

รายงานการประเมินผลสัมฤทธิ์ของ
พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓

ส่วนที่ ๑
ข้อมูลเบื้องต้น

๑. หน่วยงานผู้รับผิดชอบการประเมินผลสัมฤทธิ์ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.....

๒. หน่วยงานผู้บังคับใช้กฎหมาย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.....

๓. ผู้รักษาการตามกฎหมาย รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.....

๔. เหตุแห่งการประเมินผลสัมฤทธิ์ (ตอบได้มากกว่า ๑ ข้อ)

ครบรอบระยะเวลาที่กำหนด

ได้รับหนังสือร้องเรียนหรือข้อเสนอแนะจากผู้เกี่ยวข้องในเรื่อง (ระบุเรื่องที่ได้รับ
การร้องเรียนหรือมีข้อเสนอแนะ).....

ได้รับข้อเสนอแนะจากคณะกรรมการพัฒนากฎหมายในเรื่อง (ระบุเรื่องที่ได้รับ
การเสนอแนะให้ประเมิน).....

อื่น ๆ คือ.....

๕. วันที่มีเหตุแห่งการประเมินผลสัมฤทธิ์ ๑ มกราคม ๒๕๖๘ โดยประเมินผลที่เกิดจากการบังคับ
ใช้กฎหมายตั้งแต่วันที่ ๑๙ เมษายน ๒๕๖๓ ถึงวันที่ ๓๑ ธันวาคม ๒๕๖๗.....

๖. รายชื่อกฎที่เป็นส่วนหนึ่งของการประเมินผลสัมฤทธิ์ในรายงานฉบับนี้

๑. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษา ความมั่นคง
ปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓.....

๒. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษา ความมั่นคง
ปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๔.....

๓. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษา ความมั่นคง
ปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๗.....

๗. รายชื่อกฎที่ดำเนินการประเมินผลสัมฤทธิ์เป็นการเฉพาะ (ประเมินผลสัมฤทธิ์เป็นรายฉบับ
ตามแบบรายงานการประเมินผลสัมฤทธิ์ของกฎ) ไม่มี.....

ส่วนที่ ๒

การวิเคราะห์ความจำเป็นและผลกระทบของกฎหมาย

๘. กฎหมายนี้มีวัตถุประสงค์เพื่อแก้ปัญหาใด

พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ มีเหตุผลในการประกาศใช้ คือ โดยที่ปัจจุบันได้เกิดสถานการณ์การระบาดของโรคติดเชื้อไวรัสโคโรนา ๒๐๑๙ ในหลายประเทศทั่วโลกรวมทั้งประเทศไทย มีจำนวนผู้ติดเชื้อที่ต้องเข้ารับการรักษาพยาบาลและเสียชีวิตจากโรคดังกล่าวเป็นจำนวนมากเนื่องจากติดเชื้อได้ง่าย องค์การอนามัยโลกจึงได้ประกาศให้เป็นภาวะการแพร่ระบาดใหญ่ทั่วโลก และขณะนี้ยังไม่มีแนวทางการรักษาที่ชัดเจน ทำให้รัฐบาลต้องใช้มาตรการที่เข้มข้นเพื่อควบคุมการระบาดของโรคตามคำแนะนำขององค์การอนามัยโลก โดยเฉพาะอย่างยิ่ง การเว้นระยะห่างทางสังคม (social distancing) อันส่งผลกระทบต่อประสิทธิภาพและความต่อเนื่องในการบริหารราชการแผ่นดิน ตลอดจนการประกอบกิจกรรมทางเศรษฐกิจของภาคเอกชนอย่างรุนแรง ดังจะเห็นได้จากกรณีที่บริษัทต่าง ๆ ต้องเลื่อนประชุมใหญ่สามัญผู้ถือหุ้นออกไปโดยไม่มีกำหนด ในขณะที่จำเป็นอย่างยิ่งที่ภาคเอกชนต้องปรับเปลี่ยนอย่างรวดเร็วและฉับพลันเพื่อตอบสนองต่อสภาพการณ์ทางเศรษฐกิจที่ชะลอตัวลงอย่างทันทีทันใด ทำให้การปฏิบัติงานของภาครัฐและการประกอบกิจกรรมในทางเศรษฐกิจของเอกชนเกือบทุกภาคส่วน ซึ่งต้องมีการประชุมเพื่อปรึกษาหารือกันเป็นปกติต้องดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์.....

พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ฯ จึงเป็นกฎหมายกลางเกี่ยวกับการประชุมผ่านสื่ออิเล็กทรอนิกส์ที่มีวัตถุประสงค์เพื่อกำหนดให้การประชุมที่มีกฎหมายบัญญัติให้ต้องมีการประชุม สามารถดำเนินการประชุมผ่านสื่ออิเล็กทรอนิกส์ได้ และได้รับการรับรองว่าเป็นการประชุมที่ชอบด้วยกฎหมาย หากการประชุมได้ใช้ระบบควบคุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ที่เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ ที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด กำหนดให้การส่งหนังสือเชิญประชุมและเอกสารประกอบการประชุม สามารถส่งโดยจดหมายอิเล็กทรอนิกส์ก็ได้ กำหนดหน้าที่ขั้นต่ำของผู้มีหน้าที่จัดการประชุมผ่านสื่ออิเล็กทรอนิกส์ และกำหนดรองรับการจ่ายเบี้ยประชุมหรือค่าตอบแทนไม่ว่าจะเรียกว่าอย่างไรให้แก่ผู้ร่วมประชุมผ่านสื่ออิเล็กทรอนิกส์.....

๙. มาตรการสำคัญที่ทำให้บรรลุวัตถุประสงค์ของกฎหมายนี้ คือ

พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ ได้กำหนดกลไกอันเป็นมาตรการสำคัญเพื่อให้บรรลุวัตถุประสงค์ของกฎหมาย ดังนี้

๙.๑. บทนิยาม (มาตรา ๔)

(๑) “การประชุมผ่านสื่ออิเล็กทรอนิกส์” หมายความว่า การประชุมที่กฎหมายบัญญัติให้ต้องมีการประชุมที่ได้กระทำผ่านสื่ออิเล็กทรอนิกส์ โดยผู้ร่วมประชุมมิได้อยู่ในสถานที่เดียวกันและสามารถประชุมปรึกษาหารือและแสดงความคิดเห็นระหว่างกันได้ผ่านสื่ออิเล็กทรอนิกส์

(๒) “ผู้ร่วมประชุม” หมายความว่า ประธานกรรมการ รองประธานกรรมการ กรรมการ อนุกรรมการ เลขานุการ และผู้ช่วยเลขานุการของคณะกรรมการ คณะอนุกรรมการ

หรือคณะบุคคลอื่นตามที่กฎหมายกำหนด และให้หมายความรวมถึงผู้ซึ่งต้องชี้แจงแสดงความคิดเห็น ต่อคณะกรรมการ คณะอนุกรรมการ หรือคณะบุคคลนั้นด้วย

๙.๒ ขอบเขตการใช้บังคับของกฎหมาย (มาตรา ๕)

พระราชกำหนดนี้ไม่ใช้บังคับแก่

- (๑) การประชุมของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา
- (๒) การประชุมเพื่อจัดทำคำพิพากษาหรือคำสั่งของศาล
- (๓) การประชุมเพื่อดำเนินการตามกระบวนการจัดซื้อจัดจ้างของส่วนราชการ ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานอื่นของรัฐ
- (๔) การประชุมอื่นตามที่กำหนดในกฎกระทรวง (ปัจจุบันยังไม่มีกฎกระทรวงในเรื่องนี้)

๙.๓ การจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์

(๑) การประชุมผ่านสื่ออิเล็กทรอนิกส์ต้องเป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด โดยประกาศในราชกิจจานุเบกษา (มาตรา ๗)

(๒) การส่งหนังสือเชิญประชุมและเอกสารประกอบการประชุม จะส่งโดยจดหมายอิเล็กทรอนิกส์ก็ได้ ในกรณีนี้ ผู้มีหน้าที่จัดการประชุมต้องจัดเก็บสำเนาหนังสือเชิญประชุมและเอกสารประกอบการประชุมไว้เป็นหลักฐาน โดยจะจัดเก็บในรูปข้อมูลอิเล็กทรอนิกส์ก็ได้ (มาตรา ๘)

(๓) ในการประชุมผ่านสื่ออิเล็กทรอนิกส์ ผู้มีหน้าที่จัดการประชุมต้อง (มาตรา ๙)

- จัดให้ผู้ร่วมประชุมแสดงตนเพื่อร่วมประชุมผ่านสื่ออิเล็กทรอนิกส์ ก่อนร่วมการประชุม
- จัดให้ผู้ร่วมประชุมสามารถลงคะแนนได้ ทั้งการลงคะแนนโดยเปิดเผยและการลงคะแนวลับ
- จัดทำรายงานการประชุมเป็นหนังสือ
- จัดให้มีการบันทึกเสียงหรือทั้งเสียงและภาพ แล้วแต่กรณี ของผู้ร่วมประชุมทุกคน ตลอดระยะเวลาที่มีการประชุมในรูปข้อมูลอิเล็กทรอนิกส์ เว้นแต่เป็นการประชุมลับ
- จัดเก็บข้อมูลจรรยาจริอิเล็กทรอนิกส์ของผู้ร่วมประชุมทุกคนไว้เป็นหลักฐาน

๙.๔ การจ่ายเบี้ยประชุมหรือค่าตอบแทนอื่น (มาตรา ๑๐)

ในการประชุมผ่านสื่ออิเล็กทรอนิกส์ หากมีกรณีที่ต้องจ่ายเบี้ยประชุมหรือค่าตอบแทนไม่ว่าจะเรียกว่าอย่างไรให้แก่ผู้ร่วมประชุม ให้จ่ายเบี้ยประชุมหรือค่าตอบแทนนั้นให้แก่ผู้ร่วมประชุมซึ่งได้แสดงตนเข้าร่วมประชุมผ่านสื่ออิเล็กทรอนิกส์ด้วย

๙.๕ ผลทางกฎหมายของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (มาตรา ๑๑)

ให้ถือว่าการประชุมผ่านสื่ออิเล็กทรอนิกส์ตามพระราชกำหนดนี้เป็นการประชุมโดยชอบด้วยกฎหมาย และห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์ตามพระราชกำหนดนี้เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใดเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

๑๐. กฎหมายนี้มีบทบัญญัติกำหนดให้ประชาชนต้องกระทำการหรืองดเว้นกระทำการอย่างไร
อย่างหนึ่งหรือไม่ อย่างไร

ไม่มี

๑๑. กฎหมายนี้ยังมีความจำเป็นและสอดคล้องกับสภาพการณ์ พัฒนาการของเทคโนโลยี และวิถีชีวิต
ของประชาชนหรือไม่ เพียงใด

ด้วยความเจริญก้าวหน้าทางเทคโนโลยีในปัจจุบันทำให้การประชุมไม่จำกัดรูปแบบเพียง
การประชุม ณ สถานที่จัดประชุม ซึ่งผู้เข้าร่วมประชุมต้องมาอยู่ต่อหน้าในสถานที่เดียวกันอีกต่อไป
โดยการประชุมสามารถดำเนินการได้โดยการใช้สื่ออิเล็กทรอนิกส์ผ่านการประชุมทางไกลผ่านระบบ
จอภาพในรูปแบบ Video Conference ซึ่งผู้เข้าร่วมการประชุมไม่ต้องมาอยู่ต่อหน้ากันและไม่ต้อง
อยู่ในสถานที่เดียวกันทุกคน ทำให้เกิดความสะดวกในการประชุมมากขึ้น เนื่องจากผู้เข้าร่วม
การประชุมไม่ต้องเดินทางมาประชุมในสถานที่เดียวกันแต่ก็สามารถประชุมปรึกษาหารือกันได้
ซึ่งในภาคเอกชนมีการใช้การประชุมในรูปแบบนี้อย่างแพร่หลายเป็นปกติ และมีการให้บริการระบบ
การประชุมผ่านสื่ออิเล็กทรอนิกส์หลายรายทั้งในรูปแบบที่มีค่าใช้จ่ายและไม่มีค่าใช้จ่ายเพิ่มเติม
ที่สามารถใช้บริการได้โดยง่ายผ่านทางโทรศัพท์เคลื่อนที่ซึ่งเป็นอุปกรณ์อิเล็กทรอนิกส์ที่ประชาชน
ทั่วไปมีใช้งานในชีวิตประจำวันอย่างปกติ ดังนั้น พระราชกำหนดว่าด้วยการประชุมผ่านสื่อ
อิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ ซึ่งเป็นกฎหมายที่สนับสนุนให้การประชุมที่กฎหมายกำหนดให้ต้อง
มีการประชุม สามารถดำเนินการประชุมผ่านสื่ออิเล็กทรอนิกส์ได้ จึงมีความสอดคล้องกับสภาพการณ์
พัฒนาการของเทคโนโลยี และวิถีชีวิตของประชาชน ที่การประชุมผ่านสื่ออิเล็กทรอนิกส์เป็นเรื่องปกติ
ในสังคม

๑๒. ประโยชน์ที่ประชาชนได้รับจากการมีกฎหมายนี้ คือ

พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ ทำให้ประเทศไทย
มีกฎหมายที่ทันสมัยและสอดคล้องกับความก้าวหน้าทางเทคโนโลยีในปัจจุบัน สร้างความมั่นใจว่า
การประชุมที่มีกฎหมายบัญญัติ หากเลือกใช้วิธีการประชุมผ่านสื่ออิเล็กทรอนิกส์ก็จะได้รับการรับรอง
ว่าเป็นการประชุมที่มีผลใช้บังคับได้ตามกฎหมาย อันเป็นการอำนวยความสะดวกให้กับทั้งภาครัฐ
และภาคเอกชนโดยการนำเทคโนโลยีมาใช้ในกระบวนการทำงานและการประกอบธุรกิจ และรองรับ
แนวทางการปฏิบัติราชการที่รองรับชีวิตและการทำงานวิถีใหม่ ที่มีแนวทางการปฏิบัติงาน
ที่ผสมผสานทั้งการปฏิบัติงานที่หน่วยงานและการปฏิบัติงานที่บ้านหรือนอกสถานที่ ตั้ง
เพื่อความยืดหยุ่น เหมาะสมกับสถานการณ์และสภาพแวดล้อมที่เปลี่ยนแปลงไป นอกจากนี้
การประชุมผ่านสื่ออิเล็กทรอนิกส์ยังช่วยประหยัดเวลาและค่าใช้จ่ายในการจัดประชุมและการเดินทาง
ไปเข้าร่วมประชุม ซึ่งเป็นการช่วยบรรเทาปัญหาการจราจร ลดการใช้กระดาษและพลังงาน และลด
มลพิษต่อสิ่งแวดล้อม

๑๓. กฎหมายนี้ก่อให้เกิดผลดังต่อไปนี้หรือไม่ อย่างไร (ให้พิจารณาตอบเฉพาะประเด็นสำคัญที่ตรงกับ
วัตถุประสงค์ของกฎหมาย โดยไม่ต้องตอบทุกประเด็นก็ได้)

- เป็นอุปสรรคต่อการดำรงชีวิตหรือการประกอบอาชีพของประชาชน

พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ ทำให้การประชุม
สามารถดำเนินการได้โดยการใช้สื่ออิเล็กทรอนิกส์ผ่านการประชุมทางไกลผ่านระบบจอภาพในรูปแบบ

Video Conference ซึ่งผู้เข้าร่วมการประชุมไม่ต้องมาอยู่ต่อหน้ากันและไม่ต้องอยู่ในสถานที่เดียวกัน ทุกคน ช่วยประหยัดเวลาและค่าใช้จ่ายในการจัดประชุมและการเดินทางไปเข้าร่วมประชุม ซึ่งเป็น การช่วยบรรเทาปัญหาการจราจร ลดการใช้กระดาษและพลังงาน และลดมลพิษต่อสิ่งแวดล้อม จึงไม่ เป็นอุปสรรคต่อการดำรงชีวิต และก่อให้เกิดความสะดวกในการประกอบอาชีพของประชาชน

- ลดความเหลื่อมล้ำและสร้างความเป็นธรรมในสังคม

พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ ทำให้ประชาชน สามารถจัดประชุมหรือเข้าถึงการประชุมได้โดยง่าย โดยเฉพาะในกรณีที่ผู้เข้าร่วมการประชุมอยู่ใน พื้นที่ที่ห่างไกลจากสถานที่จัดประชุม เนื่องจากช่วยประหยัดเวลาและค่าใช้จ่ายในการจัดประชุมและ การเดินทางไปเข้าร่วมประชุม อันเป็นการลดความเหลื่อมล้ำและสร้างความเป็นธรรมในสังคม

- เป็นอุปสรรคต่อการแข่งขันหรือการเพิ่มความสามารถในการแข่งขันของประเทศ

พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ เป็นการแสดงให้เห็นถึงศักยภาพทางเทคโนโลยีการสื่อสารของประเทศ อันเป็นการช่วยเสริมสร้างความสะดวกและ ความเชื่อมั่นในการทำธุรกิจของประเทศ ในด้านสภาพแวดล้อมด้านกฎระเบียบของประเทศที่เอื้อต่อ การเริ่มต้นและดำเนินธุรกิจ จึงไม่เป็นอุปสรรคต่อการแข่งขัน และเป็นการเพิ่มความสามารถในการ แข่งขันของประเทศ

- เป็นการพัฒนากฎหมายให้สอดคล้องกับหลักสากลและพันธกรณีระหว่างประเทศ

ไม่มี

- มีผลกระทบต่อเศรษฐกิจ สังคม สิ่งแวดล้อมหรือสุขภาพ หรือผลกระทบอื่นที่สำคัญ

ไม่มี

๑๔. มีสถิติการดำเนินคดีและการลงโทษตามกฎหมาย หรือสถิติการปฏิบัติตามและการบังคับการ ให้เป็นไปตามกฎหมายอย่างไร

ไม่มี เนื่องจากเป็นกฎหมายที่ไม่มีบทกำหนดโทษ

๑๕. มีปัญหาและอุปสรรคในการบังคับใช้กฎหมายนี้หรือไม่ อย่างไร

ในช่วงระยะแรกที่กฎหมายใช้บังคับ หน่วยงานของรัฐและเอกชนยังมีความไม่เข้าใจหรือเข้าใจ คลาดเคลื่อนเกี่ยวกับขอบเขตการใช้บังคับของกฎหมาย โดยส่วนใหญ่เป็นความไม่แน่ใจว่ากฎหมาย สามารถนำมาใช้บังคับกับการประชุมในส่วนของตนได้ทันทีหรือไม่ หรือจะต้องมีการออกระเบียบหรือ ข้อบังคับของตนเกี่ยวกับการประชุมผ่านสื่ออิเล็กทรอนิกส์ให้สอดคล้องกับกฎหมายต่างหาก ก่อนหรือไม่ นอกจากนี้ เป็นความไม่แน่ใจในเรื่องของมาตรฐานการรักษาความมั่นคงปลอดภัยของ ระบบควบคุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ว่ามาตรฐานของตนสอดคล้องตามกฎหมายหรือไม่ ซึ่งไม่ใช่ปัญหาข้อกฎหมาย

ส่วนที่ ๓
การตรวจสอบเนื้อหาของกฎหมาย

๑๖. กฎหมายนี้มีความสัมพันธ์หรือใกล้เคียงกับกฎหมายอื่นหรือไม่ อย่างไร

ปัจจุบันได้มีบทบัญญัติตามกฎหมายบางฉบับที่มีการกำหนดหลักเกณฑ์รองรับการประชุมผ่านสื่ออิเล็กทรอนิกส์ ดังนี้

(๑) พระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการได้มาซึ่งสมาชิกวุฒิสภา พ.ศ. ๒๕๖๑ และพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการเลือกตั้งสมาชิกสภาผู้แทนราษฎร พ.ศ. ๒๕๖๑ มาตรา ๗ ที่กำหนดให้คณะกรรมการการเลือกตั้งมีอำนาจประชุมผ่านสื่ออิเล็กทรอนิกส์ได้ โดยกรรมการแต่ละคนอาจอยู่ ณ สถานที่แตกต่างกันได้ หากมีความจำเป็นเร่งด่วน ซึ่งต่อมาได้มีการออกระเบียบคณะกรรมการการเลือกตั้ง ว่าด้วยหลักเกณฑ์และวิธีการประชุมของคณะกรรมการการเลือกตั้งทั่วไป และการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๑ เพื่อกำหนดรายละเอียดเกี่ยวกับหลักเกณฑ์และวิธีการรองรับการดำเนินการในเรื่องดังกล่าว

(๒) ระเบียบคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ว่าด้วยข้อบังคับการประชุมคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ พ.ศ. ๒๕๕๕ ข้อ ๒๕ วรรคสอง กำหนดให้การเข้าร่วมประชุมคณะกรรมการสามารถดำเนินการแบบทางไกลผ่านสื่อได้

(๓) ระเบียบคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ว่าด้วยการประชุม ค่าตอบแทน และค่าใช้จ่ายของคณะอนุกรรมการและคณะทำงาน พ.ศ. ๒๕๕๔ ข้อ ๑๑ กำหนดให้คณะอนุกรรมการในแต่ละคณะสามารถกำหนดวิธีการประชมนอกเหนือจากการประชุมตามปกติได้ แต่จะต้องเปิดโอกาสให้ผู้เข้าร่วมประชุมทุกคนสามารถสนทนา แลกเปลี่ยนแสดงความคิดเห็นและเห็นภาพการดำเนินการประชุมได้อย่างต่อเนื่อง

(๔) ข้อบังคับสถาบันอนุญาโตตุลาการ ว่าด้วยคณะกรรมการคณะอนุญาโตตุลาการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ข้อ ๕/๑ กำหนดว่า คณะกรรมการสถาบันอนุญาโตตุลาการอาจประชุมโดยวิธีการประชุมทางไกลผ่านจอภาพ (Video Conference) หรือผ่านโทรศัพท์ (Teleconference) หรือผ่านสื่ออิเล็กทรอนิกส์ในรูปแบบอื่นได้

(๕) พระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๘ วรรคสาม ได้กำหนดให้นายกรัฐมนตรีสามารถกำหนดวิธีการประชุมคณะรัฐมนตรีโดยวิธีอื่นใด ซึ่งผู้ร่วมประชุมสามารถปรึกษาหารือกันได้แม้จะมีได้อยู่ในสถานที่เดียวกันก็ได้

(๖) พระราชกฤษฎีกาเบี้ยประชุมกรรมการ พ.ศ. ๒๕๔๗ มาตรา ๑๔ ได้กำหนดให้สามารถใช้วิธีการติดต่อสื่อสารด้วยเทคโนโลยีที่สามารถถ่ายทอดภาพและเสียงได้อย่างต่อเนื่อง ซึ่งทำให้กรรมการหรืออนุกรรมการไม่จำเป็นต้องปรากฏตัวในที่ประชุมด้วย โดยให้ถือว่ากรรมการหรืออนุกรรมการ ซึ่งใช้วิธีการติดต่อสื่อสารด้วยเทคโนโลยีดังกล่าว ร่วมประชุมคณะกรรมการหรือคณะอนุกรรมการนั้น และมีสิทธิได้รับเบี้ยประชุม

๑๗. มีการฟ้องคดีต่อศาลรัฐธรรมนูญหรือศาลปกครอง หรือการร้องเรียนต่อผู้ตรวจการแผ่นดิน หรือคณะกรรมการสิทธิมนุษยชนแห่งชาติเกี่ยวกับกฎหมายนี้ที่เรื่องและในประเด็นใด

ไม่มี

๑๘. การใช้ระบบอนุญาต ระบบคณะกรรมการ ดุลพินิจของเจ้าหน้าที่ และโทษอาญาในกฎหมายนี้ (ถ้ามี) ยังมีความเหมาะสมอยู่หรือไม่ อย่างไร

ไม่มี

ส่วนที่ ๔

ผลการประเมินผลสัมฤทธิ์ของกฎหมาย

๑๙. การรับฟังความคิดเห็น

ได้รับฟังความคิดเห็นโดยถูกต้องตามข้อ ๕ และข้อ ๖ ของแนวทางการประเมินผลสัมฤทธิ์ของกฎหมายแล้ว

ได้รับฟังความคิดเห็นโดยวิธีอื่นนอกจากผ่านระบบกลาง

ในการประเมินผลสัมฤทธิ์ของกฎหมายฉบับนี้ ได้ใช้วิธีการรับฟังความคิดเห็นของบุคคลที่เกี่ยวข้องกับการบังคับใช้กฎหมายและผู้ที่ได้รับผลกระทบทั้งภาคราชการและภาคเอกชน โดยการรับฟังความคิดเห็นผ่านระบบกลางทางกฎหมาย (<https://www.law.go.th>) มีผู้เข้ามาให้ความคิดเห็น จำนวน ๔๓ คน และมีหนังสือสอบถามความคิดเห็นไปยังผู้เกี่ยวข้อง จำนวน ๒๐ หน่วยงาน แบ่งเป็นหน่วยงานภาครัฐ จำนวน ๑๖ หน่วยงาน หน่วยงานภาคเอกชน จำนวน ๔ หน่วยงาน โดยมีหน่วยงานให้ความเห็นเป็นหนังสือ จำนวน ๒ หน่วยงาน

ผู้เกี่ยวข้องมีความเห็นเกี่ยวกับกฎหมายนี้หรือผลกระทบของกฎหมายนี้อย่างไร

ผู้เกี่ยวข้องที่ร่วมแสดงความเห็นว่า พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ มีความเหมาะสม หรือสมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง หรือสมควรยกเลิกหรือไม่ อย่างไร

ผลการรับฟังความคิดเห็น

(๑) มีความเหมาะสม จำนวน ๒๘ คน (ร้อยละ ๖๕.๑๑)

(๒) สมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง จำนวน ๑๕ คน (ร้อยละ ๓๔.๘๘)

(๓) สมควรยกเลิก ไม่มี

นอกจากนี้ผู้เกี่ยวข้องมีความเห็นเพิ่มเติมที่น่าสนใจดังนี้

- พระราชกำหนดฯ มีความเหมาะสมทางหลักการ แต่มีความเห็นเพิ่มเติม ดังนี้ มาตรา ๙ (๒)

๑. การลงคะแนนลับ กฎหมายกำหนดให้ต้องทำได้ แต่ในทางปฏิบัติ อาจทำได้ยากและอาจใช้ต้นทุนสูง การหาระบบที่เชื่อถือได้ อาจเป็นอุปสรรคของหน่วยงานขนาดเล็ก ๒. ความเสี่ยงในการควบคุมการประชุม เนื่องจากนิยาม "ผู้ร่วมประชุม" ซึ่งบัญญัติไว้อย่างกว้างครอบคลุมถึง "ผู้ซึ่งต้องชี้แจงแสดง

ความคิดเห็น" ส่งผลให้บุคคลภายนอกมีสถานะเป็นผู้ร่วมประชุมตามกฎหมาย. กรณีดังกล่าว อาจก่อให้เกิดความเสี่ยงในการรักษาความลับของการประชุม โดยเฉพาะในวาระที่เป็นการประชุมลับ. จึงมีความจำเป็นที่ผู้จัดประชุมจะต้องมีมาตรการควบคุมสิทธิการเข้าถึง และระบบการบริหารจัดการ. เข้า-ออกห้องประชุมทางอิเล็กทรอนิกส์ที่รัดกุม. เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องล่วงรู้ข้อมูลอันเป็น ความลับได้. ๓. นิยาม "การประชุมผ่านสื่ออิเล็กทรอนิกส์" ยังไม่สอดคล้องกับบริบทการประชุม. ในปัจจุบัน. ในประเด็นที่กำหนดว่า "ผู้ร่วมประชุมมิได้อยู่ในสถานที่เดียว" จึงควรปรับปรุงด้วยคำให้. ครอบคลุมถึงกรณีที่ผู้ร่วมประชุม. อาจอยู่ในสถานที่เดียวกันหรือต่างที่กันก็ได้. เพื่อให้กฎหมายมีความ. ยืดหยุ่น.

๒.๑.๑. การยกระดับนิยามและการรองรับเทคโนโลยีอนาคต. (Future-Proofing Jurisprudence) มาตรา ๔. ให้นิยาม "การประชุมผ่านสื่ออิเล็กทรอนิกส์" ไว้ค่อนข้างกว้าง. ซึ่งเป็นข้อดี. แต่ยังคงกับกระบวนทัศน์ของ Web ๒.๐ (Video Conferencing) เพื่อให้มีความ "ทันสมัยสูงสุด". กฎหมายควรเปิดช่องทางและรับรองความชอบด้วยกฎหมายของการประชุมในรูปแบบ Immersive Technology... (Metaverse)... Decentralized... Autonomous... Organizations... (DAO)... voting systems. และการใช้ Blockchain ในการยืนยันมติที่ประชุม. ซึ่งจะช่วยให้ประเทศไทยมีกฎหมาย. ที่รองรับ Web ๓.๐. อย่างแท้จริง. การแก้ไขควรมุ่งเน้นให้ครอบคลุมถึง "สื่ออิเล็กทรอนิกส์ใด ๆ. ที่สามารถพิสูจน์ตัวตนและเจตนาได้" โดยไม่อิงกับแพลตฟอร์มกลางเพียงอย่างเดียว. ๒. การบูรณาการ. กับรัฐธรรมนูญ มาตรา ๗๗ และหลักนิติธรรมดิจิทัล. พระราชกำหนดฯ. ตราขึ้นในสถานการณ์ฉุกเฉิน. (ตามมาตรา ๑๗๒ ของรัฐธรรมนูญฯ) เพื่อความรีบด่วน. แม้จะมีศักดิ์เท่าพระราชบัญญัติ. แต่ในระยะยาว. เพื่อความสง่างามและความมั่นคงทางนิติบัญญัติ. ควรพิจารณายกระดับรายละเอียดบางประการ. หรือตราเป็นพระราชบัญญัติที่มีกระบวนการรับฟังความคิดเห็นรอบด้าน. (Public Hearing) ตามมาตรา ๗๗. อย่างสมบูรณ์. เพื่อสะท้อนความต้องการของภาคธุรกิจที่มีความซับซ้อน. (Complex Corporate Governance) ให้มี "ประสิทธิภาพสูงสุด" ๓. มาตรฐานความมั่นคงปลอดภัยไซเบอร์กับ. การคุ้มครองข้อมูลส่วนบุคคล. (Security vs. Privacy) มาตรา ๗. กำหนดให้เป็นไปตามมาตรฐาน. ที่กระทรวงดิจิทัลฯ กำหนด. และมาตรา ๙ (๔) ให้บันทึกเสียงและภาพของผู้ร่วมประชุมทุกคน. เพื่อให้ "ไม่ชัดหรือแย้ม" แต่ "สอดคล้อง" กับรัฐธรรมนูญฯ มาตรา ๓๒ (สิทธิในความเป็นอยู่ส่วนตัว) และ. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล. (PDPA) กฎหมายควรระบุให้ชัดเจนถึง "Data Retention Period" (ระยะเวลาจัดเก็บข้อมูล) และ "Data Minimization" (เก็บเท่าที่จำเป็น) ในระดับตัวบท. กฎหมายหลัก. ไม่ใช่เพียงกฎหมายลำดับรอง. เพื่อสร้างความเชื่อมั่นระดับสากล. โดยเฉพาะการประชุมลับ. (Closed Session) ที่ความลับทางการค้าหรือความมั่นคงเป็นเรื่องขอขาดขาดตาย. การบังคับบันทึก. ข้อมูลจราจรคอมพิวเตอร์ต้องสอดคล้องกับสิทธิส่วนบุคคลขั้นสูง. ๔. การจัดอุปสรรคเรื่องเขตอำนาจ. ศาลและพยานหลักฐาน. (Jurisdiction & Admissibility) มาตรา ๑๑. รับรองให้ข้อมูลอิเล็กทรอนิกส์. เป็นพยานหลักฐาน. ต้องขยายความให้ชัดเจนในเรื่อง "Digital Sovereignty" (อธิปไตยทางดิจิทัล). กรณีผู้ร่วมประชุมประชุมจากต่างประเทศหรือใช้ Server ต่างประเทศ. การปรับปรุงควรระบุให้ชัดเจนว่า. ไม่ว่า Server จะตั้งอยู่ที่ใด. หากการประชุมนั้นมีผลทางกฎหมายไทย. ให้ถือว่าการกระทำนั้นเกิดขึ้น. ในราชอาณาจักรไทยอย่างสมบูรณ์. (Deemed to occur in Thailand) เพื่อเปิดช่องว่างทางกฎหมาย. ในคดีแพ่งและอาญาระหว่างประเทศ. ซึ่งจะสร้าง "ความคล่องตัวสูงสุด" ให้นักลงทุนต่างชาติ. ๕. การพิสูจน์ตัวตน. (Authentication) ที่เหนือกว่า Username/Password มาตรา ๙ (๑) กำหนดให้. ผู้ร่วมประชุมแสดงตน. ควรแก้ไขให้รองรับมาตรฐาน Digital ID (NDID) หรือ Biometric

Authentication ขั้นสูง เป็นทางเลือกมาตรฐาน เพื่อป้องกันการสวมสิทธิ์ (Deepfake impersonation) ในการประชุมระดับสูงที่มีความเสี่ยง นี่คือการสร้าง "คุณภาพสูงสุด" ในการยืนยันเจตนาของบุคคลตามกฎหมายแพ่ง

- พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ มีความเหมาะสมแล้ว กล่าวคือ สามารถรองรับบริบทสังคมและเทคโนโลยีดิจิทัลได้อย่างเหมาะสม โดยพระราชกำหนดฉบับนี้ถูกตราขึ้นเพื่อรองรับการดำเนินงานของหน่วยงานรัฐและเอกชนในยุคดิจิทัล โดยเฉพาะสถานการณ์ที่ไม่สามารถประชุมแบบเผชิญหน้าได้ จึงช่วยให้การบริหารงานและการตัดสินใจทางกฎหมายสามารถดำเนินต่อไปได้อย่างต่อเนื่อง การสร้างความชัดเจนและความชอบด้วยกฎหมายของการประชุมออนไลน์ กฎหมายได้กำหนดให้การประชุมผ่านสื่ออิเล็กทรอนิกส์ที่ปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัย เป็นการประชุมที่ชอบด้วยกฎหมาย ลดข้อโต้แย้งเรื่องความสมบูรณ์ของมติที่ประชุม และสร้างความเชื่อมั่นให้แก่ผู้เข้าร่วมประชุม มีการกำหนดมาตรฐานความมั่นคงปลอดภัยอย่างเป็นระบบ การออกประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมหลายฉบับ แสดงให้เห็นถึงการพัฒนามาตรฐานด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง ทำให้การประชุมผ่านสื่ออิเล็กทรอนิกส์มีความปลอดภัย เหมาะสม และสามารถรับให้ทันต่อเทคโนโลยีใหม่ได้ และช่วยลดต้นทุนและเพิ่มประสิทธิภาพในการประชุม การอนุญาตให้ส่งหนังสือเชิญและเอกสารประกอบการประชุมทางอิเล็กทรอนิกส์ รวมถึงการรับรองการจ่ายเบี้ยประชุมแก่ผู้เข้าร่วมประชุมออนไลน์ ช่วยลดค่าใช้จ่ายด้านเวลา การเดินทาง และเอกสาร อีกทั้งยังเพิ่มความสะดวกและรวดเร็วในการดำเนินงาน ตลอดจนโครงสร้างกฎหมายมีความยืดหยุ่น ไม่เป็นอุปสรรคต่อการพัฒนา แม้เทคโนโลยีจะเปลี่ยนแปลงอย่างรวดเร็ว แต่พระราชกำหนดฯ วางหลักการไว้ในระดับกฎหมายกลาง และใช้ประกาศกระทรวงเป็นเครื่องมือปรับรายละเอียด จึงสามารถปรับปรุงได้โดยไม่จำเป็นต้องแก้ไขหรือยกเลิกกฎหมายหลัก ดังนั้น พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ มีความเหมาะสมสอดคล้องกับสภาพสังคมดิจิทัลและหลักความมั่นคงปลอดภัยทางกฎหมาย สมควรคงไว้ใช้ต่อไป โดยอาจปรับปรุงรายละเอียดเชิงเทคนิคผ่านกฎหมายลำดับรอง เพื่อให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีในอนาคต

- ๑. การปลดล็อกข้อกีดกันที่เป็นอุปสรรคต่อ Digital Economy (De-regulation of Section ๕) มาตรา ๕ ของพระราชกำหนดนี้ ยกเว้นการบังคับใช้กับการประชุมของ (๑) รัฐสภา (๒) การพิจารณาพิพากษาคดีของศาล และ (๓) กระบวนการจัดซื้อจัดจ้างของส่วนราชการ ฯลฯ

ด้านการจัดซื้อจัดจ้าง (Procurement) การยกเว้นใน (๓) ถือเป็น "คอขวด" (Bottleneck) ที่สำคัญที่สุด การจัดซื้อจัดจ้างภาครัฐยุคใหม่ต้องเป็น e-Procurement แบบเต็มรูปแบบ (End-to-End Digital Process) เพื่อความโปร่งใส (Transparency) และตรวจสอบได้ (Accountability) การที่กฎหมายแม่บทด้าน e-Meeting ตัดเรื่องนี้ออกไป ทำให้เกิดความลังเลในการตีความและการปฏิบัติ ควรแก้ไขให้กฎหมายนี้รองรับการประชุมคณะกรรมการตรวจรับหรือเปิดซองผ่านระบบอิเล็กทรอนิกส์ได้เต็มรูปแบบ เพื่อลดต้นทุนและเวลาตามหลัก Lean Management

ด้านตุลาการและนิติบัญญัติ แม้รัฐธรรมนูญจะให้ความเป็นอิสระแก่ศาลและรัฐสภา แต่ พระราชกำหนดนี้ควรเปิดช่องทาง (Enabling Clause) ให้หน่วยงานเหล่านี้สามารถ "เลือกใช้" (Opt-in) มาตรฐานตามกฎหมายนี้ได้ หากไม่มีกฎหมายเฉพาะของตนเองกำหนดไว้ เพื่อไม่ให้เกิดสัญญาณทางกฎหมายในกรณีฉุกเฉิน และเพื่อให้สอดคล้องกับรัฐธรรมนูญ มาตรา ๑๘๘ (อำนาจตุลาการ) และหมวด ๗ (รัฐสภา) ในมิติของการอำนวยความสะดวก

๒. การยกระดับมาตรฐานความมั่นคงปลอดภัยสู่ระดับสากล. (Enhancing Cyber Security Standards - Section ๗) มาตรา ๗ กำหนดให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลฯ (MDES) กำหนด ซึ่งเป็นการผูกติดกับประกาศกระทรวง ต้องยกระดับตัวบทกฎหมายให้รองรับ Technology Neutrality (ความเป็นกลางทางเทคโนโลยี) อย่างแท้จริง ไม่ควรยึดติดกับเทคโนโลยี ปัจจุบัน Blockchain & Distributed Ledger Technology (DLT) กฎหมายควรแก้ไขให้รองรับ การเก็บข้อมูลจราจรและการลงคะแนนเสียงผ่าน Blockchain เพื่อความโปร่งใสสูงสุดและแก้ไขไม่ได้ (Immutability) ซึ่งจะทำให้มาตรา ๙.(๒) เรื่องการลงคะแนนลับและเปิดเผย มีประสิทธิภาพและความน่าเชื่อถือเทียบเท่าระดับสากล Zero Trust Architecture การกำหนดมาตรฐานความปลอดภัยไม่ควรเป็นเพียงแค่ "การเข้ารหัส" (Encryption) แบบพื้นฐาน แต่ต้องรองรับสถาปัตยกรรมความปลอดภัยแบบ Zero Trust เพื่อป้องกันการโจมตีทางไซเบอร์ที่ซับซ้อน ซึ่งสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ

๓. การขยายขอบเขตนิยามและกระบวนการให้ครอบคลุม Future of Work (Redefining Definitions & Processes) นิยาม "ผู้ร่วมประชุม" ควรปรับปรุงให้ครอบคลุมถึง AI Participants หรือปัญญาประดิษฐ์ที่ทำหน้าที่เลขานุการจดบันทึก หรือผู้ช่วยในการวิเคราะห์ข้อมูล (Data Analytics) ระหว่างประชุม โดยให้มีสถานะทางกฎหมายที่ชัดเจนในฐานะเครื่องมือสนับสนุน "สถานที่จัดการประชุม" การแก้ไขต้องระบุให้ชัดเจนยิ่งขึ้นเกี่ยวกับการประชุมใน Metaverse หรือ Virtual Reality (VR) ว่าการแสดงตนผ่าน Avatar ที่มีการยืนยันตัวตนทางดิจิทัล (Digital ID) ระดับสูง (IAL๓/AAL๓) ถือเป็น "แสดงตน" ตามมาตรา ๙.(๑) อย่างถูกต้องตามกฎหมาย เพื่อรองรับ Web ๓.๐ การจัดเก็บข้อมูล (มาตรา ๑๐) ต้องปรับปรุงให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างเคร่งครัด โดยเฉพาะเรื่องระยะเวลาการจัดเก็บ (Retention Period) และสิทธิในการถูกลืม (Right to be Forgotten) ของผู้เข้าร่วมประชุม ในส่วนที่ไม่ขัดต่อกฎหมายจดหมายเหตุ

๔. การเพิ่มประสิทธิภาพเชิงอำนาจและการบังคับใช้ (Enforcement & Authority Agility) มาตรา ๖ และมาตรา ๘ กระบวนการแจ้งเชิญประชุมและเอกสารประกอบ ปัจจุบันยังอิงกับรูปแบบ "ไฟล์เอกสาร" (Document-based) ต้องปรับปรุงสู่ระบบ Data-Driven Meeting คือการส่ง "ชุดข้อมูล" (Data Set) แทนไฟล์ PDF เพื่อให้กรรมการสามารถนำไปวิเคราะห์ต่อได้ทันที และการเชิญประชุมผ่าน Smart Contract ที่จะ Trigger การประชุมอัตโนมัติเมื่อเงื่อนไขครบถ้วน ตัดขั้นตอนธุรการที่ไม่จำเป็น ๕. ความสอดคล้องกับรัฐธรรมนูญและหลักนิติธรรม (Constitutional & Rule of Law Compliance) การปรับปรุงกฎหมายนี้ จะต้องยืนยันหลักการตามรัฐธรรมนูญ มาตรา ๒๖ ว่าด้วยการไม่จำกัดสิทธิเสรีภาพเกินความจำเป็น และมาตรา ๗๗ ที่รัฐพึงจัดให้มีกฎหมายเพียงเท่าที่จำเป็น การแก้ไขจะทำให้กฎหมายมีความ "ยืดหยุ่น" (Flexibility) ลดภาระของประชาชนและภาคเอกชนในการปฏิบัติตามกฎระเบียบยุมหยม (Regulatory Guillotine) และทำให้การใช้อำนาจรัฐผ่านที่ประชุมมีความโปร่งใส ตรวจสอบได้ผ่าน Digital Footprint ที่สมบูรณ์

- พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ มีความเหมาะสมแล้ว และยังคงมีความจำเป็นที่จะบังคับใช้ในปัจจุบัน เนื่องจากการใช้เทคโนโลยีสำหรับการประชุมทำให้ผู้ร่วมประชุมทั้งภาครัฐและภาคเอกชนสามารถปรึกษาหารือกันผ่านสื่ออิเล็กทรอนิกส์ได้โดยสะดวก แม้จะมีได้อยู่ในสถานที่เดียวกัน เป็นการประหยัดต้นทุนและระยะเวลา ในการจัดการประชุมและการเดินทางไปร่วมประชุม อีกทั้งปัจจุบันมีเทคโนโลยีการประชุมที่มีมาตรฐาน ผ่านแพลตฟอร์ม เช่น

Zoom, Microsoft Teams, Google Meet, Webex สามารถรองรับฟังก์ชัน การแสดงตนผู้เข้าร่วม, มีการสื่อสารสองทาง (ภาพ/เสียง), สามารถเข้าถึงเอกสารได้, รองรับการลงคะแนน (เปิดเผย/ลับ), มีการจัดเก็บหลักฐานปลอดภัย ซึ่งคุณสมบัติเหล่านี้ เป็นระบบประชุมออนไลน์ (e-Meeting) ที่สอดคล้องกับการประชุมผ่านสื่ออิเล็กทรอนิกส์ตามพระราชกำหนดการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ เพื่อให้มีผลทางกฎหมาย (ผู้ให้ความคิดเห็น : กรมบังคับคดี)

- พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์และกฎหมายที่เกี่ยวข้องมีความเหมาะสมกับการประชุมตามที่กำหนดในกฎกระทรวงที่มีข้อจำกัดของจำนวนผู้เข้าร่วมประชุม และมีความยืดหยุ่นเพื่ออำนวยความสะดวกของผู้ร่วมประชุมที่อยู่ต่างสถานที่ เพิ่มประสิทธิภาพการบริหารงาน ลดค่าใช้จ่ายในการเดินทางและประหยัดเวลา นอกจากนี้ มาตรการการรักษาความมั่นคงปลอดภัยของการประชุมฯ ที่ได้ปรับปรุงประกาศ ฉบับที่ ๒ มีความเหมาะสมกับสภาพการณ์ปัจจุบัน โดยกำหนดให้การลงคะแนนเสียงมีความรัดกุมและเป็นไปตามหลักสากลมากขึ้น รวมทั้งเพิ่มระดับการรักษาความลับของการประชุมที่ส่งผลทางกฎหมาย ทั้งนี้ เห็นควรบังคับใช้พระราชกำหนดดังกล่าวต่อไป เพื่อให้การรับรองระบบการประชุมและรายงานการประชุมตามมติที่ประชุมออนไลน์ชอบด้วยกฎหมาย พัฒนาการประชุมของภาครัฐมีความถูกต้องและมั่นคงปลอดภัยที่ได้มาตรฐานสากล

- พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ มีความเหมาะสมเป็นกฎหมายกลางสำหรับการดำเนินการประชุมในปัจจุบันผ่านสื่ออิเล็กทรอนิกส์ เนื่องจากกฎหมายฉบับนี้ ให้การรับรองทางกฎหมาย สอดคล้องกับบริบทการทำงานของหน่วยงานภาครัฐและเอกชน ในยุคดิจิทัลที่ต้องการความคล่องตัว ลดข้อจำกัดด้านเวลา สถานที่ โดยมีการกำหนดหลักเกณฑ์อย่างชัดเจน

- ๑. ความสอดคล้องกับรัฐธรรมนูญ ๑๐๐% - ไม่ขัดต่อมาตรา ๓ (อำนาจอธิปไตยเป็นของปวงชน พระมหากษัตริย์ทรงใช้อำนาจทางรัฐสภา คณะรัฐมนตรี และศาล) - สอดคล้องกับมาตรา ๕ (รัฐธรรมนูญเป็นกฎหมายสูงสุด และเมื่อไม่มีบทบัญญัติให้ใช้ตามประเพณีการปกครองในระบอบประชาธิปไตย) - สนับสนุนมาตรา ๔ (คุ้มครองศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาค) โดยทำให้ประชาชนและองค์กรสามารถดำเนินกิจกรรมได้แม้ในสถานการณ์จำกัดการเคลื่อนไหว - ไม่ละเมิดหมวดสิทธิเสรีภาพใด ๆ และยังสนับสนุนหลักนิติธรรม (rule of law) ๒. ความคล่องตัวและประสิทธิภาพในยุควิกฤต - มาตรา ๖ อนุญาตให้ประธานประชุมกำหนดจัดการประชุมแบบออนไลน์ได้ โดยมีผลเท่าเทียมกับการประชุมปกติ - มาตรา ๘-๙ เปิดช่องให้ใช้จดหมายอิเล็กทรอนิกส์ บันทึกข้อมูลอิเล็กทรอนิกส์ และจัดเก็บข้อมูลจราจร (traffic data) - มาตรา ๑๑ รับรองว่าข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานได้เต็มที่ (สอดคล้องกับ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์) ๓. การยกเลิกข้อจำกัดที่ล้าสมัย - ไม่กำหนดให้ต้องมีผู้เข้าร่วมบางส่วนอยู่ในสถานที่เดียวกัน - ไม่กำหนดว่าผู้เข้าร่วมต้องอยู่ในราชอาณาจักร ทำให้รองรับการทำงานแบบ global และ hybrid work ได้ดีกว่าประกาศ คสช. เดิมมาก จุดที่ควรแก้ไขเพิ่มเติมหรือปรับปรุง (เหตุผลหลักที่เลือกตัวเลข ๒) ผมแบ่งเป็น ๑๐ หมวดใหญ่ เพื่อให้ครอบคลุมทุกมิติ ทุกความเป็นไปได้ และทุกระดับความลึก ๑. รูปแบบของกฎหมาย (จากพระราชกำหนด → พระราชบัญญัติ) พระราชกำหนดเป็นกฎหมายที่ตราขึ้นในสถานการณ์ฉุกเฉินที่มีความจำเป็นรีบด่วน (มาตรา ๑๗๒ รัฐธรรมนูญ ๒๕๖๐) เมื่อสถานการณ์โควิดสิ้นสุดลงและการประชุมออนไลน์กลายเป็น “new normal” ที่ถาวร ควรยกระดับเป็นพระราชบัญญัติปกติ เพื่อความมั่นคงทางกฎหมายและ

เปิดโอกาสให้มีการถกเถียงในรัฐสภาเต็มที่ ๒. มาตรฐานความมั่นคงปลอดภัย (มาตรา ๗) ปัจจุบันอ้างอิงประกาศกระทรวงดิจิทัลฯ. ซึ่งออกตั้งแต่ปี ๒๕๖๓. เทคโนโลยีเปลี่ยนแปลงรวดเร็ว. (เช่น การใช้ AI, end-to-end encryption, zero-trust architecture, quantum-resistant encryption) ควรปรับปรุงให้รองรับมาตรฐานสากลล่าสุด. เช่น NIST SP.๘๐๐-๕๓, ISO/IEC ๒๗๐๐๑:๒๐๒๒ และ EU's eIDAS ๒.๐. รวมถึงกำหนดให้มีการทบทวนมาตรฐานทุก ๒-๓ ปี. ๓. การยืนยันตัวตนและป้องกันการปลอมแปลง (Identity Verification & Deepfake Protection) มาตรา ๙(๑) กำหนดเพียงให้ "แสดงตน" แต่ไม่ระบุวิธีการ. ควรเพิ่มเติมรูปแบบ เช่น การใช้ digital signature ตามพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์, biometric authentication, หรือ Thailand Digital ID. รวมถึงมาตรการป้องกัน deepfake (เช่น การตรวจสอบ real-time video/audio authenticity). ๔. การลงคะแนนลับที่ปลอดภัยสูงสุด (Secret Ballot) มาตรา ๙(๒) เปิดช่องให้ลงคะแนนลับได้ แต่ไม่กำหนดเทคโนโลยี. ควรระบุให้ใช้ระบบที่รับรอง anonymity และ verifiability พร้อมกัน (เช่น homomorphic encryption หรือ blockchain-based voting ที่ใช้ในเอสโตเนียและสวิตเซอร์แลนด์). ๕. ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล. ควรเพิ่มบทบัญญัติให้สอดคล้องเต็มที่กับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) โดยเฉพาะการบันทึกเสียง/ภาพ (มาตรา ๙(๔)) และข้อมูลจราจร (มาตรา ๙(๕)) ต้องกำหนด data minimization, retention period และสิทธิของ data subject อย่างชัดเจน. ๖. การเข้าถึงสำหรับผู้พิการและกลุ่มเปราะบาง (Accessibility & Inclusivity) ไม่มีบทบัญญัติเรื่องนี้เลย. ควรเพิ่มให้สอดคล้องกับอนุสัญญาว่าด้วยสิทธิคนพิการ (CRPD) และ WCAG ๒.๒ เช่น การรองรับ screen reader, captioning, อักษรมีติ, sign language interpretation. ๗. การประชุมข้ามพรมแดนและ multi-platform interoperability***. แม้ไม่มีข้อห้ามเรื่องสถานที่ แต่ควรเพิ่มบทบัญญัติให้ชัดเจนว่ารองรับผู้เข้าร่วมจากต่างประเทศเต็มที่ และกำหนดให้แพลตฟอร์มต้องมี interoperability มาตรฐาน (เช่น WebRTC) เพื่อไม่ผูกขาดกับผู้ให้บริการรายใดรายหนึ่ง. ๘. การกำกับดูแลและการตรวจสอบ (Oversight & Audit) ควรเพิ่มกลไกการตรวจสอบอิสระ เช่น ให้มีการรับรองแพลตฟอร์มโดยหน่วยงานกลาง (คล้าย ก.ล.ต. รับรองระบบ e-Shareholders Meeting) และกำหนดให้มีการ audit log ที่ตรวจสอบได้. ๙. การยกเว้นและขอบเขตการใช้บังคับ (มาตรา ๕) การยกเว้นการประชุมศาลและการจัดซื้อจัดจ้างยังเหมาะสม แต่ควรทบทวนว่าควรขยายการยกเว้นหรือไม่ เช่น การประชุมคณะกรรมการสอบสวนวินัยร้ายแรง หรือการประชุมที่ต้องใช้พยานบุคคลแบบเผชิญหน้า. ๑๐. การรองรับเทคโนโลยีเกิดใหม่ (Future-Proofing) ควรเพิ่มบทบัญญัติแบบ technology-neutral แต่มี framework สำหรับการนำเทคโนโลยีใหม่มาใช้ เช่น metaverse meetings, VR/AR, AI-assisted minute taking โดยไม่ต้องแก้กฎหมายใหม่ทุกครั้ง

- แม้ว่าพระราชกำหนดฯ. จะได้ทำหน้าที่ปลดล็อกข้อจำกัดเดิมตามประกาศ คสช. ฉบับที่ ๗๔/๒๕๕๗ (ที่ยกเลิกไปตามมาตรา ๓) โดยเฉพาะการตัดเงื่อนไขที่ต้องมีผู้เข้าร่วมประชุม ๑ ใน ๓ อยู่ในสถานที่เดียวกันออกไป ซึ่งถือว่าถูกต้องและสอดคล้องกับมาตรา ๗๗ ของรัฐธรรมนูญฯ. ที่รัฐพึงจัดให้มีกฎหมายเท่าที่จำเป็นและทันสมัย. แต่หากมองด้วยเลนส์ของ "รัฐมหาอำนาจทางดิจิทัล". กฎหมายฉบับนี้ยังมีความ "พร่อง" ในเชิงเทคนิคและเชิงปฏิบัติการที่อาจขัดขวางขีดความสามารถในการแข่งขันของประเทศ (Competitiveness) และความคล่องตัวสูงสุด (Maximum Agility)

๑. การยกกระดานิยามและการบังคับใช้ (Revisiting Section ๔ & ๕) มาตรา ๔ นิยาม "การประชุมผ่านสื่ออิเล็กทรอนิกส์" ว่างกว้างพอสมควร แต่มาตรา ๕ กลับมีข้อยกเว้นจำนวนมาก เช่น

การประชุมของรัฐสภา และการพิจารณาพิพากษาคดีของศาล. แม้รัฐธรรมนูญจะแยกอำนาจอธิปไตย (นิติบัญญัติ, บริหาร, ตุลาการ) แต่ในทางเทคนิค "มาตรฐานความปลอดภัยไซเบอร์" ควรเป็นมาตรฐานเดียวกัน การยกเว้นในมาตรา ๕ อาจทำให้เกิดมาตรฐานที่หลวมล้ำ การปรับปรุงควรเขียนให้กฎหมายนี้เป็น "มาตรฐานกลางทางเทคนิค" (Technical Baseline) ที่องค์กรตามมาตรา ๕ (สภา, ศาล) สามารถนำไปประยุกต์ใช้ได้ทันทีโดยไม่ต้องร่างระเบียบใหม่ที่ซ้ำซ้อน เพื่อความสอดคล้องกับยุทธศาสตร์ชาติและมาตรา ๒๕๔ ของรัฐธรรมนูญด้านการปฏิรูปประเทศ... นิยามควรเปิดกว้างเพื่อรองรับการประชุมในโลกเสมือนจริง (Virtual Reality) หรือการใช้อวตารที่ยืนยันตัวตนได้ (Authenticated Avatars) ซึ่งกำลังจะเป็นมาตรฐานใหม่ขององค์กรระดับโลก ไม่ใช่แค่ภาพและเสียงแบบ ๒ มิติ

๒. การรักษาความมั่นคงปลอดภัยที่เหนือกว่ามาตรฐานขั้นต่ำ (Enhancing Section ๗) มาตรา ๗ กำหนดให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลฯ (MDES) กำหนด กฎหมายไม่ควรผูกติดกับประกาศกระทรวงฯ เพียงอย่างเดียว แต่ควรระบุให้ "เทียบเท่าหรือดีกว่ามาตรฐานสากลที่เป็นที่ยอมรับในระดับนานาชาติ" (เช่น ISO/IEC ๒๗๐๐๑, NIST SP ๘๐๐-๖๓) เพื่อให้ภาคเอกชนหรือองค์กรที่มีศักยภาพสูงสามารถใช้เทคโนโลยีที่ล้ำหน้ากว่า (State-of-the-art) ได้โดยไม่ต้องรอการประกาศรับรอง ควรกำหนดหลักการ Zero Trust (ไม่ไว้ใจสิ่งใดเลย ตรวจสอบทุกขั้นตอน) เข้าไปในเจตนารมณ์ของกฎหมาย เพื่อป้องกันการรั่วไหลของข้อมูลลับในการประชุมระดับสูง ซึ่งสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. การส่งหนังสือเชิญประชุมและเอกสาร (Modernizing Section ๘) มาตรา ๘ อนุญาตให้ส่งหนังสือเชิญทางอิเล็กทรอนิกส์ได้ และต้องเก็บสำเนาไว้ ควรปรับปรุงให้รองรับการเชิญและการยืนยันการรับเอกสารผ่าน Smart Contracts บนเทคโนโลยี Blockchain เพื่อความโปร่งใส ตรวจสอบได้ และไม่สามารถแก้ไขย้อนหลัง (Immutable) ซึ่งจะช่วยลดภาระการพิสูจน์พยานหลักฐานตามมาตรา ๑๑ ระบบควรสามารถตรวจสอบความถูกต้องขององค์ประชุมและเอกสารได้โดยอัตโนมัติ (Automated Quorum Checking) เพื่อลดความผิดพลาดของมนุษย์ (Human Error)

๔. หน้าที่ของผู้จัดการประชุมและการลงคะแนน (Revamping Section ๙) มาตรา ๙ (๒) ระบุเรื่องการลงคะแนนทั้งเปิดเผยและลับ ต้องระบุให้ชัดเจนว่าการลงคะแนนลับต้องใช้เทคโนโลยีที่ "ผู้ดูแลระบบ (Admin) ก็ไม่สามารถล่วงรู้ผลโหวตรายบุคคลได้" (Privacy-Preserving Computation) เพื่อให้คำว่า "ลับ" นั้นศักดิ์สิทธิ์จริงตามเจตนารมณ์ของกฎหมายและรัฐธรรมนูญ มาตรา ๔ (ศักดิ์ศรีความเป็นมนุษย์และสิทธิส่วนบุคคล) การแสดงตนตามมาตรา ๙ (๑) ควรยกระดับจากการแค่ "แสดงตน" เป็นการ "พิสูจน์และยืนยันตัวตนทางดิจิทัล" (Digital Identity Verification) ที่มีความน่าเชื่อถือสูง (IAL/AAL ระดับสูง) เพื่อป้องกันการสวมสิทธิ์

๕. การบันทึกเสียงและภาพ vs สิทธิส่วนบุคคล (Refining Section ๙(๔)) มาตรา ๙ (๔) บังคับให้นับทุกเสียงหรือภาพของผู้ร่วมประชุม "ทุกคน" ตลอดระยะเวลา เว้นแต่การประชุมลับ ข้อนี้ อาจขัดแย้งในทางปฏิบัติกับหลักการคุ้มครองข้อมูลส่วนบุคคล (GDPR/PDPA) หากนำไปใช้ยืดหยุ่นเกินไป ควรแก้ไขให้มี "ความยืดหยุ่นตามระดับความสำคัญของการประชุม" (Tiered Approach) การบันทึกทุกอย่างตลอดเวลาอาจสร้าง "Digital Footprint" ที่เป็นภาระในการจัดเก็บและเสี่ยงต่อการรั่วไหล ควรอนุญาตให้ใช้ AI-generated Minutes (บันทึกการประชุมด้วย AI) ที่ได้รับการรับรอง

จากที่ประชุม เป็นหลักฐานแทนไฟล์วิดีโอขนาดใหญ่ได้ เพื่อลด Carbon Footprint และค่าใช้จ่ายในการจัดเก็บข้อมูล (Cloud Storage Costs)

๖. การจ่ายเบี้ยประชุม (Clarifying Section ๑๐) มาตรา ๑๐ จ่ายเบี้ยประชุมได้เหมือน การประชุมปกติ ปรับปรุงกฎหมายให้รองรับการจ่ายค่าตอบแทนผ่านสกุลเงินดิจิทัลที่ธนาคาร แห่งชาติรับรอง (CBDC) หรือระบบการชำระเงินแบบ Real-time เพื่อความคล่องตัวสูงสุดและ ลดขั้นตอนทางธุรการภาครัฐ

๗. สถานะทางกฎหมายและพยานหลักฐาน (Strengthening Section ๑๑) มาตรา ๑๑ ห้ามปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน ควรเพิ่มบทบัญญัติให้การประชุม ที่ดำเนินการผ่านระบบที่ผ่านการรับรองมาตรฐาน (Certified Platforms) ให้ถือว่าเป็นความถูกต้อง แท้จริง (Presumption of Conformity) จนกว่าจะพิสูจน์ได้ว่าเป็นอื่น เพื่อลดภาระการพิสูจน์ในชั้นศาล และสร้างความเชื่อมั่นให้กับนักลงทุนต่างชาติที่เข้าร่วมประชุม Board Meeting ข้ามทวีป

๘. พระราชกำหนดฉบับนี้ถือกำเนิดขึ้นในฐานะเครื่องมือทางกฎหมายที่จำเป็นอย่างยิ่งยุค เพื่อตอบสนองต่อภาวะวิกฤตการณ์การแพร่ระบาดของโรคโควิด-๑๙ ซึ่งบังคับให้ต้องมีการเว้น ระยะห่างทางสังคม (Social Distancing) การมีอยู่ของพระราชกำหนดนี้ถือเป็นการปลดล็อกข้อจำกัด ของประกาศ ศสช. ฉบับที่ ๗๔/๒๕๕๗ ที่กำหนดให้ผู้เข้าร่วมประชุมอย่างน้อยหนึ่งในสามต้องอยู่ใน สถานที่เดียวกัน ซึ่งไม่สอดคล้องกับสถานการณ์ฉุกเฉินในขณะนั้น ดังนั้น ในมติของการเป็น "กฎหมาย เฉพาะกิจเพื่อตอบสนองต่อวิกฤต" พระราชกำหนดฉบับนี้ได้ทำหน้าที่ของมันอย่างสมบูรณ์และน่ายกย่อง ช่วยให้การบริหารราชการแผ่นดินและภาคธุรกิจสามารถดำเนินต่อไปได้อย่างต่อเนื่อง อย่างไรก็ตาม เมื่อมองในมุมของการวางรากฐานทางกฎหมายเพื่ออนาคต (Future-Proof Legislation) ที่ต้องมีทั้ง ประสิทธิภาพ ประสิทธิผล ความมั่นคงปลอดภัยสูงสุด และสอดคล้องกับหลักนิติธรรมในระบอบ ประชาธิปไตยอย่างยั่งยืน พระราชกำหนดฉบับนี้ยังมีช่องว่างและประเด็นที่ต้องพิจารณาเพื่อการ "วิวัฒนาการ" ไปสู่กฎหมายแม่บทที่สมบูรณ์แบบยิ่งขึ้น บทวิเคราะห์นี้จะแบ่งออกเป็น ๓ ส่วนหลัก ได้แก่ ๑. ข้อดีและความเหมาะสมในบริบทเริ่มต้น การยอมรับคุณูปการของ พระราชกำหนด ในฐานะเครื่องมือแก้ปัญหาเฉพาะหน้า ๒. ประเด็นที่ควรพิจารณาเพื่อการแก้ไขเพิ่มเติมและปรับปรุง ในระยะยาว การวิเคราะห์ช่องว่างและโอกาสในการพัฒนาโดยละเอียด ๓. ข้อเสนอแนะเชิงกลยุทธ์ เพื่อการพัฒนา แนวทางการยกระดับพระราชกำหนดฉบับนี้ไปสู่พระราชบัญญัติที่สมบูรณ์

ส่วนที่ ๑: ข้อดีและความเหมาะสมในบริบทเริ่มต้น... พระราชกำหนดฉบับนี้ มีความเหมาะสมอย่างยิ่งในฐานะกฎหมายที่ตราขึ้นอย่างเร่งด่วน โดยมีคุณูปการสำคัญดังนี้ ๑.๑ การสร้างความต่อเนื่องในการดำเนินงาน (Business Continuity) เป็นหัวใจสำคัญที่ทำให้ การประชุมของคณะกรรมการต่าง ๆ ทั้งในภาครัฐและภาคเอกชน (เช่น การประชุมคณะกรรมการ บริษัท การประชุมผู้ถือหุ้น) สามารถเกิดขึ้นได้ตามกฎหมาย เป็นการรักษาเสถียรภาพทางเศรษฐกิจ และการบริหารราชการแผ่นดินไว้ได้ในยามวิกฤต ๑.๒ การปลดล็อกข้อจำกัดทางกายภาพ โดยสมบูรณ์ การยกเลิกข้อกำหนดที่ต้องมีผู้เข้าร่วมประชุมอยู่ในสถานที่เดียวกัน ถือเป็นการยอมรับ อย่างเต็มรูปแบบว่า "พื้นที่เสมือน" (Virtual Space) มีสถานะทางกฎหมายเทียบเท่า "พื้นที่จริง" (Physical Space) สำหรับการประชุม นับเป็นก้าวสำคัญของการเปลี่ยนผ่านสู่ยุคดิจิทัล ๑.๓ การวางกรอบพื้นฐานด้านความปลอดภัยและความน่าเชื่อถือ มาตรา ๗, ๘, และ ๑๑ ได้วาง หลักการสำคัญไว้ ทั้งเรื่องมาตรฐานความมั่นคงปลอดภัย การแสดงตน การบันทึกเสียงหรือภาพ

การจัดเก็บข้อมูลจรรยาบรรณอิเล็กทรอนิกส์ และการยอมรับข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน ซึ่งเป็นเสาหลักที่จำเป็นสำหรับการประชุมทางอิเล็กทรอนิกส์

ส่วนที่ ๒: ประเด็นที่ควรพิจารณาเพื่อการแก้ไขเพิ่มเติมและปรับปรุงในระยะยาว แม้จะมีข้อดีดังที่กล่าวมา แต่ในฐานะผู้เชี่ยวชาญที่มองการณ์ไกล พระราชกำหนดฉบับนี้ยังคงมีลักษณะของ "กฎหมายเชิงรับ" มากกว่า "กฎหมายเชิงรุก" ซึ่งมีประเด็นที่ควรยกระดับดังต่อไปนี้ ๒.๑ สถานะของกฎหมาย: จาก "พระราชกำหนด" สู่ "พระราชบัญญัติ" พระราชกำหนดเป็นกฎหมายที่ตราขึ้นโดยฝ่ายบริหารในสถานการณ์ฉุกเฉิน ขาดกระบวนการตรวจสอบถ่วงดุลอย่างละเอียดรอบคอบ จากฝ่ายนิติบัญญัติ การคงสถานะเป็นพระราชกำหนดในระยะยาวอาจสร้างความไม่แน่นอนและขาดความสง่างามทางนิติธรรม ควรมีการยกร่าง พระราชกำหนดฉบับนี้ขึ้นเป็น "พระราชบัญญัติ" ว่าด้วยการประชุมและการดำเนินกระบวนการทางอิเล็กทรอนิกส์" ซึ่งเป็นกฎหมายถาวรที่ผ่านกระบวนการรัฐสภาอย่างเต็มรูปแบบ เพื่อสร้างความเชื่อมั่นและเสถียรภาพทางกฎหมายในระยะยาว และขยายขอบเขตให้ครอบคลุม "กระบวนการ" อื่น ๆ นอกเหนือจากการประชุมด้วย ๒.๒ มาตรฐานความมั่นคงปลอดภัย (มาตรา ๗) การมอบอำนาจให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) เป็นผู้กำหนดมาตรฐานโดยการประกาศแต่เพียงฝ่ายเดียว อาจขาดความยืดหยุ่นและปรับตัวไม่ทันต่อการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็ว และอาจสร้างภาระให้ผู้ประกอบการต้องรอคอย การประกาศที่เป็นทางการ ตัวบทกฎหมายหลัก (พระราชบัญญัติ) ควรกำหนดเป็น "กรอบหลักการ" (Principle-based Framework) ที่ไม่ยึดติดกับเทคโนโลยีใดเทคโนโลยีหนึ่ง (Technology-Neutral) เช่น หลักการรักษาความลับ (Confidentiality), หลักการรักษาความครบถ้วนของข้อมูล (Integrity), หลักการพิสูจน์ตัวตน (Authentication), และหลักการห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) จากนั้นจึงให้ MDES หรือหน่วยงานที่เกี่ยวข้องออก "แนวปฏิบัติ (Guidelines)" และ "มาตรฐานทางเทคนิค (Technical Standards)" ที่สามารถปรับปรุงได้ตามยุคสมัย รวมถึงจัดตั้ง "ระบบการรับรอง (Certification)" แพลตฟอร์มการประชุมที่ได้มาตรฐาน เพื่อให้องค์กรต่าง ๆ สามารถเลือกใช้ได้อย่างมั่นใจ ๒.๓ นิยามและรูปแบบการประชุม ต้องก้าวข้ามการจำลองแบบกายภาพ พระราชกำหนดปัจจุบันยังคงมองการประชุมอิเล็กทรอนิกส์ในฐานะ "การจำลอง" การประชุมทางกายภาพที่เกิดขึ้นพร้อมกัน (Synchronous) กฎหมายฉบับใหม่ควรขยายขอบเขตและนิยามให้ครอบคลุมการประชุมแบบผสม (Hybrid Meeting) กำหนดหลักเกณฑ์ที่ชัดเจนในการจัดการประชุมที่มีทั้งผู้เข้าร่วมในสถานที่จริงและผ่านระบบอิเล็กทรอนิกส์ เพื่อให้เกิดความเท่าเทียมในการมีส่วนร่วม การอภิปราย และการลงคะแนน รองรับการจัดสนใจในเรื่องที่ไม่ซับซ้อนผ่านแพลตฟอร์มที่ปลอดภัย โดยให้สมาชิกเข้ามาพิจารณาและลงมติภายในกรอบเวลาที่กำหนด (เช่น ๒๔ หรือ ๔๘ ชั่วโมง) ซึ่งจะเพิ่มความคล่องตัวและประสิทธิภาพอย่างมหาศาล กำหนดหลักเกณฑ์การลงมติเวียนที่ใช้เทคโนโลยีดิจิทัล เช่น ลายมือชื่อดิจิทัล (Digital Signature) เพื่อให้มีผลผูกพันทางกฎหมายและตรวจสอบได้ ๒.๔ กลไกการลงคะแนนลับ (มาตรา ๙ (๒)) ต้องมีความโปร่งใสและตรวจสอบได้ มาตรา ๙ (๒) ระบุเพียงว่าต้อง "สามารถลงคะแนนลับได้" แต่ไม่ได้กำหนดคุณลักษณะทางเทคนิคและกระบวนการที่จำเป็น ซึ่งการลงคะแนนลับทางอิเล็กทรอนิกส์เป็นเรื่องที่ซับซ้อนและมีความเสี่ยงสูง กฎหมายควรระบุคุณสมบัติสำคัญของระบบลงคะแนนลับอิเล็กทรอนิกส์ คือ ต้องสามารถตรวจสอบความถูกต้องของการนับคะแนนได้ โดยที่ยังคงรักษาความเป็นนิรนามของผู้ลงคะแนน (Verifiable and Anonymous) ซึ่งอาจใช้เทคโนโลยีการเข้ารหัสขั้นสูง (Advanced Cryptography) หรือเทคโนโลยีบัญชีแยกประเภทแบบกระจายศูนย์ (Distributed Ledger Technology) เพื่อสร้าง

ความโปร่งใสและความเชื่อมั่นสูงสุด ๒.๕ การจัดเก็บและบูรณาการของหลักฐาน. (มาตรา ๙. (๔) และ (๕)) ต้องเข้มข้นกว่าเดิม... การ "บันทึกเสียงหรือภาพ" และ "จัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์" เป็นเพียงจุดเริ่มต้น แต่ยังคงขาดหลักประกันความครบถ้วนสมบูรณ์ (Integrity) ของหลักฐาน ควรกำหนดมาตรฐานการจัดเก็บให้รัดกุมขึ้น การประทับเวลา (Timestamping) ข้อมูลการประชุม และรายงานการประชุมอิเล็กทรอนิกส์ต้องได้รับการประทับเวลาจากหน่วยงานที่น่าเชื่อถือ (Trusted Time-Stamping Authority) การรับรองบูรณาการของข้อมูล (Data Integrity) ใช้เทคนิค Hash Function หรือลายมือชื่อดิจิทัล เพื่อรับประกันว่าไฟล์บันทึกการประชุมหรือรายงานการประชุมไม่ได้ถูกแก้ไขเปลี่ยนแปลงในภายหลัง กำหนดแนวทางการจัดการข้อมูลบันทึกการประชุมและข้อมูลจราจรให้สอดคล้องกับ PDPA อย่างชัดเจน ทั้งในเรื่องฐานการประมวลผล, สิทธิของเจ้าของข้อมูล และระยะเวลาการจัดเก็บ ๒.๖ การทบทวนข้อยกเว้น (มาตรา ๕) เพื่อการประยุกต์ใช้ที่กว้างขวางขึ้น การยกเว้นการประชุมของรัฐสภา, ศาล, และกระบวนการจัดซื้อจัดจ้าง อาจเป็นการจำกัดศักยภาพของเทคโนโลยีดิจิทัลในการเพิ่มความโปร่งใสและประสิทธิภาพ ควรกำหนด "แผนการทบทวน (Review Roadmap)" สำหรับข้อยกเว้นเหล่านี้ โดยอาจเริ่มจากการจัดซื้อจัดจ้าง ควรนำมาอยู่ภายใต้กฎหมายนี้โดยเร็วที่สุด เพราะการประชุมของคณะกรรมการจัดซื้อจัดจ้างผ่านสื่ออิเล็กทรอนิกส์ที่โปร่งใสและบันทึกได้ทุกขั้นตอน คือเครื่องมือสำคัญในการป้องกันการทุจริต... แม้การประชุมสภาเต็มรูปแบบจะมีความซับซ้อน แต่การประชุมของ "คณะกรรมการจัดการ" ควรสามารถทำผ่านสื่ออิเล็กทรอนิกส์ได้อย่างเต็มรูปแบบตามกฎหมายนี้ เพื่อเพิ่มความคล่องตัวและลดค่าใช้จ่าย การพิจารณาคดีเป็นเรื่องละเอียดอ่อน แต่กระบวนการ "บริหารจัดการคดี" หรือการประชุมภายในขององค์กรตุลาการควรสามารถใช้ประโยชน์จากกฎหมายนี้ได้ ๒.๗ การเข้าถึงและความเท่าเทียม (Digital Divide and Accessibility) พระราชกำหนดฉบับนี้ตั้งอยู่บนสมมติฐานว่าทุกคนสามารถเข้าถึงเทคโนโลยีและอินเทอร์เน็ตได้อย่างเท่าเทียม ซึ่งในความเป็นจริงยังมีความเหลื่อมล้ำทางดิจิทัลอยู่ กฎหมายฉบับปรับปรุงควรมีบทบัญญัติที่ส่งเสริม "การเข้าถึงอย่างทั่วถึง (Universal Accessibility)" โดยกำหนดให้แพลตฟอร์มการประชุมต้องรองรับผู้พิการ (เช่น มีคำบรรยายแทนเสียง, รองรับโปรแกรมอ่านหน้าจอ) และควรมีแนวปฏิบัติสำหรับองค์กรในการสนับสนุนผู้เข้าร่วมประชุมที่อาจมีข้อจำกัดทางเทคโนโลยี

ส่วนที่ ๓: ข้อเสนอแนะเชิงกลยุทธ์เพื่อการพัฒนา เพื่อยกระดับ พ.ร.ก. ฉบับนี้ให้เป็นกฎหมายดิจิทัลระดับสากล ผมขอเสนอแนวทางเชิงกลยุทธ์ดังนี้ ๑. ยกระดับสู่ "พระราชบัญญัติ" โดยเร็ว ตั้งคณะกรรมการประกอบด้วยผู้เชี่ยวชาญจากภาครัฐ เอกชน และนักวิชาการ เพื่อยกร่าง "พระราชบัญญัติว่าด้วยการประชุมและการดำเนินกระบวนการทางอิเล็กทรอนิกส์" โดยนำประเด็นใน ส่วนที่ ๒ มาพิจารณาอย่างรอบด้าน และผ่านกระบวนการรับฟังความคิดเห็นจากทุกภาคส่วน ๒. จัดตั้ง "ศูนย์กลางกำกับดูแลและส่งเสริม" มอบหมายให้หน่วยงานที่มีความเชี่ยวชาญ (เช่น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ - ETDA) ทำหน้าที่เป็นหน่วยงานกลางในการออกมาตรฐานทางเทคนิค, รับรองแพลตฟอร์ม, ให้คำปรึกษา และสร้างองค์ความรู้เกี่ยวกับการประชุมอิเล็กทรอนิกส์ที่ปลอดภัยและมีประสิทธิภาพ ๓. บูรณาการกับกฎหมายดิจิทัลอื่น ร่างกฎหมายฉบับใหม่ต้องออกแบบให้เชื่อมโยงและสอดคล้องกับระบบนิเวศกฎหมายดิจิทัลของประเทศอย่างสมบูรณ์ ทั้งพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ๔. ส่งเสริมการนำร่องและนวัตกรรม (Regulatory Sandbox) เปิดพื้นที่ให้หน่วยงานภาครัฐและบริษัทเอกชนสามารถทดลองรูปแบบ

การประชุมและการตัดสินใจทางอิเล็กทรอนิกส์ในรูปแบบใหม่ๆ ภายใต้การกำกับดูแล เพื่อนำผลลัพธ์มาพัฒนากฎระเบียบให้ทันสมัยอยู่เสมอ

- ๑. ความจำเป็นในการแก้ไข : ในมุมมองหลักนิติธรรมและกฎหมายสูงสุด ตามรัฐธรรมนูญ มาตรา ๕ กำหนดว่า รัฐธรรมนูญเป็นกฎหมายสูงสุด และกฎหมายใดขัดหรือแย้งย่อมใช้บังคับมิได้ พระราชกำหนดฯ ๒๕๖๓ บางส่วนยังไม่สอดคล้องกับหลักการในรัฐธรรมนูญ เช่น (๑) ความเหมาะสมของการใช้ “พระราชกำหนด” แทน “พระราชบัญญัติ” พระราชกำหนดต้องออกเมื่อมีความจำเป็นเร่งด่วนตาม มาตรา ๑๗๒ ของรัฐธรรมนูญ (ซึ่งอ้างอิงในตัว พ.ร.ก.) แต่การประชุมผ่านสื่ออิเล็กทรอนิกส์ในปัจจุบัน ไม่ได้อยู่ในภาวะฉุกเฉินอีกต่อไป จึงควร “ยกฐานะเป็นพระราชบัญญัติ” เพื่อให้มีความมั่นคงถาวรและการมีส่วนร่วมของรัฐสภาตามหลักประชาธิปไตย ๒. ประเด็นที่สมควรปรับปรุงเชิงกฎหมายและเทคโนโลยี ๒.๑. การบันทึกเสียง/ภาพทุกคนตลอดเวลา (มาตรา ๙(๔)) ข้อกำหนดให้บันทึกเสียงหรือเสียงและภาพ “ของผู้ร่วมประชุมทุกคนตลอดเวลา” แม้จะเป็นมาตรการด้านความปลอดภัย แต่มีความเสี่ยงต่อ: สิทธิในความเป็นส่วนตัว (มาตรา ๓๒ รัฐธรรมนูญ) เสรีภาพการแสดงความคิดเห็นทางวิชาการหรือวิชาชีพ ความปลอดภัยข้อมูลตามมาตรฐานสากล เช่น GDPR ต้องปรับให้: บันทึกเฉพาะ “ส่วนทางการประชุม” ไม่ใช่ทุกช่วงเวลา อนุญาตการประชุมลับโดยไม่มีบันทึกตามลักษณะงาน วางมาตรฐานการปกปิดข้อมูลที่ชัดเจน ๒.๒. คำนิยาม “ผู้ร่วมประชุม” ยังครอบคลุมไม่เพียงพอกับสภาพปัจจุบัน ในโลกปัจจุบันมี: ผู้สังเกตการณ์ (observer) ผู้ให้คำปรึกษาออนไลน์ (advisor) ระบบ AI/ผู้ช่วยอัตโนมัติในการประชุม ผู้เข้าร่วมเป็นฝ่ายต่างประเทศ หรือ hybrid cross-border คำนิยามปัจจุบันยังไม่รองรับสภาพดังกล่าว จึงต้องปรับให้ทันสมัยและทันสมัยเทคโนโลยี ๒.๓. ข้อห้ามการประชุมบางประเภทตามกฎหมายกระทรวง (มาตรา ๕ และ ๖) การกำหนดบางเรื่องว่าห้ามประชุมผ่านสื่ออิเล็กทรอนิกส์โดยกฎหมายกระทรวง อาจทำให้ “มาตรฐานความชัดเจนของกฎหมาย” ลดลง ควรยกระดับเป็นกฎหมายระดับพระราชบัญญัติกำหนดหลักเกณฑ์ชัดเจนตามหลักนิติธรรม (มาตรา ๒๖) ๒.๔. มาตรฐานความมั่นคงปลอดภัย (มาตรา ๗) มาตรฐานปัจจุบันอ้างอิง “มาตรฐานที่กระทรวงดิจิทัลกำหนด” เท่านั้น แต่ควรต้องยกระดับให้สอดคล้องกับ: ISO/IEC ๒๗๐๐๑, Zero Trust Architecture, National Cybersecurity Framework, หลัก ก. privacy by design และควรมีระบบ “การรับรองแพลตฟอร์ม (certification)” ระดับประเทศ เพื่อให้เกิดความเชื่อมั่นสูงสุด ๒.๕. การชำระเบี้ยประชุม (มาตรา ๑๐) ข้อกำหนดเรื่องการแสดงตนเพื่อรับเบี้ยประชุม ขณะประชุมออนไลน์ ยังไม่ครอบคลุมกรณี: ใช้ระบบ AI facial recognition การเข้าร่วมแบบ asynchronous การเข้าร่วมบางช่วงตามระเบียบ ควรปรับปรุงให้ชัดเจน ยืดหยุ่น และเป็นธรรม โดยไม่เอื้อให้เกิดการทุจริตหรือเบี่ยงเบนประเด็น ๓. ความจำเป็นในการพัฒนาเพื่อสากลระดับรัฐมหาอำนาจ สากลในปัจจุบัน (EU, US, OECD, ASEAN Digital Master Plan) กำหนดมาตรฐานสูงมากในด้าน: Cybersecurity, Privacy, Electronic identities, Cross-border e-meeting, Digital signatures และ e-voting พระราชกำหนดฯ ๒๕๖๓ ยังไม่รองรับมาตรฐานเหล่านี้ การแก้ไขจะทำให้ประเทศไทย “เป็นศูนย์กลางการประชุมดิจิทัลระดับนานาชาติ” เหมาะสมกับเศรษฐกิจดิจิทัลและรัฐบาลดิจิทัล (Digital Government) ๔. การสอดคล้องกับหลักรัฐธรรมนูญทุกมาตรา การประชุมผ่านสื่ออิเล็กทรอนิกส์เป็นกลไกที่จะต้อง: ไม่ละเมิดสิทธิส่วนบุคคล (มาตรา ๓๒) ไม่กระทบเสรีภาพ การติดต่อสื่อสาร (มาตรา ๓๖) ไม่จำกัดสิทธิเกินสมควรแก่เหตุ (มาตรา ๒๖) เคารพหลักนิติธรรม (มาตรา ๓ และมาตรา ๕) สนับสนุนการเข้าถึงข้อมูลภาครัฐ (มาตรา ๔๑) ส่งเสริมการบริหารราชการ

แบบโปร่งใส ตรวจสอบได้ การปรับปรุงพระราชกำหนดฯ จึงจำเป็นเพื่อให้สอดคล้องครบทุกมิติ อย่างแท้จริง

๑. การยกระดับนิยามและขอบเขตบังคับใช้เพื่อความคล่องตัวสูงสุด (Maximizing Agility & Scope) มาตรา ๕ ของพระราชกำหนดฯ ยกเว้นการบังคับใช้กับการประชุมของรัฐสภา การพิจารณาพิพากษาคดีของศาล และกระบวนการจัดซื้อจัดจ้าง แม้รัฐธรรมนูญจะให้อิสระแก่ฝ่ายนิติบัญญัติและตุลาการ (ตามหลักการแบ่งแยกอำนาจ) แต่ในทางปฏิบัติ "มาตรฐานทางเทคนิค" และ "ความเชื่อมั่นในพยานหลักฐานดิจิทัล" ควรเป็นมาตรฐานเดียว (Single Standard) หรือมาตรฐานที่ทำงานร่วมกันได้ (Interoperability) ควรแก้ไขให้กฎหมายนี้เป็น "กฎหมายกลางเชิงโครงสร้างพื้นฐาน" (Fundamental Infrastructure Law) ที่วางมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Baseline) ที่ทุกองค์กร รวมถึงรัฐสภาและศาล สามารถนำไปประยุกต์ใช้ได้ โดยไม่ขัดต่ออำนาจอิสระขององค์กรนั้น ๆ เพื่อให้เกิด Ecosystem การประชุมอิเล็กทรอนิกส์ที่เป็นหนึ่งเดียว ลดความซ้ำซ้อนของการลงทุนระบบ และสร้างความเท่าเทียมในการเข้าถึงความยุติธรรมผ่านระบบดิจิทัล (E-Justice) ๒. การปฏิรูปมาตรฐานความมั่นคงปลอดภัยให้เป็นระดับสากล (International Security Standardization) มาตรา ๗ กำหนดให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลฯ กำหนด ซึ่งอาจมีความล่าช้าหรือไม่ทันต่อภัยคุกคามไซเบอร์รูปแบบใหม่ (Zero-day exploits, Deepfakes) กฎหมายควรระบุให้ "มาตรฐานการรักษาความมั่นคงปลอดภัย" ต้องเป็นพลวัต (Dynamic) และอ้างอิงมาตรฐานสากลระดับสูง เช่น ISO/IEC ๒๗๐๐๑ (Information Security Management) หรือ NIST Cybersecurity Framework โดยอัตโนมัติ เพื่อให้ระบบการประชุมของไทยได้รับการยอมรับจากนานาชาติ โดยเฉพาะในการประชุมข้ามพรมแดน (Cross-border Meetings) หรือการประชุมที่มีความลับระดับชาติ ต้องมีการระบุถึงการเข้ารหัสข้อมูลขั้นสูง (End-to-End Encryption) ที่เข้มข้นกว่ากฎหมายปัจจุบัน ๓. การเพิ่มประสิทธิภาพการยืนยันตัวตนและสิทธิการประชุม (Advanced Authentication & Authorization) มาตรา ๙ (๑) กำหนดให้ ผู้ร่วมประชุมแสดงตน ซึ่งในทางปฏิบัติมักใช้แค่การเปิดกล้องหรือล็อกอินธรรมดา ซึ่งมีความเสี่ยงต่อการถูกสวมรอย (Identity Theft) ควรบัญญัติเพิ่มเติมให้รองรับและส่งเสริมการใช้ Digital ID (National Digital ID - NDID) หรือเทคโนโลยีชีวมิติ (Biometrics) ขั้นสูงในการยืนยันตัวตน เพื่อความถูกต้องแม่นยำสูงสุด ป้องกันการประชุมแทนกัน และสอดคล้องกับ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างเคร่งครัด ๔. นวัตกรรมการลงคะแนนลับและความโปร่งใส (Blockchain & Zero-Knowledge Proofs) มาตรา ๙ (๒) กล่าวถึงการลงคะแนนลับ แต่ในระบบอิเล็กทรอนิกส์ทั่วไป การรักษาความลับให้ "ลับจริง" (Truly Secret) ขณะที่ระบบยังต้องตรวจสอบได้ (Verifiable) เป็นเรื่องยากทางเทคนิค กฎหมายควรเปิดช่องหรือส่งเสริมให้นำเทคโนโลยี Blockchain หรือ Distributed Ledger Technology (DLT) มาใช้ในการลงคะแนน เพื่อรับประกันความโปร่งใส (Transparency) ที่ไม่สามารถแก้ไขข้อมูลย้อนหลังได้ (Immutability) และใช้เทคนิคทางคณิตศาสตร์เช่น Zero-Knowledge Proofs เพื่อพิสูจน์สิทธิการโหวตโดยไม่ต้องเปิดเผยตัวตนในกรณีการลงคะแนนลับ เพื่อให้ทัดเทียมกับมาตรฐานประชาธิปไตยดิจิทัลของรัฐมหาอำนาจ ๕. การบริหารจัดการข้อมูลจราจรคอมพิวเตอร์ และการคุ้มครองข้อมูลส่วนบุคคล (Data Governance & Privacy) มาตรา ๙ (๔) และ (๕) กำหนดให้บันทึกเสียง/ภาพ และเก็บข้อมูลจราจรของผู้ร่วมประชุมทุกคนตลอดระยะเวลา ซึ่งสร้างภาระในการจัดเก็บข้อมูลมหาศาล (Storage Overhead) และอาจขัดกับหลักการ Data

Minimization ของกฎหมาย PDPA (เก็บเท่าที่จำเป็น) ควรปรับปรุงให้ยืดหยุ่นขึ้น โดยอนุญาตให้ใช้เทคโนโลยี Speech-to-Text (AI Transcription) ในการทำรายงานการประชุมอัตโนมัติควบคู่ไปกับการเก็บไฟล์เสียง เพื่อลดภาระการจัดเก็บไฟล์วิดีโอขนาดใหญ่ และกำหนดระยะเวลาการทำลายข้อมูล (Data Retention Policy) ที่ชัดเจน เพื่อคุ้มครองสิทธิส่วนบุคคลของผู้เข้าร่วมตามมาตรา ๓๒ ของรัฐธรรมนูญฯ ปี ๒๕๖๐ (สิทธิในความเป็นอยู่ส่วนตัว) ๖. การรองรับเทคโนโลยีอนาคต (Future-Proofing for Web ๓.๐ & Metaverse) นิยามปัจจุบันยังยึดติดกับรูปแบบ Video Conference แบบ Web ๒.๐ (เช่น Zoom, MS Teams) ควรแก้ไขนิยามและระเบียบวิธีปฏิบัติให้รองรับการประชุมในโลกเสมือนจริง (**Metaverse**) การใช้อวตาร (Avatar) ที่ยืนยันตัวตนได้ทางกฎหมาย หรือการประชุมผ่านระบบ Hologram ซึ่งจะเป็นมาตรฐานใหม่ในอนาคต เพื่อให้ประเทศไทยมีความ "ล้ำสมัย" และมีความพร้อมทางกฎหมายสูงสุด ๗. ความสอดคล้องกับรัฐธรรมนูญอย่างสมบูรณ์ (Constitutional Alignment) การแก้ไขนี้จะช่วยเสริมสร้าง "หน้าที่ของรัฐ" ตามรัฐธรรมนูญ มาตรา ๗๘ ที่กำหนดให้รัฐพึงส่งเสริมให้ประชาชนมีความรู้ความเข้าใจ และมีส่วนร่วมในการพัฒนาประเทศผ่านช่องทางต่างๆ การมีกฎหมายประชุมอิเล็กทรอนิกส์ที่ทรงประสิทธิภาพสูงสุด จะช่วยลดความเหลื่อมล้ำในการเข้าถึงอำนาจรัฐและการบริหารจัดการ

- ส่วนที่ ๑: การประเมินคุณค่าและความจำเป็นในระยะแรก (Initial Value and Necessity Assessment) พระราชกำหนดฉบับนี้มีความเหมาะสมอย่างยิ่งในฐานะ "มาตรการรับมือวิกฤต" ด้วยเหตุผลดังนี้: ๑. การปลดล็อกทางกฎหมาย (Legal Unlocking) ก่อนพระราชกำหนดฉบับนี้ กฎหมายจำนวนมาก โดยเฉพาะกฎหมายที่เกี่ยวกับนิติบุคคล เช่น ประมวลกฎหมายแพ่งและพาณิชย์ และพระราชบัญญัติบริษัทมหาชนจำกัด กำหนดให้การประชุมสำคัญ (เช่น การประชุมผู้ถือหุ้น) ต้องเป็นการประชุมแบบกายภาพ (Physical Meeting) การตราพระราชกำหนดนี้ขึ้นมาจึงเป็นการ "ปลดล็อก" ข้อจำกัดดังกล่าว ทำให้องค์กรต่าง ๆ สามารถดำเนินกิจกรรมที่จำเป็นได้โดยไม่ขัดต่อกฎหมายในช่วงเวลาที่ไม่สามารถรวมตัวกันได้ ๒. การสร้างความเชื่อมั่นทางกฎหมาย (Providing Legal Certainty) มาตรา ๑๑ ได้ให้สถานะทางกฎหมายที่ชัดเจนว่า "การประชุมผ่านสื่ออิเล็กทรอนิกส์ตามพระราชกำหนดนี้เป็นการประชุมโดยชอบด้วยกฎหมาย" และห้ามปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน ซึ่งเป็นการสร้างความเชื่อมั่นให้แก่ทุกภาคส่วนในการนำเทคโนโลยีมาใช้ ๓. การเร่งรัดการเปลี่ยนผ่านสู่ดิจิทัล (Accelerating Digital Transformation) พระราชกำหนดนี้เป็นตัวเร่งปฏิกิริยาสำคัญที่ผลักดันให้ทั้งภาครัฐและเอกชนต้องปรับตัวและลงทุนในโครงสร้างพื้นฐานด้านดิจิทัลอย่างรวดเร็ว ซึ่งส่งผลต่อขีดความสามารถในการแข่งขันของประเทศในระยะยาว

ส่วนที่ ๒: ข้อจำกัดและประเด็นที่สมควรได้รับการปรับปรุงเพื่ออนาคต (Limitations and Areas for Future Improvement) แม้จะมีคุณูปการดังที่กล่าวมา แต่เมื่อวิกฤตการณ์ได้คลี่คลายลงและโลกได้เข้าสู่ "ภาวะปกติใหม่" (New Normal) ที่การทำงานแบบผสมผสาน (Hybrid Work) กลายเป็นมาตรฐานสากล ข้อจำกัดของพระราชกำหนดฉบับนี้ก็ปรากฏชัดเจนขึ้นในหลายมิติ ดังนี้ ๑. สถานะของกฎหมาย: จาก "พระราชกำหนด" สู่ "พระราชบัญญัติ" กระบวนการตรากฎหมายพระราชกำหนดเป็นกฎหมายที่ตราขึ้นโดยฝ่ายบริหารในสถานการณ์ฉุกเฉิน ขาดกระบวนการถ่วงดุลและรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียอย่างรอบด้านเหมือนการตราพระราชบัญญัติ โดยฝ่ายนิติบัญญัติ สมควรอย่างยิ่งที่จะยกระดับ พ.ร.ก. ฉบับนี้ให้เป็น "พระราชบัญญัติว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์" โดยผ่านกระบวนการทางรัฐสภาอย่างเต็มรูปแบบ เพื่อให้กฎหมายมีความละเอียด รอบคอบ สะท้อนความต้องการของทุกภาคส่วน และมีความยั่งยืนในระยะยาว

๒. มาตรฐานความมั่นคงปลอดภัยและเทคโนโลยี (มาตรา ๗) มาตรา ๗ กำหนดให้การประชุมต้องเป็นไปตาม "มาตรฐานการรักษาความมั่นคงปลอดภัย...ที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด" ซึ่งเป็นการผูกโยงกฎหมายหลักไว้กับกฎหมายลำดับรอง (ประกาศกระทรวง) เนื่องจากเทคโนโลยีเปลี่ยนแปลงอย่างรวดเร็ว การรอประกาศกระทรวงอาจไม่ทันต่อการเปลี่ยนแปลง และอาจสร้างภาวะ "คอขวด" ทางกฎระเบียบ (Regulatory Bottleneck) การผูกขาดทางเทคโนโลยี (Technology Lock-in) การกำหนดมาตรฐานที่เจาะจงเกินไปอาจเป็นการส่งเสริมเทคโนโลยีบางประเภทและกีดกันนวัตกรรมใหม่ ๆ ยึดหลักความเป็นกลางทางเทคโนโลยี (Technological Neutrality) กฎหมายแม่บทควรบัญญัติ "หลักการ" ที่ต้องบรรลุ แทนการกำหนด "วิธีการ" ที่ตายตัว เช่น ควรกำหนดว่าระบบที่ใช้ต้องสามารถ (๑) พิสูจน์และยืนยันตัวตนผู้เข้าร่วมประชุมได้ (Authentication & Identification), (๒) รักษาความลับของการประชุมได้ (Confidentiality), (๓) รักษาความครบถ้วนของข้อมูลและการลงคะแนนได้ (Data Integrity), (๔) สามารถตรวจสอบย้อนกลับได้ (Auditability) และ (๕) มีระบบที่ทำให้ผู้ร่วมประชุมทุกคนสามารถสื่อสารสองทางได้แบบ Real-time อ้างอิงมาตรฐานสากล ควรกำหนดให้ระบบสอดคล้องกับมาตรฐานที่เป็นที่ยอมรับในระดับสากล เช่น ISO/IEC ๒๗๐๐๑ (Information Security Management Systems) เพื่อให้เกิดการยอมรับและทำงานร่วมกันได้ในระดับนานาชาติ ๓. นิยามและขอบเขตของการประชุม นิยามในมาตรา ๔ มุ่งเน้นไปที่การประชุมแบบอิเล็กทรอนิกส์เต็มรูปแบบ (Fully Virtual) ที่ "ผู้ร่วมประชุมมิได้อยู่ในสถานที่เดียวกัน" แนวปฏิบัติสากลในปัจจุบันคือการประชุมแบบผสมผสาน ซึ่งมีผู้เข้าร่วมประชุมบางส่วนอยู่ในห้องประชุมจริง และบางส่วนเข้าร่วมผ่านระบบอิเล็กทรอนิกส์ พระราชกำหนดฉบับนี้ยังไม่มียกเว้นที่รองรับและคุ้มครองสิทธิของผู้เข้าร่วมประชุมทั้งสองรูปแบบให้เท่าเทียมกัน อย่างชัดเจน เช่น การนับองค์ประชุม สิทธิในการอภิปรายและลงคะแนน สำหรับบางกรณี เช่น การลงมติในเรื่องที่ไม่ซับซ้อน หรือการให้ความเห็นชอบรายงานการประชุม กฎหมายในต่างประเทศบางฉบับอนุญาตให้มีการดำเนินการแบบ Asynchronous (เช่น เปิดให้ลงมติผ่านระบบออนไลน์ ในกรอบเวลา ๒๔ ชั่วโมง) เพื่อเพิ่มความคล่องตัว พระราชกำหนดฉบับนี้ยังไม่รองรับแนวคิดดังกล่าว ควรเพิ่มนิยามและบทบัญญัติที่เกี่ยวข้องกับ "การประชุมแบบผสมผสาน" ให้ชัดเจน พิจารณาเพิ่มเติมบทบัญญัติที่อนุญาตให้ "การดำเนินการบางประเภท" สามารถทำได้ในรูปแบบ Asynchronous โดยกำหนดเงื่อนไขและประเภทของเรื่องที่สามารถทำได้ ๔. กระบวนการและการคุ้มครองข้อมูลส่วนบุคคล (มาตรา ๕) มาตรา ๕ (๔) กำหนดให้ต้อง "บันทึกเสียงหรือทั้งเสียงและภาพตลอดระยะเวลาที่มีการประชุม" และมาตรา ๕ (๕) กำหนดให้ "จัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์" การบังคับบันทึกการประชุมทุกครั้งและตลอดเวลา อาจขัดต่อหลักการความจำเป็น (Necessity) และหลักการจำกัดวัตถุประสงค์ (Purpose Limitation) ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) การจัดเก็บข้อมูลเสียง/ภาพ และข้อมูลจราจร เป็นภาระต้นทุนและสร้างความเสี่ยงด้านความมั่นคงปลอดภัยหากเกิดการรั่วไหล ควรแก้ไขให้การบันทึกการประชุมเป็น "ทางเลือก" หรือ "ข้อกำหนด" เฉพาะการประชุมบางประเภทที่กฎหมายเฉพาะกำหนด หรือเป็นไปตามมติของที่ประชุม โดยต้องแจ้งวัตถุประสงค์ให้ผู้เข้าร่วมประชุมทราบล่วงหน้า เพิ่มบทบัญญัติที่เชื่อมโยงกับ PDPA อย่างชัดเจน เช่น กำหนดระยะเวลาการจัดเก็บ (Retention Period) สิทธิในการเข้าถึงและแก้ไขข้อมูลของผู้ถูกบันทึก และมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บ ๕. การยกเว้น (มาตรา ๕) มาตรา ๕(๓) ยกเว้น "การประชุมเพื่อดำเนินการตามกระบวนการจัดซื้อจัดจ้างของส่วนราชการ" ขัดกับทิศทางการพัฒนา e-Government การยกเว้น

ดังกล่าวอาจเป็นอุปสรรคต่อการพัฒนาระบบ e-Bidding และ e-Procurement ให้มีความโปร่งใส และมีประสิทธิภาพสูงสุด การประชุมของคณะกรรมการพิจารณาผล หรือคณะกรรมการตรวจรับพัสดุ ควรสามารถทำผ่านสื่ออิเล็กทรอนิกส์ได้ภายใต้มาตรการความปลอดภัยที่รัดกุม เพื่อเพิ่มความคล่องตัวและลดโอกาสการทุจริต ควรพิจารณายกเลิกข้อยกเว้นในมาตรา ๕ (๓) และกำหนดให้การประชุมในกระบวนการจัดซื้อจัดจ้างสามารถทำผ่านสื่ออิเล็กทรอนิกส์ได้ โดยให้หน่วยงานที่รับผิดชอบ (เช่น กรมบัญชีกลาง) กำหนดมาตรฐานความปลอดภัยที่เข้มงวดเป็นพิเศษสำหรับการประชุมประเภทนี้

๑.๑ การปฏิวัติทางนิยามศัพท์และขอบเขตการบังคับใช้ (Ontological & Scope Revolution) ต้องขยายคำนิยามของ "สื่ออิเล็กทรอนิกส์" ให้ก้าวข้ามข้อจำกัดทางกายภาพและแพลตฟอร์มปัจจุบัน กฎหมายควรบัญญัติให้รองรับเทคโนโลยี Immersive Reality (VR/AR/MR) และ Metaverse อย่างชัดเจน โดยระบุว่า "การปรากฏตัวทางดิจิทัล" (Digital Presence) ผ่าน Avatar หรือ Hologram ที่มีการยืนยันตัวตนระดับสูง (High-Level Assurance) ให้ถือว่า มีสถานะทางกฎหมายเทียบเท่าการ "มาปรากฏตัวด้วยตนเอง" (Physical Presence) ในทุกมิติ เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ในหลักการ "ห้ามปฏิเสธความมีผลผูกพันทางกฎหมายเพียงเพราะข้อมูลนั้นอยู่ในรูปอิเล็กทรอนิกส์" แต่ยกระดับให้ชัดเจนขึ้น เพื่อลดการตีความของผู้ใช้กฎหมาย ๑.๒ การผนวกมาตรฐานความปลอดภัยแบบ "Zero Trust" และ "Biometrics" (Cybersecurity & Authentication Paradigm) ยกเลิกการพึ่งพาเพียง Username/Password และกำหนดมาตรฐานการยืนยันตัวตนแบบหลายปัจจัย (MFA) ที่อิงกับอัตลักษณ์บุคคล กฎหมายควรกำหนดให้การประชุมที่มีนัยสำคัญทางกฎหมาย (เช่น การประชุมผู้ถือหุ้นมหาชน การประชุมบอร์ดรัฐวิสาหกิจ) ต้องใช้การยืนยันตัวตนผ่าน National Digital ID (NDID) หรือเทคโนโลยี Biometric Liveness Detection เพื่อป้องกันปัญหา Deepfake หรือ AI Impersonation ซึ่งเป็นภัยคุกคามใหม่ การรักษาความปลอดภัยของข้อมูลต้องเปลี่ยนจาก Network-based เป็น Data-centric security โดยข้อมูลการประชุมต้องได้รับการเข้ารหัส (Encryption) ทั้งในขณะส่ง (In-transit) และขณะจัดเก็บ (At-rest) ตามมาตรฐานสากล (เช่น AES-๒๕๖) เป็นการสร้างหลักประกันในมาตรา ๓๒ (สิทธิในข้อมูลส่วนบุคคล) ว่าข้อมูลของผู้ร่วมประชุมจะไม่ถูกเปิดเผยหรือรั่วไหล ๓. ความคล่องตัวทางภูมิศาสตร์และ "Digital Sovereignty" (Geographical Agility) ควรแก้ไขปัญหาเรื่องสถานที่จัดการประชุมและเซิร์ฟเวอร์ (Server Location) ให้เป็นแบบ "ไร้พรมแดนโดยสมบูรณ์" (Truly Borderless) กฎหมายต้องระบุชัดเจนว่า "ไม่ว่าผู้ร่วมประชุมจะอยู่ที่ใดในโลก หรือระบบควบคุมการประชุม (Host Server/Cloud) จะตั้งอยู่ในเขตอำนาจศาลใด หากการประชุมนั้นจัดขึ้นโดยนิติบุคคลไทย หรือภายใต้กฎหมายไทย ให้ถือว่าการประชุมนั้นเกิดขึ้นในราชอาณาจักรไทยโดยสมบูรณ์" (Deemed Local Jurisdiction) สิ่งนี้จะดึงดูด Global HQ และนักลงทุนต่างชาติ ตัดปัญหาความกังวลเรื่องการใช้บริการ Cloud Service Providers ระดับโลก (AWS, Google Cloud, Azure) ซึ่งอาจมี Data Center อยู่ต่างประเทศ ลดต้นทุนและความยุ่งยากทางเทคนิค ๔. การบูรณาการ Blockchain เพื่อความโปร่งใสและตรวจสอบได้ (Immutable Audit Trails) ควรนำเทคโนโลยี Distributed Ledger Technology (DLT) หรือ Blockchain มาใช้ ในกระบวนการนับองค์ประชุมและการลงมติ เสนอให้ใช้ Smart Contracts ในการนับคะแนนเสียง และประมวลผลมติที่ประชุมโดยอัตโนมัติ เพื่อขจัดความผิดพลาดของมนุษย์ (Human Error) และการทุจริต ผลการลงมติที่บันทึกลง Blockchain จะถือเป็นพยานหลักฐานชั้นดีที่สุด (Best

Evidence) ที่ไม่สามารถแก้ไขเปลี่ยนแปลงได้ (Immutable) ซึ่งจะลดภาวะการพิสูจน์ในชั้นศาลได้อย่างมหาศาล. สร้างความเชื่อมั่นให้นักลงทุน (Trust) และลดข้อพิพาททางกฎหมายบริษัท (Corporate Litigation) ๕. การคุ้มครองข้อมูลส่วนบุคคลขั้นสูงและการจัดเก็บข้อมูล (Privacy-Preserving Architecture) ควรปรับปรุงมาตรา ๙ (๔) เรื่องการบันทึกเสียงและภาพ ให้สอดคล้องกับ PDPA และ GDPR ขั้นสูงสุด. ต้องกำหนดแนวทาง Data Minimization คือบันทึกเท่าที่จำเป็นตามกฎหมาย. หากเป็นการประชุมลับหรือเรื่องอ่อนไหว (Trade Secrets) ควรอนุญาตให้บันทึกเฉพาะ "มติ" และ "Log file" การเข้าออก โดยไม่ต้องบันทึกเนื้อหาภาพและเสียงทั้งหมด หรือใช้เทคโนโลยี Zero-Knowledge Proofs เพื่อยืนยันความถูกต้องของการประชุมโดยไม่ต้องเปิดเผยเนื้อหาข้อมูลดิบ. ลดการลิดรอนสิทธิเสรีภาพเกินความจำเป็น ตามหลักความได้สัดส่วน (Proportionality) ในมาตรา ๒๖ ของรัฐธรรมนูญ. ๖. ความต่อเนื่องทางธุรกิจและสภาวะวิกฤต (Business Continuity & Resilience) กฎหมายต้องมีบทบัญญัติพิเศษรองรับ "สภาวะวิกฤตซ้อนวิกฤต" (Compound Crises) หากเกิดเหตุการณ์ที่อินเทอร์เน็ตล่มทั้งประเทศ (Internet Blackout) หรือภัยสงครามไซเบอร์. กฎหมายต้องรองรับการประชุมผ่านระบบสื่อสารทางเลือก เช่น เครือข่ายวิทยุเฉพาะกิจ, ดาวเทียมวงโคจรต่ำ (LEO Satellites - Starlink), หรือ Mesh Network และให้ถือว่าชอบด้วยกฎหมายทันทีโดยไม่ต้องรอประกาศเพิ่มเติม เพื่อให้กลไกบริหารราชการแผ่นดินและภาคธุรกิจเดินหน้าได้โดยไม่หยุดชะงัก (Uninterruptible Operations) ๗. การยกระดับบทลงโทษและการบังคับใช้กฎหมาย (Sanctions & Enforcement) ควรปรับปรุงบทกำหนดโทษให้ทันสมัยต่ออาชญากรรมไซเบอร์. การรบกวนการประชุม (Zoom bombing), การดักฟังข้อมูลการประชุม (Eavesdropping), หรือการสวมรอยเข้าร่วมประชุม ต้องมีบทลงโทษทางอาญาที่ชัดเจนและรุนแรงขึ้นในกฎหมายเฉพาะ หรือเชื่อมโยงกับพระราชบัญญัติคอมพิวเตอร์ฯ ให้ชัดเจนเพื่อป้องปรามและรักษาความศักดิ์สิทธิ์ของการประชุม ๘. การเปิดกว้างสำหรับ "Hybrid Meeting" อย่างไร้รอยต่อ (Seamless Hybrid Integration) ควรกำหนดมาตรฐานสำหรับ Hybrid Meeting (ประชุม ณ สถานที่จริง + ออนไลน์) ให้ชัดเจน เพื่อไม่ให้เกิดความได้เปรียบเสียเปรียบระหว่างผู้ร่วมประชุมสองกลุ่ม ผู้ร่วมประชุมออนไลน์ต้องมีสิทธิในการอภิปราย ชักถาม และลงมติแบบ Real-time" เท่าเทียมกับผู้ที่อยู่ในห้องประชุม (No Latency Discrimination) กฎหมายต้องรับรองว่าปัญหาทางเทคนิค (เช่น เน็ตหลุดชั่วคราว) จะไม่ทำให้องค์ประชุมล่ม เว้นแต่จะมีนัยสำคัญ

- ๑. ยุทธศาสตร์ด้านนิติวิศวกรรมและการบูรณาการกฎหมาย (Legal Engineering & Harmonization Strategy) การปรับปรุงกฎหมายต้องมองข้าม "รูปแบบ" ไปสู่ "เนื้อหาและผลสัมฤทธิ์" โดยยึดหลักมาตรา ๗๗ ของรัฐธรรมนูญ ที่รัฐพึงจัดให้มีกฎหมายเพียงเท่าที่จำเป็น และมาตรา ๒๕๘ ข. (๔) ด้านการปรับปรุงการบริหารราชการแผ่นดิน ๑.๑. การยกระดับสู่ "Code of Digital Administrative Procedure" ควรกำหนดให้การประชุมผ่านสื่ออิเล็กทรอนิกส์มีศักดิ์และสิทธิ์ "เหนือกว่า" หรือ "เท่าเทียมแบบสมบูรณ์" (Absolute Equivalence) กับการประชุมทางกายภาพ ไม่ใช่แค่ทางเลือกสำรอง โดยแก้ไขนิยามในกฎหมายแม่บทให้คำว่า "ที่ประชุม" (Meeting Place) ในทางกฎหมายปกครอง หมายรวมถึง "พื้นที่ดิจิทัล" (Digital Space) โดยสภาพ การบังคับให้คนต้องเดินทางมาประชุมในยุคดิจิทัลถือเป็นการสร้างภาระเกินจำเป็น ๑.๒. การขยายขอบเขตอำนาจศาลและองค์กรอิสระ (Judicial & Independent Body Inclusion) ปรับปรุงมาตรา ๕ ที่ยกเว้นศาลและองค์กรอิสระ ให้เป็นระบบ "Opt-in by Default" กล่าวคือ ให้กฎหมายนี้มีผลบังคับใช้เป็นมาตรฐานขั้นต่ำ (Minimum Standard) สำหรับหน่วยงานเหล่านั้น เว้นแต่หน่วยงานนั้นจะมีระเบียบของ

ตนเองที่กำหนดมาตรฐานไว้สูงกว่าหรือเข้มข้นกว่า เพื่อไม่ให้เกิดช่องว่างในกระบวนการยุติธรรมทางอิเล็กทรอนิกส์ (e-Justice) ๒. ยุทธศาสตร์ด้านเทคโนโลยีขั้นสูงและความมั่นคงปลอดภัย (Deep Tech & Cybersecurity Superiority) เพื่อก้าวข้ามข้อจำกัดของมาตรา ๗ และมาตรา ๙ ต้องนำเทคโนโลยีระดับ Frontier มาใช้ ๒.๑ ระบบยืนยันตัวตนแบบหลายปัจจัยขั้นสูง (Advanced Multi-Factor Authentication - MFA) ควรเลิกใช้แค่การ "แสดงตนผ่านกล้อง" (Video Presence) แต่ต้องกำหนดมาตรฐานการยืนยันตัวตนระดับ IAL๓ (Identity Assurance Level ๓) ผ่านโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) หรือการใช้ Biometrics (ม่านตา/ลายนิ้วมือ/เสียง) ร่วมกับ National Digital ID เพื่อป้องกันการสวมรอยในการประชุมลับที่มีความสำคัญระดับชาติ รองรับ Self-Sovereign Identity (SSI) บน Blockchain เพื่อให้ผู้ประชุมเป็นเจ้าของข้อมูลอัตลักษณ์ของตนเองอย่างแท้จริง ๒.๒ สถาปัตยกรรมความปลอดภัยแบบ Zero Trust และ Quantum Encryption การจัดเก็บข้อมูลจราจรและเนื้อหาการประชุมต้องไม่อยู่บน Server ทั่วไป แต่ต้องเข้ารหัสระดับ Quantum-Resistant Cryptography เพื่อป้องกันการถูกถอดรหัสโดยควอนตัมคอมพิวเตอร์ในอนาคต (Future-proofing) โดยเฉพาะการประชุมคณะรัฐมนตรีหรือเรื่องความมั่นคงตามมาตรา ๑๒ สอดคล้องกับหน้าที่ของรัฐตามมาตรา ๕๒ ในการรักษาความมั่นคงของรัฐและผลประโยชน์แห่งชาติ ๓. ยุทธศาสตร์ด้านกระบวนการทำงานอัจฉริยะ (Intelligent Process Automation & AI) ยกเว้นมาตรา ๖ และมาตรา ๘ (กระบวนการประชุม) สู่ระบบอัตโนมัติ ๓.๑ การรับรองสถานะทางกฎหมายของ AI (Legal Status of AI Agents) กฎหมายควรเปิดช่องให้ยอมรับบันทึกการประชุม (Minutes) ที่ถูกจัดและสรุปโดย Artificial Intelligence (AI) ที่ผ่านการตรวจสอบความถูกต้องแล้ว ว่าเป็นเอกสารราชการที่ชอบด้วยกฎหมาย เพื่อลดภาระงานธุรการ และเพิ่มความเร็ว ควร ใช้ AI ทำหน้าที่ Sentiment Analysis (วิเคราะห์อารมณ์ในที่ประชุม) และ Fact-Checking (ตรวจสอบข้อเท็จจริง) แบบ Real-time เพื่อสนับสนุนประธานในที่ประชุม ๓.๒ Smart Contracts สำหรับการลงมติ (Blockchain Voting) ในมาตรา ๙ (๒) เรื่องการลงคะแนน เปลี่ยนจากการขานชื่อหรือติ๊กในโปรแกรม เป็นการส่ง Transaction เข้าสู่ Private Blockchain ของรัฐ จะเกิดความโปร่งใส (Transparency) ที่ตรวจสอบได้ทันที (Auditability) แก้ไขไม่ได้ (Immutability) และประมวลผลผลลัพธ์โดยอัตโนมัติ ตัดปัญหาเรื่องการนับคะแนนผิดพลาด หรือการทุจริตในการลงคะแนนลับ ๔. ยุทธศาสตร์ข้อมูลและความเป็นส่วนตัว (Data Governance & Privacy Paradigm) แก้ไขปัญหาความขัดแย้งระหว่างมาตรา ๑๐ (การจัดเก็บข้อมูล) กับสิทธิส่วนบุคคล ๔.๑ การจัดเก็บข้อมูลแบบแบ่งชั้นความลับอัตโนมัติ (Automated Data Classification) ระบบต้องสามารถแยกแยะและจัดเก็บข้อมูลตามชั้นความลับ (ลับที่สุด/ลับ/ปกปิด/เปิดเผย) โดยอัตโนมัติตามเนื้อหาที่พูด (Voice Recognition) ข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้องกับมติที่ประชุม ต้องถูก Anonymize (ทำให้เป็นนิรนาม) หรือลบทำลายตามระยะเวลาที่กำหนด (Data Retention Policy) ที่สอดคล้องกับ PDPA และมาตรา ๓๒ ของรัฐธรรมนูญ (สิทธิในความเป็นอยู่ส่วนตัว) ๔.๒ การเข้าถึงข้อมูลของประชาชน (Open Data Integration) การประชุมที่กฎหมายกำหนดให้เปิดเผย ต้องสามารถ Stream และ Publish ข้อมูลในรูปแบบ Machine-readable format (API) สู่อารมณ์ได้ทันที เพื่อให้ประชาชนตรวจสอบได้ตามหลักการ Open Government สอดคล้องกับมาตรา ๔๑ (สิทธิรับรู้ข้อมูลข่าวสาร) และมาตรา ๕๙ (รัฐต้องเปิดเผยข้อมูล) ๕. ยุทธศาสตร์ความต่อเนื่องทางธุรกิจและการบริหารวิกฤต (Business Continuity & Resilience) ๕.๑ รองรับสถานะวิกฤตสูงสุด (Disaster Recovery Protocol) กฎหมายต้องระบุ "แผนสำรองฉุกเฉิน" กรณี

เครือข่ายอินเทอร์เน็ตหลักล่มสลาย ให้สามารถประชุมผ่านเครือข่ายความถี่วิทยุเฉพาะกิจ หรือเครือข่ายดาวเทียม (Satellite Mesh Network) ได้ และให้ถือว่ามีผลตามกฎหมายทันที เพื่อความต่อเนื่องของรัฐ (State Continuity) ตามมาตรา ๒๕๘

-..ควรมีระบบประชุมกลาง ที่จำกัดไม่ให้บุคคลเดี่ยวเข้าประชุมได้มากกว่า ๑ คนในเวลา เดียวกัน

-..๑..ความคิดเห็นเกี่ยวกับพัฒนาการล่าสุดของกฎหมายและมาตรฐานที่เกี่ยวข้อง จากข้อมูล ล่าสุด (ณ วันที่ ๑๔ ธันวาคม ๒๕๖๘). พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓. ยังคงเป็นกฎหมายกลางหลักที่ใช้บังคับ โดยไม่มีการยกเลิกหรือแทนที่ด้วย พระราชบัญญัติฉบับใหม่เต็มรูปแบบ ซึ่งเป็นจุดที่ผมยังคงยืนยันว่าควรปรับปรุงให้ยกระดับ เป็นพระราชบัญญัติเพื่อความมั่นคงทางกฎหมายในระยะยาว (long-term legal stability) อย่างไรก็ตาม ผมชื่นชมอย่างยิ่งต่อการปรับปรุงประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐาน การรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ ซึ่งมีพัฒนาการต่อเนื่องจาก ฉบับ พ.ศ. ๒๕๖๓ ฉบับที่ ๒ พ.ศ. ๒๕๖๔ และฉบับล่าสุดใน พ.ศ. ๒๕๖๗ ที่เพิ่มเติมเรื่องการยืนยัน ตัวตนแบบหลายปัจจัย (multi-factor authentication) การป้องกันข้อมูลลับของรัฐ และการรองรับ เทคโนโลยีใหม่มากขึ้น การปรับปรุงนี้แสดงถึงความคล่องตัวของระบบบริหาร (administrative agility) ที่ดี แต่ยังคงมีช่องว่างในระดับกฎหมายหลัก เช่น การขาด framework สำหรับการทบทวน มาตรฐานอัตโนมัติทุก ๒ ปี หรือการบังคับใช้ zero-trust model อย่างเต็มรูปแบบ ซึ่งรัฐมหาอำนาจ อย่างสหรัฐฯ (ผ่าน NIST SP ๘๐๐-๒๐๗) และสหภาพยุโรป (ผ่าน ENISA Guidelines) ได้นำไปใช้ แล้วอย่างมีประสิทธิภาพสูงสุด ๒. ข้อเสนอแนะด้านการยกระดับกฎหมายหลัก (จากพระราชกำหนดสู่ พระราชบัญญัติที่ สมบูรณ์แบบ). ควรผลักดันให้มีการตรา “พระราชบัญญัติการประชุม ผ่านสื่ออิเล็กทรอนิกส์ พ.ศ.” อย่างเร่งด่วน โดยมีโครงสร้างครบวงจร ดังนี้ - บทนำและ วัตถุประสงค์ ขยายจากหมายเหตุท้ายพระราชกำหนดฯ ๒๕๖๓ ให้ครอบคลุมไม่เพียงวิกฤตสุขภาพ แต่รวมถึงการเปลี่ยนแปลงสภาพภูมิอากาศ (climate change) การลดการปล่อยก๊าซคาร์บอน ฟุตพริ้นท์จากการเดินทาง (carbon footprint reduction) และการส่งเสริมเศรษฐกิจดิจิทัล (digital economy) ตามเป้าหมาย SDG ๑๓ และ ๘ ของ UN - นิยามที่ทันสมัย ขยายนิยาม “สื่ออิเล็กทรอนิกส์” ให้รวม metaverse, VR/AR platforms, AI-assisted meetings (เช่น AI minute-taking และ real-time translation) และ quantum-safe communication เพื่อ future-proofing ๑๐๐% - ขอบเขตการยกเว้น (มาตรา ๕ เดิม) ทบทวนให้ชัดเจนขึ้น เช่น การประชุมศาล ควรเปิดช่องให้ใช้ hybrid model ในบางคดี (เช่น คดีแพ่งที่ไม่ต้องเผชิญหน้า) โดยอ้างอิงแนวปฏิบัติ ของ International Court of Justice ที่ใช้ virtual hearings ในยุคโควิด - ทั่วโลกกำลังดูแลใหม่ ตั้ง “คณะกรรมการกำกับดูแลการประชุมผ่านสื่ออิเล็กทรอนิกส์แห่งชาติ” (National Electronic Meetings Oversight Committee) ประกอบด้วยผู้แทนจากกระทรวงดิจิทัล, ก.ล.ด., สำนักงานศาล ยุติธรรม, ETDA และภาคเอกชน เพื่อรับรองแพลตฟอร์ม (platform certification) คล้าย ACRA ในสิงคโปร์ ๓. ข้อเสนอแนะด้านเทคโนโลยีและความมั่นคงปลอดภัย (ระดับสูงสุด, ทันสมัยที่สุด). - การยืนยันตัวตนและป้องกันภัยคุกคามใหม่ บังคับใช้ biometric + behavioral authentication และ AI-based deepfake detection (เช่น Microsoft Azure หรือ Google's DeepMind tools) รวมถึง post-quantum cryptography เพื่อป้องกันการโจมตีในยุค quantum computing - การลงคะแนนและความโปร่งใส นำร่อง blockchain-based voting สำหรับการประชุมผู้ถือหุ้น

(คล้ายระบบที่ใช้ในเอสโตเนียสำหรับ e-governance) เพื่อรับรอง end-to-end verifiability และ non-repudiation - การคุ้มครองข้อมูล เชื่อมโยงเต็มรูปแบบกับ PDPA โดยกำหนด data protection impact assessment (DPIA) สำหรับการประชุมทุกครั้ง และให้สิทธิ data subject ในการลบ recording หลังครบ retention period (เช่น ๕ ปี) - การรองรับ AI และ automation กำหนด guidelines สำหรับ AI moderator, auto-transcription, และ sentiment analysis เพื่อเพิ่มประสิทธิภาพ แต่ต้องมี human oversight เพื่อป้องกัน bias (สอดคล้อง EU AI Act)

๔. ข้อเสนอแนะด้านสังคม ความเสมอภาค และการเข้าถึง (Inclusivity & Digital Divide) - การเข้าถึงสำหรับกลุ่มเปราะบาง บังคับให้แพลตฟอร์มรองรับ WCAG ๒.๒ ระดับ AAA เต็มรูปแบบ รวม live captioning, sign language avatar, และ low-bandwidth mode สำหรับพื้นที่ห่างไกล เพื่อสอดคล้องมาตรา ๔ และ ๔๗ รัฐธรรมนูญ (ความเสมอภาคและการศึกษาตลอดชีวิต) - ลด digital divide รัฐควรสนับสนุน subsidy สำหรับ SMEs และชุมชนชนบทในการเข้าถึงแพลตฟอร์ม เช่น โครงการแจก device หรือ broadband subsidy คล้าย Digital India Initiative - ด้านจริยธรรม และสุขภาพ กำหนด guidelines ป้องกัน zoom fatigue เช่น การบังคับ break time ในประชุมยาว และ promotion ของ mental health awareness

๕. ข้อเสนอแนะด้านเศรษฐกิจและการแข่งขัน (Economic Impact & Competitiveness) - ส่งเสริมธุรกิจ ทำให้ประเทศไทยเป็น hub ของ virtual corporate governance ในอาเซียน โดยลดต้นทุนการประชุมผู้ถือหุ้น (AGM) ลง ๗๐-๙๐% และดึงดูดบริษัทต่างชาติมาจดทะเบียน (คล้าย Delaware model) - SMEs และ startup มี tax incentive สำหรับบริษัทที่ใช้ e-meeting อย่างเต็มรูปแบบ เพื่อเพิ่ม productivity และ resilience ในวิกฤต - การวัดผลกระทบ ตั้ง KPI ระดับชาติ เช่น เพิ่ม GDP contribution จาก digital economy ผ่าน e-meeting อย่างน้อย ๕% ใน ๕ ปี

๖. ข้อเสนอแนะด้านสิ่งแวดล้อมและความยั่งยืน (Sustainability) - นำ e-meeting มาเป็นเครื่องมือหลักในการลด carbon emission จากการเดินทาง (ตาม Paris Agreement) โดยประมาณการว่าหาก ๘๐% ของการประชุมรัฐและเอกชน เป็นออนไลน์ จะลด CO₂ ได้หลายล้านตันต่อปี - บังคับให้แพลตฟอร์มรายงาน carbon footprint ของ server และส่งเสริม green data centers

๗. ข้อเสนอแนะด้านการศึกษา ฝึกอบรม และการวิจัยพัฒนา - การฝึกอบรม จัดหลักสูตร compulsory สำหรับกรรมการบริษัท ประธานประชุม และเลขานุการ ผ่าน ETDA หรือมหาวิทยาลัยชั้นนำ - การวิจัย สนับสนุน R&D ในมหาวิทยาลัย เช่น พัฒนา Thai-native AI for meetings (real-time Thai dialect translation) - ความร่วมมือระหว่างประเทศ เข้าร่วม UN Digital Cooperation Forum และ ASEAN Digital Ministers อย่างแข็งขัน เพื่อ exchange best practices

๘. ข้อเสนอแนะด้านการกำกับดูแล การบังคับใช้ และการตรวจสอบ (Enforcement & Accountability) - โทษและการเยียวยา เพิ่มบทกำหนดโทษสำหรับการละเมิดมาตรฐาน (เช่น ฝ่าฝืน security) และกลไก complaint channel - การตรวจสอบอิสระ ให้ ป.ป.ช. หรือ ก.ล.ต. มีอำนาจ audit การประชุมสำคัญ - transitional provisions สำหรับการปรับปรุงกฎหมาย ให้มี grace period ๑-๒ ปี เพื่อให้องค์กรปรับตัว

๙. ความเป็นไปได้ในอนาคตและ scenario planning - Best case หากปรับปรุงตามข้อเสนอ ประเทศไทยจะเป็นผู้นำด้าน e-governance ในเอเชียตะวันออกเฉียงใต้ ภายใน ๒๐๓๐ - Worst case หากไม่ปรับปรุง อาจเกิดช่องโหว่ไซเบอร์ใหญ่ หรือสูญเสียความสามารถแข่งขันให้สิงคโปร์/ฮ่องกง - Balanced case ค่อยๆ ปรับผ่านประกาศกระทรวงก่อน แล้วยกระดับเป็น พ.ร.บ. ใน ๒-๓ ปี

๑.๑. การยกระดับโครงสร้างพื้นฐานทางเทคโนโลยี (Technological Infrastructure Uplift) Quantum-Resistant Encryption (การเข้ารหัสต้านทานควอนตัม) โลกกำลังก้าวเข้าสู่ยุค Quantum Computing. ซึ่งจะทำให้การเข้ารหัสแบบปัจจุบันเปราะบาง. กฎหมายและมาตรฐานเทคนิคต้องรองรับ การเข้ารหัสแบบ Post-Quantum Cryptography. เพื่อปกป้องความลับของการประชุมคณะรัฐมนตรี หรือการประชุมบอร์ดองค์กรชั้นนำจากการถูกถอดรหัสในอนาคต. Holographic Telepresence & Mixed Reality (MR). เสนอให้มีการวิจัยและรองรับมาตรฐานการประชุมแบบ Volumetric Video (วิดีโอที่มีมิติและปริมาตร). เพื่อให้ผู้เข้าร่วมรู้สึกเหมือนนั่งอยู่ในห้องเดียวกันจริงๆ (Co-presence) ลดความเหนื่อยล้าจากการจ้องหน้าจอ ๒ มิติ (Zoom Fatigue) และเพิ่มประสิทธิภาพในการอ่าน ภาษากาย (Non-verbal communication) ซึ่งสำคัญมากในการเจรจาต่อรองระดับสูง. ๒. การปฏิวัติ ระบบจัดการการประชุมด้วยปัญญาประดิษฐ์ (AI-Driven Meeting Orchestration). Real-time Semantic Analysis & Fact-Checking. ระบบการประชุมภาครัฐและเอกชนระดับสูงควรมี AI ที่ทำหน้าที่ตรวจสอบความถูกต้องของข้อมูล (Fact-Checking). แบบเรียลไทม์ โดยเชื่อมโยงกับ ฐานข้อมูลกฎหมายและสถิติแห่งชาติ. เพื่อป้องกันการตัดสินใจบนพื้นฐานข้อมูลที่ผิดพลาด. Automated Minute Generation & Sentiment Analysis. ยกเลิกการจดรายงานการประชุม ด้วยมนุษย์. แล้วใช้ AI (Natural Language Processing - NLP) ในการถอดความ. สรุปประเด็น และวิเคราะห์ "อารมณ์ความรู้สึก" (Sentiment) ของที่ประชุม. เพื่อเป็นข้อมูลเชิงลึก (Insight) ให้ประธานที่ประชุมบริหารจัดการบรรยากาศการประชุมได้ดียิ่งขึ้น. ทั้งนี้ ต้องสอดคล้องกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA). อย่างเคร่งครัด. Smart Agenda Management. AI ช่วยจัดสรรเวลาการประชุมแบบ Dynamic. หากวาระไหนใช้เวลาเกิน. ระบบจะคำนวณเวลาที่ เหลือและเสนอแนะการปรับตารางเวลาทันที. เพื่อให้การประชุมจบตรงเวลา. (Efficiency Optimization). ๓. นิติวิศวกรรมและการพิสูจน์ทราบตัวตน (Legal Engineering & Identity Assurance). Multimodal Biometric Authentication. เลิกใช้แค่ Username/Password. แต่บังคับ ใช้การยืนยันตัวตนแบบ Multimodal (เช่น. ใบหน้า + เสียง + ลายนิ้วมือ. หรือพฤติกรรมการพิมพ์). ในการเข้าร่วมประชุมที่มีชั้นความลับสูง. เพื่อให้มั่นใจว่า "ผู้เข้าประชุมคือตัวจริง". ตลอดระยะเวลา การประชุม (Continuous Authentication). ไม่ใช่แค่ตอน Login. Blockchain Notarization. ทุกมติ ที่โหวต. ทุกเอกสารที่แชร์. และ Log file ของการเข้าออกห้องประชุม. ต้องถูกบันทึกค่า Hash ลงบน Blockchain (Consortium Chain. สำหรับภาครัฐ/Enterprise). เพื่อทำหน้าที่เป็น "Notary Public ดิจิทัล" ที่เปลี่ยนแปลงแก้ไขไม่ได้ (Tamper-proof). ทำให้มีน้ำหนักเป็นพยานหลักฐานในชั้นศาลที่เถียง ไม่ได้ (Irrefutable Evidence). ๔. การจัดการประชุมข้ามพรมแดนและเขตอำนาจศาล (Cross-Border Jurisdiction & Sovereignty). Digital Embassy Concept. สำหรับการประชุมระหว่างประเทศ. เสนอให้กำหนดสถานะของ "ห้องประชุมเสมือน" (Virtual Meeting Room) ให้เป็นพื้นที่ที่มีเอกสิทธิ์ และความคุ้มกันทางทูตดิจิทัล (Digital Diplomatic Immunity). หาก Server ตั้งอยู่ในประเทศไทย. หรืออยู่ภายใต้การควบคุมของประเทศไทย. Universal Translation & Accessibility. ระบบต้องรองรับ การแปลภาษาอัตโนมัติ (AI Simultaneous Interpretation) และพี.เจ.เอ. สำหรับผู้พิการ (Accessibility). ระดับสูงสุด (WCAG ๓.๐). เพื่อความเท่าเทียมตามรัฐธรรมนูญ มาตรา ๒๗ ๕. มาตรการความต่อเนื่องทางธุรกิจและบริหารความเสี่ยง (Business Continuity & Risk Management). Offline-First Architecture. เสนอแนะให้ระบบการประชุมมีสถาปัตยกรรมแบบ Local-First. คือหากอินเทอร์เน็ตหลุด. ระบบยังสามารถบันทึกข้อมูลและ Cache ไว้ในเครื่องของผู้ใช้

แบบเข้ารหัส และ Sync กลับขึ้น Cloud ทันทีที่เชื่อมต่อได้ เพื่อป้องกันข้อมูลสูญหาย (Data Loss Prevention) Deepfake Defense Mechanism ต้องมีระบบตรวจจับ Deepfake แบบเรียลไทม์ เพื่อป้องกันมิถิลลาซีพที่ใช้ AI ปลอมใบหน้าและเสียงของผู้บริหารระดับสูงเข้ามาสั่งการในที่ประชุม (Impersonation Attack Prevention) ๖. มิติด้านสิ่งแวดล้อมและความยั่งยืน (Environmental Sustainability - Green Meeting) Carbon Footprint Tracking. ซอฟต์แวร์ประชุมควรมีพีเอเจอร์คำนวณว่า การประชุมครั้งนี้ช่วยลดปริมาณคาร์บอนจากการไม่เดินทางได้เท่าไร (Carbon Credit Calculation) เพื่อให้องค์กรนำไปใช้เคลมในรายงานความยั่งยืน (ESG Report) สนับสนุนนโยบาย BCG Economy ของรัฐบาล

- มิติที่ ๑: มิติเชิงยุทธศาสตร์และปรัชญา - การปรับกระบวนทัศน์ (Strategic & Philosophical Dimension - A Paradigm Shift) ๑.๑ จาก "การตอบสนองเชิงรับ" สู่ "การสร้าง ความได้เปรียบเชิงรุก" (From Reactive Response to Proactive Advantage):** กฎหมายปัจจุบัน ถูกสร้างขึ้นเพื่อ "แก้ปัญหา" การประชุมแบบเดิมที่ทำไม่ได้ แต่กฎหมายแห่งอนาคตต้องถูกออกแบบ เพื่อ "สร้างโอกาส" ในการตัดสินใจที่รวดเร็วขึ้น โปร่งใสขึ้น และมีส่วนร่วมมากขึ้น เราต้องเลิกมองว่า การประชุมอิเล็กทรอนิกส์เป็นเพียง "สิ่งทดแทน" แต่ต้องมองว่ามันเป็น "เครื่องมือยุทธศาสตร์" ในการ เพิ่มขีดความสามารถในการแข่งขันของประเทศ ๑.๒ จาก "การจำลองแบบกายภาพ" สู่ "การปลดปล่อย ศักยภาพดิจิทัล" (From Physical Emulation to Digital Emancipation) กฎหมายปัจจุบันยังมีกรอบ คิดที่พยายามจำลองการประชุมในห้องสี่เหลี่ยมมาไว้บนจอภาพ แต่ศักยภาพที่แท้จริงของดิจิทัลคือ การทำลายข้อจำกัดของ "เวลา" และ "สถานที่" โดยสิ้นเชิง กฎหมายใหม่ต้องส่งเสริมและรองรับรูปแบบ การทำงานร่วมกัน (Collaboration) ที่หลากหลาย เช่น การตัดสินใจแบบไม่พร้อมกัน (Asynchronous Decision-Making) หรือการระดมสมองแบบต่อเนื่องบนแพลตฟอร์มดิจิทัล ๑.๓ จาก "การควบคุมจาก ส่วนกลาง" สู่ "การสร้างระบบนิเวศที่ น่าเชื่อถือ" (From Centralized Control to Trusted Ecosystem) แทนที่การให้กระทรวงฯ เป็นผู้กำหนดมาตรฐานทางเทคนิคแต่เพียงผู้เดียว รัฐควรมุ่ง สร้าง "ระบบนิเวศ" ที่ประกอบด้วยหน่วยงานรับรองมาตรฐาน (Certification Bodies), ผู้ให้บริการ เทคโนโลยี (Technology Providers), ผู้เชี่ยวชาญด้านความปลอดภัย และผู้ใช้งาน โดยรัฐทำหน้าที่ เป็นผู้วางกรอบธรรมาภิบาลและส่งเสริมการแข่งขันบนพื้นฐานของคุณภาพและความปลอดภัย

มิติที่ ๒: มิติเชิงกฎหมายและธรรมาภิบาล - การยกเครื่องโครงสร้าง (Legal & Governance Dimension - A Structural Overhaul) ๒.๑ การยกระดับสถานะและขอบเขต "พระราชบัญญัติว่า ด้วยการกำกับดูแลกิจการและการดำเนินกระบวนกรทางอิเล็กทรอนิกส์" (The Digital Governance and Electronic Procedures Act) ควรใช้ชื่อที่ สะท้อนขอบเขตที่กว้างกว่าแค่ "การประชุม" แต่ครอบคลุมถึงกระบวนกรอนุมัติ, การลงมติ, และการดำเนินงานอื่น ๆ ที่ต้องอาศัยการตัดสินใจ ร่วมกันของคณะบุคคล ๒.๒ การนิยามศัพท์และการจำแนกประเภทอย่างละเอียด นิยาม "การประชุม" ใหม่ ต้องครอบคลุมทั้ง ๑) Synchronous (พร้อมกัน), ๒) Asynchronous (ไม่พร้อมกัน) และ ๓) Hybrid (ผสมผสาน) จำแนก "ระดับชั้นของการประชุม" (Meeting Tiers) จำแนกการประชุม ตามระดับความสำคัญและความเสี่ยง เช่น Tier ๑ (ระดับทั่วไป) การประชุมเพื่อหารือทั่วไป ใช้มาตรฐานความปลอดภัยพื้นฐาน Tier ๒ (ระดับสำคัญ) การประชุมที่มีการลงมติสำคัญ เช่น การอนุมัติงบประมาณ ต้องใช้มาตรฐานความปลอดภัยและการพิสูจน์ตัวตนที่สูงขึ้น Tier ๓ (ระดับ ความลับสูงสุด) การประชุมที่เกี่ยวข้องกับความมั่นคง, ข้อมูลอ่อนไหว หรือความลับทางการค้า ต้องใช้ เทคโนโลยีการเข้ารหัสแบบ End-to-End และระบบพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor

Authentication) ที่รัดกุมที่สุด ๒.๓ การสร้างหลักประกันเชิงบูรณาการของพยานหลักฐาน (Evidentiary Integrity) "ห่วงโซ่พยานหลักฐานดิจิทัล" (Digital Chain of Custody) กฎหมายต้องกำหนดให้มีกระบวนการที่ชัดเจนตั้งแต่การสร้าง, การบันทึก, การจัดเก็บ, จนถึงการนำเสนอพยานหลักฐานจากการประชุมอิเล็กทรอนิกส์ ข้อกำหนดเชิงบังคับ ๑. การพิสูจน์ตัวตนก่อนเข้าประชุม ต้องเชื่อมโยงกับระบบ Digital ID ของประเทศ ๒. การเข้ารหัสการสื่อสาร บังคับใช้การเข้ารหัสตลอดเส้นทาง (In-transit) และอาจถึงขั้นเข้ารหัสจากต้นทางถึงปลายทาง (End-to-End) สำหรับการประชุม Tier ๓ ๓. การประทับเวลาที่น่าเชื่อถือ (Trusted Timestamping) ทุกกิจกรรมสำคัญ (การล็อกอิน, การพูด, การลงคะแนน, การสิ้นสุดการประชุม) ต้องถูกประทับเวลาโดยอัตโนมัติจากแหล่งเวลาที่น่าเชื่อถือ ๔. การสร้างบันทึกกิจกรรมที่ไม่สามารถเปลี่ยนแปลงได้ (Immutable Audit Log) ใช้เทคโนโลยีเช่น Blockchain หรือ WORM (Write Once, Read Many) ในการจัดเก็บบันทึกกิจกรรม เพื่อให้สามารถตรวจสอบย้อนหลังได้โดยมั่นใจว่าไม่มีการแก้ไข ๕. ลายมือชื่อดิจิทัลสำหรับรายงานการประชุม รายงานการประชุมฉบับสุดท้ายต้องได้รับการลงนามด้วยลายมือชื่อดิจิทัลจากประธานและเลขานุการ เพื่อยืนยันความถูกต้องและมีผลทางกฎหมายสมบูรณ์ ๒.๔ การปฏิรูปกลไกการลงคะแนน ระบบต้องบันทึกการลงคะแนนของแต่ละบุคคลอย่างชัดเจนและเชื่อมโยงกับ Digital ID ลงคะแนนลับต้องใช้เทคโนโลยี Zero-Knowledge Proofs หรือเทคนิคการเข้ารหัสขั้นสูงที่สามารถ "พิสูจน์ได้ว่าการนับคะแนนถูกต้อง โดยไม่ต้องเปิดเผยว่าใครลงคะแนนอย่างไร" นี้คือมาตรฐานสูงสุดที่สร้างความไว้วางใจได้จริง ๒.๕ การกำหนดความรับผิดชอบและกลไกระงับข้อพิพาท (Liability & Dispute Resolution) กฎหมายปัจจุบันไม่ได้กล่าวถึงเรื่องนี้เลย ซึ่งเป็นช่องว่างขนาดใหญ่ ความรับผิดชอบของผู้จัดประชุม ต้องมีหน้าที่ในการเลือกใช้แพลตฟอร์มที่ได้มาตรฐานและแจ้งเงื่อนไขทางเทคนิคให้ผู้เข้าร่วมทราบล่วงหน้า ความรับผิดชอบของผู้ให้บริการแพลตฟอร์ม ต้องรับผิดชอบต่อความเสถียรและความปลอดภัยของระบบตามข้อตกลงระดับการให้บริการ (SLA) สถานะของผู้เข้าร่วมที่หลุดจากการประชุม ต้องมีบทบัญญัติที่ชัดเจนว่า หากผู้เข้าร่วมประชุมหลุดการเชื่อมต่อ ในช่วงเวลาสำคัญ (เช่น ขณะลงคะแนน) จะมีผลอย่างไร จะถือว่าไม่ครบองค์ประชุมหรือไม่ หรือจะให้มีการพักการประชุมเพื่อรอ ซึ่งต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อป้องกันการใช้เป็นข้ออ้างในการขัดขวางการประชุม กลไกระงับข้อพิพาท กำหนดให้มีกระบวนการอนุญาโตตุลาการทางออนไลน์ (Online Dispute Resolution) สำหรับข้อพิพาทที่เกิดจากการประชุมอิเล็กทรอนิกส์โดยเฉพาะ

มติที่ ๓: มติเชิงเทคโนโลยีและการปฏิบัติงาน - การสร้างเครื่องมือและมาตรฐาน (Technological & Operational Dimension - Building Tools & Standards) ๓.๑ มาตรฐานการทำงานร่วมกัน (Interoperability Standards) รัฐต้องกำหนดมาตรฐานกลางเพื่อให้แพลตฟอร์มที่แตกต่างกันสามารถเชื่อมต่อและแลกเปลี่ยนข้อมูลพื้นฐานกันได้ เช่น การยืนยันตัวตนผู้เข้าร่วมประชุม, การส่งเอกสารประกอบการประชุมอย่างปลอดภัย ๓.๒ ระบบการรับรองและการทดสอบ (Certification & Sandbox) "Thailand E-Meeting Certified" จัดตั้งหน่วยงานรับรองที่เป็นอิสระ (อาจอยู่ภายใต้ ETDA) เพื่อตรวจสอบและให้การรับรองแพลตฟอร์มการประชุมตามระดับชั้นความเสี่ยง (Tier ๑, ๒, ๓) ที่กล่าวไปข้างต้น "Regulatory Sandbox" เปิดพื้นที่ให้ผู้พัฒนานวัตกรรมใหม่ๆ ด้านการประชุม (เช่น การใช้ AI, VR) สามารถทดลองบริการได้ภายใต้การกำกับดูแล เพื่อให้กฎหมายและนวัตกรรมเติบโตไปพร้อมกัน ๓.๓ การบูรณาการกับโครงสร้างพื้นฐานดิจิทัลของประเทศ Digital ID บังคับให้ การแสดงตนต้องผ่านระบบ Digital ID แห่งชาติ Government Data Center/Cloud ส่งเสริมให้ ข้อมูลการประชุมของหน่วยงานภาครัฐถูกจัดเก็บในระบบคลาวด์กลางภาครัฐที่มีความมั่นคงปลอดภัยสูง

มิติที่ ๔: มิติเชิงสังคมและเศรษฐกิจ – การสร้างประโยชน์และลดผลกระทบ. (Socio-Economic Dimension – Creating Benefits & Mitigating Impacts). ๔.๑. การลดความเหลื่อมล้ำทางดิจิทัล. (Bridging the Digital Divide) กฎหมายต้องกำหนดให้เป็นหน้าที่ของ "ผู้จัดการประชุม" ที่จะต้องจัดหาทางเลือกหรือให้การสนับสนุนผู้เข้าร่วมประชุมที่ไม่สามารถเข้าถึงเทคโนโลยีได้ เช่น การจัดตั้งจุดบริการเข้าร่วมประชุม. (Hybrid Hub) ในระดับชุมชนหรือหน่วยงาน... ๔.๒. การสร้างศักยภาพบุคลากร. (Capacity Building) จัดทำหลักสูตรอบรมและออกใบรับรองสำหรับ "ผู้ควบคุมการประชุมอิเล็กทรอนิกส์" (Certified E-Meeting Administrator) และ "เลขานุการดิจิทัล" (Digital Corporate Secretary) เพื่อสร้างบุคลากรที่มีความเชี่ยวชาญในการจัดการประชุมให้เป็นไปตามกฎหมายและหลักปฏิบัติที่ดีที่สุด... ๔.๓. การส่งเสริมเศรษฐกิจดิจิทัล. การมีกฎหมายและมาตรฐานที่ชัดเจนจะกระตุ้นให้เกิดการพัฒนาแพลตฟอร์มการประชุมโดยผู้ประกอบการไทย. และดึงดูดการลงทุนจากต่างประเทศ. เนื่องจากไทยจะมีกรอบธรรมาภิบาลดิจิทัลที่น่าเชื่อถือ... มิติที่ ๕: มิติการรองรับอนาคต – การออกแบบเพื่อความยั่งยืน. (Future-Proofing Dimension – Designing for Sustainability) ๕.๑. ความเป็นกลางทางเทคโนโลยี. (Technology Neutrality) ตัวบทกฎหมายต้องเขียนในระดับหลักการ. เพื่อไม่ให้ล้าสมัยเมื่อมีเทคโนโลยีใหม่เกิดขึ้น... ๕.๒. การกำกับดูแลปัญญาประดิษฐ์. (AI Governance in Meetings) กฎหมายต้องวางกรอบการใช้ AI ในการประชุม. เช่น AI ช่วยสรุปประเด็น. AI ช่วยถอดเทป. หรือ AI ช่วยวิเคราะห์ข้อมูลประกอบการตัดสินใจ. โดยต้องมีหลักการเรื่องความโปร่งใส. (Transparency) และความสามารถในการอธิบายได้. (Explainability) ของ AI... ๕.๓. การรองรับสภาพแวดล้อมเสมือนจริง. (Metaverse & Immersive Environments) นิยามของ "สื่ออิเล็กทรอนิกส์" ต้องกว้างพอที่จะครอบคลุมการประชุมในรูปแบบ VR/AR และ Metaverse ซึ่งจะมีประเด็นเรื่องการพิสูจน์ตัวตนของ "อวตาร" (Avatar) และการบันทึกหลักฐานในโลกเสมือน... ๕.๔. กลไกการทบทวนกฎหมายตามกำหนดเวลา. (Scheduled Legislative Review) บรรจุมติที่กำหนดให้ต้องมีการทบทวนและปรับปรุงพระราชบัญญัตินี้ในทุกๆ ๓-๕ ปี. เพื่อให้กฎหมายสามารถไล่ตามการเปลี่ยนแปลงของเทคโนโลยีและบริบทของโลกได้ทันทั่วทั้ง

๑. เสนอให้มีกฎหมายแม่บทใหม่ระดับ "พระราชบัญญัติการประชุมดิจิทัลแห่งชาติ" พระราชกำหนดฯ ๒๕๖๓ เป็นกฎหมายในสถานการณ์ฉุกเฉิน ฉะนั้นควรยกระดับเป็นพระราชบัญญัติ เพื่อ: วางกรอบถาวร. ไม่ต้องอิงวิกฤติ. มีความมั่นคงทางกฎหมาย. ผ่านการพิจารณาของรัฐสภา. ตามมาตรา ๓. และ ๕ รัฐธรรมนูญ. สร้างมาตรฐานระดับชาติที่สามารถรองรับเทคโนโลยีก้าวกระโดด... ๒. จัดตั้ง "ศูนย์กำกับและรับรองการประชุมผ่านสื่ออิเล็กทรอนิกส์แห่งชาติ" เสนอจัดตั้งองค์กรเฉพาะทางที่มีภารกิจ: รับรองแพลตฟอร์มประชุมออนไลน์. (Certification) ตรวจสอบมาตรฐานความมั่นคงปลอดภัยและข้อมูลส่วนบุคคล. เชื่อมต่อ. Cybersecurity กับสำนักงาน. กสทช... สำนักงาน คปภ... ดีอีเอส. รองรับการประชุมงานกับประเทศมหาอำนาจ. (US, EU, China, Japan)... ๓. พัฒนา "Digital Identity" สำหรับการประชุมออนไลน์อย่างเป็นทางการ. เพื่อแก้ปัญหาการแสดงตนแบบทั่วไป. ควรมีการยืนยันตัวตนผ่าน Digital ID ระดับสูงสุด. (ระดับ ๔) การเชื่อมกับบัตรประชาชนดิจิทัล. การใช้เทคโนโลยี. Face Recognition, Voice ID. แบบไม่ละเมิดความเป็นส่วนตัว. ระบบตรวจจับการปลอมแปลงภาพ/เสียง (deepfake detection)... ๔. จัดให้มีมาตรฐาน AI ในการประชุมออนไลน์ยุคใหม่มี AI เข้าร่วมประชุมอย่างหลีกเลี่ยงไม่ได้. จึงควรมีมาตรฐานดังนี้ AI เป็น "ผู้ช่วยประชุม" (ไม่ใช่ผู้ลงคะแนน). ระบบสรุปอัตโนมัติแบบตรวจสอบย้อนกลับได้. (audit friendly) การกำหนดขอบเขตข้อมูลที่ AI จะเข้าถึงตาม PDPA และรัฐธรรมนูญ มาตรา ๓๒ การเข้ารหัสข้อมูลที่ AI ประมวล

เพื่อป้องกันการรั่วไหล...๕. ปรับปรุงการบันทึกภาพ/เสียงให้ยืดหยุ่นและปลอดภัย มาตรฐาน ๙ (๔) ปัจจุบัน บังคับค่อนข้างแข็ง ควรมีระบบใหม่ บันทึกเฉพาะ “ช่วงที่เป็นทางการ” กำหนดชัดเจนว่า “พักการประชุม” ไม่ต้องบันทึก จัดให้มี Metadata ครบ วัน-เวลา, IP, Digital Signature มีระบบ เก็บข้อมูล ๓ ชั้น Local, Cloud ในประเทศ, สำรองเพื่อความมั่นคง...๖. รองรับการประชุมข้ามชาติ และองค์กรระหว่างประเทศ เพื่อให้ไทยสามารถเป็น “International Digital Meeting Hub” ของอาเซียน ควรกำหนด: มาตรฐาน dual-language meeting การประชุมข้ามเขตอำนาจรัฐ (cross-border jurisdiction) ระบบแปลภาษาแบบ Real-time AI (พร้อมตรวจสอบความถูกต้อง) ๗. ปรับกฎการประชุมลับให้ทันเทคโนโลยียุคใหม่ การประชุมลับควรมีระบบ: การเข้ารหัสระดับทหาร (Military-grade Encryption) ระบบ self-destruct data (ลบอัตโนมัติเมื่อถึงเวลา) การปฏิเสธ การบันทึกหน้าจอโดยไม่ได้รับอนุญาต ระบบ Zero Trust Access ใช้เซิร์ฟเวอร์อยู่ภายใน ราชอาณาจักร (ไม่ฝากไว้ในต่างประเทศ)...๘. ปรับมาตรฐานความปลอดภัยตามหลักสากล ควรยกมาตรฐานด้านความปลอดภัยไซเบอร์ให้รองรับ: ISO/IEC ๒๗๐๐๑, ISO ๒๗๗๐๑ (Privacy) NIST Cybersecurity Framework Zero Trust Architecture Multi-factor Authentication End-to-end Encryption...๙. กำหนดระบบตรวจสอบทุจริตในการประชุมออนไลน์ เพื่อป้องกันปัญหา การแสดงตัวแทนคนอื่นเข้าประชุม การลงคะแนนแทน การลอบบี้หลังกล้อง การแก้ไขรายงาน การประชุมย้อนหลัง ควรเพิ่มระบบ Audit Trail ครบถ้วน Digital Evidence ที่เชื่อถือได้ตามมาตรา ๑๑ ของพระราชกำหนดฯ การผูกกระบบกับ Blockchain สำหรับความโปร่งใส...๑๐. กำหนดมาตรฐาน การบริหารจัดการข้อมูลระยะยาว เพื่อไม่ให้ข้อมูลสูญหายหรือถูกแก้ไขย้อนหลัง เก็บข้อมูลขั้นต่ำ ๕-๑๐ ปี มีระบบ hashing ป้องกันแก้ไข ใช้ timestamping ตามมาตรฐาน ETSI EU มีระบบการคืน ข้อมูลเมื่อถูกฟ้องร้องหรือสอบสวน...๑๑. กำหนดสิทธิของผู้เข้าร่วมประชุม ต้องสอดคล้องกับ รัฐธรรมนูญ สิทธิความเป็นส่วนตัว (มาตรา ๓๒) สิทธิการสื่อสาร (มาตรา ๓๖) เสรีภาพการแสดง ความเห็น (มาตรา ๓๔) ผู้เข้าร่วมต้องได้รับการแจ้งวัตถุประสงค์การบันทึก การแจ้งระยะเวลาการเก็บ ข้อมูล สิทธิในการคัดค้านการใช้ข้อมูลเกินจำเป็น...๑๒. ใช้ระบบเวลาเป็นมาตรฐานเดียว (Time Standardization) เพื่อจัดการปัญหาความคลาดเคลื่อน ใช้ National Time Server ลงเวลาในทุก รายการประชุม ป้องกันการแก้ไขเวลาย้อนหลังแบบไม่ถูกตรวจพบ...๑๓. พัฒนาระบบการประชุม Hybrid ให้เป็นมาตรฐานชาติ รองรับทั้ง On-site + Online เช่นในองค์กรชั้นนำของโลก ควรมี การันตีสองชั้นประชุมแบบอัตโนมัติ การลงคะแนนทั้ง onsite/offsite ที่เท่าเทียม ไมโครโฟนอัจฉริยะ ที่จับเสียงทุกฝั่งอย่างยุติธรรม ระบบกล้องอัตโนมัติตรวจจับผู้พูด (auto-focus)...๑๔. เสนอให้มี “โครงสร้างข้อมูลกลางแห่งชาติด้านการประชุมออนไลน์” รองรับ: หน่วยงานราชการทั้งหมด องค์กร อิสระ อปท. รัฐวิสาหกิจ เอกชนขนาดใหญ่ ลดต้นทุนมหาศาล ลดความซ้ำซ้อน เพิ่มความปลอดภัย ๑๕. พัฒนา “มาตรฐานจริยธรรมการประชุมออนไลน์” เพื่อให้สอดคล้องทั้งหลักกฎหมายและ หลักคุณธรรม เช่น มารยาทการประชุมออนไลน์ การไม่ใช้ภาพ/เสียงหลอกลวง การรักษาความลับ การใช้กล้อง/ไมค์อย่างเหมาะสม การไม่ใช้ข้อมูลการประชุมไปเผยแพร่โดยพลการ

...๑. การสร้าง “เอกราชทางดิจิทัล” ในระบบการประชุม (Digital Sovereignty & Infrastructure) นอกเหนือจากตัวพระราชกำหนดแล้ว รัฐควรผลักดันให้มีการสร้าง “แพลตฟอร์ม การประชุมแห่งชาติ” (National Secure Meeting Platform) บนระบบคลาวด์กลางภาครัฐ (Government Cloud) ที่มีมาตรฐานความปลอดภัยระดับทหาร (Military-Grade Security) หรือเทียบเท่ามาตรฐาน FedRAMP ของสหรัฐอเมริกา เพื่อลดการพึ่งพาแพลตฟอร์มต่างชาติในการ

ประชุมที่มีชั้นความลับสูง และเพื่อให้ข้อมูลจราจรคอมพิวเตอร์และข้อมูลการประชุมยังคงอยู่ ในราชอาณาจักร (Data Localization) ซึ่งสอดคล้องกับหน้าที่ของรัฐตามรัฐธรรมนูญ มาตรา ๕๒ ในการรักษาความมั่นคงของรัฐและผลประโยชน์ของชาติ ๒. การยกระดับสู่ "การประชุมอัจฉริยะ" ด้วย AI และ Automation (AI-Driven Smart Meetings) กฎหมายควรเปิดช่องและรับรองผลทางกฎหมายของการใช้ปัญญาประดิษฐ์ (Artificial Intelligence) ในบทบาทของผู้ช่วยเลขานุการ การประชุม ได้แก่ Automated Minute Taking การใช้ AI ถอดความและสรุปรายงานการประชุม แบบ Real-time ที่มีความแม่นยำสูง Quorum Check & Behavior Analysis การใช้ AI ตรวจสอบองค์ประชุมตลอดเวลา (Continuous Verification) และแจ้งเตือนหากองค์ประชุมไม่ครบถ้วน โดยอัตโนมัติ เพื่อป้องกันปัญหาทางข้อกฎหมายในภายหลัง Legal Compliance Bot มีระบบ AI ให้คำแนะนำข้อกฎหมายเบื้องต้นแก่ประธานในที่ประชุมทันทีหากมีการดำเนินการที่สุ่มเสี่ยงต่อการขัดข้องบังคับ ช่วยเพิ่มประสิทธิภาพการทำงานตามรัฐธรรมนูญ มาตรา ๗๖ ที่รัฐพึงพัฒนาระบบบริหารราชการให้มีประสิทธิภาพและทันสมัย ๓. การบูรณาการระบบ "e-Notary" และ "Smart Contracts" ในมติที่ประชุม เมื่อที่ประชุมมีมติ กฎหมายควรรับรองให้มตินั้นสามารถแปลงเป็น Smart Contract บนระบบ Blockchain ได้ทันที เพื่อให้เกิดการบังคับใช้ผลของมติโดยอัตโนมัติ (Automated Execution) เช่น การอนุมัติการจ่ายเงิน การเปลี่ยนแปลงอำนาจลงนาม หรือการส่ง การทางบริหาร สิ่งนี้จะลดขั้นตอนราชการ (Red Tape) และสร้างความโปร่งใสตรวจสอบได้ (Auditability) ขึ้นสูงสุด ซึ่งสอดคล้องกับเจตนารมณ์ในการปราบปรามการทุจริตตามหมวด ๑๐ และหมวด ๑๒ ของรัฐธรรมนูญ ๔. มาตรฐาน "ความพร้อมพิสูจน์พยานหลักฐานทางดิจิทัล" (Digital Forensics Readiness) ควรกำหนดให้ระบบการประชุมต้องมีคุณสมบัติ Non-repudiation (การห้ามปฏิเสธความรับผิดชอบ) ที่เข้มแข็ง กล่าวคือ ผู้เข้าประชุมไม่สามารถปฏิเสธได้ว่าตนไม่ได้พูด หรือไม่ได้ลงคะแนนในลักษณะนั้น ๆ โดยต้องมีการใช้ Digital Signature ที่เข้ารหัสกับทุก การกระทำ (Action Log) ที่สำคัญ เพื่อให้กระบวนการยุติธรรมตามรัฐธรรมนูญ มาตรา ๖๘ ดำเนินไปได้อย่างรวดเร็วและเป็นธรรม หากมีข้อพิพาทเกิดขึ้น หลักฐานดิจิทัลเหล่านี้ต้องมีน้ำหนัก เพียงพอในชั้นศาลโดยไม่ต้องเสียเวลาพิสูจน์ทางเทคนิคซ้ำซ้อน ๕. การรองรับ "การประชุมแบบ ผสมผสาน" (Hybrid Meeting Governance) อย่างไรก็ดีต่อไป กฎหมายฉบับปรับปรุงต้องระบุ ให้ชัดเจนถึงสถานะและศักดิ์ศรีที่ "เท่าเทียมกัน" ระหว่างผู้ที่นั่งในห้องประชุมจริง (Physical) และผู้ที่ผ่านสื่ออิเล็กทรอนิกส์ (Virtual) การนับคะแนนเสียง การใช้สิทธิอภิปราย ต้องไม่มีความเหลื่อมล้ำ (Inclusivity) เพื่อประกันความเสมอภาคตามรัฐธรรมนูญ มาตรา ๒๗ ว่าด้วยความเท่าเทียมกันในกฎหมาย และจัดการเลือกปฏิบัติ ๖. การคำนึงถึงสิ่งแวดล้อมและความยั่งยืน (Green Meeting & ESG) ควรระบุในบทนำหรือเจตนารมณ์ของกฎหมายว่า การส่งเสริมการประชุม อิเล็กทรอนิกส์ เป็นส่วนหนึ่งของนโยบายรัฐในการลดการปล่อยก๊าซคาร์บอนไดออกไซด์จากการเดินทาง (Carbon Footprint Reduction) สอดรับกับหน้าที่ของรัฐตามรัฐธรรมนูญ มาตรา ๕๗ (๒) ในการอนุรักษ์สิ่งแวดล้อม และสอดคล้องกับเป้าหมายการพัฒนาที่ยั่งยืน (SDGs) ในระดับสากล ๗. การเตรียมความพร้อมรับมือภัยคุกคามทางควอนตัม (Post-Quantum Cryptography) ในฐานะ ผู้มองการณ์ไกล กฎหมายควรกำหนดให้มาตรฐานความปลอดภัยต้องเตรียมพร้อมรองรับ Quantum Computing ที่อาจจะรหัสลับปัจจุบันได้ในอนาคต ดังนั้น ระบบการจัดเก็บข้อมูลการประชุมลับ ระดับชาติ ต้องเริ่มใช้การเข้ารหัสแบบ Quantum-Safe หรือ Post-Quantum Cryptography ตั้งแต่วันนี้ เพื่อให้ข้อมูลความลับของทางราชการและภาครัฐกิจ ปลอดภัยยั่งยืนยาวนานนับทศวรรษ

๑.๑. ยุทธศาสตร์การยกระดับกฎหมาย: กระบวนการที่สร้างการมีส่วนร่วมและความยั่งยืน จัดตั้งคณะกรรมการร่างฉบับสมบูรณ์. ควรมีการแต่งตั้งคณะกรรมการร่าง "พระราชบัญญัติว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์" (หรือชื่ออื่นที่เหมาะสมกว่า) อย่างเป็นทางการ โดยองค์ประกอบของคณะกรรมการต้องมาจากหลากหลายภาคส่วน. (Multi-stakeholder) ประกอบด้วยผู้แทนจากหน่วยงานกำกับดูแล (กระทรวงดิจิทัลฯ, สำนักงานคณะกรรมการกฤษฎีกา, ETDA) ผู้แทนจากภาคเอกชน (สภาหอการค้าแห่งประเทศไทย, สภาอุตสาหกรรมแห่งประเทศไทย, สมาคมบริษัทจดทะเบียนไทย) นักกฎหมายผู้เชี่ยวชาญด้านเทคโนโลยี. (Tech. Lawyers) และกฎหมายคุ้มครองข้อมูลส่วนบุคคล, นักวิชาการจากสถาบันการศึกษา, ผู้แทนจากภาคประชาสังคม เพื่อสะท้อนมุมมองด้านสิทธิผู้บริโภคและพลเมืองดิจิทัล. กระบวนการรับฟังความคิดเห็นสาธารณะ. เชิงรุก. (Proactive Public Consultation) แทนที่จะรอให้ร่างเสร็จแล้วจึงเปิดรับฟังความคิดเห็น ควรจัดกระบวนการรับฟังความคิดเห็นตั้งแต่ขั้นตอนการวางหลักการ เพื่อให้กฎหมายที่ออกมาตอบโจทย์ ความต้องการที่แท้จริงและลดอุปสรรคในการบังคับใช้ในภายหลัง. ๒. การขยายขอบเขตและวิสัยทัศน์ ของกฎหมายจาก "การประชุม" สู่ "ปฏิสัมพันธ์ทางดิจิทัล" บูรณาการสู่ "พระราชบัญญัติว่าด้วย ปฏิสัมพันธ์ทางดิจิทัลแบบบูรณาการ" ในระยะยาว. ประเทศไทยควรมีกฎหมายกลางที่ครอบคลุม ปฏิสัมพันธ์ทางดิจิทัลที่สำคัญทางกฎหมายทั้งหมด. ไม่ใช่แค่การประชุม. โดยอาจรวมถึงการลงมติ ทางอิเล็กทรอนิกส์. (e-Voting) สำหรับการลงมติของคณะกรรมการ. หรือผู้ถือหุ้นในเรื่องต่าง ๆ นอกวาระการประชุม. การลงลายมือชื่อดิจิทัลและการจัดการเอกสารอิเล็กทรอนิกส์. (Digital Signature & Document Management) การรับรองมติ. รายงานการประชุม. และเอกสารสำคัญอื่น ๆ การยืนยันตัวตนดิจิทัล. (Digital ID) การเชื่อมโยงกฎหมายนี้เข้ากับระบบ. National Digital ID เพื่อสร้างกระบวนการยืนยันตัวตนที่น่าเชื่อถือและไร้รอยต่อ. กำหนดมาตรฐานแบบจำแนกระดับความเสี่ยง. (Risk-Based Approach) กฎหมายไม่ควรกำหนดมาตรฐานความปลอดภัยแบบ "หนึ่งขนาด. เหมาะกับทุกคน". (One-size-fits-all) แต่ควรจำแนกประเภทของการประชุมตามระดับความเสี่ยง. และความสำคัญ. เช่น ระดับความเสี่ยงต่ำ. การประชุมภายในทีมงาน. อาจใช้แพลตฟอร์มทั่วไปได้. ระดับความเสี่ยงปานกลาง. การประชุมคณะกรรมการบริษัททั่วไป. อาจต้องมีระบบยืนยันตัวตนสองชั้น (2FA) และการเข้ารหัส. ระดับความเสี่ยงสูง. การประชุมผู้ถือหุ้นของบริษัทมหาชน. การประชุมลับของ หน่วยงานความมั่นคง. หรือการประชุมที่ต้องมีการลงคะแนนลับ. อาจต้องใช้ระบบที่ได้รับการรับรอง. มาตรฐานความปลอดภัยระดับสูง. มีการเข้ารหัสแบบ End-to-End และมีระบบ Audit Trail ที่ตรวจสอบได้ทุกขั้นตอน. ๓. ข้อเสนอแนะเชิงปฏิบัติการและการสร้างระบบนิเวศ. (Operational Recommendations & Ecosystem Building) การส่งเสริมศักยภาพและความรู้ความเข้าใจ ด้านดิจิทัล. (Digital Literacy & Capacity Building) ภาครัฐควรจัดทำคู่มือ. แนวปฏิบัติที่ดี. (Best Practices) และจัดอบรมให้แก่หน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน. โดยเฉพาะเลขานุการบริษัท. (Company Secretary) และผู้ที่เกี่ยวข้อง. เพื่อให้เข้าใจถึงข้อกฎหมายและข้อปฏิบัติด้านเทคนิค. อย่างถ่องแท้. การออกแบบเพื่อทุกคน. (Universal Design & Accessibility) กฎหมายควรส่งเสริม หรือกำหนดให้แพลตฟอร์มการประชุมต้องออกแบบโดยคำนึงถึงผู้พิการและผู้สูงอายุ. เช่น ร่องรับ. โปรแกรมอ่านหน้าจอ. (Screen Reader) มีคำบรรยายแทนเสียง. (Closed Captioning) และมีรูปแบบการใช้งานที่ง่าย. กลไกระงับข้อพิพาททางอิเล็กทรอนิกส์. (Online Dispute Resolution - ODR) ควรมีนบทบัญญัติที่รองรับกรณีเกิดข้อพิพาทจากการประชุมทางอิเล็กทรอนิกส์. เช่น กรณีระบบล่ม. ระหว่างการลงคะแนนเสียงที่สำคัญ. หรือกรณีมีข้อโต้แย้งเรื่องการยืนยันตัวตน. อาจกำหนดให้มีกลไก.

การระงับข้อพิพาทเบื้องต้นที่รวดเร็วและมีประสิทธิภาพ การรับรองผู้ให้บริการและกระบวนทนาย ทดลองนวัตกรรม (Service Provider Certification & Regulatory Sandbox) Certification ให้หน่วยงานเช่น ETDA ทำหน้าที่รับรองผู้ให้บริการแพลตฟอร์มประชุมออนไลน์ (Certified e-Meeting Provider) เพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้งาน Sandbox จัดตั้ง Regulatory Sandbox เพื่อเปิดโอกาสให้ผู้พัฒนานวัตกรรมและเทคโนโลยีใหม่ ๆ เกี่ยวกับการประชุม (เช่น การใช้ Blockchain ในการลงคะแนนเสียง) สามารถทดลองบริการได้ภายใต้การกำกับดูแลที่ยืดหยุ่น ก่อนที่จะนำมาปรับใช้ในวงกว้าง

๒๐. พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ ยังคงมีความเหมาะสมกับสภาพการณ์ปัจจุบัน (ผู้ให้ความคิดเห็น : สำนักงานอัยการสูงสุด (เป็นหนังสือ))

๒๑. พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ มีความเหมาะสมถือเป็นกฎหมายกลางที่วางหลักเกณฑ์เกี่ยวกับการประชุมผ่านสื่ออิเล็กทรอนิกส์ รวมถึงแนวทางการปฏิบัติสำหรับการประชุมผ่านสื่ออิเล็กทรอนิกส์ไว้ โดยมีวัตถุประสงค์เพื่อกำหนดให้การประชุมผ่านสื่ออิเล็กทรอนิกส์ใด ๆ สามารถดำเนินการภายใต้มาตรฐานที่กำหนดไว้ เช่น มาตรฐานการประชุมผ่านสื่ออิเล็กทรอนิกส์ มาตรฐานการประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องลับ และมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงมาตรฐานอื่น ๆ ตามประกาศกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคมที่กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับระบบควบคุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ที่กำหนดขอบเขตการประชุมผ่านสื่ออิเล็กทรอนิกส์ไว้ นอกจากนี้ ถือเป็นกรอำนวยการอำนวยความสะดวกให้กับหน่วยงานภาครัฐและภาคเอกชนที่นำเทคโนโลยีมาใช้กับกระบวนการทำงานวิถีใหม่ และมีความสอดคล้องกับสภาพการณ์ปัจจุบันสำหรับการพัฒนา กฎหมายให้มีความทันสมัยเพื่อรองรับความก้าวหน้าทางเทคโนโลยี ในเรื่องการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล ควรกำหนดมาตรการให้มี การปลอมแปลงจดหมายอิเล็กทรอนิกส์เชิญประชุมโดยแฮกเกอร์ เพื่อขโมยข้อมูลส่วนบุคคลของผู้อื่นได้ เช่น กำหนดให้ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของหน่วยงานหรือภาครัฐเท่านั้นในการส่งลิงค์ การประชุม มาตรการตรวจสอบหรือป้องกันมิให้ผู้เข้าร่วมประชุมบันทึกภาพนิ่ง วิดีโอ หรือคลิปเสียง ของผู้เข้าร่วมประชุมอื่นโดยไม่ได้รับความยินยอม มาตรการขอความยินยอมจากผู้เข้าร่วมประชุมทุกคน ในการบันทึกภาพนิ่ง วิดีโอ หรือคลิปเสียงระหว่างประชุม และการขอเพิกถอนความยินยอมหรือให้ลบ ทำลายข้อมูลด้วย ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ด้วย (ผู้ให้ความคิดเห็น : สำนักงานศาลยุติธรรม (เป็นหนังสือ))

๒๐. ได้นำรายงานการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากกฎหมายของกฎหมายฉบับนี้ (ถ้ามี) มาประกอบการพิจารณาด้วยแล้วหรือไม่

ไม่มี

๒๑. หน่วยงานได้

๒๑.๑ ออกกฎหรือดำเนินการอย่างหนึ่งอย่างใดตามที่กฎหมายบัญญัติไว้ เพื่อที่ประชาชนจะสามารถปฏิบัติตามกฎหมายหรือได้รับสิทธิประโยชน์จากกฎหมายหรือไม่ อย่างไร

ได้มีการออกกฎ ดังนี้

(๑). ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ อันเป็นการกำหนดหลักการสำคัญของ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ได้แก่ การรักษาความลับ (confidentiality) เพื่อป้องกันการเข้าถึง ใช้ หรือเปิดเผยข้อมูลโดยผู้ไม่มีสิทธิ การรักษาความถูกต้องครบถ้วน (integrity) เพื่อป้องกันข้อมูลไม่ให้อีกแก้ไข สูญหาย เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาต การรักษาสภาพพร้อมใช้งาน (availability) เพื่อให้ข้อมูลอิเล็กทรอนิกส์สามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ และการคุ้มครองข้อมูลส่วนบุคคล ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยผู้ให้บริการต้องดำเนินการตามข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการประชุมผ่านสื่ออิเล็กทรอนิกส์ใน ๑๐ วัตถุประสงค์ ดังนี้ นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล การบริหารจัดการสินทรัพย์ การควบคุมการเข้าถึง การเข้ารหัสลับข้อมูล การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ความมั่นคงปลอดภัยสำหรับการดำเนินงาน ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ และการบริหารจัดการความเสี่ยง

(๒). ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๔ อันเป็นการกำหนดมาตรฐาน การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม และมาตรฐานระบบ การลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

(๓). ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๗ อันเป็นการกำหนดให้ การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องที่มีชั้นความลับของหน่วยงานของรัฐ สามารถใช้ระบบ ควบคุมการประชุมที่ติดตั้งและให้บริการนอกราชอาณาจักรได้ โดยเพิ่มเงื่อนไขการยืนยันตัวตน แบบหลายปัจจัย และการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง หรือในลักษณะที่ผู้ให้บริการ ไม่สามารถเข้าถึงข้อมูลที่รับส่งระหว่างการประชุมได้

๒๑.๒ ดำเนินการอื่นเพื่อปฏิบัติตามและบังคับการให้เป็นไปตามกฎหมายหรือไม่ อย่างไร

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ได้มีการออกประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุม การประชุม เพื่อให้เป็นไปตามมาตรา ๗ แห่งพระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ และข้อ ๒๔ ของประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐาน การรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ และที่แก้ไขเพิ่มเติม รวมทั้งการให้บริการตรวจประเมิน และรับรองความสอดคล้องของระบบควบคุมการประชุมผ่านสื่อ อิเล็กทรอนิกส์ของผู้ให้บริการระบบควบคุมการประชุม เพื่อให้ผู้จัดการประชุมมีระบบควบคุม การประชุมที่สอดคล้องกับกฎหมายไว้เลือกใช้บริการ อันเป็นการอำนวยความสะดวกและลดภาระ การพิสูจน์ความชอบด้วยกฎหมายของระบบควบคุมการประชุมที่ได้เลือกใช้ในการประชุม

๒๒. ผลสัมฤทธิ์ของกฎหมาย

๒๒.๑ กฎหมายนี้มีการบังคับใช้หรือไม่ อย่างไร

มีการบังคับใช้จนถึงปัจจุบัน

๒๒.๒ หากมีการบังคับใช้ เกิดผลสำเร็จตามเป้าหมายที่กำหนดไว้หรือไม่ อย่างไร

เกิดผลสำเร็จตามเป้าหมายที่กำหนดไว้ เนื่องจากปรากฏว่ามีหน่วยงานทั้งภาครัฐและเอกชน ได้ดำเนินการจัดประชุมผ่านสื่ออิเล็กทรอนิกส์ควบคู่ไปกับการประชุม ณ สถานที่จัดประชุม เป็นปกติ และมีผู้ให้บริการระบบควบคุมการประชุม ที่ได้รับการรับรองจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์หลายราย

๒๒.๓ ประชาชนมีภาระหรือรัฐมีต้นทุนที่เกิดขึ้นจากการปฏิบัติตามและบังคับการให้เป็นไปตามกฎหมายอย่างไร

ระบบควบคุมการประชุมผ่านสื่ออิเล็กทรอนิกส์มีทั้งแบบที่เสียค่าบริการและไม่เสียค่าบริการเพิ่มเติมตามให้ผู้ให้บริการแต่ละรายกำหนด ซึ่งขึ้นอยู่กับลักษณะความต้องการการใช้งาน หากเป็นการประชุมทั่วไป โดยส่วนใหญ่แล้วจะเป็นแบบไม่มีค่าใช้จ่ายเพิ่มเติม ในส่วนของผู้ให้บริการระบบควบคุมการประชุมมีค่าธรรมเนียมการยื่นคำขอรับการตรวจประเมินเพื่อการรับรอง จำนวน ๒๐,๐๐๐ บาท ค่าธรรมเนียมการตรวจประเมินเพื่อการรับรอง จำนวน ๑๘๐,๐๐๐ บาท และค่าธรรมเนียมการตรวจติดตามผล จำนวน ๘๐,๐๐๐ บาท ตามประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และอัตราค่าธรรมเนียมการตรวจรับรองระบบควบคุมการประชุม ลงวันที่ ๓๑ กรกฎาคม ๒๕๖๓

๒๒.๔ เกิดผลที่ไม่ได้คาดคิดหรือไม่พึงประสงค์หรือไม่

ไม่มี

๒๓. กฎหมายนี้คุ้มค่าหรือได้สัดส่วนเมื่อเทียบประโยชน์ที่ได้รับกับภาระของประชาชนและทรัพยากรที่ใช้ในการบังคับการให้เป็นไปตามกฎหมายหรือไม่ อย่างไร

พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ เป็นการอำนวยความสะดวกให้กับทั้งภาครัฐและภาคเอกชนโดยการนำเทคโนโลยีมาใช้ในการกระบวนการทำงานและการประกอบธุรกิจ ซึ่งเป็นการช่วยประหยัดเวลาและค่าใช้จ่ายในการจัดประชุมและการเดินทางไปเข้าร่วมประชุม บรรเทาปัญหาการจราจร ลดการใช้กระดาษและพลังงาน และลดมลพิษต่อสิ่งแวดล้อม เมื่อเทียบกับภาระของประชาชนผู้ใช้บริการที่อาจมีค่าใช้จ่ายในการใช้บริการระบบควบคุมการประชุม และผู้ให้บริการที่ต้องมีค่าใช้จ่ายในเรื่องค่าธรรมเนียมการตรวจรับรองระบบควบคุมการประชุมกับประโยชน์ต่อประชาชนและรัฐทั้งในด้านเศรษฐกิจ สังคม และสิ่งแวดล้อมในภาพรวมแล้ว ถือว่าคุ้มค่า และได้สัดส่วน

๒๔. สมควรยกเลิก แก้ไข ปรับปรุงกฎหมายหรือกฎหมายหรือไม่ อย่างไร

พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ มีความเหมาะสมกับสภาพการณ์ปัจจุบัน และยังไม่ปรากฏปัญหาและอุปสรรคในการบังคับใช้กฎหมายอย่างมีนัยสำคัญ จึงสมควรบังคับใช้พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ ต่อไป ตามเดิม โดยในอนาคตหากมีความเปลี่ยนแปลงทางเทคโนโลยี ที่ส่งผลกระทบต่อพระราชกำหนดฯ มีความไม่สอดคล้องกับสภาพการณ์ปัจจุบัน หรือเกิดปัญหาและอุปสรรคในการบังคับใช้กฎหมาย จึงจะพิจารณาแก้ไขหรือปรับปรุงกฎหมายหรือกฎหมายต่อไป

๒๕. สมควรดำเนินการอื่นเพื่อปรับปรุงประสิทธิภาพในการปฏิบัติตามและบังคับการให้เป็นไปตามกฎหมาย หรือมีข้อเสนออื่นหรือไม่ อย่างไร

ไม่มี

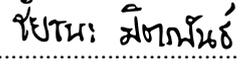
ข้าพเจ้าขอรับรองว่าข้อมูลที่ปรากฏในรายงานนี้เป็นข้อมูลที่ได้จากการตรวจสอบและวิเคราะห์อย่างถี่ถ้วนแล้ว

ลงชื่อ 

(นายพชร อนันตศิลป์)

ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๓๐ ธันวาคม ๒๕๖๘

ลงชื่อ 

(นายชัยชนะ มิตรพันธ์)

ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

๓๐ ธันวาคม ๒๕๖๘

หน่วยงานผู้รับผิดชอบ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

เจ้าหน้าที่ผู้รับผิดชอบ นายศรัลภ์ โคตะสินธ์

โทร. ๐๒-๑๔๑-๖๗๖๗ / ๐๒-๑๔๑-๖๗๖๖

อีเมล saran.co@mdes.go.th