DIGITAL CITIZENSHIP

(DIGITAL CITIZENSHIP)

ความเป็นพลเมืองดิจิทัล เป็นพลเมืองที่มีความสามารถในการใช้อินเทอร์เน็ตในการบริหารจัดการ ควบคุม กำกับตน รู้ผิดรู้ถูก และรู้เท่าทัน เป็นบรรทัดฐานในการใช้เทคโนโลยีดิจิทัลอย่างเหมาะสม มีความรับผิดชอบ เรียนรู้ที่จะใช้เทคโนโลยีอย่างชาญฉลาด และปลอดภัย พลเมืองดิจิทัลจึงต้องตระหนักถึงโอกาส และความเสี่ยงในโลกดิจิทัล เข้าใจถึงสิทธิและความรับผิดชอบในโลกออนไลน์ ความเป็นพลเมืองดิจิทัล

มติความเป็นพลเมืองดิจิทัล

1. มิติการรักษาอัตลักษณ์และข้อมูลส่วนบุคคล
2. มิติของกิจกรรมบนสื่อสังคมดิจิทัล
3. มิติทักษะและความสามารถในสภาพแวดล้อมดิจิทัล
4. มิติจริยธรรมทางดิจิทัล

มิติการรักษาอัตลักษณ์และข้อมูลส่วนบุคคล

การสร้างอัตลักษณ์ออนไลน์ เพื่อนำเสนอตัวตนบนโลกออนไลน์ พลเมืองดิจิทัลจะต้องมีความตระหนักในความเท่าเทียมกันทางดิจิทัล การรักษาความปลอดภัยของข้อมูลตนเองในสังคมดิจิทัล ที่มีความจำเป็นจะต้องบริหารจัดการข้อมูลของตนเอง รู้ว่าข้อมูลใดควรเผยแพร่และข้อมูลใดไม่ควรเผยแพร่ การปกป้องข้อมูลส่วนบุคคล การจัดการกับความเสี่ยงของข้อมูลของตนในสื่อสังคมดิจิทัล

มิติของกิจกรรมบนสื่อสังคมดิจิทัล

พลเมืองดิจิทัลทีความจำเป็นต้องมีความสามารถในการจัดการธุรกรรมการเงินทางอินเทอร์เน็ต เช่น การซื้อขายสินค้าในอินเทอร์เน็ต บัตรเครดิตอิเล็กทรอนิกส์ การค้าแบบดิจิทัล การเมืองเศรษฐกิจ อินเทอร์เน็ตเป็นได้ทั้งเครื่องมือเพิ่มการมีส่วนร่วมทางการเมืองในระบบ เช่น รัฐบาลใช้อินเทอร์เน็ตในการรับฟังความเห็นของประชาชนก่อนออกกฎหมาย การลงคะแนนเสียงอิเล็กทรอนิกส์ หรือการยื่นคำร้องออนไลน์

มิติจริยธรรมทางดิจิทัล

พลเมืองดิจิทัล จะต้องเป็นผู้รู้กฎหมายที่เกี่ยวกับคอมพิวเตอร์ การกระทำความผิดทางคอมพิวเตอร์ มีความรู้ในงานลิขสิทธิ์และเคารพทรัพย์สินทางปัญญาของผู้อื่น และการปกป้องตนเองและชุมชน มีความรับผิดชอบทางดิจิทัล รู้จักสิทธิเสรีภาพให้เกียรติในการพูดการกระทำในสังคมดิจิทัล มารยาททางดิจิทัล เข้าใจถึงการรับความในการบริหารจัดการความเสี่ยงในโลกออนไลน์ เช่น การไม่ไปรังแกและสามารถจัดการกับการถูกรังแกบนโลกไซเบอร์ **(Cyberbullying)**

การเข้าถึงดิจิทัล (Digital Access)

การรู้ดิจิทัล (Digital literacy)

Digital literacy

ทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล เป็นทักษะด้านดิจิทัลพื้นฐานที่จะเป็นตัวช่วยสำคัญในการปฏิบัติงาน การสื่อสาร และการทำงานร่วมกันกับผู้อื่นในลักษณะ “ทำน้อย ได้มาก” หรือ “Work less but get more impact” และช่วยสร้างคุณค่า (Value Co-creation) และความคุ้มค่าในการดำเนินงาน (Economy of Scale)

เข้าถึง (Access)

การเข้าถึงและใช้ประโยชน์จากเทคโนโลยีดิจิทัล และข้อมูลข่าวสาร เป็นฐานรากในการพัฒนา การสร้างความเจริญเติบโตทางเศรษฐกิจ ผู้เรียนจำเป็นต้องเข้าใจอินเทอร์เน็ตและการเข้าถึงอินเทอร์เน็ตด้วยช่องทางต่าง ๆ รวมถึง ข้อดีข้อเสียของแต่ละช่องทางได้ เพื่อให้สามารถใช้ Search Engine ค้นหาข้อมูลที่ต้องการจาก อินเทอร์เน็ตได้อย่างมีประสิทธิภาพ

การสื่อสารยุคดิจิทัล (Digital Communication)

การสื่อสารยุคดิจิทัล หมายถึง การสื่อสารระหว่างบุคคลและสังคมผ่านเครือข่ายอินเทอร์เน็ตโดยการใช้อุปกรณ์ดิจิทัลต่าง ๆ เช่น คอมพิวเตอร์ โทรศัพท์ สมาร์ทโฟน และผ่านช่องทางการสื่อสารดิจิทัล หรือดิจิทัลแพลตฟอร์ม (Digital Platform)

- การสื่อสารแบบด้วยตัวอักษร (Text)
- การสื่อสารแบบด้วยภาพนิ่ง (Image)
- การสื่อสารด้วยภาพเชิงสัญลักษณ์ (Emoticon และ Sticker)
- การสื่อสารแบบด้วยภาพเคลื่อนไหวจริง (Video)
- การสื่อสารแบบด้วยภาพเคลื่อนไหวจริงแบบทันที่ทันใด (Real Time Video/Live Video)

ความปลอดภัยยุคดิจิทัล Digital Safety)

คือการเข้าใจความรู้พื้นฐานทั่วไปของ ความปลอดภัยบนโลกอินเทอร์เน็ต โดย จะมีอันตรายที่มาจากผู้ไม่ประสงค์ดีใน โลก อินเทอร์เน็ต เครือข่าย สังคม ออนไลน์ ได้อย่างถูกต้องและปลอดภัย เพื่อการ หลีกเลี่ยงภัยคุกคาม และรับมือ กับภัยอันตรายในโลกดิจิทัล

การป้องกันข้อมูลส่วนตัวจากการถูกขโมยหรือเผยแพร่โดยไม่ได้รับอนุญาตเป็นเรื่องสำคัญ ควรใช้รหัสผ่านที่มีความซับซ้อนและไม่ใช้รหัสผ่านเดียวกันในหลายๆ บัญชี สำหรับการใช้งานโซเชียลมีเดีย ควรตั้งค่าความเป็นส่วนตัวและระมัดระวังการแบ่งปันข้อมูลส่วนตัว

รอยเท้าดิจิทัล (DIGITAL FOOTPRINT)

ร่องรอยที่ผู้ใช้อินเทอร์เน็ตและโลกไซเบอร์กระทำการต่าง ๆ ในโลกดิจิทัล เช่น การใช้งานอัปโหลด ข้อมูลส่วนตัว ไฟล์งาน รูปภาพ การใช้งานสมาร์ตโฟน แท็บเล็ต และคอมพิวเตอร์ โดยระบบต่างๆ ของอินเทอร์เน็ตจะบันทึกข้อมูลของผู้ใช้งาน เช่น ชื่อ และข้อมูลส่วนตัว วันเดินปีเกิด ตำแหน่งงาน ผลงาน ข้อมูลการศึกษา ประวัติส่วนตัว ของผู้ใช้งาน ร่องรอยดิจิทัล สามารถบอกให้ผู้อื่นทราบถึงสิ่งที่เราชอบ สิ่งที่สนใจ และสิ่งที่เราอยากทำ

รอยเท้าดิจิทัล
(Digital Footprint)

Active Digital Footprints

ร่องรอยดิจิทัล ที่ผู้ใช้เจตนาบันทึก (Active Digital Footprints) ร่องรอยดิจิทัล ของผู้ใช้งานที่เจตนาบันทึกไว้ในโลกออนไลน์ ข้อมูลที่เราตั้งใจเปิดเผยโดยที่รู้ตัว เช่น อีเมล เบอร์โทร ชื่อโปรไฟล์ เฟซบุ๊ก หรือสิ่งที่เราตั้งใจโพสต์ลงในโซเชียลมีเดีย เช่น สิ่งที่เราพูดหรือโพสต์ รูปที่เราเคยลง สิ่งที่เรากดไลก์ รีทวิต หรือแชร์ ที่ตั้งสถานที่ที่เราอยู่หรือเคยไป

Passive Digital Footprints

ร่องรอยดิจิทัล ที่ผู้ใช้ไม่เจตนาบันทึก (Passive Digital Footprints) ร่องรอยดิจิทัล ของผู้ใช้งานที่ไม่มีเจตนาบันทึกเอาไว้ในโลกออนไลน์ หรือข้อมูลแบบที่ไม่ได้ตั้งใจหรือไม่ได้รู้ตัว เช่น IP Address หรือ Search History ต่าง ๆ ที่เราถูกจัดเก็บเอาไว้ สิ่งที่เราเคยคลิกเข้าไป การซื้อสินค้าออนไลน์ของเรา การเปิดระบบ GPS

ภัยคุกคามทางไซเบอร์

หมายถึง การกระทำหรือการดำเนินการใด ๆ ผ่านการใช้ระบบสารสนเทศหรือเครือข่ายที่ก่อให้เกิดผลเสียต่อระบบข้อมูลเครือข่ายและ / หรือข้อมูลภายใน

การโจมตีทางไซเบอร์มีจุดมุ่งหมายเพื่อสร้างความเสียหายหรือเข้าควบคุมหรือเข้าถึงเอกสารและระบบที่สำคัญภายในเครือข่ายคอมพิวเตอร์ของธุรกิจหรือของส่วนบุคคล การโจมตีทางไซเบอร์เกิดจากบุคคลหรือองค์กรที่มีจุดประสงค์ทางการเมือง อาชญากรรม หรือส่วนตัวในการทำลายหรือเข้าถึงข้อมูลที่เป็นความลับ

MALWARE

มัลแวร์ หรือซอฟต์แวร์ที่เป็นอันตรายจะปลอมตัวเป็นไฟล์แนบอีเมลหรือโปรแกรมที่เชื่อถือได้ (เช่น เอกสารหรือโฟลเดอร์ไฟล์ที่เข้ารหัส) เพื่อแสวงหาประโยชน์จากไวรัสและอนุญาตให้แฮกเกอร์เข้าสู่เครือข่ายคอมพิวเตอร์ การโจมตีทางไซเบอร์ประเภทนี้มักจะทำให้ระบบไอทีทั้งเครือข่ายต้องหยุดชะงัก ตัวอย่างของมัลแวร์ ได้แก่ โทรจัน สปายแวร์ เวิร์ม ไวรัส และแอดแวร์

RANSOMWARE

แรนซัมแวร์คือซอฟต์แวร์ที่เป็นอันตรายหรือมัลแวร์ประเภทหนึ่ง ซึ่งคุกคามเหยื่อด้วยการทำลายหรือบล็อกการเข้าถึงข้อมูลหรือระบบที่สำคัญจนกว่าจะจ่ายค่าไถ่

VIRUS

มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่นๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น

WORM

สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่นๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์ของผู้ใช้

TROJAN

หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จริงๆแล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้ง โดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่อันตรายแฝงตัวมาด้วย

SPYWARE

แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ได้ระบุเอาไว้อีกด้วย

MORE

แนวปฏิบัติในสังคมดิจิทัล (DIGITAL ETIQUETTE)

จรรยามารยาทของการอยู่ร่วมกันในสังคมอินเทอร์เน็ต หรือ โลกดิจิทัลซึ่งเป็นพื้นที่ที่เปิดโอกาสให้ผู้คนเข้ามาแลกเปลี่ยน สื่อสารและทำกิจกรรมรวม กัน ทั้งในชุมชนใหญ่หรือโลกบนอินเทอร์เน็ตก็ไม่ต่างจากสังคมบนโลกแห่งความเป็นจริง ซึ่งจำเป็นต้องมีกฎ กติกาเพื่อ ใช้เป็นกลไกสำหรับการกำกับดูแลพฤติกรรมและการปฏิสัมพันธ์ของสมาชิก

สุขภาพดียุคดิจิทัล (DIGITAL HEALTH)

เรียนรู้อันตรายและผลกระทบด้านสุขภาพในแง่มุมต่าง ๆ ไม่ว่าจะเป็นด้านสุขภาพกาย สุขภาพจิต โรคที่เกิดขึ้น รวมถึงความสัมพันธ์และผลกระทบต่อเยาวชน การใช้อินเทอร์เน็ตและสื่อดิจิทัล เพื่อป้องกัน หลีกเลี่ยง ลดผลกระทบ จนถึงวิธีการรักษาเบื้องต้น ทั้งต่อตนเอง และคนใกล้ตัว เพื่อให้สามารถใช้ชีวิตอย่างมีความสุขในยุคดิจิทัลได้

กฎหมายดิจิทัล (DIGITAL LAW)

กฎหมายดิจิทัลในประเทศไทย

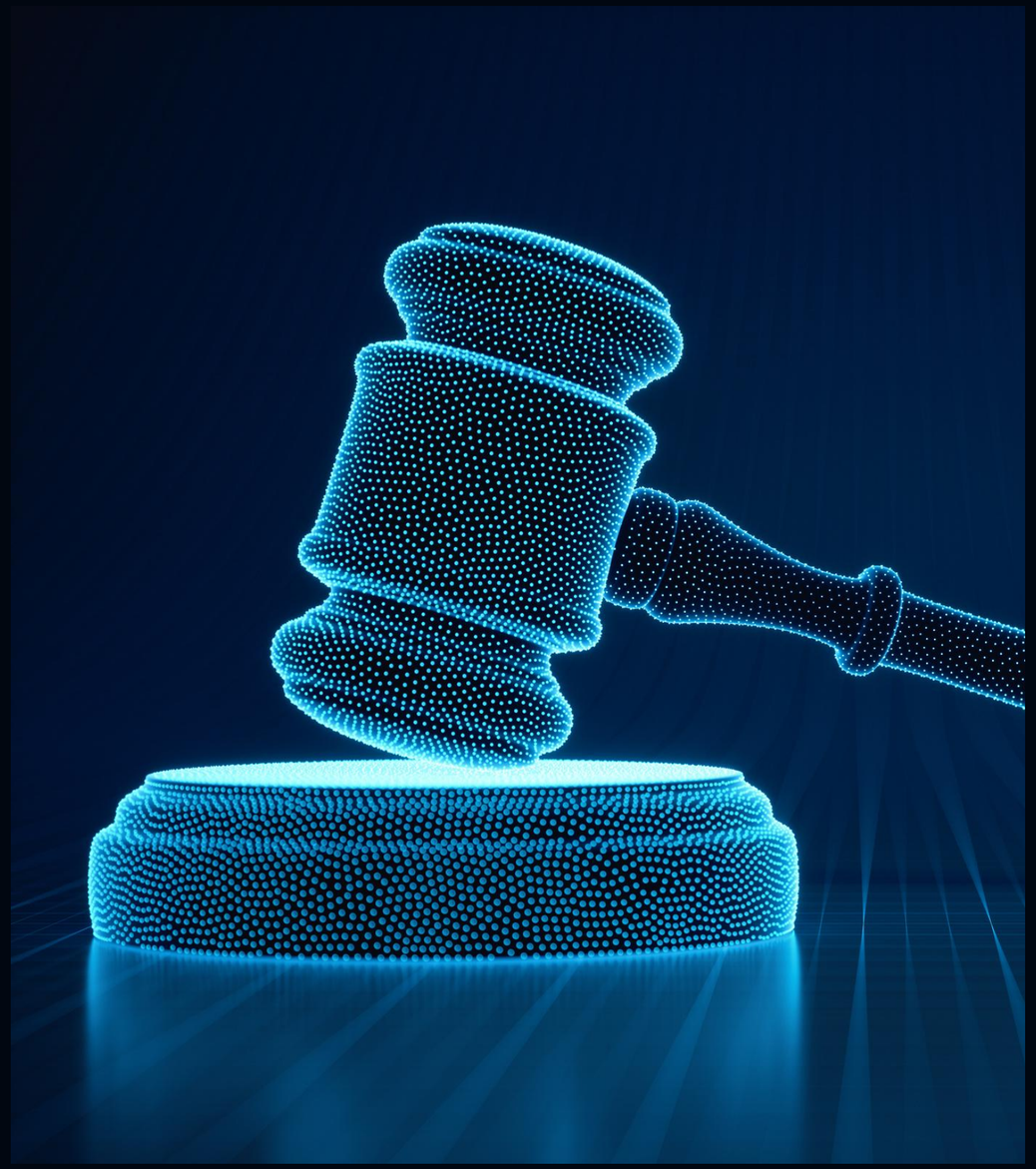
1. กฎหมายธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562 เป็นกฎหมายกลางที่รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ ให้มีผลผูกพันและใช้บังคับได้ตามกฎหมาย ซึ่งได้ประกาศเป็นกฎหมายแล้ว เมื่อวันที่ 22 พฤษภาคม 2562 และมีผลใช้บังคับเมื่อวันที่ 23 พฤษภาคม 2562

- ธุรกรรมทางแพ่งและพาณิชย์ เช่น การทำสัญญากู้ยืมเงินทางอิเล็กทรอนิกส์ การปลดหนี้เงินกู้ทางอิเล็กทรอนิกส์ แต่ไม่ใช้กับธุรกรรมเกี่ยวกับครอบครัวและธุรกรรมเกี่ยวกับมรดก
- ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ เช่น คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐ เช่น การยื่นภาษีทางออนไลน์ เป็นต้น

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 ที่สภานิติบัญญัติแห่งชาติให้ความเห็นชอบเมื่อเดือนธันวาคม 2559 และได้ประกาศลงราชกิจจานุเบกษา เมื่อวันที่ 24 มกราคม 2560 มีผลบังคับใช้แล้วในวันที่ 24 พ.ค. 2560 ซึ่งมีสาระสำคัญ เช่น การฝากร้านใน Facebook และ Instagram ถือว่าเป็นสแปม มีโทษปรับ 200,000 บาท ส่ง SMS โฆษณาโดยไม่รับความยินยอมให้ผู้รับสามารถปฏิเสธข้อมูลนั้นได้ ถือว่าเป็นสแปม มีโทษปรับ 200,000 บาท ส่ง Email ขายของ ถือว่าเป็นสแปม มีโทษปรับ 200,000 บาท



กฎหมายคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

PDPA ย่อมาจาก Personal Data Protection เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคลเพื่อรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ได้ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และปัจจุบันได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565

การคุ้มครองข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ ทั้งทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล, เลขประจำตัวประชาชน, เบอร์โทรศัพท์มือถือ, อาชีพ, ข้อมูลการศึกษา, ข้อมูลการเงิน, รูปถ่าย

ข้อมูลส่วนบุคคล (PERSONAL DATA)

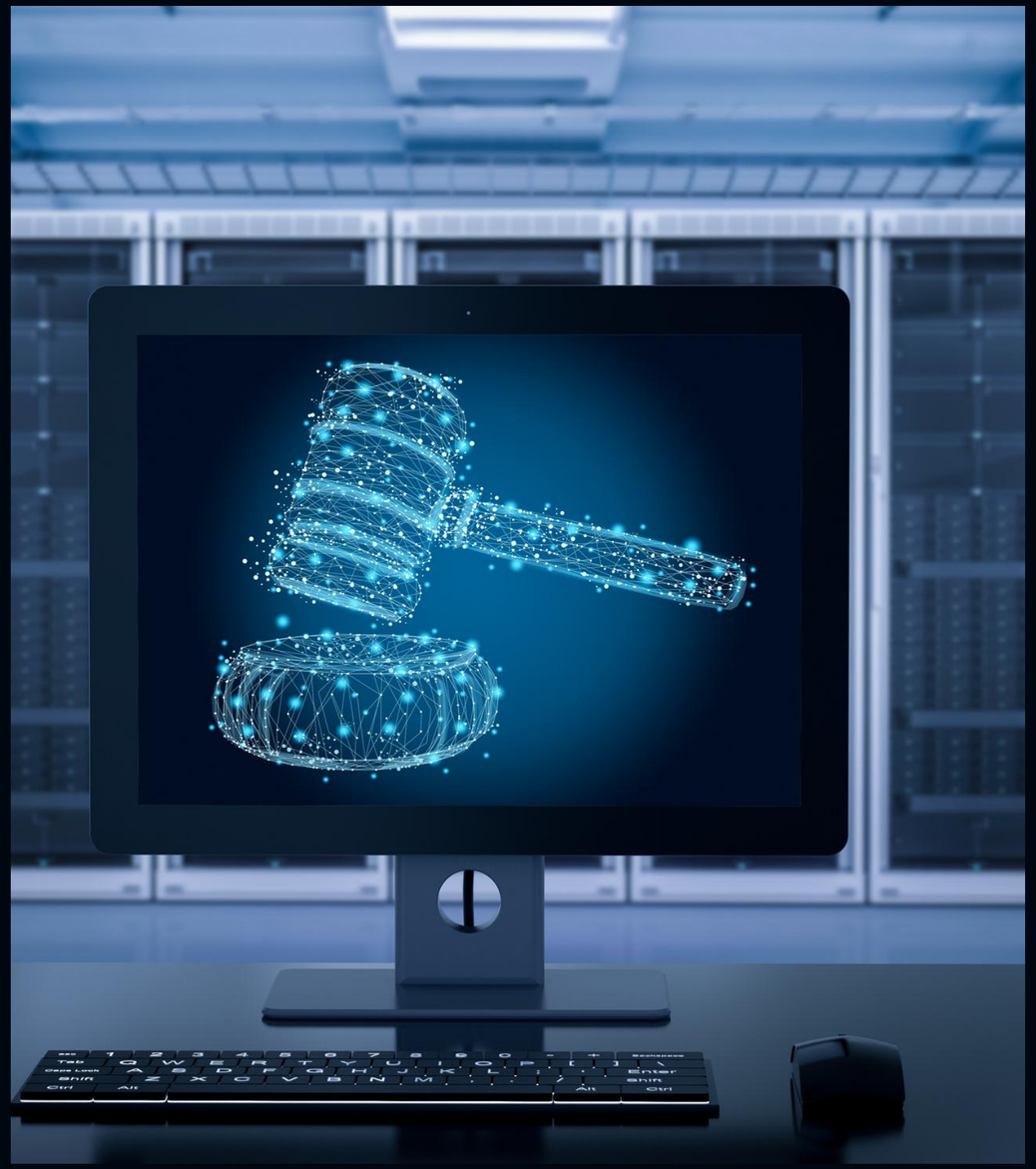
คือ ข้อมูลใด ๆ ที่สามารถระบุตัวบุคคลนั้นได้ (ระบุไปถึงเจ้าของข้อมูล) ไม่ว่าจะเป็นทางตรงหรือทางอ้อมก็ตาม เช่น ชื่อ-นามสกุล หรือชื่อเล่น เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต ที่อยู่, อีเมล์, เลขโทรศัพท์

ข้อมูลส่วนบุคคลที่อ่อนไหว (SENSITIVE PERSONAL DATA)

คือ ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิศาสนาหรือปรัชญา

กฎหมายความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศที่กระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ ซึ่งมีบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม พ.ศ. 2562



เกร็ดความรู้เพิ่มเติม

เทคนิคการสืบค้นข้อมูล
1. เลือก Search Engine ที่เหมาะสม
2. เลือกเว็บไซต์ที่อยู่ใกล้และอยู่ในช่วงเวลาที่เหมาะสม
3. การเลือกใช้คำสำคัญ (Keyword) หรือหัวเรื่อง (Subject) ที่ตรงกับเรื่องที่ต้องการ
4. กำหนดขอบเขตของคำค้น โดยใช้ตัวเชื่อมบูลีน (Boolean Operators) เช่น AND OR NOT NEAR BEFORE เป็นต้น หรือการค้นวลี (Phrase Searching) การตัดคำ หรือการใช้คำเหมือน

1. การค้นหาแบบพื้นฐาน (Basic Search) เป็นการค้นหาสารสนเทศอย่างง่ายๆ ไม่ซับซ้อน โดยใช้คำโดดๆ หรือผสมเพียง 1 คำ ในการสืบค้นข้อมูล
2. การค้นหาแบบขั้นสูง (Advanced Search) เป็นการค้นหาที่ซับซ้อนมากกว่าแบบพื้นฐาน โดยใช้คำเชื่อม 3 ตัว คือ AND, OR, NOT

ประเภททรัพยากรสารสนเทศ
- ทรัพยากรสารสนเทศตีพิมพ์ (Printed materials)
- ทรัพยากรสารสนเทศไม่ตีพิมพ์ (Non-printed materials)
- ทรัพยากรอิเล็กทรอนิกส์ (Electronic materials)

ความหมายของ HTTP และ HTTPS
- HTTP เป็นตัวเรียกให้เซิร์ฟเวอร์ส่งข้อมูลมาให้เพื่อแสดงผลบนหน้าจอได้อย่างถูกต้อง โดยเป็นการส่งข้อมูลแบบ Clear text *ไม่ได้ทำการเข้ารหัส* ทำให้สามารถถูกดักจับและอ่านข้อมูลได้ง่าย
- HTTPS *จะเป็นโปรโตคอลที่เข้ารหัสในการสื่อสาร* โดยใช้ Asymmetric Algorithm