การจัดการร่องรอยดิจิทัลของพลเมืองดิจิทัลในยุคศตวรรษที่ 21

Digital Footprint Management for 21st Century Digital Citizens

นนทนันท์ แย้มวงษ์[1], อรรถพร ธนูเพ็ชร์[2*] และ ณกัญญา ชุ่มสมบัติ[3]

Nonthanun Yamwong[1], Athaporn Thanupetch[2*] and Nakanya Chumsombat[3]

สาขาวิชาบรรณารักษศาสตร์และสารสนเทศศาสตร์ คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏพระนคร[1, 2]

นักวิชาการอิสระ[3]

Faculty of Humanities and Social Sciences, Phranakhon Rajabhat University[1, 2]

Independent Scholar[3]

e-mail: nonthanun.y@pnru.ac.th[1] Athaporn.t@pnru.ac.th[2] and nakanyakai@gmail.com[3]

Received: February 15, 2025; Revised: November 28, 2025; Accepted: January 23, 2026

บทคัดย่อ

การดำรงอยู่ของร่องรอยดิจิทัล (Digital Footprints) กลายเป็นสิ่งที่หลีกเลี่ยงไม่ได้ในยุคดิจิทัล ไม่ว่าจะเป็นข้อมูลที่ผู้ใช้งานเปิดเผยทั้งโดยตั้งใจหรือไม่ตั้งใจ ร่องรอยดิจิทัลเหล่านี้สามารถส่งผลต่อชื่อเสียง โอกาสทางการศึกษา การทำงาน และแม้แต่ความปลอดภัยในชีวิตประจำวัน โดยเฉพาะในกลุ่มเยาวชนซึ่งเป็นผู้ใช้งานอินเทอร์เน็ตส่วนใหญ่ บุคคลกลุ่มนี้ยังขาดความตระหนักรู้และทักษะในการจัดการข้อมูลส่วนบุคคลของตนเองอย่างเหมาะสม เพื่อหลีกเลี่ยงการถูกนำข้อมูลไปใช้ในทางก่อให้เกิดผลกระทบด้านลบ บทความนี้มีวัตถุประสงค์เพื่อศึกษาแนวทางในการจัดการร่องรอยดิจิทัลของพลเมืองดิจิทัลในศตวรรษที่ 21 โดยเนื้อหาครอบคลุมถึงความหมายและประเภทของร่องรอยดิจิทัล ผลกระทบในเชิงมิติด้านต่าง ๆ รวมทั้งกฎหมายที่เกี่ยวข้อง แนวทางการส่งเสริมการรู้เท่าทันร่องรอยดิจิทัลในสถานศึกษา บทบาทของเทคโนโลยีในการจัดการข้อมูลดิจิทัล รวมถึงการสร้างจริยธรรมและวินัยดิจิทัลในกลุ่มเยาวชน ทั้งนี้ยังได้วิเคราะห์อุปสรรคที่พบในปัจจุบัน และนำเสนอข้อเสนอแนะเชิงนโยบายเพื่อพัฒนาพลเมืองดิจิทัลที่มีความรับผิดชอบ ผลการศึกษาเสนอว่า การจัดการร่องรอยดิจิทัลอย่างมีประสิทธิภาพ จำเป็นต้องอาศัยการมีส่วนร่วมจากหลายภาคส่วน ทั้งภาครัฐ สถานศึกษา ครอบครัว และผู้ใช้งานเอง โดยเน้นในการสร้างความรู้เท่าทัน การใช้เทคโนโลยีอย่างมีจิตสำนึกในความรับผิดชอบตามกรอบของกฎหมาย จริยธรรม และการใช้เทคโนโลยีอย่างชาญฉลาด เพื่อเสริมสร้างความปลอดภัยและความยั่งยืนในระบบนิเวศดิจิทัล

คำสำคัญ: ร่องรอยดิจิทัล พลเมืองดิจิทัล ความปลอดภัยไซเบอร์ จริยธรรมดิจิทัล ความเป็นส่วนตัวออนไลน์

Abstract

A digital footprint forms both intentionally and unintentionally and affects opportunities in education, employment, and everyday safety. Especially youth who lack awareness and the skills to manage their personal data appropriately. This article, therefore, explores strategies for managing digital footprints among 21st-century digital citizens. It begins by defining digital footprints and outlining their various types. The discussion then addresses the multidimensional impacts these footprints can have. Relevant legal frameworks governing personal data protection are also examined. The article highlights the role of education in developing digital- footprint literacy. It further explains how technology can support responsible data management. Emphasis is placed on nurturing digital ethics

and discipline among young users. Current challenges in digital-footprint management are analyzed in detail. In light of these challenges, policy recommendations are proposed. The study argues that effective management requires collaboration among multiple sectors. Governments, educational institutions, families, and individuals all share responsibility. Ultimately, raising awareness and using technology wisely are key to ensuring a safer digital ecosystem.

Keywords: Digital Footprint, Digital Citizen, Cybersecurity, Digital Ethics, Online Privacy

ความนำ

ในโลกยุคดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทอย่างมากในชีวิตประจำวัน การเชื่อมต่อระหว่างผู้คนผ่านเครือข่ายอินเทอร์เน็ตเกิดขึ้นอย่างรวดเร็ว ส่งผลให้กิจกรรมหลากหลายไม่ว่าจะเป็นการเรียน การทำงาน การสื่อสาร หรือความบันเทิง ต่างพึ่งพาแพลตฟอร์มดิจิทัลอย่างหลีกเลี่ยงไม่ได้ อย่างไรก็ตาม การใช้งานเทคโนโลยีเหล่านี้ มีการทิ้งร่องรอยดิจิทัลหรือข้อมูลบางอย่างที่สะท้อนตัวตน พฤติกรรม และความคิดเห็นของผู้ใช้งานไว้อย่างไม่รู้ตัว ซึ่งหากขาดความตระหนักรู้และการจัดการอย่างเหมาะสม อาจส่งผลกระทบต่อความเป็นส่วนตัว ความปลอดภัย และภาพลักษณ์ของบุคคลในระยะยาวได้ ดังนั้นร่องรอยดิจิทัล (Digital Footprint) จึงเป็นประเด็นที่มีความสำคัญอย่างยิ่ง โดยเฉพาะในบริบทของพลเมืองดิจิทัล (Digital Citizen) ซึ่งหมายถึงบุคคลที่ดำรงชีวิตอยู่ในโลกยุคใหม่ที่เทคโนโลยีสารสนเทศมีบทบาทสูง และมีหน้าที่ต้องใช้งานเทคโนโลยีสารสนเทศอย่างมีจริยธรรม มีความรับผิดชอบต่อตนเองและผู้อื่น พลเมืองดิจิทัลที่ดีจำเป็นต้องมีความรู้และทักษะในการจัดการข้อมูลส่วนตัว พฤติกรรมออนไลน์ และการสื่อสารผ่านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นทั้งต่อตนเองและสังคม (สถาบันสื่อเด็กและเยาวชน, 2562)

จากความเปลี่ยนแปลงของโลกในศตวรรษที่ 21 ที่เต็มไปด้วยโอกาสและความท้าทายใหม่ ๆ การรู้เท่าทันและจัดการร่องรอยดิจิทัลจึงเป็นทักษะจำเป็นที่ทุกคน โดยเฉพาะเยาวชน นักเรียน นักศึกษา และประชาชนทั่วไป ควรได้รับการส่งเสริมและฝึกฝนอย่างต่อเนื่อง โดยการศึกษาและเรียนรู้ข้อมูลข่าวสารและเทคโนโลยีสารสนเทศใหม่ ๆ ตลอดเวลา เพื่อให้สามารถ รู้วิธีปกป้องข้อมูลส่วนตัวและควบคุมร่องรอยดิจิทัลของตน สามารถคิดวิเคราะห์แยกแยะข่าวสารที่ถูกต้องและไม่ตกเป็นเหยื่อของข้อมูลเท็จ มีความเข้าใจการทำงานของเทคโนโลยีสารสนเทศและผลกระทบของการใช้งานออนไลน์

วัตถุประสงค์

ศึกษาแนวทางในการจัดการร่องรอยดิจิทัล ของพลเมืองดิจิทัลในศตวรรษที่ 21 โดยเนื้อหาครอบคลุมถึงความหมายและประเภทของร่องรอยดิจิทัล ผลกระทบในมิติต่าง ๆ กฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล แนวทางการส่งเสริมการรู้เท่าทันร่องรอยดิจิทัลในสถานศึกษา บทบาทของเทคโนโลยีในการจัดการข้อมูลดิจิทัล รวมถึงการสร้างจริยธรรมและวินัยดิจิทัลในกลุ่มเยาวชน

1. ความหมายของพลเมืองดิจิทัลและร่องรอยดิจิทัล

การเปลี่ยนผ่านของสังคมเข้าสู่ยุคดิจิทัลในศตวรรษที่ 21 ทำให้วิถีชีวิตของผู้คนต้องเข้าไปเกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างหลีกเลี่ยงไม่ได้ ไม่ว่าจะเป็นการติดต่อสื่อสาร การศึกษา การทำธุรกรรมทางการเงิน หรือแม้แต่กิจกรรมบันเทิง ล้วนต้องพึ่งพาอินเทอร์เน็ตและแพลตฟอร์มออนไลน์ในรูปแบบต่าง ๆ ด้วยเหตุนี้บทบาทของพลเมืองจึงขยายออกไปจากการเป็นสมาชิกของสังคมในโลกแห่งความจริง สู่การเป็นสมาชิกของสังคม

ในโลกดิจิทัล ซึ่งจำเป็นต้องมีความรู้ ความเข้าใจ และจริยธรรมในการใช้งานเทคโนโลยี จึงเกิดแนวคิดที่เรียกว่า พลเมืองดิจิทัล (Digital Citizen) ขึ้น โดยคุณลักษณะของพลเมืองดิจิทัลที่ดีประกอบด้วยหลายด้าน ได้แก่ ความรู้เท่าทันดิจิทัล (Digital Literacy) คือ มีความเข้าใจวิธีใช้งานเทคโนโลยีและสื่อสารออนไลน์ได้อย่างถูกต้อง การมีจริยธรรมดิจิทัล (Digital Ethics) คือใช้เทคโนโลยีอย่างมีคุณธรรม ไม่รังแกผู้อื่น ไม่สร้างข่าวปลอม มีความรับผิดชอบส่วนบุคคล (Responsibility) คือ มีวินัยในการใช้งาน รู้จักปกป้องข้อมูลส่วนตัวของตนเอง และผู้อื่น ตลอดจนการมีส่วนร่วมในสังคม (Civic Engagement) คือใช้เทคโนโลยีเพื่อส่งเสริมสิ่งที่ดีงาม และร่วมแก้ไขปัญหาทางสังคม (สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ, 2562)

สิ่งหนึ่งที่เกี่ยวข้องกับการเป็นพลเมืองดิจิทัล คือ ร่องรอยดิจิทัล (Digital Footprint) ซึ่งหมายถึง หลักฐานหรือข้อมูลที่บุคคลทิ้งไว้บนโลกออนไลน์จากการใช้งานอินเทอร์เน็ต ร่องรอยเหล่านี้อาจเป็นสิ่งที่เกิดแบบตั้งใจหรือไม่ตั้งใจก็ได้ แต่ล้วนสามารถถูกติดตาม วิเคราะห์ และนำมาใช้ได้ทั้งในทางบวกและทางลบ (ปริญญา หอมเอนก, 2565)

การเข้าสู่ยุคดิจิทัลทำให้ผู้คนต้องพึ่งพาเทคโนโลยีในชีวิตประจำวัน ทั้งการสื่อสาร การศึกษา และธุรกรรมออนไลน์ จึงเกิดแนวคิด “พลเมืองดิจิทัล” ที่เน้นความรู้เท่าทัน จริยธรรม ความรับผิดชอบ และการมีส่วนร่วมในสังคมออนไลน์อย่างสร้างสรรค์ อีกทั้งยังต้องตระหนักถึง ร่องรอยดิจิทัล ซึ่งเป็นข้อมูลที่ผู้ใช้ทิ้งไว้บนโลกออนไลน์ อาจถูกนำไปใช้ได้ทั้งในทางบวกและทางลบ

2. ประเภทของร่องรอยดิจิทัล

ร่องรอยดิจิทัลแบ่งออกเป็นสองประเภท คือร่องรอยดิจิทัลแบบตั้งใจ และแบบไม่ตั้งใจ ซึ่งทั้งสองประเภทนี้มีผลต่อการสร้างตัวตนดิจิทัลและความเป็นส่วนตัวของผู้ใช้งาน (ฉัตรพงศ์ ชูแสงนิล, 2562) โดยมีรายละเอียดดังนี้

2.1 ร่องรอยดิจิทัลแบบตั้งใจ (Active Digital Footprint) เป็นข้อมูลที่ผู้ใช้เผยแพร่ด้วยตนเอง เช่น การโพสต์ข้อความบนเฟซบุ๊ก การแชร์ภาพบนอินสตาแกรม หรือการแสดงความคิดเห็นบนยูทูบ ซึ่งเป็นข้อมูลที่ผู้ใช้สามารถควบคุมได้บางส่วน

2.2 ร่องรอยดิจิทัลแบบไม่ตั้งใจ (Passive Digital Footprint) เป็นข้อมูลที่ถูกบันทึกไว้โดยอัตโนมัติจากพฤติกรรมของผู้ใช้งาน เช่น การเข้าเว็บไซต์ การคลิกลิงก์ การใช้ GPS หรือการเก็บข้อมูลผ่านคุกกี้ ซึ่งผู้ใช้ส่วนใหญ่มักไม่รู้ว่าข้อมูลเหล่านี้ได้ถูกจัดเก็บไว้แล้ว

ผู้ใช้ดิจิทัลต้องเข้าใจว่าทุก ๆ ครั้งที่คลิกคือร่องรอยและเป็นสิ่งสำคัญที่ต้องตระหนักรู้ของพลเมืองดิจิทัลในยุคปัจจุบัน เพราะข้อมูลบนอินเทอร์เน็ตไม่ใช่เรื่องส่วนตัวเพียงอย่างเดียว แต่ยังส่งผลต่อชื่อเสียง ความปลอดภัย หรือแม้แต่โอกาสทางการศึกษาและอาชีพ ดังนั้นความตระหนักรู้และการจัดการร่องรอยดิจิทัลอย่างเหมาะสม จึงเป็นหน้าที่พื้นฐานของพลเมืองดิจิทัลที่มีคุณภาพ

3. ความสำคัญของการจัดการร่องรอยดิจิทัล

ร่องรอยดิจิทัลได้กลายเป็นหนึ่งในปัจจัยสำคัญที่มีอิทธิพลต่อชีวิตของผู้คน ทั้งในด้านการเรียน การทำงาน หรือการใช้ชีวิตส่วนตัว เนื่องจากพฤติกรรมออนไลน์สามารถถูกติดตาม วิเคราะห์ และนำไปใช้ในวัตถุประสงค์ต่าง ๆ ได้ การจัดการร่องรอยดิจิทัลจึงไม่ใช่เพียงเรื่องของการจัดการความเป็นส่วนตัวเท่านั้น แต่ยังเป็นเรื่องของความปลอดภัย ภาพลักษณ์ โอกาส และจริยธรรมของผู้ใช้ (Tufekci, 2017) โดยความสำคัญสามารถแบ่งออกในแต่ละด้านได้ดังนี้

3.1 ด้านความปลอดภัยของข้อมูลส่วนบุคคล เนื่องจากร่องรอยดิจิทัลสามารถเปิดเผยข้อมูลที่อ่อนไหว เช่น หมายเลขโทรศัพท์ ที่อยู่อีเมล หรือแม้แต่พฤติกรรมส่วนบุคคล ซึ่งหากตกไปอยู่ในมือของผู้ไม่ประสงค์ดี อาจนำไปสู่การขโมยข้อมูลตัวตน (Identity Theft) การหลอกลวง การแฮ็กบัญชี หรือแม้กระทั่ง

การถูกข่มขู่ทางไซเบอร์ (Cyberbullying/Cyberstalking) ได้ ดังนั้นการจัดการร่องรอยดิจิทัลจึงเป็นกลไกสำคัญในการป้องกันตนเองจากภัยคุกคามออนไลน์

3.2 ด้านภาพลักษณ์และชื่อเสียงในโลกออนไลน์ เพราะทุกสิ่งที่โพสต์บนโลกออนไลน์มักจะ คงอยู่ถาวร ไม่ว่าจะตั้งใจหรือไม่ ตั้งแต่โพสต์เก่าใน Facebook ทวีตใน X (Twitter เดิม) หรือแม้กระทั่งคอมเมนต์ในวิดีโอ สามารถถูกนำกลับมาเปิดเผยในภายหลังได้ แม้จะลบออกแล้วก็ตาม สิ่งเหล่านี้สามารถสะท้อนทัศนคติ ความคิด และพฤติกรรมของบุคคล ซึ่งอาจส่งผลโดยตรงต่อภาพลักษณ์ ไม่ว่าจะในด้านบวกหรือด้านลบ โดยเฉพาะในกรณีของผู้ที่ ต้องการสมัครงาน สมัครเรียน หรือเข้าสู่ตำแหน่งที่ มีบทบาทต่อสาธารณะ ข้อมูลจาก CareerBuilder ประจำปี 2018 (เผยแพร่เมื่อวันที่ 9 สิงหาคม 2561) กล่าวว่า ในหลายประเทศ บริษัทมีการคัดเลือกผู้สมัครงานผ่านสื่อสังคมออนไลน์ หากพบว่าบุคคลนั้นเคยโพสต์ข้อความเหยียดเพศ เหยียดเชื้อชาติ หรือใช้ถ้อยคำรุนแรง อาจส่งผลให้ถูกปฏิเสธโดยไม่แจ้งเหตุผล นอกจากนี้ สื่อยังสามารถค้นหาร่องรอยดิจิทัลเพื่อโจมตีบุคคลสาธารณะหรือผู้มีชื่อเสียง ทำให้เกิดความเสียหายต่อชื่อเสียงและหน้าที่การงานอย่างรุนแรง ส่งผลกระทบต่อโอกาสทางการศึกษาและการประกอบอาชีพ

ปัจจุบันสถานศึกษาและองค์กรเริ่มหันมาใช้ร่องรอยดิจิทัลเป็นหนึ่งในเกณฑ์พิจารณาผู้สมัคร ไม่เพียงแต่มองคุณสมบัติทางวิชาการหรือความสามารถเท่านั้น แต่ยังพิจารณาทัศนคติ จริยธรรม และพฤติกรรมจากพฤติกรรมออนไลน์ด้วย ผู้ที่ทิ้งร่องรอยที่สะท้อนพฤติกรรมไม่เหมาะสม เช่น การละเมิดลิขสิทธิ์ การโพสต์เนื้อหาลามกอนาจาร หรือการแสดงความคิดเห็นในลักษณะก้าวร้าว อาจถูกตัดสินและเสียโอกาสในเส้นทางวิชาชีพ แม้จะมีความสามารถสูงก็ตาม

3.3 ด้านจริยธรรมและการอยู่ร่วมกันในสังคมดิจิทัล เพราะการจัดการร่องรอยดิจิทัลไม่ได้หมายถึงการซ่อนตัวหรือหลีกเลี่ยงจากโลกออนไลน์ แต่คือการมีจริยธรรมในการสร้างตัวตนบนโลกดิจิทัลอย่างเหมาะสม รู้จักการเคารพสิทธิของผู้อื่น รับผิดชอบต่อสิ่งที่ตนเองเผยแพร่ซึ่งเป็นรากฐานของการเป็นพลเมืองดิจิทัลที่ดี

ร่องรอยดิจิทัลมีอิทธิพลอย่างมากต่อชีวิตในยุคดิจิทัล ทั้งด้านการเรียน การทำงาน และภาพลักษณ์ส่วนบุคคล เพราะข้อมูลและพฤติกรรมออนไลน์ สามารถถูกติดตามและนำไปใช้ได้ในหลายวัตถุประสงค์ (Tufekci, 2017) การจัดการร่องรอยดิจิทัลจึงมีความสำคัญต่อความปลอดภัยของข้อมูลส่วนบุคคล ป้องกันการขโมยข้อมูลและภัยคุกคามไซเบอร์ อีกทั้งยังช่วยรักษาภาพลักษณ์และชื่อเสียงในโลกออนไลน์ ซึ่งอาจมีผลต่อโอกาสทางการศึกษาและอาชีพ นอกจากนี้ ยังสะท้อนถึงจริยธรรมในการอยู่ร่วมกันในสังคมดิจิทัล ที่ผู้ใช้ควรเคารพสิทธิผู้อื่นและรับผิดชอบต่อสิ่งที่ตนเผยแพร่บนโลกออนไลน์

4. ผลกระทบจากร่องรอยดิจิทัล

การทิ้งร่องรอยดิจิทัลไว้โดยขาดความตระหนักรู้ อาจส่งผลเสียต่อบุคคลในหลากหลายมิติ ทั้งมิติด้านการงาน การศึกษา และชีวิตส่วนตัว หลายกรณีที่เกิดขึ้นจริงในสังคมได้แสดงให้เห็นอย่างชัดเจนว่า สิ่งที่ทำบนโลกออนไลน์อาจย้อนกลับมาส่งผลกับโลกความเป็นจริง ไม่ว่าผู้ใช้งานจะตั้งใจหรือไม่ก็ตาม ตัวอย่างเช่น

4.1 ถูกปฏิเสธงานจากโพสต์ในอดีตซึ่งในหลายประเทศโดยเฉพาะสหรัฐอเมริกา แคนาดา และอังกฤษ บริษัทหรือองค์กรต่าง ๆ นิยมตรวจสอบประวัติผู้สมัครงานผ่านสื่อสังคมออนไลน์ เช่น Facebook, X (Twitter), LinkedIn หรือ Instagram เพื่อพิจารณาทัศนคติและพฤติกรรมของผู้สมัคร หลายกรณีพบว่าผู้สมัครงานบางคนพลาดโอกาสในการได้งานเพียงเพราะโพสต์เก่า ๆ ที่แสดงความเห็นในเชิงเหยียดสีผิว เหยียดเพศ หรือใช้ถ้อยคำหยาบคาย แม้โพสต์นั้นจะมีอายุหลายปีแล้วก็ตาม

ตัวอย่างกรณีที่เคยเป็นข่าวคือ ผู้สมัครงานตำแหน่งครูในสหรัฐอเมริกา ถูกปฏิเสธการว่าจ้างหลังจากโรงเรียนพบว่า เขาเคยโพสต์ภาพดื่มแอลกอฮอล์อย่างไม่เหมาะสมบนโซเชียลมีเดียเมื่อสมัยยังเป็น

นักศึกษา แม้ว่าเขาจะมีคุณสมบัติด้านวิชาการและประสบการณ์ครบถ้วนตามที่ต้องการก็ตาม (“ Many companies reject,”2014)

4.2 เด็กนักเรียนถูกกลั่นแกล้งและแบล็กเมลจากร่องรอยดิจิทัล โดยเกิดจากการไม่รู้ไม่เข้าใจผลกระทบของร่องรอยดิจิทัลของกลุ่มวัยรุ่น อาจนำไปสู่เหตุการณ์กลั่นแกล้งออนไลน์ (Cyberbullying) หรือการแบล็กเมลในโลกไซเบอร์ เช่น การส่งภาพส่วนตัวให้กับเพื่อนหรือแฟน แล้วเกิดการหลุดออกไปในวงกว้าง กลายเป็นประเด็นในสังคม ส่งผลให้ผู้ถูกกระทำมีความเครียด ซึมเศร้า หรือถึงขั้นต้องลาออกจากสถานศึกษา กรณีในประเทศไทยเคยมีนักเรียนหญิงชั้นมัธยมศึกษาคนหนึ่งส่งภาพไม่เหมาะสมให้เพื่อนสนิท ต่อมาภาพดังกล่าวถูกแชร์ในกลุ่มไลน์ของโรงเรียนอย่างรวดเร็ว จนทำให้ไม่สามารถใช้ชีวิตในโรงเรียนได้ตามปกติ

4.3 ร่องรอยดิจิทัลที่ถูกใช้ในการโจมตีทางการเมืองหรือสังคม ในกรณีของบุคคลสาธารณะ เช่น นักการเมือง ดารา หรือยูทูบเบอร์ ร่องรอยดิจิทัลกลายเป็นอาวุธที่สามารถใช้โจมตีหรือทำลายความน่าเชื่อถือได้ หากพบว่า เคยแสดงความคิดเห็นหรือมีพฤติกรรมที่ขัดต่อจริยธรรม สังคมอาจนำโพสต์เก่า ๆ ขึ้นมาเพื่อประณามและต่อต้าน จนกระทั่งเกิดกระแสแบน (Cancel Culture)

ร่องรอยดิจิทัลจึงไม่ใช่เพียงข้อมูลเบื้องหลังที่ไม่มีความหมาย แต่เป็นหลักฐาน ที่สามารถใช้ตัดสินพฤติกรรมของบุคคลได้อย่างมีนัยสำคัญ และสามารถย้อนกลับมาสร้างผลกระทบได้ ในเวลาที่ไม่คาดคิด การมีความรู้เท่าทันและจัดการร่องรอยดิจิทัลอย่างรอบคอบจึงเป็นเรื่องจำเป็นที่ทุกคนควรตระหนัก

5. ทักษะดิจิทัลของพลเมืองในศตวรรษที่ 21

ในโลกยุคดิจิทัล การใช้เทคโนโลยีอย่างรู้เท่าทัน มีจริยธรรมและมีความรับผิดชอบเป็นหัวใจสำคัญ ผู้ใช้จำเป็นต้องมีทักษะดิจิทัลที่สอดคล้องกับการเปลี่ยนแปลงของสังคมโลกในศตวรรษที่ 21 โดยเฉพาะเมื่อพูดถึงการจัดการร่องรอยดิจิทัลอย่างเหมาะสม ซึ่งมีแนวทางดังนี้ (สำนักงานบริหารและพัฒนาองค์ความรู้, 2564)

5.1 ความรู้เท่าทันดิจิทัล (Digital Literacy) ซึ่งเป็นความสามารถในการเข้าถึง เข้าใจ และรู้วิธีการใช้เทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ ผู้มีความรู้เท่าทันดิจิทัล จะสามารถรู้จักเลือกใช้เครื่องมือออนไลน์อย่างเหมาะสม เข้าใจวิธีการทำงานของแพลตฟอร์มต่าง ๆ วิเคราะห์แหล่งที่มาของข้อมูล ป้องกันตนเองจากการถูกหลอกลวงทางออนไลน์ เช่น ฟิชชิง (Phishing) หรือไวรัสคอมพิวเตอร์ ความรู้เท่าทันดิจิทัลจึงเป็นรากฐานสำคัญในการลดความเสี่ยงจากการทิ้งร่องรอยดิจิทัลโดยไม่รู้ตัว

5.2 ความรู้เท่าทันสื่อ (Media Literacy) ในด้านการวิเคราะห์ วิจารณ์ และแยกแยะข้อมูลอย่างรอบด้าน พลเมืองดิจิทัลที่มีทักษะนี้ จะสามารถแยกแยะข่าวจริงและข่าวปลอม วิเคราะห์เจตนาของผู้ผลิตสื่อ เข้าใจผลกระทบของเนื้อหาต่อผู้อื่น ไม่เผยแพร่เนื้อหาที่อาจก่อให้เกิดความเข้าใจผิดหรือความเกลียดชัง ทักษะนี้ช่วยให้บุคคลตระหนักถึงผลกระทบของสิ่งที่ตนเผยแพร่ และตัดสินใจก่อนที่จะโพสต์ แสดงความคิดเห็น หรือแชร์ข้อมูล

5.3 การรู้สารสนเทศ (Information Literacy) โดยต้องสามารถเข้าถึง ประเมิน และใช้งานข้อมูลได้อย่างเหมาะสม ทักษะนี้รวมถึงการค้นหาข้อมูลที่ถูกต้องจากแหล่งที่เชื่อถือได้ สามารถประเมินคุณภาพของข้อมูลได้

5.4 การอ้างอิงแหล่งข้อมูลอย่างเหมาะสม ในการรักษาความเป็นส่วนตัวของตนเองและผู้อื่น เมื่อเผยแพร่ข้อมูล ทักษะนี้มีความสำคัญต่อการจัดการร่องรอยดิจิทัล โดยเฉพาะในการผลิตเนื้อหาหรือการโพสต์ข้อมูลต่าง ๆ ให้สอดคล้องกับหลักจริยธรรมและความปลอดภัย

5.5 การมีจริยธรรมและความรับผิดชอบทางดิจิทัล (Digital Ethics & Responsibility) โดยต้องรู้จักขอบเขตของการใช้เสรีภาพ มีจริยธรรมและความรับผิดชอบ เคารพสิทธิและความเป็นส่วนตัวของผู้อื่น ไม่คุกคามหรือรังแกทางไซเบอร์ ไม่ละเมิดลิขสิทธิ์หรือนำเนื้อหาผู้อื่นมาใช้โดยไม่ได้รับอนุญาต รวมทั้งการมีวินัยในการใช้เทคโนโลยี และไม่ใช้เพื่อก่ออันตราย

ผู้ที่มีจริยธรรมทางดิจิทัลจะสามารถควบคุมพฤติกรรมของตนบนโลกออนไลน์ได้ดี และลดความเสี่ยงจากการสร้างร่องรอยดิจิทัลในเชิงลบ การพัฒนาทักษะดิจิทัลเป็นกลไกสำคัญในการควบคุมร่องรอยดิจิทัลให้กลายเป็นสิ่งที่สร้างภาพลักษณ์เชิงบวก และปกป้องตนเองจากผลกระทบในระยะยาว

6. เครื่องมือและวิธีการตรวจสอบร่องรอยดิจิทัล

ในยุคที่ข้อมูลทุกอย่างสามารถถูกบันทึก ตรวจสอบ และย้อนกลับได้ การตระหนักรู้ถึงร่องรอยดิจิทัลจึงเป็นเรื่องจำเป็นสำหรับทุกคน โดยเฉพาะพลเมืองดิจิทัลที่ต้องการใช้เทคโนโลยีอย่างมีความรับผิดชอบ ขั้นตอนสำคัญของการจัดการร่องรอยดิจิทัล คือ การตรวจสอบร่องรอยซึ่งเป็นกระบวนการที่ช่วยให้รู้ว่าข้อมูลใดของผู้ใช้อยู่บนอินเทอร์เน็ตบ้าง ใครสามารถเข้าถึงได้ และจะจัดการอย่างไรให้เหมาะสม (Cyber B.A.A.P., 2024) ซึ่งมีแนวทางดังนี้

6.1 การค้นหาตัวเองบนอินเทอร์เน็ต (Self-Googling) ซึ่งเป็นวิธีหนึ่งในการตรวจสอบร่องรอยดิจิทัลของตนเอง โดยการลองค้นหาชื่อตนเองผ่าน Google หรือเครื่องมือค้นหาอื่น เช่น Bing หรือ DuckDuckGo เพื่อดูว่ามีข้อมูลอะไรเกี่ยวกับตัวเราปรากฏอยู่บ้าง ทั้งที่ตั้งใจและไม่ตั้งใจเผยแพร่ และที่อาจเกิดจากผู้อื่น

6.2 การตรวจสอบโปรไฟล์โซเชียลมีเดีย เช่น Facebook, Instagram, X (Twitter), TikTok และ LinkedIn ซึ่งมักจะเป็นแหล่งหลักของร่องรอยดิจิทัล ผู้ใช้งานควรเข้าไปตรวจสอบ เช่น โปรไฟล์ของตนเป็นสาธารณะหรือส่วนตัว มีโพสต์ใดบ้างที่เปิดให้คนทั่วไปเห็น เคยแสดงความคิดเห็นหรือแชร์เนื้อหาที่อาจไม่เหมาะสมหรือไม่ แพลตฟอร์มส่วนใหญ่มีระบบ Privacy Settings ที่สามารถปรับให้แสดงเฉพาะกลุ่ม เช่น เพื่อนเท่านั้น หรือเฉพาะผู้ติดตามที่อนุญาติ

6.3 การใช้เครื่องมือช่วยจากผู้ให้บริการอินเทอร์เน็ต โดยบริการจาก Google เช่น Google Account–My Activity สามารถตรวจสอบกิจกรรมที่เชื่อมโยงกับบัญชี Google Privacy Checkup สามารถช่วยแนะนำการตั้งค่าความเป็นส่วนตัวที่เหมาะสม Google Alerts สามารถตั้งค่าให้ Google แจ้งเตือนเมื่อชื่อของผู้ใช้ถูกพูดถึงหรือเผยแพร่บนเว็บไซต์ใหม่ ใช้เครื่องมือ เช่น Have I Been Pwned เพื่อทำการตรวจสอบว่าอีเมลหรือรหัสผ่านเคยรั่วไหลหรือไม่ และ DeleteMe / PrivacyDuck (สำหรับต่างประเทศ) เพื่อบริการลบข้อมูลส่วนบุคคล

6.4 การวิเคราะห์พฤติกรรมผ่านข้อมูลกิจกรรม โดยใช้แพลตฟอร์ม เช่น Facebook หรือ Instagram ซึ่งจะมีหน้า กิจกรรมของผู้ใช้ (Your Activity) ที่ผู้ใช้สามารถเข้าไปดูได้ว่า เคยโพสต์อะไรไว้บ้าง เคยกดไลก์ แชร์ หรือแสดงความคิดเห็นในเนื้อหาใด รวมทั้งเคยใช้แอปพลิเคชันใดเชื่อมต่อกับบัญชีโซเชียลมีเดียบ้าง

ในยุคที่ข้อมูลสามารถถูกบันทึกและตรวจสอบได้ตลอดเวลา การตระหนักรู้และจัดการร่องรอยดิจิทัลจึงเป็นสิ่งจำเป็น โดยเฉพาะสำหรับพลเมืองดิจิทัลที่ต้องการใช้เทคโนโลยีอย่างมีความรับผิดชอบ ขั้นตอนสำคัญคือการตรวจสอบร่องรอยของตนเอง เช่น การค้นหาชื่อบนอินเทอร์เน็ต (Self-Googling) และการตรวจสอบโปรไฟล์โซเชียลมีเดีย เพื่อควบคุมความเป็นส่วนตัว การใช้เครื่องมือช่วยจากผู้ให้บริการ เช่น Google Privacy Checkup หรือ Have I Been Pwned เพื่อตรวจสอบการรั่วไหลของข้อมูล และการวิเคราะห์พฤติกรรมผ่านข้อมูลกิจกรรมในแพลตฟอร์มต่าง ๆ เพื่อจัดการข้อมูลให้เหมาะสมและปลอดภัย

7. เทคนิคการป้องกันและจัดการร่องรอยดิจิทัล

เมื่อเข้าใจถึงความหมาย ผลกระทบ และวิธีการตรวจสอบร่องรอยดิจิทัลแล้ว ขั้นตอนสำคัญต่อไปคือการป้องกันและจัดการร่องรอยดิจิทัลอย่างมีประสิทธิภาพ เพื่อไม่ให้ข้อมูลกลายเป็นจุดอ่อนที่ถูกนำไปใช้ในทางที่

ผิด หรือส่งผลกระทบด้านลบในอนาคต การจัดการเหล่านี้ไม่ใช่เพียงการลบข้อมูล แต่คือกระบวนการที่ต้องใช้ทักษะ ความรอบคอบ และวินัยอย่างต่อเนื่อง ซึ่งกระทำผ่านกระบวนการต่อไปนี้ (Grassi et al., 2017)

7.1 การคิดก่อนโพสต์ (Think Before You Post) โดยต้องพิจารณาให้รอบคอบก่อนเผยแพร่ข้อมูลใด ๆ เพราะสิ่งที่เผยแพร่ออกไปอาจคงอยู่ถาวร หรือถูกจับภาพหน้าจอไว้แม้เราจะลบในภายหลัง แนวทางพิจารณาใช้ 3 คำถาม ได้แก่ (1) สิ่งที่โพสต์เป็นความจริงหรือไม่ (2) สิ่งที่โพสต์เหมาะสมหรือไม่ และ (3) สิ่งที่โพสต์จำเป็นต้องแชร์หรือไม่

7.2 การตั้งค่าความเป็นส่วนตัว (Privacy Settings) โดยผู้ใช้ควรปรับค่าความเป็นส่วนตัวในบัญชีโซเชียลมีเดีย เพื่อควบคุมผู้ที่สามารถเห็นเนื้อหาได้ เช่น ตั้งค่าให้เฉพาะเพื่อนเห็นโพสต์ จำกัดการแท็กชื่อหรือโพสต์บนไทม์ไลน์ ปิดการเข้าถึงตำแหน่ง (Location) อัตโนมัติ ปิดการเข้าถึงข้อมูลบัญชีจากแอปพลิเคชันภายนอก และควรเข้าไปตรวจสอบและอัปเดตการตั้งค่าเหล่านี้อย่างสม่ำเสมอ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงนโยบายจากแพลตฟอร์ม

7.3 ใช้รหัสผ่านที่ปลอดภัย และเปิดใช้งานการยืนยันตัวตนสองขั้นตอน (2FA) เพื่อรักษาความปลอดภัยของบัญชีซึ่งเป็นอีกหนึ่งวิธีในการควบคุมร่องรอยดิจิทัล โดยแนวทางที่ปลอดภัย ได้แก่ ใช้รหัสผ่านที่ยาว ผสมตัวอักษร ตัวเลข และสัญลักษณ์ หลีกเลี่ยงการใช้รหัสผ่านซ้ำในหลายบัญชี ใช้แอปพลิเคชันจัดการรหัสผ่าน เช่น Bitwarden หรือ 1Password เปิดระบบ 2FA เพื่อเพิ่มความปลอดภัย

7.4 ลบบัญชีที่ไม่ใช้แล้ว ยกเลิกการเชื่อมต่อบัญชีต่าง ๆ ที่เชื่อมผ่าน Facebook หรือ Google เคลียร์ประวัติการค้นหา หรือข้อมูลการใช้งานในเว็บเบราว์เซอร์ และทำการลบโพสต์หรือภาพเก่าที่อาจส่งผลกระทบต่อภาพลักษณ์ในอนาคต

7.5 ไม่ใช้ชื่อจริงหรือชื่อเดียวกันในหลายแพลตฟอร์ม ควรพิจารณาใช้ชื่อผู้ใช้ (Username) ที่แตกต่างกันในแต่ละแพลตฟอร์ม โดยเฉพาะในเว็บไซต์สาธารณะ หรือเว็บบอร์ด

7.6 เรียนรู้และอัปเดตความรู้เกี่ยวกับแนวทางการป้องกันตัวเองบนออนไลน์ นโยบายความเป็นส่วนตัวของแอปหรือแพลตฟอร์มต่าง ๆ ตลอดจนมีการติดตามข่าวสารด้านความปลอดภัยทางไซเบอร์ (Cybersecurity) สม่ำเสมอ

การป้องกันและจัดการร่องรอยดิจิทัลอย่างมีประสิทธิภาพต้องใช้ทักษะ ความรอบคอบ และวินัยอย่างต่อเนื่อง (Grassi et al., 2017) โดยแนวทางสำคัญ ได้แก่ การคิดรอบคอบก่อนโพสต์ (Think Before You Post) เพื่อหลีกเลี่ยงข้อมูลที่ไม่เหมาะสม การตั้งค่าความเป็นส่วนตัว (Privacy Settings) ในโซเชียลมีเดีย การใช้รหัสผ่านที่ปลอดภัยและเปิดใช้งานการยืนยันตัวตนสองขั้นตอน (2FA) การลบบัญชีหรือข้อมูลที่ไม่ใช้แล้ว การใช้ชื่อผู้ใช้แตกต่างกันในแต่ละแพลตฟอร์ม และการเรียนรู้และติดตามข้อมูลด้านความปลอดภัยออนไลน์อย่างสม่ำเสมอ เพื่อรักษาความปลอดภัย ข้อมูลส่วนตัว และภาพลักษณ์ในโลกดิจิทัล

การจัดการร่องรอยดิจิทัลไม่ใช่เรื่องของเทคโนโลยีเพียงอย่างเดียว แต่เป็นเรื่องของนิสัยดิจิทัลที่ต้องปลูกฝังและฝึกฝนให้เกิดขึ้นเป็นกิจวัตร สำหรับพลเมืองดิจิทัลที่มีความรับผิดชอบในศตวรรษที่ 21

8. กฎหมายและสิทธิด้านข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal Data) ถือเป็นทรัพย์สินทางดิจิทัล มีความจำเป็นที่ต้องมีกฎหมายเข้ามาควบคุมเพื่อสร้างกรอบแนวปฏิบัติทั้งในระดับประเทศและสากล ซึ่งประกอบด้วย

8.1 กฎหมายและสิทธิด้านข้อมูลส่วนบุคคลสำหรับประเทศไทย โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act) หรือ PDPA มีเป้าหมายเพื่อควบคุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้เป็นธรรมและปลอดภัย โดยหลักการสำคัญของ PDPA คือ (1) ความยินยอม (Consent) ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนจะเก็บหรือใช้ (2) วัตถุประสงค์ชัดเจน (Purpose Limitation) โดยต้องแจ้ง

จุดประสงค์การใช้ข้อมูลอย่างชัดเจน (3) สิทธิของเจ้าของข้อมูล (Data Subject Rights) (4) ขอเข้าถึงข้อมูลของตน (5) ขอให้ลบหรือทำลายข้อมูล (6) ขอให้แก้ไขข้อมูล (7) คัดค้านการใช้ข้อมูล (8) เพิกถอนความยินยอมได้ทุกเมื่อ (9) การรักษาความปลอดภัยของข้อมูล (Security) ผู้เก็บข้อมูลต้องดูแลไม่ให้รั่วไหล และ (10) บทลงโทษโดยมีโทษทั้งทางปกครอง อาญา และแพ่ง เช่น ปรับ หรือจำคุกในกรณีร้ายแรง

8.2 กฎหมายและแนวปฏิบัติสากล เพื่อรองรับโลกออนไลน์ที่ไร้พรมแดน ได้มีการออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลของพลเมือง ในหลายประเทศ เช่น

EU GDPR (General Data Protection Regulation แห่งสหภาพยุโรป) ประกอบด้วย (1) กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เข้มงวดที่สุดในโลก (2) มีบทลงโทษสูงถึง 4% ของรายได้ทั่วโลกขององค์กร และ (3) เน้นสิทธิของเจ้าของข้อมูล และการขอความยินยอมอย่างชัดเจน (Regulation (EU) 2016/679, 2016)

US CCPA (California Consumer Privacy Act แห่งสหรัฐอเมริกา) ประกอบด้วย (1) ให้สิทธิผู้บริโภคให้สามารถ รู้ ลบ และควบคุม ข้อมูลที่บริษัทเก็บจากตนได้ (2) บังคับใช้ในรัฐแคลิฟอร์เนีย แต่มีผลกระทบต่อบริษัทระดับโลกที่มีผู้ใช้งานในพื้นที่นั้น (State of California Department of Justice, 2024)

โดยกฎหมายทั้ง 2 ประเภทมีความเหมือนและแตกต่างกันดังนี้

ด้านความเหมือนคือ

1) ทั้ง GDPR (สหภาพยุโรป) และ CCPA (สหรัฐอเมริกา) เป็นกฎหมายที่มุ่งคุ้มครอง ข้อมูลส่วนบุคคลของผู้ใช้ และให้สิทธิแก่เจ้าของข้อมูลในการเข้าถึง ควบคุม หรือจัดการข้อมูลของตนเอง

2) กฎหมายทั้งสองประเภทเน้นให้ องค์กรมีความรับผิดชอบ ต่อการเก็บ ใช้ และปกป้องข้อมูลส่วนบุคคล

3) ทั้งคู่มีผลกระทบต่อองค์กรระดับโลก หากมีผู้ใช้งานจากพื้นที่ที่กฎหมายบังคับใช้

ด้านความแตกต่างคือ

1) พื้นที่บังคับใช้: GDPR บังคับใช้ใน ทั้งสหภาพยุโรปและองค์กรที่ทำธุรกิจกับผู้ใช้ยุโรป ส่วน CCPA บังคับใช้เฉพาะ รัฐแคลิฟอร์เนีย แต่มีผลกระทบต่อบริษัทระดับโลกที่มีผู้ใช้ในรัฐนั้น

2) ระดับบทลงโทษ: GDPR มีบทลงโทษสูงถึง 4% ของรายได้ทั่วโลกขององค์กร ขณะที่ CCPA มีบทลงโทษที่เจาะจงมากกว่าแต่ไม่สูงเท่า GDPR

3) การขอความยินยอมและสิทธิของผู้ใช้: GDPR เน้น ความยินยอมอย่างชัดเจน (Explicit Consent) ก่อนเก็บหรือใช้ข้อมูล ในขณะที่ CCPA เน้นสิทธิผู้บริโภคในการ รู้ ลบ และควบคุมข้อมูล มากกว่าการขอความยินยอมล่วงหน้า

9. ความท้าทายของพลเมืองดิจิทัลในอนาคต

สำหรับความท้าท้ายของพลเมืองดิจิทัลในอนาคตในศตวรรษที่ 21 เป็นเรื่องที่สำคัญมากในยุคนี้ และส่งผลกระทบอย่างลึกซึ้งต่อ ทั้งสถานศึกษา ครอบครัว และสังคม ซึ่งแต่ละภาคส่วนก็เผชิญกับความท้าทายที่แตกต่างกันดังนี้

9.1 การขาดความรู้ในการสอนเรื่องร่องรอยดิจิทัลของสถานศึกษา ครูและผู้บริหารไม่เข้าใจว่าร่องรอยดิจิทัลคืออะไร และควรจัดการอย่างไร ยังไม่มีการบูรณาการเรื่องการใช้เทคโนโลยีอย่างมีความรับผิดชอบลงในแผนการสอนอย่างชัดเจน ตลอดจนเป็นเรื่องของการควบคุมหรือแนะแนวการใช้โซเชียลมีเดียของนักเรียนยังเป็นเรื่องที่ท้าทาย ซึ่งสถานศึกษาควรบรรจุเรื่องทักษะพลเมืองดิจิทัลในหลักสูตรอย่างเป็นระบบ

9.2 พ่อแม่ผู้ปกครองขาดความรู้เรื่องดิจิทัล ไม่สามารถให้คำแนะนำลูกเกี่ยวกับความเสี่ยงของการทิ้งร่องรอยดิจิทัล พ่อแม่บางคนโพสต์ภาพหรือข้อมูลของลูกโดยไม่คำนึงถึงอนาคตของเด็ก (Sharenting) การควบคุม

พฤติกรรมออนไลน์ของลูก โดยพ่อแม่ขาดเครื่องมือและทักษะในการติดตามหรือแนะนำลูกให้ใช้อินเทอร์เน็ตอย่างปลอดภัย

9.3 การที่ผู้คนในสังคมแชร์ข้อมูลมากเกินไป โดยไม่ตระหนักถึงผลกระทบ เช่น การถูกขโมยตัวตน (Identity Theft) การขาดกฎหมายและการบังคับใช้ โดยยังไม่มีการควบคุมหรือบทลงโทษที่ชัดเจนเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล รวมทั้งค่านิยมสังคมในเรื่อง การโชว์ตัวตน โดยคนในสังคมให้คุณค่ากับยอดไลก์ยอดแชร์มากกว่าความปลอดภัยหรือศีลธรรมดิจิทัล

สำหรับแนวทางการรับมือกับความท้าทายดังกล่าวสามารถดำเนินการได้ดังนี้

1) บูรณาการเข้าไปในหลักสูตรการเรียนการสอน จัดอบรมเชิงปฏิบัติการหรืออบรมพิเศษ เชิญวิทยากรผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์หรือจริยธรรมดิจิทัล จัดอบรมเชิงปฏิบัติการฝึกใช้เครื่องมือตรวจสอบและลบร่องรอยดิจิทัลจริง ฝึกวิเคราะห์กรณีศึกษาเกี่ยวกับผลกระทบจากร่องรอยดิจิทัล ส่งเสริมวินัยดิจิทัลผ่านกิจกรรมสร้างสรรค์ เช่น ประกวดวิดีโอ/โปสเตอร์หัวข้อ คิดก่อนโพสต์

2) ส่งเสริมบทบาทของครูเป็นในการเป็นโค้ชดิจิทัล ครูควรเป็นแบบอย่างในการใช้งานอินเทอร์เน็ตอย่างรับผิดชอบ ให้คำแนะนำผู้เรียนเรื่องความปลอดภัยในโลกออนไลน์เป็นประจำ ติดตามพฤติกรรมออนไลน์ของนักเรียนเชิงสร้างสรรค์ เช่น การเปิดเพจวิชาการหรือกลุ่มเรียนรู้

3) ผู้ปกครองหรือครอบครัวควรมีบทบาทร่วมกับสถานศึกษา โดยสร้างความเข้าใจร่วมกันระหว่างบ้านและโรงเรียนในเรื่องร่องรอยดิจิทัล ร่วมมือในการจัดอบรมครอบครัวดิจิทัลเพื่อส่งเสริม การใช้อินเทอร์เน็ตอย่างปลอดภัยในครอบครัว

4) สังคมควรส่งเสริมการรู้เท่าทันดิจิทัลในทุกกลุ่มอายุ และสร้างกฎหมายปกป้องข้อมูลส่วนบุคคลที่เข้มแข็ง

10. ความท้าทายและอุปสรรคในการจัดการร่องรอยดิจิทัล

แม้ว่าการจัดการร่องรอยดิจิทัลจะเป็นเรื่องสำคัญในยุคเทคโนโลยีสารสนเทศแต่ในทางปฏิบัติกลับพบว่า การดำเนินการจัดการเหล่านี้ไม่ใช่เรื่องง่าย ด้วยเหตุจากความเปลี่ยนแปลงของเทคโนโลยีอย่างรวดเร็ว ความซับซ้อนของข้อมูล และพฤติกรรมของผู้ใช้งานที่มักขาดความระมัดระวัง ส่งผลให้เกิดอุปสรรคหลายประการทั้งในระดับบุคคล ระดับสังคม และระดับนโยบาย สามารถสรุปเป็นประเด็นดังนี้

10.1 การขาดความตระหนักรู้ (Lack of Awareness) ของผู้ใช้จำนวนมากที่ยังไม่เข้าใจว่า ทุกการคลิกหรือทุกโพสต์ สามารถสร้างร่องรอยดิจิทัลถาวรได้ ขาดความรู้เกี่ยวกับผลกระทบในระยะยาว เช่น การถูกติดตาม การขโมยข้อมูล หรือการสูญเสียโอกาสทางสังคม หลายคนมองว่าเป็นเรื่องไกลตัว จึงไม่ได้ใส่ใจในการจัดการร่องรอยดิจิทัลของตนเอง

10.2 พฤติกรรมการใช้งานแบบขาดความระมัดระวัง แชร์ข้อมูลส่วนตัวหรือโพสต์โดยไม่คิดให้รอบคอบ ใช้แอปพลิเคชันหรือเว็บไซต์โดยไม่อ่านข้อตกลงความเป็นส่วนตัว ใช้รหัสผ่านซ้ำ หรือไม่มีการป้องกันข้อมูลอย่างเหมาะสม

10.3 หลายคนขาดทักษะด้านเทคโนโลยีและการรู้เท่าทันดิจิทัล ไม่รู้วิธีตรวจสอบหรือลบร่องรอยดิจิทัล เช่น การตั้งค่าความเป็นส่วนตัว การล้างข้อมูล หรือการควบคุมสิทธิ์แอป ขาดความรู้ในการใช้เครื่องมือตรวจสอบร่องรอยดิจิทัล (Digital Footprint Check Tools)

10.4 ขอบเขตของกฎหมายและการบังคับใช้ โดยกฎหมายบางฉบับ ยังไม่สามารถครอบคลุมพฤติกรรมออนไลน์ที่เปลี่ยนแปลงอย่างรวดเร็ว การบังคับใช้กฎหมายในโลกออนไลน์ยังมีข้อจำกัด เช่น ไม่สามารถควบคุมข้อมูลที่อยู่บนเซิร์ฟเวอร์ต่างประเทศได้ หลายกรณียากต่อการระบุผู้กระทำผิด (เช่น กรณีบัญชีปลอม หรือการโพสต์แบบนิรนาม)

10.5 วัฒนธรรมการใช้อินเทอร์เน็ตแบบแชร์ด่วนในสื่อสังคมออนไลน์กระตุ้นให้ผู้ใช้ โพสต์ แชร์ และแสดงความคิดเห็นอย่างรวดเร็ว วัฒนธรรมไวรัลทำให้ข้อมูลหลุดเร็วและกระจายอย่างควบคุมไม่ได้ ผู้คนมักไม่ได้กลั่นกรองข้อมูลก่อนแชร์ เพราะมุ่งเน้นความไวและยอดไลก์

10.6 ร่องรอยดิจิทัลไม่ได้อยู่เฉพาะในโซเชียลมีเดีย แต่กระจายอยู่ในเว็บไซต์ แอปพลิเคชัน อุปกรณ์ IoT และฐานข้อมูลขององค์กรต่าง ๆ การจัดการข้อมูลข้ามแพลตฟอร์มจึงมีความยุ่งยากและต้องใช้ความรู้เชิงเทคนิค เนื่องจากความซับซ้อนของข้อมูลและเทคโนโลยี

10.7 ระบบการศึกษาที่ยังปรับตัวไม่ทัน โดยหลักสูตรในหลายสถานศึกษายังไม่ได้เน้นทักษะชีวิตดิจิทัล ครูบางส่วนยังไม่เข้าใจประเด็นร่องรอยดิจิทัลอย่างลึกซึ้ง ขาดแหล่งเรียนรู้ที่เหมาะสมและสื่อการสอนที่ทันสมัย

การจัดการร่องรอยดิจิทัลแม้จะเป็นสิ่งจำเป็น แต่ก็เผชิญกับอุปสรรคหลากหลายประการทั้งจากภายในตัวผู้ใช้เองและจากบริบทภายนอก การแก้ไขปัญหาเหล่านี้จึงต้องอาศัยความร่วมมือจากหลายภาคส่วน ทั้งรัฐ สถานศึกษา องค์กร และบุคคลทั่วไป เพื่อสร้างระบบนิเวศดิจิทัลที่ปลอดภัยและรับผิดชอบร่วมกันอย่างยั่งยืน

11. บทบาทของเทคโนโลยีในการจัดการร่องรอยดิจิทัล

ในขณะที่เทคโนโลยีดิจิทัลเป็นต้นเหตุของการเกิดร่องรอยดิจิทัลจำนวนมาก ขณะเดียวกันเทคโนโลยีก็เป็นเครื่องมือสำคัญที่สามารถใช้ในการบริหาร จัดการ ควบคุม และลดความเสี่ยงจากร่องรอยดิจิทัลได้อย่างมีประสิทธิภาพ หากมีการนำมาใช้อย่างถูกวิธี เทคโนโลยีจะเป็นกลไกสำคัญที่ช่วยเสริมสร้างความปลอดภัยและความเป็นส่วนตัวในโลกออนไลน์ได้เป็นอย่างมาก (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2568) ดังนี้

11.1 เป็นเครื่องมือควบคุมความเป็นส่วนตัว (Privacy Tools) โดยใช้ฟีเจอร์การตั้งค่าความเป็นส่วนตัวบนแพลตฟอร์มต่าง ๆ (Facebook, Instagram, Google) ช่วยให้ผู้ใช้ควบคุมว่าใครจะเห็นข้อมูลอะไรของตนบ้าง แอป VPN (Virtual Private Network) ใช้ปกปิดตำแหน่งและข้อมูลการใช้งานอินเทอร์เน็ต เพื่อความเป็นส่วนตัวมากยิ่งขึ้น ฟีเจอร์ลบร่องรอยอัตโนมัติ เช่น Google My Activity ที่อนุญาตให้ลบประวัติการใช้งานทุก 3 เดือน

11.2 เป็นเครื่องมือหรือโปรแกรมจัดการร่องรอยดิจิทัลและเว็บไซต์ ที่ช่วยให้ผู้ใช้งานสามารถตรวจสอบว่าตนเองได้ทิ้งร่องรอยอะไรไว้ในโลกออนไลน์ เช่น JustDelete.Me เป็นการรวมลิงก์ที่ช่วยให้ลบบัญชีออกจากเว็บไซต์ต่าง ๆ ได้ง่ายขึ้น , Mine ใช้เพื่อวิเคราะห์อีเมลว่าถูกใช้ลงทะเบียนกับบริการใดบ้าง , AccountKiller ที่ช่วยแนะนำวิธีลบบัญชีจากแพลตฟอร์มออนไลน์ต่าง ๆ อย่างละเอียด

11.3 เทคโนโลยี AI และ Machine Learning เป็นเครื่องมือที่ใช้ในการตรวจจับและแจ้งเตือนพฤติกรรมเสี่ยงทางไซเบอร์ เช่น การถูกแฮก หรือการรั่วไหลของข้อมูล บริษัทหลายแห่งใช้ AI วิเคราะห์ข้อมูลผู้ใช้เพื่อให้คำแนะนำเรื่องความปลอดภัย ระบบอัจฉริยะนี้สามารถที่จะลบร่องรอยอัตโนมัติ หรือเตือนผู้ใช้ก่อนโพสต์เนื้อหาที่เป็นความเสี่ยง

11.4 เทคโนโลยีการเข้ารหัส (Encryption) โดยการเข้ารหัสข้อมูลแบบ End-to-End เช่น ในแอป WhatsApp และ Signal ช่วยให้ข้อมูลที่ส่งไม่สามารถถูกดักฟังระหว่างทาง ใช้เพื่อป้องกันการเข้าถึงข้อมูลส่วนตัวโดยไม่ได้รับอนุญาต เป็นพื้นฐานของความปลอดภัยในการจัดการข้อมูลร่องรอยดิจิทัลในองค์กร

11.5 เทคโนโลยีระบบการยืนยันตัวตนขั้นสูง (Multi-Factor Authentication–MFA) เพื่อเข้าถึงบัญชี เพิ่มระดับความปลอดภัย เช่น ต้องยืนยันตัวผ่าน SMS, Email, หรือแอป OTP ลดความเสี่ยงจากการถูกเข้าถึงบัญชีโดยไม่ได้รับอนุญาต

11.6 เป็นเครื่องมือในการสแกนตัวตนออนไลน์ เช่น เครื่องมืออย่าง Google Search, Social Searcher, Pipl, หรือ BeenVerified ใช้ค้นหาร่องรอยของตนเองบนโลกออนไลน์ ทำให้ผู้ใช้งานสามารถรู้ว่าตัวตนดิจิทัลของตน ปรากฏอยู่ที่ไหน และควรลบหรือตั้งค่าใหม่ตรงจุดใด

ในยุคที่ข้อมูลส่วนบุคคลถูกเชื่อมโยงกับกิจกรรมแทบทุกอย่างบนโลกออนไลน์ การใช้เครื่องมือปกป้องความเป็นส่วนตัวจึงกลายเป็นทักษะจำเป็น โดยการตั้งค่าความเป็นส่วนตัวบนแพลตฟอร์มสังคมออนไลน์ และการใช้ VPN ถือเป็นวิธีพื้นฐานที่ช่วยปกปิดตัวตนและลดการถูกติดตามข้อมูลได้อย่างมีประสิทธิภาพ นอกจากนี้ แพลตฟอร์มการจัดการร่องรอยดิจิทัล ยังช่วยให้ผู้ใช้งานสามารถบริหารจัดการบัญชีและข้อมูลที่หลงเหลือได้อย่างเป็นระบบ ช่วยลดความเสี่ยงจากข้อมูลที่ถูกละเลยไว้ในอดีต ขณะเดียวกันผู้ใช้ควรปรับตั้งค่าความเป็นส่วนตัวอย่างสม่ำเสมอและหลีกเลี่ยงการให้ข้อมูลส่วนตัวที่มากเกินความจำเป็น

12. การสร้างจริยธรรมและวินัยดิจิทัลในกลุ่มเยาวชน

เยาวชนในศตวรรษที่ 21 เติบโตมากับเทคโนโลยีและเครือข่ายอินเทอร์เน็ต ถือเป็นพลเมืองดิจิทัลโดยกำเนิด (Digital Natives) การเข้าถึงเทคโนโลยีอย่างกว้างขวางไม่ได้หมายความว่าจะมีความเข้าใจหรือมีจริยธรรมในการใช้งานอย่างถูกต้องเสมอไป การส่งเสริม จริยธรรมและวินัยดิจิทัล จึงเป็นหัวใจสำคัญที่ต้องปลูกฝังตั้งแต่วัยเยาว์ เพื่อให้สามารถจัดการร่องรอยดิจิทัลของตนได้อย่างมีความรับผิดชอบ

สำหรับเป้าหมายของการสร้างจริยธรรมดิจิทัล เพื่อส่งเสริมให้เยาวชนรู้จักเคารพสิทธิของผู้อื่น ในโลกออนไลน์ สร้างความเข้าใจเรื่องผลกระทบจากการกระทำในสื่อดิจิทัล พัฒนาพฤติกรรมการใช้อินเทอร์เน็ตอย่างปลอดภัยและสร้างสรรค์ และลดปัญหาการกลั่นแกล้งออนไลน์ (Cyberbullying) การใช้ถ้อยคำไม่เหมาะสมและรู้สึกผิดต่อการแชร์ข้อมูลเท็จ โดยแนวทางการส่งเสริมจริยธรรมและวินัยดิจิทัลมีดังนี้

12.1 แนวทางการศึกษาแบบบูรณาการ โดยสอดแทรกหัวข้อจริยธรรมดิจิทัลในทุกระดับชั้น เช่น การให้เครดิตแหล่งที่มา การเคารพความเป็นส่วนตัวของผู้อื่น การไม่ใช้ข้อมูลปลอมเพื่อหลอกลวง ส่งเสริมให้ผู้เรียนตั้งคำถามกับพฤติกรรมดิจิทัลของตนเอง

12.2 แนวทางการเรียนรู้แบบลงมือทำ (Active Learning) การใช้สถานการณ์จำลอง (Simulation) ให้เยาวชนรับบทเป็นผู้โพสต์ ผู้รับสาร หรือผู้เฝ้าดู เพื่อเข้าใจผลกระทบหลายด้าน ให้สร้างเนื้อหาออนไลน์ด้วยตนเอง เช่น คลิปสั้น อินโฟกราฟิก หรือโพสต์ ให้ผู้เรียนวิเคราะห์ว่ามีผลต่อภาพลักษณ์ดิจิทัลอย่างไร

12.3 แนวทางด้านการให้คำปรึกษาและการแนะแนว โรงเรียนควรมีระบบแนะแนวเกี่ยวกับพฤติกรรมบนโลกออนไลน์ เปิดพื้นที่ปลอดภัยให้เยาวชนพูดคุยเรื่องประสบการณ์หรือปัญหาที่พบ สร้างระบบพี่เลี้ยง (Digital Peer Mentoring) ให้รุ่นพี่แนะนำรุ่นน้อง

12.4 แนวทางด้านการมีส่วนร่วมของผู้ปกครอง โดยการสื่อสารกับผู้ปกครองให้เข้าใจว่าโลกออนไลน์มีผลกับชีวิตเด็กมากเพียงใด จัดอบรมร่วมกัน สำหรับ บ้าน-โรงเรียน เช่น จัดอบรมเชิงปฏิบัติการการสร้างลูกให้เป็นพลเมืองดิจิทัล สร้างแนวทางการใช้เทคโนโลยีในครอบครัวร่วมกัน เช่น ข้อตกลงการใช้งานโทรศัพท์มือถือ

การบูรณาการด้านจริยธรรมดิจิทัลในทุกวิชา จะเป็นการปลูกฝังการให้เครดิตกับแหล่งข้อมูลและการเคารพความเป็นส่วนตัวตั้งแต่ต้น การเรียนรู้แบบลงมือทำและสถานการณ์จำลอง ทำให้ผู้เรียนเข้าใจผลกระทบของพฤติกรรมออนไลน์ผ่านประสบการณ์จริง การส่งเสริมการสร้างสื่อออนไลน์โดยผู้เรียนเพื่อให้รู้และตระหนักถึงภาพลักษณ์ดิจิทัลของตนเอง นอกจากนั้นสถานศึกษาควรมีระบบแนะแนวด้านการใช้สื่อออนไลน์อย่างปลอดภัย พร้อมเปิดพื้นที่ให้เด็กปรึกษาเรื่องปัญหาดิจิทัล พัฒนาระบบพี่เลี้ยงดิจิทัลให้รุ่นพี่ช่วยชี้แนะรุ่นน้องในการใช้งานเทคโนโลยีอย่างเหมาะสม รวมทั้งมีการส่งเสริมความร่วมมือระหว่างบ้านและโรงเรียน โดยจัดอบรมผู้ปกครองและสร้างข้อตกลงการใช้เทคโนโลยีร่วมกันในครอบครัว

สรุป

ร่องรอยดิจิทัล กลายเป็นสิ่งที่หลีกเลี่ยงไม่ได้ ทุกการค้นหา คลิก แชร์ หรือโพสต์ ล้วนทิ้งข้อมูลบางอย่างไว้ในระบบ ซึ่งข้อมูลเหล่านี้สามารถส่งผลกระทบต่อผู้ใช้ในระยะยาว ทั้งในเชิงบวกและเชิงลบ

การจัดการร่องรอยดิจิทัลจำเป็นต้องมีวินัยดิจิทัลซึ่งจะช่วยให้สามารถควบคุมร่องรอยดิจิทัลได้ดียิ่งขึ้น เพราะจะรู้จักคิดไตร่ตรองก่อนกระทำ ลดโอกาสการสร้างร่องรอยดิจิทัลในเชิงลบ และเพิ่มพูนร่องรอยดิจิทัลในเชิงบวกที่ส่งเสริมภาพลักษณ์และโอกาส

จริยธรรมและวินัยดิจิทัลไม่ใช่แค่การทำดีในโลกออนไลน์ แต่คือการสร้างรากฐานทางพฤติกรรมที่จะติดตัวไปตลอดชีวิต ทั้งในฐานะผู้เรียน ผู้ทำงาน และการเป็นพลเมืองในโลกดิจิทัลที่ซับซ้อนเพื่ออนาคตที่ปลอดภัยและยั่งยืน

ข้อเสนอแนะ

การจัดการร่องรอยดิจิทัลอย่างมีประสิทธิภาพควรดำเนินการทั้งในระดับสังคมไทยและระดับโลก โดยภาครัฐต้องออกกฎหมายและมาตรการคุ้มครองข้อมูลส่วนบุคคลที่รัดกุม พร้อมกลไกการบังคับใช้ที่เข้มแข็ง และส่งเสริมความรู้เท่าทันดิจิทัลในระดับนโยบายการศึกษา พัฒนาระบบสนับสนุนให้ครู ผู้ปกครอง และนักเรียนสามารถใช้งานเทคโนโลยีได้อย่างปลอดภัย สถานศึกษาควรบูรณาการความรู้เรื่องการจัดการร่องรอยดิจิทัลและจริยธรรมดิจิทัลในหลักสูตร จัดกิจกรรมที่เน้นการปฏิบัติจริง ส่งเสริมแนวคิดก่อนคลิกและความรับผิดชอบในโลกดิจิทัล ผู้ปกครองควรเรียนรู้การใช้อินเทอร์เน็ตอย่างปลอดภัยไปพร้อมกับบุตรหลาน ใช้การสื่อสารสร้างความเข้าใจและไว้วางใจ รวมถึงสร้างบรรยากาศที่ส่งเสริมการใช้เทคโนโลยีอย่างสร้างสรรค์ สำหรับบุคคลทั่วไปควรหมั่นตรวจสอบร่องรอยดิจิทัลของตน ใช้เทคโนโลยีในการป้องกันข้อมูลส่วนตัว เคารพผู้อื่นในโลกออนไลน์ และพิจารณาให้รอบคอบก่อนแสดงพฤติกรรม การจัดการร่องรอยดิจิทัลไม่ใช่เพียงการลบอดีต แต่คือการวางแผนเพื่ออนาคตด้วยความเข้าใจและความรับผิดชอบต่อพฤติกรรมออนไลน์ พลเมืองดิจิทัลในศตวรรษที่ 21 จึงควรมีทักษะที่ทันสมัย รู้เท่าทัน รู้คิด รู้จัดการ และรู้รับผิดชอบต่อร่องรอยดิจิทัลของตนเอง เพื่อร่วมสร้างสังคมดิจิทัลที่ปลอดภัย โปร่งใส และมีคุณภาพอย่างยั่งยืน

เอกสารอ้างอิง

ฉัตรพงศ์ ชูแสงนิล. (2562, 31 ตุลาคม). *ร่องรอยดิจิทัล (Digital footprint).* SciMath. https://www.scimath.org/article-technology/item/10617-digital-footprint

ปริญญา หอมเอนก. (2565, 3 พฤษภาคม). Digital identity–digital footprint ความโยงใยที่คุณอาจไม่รู้. *กรุงเทพธุรกิจ*. https://www.bangkokbiznews.com/columnist/1002163

สถาบันสื่อเด็กและเยาวชน. (2562). *พลเมืองดิจิทัล (Digital citizenship).* สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ.

สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ. (2562, 27 มีนาคม). *พลเมืองดิจิทัล (Digital citizenship).* https://www.thaihealth.or.th/พลเมืองดิจิทัล-digital-citizenship-2

สำนักงานบริหารและพัฒนาองค์ความรู้. (2564, 28 ตุลาคม). *พลเมืองดิจิทัลแห่งศตวรรษที่ 21*. https://www.okmd.or.th/okmd-opportunity/opportunities-2021/4641

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2568, 27 กุมภาพันธ์). *Digital footprint: อย่าปล่อยให้ 'ร่องรอยดิจิทัล' หลอนหลอกชั่วชีวิต.* https://www.etda.or.th/th/Useful-Resource/ETDA_Digital_Footprint.aspx

Cyber B.A.A.P. (2024, June 10). *How to check your digital footprint*. https://www.cyberbaap.org/how-to-check-your-digital-footprint/

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). *Digital identity guidelines: Authentication and lifecycle management* (Special publication 800-63B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

Many companies reject candidates due to social media posts: Study. (2014, September 15). *The Times of India*. https://timesofindia.indiatimes.com/social/many-companies-reject-candidates-due-to-social-media-posts-study/articleshow/42543878.cms

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). (2016, May 4). *Official Journal of the European Union*. L119, 4.5.2016, pp. 1–88. https://eur-lex.europa.eu/eli/reg/2016/679oj

State of California Department of Justice. (2024, March 13). *California consumer privacy act (CCPA)*. https://oag.ca.gov/privacy/ccpa

Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.