



การแก้ไขเพิ่มเติมกฎหมายคุ้มครองผู้บริโภคจากการรับข้อมูลอิเล็กทรอนิกส์ ที่ไม่พึงประสงค์บนโทรศัพท์มือถือ*

AMENDMENTS TO THE CONSUMER PROTECTION LAW CONCERNING THE RECEPTION OF UNSOLICITED ELECTRONIC INFORMATION ON MOBILE PHONES

ณรงค์ ศรีสุวรรณ*, ชัดชัย กลั่นความดี

Narong Srisuwan*, Chatchai Kankwamdee

คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพธนบุรี กรุงเทพมหานคร ประเทศไทย

Faculty of Law, Bangkokthonburi University, Bangkok, Thailand

*Corresponding author E-mail: narong.sri68@gmail.com

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาปัญหาทางกฎหมายเกี่ยวกับความรับผิดชอบของรัฐและภาคเอกชนตามหลักสิทธิมนุษยชน ในกรณีที่มีการนำเข้าสู่ข้อมูลอิเล็กทรอนิกส์ซึ่งมีมาตรการป้องกันการเข้าถึงข้อมูล และเกี่ยวข้องกับมาตรการป้องกันและปราบปรามการกระทำความผิดอันเป็นการฉ้อโกงทรัพย์ รวมถึงการเข้าถึงข้อมูลส่วนบุคคลของผู้อื่นโดยมิได้รับอนุญาต เกิดความเสียหายแก่ประชาชนผู้บริโภค 2) ศึกษาแนวคิดและทฤษฎีว่าด้วยความรับผิดชอบของผู้นำเข้าสู่ข้อมูลอิเล็กทรอนิกส์โดยปราศจากความยินยอมของเจ้าของข้อมูล โดยพิจารณาหลักความรับผิดของการกระทำและความเสียหาย ปัญหาการพิสูจน์สิทธิของผู้เสียหาย 3) ศึกษาแนวคิดทางกฎหมายที่เสนอให้ธนาคารและผู้ให้บริการโทรศัพท์เคลื่อนที่ร่วมรับผิดชอบต่อผู้บริโภคในฐานะผู้ใช้บริการ มีบทบาทสำคัญในระบบธุรกรรมทางการเงินและทางอิเล็กทรอนิกส์ การวิจัยเชิงคุณภาพ โดยใช้วิธีการสังเกตการณ์และการสัมภาษณ์เชิงลึกกับกลุ่มเป้าหมายซึ่งเป็นประชาชนผู้ใช้บริการโทรศัพท์เคลื่อนที่ทั่วไปในฐานะผู้บริโภค การศึกษารวบรวมเอกสาร งานวิจัย และกฎหมายที่เกี่ยวข้องทั้งในระดับกฎหมายภายในประเทศและหลักการระหว่างประเทศ เพื่อนำข้อมูลมาวิเคราะห์ด้วยวิธีการวิเคราะห์เชิงเนื้อหา พบว่า 1) ระบบกฎหมายไทยยังขาดบทบัญญัติที่กำหนดความรับผิดชอบของรัฐไว้อย่างชัดเจนและเป็นรูปธรรมในการคุ้มครองและเยียวยาประชาชนผู้เสียหายจากการละเมิดข้อมูลอิเล็กทรอนิกส์ 2) ข้อกฎหมายในปัจจุบันยังไม่ก่อให้เกิดผลคุ้มครองต่อผู้บริโภคอย่างมีประสิทธิภาพในทางปฏิบัติ 3) แนวคิดที่รัฐกำหนดให้ธนาคารและผู้ให้บริการโทรศัพท์เคลื่อนที่เป็นผู้รับผิดชอบต่อผู้บริโภคยังไม่สอดคล้องกับหลักการชี้แนะขององค์การสหประชาชาติว่าด้วยธุรกิจกับสิทธิมนุษยชน ซึ่งกำหนดให้รัฐต้องมีบทบาทในการปกป้องสิทธิ และร่วมกับภาคเอกชนในการป้องกัน แก้ไข ฟื้นฟู และเยียวยาความเสียหายแก่ประชาชนผู้บริโภคอย่างเป็นระบบและยั่งยืน

คำสำคัญ: สิทธิมนุษยชน, ข้อมูลอิเล็กทรอนิกส์, แพลตฟอร์มดิจิทัล, อาชญากรรมทางเทคโนโลยี, ผู้บริโภค

Abstract

This research aims to: 1) examine legal issues concerning the responsibilities of the State and the private sector under human rights principles in cases involving the importation of electronic data protected by access control measures, particularly in relation to measures for the prevention and suppression of fraud offences and unauthorized access to personal data, which result in harm to consumers; 2) study legal concepts and theories regarding the liability of parties who import electronic data without the consent of data owners, with particular consideration of principles of liability for wrongful acts and damages, as well as issues related to the burden of proof and the enforcement of victims' rights; and 3) examine legal approaches proposing joint liability of banks and mobile network operators toward consumers, given their significant roles in financial and electronic transaction systems. This study employs a qualitative research methodology, using observation and in-depth interviews with a target group consisting of general mobile phone users as consumers. In addition, relevant documents, academic studies, and legal instruments at both the domestic and international levels were collected and analyzed through content analysis. The findings reveal that: 1) the Thai legal system lacks clear and concrete provisions defining the responsibilities of the State in protecting and providing remedies to consumers harmed by violations of electronic data; 2) existing legal provisions do not effectively ensure consumer protection in practice; and 3) the approach that assigns responsibility primarily to banks and mobile network operators is not fully consistent with the United Nations Guiding Principles on Business and Human Rights, which emphasize the State's duty to protect human rights and its obligation to work in cooperation with the private sector to prevent violations, address harms, and provide effective remedies and rehabilitation for affected consumers in a systematic and sustainable manner

Keywords: Human Rights, Electronic Data, Platforms, Technology Crime, Consumers

บทนำ

พัฒนาการของเทคโนโลยีสารสนเทศและการสื่อสารในประเทศไทยมีจุดเริ่มต้นสำคัญตั้งแต่ช่วงปลายทศวรรษ 2530 โดย องค์การโทรศัพท์แห่งประเทศไทย ได้สรุปว่า การพัฒนาระบบอินเทอร์เน็ตในประเทศไทยเริ่มต้นขึ้นเมื่อปี พ.ศ. 2530 จากความร่วมมือระหว่างมหาวิทยาลัยสงขลานครินทร์และสถาบันเทคโนโลยีแห่งเอเชียในการทดลองใช้งานระบบจดหมายอิเล็กทรอนิกส์ ภายใต้การสนับสนุนจากเครือรัฐออสเตรเลีย ซึ่งถือเป็นจุดเริ่มต้นของการสื่อสารอิเล็กทรอนิกส์ในประเทศไทยอย่างเป็นรูปธรรม (องค์การโทรศัพท์แห่งประเทศไทย, 2567) การพัฒนาในระยะเริ่มต้นดังกล่าวมีบทบาทสำคัญในการวางรากฐานด้านโครงสร้างพื้นฐานทางเทคโนโลยี และสร้างความตระหนักถึงศักยภาพของการสื่อสารผ่านระบบดิจิทัลในวงกว้าง ต่อมา เครือข่ายอินเทอร์เน็ตได้ขยายตัว



ไปยังสถาบันการศึกษาหลายแห่ง จนเกิดเป็นเครือข่ายที่เรียกว่า “Campus Network” และได้รับการพัฒนาอย่างต่อเนื่องเป็นระบบ “ไทยสาร” และ “ไทยเน็ต” ซึ่งช่วยให้ประเทศไทยสามารถใช้งานอินเทอร์เน็ตได้ตลอด 24 ชั่วโมง และนำไปสู่การเปิดให้บริการอินเทอร์เน็ตเชิงพาณิชย์เป็นครั้งแรกในปี พ.ศ. 2538 การเปลี่ยนผ่านดังกล่าวไม่เพียงส่งผลต่อการศึกษาและการวิจัยเท่านั้น แต่ยังเป็นจุดเปลี่ยนสำคัญที่ทำให้เทคโนโลยีอินเทอร์เน็ตเริ่มเข้ามามีบทบาทต่อภาคเศรษฐกิจและสังคมในวงกว้างมากยิ่งขึ้น จากจุดเริ่มต้นดังกล่าว สถาบันเอเน็ตได้สรุปว่า อินเทอร์เน็ตได้พัฒนาจากเครื่องมือสื่อสารเฉพาะกลุ่ม ไปสู่การเป็นเทคโนโลยีพื้นฐานที่มีอิทธิพลอย่างสูงต่อการดำเนินชีวิตประจำวัน การประกอบกิจกรรมทางเศรษฐกิจ และโครงสร้างสังคมของประเทศ (สถาบันเอเน็ต, 2567) การเข้าถึงข้อมูลข่าวสาร การทำธุรกรรมออนไลน์ และการใช้แพลตฟอร์มดิจิทัลต่าง ๆ กลายเป็นส่วนหนึ่งของชีวิตประชาชนอย่างหลีกเลี่ยงไม่ได้ ส่งผลให้ความสัมพันธ์ระหว่างประชาชนกับเทคโนโลยีมีความใกล้ชิดและซับซ้อนมากขึ้น ในบริบทดังกล่าว สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ได้ชี้ให้เห็นว่า การพัฒนาเทคโนโลยีสารสนเทศอย่างรวดเร็ว ส่งผลให้ผู้ให้บริการอินเทอร์เน็ตทั้งภาครัฐและเอกชน เช่น AIS, True และ NT เข้ามามีบทบาทสำคัญในการขยายการเข้าถึงบริการดิจิทัลสู่ประชาชน ภายใต้กรอบการกำกับดูแลของคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2566) บทบาทของผู้ให้บริการเหล่านี้มีได้จำกัดอยู่เพียงการให้บริการด้านเทคนิคเท่านั้น หากแต่ยังเกี่ยวข้องโดยตรงกับการจัดการข้อมูล การรักษาความปลอดภัยของระบบ และการคุ้มครองสิทธิของผู้ใช้บริการในโลกดิจิทัล

ขณะเดียวกัน ธนาคารแห่งประเทศไทยได้ส่งเสริมให้ภาคธุรกิจการเงินพัฒนาเทคโนโลยีทางการเงิน หรือ FinTech เพื่อรองรับพฤติกรรมผู้บริโภคที่หันมาใช้บริการออนไลน์มากขึ้น ไม่ว่าจะเป็นการใช้ Mobile Banking การชำระเงินผ่านแพลตฟอร์มดิจิทัล หรือการทำธุรกรรมทางการเงินโดยไม่ต้องพึ่งพาสาชาธนาคารแบบดั้งเดิม แนวทางดังกล่าวสอดคล้องกับกรอบ “Protect, Respect and Remedy” ขององค์การสหประชาชาติ ซึ่งกำหนดหน้าที่ของรัฐในการคุ้มครองสิทธิมนุษยชน และความรับผิดชอบของภาคธุรกิจในการเคารพสิทธิและจัดให้มีการเยียวยาเมื่อเกิดความเสียหายจากกิจกรรมทางเศรษฐกิจและเทคโนโลยี (United Nations, 2011); (ตลาดหลักทรัพย์แห่งประเทศไทย, 2567) อย่างไรก็ตามการขยายตัวของแพลตฟอร์มดิจิทัลและการใช้โทรศัพท์มือถือในการทำธุรกรรมได้ก่อให้เกิดความเสี่ยงด้านอาชญากรรมไซเบอร์เพิ่มมากขึ้น โดยเฉพาะรูปแบบการหลอกลวงผ่านอินเทอร์เน็ต เช่น SMS หลอกลวง ลิงก์ปลอม และการโจมตีแบบ Phishing ที่มุ่งขโมยข้อมูลส่วนบุคคลและข้อมูลทางการเงินของผู้ใช้บริการ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี ที่สรุปว่า ผู้บริโภคจำนวนมากตกเป็นเหยื่อการโจมตีโดยไม่รู้เท่าทัน ส่งผลให้เกิดความเสียหายทั้งในระดับบุคคล ครั้วเรือน และระบบเศรษฐกิจของประเทศ โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ระบุว่าความเสียหายจากอาชญากรรมไซเบอร์ในประเทศไทยมีมูลค่าสูงถึงหลายหมื่นล้านบาทต่อปี และมีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง (มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี, 2568) ความจำเป็นในการศึกษาประเด็นการคุ้มครองผู้บริโภคจากการรับข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์บนโทรศัพท์มือถือ เกิดขึ้นจากบริบทของสังคมไทยที่ประชาชนพึ่งพาเทคโนโลยีดิจิทัลในชีวิตประจำวันอย่างกว้างขวาง โดยเฉพาะการใช้โทรศัพท์มือถือเป็นเครื่องมือหลักในการสื่อสาร การเข้าถึงข้อมูลข่าวสาร การใช้แพลตฟอร์มโซเชียลมีเดีย และการทำธุรกรรมทางการเงินผ่านระบบออนไลน์ ความเปลี่ยนแปลงดังกล่าวมิได้เป็นเพียงการเปลี่ยนรูปแบบการใช้เทคโนโลยีเท่านั้น หากแต่สะท้อนถึงการเปลี่ยนแปลงเชิงโครงสร้างด้านพฤติกรรม

ของประชาชนที่หันมาพึ่งพาระบบดิจิทัลมากขึ้นอย่างมีนัยสำคัญ ข้อมูลจากธนาคารแห่งประเทศไทยสรุปได้ว่า ในปี พ.ศ. 2567 จำนวนผู้ใช้งาน Mobile Banking ในประเทศไทยเพิ่มขึ้นมากกว่า 30 ล้านบัญชี ซึ่งแสดงให้เห็นว่าบริการทางการเงินได้เคลื่อนย้ายจากช่องทางดั้งเดิมไปสู่แพลตฟอร์มดิจิทัลอย่างชัดเจน (ธนาคารแห่งประเทศไทย, 2567) การขยายตัวของบริการดังกล่าวช่วยเพิ่มความสะดวกและประสิทธิภาพในการเข้าถึงบริการทางการเงินของประชาชน แต่ในขณะเดียวกันก็ทำให้ประชาชนจำนวนมากต้องเผชิญกับความเสี่ยงรูปแบบใหม่ที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคลและการฉ้อโกงทางเทคโนโลยี โดยเฉพาะในกรณีการทำธุรกรรมทางการเงินเชื่อมโยงกับการรับข้อมูลอิเล็กทรอนิกส์ผ่านโทรศัพท์มือถืออย่างต่อเนื่อง สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ได้สรุปว่า ความเสี่ยงทางไซเบอร์มีแนวโน้มเพิ่มสูงขึ้นควบคู่ไปกับการขยายตัวของกิจกรรมออนไลน์ โดยเฉพาะการโจมตีในรูปแบบใหม่ที่ผสมผสานทั้งเทคนิคทางดิจิทัลและกลวิธีทางจิตวิทยา หรือที่เรียกว่า Social Engineering เช่น การแอบอ้างเป็นหน่วยงานของรัฐ ธนาคาร หรือผู้ให้บริการโทรคมนาคม เพื่อหลอกล่อให้ประชาชนเปิดเผยข้อมูลส่วนบุคคล รหัสผ่าน หรือข้อมูลทางการเงิน (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2566) กลวิธีดังกล่าวมีลักษณะซับซ้อนและแนบเนียนมากขึ้น ทำให้ประชาชนทั่วไป โดยเฉพาะผู้สูงอายุและผู้ที่มีทักษะด้านเทคโนโลยีต่ำ ตกเป็นเหยื่อได้ง่าย แม้จะไม่ได้มีเจตนาประมาทเล่นเล่อก็ตาม สถานการณ์ดังกล่าวสะท้อนให้เห็นว่า ปัญหาภัยไซเบอร์ไม่ได้เกิดจากปัจจัยทางเทคนิคเพียงอย่างเดียว แต่ยังเกี่ยวข้องกับระดับความรู้ ความเข้าใจ และความสามารถของประชาชนในการแยกแยะข้อมูลจริงและข้อมูลเท็จ การขาดความรู้เท่าทันเทคโนโลยี (digital literacy) จึงกลายเป็นช่องว่างสำคัญที่เอื้อต่อการแพร่กระจายของข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์ และทำให้ความเสียหายขยายตัวอย่างรวดเร็ว ทั้งในมิติของสิทธิส่วนบุคคล ความมั่นคงทางทรัพย์สิน และความเชื่อมั่นในระบบดิจิทัลโดยรวม ภายใต้บริบทดังกล่าว การคุ้มครองสิทธิของประชาชนในยุคดิจิทัลจึงเป็นประเด็นที่มีความท้าทายอย่างยิ่ง และไม่อาจพึ่งพามาตรการทางกฎหมายแบบเดิมได้เพียงลำพัง การกำหนดบทบาทของรัฐและภาคธุรกิจในการป้องกัน ดูแล และเยียวยาผู้บริโภคจำเป็นต้องสอดคล้องกับหลักสิทธิมนุษยชน โดยเฉพาะหลักการคุ้มครองสิทธิในความเป็นส่วนตัว สิทธิในทรัพย์สิน และสิทธิในการได้รับการเยียวยาอย่างเป็นธรรม เมื่อเกิดความเสียหายจากการใช้เทคโนโลยีดิจิทัล

ดังนั้น การศึกษาวิจัยในประเด็นการแก้ไขเพิ่มเติมกฎหมายคุ้มครองผู้บริโภคจากการรับข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์บนโทรศัพท์มือถือ จึงมีความสำคัญอย่างยิ่ง ไม่เพียงในเชิงกฎหมายเท่านั้น แต่ยังมีนัยสำคัญต่อการพัฒนานโยบายสาธารณะ การยกระดับมาตรการความปลอดภัยไซเบอร์ และการสร้างความเชื่อมั่นให้แก่ประชาชนต่อระบบบริการออนไลน์ของประเทศในระยะยาว ทั้งนี้ เพื่อให้การพัฒนาเทคโนโลยีดิจิทัลเป็นไปควบคู่กับการคุ้มครองสิทธิและศักดิ์ศรีความเป็นมนุษย์ของผู้บริโภคอย่างแท้จริง

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาปัญหากฎหมายความรับผิดชอบของรัฐ และภาคเอกชน ตามหลักสิทธิมนุษยชน เมื่อมีผู้นำเข้าข้อมูลอิเล็กทรอนิกส์ที่มีมาตรการป้องกันการเข้าถึง และมาตรการป้องกันปราบปรามการกระทำความผิดอันเป็นการฉ้อโกงทรัพย์ การเข้าถึงข้อมูลส่วนบุคคลของผู้อื่นโดยมิได้รับอนุญาต

2. เพื่อศึกษาแนวคิดและทฤษฎีความรับผิดชอบเกี่ยวกับความรับผิดชอบของผู้นำเข้าข้อมูลอิเล็กทรอนิกส์โดยปราศจากความยินยอม



3. เพื่อศึกษาแนวคิดที่ให้ธนาคารและค่ายโทรศัพท์มือถือร่วมรับผิดชอบต่อประชาชนผู้บริโภค

วิธิดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ซึ่งมีวัตถุประสงค์เพื่อทำความเข้าใจปัญหาเชิงลึกเกี่ยวกับการคุ้มครองผู้บริโภคจากการรับข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์บนโทรศัพท์มือถือ โดยมุ่งเน้นการวิเคราะห์ปัญหาในมิติทางกฎหมาย สิทธิมนุษยชน และบริบททางสังคมของผู้ได้รับผลกระทบ การเลือกใช้ระเบียบวิธีวิจัยเชิงคุณภาพช่วยให้ผู้วิจัยสามารถเข้าถึงประสบการณ์จริงของผู้บริโภค ความรู้สึก การรับรู้ และผลกระทบที่เกิดขึ้นจากการละเมิดสิทธิในชีวิตประจำวัน ซึ่งไม่สามารถอธิบายได้อย่างครบถ้วนด้วยข้อมูลเชิงปริมาณเพียงอย่างเดียว การออกแบบการวิจัยใช้วิธีการสัมภาษณ์เชิงลึกควบคู่กับการวิจัยเอกสาร เพื่อสะท้อนทั้งมุมมองของประชาชนในฐานะผู้บริโภคและโครงสร้างของระบบกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลอิเล็กทรอนิกส์ โดยกรอบแนวคิดหลักของการวิจัยอยู่ภายใต้หลักสิทธิมนุษยชนและหลักการชี้แนะว่าด้วยธุรกิจกับสิทธิมนุษยชนขององค์การสหประชาชาติ (United Nations Guiding Principles on Business and Human Rights: UNGP) ซึ่งเน้นบทบาทหน้าที่ของรัฐในการคุ้มครองสิทธิ หน้าที่ของภาคเอกชนในการเคารพสิทธิ และการจัดให้มีกลไกการเยียวยาที่มีประสิทธิภาพแก่ผู้ได้รับความเสียหายในส่วนของกระบวนการรวบรวมข้อมูลเชิงประจักษ์ ผู้วิจัยใช้วิธีการสัมภาษณ์เชิงลึกกับประชาชนทั่วไปที่ใช้บริการโทรศัพท์มือถือ มีการติดตั้งหรือใช้งานแพลตฟอร์มธนาคารบนโทรศัพท์ และเคยได้รับหรือได้รับผลกระทบจากการรับข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์ เช่น ข้อความสั้น (SMS) หรือข้อความที่มีการแนบลิงก์อิเล็กทรอนิกส์ในลักษณะหลอกลวง การคัดเลือกผู้ให้ข้อมูลเป็นไปตามหลักการคัดเลือกแบบเจาะจง (Purposive Sampling) โดยมุ่งเน้นผู้ที่มีประสบการณ์ตรงกับเหตุการณ์ดังกล่าว เพื่อให้ข้อมูลที่ได้สามารถสะท้อนปัญหา ผลกระทบ และช่องว่างของการคุ้มครองทางกฎหมายที่เกิดขึ้นจริงในทางปฏิบัติ การสัมภาษณ์ดำเนินการในลักษณะกึ่งโครงสร้าง (Semi-structured Interview) โดยผู้วิจัยจัดเตรียมประเด็นคำถามหลักไว้ล่วงหน้า แต่เปิดโอกาสให้ผู้ให้ข้อมูลสามารถอธิบายรายละเอียด ประสบการณ์ ความรู้สึก และการรับรู้ต่อบทบาทของรัฐ ธนาคาร และผู้ให้บริการโทรศัพท์เคลื่อนที่ได้อย่างอิสระ วิธีการดังกล่าวช่วยให้ผู้วิจัยได้รับข้อมูลเชิงคุณภาพที่มีความลึกซึ้ง สะท้อนมุมมองของผู้บริโภคในบริบทชีวิตจริง และสามารถเชื่อมโยงประสบการณ์ส่วนบุคคลเข้ากับโครงสร้างของระบบกฎหมายและนโยบายสาธารณะได้อย่างชัดเจน

ควบคู่กับการเก็บข้อมูลภาคสนาม ผู้วิจัยได้ดำเนินการวิจัยเอกสาร (Documentary Research) โดยรวบรวมและศึกษาวิเคราะห์เอกสารที่เกี่ยวข้องกับการรับข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์ ซึ่งมีความเชื่อมโยงกับการกระทำความผิดตามกฎหมายว่าด้วยอาชญากรรมทางเทคโนโลยี การคุ้มครองข้อมูลส่วนบุคคล และการคุ้มครองผู้บริโภค เอกสารที่นำมาศึกษาจำแนกออกเป็น 4 กลุ่ม ได้แก่

1. กฎหมายและกรอบความตกลงระหว่างประเทศด้านสิทธิมนุษยชน ซึ่งใช้เป็นฐานในการวิเคราะห์หน้าที่ของรัฐและมาตรฐานการคุ้มครองสิทธิขั้นพื้นฐานของประชาชน
2. กฎหมายต่างประเทศ โดยเฉพาะของประเทศสิงคโปร์และสหรัฐอเมริกา เพื่อใช้เป็นกรณีศึกษาเชิงเปรียบเทียบเกี่ยวกับแนวทางการกำหนดความรับผิดชอบและมาตรการคุ้มครองผู้บริโภคในบริบทดิจิทัล

3. กฎหมายภายในประเทศที่เกี่ยวข้องกับข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ และการคุ้มครองผู้บริโภค ซึ่งเป็นกรอบหลักในการวิเคราะห์ปัญหาทางกฎหมายของประเทศไทย

4. งานวิชาการ บทความวิจัย และเอกสารที่สะท้อนปรากฏการณ์ความเสียหายจากการละเมิดสิทธิมนุษยชน โดยเฉพาะสิทธิในฐานะผู้บริโภคจากการใช้เทคโนโลยีดิจิทัล

การวิเคราะห์ข้อมูลดำเนินการเป็นลำดับขั้น เริ่มจากการจำแนกและจัดระบบข้อมูลที่ได้จากการสัมภาษณ์และเอกสาร เพื่อให้สอดคล้องกับประเด็นการศึกษา จากนั้นจึงทำการวิเคราะห์เชิงเนื้อหา (Content Analysis) ของบทบัญญัติกฎหมาย แนวคิด หลักการ และทฤษฎีที่เกี่ยวข้องกับสิทธิเสรีภาพ หน้าที่ของรัฐ และความรับผิดชอบของภาคเอกชน โดยพิจารณาทั้งในเชิงโครงสร้างของกฎหมายและการบังคับใช้ในทางปฏิบัติเมื่อได้ผลการวิเคราะห์ในแต่ละส่วนแล้ว ผู้วิจัยนำข้อมูลดังกล่าวมาวิเคราะห์เชิงเปรียบเทียบและสังเคราะห์ร่วมกับหลัก UNGP เพื่อประเมินความเหมาะสม ข้อจำกัด และช่องว่างของระบบกฎหมายไทยในปัจจุบัน ท้ายที่สุด การสังเคราะห์ผลการวิจัยมุ่งเสนอแนวทางเชิงนโยบายในการปรับปรุงกฎหมายและกลไกการคุ้มครองผู้บริโภคจากการรับข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์ให้สอดคล้องกับบริบทดิจิทัลในปัจจุบัน โดยคำนึงถึงการสร้างสมดุลระหว่างการส่งเสริมการใช้เทคโนโลยีดิจิทัลกับการคุ้มครองสิทธิมนุษยชนของประชาชนอย่างเป็นระบบและยั่งยืน

ผลการวิจัย

การศึกษาวิจัยเรื่อง การแก้ไขเพิ่มเติมกฎหมายคุ้มครองผู้บริโภคจากการรับข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์บนโทรศัพท์มือถือ พบว่า ปัญหาดังกล่าวสะท้อนถึงความท้าทายเชิงโครงสร้างของระบบกฎหมายไทยในการรับมือกับความเสียหายในสังคมดิจิทัล ซึ่งมีลักษณะซับซ้อน เปลี่ยนแปลงอย่างรวดเร็ว และเกี่ยวข้องกับผู้มีส่วนได้เสียหลายฝ่าย ทั้งภาครัฐ ภาคเอกชน และประชาชนผู้บริโภค ผลการวิจัยชี้ให้เห็นว่า แม้กฎหมายไทยจะมีการพัฒนาให้ครอบคลุมเทคโนโลยีดิจิทัลมากขึ้น แต่การบังคับใช้และการกำหนดความรับผิดชอบยังไม่สามารถตอบสนองต่อรูปแบบความเสียหายที่เกิดขึ้นจริงในทางปฏิบัติได้อย่างมีประสิทธิภาพ ทั้งนี้ สามารถอธิบายผลการวิจัยให้สอดคล้องกับวัตถุประสงค์การศึกษาได้ดังต่อไปนี้

ผลการวิจัยตามวัตถุประสงค์ข้อที่ 1

มุ่งศึกษาปัญหากฎหมายเกี่ยวกับความรับผิดของรัฐและภาคเอกชนตามหลักสิทธิมนุษยชน พบว่า แม้ประเทศไทยจะมีกฎหมายหลายฉบับที่เกี่ยวข้องกับการคุ้มครองผู้บริโภค การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และการคุ้มครองข้อมูลส่วนบุคคล แต่กฎหมายเหล่านี้ยังมีลักษณะแยกส่วนและขาดการบูรณาการเชิงระบบ โดยเฉพาะในประเด็นการกำหนดความรับผิดชอบเมื่อเกิดการนำเข้าสู่ข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์ หรือการเข้าถึงข้อมูลส่วนบุคคลโดยมิได้รับอนุญาตผ่านโทรศัพท์มือถือ พบว่า กฎหมายไทยยังไม่สามารถกำหนดบทบาทหน้าที่ของรัฐได้อย่างชัดเจนในฐานะ “ผู้มีหน้าที่คุ้มครองสิทธิ” (Duty Bearer) ตามหลักสิทธิมนุษยชน กล่าวคือ แม้รัฐจะมีหน่วยงานกำกับดูแลหลายหน่วย แต่ยังขาดกลไกเชิงรุกในการป้องกันความเสียหาย การกำกับดูแลผู้ให้บริการ และการเยียวยาผู้เสียหายอย่างเป็นทางการเป็นรูปธรรม ในขณะเดียวกัน บทบาทของภาคเอกชน เช่น ผู้ให้บริการโทรศัพท์เคลื่อนที่และผู้ให้บริการแพลตฟอร์มดิจิทัล ยังถูกมองในเชิงผู้ให้บริการตามสัญญา มากกว่าผู้มีอำนาจควบคุมความเสี่ยงในระบบการสื่อสารและข้อมูล ส่งผลให้หลักสิทธิมนุษยชนยังไม่ถูก



นำมาปรับใช้เป็นการรอบในการกำหนดความรับผิดชอบอย่างแท้จริง ความไม่ชัดเจนดังกล่าวทำให้ผู้บริโภคตกอยู่ในสถานะที่ต้องแบกรับความเสี่ยงและความเสียหายเป็นหลัก ทั้งด้านทรัพย์สิน ข้อมูลส่วนบุคคล และความมั่นคงทางเศรษฐกิจ ขณะที่กลไกของรัฐยังไม่สามารถตอบสนองต่อพฤติกรรมของอาชญากรไซเบอร์ที่มีการพัฒนาอย่างต่อเนื่องได้อย่างมีประสิทธิภาพ

วัตถุประสงค์ข้อที่ 2

ได้ศึกษาแนวคิดและทฤษฎีความรับผิดชอบเกี่ยวกับการนำเข้าสู่ข้อมูลอิเล็กทรอนิกส์โดยปราศจากความยินยอมของเจ้าของข้อมูล พบว่า แนวคิดทางกฎหมายที่มุ่งเน้นความรับผิดชอบของผู้ก่อให้เกิดความเสี่ยง (Risk-based Liability) รวมถึงแนวคิดความรับผิดเชิงป้องกันและการเยียวยาผู้เสียหาย ยังไม่ได้รับการนำมาปรับใช้อย่างเป็นระบบในกฎหมายไทย ผลการวิจัยสะท้อนให้เห็นว่า ในทางปฏิบัติ การรับข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์ เช่น ข้อความสั้นหรือข้อความที่มีการแนบลิงก์หลอกลวง เป็นปัญหาที่เกิดขึ้นในวงกว้างและส่งผลกระทบต่อผู้บริโภคจำนวนมาก เมื่อผู้ใช้โทรศัพท์มือถือหลงเชื่อและดำเนินการตามข้อมูลดังกล่าว มักนำไปสู่การถูกเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลทางการเงินโดยมิชอบ อย่างไรก็ตาม กฎหมายไทยยังไม่สามารถระบุผู้รับผิดชอบได้อย่างชัดเจนไม่ว่าจะเป็นผู้นำเข้าสู่ข้อมูล ผู้ให้บริการเครือข่าย หรือผู้ที่มีบทบาทเกี่ยวข้องกับระบบประมวลผลข้อมูล ความคลุมเครือนี้ส่งผลให้ภาระการพิสูจน์ตกอยู่กับผู้เสียหายเป็นหลัก ผู้บริโภคต้องเผชิญกับความยากลำบากในการรวบรวมพยานหลักฐานและการเรียกร้องสิทธิของตนเอง ขณะเดียวกัน ผู้ที่มีศักยภาพในการควบคุมหรือป้องกันความเสี่ยงกลับไม่ต้องรับผิดชอบในระดับที่เหมาะสม ผลการวิจัยชี้ให้เห็นว่า ระบบกฎหมายไทยยังขาดแรงจูงใจเชิงโครงสร้างที่จะผลักดันให้เกิดการป้องกันความเสียหายล่วงหน้าอย่างจริงจัง

วัตถุประสงค์ข้อที่ 3

ซึ่งศึกษาความเหมาะสมของแนวคิดในการกำหนดให้ธนาคารและผู้ให้บริการโทรศัพท์เคลื่อนที่ร่วมรับผิดชอบกับผู้บริโภค พบว่า แนวคิดดังกล่าวยังไม่ถูกนำมาปรับใช้ในกฎหมายไทยอย่างสอดคล้องกับหลักการชี้แนะขององค์การสหประชาชาติว่าด้วยธุรกิจกับสิทธิมนุษยชน (UN Guiding Principles on Business and Human Rights: UNGP) ในทางปฏิบัติ ความรับผิดชอบของธนาคารและผู้ให้บริการโทรศัพท์มือถือยังคงจำกัดอยู่ในกรอบของสัญญาหรือเงื่อนไขการให้บริการ ซึ่งมักมีลักษณะเอื้อประโยชน์ต่อผู้ให้บริการมากกว่าผู้บริโภค บทบาทของหน่วยงานเหล่านี้ในฐานะผู้ให้บริการโครงสร้างพื้นฐานด้านข้อมูลและระบบการเงิน ซึ่งมีศักยภาพในการป้องกันตรวจสอบ และลดความเสี่ยง กลับไม่ได้รับการสะท้อนอย่างชัดเจนในกฎหมาย ส่งผลให้การคุ้มครองผู้บริโภคไม่สอดคล้องกับระดับความเสี่ยงที่ประชาชนต้องเผชิญในชีวิตประจำวัน ยังพบว่า การขาดกรอบความรับผิดชอบร่วมกันระหว่างรัฐและภาคเอกชน ก่อให้เกิดความเหลื่อมล้ำในการเข้าถึงการเยียวยาความเสียหาย ผู้บริโภคจำนวนมากไม่สามารถเรียกร้องสิทธิได้อย่างมีประสิทธิภาพ และต้องรับภาระความเสียหายทางเศรษฐกิจด้วยตนเอง

โดยสรุป ผลการวิจัยชี้ให้เห็นว่า กฎหมายไทยยังมีช่องว่างสำคัญในการคุ้มครองผู้บริโภคจากการรับข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์ ทั้งในด้านการป้องกัน การกำหนดความรับผิด และการเยียวยา หากไม่มีการปรับปรุงกฎหมายให้สอดคล้องกับหลัก UNGPs และบริบทของสังคมดิจิทัลในปัจจุบัน ย่อมมีความเสี่ยงที่ผู้บริโภคจะยังคงถูกละเมิดสิทธิมนุษยชน และได้รับความเสียหายทางเศรษฐกิจอย่างต่อเนื่องในระยะยาว

อภิปรายผล

ผลการวิจัยสะท้อนว่ากฎหมายไทยยังไม่สามารถรองรับความซับซ้อนของภัยคุกคามทางดิจิทัลที่เปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะด้านความรับผิดของรัฐและภาคเอกชนเมื่อเกิดการนำเข้าสู่ข้อมูลอิเล็กทรอนิกส์ โดยมีขอบ การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต และรูปแบบการฉ้อโกงออนไลน์ที่มีความหลากหลายมากขึ้น ประเด็นนี้สอดคล้องกับงานของ สุพัตรา ศรีสวัสดิ์ ที่สรุปชี้ให้เห็นว่าโครงสร้างกฎหมายไทยยังคงให้ความสำคัญกับการแก้ไขเหตุหลังเกิดความเสียหาย มากกว่าการพัฒนากลไกป้องกันล่วงหน้า ทำให้ผู้บริโภคอยู่ในสถานะเสี่ยงสูงในการใช้งานแพลตฟอร์มดิจิทัลและบริการทางการเงินออนไลน์ (สุพัตรา ศรีสวัสดิ์, 2566) ข้อค้นพบนี้ยังได้รับการสนับสนุนจากรายงานของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งระบุว่าความเสียหายจากอาชญากรรมไซเบอร์ในประเทศไทยเพิ่มสูงขึ้นอย่างต่อเนื่อง สะท้อนให้เห็นถึงประสิทธิภาพในการคุ้มครองผู้บริโภคที่ยังไม่เพียงพอในปัจจุบัน ด้านความรับผิดตามหลักสิทธิมนุษยชน ผลการวิเคราะห์พบว่าการบูรณาการหลักการ UN Guiding Principles on Business and Human Rights (UNGPs) เข้ากับระบบกฎหมายไทยยังอยู่ในระดับจำกัด แม้หลักการดังกล่าวจะระบุให้รัฐมีหน้าที่ในการคุ้มครองประชาชน และกำหนดให้ภาคธุรกิจต้องรับผิดชอบต่อผลกระทบที่เกิดขึ้นต่อผู้ใช้บริการงานของ Ramasastry, A. ที่สรุปว่าประเทศที่นำ UNGPs ไปใช้ในเชิงนโยบาย เช่น สหภาพยุโรปและออสเตรเลีย สามารถยกระดับความปลอดภัยดิจิทัลและลดข้อพิพาทระหว่างผู้บริโภคกับภาคธุรกิจได้อย่างมีประสิทธิภาพ ซึ่งแตกต่างจากประเทศไทยที่ยังขาดการกำหนดความรับผิดร่วมระหว่างหน่วยงานรัฐ ราชการ และค่ายโทรศัพท์มือถืออย่างเป็นระบบ (Ramasastry, A., 2015) ประเด็นเกี่ยวกับความรับผิดของผู้นำเข้าสู่ข้อมูลอิเล็กทรอนิกส์โดยไม่ได้รับความยินยอมพบว่ามีผลสอดคล้องกับงานของ มาลีทอง พันธุ์สกุล ที่สรุปว่ากฎหมายไทยยังไม่มีมาตรฐานที่ชัดเจนสำหรับหน้าที่ของผู้ควบคุมข้อมูล (Data Controller) และมาตรฐานการคุ้มครองข้อมูลยังไม่เข้มแข็งพอ ส่งผลให้ประชาชนไม่ได้รับความคุ้มครองเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล (มาลีทอง พันธุ์สกุล, 2565) ข้อค้นพบนี้ยังได้รับการสนับสนุนจากงานของ วรวิทย์ ปัญจพร ที่สรุปให้เห็นว่ากฎหมายไทยยังไม่สามารถรับมือกับภัยไซเบอร์ที่ซับซ้อน เช่น การหลอกลวงผ่าน SMS ฟิชซิง หรือการใช้บัญชีม้า ทั้งที่เป็นรูปแบบที่แพร่หลายมากในปัจจุบัน ซึ่งสะท้อนให้เห็นถึงความจำเป็นในการยกระดับมาตรฐานด้านความปลอดภัยอย่างเร่งด่วน ในส่วนของความรับผิดร่วมของธนาคารและผู้ให้บริการโทรคมนาคม ผลการศึกษาชี้ว่าโครงสร้างปัจจุบันยังปล่อยให้ผู้บริโภคเป็นฝ่ายรับความเสี่ยงเกือบทั้งหมด ซึ่งต่างจากมาตรฐานสากล เช่น กฎระเบียบ GDPR ของสหภาพยุโรปที่กำหนดให้ผู้ให้บริการดิจิทัลและธนาคารต้องดำเนินมาตรการป้องกันเชิงรุก และต้องชดใช้ความเสียหายหากเกิดเหตุละเมิดข้อมูลจากความบกพร่องของระบบ (วรวิทย์ ปัญจพร, 2564) ดังนั้นภาคธุรกิจดิจิทัลควรมีการระร่วมในการคุ้มครองข้อมูลผู้ใช้ เพื่อไม่ให้เกิดความเสี่ยงเชิงโครงสร้างต่อระบบการเงินและสังคมดิจิทัลโดยรวม เมื่อเปรียบเทียบกับงานวิจัยอื่นในสาขาความปลอดภัยไซเบอร์และกฎหมายเทคโนโลยี โดยเฉพาะประเด็นเกี่ยวกับความจำเป็นในการกำหนดความรับผิดร่วม การพัฒนามาตรการป้องกันเชิงรุก และการยกระดับมาตรฐานความปลอดภัยให้สอดคล้องกับหลักสิทธิมนุษยชนสากล ภาพรวมของข้ออภิปรายชี้ให้เห็นว่า ประเทศไทยควรเร่งปรับปรุงกฎหมายและระบบกำกับดูแลด้านเทคโนโลยีให้ทันต่อพลวัตของภัยคุกคามออนไลน์ เพื่อสร้างความปลอดภัยให้แก่ผู้บริโภคและเสริมสร้างความเชื่อมั่นในระบบดิจิทัลของประเทศ



สรุปและข้อเสนอแนะ

การแก้ไขเพิ่มเติมกฎหมายคุ้มครองผู้บริโภคจากการรับข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์บนโทรศัพท์มือถือ สามารถสรุปได้ว่า ระบบกฎหมายไทยในปัจจุบันยังไม่สามารถรองรับความซับซ้อนของภัยคุกคามในสังคมดิจิทัลได้อย่างเพียงพอ โดยเฉพาะในประเด็นความรับผิดชอบของรัฐ ธนาคาร และผู้ให้บริการโทรคมนาคม เมื่อเกิดการนำเข้าสู่ข้อมูลอิเล็กทรอนิกส์โดยมิชอบ การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต หรือการฉ้อโกงผ่านระบบออนไลน์และโทรศัพท์มือถือ แม้ประเทศไทยจะมีกฎหมายหลายฉบับที่เกี่ยวข้องกับการคุ้มครองผู้บริโภค การป้องกันอาชญากรรมทางเทคโนโลยี และการคุ้มครองข้อมูลส่วนบุคคล แต่กฎหมายเหล่านี้ยังมีลักษณะกระจัดกระจาย และมุ่งเน้นการแก้ไขปัญหาภายหลังเกิดความเสียหาย มากกว่าการออกแบบกลไกเชิงป้องกันล่วงหน้า (preventive mechanisms) ที่สามารถลดความเสี่ยงก่อนที่ผู้บริโภคจะตกเป็นเหยื่อ ความไม่เชื่อมโยงกันของกฎหมายและหน่วยงานที่เกี่ยวข้อง ส่งผลให้การกำกับดูแลขาดประสิทธิภาพ และไม่สามารถรับมือกับพฤติกรรมของอาชญากรไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็วได้อย่างทันที่ ผลการวิจัยยังชี้ให้เห็นว่า ระบบกฎหมายไทยยังขาดกรอบที่กำหนด “ความรับผิดชอบ” (shared responsibility) ของหน่วยงานที่มีบทบาทสำคัญในระบบดิจิทัล ไม่ว่าจะเป็นรัฐในฐานะผู้กำหนดนโยบายและผู้คุ้มครองสิทธิ ธนาคารในฐานะผู้ดูแลระบบธุรกรรมทางการเงิน หรือผู้ให้บริการโทรคมนาคมในฐานะผู้ควบคุมโครงสร้างพื้นฐานด้านการสื่อสารและข้อมูล ความรับผิดชอบของหน่วยงานเหล่านี้ยังคงถูกจำกัดอยู่ในกรอบสัญญาหรือข้อกำหนดการให้บริการเป็นรายกรณี ส่งผลให้ผู้บริโภคต้องแบกรับความเสี่ยงและภาระความเสียหายด้วยตนเองเป็นหลัก เพื่อยกระดับประสิทธิภาพของระบบคุ้มครองผู้บริโภคในยุคดิจิทัล ประเทศไทยควรเร่งปรับปรุงกฎหมายและมาตรการกำกับดูแลให้สอดคล้องกับพฤติกรรมการใช้เทคโนโลยีของประชาชนในปัจจุบัน โดยควรกำหนดภาระหน้าที่ของธนาคารและผู้ให้บริการโทรคมนาคมให้มีความชัดเจนมากยิ่งขึ้น ทั้งในด้านการป้องกันความเสี่ยง การตรวจสอบความผิดปกติ และการร่วมรับผิดชอบเมื่อเกิดความเสียหายจากการละเมิดข้อมูลหรือการฉ้อโกงออนไลน์ นอกจากนี้ ควรพัฒนามาตรการเชิงรุกควบคู่ไปกับการบังคับใช้กฎหมาย เช่น การจัดให้มีระบบกรองข้อความและลิงก์อิเล็กทรอนิกส์ที่มีความเสี่ยง การตรวจจับธุรกรรมทางการเงินที่ผิดปกติแบบเรียลไทม์ และระบบแจ้งเตือนผู้ใช้บริการทันทีเมื่อพบพฤติกรรมที่อาจก่อให้เกิดความเสียหาย มาตรการเหล่านี้ควรถูกกำหนดให้เป็นหน้าที่ตามกฎหมายหรือมาตรฐานขั้นต่ำที่ผู้ให้บริการต้องปฏิบัติตาม ไม่ใช่เพียงมาตรการโดยสมัครใจ ในขณะเดียวกัน การคุ้มครองผู้บริโภคไม่อาจอาศัยกลไกทางกฎหมายและเทคโนโลยีเพียงอย่างเดียว การส่งเสริมความรู้เท่าทันดิจิทัล (digital literacy) ในกลุ่มประชาชนยังคงเป็นปัจจัยสำคัญในการลดความเสี่ยงขั้นพื้นฐาน รัฐควรมีบทบาทในการสนับสนุนการให้ความรู้แก่ประชาชนเกี่ยวกับการรับมือกับข้อมูลอิเล็กทรอนิกส์ที่ไม่พึงประสงค์ การรู้เท่าทันกลโกงออนไลน์ และการปกป้องข้อมูลส่วนบุคคลของตนเองอย่างโดยสรุป การคุ้มครองผู้บริโภคในยุคดิจิทัลจำเป็นต้องอาศัยการทำงานร่วมกันอย่างเป็นระบบระหว่างรัฐ ภาครัฐ ภาคธุรกิจ และสังคมในภาพรวม ไม่ใช่เพียงการบังคับใช้กฎหมายภายหลังเกิดเหตุเท่านั้น การสร้างระบบความปลอดภัยดิจิทัลที่มีประสิทธิภาพจึงต้องผสมทั้งมาตรการทางกฎหมาย เทคโนโลยี และการพัฒนาทักษะของผู้ใช้งาน เพื่อให้ประชาชนสามารถใช้เทคโนโลยีดิจิทัลได้อย่างปลอดภัย มีความเชื่อมั่น และได้รับการคุ้มครองสิทธิมนุษยชนอย่างแท้จริงในระยะยาว

เอกสารอ้างอิง

- ตลาดหลักทรัพย์แห่งประเทศไทย. (2567). หลักการ UNGP และธุรกิจกับสิทธิมนุษยชน. เรียกใช้เมื่อ 20 สิงหาคม 2568 จาก <https://setsustainability.com>
- ธนาคารแห่งประเทศไทย. (2567). ความก้าวหน้าด้านการเงินดิจิทัลในประเทศไทย. เรียกใช้เมื่อ 22 สิงหาคม 2568 จาก <https://www.bot.or.th>
- มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี. (2568). Phishing Mail และภัยคุกคามออนไลน์. เรียกใช้เมื่อ 19 สิงหาคม 2568 จาก <https://www.kmutt.ac.th>
- มาลีทอง พันธุ์สกุล. (2565). การละเมิดข้อมูลส่วนบุคคลและความรับผิดทางกฎหมายในยุคดิจิทัล. กรุงเทพมหานคร: มหาวิทยาลัยธรรมศาสตร์.
- วรวิทย์ ปัญจพร. (2564). กฎหมายคอมพิวเตอร์และความท้าทายในการบังคับใช้. (พิมพ์ครั้งที่ 5). กรุงเทพมหานคร: สำนักพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.
- สถาบันแอนเน็ต. (2567). ประวัติความเป็นมาของอินเทอร์เน็ตในประเทศไทย. เรียกใช้เมื่อ 20 สิงหาคม 2568 จาก <https://www.anet.net.th>
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2566). รายงานสถานการณ์อาชญากรรมไซเบอร์ของประเทศไทย. เรียกใช้เมื่อ 22 สิงหาคม 2568 จาก <https://www.kmutt.ac.th>
- สุพัตรา ศรีสวัสดิ์. (2566). การคุ้มครองผู้บริโภคจากภัยไซเบอร์ในประเทศไทย. กรุงเทพมหานคร: สถาบันกฎหมายและสังคม.
- องค์การโทรศัพท์แห่งประเทศไทย. (2567). ประวัติการใช้อินเทอร์เน็ตในประเทศไทย. เรียกใช้เมื่อ 22 สิงหาคม 2568 จาก <https://www.tot.co.th>
- Ramasastri, A. (2015). Corporate social responsibility versus business and human rights: Bridging the gap between responsibility and accountability. *Journal of Human Rights*, 14(2), 237-259.
- United Nations. (2011). Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework. New York: United Nations.