

พ.ร.ก.อาชญากรรมทางเทคโนโลยีฉบับใหม่ : ยกระดับปราบปราม ‘มัลแวร์’

ปัจจุบันรูปแบบอาชญากรรมทางการเงินได้พัฒนาไปอย่างมีนัยสำคัญ กลุ่มอาชญากรไม่เพียงแต่โอนเงินออกจากบัญชีผู้เสียหายเท่านั้น แต่ยังแปลงสภาพเงินที่ได้จากการกระทำความผิดเป็นสินทรัพย์ดิจิทัล (Digital Assets) ซึ่งทำให้การติดตามและตรวจสอบเส้นทางการเงินทำได้ยากยิ่งขึ้น

เพื่อจัดการกับปัญหาดังกล่าว ภาครัฐจึงได้มีการตราพระราชกำหนด (พ.ร.ก.) สองฉบับ ได้แก่ พ.ร.ก. กำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 และ พ.ร.ก. การประกอบธุรกิจสินทรัพย์ดิจิทัล (ฉบับที่ 2) พ.ศ. 2568 เพื่อให้ใช้ในทางที่สอดคล้องกัน โดยให้มีผลใช้ 13 เม.ย. 2568 ผู้เขียนขอสรุปใจความสำคัญตามประเด็น ดังนี้

● เหตุผลในการปรับปรุง พ.ร.ก. สินทรัพย์ดิจิทัล?

เหตุผลสำคัญคือ เพื่อกำกับและควบคุมธุรกิจสินทรัพย์ดิจิทัลที่อยู่นอกประเทศไทย แต่มีการให้บริการแก่บุคคลในไทย ที่ผ่านมา ผู้กระทำความผิดมักโอนเงินที่ได้จากการกระทำความผิดไปยังแพลตฟอร์มสินทรัพย์ดิจิทัลในต่างประเทศ เพื่อหลีกเลี่ยงการบังคับใช้กฎหมายไทย พ.ร.ก. ฉบับใหม่ จึงกำหนดให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต่างชาติที่ให้บริการแก่ลูกค้าในไทย ในลักษณะที่มีการชักชวน หรือโฆษณาด้วยวิธีการใด ๆ กับบุคคลในไทย ต้องขออนุญาตตามกฎหมายไทย โดยหากฝ่าฝืนกระทรวง DE อาจปิดกั้นการเข้าถึงได้

ลักษณะที่ถือว่าเป็น “การให้บริการในไทย” ได้แก่ (1) การแสดงผลในการประกอบธุรกิจเป็นภาษาไทย ทั้งหมดหรือบางส่วน (2) การจดทะเบียนโดเมนที่เกี่ยวข้องกับประเทศไทย เช่น .th หรือ .ไทย หรือชื่ออื่นใดที่หมายถึงประเทศไทย (3) การกำหนดให้ชำระเงินเป็นสกุลเงินบาท หรือผ่านบัญชีเงินฝากหรือบัญชีอิเล็กทรอนิกส์ในประเทศไทย

(4) การกำหนดให้ใช้กฎหมายไทยเป็นกฎหมายที่ใช้บังคับหรือกำหนดให้ดำเนินคดี



กรุงเทพธุรกิจ Legal Vision นิติทัศน์ 4.0

● ดร.สุมาพร มานะสันต์

ผู้อำนวยการส่วนกฎหมายการอบรม
การลงโทษและเศรษฐกิจระหว่างประเทศ
สำนักงานเศรษฐกิจการคลัง

ในศาลไทย (5) การจ่ายค่าบริการแก่ผู้ให้บริการสืบค้น เพื่อช่วยให้ผู้ให้บริการในไทยเข้าถึงบริการเป็นการเฉพาะ (6) การมีสำนักงานหรือบุคลากรในประเทศไทย เพื่อสนับสนุนการให้บริการ (7) ลักษณะอื่นๆ ที่คณะกรรมการ ก.ล.ต. อาจประกาศกำหนดเพิ่มเติมในอนาคต

นอกจากนี้ ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลในไทย ยังมีหน้าที่คัดกรองและเฝ้าระวังการให้บริการที่เกี่ยวข้องกับบุคคล หรือกระเป๋าสินทรัพย์ที่อยู่ในบัญชี Blacklist โดยกฎหมายได้กำหนดโทษหากไม่ปฏิบัติตาม



และยังให้มีโทษรวมถึง “เจ้าของบัญชีสินทรัพย์ดิจิทัล” ด้วย

● มีการจัดตั้ง สปอท.

กฎหมายกำหนดให้มีการจัดตั้ง ศูนย์ปฏิบัติการเพื่อป้องกันและปราบปราม

อาชญากรรมทางเทคโนโลยี (สปอท.) เพื่อทำหน้าที่เป็นศูนย์กลางในการรับแจ้งเหตุ ตรวจสอบ รวบรวม และแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐและภาคเอกชน อำนาจสำคัญประการหนึ่งของ สปอท. คือการประกาศรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลที่เกี่ยวข้องกับการกระทำความผิด

● มาตรการคัดกรอง SMS ที่มีความเสี่ยง

กฎหมายกำหนดให้สำนักงาน กสทช. มีหน้าที่กำหนดมาตรฐานให้ผู้ให้บริการเครือข่ายโทรศัพท์และผู้ให้บริการโทรคมนาคม ตรวจสอบและคัดกรองข้อความสั้นทางโทรศัพท์มือถือ (SMS) ที่มีความเสี่ยงต่อการหลอกลวง เช่น ข้อความเชิญชวนให้เล่นการพนันออนไลน์ หรือข้อความชักชวนให้ลงทุนในธุรกิจที่ผิดกฎหมาย

● การระงับให้บริการโทรคมนาคมและการแพร่หลายของข้อมูลคอมพิวเตอร์

กฎหมายกำหนดกลไกเพื่อให้การ
ระงับบริการสามารถทำได้อย่างรวดเร็ว เมื่อ
พบหลักฐานอันควรเชื่อว่ามีผู้ใช้บริการ
โทรคมนาคมเพื่อกระทำความผิด หน่วยงาน
ที่เกี่ยวข้องอย่างสำนักงานตำรวจแห่งชาติ
กรมสอบสวนคดีพิเศษ (DSI) สำนักงาน
ป้องกันและปราบปรามการฟอกเงิน (ปปง.)
หรือ ศปอท. สามารถแจ้งให้สำนักงาน กสทช.
สั่งระงับการให้บริการโดยทันที รวมถึงมี
อำนาจระงับเว็บไซต์ที่ให้บริการสินทรัพย์
ดิจิทัลโดยไม่ได้รับอนุญาตตามกฎหมาย

● การกำหนดความรับผิดชอบร่วมของ ภาคเอกชน

กฎหมายกำหนดให้ภาคเอกชน (ธนาคาร
ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ผู้ให้
บริการสื่อสังคมออนไลน์ และผู้ให้บริการ
โทรคมนาคม) มีหน้าที่ปฏิบัติตามมาตรฐาน
หรือมาตรการป้องกันอาชญากรรมทาง
เทคโนโลยี (มาตรฐานฯ) ที่หน่วยงานกำกับ
ดูแลกำหนด หากไม่ปฏิบัติตามมาตรฐาน
ดังกล่าวและเกิดความเสียหายจากการ
กระทำความผิดอาชญากรรมทางเทคโนโลยี
ภาคเอกชนจะต้องมีส่วนร่วมรับผิดชอบในความ
เสียหายที่เกิดขึ้น โดยศาลจะเป็นผู้พิจารณา
สัดส่วนความรับผิดชอบตามความเหมาะสม

อย่างไรก็ดี หากภาคเอกชนสามารถ
พิสูจน์ได้ว่าได้ปฏิบัติตามมาตรฐานที่กำหนด
โดยหน่วยงานกำกับดูแลแล้ว ก็อาจไม่ต้อง
รับผิดชอบต่อความเสียหายที่เกิดขึ้น

มาตรฐานฯ ที่กล่าวมานั้น หน่วยงาน
กำกับดูแล เช่น ธปท. สำนักงาน ก.ล.ต. และ
สำนักงาน กสทช.มีหน้าที่กำหนดเพื่อให้
ผู้ประกอบธุรกิจที่ตนเองกำกับดูแล เช่น ธนาคาร
ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลผู้ให้บริการ
เครือข่ายโทรศัพท์ และผู้ให้บริการสื่อสังคม
ออนไลน์ ปฏิบัติตามมาตรฐานดังกล่าว

● ความรับผิดชอบของการและผู้บริหาร

กฎหมายกำหนดความรับผิดชอบบุคคล
ของกรรมการและผู้บริหารไว้อย่างชัดเจน
ในกรณีนี้ ศปอท. ได้ประกาศรายชื่อบุคคล
หรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลที่เกี่ยวข้อง
กับการกระทำความผิด และขอให้หน่วยงาน
เอกชนดำเนินการปฏิเสธการเปิดบัญชีระงับ
การให้บริการ หรือปิดบัญชี แต่หน่วยงาน
เอกชนไม่ปฏิบัติตาม

ในกรณีดังกล่าว นอกจากบริษัทจะ
ต้องรับโทษปรับแล้ว หากความผิดนั้นเกิด
จากการสั่งการหรือการละเลยของกรรมการ
หรือผู้บริหาร บุคคลเหล่านั้นจะต้องรับผิดชอบ
เป็นการส่วนตัว โดยมีทั้งโทษจำคุกและปรับ

● บทลงโทษกรณีการลงทะเบียนซิมการ์ด ไม่ถูกต้อง

กฎหมายยังได้กำหนดบทลงโทษสำหรับ
การลงทะเบียนซิมการ์ดที่ไม่ถูกต้อง โดย
ทั้งผู้ซื้อและผู้ขายเลขหมายโทรศัพท์ที่ลง
ทะเบียนไม่ถูกต้อง หากกระทำโดย “รู้หรือ
ควรรู้” ว่าจะมีการนำเลขหมายนั้นไปใช้ในการ
กระทำความผิด จะมีโทษทั้งจำคุกและปรับ

● กลไกการเงินให้แก่อัยการ

กฎหมายกำหนดให้หน่วยงานที่เกี่ยวข้อง
เช่น สำนักงานตำรวจแห่งชาติ กรมสอบสวน
คดีพิเศษหรือธนาคาร มีหน้าที่รายงานข้อมูล
ธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทาง
เทคโนโลยีให้สำนักงาน ปปง. ตรวจสอบ
เมื่อสำนักงาน ปปง. ตรวจสอบแล้ว จะประกาศ
บัญชีต้องสงสัยในราชกิจจานุเบกษา และ
แจ้งให้ผู้เสียหายยื่นคำร้องขอคืนเงินพร้อม
หลักฐานเพื่อเสนอให้คณะกรรมการธุรกรรม
ตามกฎหมาย ปปง. พิจารณาสั่งคืนเงินให้แก่
ผู้เสียหายต่อไป ทั้งนี้ รายละเอียดของ
กระบวนการดังกล่าวจะมีการกำหนดใน
กฎกระทรวงต่อไป

ท้ายที่สุด ผู้เขียนเห็นว่า การปรับปรุง
กฎหมายครั้งนี้แสดงให้เห็นถึงการปรับ
ตัวของกฎหมายไทยเพื่อรับมือกับความ
ท้าทายใหม่ในโลกดิจิทัลที่มีลักษณะ
ไร้พรมแดน และมีการเชื่อมโยงธุรกรรม
ทางการเงินระหว่างประเทศอย่างรวดเร็ว

สำหรับภาคธุรกิจ การปฏิบัติตาม
มาตรฐานหรือมาตรการป้องกันที่หน่วย
งานกำกับดูแลจะประกาศกำหนด ถือเป็น
สิ่งที่จำเป็นที่ควรศึกษาอย่างรอบคอบ เพื่อ
หลีกเลี่ยงความรับผิดทั้งขององค์กรและ
ผู้บริหาร **สำหรับประชาชน**การปรับปรุงกฎหมาย
ในครั้งนี้ จะช่วยเพิ่มความคุ้มครองและกลไก
การเยียวยาให้แก่ผู้เสียหาย พร้อมทั้งเพิ่ม
ประสิทธิภาพให้กับหน่วยงานภาครัฐในการ
ติดตามเส้นทางการเงินที่เกี่ยวข้องกับการ
กระทำความผิดได้ครอบคลุมขึ้น