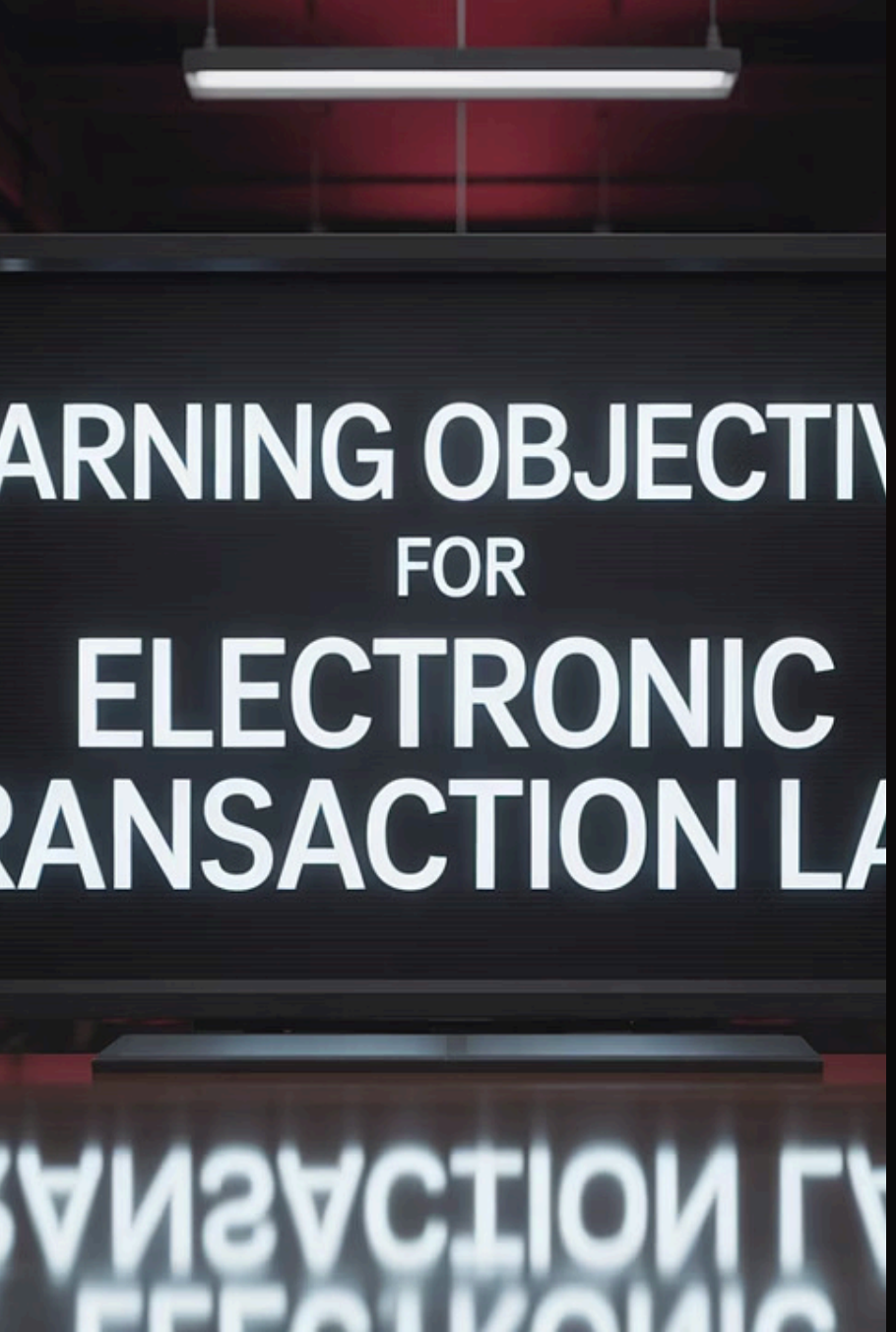
กฎหมายการทำธุรกรรมอิเล็กทรอนิกส์

เรียบเรียงโดย รศ.ดร.สุรีรัตน์ อินทร์หม้อ



จุดประสงค์การเรียนรู้

- เข้าใจพื้นฐานและหลักการของธุรกรรมอิเล็กทรอนิกส์ด้านคำจำกัดความ ความสำคัญและประเภทของธุรกรรมอิเล็กทรอนิกส์ต่างๆ
- เข้าใจกรอบกฎหมายที่ควบคุมและคุ้มครองธุรกรรมอิเล็กทรอนิกส์ ในระดับชาติและระดับนานาชาติ
- เรียนรู้มาตรฐานความปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ และการประยุกต์ใช้เทคนิคต่างๆ เพื่อรักษาความปลอดภัยของข้อมูล
- มีความสามารถในการวิเคราะห์และประยุกต์ใช้ความรู้ในสถานการณ์จริง ผ่านกรณีตัวอย่างและการอภิปรายเกี่ยวกับความท้าทายในการนำกฎหมายและมาตรฐานไปใช้

ความหมายและหลักการของธุรกรรมทางอิเล็กทรอนิกส์

ตาม มาตรา 3 ของพระราชบัญญัติฯ "ธุรกรรมทางอิเล็กทรอนิกส์" หมายถึง การกระทำใด ๆ ที่เกี่ยวข้องกับข้อมูลที่ได้จัดทำ ส่ง รับ ส่งต่อ เก็บรักษาหรือประมวลผลโดยวิธีการทางอิเล็กทรอนิกส์ รวมถึงการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ เพื่อวัตถุประสงค์ทางกฎหมาย

ตัวอย่างเช่น การซื้อขายสินค้าออนไลน์ การสมัครสมาชิกเว็บไซต์ และการโอนเงินผ่านแอปธนาคาร

ลายมือชื่ออิเล็กทรอนิกส์

"ลายมือชื่ออิเล็กทรอนิกส์" (Electronic Signature) หมายถึง ข้อมูลอิเล็กทรอนิกส์ที่แนบหรือเชื่อมโยงกับข้อมูลอิเล็กทรอนิกส์อื่น เพื่อใช้แสดงว่าบุคคลนั้นให้ความยินยอม หรือยืนยันในเนื้อหาของข้อมูล

- การกดปุ่ม "ยอมรับเงื่อนไข"
- การพิมพ์ชื่อท้ายอีเมล
- การใช้ลายเซ็นดิจิทัล (digital certificate)

หลักการรับรองความถูกต้องของข้อมูลและเอกสารอิเล็กทรอนิกส์

ตาม มาตรา 7 และ มาตรา 8 แห่ง พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 กำหนดว่า เอกสารอิเล็กทรอนิกส์จะมีผลตามกฎหมายเช่นเดียวกับเอกสารกระดาษ หากสามารถเข้าถึง ตรวจสอบ และเก็บรักษาได้อย่างเหมาะสม

การระบุตัวผู้ส่ง/ผู้ลงนาม

ต้องสามารถระบุตัวตนของผู้ส่งหรือผู้ลงนามในเอกสารได้อย่างชัดเจน

ความครบถ้วนและไม่มีการเปลี่ยนแปลง

ข้อมูลต้องมีความครบถ้วนและไม่มีการเปลี่ยนแปลงหลังจากลงลายมือชื่ออิเล็กทรอนิกส์

ความสามารถในการตรวจสอบย้อนหลัง

ต้องสามารถตรวจสอบย้อนหลังได้ (Auditability) เพื่อยืนยันความถูกต้องของข้อมูล

ความน่าเชื่อถือและผลทางกฎหมายของเอกสารอิเล็กทรอนิกส์

เอกสารอิเล็กทรอนิกส์มีผลทางกฎหมายเทียบเท่าเอกสารกระดาษ โดยหลักการตามกฎหมาย

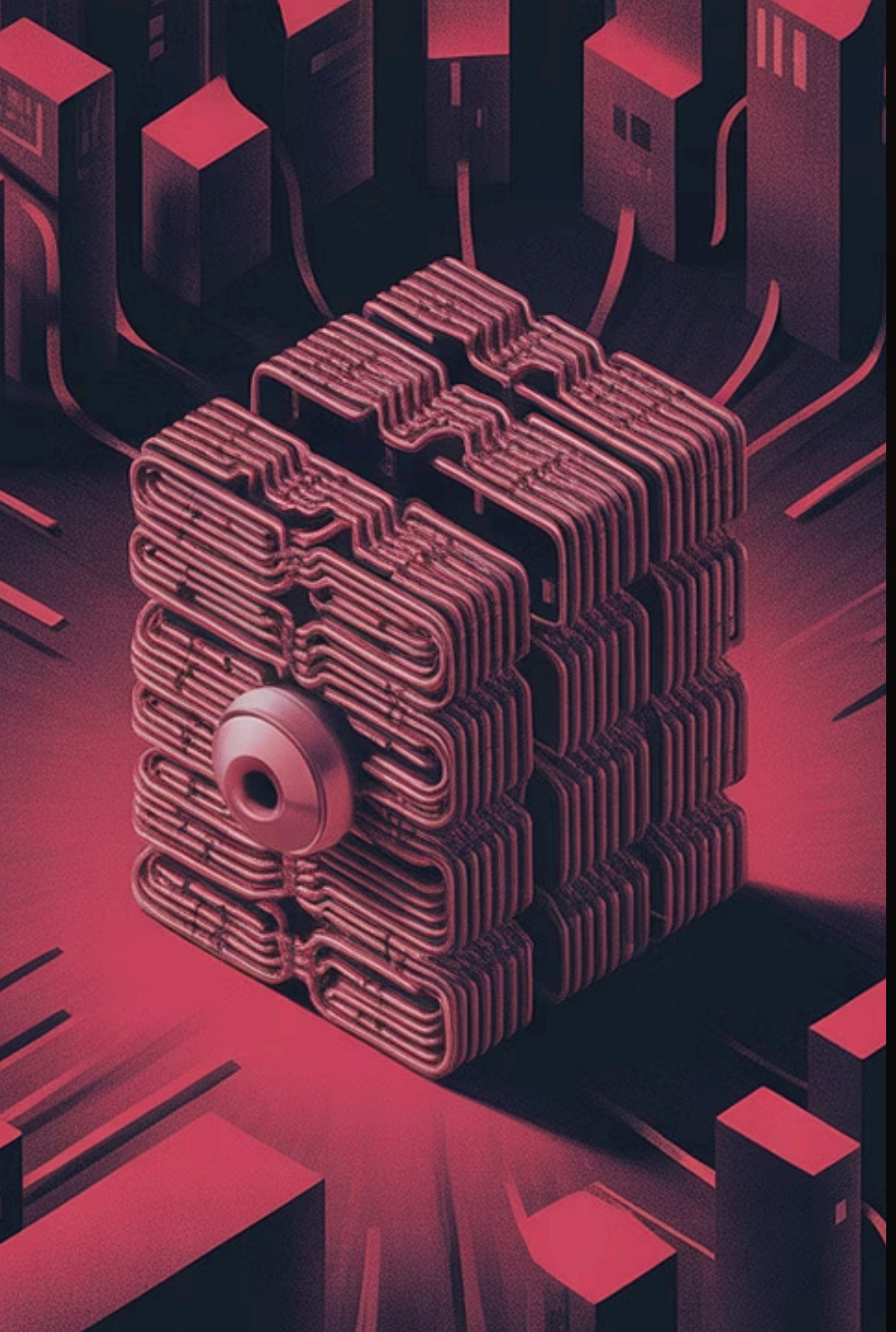
> มาตรา 7 แห่ง พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ระบุว่า "ข้อมูลอิเล็กทรอนิกส์ย่อมมีผลทางกฎหมายใช้ได้เช่นเดียวกับข้อมูลที่จัดทำไว้เป็นลายลักษณ์อักษร"

หากเอกสารอิเล็กทรอนิกส์สามารถเข้าถึง ตรวจสอบ และใช้งานได้อย่างเหมาะสม จะถือว่าเอกสารนั้นชอบด้วยกฎหมาย ไม่จำเป็นต้องอยู่ในรูปแบบกระดาษ

การใช้เอกสารอิเล็กทรอนิกส์ในทางกฎหมาย

- ใช้เป็นพยานหลักฐานในศาล
- ใช้ในการทำสัญญาทางธุรกิจ เช่น การเสนอราคา ใบสั่งซื้อ ใบแจ้งหนี้
- มีผลผูกพันตามสัญญา หากมีการแสดงเจตนาและยืนยันตัวตนอย่างชัดเจน

ตัวอย่างเช่น สัญญาเงินกู้ที่ลงนามผ่านแพลตฟอร์มอิเล็กทรอนิกส์โดยมี OTP ยืนยันตัวตน และใบเสร็จรับเงินที่ออกโดยระบบอัตโนมัติของร้านค้าออนไลน์ มีผลใช้ยื่นภาษีได้ตามกฎหมาย



คุณสมบัติของเอกสารอิเล็กทรอนิกส์ที่น่าเชื่อถือ

แนวทางการตรวจสอบย้อนกลับ **(Traceability)**

- สามารถแสดงแหล่งที่มาของข้อมูล เช่น IP Address ชื่อผู้ใช้งาน
- มีระบบ Log File ที่จัดเก็บเหตุการณ์การเข้าถึงหรือแก้ไขเอกสาร
- ใช้เทคโนโลยีเช่น Blockchain เพื่อยืนยันความถูกต้องและลำดับเหตุการณ์

แนวทางในการจัดเก็บข้อมูลให้ปลอดภัย

- จัดเก็บบนระบบที่มีการเข้ารหัส (Encryption)
- ใช้การยืนยันตัวตนแบบ 2 ชั้น (Two-Factor Authentication)
- มีการกำหนดสิทธิการเข้าถึง (Access Control)
- มีการสำรองข้อมูล (Backup) อย่างสม่ำเสมอ

มาตรา 8 ของ พ.ร.บ. ธุรกรรมฯ

> "หากกฎหมายกำหนดให้ต้องมีการจัดทำเอกสารเป็นลายลักษณ์อักษร การจัดเก็บในรูปแบบอิเล็กทรอนิกส์ก็ให้ถือว่าถูกต้องตามกฎหมาย หากสามารถเข้าถึง ตรวจสอบ และเก็บรักษาได้ในระยะเวลาที่เหมาะสม"

ระบบบัญชีของบริษัท

เก็บข้อมูลใบกำกับภาษีในระบบ Cloud พร้อม timestamp และลายเซ็นดิจิทัล

ระบบ **E-Document** ขององค์กรภาครัฐ

มีประวัติการแก้ไข และจำกัดสิทธิ์การดูเอกสารเฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง

การควบคุมดูแลการชำระเงินทางอิเล็กทรอนิกส์

การชำระเงินทางอิเล็กทรอนิกส์ (Electronic Payment) นิยามตามมาตรา 3 ของพระราชกฤษฎีกา พ.ศ. 2551 หมายถึง "การโอนสิทธิการถือครองเงิน หรือการโอนสิทธิการถอนเงิน หรือหักเงินจากบัญชีเงินฝากของผู้ใช้บริการที่เปิดไว้กับผู้ให้บริการ ด้วยวิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือบางส่วน"

- การสแกน QR Code เพื่อโอนเงินผ่าน Mobile Banking
- การจ่ายเงินผ่านแอปพลิเคชัน e-Wallet เช่น TrueMoney Wallet, ShopeePay
- การหักบัญชีอัตโนมัติสำหรับค่าสาธารณูปโภค (เช่น ค่าไฟฟ้า)
- การซื้อสินค้าออนไลน์โดยใช้ Internet Banking

บัตรอิเล็กทรอนิกส์

บัตรอิเล็กทรอนิกส์ (Electronic Card) นิยามตามพระราชกฤษฎีกา พศ. 2551 หมายถึง "บัตรหรือสิ่งอื่นใดที่มีข้อมูลหรือรหัสซึ่งสามารถใช้ระบุตัวบุคคล หรือใช้ชำระเงิน โอนเงิน หรือเบิกถอนเงินได้ โดยไม่จำเป็นต้องใช้เงินสดในการทำธุรกรรมนั้น"

ประเภทบัตร	ลักษณะการใช้งาน
บัตรเครดิต (Credit Card)	ใช้จ่ายก่อนแล้วชำระภายหลัง ตามวงเงินที่ธนาคารอนุมัติ
บัตรเดบิต (Debit Card)	หักเงินจากบัญชีโดยตรงทันทีที่ใช้
บัตรเติมเงิน (Prepaid Card)	เติมเงินล่วงหน้าแล้วใช้จ่าย เช่น บัตร BTS, MRT หรือบัตรซื้อสินค้าออนไลน์
บัตรสวัสดิการแห่งรัฐ	ใช้จ่ายเฉพาะในรายการที่รัฐกำหนด ผ่านระบบอิเล็กทรอนิกส์

ความสำคัญของการชำระเงินทางอิเล็กทรอนิกส์

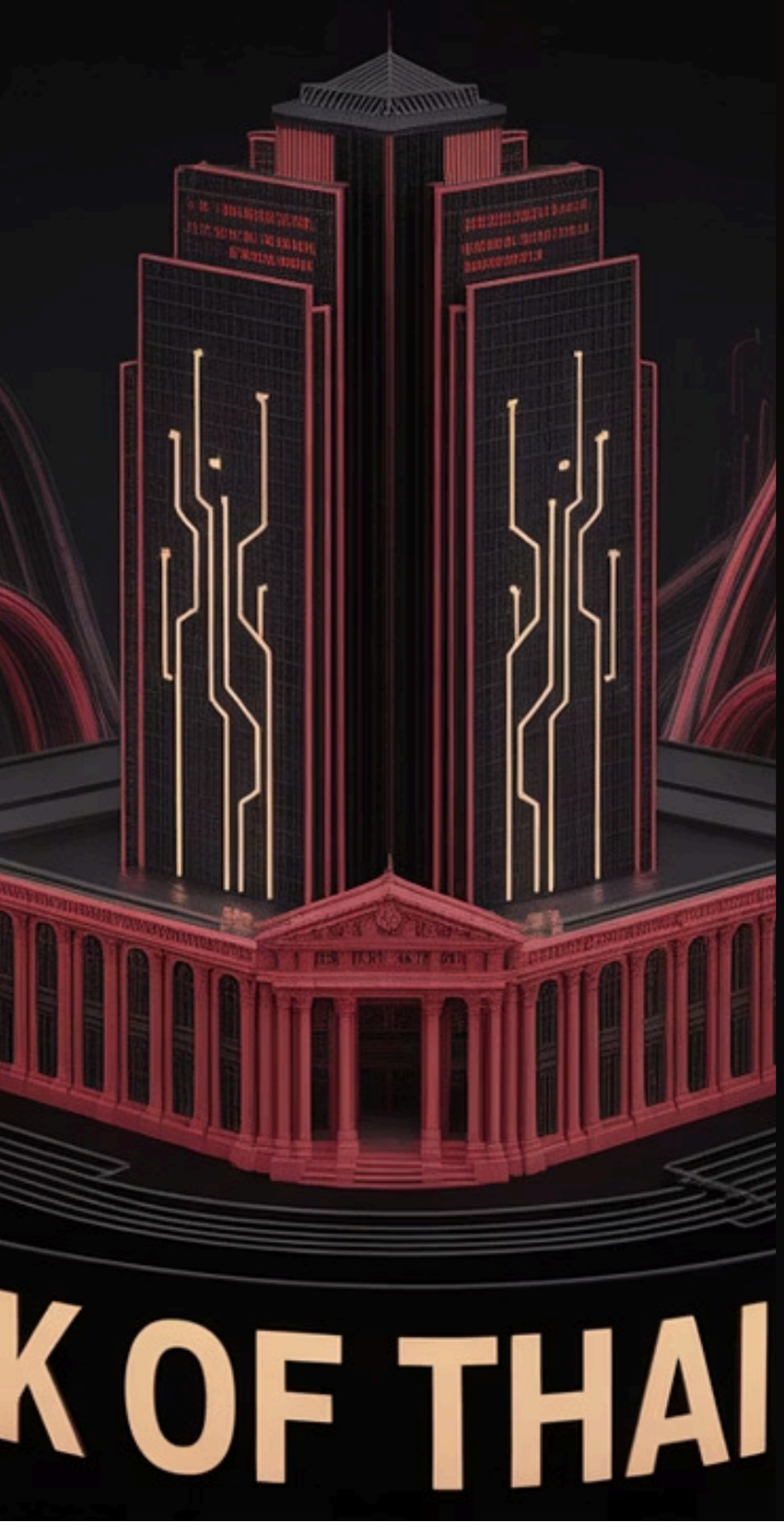
การชำระเงินทางอิเล็กทรอนิกส์และบัตรอิเล็กทรอนิกส์เป็นหัวใจสำคัญของระบบการเงินดิจิทัลในปัจจุบัน พระราชกฤษฎีกาฉบับนี้จึงมีบทบาทสำคัญในการกำกับ ดูแล และสร้างความปลอดภัยให้แก่ผู้ใช้บริการ รวมถึงสนับสนุนให้ธุรกิจสามารถดำเนินธุรกรรมทางการเงินได้อย่างมีมาตรฐานและเชื่อถือได้

ประโยชน์ต่อผู้บริโภค

- สะดวก รวดเร็ว ไม่ต้องพกเงินสด
- ทำธุรกรรมได้ทุกที่ ทุกเวลา
- มีประวัติการใช้จ่ายที่ตรวจสอบได้

ประโยชน์ต่อธุรกิจ

- ลดต้นทุนการจัดการเงินสด
- เพิ่มประสิทธิภาพในการรับชำระเงิน
- ขยายฐานลูกค้าได้กว้างขึ้น



การควบคุมบริการทางการเงินอิเล็กทรอนิกส์

การให้บริการทางการเงินผ่านช่องทางอิเล็กทรอนิกส์ เช่น e-Wallet, QR Payment และ Internet Banking อยู่ภายใต้การควบคุมของธนาคารแห่งประเทศไทย (ธปท.) และกฎหมายสำคัญ ได้แก่ พระราชกฤษฎีกา ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 และพระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560

การขออนุญาต

ผู้ให้บริการต้องขออนุญาตหรือขึ้นทะเบียนกับ ธปท. เพื่อให้มั่นใจว่ามีมาตรฐานความปลอดภัยที่เพียงพอ

ระบบรักษาความปลอดภัย

ต้องมีระบบรักษาความปลอดภัยของข้อมูล เช่น การเข้ารหัส การพิสูจน์ตัวตนแบบหลายปัจจัย (2FA)

การแจ้งข้อมูล

ต้องแจ้งผู้ใช้บริการเกี่ยวกับค่าธรรมเนียม เงื่อนไขบริการ และสิทธิความคุ้มครอง

ระบบสำรองข้อมูล

ต้องมีระบบสำรองข้อมูลและระบบป้องกันความเสี่ยง เพื่อสร้างความมั่นคงและความต่อเนื่องในการให้บริการ

การเปรียบเทียบบริการชำระเงินอิเล็กทรอนิกส์

ประเภทบริการ	ลักษณะเด่น	ตัวอย่างการใช้งาน	การควบคุมหลัก
e-Wallet	ชำระเงินและเก็บเงินในแอป	เติมเงินเข้า TrueMoney เพื่อจ่ายค่า Netflix	วงเงินจำกัด, KYC
QR Payment	สแกนจ่ายแบบไม่ใช้เงินสด	จ่ายค่าแท็กซี่ผ่าน PromptPay QR	EMVCo, ตรวจสอบ QR
Internet Banking	ธุรกรรมผ่านเว็บ/แอปธนาคาร	โอนเงินให้เพื่อนผ่านแอป SCB Easy	2FA, การเข้ารหัส, แจ้งเตือน

การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรม

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA – Personal Data Protection Act) ซึ่งมีผลใช้บังคับเต็มรูปแบบตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565

ข้อมูลส่วนบุคคล

ตามมาตรา 6 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้ความหมายของ "ข้อมูลส่วนบุคคล" ว่าหมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาที่ทำให้สามารถระบุตัวตนของบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม

ตัวอย่าง

- ชื่อ-นามสกุล
- หมายเลขบัตรประชาชน
- เบอร์โทรศัพท์
- ที่อยู่ อีเมล
- รูปถ่าย เสียง
- ลายนิ้วมือ
- IP Address
- รหัสลูกค้า
- พิกัดตำแหน่ง GPS

ข้อมูลส่วนบุคคลอ่อนไหว

ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data) ตามมาตรา 26 คือข้อมูลที่มีความอ่อนไหวเป็นพิเศษ

- เชื้อชาติ, ศาสนา, ความคิดเห็นทางการเมือง
- ข้อมูลสุขภาพ, พฤติกรรมทางเพศ, ประวัติอาชญากรรม
- ข้อมูลชีวภาพ (Biometric) เช่น ลายนิ้วมือ, สแกนใบหน้า, เสียง

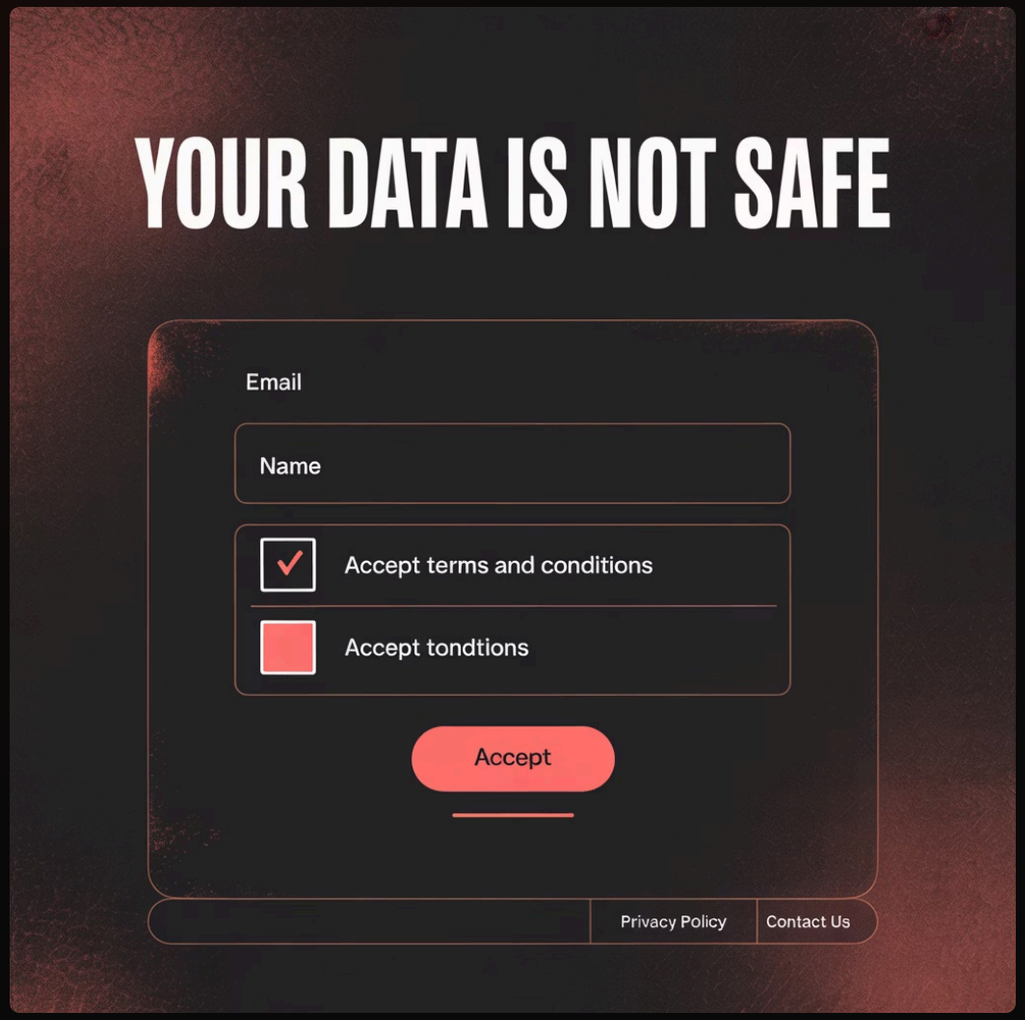
การเก็บและใช้ข้อมูลประเภทนี้ต้องได้รับ "ความยินยอมโดยชัดแจ้ง" จากเจ้าของข้อมูล ซึ่งหมายถึง การที่เจ้าของข้อมูลได้ให้ความยินยอม โดยตั้งใจ ชัดเจน และทราบข้อเท็จจริงอย่างเพียงพอ ในรูปแบบที่สามารถตรวจสอบได้ ไม่คลุมเครือ หรือแฝงไว้ในเงื่อนไขอื่น

ลักษณะของ "ความยินยอมโดยชัดแจ้ง"

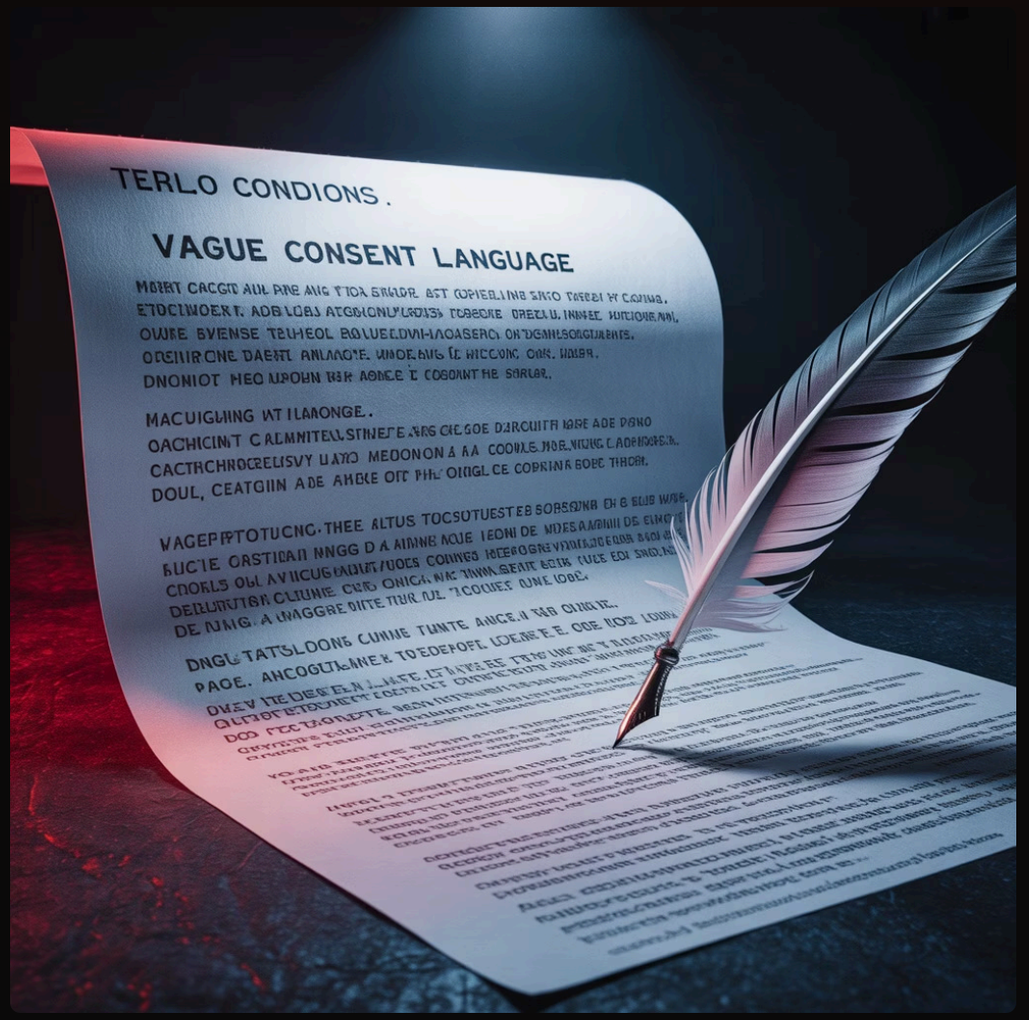
- **ต้องเป็นการยินยอมอย่างอิสระ**
  โดยไม่ถูกบังคับ กดดัน หรือทำให้เข้าใจผิด
- **ต้องเฉพาะเจาะจง**
  มีการระบุวัตถุประสงค์การใช้ข้อมูลอย่างชัดเจน
- **ต้องมีการแจ้งข้อมูลก่อนยินยอม**
  เช่น วัตถุประสงค์ ระยะเวลา บุคคลที่ข้อมูลจะถูกส่งต่อ
- **ต้องสามารถพิสูจน์ได้ว่าได้รับความยินยอม**
  โดยมีหลักฐาน เช่น ระบบบันทึก log หรือกล่องติ๊กถูกที่ผู้ใช้กดเอง
- **ต้องมีช่องทางให้ "ถอนความยินยอม" ได้ตลอดเวลา**
  โดยไม่เสียสิทธิหรือบริการ

ความยินยอมแบบ "ไม่ชัดแจ้ง" ที่ไม่ถือว่าเพียงพอ

- กล่องติ๊ก "ให้ความยินยอม" ที่ถูกเลือกไว้ล่วงหน้า (pre-checked)
- ข้อความรวมไว้ในข้อตกลงทั่วไปโดยไม่ได้แยกเป็นหัวข้อเฉพาะ
- การขอความยินยอมโดยไม่แจ้งวัตถุประสงค์อย่างชัดเจน



กล่องติ๊กที่ถูกเลือกไว้ล่วงหน้า ไม่ถือเป็นความยินยอมโดยชัดแจ้ง



ข้อความที่ซ่อนอยู่ในเงื่อนไขทั่วไป ไม่ถือเป็นความยินยอมโดยชัดแจ้ง

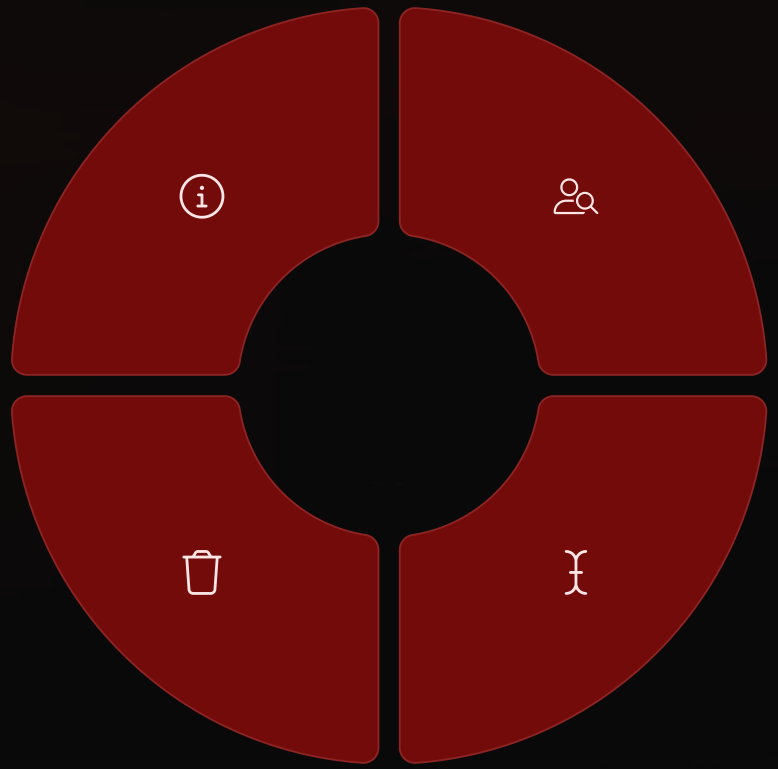
สิทธิของเจ้าของข้อมูล 8 ประการ

สิทธิในการรับรู้

สอบถามว่าเก็บข้อมูลอะไร ทำเพื่ออะไร ใช้กับใคร

สิทธิในการเข้าถึงข้อมูล

ขอสำเนาข้อมูลส่วนตัว หรือสอบถามว่าองค์กรใช้ข้อมูลอย่างไร



สิทธิในการลบข้อมูล

ขอให้ลบข้อมูลเมื่อไม่มีเหตุผลทางกฎหมายในการเก็บรักษาอีกต่อไป

สิทธิในการแก้ไขข้อมูล

ขอให้แก้ไขข้อมูลที่ไม่ถูกต้อง หรือไม่เป็นปัจจุบัน

สิทธิของเจ้าของข้อมูล (ต่อ)

สิทธิในการถอนความยินยอม

สามารถถอนคำยินยอมในการเก็บข้อมูลได้ตลอดเวลา

สิทธิในการคัดค้าน

คัดค้านการประมวลผลข้อมูล เช่น การตลาดแบบตรง หรือการวิเคราะห์พฤติกรรมได้

สิทธิในการจำกัดการประมวลผลข้อมูล

จำกัดการใช้ข้อมูลชั่วคราวในกรณีมีข้อพิพาทหรือการตรวจสอบ

สิทธิในการโอนย้ายข้อมูล

ขอให้ส่งหรือย้ายข้อมูลส่วนตัวไปยังผู้ให้บริการรายอื่นได้

ตัวอย่างสถานการณ์การใช้สิทธิ์ของเจ้าของข้อมูล

สถานการณ์	สิทธิของเจ้าของข้อมูล
บริษัทเก็บอีเมลลูกค้าเพื่อส่งโฆษณา	ต้องแจ้งวัตถุประสงค์ให้ชัดเจน และต้องได้รับความยินยอม
นักศึกษาขอให้มหาวิทยาลัยลบข้อมูลรูปถ่ายบนเว็บไซต์	ใช้ "สิทธิในการลบข้อมูล"
ผู้บริโภคต้องการรู้ว่าแอปใช้ข้อมูลพิกัดตำแหน่งทำอะไร	ใช้ "สิทธิในการเข้าถึงข้อมูล"

หน้าที่ของธุรกิจในการเก็บรักษาข้อมูล

หน้าที่ของธุรกิจในการเก็บ รักษา และเปิดเผยข้อมูลอย่างปลอดภัยและตามความยินยอม ตามที่กำหนดไว้ใน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

การเก็บข้อมูล

เก็บเฉพาะเท่าที่จำเป็น มีวัตถุประสงค์ชัดเจน แจ้งเจ้าของข้อมูลล่วงหน้า

การรักษาความปลอดภัย

มีระบบป้องกันการเข้าถึงโดยมิชอบ เข้ารหัสข้อมูล กำหนดสิทธิ์การเข้าถึง

การเปิดเผยข้อมูล

ต้องได้รับความยินยอมก่อนเปิดเผยแก่บุคคลภายนอก ใช้เฉพาะตามวัตถุประสงค์ที่ระบุไว้

ตัวอย่างหน้าที่ของธุรกิจตาม PDPA

ร้านค้าออนไลน์

เก็บชื่อ ที่อยู่ และเบอร์โทรศัพท์ เพื่อจัดส่งสินค้า ต้องแจ้งลูกค้าชัดเจนว่าข้อมูลจะใช้เพื่ออะไร และไม่ใช้ในกิจกรรมทางการตลาดโดยไม่ขอความยินยอมจากลูกค้าก่อน

บริษัทประกันภัย

ต้องเก็บประวัติสุขภาพของลูกค้าไว้ในฐานข้อมูลที่เข้ารหัส และจำกัดสิทธิ์เข้าถึงเฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น

ขั้นตอน	สิ่งที่ต้องทำ	อ้างอิงตาม พ.ร.บ.
1. เก็บข้อมูล	ขอความยินยอม + แจ้งวัตถุประสงค์	มาตรา 19–22
2. รักษาข้อมูล	ใช้มาตรการรักษาความปลอดภัย	มาตรา 37
3. เปิดเผยข้อมูล	เปิดเผยเท่าที่จำเป็น พร้อมยินยอม	มาตรา 23

ความมั่นคงปลอดภัยทางไซเบอร์ในธุรกรรมอิเล็กทรอนิกส์

มาตรา 4 ของ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้ให้ความหมายของ "ภัยคุกคามทางไซเบอร์" ว่าหมายถึง การกระทำที่อาจก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล เครือข่าย ระบบคอมพิวเตอร์ ระบบควบคุม หรือโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญของประเทศ

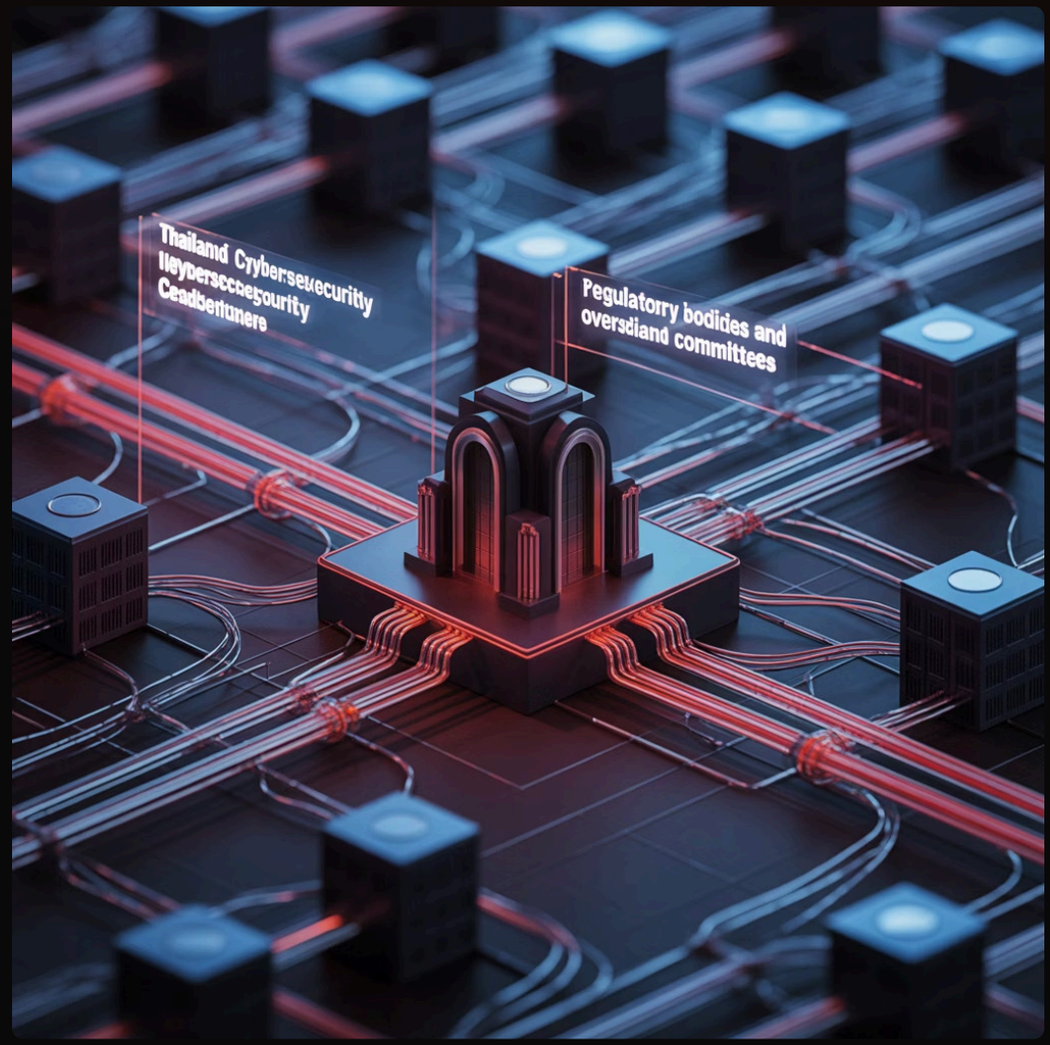
- การเจาะระบบ (Hacking) เพื่อขโมยข้อมูลส่วนตัวหรือทางการเงิน
- โปรแกรมมัลแวร์ (Malware) และแรนซัมแวร์ (Ransomware) ที่เข้ารหัสไฟล์แล้วเรียกค่าไถ่
- การโจมตีแบบ DDoS (Distributed Denial of Service) ทำให้ระบบล่ม
- การหลอกลวงแบบฟิชชิ่ง (Phishing) ที่หลอกให้ผู้ใช้กรอกข้อมูลสำคัญผ่านอีเมลปลอม
- การรั่วไหลของข้อมูลในองค์กรจากบุคคลภายใน (Insider Threat)

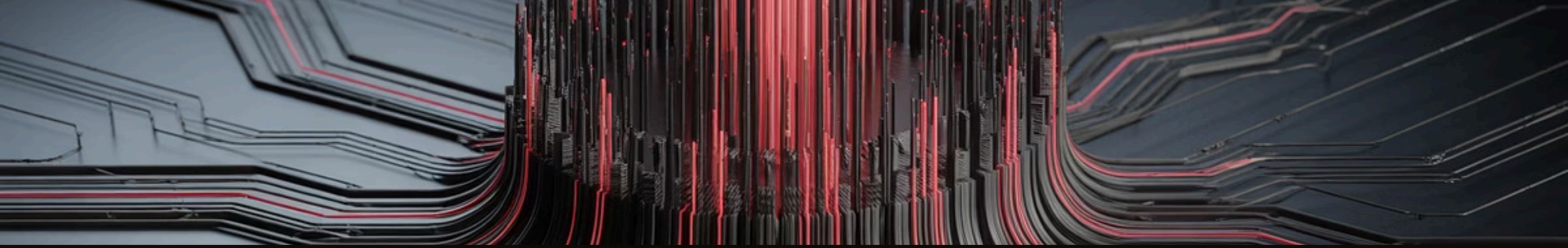
พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัติเกี่ยวกับมาตรการป้องกันตาม พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีเป้าหมายในการวางกรอบควบคุมภัยคุกคามไซเบอร์ระดับชาติ โดยเฉพาะในระบบโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญ (Critical Information Infrastructure: CII)

โครงสร้างหลักของ พ.ร.บ.

- คณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ (กกม.)
- สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม (สดช.)
- หน่วยงานกำกับดูแล (Regulators) ในแต่ละสาขา เช่น พลังงาน การเงิน โทรคมนาคม





ระดับความรุนแรงของภัยคุกคามไซเบอร์

ระดับเฝ้าระวัง

มีความเสี่ยงทั่วไปที่อาจเกิดขึ้น จะต้องมีการแจ้งเตือนวางระบบเฝ้าระวัง

ระดับร้ายแรง

สถานการณ์เริ่มส่งผลกระทบต่อความมั่นคงหรือระบบสำคัญ จะต้องแจ้งหน่วยงานที่เกี่ยวข้องทันที เพื่อดำเนินการตรวจสอบถึงสาเหตุที่เกิดภัยคุกคามนี้ขึ้น

ระดับวิกฤติ

เริ่มส่งผลกระทบความมั่นคงหรือประชาชนในวงกว้าง จะต้องมีประกาศเหตุฉุกเฉิน และดำเนินการออกคำสั่งควบคุมโดยภาครัฐ

แนวทางปฏิบัติในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์

การตรวจจับและเฝ้าระวัง

ใช้ระบบแจ้งเตือน เช่น IDS/IPS หรือ SOC เพื่อตรวจพบพฤติกรรมผิดปกติ เช่นระบบแจ้งเตือนการ Login ผิดพลาดหลายครั้งในเวลาสั้น ๆ

การแจ้งเหตุ

หากพบเหตุการณ์เข้าข่าย "ภัยคุกคามไซเบอร์" ตาม พ.ร.บ. ต้องแจ้งหน่วยงานที่เกี่ยวข้อง เช่น ศูนย์ความมั่นคงไซเบอร์ภาครัฐ (NCSC) ภายใน 24 ชม.

การประเมินและควบคุมความเสียหาย

วิเคราะห์ระดับความรุนแรง แยกระบบที่ได้รับผลกระทบ เพื่อป้องกันการลุกลาม เช่นการปิดระบบเครือข่ายที่ได้รับผลกระทบชั่วคราว

การฟื้นฟูและกู้คืนระบบ

ใช้ข้อมูลสำรอง (Backup) เพื่อกู้คืนระบบให้กลับมาใช้งานได้ เช่นมีการใช้ Backup Server ที่ไม่มีมัลแวร์

การรายงานและวิเคราะห์เหตุการณ์

สรุปบทเรียน เหตุการณ์ที่เกิดขึ้น จุดอ่อนในระบบ และแนวทางป้องกันในอนาคต เช่นมีการจัดประชุมทีม IT สรุปผลการฟื้นฟู พร้อมแผนเสริมความแข็งแกร่ง

เครื่องมือในการตอบสนองต่อภัยคุกคามทางไซเบอร์

ระบบตรวจจับการบุกรุก (IDS)

ตรวจจับกิจกรรมที่ผิดปกติหรือมีลักษณะเป็นภัยคุกคาม ที่อาจเกิดขึ้นกับเครือข่ายหรือระบบคอมพิวเตอร์ขององค์กร เช่น Network-based IDS (NIDS), Host-based IDS (HIDS)

ระบบบันทึกเหตุการณ์ (Log Management)

รวบรวม วิเคราะห์ และจัดเก็บบันทึกกิจกรรมที่เกิดขึ้นภายในระบบเครือข่าย คอมพิวเตอร์ หรือแอปพลิเคชัน เพื่อตรวจสอบเหตุการณ์ผิดปกติ

ระบบสำรองข้อมูลอัตโนมัติ

สำรองข้อมูลจากระบบหลักไปยังพื้นที่จัดเก็บสำรอง โดยดำเนินการโดยอัตโนมัติตามเวลาที่กำหนด เพื่อกู้คืนข้อมูลเมื่อเกิดเหตุการณ์ไม่คาดคิด

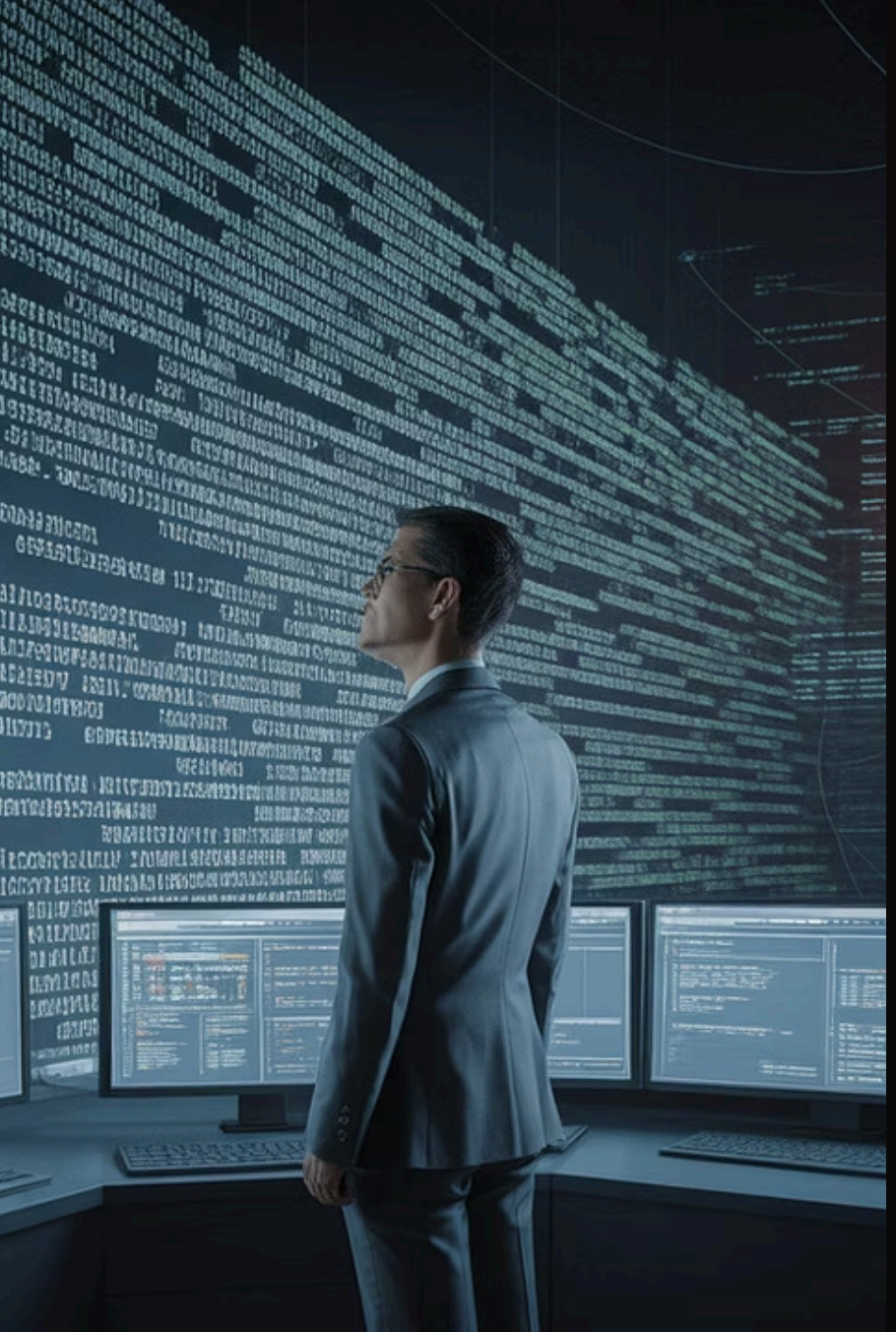
เครื่องมือในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (ต่อ)

คู่มือการรับมือเหตุการณ์ **(Incident Response Plan)**

เอกสารแผนปฏิบัติการ ที่องค์กรจัดทำขึ้น เพื่อระบุขั้นตอน วิธีการ และบทบาทหน้าที่ของแต่ละฝ่ายในการตอบสนองต่อ "เหตุการณ์ด้านความปลอดภัยทางไซเบอร์" (เช่น การโจมตีจากแฮกเกอร์, แรนซัมแวร์, การรั่วไหลของข้อมูลส่วนบุคคล)

ทีมตอบสนองเหตุการณ์ **(CSIRT)**

ทีมผู้เชี่ยวชาญเฉพาะทาง ที่รับผิดชอบในการตรวจสอบ ตอบสนอง วิเคราะห์ และกู้คืนจากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ เช่น การถูกโจมตีจากแฮกเกอร์ การแพร่กระจายของมัลแวร์ การรั่วไหลของข้อมูล



บทลงโทษจากการกระทำผิดทางคอมพิวเตอร์

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 "การกระทำผิดทางคอมพิวเตอร์" หมายถึง การกระทำที่เกี่ยวข้องกับการใช้ "คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์" โดยมีเจตนาในการละเมิดสิทธิของผู้อื่น ฝ่าฝืนกฎหมาย หรือสร้างความเสียหายแก่บุคคล องค์กร หรือสาธารณะ

ประเภทของความผิดทางคอมพิวเตอร์

ความผิดเกี่ยวกับระบบคอมพิวเตอร์

การเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต (มาตรา 5–7) การดักข้อมูลที่ส่งในระบบคอมพิวเตอร์ (มาตรา 8) และการรบกวนหรือขัดขวางระบบให้หยุดทำงาน (DoS Attack) (มาตรา 9–10)

ความผิดเกี่ยวกับข้อมูลคอมพิวเตอร์

การแก้ไข เปลี่ยนแปลง หรือทำลายข้อมูลโดยมิชอบ (มาตรา 11–12) และการส่งข้อมูลเท็จหรือข้อมูลที่เป็นอันตรายต่อประชาชน เช่น ข้อมูลปลอม ข่าวปลอม (มาตรา 14)

ความผิดเกี่ยวกับการใช้คอมพิวเตอร์ละเมิดสิทธิ

การเผยแพร่ภาพบุคคลโดยไม่ได้รับความยินยอม (มาตรา 16) และการใช้ข้อมูลเพื่อหลอกลวงหรือแอบอ้างเป็นบุคคลอื่น (มาตรา 17)

ความผิดที่เกี่ยวข้องกับความมั่นคงของรัฐ

การเผยแพร่ข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอมแปลง ปลุกระดม หรือปล่อยข่าวลวงเพื่อให้ประชาชนหวาดกลัว (มาตรา 14 วรรค 2)

ความผิดที่พบบ่อยและบทลงโทษ

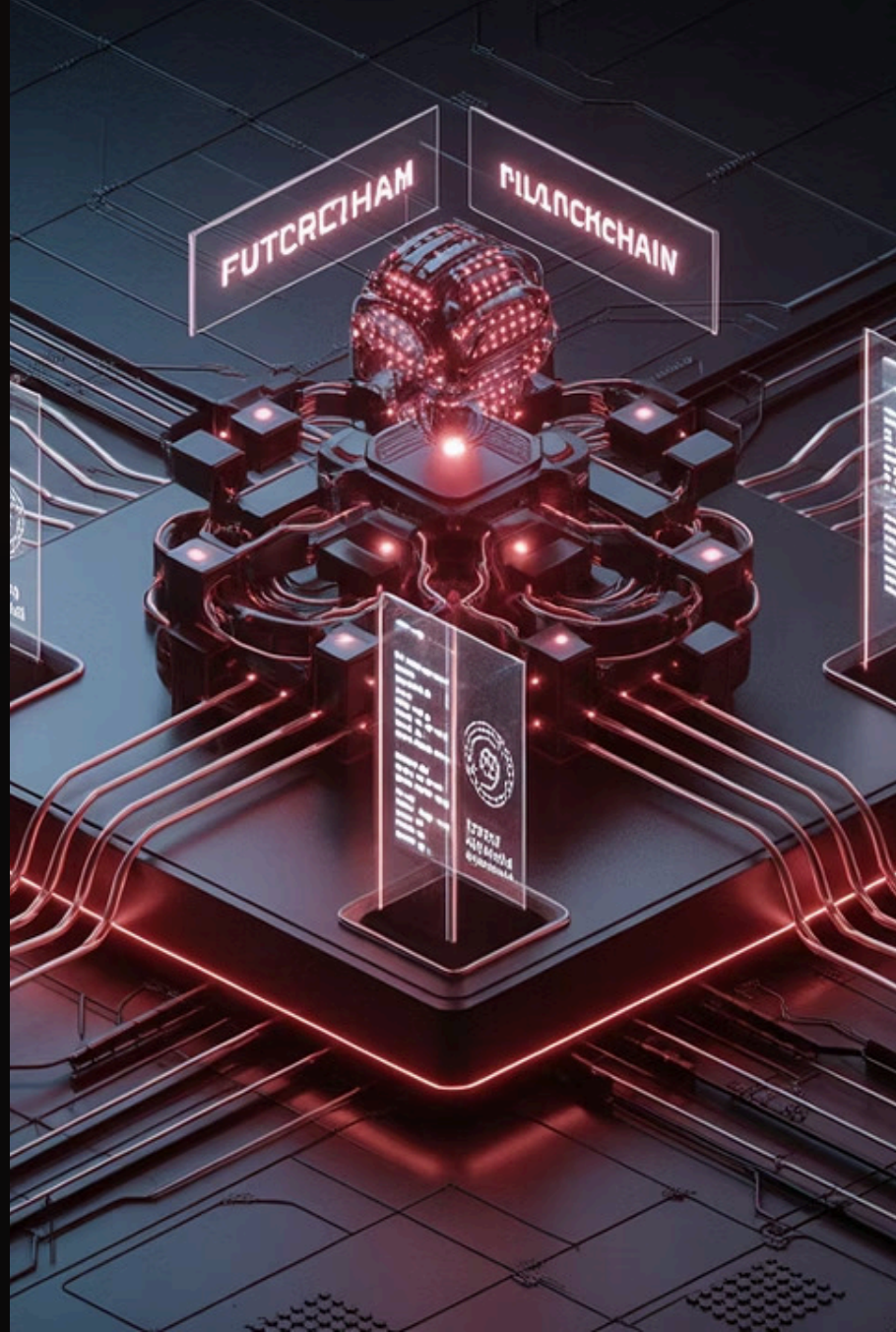
ประเภทความผิด	รายละเอียด	บทลงโทษตามกฎหมาย
การแฮกระบบ (Hacking)	เข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ	จำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท หรือทั้งจำทั้งปรับ (มาตรา 5)
เข้าถึงข้อมูลโดยมิชอบ	ลักลอบเปิดดูหรือคัดลอกข้อมูลของผู้อื่น	จำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท (มาตรา 7)
ส่งอีเมลสแปม (Spam)	ส่งข้อมูลอิเล็กทรอนิกส์รบกวนผู้อื่นจำนวนมาก	ปรับทางแพ่งหรืออาญา ขึ้นกับผลกระทบที่เกิดขึ้น

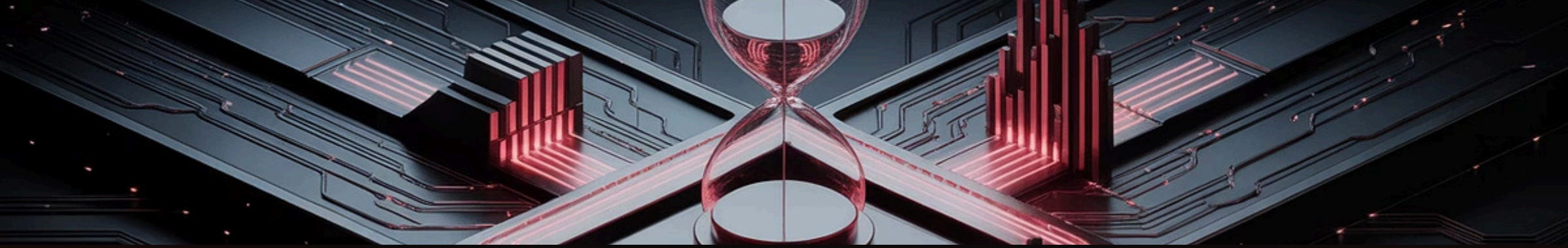
ความผิดที่พบบ่อยและบทลงโทษ (ต่อ)

ประเภทความผิด	รายละเอียด	บทลงโทษตามกฎหมาย
เผยแพร่ข้อมูลเท็จ	นำเข้าข้อมูลเท็จสู่ระบบคอมพิวเตอร์ จนผู้อื่นเสียหาย	จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ (มาตรา 14)
บิดเบือนข้อมูลเกี่ยวกับภัยพิบัติ / ความมั่นคง	ส่งข้อมูลที่ทำให้ประชาชนตื่นตระหนก	จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท
ละเมิดสิทธิส่วนบุคคล	เผยแพร่ข้อมูลส่วนตัวหรือภาพโดยไม่ยินยอม	จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท

แนวโน้มเทคโนโลยีและกฎหมายในอนาคต

ในยุคที่เทคโนโลยีเปลี่ยนแปลงอย่างรวดเร็ว กฎหมายเทคโนโลยีสารสนเทศมีบทบาทสำคัญในการสร้างสมดุลระหว่าง "การส่งเสริมนวัตกรรม" และ "การปกป้องสิทธิผู้บริโภคและสังคม" โดยเฉพาะกับ 3 เทคโนโลยีที่ทรงอิทธิพล ได้แก่ AI, Blockchain และ Metaverse





กฎหมายในยุค **AI (Artificial Intelligence)**

กฎหมายในยุค AI หมายถึงกฎหมายที่กำหนด สิทธิ หน้าที่ และความรับผิดชอบ ของบุคคล องค์กร และรัฐในการพัฒนาและใช้งานเทคโนโลยีปัญญาประดิษฐ์ โดยเน้นการกำกับดูแลเพื่อให้เกิดความโปร่งใส ยุติธรรม และปลอดภัยต่อสังคม ขณะเดียวกันก็ส่งเสริมนวัตกรรมอย่างมีจริยธรรม

ความรับผิดชอบ **(Accountability)**

หาก AI ตัดสินใจผิดพลาด เช่น การวิเคราะห์สินเชื่อผิด การแนะนำข้อมูลเท็จ ใครควรรับผิด?

ความโปร่งใส **(Explainability)**

อัลกอริธึมของ AI ต้องสามารถอธิบายการตัดสินใจได้หรือไม่?

การคุ้มครองข้อมูลส่วนบุคคล **(PDPA)**

AI ต้องไม่ละเมิดข้อมูลที่ไม่ใช่ของตน เช่น การใช้ภาพจากกล้องวงจรปิดวิเคราะห์พฤติกรรมโดยไม่ขอความยินยอม

แนวโน้มกฎหมาย AI ในต่างประเทศและไทย

แนวโน้มในต่างประเทศ

ประเทศในสหภาพยุโรปกำลังบังคับใช้ EU AI Act ซึ่งแบ่งระดับความเสี่ยงของ AI (สูง-ต่ำ) และควบคุมการใช้งานอย่างเข้มงวด

แนวโน้มในประเทศไทย

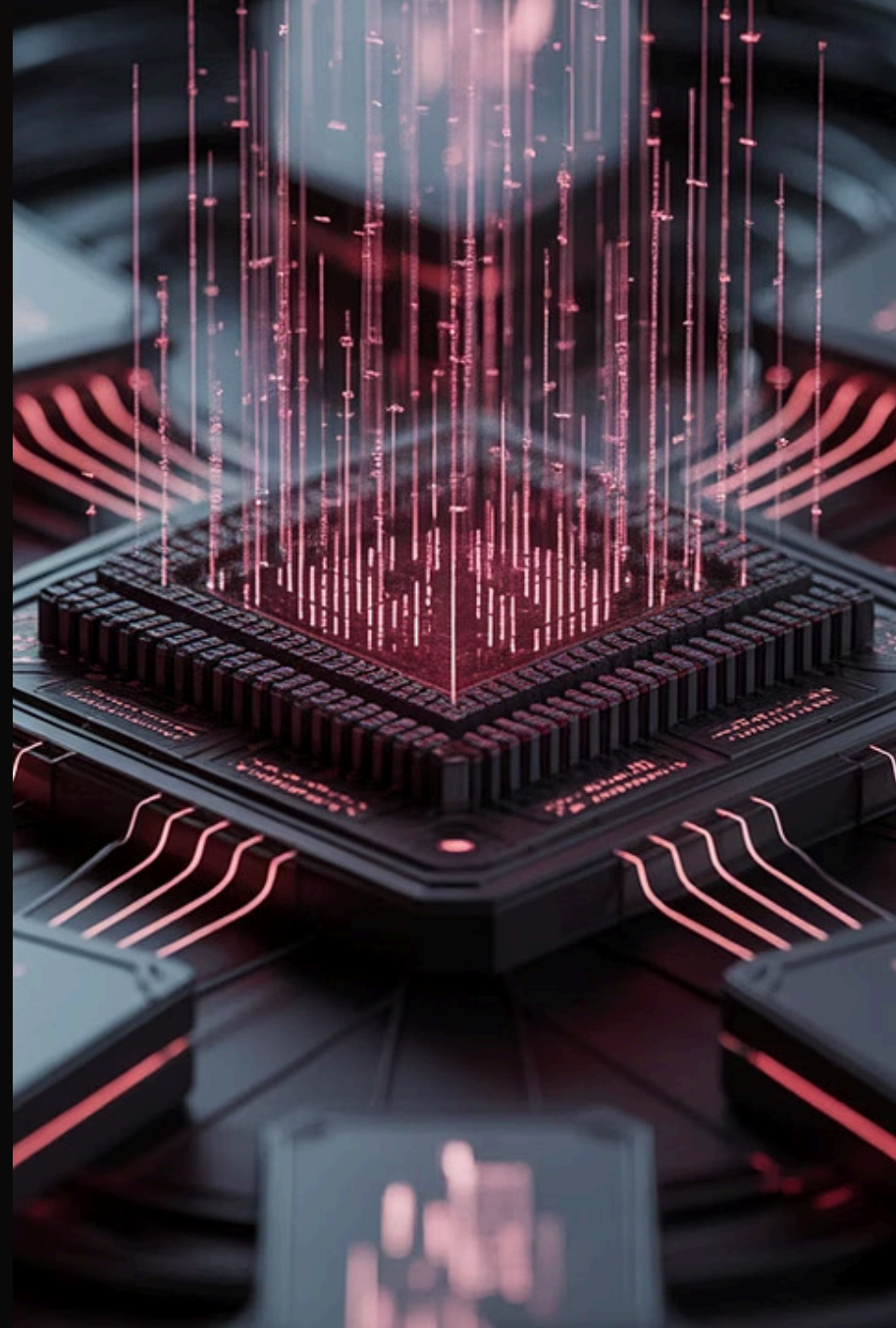
มีแนวโน้มที่จะออกแนวทางควบคุม AI ตามแผนดิจิทัลแห่งชาติ เช่น การออก แนวปฏิบัติจริยธรรม AI (AI Ethics Guideline) ของกระทรวง DE

ตัวอย่างเช่น ระบบ AI วิเคราะห์ใบหน้าสำหรับ e-KYC ต้องอยู่ภายใต้การควบคุมตาม PDPA และต้องได้รับความยินยอมก่อนประมวลผลข้อมูลชีวมิติ

กฎหมายในยุค **Blockchain** และ **Smart Contracts**

Blockchain คือเทคโนโลยีการจัดเก็บข้อมูลแบบกระจายศูนย์ (Distributed Ledger Technology) ซึ่งข้อมูลแต่ละชุดจะถูกจัดเก็บใน "บล็อก" และเชื่อมต่อกันเป็น "สายโซ่ (Chain)" โดยไม่สามารถแก้ไขหรือลบย้อนหลังได้ง่าย จึงมีความน่าเชื่อถือสูง

Smart Contract คือโปรแกรมคอมพิวเตอร์ที่ทำงานโดยอัตโนมัติบนระบบ Blockchain เมื่อเงื่อนไขที่กำหนดไว้ในสัญญาเป็นจริง สัญญาจะดำเนินการโดยไม่ต้องผ่านตัวกลาง เช่น ธนาคาร ทนายความ หรือหน่วยงานกลาง



ประเด็นทางกฎหมายเกี่ยวกับ **Blockchain**

ความน่าเชื่อถือของสัญญาอัจฉริยะ

Smart Contract จะยึดถือเป็นสัญญาตามกฎหมายได้หรือไม่ หากไม่มีการลงนามแบบดั้งเดิม?

การระบุตัวตนบนเครือข่าย **Blockchain**

บุคคลนิรนาม (Anonymous) สร้างปัญหาเรื่องการฟอกเงินหรือธุรกรรมผิดกฎหมาย

ทรัพย์สินดิจิทัล **(Digital Assets)**

ความเป็นเจ้าของของ Token, NFT, หรือสินทรัพย์ในระบบ Blockchain ต้องมีกฎหมายรองรับ

แนวโน้มกฎหมาย **Blockchain** ในประเทศไทย

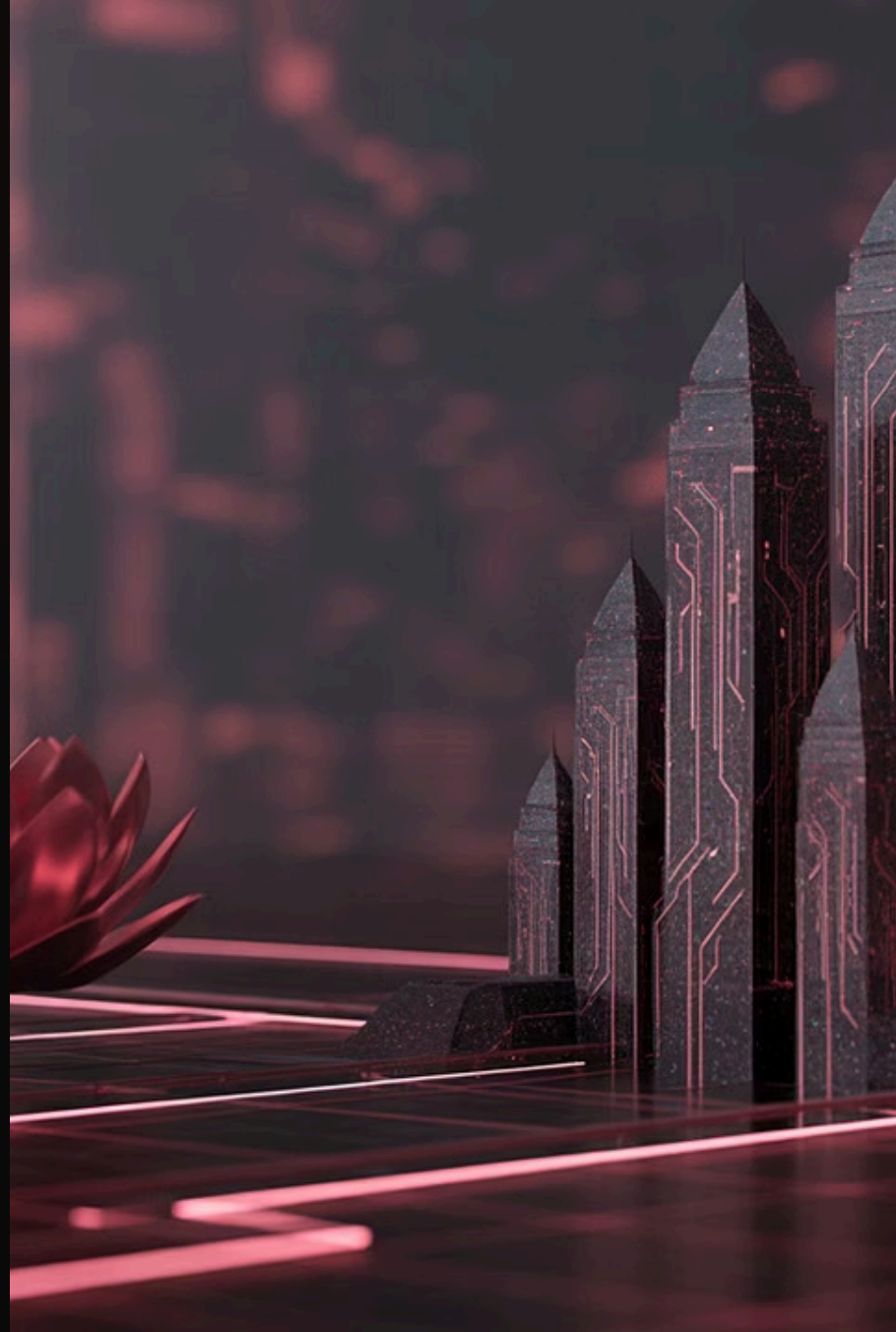
กฎหมายปัจจุบัน

- พระราชกำหนดว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561
- เกณฑ์กำกับจาก ก.ล.ต. ในการระดมทุนผ่าน ICO หรือการเปิดตลาดซื้อขายสินทรัพย์ดิจิทัล

แนวโน้มในอนาคต

- กฎหมายรองรับ Smart Contract ที่มีความผูกพันตามกฎหมาย
- การกำกับดูแล DeFi (Decentralized Finance) และ NFT (Non-Fungible Token)

ตัวอย่างเช่น ธุรกิจที่ใช้ Smart Contract เพื่อจ่ายค่าประกันภัยอัตโนมัติ ต้องมีการตรวจสอบ Source Code และข้อกำหนดตาม พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544



กฎหมายในยุค **Metaverse** (โลกเสมือนจริง)

กฎหมายเทคโนโลยีสารสนเทศในยุค Metaverse หมายถึง กฎหมายที่ใช้กำกับดูแลพฤติกรรม สิทธิ หน้าที่ และธุรกรรมที่เกิดขึ้นภายใน "สภาพแวดล้อมเสมือนจริง" ซึ่งผู้ใช้งานมีปฏิสัมพันธ์ผ่านตัวแทนดิจิทัล (Avatar) และระบบเทคโนโลยี VR/AR หรือ Web3 โดยเฉพาะด้านความเป็นส่วนตัว ทรัพย์สินดิจิทัล และความรับผิดชอบของผู้ให้บริการ

ประเด็นทางกฎหมายเกี่ยวกับ **Metaverse**

การคุ้มครองข้อมูลส่วนบุคคล

ในโลกเสมือน ข้อมูลชีวมิติ การเคลื่อนไหวร่างกาย พฤติกรรมของผู้ใช้ ถือเป็นข้อมูลละเอียดอ่อน ต้องมีการควบคุมการใช้งานอย่างไรบ้าง

การละเมิดสิทธิในพื้นที่เสมือน

เช่น การคุกคามทางเพศใน Avatar หรือการลอกเลียนวัตถุดิจิทัล

ทรัพย์สินเสมือน **(Virtual Assets)**

สินค้าหรือที่ดินใน Metaverse จะมีสถานะทางกฎหมายอย่างไร?

แนวโน้มกฎหมาย **Metaverse** ในต่างประเทศและไทย

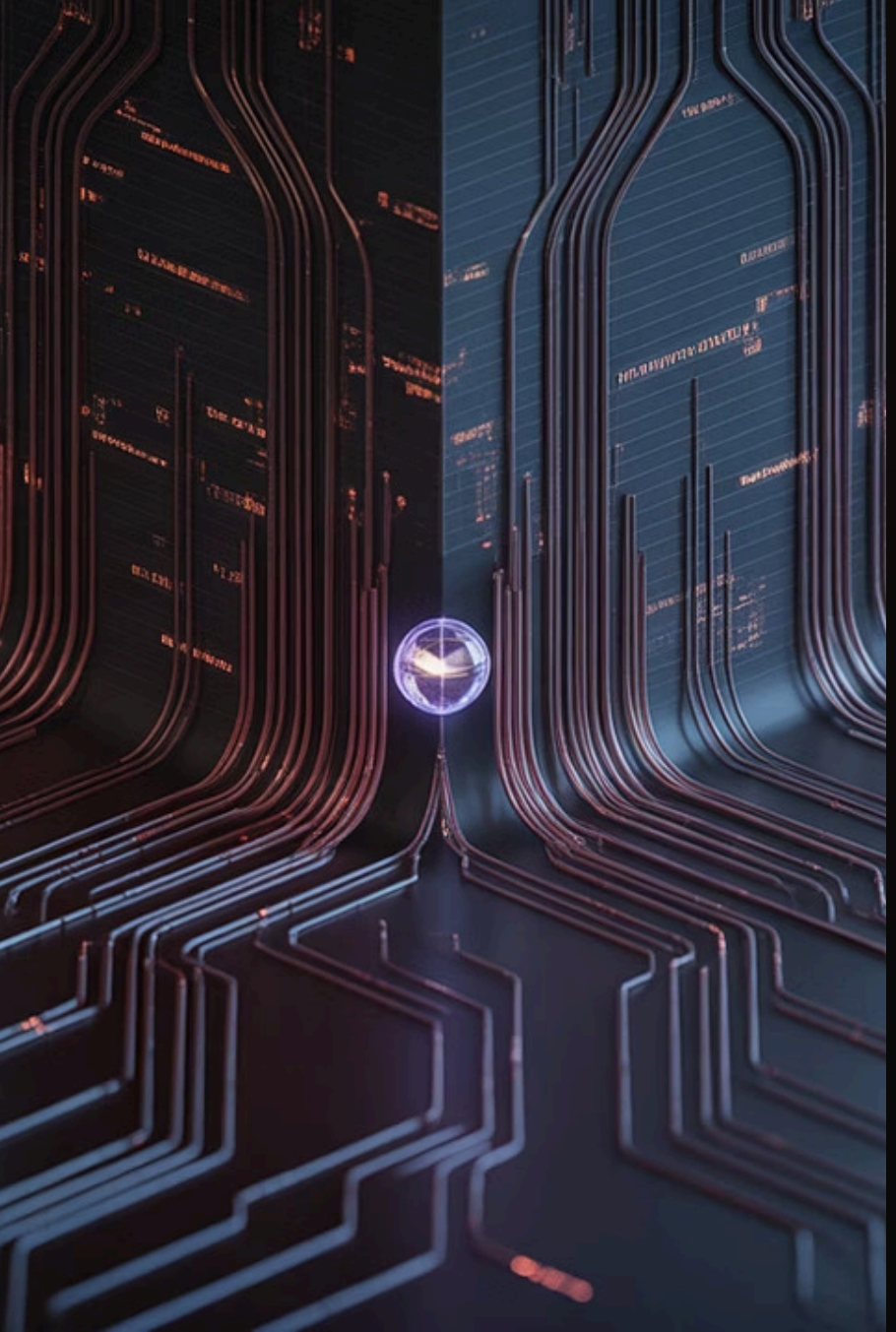
แนวโน้มในต่างประเทศ

กฎหมายในหลายประเทศเริ่มศึกษา กฎหมายแพ่งและพาณิชย์ใน Metaverse เช่น สัญญาในโลกเสมือน, สิทธิครอบครอง NFT

แนวโน้มในประเทศไทย

อาจปรับปรุง กฎหมายทรัพย์สินทางปัญญา ให้รองรับทรัพย์สินดิจิทัล และเพิ่มแนวทางใน PDPA และ พ.ร.บ. คอมพิวเตอร์

ตัวอย่างเช่น บริษัทไทยเปิดร้านค้าเสมือนใน Metaverse หากมีการละเมิดเครื่องหมายการค้า (โลโก้) ต้องสามารถใช้กฎหมายทรัพย์สินทางปัญญาในการร้องเรียนและยุติการใช้งานได้



แนวโน้มของกฎหมายเทคโนโลยีสารสนเทศในอนาคต

แนวโน้มของกฎหมายเทคโนโลยีสารสนเทศในอนาคตจะเน้นที่ "การสร้างกติกากลาง" ที่สมดุลระหว่าง การคุ้มครองสิทธิ และ การส่งเสริมนวัตกรรม โดยต้องมีการอัปเดตกฎหมายอย่างต่อเนื่อง พร้อมสร้างความเข้าใจร่วมกันในสังคมเกี่ยวกับการใช้เทคโนโลยีใหม่อย่างมีจริยธรรมและความรับผิดชอบ

สมดุลระหว่างนวัตกรรมและการคุ้มครอง

กฎหมายต้องไม่เป็นอุปสรรคต่อการพัฒนาเทคโนโลยี แต่ต้องคุ้มครองสิทธิของประชาชนอย่างเพียงพอ

ความร่วมมือระหว่างประเทศ

เทคโนโลยีไม่มีพรมแดน กฎหมายต้องมีความสอดคล้องกันในระดับสากล

ความยืดหยุ่นและปรับตัวได้

กฎหมายต้องสามารถปรับตัวให้ทันกับเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

บทสรุป

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศมีบทบาทอย่างลึกซึ้งในชีวิตประจำวันและระบบเศรษฐกิจ การทำธุรกรรมทางอิเล็กทรอนิกส์จึงกลายเป็นหัวใจสำคัญของการดำเนินธุรกิจสมัยใหม่

กฎหมายที่เกี่ยวข้อง

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560, พระราชกฤษฎีกาว่าด้วยการควบคุมธุรกิจการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ความสำคัญ

กฎหมายเหล่านี้เป็นกลไกสำคัญในการส่งเสริมความน่าเชื่อถือ ความปลอดภัย และสิทธิของผู้ใช้งาน

บทสรุป (ต่อ)

องค์กรธุรกิจจำเป็นต้องเข้าใจทั้งในด้านสิทธิ หน้าที่ และบทลงโทษตามกฎหมาย โดยเฉพาะเรื่องความเป็นส่วนตัวของข้อมูล ความมั่นคงทางไซเบอร์ การใช้บริการ e-Payment การใช้ Smart Contracts และการดำเนินงานในโลกเสมือน (Metaverse) ซึ่งล้วนมีความเกี่ยวข้องกับการบริหารความเสี่ยงทางดิจิทัล

แนวโน้มของกฎหมายในอนาคตจึงมุ่งเน้นการปรับตัวให้เท่าทันเทคโนโลยี เช่น AI Blockchain และ Web 3.0 พร้อมทั้งกำหนดมาตรการเชิงรุกเพื่อคุ้มครองประชาชนและสร้างความเชื่อมั่นให้กับผู้บริโภค

บทสรุป (ต่อ)

กล่าวโดยสรุป การเรียนรู้กฎหมายเทคโนโลยีสารสนเทศไม่เพียงแต่ช่วยให้นักศึกษามีความรู้ความเข้าใจในบริบทของกฎหมายที่เกี่ยวข้องกับโลกดิจิทัลเท่านั้น แต่ยังช่วยส่งเสริมจริยธรรมทางธุรกิจ การกำกับดูแลกิจกรรมออนไลน์อย่างมีธรรมาภิบาล และการใช้เทคโนโลยีเพื่อสร้างนวัตกรรมอย่างรับผิดชอบในยุคเศรษฐกิจดิจิทัลอีกด้วย

ขอบคุณ

กฎหมายการทำธุรกรรมอิเล็กทรอนิกส์

เรียบเรียงโดย รศ.ดร.สุรีรัตน์ อินทร์หม้อ