สำหรับการเลือกซื้อสินค้าและบริการ (Online Shopping Sites)

การใช้งานเครือข่ายอินเตอร์เน็ตนั้น บุคคลทั่วไปสามารถเข้าสู่โลกไซเบอร์ได้โดยการใช้คอมพิวเตอร์ที่มีการเชื่อมโยงเครือข่ายอินเตอร์เน็ตโดยตรงเพื่อเชื่อมต่อกับระบบเครือข่ายอินเตอร์เน็ตหรืออาจใช้คอมพิวเตอร์ประกอบกับอุปกรณ์เชื่อมต่อที่เรียกว่า “โมเด็ม (Modem)” เพื่อเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ขนาดใหญ่ก่อนจะเข้าสู่ระบบอินเตอร์เน็ต[5] จนกระทั่งในปัจจุบันมีการพัฒนาให้การส่งข้อมูลสามารถทำได้ด้วยการส่งผ่านระบบบอร์ดแบนด์ ผ่านสายเคเบิลรูปแบบต่าง ๆ ไม่ว่าจะเป็นสายแบบ Coaxial Cable แบบ Fiber Optic หรือแบบ Copper Wires เพื่อให้การส่งผ่านข้อมูลสามารถทำได้รวดเร็วมากยิ่งขึ้น และพัฒนาต่อมาเป็นระบบ Wi-Fi ระบบดาวเทียม และผ่านเทคโนโลยีโทรศัพท์เคลื่อนที่ 3G/4G”[6]

สำหรับประเทศไทยนั้นอินเตอร์เน็ตเริ่มขึ้นเมื่อปี พ.ศ. 2530 โดยการเชื่อมต่อมินิคอมพิวเตอร์ของมหาวิทยาลัยสงขลานครินทร์และสถาบันเทคโนโลยีแห่งเอเชีย (AIT) ไปยังมหาวิทยาลัยเมลเบิร์น ประเทศออสเตรเลีย แต่ในครั้งนั้นยังเป็นการเชื่อมต่อโดยผ่านสายโทรศัพท์ซึ่งสามารถส่งข้อมูลได้ช้าและเป็นการชั่วคราวเท่านั้น จนกระทั่งในปี พ.ศ. 2535 ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ได้ทำการเชื่อมต่อคอมพิวเตอร์กับมหาวิทยาลัย 6 แห่ง ได้แก่ จุฬาลงกรณ์มหาวิทยาลัย สถาบันเทคโนโลยีแห่งเอเชีย (AIT)

---

[5] คำอธิบายความหมายของอินเตอร์เน็ตในคดี ACLU v Reno.

[6] Wikipedia. (n.d.). *Internet.* Retrieved January 25, 2015, from http://en.wikipedia.org/wiki/Internet

มหาวิทยาลัยสงขลานครินทร์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) มหาวิทยาลัยธรรมศาสตร์ และมหาวิทยาลัยเกษตรศาสตร์ เข้าด้วยกันเรียกว่า “เครือข่ายไทยสาร”

การให้บริการอินเตอร์เน็ตในประเทศไทยได้เริ่มต้นขึ้นเป็นครั้งแรกเมื่อเดือนมีนาคม พ.ศ. 2538 โดยความร่วมมือของรัฐวิสาหกิจ 3 แห่ง คือ การสื่อสารแห่งประเทศไทย องค์การโทรศัพท์แห่งประเทศไทยและสำนักงานส่งเสริมวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) โดยให้บริการในนามบริษัท อินเทอร์เน็ต ประเทศไทย จำกัด (หรือ INET) ซึ่งถือเป็นผู้ให้บริการอินเตอร์เน็ตเชิงพาณิชย์รายแรกของประเทศไทย”[7]

สภาพสังคมที่เปลี่ยนแปลงไปจากการใช้งานอินเตอร์เน็ต

การขยายตัวของเครือข่ายอินเตอร์เน็ต ส่งผลให้เกิดการค้าการพาณิชย์ผ่านเครือข่ายอินเตอร์เน็ต ไม่ว่าจะเป็นการซื้อขายสินค้าหรือบริการก็ตาม อย่างไรก็ดีการพาณิชย์อิเล็กทรอนิกส์นั้นไม่ได้เจาะจงเฉพาะเรื่องของการซื้อขายเท่านั้น แต่หมายความรวมไปถึงกระบวนการพัฒนาการตลาด การขาย การส่ง การให้บริการ และการชำระราคาสำหรับสินค้าและบริการ

แต่เดิมนั้นการพาณิชย์อิเล็กทรอนิกส์หมายความถึงกระบวนการที่จะอำนวยให้ธุรกรรมการค้าทางอิเล็กทรอนิกส์เกิดขึ้นได้ เช่น การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic Data Interchange หรือ EDI) และการโอนเงินทางอิเล็กทรอนิกส์ (Electronic Funds Transfer หรือ EFI) เป็นต้น กระบวนการดังกล่าวถูกใช้ครั้งแรกในช่วงปลายของทศวรรษที่ 1970 เพื่อใช้ในการส่งเอกสารทางการค้าจำพวกใบสั่งซื้อหรือ Invoice ทางอิเล็กทรอนิกส์เป็นหลัก แต่เมื่อมีการใช้งานบัตรเครดิต การใช้เครื่องเบิกถอนเงินสดอัตโนมัติ (ATM) และการใช้บริการธนาคารผ่านทางโทรศัพท์ (Mobile Banking) มากขึ้นในช่วงทศวรรษที่ 1980 ระบบการธนาคารทางอิเล็กทรอนิกส์จึงกลายมาเป็นส่วนหนึ่งของระบบการพาณิชย์อิเล็กทรอนิกส์เช่นกัน[8]

อย่างไรก็ดีในปี ค.ศ. 1990 เมื่อมีการพัฒนาเว็บไซต์และระบบ World Wide Web สำหรับการเชื่อมโยงข้อมูลต่าง ๆ ในช่วงแรก National Science Foundation (NSF) ซึ่งเป็นหน่วยงานกลางของสหรัฐอเมริกาห้ามใช้เครือข่ายดังกล่าวเพื่อการค้าจนกระทั่งปี ค.ศ. 1995 จึงมีการเปิดให้ใช้เพื่อวัตถุประสงค์ทางการค้าได้ แต่ยังจำเป็นต้องมีการพัฒนาระบบความปลอดภัยในการใช้งานอินเตอร์เน็ตอีกประมาณ 4 ปี จนกระทั่งในปี ค.ศ. 2000 บริษัทในทวีปยุโรปและทวีปอเมริกาจำนวนมากเสนอบริการผ่านทางเครือข่าย World Wide Web นับแต่นั้นเป็นต้นมา

---

[7] วิกิพิเดีย. (ม.ป.ป.). *อินเทอร์เน็ต*. สืบค้น 25 มกราคม 2558, จาก http://th.wikipedia.org/wiki/อินเทอร์เน็ต

[8] Wikipidia. (n.d.). *Electronic Commerce.* Retrieved January 25, 2015, from http://en.wikipedia.org/wiki/E_commerce สืบค้นเมื่อวันที่ 25 มกราคม 2558

คนทั่วไปจึงเริ่มรู้จักความหมายของคำว่า “การพาณิชย์อิเล็กทรอนิกส์ (E-commerce)” ซึ่งหมายถึงความสามารถในการซื้อสินค้าผ่านทางอินเตอร์เน็ตโดยใช้ระบบการเก็บรักษาความปลอดภัย (Secure Protocols) และบริการชำระเงินทางอิเล็กทรอนิกส์[9]

อินเตอร์เน็ตก่อให้เกิดการปฏิสัมพันธ์และกิจกรรมทางสังคมในวงกว้างไม่ว่าจะเป็นเว็บไซต์เครือข่ายสังคมออนไลน์ที่เปิดโอกาสให้ผู้ใช้งานสามารถเพิ่มเติมข้อมูลต่าง ๆ อีกทั้งยังสามารถค้นหาข้อมูลต่าง ๆ และสามารถที่จะสื่อสารกันระหว่างกลุ่มบุคคลได้ นอกจากนี้ เว็บไซต์บางแห่งยังสนับสนุนการสร้างเครือข่ายทางการค้าและธุรกิจ บางเว็บไซต์เปิดให้มีการสร้างและรวบรวมวีดีโอและรูปภาพของผู้ใช้งานได้

การใช้งานเครือข่ายอินเตอร์เน็ตก่อให้เกิดปัญหาและความกังวลเกี่ยวกับความเป็นส่วนตัวและข้อมูลส่วนบุคคล รวมทั้งการเผยแพร่งานอันมีลิขสิทธิ์ของผู้อื่นซึ่งแตกต่างไปจากเดิมอย่างมาก รวมทั้งยังมีการใช้อินเตอร์เน็ตเป็นเครื่องมือในทางการเมืองไม่ว่าจะในเชิงสร้างสรรค์อย่างการรวบรวมสิ่งของรับบริจาคหรือการแจ้งข้อมูลข่าวสารสำคัญ หรือในเชิงทำลายสังคมอย่างการสร้างความขัดแย้งในกลุ่มเชื้อชาติศาสนา อันนำไปสู่ความพยายามที่จะตรวจสอบและป้องกันรัฐบาลบางประเทศอย่างสาธารณรัฐอิสลามอิหร่าน สาธารณรัฐประชาธิปไตยประชาชนเกาหลี (เกาหลีเหนือ) สาธารณรัฐประชาชนจีน หรือราชอาณาจักรซาอุดีอาระเบีย ห้ามประชาชนมิให้ใช้งานอินเตอร์เน็ตในส่วนที่มีเนื้อหาเกี่ยวกับศาสนาและการเมือง[10] บางประเทศอย่างในสาธารณรัฐแห่งสหภาพเมียนมาร์ในอดีตก็เคยห้ามประชาชนครอบครองเครื่องคอมพิวเตอร์ที่มีการเชื่อมต่อกับเครือข่ายอินเตอร์เน็ต[11] ในประเทศแถบสแกนดิเนเวีย ผู้ประกอบการอินเตอร์เน็ตสมัครใจที่จะจำกัดการเข้าถึงเว็บไซต์ที่หน่วยงานที่เกี่ยวข้องระบุไว้ เพื่อหลีกเลี่ยงการออกกฎหมายควบคุมการใช้งาน ซึ่งเว็บไซต์ส่วนใหญ่ที่มีการจำกัดนั้นเป็นเว็บไซต์ที่เกี่ยวข้องกับภาพลามกของเด็ก แต่หลายประเทศก็มีการออกกฎหมายที่เกี่ยวข้องในเรื่องนี้โดยตรงอย่างในสหรัฐอเมริกาที่ห้ามการครอบครองหรือทำให้แพร่หลายซึ่งสื่อบางประเภทรวมทั้งภาพลามกของเด็กผ่านทางอินเตอร์เน็ต[12]

ลักษณะพิเศษของอินเตอร์เน็ตที่ไม่มีพรมแดน ไม่จำเป็นต้องเปิดเผยตัวตนของผู้ใช้งานก่อให้เกิดปัญหาในการควบคุมดูแลการใช้งานมากยิ่งขึ้น นอกเหนือจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มีรูปแบบพิเศษจากการใช้คอมพิวเตอร์แล้ว รูปแบบอาชญากรรมหรือการเอารัดเอา

---

[9] Ibid.

[10] Wikipedia. (n.d.). *Internet.* Retrieved January 25, 2015, from http://en.wikipedia.org/wiki/Internet.

[11] John T. Soma, Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?, Harvard Journal on Legislation, Summer, 1997, 34 Harv. J. on Legis. 317, at 353.

[12] Wikipedia. (n.d.). *Internet.* Retrieved January 25, 2015, from http://en.wikipedia.org/wiki/Internet

เปรียบที่เคยมีอยู่ในอดีตก็สามารถทำได้ง่ายขึ้นเมื่อมีการใช้งานอินเตอร์เน็ต ในบางประเทศจึงมีความพยายามที่จะออกกฎหมายควบคุมกิจกรรมที่เกี่ยวข้องกับพาณิชย์อิเล็กทรอนิกส์หรือการใช้งานอินเตอร์เน็ต รวมถึงการคุ้มครองผู้ใช้งานซึ่งต้องเปิดเผยข้อมูลส่วนบุคคลมิให้มีการนำข้อมูลเช่นว่านั้นไปใช้หรือเปิดเผยในทางที่มิชอบ

2.2 วิวัฒนาการของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ

กฎหมายที่เกี่ยวข้องกับการคุ้มครองสิทธิในความเป็นส่วนตัว (Privacy) นั้นเป็นหลักการสากลที่ใช้บังคับในทุกประเทศทั่วโลก โดยมีกฎหมายที่เกี่ยวข้องหลายฉบับซึ่งมีวัตถุประสงค์แตกต่างกันไป บางฉบับต้องการแก้ไขปัญหาความไม่เป็นธรรมของการใช้อำนาจอันไม่ชอบด้วยกฎหมาย เช่น การจับ การค้น หรือการเฝ้าสังเกตการณ์ เป็นต้น ในขณะที่บางฉบับก็ต้องการสนับสนุนให้เกิดการพาณิชย์อิเล็กทรอนิกส์ที่มีความน่าเชื่อถือมากยิ่งขึ้นและบางฉบับก็เพื่อให้เป็นไปตามพันธะผูกพันตามสนธิสัญญาระหว่างประเทศและเพื่อให้การค้าระหว่างประเทศนั้นสามารถดำเนินไปได้ โดยข้อมูลส่วนบุคคล (Personal Data) นั้น จัดได้ว่าเป็นวัตถุแห่งสิทธิชนิดหนึ่งที่รวมอยู่ในสิทธิในความเป็นส่วนตัว (Rights of Privacy)[13] โดยมีแนวคิดสำคัญให้ผู้เป็นเจ้าของข้อมูลนั้นมีอำนาจในการควบคุมจัดการข้อมูลของตนเองได้

แนวความคิดพื้นฐานเรื่องสิทธิความเป็นส่วนตัว (Privacy Rights) ในความเป็นอยู่ในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นส่วนตัวของบุคคล เป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์ซึ่งได้รับการยอมรับและกำหนดไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชนขององค์การสหประชาชาติตั้งแต่ปี ค.ศ. 1948 โดยในข้อ 12 บัญญัติว่า บุคคลย่อมไม่ถูกแทรกแซงโดยพลการในความเป็นส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือไม่อาจถูกลบหลู่ในเกียรติยศและชื่อเสียง ทั้งนี้ บุคคลทุกคนย่อมมีสิทธิที่จะได้รับการปกป้องคุ้มครองโดยกฎหมายอันเนื่องจากการก้าวล่วงสิทธิเช่นนั้น[14]

สิทธิในความเป็นส่วนตัวนี้ได้รับการยอมรับมากขึ้นเมื่อมีการพัฒนาเทคโนโลยีสารสนเทศในช่วงทศวรรษที่ 1960 ถึง 1970 เนื่องจากการเกิดขึ้นของระบบคอมพิวเตอร์ที่สามารถควบคุมและสั่งการเกี่ยวกับการเก็บรวบรวมและการจัดการข้อมูลส่วนบุคคลได้ จากในอดีตที่ปัญหา

---

[13] จาก “การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย,” โดย จันทจิรา เอี่ยมมยุรา, 2547, *วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์,* 34 (4), น. 627.

[14] Article 12 of UN Declaration of Human Rights “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.”

เรื่องการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่มีความรุนแรงมากนักเพราะการดำเนินการต่าง ๆ อยู่ในรูปของกระดาษเอกสารเป็นส่วนใหญ่ แต่เมื่อมีการพัฒนาเทคโนโลยีคอมพิวเตอร์มากยิ่งขึ้น เริ่มมีการจัดเก็บข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ ทำให้การจัดเก็บการใช้ และการเปิดเผยข้อมูลนั้นสามารถกระทำได้โดยง่าย ส่งผลให้เกิดการละเมิดสิทธิในความเป็นส่วนตัวในเรื่องเกี่ยวกับข้อมูลส่วนบุคคลมากยิ่งขึ้น จึงนำไปสู่แนวคิดในการพัฒนากฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลดังกล่าว โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกของโลกเกิดขึ้นที่รัฐเฮสเซิน (Hessen หรือ Hesse) ในสหพันธ์สาธารณรัฐเยอรมนีในปี ค.ศ. 1970 หลังจากนั้นจึงเกิดการประกาศใช้เป็นกฎหมายในอีกหลายประเทศในเวลาต่อมา เช่นในราชอาณาจักรสวีเดนในปี ค.ศ. 1973 สหรัฐอเมริกาในปี ค.ศ. 1974 สหพันธ์สาธารณรัฐเยอรมนีในปี ค.ศ. 1977 และสาธารณรัฐฝรั่งเศสในปี ค.ศ. 1978[15]

ทั้งนี้การขยายตัวของกลุ่มผู้ใช้งานอินเตอร์เน็ตส่งผลให้การคุ้มครองข้อมูลส่วนบุคคลกลายเป็นเรื่องระดับสากลที่รัฐบาลหลายประเทศต่างให้ความสำคัญและนำไปสู่การออกกฎหมายที่เกี่ยวข้องเพื่อให้ความคุ้มครองแก่ผู้ใช้งานเครือข่ายอินเตอร์เน็ต โดยการคุ้มครองข้อมูลส่วนบุคคลจำเป็นต้องพิจารณาถึงมาตรฐานขั้นต่ำที่ต้องใช้ในการจัดการข้อมูลของบุคคล และวิธีปฏิบัติที่จะทำให้สามารถรักษามาตรฐานเหล่านั้นไว้ได้[16] องค์กรระหว่างประเทศอย่างองค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (The Organization for Economic Co-operation and Development – OECD) ได้เล็งเห็นถึงปัญหาของการล่วงละเมิดในสิทธิความเป็นส่วนตัวสืบเนื่องมาจากการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคล โดยเฉพาะการใช้งานคอมพิวเตอร์เพื่อการประมวลผลข้อมูลส่วนบุคคลดังกล่าว โดยบางประเทศเลือกที่จะออกกฎหมายเฉพาะเรื่องการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปโดยไม่ได้คำนึงถึงการใช้งานเทคโนโลยี ในขณะที่บางประเทศใช้กลไกทางกฎหมายควบคุมการใช้งานเครื่องคอมพิวเตอร์แทน ภาคีสมาชิกขององค์การ OECD จึงหาข้อสรุปร่วมกันและในวันที่ 23 กันยายน ค.ศ. 1980 จึงได้รับรองแนวปฏิบัติและข้อแนะนำว่าด้วยการคุ้มครองความเป็นส่วนตัวและการส่งโอนข้อมูลส่วนบุคคลข้ามพรมแดน (OECD Guidelines on

---

[15] *Data Protection and Privacy Law.* Retrieved August 7, 2014, from https://www.privacyinternational.org/issues/data-protection-and-privacy-law

[16] Rosemary Jay and Angus Hamilton, Data Protection Law and Practice, p. 1.

the Protection of Privacy and Transborder Flows of Personal Data 1980)[17] เพื่อสร้างแนวทางที่สอดคล้องกันของกฎหมาย โดยมีหลักการพื้นฐานสำคัญ 8 ประการ ได้แก่[18]

(1) หลักการเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด (Collection Limitation Principle) หมายความว่า การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องดำเนินการโดยชอบด้วยกฎหมายและด้วยความเป็นธรรม เหมาะสม โดยเจ้าของข้อมูลนั้นได้รับทราบและให้ความยินยอมในการเก็บรวบรวม

(2) หลักคุณภาพของข้อมูลส่วนบุคคล (Data Quality Principle) หมายความว่า ข้อมูลส่วนบุคคลที่จัดเก็บจะต้องสัมพันธ์และจำเป็นต่อวัตถุประสงค์ของการได้มาซึ่งข้อมูลนั้นและต้องเป็นข้อมูลที่ถูกต้อง ครบถ้วนและต้องมีการปรับปรุงข้อมูลให้เป็นปัจจุบันตรงตามความเป็นจริงเสมอ

(3) หลักการกำหนดขอบเขตวัตถุประสงค์ (Purpose Specification Principle) หมายความว่า จะต้องมีการกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลและต้องแจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลก่อนและการใช้ข้อมูลส่วนบุคคลนั้นจะต้องสอดคล้องกับวัตถุประสงค์ดังกล่าวหรือวัตถุประสงค์ที่ได้มีการแจ้งแก้ไขเพิ่มเติมแล้ว

(4) หลักการใช้ข้อมูลส่วนบุคคลอย่างจำกัด (Use Limitation Principle) หมายความว่า ต้องไม่เปิดเผยหรือทำให้แพร่หลายซึ่งข้อมูลส่วนบุคคล หรือใช้เพื่อวัตถุประสงค์อย่างอื่นนอกเหนือจากที่ได้แจ้งให้เจ้าของข้อมูลทราบก่อน เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลหรือดำเนินการโดยอาศัยอำนาจตามกฎหมาย

(5) หลักการรักษาความปลอดภัย (Security Safeguards Principle) หมายความว่า ต้องหามาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อจัดเก็บข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ให้มีความปลอดภัยจากการสูญหาย การเข้าถึง การใช้ การทำลาย การแก้ไขเปลี่ยนแปลงหรือการเปิดเผยโดยไม่มีอำนาจจะทำได้

(6) หลักความโปร่งใส (Openness Principle) หมายความว่า ควรกำหนดนโยบายทั่วไปในเรื่องความโปร่งใสของการพัฒนา ทางปฏิบัติ และนโยบายเกี่ยวกับข้อมูลส่วนบุคคลโดยระบุถึงชนิดของข้อมูลส่วนบุคคล วัตถุประสงค์ของการใช้ ตลอดจนข้อมูลของผู้ดูแลควบคุมข้อมูลส่วนบุคคลนั้น

---

[17] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* (n.d.). Retrieved January 25, 2015, from http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[18] *OECD Privacy Principles.* Retrieved January 25, 2015, from http://oecdprivacy.org/

(7) หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle) หมายความว่า เจ้าของข้อมูลมีสิทธิได้รับการยืนยันจากผู้ดูแลควบคุมข้อมูลส่วนบุคคลว่ามีข้อมูลที่เกี่ยวข้องกับตนหรือไม่ และมีสิทธิได้รับการแจ้งให้ทราบเกี่ยวกับข้อมูลของตนภายในระยะเวลา วิธีการ รูปแบบและค่าใช้จ่ายที่เหมาะสม และหากคำขอถูกปฏิเสธมีสิทธิรับทราบเหตุผลและมีสิทธิโต้แย้งคัดค้านเหตุผลเช่นว่านั้นได้ รวมทั้งมีสิทธิโต้แย้งเกี่ยวกับข้อมูลของตนเพื่อขอให้ลบ แก้ไข เปลี่ยนแปลง เพิ่มเติมให้สมบูรณ์ได้

(8) หลักความรับผิดชอบ (Accountability Principle) หมายความว่า ผู้ดูแลควบคุมข้อมูลส่วนบุคคลจะต้องปฏิบัติตามมาตรการที่กำหนดเพื่อให้หลักการคุ้มครองข้อมูลส่วนบุคคลนั้นเกิดประสิทธิภาพในการบังคับใช้

จากผลของแนวปฏิบัติและข้อแนะนำดังกล่าว ในปี 1981 คณะมนตรีแห่งยุโรปจึงเปิดให้มีการลงนามในสนธิสัญญา Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[19]

ต่อมาวันที่ 14 ธันวาคม ค.ศ. 1990 สหประชาชาติได้รับรองแนวทางในการกำหนดหลักเกณฑ์เพื่อควบคุมข้อมูลส่วนบุคคลที่จัดเก็บด้วยระบบคอมพิวเตอร์ (Guidelines for the Regulation of Computerized Personal Data Files) โดยมีสาระสำคัญเพื่อกำหนดแนวทางการปฏิบัติในการใช้ข้อมูลส่วนบุคคลอย่างเป็นธรรม โดยแนะนำให้ภาคีสมาชิกแห่งสหประชาชาตินำเอาหลักการดังกล่าวไปกำหนดไว้เป็นส่วนหนึ่งของกฎหมายภายในเพื่อเป็นหลักประกันในเบื้องต้นสำหรับการคุ้มครองข้อมูลส่วนบุคคล[20]

โดยพื้นฐานแล้ว กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลนั้นอาจแบ่งออกได้เป็น 2 กลุ่ม คือ กลุ่มกฎหมายทั่วไปในเรื่องการคุ้มครองข้อมูลส่วนบุคคล กับกลุ่มกฎหมายเฉพาะเรื่องเฉพาะธุรกิจ ซึ่งมีการสอดแทรกเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเด็นที่เกี่ยวข้องกับธุรกิจนั้น ๆ ด้วย ในหลายประเทศต่างก็มีวิวัฒนาการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลที่น่าสนใจ ซึ่งหลักการพื้นฐานของของกฎหมายการคุ้มครองข้อมูลส่วนบุคคลไม่ว่าจะประเทศใดมีเงื่อนไขสำคัญคล้ายกัน กล่าวคือ กฎหมายกำหนดให้ (1) การได้มาซึ่งข้อมูลส่วนบุคคลนั้นจะต้องได้มาโดยชอบด้วยกฎหมายและเป็นธรรม (2) ต้องใช้ข้อมูลนั้นตามวัตถุประสงค์แรกของการได้มา (3) ข้อมูลนั้นได้มาอย่างสัมพันธ์กับวัตถุประสงค์ของการได้มาต้องเพียงพอแต่ไม่เกินกว่า

---

[19] *Data Protection and Privacy Law.* Retrieved August 7, 2014, from https://www.privacyinternational.org/issues/data-protection-and-privacy-law

[20] *Guideline for the Regulation of Computerized Personal Data Files.* Retrieved January 25, 2015, from http://www.refworld.org/pdfid/3ddcafaac.pdf

ความจำเป็นตามวัตถุประสงค์ (4) เป็นข้อมูลที่ถูกต้องและเป็นปัจจุบัน (5) ผู้เป็นเจ้าของข้อมูลสามารถเข้าถึงและตรวจสอบได้ (6) ข้อมูลนั้นถูกเก็บไว้อย่างปลอดภัย และ (7) ข้อมูลนั้นต้องถูกทำลายทันทีที่วัตถุประสงค์นั้นสิ้นสุดลง[21]

2.2.1 วิวัฒนาการของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหรัฐอเมริกา

รัฐธรรมนูญของสหรัฐอเมริกามิได้บัญญัติคุ้มครองสิทธิในความเป็นส่วนตัวไว้ชัดแจ้ง โดยตรงคงมีเพียงการคุ้มครองสิทธิในความปลอดภัยในร่างกาย เคหสถาน ทรัพย์สิน ให้พ้นจากการค้น การจับหรือการยึดโดยปราศจากเหตุอันสมควร (4th Amendment) แต่ศาลสูงของสหรัฐอเมริกาให้การรับรองว่าสิทธิในความเป็นส่วนตัวนั้นแท้จริงแล้วเป็นรากฐานตามกรอบของรัฐธรรมนูญนั้นเองเพียงแต่ไม่ได้เขียนไว้ชัดแจ้งเท่านั้น[22] จากแนวความคิดดังกล่าวนำไปสู่พัฒนาการของกฎหมายทั้งจากแนวคำพิพากษาของศาลและกระบวนการนิติบัญญัติ

ในสหรัฐอเมริกานั้นมีกฎหมายที่คุ้มครองข้อมูลส่วนบุคคลกระจัดกระจายอยู่หลายฉบับ มิได้มีความเป็นเอกเทศชัดเจน โดยกฎหมายที่มีส่วนเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลบัญญัติไว้ใน The Privacy Act of 1974[23] ซึ่งกำหนดให้หน่วยงานของรัฐจะต้องปฏิบัติต่อข้อมูลส่วนบุคคลอย่างเหมาะสมและเป็นธรรมและห้ามมิให้มีการเปิดเผยข้อมูลเว้นแต่มีเหตุตามที่กฎหมายกำหนด อย่างไรก็ดีกฎหมายฉบับนี้มุ่งคุ้มครองข้อมูลส่วนบุคคลเฉพาะที่จัดเก็บโดยหน่วยงานของรัฐเท่านั้น มิได้รวมถึงข้อมูลส่วนบุคคลที่จัดเก็บโดยเอกชนด้วยแต่อย่างใด นอกจากนี้ยังมีข้อวิพากษ์วิจารณ์ด้วยว่าการใช้บังคับกฎหมายฉบับนี้ไม่มีประสิทธิภาพตามความมุ่งหมายเพราะการตีความบทนิยามของกฎหมายเกี่ยวกับการใช้งานตามปกติ (“Routine Use”)

ในส่วนของการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเอกชนนั้น มีการบัญญัติเป็นกฎหมายเฉพาะเรื่องหลายฉบับ ทั้งกฎหมายในระดับประเทศและกฎหมายระดับมลรัฐ ในระดับของรัฐบาลกลางนั้นไม่มีหน่วยงานที่รับผิดชอบดูแลเรื่องการคุ้มครองข้อมูลส่วนบุคคลโดยตรง แต่เป็นบทบาทหน้าที่ของคณะกรรมาธิการการค้าแห่งสหพันธรัฐ (Federal Trade Commission) ที่ควบคุมบังคับใช้กฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและสิทธิในความเป็นส่วนตัว เนื่องจากเป็นเรื่องที่เกี่ยวข้องกับการค้าการบริการและการคุ้มครองผู้บริโภคซึ่งเป็นอำนาจหน้าที่โดยตรงของคณะกรรมการดังกล่าว และยังมีบทบาทสำคัญในการวิเคราะห์วิจัย วางแนวทางบังคับใช้และ

---

[21] *Data Protection and Privacy Law.* Retrieved August 7, 2014, from https://www.privacyinternational.org/issues/data-protection-and-privacy-law

[22] From “Privacy for Children,” by Benjamin Shmueli and Ayelet Blecher-Prigat, 2011, *Columbia Human Rights Law Review,* (42: 759), p. 764 .

[23] 5 U.S.C. § 552a.

ตีความกฎหมายเกี่ยวกับประเพณีการค้าดังกล่าวด้วย ซึ่งในเดือนมีนาคม ค.ศ. 2012 คณะกรรมการได้ออกรายงานวิจัยฉบับหนึ่งชื่อ การคุ้มครองความเป็นส่วนตัวของผู้บริโภคในศักราชแห่งการเปลี่ยนแปลงที่รวดเร็ว : คำแนะนำสำหรับธุรกิจและผู้กำหนดนโยบาย (Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers) เพื่อนำเสนอมาตรการในการปกป้องสิทธิในความเป็นส่วนตัวของผู้บริโภคและให้ภาคธุรกิจพัฒนามาตรการส่วนตัวเพื่อการคุ้มครองดังกล่าวด้วย

พัฒนาการของกฎหมายเพื่อการคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคลของสหรัฐอเมริกาจัดได้ว่ามีความก้าวหน้ามากกว่าประเทศอื่นอย่างเห็นได้ชัดโดยเฉพาะเมื่อพิจารณาในบริบทของการคุ้มครองผู้ใช้งานอินเตอร์เน็ต ในปี ค.ศ. 2013 มีการนำเสนอร่างกฎหมายชื่อ Do Not Track Online Act of 2013 ซึ่งให้อำนาจคณะกรรมาธิการการค้าแห่งสหพันธรัฐในการกำหนดมาตรการเปิดช่องให้ผู้ใช้งานสามารถแสดงเจตนาไม่ให้ผู้ประกอบการเว็บไซต์เก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคล ไม่ว่าจะเป็นข้อมูลที่ใช้สำหรับระบุตัวตนหรือข้อมูลเกี่ยวกับพฤติกรรมการใช้งานอินเตอร์เน็ตก็ตาม[24] ซึ่งถือเป็นความก้าวหน้าของกฎหมายระดับรัฐบาลกลางครั้งสำคัญเกี่ยวกับการออกกฎหมายควบคุมการใช้งานอินเตอร์เน็ตโดยตรงเพื่อคุ้มครองความเป็นส่วนตัวของผู้ใช้งานหลังจากที่ไม่มีการออกกฎหมายระดับรัฐบาลกลางเกี่ยวกับการใช้งานอินเตอร์เน็ตโดยตรงมาเป็นเวลานานนับแต่กฎหมายคุ้มครองความเป็นส่วนตัวของเด็กจากการใช้งานอินเตอร์เน็ต[25]

กฎหมายอีกฉบับหนึ่งที่เป็นร่างกฎหมายและมีความน่าสนใจคือกฎหมาย Application Privacy, Protection, and Security Act of 2013 ซึ่งบังคับให้ผู้พัฒนาโปรแกรมใช้งานผ่านโทรศัพท์เคลื่อนที่ต้องได้รับความยินยอมก่อนเก็บข้อมูลส่วนตัวของผู้ใช้งานโปรแกรมและกำหนดให้ผู้พัฒนาโปรแกรมจะต้องจัดหามาตรการที่เหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลที่เก็บรวบรวมไว้โดยไม่มีอำนาจ[26]

นอกเหนือจากกฎหมายดังกล่าวแล้วยังมีกฎหมายระดับรัฐบาลกลางอีกหลายฉบับที่เกี่ยวข้องกับการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคล ซึ่งบางฉบับใช้บังคับเฉพาะข้อมูล

---

[24] *ความคืบหน้าของการพิจารณาร่างกฎหมาย Do-Not-Track Online Act of 2013.* สืบค้น 25 มกราคม 2558, จาก http://beta.congress.gov/bill/113th-congress/senate-bill/418

[25] The Children's Online Privacy Protection Act of 1998 (COPPA) (15 U.S.C. §§6501-6506).

[26] *สาระสำคัญของกฎหมายและความคืบหน้าในการพิจารณาร่างกฎหมาย Application Privacy, Protection, and Security Act of 2013.* สืบค้น 25 มกราคม 2558, จาก http://www.opencongress.org/bill/hr1913-113/show

บางประเภท เช่น เรื่องเกี่ยวกับข้อมูลทางการเงิน[27] ประวัติการรักษาพยาบาล[28] ข้อมูลการยืมวิดีโอ[29] ข้อมูลสมาชิกเคเบิลทีวี[30] หรือข้อมูลเกี่ยวกับนักเรียน[31] เป็นต้น บางฉบับใช้บังคับกับกิจกรรมที่เกี่ยวข้องกับการใช้ข้อมูลส่วนบุคคล เช่น การทำการตลาดด้วยวิธีโทรศัพท์หรือไปรษณีย์อิเล็กทรอนิกส์ เป็นต้น นอกจากนี้ยังมีกฎหมายที่เกี่ยวข้องกับการคุ้มครองผู้บริโภคในภาพรวม ซึ่งถึงแม้ว่าจะไม่เกี่ยวกับการคุ้มครองสิทธิในความเป็นส่วนตัวโดยตรง แต่สามารถนำมาใช้ควบคุมมิให้เกิดการปฏิบัติทางการค้าอย่างไม่เป็นธรรมรวมไปถึงการเปิดเผยข้อมูลส่วนบุคคลด้วย เช่น กฎหมายว่าด้วยคณะกรรมาธิการการค้าแห่งสหพันธรัฐ[32] ซึ่งเป็นกฎหมายคุ้มครองผู้บริโภคในระดับรัฐบาลกลางเพื่อป้องกันทางปฏิบัติทางการค้าที่ไม่เป็นธรรมไม่ว่าจะเป็นการค้าในโลกความเป็นจริงหรือในโลกออนไลน์ก็ตาม ซึ่งที่ผ่านมาคณะกรรมาธิการการค้าแห่งสหพันธรัฐก็ได้

---

[27] The Fair Credit Reporting Act (15 U.S.C. §1681) and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108-159) เป็นกฎหมายที่ใช้บังคับกับการรายงานข้อมูลเครดิตของผู้บริโภคเพื่อประกอบการอนุมัติสินเชื่อหรือการรับประกันภัย

The Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827) เป็นกฎหมายที่ควบคุมการเก็บรวบรวม ใช้และเปิดเผยข้อมูลทางการเงิน โดยใช้บังคับสถาบันการเงินทุกประเภทไม่ว่าจะเป็นธนาคาร บริษัทหลักทรัพย์ และบริษัทประกันภัย ตลอดจนการประกอบธุรกิจอื่นที่เกี่ยวข้องกับผลิตภัณฑ์ทางการเงินและสินเชื่อ โดยกฎหมายจำกัดการเปิดเผยข้อมูลส่วนบุคคลที่ไม่เป็นที่เผยแพร่และในบางกรณีบังคับให้สถาบันการเงินต้องแจ้งถึงนโยบายการปฏิบัติเกี่ยวกับการเก็บรักษาความลับของตนและให้สิทธิแก่ลูกค้าเจ้าของข้อมูลในการไม่ยินยอมให้เผยแพร่ข้อมูลของตน.

[28] The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) เป็นกฎหมายที่ควบคุมข้อมูลเกี่ยวกับการรักษาพยาบาล โดยใช้บังคับกับผู้ให้บริการด้านการแพทย์และสาธารณสุข ผู้ประมวลผลข้อมูล ร้านขายยา และบุคคลที่เข้ามาเกี่ยวข้องกับข้อมูลดังกล่าว ทั้งนี้ มีการออกกฎหมายลำดับรองเพื่อวางรายละเอียดของการบังคับใช้และควบคุมข้อมูลด้วย เช่น The Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule) (45 C.F.R. Parts 160 and 164) ซึ่งเป็นมาตรฐานที่ใช้กับการเก็บรวบรวมและใช้ข้อมูลด้านสุขภาพที่ได้รับความคุ้มครอง (protected health information หรือ PHI) The Security Standards for the Protection of Electronic Protected Health Information (HIPAA Security Rule) (45 C.F.R. 160 and 164) ซึ่งเป็นมาตรฐานสำหรับคุ้มครองความปลอดภัยของข้อมูลด้านสุขภาพ The Standards for Electronic Transactions (HIPAA Transactions Rule) (45 C.F.R. 160 and 162) ซึ่งเป็นมาตรฐานสำหรับคุ้มครองการส่งผ่านข้อมูลด้านสุขภาพโดยใช้สื่ออิเล็กทรอนิกส์ เป็นต้น.

[29] The Video Privacy Protection Act of 1988 (18 U.S.C. §2710 (2002).

[30] Cable TV Privacy Act of 1984 (47 USC §551).

[31] Family Educational Rights and Privacy Act of 1974 (20 USC §1232g).

[32] The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act).

ดำเนินการต่อผู้ประกอบการที่ฝ่าฝืนไม่แจ้งนโยบายความเป็นส่วนตัวและผู้ฝ่าฝืนเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีอำนาจ

นอกเหนือจากกฎหมายในระดับรัฐบาลกลางแล้ว ในแต่ละมลรัฐก็อาจมีกฎหมายภายในของตนเองสำหรับการคุ้มครองข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวเช่นกัน ซึ่งบางเรื่องอาจซ้ำซ้อนกับกฎหมายของรัฐบาลกลางและต้องบังคับตามกฎหมายรัฐบาลกลาง แต่มีกฎหมายระดับมลรัฐอีกหลายเรื่องที่รัฐบาลกลางไม่ได้วางมาตรการในเรื่องนั้นไว้และมีผลใช้บังคับได้ โดยเฉพาะในมลรัฐแคลิฟอร์เนียซึ่งมีหน่วยงานคุ้มครองสิทธิความเป็นส่วนตัวโดยตรงและมีกฎหมายในเรื่องการคุ้มครองสิทธิความเป็นส่วนตัวค่อนข้างก้าวหน้า เช่น กฎหมาย The Shine the Light Law (CA Civil Code §1798.83) กำหนดให้ผู้ประกอบการต้องเปิดเผยข้อมูลของบุคคลภายนอกที่ตนจะนำข้อมูลส่วนบุคคลที่ได้มานั้นไปเปิดเผยให้หรือกฎหมาย The Data Security Law (CA Civil Code §1798.81.5) ซึ่งกำหนดให้ผู้ประกอบการจัดหามาตรการรักษาความปลอดภัยในข้อมูลส่วนบุคคลอย่างเหมาะสมเพื่อป้องกันการเข้าถึง ทำลาย ใช้ แก้ไข หรือเปิดเผยโดยไม่มีอำนาจ[33]

ในมลรัฐแคลิฟอร์เนียนั้นมีการพัฒนากฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในจากการใช้งานอินเตอร์เน็ตที่น่าสนใจอีกฉบับหนึ่ง คือ The California's Online Privacy Protection Act of 2003 (OPPA) (CA Bus. & Prof. Code §§22575-22579) ซึ่งกำหนดให้ผู้ประกอบการเว็บไซต์ที่รวบรวมข้อมูลส่วนบุคคลของผู้มีถิ่นที่อยู่ในมลรัฐแคลิฟอร์เนียจะต้องกำหนดนโยบายเกี่ยวกับสิทธิความเป็นส่วนตัวแสดงไว้บนหน้าเว็บไซต์อย่างชัดเจนและนโยบายดังกล่าวจะต้องเป็นไปตามเงื่อนไขที่กำหนดด้วย ได้แก่ การระบุประเภทของข้อมูลที่มีการรวบรวมโดยผู้ประกอบการเว็บไซต์ วิธีการที่จะมีการส่งต่อข้อมูลให้แก่บุคคลภายนอกและขั้นตอนในการตรวจสอบและแก้ไขข้อมูลโดยผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลนั้น

2.2.2 วิวัฒนาการของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศในกลุ่มสหภาพยุโรป

ในสหภาพยุโรปนั้นถือว่าการคุ้มครองสิทธิในความเป็นส่วนตัวมิใช่เพียงมาตรการคุ้มครองผู้บริโภคเท่านั้น แต่ถือเป็นสิทธิมนุษยชนประการหนึ่งที่ต้องกำหนดไว้ในรัฐธรรมนูญและมีความสัมพันธ์กับเรื่องของการคุ้มครองข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัวถูกกล่าวถึงครั้งแรกในข้อ 8 แห่ง สนธิสัญญาสหภาพยุโรปว่าด้วยสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน (The European Convention of Human Rights and Fundamental Freedoms - ECHR) โดยกำหนดว่าบุคคลทุกคนย่อมมีสิทธิในชีวิตความเป็นส่วนตัว ชีวิตครอบครัว ความเป็นอยู่ในบ้านและ

---

[33] Ieuan Jolly. (n.d.). *Data protection in United States: overview.* Retrieved January 15, 2015, from http://uk.practicallaw.com/6-502-0467#a233354

ความเป็นอยู่ที่เกี่ยวเนื่องกัน (Everyone has the right to respect for his or her private and family life, home and correspondence.)

อย่างไรก็ดี การพัฒนาทางเทคโนโลยีที่ก้าวหน้าอย่างรวดเร็วส่งผลให้การคุ้มครองสิทธิในความเป็นส่วนตัวเป็นไปได้ยากยิ่งขึ้น สหภาพยุโรปจึงพัฒนาหลักการเพื่อตอบสนองต่อความก้าวหน้าทางเทคโนโลยี ด้วยการขยายกรอบของสิทธิในความเป็นส่วนตัวให้ครอบคลุมไปถึงการให้ความคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ภายหลังจากที่องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ได้ออกแนวทางในการคุ้มครองความเป็นส่วนตัวและการส่งโอนข้อมูลส่วนบุคคลข้ามพรมแดนในปี ค.ศ. 1980 แล้ว สหภาพยุโรปได้ออกกฎหมายของตนเองเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในปี ค.ศ. 1995 (The Data Protection Directive 95/46/EC) ซึ่งมีวัตถุประสงค์ในการกำหนดกรอบอย่างกว้างเพื่อคุ้มครองความเป็นส่วนตัวเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและสร้างความเป็นหนึ่งเดียวกันของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของรัฐภาคีสมาชิก โดยมีการกำหนดหลักการสำคัญในเรื่องการรักษาคุณภาพของข้อมูล มาตรฐานของการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย การประมวลผลข้อมูลชนิดพิเศษ สิทธิของเจ้าของข้อมูลในการได้รับแจ้งข้อมูลต่าง ๆ สิทธิของเจ้าของข้อมูลในการคัดค้านการประมวลผลข้อมูล การรักษาความปลอดภัยในการประมวลข้อมูลและการส่งผ่านข้อมูลส่วนบุคคลไปยังประเทศที่สาม (ประเทศนอกกลุ่มสหภาพยุโรป)

ต่อมามีการอาศัยอำนาจตามข้อ 285 ของสนธิสัญญาก่อตั้งสหภาพยุโรปจัดตั้งหน่วยงานกลางที่ทำหน้าที่ดูแลการคุ้มครองข้อมูล ซึ่งปัจจุบันรู้จักในชื่อ The European Data Protection Supervisor หลังจากนั้นสหภาพยุโรปจึงออก Data Protection Regulation 45/2001/EC4 เพื่อแก้ไขเพิ่มเติมกฎหมาย The Data Protection Directive 95/46/EC ฉบับเดิมให้มีความสมบูรณ์มากยิ่งขึ้นและกำหนดรายละเอียดเกี่ยวกับหน่วยงานที่ควบคุมดูแลการคุ้มครองข้อมูลและในปี ค.ศ. 2002 สหภาพยุโรปออกกฎหมาย The e-Privacy Directive 2002/58/EC อีกฉบับเพื่อแก้ไขเพิ่มเติม The Directive 95/46/EC ฉบับเดิม โดยมุ่งคุ้มครองข้อมูลสืบเนื่องจากการสื่อสารทางอิเล็กทรอนิกส์และอินเตอร์เน็ตโดยเฉพาะโดยมาตรา 15 ของ The e-Privacy Directive เปิดโอกาสให้รัฐภาคีสมาชิกสามารถออกกฎหมายภายในเพื่อประโยชน์ในการดำเนินคดีอาญาหรือเพื่อประโยชน์สาธารณะอย่างอื่นภายใต้กฎหมาย The e-Privacy Directive ได้และในปี ค.ศ. 2006 สหภาพยุโรปได้ออกกฎหมาย The Data Retention Directive 2006/24/EC6 เพื่อบังคับให้ผู้ประกอบการด้านการสื่อสารจะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เป็นระยะเวลาตามที่กำหนดเพื่อให้หน่วยงานผู้บังคับใช้กฎหมายสามารถตรวจสอบและดำเนินคดีกับผู้กระทำความผิดได้

ที่สำคัญกฎบัตรว่าด้วยสิทธิขั้นพื้นฐานของสหภาพยุโรป (EU Charter of Fundamental Rights) ซึ่งเปรียบเสมือนกฎหมายในระดับรัฐธรรมนูญของสหภาพยุโรปยังมีการปรับปรุงสิทธิในความเป็นส่วนตัวและเพิ่มเติมสิทธิในการได้รับความคุ้มครองในข้อมูลเข้าไปด้วยโดยในข้อ 8 ของกฎบัตร ซึ่งเป็นบทบัญญัติที่กล่าวถึงการคุ้มครองข้อมูลส่วนบุคคล กำหนดให้ (1) บุคคลทุกคนมีสิทธิได้รับความคุ้มครองในข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน (2) ข้อมูลดังกล่าวจะถูกนำไปประมวลผลอย่างเป็นธรรมเพื่อวัตถุประสงค์ที่กำหนดไว้บนพื้นฐานความยินยอมของผู้นั้นหรือมีอำนาจที่จะกระทำได้โดยชอบตามที่กฎหมายบัญญัติไว้และทุกคนมีสิทธิที่จะเข้าถึงข้อมูลที่เก็บรวบรวมจากผู้นั้น รวมทั้งมีสิทธิขอให้แก้ไขปรับปรุงข้อมูลให้ถูกต้องและ (3) การปฏิบัติตามบทบัญญัติดังกล่าวจะต้องได้รับการตรวจสอบโดยหน่วยงานที่มีความอิสระ

ด้วยเหตุนี้จึงกล่าวได้ว่าสหภาพยุโรปและประเทศภาคีสมาชิกได้ให้การรับรองสิทธิในความเป็นส่วนตัวและให้ความสำคัญต่อสิทธิที่จะได้รับความคุ้มครองในข้อมูลส่วนบุคคล อย่างไรก็ดีแนวทางในการให้ความคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศซึ่งเป็นภาคีของสหภาพยุโรปอาจจะมีความแตกต่างกันไปบ้าง สืบเนื่องจากประวัติศาสตร์ทางกฎหมายและความคุ้นเคยต่อเทคโนโลยีสารสนเทศที่พัฒนาขึ้นนั้นแตกต่างกัน ในที่นี้ขอกล่าวถึงแนวคิดและวิวัฒนาการในการคุ้มครองข้อมูลส่วนบุคคลของประเทศในกลุ่มสหภาพยุโรป 4 ประเทศ ได้แก่ ประเทศอังกฤษ ราชอาณาจักรเนเธอร์แลนด์ และสหพันธ์สาธารณรัฐเยอรมนี และสมาพันธรัฐสวิส

2.2.2.1 ประเทศอังกฤษ

ประเทศอังกฤษไม่มีรัฐธรรมนูญที่บัญญัติรับรองสิทธิขั้นพื้นฐานของประชาชนเป็นลายลักษณ์อักษร อย่างไรก็ดีในฐานะสมาชิกของสหภาพยุโรปได้มีการออกกฎหมายสิทธิมนุษยชน The Human Rights Act of 1998 เพื่อให้เป็นไปตามสนธิสัญญาสหภาพยุโรปว่าด้วยสิทธิมนุษยชน (The European Convention on Human Rights (ECHR)) ซึ่งมีการบัญญัติสิทธิมนุษยชนขั้นพื้นฐานให้รวมไปถึงสิทธิในความเป็นส่วนตัวด้วย

ที่ผ่านมาศาลยุติธรรมของประเทศอังกฤษได้พัฒนาหลักกฎหมายเรื่องสิทธิในความเป็นส่วนตัวมาโดยตลอดนับแต่ปี ค.ศ.1849 เพื่อป้องกันการเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีอำนาจ ในปี ค.ศ. 1970 ภายหลังจากการออกกฎหมายไม่แบ่งแยกเพศและสีผิวในประเทศอังกฤษ (Sex Discrimination Act of 1971 และ Race Relation Act of 1968) ประกอบกับการใช้งานคอมพิวเตอร์ ที่เริ่มแพร่หลายขึ้น แนวความคิดเกี่ยวกับสิทธิในความเป็นส่วนตัวจึงเริ่มได้รับความสนใจมากขึ้นในช่วงเวลานี้มีการเสนอร่างกฎหมายเกี่ยวกับสิทธิในความเป็นส่วนตัวหลายฉบับเข้าสู่การพิจารณาของรัฐสภา แต่ก็ไม่สามารถผ่านกฎหมายได้จนกระทั่งในปี ค.ศ. 1972 รัฐบาลพรรคแรงงานของประเทศอังกฤษได้เสนอนาย Kenneth Younger ให้เป็นประธานคณะกรรมการ

Committee on Privacy จึงเริ่มมีการสำรวจทัศนคติของประชาชนทั่วไปเกี่ยวกับสิทธิในความเป็นส่วนตัวโดยมุ่งเน้นศึกษากรณีผลกระทบจากการขยายตัวของการใช้งานคอมพิวเตอร์ และสรุปเป็นแนวทางในการจัดการข้อมูลส่วนบุคคลจากการใช้งานคอมพิวเตอร์ (The Report of the Committee on Privacy 1972) หรือที่รู้จักกันในอีกชื่อหนึ่งว่า The Younger Report 1972[34] แต่รายงานฉบับดังกล่าวมุ่งเน้นที่การรักษาความปลอดภัยของข้อมูลและการเข้าถึงข้อมูล โดยมิได้ให้ความสำคัญกับการใช้หรือเปิดเผยข้อมูลดังกล่าวแต่อย่างใด

หลังจากรายงานฉบับดังกล่าวถูกเผยแพร่ได้ประมาณ 3 ปี รัฐบาลได้ตีพิมพ์สมุดปกขาว (White Paper) 2 ฉบับได้แก่ Computer and Privacy เพื่อประกาศเจตนาของรัฐบาลที่จะออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลและ Computers: Safeguards for Privacy ซึ่งกล่าวถึงการใช้งานคอมพิวเตอร์ในทางราชการ หลังจากนั้นรัฐบาลจึงจัดตั้งคณะกรรมการคุ้มครองข้อมูลในเดือนกรกฎาคม 1976 ภายใต้การนำของ Sir Norman Lindop ประธานกรรมการคนแรก

หลังจากรัฐบาลออกสมุดปกขาวดังกล่าวแล้วก็ไม่มีการออกกฎหมายที่เกี่ยวข้องแต่อย่างใด จนกระทั่งในเดือนธันวาคมปี ค.ศ. 1978 Lindop ซึ่งเป็นประธานกรรมการคุ้มครองข้อมูลได้จัดทำรายงานของคณะกรรมการขึ้น (Report of the Committee on Data Protection) หรือที่รู้จักกันในอีกชื่อหนึ่งว่า The Lindop Report 1978[35] เพื่อให้คำแนะนำแก่รัฐบาลในการหาแนวทางในการคุ้มครองข้อมูลจากการใช้งานคอมพิวเตอร์ที่เหมาะสม ลักษณะเดียวกับ The Younger Report โดยมุ่งเน้นทั้งในภาคราชการและเอกชน รายงานฉบับนี้เสนอว่าการบังคับใช้กฎหมายควรจะต้องถูกตรวจสอบดูแลโดยหน่วยงานคุ้มครองข้อมูลที่มีความเป็นอิสระ

แต่หลังจากนั้นก็ยังไม่มีการออกกฎหมายที่เกี่ยวข้องจนกระทั่งมีการจัดตั้งสภายุโรป (Council of Europe) โดยมีการร่างสนธิสัญญาว่าด้วยการคุ้มครองบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ (Convention for the Protection of Individuals with regard to automatic processing of personal data – Treaty 108) โดยสนธิสัญญาฉบับนี้รับรองคุณค่าพื้นฐานของความเป็นส่วนตัวและการส่งโอนข้อมูลระหว่างบุคคล หลังจากนั้นประเทศอังกฤษจึงออกพระราชบัญญัติคุ้มครองข้อมูล ค.ศ. 1984 (The Data Protection Act of 1984) ก่อนจะลงชื่อเข้าร่วมในสนธิสัญญาฉบับดังกล่าว

พระราชบัญญัติคุ้มครองข้อมูล ค.ศ. 1984 ได้กลายเป็นต้นแบบของกระบวนการจัดการข้อมูลส่วนบุคคลที่เหมาะสม โดยวางหลักการพื้นฐาน 8 ประการ ได้แก่

---

[34] Rosemary Jay and Angus Hamilton, Data Protection Law and Practice, p. 2.

[35] Rosemary Jay and Angus Hamilton, Data Protection Law and Practice, p. 3.

(1) ข้อมูลส่วนบุคคลจะต้องถูกจัดเก็บและถูกประมวลผลอย่างเป็นธรรมโดยชอบด้วยกฎหมาย

(2) การยึดถือข้อมูลส่วนบุคคลไว้จะกระทำได้ต่อเมื่อเป็นไปตามวัตถุประสงค์อันชอบด้วยกฎหมายที่กำหนดไว้โดยเฉพาะอย่างน้อย 1 วัตถุประสงค์

(3) ข้อมูลส่วนบุคคลที่ยึดถือไว้เพื่อวัตถุประสงค์ใดจะต้องไม่ถูกนำไปใช้หรือเปิดเผยแตกต่างไปจากวัตถุประสงค์ดังกล่าว

(4) ข้อมูลส่วนบุคคลที่ยึดถือไว้เพื่อวัตถุประสงค์ใดจะต้องเพียงพอและเกี่ยวข้องกับวัตถุประสงค์ดังกล่าว

(5) ข้อมูลส่วนบุคคลที่ยึดถือไว้จะต้องถูกต้องและเป็นปัจจุบัน

(6) ข้อมูลส่วนบุคคลที่ยึดถือไว้เพื่อวัตถุประสงค์ใดจะต้องไม่ยึดถือไว้นานเกินกว่าความจำเป็นในการจัดการเพื่อวัตถุประสงค์นั้น

(7) บุคคลมีสิทธิได้รับแจ้งจากผู้ใช้ข้อมูลในช่วงเวลาที่เหมาะสมและไม่มีค่าใช้จ่ายให้ทราบถึงการใช้ข้อมูลของบุคคลนั้นและมีสิทธิเข้าถึงข้อมูล ตรวจสอบข้อมูลที่ยึดถือไว้โดยผู้ใช้ข้อมูล รวมทั้งมีสิทธิขอแก้ไขให้ถูกต้องได้

(8) ต้องจัดให้มีมาตรการป้องกันที่เหมาะสมเพื่อมิให้เกิดการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตหรือแก้ไขเปลี่ยนแปลง เปิดเผย หรือทำลายข้อมูลส่วนบุคคล รวมทั้งป้องกันไม่ให้เกิดการสูญหายหรือทำลายโดยไม่ตั้งใจด้วย[36]

อย่างไรก็ดีหลักการดังกล่าวได้บัญญัติไว้อย่างกว้าง ๆ จึงมีความไม่ชัดเจนในทางปฏิบัติจำเป็นต้องมีการแต่งตั้งนายทะเบียนคุ้มครองข้อมูลข่าวสาร (Data Protection Registrar) และคณะกรรมการพิจารณาเฉพาะเรื่อง (Data Protection Tribunal) เพื่อการบังคับใช้กฎหมายอย่างมีประสิทธิภาพ ต่อมาในปี ค.ศ. 1995 เมื่อสหภาพยุโรปได้บัญญัติ The Data Protection Directive 95/46/EC เพื่อให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลและบังคับให้รัฐภาคีจะต้องออกกฎหมายภายในของตนเพื่ออนุวัตการให้เป็นไปตามความตกลงฉบับดังกล่าวภายในวันที่ 24 ตุลาคม ค.ศ. 1998 ต่อมาประเทศอังกฤษจึงได้ออกกฎหมายภายในของตนโดยตราพระราชบัญญัติการคุ้มครองข้อมูลข่าวสาร ค.ศ. 1998 (The Data Protection Act of 1998) ซึ่งมีผลบังคับใช้ในวันที่ 1 มีนาคม ค.ศ. 2000

กฎหมายฉบับใหม่ของประเทศอังกฤษได้สร้างมาตรฐานขึ้นมาจากกฎหมายเดิมโดยยังคงหลักการพื้นฐาน 8 ประการไว้และเพิ่มเติมบทนิยามของคำว่าการประมวลผล (Processing)

---

[36] สันธาน ขันธมณี และดำรง ทรัพยผล. (2552). *กฎหมายคุ้มครองข้อมูลส่วนบุคคล* (รายงาน. สำนักงานศาลยุติธรรม). สืบค้น 25 มกราคม 2558, จาก http://www.coj.go.th/iad/userfiles/file/dataprotection.doc

ซึ่งรวมถึงการกระทำต่อข้อมูลเกือบจะทุกรูปแบบและกฎหมายฉบับนี้ถูกใช้เป็นกฎหมายภายในของประเทศอังกฤษจนถึงปัจจุบัน

2.2.2.2 ราชอาณาจักรเนเธอร์แลนด์

รัฐธรรมนูญของราชอาณาจักรเนเธอร์แลนด์ได้ให้การรับรองสิทธิในความเป็นส่วนตัวของประชาชนไว้โดยชัดแจ้ง โดยในมาตรา 10 กำหนดว่า (1) ทุกคนมีสิทธิได้รับการเคารพในความเป็นส่วนตัว เว้นแต่มีกฎหมายที่ออกโดยรัฐสภากำหนดไว้เป็นอย่างอื่น (2) กฎเกณฑ์สำหรับการคุ้มครองความเป็นส่วนตัวต้องบัญญัติเป็นกฎหมายของรัฐสภาโดยคำนึงถึงหลักการที่เหมาะสมในการเก็บรวบรวมและการเผยแพร่ข้อมูลส่วนบุคคล (3) กฎเกณฑ์เกี่ยวกับสิทธิของบุคคลที่จะได้รับทราบข้อมูลของตนที่ถูกเก็บรวบรวม และการใช้ข้อมูลนั้น ตลอดจนสิทธิในการแก้ไขข้อมูลให้ถูกต้องจะต้องกำหนดไว้ในกฎหมายของรัฐสภา[37]

ในปี ค.ศ.1988 ราชอาณาจักรเนเธอร์แลนด์ได้ตรากฎหมาย The Dutch Data Registration Act of 1988 ซึ่งวางแนวปฏิบัติที่เหมาะสมกับแฟ้มข้อมูลส่วนบุคคลโดยการเก็บรวบรวมหรือจัดทำแฟ้มข้อมูลส่วนบุคคลจะทำได้ต้องเป็นไปเพื่อประโยชน์ของผู้ควบคุมแฟ้มข้อมูลส่วนบุคคลดังกล่าวเท่านั้น และผู้ควบคุมข้อมูลดังกล่าวจะต้องใช้มาตรการที่เหมาะสมในการเก็บรักษาข้อมูลนั้นให้ปลอดภัยและต้องรับผิดในความสูญหายหรือเสียหายสืบเนื่องจากการไม่ปฏิบัติตามเงื่อนไขที่กฎหมายกำหนด ทั้งนี้การเปิดเผยข้อมูลจะทำได้ต่อเมื่อเป็นไปตามกฎหมายหรือได้รับความยินยอมจากเจ้าของข้อมูลเท่านั้นและผู้ควบคุมข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงการรวบรวมข้อมูลเช่นนั้นและอนุญาตให้เจ้าของข้อมูลสามารถเข้าถึงแฟ้มข้อมูลและขอแก้ไขข้อมูลของตนได้ โดยมีการจัดตั้งหน่วยงาน The Registration Chamber (Registratiekamer) เพื่อทำหน้าที่เป็นหน่วยงานคุ้มครองข้อมูลของประเทศ มีอำนาจกำกับดูแลการดำเนินการเกี่ยวกับแฟ้มข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย[38]

---

[37] The Constitution of the Kingdom of the Netherlands 2008, Article 10:

1. Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament.

2. Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data.

3. Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament.

[38] Global Internet Liberty Campaign. (n.d.). *Privacy and Human Rights Survey.* Retrieved January 25, 2015, from http://gilc.org/privacy/survey/surveylz.html#

ต่อมาในปี ค.ศ. 1998 มีการแก้ไขเพิ่มเติม The Dutch Data Registration Act เพื่อกำหนดเงื่อนไขเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสหภาพยุโรปและ ในปี ค.ศ. 2000 ราชอาณาจักรเนเธอร์แลนด์ได้ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล Wet Bescherming Persoonsgegevens (WBP: Dutch Personal Data Protection Act) เพื่ออนุวัตการให้เป็นไปตาม The Data Protection Directive 95/46/EC ซึ่งเป็นกฎหมายที่แก้ไขเพิ่มเติมจาก The Dutch Data Registration Act เดิมและมีผลใช้บังคับในวันที่ 1 กันยายน ค.ศ. 2001 โดยกฎหมายให้อำนาจในการออกพระราชกฤษฎีกาเพื่อกำหนดข้อยกเว้นในการปฏิบัติตามเงื่อนไขของกฎหมายสำหรับองค์กรหรือหน่วยงานบางประเภท

ต่อมาปี ค.ศ. 2007 และปี ค.ศ. 2008 มีการจัดทำรายงานประเมินการใช้บังคับกฎหมายฉบับนี้ได้ข้อสรุปว่ากฎหมายฉบับนี้สร้างภาระให้แก่หน่วยงานปกครองและในวันที่ 5 กุมภาพันธ์ ค.ศ. 2009 จึงมีการเสนอร่างกฎหมายต่อรัฐสภาเพื่อแก้ไขเพิ่มเติมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล แต่ข้อเสนอในการแก้ไขกลับสร้างภาระในการจัดการมากยิ่งขึ้น เช่น การยกเลิกเงื่อนไขการขออนุญาตในกรณีที่มีการโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสหภาพยุโรปซึ่งไม่มีเงื่อนไขในการให้ความคุ้มครองเช่นเดียวกัน แม้ว่าการโอนนั้นจะกระทำภายใต้เงื่อนไขข้อตกลงของสัญญาก็ตาม โดยมีการกำหนดไว้ในมาตรา 77(2) ว่าไม่อาจอนุญาตได้เว้นแต่จะใช้สัญญารูปแบบและข้อความตามที่กำหนดโดยไม่มีการแก้ไขถ้อยคำซึ่งเป็นการกำหนดหลักเกณฑ์เป็นพิเศษเพิ่มเติมจากพันธกรณีตาม The Data Protection Directive 95/46/EC เช่นเดียวกับประเทศสเปน[39] หรือการแก้ไขเพิ่มเติมกฎหมายเพื่อลดหน้าที่ของผู้ควบคุมข้อมูลในกรณีที่มีการจัดส่งข้อมูลส่วนบุคคลให้แก่บุคคลภายนอกเพื่อประโยชน์ในการทำการตลาดแบบตรง โดยกำหนดให้ผู้ควบคุมข้อมูลนั้นต้องแจ้งให้เจ้าของข้อมูลนั้นทราบถึงการโอนและให้โอกาสในการโต้แย้งด้วยการโฆษณาลงในหนังสือพิมพ์ท้องถิ่น[40]

เนื่องจากวิธีการทำการตลาดที่เกิดขึ้นหลายรูปแบบตามพัฒนาการของเทคโนโลยี รวมทั้งการโทรศัพท์ ส่งข้อความไปรษณีย์อิเล็กทรอนิกส์ การส่งข้อความสั้น (SMS) และรูปแบบทางอิเล็กทรอนิกส์อย่างอื่น ในวันที่ 1 ตุลาคม ค.ศ. 2009 จึงมีการออกกฎหมายกำหนดหน้าที่ให้ผู้ทำการตลาดในลักษณะเช่นนี้จะต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองเจ้าของข้อมูลด้วย เช่น การจัดทำทะเบียนห้ามโทร (“do-not-call registry” หรือ “opt-out register) โดยให้สิทธิเจ้าของ

---

[39] จาก “การโอนข้อมูลส่วนบุคคลระหว่างประเทศ,” โดย ปฏิวัติ อุ่นเรือน, 2547, *วารสารนิติศาสตร์มหาวิทยาลัยธรรมศาสตร์,* 34 (4), น. 589.

[40] *Country Report on Privacy – The Netherlands: Legal Framework.* Retrieved August 7, 2014, from https://www.privacyinternational.org/reports/the-netherlands/i-legal-framework

ข้อมูลที่จะแจ้งห้ามมิให้ผู้ทำการตลาดโทรศัพท์หา นอกจากนี้ยังมีการออกกฎหมายควบคุมการส่งข้อความไปยังไปรษณีย์อิเล็กทรอนิกส์และข้อความสั้นด้วย ซึ่งเป็นกฎหมายที่ห้ามการส่งข้อความไปยังเจ้าของข้อมูลเว้นแต่จะมีการลงทะเบียนว่าต้องการสื่อการตลาดนั้น ("opt-in regime") มีข้อยกเว้นเพียงประการเดียวในกรณีที่เป็นข้อมูลการติดต่อซึ่งรวบรวมจากการขายสินค้าหรือบริการ อาจใช้เพื่อการแจ้งข้อมูลการตลาดของผลิตภัณฑ์อย่างเดียวกันของผู้ขายนั้นเองได้[41]

นอกเหนือจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแล้ว ราชอาณาจักรเนเธอร์แลนด์ยังมีกฎหมายเฉพาะเรื่องที่กล่าวถึงสิทธิในความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลบางประเภทเป็นการเฉพาะ เช่น กฎหมายการทำหน้าที่ของตำรวจ (Dutch Police Data Act of 2008) การค้นเคหสถาน (Dutch Act on Entering of Buildings and Houses of 1994) ข้อมูลการตรวจรักษาของแพทย์ (Dutch Medical Examinations Act of 1997 และ Dutch Medical Treatment Act of 1997) ข้อมูลประกันสังคม (Dutch Social Security System Act of 1997) เป็นต้น

ในการให้ความคุ้มครองข้อมูลส่วนบุคคลนั้น มีการจัดตั้งหน่วยงานชื่อ Dutch Data Protection Authority (College Bescherming Persoonsgegevens - CBP) เพื่อกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย โดยมีอำนาจหน้าที่ในการกำหนดแนวทางการใช้กฎหมายด้วยในเดือนธันวาคม ค.ศ. 2007 หน่วยงาน CBP ได้ออกแนวทางการจัดการข้อมูลส่วนบุคคลที่เผยแพร่บนเครือข่ายอินเตอร์เน็ตตามกฎหมายการคุ้มครองข้อมูลส่วนบุคคล (Guidelines on the processing of personal data in publications on the Internet based on the Dutch Data Protection Act) ซึ่งวางแนวทางในการเผยแพร่สิ่งพิมพ์ที่ปรากฏข้อมูลส่วนบุคคลบนเครือข่ายอินเตอร์เน็ตว่าต้องมีลักษณะอย่างไรและจะเผยแพร่ได้เมื่อใด ภายใต้เงื่อนไขอย่างไร รวมทั้งกำหนดแนวทางให้แก่ประชาชนผู้เป็นเจ้าของข้อมูลเช่นนั้นว่าสามารถดำเนินการอย่างไรได้เมื่อมีการเผยแพร่ข้อมูลของตน[42] หลังจากนั้นหน่วยงาน CBP ก็ออกแนวทางอีกหลายเรื่อง เช่น ในเดือนมกราคม ค.ศ. 2009 กำหนดแนวทางการใช้ข้อมูลจากป้ายทะเบียน (De toepassing van automatische kentekenherkenning door de politie หรือ Application of Automatic Number Plate Recognition by the Police) โดยกำหนดให้การได้มาซึ่งข้อมูลส่วนบุคคลจากเลขทะเบียนรถยนต์โดยตำรวจจะทำได้ต่อเมื่อมีอุบัติเหตุเกิดขึ้นและมีการตรวจสอบข้อมูลป้ายทะเบียนจนพบข้อมูลของผู้เป็นเจ้าของ เพราะหากปล่อยให้ตำรวจเก็บข้อมูลก็อาจส่งผลให้ผู้ใช้ถนนตกเป็นผู้ต้องสงสัยได้โดยง่ายและยังนำไปสู่การ

---

[41] Ibid.

[42] *Privacy legislation also applies on the Internet – Guidelines finalised on the publication of personal data on the Internet.* Retrieved January 25, 2015, from http://www.dutchdpa.nl/Pages/en_pb_20071211_privacy_legislation_internet.aspx

ละเมิดสิทธิในความเป็นส่วนตัวได้อีกด้วย[43] ในเดือนสิงหาคม ค.ศ. 2009 หน่วยงาน CBP กำหนดแนวทางการเผยแพร่ข้อมูลของรัฐที่มีข้อมูลส่วนบุคคลจำพวกหมายเลขประจำตัวบุคคลร่วมอยู่ด้วย เนื่องจากการเผยแพร่ข้อมูลดังกล่าวอาจนำไปสู่การฉ้อโกงโดยใช้หมายเลขประจำตัวบุคคลได้[44]

นอกจากบทบาทในการกำหนดแนวทางการใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว หน่วยงาน CBP ยังทำหน้าที่ให้ความเห็นร่างกฎหมายที่อาจกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลด้วย ครั้งหนึ่งมีการเสนอร่างกฎหมายเพื่อเก็บข้อมูลคนไข้ในรูปอิเล็กทรอนิกส์เพื่อให้ผู้บริการทางการแพทย์และสาธารณสุขใช้ร่วมกัน โดยหน่วยงาน CBP ให้ความเห็นว่าเป็นเรื่องที่มีความเสี่ยงอย่างมากที่จะให้ผู้ให้บริการทุกหน่วยงานสามารถเข้าถึงข้อมูลดังกล่าวได้เพราะอาจนำไปสู่การใช้ข้อมูลเช่นนั้นอย่างไม่เหมาะสมและกระทบต่อสิทธิในข้อมูลส่วนบุคคล โดยควรจำกัดเฉพาะกรณีที่มีเหตุฉุกเฉินเท่านั้นที่จะให้ผู้ทำหน้าที่ดูแลผู้ป่วยในขณะนั้นเข้าถึงข้อมูลได้[45] นอกจากนี้ ในปี ค.ศ. 2007 หน่วยงาน CBP ยังให้ความเห็นเกี่ยวกับการจัดทำข้อมูลของเด็ก (elektronisch kinddossier jeugdgezondheidzorg – EKD หรือ electronic child record for the youth healthcare sector) โดยจะเก็บข้อมูลเกี่ยวกับสุขภาพของเด็กไว้ตั้งแต่แรกเกิด รวมทั้งข้อมูลการฉีดวัคซีน ทั้งนี้หน่วยงาน CBP เห็นว่าว่าจะมีการนำข้อมูลเช่นว่านี้ไปใช้ในทางอื่นที่มิใช่ด้านการแพทย์ เช่น อาจนำไปใช้เพื่อการควบคุมความสงบเรียบร้อย โดยจัดทำบัญชีรายชื่อเยาวชนที่มีความเสี่ยง (VIR หรือ verwijsindex risicojongeren หรือ national reference index of young people at risk) เป็นต้น[46]

2.2.2.3 สหพันธ์สาธารณรัฐเยอรมนี

รัฐธรรมนูญของสหพันธ์สาธารณรัฐเยอรมนี (Grundgesetz หรือ The Basic Law) ได้ให้การรับรองสิทธิในความเป็นส่วนตัวของประชาชนไว้โดยชัดแจ้ง โดยในมาตรา 10 กำหนดว่าสิทธิในความเป็นส่วนตัวในหนังสือ จดหมายและการสื่อสารจะล่วงละเมิดมิได้และข้อจำกัดสิทธิดังกล่าวจะกระทำได้ต่อเมื่อมีกฎหมายให้อำนาจ หากการจำกัดสิทธิโดยกฎหมายเช่นว่านี้เป็นไปเพื่อประโยชน์ในการปกป้องการปกครองระบอบเสรีประชาธิปไตยหรือเพื่อความคงอยู่หรือความ

---

[43] *Country Report on Privacy – The Netherlands: Legal Framework.* Retrieved August 7, 2014, from https://www.privacyinternational.org/reports/the-netherlands/i-legal-framework

[44] *Country Report on Privacy – The Netherlands: Legal Framework.* Retrieved August 7, 2014, from https://www.privacyinternational.org/reports/the-netherlands/i-legal-framework

[45] *Eleventh Annual Report of the Article 29 Working Party on Data Protection.* Retrieved January 25, 2015, from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/11th_annual_report_en.pdf

[46] *EPIC --- Privacy and Human Rights Report 2006 Kingdom of the Netherlands.* Retrieved January 25, 2015, from http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Kingdom-3.html

มั่นคงของรัฐ กฎหมายอาจกำหนดให้ไม่จำต้องแจ้งให้ผู้ต้องเสื่อมเสียสิทธิทราบและการเยียวยาความเสียหายจะได้รับการตรวจสอบโดยหน่วยงานที่แต่งตั้งโดยรัฐสภาแทนการฟ้องเป็นคดีต่อศาล[47]

นอกจากสิทธิในความเป็นส่วนตัวแล้ว สิทธิที่เกี่ยวกับข้อมูลส่วนบุคคลถือเป็นสิทธิขั้นพื้นฐานประการหนึ่งที่รัฐธรรมนูญให้ความคุ้มครองด้วย โดยในปี ค.ศ. 1983 เกิดคดีเรื่องหนึ่งที่เกี่ยวข้องกับกฎหมายเรื่องการสำรวจสำมะโนครัวประชากร โดยมีการเก็บรวบรวมและบันทึกข้อมูลส่วนบุคคลไว้ ศาลรัฐธรรมนูญของสหพันธ์สาธารณรัฐเยอรมนีให้การยอมรับสิทธิในการตัดสินใจเกี่ยวกับข้อมูลของตนเอง (The right of informational self-determination) คดีดังกล่าวศาลพิพากษาไว้มีใจความส่วนหนึ่งว่า ในบริบทของการจัดการข้อมูลสมัยใหม่ การคุ้มครองบุคคลในด้านการรวมรวม จัดเก็บ ใช้และเปิดเผยข้อมูลส่วนบุคคล ถือเป็นเรื่องที่กระทบต่อสิทธิส่วนบุคคลขั้นพื้นฐานภายใต้รัฐธรรมนูญ ซึ่งสิทธิขั้นพื้นฐานนี้ให้การรับรองอำนาจของบุคคลผู้เป็นเจ้าของข้อมูลในอันที่จะกำหนดเงื่อนไขการเปิดเผยและการใช้ข้อมูลของตนได้ โดยสิทธิเช่นว่านี้จะถูกจำกัดได้ก็ต่อเมื่อประโยชน์สาธารณะมีความสำคัญมากกว่า[48] ศาลในคดีนี้ได้นำเอาหลักการของสิทธิในการตัดสินใจเกี่ยวกับข้อมูลตนเองมาจากสิทธิขั้นพื้นฐานและเสรีภาพของบุคคลตามมาตรา 1 และ 2 ของรัฐธรรมนูญ[49]

---

[47] BASIC LAW for the Federal Republic of Germany, Article 10 (Privacy of letters, posts, and telecommunications).

(1) Privacy of letters, posts, and telecommunications shall be inviolable.

(2) Restrictions may only be ordered pursuant to a statute. Where a restriction serves to protect the free democratic basic order or the existence or security of the Federation, the statute may stipulate that the person affected shall not be informed of such restriction and that recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by Parliament.

[48] *Informational Self-Determination.* Retrieved January 25, 2015, from http://en.wikipedia.org/wiki/Informational_self-determination

[49] BASIC LAW for the Federal Republic of Germany, Article 1 (Protection of human dignity).

(1) The dignity of man inviolable. To respect and protect it is the duty of all state authority.

(2) The German people therefore acknowledge inviolable and inalienable human rights as the basis of every community, of peace and of justice in the world.

(3) The following basic rights bind the legislature, the executive and the judiciary as directly enforceable law.

BASIC LAW for the Federal Republic of Germany, Article 2 (Rights of liberty).

ในส่วนที่เกี่ยวกับกฎหมายในเรื่องความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลนั้น สหพันธ์สาธารณรัฐเยอรมนีถือเป็นประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เคร่งครัดที่สุดประเทศหนึ่งในกลุ่มสหภาพยุโรป โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกเกิดขึ้นในรัฐเฮสเซิน (Hessen หรือ Hesse) ในปี ค.ศ. 1970 ต่อมาในปี ค.ศ. 1977 สหพันธ์สาธารณรัฐเยอรมนีได้ตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับประเทศ (Bundesdatenschutzgesetz - BDSG) ซึ่งมีการแก้ไขหลายครั้ง การแก้ไขครั้งสำคัญเกิดขึ้นในปี ค.ศ. 2001 เพื่อให้สอดคล้องกับกฎหมายของสหภาพยุโรปในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

หลักการสำคัญพื้นฐานของกฎหมาย BDSG คือการคุ้มครองสิทธิในความเป็นส่วนตัวซึ่งถูกกระทบจากการเก็บและใช้ข้อมูลส่วนบุคคล กฎหมายคุ้มครองไปถึงการเก็บรวบรวม การประมวลผลและการใช้ข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐ รวมทั้งการดำเนินการโดยเอกชนที่ใช้ระบบประมวลผลเพื่อการค้าและธุรกิจ

ในปี ค.ศ. 2001 มีการแก้ไขกฎหมาย BDSG ให้รวมถึงบทบัญญัติเกี่ยวกับการส่งผ่านข้อมูลส่วนบุคคลไปยังต่างประเทศ การสอดส่องผ่านกล้องวีดิโอ การปกปิดชื่อและการใช้นามแฝง การใช้บัตรสมาร์ทการ์ด การเก็บรวบรวมข้อมูลที่มีลักษณะต้องห้ามหรือมีความอ่อนไหว เช่น สีผิว เชื้อชาติ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา การเข้าร่วมเป็นสมาชิกในกลุ่ม ข้อมูลด้านสุขภาพเป็นต้น ซึ่งให้สิทธิแก่เจ้าของข้อมูลในการปฏิเสธการอนุญาตให้เก็บข้อมูลนั้นได้และยังกำหนดให้บริษัทเอกชนที่เก็บรวมรวม ประมวลผลและใช้ข้อมูลส่วนบุคคล จะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตนเองด้วยต่างหากจากเจ้าหน้าที่ของรัฐ มิฉะนั้นการประมวลผลข้อมูลทุกครั้งจะต้องจดทะเบียนต่อคณะกรรมการคุ้มครองข้อมูลของรัฐ (The Federal Commissioner for Data Protection and Freedom of Information หรือ Bundesbeauftragter für den Datenschutz und die Informationsfreiheit - BfDI) กฎหมายฉบับนี้ยังกำหนดให้ต้องขอความยินยอมจากเจ้าของข้อมูลที่เก็บรวบรวมภายหลังจากการแจ้งให้ทราบแล้วด้วย

ต่อมามีการพิจารณาแก้ไขปรับปรุงกฎหมาย BDSG ครั้งสำคัญในปี ค.ศ. 2005 สืบเนื่องจากข้อแนะนำของผู้เชี่ยวชาญที่มีการจัดทำขึ้นตั้งแต่ปี ค.ศ. 2001[50] โดยมีการแนะนำให้ลดจำนวน

---

(1) Everyone has the right to the free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral code.

(2) Everyone has the right to life and to inviolability of his person. The freedom of the individual is inviolable. These rights may only be encroached upon pursuant to a law.

[50] *Country Report on Privacy - Germany: Legal Framework*. Retrieved August 7, 2014, from https://www.privacyinternational.org/reports/germany/i-legal-framework

กฎหมายที่กล่าวถึงรายละเอียดของการคุ้มครองความเป็นส่วนตัวลงให้เหลือเพียงกฎหมายฉบับเดียวแล้วจึงนำรายละเอียดไปใส่ไว้ในกฎหมายลำดับรองเท่าที่จำเป็น ต่อมาในปี ค.ศ. 2006 มีการแก้ไขเพิ่มเติมเงื่อนไขเกี่ยวกับการมีเจ้าหน้าที่คุ้มครองข้อมูลประจำบริษัทเอกชนโดยจากเดิมที่กำหนดให้บริษัทที่มีพนักงาน 4 คน ต้องมีเจ้าหน้าที่คุ้มครองข้อมูล ปรับเปลี่ยนเงื่อนไขเป็นบริษัทที่มีพนักงาน 9 คนขึ้นไป ซึ่งส่งผลให้บริษัทขนาดเล็กไม่ถูกบังคับให้ต้องมีเจ้าหน้าที่คุ้มครองข้อมูลต่อไป นอกจากนี้ในปี ค.ศ. 2009 มีการปรับปรุงกฎหมายเรื่องการใช้ระบบให้คะแนนเครดิต การประมวลผลข้อมูลโดยผู้ประมวลผลซึ่งเป็นบุคคลภายนอกแทนผู้ควบคุมข้อมูล สิทธิของเจ้าของข้อมูลในการเข้าถึงฐานข้อมูลเครดิตและหน้าที่ของบริษัทในการแจ้งให้ทราบถึงการสูญหายของข้อมูลจำนวนมาก

นอกเหนือจากกฎหมาย BDSG ซึ่งเป็นกฎหมายทั่วไปแล้ว สหพันธ์สาธารณรัฐเยอรมนียังออกกฎหมายที่ใช้กับการให้บริการออนไลน์เป็นการเฉพาะด้วย เรียกโดยรวมว่ากฎหมายว่าด้วยบริการสารสนเทศและการสื่อสาร (Informations- und Kommunikationsdienste-Gesetz - IuKDG) โดยประกอบด้วยบทบัญญัติของกฎหมายสำคัญ 3 เรื่อง ได้แก่รัฐบัญญัติบริการสารสนเทศ รัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคลจากการบริการสารสนเทศและรัฐบัญญัติลายมือชื่อดิจิทัล โดยกฎหมายดังกล่าวจะใช้กับการให้บริการออนไลน์ที่อยู่ภายใต้นิยามคำว่า บริการสารสนเทศ (Teleservice) ซึ่งหมายความถึงบริการสารสนเทศและการสื่อสารที่อยู่ในรูปอิเล็กทรอนิกส์ทุกประเภทที่ถูกออกแบบมาเพื่อให้บุคคลใช้ข้อมูลที่มีความหลากหลายรูปแบบประกอบกัน เช่น ลักษณะ ภาพ หรือเสียง เป็นต้น และเป็นบริการที่มีการส่งผ่านด้วยวิธีการโทรคมนาคม[51]

ในส่วนของรัฐบัญญัติการคุ้มครองข้อมูลส่วนบุคคลจากบริการสารสนเทศนั้นมีผลใช้บังคับครั้งแรกในปี ค.ศ. 1997 เพื่อคุ้มครองข้อมูลส่วนบุคคลที่ได้มาจากการใช้งานบนเครือข่ายอินเตอร์เน็ตโดยมุ่งเน้นให้ผู้ประกอบการเว็บไซต์ต้องจัดให้มีการแจ้งเตือนให้ทราบข้อมูลติดต่อของผู้ประกอบการ ตลอดจนการเก็บรวบรวมและการใช้ข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลนั้น และจะต้องไม่ใช้มาตรการบังคับให้เจ้าของข้อมูลจำต้องให้ความยินยอมเพื่อให้ได้รับบริการที่ดีกว่าปกติ อย่างไรก็ดีเนื่องจากนิยามของกฎหมายที่ค่อนข้างจำกัดรูปแบบและไม่เหมาะสมกับการขยายตัวของการใช้งานอินเตอร์เน็ต ซึ่งมักสร้างความไม่ชัดเจนในการปรับใช้กฎหมายเสมอ ในปี ค.ศ. 2007 จึงมีการตรารัฐบัญญัติสื่อสารสนเทศ (Telemedia Act) เพื่อใช้บังคับแทนกฎหมายว่าด้วยบริการสารสนเทศและการสื่อสารทั้งหมด โดยยังคงเนื้อหาสาระในการ

---

[51] Joel R. Reidenberg and Paul M. Schwartz. (n.d.). *Data Protection Law and On-Line Services: Regulatory Responses.* Retrieved January 25, 2015, from http://ec.europa.eu/justice/data-protection/document/studies/files/19981201_dp_law_online_regulatory_en.pdf

คุ้มครองข้อมูลส่วนบุคคลตามกฎหมายเดิมและเพิ่มขอบเขตให้มีความครอบคลุมชัดเจนมากยิ่งขึ้น โดยในมาตรา 13 กำหนดหน้าที่ของผู้ให้บริการในการคุ้มครองข้อมูลส่วนบุคคล เช่น ต้องแจ้งให้ผู้ใช้งานทราบรายละเอียดของข้อมูลและเหตุผลในการเก็บรวบรวมและประมวลผลข้อมูลนั้นเป็นต้น[52]

นอกเหนือจากกฎหมายกลางของประเทศแล้ว เนื่องจากสหพันธ์สาธารณรัฐเยอรมนีมีรูปแบบการปกครองแบบสหพันธ์สาธารณรัฐประชาธิปไตยแบบรัฐสภา แบ่งการปกครองในระบบสหพันธรัฐ มีทั้งหมด 16 รัฐ แต่ละรัฐจะมีรัฐบาลท้องถิ่นเป็นของตัวเองและจะมีกระทรวงการปกครองบริหารสูงสุดซึ่งจะดูแลรัฐทุกรัฐของสหพันธ์สาธารณรัฐเยอรมนี[53] ในแต่ละรัฐจึงออกกฎระเบียบเฉพาะเพื่อคุ้มครองข้อมูลส่วนบุคคลของตนเองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป และมีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อบังคับตามกฎหมายของรัฐด้วย[54] อย่างไรก็ดีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหพันธ์สาธารณรัฐเยอรมนีก็ไม่มีบทบัญญัติที่กล่าวถึงเด็กเป็นการเฉพาะแต่อย่างใด

2.2.2.4 สมาพันธรัฐสวิส

ในอดีตรัฐธรรมนูญของสมาพันธรัฐสวิสในมาตรา 36 (4) ได้ให้หลักประกันการเก็บรักษาความลับของจดหมายและไปรษณีย์โทรเลขไว้[55] ซึ่งรัฐธรรมนูญฉบับนี้มีการแก้ไขเพิ่มเติมในเวลาต่อมาโดยในวันที่ 1 มกราคม ค.ศ. 2000 ซึ่งเป็นวันที่รัฐธรรมนูญฉบับใหม่มีผลใช้บังคับได้มีการขยายขอบเขตการคุ้มครองสิทธิในความเป็นส่วนตัวเพิ่มเติมออกไปโดยกำหนดไว้ในมาตรา 13 รับรองสิทธิของประชาชนในการได้รับการเคารพความเป็นส่วนตัว ชีวิตครอบครัว เคหสถาน และความลับของไปรษณีย์และการสื่อสารและมีสิทธิได้รับความคุ้มครองจากการใช้ข้อมูลส่วนบุคคลในทางมิชอบ[56]

---

[52] Henning Krieg. (n.d.). *German Telemedia Act introduces new rules for New Media.* Retrieved January 25, 2015, from http://www.twobirds.com/en/news/articles/2007/german-tele-media-act-new-rules

[53] *Germany.* Retrieved January 15, 2015, http://en.wikipedia.org/wiki/Germany

[54] *The North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information (LDI NRW), Data Protection.* Retrieved January 25, 2015, from https://www.ldi.nrw.de/LDI_EnglishCorner/mainmenu_DataProtection/Inhalt2/authorities/regulation.php

[55] 1874 Constitution of Switzerland, Section 36(4): The inviolability of the secrecy of letters and telegrams is guaranteed.

[56] Switzerland Constitution, Article 13, Protection of Privacy:

(1) Every person has the right to respect for his or her private and family life, home, and secrecy of mail and telecommunication.

กฎหมายของประเทศที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลถูกบัญญัติขึ้นครั้งแรกในปี ค.ศ. 1992 ชื่อว่า The Federal Act of Data Protection (Loi fédérale sur la protection des données - LPD) ซึ่งวางเงื่อนไขเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลทั้งที่ครอบครองโดยหน่วยงานของรัฐและเอกชน กฎหมายฉบับนี้กำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องกระทำโดยชอบด้วยกฎหมายและเป็นธรรม กล่าวคือจะต้องใช้วิธีการที่ชอบด้วยกฎหมายในการเก็บรวบรวมโดยให้เจ้าของข้อมูลนั้นทราบก่อน และต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ห้ามมิให้ใช้การแอบบันทึกข้อมูลโดยเจ้าของข้อมูลไม่รู้ตัวล่วงหน้า[57] โดยการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นถือเป็นการประมวลผลข้อมูลอย่างหนึ่งตามนิยามและวางข้อจำกัดในการใช้และเปิดเผยข้อมูลต่อบุคคลที่สาม บริษัทเอกชนจะต้องจดทะเบียนหากมีการประมวลผลข้อมูลที่มีความละเอียดอ่อนหรือมีการโอนข้อมูลไปยังบุคคลภายนอก การโอนข้อมูลไปยังต่างประเทศจะต้องจดทะเบียนและประเทศของผู้รับโอนจะต้องมีกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลอย่างเดียวกัน และเจ้าของข้อมูลมีสิทธิเข้าถึงข้อมูลและมีสิทธิแก้ไขข้อมูลให้ถูกต้องได้[58]

ในเดือนมิถุนายน ค.ศ. 1999 คณะทำงานคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปได้ประกาศว่ากฎหมายของสมาพันธรัฐสวิสเป็นไปตามมาตรฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (EU Data Protection Directive) และในเดือนกรกฎาคม ค.ศ. 2000 คณะกรรมการสหภาพยุโรปอนุญาตให้โอนข้อมูลส่วนบุคคลไปยังสมาพันธรัฐสวิสได้โดยมีการรับรองอีกครั้งในวันที่ 20 ตุลาคม ค.ศ. 2004

ในเดือนมีนาคม ค.ศ. 2006 มีการเสนอแก้ไขกฎหมาย LPD โดยเพิ่มเติมเรื่องสำคัญ เช่น หน้าที่แจ้งให้เจ้าของข้อมูลทราบเกี่ยวกับการเก็บรวบรวมข้อมูลและวัตถุประสงค์ในการรวบรวมและแจ้งให้ทราบหากจะมีการโอนข้อมูลนั้นต่อไปให้บุคคลภายนอก นอกจากนี้ยังกำหนดมาตรการในการออกเครื่องหมายรับรองคุณภาพการคุ้มครองข้อมูลส่วนบุคคล แก้ไขเงื่อนไขเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศและกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลที่ต้องการโอนข้อมูลให้บุคคลภายนอกจะต้องแจ้งให้คณะกรรมการทราบเกี่ยวกับสัญญากับบุคคลภายนอกและเงื่อนไข

---

(2) Every person has the right to be protected against abuse of personal data.

[57] Walder Wyss Ltd. (n.d.). *Collecting Data is Data Processing.* Retrieved January 25, 2015, from http://www.dataprotection.ch/en/collecting-personal-data.asp

[58] Global Internet Liberty Campaign. (n.d.). *Privacy and Human Rights Survey.* Retrieved January 25, 2015, from http://gilc.org/privacy/survey/surveylz.html#

การคุ้มครองข้อมูลส่วนบุคคลของบุคคลภายนอกดังกล่าว เป็นต้น โดยการแก้ไขเพิ่มเติมมีผลบังคับใช้ในปี ค.ศ. 2008[59]

นอกจากกฎหมาย LPD แล้ว กฎหมายคุ้มครองความเป็นส่วนตัวของสมาพันธรัฐสวิสยังกระจัดกระจายอยู่ในประมวลกฎหมายแพ่ง ประมวลกฎหมายอาญาและกฎหมายพิเศษอีกด้วย เช่น การคุ้มครองความเป็นส่วนตัวของพนักงานจากการสอดส่องตรวจตรา ข้อมูลสารสนเทศ สถิติการรักษาพยาบาล การเก็บรักษาความลับในวิชาชีพรวมทั้งด้านการแพทย์และกฎหมาย งานวิจัยทางการแพทย์และบัตรประจำตัวประชาชน เป็นต้น

ในด้านหน่วยงานที่กำกับดูแลการปฏิบัติตามและการบังคับใช้กฎหมายนั้น มีการตั้งเจ้าหน้าที่ Federal Data Protection and Information Commissioner (the Commissioner, or FDPIC) ซึ่งจะทำหน้าที่เก็บรักษาทะเบียนแฟ้มข้อมูล กำกับดูแลหน่วยงานทั้งภาครัฐและเอกชน ให้คำแนะนำ จัดทำรายงาน ตรวจสอบการบังคับใช้กฎหมาย ตลอดจนทำหน้าที่เป็นผู้ไกล่เกลี่ยข้อพิพาทที่เกี่ยวข้องด้วย[60]

นอกเหนือจากกฎหมาย LPD แล้ว เนื่องจากสวิตเซอร์แลนด์ได้เริ่มใช้การปกครองระบอบประชาธิปไตยแบบรัฐสภา แต่มีลักษณะการรวมตัวของรัฐ (Canton) ต่าง ๆ รวม 26 รัฐ อยู่ภายใต้รัฐบาลกลาง เรียกว่า สมาพันธรัฐ[61] ในหลายรัฐมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลและคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของรัฐนั้นเอง[62] และเพื่อสร้างความร่วมมือในการดำเนินงานและการแลกเปลี่ยนความคิดเห็น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของรัฐได้รวมตัวกันตั้งเป็นสมาคม PRIVATIM ในเดือนมีนาคม ค.ศ. 2000 และมีการแต่งตั้งคณะทำงานภายใน เช่น คณะทำงานปัญหาข้อมูลด้านสุขภาพ เป็นต้น[63]

อย่างไรก็ดีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสมาพันธรัฐสวิสก็ไม่มีบทบัญญัติที่กล่าวถึงเด็กเป็นการเฉพาะแต่อย่างใด

---

[59] *The History of Data Protection in Switzerland.* Retrieved January 25, 2015, from http://www.edoeb.admin.ch/org/00129/00132/index.html?lang=en

[60] *Task of the Federal Data Protection and Information Commissioner.* Retrieved January 25, 2015, from http://www.edoeb.admin.ch/org/00126/index.html?lang=en

[61] Switzerland. Retrieved January 25, 2015, from http://en.wikipedia.org/wiki/Switzerland

[62] *Swiss Data Protection – Legal Framework.* Retrieved January 25, 2015, from http://www.dataprotection.ch/en/legal-framework.asp

[63] *Country Report on Privacy - Switzerland: Legal Framework.* Retrieved August 7, 2014, from https://www.privacyinternational.org/reports/switzerland/i-legal-framework

2.2.3 วิวัฒนาการของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศญี่ปุ่น

รัฐธรรมนูญของประเทศญี่ปุ่นในมาตรา 13 ให้การรับรองว่า สิทธิในชีวิต เสรีภาพและการดำเนินชีวิตอย่างปกติสุขถือเป็นเงื่อนไขสำคัญในการออกกฎหมายและการบริหารงานของรัฐบาล เว้นแต่จะเป็นการขัดต่อประโยชน์สาธารณะและในมาตรา 21 ให้เสรีภาพแก่ประชาชนในการติดต่อสื่อสารและแสดงความคิดเห็น กับในมาตรา 35 กำหนดถึงการค้นและการยึดต้องกระทำโดยมีหมายศาลบนพื้นฐานของเหตุผลอันสมควร[64]

ในปี ค.ศ. 1963 ศาลฎีกาของประเทศญี่ปุ่นได้รับรองสิทธิในความเป็นส่วนตัวโดยถือเป็นสิทธิอย่างหนึ่งตามมาตรา 13 ของรัฐธรรมนูญ นับแต่นั้นมาสิทธิในความเป็นส่วนตัวของประชาชนได้รับการรับรองและปรับใช้กับข้อเท็จจริงต่าง ๆ ผ่านหลักกฎหมายทั่วไปในเรื่องละเมิดตามประมวลกฎหมายแพ่ง[65]

ในปี ค.ศ. 1999 รัฐบาลญี่ปุ่นตระหนักถึงการขยายตัวของสังคมข้อมูลข่าวสาร เครือข่ายสารสนเทศนานาชาติและระบบพาณิชย์อิเล็กทรอนิกส์ จึงประกาศโครงการตระเตรียมร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยอาศัยหลักการพื้นฐาน 5 ประการ ได้แก่[66]

---

[64] Japan Constitution, Article 13:

All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs.

Japan Constitution, Article 21:

Freedom of assembly and association as well as speech, press and all other forms of expression are guaranteed.

No censorship shall be maintained, nor shall the secrecy of any means of communication be violated.

Japan Constitution, Article 35:

The right of all persons to be secure in their homes, papers and effects against entries, searches and seizures shall not be impaired except upon warrant issued for adequate cause and particularly describing the place to be searched and things to be seized, or except as provided by Article 33.

Each search or seizure shall be made upon separate warrant issued by a competent judicial officer.

[65] *Country Report on Privacy - Japan: Legal Framework.* Retrieved August 7, 2014, from https://www.privacyinternational.org/reports/japan/i-legal-framework

[66] จาก “กฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลในประเทศญี่ปุ่น” โดย กิตติศักดิ์ ปรกติ, 2547, *วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์,* 34(4), น.525

(1) ต้องกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลให้ชัดเจนและจัดระบบข้อมูลตามวัตถุประสงค์ที่ประกาศไว้

(2) การจัดเก็บข้อมูลส่วนบุคคลต้องกระทำโดยชอบด้วยกฎหมายและใช้วิธีการที่เหมาะสม

(3) การเก็บรักษาและปรับปรุงข้อมูลให้แน่นอนถูกต้องและเป็นปัจจุบันอยู่เสมอ

(4) จัดระบบรักษาความปลอดภัยให้แก่ข้อมูลที่จัดเก็บ

(5) จัดระบบการจัดเก็บและใช้ข้อมูลภายใต้หลักความโปร่งใส

ต่อมาวันที่ 23 พฤษภาคม ค.ศ. 2003 รัฐสภาได้พิจารณาร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในฐานะที่เป็นกฎหมายทั่วไป โดยมีกฎหมายเฉพาะเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอีก 4 ฉบับ ที่พิจารณาไปพร้อมกันได้แก่ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในความครอบครองดูแลของหน่วยงานฝ่ายปกครอง กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในความครอบครองดูแลขององค์กรอิสระและองค์การมหาชนอื่น กฎหมายว่าด้วยการจัดตั้งคณะกรรมการวินิจฉัยการเปิดเผยและการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายว่าด้วยการเตรียมการบังคับให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในความครอบครองดูแลของหน่วยงานฝ่ายปกครอง โดยมีการตราเป็นกฎหมายในวันที่ 30 พฤษภาคม ค.ศ. 2003[67]

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้ในวันที่ 1 เมษายน ค.ศ. 2005 โดยกฎหมายดังกล่าวให้นิยามของข้อมูลส่วนบุคคลไว้หมายถึงข้อมูลที่เกี่ยวข้องกับบุคคลที่ยังมีชีวิตและสามารถใช้เพื่อระบุตัวตนของบุคคลนั้นได้ ไม่ว่าจะเป็นชื่อ วันเกิดหรือข้อมูลอย่างอื่น นอกจากนี้ ยังกล่าวถึงการจัดการข้อมูลส่วนบุคคลขององค์กรธุรกิจ สอดคล้องกับหลักการคุ้มครองข้อมูลตามแนวทางของ OECD ด้วยและเพื่อเป็นการสนับสนุนระบบการวางข้อกำหนดของตนเองและจัดการเรื่องร้องเรียนเกี่ยวกับข้อมูลส่วนบุคคลในภาคเอกชน กฎหมายยังให้อำนาจแก่รัฐมนตรีที่เกี่ยวข้องในการจัดตั้งหน่วยงานเพื่อการคุ้มครองข้อมูลส่วนบุคคลในเรื่องเกี่ยวกับอำนาจหน้าที่ของตนเอง รวมทั้งมีอำนาจออกข้อแนะนำหรือคำสั่งเพื่อให้ภาคธุรกิจปฏิบัติตามโดยกำหนดโทษทางอาญาในกรณีที่มีการฝ่าฝืน

ข้อน่าสนใจของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่นนั้นอยู่ที่ลักษณะของการตรากฎหมายที่วางมาตรฐานการคุ้มครองไม่เคร่งครัดจนเกินไปและยอมให้มีการตรากฎหมายเฉพาะที่มีความเคร่งครัดมากกว่าสำหรับข้อมูลส่วนบุคคลบางประเภท นอกจากนี้แม้ว่าลักษณะของกฎหมายที่มีการตราขึ้นจะยึดหลักการอย่างเดียวกับสหภาพยุโรปที่ถือว่าการคุ้มครองข้อมูลส่วนบุคคลเป็นการคุ้มครองสิทธิในสภาพบุคคล มิใช่สิทธิในทรัพย์สินอีกทั้งวางกลไกให้

---

[67] *กฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลในประเทศญี่ปุ่น* (น. 527). เล่มเดิม.

สิทธิแก่ผู้เป็นเจ้าของข้อมูลและมาตรการในการคุ้มครองที่คล้ายกัน แต่กฎหมายญี่ปุ่นนั้นมีลักษณะที่เป็นคุณแก่ผู้ประกอบการมากกว่ากฎหมายของประเทศในสหภาพยุโรป เช่น ไม่ได้ใช้มาตรการบังคับให้ผู้ประกอบการจะต้องขอความยินยอมจากเจ้าของข้อมูลก่อนการเก็บหรือใช้ข้อมูลส่วนบุคคล (opt-in) แต่วางกลไกให้สามารถเก็บรวบรวมได้ แล้วต้องแจ้งให้เจ้าของข้อมูลนั้นทราบ โดยเจ้าของข้อมูลมีสิทธิที่จะโต้แย้งหรือขอให้ลบข้อมูลนั้นได้ (opt-out) และไม่มีกลไกการห้ามโอนข้อมูลส่วนบุคคลไปยังประเทศที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ต่ำกว่าแต่อย่างใด เป็นต้น[68]

อย่างไรก็ดีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่นก็ไม่มีบทบัญญัติที่กล่าวถึงเด็กเป็นการเฉพาะแต่อย่างใด คงมีเพียงการกล่าวถึงในกฎหมายลำดับรอง (Cabinet Order) ที่ออกโดยอาศัยอำนาจตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดไว้ในมาตรา 8 ว่าในกรณีที่เจ้าของข้อมูลส่วนบุคคลนั้นเป็นผู้เยาว์ อาจเรียกให้ผู้ประกอบการเปิดเผยข้อมูลที่จัดเก็บ แก้ไขข้อมูล ยุติการใช้ หรืออธิบายเหตุผลของการดำเนินการตามที่กำหนดไว้ โดยผ่านทางผู้แทนโดยชอบธรรมก็ได้ ซึ่งไม่ได้กำหนดเกณฑ์อายุของผู้เยาว์หรือวิธีการดำเนินการไว้เป็นพิเศษแต่อย่างใด

2.2.4 วิวัฒนาการของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในสาธารณรัฐเกาหลี

รัฐธรรมนูญของสาธารณรัฐเกาหลีได้ให้ความคุ้มครองในเสรีภาพและความลับในความเป็นส่วนตัว โดยสิทธิในความเป็นอยู่และการครอบครองเคหสถานของตนจะต้องได้รับการเคารพ การค้นและยึดในเคหสถานจะกระทำไม่ได้เว้นแต่จะมีหมายศาล[69] และการล่วงละเมิดต่อความเป็นส่วนตัวตลอดจนความเป็นส่วนตัวในการสื่อสารจะกระทำมิได้[70]

ในอดีตการคุ้มครองข้อมูลส่วนบุคคลในสาธารณรัฐเกาหลีนั้นมุ่งเน้นในภาครัฐมากกว่าภาคเอกชน สืบเนื่องจากมีการใช้ข้อมูลหมายเลขบัตรประจำตัวประชาชนและข้อมูลทะเบียนบ้านอย่างแพร่หลาย ในปี ค.ศ. 1995 จึงมีการตรารัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่เก็บรักษาโดยหน่วยงานของรัฐ (The Act on the Protection of Personal Information Maintained by Public

---

[68] แหล่งเดิม.

[69] The Constitution of the Republic of Korea, Section 16:

All citizens shall be free from intrusion into their place of residence. In case of search or seizure in a residence, a warrant issued by a judge upon request of a prosecutor shall be presented.

[70] The Constitution of the Republic of Korea, Section 17:

The privacy of no citizen shall be infringed

The Constitution of the Republic of Korea, Section 18:

Privacy of correspondence of no citizen shall be infringed.

Agencies) (공공기관의 개인정보보호에 관한 법률) ซึ่งควบคุมการเก็บข้อมูลส่วนบุคคลให้เป็นไปตามแนวปฏิบัติและข้อแนะนำขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ว่าด้วยการคุ้มครองความเป็นส่วนตัวและการส่งโอนข้อมูลส่วนบุคคลข้ามพรมแดน ดังนั้นกฎหมายฉบับนี้จึงวางอยู่บนหลักการสำคัญ 8 ประการ ในการคุ้มครองข้อมูลส่วนบุคคลตามที่ปรากฏอยู่ในแนวปฏิบัติดังกล่าว[71]

รัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่เก็บรักษาโดยหน่วยงานของรัฐกำหนดเงื่อนไขให้หน่วยงานของรัฐมีหน้าที่ดูแลฐานข้อมูลส่วนบุคคลและต้องรายงานฐานข้อมูลนั้นไปยังกระทรวงมหาดไทย (Ministry of Government Administration and Home Affairs) ซึ่งเป็นผู้รักษาการตามกฎหมายโดยกระทรวงมหาดไทยจะประกาศรายชื่อฐานข้อมูลดังกล่าวในสื่อสิ่งพิมพ์ที่เผยแพร่ทั่วไป และกระทรวงมหาดไทยมีอำนาจในการขอข้อมูลที่เกี่ยวข้องจากผู้เก็บรักษาข้อมูลนั้นและให้ความเห็นเกี่ยวกับแนวทางปฏิบัติในการดูแลข้อมูลส่วนบุคคลได้ด้วย อย่างไรก็ดีกฎหมายฉบับนี้ถูกวิพากษ์วิจารณ์อย่างมากว่าไม่มีประสิทธิภาพในการบังคับใช้ เนื่องจากกระทรวงมหาดไทยไม่ได้เข้มงวดต่อการปฏิบัติตามกฎหมายดังกล่าว ในปี ค.ศ. 1999 มีการแก้ไขกฎหมายฉบับนี้เพื่อเพิ่มอำนาจให้แก่กระทรวงมหาดไทยและวางกระบวนการให้เจ้าของข้อมูลสามารถเข้าถึงและตรวจสอบข้อมูลส่วนบุคคลของตนได้ ตลอดจนวางเงื่อนไขจำกัดการเปิดเผยข้อมูลส่วนบุคคล อย่างไรก็ดีการแก้ไขเพิ่มเติมดังกล่าวยังคงขาดกระบวนการตรวจสอบการบังคับใช้กฎหมายที่เป็นอิสระ[72]

ทั้งนี้กลไกการให้ความคุ้มครองข้อมูลส่วนบุคคลในภาครัฐยังปรากฏในกฎหมายเฉพาะเรื่องอีกหลายเรื่อง เช่น รัฐบัญญัติว่าด้วยความลับในการสื่อสาร (The Act on Communication Secrets) (통신비밀보호법) รัฐบัญญัติธุรกิจโทรคมนาคม (The Telecommunications Business Act) (전기통신사업법) รัฐบัญญัติว่าด้วยการแพทย์ (The Medical Act) (의료법) เป็นต้น

ส่วนภาคเอกชนนั้นกลไกของกฎหมายที่จะให้ความคุ้มครองข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมโดยภาคเอกชนในช่วงแรกคงมีเพียงเฉพาะบางกิจการที่ถูกกำหนดไว้ในกฎหมายเฉพาะ เช่น รัฐบัญญัติว่าด้วยข้อมูลเครดิต (The Credit Information Act) (신용정보의 이용 및 보호에 관한 법률) รัฐบัญญัติว่าด้วยธุรกรรมทางอิเล็คทรอนิกส์ (The Framework Act on Electronic Commerce) (전자거래기본법) รัฐบัญญัติว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ (The Electronic

---

[71] *Data Protection.* Retrieved August 7, 2014, from http://koreanlii.or.kr/w/index.php/Data_protection

[72] *Country Report on Privacy – South Korea: Legal Framework.* Retrieved August 7, 2014, from https://www.privacyinternational.org/reports/south-korea/i-legal-framework

Signature Act) (전자서명법) และรัฐบัญญัติคุ้มครองข้อมูลและการใช้งานเครือข่ายสารสนเทศและการสื่อสาร (The Act on Promotion of Information and Communication Network Utilization and Information Protection) (정보통신망이용촉진 및 정보보호 등에 관한 법률)

รัฐบัญญัติคุ้มครองข้อมูลและการใช้งานเครือข่ายสารสนเทศและการสื่อสาร มีวัตถุประสงค์สำคัญในการสนับสนุนการใช้เครือข่ายสารสนเทศและการสื่อสาร จึงมุ่งให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้บริการเครือข่ายสารสนเทศและการสื่อสารและสร้างความมั่นใจให้ผู้ใช้เครือข่ายสามารถใช้งานได้อย่างปลอดภัย[73] อย่างไรก็ดีกฎหมายฉบับนี้ก็ยังไม่สามารถปรับใช้กับการคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชนกรณีทั่วไปที่ไม่ได้มีการใช้งานเครือข่ายสารสนเทศและการสื่อสารได้ จึงมีแนวความคิดในการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในลักษณะที่เป็นกฎหมายทั่วไป จนกระทั่งในเดือนมีนาคม ค.ศ. 2011 จึงมีการประกาศใช้รัฐบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (The Personal Information Protection Act) (개인정보보호법/個人情報保護法) ซึ่งมีผลใช้บังคับในวันที่ 30 กันยายน ค.ศ. 2011 และมีลักษณะเป็นกฎหมายทั่วไปที่ใช้กับทั้งภาครัฐและเอกชน โดยไม่กระทบต่อกฎหมายเฉพาะเรื่องที่มีผลบังคับอยู่ก่อนแล้ว[74]

2.3 แนวคิดเกี่ยวกับสิทธิเด็กกับการคุ้มครองข้อมูลส่วนบุคคลของเด็ก

แนวความคิดสากลยอมรับตรงกันว่าเด็กยังไม่มีความพร้อมทั้งด้านกายภาพและจิตใจ จึงจำเป็นต้องได้รับการปกป้องดูแลเป็นพิเศษ รวมทั้งการคุ้มครองโดยกฎหมายที่เหมาะสมตั้งแต่ช่วงเวลาก่อนและภายหลังจากที่เด็กเกิด[75] แนวคิดดังกล่าวเป็นเหตุผลสำคัญที่หลักกฎหมายของทุกประเทศทั่วโลกกำหนดให้ผู้เยาว์ที่ยังไม่บรรลุนิติภาวะยังไม่อาจตัดสินใจได้ด้วยตนเองและจะต้องให้ผู้แทนโดยชอบธรรมเป็นผู้ทำหน้าที่ตัดสินใจแทน ด้วยเหตุนี้อาจทำให้ดูเหมือนว่าเด็กไม่มีอำนาจจัดการดูแลชีวิตของตนเองได้ แต่ในความเป็นจริงแล้วเด็กเป็นส่วนหนึ่งของสังคมซึ่งมีสิทธิและความรับผิดชอบของตนเองที่ต้องได้รับการยอมรับด้วย

---

[73] Act on Promotion of Information and Communication Network Utilization and Information Protection, Section 1

[74] *Personal Information Protection Act.* Retrieved January 25, 2015, from http://koreanlii.or.kr/w/index.php/Personal_Information_Protection_Act

[75] คำนำในปฏิญญาสากลว่าด้วยสิทธิเด็กขององค์การสหประชาชาติ

Whereas the child, by reason of his physical and mental immaturity, needs special safeguards and care, including appropriate legal protection, before as well as after birth.

สิทธิของเด็กได้รับการกล่าวถึงครั้งแรกในหนังสือ Commentaries on the Law of England ของ Sir William Blackstone (ค.ศ. 1765 - ค.ศ. 1769) โดยกล่าวถึงหน้าที่ของผู้ปกครองต่อเด็ก 3 ประการ ได้แก่ หน้าที่ดูแล คุ้มครองและให้การศึกษา ซึ่งหน้าที่ดังกล่าวถือเป็นสิทธิของเด็กที่จะได้รับจากผู้ปกครองของตน

ต่อมาในปี ค.ศ. 1924 องค์การสันนิบาตชาติ (The League of Nations) ได้ออกปฏิญญาสากลเจนีวาว่าด้วยสิทธิเด็ก ซึ่งประกาศสิทธิของเด็กที่จะได้รับการส่งเสริมพัฒนาการตามปกติ สิทธิของเด็กผู้ยากไร้ที่จะได้รับอาหาร สิทธิของเด็กที่ป่วยที่จะได้รับการรักษา สิทธิของเด็กที่มีพัฒนาการช้าที่จะได้รับการปรับปรุงแก้ไข สิทธิของเด็กผู้กำพร้าที่จะได้รับที่อยู่อาศัยและสิทธิที่จะได้รับการคุ้มครองจากการหาประโยชน์โดยมิชอบ

ต่อมาสมัชชาใหญ่แห่งสหประชาชาติได้ออกปฏิญญาสากลว่าด้วยสิทธิเด็กขององค์การสหประชาชาติในปี ค.ศ. 1959 ภายหลังจากมีการกำหนดปฏิญญาสากลว่าด้วยสิทธิมนุษยชนโดยวางหลักการ 10 ประการเพื่อคุ้มครองสิทธิของเด็ก ซึ่งรวมทั้งสิทธิที่มีลักษณะเหมือนบุคคลทั่วไป สิทธิที่จะได้รับความคุ้มครองพิเศษและสิทธิที่จะได้รับความคุ้มครองจากการแบ่งแยกกลุ่มเชื้อชาติและในวันที่ 20 พฤศจิกายน ค.ศ. 1989 ซึ่งเป็นวันที่ปฏิญญาสากลว่าด้วยสิทธิเด็กขององค์การสหประชาชาติใช้บังคับครบ 30 ปี สหประชาชาติได้ประกาศใช้อนุสัญญาว่าด้วยสิทธิเด็กและเปิดให้ภาคีสมาชิกลงนาม

พื้นฐานแห่งสิทธิของเด็กภายใต้กฎหมายระหว่างประเทศในเรื่องสิทธิมนุษยชนนั้นประกอบด้วยสิทธิ 2 ประเภท สิทธิประเภทแรกเป็นสิทธิมนุษยชนที่มีอยู่ในฐานะบุคคลคนหนึ่งของสังคมเช่นเดียวกับผู้ใหญ่ แต่ก็อาจมีสิทธิบางอย่างถูกจำกัดอยู่จนกว่าจะอายุถึงเกณฑ์ที่กำหนด เช่นสิทธิในการสมรส สิทธิประเภทที่สองคือสิทธิที่จะได้รับความคุ้มครองบางอย่างในฐานะที่เป็นเด็กหรือเยาวชน ทั้งนี้เด็กย่อมมีสิทธิในความเป็นส่วนตัวด้วย ซึ่งมาตรา 16 ของอนุสัญญาดังกล่าวก็ให้การรับรองไว้และสิทธิในความเป็นส่วนตัวนี้ย่อมต้องนำมาปรับใช้กับการให้ความคุ้มครองข้อมูลส่วนบุคคลของเด็กด้วยและรัฐภาคีถือว่ามีพันธกรณีที่จะต้องสร้างหลักประกันในส่วนนี้ให้แก่เด็ก

2.4 วิวัฒนาการของการคุ้มครองข้อมูลส่วนบุคคลของเด็กในประเทศไทย

สำหรับประเทศไทยนั้นอาจกล่าวได้ว่า วิวัฒนาการของกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของเด็กถูกแยกออกได้เป็น 2 ส่วน คือ วิวัฒนาการของการคุ้มครองข้อมูลส่วนบุคคลและวิวัฒนาการของการคุ้มครองเด็ก โดยการพัฒนากฎหมายที่เกี่ยวข้องนั้น นับได้ว่ายังขาดการเชื่อมโยงการคุ้มครองทั้ง 2 ส่วนเข้าด้วยกันโดยมีวิวัฒนาการในแต่ละส่วนดังนี้

2.4.1 วิวัฒนาการของการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย

ในส่วนที่เกี่ยวข้องกับการให้ความคุ้มครองข้อมูลส่วนบุคคลนั้น ในอดีตมีการบังคับใช้กฎหมายในเรื่องสิทธิความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลผ่านทางกลไกของกฎหมายแพ่งและพาณิชย์และกฎหมายอาญาเป็นสำคัญ แต่ด้วยลักษณะพิเศษของอินเตอร์เน็ตที่ทำให้สามารถติดต่อกันได้โดยไม่จำเป็นต้องเห็นหน้าหรือพูดคุยกันและไม่จำกัดว่าแต่ละฝ่ายจะอยู่ในประเทศใด ทำให้มีข้อจำกัดและอุปสรรคในการบังคับใช้กฎหมายกับกิจกรรมที่เกิดขึ้นบนเครือข่ายอินเตอร์เน็ต จึงมีความพยายามที่จะพัฒนากฎหมายที่เกี่ยวข้องในส่วนนี้ให้สามารถคุ้มครองผู้บริโภคและอุดช่องว่างของกฎหมายเพื่อให้ปรับใช้กับการทำธุรกรรมต่าง ๆ ผ่านอินเตอร์เน็ตได้อย่างมีประสิทธิภาพ โดยเมื่อวันที่ 28 กุมภาพันธ์ พ.ศ. 2539 คณะรัฐมนตรีได้มีมติเห็นชอบต่อนโยบายเทคโนโลยีสารสนเทศ (IT 2000) ตามที่เสนอโดยกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม เพื่อพัฒนาสังคมและเสริมสร้างความแข็งแกร่งทางธุรกิจ อุตสาหกรรมและการค้าระหว่างประเทศในการก้าวเข้าสู่สังคมสารสนเทศ ซึ่งเป็นยุคเศรษฐกิจใหม่แห่งศตวรรษที่ 21 โดยหนึ่งในมาตรการที่สำคัญคือ การปฏิรูปกฎหมายเทคโนโลยีสารสนเทศ

ต่อมาเมื่อสิ้นสุดระยะเวลาของกรอบนโยบายเทคโนโลยีสารสนเทศฉบับแรกไปแล้ว ก็มีการกำหนดกรอบนโยบายเทคโนโลยีสารสนเทศ พ.ศ. 2544 – 2553 (IT 2010) โดยมีการกำหนดเป้าหมายเกี่ยวกับการพัฒนาพาณิชย์อิเล็กทรอนิกส์ให้เป็นเครื่องมือสำคัญในการประกอบธุรกิจเอาไว้ด้วย ซึ่งจัดเป็นยุทธศาสตร์ในการส่งเสริมให้มีการพัฒนาศักยภาพของผู้ประกอบการในการทำธุรกรรมทางพาณิชย์อิเล็กทรอนิกส์[76] และในการจัดทำกรอบนโยบายเทคโนโลยีสารสนเทศ พ.ศ. 2554 - 2563 (IT 2020) ยังคงมีการนำแนวคิดของกรอบนโยบายฉบับเดิมกับสถานภาพการพัฒนาเทคโนโลยีสารสนเทศในขณะนั้นมาเป็นส่วนประกอบสำคัญในการจัดทำกรอบนโยบายฉบับใหม่[77] มีการขยายพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารรวมทั้งอินเตอร์เน็ตความเร็วสูงให้กระจายไปถึงประชาชนทั่วประเทศ รวมทั้งการปรับปรุงกฎหมายให้เหมาะสมทันต่อการเปลี่ยนแปลง[78]

การพัฒนากฎหมายเทคโนโลยีสารสนเทศถือว่าเป็นปัจจัยสำคัญของการดำรงอยู่ของสังคมในศตวรรษที่ 21 ในปีพ.ศ. 2540 คณะรัฐมนตรีได้เห็นชอบให้มีการพัฒนากฎหมายเทคโนโลยีสารสนเทศขึ้น 6 ฉบับ ได้แก่

---

[76] จาก “ประเด็น ปัญหา และแนวทางในการพัฒนาการคุ้มครองผู้บริโภคในการซื้อสินค้าและบริการออนไลน์” โดย อารยา สิงห์สงบ, 2548 (ตุลาคม), *วารสารกฎหมาย (จุฬาลงกรณ์มหาวิทยาลัย),* 24 (2), น. 163-173.

[77] กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ. 2554 – 2563 ของประเทศไทย (น. 7).

[78] แหล่งเดิม.

(1) กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ เพื่อรองรับผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ วิธีส่งและรับข้อมูลอิเล็กทรอนิกส์ รวมทั้งการรับฟังพยานหลักฐาน และการชั่งน้ำหนักพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ให้เสมอกับหนังสือหรือหลักฐานที่เป็นหนังสือและมีการตั้งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ขึ้นเพื่อดำเนินการต่าง ๆ ตามกฎหมายฉบับนี้ ปัจจุบันมีการตราเป็นกฎหมายแล้วโดยมีผลใช้บังคับเมื่อวันที่ 3 เมษายน พ.ศ. 2545

(2) กฎหมายว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ เพื่อรองรับผลทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์ เพื่อให้การใช้ลายมือชื่ออิเล็กทรอนิกส์เป็นที่น่าเชื่อถือเช่นเดียวกับการลงลายมือชื่อแบบธรรมดา สามารถระบุตัวบุคคลผู้ลงลายมือชื่อ สามารถแสดงได้ว่าบุคคลนั้นเห็นด้วยกับข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่ออิเล็กทรอนิกส์กำกับอยู่ อย่างไรก็ดี กฎหมายฉบับนี้ไม่ได้มีการจัดทำแยกเป็นอีกหนึ่งฉบับ เพราะได้มีการรวมหลักการไว้กับกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(3) กฎหมายว่าด้วยการโอนเงินทางอิเล็กทรอนิกส์ การโอนเงินทางอิเล็กทรอนิกส์มีขึ้นในประเทศไทยมาเป็นเวลานานแล้ว ตั้งแต่มีการนำเทคโนโลยีทางด้านคอมพิวเตอร์มาใช้ในระบบธนาคาร เช่น บริการออนไลน์ ระบบเงินฝาก เป็นต้น ซึ่งสามารถรับฝาก ถอน หรือโอนต่างสาขาธนาคารได้ แต่เนื่องจากยังไม่มีกฎหมายที่เกี่ยวข้องกับการโอนเงินอิเล็กทรอนิกส์บัญญัติไว้โดยเฉพาะ มีแต่เพียงระเบียบธนาคารแห่งประเทศไทยและประกาศของธนาคารแห่งประเทศไทยที่เกี่ยวกับการโอนเงินเท่านั้น กฎหมายเกี่ยวกับการโอนเงินอิเล็กทรอนิกส์จึงมีขึ้นเพื่อวางกฎเกณฑ์ให้การทำธุรกรรมทางการเงินสามารถทำได้สะดวกปลอดภัย อันจะส่งผลให้ผู้บริโภคได้รับความคุ้มครองมากขึ้น อย่างไรก็ดีกฎหมายนี้มิได้ถูกพัฒนาเป็นกฎหมายระดับพระราชบัญญัติ เพราะหลังจากที่มีการดำเนินงานของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์แล้ว คณะกรรมการฯ ได้จัดทำเป็นกฎหมายลำดับรองภายใต้มาตรา 32 ของกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์แทน ปัจจุบันมีการตราเป็นพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551

(4) กฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ อาชญากรรมทางคอมพิวเตอร์บางประเภทอาจส่งผลต่อความมั่นคงของประเทศได้ ดังนั้นจึงมีการตรากฎหมายขึ้นมาเพื่อปกป้องสังคมต่อการกระทำของอาชญากร โดยกำหนดฐานความผิดและบทลงโทษอาชญากรที่กระทำผิดกฎหมายเกี่ยวกับคอมพิวเตอร์และกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ที่เกี่ยวข้อง ปัจจุบันมีการตราเป็นพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยมีผลใช้บังคับเมื่อวันที่ 18 กรกฎาคม พ.ศ. 2550

(5) กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ได้จัดทำขึ้นเพื่อคุ้มครองสิทธิขั้นพื้นฐานในความเป็นส่วนตัว โดยมุ่งคุ้มครองข้อมูลส่วนบุคคลที่อาจมีการละเมิดและสามารถนำไปใช้ในทางมิชอบได้โดยง่าย

(6) กฎหมายว่าด้วยการพัฒนาโครงสร้างพื้นฐานสารสนเทศ ได้จัดทำขึ้นเพื่อพัฒนาโครงสร้างพื้นฐานสารสนเทศ และให้ประชาชนเข้าถึงสารสนเทศได้อย่างทั่วถึงและเท่าเทียมกัน อันจะช่วยลดความเหลื่อมล้ำของสังคมตามเจตนารมณ์ในมาตรา 78 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 แต่หลังจากคณะกรรมการกฤษฎีกาพิจารณาแล้วเสร็จได้มีการส่งมอบเรื่องให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารดำเนินการต่อไป อย่างไรก็ดี ภายหลังการปรับปรุงระบบราชการและไม่ได้มีการยืนยันร่างกฎหมายเมื่อมีการเปลี่ยนแปลงรัฐบาล ร่างกฎหมายฉบับนี้จึงตกไป

ในส่วนที่เกี่ยวข้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลนั้นถูกใช้เป็นมาตรการในการคุ้มครองหรือปกป้องสังคมจากการใช้เทคโนโลยีสารสนเทศและการสื่อสารในทางเสียหายหรือละเมิดต่อสิทธิขั้นพื้นฐานของผู้เป็นเจ้าของข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิที่ได้รับการรับรองไว้ในรัฐธรรมนูญ[79] ที่ผ่านมาได้มีการร่างกฎหมายฉบับนี้และผ่านการพิจารณาของคณะกรรมการกฤษฎีกาแล้วตั้งแต่ปี พ.ศ. 2552 แต่เมื่อมีการนำเข้าสู่การพิจารณาของคณะรัฐมนตรีและผ่านเข้าสู่การพิจารณาของรัฐสภาแล้ว กลับมีการยุบสภาเสียก่อนถึง 2 คราว กฎหมายฉบับนี้จึงมีสถานะเป็นเพียงร่างกฎหมายจนถึงปัจจุบัน โดยร่างกฎหมายดังกล่าวกำหนดหลักเกณฑ์กระบวนการและการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลในลักษณะที่เป็นการทั่วไป อย่างไรก็ดี กฎหมายไม่ได้กล่าวถึงข้อมูลส่วนบุคคลของเด็กไว้เป็นพิเศษแต่อย่างใด จึงต้องยึดถือตามเงื่อนไขที่ปรับใช้กับบุคคลทั่วไปด้วย

นอกเหนือจากร่างกฎหมายทั่วไปดังกล่าวแล้ว ที่ผ่านมาประเทศไทยมีกฎหมายในระดับพระราชบัญญัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลอื่นอีก ได้แก่ พระราชบัญญัติข้อมูล

---

[79] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 มาตรา 35

สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง

การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ.

ข่าวสารของราชการ พ.ศ. 2540 และพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 ซึ่งถือว่าเป็นกฎหมายที่มีกลไกการคุ้มครองข้อมูลเฉพาะเรื่อง

2.4.2 วิวัฒนาการของการคุ้มครองเด็กในประเทศไทย

ในอดีตเคยมีการตราพระราชบัญญัติควบคุมเด็กและนักเรียน พ.ศ. 2481 ซึ่งต่อมาถูกยกเลิกไปโดยประกาศคณะปฏิวัติฉบับที่ 132 โดยมีวัตถุประสงค์เพื่อส่งเสริมและคุ้มครองความประพฤติ การแต่งกาย และจรรยามารยาทของเด็กและนักเรียนให้รัดกุมยิ่งขึ้น จึงมีลักษณะเหมือนการควบคุมเด็กและนักเรียนให้อยู่ในกฎระเบียบวินัยมากกว่าที่จะมุ่งคุ้มครองสิทธิของเด็ก ต่อมาในเดือนพฤศจิกายน พ.ศ. 2515 มีการตราประกาศคณะปฏิวัติฉบับที่ 294 โดยมีวัตถุประสงค์สำคัญเพื่อกำหนดวิธีการให้การสงเคราะห์และการคุ้มครองเด็กที่เหมาะสมแก่เด็กและแก่สภาพของสังคม ซึ่งถือว่าเป็นกฎหมายที่มุ่งคุ้มครองเด็กเป็นสำคัญ

หลังจากนั้นในวันที่ 27 มีนาคม พ.ศ. 2535 ประเทศไทยได้ให้สัตยาบันต่ออนุสัญญาว่าด้วยสิทธิเด็ก[80] ซึ่งในข้อ 2 ของอนุสัญญาได้กำหนดให้รัฐภาคีจะต้องเคารพและประกันสิทธิตามที่กำหนดไว้ในอนุสัญญาดังกล่าวแก่เด็กแต่ละคนที่อยู่ในเขตอำนาจของตน โดยปราศจากการเลือกปฏิบัติและจะดำเนินมาตรการที่เหมาะสมทั้งปวง เพื่อที่จะประกันว่าเด็กได้รับการคุ้มครองจากการเลือกปฏิบัติหรือการลงโทษในทุกรูปแบบ บนพื้นฐานของสถานภาพ กิจกรรมความคิดเห็นที่แสดงออกหรือความเชื่อของบิดา มารดา ผู้ปกครองตามกฎหมาย หรือสมาชิกในครอบครัวของเด็ก

มาตรการสำคัญประการหนึ่งที่จะให้หลักประกันการเคารพต่อสิทธิเด็กคือมาตรการทางกฎหมายในช่วงปลายปี พ.ศ. 2545 จึงมีการเสนอร่างกฎหมายเพื่อการคุ้มครองสวัสดิภาพของเด็กเข้าสู่การพิจารณาของรัฐสภาและนำไปสู่การตราพระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546

พระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 กำหนดเงื่อนไขสำคัญในมาตรา 27 เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของเด็กไว้เป็นการเฉพาะว่าห้ามมิให้ผู้ใดโฆษณาหรือเผยแพร่ทางสื่อมวลชนหรือสื่อสารสนเทศประเภทใด ซึ่งข้อมูลเกี่ยวกับตัวเด็กหรือผู้ปกครอง โดยเจตนาที่จะทำให้เกิดความเสียหายแก่จิตใจ ชื่อเสียง เกียรติคุณหรือสิทธิประโยชน์อื่นใดของเด็กหรือเพื่อแสวงหาประโยชน์สำหรับตนเองหรือผู้อื่นโดยมิชอบ และได้วางโทษทางอาญาไว้ในมาตรา 29 หากมีการฝ่าฝืนเงื่อนไขดังกล่าว

กฎหมายฉบับนี้ได้ให้คำจำกัดความว่า “เด็ก” หมายถึงบุคคลที่มีอายุต่ำกว่า 18 ปีบริบูรณ์ แต่เนื่องจากพระราชบัญญัติคุ้มครองเด็กนั้นขาดความชัดเจนในการปฏิบัติประกอบกับ

---

[80] *United Nations Treaty Collection Database, Convention on the Rights of the Child.* Retrieved January 25, 2015, from https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11&chapter=4&lang=en

การเข้าถึงสื่อเทคโนโลยีสารสนเทศได้อย่างง่ายดายมากขึ้น ในการประชุมคณะกรรมการคุ้มครองเด็กแห่งชาติครั้งที่ 5/2550 จึงมีการแต่งตั้งคณะอนุกรรมการคุ้มครองข้อมูลส่วนตัวของเด็กบนระบบเทคโนโลยีสารสนเทศ โดยจะทำหน้าที่ในการออกมาตรการคุ้มครองเด็กเพื่อไม่ให้ผู้ให้บริการเว็บไซต์และอินเตอร์เน็ตละเมิดสิทธิเด็กโดยการเปิดเผยข้อมูลส่วนตัวของเด็กที่มีอายุต่ำกว่า 18 ปี ภายหลังการแต่งตั้งแล้ว คณะอนุกรรมการส่งหนังสือขอความร่วมมือเกี่ยวกับการป้องกันข้อมูลส่วนตัวของเด็กส่งถึงผู้ประกอบการเว็บไซต์หลายราย[81] เป็นประกาศคณะกรรมการคุ้มครองเด็กแห่งชาติ เรื่องการคุ้มครองข้อมูลส่วนตัวของเด็กที่ใช้บริการอินเทอร์เน็ต[82] อย่างไรก็ดีในทางปฏิบัติไม่พบกลไกการบังคับให้ปฏิบัติตามประกาศฉบับดังกล่าวอย่างจริงจังแต่อย่างใดซึ่งจะได้กล่าวถึงในรายละเอียดและสภาพปัญหาของประกาศฉบับนี้ในบทต่อไป

---

[81] มูลนิธิเด็ก. (ม.ป.ป.). *ข้อมูลเด็กบนโลกอินเตอร์เน็ต ความลับที่ห้ามเปิดเผย.* สืบค้น 7 สิงหาคม 2557, จาก http://www.ffc.or.th/ffc_scoop/2551/scoop_2551_02_04.php

[82] สมาคมผู้ดูแลเว็บไทย. สืบค้น 25 มกราคม 2558, จาก http://www.webmaster.or.th/news/protect-privacy-for-child-on-internet