**รายงานสรุป**
**NBTC Public Forum ครั้งที่ ๑/๒๕๖๕**
**“กฎหมาย PDPA กับมิติใหม่ของการจัดการปัญหา SCAM”**
**วันจันทร์ที่ ๓๐ พฤษภาคม ๒๕๖๕ เวลา ๑๓.๐๐ – ๑๖.๓๐ น.**
**ณ อาคารหอประชุมชั้น ๑ สำนักงาน กสทช. พหลโยธินซอย ๘ กรุงเทพฯ**

วันจันทร์ที่ ๓๐ พฤษภาคม ๒๕๖๕ สำนักงานกสทช. ได้จัดงาน NBTC Public Forum ครั้งที่ ๑/๒๕๖๕ เรื่อง “กฎหมาย PDPA กับมิติใหม่ของการจัดการปัญหา Scam” ณ อาคารหอประชุมชั้น ๑ สำนักงาน กสทช. พหลโยธินซอย ๘ โดยมีศาสตราจารย์ ดร.พิรงรอง รามสูต กสทช. เป็นประธานกล่าวเปิดงาน การเสวนาครั้งนี้มีวิทยากรจำนวน ๕ ท่าน ได้แก่ นายอาทิตย์ สุริยะวงศ์กุล อนุกรรมการด้านการสื่อสารและเทคโนโลยีสารสนเทศ สภาองค์กรของผู้บริโภค, พลตำรวจตรีนิเวศน์ อาภาวศิน ผู้บังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี (ผบก.ตอท.) , รองศาสตราจารย์ ดร.ทศพล ทรรศนกุลพันธ์ กรรมการคุ้มครองข้อมูลส่วนบุคคล, ดร.รอม หิรัญพฤกษ์ ผู้ทรงคุณวุฒิด้านเทคโนโลยีสารสนเทศ, นายประวิทย์ ลี่สถาพรวงศา ประธานอนุกรรมการคุ้มครองผู้บริโภคด้านกิจการโทรคมนาคม โดยมีนางสาวกรรณิการ์ กิจติเวชกุล เป็นผู้ดำเนินรายการ

**ศาสตราจารย์ ดร. พิรงรอง รามสูต** กล่าวเปิดการเสวนาว่า วันที่ ๑ มิถุนายน ๒๕๖๕ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีผลบังคับใช้หลังจากล่าช้ามา ๒ ปี เนื่องจากสถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา ๑๙ โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ หรือ เนคเทค เป็นผู้ยกร่างกฎหมายฉบับนี้ ประเทศไทยมีการใช้ประโยชน์จากพื้นที่ออนไลน์ค่อนข้างสูง คนไทยติดอันดับ ๑ ของโลกในการซื้อสินค้าออนไลน์ประจำทุกสัปดาห์ อัตราเฉลี่ยอยู่ที่ร้อยละ ๖๗.๕ ขณะที่ค่าเฉลี่ยของโลกคือร้อยละ ๕๘.๕ และ คนไทยติดอันดับ ๔ ของโลกในการชำระเงินผ่านโทรศัพท์เคลื่อนที่ หรือคิดเป็นร้อยละ ๓๓.๑ ขณะที่ค่าเฉลี่ยของโลกคือร้อยละ ๒๕.๕ คนไทยใช้เฟซบุ๊กติดอันดับ ๘ ของโลก หรือจำนวน ๕๘.๓ ล้านคน สถิติดังกล่าวจึงสะท้อนให้เห็นว่า เหตุใดข้อมูลส่วนบุคคลของคนไทยจึงเกิดการรั่วไหลและเกิดปัญหาการละเมิดข้อมูลออนไลน์

ในต่างประเทศมีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ปี พ.ศ. ๒๕๔๒ และมีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นกลไกในการกำกับดูแล สำหรับประเทศไทย หากเป็นข้อมูลส่วนบุคคลที่อยู่ในฐานข้อมูลของรัฐจะอยู่ในความดูแลของพระราชบัญญัติข้อมูลข่าวสารของราชการ ซึ่งเป็นกฎหมายที่มีวัตถุประสงค์ที่แตกต่างจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ดังนั้นเมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้แล้ว ถือเป็นโอกาสที่จะได้แลกเปลี่ยนความรู้ว่า กฎหมายฉบับนี้จะส่งผลต่อการเพิ่มโอกาสในการจัดการปัญหา Scam อย่างไรได้บ้าง โดยเฉพาะในประเด็นของความเป็นส่วนตัวซึ่งการคุ้มครองข้อมูลส่วนบุคคลอาจไม่ใช่วัฒนธรรมพื้นฐานของคนไทย เราจึงต้องสร้างความเข้าใจ การสร้างความตระหนักรู้ การสร้างนิสัย หรือแบบแผนการปฏิบัติที่ดีให้กับประชาชน

ศาสตราจารย์ ดร.พิรงรองฯ เห็นว่า การคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องที่ทุกภาคส่วนต้องร่วมมือกัน โดยเฉพาะผู้รับใบอนุญาต การทำ Privacy by design ต้องร่วมกันระหว่างผู้บริโภคและผู้รับใบอนุญาต

ขณะที่การตระหนักรู้เรื่องข้อมูลส่วนบุคคลยังไม่ใช่วัฒนธรรมของไทย สังคมไทยแต่เดิมไม่ให้ความสำคัญกับข้อมูลส่วนบุคคล แต่ปัจจุบันข้อมูลส่วนบุคคลเป็นทองคำเพราะสามารถนำไปวิเคราะห์พฤติกรรมการตลาดได้ ดังนั้นในอนาคตทุกส่วนต้องร่วมมือกันป้องกัน จึงต้องมีคณะทำงานร่วมกันในหลายมิติเป็นความร่วมมือในระดับที่เท่าเทียมทั้งภาครัฐและภาคประชาสังคม

**นายอาทิตย์ สุริยะวงศ์กุล** นำเสนอแนวทางการจัดการปัญหาการหลอกลวงทางโทรศัพท์กับกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยยกตัวอย่างศูนย์คุ้มครองผู้ใช้บริการทางการเงิน หรือ เว็บไซต์ 1213.or.th ซึ่งให้ความสำคัญกับปัญหา Scam และได้แสดงให้เห็นขั้นตอนของการถูกหลอกลวง เช่น มิจฉาชีพอาจได้เลขหมายโทรศัพท์เคลื่อนที่จากการสุ่ม หรือจากข้อมูลที่รั่วไหล จากนั้นโทรศัพท์หาเหยื่อเพื่อหลอกถามสถานะทางการเงิน หากเงินน้อยจะถูกล่อลวงให้ไปทำธุรกรรมที่ตู้เอทีเอ็ม เงินมากอาจล่อลวงให้ไปดำเนินการที่ธนาคารสาขา จุดเริ่มต้นของการล่อลวงคือ การติดต่อผ่านเลขหมายโทรศัพท์ของเหยื่อ จากนั้นใส่เนื้อหาปลอม เช่น การหลอกว่าติดต่อจากธนาคารให้กู้เงิน ตามด้วยการสร้างความน่าเชื่อถือให้เหยื่อหลงเชื่อว่าเป็นบุคคลหรือหน่วยงานที่อ้างโดยการรู้ข้อมูลบางอย่างเช่น สามารถเรียกชื่อนามสกุลของเหยื่อได้ถูกต้อง เมื่อเหยื่อหลงเชื่อก็จะขอให้ทำตามขั้นตอนเพื่อโอนเงินให้กับมิจฉาชีพ ทั้งนี้ข้อมูลที่มิจฉาชีพใช้มี ๒ ส่วนคือ ๑) ข้อมูลที่ใช้ในการติดต่อ เช่น เลขหมายโทรศัพท์ อีเมล id line เป็นต้น ๒) ข้อมูลที่ทำให้เกิดความน่าเชื่อถือ เช่น สถานะทางการเงิน อาชีพ ชื่อนามสกุล ที่อยู่ เป็นต้น นายอาทิตย์ยังได้ยกตัวอย่างกรณีข้อมูลรั่วไหลปี ๒๕๖๑ – ๒๕๖๔ ซึ่งเกี่ยวข้องกับเลขหมายโทรศัพท์เคลื่อนที่ เช่น กรณีข้อมูลลูกค้าเว็บไซต์ ไอทรูมาร์ท (iTrueMart) จำนวนประมาณ ๔๖,๐๐๐ แฟ้ม รั่วไหลเมื่อต้นเดือนมีนาคม ๒๕๖๑ เป็นแฟ้มภาพสำเนาบัตรประจำตัวประชาชน ใบขับขี่ และหนังสือเดินทาง ที่ใช้ลงทะเบียนซิมกับผู้ให้บริการโทรศัพท์เคลื่อนที่ โดยบริษัทได้ปิดการเข้าถึงสำเร็จในวันที่ ๑๒ เมษายน ๒๕๖๑

สำหรับวิธีการชักจูงใจเพื่อให้การหลอกลวงสำเร็จมีงานศึกษาพบว่ามี ๕ ขั้นตอน ได้แก่ ๑) การสร้างความน่าเชื่อถือ เช่น อ้างว่าเป็นเจ้าหน้าที่จากศาล และอาจทราบข้อมูลส่วนบุคคลของเหยื่อ ๒) สร้างความวิตกกังวลให้กับเหยื่อ เช่น ท่านได้รับหมายศาล ๓) ให้ติดต่อกลับโดยเสนอความช่วยเหลือเพื่อสร้างความรู้สึกเห็นอกเห็นใจและความเป็นพวกเดียวกันเพื่อให้เหยื่อติดต่อกลับตามช่องทางที่กำหนด ๔) การกำหนดเส้นตาย เร่งด่วนให้รีบดำเนินการเพื่อให้เหยื่อไม่สามารถตรวจสอบข้อเท็จจริงได้ ๕) ปิดงานโดยขอให้เหยื่อทำตามที่มิจฉาชีพกำหนด

นายอาทิตย์เสนอว่า จาก ๕ ขั้นตอนดังกล่าวจะเห็นได้ว่า หน่วยงานกำกับดูแลสามารถเข้าแทรกแซงได้ในขั้นตอนที่ ๑, ๓ และ ๕ โดยขั้นตอนที่ ๑ มิจฉาชีพสามารถสร้างความเชื่อถือเพราะรู้ข้อมูลส่วนบุคคลของเหยื่อ ข้อมูลส่วนบุคคลที่รั่วไหลทำให้มิจฉาชีพสามารถนำไปสร้างความน่าเชื่อถือ ขั้นตอนที่ ๓ คือ เมื่อเหยื่อติดต่อกลับไปยังเลขหมายของมิจฉาชีพ ซึ่งไม่มีระบบแจ้งเตือนว่า เลขหมายที่ให้ติดต่อกลับนั้นมีความผิดปกติ และขั้นตอนที่ ๕ การป้องกันอาจอยู่ที่สถาบันทางการเงิน เช่น ให้มีการแจ้งเตือนกรณีมีการโอนเงินไปยังบัญชีที่พบว่ามีความผิดปกติ เป็นต้น

ทั้งนี้การหลอกลวงยังเกี่ยวข้องกับบริบททางสังคมที่เอื้อให้เกิดการหลอกลวง เช่น ๑) หน่วยงานของรัฐและเอกชนต่างขอให้ประชาชนต้องลงทะเบียนออนไลน์เพื่อขอรับบริการมากขึ้น ทั้งที่อาจ

จำเป็นหรือไม่จำเป็นต่อการให้บริการ ทำให้ประชาชนกังวลว่า หากไม่ให้ข้อมูลส่วนบุคคลอาจไม่ได้รับบริการ และทำให้เห็นว่าการให้ข้อมูลส่วนบุคคลเป็นเรื่องปกติ เพราะทั้งหน่วยงานรัฐและหน่วยงานเอกชนต่างต้องการข้อมูลส่วนบุคคลกันอย่างมาก ๒) ช่องทางติดต่อหน่วยงานรัฐมีความหลากหลายจนประชาชนไม่สามารถแยกแยะได้ว่า ช่องทางใดเป็นช่องทางที่แท้จริงหรือช่องทางหลอกลวง ตัวอย่าง ประเทศสิงคโปร์ จะกำหนดชื่อโดเมนไว้อย่างชัดเจน ทั้งเว็บไซต์ และอีเมล เพื่อเป็นช่องทางติดต่อสำหรับประชาชนและประชาสัมพันธ์ให้ประชาชนรับทราบ หากไม่ใช่ชื่อโดเมนที่ระบุ จะไม่ใช่หน่วยงานของรัฐ ขณะที่การจดทะเบียนเว็บไซต์ของไทยมีความหลากหลายมากทำให้แยกแยะได้ยาก หรือ การลงทะเบียนฉีดวัคซีนของไทยมีหลายช่องทางมีความหลากหลายมาก ทำให้มิจฉาชีพมีโอกาสเพิ่มมากขึ้นในการสร้างช่องทางหลอกลวงได้ ๓) วิธีการดำเนินธุรกิจในปัจจุบันสร้างความเคยชินให้ผู้บริโภคต้องให้ข้อมูลส่วนบุคคล เช่น การสั่งสินค้าออนไลน์ ต้องใส่เลขหมายโทรศัพท์ของผู้สั่งสินค้าด้วย และผู้บริโภคสินค้าออนไลน์ต้องเคยชินกับการได้รับการติดต่อจากบุคคลแปลกหน้าได้ตลอดเวลา ไม่สามารถปฏิเสธเลขหมายแปลกหน้าได้ ๔) สิ่งที่มิจฉาชีพเสนอไม่ใช่สิ่งที่เกินจากความเป็นไปได้ เป็นสิ่งที่เกิดขึ้นจริง การหลอกลวงจึงประสบความสำเร็จสูง

นายอาทิตย์ได้นำเสนอกรณีประเทศสิงคโปร์ว่ามีการตั้งศูนย์ศึกษาพฤติกรรมศาสตร์เพื่อหาเหตุผลว่าทำไมประชาชนเชื่อสิ่งที่มิจฉาชีพหลอกลวงเพื่อเป็นข้อมูลพื้นฐานในการจัดการปัญหาและมีการจัดตั้งคณะกรรมการร่วมระหว่างกระทรวงมหาดไทย สำนักงานตำรวจแห่งชาติ กระทรวงสื่อสาร กระทรวงพาณิชย์ และธนาคารกลาง โดยประเทศสิงคโปร์พบว่า แก๊งมิจฉาชีพ ไม่ได้ตั้งอยู่ในสิงคโปร์แต่ใช้ภาษาจีนในการหลอกลวงประชาชนสิงคโปร์ มาเลเซีย ไต้หวัน ฮ่องกง จึงเกิดเป็นความร่วมมือระหว่างประเทศในการแก้ไขปัญหานี้ สิงคโปร์ตั้ง “สแกมชิล” (Scam shield) เพื่อรับแจ้งปัญหาและเป็นฐานข้อมูล

ประเทศไทยมีการกำหนดระยะเวลาในการแก้ไขปัญหาแก๊งหลอกลวงทางการเงิน จากข้อมูลของเว็บไซต์ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย ได้แจ้งรายละเอียดของระยะเวลาในการรับเรื่องร้องเรียนและแก้ไขปัญหาของธนาคารไทยที่ได้สัญญาไว้ โดยแจ้งว่า หากผู้ร้องเรียนติดต่อผ่านเว็บไซต์หรืออีเมลธนาคารทุกแห่งจะสามารถรับเรื่องร้องเรียนได้ภายใน ๑ วัน การแจ้งผลความคืบหน้าการดำเนินการได้ภายใน ๑๕ วัน โดยธนาคารที่สามารถรับเรื่องร้องเรียนและแจ้งผลดำเนินการได้เร็วที่สุดคือ ธนาคารเกียรตินาคิน รวมถึงมีการวัดผลการให้บริการของ Call center และ การแก้ไขปัญหาเรื่องร้องเรียนของธนาคารแต่ละแห่งเพื่อทำให้เกิดการแข่งขัน

สำหรับแพลตฟอร์มของผู้ให้บริการที่กระตุ้นผู้ใช้บริการแบบ Look at me และแบบ Look at this โดยแบบ Look at me จะมีความเสี่ยงเรื่องข้อมูลส่วนบุคคลมากกว่า ควรมีการทำงานร่วมกับ กลุ่มโฆษณา หรือกลุ่มกิจกรรมออนไลน์ ซึ่งมักจัดกิจกรรมที่กระตุ้นให้บุคคลเปิดเผยข้อมูลส่วนบุคคลในพื้นที่สาธารณะ เช่น ชื่อ สกุล เบอร์โทร วันเกิด เพื่อรับรางวัล หรือการจัดเกมที่ทำให้รู้ข้อมูลส่วนบุคคล เช่น คุณเป็นใครในวันเกิด และควรต้องทำงานร่วมกับ สมาคมโฆษณาแห่งประเทศไทย สมาคมโฆษณาดิจิทัลประเทศ เพื่อแนะนำว่าควรหลีกเลี่ยงกิจกรรมประเภทที่เปิดเผยข้อมูลส่วนบุลคลต่อสาธารณะ เป็นต้น

นายอาทิตย์เสนอในตอนท้ายว่า เครื่องมือในการแก้ไขปัญหาควรคำนึงถึงองค์ประกอบดังนี้ ๑) ตลาด ผู้กำกับกิจการต้องดูแล ผู้บริโภคไม่สามารถทำให้ตัวเองปลอดภัยได้ด้วยตัวเอง แต่ต้องพึ่งพาผู้ให้บริการ หากสภาพการแข่งขันไม่ไปสู่ความปลอดภัยที่ดีขึ้นจะทำให้ผู้บริโภคอยู่ยากขึ้น ๒) พฤติกรรม มีพฤติกรรมที่ปลอดภัย ๓) เทคโนโลยี ให้ทำPrivacy by design ๔) การบังคับใช้กฎหมาย

สำหรับในช่วงการเสวนาเรื่อง “กฎหมาย PDPA กับมิติใหม่ของการจัดการปัญหา SCAM” เริ่มโดย **พล.ต.ต.นิเวศน์ อาภาวศิน** ผู้บังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี (ผบก.ตอท.) กล่าวถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ว่าเป็นไปเปิดโอกาสให้ภาครัฐสามารถดำเนินการต่าง ๆ ได้แต่จะต้องมีการออกประกาศรองรับด้วย สำหรับสาเหตุของข้อมูลที่รั่วไหลเกิดจาก ๑) มิจฉาชีพเจาะระบบนำข้อมูลไปขายในโลกออนไลน์ เว็บไซต์ใหญ่ที่สุดคือ Raidforums.com ซึ่งได้นำข้อมูลของโรงพยาบาลปราจีนบุรีไปขาย ประเทศไทยได้ดำเนินการและนำไปสู่การปิดเว็บไซต์นี้ได้ในที่สุด มีชาวโปรตุเกสอายุ ๒๑ ปี เป็นผู้ดำเนินการ ข้อมูลที่รั่วไหลเป็นหลักหมื่นล้านรายการทั่วโลก ๒) การหลอกล่อให้ผู้ใช้บริการกรอกข้อมูลส่วนบุคคล เช่น การส่งข้อความสั้นแจ้งว่า เป็นผู้โชคดีได้รับรางวัลให้กรอกข้อมูลส่วนบุคคล ๓. การฟิชชิ่ง (Phishing) โดยสร้างเว็บไซต์หลอกลวง ๔. การขายข้อมูลส่วนบุคคล ซึ่งมีความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

ทั้งนี้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีโทษทางอาญา การมีกฎหมายฉบับนี้จึงทำให้ผู้รับผิดชอบข้อมูลส่วนบุคคลต้องมีความระมัดระวังและมีกลไกในการรักษาข้อมูลส่วนบุคคลตามมาตรฐานสากล เนื่องจากมีโทษทางอาญาตามมาตรา ๗๙ หากฝ่าฝืนตามมาตรา ๒๗ วรรคหนึ่ง มาตรา ๒๘ อันเกี่ยวเนื่องกับข้อมูลส่วนบุคคลตามมาตรา ๒๖ มีโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท โดยผู้ที่มีความรับผิดชอบโดยตรงคือ ผู้ควบคุมข้อมูลส่วนบุคคล คือ บริษัทเอกชน ห้างร้าน อย่างไรก็ตามกฎหมายเอาผิดกับผู้ควบคุมข้อมูลส่วนบุคคล แต่สำหรับมิจฉาชีพเจาะระบบข้อมูล หรือ แฮกเกอร์ กฎหมายฉบับนี้ไม่สามารถเอาผิดได้ แต่จะเป็นพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

กรณีของบุคคลที่ยินยอมขายข้อมูลส่วนบุคคลเพื่อนำไปใช้ในการกระทำความผิด เช่น ‘บัญชีม้า’ คนยอมขายบัญชีส่วนบุคคลเพื่อนำไปใช้ในการกระทำความผิด แม้จับกุมได้ก็ยังไม่มีความผิดหากบัญชีดังกล่าวยังไม่ถูกนำไปใช้ในการกระทำความผิด การนำกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกฎหมายจากต่างประเทศมาใช้จึงต้องพิจารณาบริบทของประเทศไทย ต่างประเทศไม่ยินยอมขายข้อมูลส่วนบุคคลของตนเอง แต่ด้วยสภาพเศรษฐกิจทำให้คนไทยยินยอมขายข้อมูลส่วนบุคคลของตนเองด้วย

พล.ต.ต.นิเวศน์ เสนอว่า ประชาชนควรระมัดระวังการให้ข้อมูลส่วนบุคคลโดยมีสิ่งที่ต้องระมัดระวัง เช่น เมื่อไปงานอีเวนต์ต่าง ๆ และมีข้อเสนอให้กรอกข้อมูลส่วนบุคคล ขอให้ประชาชนอ่านว่าข้อมูลดังกล่าวเป็นการนำไปใช้ทำอะไรบ้างตามกฎหมาย และหากเป็นเรื่องไม่สำคัญอย่านำเลขหมายโทรศัพท์หลักของตนเองไปใช้ในการลงทะเบียนแต่ให้ใช้เลขหมายสำรองแทน และให้จับภาพหน้าจอเก็บไว้ทุกครั้งว่า ได้ให้ข้อมูลส่วนบุคคลไว้กับบริษัทนั้น ๆ ไว้ เพื่อหากมีปัญหาสามารถร้องเรียนคณะกรรมการคุ้มครองข้อมูลส่วน

บุคคลให้ตรวจสอบได้ และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลควรมีระบบออนไลน์ในการรับเรื่องร้องเรียนเพื่อรับทราบปัญหา เช่น ระบบรับแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ เปิดบริการ ๓ เดือน มีคนแจ้งความเดือนละหนึ่งหมื่นราย ความเสียหายหนึ่งพันห้าร้อยล้านบาทต่อเดือน หรือ ไม่ต่ำว่าสิบล้านบาทต่อวัน

สำหรับสาเหตุหลักและข้อเสนอในมุมมองของ พล.ต.ต.นิเวศน์ เห็นว่า

๑) ช่องทางในการติดต่อสื่อสาร เทคโนโลยีทำให้มิจฉาชีพสามารถปลอมเลขหมายโทรศัพท์ได้ ทำให้คนหลงเชื่อ ซึ่งอันตรายและเป็นปัญหาความมั่นคง หากเราไม่สามารถแยกแยะได้ว่า เลขหมายใดจริงหรือปลอม จึงต้องมีฐานข้อมูลเลขหมายโทรศัพท์ของผู้ให้บริการทั้ง ๔ ราย แยกเป็นเลขหมายที่ใช้บริการกับผู้ให้บริการ และเลขหมายที่อยู่กับสำนักงาน กสทช. ในกรณีที่พบเลขหมายที่นอกเหนือจากในฐานข้อมูลให้ตั้งข้อสังเกตว่า อาจเป็นเลขหมายปลอม และหากเป็นเลขหมายที่ไม่สามารถยืนยันตัวตนได้ก็ไม่ต้องแสดงเลขหมายบนหน้าจอ แทนการใส่เลขหมายบวก ฯลฯ

๒) กรณีบัญชีม้า มีการขายเลขที่บัญชีและให้คนร้ายใช้ในการโอนเงิน ซึ่งใช้เวลาเพียงไม่กี่นาทีในการโอนเงินของผู้เสียหาย ทำให้การติดตามช่วยเหลือทำได้ไม่ทัน และส่วนใหญ่เป็นมิจฉาชีพจากต่างประเทศ เช่น ชาวจีนในกัมพูชา จึงต้องใช้กลไกของสถาบันการเงินมาใช้ในการป้องกัน โดยเสนอให้ธนาคารแห่งประเทศไทยระงับเส้นทางการทำธุรกรรมออนไลน์ เช่น เมื่อตำรวจได้รับแจ้งบัญชีม้า ให้ธนาคารระงับเส้นทางธุรกรรมออนไลน์ทั้งหมดของบัญชีนั้น ๆ เช่นอาจเกี่ยวเนื่องกับ ๑๐๐ บัญชี ก็ให้ระงับไว้ก่อน เพราะมีพฤติการณ์ที่นำบัญชีไปใช้ในการกระทำผิดกฎหมาย แต่การดำเนินการดังกล่าวยังทำได้ยากเนื่องจากอาจมีปัญหาการละเมิดข้อมูลส่วนบุคคล

๓) เรื่องการประชาสัมพันธ์ ควรแนะนำให้ผู้บริโภคสามารถแยกแยะจริงกับปลอม ให้ได้ เช่น ลักษณะของเว็บไซต์ เพจที่เป็นของจริง สำหรับการโอนเงิน ที่เกิดจากการโอนเงินไปหาคนร้ายด้วยตนเอง นั้น ควรแนะนำให้ผู้บริโภคตรวจสอบโดยโทรกลับหาคนร้ายเพื่อตรวจสอบว่า ใช่ตัวจริงหรือไม่ และควรมีการส่งข้อความสั้นประชาสัมพันธ์แจ้งข้อมูลพื้นฐานนี้ให้ประชาชนได้ทราบว่าอย่าโอนเงินให้ใครถ้ายังยืนยันตัวตนผู้รับไม่ได้ หรือกรณีที่ไม่สามารถยืนยันตัวตนได้อาจมีเสียงแจ้งเตือนว่า เป็นเลขหมายต่างประเทศโปรดใช้ความระมัดระวัง เพื่อให้ผู้บริโภครับทราบ ส่วนคณะกรรมการข้อมูลส่วนบุคคลควรมีช่องทางให้ประชาชนได้แจ้งปัญหาด้วย

สำหรับ**นายสุทธิศักดิ์ ตันตะโยธิน** รองเลขาธิการ สำนักงาน กสทช. กล่าวถึงการดำเนินการของกสทช.ที่ผ่านมาว่า สำนักงาน กสทช. ได้เริ่มแก้ไขปัญหาตั้งแต่ “สแปม” (spam) และพัฒนามาเป็น “สแกม” (scam) จากข้อความสั้นรบกวนเป็นหลอกลวง สำนักงาน กสทช. ได้ออกมาตรการได้จัดระเบียบ sender name โดยให้มีการลงทะเบียนผู้ส่งข้อความสั้น รวมทั้ง URL จากนั้นมิจฉาชีพเปลี่ยนรูปแบบเป็นการโทรหลอกลวง เป็นแก๊งคอลเซ็นเตอร์ ซึ่งในกรณีทราฟฟิกการโทรเข้าที่มาจากต่างประเทศไม่มีการกำหนดเลขหมาย ต้นทาง (Non Calling Line Identification) ให้ดำเนินการเพิ่ม Prefix โดยใช้เครื่องหมาย “+

๖๙๗” นำหน้าเลขหมายที่บริษัทให้บริการแก่ผู้ใช้บริการ เพื่อให้ประชาชนทราบว่าเป็นการโทรเข้าจากต่างประเทศ กรณีที่ไม่สามารถใส่ Prefix ผู้รับใบอนุญาตจะต้องส่งทราฟฟิกประเภท Non Calling Line Identification ไปยังผู้ให้บริการโทรศัพท์ระหว่างประเทศ (IDD) เพื่อนำเข้าทราฟฟิกดังกล่าวไปยังผู้ใช้บริการ และมีการดำเนินการติดตามตรวจสอบทราฟฟิกการโทรเข้าจากต่างประเทศที่มีพฤติกรรมการใช้งานที่ผิดปกติ และมีแนวโน้มการใช้งานที่อาจเข้าข่ายเป็นการกระทำผิดกฎหมายและดำเนินการระงับทราฟฟิกการโทรดังกล่าว รวมถึงการให้ความรู้เพื่อให้ประชาชนสามารถป้องกันตัวเองได้ โดยการประชาสัมพันธ์ในรูปแบบอินโฟร์กราฟิก เพื่อเป็นการให้ความรู้และเป็น “Scam alert” ให้กับประชาชน

สำนักงาน กสทช. มีประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคลสิทธิในความเป็นส่วนตัวและเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม พ.ศ. ๒๕๔๙ และได้ปรับปรุงแล้วเพื่อนำเสนอ กสทช. ชุดใหม่ โดย จะนำเข้าที่ประชุมคณะอนุกรรมการคุ้มครองผู้บริโภคด้านกิจการโทรคมนาคม และนำไปรับฟังความคิดเห็นสาธารณะทั้งภาคประชาชน ภาควิชาการ หน่วยงานที่เกี่ยวข้อง เพื่อให้สอดคล้องกับ พ.ร.บ.ข้อมูลส่วนบุคคลฯ และจะได้ดำเนินการ “Scam Alert” อย่างต่อเนื่อง และนำลงไว้ในเว็บไซต์ให้เป็นปัจจุบันด้วย กรณีของข้อความสั้นหากพบว่า เป็น spam ผู้ให้บริการจะต้องระงับข้อความสั้นดังกล่าวภายใน ๓ ชั่วโมง และกรณีมีการขอลงทะเบียนเลขหมายมากกว่า ๕ เลขหมายต้องลงทะเบียนที่ศูนย์บริการของผู้ให้บริการเท่านั้น เพื่อป้องกันมิจฉาชีพลงทะเบียน

**รศ.ดร. ทศพล ทรรศนกุลพันธ์** กรรมการคุ้มครองข้อมูลส่วนบุคคล ได้ให้ความเห็นว่า มิจฉาชีพทราบข้อมูลของเหยื่อได้ ๓ วิธี คือ ๑) การสุ่มเดา ๒) การได้ข้อมูลส่วนบุคคลของเหยื่อ เช่น เหยื่อซื้อขายออนไลน์เป็นประจำ อาจได้ข้อมูลจากผู้ส่งสินค้าออนไลน์ จึงแอบอ้างเป็นผู้แทน ส่งสินค้า ๓) เหยื่อบางกลุ่มอาจเข้าไปเกี่ยวข้องกับการทำธุรกรรมสีเทาและมิจฉาชีพได้ข้อมูลมา จึงนำมาข่มขู่ กิจกรรมของผู้ใช้บริการอินเทอร์เน็ตที่ต้องเผชิญความเสี่ยงต่อการถูกล่อลวง โดยอาศัยแพลตฟอร์ม ได้แก่ แพลตฟอร์มเครือข่ายสังคมออนไลน์ทำให้ผู้ใช้งานสามารถพบเจอผู้คนที่รู้จัก หรือกลุ่มคนที่มีความคิด ความชอบคล้ายกัน เป็นการสร้างชุมชนในโลกออนไลน์ในลักษณะ Look at Me จึงมีข้อมูลส่วนบุคคลมาก เช่น เฟซบุ๊ก อินสตาแกรม และ แพลตฟอร์มในรูปแบบ Look at this คือ การให้ผู้ใช้งานเลือกที่จะเห็นเนื้อหาที่ตัวเองสนใจมากกว่าการเผยข้อมูลส่วนบุคคลให้ผู้อื่นล่วงรู้ เช่น ทวิตเตอร์ เป็นต้น

รศ.ดร.ทศพลมีข้อสังเกตต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ดังนี้ ๑) มาตรา ๑๙, ๒๑ และ ๒๒ กำหนดให้เก็บข้อมูลส่วนบุคคลให้น้อยที่สุดตามวัตถุประสงค์และตามความจำเป็น ๒) มาตรา ๒๐ สำหรับกรณีของกลุ่มผู้เยาว์ ผู้ไร้ความสามารถ มีขั้นตอนการขอรับความยินยอมจากบุคคลกลุ่มนี้หรือไม่ซึ่งต้องระมัดระวังเพราะเริ่มมีการสร้างแพลตฟอร์มเป็นการเฉพาะสำหรับบุคคลกลุ่มนี้แล้ว ซึ่งถือเป็นความเสี่ยงที่จะเกิดขึ้นได้ ๓) แอปพลิเคชันบางประเภทสามารถดูดข้อมูลส่วนบุคคลแบบอัตโนมัติ ขณะที่ตามมาตรา ๒๕ ระบุว่า ห้ามไม่ให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง ซึ่งสามารถป้องกันได้ด้วยการออกแบบระบบของผู้ให้บริการ ๔) มาตรา

๒๖ ห้ามไม่ให้เก็บข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ พฤติกรรมทางเพศ ศาสนาหรือปรัชญา ขณะที่บัตรประจำตัวประชาชนของคนไทยระบุข้อมูลศาสนาไว้ชัดเจนด้านหน้าบัตร ทำอย่างไรที่จะเก็บข้อมูลแต่ไม่ต้องแสดงได้หรือไม่

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ใช้บังคับได้กับผู้ประกอบการที่ตั้งอยู่ในประเทศไทยรวมถึงผู้ประกอบการที่เสนอบริการเข้ามาในประเทศไทยด้วย พ.ร.บ.ฉบับนี้มีประโยชน์ในการคุ้มครองผู้บริโภคหลายมาตรา เช่น มาตรา ๒๓, ๓๐, ๓๑, ๓๓, ๓๔, ๓๖, ๓๗ และ ๗๙ รวมถึงกรณีที่มีการรั่วไหลของข้อมูลส่วนบุคคล คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะตั้งคณะกรรมการผู้เชี่ยวชาญและอนุกรรมการย่อยเฉพาะด้านในแต่ละประเภท เช่น ด้านจริยธรรมเกี่ยวกับผู้ป่วย โดยมีพ.ร.บ.ฉบับนี้เป็นหลักการรองรับ และเห็นว่าควรมีการพิจารณาว่า ข้อมูลคืออะไรในกฎหมายไทย ข้อมูลถือเป็นทรัพย์หรือไม่ หากเป็นทรัพย์ กรณีได้ข้อมูลไปอย่างไม่ถูกต้องถือว่ามีความผิดได้

**ดร. รอม หิรัญพฤกษ์** ผู้ทรงคุณวุฒิด้านเทคโนโลยีสารสนเทศ ได้ให้ความเห็นว่า ภัยทางเทคโนโลยีที่เกิดขึ้นในประเทศไทย เป็นเหตุการณ์เกิดมาแล้วในต่างประเทศ เป็นปรากฏการณ์ที่เกิดซ้ำในบ้านเรา ๓๐ ปีที่แล้วตนเองพยายามให้คนไทยเข้าถึงข้อมูลข่าวสาร แต่เมื่อทุกคนสามารถเข้าถึงข้อมูลข่าวสารกลับไม่สามารถแยกแยะจริงกับเท็จ และเต็มไปด้วยเฟกนิวส์ ยกตัวอย่าง กรณีของบริษัท Cambridge Analytica ซึ่งเป็นบริษัทวิเคราะห์ข้อมูลทราบรายละเอียดของข้อมูลของประชาชน ในการเลือกตั้งทำให้สามารถวางแผนนโยบายกับประชาชนได้ ขณะที่ประชาชนไม่ได้บันทึกไว้ว่า เขาได้โฆษณา หรือสัญญาไว้อย่างไร ปัญหาจึงไม่ได้จำกัดเฉพาะสแกม เช่น เหตุการณ์ของประเทศเกาหลี chat room หลอกเด็กผู้หญิง จากนั้นแบลกเมล์ และต้องกลายเป็นทาส โดยมีคนนับพันจ่ายเงินเพื่อได้เข้าไปดูภาพเหล่านั้น แม้จะถูกจับได้แต่ภาพเหล่านั้นก็ได้กระจายไปยังที่ต่างๆ ไม่ใช่เฉพาะเกาหลี ประเทศไทยจึงต้องติดตามสถานการณ์สภาพปัญหาในต่างประเทศ เพราะไม่นานปัญหาดังกล่าวจะเกิดขึ้นกับประเทศไทย มิจฉาชีพแสวงหาจุดอ่อนช่องโหว่ของซอฟแวร์หรือฮาร์ดแวร์ของระบบอินเทอร์เน็ต มีตลาดอาวุธอีกประเภทหนึ่งที่ซ่อนอยู่แต่ประเทศไทยไม่เคยทราบและเครื่องมือเหล่านี้ไปอยู่ในมือโจร และมาสแกมข้อมูลของคนไทย

**นายประวิทย์ ลี่สถาพรวงศา** ประธานอนุกรรมการคุ้มครองผู้บริโภคด้านกิจการโทรคมนาคม กล่าวว่า สแกมเป็นอาชญากรรมทางเทคโนโลยี สิ่งที่มิจฉาชีพใช้คือข้อมูล ซึ่งกฎหมายฉบับนี้จะสามารถช่วยแก้ไขปัญหาได้ โดยเฉพาะช่วยจัดการกับข้อมูลขนาดใหญ่ที่เอกชนถืออยู่ได้ แต่ถ้าเป็นข้อมูลที่มิจฉาชีพสร้างขึ้นเองจะแก้ไขได้ยาก มิจฉาชีพใช้ข้อมูล ใช้เทคโนโลยี และการสร้างเรื่องหลอกประชาชน เหตุผลที่มีการระบาดหนักเนื่องจากต้นทุนทางเทคโนโลยีต่ำลง เช่น สหรัฐอเมริกาพบว่า ประชาชน ๑ ใน ๓ ถูกหลอก โดย ๑ ใน ๕ ของประชาชนถูกหลอกซ้ำ การระมัดระวังไม่ได้แก้ไขปัญหาได้ทั้งหมดเพราะแม้คนที่เคยโดนหลอกแล้ว ยังถูกหลอกซ้ำได้อีก มูลค่าความเสียหาย ๒๙ พันล้านเหรียญในหนึ่งปี กลวิธีในการหลอกลวงมาได้หลายรูปแบบ ทำนายว่าอนาคตเทคโนโลยีจะทำให้มิจฉาชีพสามารถวิดีโอคอลได้เหมือนตำรวจจริง เพราะฉะนั้นการสร้างความรู้ความเข้าใจเป็นเรื่องดีแต่ไม่ได้แก้ไขปัญหาได้ทั้งหมด นายประวิทย์เห็นว่า พ.รบ.ข้อมูลส่วนบุคคลฯ ช่วยสร้างความตระหนักรู้กับประชาชนในการดูแลข้อมูลส่วนบุคคล ขณะที่ภาครัฐได้แนะนำวิธีการระมัดระวังการถูกหลอก

จากมิจฉาชีพ และการดำเนินการภายหลังจากการถูกหลอก ซึ่งต้องยอมรับว่าทุกอาชีพสามารถถูกหลอกได้ แม้แต่หมอ อัยการ ผู้พิพากษา เพราะความแนบเนียนของมิจฉาชีพ ดังนั้นจึงไม่ควรอคติกับผู้เสียหายที่ถูกหลอก เช่น เป็นเพราะความโลภ หรือความโง่ เพื่อให้ได้ข้อเท็จจริงเกี่ยวกับวิธีการของมิจฉาชีพ

ที่ผ่านมาได้มีการแก้ไขปัญหาที่มีขึ้นแล้ว ได้แก่ Call numbering Call blocking แต่ก็ยังมีจุดอ่อนที่ไม่สามารถแก้ไขปัญหาได้ทั้งหมด การจัดหมวดหมู่ของเบอร์โทรเพื่อทราบว่าเป็นเลขหมายของมิจฉาชีพ อย่างไรก็ตามปัจจุบันก็มีการแปลงเลขหมายและยิงเข้ามาจากต่างประเทศได้ ซึ่งหากเป็นจริงเชื่อว่ามีหนอนบ่อนไส้จากผู้ให้บริการในประเทศไทยที่รับจ้างแปลงเลขหมายให้กับมิจฉาชีพ ดังนั้นในเรื่องนี้นักเทคนิคต้องช่วยในการคิดวิธีการในการแก้ไข เช่น ประเทศอินเดีย อยู่ระหว่างดำเนินการ คอลเดลิเวอร์ลิ่ง (call delivering) เพื่อยืนยันว่า เลขหมายใดเป็นเลขหมายจริง หากไม่ตรงถือเป็นเลขหมายปลอมทั้งหมด หรืออาจติดคำเตือนเป็นเสียง กรณีที่เป็นเลขหมายจากต่างประเทศ เพื่อให้ผู้รับสายได้ทราบ ประเทศนิวซีแลนด์สนับสนุนให้ภาคอุตสาหกรรมโทรคมนาคมและผู้บริโภครวมตัวกันและทำระบบรายงานไปผู้รับใบอนุญาตเพื่อปิดกั้นเลขหมายมิจฉาชีพทั้งฝั่งผู้ส่งและผู้รับเลขหมาย ออสเตรเลียมีองค์กร ACCC ดูแลปัญหาโดยตรง

นายประวิทย์กล่าวว่า กฎหมายฉบับนี้สามารถป้องกันข้อมูลส่วนบุคคลขนาดใหญ่ได้ แต่ไม่สามารถป้องกันได้ทั้งหมด และเป็นปัญหาเทคนิคที่ควรมีการระดมความคิดทางเทคนิคในการป้องกัน เช่น การใช้ Label call การใช้ระบบการ Block ที่มีความถูกต้องแม่นยำ การใช้ Who’s call ที่มีความถูกต้องและไม่ทำให้สุจริตชนต้องเดือดร้อน เพราะเลขหมายโดนรวมกลุ่มอยู่ในแก๊งมิจฉาชีพด้วย รวมถึงการให้ความรู้กับผู้บริโภคซึ่งต้องไม่ใช่ความรู้ชุดเดียวที่สามารถใช้ได้ตลอดไป แต่ต้องมีการปรับปรุงให้เท่าทันกับสถานการณ์

สำหรับการรักษาข้อมูลของผู้ให้บริการโทรศัพท์เคลื่อนที่ ต้องการความเป็นมืออาชีพ พบว่ามีการรั่วไหลข้อมูลจากจุดที่มีการลงทะเบียนใช้บริการ ผู้ควบคุมข้อมูลนอกจากโดนปรับต้องมีการติดตามด้วย หากพบว่า ยังกระทำผิดซ้ำควรมีการเพิกถอนการอนุญาตทางวิชาชีพ และต้องดูแลทางเทคนิคทางซอฟแวร์และฮาร์ดแวร์ ยกตัวอย่างคดีรั่วข้อมูลที่ไม่สามารถทราบได้ว่า ผู้กระทำผิดได้ขายข้อมูลให้กับใครบ้าง เพราะขาดผู้เชี่ยวชาญที่สามารถตรวจสอบได้ กฎหมายอย่างเดียวจึงไม่สามารถแก้ไขปัญหาได้ทั้งหมดแต่ต้องมีองค์ประกอบอื่นร่วมด้วย

นายประวิทย์ กล่าวว่าที่ผ่านมา กสทช. ไม่เคยขอข้อมูลส่วนบุคคลของผู้บริโภคทั้งข้อมูลบัตรประจำตัวประชาชน หรือชื่อผู้ใช้บริการ แต่เป็นผู้ให้บริการเก็บข้อมูลดังกล่าว ทั้งนี้ในยุคปัญหา ๓ จังหวัดชายแดนใต้ จึงขอให้ลงทะเบียนซิมเพื่อป้องกันปัญหาอาชญกรรมและเพื่อความมั่นคง

**ตัวแทนบริษัท ดีแทค ไตรเน็ต จำกัด** ให้ความเห็นว่าบริษัทฯ ไม่สามารถบล็อกข้อความสั้นหรือโทรหลอกลวง ได้ทั้งหมด บริการที่เพิ่มเติมของบริษัทฯ เป็นเครื่องมือของ third party กรณีที่ได้ผู้ใช้บริการได้รับลิงก์สีเทาจะสามารถบล็อกลิงก์นั้นให้ได้ทันที บริษัทฯ ป้องกันข้อมูลส่วนบุคคล โดยต้องเป็นผู้มีอำนาจตามกฎหมายจึงขอข้อมูลส่วนบุคคลได้ ซึ่งได้แก่ สำนักงานตำรวจแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ธนาคารแห่งประเทศไทย และ กสทช. และควรสร้างแพลตฟอร์มกลางของประเทศเชื่อมโยงทุกหน่วยงานเพื่อ

แก้ไขปัญหานี้ มีการทำรายงาน และการติดตามปัญหาตลอดเวลา  กสทช. สามารถประสานผู้รับใบอนุญาต ผ่านสมาคมโทรคมนาคมแห่งประเทศไทย เพื่อยับยั้งการโอนเงินได้

.....