

ความรับผิดชอบทางดิจิทัลขององค์กร: กุญแจสู่สังคมดิจิทัลอย่างมีจริยธรรมที่ยั่งยืน

Corporate Digital Responsibility: The Key to a Sustainable and Ethical Digital Society

Received: 14 February 2025

Revised: 25 April 2025

Accepted: 30 April 2025

เอกวิทย์ โทบุรินทร์, คณะศึกษาศาสตร์ มหาวิทยาลัยบูรพา

บทคัดย่อ ความรับผิดชอบทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) เป็นแนวคิดที่ขยายจาก ความรับผิดชอบต่อสังคมขององค์กร เพื่อตอบสนองต่อความท้าทายด้านจริยธรรม ความเป็นส่วนตัว ความยั่งยืน และการเข้าถึงเทคโนโลยี ในยุคดิจิทัล (Lobschat et al., 2021) โดยมี 4 เสาหลัก ได้แก่ จริยธรรมทางดิจิทัลและปัญญาประดิษฐ์ ความเป็นส่วนตัวและความปลอดภัยทางไซเบอร์ การพัฒนาดิจิทัลอย่างยั่งยืน และการเข้าถึงเทคโนโลยีอย่างเท่าเทียม (Scarpi & Pantano, 2024; Mihale-Wilson et al., 2022; Cheng & Zhang, 2023; Rugeviciute & Courboulay, 2024) ช่วยให้องค์กรเสริมสร้างความไว้วางใจ ลดความเสี่ยงทางกฎหมาย และสอดคล้องกับมาตรฐานการกำกับดูแลด้านดิจิทัล (Oduro et al., 2024) หลายองค์กรชั้นนำได้ใช้ เช่น บริษัท กูเกิ้ล จำกัด (Google LLC) กับหลักจริยธรรม บริษัทแอปเปิล อิงค์ (Apple Inc) กับนโยบายความเป็นส่วนตัว และบริษัท ไมโครซอฟท์ คอร์ปอเรชั่น (Microsoft Corporation) กับกลยุทธ์ความยั่งยืนทางดิจิทัล (Kunz et al., 2024; Carl & Hinz, 2024; Elliott & Copilah-Ali, 2024) สำหรับประเทศไทย ธุรกิจขนาดใหญ่ เช่น ธนาคารไทยพาณิชย์ ธนาคารกสิกรไทย บริษัท พีทีที ดิจิตอล โซลูชั่น จำกัด บริษัท ทู คอร์ปอเรชั่น จำกัด และ บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) กำลังดำเนินมาตรการที่สอดคล้องกับ กฎหมายคุ้มครองข้อมูลส่วนบุคคลและการพัฒนาโครงสร้างพื้นฐานดิจิทัลที่ปลอดภัย (Cheng & Zhang, 2023; Keskin & Esen, 2024) แนวโน้มของความรับผิดชอบต่อดิจิทัลขององค์กรในอนาคตที่สะท้อนถึง การกำกับดูแลที่เข้มงวดขึ้นในระดับสากล โดยเฉพาะด้านปัญญาประดิษฐ์ และการจัดการข้อมูล (Hartley et al., 2024) และความจำเป็นที่องค์กรต้อง พัฒนาแนวทางปฏิบัติด้านจริยธรรมดิจิทัลให้เป็นมาตรฐาน (Herden et al., 2021) จึงเป็นกลยุทธ์ที่องค์กรต้องปรับใช้เพื่อความยั่งยืนและความสามารถในการแข่งขันในยุคดิจิทัล

คำสำคัญ: ความรับผิดชอบทางดิจิทัล จริยธรรม ความยั่งยืน

Abstract Corporate Digital Responsibility (CDR) has emerged as a critical framework for organizations navigating the ethical, legal, and social implications of digital transformation. Expanding upon Corporate Social Responsibility (CSR), CDR addresses four key dimensions: Digital Ethics & AI Responsibility, Data Privacy & Cybersecurity,

Sustainable Digital Development, and Inclusive Digitalization. These pillars guide organizations in integrating ethical digital practices into their operations, ensuring compliance with regulations, fostering consumer trust, and promoting sustainability.

This article explores the importance of CDR in mitigating risks associated with data privacy violations, cybersecurity threats, algorithmic biases, and lack of digital transparency. The discussion highlights real-world applications by leading global companies such as Google LLC (AI Ethics), Apple Inc (Privacy Policy), and Microsoft Corporation (Sustainable Digital Strategy). Additionally, it examines the CDR landscape in Thailand, focusing on compliance with the Personal Data Protection Act, digital sustainability initiatives, and the adoption of CDR principles by major corporations, including The Siam Commercial Bank Public Company Limited (SCB), Kasikornbank Public Company Limited (KBank), PTT Digital Solutions Company Limited (PTT Digital), True Corporation Public Company Limited (True), and Advanced Info Service Public Company Limited (AIS).

Furthermore, this paper analyzes the long-term impact of CDR on corporate reputation, legal compliance, and sustainable digital growth. The future trajectory of CDR is also considered, with an emphasis on stricter global AI regulations, ethical data governance, and digital responsibility in the emerging metaverse economy. As organizations increasingly integrate digital solutions, establishing a strong CDR framework is no longer optional but essential for ethical business practices and long-term resilience.

Keywords: Corporate Digital Responsibility, Ethics, Sustainable Development

บทนำ

ความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) มีพัฒนาการมาจากความรับผิดชอบต่อสังคมขององค์กร (Corporate Social Responsibility - CSR) ซึ่งเป็นไปตามการแปรผันของเทคโนโลยีที่มีการพัฒนาและการเข้ามามีบทบาทอย่างรวดเร็วให้ครอบคลุมถึงผลกระทบที่เกิดจากการใช้เทคโนโลยีดิจิทัลในภาคธุรกิจ (Lobschat et al., 2021) ซึ่งมุ่งเน้นให้องค์กรดำเนินกิจกรรมทางดิจิทัลอย่างมีจริยธรรมในยุคที่เทคโนโลยี ปัญญาประดิษฐ์ (Artificial Intelligence - AI) บิ๊กดาต้า (Big Data) และบล็อกเชน (Blockchain) ในการดำเนินธุรกิจ ประกอบกับรายงานของ World Economic Forum (2022) ระบุว่า องค์กรที่ละเลยการจัดการด้านการใช้ข้อมูลอย่างมีจริยธรรมหรือไม่มีความรับผิดชอบต่อทางดิจิทัลขององค์กรที่ชัดเจน อาจสูญเสียรายได้จากการถูกฟ้องร้องด้านข้อมูล คิดเป็น 4-6% ของรายได้ต่อปี ในธุรกิจที่เกี่ยวข้องโดยตรงกับผู้บริโภค

ในบริบทของประเทศไทย รัฐบาลได้กำหนดเป็นแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2566-2570 ที่มุ่งเน้นการยกระดับโครงสร้างพื้นฐานและความสามารถทางดิจิทัลของประเทศอย่างรอบด้าน โดยมีเป้าหมายให้ภาคเอกชนโดยเฉพาะภาคธุรกิจและภาคประชาชนสามารถใช้เทคโนโลยีได้อย่างปลอดภัย ยั่งยืน และมีจริยธรรม โดยมีแนวคิดความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) ที่นำมาประยุกต์ใช้ โดยเฉพาะการคุ้มครองข้อมูล การใช้ปัญญาประดิษฐ์อย่างมีความรับผิดชอบ และการลดช่องว่างทางดิจิทัล ซึ่งเป็นยุทธศาสตร์สำคัญของแผนดังกล่าว (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2566) มีองค์ประกอบสำคัญได้แก่

1. จริยธรรมทางดิจิทัลและความรับผิดชอบต่อด้านปัญญาประดิษฐ์ (Digital Ethics & AI Responsibility) คือ การพัฒนาปัญญาประดิษฐ์อย่างมีความรับผิดชอบ มีความเป็นกลางในการประมวลผลข้อมูลที่สำคัญกับความโปร่งใสตรวจสอบได้
2. ความเป็นส่วนตัวของข้อมูลและความปลอดภัยทางไซเบอร์ (Data Privacy & Cybersecurity) เป็นการปกป้องข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยทางไซเบอร์
3. การพัฒนาดิจิทัลอย่างยั่งยืน (Sustainable Digital Development) การใช้เทคโนโลยีดิจิทัลที่เป็นมิตรกับสิ่งแวดล้อม
4. การเข้าถึงเทคโนโลยีดิจิทัลเท่าเทียม (Inclusive Digitalization) การทำให้ทุกคนสามารถเข้าถึงเทคโนโลยีดิจิทัลอย่างเท่าเทียม

จะเห็นได้ว่า ความรับผิดชอบต่อทางดิจิทัลขององค์กร เป็นองค์ประกอบสำคัญที่ช่วยให้องค์กรขับเคลื่อนในยุคดิจิทัลได้อย่างยั่งยืน ซึ่งเป็นยุคที่มีการเปลี่ยนแปลงอย่างรวดเร็วจากการพัฒนาของเทคโนโลยีแบบก้าวกระโดด องค์กรที่ไม่สามารถปรับตัวได้ทันกับบริบททางดิจิทัล อาจสูญเสียความสามารถในการแข่งขัน และหายไปจากระบบเศรษฐกิจทุนนิยมอย่างรวดเร็วแน่นอน

นอกจากบริบทในระดับนโยบายที่ส่งผลกระทบต่อสังคมในภาพรวมแล้ว แนวคิดเรื่องความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) ยังมีความสำคัญต่อการดำเนินงานภายในองค์กรด้วย โดยเฉพาะในด้านการบริหารทรัพยากรบุคคล การพัฒนาทักษะดิจิทัลของพนักงาน การกำหนดนโยบายความปลอดภัยของข้อมูลภายใน การส่งเสริมวัฒนธรรมองค์กรที่คำนึงถึงจริยธรรมทางดิจิทัล ตลอดจนการจัดการความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยี ซึ่งแนวทางดังกล่าวสะท้อนให้เห็นว่า (Corporate Digital Responsibility - CDR) มิได้เป็นเพียงแนวคิดระดับนโยบาย แต่ยังเป็นภารกิจเชิงกลยุทธ์และการจัดการเชิงปฏิบัติภายในองค์กรอย่างแท้จริง

ความแตกต่างระหว่างความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) กับ ความรับผิดชอบต่อสังคมขององค์กร (Corporate Social Responsibility - CSR)

ความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) มีรากฐานจากพัฒนาการของความรับผิดชอบต่อสังคมขององค์กร (Corporate Social Responsibility - CSR) โดยมีแนวคิดที่แตกต่างกันอย่างมีนัยสำคัญในเชิงบริบทกับประเด็นที่ให้ความสำคัญ โดยความรับผิดชอบต่อสังคมขององค์กร (Corporate Social Responsibility - CSR) จะเน้นการดำเนินธุรกิจที่คำนึงถึงสังคม

ชุมชน และสิ่งแวดล้อมในภาพรวม ในขณะที่ความรับผิดชอบทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) จะมุ่งเน้นเฉพาะสิ่งที่เกิดขึ้นจากการใช้งานเทคโนโลยีดิจิทัล เช่น ความโปร่งใสในการใช้ข้อมูล การใช้ปัญญาประดิษฐ์อย่างมีจริยธรรม ความปลอดภัยทางไซเบอร์ ตลอดจนการเข้าถึงเทคโนโลยีอย่างเป็นธรรม ซึ่งแนวคิดความรับผิดชอบทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) ไม่ได้มีเพียงแต่การขยายความจากความรับผิดชอบต่อสังคมขององค์กร (Corporate Social Responsibility - CSR) เท่านั้น แต่ยังเป็นการปรับทิศทางให้เท่าทันต่อขับเคลื่อนบนพื้นฐานของการเปลี่ยนแปลงของสังคมดิจิทัล โดยองค์กรต้องพิจารณาทั้งผลกระทบภายนอกและการจัดการภายในที่เกี่ยวข้องกับการใช้เทคโนโลยีอย่างเป็นระบบและมีความรับผิดชอบเพื่อให้การดำเนินการดังกล่าวช่วยให้ขับเคลื่อนองค์กรอยู่บนพื้นฐานของความรับผิดชอบต่ออย่างยั่งยืนต่อไป

ความสำคัญของความรับผิดชอบทางดิจิทัลขององค์กรและสังคม

เนื่องจากเทคโนโลยีดิจิทัลมีการเปลี่ยนแปลงตลอดเวลาอิทธิพลโดยตรงต่อสภาพเศรษฐกิจ สังคม และสิ่งแวดล้อม จึงทำให้การกำกับดูแลด้านดิจิทัลมีความสำคัญเพิ่มขึ้น (Oduro et al., 2024) ในปัจจุบันหลายองค์กรธุรกิจจึงให้ความสำคัญกับความรับผิดชอบทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) มีความสำคัญหลายด้านหลากหลายมิติ เช่น การสร้างความเชื่อมั่นให้กับลูกค้าและผู้มีส่วนได้ส่วนเสีย องค์กรที่มโนนโยบายความเป็นส่วนตัวที่เข้มแข็ง เช่น บริษัทแอปเปิล (Apple Inc) และบริษัทกูเกิ้ล (Google LLC) ได้รับความไว้วางใจจากผู้บริโภคมากขึ้น (Carl & Hinz, 2024) กับการลดความเสี่ยงด้านกฎหมายและการกำกับดูแล กฎหมายคุ้มครองข้อมูล เช่น ระเบียบทั่วไปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation - GDPR) ของสหภาพยุโรป รวมถึงการปกป้องข้อมูลส่วนบุคคล (Personal Data Protection Act - PDPA) ของไทย กำหนดให้องค์กรต้องปฏิบัติตามมาตรฐานด้านความปลอดภัยของข้อมูล หากบริษัทใดละเลย อาจถูกปรับเป็นจำนวนเงินมหาศาล (Cheng & Zhang, 2023) และการเพิ่มความสามารถในการแข่งขันขององค์กร องค์กรที่ดำเนินธุรกิจบนพื้นฐานของความรับผิดชอบทางดิจิทัลขององค์กรมักได้รับการยอมรับจากตลาดทุนและนักลงทุน เช่น Microsoft ที่มีการลงทุนด้าน Green IT และ จริยธรรมปัญญาประดิษฐ์ ทำให้ได้รับการสนับสนุนจากผู้ถือหุ้นและนักลงทุนที่ให้ความสำคัญกับสิ่งแวดล้อม สังคม และธรรมาภิบาล (Environmental, Social, and Governance - ESG) เป็นต้น

ปัญหา อุปสรรค และความเสี่ยงหากไม่มีความรับผิดชอบทางดิจิทัลขององค์กร

1. การละเมิดความเป็นส่วนตัวของข้อมูล เช่น การรั่วไหลของข้อมูลลูกค้าอาจส่งผลกระทบต่อความน่าเชื่อถือขององค์กร และการกระทำผิดกฎหมายที่เกี่ยวข้อง
2. การใช้ปัญญาประดิษฐ์อย่างไม่มีจริยธรรม เช่น การออกแบบอัลกอริทึมที่มีอคติอาจสร้างความเสียหายต่อภาพลักษณ์องค์กร (Scarpi & Pantano, 2024)
3. การขาดความไว้วางใจจากผู้บริโภค เช่น ผู้บริโภคเริ่มให้ความสำคัญกับความโปร่งใสทางดิจิทัล (Digital Transparency) เพิ่มขึ้น องค์กรที่ไม่มีนโยบายดังกล่าวที่จะกระทบต่อความน่าเชื่อถือตลอดจน

คุณภาพในการบริการ และความปลอดภัยของข้อมูลผู้มาใช้บริการ

4. ความเสี่ยงต่อสิ่งแวดล้อมจากเทคโนโลยีดิจิทัล เช่น ในกรณีที่ศูนย์ข้อมูล (Data center) ที่ขาดการจัดการพลังงานอย่างมีประสิทธิภาพจะส่งผลก่อให้เกิดการสร้างคาร์บอนฟุตพริ้นท์ (Carbon Footprint) ปริมาณมาก ซึ่งขัดกับเป้าหมายด้านความยั่งยืน (Cheng & Zhang, 2023)

ตัวอย่างที่เห็นได้ชัดคือกรณีของบริษัท เฟสบุ๊ก (Facebook Inc) ซึ่งถูกปรับเป็นจำนวนเงินกว่า 5 พันล้านดอลลาร์โดยคณะกรรมการการค้าสหรัฐ (Federal Trade Commission - FTC) ในปี 2019 จากเหตุการณ์การละเมิดข้อมูลส่วนบุคคลผ่านบริษัท เคมบริดจ์ อกนาไลติกา (Cambridge Analytica) ซึ่งเข้าถึงข้อมูลของผู้ใช้กว่า 87 ล้านคนโดยไม่ได้รับความยินยอม ส่งผลกระทบต่อชื่อเสียงและความไว้วางใจในระดับโลก (FTC, 2019) ดังนั้น ความรับผิดชอบทางดิจิทัลขององค์กร จึงมีความสำคัญต่อการดำเนินธุรกิจอย่างรับผิดชอบทั้งในด้าน จริยธรรม เทคโนโลยี ความเป็นส่วนตัว ความมั่นคงทางไซเบอร์ และความยั่งยืน การไม่ดำเนินการตามหลักดังกล่าวมีความเสี่ยงสูงที่จะไปสู่ปัญหาด้านกฎหมาย และความน่าเชื่อถือขององค์กร อาจส่งผลกระทบต่อผลประโยชน์ประกอบการผู้ประกอบการโดยตรง

องค์ประกอบของความรับผิดชอบทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR)

ความรับผิดชอบทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) เป็นแนวคิดที่กำกับดูแลการใช้เทคโนโลยีดิจิทัลในองค์กรให้เป็นไปอย่างมีจริยธรรมและสอดคล้องกับหลักการความยั่งยืน แบ่งเป็น 4 เสาหลัก (Pillars) ซึ่งครอบคลุมประเด็นสำคัญที่องค์กรต้องคำนึงถึง ได้แก่ (1) Digital Ethics & AI Responsibility (2) Data Privacy & Cybersecurity (3) Sustainable Digital Development และ (4) Inclusive Digitalization (Scarpi & Pantano, 2024; Mihale-Wilson et al., 2022; Cheng & Zhang, 2023; Rugeviciute & Courboulay, 2024)

1. จริยธรรมทางดิจิทัลและความรับผิดชอบต่อปัญญาประดิษฐ์ (Digital Ethics & AI Responsibility) เป็นแนวทางปฏิบัติทางจริยธรรมในการใช้ปัญญาประดิษฐ์ และเทคโนโลยีดิจิทัลมุ่งเน้นลดการมีอคติของอัลกอริทึม (Algorithmic Bias) การตัดสินใจที่ไม่โปร่งใส (Black-box AI) และการใช้งานในทางที่ผิด สอดคล้องกับ Scarpi & Pantano (2024) ได้เน้นย้ำว่าการพัฒนาปัญญาประดิษฐ์ควรให้ความสำคัญกับ “จริยธรรมปัญญาประดิษฐ์” ซึ่งรวมถึง การลดอคติ (Bias Mitigation) การออกแบบให้มีความโปร่งใส (Explainable AI) และการกำกับดูแลการใช้งานอย่างมีความรับผิดชอบ

2. ข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยทางไซเบอร์ (Data Privacy & Cybersecurity) เป็นการคุ้มครองข้อมูลและความปลอดภัยทางไซเบอร์ เนื่องจากในปัจจุบันข้อมูลดิจิทัลกลายเป็นทรัพย์สินที่มีมูลค่าสูงสุดขององค์กร และการจัดการข้อมูลอย่างไม่เหมาะสมอาจก่อให้เกิดความเสี่ยงทั้งในด้านกฎหมายและผลกระทบต่อภาพลักษณ์ขององค์กร สอดคล้องกับ Mihale-Wilson et al. (2022) ระบุว่า ความเป็นส่วนตัวของข้อมูล (Data Privacy) และความปลอดภัยของระบบสารสนเทศ (Information Security) เป็นองค์ประกอบสำคัญ องค์กรต้องมีมาตรการปกป้องข้อมูล เช่น การเข้ารหัสข้อมูล (Encryption) การควบคุมการเข้าถึง (Access Control) และการใช้เทคโนโลยีบล็อกเชน (Blockchain) เพื่อเพิ่มความโปร่งใสของข้อมูล โดยมีมาตรฐานและกฎหมายสำคัญที่เกี่ยวข้องกับความเป็นส่วนตัวของ

ข้อมูล (Data Privacy) เช่น กฎหมายคุ้มครองข้อมูลของสหภาพยุโรป (General Data Protection Regulation - GDPR) กับ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย (Personal Data Protection Act - PDPA) และ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคแห่งรัฐแคลิฟอร์เนีย ประเทศสหรัฐอเมริกา (California Consumer Privacy Act - CCPA) เป็นต้น

3. การพัฒนาดิจิทัลอย่างยั่งยืน (Sustainable Digital Development) เป็นการพัฒนาเทคโนโลยีดิจิทัลที่ยั่งยืนเป็นมิตรกับสิ่งแวดล้อมการใช้เทคโนโลยีดิจิทัลที่ไม่มีมาตรการด้านความยั่งยืนอาจส่งผลกระทบต่อสิ่งแวดล้อมโดยตรง เช่น การใช้พลังงานสูงของดาต้าเซ็นเตอร์ (Data Centers), การกำจัดขยะอิเล็กทรอนิกส์ (E-waste), และการปล่อยคาร์บอนจากโครงสร้างพื้นฐานดิจิทัล สอดคล้องกับ Cheng & Zhang (2023) ได้นำเสนอแนวคิดเกี่ยวกับเทคโนโลยีสารสนเทศสีเขียว (Green IT) และแนวปฏิบัติด้านดิจิทัลอย่างยั่งยืน (Sustainable Digital Practices) ซึ่งเน้นให้บริษัทใช้เทคโนโลยีที่ช่วยลดผลกระทบต่อสิ่งแวดล้อม เช่น การใช้พลังงานหมุนเวียนในดาต้าเซ็นเตอร์ (Renewable Energy for Data Centers) กับการพัฒนาโครงสร้างพื้นฐานระบบคลาวด์ที่เป็นมิตรต่อสิ่งแวดล้อม (Green Cloud Computing) และการออกแบบผลิตภัณฑ์เทคโนโลยีที่สามารถรีไซเคิลได้ (Sustainable Product Design) ตัวอย่างบริษัทที่ให้ความสำคัญกับการพัฒนาดิจิทัลอย่างยั่งยืน (Sustainable Digital Development) เช่น บริษัท ไมโครซอฟท์ คอร์ปอเรชั่น มุ่งสู่คาร์บอนเนกาทีฟ (Carbon Negative) การลดการปล่อยก๊าซเรือนกระจกในห่วงโซ่อุปทาน และการลงทุนในโครงการดักจับคาร์บอนภายในปี 2030 บริษัท กูเกิล จำกัด ใช้พลังงานสะอาดสำหรับดาต้าเซ็นเตอร์ (Data Centers) เป็นต้น

4. การเปลี่ยนผ่านสู่ดิจิทัลแบบครอบคลุม (Inclusive Digitalization) เป็นการเข้าถึงเทคโนโลยีดิจิทัลอย่างเท่าเทียมในหลายพื้นที่ทั่วโลก การเข้าถึงเทคโนโลยียังมีข้อจำกัด จึงต้องให้ความสำคัญกับความครอบคลุมทางดิจิทัล (Digital Inclusivity) หรือการทำให้ทุกคนสามารถเข้าถึงเทคโนโลยีอย่างเท่าเทียมกัน สอดคล้องกับ Rugeviciute & Courboulay (2024) ได้เน้นย้ำว่าการลดช่องว่างทางดิจิทัล (Digital Divide) และการส่งเสริมการรู้เท่าทันดิจิทัล (Digital Literacy) ในสังคมเป็นองค์ประกอบสำคัญ โดยเทคโนโลยีดิจิทัลไม่ควรเป็นเพียงเครื่องมือของภาคธุรกิจ แต่ต้องเป็นเครื่องมือที่ช่วยเสริมสร้างโอกาสทางเศรษฐกิจและสังคมให้กับทุกกลุ่มประชากร ตัวอย่างแนวทางที่ช่วยส่งเสริมการเปลี่ยนผ่านสู่ดิจิทัลแบบครอบคลุม (Inclusive Digitalization) เช่น การให้บริการอินเทอร์เน็ตความเร็วสูงในพื้นที่ชนบท และการออกแบบส่วนติดต่อผู้ใช้กับประสบการณ์ผู้ใช้ (User Interface - UI/ User Experience - UX) ที่เป็นมิตรกับผู้ใช้ทุกกลุ่ม กับการพัฒนาแพลตฟอร์มที่รองรับผู้พิการและผู้สูงอายุ

ดังนั้นองค์กรที่นำความรับผิดชอบต่อทางดิจิทัลขององค์กรไปใช้จะได้รับประโยชน์ทั้งในแง่ของความน่าเชื่อถือ ภาพลักษณ์ทางธุรกิจ และการปฏิบัติตามกฎหมาย ขณะที่องค์กรที่ละเลย อาจเผชิญกับความเสี่ยงด้านกฎหมาย ความเสียหายต่อชื่อเสียง และความสูญเสียอื่นที่เกี่ยวข้องในระยะยาว

ผลกระทบของความรับผิดชอบต่อทางดิจิทัลขององค์กรต่อองค์กรและสังคม

ความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) เป็นกรอบแนวคิดที่ช่วยให้องค์กรสามารถดำเนินธุรกิจบนพื้นฐานของจริยธรรมและความโปร่งใส มีบทบาทสำคัญ

ในการสร้างความน่าเชื่อถือให้กับองค์กรและสนับสนุนความยั่งยืนทางดิจิทัลในระดับสังคม (Oduro et al., 2024; Rugeviciute & Courboulay, 2024) ดังนี้

1. ช่วยเพิ่มความน่าเชื่อถือขององค์กร องค์กรที่มีนโยบายที่ชัดเจนและดำเนินการอย่างโปร่งใสสามารถสร้างความเชื่อมั่นในตราสินค้า (Brand Trust) และเสริมสร้างการรับรู้ของสาธารณชนต่อองค์กรในระยะยาว (Corporate Reputation) ซึ่งเป็นปัจจัยสำคัญที่ช่วยให้ธุรกิจสามารถแข่งขันได้ในยุคดิจิทัล (Oduro et al., 2024) ได้แก่ การบริหารข้อมูลลูกค้าและการปกป้องความเป็นส่วนตัว เป็นประเด็นสำคัญที่ส่งผลโดยตรงต่อความไว้วางใจของผู้บริโภค และการใช้ปัญญาประดิษฐ์อย่างมีความรับผิดชอบ สามารถลดปัญหาการเลือกปฏิบัติของอัลกอริทึมและเพิ่มความโปร่งใสในการตัดสินใจขององค์กร กับการลดความเสี่ยงด้านกฎหมาย เช่น การละเมิดกฎระเบียบด้านการคุ้มครองข้อมูลส่วนบุคคล ระเบียบทั่วไปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation - GDPR) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act - PDPA) ซึ่งอาจนำไปสู่ค่าปรับที่สูงและความเสียหายต่อชื่อเสียงขององค์กร

2. ความยั่งยืนทางดิจิทัล หากการพัฒนาเทคโนโลยีดิจิทัลไม่ได้คำนึงถึงความยั่งยืนอาจก่อให้เกิดผลกระทบด้านสิ่งแวดล้อม เช่น ปริมาณการใช้พลังงานที่สูงในดาต้าเซ็นเตอร์ (Data Center Energy Consumption) การกำจัดขยะอิเล็กทรอนิกส์ (E-waste) และการปล่อยก๊าซเรือนกระจก (Carbon Emission) (Rugeviciute & Courboulay, 2024)

ความรับผิดชอบต่อทางดิจิทัลขององค์กรเป็นกรอบแนวคิดทางจริยธรรม และเป็นกลไกสำคัญที่ช่วยเพิ่มความน่าเชื่อถือขององค์กรและส่งเสริมความยั่งยืนทางดิจิทัลนั่นเอง

ตัวอย่างองค์กรที่มีความรับผิดชอบต่อทางดิจิทัล

ความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) ได้กลายเป็นแนวทางสำคัญในการดำเนินธุรกิจของบริษัทชั้นนำระดับโลก รวมถึงองค์กรในประเทศไทย โดยมีเป้าหมายเพื่อเสริมสร้างความโปร่งใสด้านการใช้เทคโนโลยี ลดความเสี่ยงด้านความปลอดภัยข้อมูล และส่งเสริมความยั่งยืน (Kunz et al., 2024; Carl & Hinz, 2024; Elliott & Copilah-Ali, 2024)

1. กรณีศึกษาองค์กรข้ามชาติ เช่น บริษัท กูเกิล จำกัด มีแนวปฏิบัติด้านจริยธรรมของปัญญาประดิษฐ์และความรับผิดชอบต่ออัลกอริทึม การกำหนดแนวทางเพื่อรับรองว่าการพัฒนาและใช้งานปัญญาประดิษฐ์เป็นไปอย่างมีจริยธรรมและลดอคติของอัลกอริทึม (Kunz et al., 2024) มีมาตรการที่สำคัญ คือ (1) การพัฒนาหลักการปัญญาประดิษฐ์ของกูเกิล (Google AI Principles) ซึ่งครอบคลุมแนวทางการพัฒนาที่รับผิดชอบต่อ (2) การตรวจสอบอัลกอริทึมเพื่อป้องกันอคติในการวิเคราะห์ข้อมูล (3) การลงทุนในปัญญาประดิษฐ์ที่สามารถอธิบายได้ (Explainable AI - XAI) เพื่อให้ระบบปัญญาประดิษฐ์มีความโปร่งใสและสามารถอธิบายการทำงานของตนเองได้ (4) การสนับสนุนปัญญาประดิษฐ์เพื่อประโยชน์ทางสังคม (AI for Social Good) ซึ่งมุ่งเน้นการนำไปใช้เพื่อประโยชน์ทางสังคม เช่น การพยากรณ์ภัยพิบัติทางธรรมชาติ (Disaster Prediction) เป็นต้น

2. กรณีสึกษาองค์กรในประเทศไทย มีหลายองค์กรชั้นนำที่ได้เริ่มดำเนินการมาตรการด้านความรับผิดชอบต่อดิจิทัล โดยเฉพาะอย่างยิ่งในภาคธนาคาร โทรคมนาคม และพลังงาน (Cheng & Zhang, 2023; Keskin & Esen, 2024) เช่น ธนาคารไทยพาณิชย์ กับธนาคารกสิกรไทย ที่มีการนำมาตรฐานความเป็นส่วนตัวของข้อมูลและความมั่นคงปลอดภัยทางไซเบอร์ (Data Privacy & Cybersecurity) ไปใช้เพื่อสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act - PDPA) ของประเทศไทยใช้มาตรการการเข้ารหัสข้อมูลลูกค้า เพื่อป้องกันการโจรกรรมทางไซเบอร์ การใช้ปัญญาประดิษฐ์ในการตรวจจับธุรกรรมที่ผิดปกติ และป้องกันการฉ้อโกงทางการเงิน การพัฒนาระบบข้อมูลระดับต้นทางดิจิทัล (Digital ID) และ การพิสูจน์และยืนยันตัวตนทางอิเล็กทรอนิกส์ (e-KYC - Know Your Customer) เพื่อเพิ่มความปลอดภัยของธุรกรรมออนไลน์ และมีแนวทางการจัดการความเสี่ยงด้านไซเบอร์ ตามมาตรฐานสากล เช่น ISO/IEC 27001 ในส่วนบริษัทพลังงานและดิจิทัล บริษัท พีทีที ดิจิตอล โซลูชัน จำกัด บริษัท ทู คอร์ปอเรชั่น จำกัด และ บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) มีมาตรการขององค์กรพลังงานและโทรคมนาคมไทย เช่น (1) บริษัท พีทีที ดิจิตอล โซลูชัน จำกัด ได้นำปัญญาประดิษฐ์ และ อินเทอร์เน็ตในทุกสรรพสิ่ง มาใช้เพื่อเพิ่มประสิทธิภาพการใช้พลังงานและลดของเสียจากกระบวนการผลิต (2) บริษัท ทู คอร์ปอเรชั่น จำกัด และ บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) ดำเนินการพัฒนาเครือข่าย 5G สีเขียว (5G Green Network) ที่ใช้พลังงานน้อยลงและเป็นมิตรต่อสิ่งแวดล้อม และ (3) เอไอเอส คลาวด์พลัส (AIS Cloud+) เสนอแพลตฟอร์มการประมวลผลแบบคลาวด์ (Cloud Computing) ที่เป็นมิตรกับสิ่งแวดล้อม

ความรับผิดชอบต่อทางดิจิทัลขององค์กรจึงเป็นแนวทางที่องค์กรระดับโลกและองค์กรในไทยกำลังนำมาใช้เพื่อเพิ่มความโปร่งใสและลดความเสี่ยงในการใช้เทคโนโลยี จะเห็นได้ว่าจากกรณีสึกษาองค์กรข้ามชาติแสดงให้เห็นว่าการนำไปใช้สามารถช่วยให้องค์กรสามารถเพิ่มความไว้วางใจของลูกค้า ป้องกันปัญหาทางกฎหมาย และลดผลกระทบต่อสิ่งแวดล้อมได้ สำหรับในประเทศไทย อุตสาหกรรมการเงินและโทรคมนาคมเป็นผู้นำในการดำเนินการ โดยให้ความสำคัญกับการปกป้องข้อมูลลูกค้า ความปลอดภัยทางไซเบอร์ และความยั่งยืนของเทคโนโลยี กับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและแนวทางการกำกับดูแลดิจิทัลที่เหมาะสมจะช่วยให้องค์กรไทยสามารถสร้างความได้เปรียบในการแข่งขันและป้องกันความเสี่ยงด้านดิจิทัลในอนาคต

แนวทางการนำความรับผิดชอบต่อทางดิจิทัลขององค์กร ไปใช้ในประเทศไทย

การนำความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) มาใช้ในประเทศไทยมีความสำคัญเพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะในภาคธุรกิจที่ต้องปรับตัวให้สอดคล้องกับแนวทางการกำกับดูแลที่เข้มงวดขึ้น และการตระหนักรู้ของผู้บริโภคเกี่ยวกับ ความเป็นส่วนตัวของข้อมูล จริยธรรมทางดิจิทัล และความยั่งยืนของเทคโนโลยี (Mihale-Wilson et al., 2022; Herden et al., 2021)

1. การพัฒนารอบความรับผิดชอบต่อทางดิจิทัลขององค์กรที่เหมาะสมกับประเทศไทย องค์กรไทยหลายแห่งเริ่มกำหนดแนวทาง เพื่อใช้เป็นแนวปฏิบัติในการดำเนินงานดิจิทัลอย่างมีความรับผิดชอบต่อ โดยมีองค์ประกอบสำคัญ ดังนี้

(1) การกำกับดูแลข้อมูลและความปลอดภัยทางไซเบอร์ (Data Governance & Cybersecurity) ได้แก่ ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act - PDPA) และการปรับใช้มาตรฐานความปลอดภัยของข้อมูล เช่น ISO/IEC 27001 กับการใช้ปัญญาประดิษฐ์ และ บล็อกเชน (Blockchain) เพื่อลดความเสี่ยงด้านความปลอดภัยของข้อมูล เนื่องจากรายงานของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (Electronic Transactions Development Agency Public Organization - ETDA) (2566) พบว่า มีเหตุการณ์ข้อมูลรั่วไหลที่ถูกรายงานมากกว่า 700 เหตุการณ์ในรอบปี โดยเกือบ 30% เกิดจากการไม่มีระบบจัดเก็บข้อมูลที่ปลอดภัยเพียงพอ แต่ถ้าวองค์กรที่นำกรอบความรับผิดชอบทางดิจิทัลขององค์กรไปใช้สามารถลดความเสี่ยงด้านข้อมูลได้เฉลี่ย 30 - 40% ภายใน 2 ปี เช่นกัน (Gartner., 2022)

(2) แนวปฏิบัติด้านจริยธรรมของปัญญาประดิษฐ์และเทคโนโลยีดิจิทัล (AI & Ethical Digital Practices) ได้แก่ การพัฒนาปัญญาประดิษฐ์ที่โปร่งใส (Explainable AI - XAI) กับการลดอคติของอัลกอริทึม (Algorithmic Bias Reduction) และการสนับสนุนธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance) ผ่านการกำกับดูแลของภาครัฐและเอกชน

(3) การพัฒนาเทคโนโลยีที่ยั่งยืน (Sustainable Digital Development) ได้แก่ การสนับสนุนเทคโนโลยีสารสนเทศสีเขียว (Green IT) และระบบคลาวด์ที่ปล่อยคาร์บอนสุทธิเป็นศูนย์ (Carbon-Neutral Cloud Computing) การลดของเสียอิเล็กทรอนิกส์ (E-Waste Management) กับการใช้พลังงานสะอาดในการดำเนินธุรกิจดิจิทัล

(4) การส่งเสริมการเข้าถึงเทคโนโลยีดิจิทัลอย่างเท่าเทียม (Inclusive Digitalization) ได้แก่ การขยายโครงสร้างพื้นฐานเครือข่าย 5G และเครือข่ายอินเทอร์เน็ตความเร็วสูงแบบกว้าง (Broadband) ให้ครอบคลุมทั่วประเทศ กับการพัฒนาแพลตฟอร์มดิจิทัลที่เข้าถึงง่ายสำหรับ กลุ่มเปราะบาง เป็นต้น

2. การฝึกอบรมพนักงานเกี่ยวกับจริยธรรมดิจิทัลและความรับผิดชอบทางดิจิทัลขององค์กร

การฝึกอบรมและสร้างความเข้าใจเกี่ยวกับความรับผิดชอบทางดิจิทัลขององค์กร ในองค์กรเป็นปัจจัยสำคัญที่ช่วยให้พนักงานมีความพร้อมในการปฏิบัติตามแนวทางดิจิทัลที่มีความรับผิดชอบ (Herden et al., 2021)

แนวทางฝึกอบรมพนักงานในองค์กรของประเทศไทย

(1) การฝึกอบรมด้านความเป็นส่วนตัวและการรักษาข้อมูล ได้แก่ การให้ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและกฎหมายคุ้มครองข้อมูลในระดับสากล ฝึกอบรมการจัดการข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยทางไซเบอร์ (Data Privacy & Cybersecurity)

(2) การอบรมด้านจริยธรรมปัญญาประดิษฐ์และความรับผิดชอบของอัลกอริทึม (Algorithmic Accountability) ได้แก่ การสร้างความเข้าใจเกี่ยวกับอคติในระบบปัญญาประดิษฐ์ (Bias in AI) และผลกระทบต่อผู้ใช้งาน กับการฝึกอบรมพนักงานที่พัฒนาปัญญาประดิษฐ์ให้มีแนวทางที่โปร่งใสและเป็นธรรม

3. การสร้างวัฒนธรรมองค์กรที่คำนึงถึงความยั่งยืนของเทคโนโลยี ได้แก่ การปลูกฝังแนวคิดแนวปฏิบัติทางดิจิทัลอย่างยั่งยืน (Sustainable Digital Practices) ในกระบวนการทำงาน กับการจัดฝึกอบรมเกี่ยวกับการลดผลกระทบด้านสิ่งแวดล้อมของเทคโนโลยี

อีกทั้งจากข้อมูลของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ระบุว่า ณ ปี พ.ศ. 2566 มีองค์กรที่ขึ้นทะเบียนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เพียงประมาณ 27% ของกลุ่มเป้าหมายทั้งหมด สะท้อนให้เห็นถึงความจำเป็นเร่งด่วนในการผลักดันความรับผิดชอบทางดิจิทัลขององค์กร โดยเฉพาะองค์กรในประเทศไทยต้องพัฒนากรอบแนวความรับผิดชอบทางดิจิทัลขององค์กรที่เหมาะสมกับบริบทของประเทศ โดยเน้น การกำกับดูแลข้อมูล ความปลอดภัยไซเบอร์ จริยธรรม และการพัฒนาเทคโนโลยีอย่างยั่งยืน โดยการฝึกอบรมพนักงานจะเป็นหัวใจสำคัญของการนำไปใช้จริง เพื่อให้มั่นใจว่าการดำเนินธุรกิจดิจิทัลในประเทศไทยสอดคล้องกับมาตรฐานสากลช่วยสร้างความได้เปรียบทางการแข่งขันและความไว้วางใจจากผู้บริโภคในระยะยาว

แนวโน้มของความรับผิดชอบทางดิจิทัลขององค์กรในอนาคต

การเปลี่ยนแปลงทางเทคโนโลยีและการเติบโตของเศรษฐกิจดิจิทัลทำให้ ความรับผิดชอบทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) มีบทบาทสำคัญมากขึ้น โดยเฉพาะในประเด็นที่เกี่ยวข้องกับการกำกับดูแลปัญญาประดิษฐ์ (AI Governance) และเศรษฐกิจดิจิทัล (Digital Economy) ซึ่งมีการพัฒนาอย่างรวดเร็วและซับซ้อนมากขึ้น (Hartley et al., 2024; Wirtz et al., 2022)

1. การกำกับดูแลปัญญาประดิษฐ์ (AI Governance) และความโปร่งใสทางดิจิทัล มีความจำเป็นในการกำกับดูแล เทคโนโลยีปัญญาประดิษฐ์ ที่กำลังได้รับการพัฒนาอย่างต่อเนื่องและถูกนำมาใช้ในภาคธุรกิจหลากหลายด้าน ตั้งแต่ ระบบการแนะนำสินค้า (Recommendation Systems) ไปจนถึงปัญญาประดิษฐ์เชิงสร้างสรรค์ (Generative AI) อย่างไรก็ตาม การใช้งานปัญญาประดิษฐ์ที่ไม่มีการกำกับดูแลที่เหมาะสมอาจนำไปสู่ ปัญหาด้านจริยธรรม ความเป็นส่วนตัว และอคติของอัลกอริทึม (Hartley et al., 2024)

มีแนวทางที่องค์กรต้องคำนึงถึงในการใช้ปัญญาประดิษฐ์ อย่างมีความรับผิดชอบ ได้แก่ (1) การพัฒนา ปัญญาประดิษฐ์ที่สามารถอธิบายได้ (Explainable AI - XAI) เพื่อลดอคติและเพิ่มความโปร่งใส (2) การใช้ จริยธรรมปัญญาประดิษฐ์แนวทาง (Guidelines) ในการออกแบบและพัฒนาปัญญาประดิษฐ์ (3) การกำกับดูแลการตัดสินใจอัตโนมัติ (Automated Decision-Making) เพื่อป้องกันอคติที่เกิดจากอัลกอริทึม (Algorithmic Bias)

มาตรการระดับโลกที่เกี่ยวข้องกับธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance) ได้แก่ (1) กฎหมายปัญญาประดิษฐ์ของสหภาพยุโรปที่เน้นเรื่องความปลอดภัยและจริยธรรม (EU AI Act) (2) แนวทางสากลที่เน้นเรื่องปัญญาประดิษฐ์ ที่เป็นมิตรต่อสังคม (OECD AI Principles) และ (3) มาตรฐานด้านระบบบริหารจัดการปัญญาประดิษฐ์ (AI Management System ISO/IEC 42001)

2. บทบาทของความรับผิดชอบต่อทางดิจิทัลขององค์กร ในเศรษฐกิจดิจิทัล (Corporate Digital Responsibility in the Digital Economy) (1) ในบริบทของเศรษฐกิจดิจิทัล เศรษฐกิจดิจิทัลมีการเติบโตอย่างก้าวกระโดด โดยองค์กรต้องพึ่งพา บิ๊กดาต้า (Big Data) คลาวด์คอมพิวติ้ง (Cloud Computing) ปัญญาประดิษฐ์ และ บล็อกเชน (Blockchain) มากขึ้น ซึ่งนำไปสู่การกำกับดูแลเทคโนโลยีเหล่านี้ให้มีความรับผิดชอบต่อ (Wirtz et al., 2022) กับประเด็นสำคัญที่เกี่ยวข้องกับความรับผิดชอบต่อทางดิจิทัลขององค์กร และ เศรษฐศาสตร์ดิจิทัล ได้แก่ (1) การกำกับดูแลแพลตฟอร์มดิจิทัล (Digital Platform Governance) เช่น E-commerce, Social Media, FinTech (2) การพัฒนามาตรฐานด้านภาษีดิจิทัล (Digital Taxation) และ การแข่งขันอย่างเป็นธรรม (Fair Competition) และ (3) การสร้างโมเดลเศรษฐกิจฐานข้อมูล (Data Economy) ที่โปร่งใส เช่น จริยธรรมในการแบ่งปันข้อมูล (Data Sharing Ethics)

3. ความท้าทายของความรับผิดชอบต่อทางดิจิทัลขององค์กรในอนาคต อุปสรรคสำคัญ ที่องค์กรต้องเผชิญในอนาคต เช่น (1) ต้นทุนและการลงทุนที่สูง การพัฒนาเทคโนโลยีที่มีความรับผิดชอบต่อ เช่น เทคโนโลยีสารสนเทศสีเขียว (Green IT) หรือปัญญาประดิษฐ์ที่โปร่งใสอาจมีต้นทุนที่สูง (Hartley et al., 2024) (2) ความซับซ้อนของกฎระเบียบดิจิทัลในแต่ละประเทศ ข้อกำหนดด้านการคุ้มครองข้อมูล (Data Protection) กฎระเบียบเกี่ยวกับปัญญาประดิษฐ์ (AI Regulations) และ ภาษีดิจิทัล (Digital Tax) แตกต่างกันในแต่ละภูมิภาค ทำให้ยากต่อการปฏิบัติตามกฎระเบียบสากล (Wirtz et al., 2022) และ (3) ความขัดแย้งระหว่างนโยบายภาครัฐและภาคเอกชน บางครั้งมาตรการด้านความเป็นส่วนตัวของผู้ใช้ เช่น กฎระเบียบคุ้มครองข้อมูลส่วนบุคคลทั่วไป General Data Protection Regulation - GDPR) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act - PDPA) อาจขัดแย้งกับแนวทางการเก็บข้อมูลขององค์กรที่ต้องการใช้ปัญญาประดิษฐ์ และ บิ๊กดาต้า (Big Data) เพื่อวิเคราะห์พฤติกรรมลูกค้า

ความรับผิดชอบต่อทางดิจิทัลขององค์กรจะมีบทบาทสำคัญมากขึ้นในอนาคต โดยเฉพาะในการกำกับดูแลปัญญาประดิษฐ์ และเศรษฐกิจดิจิทัล องค์กรต้องเตรียมพร้อมสำหรับมาตรการกำกับดูแล และเทคโนโลยีดิจิทัลต้องได้รับการออกแบบให้มีความรับผิดชอบต่อ เพื่อให้เกิดความยั่งยืนและลดความเสี่ยงด้านกฎหมายและจริยธรรม นอกจากการกำกับดูแลระดับองค์กรแล้ว แนวโน้มสำคัญในอนาคต คือ การขยายแนวคิดความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility CDR) ไปสู่ระดับสังคม ผ่านแนวคิดความรับผิดชอบต่อทางดิจิทัลในระดับสังคม (Social Digital Responsibility SDR) ที่มุ่งเน้นการสร้างพลเมืองดิจิทัลที่ตระหนักรู้ มีจริยธรรม และใช้เทคโนโลยีอย่างรับผิดชอบต่อสังคม



แผนภูมิที่ 1 แสดงให้เห็นการบูรณาการขององค์ประกอบหลัก 4 ด้าน ได้แก่ การรู้เท่าทันดิจิทัล ความรับผิดชอบทางจริยธรรม พฤติกรรมทางสังคม และการมีส่วนร่วมของพลเมือง ซึ่งร่วมกันเป็นรากฐานแนวคิดของความรับผิดชอบต่อทางดิจิทัลในระดับสังคม

ข้อเสนอเพื่อการประยุกต์ใช้แนวคิดความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR)

หากพิจารณาความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) ในส่วนของกรอบแนวคิดจะพบว่ามีความครอบคลุมในหลายมิติ เช่น จริยธรรม เทคโนโลยี ความปลอดภัย และการเข้าถึงเทคโนโลยีอย่างเป็นธรรม โดยแนวคิดดังกล่าวสามารถนำไปประยุกต์ใช้ได้ทั้งในระดับปฏิบัติการและระดับนโยบายอย่างเป็นระบบ สำหรับข้อเสนอแนะนี้ได้้นำแนวคิดพื้นฐานจาก คณะกรรมาธิการยุโรป (European Commission, 2020) กับ องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD, 2021) และองค์การการศึกษา วิทยาศาสตร์ และวัฒนธรรมแห่งสหประชาชาติ (UNESCO, 2022) มาประกอบการพิจารณานำเสนอเบื้องต้น ดังนี้

1. แนวทางการประยุกต์ใช้ในระดับองค์กร

(1) การกำหนดนโยบายด้านจริยธรรมทางดิจิทัล องค์กรควรกำหนดนโยบายหรือแนวปฏิบัติ ภายในเกี่ยวกับการใช้เทคโนโลยีดิจิทัลที่เน้นความรับผิดชอบต่อ ความโปร่งใส และความเป็นธรรมต่อผู้มีส่วนได้ส่วนเสีย (European Commission, 2020)

(2) การส่งเสริมทักษะและการเรียนรู้ด้านดิจิทัลของบุคลากร ควรมีการอบรมหรือกิจกรรม พัฒนาศักยภาพบุคลากรในเรื่องเทคโนโลยีดิจิทัล ความปลอดภัยทางไซเบอร์ และจริยธรรมในการใช้ข้อมูล เพื่อเสริมสร้างความพร้อมของบุคลากรในการทำงานยุคดิจิทัลอย่างมีจริยธรรม (UNESCO, 2022)

(3) การจัดการความเสี่ยงและความปลอดภัยของข้อมูล องค์กรควรมีระบบบริหารความเสี่ยง และมาตรการป้องกันที่เหมาะสมสำหรับการใช้เทคโนโลยี โดยเฉพาะข้อมูลส่วนบุคคล ความมั่นคงของระบบ และการใช้ปัญญาประดิษฐ์อย่างรับผิดชอบ

(4) การประเมินองค์กรด้านความรับผิดชอบต่อทางดิจิทัล สนับสนุนให้มีการประเมินความพร้อมหรือดัชนีชี้วัดภายในที่เกี่ยวข้องกับองค์ประกอบของความรับผิดชอบต่อทางดิจิทัลขององค์กร เพื่อใช้ในการพัฒนาองค์กรอย่างต่อเนื่อง

2. แนวทางการสนับสนุนในระดับนโยบายสาธารณะ

(1) การจัดทำแนวปฏิบัติกลาง (Guidelines) ด้านความรับผิดชอบต่อทางดิจิทัลขององค์กร ภาครัฐควรสนับสนุนการพัฒนาแนวปฏิบัติหรือมาตรฐานกลางด้านความรับผิดชอบต่อทางดิจิทัลขององค์กรที่สามารถปรับใช้ได้ทั้งในภาคเอกชน ภาครัฐ และองค์กรภาคสังคม ซึ่งเป็นแนวทางที่หลายประเทศในยุโรปเริ่มดำเนินการ (European Commission, 2020)

(2) การกำหนดความรับผิดชอบต่อทางดิจิทัลขององค์กร ไว้ในแผนพัฒนาองค์กรภาคเอกชน และภาครัฐ ควรมีการบูรณาการความรับผิดชอบต่อทางดิจิทัลขององค์กร เข้าไว้ในแผนพัฒนาองค์กรของภาครัฐ หรือแผนงานเชิงยุทธศาสตร์ด้านดิจิทัลของประเทศ

(3) การใช้ความรับผิดชอบต่อทางดิจิทัลขององค์กร เป็นส่วนหนึ่งของตัวชี้วัดธรรมาภิบาลหรือความยั่งยืน ส่งเสริมให้องค์กรใช้ความรับผิดชอบต่อทางดิจิทัลขององค์กร เป็นเกณฑ์หนึ่งในการประเมินการดำเนินงานด้านการบริหารจัดการภาครัฐที่เน้นธรรมาภิบาลยุคดิจิทัล (OECD, 2021)

(4) การสร้างความร่วมมือระหว่างกันในทุกภาคส่วน ตลอดจนการสนับสนุนความร่วมมือระหว่างภาครัฐ ภาคเอกชน และสถาบันการศึกษา ในการพัฒนาองค์ความรู้ กับระบบสนับสนุนการดำเนินงานด้านความรับผิดชอบต่อทางดิจิทัลขององค์กรอย่างต่อเนื่อง

กล่าวได้ว่า แนวคิดความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) เป็นมากกว่ากรอบแนวคิดเชิงจริยธรรม โดยเป็นกลยุทธ์สำคัญที่องค์กรสามารถนำไปประยุกต์ใช้เพื่อสร้างความสมดุลระหว่างประสิทธิภาพของเทคโนโลยีกับความมั่นคงทางสังคมและจริยธรรม การนำความรับผิดชอบต่อทางดิจิทัลขององค์กร ให้เป็นส่วนหนึ่งของนโยบายหรือแผนพัฒนาระดับชาติ จะช่วยให้ทุกภาคส่วนสามารถดำเนินงานในองค์กรยุคดิจิทัลได้อย่างเป็นระบบ สามารถตรวจสอบได้ และรับผิดชอบต่อผู้มีส่วนได้ส่วนเสียในทุกมิติ องค์กรที่สามารถบูรณาการแนวคิดนี้ได้อย่างเป็นระบบ จะทำให้องค์กรมีความพร้อมรับมือกับการขับเคลื่อนของสังคมดิจิทัลอย่างยั่งยืนในระยะยาว

ตารางที่ 1 สรุปข้อเสนอเพื่อการประยุกต์ใช้ความรับผิดชอบทางดิจิทัลขององค์กรในระดับองค์กรและจากคณะกรรมการยุโรป (European Commission, 2020) กับ องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD, 2021) และ องค์การการศึกษา วิทยาศาสตร์ และวัฒนธรรมแห่งสหประชาชาติ (UNESCO, 2022)

ระดับข้อเสนอ	หัวข้อข้อเสนอ	เป้าหมาย/แนวทาง
ระดับองค์กร	การกำหนดนโยบายด้านจริยธรรมทางดิจิทัล	กำหนดนโยบายภายในเกี่ยวกับการใช้เทคโนโลยีอย่างมีจริยธรรมและเป็นธรรม
ระดับองค์กร	การส่งเสริมทักษะและการเรียนรู้ด้านดิจิทัลของบุคลากร	จัดอบรมและพัฒนาทักษะบุคลากรเกี่ยวกับดิจิทัล จริยธรรม และความปลอดภัยทางไซเบอร์
ระดับองค์กร	การจัดการความเสี่ยงและความปลอดภัยของข้อมูล	มีระบบบริหารความเสี่ยงและมาตรการป้องกันข้อมูล ความมั่นคง และปัญญาประดิษฐ์ที่เหมาะสม
ระดับองค์กร	การประเมินองค์กรด้านความรับผิดชอบทางดิจิทัล	สร้างดัชนีชี้วัดหรือกลไกประเมินตนเองเกี่ยวกับความรับผิดชอบทางดิจิทัลขององค์กรเพื่อพัฒนาองค์กร
ระดับนโยบาย	การจัดทำแนวปฏิบัติกลาง (Guidelines) ด้านความรับผิดชอบทางดิจิทัลขององค์กร	สนับสนุนการออกแนวปฏิบัติกลางที่ใช้ได้กับทุกองค์กร
ระดับนโยบาย	การกำหนดความรับผิดชอบทางดิจิทัลขององค์กร ในแผนพัฒนาองค์กรและภาครัฐ	บูรณาการแนวคิดความรับผิดชอบทางดิจิทัลขององค์กร ในแผนพัฒนาองค์กรและยุทธศาสตร์ดิจิทัลระดับชาติ
ระดับนโยบาย	การใช้ความรับผิดชอบทางดิจิทัลขององค์กร เป็นตัวชี้วัดธรรมาภิบาลหรือความยั่งยืน	ผลักดันความรับผิดชอบทางดิจิทัลขององค์กร ให้เป็นเกณฑ์ประเมินในระบบธรรมาภิบาล
ระดับนโยบาย	การสร้างความร่วมมือในทุกภาคส่วน	ส่งเสริมความร่วมมือภาครัฐ เอกชน และการศึกษา ในการสร้างองค์ความรู้และระบบสนับสนุนความรับผิดชอบทางดิจิทัลขององค์กร

สรุปและข้อเสนอแนะ

ความรับผิดชอบทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) ไม่ใช่เพียงแนวคิดเชิงจริยธรรม แต่ได้กลายเป็นกลยุทธ์สำคัญสำหรับองค์กรในการสร้างความยั่งยืนในยุคดิจิทัล องค์กรที่ตระหนักถึงความรับผิดชอบทางดิจิทัลขององค์กรและนำไปปรับใช้ในการดำเนินงานสามารถลดความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล ขณะที่ยังคงรักษาความไว้วางใจจากลูกค้าและผู้มีส่วนได้ส่วนเสีย

1. การใช้เทคโนโลยีอย่างมีจริยธรรมเป็นข้อได้เปรียบทางการแข่งขัน ได้แก่ (1) การจัดการข้อมูลอย่างโปร่งใสและปลอดภัยช่วยสร้างความเชื่อมั่นในตราสินค้า (Brand Trust) และลดความเสี่ยงด้านกฎหมาย (Oduro et al., 2024) กับ (2) มาตรการคุ้มครองข้อมูลส่วนบุคคลที่ดีสามารถเพิ่มความเชื่อมั่นของผู้บริโภคต่อองค์กร

2. การช่วยเพิ่มประสิทธิภาพในการบริหารจัดการองค์กร ได้แก่ (1) การออกแบบระบบดิจิทัลให้มีความรับผิดชอบ เช่น จริยธรรมปัญญาประดิษฐ์ และ ธรรมาภิบาลข้อมูลสามารถช่วยให้องค์กรทำงานได้อย่างมีประสิทธิภาพมากขึ้น (Rugeviciute & Courboulay, 2024) กับ (2) การใช้เทคโนโลยีสารสนเทศสีเขียว (Green IT) และแนวทางการเปลี่ยนผ่านสู่ดิจิทัลอย่างยั่งยืน (Sustainable Digitalization) ลดผลกระทบต่อสิ่งแวดล้อม

3. การเป็นเครื่องมือสำคัญในการบริหารความเสี่ยง ได้แก่ (1) การมีกลยุทธ์ความรับผิดชอบต่อทางดิจิทัลขององค์กร ที่แข็งแกร่งช่วยลดความเสี่ยงที่เกี่ยวข้องกับ อคติของปัญญาประดิษฐ์ (AI Bias) การรั่วไหลของข้อมูล (Data Breaches) และ การปฏิบัติตามกฎระเบียบ (Regulatory Compliance) กับ (2) ความรับผิดชอบต่อทางดิจิทัลขององค์กร ยังช่วยให้องค์กรเตรียมพร้อมรับมือกับมาตรการกำกับดูแลด้านเทคโนโลยีในอนาคต

ข้อเสนอแนะสำหรับองค์กรในประเทศไทย

1. การบูรณาการความรับผิดชอบต่อทางดิจิทัลขององค์กรเข้ากับกลยุทธ์องค์กร ได้แก่ (1) องค์กรควรมีกรอบความรับผิดชอบต่อทางดิจิทัลขององค์กร ที่สอดคล้องกับบริบทของธุรกิจไทยและมาตรฐานสากล (Mihale-Wilson et al., 2022) กับ (2) ผู้บริหารต้องผลักดันให้ความรับผิดชอบต่อทางดิจิทัลขององค์กรเป็นส่วนหนึ่งของธรรมาภิบาลขององค์กร (Corporate Governance)

2. การพัฒนาความรู้และฝึกรอบมพนักงานด้านจริยธรรมทางดิจิทัล (Digital Ethics) ได้แก่ (1) การอบรมเกี่ยวกับจริยธรรมปัญญาประดิษฐ์ ข้อมูลส่วนบุคคล (Data Privacy) และความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) เป็นสิ่งจำเป็นสำหรับองค์กรที่ใช้เทคโนโลยีดิจิทัล (Herden et al., 2021) และ (2) ส่งเสริมให้พนักงานเข้าใจถึง บทบาทของความรับผิดชอบต่อทางดิจิทัลขององค์กร (Corporate Digital Responsibility - CDR) และผลกระทบของการใช้เทคโนโลยีอย่างขาดความรับผิดชอบต่อ

3. การลงทุนในเทคโนโลยีที่ปลอดภัยและยั่งยืน ได้แก่ (1) การพิจารณาการใช้บล็อกเชน (Blockchain) และ ปัญญาประดิษฐ์เพื่อเพิ่มความโปร่งใสในการจัดการข้อมูล (Cheng & Zhang, 2023) (2) การใช้เทคโนโลยีสารสนเทศสีเขียว (Green IT) และแนวทางการยั่งยืนทางดิจิทัล (Digital Sustainability) เพื่อลดการใช้พลังงานของดาต้าเซิร์ฟเวอร์

4. การปฏิบัติตามมาตรฐานและกฎหมายด้านความรับผิดชอบต่อทางดิจิทัลขององค์กร ได้แก่ (1) การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และแนวทางการกำกับดูแลด้านปัญญาประดิษฐ์ และความรับผิดชอบต่อทางดิจิทัล (Digital Responsibility) ระดับสากล (Keskin & Esen, 2024) กับ (2) การสร้างรายการตรวจสอบการปฏิบัติตามแนวทางการรับผิดชอบต่อทางดิจิทัลขององค์กร (CDR Compliance Checklist) สำหรับธุรกิจในทุกอุตสาหกรรมต่าง

ความรับผิดชอบต่อทางดิจิทัลขององค์กรจึงเป็นความจำเป็นสำหรับองค์กรที่เติบโตอย่างยั่งยืนในยุคดิจิทัลและเป็นกลยุทธ์ที่แข็งแกร่งช่วยเพิ่มความสามารถในการแข่งขัน และสร้างความเชื่อมั่นจากผู้มีส่วนได้ส่วนเสีย หากองค์กรในประเทศไทยดำเนินมาตรการด้านความรับผิดชอบต่อทางดิจิทัลขององค์กร

อย่างจริงจัง ผ่านการพัฒนากรอบนโยบาย ฝึกอบรมพนักงาน และปฏิบัติตามกฎระเบียบที่เกี่ยวข้องแล้ว จะได้รับการพัฒนาอย่างยั่งยืนอันจะเป็นประโยชน์ต่อสังคมในภาพรวมต่อไป

บรรณานุกรม

- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2566). *แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2566-2570*. กรุงเทพฯ: สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2566). *รายงานพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย พ.ศ. 2566*. กรุงเทพฯ: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.
- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2566). *รายงานผลการดำเนินงานประจำปี 2566 ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562*. กรุงเทพฯ: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.
- Alkredes, A., Dennehy, D., Dwivedi, Y., & Roderick, S. (2024). *Corporate digital responsibility: A preliminary review*. In SaudiCIS 2024 Proceedings. Association for Information Systems. Retrieved from <https://aisel.aisnet.org/saudicis2024/48>
- Carl, K. V., & Hinz, O. (2024). What we already know about corporate digital responsibility in IS research: A review and conceptualization of potential CDR activities. *Electronic Markets*, 34(27). doi.org/10.1007/s12525-024-00708-0
- Cheng, C., & Zhang, M. (2023). Conceptualizing corporate digital responsibility: A digital technology development perspective. *Sustainability*, 15(2319). doi.org/10.3390/su15032319
- Elliott, K., & Copilah-Ali, J. (2024). Implementing corporate digital responsibility (CDR): Tackling wicked problems for the digital era: Pilot study insights. *Organizational Dynamics*, 53(101040). doi.org/10.1016/j.orgdyn.2024.101040
- European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>
- Federal Trade Commission. (2019). *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. Retrieved from <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-facebook>
- Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. *Harvard Data Science Review*, 1(1). doi.org/10.1162/99608f92.8cd550d1
- Gartner. (2022). *Top Strategic Technology Trends for 2022: Digital Responsibility*. Retrieved from <https://www.gartner.com/en/articles/top-strategic-technology-trends-for-2022>

- Hartley, N., Kunz, W., & Tarbit, J. (2024). The corporate digital responsibility (CDR) calculus: How and why organizations reconcile digital and ethical trade-offs for growth. *Organizational Dynamics*, 53(101056). doi.org/10.1016/j.orgdyn.2024.101056
- Herden, C. J., Alliu, E., Cakici, A., Cormier, T., Deguelle, C., Gambhir, S., Griffiths, C., Gupta, S., Kamani, S. R., Kiratli, Y.-S., Kispataki, M., Lange, G., Moles de Matos, L., Triperio Moreno, L., Betancourt Nunez, H. A., Pilla, V., Raj, B., Roe, J., Skoda, M., Song, Y., Ummadi, P. K., & Edinger-Schons, L. M. (2021). Corporate digital responsibility: New corporate responsibilities in the digital age. *NachhaltigkeitsManagement Forum*, 29(1), 13-29. doi.org/10.1007/s00550-020-00509-x
- Katenova, M. (2023). Corporate digital responsibility: Benefits and new opportunities. *East-West Journal of Economics and Business*, XXV(1 & 2), 77-85. Retrieved from <https://www.u-picardie.fr/eastwest/fichiers/art273.pdf>
- Keskin, H., & Esen, E. (2024). Guideline for corporate digital responsibility (CDR) in global environment. In TUBA (Ed.), *Corporate digital responsibility and sustainability: Emerging issues and future perspectives* (pp. 589-600). *Turkish Academy of Sciences*. doi.org/10.53478/TUBA.978-625-6110-04-5.ch33
- Kunz, W. H., & Wirtz, J. (2024). Corporate digital responsibility (CDR) in the age of AI: Implications for interactive marketing. *Journal of Research in Interactive Marketing*, 18(1), 31-37. doi.org/10.1108/JRIM-06-2023-0176
- Kunz, W. H., Wirtz, J., Hartley, N., & Tarbit, J. (2024). The importance of corporate digital responsibility in a digital service world. In L. Matosas-Lopez (Ed.), *The impact of digitalization on current marketing strategies* (pp. 183-193). *Emerald Publishing*. doi.org/10.1108/978-1-83753-686-320241011
- Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, 122, 875-888. doi.org/10.1016/j.jbusres.2019.10.006
- Merbecks, U. (2024). Corporate digital responsibility (CDR) in Germany: Background and first empirical evidence from DAX 30 companies in 2020. *Journal of Business Economics*, 94(1025-1049). doi.org/10.1007/s11573-023-01148-6
- Michale-Wilson, C., Hinz, O., van der Aalst, W., & Weinhardt, C. (2022). Corporate digital responsibility: Relevance and opportunities for business and information systems engineering. *Business & Information Systems Engineering*, 64(2), 127-132. doi.org/10.1007/s12599-022-00746-y

- Oduro, S., Haylemariam, L. G., & Umar, R. M. (2024). Influence of corporate digital responsibility on financial performance: The mediating role of firm reputation. *Business Ethics, the Environment & Responsibility*, 0(0), 1-15. doi.org/10.1111/beer.12766
- OECD. (2019). *OECD Principles on Artificial Intelligence*. Paris: Organisation for Economic Co-operation and Development.
- Rugeviciute, A., & Courboulay, V. (2024). *Empowering organizations for sustainable digitalization: A corporate digital responsibility maturity model approach*. ICT for Sustainability (ICT4S) 2024 Conference Preprint. HAL Archives. Retrieved from <https://hal.science/hal-04554663v1>
- Scarpi, D., & Pantano, E. (2024). "With great power comes great responsibility": Exploring the role of Corporate Digital Responsibility (CDR) for Artificial Intelligence Responsibility in Retail Service Automation (AIRRSA). *Organizational Dynamics*, 53(1), 101030. doi.org/10.1016/j.orgdyn.2024.101030
- Shaw, P., Price, R., Elliott, K., Copilah-Ali, J., Huntingford, J., & Ionescu, O. (2024). *Corporate digital responsibility (CDR): Securing our digital futures*. IEEE Standards Association White Paper. Retrieved from <https://standards.ieee.org>
- UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. Paris: United Nations Educational, Scientific and Cultural Organization.
- Wirtz, J., Kunz, W. H., Hartley, N., & Tarbit, J. (2022). Corporate digital responsibility in service firms and their ecosystems. *Journal of Service Research*, 0(0), 1-18. doi.org/10.1177/10946705221130467
- World Economic Forum. (2022). *Digital Responsibility: A framework for ethical technology use*. Retrieved from <https://www.weforum.org/agenda/2022/05/framework-for-digital-responsibility/>