

จริยธรรมและกฎหมายดิจิทัล

ภาชญา เชี่ยวชาญ

จริยธรรมดิจิทัลได้กลายเป็นประเด็นสำคัญในยุคดิจิทัล ที่เกี่ยวข้องกับมิติทางจริยธรรมของความสัมพันธ์ระหว่างสิทธิมนุษยชน เทคโนโลยีดิจิทัล และสังคม ด้วยความเป็นส่วนตัวและการปกป้องข้อมูลในสภาพแวดล้อมดิจิทัล ผู้คนส่วนใหญ่จะไม่สนใจที่จะตระหนักถึงพฤติกรรมของพวกเขาในโลกออนไลน์ จึงทำให้เกิดปัญหาต่างๆ ตามมา เช่น ความเป็นส่วนตัวของข้อมูล การเข้าถึงข้อมูลที่ไม่สามารถเข้าถึงได้ การลอกเลียนแบบ และเนื้อหาปลอม ซึ่งล้วนแล้วแต่เป็นการเพิ่มอาชญากรรมไซเบอร์ กลุ่มเด็กและเยาวชนที่มีการใช้งานออนไลน์มากที่สุด จึงอาจเป็นกลุ่มที่มีความเสี่ยงต่อการมีพฤติกรรมที่ผิดหลักจริยธรรม และอาจตกเป็นเหยื่อหรือถูกภัยคุกคามบนโลกออนไลน์ได้มากที่สุดจากการที่ไม่รู้เท่าทันบุคคลหรือพฤติกรรมของบุคคลบนโลกออนไลน์ ประเด็นด้านจริยธรรมดิจิทัลเป็นเรื่องที่ทั่วโลกให้ความสนใจที่จะแก้ไขปัญหาที่เกิดขึ้น และหาแนวทางป้องกันปัญหา รวมถึงการให้ความรู้ ส่งเสริมให้บุคคลในกลุ่มต่างๆ มีพฤติกรรมสารสนเทศและจริยธรรมดิจิทัลที่ดี นำไปสู่การเป็นพลเมืองดิจิทัลที่ดีต่อไป ในประเทศไทยได้ให้ความสำคัญถึงการกำหนดนโยบายและแผนพัฒนาคนในประเทศให้ตระหนักถึงจริยธรรมดิจิทัลในการดำเนินชีวิต การทำงาน และการอยู่ร่วมกันของคนในสังคมในยุคดิจิทัล ที่จะทำให้ประชาชนในประเทศมีความรู้และฝึกฝนพฤติกรรมจริยธรรมด้านดิจิทัลที่ดี ซึ่งหมายถึงการใช้สื่ออย่างเหมาะสมและเคารพความเป็นส่วนตัวและทรัพย์สินของตนเองและผู้อื่น ดังนั้นสิ่งเหล่านี้เป็นความท้าทายที่ประเทศต่างๆ จำเป็นต้องแก้ไขปัญหา และเป็นการเตรียมความพร้อมของคนในการเปลี่ยนผ่านสู่ยุคดิจิทัล

ในบทนี้จะมีเนื้อหาที่ทำให้เกิดความรู้ความเข้าใจหลักการของจริยธรรมดิจิทัล ประเด็นการพิจารณาจริยธรรมดิจิทัลตามที่ปรากฏอยู่ในชีวิตประจำวัน ตระหนักถึงการกระทำผิดหรือละเมิดและแนวทางป้องกันจริยธรรมดิจิทัล มีความเข้าใจและเล็งเห็นถึงความสำคัญของกฎหมายลิขสิทธิ์และกฎหมายที่เกี่ยวข้อง สามารถวิเคราะห์และวินิจฉัยเกี่ยวกับปัญหาและภัยคุกคามในการใช้เทคโนโลยีดิจิทัลได้ รวมถึงรู้วิธีและแนวทางในการรักษาความปลอดภัยในการใช้เทคโนโลยีดิจิทัล

5.1 จริยธรรมดิจิทัล

5.1.1 ความหมายและความสำคัญของจริยธรรมดิจิทัล

จริยธรรม หมายถึง แนวทางประพฤติปฏิบัติตนเพื่อการบรรลุถึงสภาพชีวิตอันทรงคุณค่าพึงประสงค์ (สำนักงานคณะกรรมการศึกษาแห่งชาติ, 2522) และข้อประพฤติปฏิบัติศีลธรรม กฎศีลธรรม (พจนานุกรมไทยฉบับราชบัณฑิตยสถาน, 2546) ซึ่งความสัมพันธ์ของหลักทางศีลธรรม ได้แก่ ความดี ความชั่ว หรือหน้าที่กฎเกณฑ์ทางศีลธรรม (Robert N. Barger, 2008) เป็นกฎเกณฑ์และมาตรฐานของการประพฤติปฏิบัติในสังคมซึ่งบุคคลพัฒนาขึ้นจนกระทั่งมีพฤติกรรมเป็นของตนเอง โดยเกิดขึ้นจากกระบวนการทางความคิดอย่างมีเหตุผลและต้องอาศัยวุฒิภาวะทางปัญญา โดยสังคมจะเป็นตัวตัดสินผลของการกระทำนั้นว่าเป็นการกระทำที่ถูกต้องหรือผิด บุคคลช่วงวัยรุ่นจะมีพฤติกรรมเพื่อทำตามหน้าที่ของสังคม โดยรู้ถึงบทบาทและหน้าที่ในฐานะเป็นหน่วยหนึ่งของสังคมนั้น จึงมีหน้าที่ทำตามกฎเกณฑ์ต่างๆ ที่สังคมกำหนดให้หรือคาดหวังไว้และพยายามที่จะตีความหมายของหลักการและมาตรฐานทางจริยธรรมด้วยวิจารณญาณ (Kohlberg อ้างถึงใน สุรางค์ โค้วตระกูล, 2556) ซึ่งกล่าวได้ว่าเป็นศาสตร์เกี่ยวกับอุดมคติของมนุษย์หรือศาสตร์ของหน้าที่ทางศีลธรรม (Kidder, Rush Worth, 2003) โดยจะกำหนดว่าอะไรเป็นพฤติกรรมที่ดีหรือเป็นอันตรายต่อบุคคล (Paul, Richard; Elder, Linda, 2006) จึงสรุปได้ว่าจริยธรรม หมายถึงธรรมที่เป็นข้อประพฤติ ศีลธรรมอันดี เป็นแนวทางกฎเกณฑ์ในการประพฤติปฏิบัติในสิ่งที่ถูกต้องเหมาะสม บุคคลที่มีจริยธรรมจะทำให้เป็นคนที่มีคุณภาพและเป็นที่ยอมรับของสังคมส่วนรวม จริยธรรมขึ้นอยู่กับมาตรฐานที่ดีของความถูกต้องและผิดที่กำหนดสิ่งที่มนุษย์ควรจะทำมักจะอยู่ในแง่ของสิทธิหน้าที่ผลประโยชน์ต่อสังคมความเป็นธรรมหรือคุณธรรมที่เฉพาะเจาะจง

เมื่อเกิดการเปลี่ยนผ่านยุคของการปฏิสัมพันธ์และการสื่อสารของมนุษย์ โดยมีข้อมูลข่าวสาร และสารสนเทศในรูปแบบต่างๆ มากขึ้น และเริ่มมีการนำเทคโนโลยีคอมพิวเตอร์มาใช้กันอย่างแพร่หลาย จึงเป็นจุดเริ่มต้นของจริยธรรมด้านคอมพิวเตอร์ (Computer Ethics) โดยที่แนวคิดเรื่องจริยธรรมคอมพิวเตอร์เกิดขึ้นในทศวรรษที่ 1940 โดย Norbert Wiener อาจารย์จากสถาบันเทคโนโลยีแมสซาชูเซตส์ (MIT) และได้มีการกล่าวถึงจริยธรรมคอมพิวเตอร์มาอย่างต่อเนื่อง จนถึงในปี ค.ศ. 1995 จริยธรรมทางคอมพิวเตอร์ในที่สุดจะกลายเป็นระบบจริยธรรมระดับโลกและหลังจากนั้นจริยธรรมทางคอมพิวเตอร์จึงกลายเป็นมาตรฐานจริยธรรมของยุคข้อมูลข่าวสาร (Bynum, Terrell, 2014) ไปพร้อมกับจริยธรรมสารสนเทศ (Information Ethics) ขึ้นมา ซึ่งถูกกำหนดให้เป็นสาขาของจริยธรรมที่มุ่งเน้นไปที่ความสัมพันธ์ระหว่างการสร้างองค์การเผยแพร่ การใช้ข้อมูล จรรยาบรรณและจรรยาบรรณที่ควบคุมพฤติกรรมของมนุษย์ในสังคม (Joan, Reitz M., 2010) จริยธรรมสารสนเทศได้พัฒนาขึ้นเพื่อให้สัมพันธ์กับสาขาต่างๆ เช่น จริยธรรมด้านคอมพิวเตอร์ (Floridi, Luciano, 1999) จรรยาบรรณทางการแพทย์วารสารศาสตร์ (Floridi, Luciano, 2005) และปรัชญาทางสารสนเทศ การถ่ายทอดข้อมูล

และการรู้สารสนเทศ เป็นเรื่องสำคัญในการสร้างรากฐานทางจริยธรรมที่ส่งเสริมการปฏิบัติอย่างเป็นธรรม จริยธรรมสารสนเทศจะตรวจสอบประเด็นที่เกี่ยวข้องกับการเป็นเจ้าของ การเข้าถึง ความเป็นส่วนตัว ความปลอดภัยและชุมชน (Moran, Barbara A., et al., 2013)

เมื่ออินเทอร์เน็ตเข้ามามีบทบาทต่อการจัดการสารสนเทศ การสื่อสาร จริยธรรมทางอินเทอร์เน็ต (Internet Ethics) จึงมีความสำคัญตามมาในการที่จะใช้งานอินเทอร์เน็ตได้เกิดประโยชน์และเหมาะสมกับทุกคนนั้น จึงต้องการพฤติกรรมทางจริยธรรมในส่วนของผู้ใช้และผู้ให้บริการ ที่จะต้องมีพฤติกรรมออนไลน์ที่เหมาะสม (Marion G. Ben-Jacob, 2017) ทั้งด้านการสร้างและการใช้งานเนื้อหาสารสนเทศ และสื่อดิจิทัล นอกจากนี้ยังเกี่ยวข้องกับการมารยาทเน็ต (Netiquette) มารยาทและจริยธรรมตามนิยามมีความสัมพันธ์ใกล้เคียงกัน มารยาทที่ถูกกำหนดให้เป็นกฎทั่วไปของพฤติกรรมส่วนบุคคลในสังคมสุภาพและจริยธรรมมีความเกี่ยวข้องกับศีลธรรมการปฏิบัติต่อคำถามเชิงจริยธรรมถูกต้องตามหลักศีลธรรมและเกียรติ (Larry Scheuermann, Gary Taylor, 1997) ซึ่งจะแสดงรายละเอียดในบทต่อไป และการเปลี่ยนผ่านสู่ยุคสังคมดิจิทัลในศตวรรษที่ 21 ที่การพัฒนาการของเทคโนโลยีสู่ความเป็นดิจิทัลและนำไปใช้อย่างแพร่หลายในการพัฒนาด้านต่างๆ ของบุคคล กลุ่มบุคคล องค์กร และสังคม ซึ่งจะต้องคำนึงถึงบังคับ กฎเกณฑ์และกฎหมายที่เกี่ยวข้องด้วย โดยเฉพาะอย่างยิ่งในเรื่องของค่านิยมทางจริยธรรมและข้อจำกัด จึงนำมาซึ่งการกำหนดความหมายและขอบเขตของจริยธรรมดิจิทัล

จริยธรรมดิจิทัล (Digital Ethics) หมายถึงการประพฤติปฏิบัติและหลักการทางจริยธรรมเชิงปฏิสัมพันธ์แบบดิจิทัลระหว่างคน ธุรกิจ สังคม และสิ่งต่างๆ (Gartner, 2015) โดยจะต้องคำนึงถึงความเป็นส่วนตัว ความถูกต้อง ความเป็นเจ้าของ และการเข้าถึงเทคโนโลยีดิจิทัล ซึ่งเกี่ยวข้องกับวิธีการดำเนินชีวิตในการเข้าถึงและการใช้อินเทอร์เน็ต เทคโนโลยีและสื่อดิจิทัลเป็นสิทธิขั้นพื้นฐานของมนุษย์ในสังคมข้อมูลทั่วโลก ที่เป็นไปตามหลักคุณธรรม จริยธรรม และจรรยาบรรณวิชาชีพที่มีเป้าหมายในการกำหนดความรับผิดชอบต่อสังคม (Matthew N. O. Sadiku, et al., 2017) และเป็นสิ่งที่ถูกต้องตามกฎหมายสิ่งที่สามารถทำได้โดยเทคโนโลยีดิจิทัลและสิ่งที่เป็นที่ต้องการทางจริยธรรมซึ่งหลักการและพฤติกรรมทางจริยธรรมที่แข็งแกร่งจึงมีความสำคัญมากขึ้นในยุคสังคมดิจิทัลที่กำลังพัฒนาและเป็นปัจจัยสำคัญในการสร้างความไว้วางใจ (the Association of Chartered Certified Accountants: ACCA, 2017) เมื่อการเชื่อมต่อและสื่อสารกันด้วยเทคโนโลยีดิจิทัลก่อให้เกิดความท้าทายใหม่ๆ จริยธรรมดิจิทัลเกิดขึ้นจากการเปลี่ยนแปลงของยุคสมัย จากความสำคัญของจริยธรรมต่อการดำเนินชีวิตของคนในสังคม ช่วยควบคุมความเจริญทางด้านวัตถุและจิตใจของคนให้เติบโตไปพร้อมกัน หากนำความเจริญก้าวหน้าทางเทคโนโลยีมาพัฒนาในด้านที่ผิดจะทำให้ความเดือดร้อนแก่คนทั่วไป

เมื่อสังคมเปลี่ยนแปลงมาสู่ยุคที่สังคมถูกขับเคลื่อนด้วยเทคโนโลยีนั้น คนในสังคมจึงต้องมีทักษะของการใช้เทคโนโลยีสารสนเทศและเทคโนโลยีดิจิทัลในการเข้าถึงข้อมูลสารสนเทศและการประเมินสารสนเทศก่อนที่นำไปใช้ตามความต้องการ ซึ่งการดำเนินการดังกล่าวนอกจากจะต้องอาศัยทักษะการรู้ดิจิทัลที่ดีแล้วจำเป็นจะต้องมีจริยธรรมที่เหมาะสมด้วย เพื่อให้คนในสังคมดิจิทัลตระหนักถึงความเป็นส่วนตัว (Privacy) ความถูกต้อง (Accuracy) ความเป็นเจ้าของ (Property) การเข้าถึงข้อมูล (Accessibility) ของตนเองและผู้อื่น (Valacich & Schneider, 2012) และจริยธรรมดิจิทัลนั้น มีความหมายที่แตกต่างกัน แต่มีความเชื่อมโยงกับจริยธรรมด้านเทคโนโลยีต่างๆ ขึ้นอยู่กับยุคสมัยของเทคโนโลยีและการให้ความสำคัญของบุคคล กลุ่มบุคคล หน่วยงาน องค์กร และวิชาชีพที่แตกต่างกันไป

ประเด็นหลักของจริยธรรมดิจิทัลนั้นเกี่ยวกับความเป็นส่วนตัว ทรัพย์สินทางปัญญา ความเป็นธรรมทางอิเล็กทรอนิกส์ และความไม่จำกัดเฉพาะกลุ่ม (Patrignani, 2009) รวมถึงเน้นในเรื่องสำคัญอื่นๆ ของจริยธรรมดิจิทัล เช่น การกำกับดูแลระบบอินเทอร์เน็ต ความขัดแย้งทางไซเบอร์ และการก่ออาชญากรรมทางดิจิทัล รวมถึงจริยธรรมดิจิทัลมีความสำคัญในการใช้เทคโนโลยีในปัจจุบันซึ่งมีการใช้อินเทอร์เน็ตและสื่อสังคมออนไลน์เป็นอย่างมากในยุคดิจิทัล โดยเฉพาะกลุ่มเยาวชน (Rafael Capurro, 2016) ในการศึกษาและทำวิจัยด้านนี้ จำเป็นจะต้องศึกษาด้านการสื่อสาร กฎหมาย สารสนเทศศึกษา ปรัชญา ศาสตร์ทางการเมือง วิทยาการคอมพิวเตอร์ และด้านธุรกิจในหัวข้อต่างๆ ที่มีตั้งแต่การแอบอ้างไปจนถึงการละเมิดลิขสิทธิ์ (Don Heider, 2017) จะเห็นได้ว่าจริยธรรมดิจิทัลนั้นเกี่ยวข้องกับผลกระทบของเทคโนโลยีสารสนเทศและการสื่อสารดิจิทัลในสังคมและสิ่งแวดล้อมโดยรวม จึงควรนำหลักจริยธรรมมาเป็นส่วนหนึ่งในการแก้ไขปัญหาและหาแนวทางที่ยั่งยืนต่อความท้าทายของเทคโนโลยีในยุคดิจิทัลได้ ซึ่งบริบทของจริยธรรมดิจิทัลเป็นส่วนหนึ่งของการพัฒนาทักษะของบุคคลสู่ความเป็นพลเมืองดิจิทัลที่ดี

5.1.2 ประเด็นการพิจารณาจริยธรรมดิจิทัล

จริยธรรมในการจัดการสารสนเทศและดิจิทัลประกอบไปด้วยประเด็นหลัก 4 ประเด็น ได้แก่ (Mason, Mason & Culnan, 1995, Valacich & Schneider, 2012)

1. ความเป็นส่วนตัว (Privacy)

ข้อมูลส่วนบุคคล การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้น เช่น รูปถ่าย ภาพถ่ายบุคคล สถานที่ของบุคคล เป็นต้น ความเป็นส่วนตัวของข้อมูลและสารสนเทศ เป็นสิทธิ์ที่เจ้าของสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น การละเมิดความเป็นส่วนตัว เช่น การถูกรวบรวมข้อมูลส่วนบุคคลสร้างเป็นฐานข้อมูลแล้วเอาไปขาย หรือทำธุรกิจผ่าน

เว็บไซต์เพื่อรวบรวมข้อมูลไปขาย การใช้โปรแกรมเพื่อดักจับและวิเคราะห์การใช้อินเทอร์เน็ต การส่งสแปมเมล (Spam Mail)

2. ความถูกต้อง (Accuracy)

สภาพที่สารสนเทศนั้น ปราศจากความผิดพลาด มีความสมบูรณ์ สอดคล้องกับความเป็นจริง และมีความเป็นปัจจุบัน สารสนเทศที่ผิดพลาดส่งผลกระทบต่อชีวิตของบุคคล โดยเฉพาะอย่างยิ่งหากสารสนเทศนั้น ก่อให้เกิดการได้เปรียบเสียเปรียบในกิจกรรมสำคัญ การให้และรับสารสนเทศที่ถูกต้องแม่นยำจะช่วยให้ผู้รับหลีกเลี่ยงอคติในแหล่งสารต่างๆ ที่อาจมีอยู่ได้ หากการสืบค้นสารสนเทศที่ไม่ใช่สารสนเทศที่เป็นทางการหรือเอกสารวิชาการ อาจเป็นไปได้ที่สารสนเทศเหล่านั้น ไม่ได้รับการตรวจสอบหรือตรวจทานจากนักวิชาการหรือผู้เชี่ยวชาญในด้านนั้นๆ ผู้เสนอสารสนเทศนั้นอาจอ้างว่าตนเองเป็นใครก็ได้ ดังนั้นเพื่อความมั่นใจว่าได้สารสนเทศที่ถูกต้อง เมื่อรับสารอาจต้องตีความและประเมินสารสนเทศนั้นก่อน เช่น ผู้เขียนกล่าวถึงหรือต้องการจะสื่อถึงอะไร มีหลักฐานเชิงประจักษ์ใดมาสนับสนุน ที่ซึ่งหาได้จากที่ใดบ้าง และข้อมูลจากที่อื่นซึ่งปฏิเสธหรือตรงข้ามกับสิ่งที่ผู้เสนอนำมาเสนอหรือไม่ หากข้อมูลนั้นผิดมีใครเป็นผู้รับผิดชอบและหากเชื่อในสารที่ผิดจะก่อความเสียหายให้กับเรามากแค่ไหน เพื่อการให้และรับสารที่ถูกต้องแม่นยำ ความถูกต้องของข้อมูลที่เกิดจากการใช้คอมพิวเตอร์เพื่อการรวบรวม จัดเก็บ และเรียกใช้ข้อมูลนั้น โดยความถูกต้องของข้อมูลจะส่งผลถึงความน่าเชื่อถือได้ของข้อมูล ทั้งนี้ข้อมูลจะมีความน่าเชื่อถือมากน้อยเพียงใดย่อมขึ้นอยู่กับความถูกต้องในการ บันทึกข้อมูลด้วย ต้องมีผู้รับผิดชอบในเรื่องความถูกต้อง มีการตรวจสอบความถูกต้องก่อนการบันทึก

3. ความเป็นเจ้าของ (Property)

ลิขสิทธิ์นั้นเป็นสิทธิแต่เพียงผู้เดียวของผู้สร้างสรรค์ที่จะกระทำการใดๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้นตามประเภทลิขสิทธิ์ที่กฎหมายกำหนด เช่น งานวรรณกรรม โปรแกรมคอมพิวเตอร์ นาฏกรรม ศิลปกรรม ดนตรีกรรม โสตทัศนวัสดุ ภาพยนตร์ สิ่งบันทึกเสียง งานแพร่เสียงแพร่ภาพ กฎหมายลิขสิทธิ์ยังให้ความคุ้มครองถึงสิทธิของนักแสดงด้วย เป็นต้น กรรมสิทธิ์ในการถือครองทรัพย์สินซึ่ง อาจเป็นทรัพย์สินทั่วไปที่จับต้องได้เช่น คอมพิวเตอร์ หรืออาจเป็นทรัพย์สินทางปัญญาที่จับต้องไม่ได้ เช่น บทเพลง โปรแกรมคอมพิวเตอร์แต่สามารถถ่ายทอดและบันทึกลงในสื่อต่างๆ ได้เช่น สิ่งพิมพ์เทป ซีดีรอม เป็นต้น

4. การเข้าถึงข้อมูล (Accessibility)

สิทธิในการเข้าใช้งานโปรแกรมหรือระบบคอมพิวเตอร์ ซึ่งมักจะมีกำหนดสิทธิ์ตามระดับของผู้ใช้งาน เพื่อการป้องกันการเข้าดำเนินการต่างๆ กับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้องและเป็นการรักษาความลับของข้อมูล ตัวอย่างสิทธิในการใช้งานระบบ เช่น การบันทึก การแก้ไขหรือปรับปรุง และการลบ เป็นต้น การออกแบบระบบที่มีการรักษาความปลอดภัยในการเข้าถึงข้อมูลของผู้ใช้

5.1.3 การกระทำผิดหลักจริยธรรมดิจิทัล

ในปัจจุบันเทคโนโลยีดิจิทัลมีความสำคัญต่อการเรียนรู้และการดำเนินชีวิต ทำให้การเข้าถึงเทคโนโลยีดิจิทัลมีปริมาณเพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะกลุ่มเด็กและเยาวชนที่เกิดมาพร้อมกับยุคของอินเทอร์เน็ตและสื่อดิจิทัลที่ถือว่าเป็นชาวดิจิทัล (Digital Native) ที่อยู่ในช่วงอายุระหว่าง 15-25 ปี ซึ่งมีความสามารถในการใช้งานอินเทอร์เน็ตสื่อดิจิทัลและเครือข่ายสังคมออนไลน์ มีศักยภาพในการเรียนรู้และใช้งานเทคโนโลยีดิจิทัลสูง แต่เนื่องจากสิ่งที่พวกเขาารู้สึกว่าคุ้นเคยดีอาจถูกมองข้ามการสร้างและรับสารอย่างมีการคิดวิเคราะห์ แยกแยะ และรู้เท่าทันข้อมูลข่าวสาร โดยไม่ไหลไปตามกระแสข้อมูลข่าวสารของโลกเสมือนจริงนี้ ซึ่งข้อมูลสถิติการใช้งานอินเทอร์เน็ตของคนไทยปี 2561 จากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ระบุว่ากลุ่มคนช่วงอายุ 18-37 ปี (Gen Y) เป็นกลุ่มที่ใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์มากที่สุดโดยเฉลี่ย 10 ชั่วโมงต่อวัน รับส่งข่าวสารผ่านสังคมออนไลน์ และเป็นกลุ่มที่มีความเสี่ยงต่อการถูกละเมิดข้อมูลส่วนตัวมากที่สุด

ผลสำรวจการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พบว่าเด็กและเยาวชนอายุระหว่าง 15-24 ปี มีอัตราการเข้าถึงอินเทอร์เน็ตสูงถึง 89.8% และการใช้งานเครือข่ายสังคมออนไลน์ ส่วนใหญ่เป็นกลุ่มนักเรียน นักศึกษา หรือวัยรุ่น โดยกลุ่มดังกล่าวมีการเปิดเผยข้อมูลส่วนตัว และเปิดเผยความเป็นตัวตนชัดเจนขึ้น (สำนักงานสถิติแห่งชาติ, 2560) พฤติกรรมสารสนเทศในการโพสต์ข้อความและรูปภาพ การแสดงความคิดเห็นการทำธุรกรรมออนไลน์ เป็นต้น ทำให้เกิดความเสี่ยงในการถูกล่อลวงทางโลกออนไลน์ ปัญหาการกลั่นแกล้งบนโลกไซเบอร์ (Cyberbullying) มากขึ้นอีกทั้งยังขาดความเข้าใจในสิทธิของการสร้างสรรค์ แก๊ซัดดแปลง การนำไปใช้ และการเผยแพร่สารสนเทศในรูปแบบต่างๆ รวมถึงการใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์ ซึ่งปัญหาการละเมิดทรัพย์สินทางปัญญาบนระบบคอมพิวเตอร์และระบบออนไลน์ยังคงมีอย่างต่อเนื่อง โดยเกิดจากทัศนคติที่ผิดหรือการเจตนาด้วย นอกจากนี้ยังมีปัญหาการติดการพนันออนไลน์ซึ่งเข้าถึงพนันเร็วกว่าวัยอันสมควรจะมีปัญหาต่อพฤติกรรมและพัฒนาการทางอารมณ์ จนกระทั่งมีปัญหาต่อการอยู่ในสังคม ตลอดจนแนวโน้มของการเข้าสู่การพนันของเด็กและเยาวชนในประเทศไทยที่เพิ่มสูงขึ้นอย่างมาก

ตั้งแต่เทคโนโลยีการสื่อสารพัฒนาอย่างก้าวล้ำสู่ยุคการสื่อสารแบบออนไลน์นั้น กลับส่งผลไปในด้านลบต่อชีวิตประจำวันและความสัมพันธ์ของคนในสังคมอย่างชัดเจนยิ่งขึ้น จนกลายเป็นประเด็นทางสังคมที่ทั้งสื่อและกฎหมาย ประชาชนเองจะต้องให้ความสำคัญในการป้องกันและแก้ไขปัญหาเหล่านี้ โดยเฉพาะกับกลุ่มวัยรุ่นที่ใช้เวลาไปกับสื่อออนไลน์วันละหลายชั่วโมง จนอาจนำไปสู่ความขัดแย้ง ทะเลาะวิวาท จนถึงขั้นทำร้ายร่างกายตามมา อีกทั้งยังเกิดปัญหาการที่ไม่มีตัวตนอยู่จริงหรือมีตัวตนซ่อนเร้นในโลกออนไลน์ ทำให้คนมีอิสระในการแสดงความคิดเห็นหรือแสดงอารมณ์แรงออกมาในสังคมมากขึ้น โดยเฉพาะในสังคมวัยรุ่นสมัยนี้ที่มีการสื่อสารที่ทำให้เกิดการวิบัติของภาษา และเกิดความรุนแรงในการพูด ซึ่งจะนำไปสู่การวิวาทได้ง่ายขึ้นในสื่อสังคมออนไลน์ จากความ

รุนแรงทาง ความสัมพันธ์ในการสื่อสารกลายเป็นความรุนแรงทางกายภาพ (ปิยวัฒน์ เกตุวงศา อ่างใน สำนักงานรัฐบาลอิเล็กทรอนิกส์, 2558)

5.1.3.1 ปัญหาการกระทำผิดหลักจริยธรรมดิจิทัลส่วนใหญ่ที่พบ ในทั้ง 4 ด้าน ได้แก่

1) ปัญหาด้านความเป็นส่วนตัว (Privacy)

(1) พฤติกรรมการกลั่นแกล้งบนโลกออนไลน์ (Cyberbullying) โดยกระทำการโพสต์ด้วยถ้อยคำที่ไม่เหมาะสม เช่น ด่าทอ พุดจาส์อเสียด ให้อาย ดูถูก หรือข่มขู่ทำร้าย และกระทำการแอบอ้าง การสวมรอย หรือปลอมแปลงเป็นผู้อื่น รวมถึงการแบ่งปันภาพที่ไม่เหมาะสม

(2) การเปิดเผยข้อมูลส่วนตัวหรือจะเป็นของตนเองหรือผู้อื่นมากเกินไป ก่อให้เกิดการหลอกลวงผ่านสื่อ จากสถานการณ์ดังกล่าว ซึ่งเป็นการละเมิดสิทธิความเป็นส่วนตัวและ ก่อให้เกิดความเสียหายต่อผู้อื่น เช่น การให้วันเดือนปีเกิดที่แท้จริงผ่านสื่อสังคมออนไลน์

(3) การถูกเข้าถึงหรือรบกวนทางระบบสารสนเทศหรืออุปกรณ์ส่วนตัว เช่น การถูกรวบรวมข้อมูลส่วนบุคคลเป็นฐานข้อมูลแล้วนำไปขาย หรือใช้เพื่อการอื่นๆ ที่เป็นผลประโยชน์ การใช้โปรแกรมเพื่อดักจับและวิเคราะห์การใช้อินเทอร์เน็ต การส่งสแปมเมลมารบกวนหรือทำให้เกิด อีเมลขยะ

(4) พฤติกรรมของตนเองที่ก่อให้เกิดความเสี่ยง เช่น การไม่เปลี่ยนแปลงรหัสผ่านหรือใช้รหัสเดียวกับทุกระบบ ใช้งานคอมพิวเตอร์สาธารณะ/อุปกรณ์เคลื่อนที่ของผู้อื่นมักตั้งค่า ให้อุปกรณ์ดังกล่าวจดจำรหัสผ่าน การแชร์ตำแหน่ง (Location) แบบทันที (Real Time) ซึ่งพฤติกรรม เหล่านี้ถือเป็นการสร้างความไม่ปลอดภัยให้กับเจ้าของข้อมูล

(5) ปัญหาการรบกวนความเป็นส่วนตัวจากการส่งข้อความชักชวนให้ เข้าร่วมเครือข่ายธุรกิจขายตรง หรือการโฆษณาขายสินค้าและบริการต่างๆ

2) ความถูกต้อง (Accuracy)

(1) ปัญหาด้านการแสดงหรือยืนยันตัวตนที่แท้จริงเป็นพื้นฐานสำคัญของ ชุมชนของเรา เราเชื่อว่าผู้คนจะมีความรับผิดชอบต่อกำพูดและการกระทำของตนเองมากขึ้น เมื่อใช้ ข้อมูลระบุตัวตนที่แท้จริง จึงเป็นเหตุผลที่เราขอให้ผู้ใช้งานใช้ชื่อที่แท้จริงของตนเองบนโลกออนไลน์ ทำให้สื่อสังคมออนไลน์ต่างๆ ต้องมีนโยบายตัวตนที่แท้จริงของเรามุ่งหวังที่จะสร้างสภาพแวดล้อม ที่ปลอดภัยซึ่งผู้คนสามารถไว้วางใจและเชื่อถือกันได้

(2) ปัญหาการรับรู้สารสนเทศที่ไม่ทันสมัยในเฟซบุ๊กหรือสื่อสังคม ออนไลน์อื่นๆ ซึ่งเกิดจากการแชร์ต่อกันไปเรื่อยๆ หรือการแชร์ซ้ำๆ โดยที่ผู้ที่ทำการแชร์หรือผู้รับ สารสนเทศมีความรู้เท่าไม่ถึงการณ์ หรือไม่ได้ใช้วิจารณญาณในการสังเกตและอ่านสารสนเทศนั้นก่อน ทำการแชร์ รวมถึงการกดไลค์ และการโพสต์ด้วย ซึ่งทำให้ไม่ทราบแน่ชัดว่าสารสนเทศนั้นมี เนื้อหาที่ถูกต้อง มีความทันสมัย ทันทต่อเหตุการณ์ และเป็นปัจจุบันหรือไม่ จึงทำให้เกิดปัญหาการเข้าใจ

ผิดและการรับรู้สารสนเทศที่ไม่ถูกต้องได้ นอกจากนี้ยังอาจเป็นพฤติกรรมที่เป็นการกระทำผิดกฎหมาย ทั้งกฎหมายลิขสิทธิ์ และพระราชบัญญัติ ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ อีกด้วย

3) ปัญหาด้านความเป็นเจ้าของ

(1) การใช้สารสนเทศที่ละเมิดลิขสิทธิ์

เช่น รูปภาพ วิดีโอ สารสนเทศแบบมัลติมีเดียอื่นๆ ฟอนท์ ซึ่งมีการสงวนลิขสิทธิ์หรือมีสัญญาอนุญาต โดยที่ไม่ได้รับอนุญาตหรือไม่มีการอ้างอิงแหล่งที่มาที่ถูกต้อง และอาจละเมิดทรัพย์สินทางปัญญา

(2) ปัญหาด้านการคัดลอกหรือขโมยผลงานผู้อื่น (Plagiarism)

การขโมยความคิดเป็นหนึ่งในรูปแบบการประพฤติผิดทางวิทยาศาสตร์ที่ร้ายแรงที่สุดที่แพร่หลายในปัจจุบัน (Debnatha, 2016) ปัญหาที่เกิดขึ้นเพราะการขาดความรู้ความเข้าใจเรื่องลิขสิทธิ์ และวิธีการอ้างอิงถึงผลงานที่นำมาใช้อย่างถูกต้อง จากการสำรวจของที่ประชุมอธิการบดีแห่งประเทศไทย (ทปอ.) โดยนิด้าโพล พบว่านิสิตนักศึกษา 48% เคยลอกรายงาน ผลงานคนอื่น และ 21% เคยให้คนอื่นทำรายงานให้ ขณะที่นิสิตนักศึกษาที่เคยลอกรายงานคนอื่น มีมากกว่า 60% และคิดว่าการลอกรายงานคนอื่นผิดเล็กน้อย ไม่ร้ายแรง และนิสิตนักศึกษาที่เคยให้คนอื่นทำรายงานให้ มีมากกว่า 60% คิดว่าการให้คนอื่นทำรายงานให้ผิดเล็กน้อย ไม่ร้ายแรง อีกทั้งนิสิตนักศึกษาที่เคยทำสารนิพนธ์ ภาคนิพนธ์ วิทยานิพนธ์ มินิโปรเจค โครงการและปัญหาพิเศษ มีอย่างน้อย 4% ที่เคยคัดลอกงานผู้อื่น โดยไม่มีการอ้างอิง แต่ภาคนิพนธ์มีสัดส่วนของนิสิตนักศึกษาที่เคยคัดลอกงานผู้อื่นโดยไม่มีการอ้างอิงมากกว่าการทำกิจกรรมอื่นๆ และเหตุผลที่นิสิตนักศึกษายกมาอ้างมากที่สุดในการไม่อ้างอิง 5 ประการ ได้แก่ ลืมอ้างอิงหรืออ้างไม่ครบ ใช้เป็นแนวทางในการศึกษา ทำไม่ทัน สะเพร่า ทำให้เพื่อความสะดวกและรวดเร็ว หาแหล่งอ้างอิงไม่ได้หรือแหล่งอ้างอิงไม่ชัดเจน และรู้เท่าไม่ถึงการณ์ ไม่รู้ว่าผิด ไม่ตั้งใจ (เดลินิวส์, 2557)

(3) พฤติกรรมการคัดลอกผลงานทางวิชาการ

เป็นปัญหาที่เกิดจากการขาดจิตสำนึก และการไม่มีคุณธรรมจริยธรรม ขาดจรรยาบรรณทางวิชาการ ซึ่งผู้สร้างสรรค์ผลงานวิชาการ โดยเฉพาะนักศึกษาควรตระหนักในปัญหาเหล่านี้ เพราะนอกจากจะเป็นพฤติกรรมที่ไม่เหมาะสมแล้ว ยังส่งผลให้การสร้างองค์ความรู้ใหม่ๆ จากผลงานวิชาการไม่มีความก้าวหน้า ไม่สามารถพัฒนาได้อย่างต่อเนื่อง ขาดความน่าเชื่อถือ เสื่อมเสียเกียรติและชื่อเสียงทั้งตนเอง และสถาบันที่ศึกษา ดังปรากฏเป็นข่าวใหญ่ และเป็นประเด็นการหารือในเวทีสัมมนาวิชาการในปัจจุบัน (กัญจนา บุญยเกียรติ, 2554 อ้างใน วิศรุจน์ เมืองปลื้ม และวิชุดา กิจธรรม, 2560)

(4) ปัญหาการละเมิดลิขสิทธิ์

ในประเทศไทยนั้นปัญหาการละเมิดลิขสิทธิ์ซอฟต์แวร์มีความรุนแรงเพิ่มมากขึ้น โดยเฉพาะกับกลุ่มที่มีรายได้น้อย และกลุ่มเด็ก เยาวชน นักเรียน นักศึกษา โดยสาเหตุของการละเมิดลิขสิทธิ์ซอฟต์แวร์ในประเทศไทย อาจเป็นไปได้หลายประการ เช่น ตัวซอฟต์แวร์ละเมิดลิขสิทธิ์มีคุณภาพเทียบเท่าของแท้ ซอฟต์แวร์ของแท้มีราคาแพง การละเมิดลิขสิทธิ์ทำได้ง่ายและรวดเร็ว อีกทั้งสามารถจัดหาได้ง่าย และอาจมีเหตุผลทางจิตวิทยา และจริยธรรมเข้ามาเกี่ยวข้อง เช่น เรื่องการเอื้อเฟื้อเผื่อแผ่ ผู้บริโภคอาจมีการแบ่งปันกัน จึงทำให้ผู้ที่ได้ละเมิดลิขสิทธิ์ไม่คิดว่าตนเองได้กระทำความผิด และยังคงเกี่ยวข้องกับความรู้กฎหมาย และกลไกในการบังคับใช้กฎหมายที่ยังไม่มีประสิทธิภาพเท่าที่ควร และการหาตัวผู้กระทำความผิดสามารถทำได้ยาก นอกจากนี้ความไม่ตระหนักว่าการดาวน์โหลดซอฟต์แวร์ละเมิดลิขสิทธิ์อาจทำให้เสี่ยงต่อการถูกโจมตีทางไซเบอร์ ก็อาจเป็นปัจจัยหนึ่งทำให้เกิดการละเมิดลิขสิทธิ์ซอฟต์แวร์ได้เช่นกัน (วิภาวดี อวยพร, 2560)

4) ปัญหาด้านการเข้าถึงข้อมูล (Accessibility)

สิทธิในการเข้าใช้งานโปรแกรมหรือระบบคอมพิวเตอร์ ซึ่งมักจะมีกำหนดสิทธิตามระดับของผู้ใช้งาน ทั้งนี้ เพื่อการป้องกันการเข้าไปดำเนินการต่างๆ กับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้อง และเป็นการรักษาความลับของข้อมูล ตัวอย่างสิทธิในการใช้งานระบบ เช่น การบันทึก การแก้ไขหรือปรับปรุง และการลบ เป็นต้น การกำหนดสิทธิตามระดับผู้ใช้งาน เพื่อป้องกันการเข้าไปดำเนินการต่างๆ กับข้อมูลของผู้ที่ไม่เกี่ยวข้อง การออกแบบระบบที่มีการรักษาความปลอดภัยในการเข้าถึงข้อมูลของผู้ใช้

(1) ปัญหาด้านการใช้อินเทอร์เน็ตและจริยธรรมดิจิทัล อาจเกิดจากผู้ที่มีทักษะการใช้งานอินเทอร์เน็ตและเทคโนโลยีสารสนเทศที่ไม่มากพอ หรือขาดความรู้เท่าทันเทคโนโลยี สื่อ กลุ่มผู้ใช้ และลักษณะสังคมออนไลน์ จึงอาจทำให้เกิดปัญหาการใช้งานในทางที่ไม่ถูกต้องเหมาะสม จากงานวิจัยของ อัญญาปารย์ และคณะ (2558) พบว่า ทักษะการใช้เทคโนโลยีสารสนเทศที่นักศึกษาระดับปริญญาตรีมหาวิทยาลัยราชภัฏกลุ่มภาคตะวันออกเฉียงเหนือ ควรได้รับการส่งเสริมในการสืบค้น การเลือกสรร การสร้างงาน และการสื่อสาร ตามลำดับ

(2) ปัญหาอินเทอร์เน็ตกับเยาวชนไทยอาจถือได้ว่าเป็นเรื่องของโรคระบาดทางอินเทอร์เน็ต (Internet Addiction Disorder) และโรค Webaholic ที่ผู้ใช้มักมีความต้องการสูงในการใช้งานระบบออนไลน์ทำให้ส่งผลร้ายทั้งในเรื่องของสุขภาพร่างกายความสมดุลทางอารมณ์และปัญหานี้จะเป็นจุดเริ่มของการก่อตัวสำหรับปัญหาอื่นๆ ที่ตามมา เช่น ประสิทธิภาพของการเรียนและการทำงานลดต่ำลงและค่าใช้จ่ายในการใช้บริการและการเชื่อมต่อสูงมากขึ้น ในประเทศไทยเองก็มีผู้ติดโรคนี้เป็นจำนวนไม่น้อยส่วนใหญ่มักเป็นนักศึกษาที่ติดการท่องเว็บไซต์ดาวน์โหลดโปรแกรม

รูปภาพไฟล์หรือพุดคุยสนทนากับผู้อื่นในอินเทอร์เน็ตโดยจะทำทุกครั้งที่มีโอกาสและสิ่งที่น่าเป็นห่วงคือ การเข้าไปใช้บริการในเว็บไซต์ที่ไม่เหมาะสม (เย็น ภูววรรณ และสมชาย นำประเสริฐชัย, 2546: 15)

(3) ปัญหาการเข้าถึงข้อมูลลามกอนาจาร และปัญหาการเผยแพร่ข้อมูลที่ทำให้ผู้อื่นเสื่อมเสียชื่อเสียง เนื่องจากเป็นกลุ่มเยาวชนที่มีทักษะการใช้เทคโนโลยีและส่วนใหญ่มีโอกาสในการเข้าใช้สังคมเครือข่ายออนไลน์ ซึ่งอาจเกิดปัญหาการใช้และขาดการตระหนักรู้ถึงจริยธรรมในการใช้เครือข่ายสังคมออนไลน์ได้

ปัญหาส่วนใหญ่ที่เกิดขึ้นกับกลุ่มคนในสังคมดิจิทัล โดยเฉพาะกลุ่มผู้ใช้เครือข่ายสังคมออนไลน์ ซึ่งเป็นพื้นที่สาธารณะที่คนในสังคมออนไลน์นี้ใช้ร่วมกันในการโพสต์ข้อความ ดาวน์โหลดข้อมูล โหวตเพื่อแสดงความคิดเห็น รวมถึงการแชร์ข้อมูลร่วมกัน ผู้ใช้จึงจำเป็นต้องคำนึงถึงการใช้งานเครือข่ายสังคมออนไลน์ ในด้านความถูกต้อง สิทธิความเป็นส่วนตัว มารยาทและจริยธรรมในการใช้เครือข่ายสังคมออนไลน์อย่างสร้างสรรค์ โดยเฉพาะอย่างยิ่งการใช้เครือข่ายสังคมออนไลน์ในกลุ่มเยาวชนที่มีการใช้กันอย่างแพร่หลาย ทำให้เกิดผลกระทบต่อการเรียนรู้และการดำเนินชีวิตประจำวันอย่างมาก โดยเฉพาะกลุ่มเยาวชนอาจขาดวิจารณญาณในการใช้เครือข่ายสังคมออนไลน์และมีพฤติกรรมการใช้ที่ไม่เหมาะสม เช่น การเปิดเผยข้อมูลส่วนตัว การแสดงความคิดเห็นการใช้ภาษา การละเมิดสิทธิส่วนบุคคล และพบว่าผู้ใช้เครือข่ายสังคมออนไลน์จำนวนมากมีพฤติกรรมการละเมิดสิทธิความเป็นส่วนตัวของผู้อื่น เช่น การนำข้อมูลส่วนบุคคลของผู้อื่นมาเผยแพร่ การใช้ภาพและข้อมูลอื่นๆ โดยที่ผู้นั้นมิได้รับรู้และยินยอม (คนาริปี ทองรวีวงศ์, 2553) อย่างไรก็ตามหลักจริยธรรมดิจิทัลในแต่ละประเด็นนั้นมีความเชื่อมโยงหรือเกี่ยวข้องกัน จึงอาจแยกไม่ได้ชัดเจนว่าปัญหาเหตุการณ์ หรือการกระทำนั้นๆ เป็นความผิดจริยธรรมดิจิทัลในด้านใด เพราะอาจมีความผิดในหลายประเด็นร่วมกัน

5.1.4 บทบาทขององค์กรต่อการมีจริยธรรมดิจิทัล

จากสภาพปัญหาการใช้งานเทคโนโลยีสารสนเทศ สื่อดิจิทัล และสื่อสังคมออนไลน์ของเยาวชนที่กล่าวมาข้างต้น หน่วยงานหรือองค์กรต่างๆ ควรมีบทบาทในการหาแนวทางเพื่อแก้ไขและป้องกันปัญหา และส่งเสริมจริยธรรมดิจิทัลให้กับประชาชน ทำให้เกิดการตระหนักถึงความท้าทายและทางเลือกสำหรับชีวิตของแต่ละบุคคลและสังคม และเล็งเห็นถึงความสำคัญของจริยธรรมแบบดิจิทัล ซึ่งเป็นประเด็นหนึ่งที่สำคัญต่อการติดต่อสื่อสารกันระหว่างบุคคลเพื่อให้เข้าใจและส่งเสริมความหลากหลายทางวัฒนธรรมของมนุษย์ ด้วยเหตุนี้ควรต้องมองหาหลักการทางจริยธรรมร่วมกันเพื่อให้วัฒนธรรมดิจิทัลสามารถกลายเป็นการแสดงออกที่แท้จริงของเสรีภาพและความคิดสร้างสรรค์ของมนุษย์

5.1.4.1 บทบาทของหน่วยงานภาครัฐ

ประเทศไทยความสำคัญกับการส่งเสริมการใช้ดิจิทัลอย่างสร้างสรรค์และรับผิดชอบต่อสังคม วัฒนธรรมและเสริมสร้างทักษะดิจิทัลเด็กเยาวชน ให้สามารถเข้าถึงเรียนรู้ และได้ประโยชน์จากการใช้เทคโนโลยีดิจิทัลอย่างปลอดภัยสร้างสรรค์มีจริยธรรมและตระหนัก ถึงผลกระทบต่อสังคม เพื่อเตรียมความพร้อมของประชาชนไทยสู่การเป็นพลเมืองดิจิทัลในอนาคตต่อไป (มาลี วงศาโรจน์, 2559) จากยุทธศาสตร์ประเทศไทย 4.0 มุ่งเน้นให้ประชาชนโดยเฉพาะในกลุ่มผู้เรียนให้ได้รับการพัฒนาอย่างมีคุณภาพทั้งความรู้ ทักษะอาชีพ ทักษะชีวิต ทักษะการทำงาน ที่สอดคล้องกับความต้องการของตลาดงาน รวมทั้งมีคุณธรรม จริยธรรม มีจิตสาธารณะและสามารถปรับตัวอยู่ร่วมกับผู้อื่นในสังคมได้ การเพิ่มความฉลาดทางศีลธรรมที่เป็นการปลูกฝังด้านจริยธรรม คุณธรรมให้แก่เด็กไทยที่เกิดในยุคดิจิทัล เพื่อเป็นการป้องกันปัญหาอาชญากรรมเด็กและวัยรุ่นในอนาคต ซึ่งข้อมูลปัจจุบันนี้พบว่าเด็กและเยาวชนที่กระทำผิดจำนวนมากในแต่ละปี ซึ่งความฉลาดทางศีลธรรมจะทำให้เด็กมีศีลธรรม ละอายต่อการกระทำผิด

ดังนั้นต้นทุนชีวิตของเด็กเยาวชนไทยในยุคดิจิทัลทุกคนจะต้องมีอย่างน้อย 3 ทักษะ ได้แก่ ความฉลาดทางเชาวน์ ความฉลาดทางอารมณ์และความฉลาดทางศีลธรรม (กรมสุขภาพจิต, 2560) นอกจากนี้จากการประเมินความต้องการจำเป็นในการพัฒนาการรู้เท่าทันสื่อดิจิทัล และพฤติกรรมการใช้สื่อดิจิทัลในการจัดการเรียนรู้แก่ผู้เรียนของนักศึกษาวิชาชีพครู โดยเฉพาะการพัฒนาการรู้เท่าทันสื่อดิจิทัลด้านเทคนิคในการเลือกซอฟต์แวร์และโปรแกรมที่มีความเหมาะสมต่อการเรียนรู้หรือการทำงานที่เฉพาะเจาะจงนั้นมีความต้องการจำเป็นในการพัฒนามากที่สุด รวมถึงการรู้หลักจรรยาบรรณคุณธรรม และกฎหมายที่เกี่ยวข้องกับ การผลิตเนื้อหาที่มีการใช้แหล่งทรัพยากรดิจิทัล (พิศุทธิภา และ วิชชุดา, 2559) ดังนั้นสิ่งสำคัญคือการพัฒนาทักษะด้านต่างๆที่จำเป็นสำหรับการเป็นพลเมืองดิจิทัลที่ดี ซึ่งรวมไปถึงการคิด วิเคราะห์ การรู้เท่าทันสื่อและการใช้เทคโนโลยีอย่างมีคุณธรรม จริยธรรม และมีความรับผิดชอบต่อสังคม ซึ่งสามารถตอบปัญหาความท้าทายที่ประเทศกำลังเผชิญอยู่หรือเพิ่มโอกาสในการพัฒนาทางเศรษฐกิจและสังคม

ประเด็นที่ความสำคัญอีกประการหนึ่งคือ การพัฒนาทุนมนุษย์สู่ยุคดิจิทัล ด้วยการเตรียมความพร้อมให้บุคลากรทุกกลุ่มมีความรู้และทักษะที่เหมาะสมต่อการดำเนินชีวิตในยุคดิจิทัล มีความสามารถในการพัฒนาและใช้สารสนเทศอย่างมีประสิทธิภาพ มีความตระหนัก ความรู้ ความเข้าใจ มีทักษะการใช้เทคโนโลยีดิจิทัลให้เกิดประโยชน์และสร้างสรรค์ ด้วยการส่งเสริมแนวปฏิบัติที่ดีในโลกดิจิทัล(กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2559) ในการแก้ไขปัญหาทางศีลธรรมตามมาตรฐานที่จะส่งเสริมและสร้างความรู้ความเข้าใจให้เด็กและเยาวชนนำวิธีการปฏิบัติว่าควรจะเป็นโลกแห่งชีวิตไปใช้การสื่อสารแบบดิจิทัลเพื่อจุดประสงค์ทางจริยธรรมที่ดี ดังนั้นจริยธรรม

ดิจิทัลจึงเป็นสิ่งสำคัญที่ช่วยพัฒนาให้ผู้เรียนมีลักษณะที่พึงประสงค์ตามที่กระทรวงศึกษาธิการได้กำหนดไว้ และนำไปสู่การเป็นพลเมืองดิจิทัลที่ดีของสังคม

ในบริบทของประเทศไทยได้มีการกำหนดการส่งเสริมทักษะทางดิจิทัลและจริยธรรมในนโยบายของแผนการพัฒนาด้านต่างๆ เช่น แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ.2560-2564) ได้ระบุวัตถุประสงค์หนึ่งของยุทธศาสตร์การเสริมสร้างและพัฒนาศักยภาพทุนมนุษย์ไว้ว่า เพื่อเตรียมความพร้อมคนในสังคมไทยให้มีทักษะในการดำรงชีวิต สังคม และระบบเศรษฐกิจของประเทศไทยให้สามารถปรับตัวรองรับผลกระทบจากการเปลี่ยนแปลงได้อย่างเหมาะสมสำหรับยุคศตวรรษที่ 21 และสังคมดิจิทัลแนวทางการพัฒนาดิจิทัลของกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. 2560-2564 ได้กำหนดยุทธศาสตร์การพัฒนาที่ส่งเสริมในประชาชนมีความรู้เท่าทันข้อมูลข่าวสาร และมีทักษะในการใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างมีความรับผิดชอบต่อสังคม และให้ความสำคัญกับการพัฒนาพลเมืองที่ฉลาด รู้เท่าทันข้อมูล และมีความรับผิดชอบ เพื่อให้เกิดการใช้เทคโนโลยีดิจิทัลอย่างสร้างสรรค์

5.1.4.2 บทบาทของสถาบันการศึกษา

การพัฒนาแนวทางการส่งเสริมจริยธรรมดิจิทัลนั้นได้รับความนิยมน้อยอย่างแพร่หลาย ในมหาวิทยาลัยหรือสถาบันการศึกษาในระดับอุดมศึกษา นักวิชาการด้านการศึกษาและนักวิชาการด้านเทคโนโลยี รวมถึงองค์กรด้านการศึกษาต่างให้ความสำคัญกับจริยธรรมดิจิทัลโดยมีการศึกษาพฤติกรรมของแต่ละกลุ่มบุคคลและทำการวิจัย การบรรยายให้ความรู้ การเปิดหลักสูตรอบรม การเขียนบทความบนเว็บไซต์ การเขียนเป็นหนังสือและตำรา จัดการเรียนการสอนในหลักสูตรการศึกษาระดับอุดมศึกษา รวมถึงการให้ความสำคัญกับจริยธรรมดิจิทัลในด้านการดำเนินธุรกิจ (Frank Buytendijk, 2016) มหาวิทยาลัยในต่างประเทศให้ความสำคัญในการส่งเสริมจริยธรรมดิจิทัลของนักศึกษาทั้งในภาพรวมและเฉพาะเจาะจงในสายงานวิชาชีพต่างๆ เพื่อจัดการกับความท้าทายด้านจริยธรรมที่เกิดจากนวัตกรรมดิจิทัล จริยธรรมมีผลต่อการพัฒนาด้านเทคโนโลยี วิทยาศาสตร์ การเมือง กฎหมาย ธุรกิจและในทุกด้านของสังคม (Luciano Floridi, 2017) สมาคมวิชาชีพด้านคอมพิวเตอร์และวิศวกรรมของสหรัฐอเมริกา ได้พัฒนาจริยธรรมและจรรยาบรรณในวิชาชีพอย่างกว้างขวาง และกำหนดให้เป็นเงื่อนไขสำหรับการเป็นสมาชิกที่ควรปฏิบัติตามหลักเกณฑ์ดังกล่าว และกลายเป็นกฎหมายบังคับเมื่อถูกนำมาใช้โดยคณะกรรมการออกใบอนุญาตของรัฐบาลหรือหน่วยงานกำกับดูแลวิชาชีพด้านคอมพิวเตอร์และวิศวกรรม (Matthew N. O. Sadiku, et al., 2017) ในแผนการศึกษาแห่งชาติ พ.ศ. 2560-2576 ได้ระบุวัตถุประสงค์หนึ่งของยุทธศาสตร์การพัฒนาศักยภาพคนทุกช่วงวัย และสร้างสังคมแห่งการเรียนรู้ไว้ว่า เพื่อพัฒนาคนไทยให้เป็นพลเมืองที่ดี มีคุณลักษณะ ทักษะ และสมรรถนะ ตรงตามมาตรฐานการศึกษาของชาติสอดคล้องกับทักษะการเรียนรู้ในศตวรรษที่ 21

นักวิชาการด้านการศึกษา และนักวิชาการด้านเทคโนโลยี รวมถึงองค์กรด้านการศึกษาต่างให้ความสำคัญกับจริยธรรมดิจิทัล (Digital Ethics) มีการศึกษาพฤติกรรมของแต่ละกลุ่มบุคคลและทำการวิจัย การบรรยายให้ความรู้ การเปิดหลักสูตรอบรม การเขียนบทความบนเว็บไซต์ การเขียนเป็นหนังสือและตำรา จัดการเรียนการสอนในหลักสูตรการศึกษาระดับอุดมศึกษา รวมถึงการให้ความสำคัญกับจริยธรรมดิจิทัลในด้านการดำเนินธุรกิจ (Frank Buytendijk, 2016) ผู้สอนจึงต้องสอนผู้เรียนให้มีประสิทธิผลและมีจริยธรรมในการสร้างสรรค์งานด้านดิจิทัล (DeVoss, Eidman-Aadahl และ Hicks, 2010) ผู้เรียนควรได้รับโอกาสในการใช้เครื่องมือดิจิทัลเพื่อให้ได้ทักษะที่จำเป็นสำหรับศตวรรษที่ 21 เพื่อช่วยให้ผู้ใช้เทคโนโลยีเป็นผู้รับผิดชอบ นักเรียน นักศึกษา หรือกลุ่มเยาวชนที่ในทุกวันนี้เริ่มใช้งานอุปกรณ์เทคโนโลยีมากขึ้น ทั้งที่บ้าน ที่ทำงาน สถาบันการศึกษา สถานที่สาธารณะ และหน่วยงานต่างๆ ทั่วไป ทุกคนมีการเตรียมตัวหรือเตรียมความพร้อมที่จะเป็นพลเมืองดิจิทัลที่ดีแล้วหรือยัง อาทิเช่น กฎเกณฑ์ด้านต่างๆ ด้านปลอดภัยและความรับผิดชอบต่อเทคโนโลยีในโลกของเทคโนโลยีเสมือนจริงนั้น พลเมืองดิจิทัลจะต้องมีความรู้ความเข้าใจ ความรู้สึกนึกคิด จริยธรรมต่อสังคม และทักษะด้านเทคโนโลยีต่างๆ การปฏิสัมพันธ์ของทักษะเหล่านี้ก่อให้เกิดพลเมืองดิจิทัลที่เหมาะสมสำหรับศตวรรษที่ 21 (Dede, 2010)

ทักษะการรู้ดิจิทัลจึงเป็นความสำคัญประเด็นหนึ่งที่จะส่งเสริมจริยธรรมดิจิทัลซึ่งจะนำไปสู่การเป็นพลเมืองดิจิทัลที่ดีได้ และมีส่วนในทุกประเภทของอาชีพและในชีวิตประจำวัน การรู้ดิจิทัลและข้อมูลรวมถึงความรู้พื้นฐานด้านตรรกะและคณิตศาสตร์มีความสำคัญมากขึ้นและควรได้รับการพิจารณาว่าเป็นทักษะที่สามารถถ่ายทอดได้ในสาขาต่างๆ ความรู้และความเข้าใจที่ลึกซึ้งยิ่งขึ้นเกี่ยวกับกระบวนการและเทคโนโลยีดิจิทัลนี้ควรแตกต่างจากความสามารถที่เรียบง่ายในการใช้งาน (ET2020–Peer Learning Activity (PLA), 2016) นักศึกษาของมหาวิทยาลัยหลายแห่งในประเทศไทยมีทักษะการรู้ดิจิทัลในด้านการตระหนักรู้ในระดับต่ำกว่าเมื่อเทียบกับนักศึกษามหาวิทยาลัยของรัฐ จึงควรมีการวางแผนกลยุทธ์เร่งพัฒนานักศึกษาให้มีการรู้ดิจิทัลในด้านการตระหนักรู้เพิ่มมากขึ้น โดยจัดเป็นรายวิชาศึกษาทั่วไปรายวิชาเฉพาะหรือบูรณาการในการเรียนการสอนรายวิชาต่างๆ รวมทั้งการวัดและติดตามผลอย่างต่อเนื่องเมื่อพบปัญหาหรืออุปสรรคในการดำเนินการจะได้แก้ไขได้ทันท่วงที (เววตา เตชาทวิวรรณ และ อัจศรา ประเสริฐสิน, 2559) ทั้งนี้เพื่อเป็นแนวทางในการอบรม การสอนและการให้ความรู้ด้านการใช้เครือข่ายสังคมออนไลน์ เพื่อให้นักศึกษาสามารถป้องกันตนเอง แนะนำผู้อื่นจากการแสดงพฤติกรรมที่ไม่เหมาะสม และเป็นการส่งเสริมให้มีจริยธรรมการใช้เครือข่ายสังคมออนไลน์อย่างถูกต้องและสร้างสรรค์ต่อไป

ดังนั้นปัญหาที่เป็นความท้าทายของสถาบันการศึกษา คือการพัฒนาคุณสมบัติทั่วไป ทักษะด้านต่างๆ และจริยธรรมดิจิทัลของนักศึกษาและบัณฑิตมักไม่ได้เป็นเรื่องที่ถูกอภิปรายหรือทำการวิจัยและการออกแบบหลักสูตร บางทักษะทั่วไปและทักษะของบัณฑิต อาทิเช่น

ทักษะความรู้สารสนเทศ จริยธรรม ความเป็นมืออาชีพที่มหาวิทยาลัยได้สอดแทรกไว้ในหลักสูตร ซึ่งอาจกล่าวได้ว่าเพื่อส่งเสริมทักษะในการรับผิดชอบ การมีคุณธรรมและจริยธรรมอย่างไรก็ตาม การเปลี่ยนแปลงของสภาพสังคม และนโยบายในการพัฒนาชาติเป็นสิ่งสำคัญที่จะขับเคลื่อนและความพยายามในการปรับปรุงสังคม (Richards, 2010 และ Bennett et al., 2008)

หลักสูตรและการเรียนรู้ในระดับมหาวิทยาลัยควรมีความรับผิดชอบต่อมากขึ้น ในการอำนวยความสะดวกในการส่งเสริมทักษะความรู้ต่างๆ ผู้การเป็นพลเมืองดิจิทัล เช่น การคิด วิเคราะห์อย่างสร้างสรรค์ การสังเคราะห์ การสร้างและการประเมินสารสนเทศและสื่อดิจิทัลสามารถ ช่วยให้นักศึกษากลายเป็นพลเมืองที่มีส่วนร่วมและมีความมุ่งมั่น การเรียนการสอนแบบดั้งเดิมที่ ผสมผสานกับการเรียนรู้เทคโนโลยีดิจิทัล มีความสำคัญในการพัฒนาทัศนคติในการปฏิบัติตาม อย่างเต็มที่ และส่งเสริมจริยธรรมดิจิทัลของนักศึกษาไปด้วยความคุ้นชินเหมือนการดำรงชีวิตด้วยความมีคุณธรรม จริยธรรม และซื่อสัตย์สุจริต มีความรับผิดชอบต่อตนเอง วิชาชีพและสังคม เคารพ กฎระเบียบ ข้อบังคับ สิทธิและรับฟังความคิดเห็นของผู้อื่น และสามารถวิเคราะห์ผลกระทบจากการใช้ สารสนเทศต่อบุคคลหรือองค์กรและสังคม โดยอยู่บนพื้นฐานของการตระหนักรู้และรับผิดชอบต่อ เทคโนโลยี นำเทคโนโลยีไปปรับใช้ ประยุกต์ใช้สู่การพัฒนานวัตกรรมก่อให้เกิดประโยชน์ต่อตนเอง และสังคม เพื่อให้นักศึกษาเห็นถึงความสำคัญและความรับผิดชอบต่อข้อมูลและการกระทำของตน เมื่อใช้อินเทอร์เน็ต อุปกรณ์ดิจิทัล สื่อดิจิทัล และสังคมออนไลน์ คำนึงถึงความปลอดภัยและปฏิบัติตาม กฎเกณฑ์ กฎหมาย ค่านิยมของสังคมที่ถูกต้อง และมีพฤติกรรมตามหลักจริยธรรมในยุคสังคม ดิจิทัล มีความตระหนักถึงการเป็นผู้สร้างและผู้รับสารสนเทศ เคารพสิทธิและความเป็นส่วนตัวของผู้อื่น ใช้กฎของโลกแห่งความเป็นจริงที่นำไปใช้กับโลกดิจิทัล เช่น ใช้รูปแบบการเขียนที่เหมาะสม หลีกเลี่ยง การโจมตีส่วนบุคคล และไม่กระทำการขโมย คัดลอก ดัดแปลงผลงานของผู้อื่น หรือนำไปใช้โดยไม่ได้รับ อนุญาตจากเจ้าของผลงานเพื่อให้จบไปเป็นบัณฑิตที่มีทักษะด้านคุณธรรมและจริยธรรมในการดำเนิน ชีวิตและการทำงานในยุคดิจิทัล

การส่งเสริมจริยธรรมดิจิทัลจึงเป็นสิ่งสำคัญที่ควรทำการศึกษาและผลักดัน ให้เกิดขึ้น ซึ่งเป็นประเด็นหนึ่งที่สำคัญของการอยู่ร่วมในสังคมและนำไปสู่การเป็นพลเมืองดิจิทัลที่มี คุณภาพ เพื่อให้กลุ่มเยาวชนที่กำลังจะก้าวไปสู่การเป็นกำลังคนในยุคสังคมดิจิทัล เป็นบุคลากรที่ ทำงานด้วยความสามารถในการเข้าถึงเรียนรู้ และได้ประโยชน์จากการใช้เทคโนโลยีดิจิทัลอย่างปลอดภัย มีความคิดสร้างสรรค์ มีจริยธรรม ตระหนักถึงผลกระทบต่อสังคม ใช้เทคโนโลยีดิจิทัลอย่างชาญฉลาด และมีความเชี่ยวชาญในการประกอบอาชีพตามระดับมาตรฐานสากลเพื่อนำไปสู่การเป็นพลเมืองที่ดีใน ยุคดิจิทัลที่ดี ซึ่งจะเป็นกำลังสำคัญในการตอบโต้การพัฒนาเศรษฐกิจและสังคมของประเทศทั้งใน ระดับองค์กรและระดับประเทศต่อไป

5.2 ความปลอดภัยทางเทคโนโลยีดิจิทัล

การความปลอดภัยทางเทคโนโลยีดิจิทัล เป็นอีกสิ่งหนึ่งที่สำคัญในโลกดิจิทัลที่คนเราต้องตระหนัก รู้วิธีป้องกันและหลีกเลี่ยงไม่ให้เกิดความเสี่ยง เพราะในโลกดิจิทัลนั้นแฝงไปด้วยภัยอันตรายต่างๆ มากมาย ที่อาจทำให้บุคคล องค์กร และสังคมได้รับความเสียหายได้ ไม่ว่าจะเป็นการถูกแฮคข้อมูล การถูกโจรกรรมข้อมูลที่สำคัญ การถูกขโมยรหัสผ่าน การถูกละเมิดทรัพย์สินทางปัญญา การถูกโจรกรรมทรัพย์สิน หรือการติดไวรัส และการโจมตีเฟิร์มแวร์ ซึ่งล้วนแต่เป็นภัยร้ายทั้งสิ้น อาจมีผลทำให้เกิดปัญหาทางธุรกิจจนถึงขั้น ต้องปิดตัวลงในที่สุดได้ ดังนั้นระบบความปลอดภัยในโลกดิจิทัลนี้ จึงมีความสำคัญที่จะทำให้ผู้ใช้อินเทอร์เน็ตและเทคโนโลยีดิจิทัลมีความปลอดภัย องค์กรนั้นสามารถสร้างระบบความปลอดภัยที่เข้มแข็ง ในการป้องกันข้อมูลจากการโจรกรรม หรือการโจมตีจากเฟิร์มแวร์ได้อย่างมีประสิทธิภาพ ซึ่งเป็นส่วนสำคัญ ทำให้เรานั้นปลอดภัยจากภัยร้าย ในโลกไซเบอร์ได้ในที่สุด

5.2.1 ภัยคุกคามในการใช้เทคโนโลยีดิจิทัล

ภัยคุกคามทางไซเบอร์ หมายถึงการกระทำหรือการดำเนินการโดยมิชอบ จากใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติกรรมแวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว (พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

การบูรณาการทางดิจิทัลเป็นอีกหนึ่งภัยคุกคามที่จะเป็นโมเดลธุรกิจหลักของอาชญากรคอมพิวเตอร์ส่วนใหญ่ และเป็นแรงผลักดันให้เกิดอุปขายอื่นๆ ที่จะหลอกลวงตามมา ขณะที่ช่องโหว่ในอุปกรณ์ด้านอินเทอร์เน็ตเพื่อสรรพสิ่ง (Internet of Things: IoT) จะเริ่มขยายพื้นที่ของการโจมตีอย่างเห็นได้ชัด เนื่องจากอุปกรณ์เหล่านี้จะเชื่อมต่อถึงกันมากยิ่งขึ้นจนเป็นสภาพแวดล้อมแบบอัจฉริยะในทุกแห่งหน อุปขายหลอกลวงทางอีเมลธุรกิจจะตกเหยื่อที่เป็นองค์กรมากขึ้นเพื่อหลอกเอาเงินยุคสมัยของข่าวปลอมและการโฆษณาชวนเชื่อทางอินเทอร์เน็ตจะยังคงดำเนินต่อไปด้วยกลวิธีต่างๆ ของอาชญากรคอมพิวเตอร์ การเรียนรู้ของเครื่องจักร (Machine Learning) และแอปพลิเคชันด้านบล็อกเชน (Blockchain) จะมีบทบาทที่ทำให้องค์กรต่างๆ จะต้องเผชิญกับความท้าทายใน

การปรับตัวให้ทันกับการบังคับใช้กฎหมายการปกป้องข้อมูลทั่วไป (General Data Protection Regulation: GDPR) สิ่งเหล่านี้คือภัยคุกคามที่เข้ามาบีบคั้นในยุคดิจิทัลและจะเป็นข้อพิสูจน์ว่าระบบการรักษาความปลอดภัยแบบใดที่จะเหมาะสมในการระบุและตรวจจับภัยคุกคามได้ เมื่อสภาพแวดล้อมเริ่มเชื่อมต่อกันมากขึ้นและซับซ้อนยิ่งขึ้น



ภาพที่ 5.1 ภัยคุกคามทางไซเบอร์

ที่มา: <https://www.cybersecurity-insiders.com/top-15-cyber-threats-for-2019/>

ภัยคุกคามทางไซเบอร์ได้ขยายขอบเขตสร้างความเสียหายให้แก่เศรษฐกิจ ภาพลักษณ์ และสังคมรุนแรงขึ้นเรื่อยๆ โดยเฉพาะอย่างยิ่งหน่วยงานภาครัฐที่ถือว่าเป็นหน้าตาของประเทศ รวมไปถึงถึงอาจจะมีข้อมูลที่จะเสียก่อนหลายๆ อย่างเก็บไว้อยู่ ซึ่งส่วนใหญ่มักจะเกิดกับองค์กรหรือสถาบันการเงิน ดังนั้นผู้ใช้งานบนโลกไซเบอร์จึงจะต้องเข้าใจถึงการใช้งานที่ไม่ก่อให้เกิดภัยต่อตนเอง องค์กร และสังคม เช่น ไม่คลิกลิงก์แปลกปลอม ไม่เข้าเว็บไซต์ที่เป็นอันตราย และต้องใช้ระบบอีเมลให้ดี เพราะอาจทำให้เกิดปัญหาการโดนขโมยข้อมูลได้

5.2.2 การรักษาความปลอดภัยในการใช้เทคโนโลยีดิจิทัล

ไม่ว่าจะเป็นการใช้งานสมาร์ทโฟน สื่อสังคมออนไลน์ อีคอมเมิร์ซหรือวิธีการอื่นๆ ที่เพิ่มขึ้นเราทุกคนต่างให้ข้อมูลส่วนบุคคลของเราไปบนอินเทอร์เน็ตมากขึ้นเรื่อยๆ ทำให้สิ่งต่างๆ ออนไลน์ง่ายขึ้นบางครั้งเราก็ทำสิ่งที่อันตรายมากขึ้น ในยุคที่การเชื่อมต่อเป็นเรื่องง่ายจนคนเราอาจไม่ได้นึกถึงอันตรายที่อยู่บนโลกอินเทอร์เน็ต บนสื่อสังคมออนไลน์ และในแอปพลิเคชันที่เราใช้กันอยู่ทุกวัน การใช้เทคโนโลยีดิจิทัลและเครือข่ายสังคมออนไลน์ หรือเรียกอย่างง่ายว่า “โลกไซเบอร์” ซึ่งเป็นข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป โดยทำให้เกิดเหตุการณ์ที่เกี่ยวกับความมั่นคง

ปลอดภัยไซเบอร์ที่เป็นเหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใดๆ ที่มีขอบซึ่งกระทำผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ การรักษาความมั่นคงปลอดภัยไซเบอร์ จึงเป็นมาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ (พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) อาจหมายถึงภาพรวมของเครื่องมือ (Tools), นโยบาย (Policies), แนวคิดการรักษาความปลอดภัย (Security Concepts), การรักษาความปลอดภัย (Security Safeguards), วิธีการบริหารความเสี่ยง (Risk Management Approaches), การปฏิบัติ (Actions), แนวทาง (Guidelines), การอบรม (Training), วิธีปฏิบัติที่เป็นเลิศ (Best Practices), การรับประกัน (Assurance) และเทคโนโลยี (Technologies) ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์สำหรับเชื่อมต่อกับคอมพิวเตอร์, ข้อมูลส่วนตัว, โครงสร้างพื้นฐาน, แอปพลิเคชัน, บริการ, ระบบสารสนเทศ และ ภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์ (สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU), 2008)

สำหรับประเทศไทย ยังไม่มีนิยามที่ชัดเจน วารสารสถาบันวิชาการป้องกันประเทศ ได้ให้นิยามคำว่า ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อให้องค์กร ปราศจากความเสียหายและความเสี่ยงที่มีผลต่อความปลอดภัยของข้อมูลข่าวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการก่ออาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่างๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล 3 ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) (ส่วนนโยบายรัฐบาลอิเล็กทรอนิกส์ สำนักงานรัฐบาลอิเล็กทรอนิกส์, 2559)

การรักษาความปลอดภัยแบบดิจิทัล (Digital Security) เป็นการป้องกันตัวตนออนไลน์ อาชญากรกำลังค้นหาวิธีใหม่ในการใช้งานและขโมยข้อมูลจากผู้ใช้ดิจิทัล เพื่อผลประโยชน์ส่วนตัว การรักษาความปลอดภัยแบบดิจิทัลจึงเป็นคำที่ครอบคลุมซึ่งรวมถึงเครื่องมือที่ผู้ใช้สามารถใช้เพื่อรักษาความปลอดภัยข้อมูลส่วนบุคคล สินทรัพย์ และเทคโนโลยีในโลกออนไลน์และสมาร์ทโฟน สามารถใช้เพื่อปกป้องตัวตน รวมถึงซอฟต์แวร์ป้องกันไวรัส, เว็บเซิร์ฟเวอร์, ไซเบอร์เมตริก และอุปกรณ์ส่วนตัวที่

ปลอดภัยที่ผู้ใช้พกติดตัวทุกวัน เป็นอุปกรณ์รักษาความปลอดภัยแบบดิจิทัลเพราะให้อิสรภาพในการสื่อสาร การเดินทาง เอกลักษณ์ดิจิทัลในวิธีที่สะดวกและปลอดภัย เมื่อพิจารณาถึงการเปลี่ยนแปลงอย่างรวดเร็วของภูมิทัศน์ดิจิทัลเป็นเรื่องธรรมดาที่ความปลอดภัยได้รับการพัฒนาที่ความเร็วใกล้เคียงกันซึ่งทำให้เราทุกคนต้องติดตามการพัฒนาล่าสุดและเพื่อให้แน่ใจว่าเรามีความปลอดภัยทางดิจิทัล เครื่องมือความปลอดภัยดิจิทัลที่สำคัญที่สุดที่ทุกคนสามารถใช้ได้ฟรีและเข้าถึงเครื่องมือเหล่านั้นได้ ความเสี่ยงด้านความปลอดภัยแบบดิจิทัลนั้นเป็นปัญหาทางเทคนิค แต่การเปลี่ยนแปลงลักษณะและขนาดของเหตุการณ์ความปลอดภัยทางดิจิทัลกำลังผลักดันให้ประเทศต่างๆ ประเมินกลยุทธ์และนโยบายใหม่ ดังนั้นเราควรระมัดระวังเกี่ยวกับสิ่งที่เราแบ่งปันแบบดิจิทัลและระมัดระวังเป็นพิเศษเมื่อได้รับข้อมูลที่เราสงสัยว่าอาจเป็นการหลอกลวง

5.3 กฎหมายลิขสิทธิ์และความคิดสร้างสรรค์ทางดิจิทัล

5.3.1 กฎหมายลิขสิทธิ์

5.3.1.1 งานอันมีลิขสิทธิ์ในปัจจุบันถูกบันทึกและนำเสนอในรูปแบบดิจิทัล (Digital) บนเครือข่ายอินเทอร์เน็ต จึงได้รับผลกระทบจากพัฒนาการทางเทคโนโลยีสารสนเทศเป็นอย่างมาก ซึ่งส่งผลกระทบต่อการถ่ายทอด ดัดแปลง ทำซ้ำได้อย่างรวดเร็วและข้อมูลยังเหมือนเดิม จึงจำเป็นต้องแก้ไขกฎหมายในพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 เป็นฉบับใหม่ขึ้นมาเพื่อบังคับใช้ให้ครอบคลุมมากขึ้น ด้วยการแก้ไขและเพิ่มเติมบทลงโทษเพื่อคุ้มครองเจ้าของลิขสิทธิ์ รวมทั้งเป็นส่วนหนึ่งในการขับเคลื่อนเศรษฐกิจเชิงดิจิทัล (Digital Economy) ในการขับเคลื่อนเศรษฐกิจของประเทศ และสอดคล้องกับสภาพการณ์ของสังคมที่กำลังเปลี่ยนผ่านเข้าสู่ยุคดิจิทัลซึ่งได้ออกมาเป็นพระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 2) พ.ศ. 2558 ที่กำหนดให้มีการคุ้มครองงานอันมีลิขสิทธิ์หรือสิทธิของนักแสดง รวมทั้งกำหนดข้อยกเว้นการกระทำละเมิดลิขสิทธิ์และสิทธิของนักแสดงเพิ่มขึ้น รวมทั้งให้ศาลมีอำนาจสั่งผู้ละเมิดลิขสิทธิ์ต้องจ่ายค่าเสียหายเพิ่ม และสั่งริบหรือทำลายสิ่งที่ใช้กระทำความผิด โดยสรุปเป็นสาระสำคัญได้ดังนี้

1) เพิ่มข้อยกเว้นการละเมิดลิขสิทธิ์

(1) มาตรา 32/1 การจำหน่ายต้นฉบับหรือสำเนางานอันมีลิขสิทธิ์โดยผู้ได้มาซึ่งกรรมสิทธิ์ในต้นฉบับหรือสำเนางานอันมีลิขสิทธิ์นั้นโดยชอบด้วยกฎหมาย มิให้ถือว่าเป็นการละเมิดลิขสิทธิ์

(2) มาตรา 32/2 การกระทำแก่งานอันมีลิขสิทธิ์ที่ทำหรือได้มาโดยชอบด้วยกฎหมายในระบบคอมพิวเตอร์ที่มีลักษณะเป็นการทำซ้ำที่จำเป็นต้องมีสำหรับการนำสำเนามาใช้ เพื่อให้อุปกรณ์ที่ใช้ในระบบคอมพิวเตอร์หรือกระบวนการส่งงานอันมีลิขสิทธิ์ทางระบบคอมพิวเตอร์ทำงานได้ตามปกติ มิให้ถือว่าเป็นการละเมิดลิขสิทธิ์

(3) มาตรา 32/3 ในกรณีที่มีหลักฐานอันควรเชื่อได้ว่าการละเมิดลิขสิทธิ์ในระบบคอมพิวเตอร์ของผู้ให้บริการ เจ้าของลิขสิทธิ์อาจยื่นคำร้องต่อศาลเพื่อมีคำสั่งให้ผู้ให้บริการระงับการละเมิดลิขสิทธิ์นั้น

2) ความรับผิดชอบของผู้ให้บริการ (Internet Service Provider: ISP) บัญญัติขึ้นเพื่อปกป้องเจ้าของลิขสิทธิ์จากการละเมิดผ่านทางอินเทอร์เน็ต อันเป็นการสื่อสารแบบใหม่ในรูปแบบดิจิทัล ทั้งนี้ผู้ให้บริการ คือผู้ให้บริการแก่บุคคลอื่นให้เข้าสู่อินเทอร์เน็ต หรือสามารถติดต่อกันได้ผ่านระบบคอมพิวเตอร์ หรือผู้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

ส่วนในกรณีที่มีหลักฐานที่เชื่อว่าการละเมิดลิขสิทธิ์ในคอมพิวเตอร์ของผู้ให้บริการ เจ้าของลิขสิทธิ์อาจยื่นคำร้องต่อศาลสั่งให้ผู้ให้บริการระงับการละเมิดลิขสิทธิ์นั้นได้ หากเป็นกรณีที่ผู้ให้บริการไม่ใช่ผู้ควบคุม ริเริ่ม หรือสั่งการให้มีการละเมิดลิขสิทธิ์ในระบบคอมพิวเตอร์ และผู้ให้บริการได้ดำเนินการตามคำสั่งของศาลแล้ว ผู้บริการไม่ต้องรับผิดชอบต่อความเสียหายใดๆ ที่เกิดขึ้นตามคำสั่งของศาลอีก

3) ธรรมชาติของนักแสดง คือ นักแสดงที่เป็นผู้ถ่ายทอดผลงานเองย่อมมีสิทธิแสดงว่าตนเป็นนักแสดงและมีสิทธิห้ามบุคคลอื่นบิดเบือน ตัดทอน ดัดแปลง หรือทำการอื่นๆ จนเกิดความเสียหายหรือเกียรติคุณของนักแสดง และเมื่อนักแสดงเกิดเสียชีวิต ทายาทของนักแสดงมีสิทธิฟ้องร้องบังคับตามสิทธิได้ตลอดอายุแห่งการคุ้มครองสิทธิของนักแสดง เว้นแต่มีการตกลงกันไว้เป็นอย่างอื่นเป็นลายลักษณ์อักษร

4) ข้อมูลการบริการสิทธิ คือ ข้อมูลที่บ่งชี้ถึงผู้สร้างสรรค์ งานสร้างสรรค์ นักแสดง การแสดง เจ้าของลิขสิทธิ์ หรือระยะเวลาและเงื่อนไขการใช้งานอันมีลิขสิทธิ์ ตลอดจนตัวเลขหรือรหัสแทนข้อมูลดังกล่าว โดยข้อมูลนี้เกี่ยวข้องหรือติดอยู่กับงานอันมีลิขสิทธิ์หรือสิ่งที่บันทึกการแสดง

5.3.1.2 ข้อยกเว้นบางประการที่ไม่ถือว่าการละเมิดมาตรการทางเทคโนโลยีมีดังนี้

1) การหลบเลี่ยงมาตรการทางเทคโนโลยีเพื่อประโยชน์ทางการวิจัย วิเคราะห์ และหาข้อบกพร่องของเทคโนโลยีการเข้ารหัส หรือเพื่อการทดสอบ ตรวจสอบ หรือแก้ไขระบบ ความมั่นคงปลอดภัยของคอมพิวเตอร์

2) กรณีเป็นการกระทำของเจ้าพนักงานผู้มีอำนาจตามกฎหมายทำไปเพื่อป้องกันประเทศ หรือรักษาความมั่นคงแห่งชาติ

5.3.1.3 ทั้งนี้ในส่วนของพระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 3) พ.ศ. 2558 ได้มีการแก้ไขเพิ่มเติมจากเดิม เนื่องจากในปัจจุบันมีปัญหาการทำซ้ำ โดยการบันทึกเสียงหรือภาพหรือทั้งสองกรณี ระหว่างการฉายภาพยนตร์ทั้งภาพยนตร์ไทยและภาพยนตร์ต่างประเทศโดยไม่ได้รับอนุญาต แล้วนำไปทำซ้ำในสื่อต่างๆ เช่น แผ่นซีดีหรือแผ่นดีวีดี ออกจำหน่าย ทำให้เกิดความเสียหายเป็นอย่างมาก

โดยอาศัยข้อยกเว้นการละเมิดลิขสิทธิ์ตามกฎหมายที่ว่าเป็นการทำซ้ำเพื่อประโยชน์ของตนเอง จึงได้มีการกำหนดให้การทำซ้ำในลักษณะดังกล่าวเป็นความผิดเฉพาะและได้รับโทษเช่นเดียวกับการละเมิดเพื่อการค้า มีสาระสำคัญ 2 ดังนี้

1) การแอบถ่ายในโรงภาพยนตร์ คือการทำซ้ำ (Camcording Provision) โดยการบันทึกเสียงหรือภาพจากภาพยนตร์อันมีลิขสิทธิ์โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์ ในระหว่างการฉายภาพยนตร์ ให้ถือเป็นการละเมิดลิขสิทธิ์ และห้ามไม่ให้อาศัยข้อยกเว้นการละเมิดลิขสิทธิ์ในเรื่องการทำซ้ำเพื่อประโยชน์ของตนเองด้วย

2) ข้อยกเว้นในการทำซ้ำหรือดัดแปลงเพื่อประโยชน์ของคนพิการ ให้มีการอนุญาตการทำซ้ำหรือดัดแปลงงานอันมีลิขสิทธิ์เพื่อประโยชน์ของคนพิการที่ไม่สามารถเข้าถึงงานอันมีลิขสิทธิ์ได้ จากความบกพร่องทางการได้ยิน เห็น สติปัญญา หรือการเรียนรู้ และความบกพร่องอื่นๆ ที่กำหนดไว้ในพระราชกฤษฎีกาและการทำซ้ำจะต้องไม่เป็นการกระทำที่หากำไร

5.3.2 กฎหมายด้านจริยธรรมและความปลอดภัยในการใช้เทคโนโลยีดิจิทัล

5.3.2.1 พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เป็นพระราชบัญญัติ เพื่อปกป้องระบบคอมพิวเตอร์และโครงข่ายเทคโนโลยีสารสนเทศ ของโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ หรือ บริการที่สำคัญของประเทศมีความมั่นคงปลอดภัยสามารถให้บริการได้เป็นปกติ และหน่วยงานสามารถรับมือกับภัยคุกคามทางไซเบอร์ ได้อย่างทันท่วงที โดยสรุปเป็นสาระสำคัญกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้ดังนี้

1) กำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐ มีมาตรฐานและมีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้แก่ โครงสร้างพื้นฐานด้านความมั่นคง ของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศ และโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุขและด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

2) มีการเฝ้าระวังภัยคุกคามและมีแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ

3) มีการร่วมมือและประสานงานกันกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อมีภัยร้ายแรงที่ทำให้การให้บริการที่สำคัญไม่สามารถทำงานได้ จนทำให้ประชาชนเดือดร้อน

สิ่งที่ประชาชนจะได้รับจากการมีพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ คือการมีระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญมีความปลอดภัยสามารถให้บริการได้อย่างต่อเนื่อง มีแนวทางในการรับมือภัยคุกคามทางไซเบอร์ไม่ให้เกิดผลกระทบเป็นวงกว้างและกลับมาทำงานได้อย่างรวดเร็ว รวมถึงมีการจัดตั้งหน่วยงานขึ้นมาดูแลมาตรฐาน

ด้านความปลอดภัยไซเบอร์และให้ความช่วยเหลือแก่หน่วยงานโครงสร้างพื้นฐานที่สำคัญ เมื่อเกิดภัยคุกคามร้ายแรง การเข้าไปแก้ไขปัญหา ที่ต้องเข้าถึงทรัพย์สินจะต้องใช้คำสั่งศาล เพื่อคุ้มครองสิทธิ โดยมีมาตรการที่ใช้แก้ปัญหาเพื่อรักษา ความมั่นคงปลอดภัยไซเบอร์ โดยใช้บุคลากรกระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวข้องกับคอมพิวเตอร์ใดๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ อีกทั้งยังมีนโยบายด้านการพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐและเอกชน และการสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2562)

5.3.2.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ด้วยความก้าวหน้าทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว และแนวโน้มเกิดการละเมิดสิทธิในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวมีเพิ่มมากขึ้น โดยเฉพาะการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์หรือเปิดเผยโดยมิชอบ หรือโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล เพื่อประโยชน์ในทางการค้า หรือเพื่อประโยชน์ในการนำข้อมูลส่วนบุคคลไปใช้ในการกระทำผิดต่างๆ เช่น การฉ้อโกง การหมิ่นประมาท เป็นต้น ซึ่งปัญหาเหล่านี้ ย่อมส่งผลกระทบต่อความเชื่อมั่นในการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามนโยบายของรัฐบาล ดังนั้น จึงมีความจำเป็นที่ประเทศไทยจะต้องเร่งผลักดันให้มีกฎหมายว่า ด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศ เพื่อสร้างกลไกการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นมาตรฐานเดียวกันและสอดคล้องกับมาตรฐานที่เป็นสากล โดยต้องไม่สร้างภาระหน้าที่แก่ผู้เกี่ยวข้องจนกลายเป็นข้อจำกัดหรืออุปสรรคในการประกอบธุรกิจการค้าหรือการให้บริการของภาคส่วนต่างๆ จนเกินสมควร เพื่อแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2562) โดยสรุปเป็นสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้ดังนี้

- 1) บุคคลเจ้าของข้อมูลต้องให้ความยินยอม การเก็บรวบรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคล
- 2) ผู้เก็บรวบรวมข้อมูลส่วนบุคคลต้องรักษาความมั่นคงปลอดภัยของข้อมูลไม่ให้มีการเปลี่ยนแปลงแก้ไขหรือมีใครเข้าถึงได้โดยมิชอบ
- 3) บุคคลเจ้าของข้อมูล มีสิทธิถอนความยินยอม หรือขอให้ลบหรือทำลายข้อมูลได้ เมื่อถูกนำไปใช้ในทางไม่ชอบด้วยกฎหมาย

โดยมีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ทำหน้าที่กำหนดมาตรฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และให้ความรู้และการฝึกอบรมแก่หน่วยงานรัฐ เอกชน และบุคคลทั่วไป ในการคุ้มครองข้อมูลส่วนบุคคล รวมถึงกำหนดให้มี

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ที่เป็นผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์ เป็นที่ ประจักษ์ในด้านคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ ด้านการเงิน หรือด้านอื่น ทั้งนี้ต้อง เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล โดยมีปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจ และสังคมเป็นรองประธานกรรมการ ซึ่งคณะกรรมการนี้มีหน้าที่พิจารณาเรื่องร้องเรียนเมื่อมีการละเมิด ตรวจสอบผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหาย แก่เจ้าของข้อมูล และใกล้เคียงข้อพิพาท

สิ่งที่ประชาชนจะได้รับจากการมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล คือมีหน่วยงานที่ช่วยกำกับดูแลและป้องกันการล่วงละเมิดความเป็นส่วนตัวของข้อมูลส่วนบุคคล ปกป้องความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล และความเดือดร้อนรำคาญ สร้างกลไกหรือมาตรฐาน การกำกับดูแลในการคุ้มครองข้อมูลส่วนบุคคล รวมถึงสามารถฟ้องเรียกค่าสินไหมทดแทนกรณี ถูกละเมิดข้อมูลส่วนบุคคล

5.3.2.3 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวทางการให้บริการ คลาวด์ พ.ศ. 2562

ในปัจจุบันการให้บริการธุรกรรมทางอิเล็กทรอนิกส์มีการให้บริการคลาวด์ (Cloud Computing) อย่างแพร่หลาย อาศัยจากการให้บริการคลาวด์จากผู้ประกอบการรายอื่น เพื่อให้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่ใช้บริการคลาวด์ มีความมั่นคงปลอดภัย ความน่าเชื่อถือ และ มาตรฐานในการให้บริการ ซึ่งเป็นที่ยอมรับในระดับสากล แนวทางการให้บริการคลาวด์ ฉบับนี้มีวัตถุประสงค์เพื่อให้ผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ใช้อ้างอิง ประกอบการพิจารณา บริการของผู้ให้บริการคลาวด์ โดยคำนึงถึงหลักเกณฑ์ขั้นพื้นฐาน ซึ่งเป็นมาตรฐานขั้นต่ำในการลด ความเสี่ยงจากภัยคุกคาม โดยจะต้องตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ รวมทั้งปรับปรุง มาตรการเพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสม

1) หลักเกณฑ์การให้บริการ เพื่อให้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่ใช้ บริการคลาวด์ มีความมั่นคงปลอดภัย เชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล ผู้ใช้บริการควรพิจารณาข้อมูลที่เกี่ยวข้องกับบริการตามแนวทางที่กำหนด ดังนี้

(1) นโยบายและแนวทางปฏิบัติขององค์กร

ผู้ให้บริการควรพิจารณานโยบายและแนวปฏิบัติในองค์กรของผู้ ให้บริการที่เกี่ยวข้องกับกระบวนการทำงาน โดยมีนโยบายการพัฒนาทรัพยากรบุคคลากรให้มีความรู้ ความเข้าใจในเรื่องความมั่นคงปลอดภัยของข้อมูล นโยบายการจัดการสินทรัพย์และการ เปลี่ยนแปลง รวมถึงการบริหารความเสี่ยง และการติดตามดูแลการให้บริการ โดยมีมาตรการ ป้องกันเพื่อรักษาความมั่นคงปลอดภัยแก่สินทรัพย์ทางกายภาพ เช่น การกำหนดควบคุมพื้นที่

ความปลอดภัยในพื้นที่หวงห้าม การควบคุมการเข้าออกพื้นที่ อีกทั้งมาตรการป้องกันสำหรับความมั่นคงปลอดภัยและความน่าเชื่อถือทางเทคนิค เช่น โครงสร้างระบบเสมือน (Virtual Infrastructure) และสภาพแวดล้อมของระบบ การควบคุมการเข้าถึง การยืนยันตัวตน การตรวจสอบสิทธิของผู้ใช้งาน ระบบความมั่นคงปลอดภัยเครือข่าย การคุ้มครองข้อมูล การเข้ารหัส การวิเคราะห์ ออกแบบและพัฒนา ระบบตามวัฏจักรการพัฒนาระบบงาน แนวทางการรักษาความปลอดภัยในการพัฒนาซอฟต์แวร์และ (Application Programming Interface: API) และแนวทางในการรักษาความปลอดภัยในการจ้างบุคคลภายนอก (Outsourcing)

(2) ประสิทธิภาพการให้บริการ

ผู้ให้บริการควรพิจารณาข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ที่เกี่ยวข้องกับสภาพพร้อมใช้งาน ระยะเวลาการตอบสนอง ความสามารถรองรับปริมาณงาน บริการสนับสนุนโดยมีช่องทางและเวลาที่ผู้ให้บริการสามารถแจ้งปัญหา หรือติดต่อสอบถามจากผู้ให้บริการ เช่น การกำหนดให้ผู้ให้บริการสามารถติดต่อผู้ให้บริการได้ตลอด 24 ชั่วโมง และระยะเวลาในการแก้ไขปัญหา การใช้งานตั้งแต่เริ่มต้นจนปัญหานั้นสิ้นสุด และกระบวนการยุติสัญญา

(3) การรักษาความมั่นคงปลอดภัย

ผู้ให้บริการควรพิจารณามาตรการ การรักษาความมั่นคงปลอดภัยในระบบสารสนเทศในข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ที่เกี่ยวข้องกับความน่าเชื่อถือของบริการ การพิสูจน์ตัวตนและการอนุญาต การเข้ารหัส การรายงานเหตุการณ์และการจัดการรักษาความมั่นคงปลอดภัย การบันทึกและการตรวจสอบข้อมูลการใช้งานระบบ การตรวจสอบขั้นตอนกระบวนการทำงานและความปลอดภัยการจัดการช่องโหว่ และธรรมาภิบาล

(4) การจัดการข้อมูล

ผู้ให้บริการควรพิจารณาข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ที่เกี่ยวข้องกับการจัดประเภทข้อมูล การสำรองข้อมูลและการเรียกคืนข้อมูล วงจรชีวิตของข้อมูล และการโอนย้ายข้อมูล

(5) การคุ้มครองข้อมูลส่วนบุคคล

ผู้ให้บริการควรพิจารณาข้อตกลงระดับการให้บริการ ที่เกี่ยวข้องกับแนวปฏิบัติตามมาตรฐานสากลในการคุ้มครองข้อมูลส่วนบุคคล การระบุวัตถุประสงค์การเก็บข้อมูล การเก็บรักษาข้อมูลเท่าที่จำเป็น การใช้ เก็บรักษาและการเปิดเผย ความโปร่งใสและการแจ้งเตือน ความรับผิดชอบต่อข้อมูล สถานที่จัดเก็บข้อมูล และการอำนวยความสะดวกในการเข้าถึงข้อมูล

5.3.2.4 กฎเกณฑ์การใช้งานสื่อสังคมออนไลน์

ด้วยที่ตั้งแต่เทคโนโลยีการสื่อสารพัฒนาอย่างก้าวล้ำ สื่อสังคมออนไลน์ กลับส่งผลไปในการลอบต่อชีวิตประจำวันและความสัมพันธ์ของคนในสังคมอย่างชัดเจนยิ่งขึ้น จนกลายเป็นประเด็นทางสังคมที่ทั้งสื่อ กฎหมายและประชาชนเองจะต้องให้ความสำคัญในการป้องกัน และแก้ไขปัญหาต่างๆ ที่เกิดขึ้นจากการใช้สื่อสังคมออนไลน์ ในเอกสารประกอบการเรียนการสอนฉบับนี้ขอยกตัวอย่างกฎเกณฑ์การใช้งานของเฟซบุ๊ก (Facebook) ซึ่งเป็นสื่อสังคมออนไลน์ที่ได้รับความนิยมมากที่สุดทั่วโลกมาเป็นเวลาหลายปี เมื่อมีผู้คนเข้ามาใช้งานเฟซบุ๊ก เพื่อแบ่งปันเรื่องราวของตัวเอง รับข่าวสารเกี่ยวกับความเป็นไปของโลกผ่านมุมมองของผู้อื่น และเชื่อมต่อกับเพื่อน เพื่อต้องการให้ผู้ใช้งานมีความปลอดภัยเมื่อใช้งาน ทางเฟซบุ๊กได้ให้บริการพีเจอร์ นโยบาย และเครื่องมืออย่างหลากหลาย ซึ่งถูกออกแบบขึ้นเพื่อรักษาข้อมูลส่วนตัวและตัวตนของพวกเขาจากอันตรายที่มาจากผู้ไม่ประสงค์ดี ผู้ใช้เองนั้นควรจะต้องหมั่นรักษาข้อมูลออนไลน์ของตนเองให้ปลอดภัยอยู่เสมอ ด้วยการปฏิบัติตามขั้นตอนเพื่อความปลอดภัย

1) เฟซบุ๊กจึงได้มีนโยบายและกฎเกณฑ์ออกมาเพื่อรักษาความปลอดภัย เช่น กฎเกณฑ์ในการโพสต์ข้อมูลต่างๆ บนเฟซบุ๊ก ได้แก่

(1) ห้ามโพสต์ภาพโป๊เปลือยทั้งผู้ใหญ่และเด็ก รวมทั้งกิจกรรมทางเพศ เนื้อหาขบถและกรณีเด็ก แม่พ่อแม่โพสต์เองก็ไม่สามารถกระทำได้

(2) ภาพห้วนมเพศหญิง เว้นแต่เป็นการประท้วง, การให้นมบุตรหรือรักษามะเร็งเต้านม

(3) การใส่ความเหยียดจากเหตุร้ายแรง เช่นบอกว่าเหยื่อเป็นคนโกหกหรือบอกว่าเหยื่อถูกจ้างให้สร้างความเข้าใจผิดต่อสถานการณ์

(4) การยอมรับและส่งเสริมอาชญากรรม ไม่ว่าผู้ใช้จะก่อเอง หรือคนอื่นก่อ เช่น การทำร้ายคนหรือสัตว์ โจรกรรม ค้ามนุษย์

(5) การยอมรับ การใช้ การส่งเสริมเกี่ยวกับกัญชา ยาเสพติด และปืนที่ผิดกฎหมาย รวมถึงการซื้อขายแลกเปลี่ยน และการแสดงความสนใจก็ทำไม่ได้

(6) การข่มขืนหรือเรียกร้องความรุนแรง ต่อคน กลุ่มคน สถานที่เสี่ยง รวมทั้งวิธีผลิต ใช้ระเบิดเพื่อความรุนแรงและความรุนแรงจากผลการเลือกตั้ง

(7) ข้อมูลส่วนตัว บัตรที่ออกโดยรัฐ เลขบัตรประชาชน พาสปอร์ต รหัสผ่าน ข้อมูลการแพทย์ ข้อมูลทางการเงิน ช่องทางติดต่อที่ละเมิดสิทธิ

(8) คำพูดที่แสดงความเกลียดชัง ซึ่งโจมตีเผ่าพันธุ์ เชื้อชาติ ศาสนา เพศ ประเทศที่กำเนิด ธรรมเนียมและอัตลักษณ์ทางเพศ ความพิการ โรคภัยหรือข่มขู่คุกคาม ลดทอนคุณค่าผู้อื่น

(9) เนื้อหาที่ส่งเสริม แนะนำการฆ่าตัวตายและการทำร้ายตัวเอง

(10) การสร้างโปรไฟล์ปลอม ปลอมเป็นผู้อื่นหรือละเมิดทรัพย์สินทางปัญญา สแปมเมล และแอบอ้างให้คลิกไลค์หรือแชร์ (<https://www.facebook.com/communitystandards>)
ดังนั้น การปฏิบัติตามขั้นตอนเพื่อรักษาความปลอดภัยและปกป้องข้อมูลและบัญชีผู้ใช้งานจึงมีความสำคัญเป็นอย่างยิ่ง แม้ว่าความสำคัญของความปลอดภัยทางช่องทางออนไลน์และความเป็นส่วนตัวเป็นสิ่งที่รับรู้และเข้าใจในวงกว้างของประเทศไทย แต่ก็ยังมีผู้ใช้งานอินเทอร์เน็ตอีกมากที่ละเลยการปฏิบัติตามกฎพื้นฐานด้านความปลอดภัย ทำให้ข้อมูลส่วนตัวและความปลอดภัยของผู้ใช้มีความเปราะบางมากยิ่งขึ้น

5.3.3 ความคิดสร้างสรรค์ทางดิจิทัล

จากปัญหาการกระทำผิดหลักจริยธรรมดิจิทัลที่เกิดขึ้นจากพฤติกรรมสารสนเทศบนเครือข่ายอินเทอร์เน็ต สื่อสังคมออนไลน์ และเทคโนโลยีดิจิทัลต่างๆ นำไปสู่การหาแนวทางแก้ไขปัญหาและป้องกัน จึงเกิดเป็น โดยมีข้อกำหนดกฎเกณฑ์ ข้อบังคับและกฎหมายต่างๆ เพื่อการรักษาความปลอดภัยในการใช้เทคโนโลยีดิจิทัล ดังที่กล่าวมาข้างต้น และเพื่อให้เกิดความสะดวกรวดเร็วจึงมีการดำเนินชีวิตในยุคดิจิทัลนี้ จึงมีแนวทางที่เป็นทางเลือกที่ดีในการใช้สารสนเทศเพื่อลดปัญหาการกระทำผิดหลักจริยธรรมดิจิทัล คือการรู้เท่าทันดิจิทัล โดยมีวิธีการง่ายๆ อย่างเช่น เมื่อเราค้นหาที่มาของเนื้อหาควรใช้เนื้อหาจากงานต้นฉบับ ทำการตรวจสอบสัญญาภายใต้งานอย่างระมัดระวัง โดยอ่านข้อกำหนด เงื่อนไข นโยบายลิขสิทธิ์ หรือเอกสารใดๆ อย่างระมัดระวัง ก่อนใช้เนื้อหา หากมีการกล่าวถึงการใช้งานที่จำกัด ให้ทำตามคำแนะนำดังกล่าว ควรอ่านเนื้อหาให้เข้าใจแล้วสังเคราะห์และเรียบเรียงประโยคใหม่ด้วยรูปแบบการเขียนที่เป็นของตนเอง และแสดงแหล่งที่มาอาจติดต่อสื่อสารกับเจ้าของงาน เพื่อขออนุญาตใช้งานที่เจ้าของงานสร้างขึ้น และที่สำคัญที่สุดคือการปฏิบัติตามการใช้ลิขสิทธิ์ที่เป็นธรรม (วิกิพีเดีย, 2561) และอีกแนวทางหนึ่งคือ การใช้ข้อมูลเปิด หรือคลังทรัพยากรสารสนเทศแบบเปิด ที่ซึ่งเป็นความคิดสร้างสรรค์ทางดิจิทัล

5.3.3.1 ข้อมูลเปิด (Open Data)

ข้อมูลเปิด (Open Data) คือข้อมูลที่เราสามารถนำไปใช้ได้อย่างเสรี ไม่มีข้อจำกัด สามารถนำกลับมาใช้ใหม่ (Reuse) และแจกจ่ายต่อได้ ทั้งนี้ต้องระบุแหล่งที่มาและต้องใช้เงื่อนไขเดียวกันกับที่มาหรือตามที่เจ้าของงานกำหนด โดยข้อมูลดังกล่าวต้องอยู่ในรูปแบบที่สะดวกต่อการนำไปใช้งานต่อและสามารถปรับปรุงแก้ไขได้ (หรือเรียกได้ว่าอยู่ในรูปแบบที่อ่านได้โดยคอมพิวเตอร์) ส่วนค่าใช้จ่ายในการได้มาซึ่งข้อมูลนั้นก็ไม่ต้องไม่มากไปกว่าค่าใช้จ่ายในการทำสำเนา โดยเฉพาะการดาวน์โหลดผ่านอินเทอร์เน็ต ซึ่งข้อมูลทั้งหมดที่อยู่บนเว็บไซต์ Data.go.th นี้ เป็นข้อมูลเปิดของภาครัฐ (Open Government Data) ทุกวันนี้หลายประเทศมีกระแสเรียกร้องให้มีการนำข้อมูลเปิด (Open Data) มาใช้เพื่อช่วยแก้ปัญหาการคอร์รัปชัน ในประเทศไทยเองก็มีคนตั้งคำถามไว้มากมายว่า

“Open Data” นั่นคืออะไร และเมื่อมีแล้วจะช่วยแก้ปัญหาคอร์รัปชันได้จริงหรือไม่ ข้อมูลเปิด โดยเฉพาะข้อมูลเปิดภาครัฐ หรือ “Open Government Data” มีส่วนช่วยสร้างความโปร่งใสในการดำเนินงานของรัฐ

1) หลักสำคัญของข้อมูลเปิดนั้น เป็นความสำคัญที่สนับสนุนให้เกิดการทำงานร่วมกัน (interoperability) อย่างเป็นทางการแบ่งเป็น 3 ประการ ได้แก่

(1) Availability and Access คือ ข้อมูลที่เปิดเผยต้องสามารถใช้งานได้ทั้งหมดและกรณีที่มีค่าใช้จ่ายจะต้องไม่มากกว่าการทำสำเนา สำหรับการเผยแพร่จะต้องอยู่ในรูปแบบที่ง่ายต่อการใช้งานและสามารถแก้ไขได้ สามารถดาวน์โหลดฟรีผ่านอินเทอร์เน็ต

(2) Re-use and Redistribution คือ ข้อมูลที่เผยแพร่ต้องถูกจัดเตรียมภายใต้เงื่อนไข การอนุญาตให้นำมาใช้ใหม่และเผยแพร่ได้ รวมถึงการใช้ชุดข้อมูลร่วมกับชุดข้อมูลอื่นๆ

(3) Universal Participation คือ ทุกคนสามารถที่จะใช้ข้อมูลได้ ไม่ว่าจะเป็นการใช้งานไปใช้ การเข้าถึง การเผยแพร่ โดยไม่ติดเรื่องข้อจำกัดใดๆ แต่ทั้งนี้จะต้องเป็นไปตามวัตถุประสงค์ของเจ้าของข้อมูลนั้นๆ เช่น หากเป็นข้อมูลที่ไม่อนุญาตให้ใช้งานเชิงพาณิชย์ (Non-Commercial) จะไม่สามารถนำไปใช้ในเชิงพาณิชย์ได้ หรือข้อมูลนั้นอาจมีข้อจำกัดในการใช้งานเพื่อวัตถุประสงค์บางอย่างเช่น ใช้ในการศึกษาเท่านั้น ก็จะไม่สามารถนำไปใช้ได้

2) ประโยชน์ที่ได้รับจากการใช้ข้อมูลเปิด (Open Data)

(1) ความโปร่งใส (Transparency) เป็นการเปิดเผยข้อมูลของภาครัฐให้ประชาชนและภาคประชาสังคมเข้าถึงข้อมูลและสามารถตรวจสอบการดำเนินงานของภาครัฐตามนโยบายที่ประกาศให้ไว้กับประชาชน

(2) การยกเว้นมูลค่าทางสังคมและเชิงพาณิชย์ (Releasing Social and Commercial Value) ในยุคดิจิทัลข้อมูลเป็นทรัพยากรที่สำคัญสำหรับสร้างนวัตกรรม การเปิดเผยข้อมูลของภาครัฐเป็นแหล่งข้อมูลหนึ่งที่ช่วยผลักดันการสร้างนวัตกรรมและบริการใหม่ๆ เผยแพร่สู่สังคมและเชิงพาณิชย์

(3) การมีส่วนร่วมและข้อตกลง (Participation and Engagement) ประชาชนซึ่งเป็นผู้มีส่วนได้ส่วนเสียได้มีส่วนร่วมแสดงความคิดเห็นต่อการดำเนินงานของภาครัฐ ที่มีผลต่อชีวิตความเป็นอยู่ รวมทั้งนำความคิดเห็นดังกล่าวไปประกอบการพิจารณากำหนดนโยบายและการตัดสินใจของภาครัฐเป็นการสร้างปฏิสัมพันธ์ กับประชาชนมากขึ้น

ทุกคนในประเทศไทยสามารถนำข้อมูลจากระบบข้อมูลเปิดไปใช้งานได้ ไม่ว่าจะเป็นหน่วยงานภาครัฐ หรือภาคเอกชน ตลอดจนการนำข้อมูลเหล่านี้ไปทำการวิจัยค้นคว้าเชิงข้อมูลก็สามารถทำได้ไม่ติดข้อจำกัดใดๆ โดยผู้ใช้งานสามารถดาวน์โหลดไฟล์ชุดข้อมูลในรูปแบบต่างๆ ตามที่ต้องการในแต่ละหัวข้อที่ปรากฏบนเว็บไซต์ได้ด้วยตนเอง ซึ่งการกำหนดรูปแบบของข้อมูลเปิด

ภาครัฐมีผลต่อการนำชุดข้อมูลไปประยุกต์ใช้สร้างสรรค์นวัตกรรม เพื่อตอบสนองการขับเคลื่อนนโยบายดิจิทัลเพื่อเศรษฐกิจและสังคม (สำนักงานพัฒนารัฐบาลดิจิทัล, 2559; องค์การต่อต้านคอร์รัปชัน (ประเทศไทย), 2560)

5.3.3.2 แหล่งรวมสื่อการเรียนรู้แบบเปิด (Open Educational Resources: OER)

การเรียนรู้ที่มีคุณค่า คือการเรียนรู้แบบร่วมมือ การแบ่งปันความรู้ ไม่ยึดถือในความเป็นเจ้าของมากเกินไปขาดโอกาสการเข้าถึงโอกาสการเรียนรู้ของผู้อื่น แนวคิดการสร้างช่องทางทางการเรียนรู้ที่เข้าถึงได้อิสระเสรี จึงเป็นแนวคิดของการส่งเสริมการเรียนรู้ตลอดชีวิต (Lifelong Learning) โดยมีหัวใจสำคัญอยู่ที่การแบ่งปันแหล่งทรัพยากรด้านการศึกษาที่มีคุณภาพสู่สังคมโลกเพื่อนำไปใช้ประโยชน์ทางการศึกษาได้อย่างเสรี แหล่งทรัพยากรด้านการศึกษาแบบเปิด (Open Educational Resources: OER) จึงก่อกำหนดขึ้นมาภายใต้แนวคิดดังกล่าว โดยมีจุดเริ่มต้นมาจากโครงการขององค์การการศึกษา วิทยาศาสตร์ และวัฒนธรรมแห่งสหประชาชาติ หรือยูเนสโก (UNESCO) ที่ร่วมมือกับมหาวิทยาลัยเทคโนโลยีแมสซาชูเซตส์ (Massachusetts Institute of Technology หรือ MIT) สถาบันอุดมศึกษาที่มีชื่อเสียงด้านเทคโนโลยีของประเทศสหรัฐอเมริกา โดยพัฒนา รวบรวมสื่อการเรียนรู้ในรูปแบบอิเล็กทรอนิกส์แบบเปิด (Open Courseware) เผยแพร่ไว้ในเว็บไซต์ ที่มีวัตถุประสงค์ทุกคนสามารถนำไปใช้ได้โดยไม่มีค่าใช้จ่ายและไม่มีข้อจำกัดในการใช้งาน ความสำเร็จของโครงการทำให้แนวคิดในการพัฒนาและแบ่งปันความรู้แก่มวลมนุษยชาติ (บุญเลิศ อรุณพิบูลย์, 2556)

ในประเทศไทยนั้นการพัฒนาค้นคว้าทรัพยากรการศึกษาแบบเปิด (Open Educational Resources (OER), oer.learn.in.th) ภายใต้โครงการระบบสื่อสาระออนไลน์เพื่อการเรียนรู้ทางไกลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารีในโอกาสฉลองพระชนมายุ 5 รอบ 2 เมษายน 2558 เป็นการพัฒนาระบบออนไลน์เพื่อการเรียนรู้ขนาดใหญ่เพื่อให้ได้สื่อสาระเพื่อครูในการนำไปใช้สร้างสื่อการสอน และเป็นระบบการเรียนรู้อิเล็กทรอนิกส์ (e-Learning) เพื่อการเรียนรู้ทางไกลสำหรับนักเรียนทั่วราชอาณาจักร ผ่านเครือข่ายอินเทอร์เน็ต ซึ่งในส่วนของคลังทรัพยากรการศึกษาแบบเปิดนั้นจะเป็นคลังเก็บภาพ คลิปวีดิโอ แผนภาพ ผังมโนทัศน์ แบบทดสอบ เกม การศึกษา สื่อแอนิเมชันเพื่อใช้ในการศึกษา ที่ครูทุกคนสามารถเข้าถึง นำมาปรับปรุง และเอาไปใช้งานโดยไม่ละเมิดกฎหมายลิขสิทธิ์



ภาพที่ 5.2 คลังทรัพยากรการศึกษาแบบเปิด (Open Educational Resources: OER) ที่มา: โครงการระบบสื่อสาระออนไลน์เพื่อการเรียนรู้ทางไกลเฉลิมพระเกียรติฯ, สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ



ภาพที่ 5.3 หน้าเว็บไซต์คลังทรัพยากรการศึกษาแบบเปิด (Open Educational Resources: OER) ที่มา: โครงการระบบสื่อสาระออนไลน์เพื่อการเรียนรู้ทางไกลเฉลิมพระเกียรติฯ, สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

สารสนเทศที่อยู่ในคลังไปใช้ภายใต้สัญญาอนุญาต Creative Commons คือ ใช้ได้โดยไม่ต้องขออนุญาตเจ้าของ แต่ต้องดูสัญญาให้ชัดว่าเจ้าของอนุญาตแบบไหนและไม่อนุญาตแบบไหน เช่น ส่วนมากถ้าไม่อนุญาตก็นำไปหารายได้ แต่ใช้ทำสื่อทเรียนออนไลน์สามารถทำได้เลย นอกจากนี้ได้มีการเชื่อมความร่วมมือกับหน่วยงานอื่น โดยเอาข้อมูลภาพทั้งหมดที่อยู่ในฐานข้อมูลของหน่วยงานอื่นมาซ้ำในระบบของคลัง ทำให้คนจำนวนมากเข้าถึงสิ่งง่ายขึ้นไม่จำกัดในหน่วยงานตนเอง หลายองค์กรเป็นเจ้าของสื่อแต่ไม่สามารถเผยแพร่สื่อผ่านช่องทางออนไลน์ได้ ทำให้คลังเป็นที่เผยแพร่ที่ค่อนข้างใหญ่พอสมควร ไม่มีข้อจำกัดเรื่องขนาด อีกทั้งคลังทรัพยากรการศึกษาแบบเปิดนั้นยังเป็นแหล่งรวบรวมสื่อที่เป็นแนวทางของนิทรรศการ (Galleries) ห้องสมุด (Libraries) เช่น ไฟล์ pdf ของหนังสือต่างๆ รวมถึงเป็นแหล่งรวบรวมสื่อจดหมายเหตุ (Archives) และพิพิธภัณฑ์ (Museums) จากหน่วยงานต่างๆ หรือที่เรียกว่า “GLAM” เพื่อนำไปสู่การเรียนการสอนตลอดชีวิตอีกด้วย (บุญเลิศ อรุณพิบูลย์, 2562) โดยทางโครงการฯ ได้ต่อยอดการดำเนินงานคลังทรัพยากรการศึกษาแบบเปิดสู่แนวคิด GLAM (Galleries, Libraries and Learning Centers, Archives and Museums) คือ การพัฒนาระบบที่อำนวยความสะดวกแก่ผู้ใช้บริการในการค้นหา และเข้าถึงสื่อการเรียนรู้ดิจิทัลที่ต้องการแบบ One Search

จากฐานข้อมูลและระบบบริหารจัดการที่แตกต่างและหลากหลาย เป็นการร่วมมือข้ามกลุ่มความรู้และสถาบัน (Cross-Disciplinary and Organizational Collaboration) เพื่อสร้างสรรค์และแบ่งปันสื่อความรู้ดิจิทัลภายในหอศิลป์และสตูดิโอ (Galleries) ห้องสมุดและศูนย์การเรียนรู้ (Libraries and Learning Centers) จดหมายเหตุ (Archives) และพิพิธภัณฑ์ (Museums) นี้จะเป็นการก้าวสู่การเรียนการสอนรูปแบบใหม่ ที่เน้นความร่วมมือ อันจะช่วยสร้างการเรียนรู้ที่มีคุณค่า เกิดการแบ่งปันความรู้ ไม่ยึดถือในความเป็นเจ้าของมากเกินไปขาดโอกาสการเข้าถึงโอกาสการเรียนรู้ของผู้อื่น สนับสนุนแนวคิดการสร้างช่องทางการเรียนรู้ที่เข้าถึงได้อิสระเสรี แนวคิดของการส่งเสริมการเรียนรู้ตลอดชีวิต (Lifelong Learning) โดยมีหัวใจสำคัญอยู่ที่การแบ่งปันแหล่งทรัพยากรด้านการศึกษาที่มีคุณภาพสู่สังคมโลก เพื่อนำไปใช้ประโยชน์ทางด้านการศึกษาได้อย่างเสรีต่อไป เพื่อส่งเสริมให้ผู้ใช้ทรัพยากรสารสนเทศได้รับความรู้และความเข้าใจ เกิดแลกเปลี่ยนแนวคิด และประสบการณ์เกี่ยวกับการพัฒนาและการใช้งานคลังทรัพยากรการศึกษาแบบเปิด และได้รับความรู้ความเข้าใจเกี่ยวกับคุณธรรม และจริยธรรมทางด้านวิชาการ การจัดการทรัพย์สินทางปัญญา การใช้งานลิขสิทธิ์ที่เป็นธรรมในการเรียนการสอน และสัญญาอนุญาตที่เกี่ยวข้องในการเรียนการสอนแบบเปิดอย่างถูกต้อง ทำให้เกิดการสร้าง และการขยายเครือข่ายหรือกลุ่มผู้ปฏิบัติ (Community of Practice) สร้างสรรค์และเผยแพร่องค์ความรู้ ผ่านคลังทรัพยากรการศึกษาแบบเปิด และความร่วมมือข้ามกลุ่มความรู้ และสถาบัน เพื่อสนับสนุนการเรียนรู้ตลอดชีวิตและการศึกษาแบบเปิด ผ่านเทคโนโลยีที่เหมาะสม

นอกจากแหล่งทรัพยากรสารสนเทศในยุคดิจิทัลที่เปลี่ยนแปลงไปสู่การเปิดกว้าง เพื่อลดข้อจำกัดในการสร้างสรรค์ การเข้าถึง การใช้และการแบ่งปันสารสนเทศแล้วนั้น ทักษะความรู้ของคนก็จะต้องมีความพร้อมควบคู่กันไปด้วย ซึ่งความคิดสร้างสรรค์ทางดิจิทัล (Digital Creativity) ที่ เป็นความสามารถในการใช้เทคโนโลยีและเครื่องมือดิจิทัลต่างๆ ให้เป็นประโยชน์ เช่น เขียนโค้ด และโปรแกรมเป็นสร้างคอนเทนต์และศิลปะในรูปแบบดิจิทัลได้ เป็นต้น ซึ่งเป็นประเด็นหนึ่งในความฉลาดทางดิจิทัลที่จำเป็นต่อการใช้ชีวิตในยุคดิจิทัล โดยนำความคิดสร้างสรรค์ไปประยุกต์ใช้ให้เกิดการพัฒนาคนและองค์กรด้านต่างๆ ยกตัวอย่างเช่น การคิดสร้างสรรค์โฆษณาในสื่อดิจิทัลที่จะต้องปรับตัวให้เข้ากับยุคสื่อที่เปลี่ยนแปลง วิธีการคิดสร้างสรรค์โฆษณาในสื่อดิจิทัลมีที่มาของความคิดสร้างสรรค์ เกิดจากโจทย์ทางการสื่อสารและประสบการณ์ โดยให้ความสำคัญไปที่กลุ่มเป้าหมายและผลิตภัณฑ์ ซึ่งองค์ประกอบของความคิดสร้างสรรค์เกิดจากความสามารถทางสติปัญญาและ ความสามารถทางด้านจิตใจและความรู้สึก

โดยแบ่งประเภทของความคิดสร้างสรรค์จากแนวคิด และตำแหน่งของผลิตภัณฑ์ ได้ดังนี้

1) ด้านการตลาดก็มีการพัฒนานักสร้างสรรค์แผนการตลาดในยุคดิจิทัลที่จะเป็นการเตรียมความพร้อมเข้าสู่ตลาดการแข่งขันที่ต้องใช้องค์ความรู้ ทั้งจากในและนอกห้องเรียน การเข้าร่วมกิจกรรมในครั้งนี้จึงเป็นการเปิดโอกาสให้คนรุ่นใหม่ รวมถึงครูอาจารย์ บุคลากรด้านการศึกษา สถานศึกษา และผู้ที่มีประสบการณ์ ความรู้ ความเชี่ยวชาญจากหลากหลายกลุ่มธุรกิจ ได้พัฒนาทักษะการใช้สื่อเทคโนโลยีดิจิทัลอย่างสร้างสรรค์

2) ความคิดสร้างสรรค์การผลิต และบริการงานพิมพ์ดิจิทัล ซึ่งปัจจุบันธุรกิจสิ่งพิมพ์ต้องปรับตัวเป็นอย่างมาก เพื่อเพิ่มมูลค่าในตัวผลิตภัณฑ์ และบริการ ช่วยสร้างความคิดผลิตสิ่งพิมพ์ที่เป็นเอกลักษณ์ แปลกใหม่ มีความแตกต่าง สามารถแข่งขันได้

อย่างไรก็ตามความสำคัญของจริยธรรมและกฎหมายดิจิทัล ไม่ได้อยู่ที่การกำหนดหลักการทางจริยธรรม คุณธรรมเพื่อการอยู่ร่วมกันในสังคม หรือการจัดการแหล่งทรัพยากรสารสนเทศด้วยสื่อและเทคโนโลยีดิจิทัล หรือการประยุกต์ใช้ความคิดสร้างสรรค์เพื่อจัดการสารสนเทศหรืองานต่างๆ ให้มีความสามารถดำเนินการต่อไปได้ในการเปลี่ยนผ่านสู่ความเป็นยุคดิจิทัล แต่สำคัญที่สุดคือคน หาก เทคโนโลยี โครงสร้างพื้นฐาน ทรัพยากรสารสนเทศและองค์กรต่างๆ มีความพร้อมแต่คนไม่พร้อม ไม่มีการปรับตัวหรือพัฒนา และมีความรู้เท่าทันต่อการเปลี่ยนแปลงต่างๆ นั้น การพัฒนาในภาพรวมก็อาจจะไม่สามารถดำเนินไปสู่ความเป็นดิจิทัลได้อย่างมีประสิทธิภาพสูงสุด

สรุป

เมื่อก้าวเข้าสู่ยุคดิจิทัลที่ผู้คนหันมาใช้เทคโนโลยีกันเพิ่มมากขึ้นจึงต้องมีจริยธรรมและกฎหมายที่เกี่ยวข้องกับดิจิทัลเกิดขึ้นกลายเป็นจริยธรรมดิจิทัล (Digital Ethics) ที่ควบคุมประพฤติปฏิบัติและหลักการทางจริยธรรมเชิงปฏิสัมพันธ์แบบดิจิทัล โดยจะต้องคำนึงถึงความเป็นส่วนตัว ความถูกต้อง ความเป็นเจ้าของ และการเข้าถึงเทคโนโลยีดิจิทัล ซึ่งในจริยธรรมในการจัดการสารสนเทศและดิจิทัลประกอบไปด้วยประเด็นหลัก 4 ประเด็น ได้แก่ ความเป็นส่วนตัว ความถูกต้อง ความเป็นเจ้าของ และการเข้าถึงข้อมูล

นอกจากนี้ยังมีการออกกฎหมายที่เกี่ยวข้องกับดิจิทัล ได้แก่ กฎหมายลิขสิทธิ์ พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวทางการใช้บริการคลาวด์ เป็นต้น ซึ่งเป็นกฎหมายที่ใช้ในการควบคุม ตรวจสอบ และกำกับดูแลการใช้เทคโนโลยีดิจิทัลของคนไทย เพื่อป้องกันการกระทำผิดกฎหมายและการละเมิดลิขสิทธิ์ จึงเกิดเป็นแนวคิดการใช้ข้อมูลเปิด (Open Data) ที่ผู้คนสามารถแลกเปลี่ยนและนำข้อมูลไปใช้ได้อย่างเสรี ไม่มีข้อจำกัด สามารถนำกลับมาใช้ใหม่ (Reuse) และแจกจ่ายต่อได้ ภายใต้สัญญาอนุญาตที่กำหนด และคลังทรัพยากรสารสนเทศแบบเปิด (Open Educational Resources: OER) ที่เป็นแหล่งการเรียนรู้แบบร่วมมือ การแบ่งปันความรู้ และสร้างช่องทางการเรียนรู้ที่เข้าถึงได้อิสระเสรี

คำถามทบทวน

1. จงอธิบายความหมายและความสำคัญของจริยธรรมดิจิทัล (Digital Ethics)
2. ปัญหาการกระทำผิดหลักจริยธรรมดิจิทัลมีทั้งหมดกี่ด้านพร้อมอธิบาย
3. จงอธิบายความหมายของภัยคุกคามทางไซเบอร์และความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)
4. จงยกตัวอย่างภัยคุกคามที่เกิดจากการใช้เทคโนโลยีในปัจจุบัน
5. จงอธิบายนโยบายและกฎเกณฑ์เพื่อรักษาความปลอดภัยในการใช้งานสื่อสังคมออนไลน์ เฟซบุ๊ก
6. นักศึกษามีแนวทางในการรักษาความปลอดภัยในการใช้เทคโนโลยีดิจิทัลอย่างไรในชีวิตประจำวัน
7. ถ้านักศึกษามั่นใจว่าวิดีโอภาพยนตร์ที่กำลังฉายลงไอจีสตอรี่ของนักศึกษาเองตลอดการชมภาพยนตร์ นักศึกษาคิดว่าการกระทำดังกล่าวผิดจริยธรรมหรือผิดกฎหมายหรือไม่อย่างไร
8. จงอธิบายความหมายของข้อมูลเปิด (Open Data) หลักสำคัญของข้อมูลแบบเปิดและประโยชน์ที่ได้รับจากการจากการใช้ข้อมูลเปิด
9. จงอธิบายความสำคัญของแหล่งรวมสื่อการเรียนรู้แบบเปิด (Open Educational Resources: OER) และประโยชน์ที่ได้รับจากการใช้แหล่งรวมสื่อการเรียนรู้แบบเปิด
10. นักศึกษาสามารถนำความรู้ในด้านจริยธรรมดิจิทัลและกฎหมายลิขสิทธิ์ไปประยุกต์ใช้ในการเรียนและการทำงานในสาขาของตนเองได้อย่างไรบ้าง