การประกันภัยความรับผิดทางไซเบอร์ : ศึกษาความคุ้มครองความรับผิดที่เกิดจากการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

CYBER LIABILITY INSURANCE : STUDY ON COVERAGE FOR LIABILITY FROM BREACH OF PERSONAL DATA PROTECTION ACT 2019

จีระศักดิ์ เสมมีสุข

Jerasak Semmesuk

ANZIIF (Assoc) CIP

ทนายความ นิติศาสตรมหาบัณฑิต สาขากฎหมายเอกชน

คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ : Jerasak.semmesuk@gmail.com

Attorney-at-law Master of Laws Program in Private law,

Faculty of Law, Thammasat University : Jerasak.semmesuk@gmail.com

Received : May 12, 2021

Revised : August 08, 2021

Accepted : August 19, 2021

บทคัดย่อ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหลักเกณฑ์ และกำกับการเก็บรวมรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล หากบริหารจัดการข้อมูลส่วนบุคคลโดยฝ่าฝืนต่อบทบัญญัติของกฎหมายและก่อความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล และ/หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลย่อมมีความผิดทางแพ่ง โทษทางอาญา และโทษทางปกครอง และเกิดค่าใช้จ่ายในการต่อสู้คดีและเพื่อตอบสนองเหตุเบื้องต้นตามที่กฎหมายกำหนด เช่น เพื่อการบอกกล่าวการเกิดเหตุละเมิดแก่เจ้าของข้อมูลส่วนบุคคล และการบอกกล่าวการเกิดเหตุละเมิดสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งค่าใช้จ่ายเพื่อการเฝ้าระวัง การเยียวยาแก้ไขการละเมิดข้อมูลส่วนบุคคล ย่อมเกิดเป็นความเสียหายทางการเงินแก่ผู้ประกอบการ และหากไม่ได้รับการเยียวยาก็จะกระทบสิทธิของเจ้าของข้อมูลส่วนบุคคลก็คือประชาชน

ดังนั้น การประกันภัยทางไซเบอร์ โดยเฉพาะส่วนของประกันภัยความรับผิด จึงเป็นเครื่องมือในการบริหารความเสี่ยงต่อความเสียหายทางการเงินขององค์กร ผู้เขียนศึกษาวิเคราะห์ความคุ้มครองของกรมธรรม์ประกันภัยความรับผิดทางไซเบอร์ที่มีอยู่ในประเทศไทยว่าครอบคลุมความรับผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่เพียงใด รวมทั้งมีข้อเสนอแนะบางประการเพื่อให้การนำเอาการประกันภัยทางไซเบอร์ใช้เกิดประสิทธิผลมากขึ้น ได้แก่ การนำหลักการบริหารความเสี่ยงทั่วไปมาใช้กับการประเมินความเสี่ยงด้านไซเบอร์ขององค์กร การสนับสนุนให้มีการศึกษาความเป็นไปได้ในการนำเอาประกันภัยความรับผิดทางไซเบอร์มาเป็นประกันภัยภาคบังคับ และการจัดทำกรมธรรม์ประกันภัยความรับผิดทางไซเบอร์มาตรฐานภาษาไทย

คำสำคัญ

ประกันภัยความรับผิดทางไซเบอร์ ประกันภัยค้ำจุน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ABSTRACT

The Personal Data Protection Act, B.E. 2562 (2019) provides rules and regulates the collection, storage, use, processing, and disclosure of personal data. With this being enforced, in the case where the personal data controller and/or personal data processor operates in relation to the management of personal data in a way that violates the provisions of the relevant legislation, relatively causing harm to the data subject, the personal data controller and/or personal data processor shall be held liable for civil, criminal and administrative sanctions which may involve expenses in the support of litigation, and for complying with the fundamental legal requirements such as for proper notification in an event of a data breach to the data subject, and notification in an event of a data breach to the Personal Data Protection Committee ("PDPC"). Furthermore, the incurred costs and expenses on monitoring, remedial measures for personal data breach restitution would result in financial damage to the business operator. On the other hand, without such remedy, the data subject's right, which means the right of the public as a whole, would be definitely affected.

Therefore, cyber insurance, especially the section of liability insurance is a mechanism intended for the risk management of financial loss for an entity. In this research, the author carries out an analysis on the adequacy and the scope of application of the available liability coverage of cyber-liability insurance policy in connection with the Personal Data Protection Act, B.E. 2562 (2019) in Thailand, including giving certain recommendations regarding more efficient application of cyber-insurance; for example, the integration of the general risk management principles into the cyber-risk assessment in an organization, the support of feasibility study on the implementation of mandatory cyber-liability insurance as well as the preparation of the standard cyber-liability insurance policy in the Thai language version.

Keywords

Cyber liability insurance, liability insurance, Personal Data Protection Act 2019

1. บทนำ

โลกในยุคดิจิทัล เทคโนโลยีพัฒนาไปอย่างมาก ชีวิตมนุษย์เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์อยู่ตลอดเวลา เช่น การใช้โทรศัพท์มือถือ สื่อสังคมออนไลน์ ธุรกรรมทางการเงิน การซื้อสินค้าต่าง ๆ การแลกเปลี่ยนข้อมูลโดยเฉพาะข้อมูลส่วนบุคคลจึงเป็นไปโดยง่าย ทั้งที่เจ้าของข้อมูลส่วนบุคคลอาจรู้ตัวหรือไม่รู้ตัวว่าได้ให้ข้อมูลส่วนบุคคล ความสะดวกสบายจากเทคโนโลยีเหล่านี้จึงเป็นดาบสองคม ผู้ประกอบการบางรายอาจได้ข้อมูลส่วนบุคคลมาโดยไม่ได้รับความยินยอม หรือนำข้อมูลส่วนบุคคลที่ได้รับมาไปใช้ในทางที่ผิดไปจากวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ไว้ รวมทั้งหากการบริหารจัดการและรักษาความปลอดภัยข้อมูลไม่ดีพอ มิจฉาชีพอาจได้ข้อมูลส่วนบุคคลเหล่านี้ไปหาประโยชน์ในทางทุจริต

ตัวอย่างกรณีศึกษา การละเมิดข้อมูลส่วนบุคคลในต่างประเทศที่เป็นข่าวโด่งดังระดับโลก เช่น กรณีสื่อสังคมออนไลน์ Facebook ถูกคณะกรรมาธิการการค้าแห่งรัฐบาลกลาง (Federal Trade Commission – FTC) ฟ้องฐานละเมิดสิทธิความเป็นส่วนตัวของผู้ใช้งานจำนวน 8 ข้อหา รวมถึงข้อหาว่าหลอกลวงผู้ใช้งานว่าสามารถตั้งค่าความเป็นส่วนตัวให้เฉพาะผู้ที่เป็นเพื่อนสามารถเข้าถึง แต่ไม่ได้เปิดเผยให้ผู้ใช้ทราบอย่างเพียงพอว่าการตั้งค่าอื่นอนุญาตให้แชร์ข้อมูลเดียวกันกับนักพัฒนาแอปที่เพื่อน ๆ ใช้ ตัวอย่างเช่น ผู้ใช้งานนายเอ กำหนดให้ผู้ใช้งานนางสาวบี ซึ่งเป็นเพื่อนของตน เข้าถึงข้อมูลส่วนบุคคลของนายเอได้ แต่กลายเป็นว่าผู้พัฒนาแอพลิเคชั่นที่ นางสาวบี ใช้งาน ก็สามารถเข้าถึงข้อมูลส่วนตัวของนายเอได้ด้วย โดยท้ายที่สุด Facebook ตกลงยอมชำระค่าปรับทางแพ่ง (civil penalty) จำนวน 5 พันล้านเหรียญสหรัฐอเมริกา และต้องปรับปรุงนโยบายด้านข้อมูลส่วนบุคคล[1]

สิทธิในข้อมูลส่วนบุคคลในประเทศไทยไม่ใช่เรื่องแปลกใหม่ เพราะเป็นสิทธิที่ได้รับความคุ้มครองไว้ในรัฐธรรมนูญ ทั้งในฉบับก่อน คือ ฉบับปี พ.ศ. 2550 ในมาตรา 35 วรรคสาม และตามรัฐธรรมนูญฉบับปัจจุบัน คือ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 หมวด 3 สิทธิเสรีภาพของปวงชนชาวไทย มาตรา 32 บัญญัติว่า

“บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ”[2]

ประเทศไทยประสบปัญหาการล่วงละเมิดสิทธิในข้อมูลส่วนบุคคลเช่นเดียวกัน “เนื่องจากมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวกและรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม”[3] ประเทศไทยจึงได้ประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีสาระสำคัญอยู่ที่การกำกับเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล (data subject) รวมทั้งบทกำหนดโทษที่

---

[1] Lesley Fair, ‘FTC’s $5 billion Facebook settlement: Record-breaking and history-making’ (Federal Trade Commission, 2019) <https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-recordbreaking-history> accessed 16th Nov 2020.

[2] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 32.

[3] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เหตุผลในการประกาศใช้.

เกี่ยวข้อง[4] มีบทบัญญัติเกี่ยวกับการร้องเรียน โดยให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง[5] อีกทั้งกำหนดให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล (data controller) หรือผู้ประมวลผลข้อมูลส่วนบุคคล (data processor)[6]

สิ่งผู้เขียนเห็นว่ามีความสำคัญ และต้องการนำเสนอในบทความฉบับนี้ก็คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ หากฝ่าฝืนจะมีบทลงโทษ โดยมีการกำหนดโทษไว้ถึงสามประเภท ได้แก่ ในหมวดที่ 6 ความรับผิดทางแพ่ง หมวดที่ 7 ส่วนที่หนึ่ง โทษอาญา ส่วนที่สอง โทษทางปกครอง โดยในส่วนความรับผิดทางแพ่งได้กำหนดให้มีค่าเสียหายเชิงลงโทษ[7] และต้องชดใช้ค่าสินไหมทดแทนรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย[8] และในหมวดที่ 7 ส่วนที่สอง โทษทางปกครอง ซึ่งการกระทำผิดบางฐานกำหนดค่าปรับทางปกครองสูงถึงห้าล้านบาท[9]

ผู้ประกอบการที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจเผชิญความเสี่ยงต่อความรับผิดตามกฎหมาย ทำให้เกิดความเสียหายทางการเงินหากมีการดำเนินงานที่บกพร่องและต้องรับผิด ดังนั้นผู้ประกอบการอาจบรรเทาความเสียหายที่อาจเกิดขึ้นอันเป็นผลมาจากความรับผิดจากการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมทั้งค่าใช้จ่ายต่าง ๆ เช่น ค่าใช้จ่ายในการต่อสู้คดีหรือดำเนินการทางกฎหมายโดยการทำประกันภัยความรับผิดทางไซเบอร์ (cyber liability insurance) แต่เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังเป็นสิ่งที่มีความแปลกใหม่ในประเทศไทย การประกันภัยความรับผิดทางไซเบอร์ในหมวดที่เกี่ยวข้องกับการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ก็เป็นสิ่งที่แปลกใหม่เช่นกัน ผู้เขียนจึงขอนำเสนอการวิเคราะห์ความคุ้มครองของประกันภัยความรับผิดทางไซเบอร์ที่มีจำหน่ายอยู่ในประเทศไทย ทั้งนี้ ปัจจุบันกรมธรรม์ประกันภัยชนิดนี้ยังไม่มีแบบมาตรฐาน มีเพียงแบบที่ได้รับอนุญาตจากสำนักงาน คปภ. เพื่อใช้เฉพาะรายสำหรับบริษัทผู้ขออนุญาตแบบ ผู้เขียนจึงวิเคราะห์โดยอ้างอิงจากกรมธรรม์ประกันภัยการบริหารความเสี่ยงทางไซเบอร์ขององค์กร แบบที่ 1 (Cyber Enterprise Risk Management Insurance Policy Version 1) ฉบับของบริษัท ซับบ์สามัคคีประกันภัย จำกัด (มหาชน) กรมธรรม์ประกันภัยนี้เป็นฉบับที่ได้รับอนุมัติแบบจาก คปภ. และใช้ในภูมิภาคเอเชียแปซิฟิก

บทความฉบับนี้ ผู้เขียนมุ่งศึกษาเฉพาะส่วนความคุ้มครองความรับผิดตามกฎหมายต่อบุคคลภายนอก อันเกิดจากการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่กระทำโดยผู้เอาประกันภัยต่อข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ หรือที่เรียกว่าเป็นความรับผิดทางไซเบอร์ โดยไม่รวมถึงการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอื่น และผู้เขียนจะให้ความสำคัญกับการกระทำผิดประเภทการละเมิดข้อมูลส่วนบุคคลเพราะเป็นฐานความผิดที่มีโทษสูง และตั้งประเด็นปัญหาเพื่อการศึกษาว่า ความคุ้มครองตามกรมธรรม์ประกันภัยความรับผิดทางไซเบอร์ที่มีอยู่ในปัจจุบันเพียงพอต่อการคุ้มครองผู้เอาประกันภัยเพื่อการชดใช้ค่าเสียหายอันเกิดจากการไม่ปฏิบัติ

---

[4] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 3 (1).

[5] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 3 (2).

[6] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 5.

[7] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 78.

[8] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 77 วรรคสอง.

[9] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 84 และ มาตรา 87.

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ หรือมีความเสียหายหรือความรับผิดประเภทใดที่กฎหมายบัญญัติให้ต้องรับผิดแต่กรมธรรม์ไม่ได้ให้ความคุ้มครอง และเสนอแนะแนวทางเพื่อให้ผู้เอาประกันภัยได้รับความคุ้มครองที่สอดคล้องกับความรับผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. สรุปสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ผู้เขียนสรุปสาระสำคัญเบื้องต้นของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อทำความเข้าใจขอบเขตการบังคับใช้ของพระราชบัญญัตินี้ ความหมายของข้อมูลส่วนบุคคล การไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และการละเมิดข้อมูลส่วนบุคคล บุคคลผู้มีหน้าที่ตามพระราชบัญญัตินี้ และบทลงโทษ

2.1 ขอบเขตการบังคับใช้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นบทบัญญัติทั่วไปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (comprehensive law)[10] มีผลบังคับใช้เป็นการทั่วไป เว้นแต่มีบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอื่นใดโดยเฉพาะแล้ว[11] อย่างไรก็ตาม หากเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ก็ยังคงต้องบังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติที่มีอยู่เฉพาะแล้วนั้นหรือไม่ก็ตาม[12] และครอบคลุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในประเทศไทย ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือประเทศไทยก็ตาม[13]

โดยสรุป พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บังคับใช้กับการประกอบธุรกิจไม่ว่าประเภทใดหรือการดำเนินกิจกรรมใด ๆ ที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยยกเว้นกิจการบางประเภทที่ไม่อยู่ภายใต้พระราชบัญญัตินี้ เช่น กิจการด้านความมั่นคงของหน่วยงานรัฐ เป็นต้น[14]

2.2 ความหมายของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่จะไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรมหรือเสียชีวิตไปแล้ว[15] ตัวอย่างเช่น ชื่อนามสกุล ที่อยู่ ภูมิลำเนา หมายเลขบัตรประชาชน หมายเลขพาสปอร์ต อาชีพ สถานที่ทำงาน หมายเลขโทรศัพท์ เป็นต้น

ข้อมูลส่วนบุคคลบางประเภท เป็นข้อมูลส่วนบุคคลอันมีลักษณะต้องห้าม[16] หรือ เป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (sensitive data) เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา

---

[10] บรรเจิด ภาคาพันธุ์, 'ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในธุรกิจประกันชีวิต' (2563) 1 วารสารบัณฑิตศึกษานิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 120, 127.

[11] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 3.

[12] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 3 (1).

[13] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 5 วรรคหนึ่ง.

[14] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 4.

[15] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 6 วรรคหนึ่ง.

[16] สำนักงานเลขาธิการสภาผู้แทนราษฎร, เอกสารประกอบการพิจารณา ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..., อ.พ. 6/2556 สมัยสามัญทั่วไป (ตุลาคม 2556) 59.

พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด ซึ่งกฎหมายให้ความสำคัญมากกว่าข้อมูลส่วนบุคคลทั่วไป โดยห้ามทำการเก็บรวบรวมข้อมูลเหล่านี้ หากไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล[17]

2.3 ผู้มีหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดบุคคลที่เกี่ยวข้องกับการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลไว้สองประเภท ได้แก่ ผู้ควบคุมข้อมูลส่วนบุคคล และ ผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล[18] ตัวอย่างเช่น ผู้ประกอบธุรกิจโรงแรมต้องได้ข้อมูลส่วนบุคคลของผู้ที่จะเข้าพัก เช่น ชื่อ นามสกุล ที่อยู่ ภูมิลำเนา หมายเลขบัตรประชาชน หมายเลขโทรศัพท์ เป็นต้น ผู้ประกอบธุรกิจโรงแรมจึงเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามความหมายของพระราชบัญญัตินี้

ผู้ประมวลผลข้อมูลส่วนบุคคล หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล[19] ตามตัวอย่างข้างต้น ผู้ประกอบธุรกิจโรงแรมที่ได้เก็บรวมรวมข้อมูลส่วนบุคคลของบรรดาผู้มาพัก ส่งต่อไปให้แก่บริษัทที่ปรึกษาด้านการตลาด เพื่อให้วิเคราะห์ข้อมูลว่ากลุ่มลูกค้าช่วงอายุเท่าใดมีกำลังซื้อสูง และกลุ่มนี้มีความสนใจกิจกรรมแบบใด เพื่อผู้ประกอบธุรกิจโรงแรมจะนำมาทำการตลาดกับลูกค้ากลุ่มดังกล่าวเช่นนี้ บริษัทที่ปรึกษาด้านการตลาดซึ่งไม่ได้เป็นผู้เก็บรวมรวมข้อมูลส่วนบุคคล ย่อมเป็นผู้ประมวลผลข้อมูลส่วนบุคคลตามความหมายของพระราชบัญญัตินี้

2.4 การคุ้มครองข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลจะเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ก่อนหรือในขณะที่จะเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้[20]

การให้ความยินยอมจากเจ้าของข้อมูลส่วนบุคคลจึงเป็นหลักการสำคัญในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รูปแบบของการให้ความยินยอมนั้น ต้องเป็นความยินยอมโดยชัดแจ้งเป็นหนังสือ หรืออาจเป็นการผ่านระบบอิเล็กทรอนิกส์ก็ได้[21] โดยการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว[22]

---

[17] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 26 วรรคหนึ่ง.

[18] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 6 วรรคสอง.

[19] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 6 วรรคสาม.

[20] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 19 วรรคหนึ่ง.

[21] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 19 วรรคสอง.

[22] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 19 วรรคสาม.

พระราชบัญญัตินี้อนุญาตให้เก็บรวบรวมข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอมบางกรณี ตัวอย่างเช่น การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา ตามมาตรา 24 (3)[23] หรือ การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ไม่ว่าด้วยเหตุใดก็ตาม ตามมาตรา 26 (1) เป็นต้น[24]

2.5 การไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และการละเมิดข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ควบคุมการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามบทบัญญัติ เช่น การนำข้อมูลที่ได้เก็บรวบรวมไว้ไปใช้ผิดจากวัตถุประสงค์ที่ได้รับความยินยอมโดยการนำไปหาประโยชน์ทางการตลาด หรือ การนำไปขายเพื่อประโยชน์ทางธุรกิจ หรือเกิดการละเมิดข้อมูลส่วนบุคคล ย่อมเป็นเหตุให้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลเกิดความรับผิด

บทความนี้ผู้เขียนให้ความสำคัญกับการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ในส่วนของการละเมิดข้อมูลส่วนบุคคล เพราะเป็นความผิดที่มีโทษสูงและก่อความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลได้มาก หากเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้อธิบายความหมายของการละเมิดข้อมูลส่วนบุคคลเอาไว้โดยเฉพาะ จึงต้องศึกษาจากคำอธิบายที่มีอยู่ในกฎหมายต่างประเทศ โดยผู้เขียนยกตัวอย่างจากคำนิยามในกฎหมาย General Date Protection Regulation (GDPR) ของสหภาพยุโรป มาตรา 4 (12)

‘การละเมิดข้อมูลส่วนบุคคล หมายถึง การละเมิดความปลอดภัยที่นำไปสู่การทำลาย สูญเสีย เปลี่ยนแปลง เปิดเผยโดยไม่ได้รับอนุญาต หรือการเข้าถึงข้อมูลส่วนบุคคลที่ถูกส่ง เก็บรักษา หรือประมวลผล โดยอุบัติเหตุหรือไม่ชอบด้วยกฎหมาย’[25]

ซึ่งผู้เขียนเห็นว่าสมควรนำมาศึกษาเทียบเคียง เพราะกฎหมาย GDPR ของสหภาพยุโรปเป็นกฎหมายที่มีความเข้มงวดด้านความเป็นส่วนตัวและมีความปลอดภัยมากที่สุดของโลก[26]

การละเมิดข้อมูลส่วนบุคคล อาจเกิดจากการกระทำของบุคคลภายนอก เช่น การขโมยอัตลักษณ์เพื่อการนำไปสวมรอย (identity theft) การลักขโมยอุปกรณ์คอมพิวเตอร์ที่มีข้อมูลส่วนบุคคล เป็นต้น รวมทั้งอาจเกิดจากการกระทำหรือ ละเว้นกระทำการของผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลก็ได้ เช่น การส่งข้อมูลส่วนบุคคลผิดตัวผู้รับ การเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต[27]

---

[23] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 24 (3).

[24] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 26 (1).

[25] General Data Protection Regulation (European Union) art. 4 (12).

[26] ‘General Data Protection Regulation (GDPR)’ (European Union) <https://gdpr.eu/tag/gdpr/> accessed 7th Apr 2021.

[27] ญาดา กาศยปนันท์, ‘เจาะลึกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และแนวปฏิบัติที่ถูกต้องสำหรับธุรกิจเช่าซื้อและลีสซิ่ง’ (โครงการอบรมวิชาการด้านธุรกิจเช่าซื้อ, สมาคมธุรกิจเช่าซื้อไทย ,โรงแรมสยามแอทสยาม, 10 พฤศจิกายน 2563) 26.

นอกจากนี้ บทบัญญัติในพระราชบัญญัตินี้ยังกำหนดหน้าที่บางประการแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล เช่น หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล อันเป็นการกำหนดมาตรการเชิงป้องกัน[28] และหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการบันทึกรายการเพื่อการตรวจสอบ[29] เป็นต้น หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล[30] หากมีการฝ่าฝืนบทบัญญัติจนเป็นเหตุให้เจ้าของข้อมูลได้รับความเสียหาย ก็ถือเป็นการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับผิด[31]

มาตรการเชิงป้องกันที่ผู้เขียนเห็นว่ามีความน่าสนใจมาตรการหนึ่ง คือ การกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า[32] ซึ่งผู้เขียนเห็นว่ามีความน่าสนใจ เพราะการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ ย่อมเกิดค่าใช้จ่ายแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

2.6 ประเภทของบทลงโทษ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติบทลงโทษการไม่ปฏิบัติตามบทบัญญัติโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลไว้สามประเภท ได้แก่ ความรับผิดทางแพ่ง โทษทางอาญา และโทษทางปกครอง

2.6.1 ความรับผิดทางแพ่ง

หากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องรับผิดชดใช้ค่าสินไหมทดแทนเพื่อความเสียหายอันเกิดจากเหตุนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่าความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากความผิดของข้อมูลส่วนบุคคลนั้นเอง[33] จากบทบัญญัตินี้ผู้เขียนเห็นว่าเป็นการนำหลักความรับผิดโดยเคร่งครัด (strict liability) มาใช้ โดยค่าสินไหมทดแทนนี้ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย[34]

ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจ่ายค่าสินไหมทดแทนเพื่อการลงโทษ (punitive damages) เพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่ศาลเห็นสมควร แต่ไม่

---

[28] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 37.

[29] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 39.

[30] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 40.

[31] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 77.

[32] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 37 (4).

[33] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 77 (1) และ (2).

[34] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 77 วรรคสอง.

เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง ทั้งนี้ โดยคำนึงถึงพฤติการณ์ต่าง ๆ เช่น ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ สถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล การที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความเสียหายที่เกิดขึ้น หรือการที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย[35]

2.6.2 โทษอาญา

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติให้การฝ่าฝืนกฎหมายฉบับนี้มีโทษทางอาญา ตัวอย่างเช่น กรณีผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (ฝ่าฝืนมาตรา 27 วรรคหนึ่ง) กรณีบุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนมาจากการเปิดเผยโดยความยินยอมจะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น (ฝ่าฝืนมาตรา 27 วรรคสอง) โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ[36] และถ้าการกระทำดังกล่าวข้างต้นนี้มีเจตนาพิเศษ คือ เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น จะมีโทษหนักขึ้น คือต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาทหรือทั้งจำทั้งปรับ[37] เป็นต้น โดยมีข้อสังเกตว่าความผิดในกลุ่มนี้เป็นความผิดอันยอมความได้[38]

รวมทั้งกรณีที่ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ[39] โดยความผิดตามมาตรานี้มีข้อสังเกตว่าไม่ใช่ความผิดอันยอมความได้

2.6.3 โทษทางปกครอง

โทษทางปกครองเป็นมาตรการลงโทษอีกลักษณะที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดไว้นอกเหนือไปจากการชดใช้ค่าสินไหมทดแทนทางแพ่ง

โทษทางปกครอง คือ สภาพบังคับ (sanction) สำหรับการกระทำที่ฝ่าฝืนข้อห้ามตามกฎหมาย หรือไม่ปฏิบัติตามบทบัญญัติที่กฎหมายบัญญัติให้ต้องกระทำ และข้อห้ามมิให้กระทำการ หรือบังคับให้กระทำการนั้น ยังมิใช่เรื่องร้ายแรงถึงระดับผิดศีลธรรม หรือความสงบเรียบร้อยของสังคม หรือความมั่นคงของรัฐ หรือกระทบต่อสิ่งแวดล้อม ผู้กระทำที่ฝ่าฝืนกฎหมายที่มีโทษทางปกครอง มิใช่อาชญากร แต่เป็นการกระทำที่ผิดกฎระเบียบเล็กน้อยในสังคมเท่านั้น[40]

---

[35] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 78 วรรคหนึ่ง.

[36] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 79 วรรคหนึ่ง.

[37] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 79 วรรคสอง.

[38] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 79 วรรคสาม.

[39] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 80 วรรคหนึ่ง.

[40] กมลชัย รัตนสกาววงศ์, ‘ทฤษฎีและแนวคิดเกี่ยวกับการกำหนดโทษทางปกครองในการตรากฎหมาย’ (โครงการสัมมนา เรื่อง หลักเกณฑ์ในการกำหนดโทษทางปกครองในการตรากฎหมาย, สำนักงานคณะกรรมการกฤษฎีกา, 2560), 1 <http://web.krisdika.go.th /data/outsite data/article77/file77/c06.pdf.> สืบค้นเมื่อ 12 มกราคม 2564.

การฝ่าฝืนบทบัญญัติที่มีโทษทางปกครอง ตัวอย่างเช่น ผู้ควบคุมข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนโดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล (ฝ่าฝืนมาตรา 26 วรรคหนึ่ง) หรือ ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมโดยไม่เป็นไปตามกฎหมาย (ฝ่าฝืนมาตรา 26 วรรคสาม) หรือผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (ฝ่าฝืนมาตรา 27 วรรคหนึ่ง) หรือ ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนไปยังต่างประเทศโดยไม่เป็นไปตามกฎหมาย (ฝ่าฝืนมาตรา 28) ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท[41] หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดส่งหรือโอนข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนหรือประวัติอาชญากรรม โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท[42] เป็นต้น

เนื่องจากโทษปรับทางปกครองไม่ใช่การกระทำผิดทางอาญา ดังนั้น หากจำเลยไม่ชำระค่าปรับทางปกครองรัฐจะต้องดำเนินการบังคับชำระค่าปรับในลักษณะหนี้ทางแพ่งตามประมวลกฎหมายวิธีพิจารณาความแพ่ง[43]

3. วิเคราะห์ความคุ้มครองของการประกันภัยความรับผิดทางไซเบอร์

ความคุ้มครองของการประกันภัยความรับผิดทางไซเบอร์จำกัดอยู่เพียงความรับผิดที่เกิดจากความเสี่ยงภัยทางอิเล็กทรอนิกส์ ความผิดอันเกิดจากการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่เกิดในลักษณะอื่น ๆ ที่ไม่เป็นอิเล็กทรอนิกส์ จะไม่อยู่ในขอบเขตของกรมธรรม์ประกันภัยประเภทนี้ และเพื่อตอบประเด็นปัญหาว่า ความคุ้มครองตามกรมธรรม์ประกันภัยความรับผิดทางไซเบอร์ที่มีอยู่ในปัจจุบันเพียงพอต่อการคุ้มครองผู้เอาประกันภัย เพื่อการชดใช้ค่าเสียหายอันเกิดจากการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ หรือมีความเสียหายหรือความรับผิดประเภทใดที่กฎหมายบัญญัติให้ต้องรับผิดแต่กรมธรรม์ไม่ได้ให้ความคุ้มครอง ผู้เขียนแบ่งเนื้อหาออกเป็น 2 หัวข้อ ได้แก่ ความคุ้มครองของกรมธรรม์ประกันภัยความรับผิดทางไซเบอร์ และ ข้อยกเว้นความคุ้มครองของกรมธรรม์ประกันภัยความรับผิดทางไซเบอร์

3.1 ความคุ้มครองของกรมธรรม์ประกันภัยความรับผิดทางไซเบอร์

กรมธรรม์ประกันภัยการบริหารความเสี่ยงทางไซเบอร์ขององค์กร แบบที่ 1 ของบริษัท ซับบ์สามัคคีประกันภัย จำกัด (มหาชน) ที่ได้รับอนุมัติแบบจากสำนักงาน คปภ. ให้ใช้เป็นการทั่วไปสำหรับบริษัท เป็นกรมธรรม์ประกันภัยฉบับภาษาอังกฤษ แต่เนื่องจากผู้รับประกันภัยแต่ละบริษัทมักจะไม่เปิดเผยเนื้อความในกรมธรรม์ประกันภัยที่ไม่ใช่แบบมาตรฐานออกสู่สาธารณะ ทำให้ผู้เขียนไม่สามารถหาแหล่งอ้างอิงที่เปิดเผยเป็นสาธารณะในประเทศ ท่านผู้ที่มีความสนใจสามารถศึกษาเนื้อหาของกรมธรรม์ประกันภัยซึ่งมีเนื้อความครบถ้วนได้ที่ www.steel-line.com.au ซึ่งเป็นเว็บไซต์ของประเทศออสเตรเลีย ผู้เขียนเลือกวิเคราะห์จากกรมธรรม์ฉบับนี้เพราะเป็นกรมธรรม์ประกันภัยการบริหารความเสี่ยงทางไซเบอร์ขององค์กร แบบที่ 1 แบบเดียวกับที่ใช้ในกลุ่มซับบ์ฯ ประเทศไทย

สาเหตุประการสำคัญที่ต้องมีการประกันภัยไซเบอร์นั้นก็เพราะ ความเสี่ยงภัยทางไซเบอร์นั้นเริ่มมีจำนวนมากขึ้นตามเทคโนโลยีที่พัฒนา แต่การประกันภัยทรัพย์สิน ประกันภัยความรับผิดต่อบุคคลภายนอก รวมทั้งประกันภัยความรับผิดทางวิชาชีพโดยทั่วไปนั้น ยกเว้นความเสียหายหรือความรับผิดอันเกิดจากไซเบอร์ จึงเกิดเป็นช่องว่างความคุ้มครอง

[41] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 84.

[42] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 87.

[43] กมลชัย รัตนสกาววงศ์ (เชิงอรรถ 40) 3.

ความคุ้มครองส่วนที่ผู้เขียนจะวิเคราะห์ คือ การประกันภัยความรับผิดทางไซเบอร์ต่อบุคคลภายนอก (third party insurance) ซึ่งให้ความคุ้มครองความรับผิดตามกฎหมายของผู้เอาประกันภัยที่มีต่อบุคคลภายนอกซึ่งไม่ใช่คู่สัญญาประกันภัย ได้แก่ ความคุ้มครองความรับผิดต่อความเป็นส่วนตัว (privacy liability) ความคุ้มครองความรับผิดจากความปลอดภัยของเครือข่าย (network security liability) ซึ่งเป็นหมวดที่เกี่ยวข้องกับความคุ้มครองการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และผู้เขียนได้แยกความคุ้มครองค่าใช้จ่ายที่เกี่ยวข้องการเรียกร้องค่าสินไหมทดแทนออกมาวิเคราะห์เป็นอีกหัวข้อหนึ่ง

3.1.1 ความคุ้มครองความรับผิดต่อความเป็นส่วนตัว

ความคุ้มครองส่วนนี้จะชดใช้ค่าเสียหายและค่าใช้จ่ายในการเรียกร้องค่าสินไหมทดแทนเพื่อความเป็นส่วนตัว (privacy claims expenses) ที่เกิดจากการเรียกร้องค่าสินไหมทดแทนเพื่อความเป็นส่วนตัว (privacy claim) ที่เกี่ยวกับเหตุการณ์การละเมิดความเป็นส่วนตัว (privacy wrongful act) ที่ได้กระทำต่อผู้เอาประกันภัยเป็นครั้งแรกในระหว่างระยะเวลาเอาประกันภัย และได้รายงานต่อผู้รับประกันภัยตามเงื่อนไขของกรมธรรม์

การเรียกร้องค่าสินไหมทดแทนเพื่อความเป็นส่วนตัว ตามกรมธรรม์ประกันภัย หมายถึง การบอกกล่าวเรียกร้องเป็นลายลักษณ์อักษร การฟ้องร้องดำเนินคดีแพ่ง การดำเนินการยื่นข้อพิพาทต่ออนุญาโตตุลาการ การดำเนินการทางปกครอง ที่ได้กระทำต่อผู้เอาประกันภัยเพื่อเรียกค่าเสียหายเป็นตัวเงิน หรือเพื่อให้มีมาตรการบรรเทาความเสียหายที่ไม่เป็นตัวเงิน อันมีสาเหตุมาจากการละเมิดความเป็นส่วนตัว[44] ไม่ได้จำกัดเฉพาะการถูกดำเนินคดีตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การละเมิดความเป็นส่วนตัว ตามกรมธรรม์ประกันภัย หมายถึง ความผิดพลาด การแถลงที่คลาดเคลื่อน การแถลงที่ทำให้เกิดความเข้าใจผิด ซึ่งหมายถึง การที่ผู้เอาประกันภัยใช้ถ้อยคำหรือข้อความใด ๆ อันผิดพลาด คลาดเคลื่อน หรือกำกวมจนทำให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยความเข้าใจผิด โดยการละเมิดความเป็นส่วนตัว รวมไปถึงการกระทำ การละเว้นการกระทำ ความประมาท การฝ่าฝืนต่อหน้าที่ หรือเป็นความเสียหายส่วนบุคคล (personal injury) อื่น ๆ เช่น การให้ข้อมูลส่วนบุคคลที่ผิดพลาดจนเป็นเหตุให้เจ้าของข้อมูลส่วนบุคคลถูกถูกจับกุม กักขัง เป็นต้น ทั้งนี้ อาจจะเป็นเหตุการณ์ที่เกิดขึ้นจริง หรือเป็นเพียงข้อกล่าวหา หรืออาจเกิดจากการพยายามกระทำโดยผู้เอาประกันภัยก็ได้ อันเป็นผลให้เกิดความผิดพลาดซึ่งผู้เอาประกันภัยต้องรับผิด หรืออาจต้องร่วมรับผิดตามกฎหมาย เนื่องจากตนมีหน้าที่การบริหารจัดการ จัดเก็บ ทำลาย หรือควบคุมข้อมูลส่วนบุคคล หรือ การฝ่าฝืนนโยบายความเป็นส่วนตัว (privacy policy) ของผู้เอาประกันภัยเอง[45] ตัวอย่างเช่น ในนโยบายความเป็นส่วนตัวของผู้เอาประกันภัยแถลงว่าการจัดเก็บข้อมูลส่วนบุคคลจะนำไปทำอะไรบ้าง แต่กลับนำไปทำอย่างอื่นนอกเหนือจากนโยบายที่ได้แถลงไว้ เป็นต้น ข้อสำคัญคือ การละเมิดความเป็นส่วนตัว ต้องเกิดขึ้นจากการกระทำโดยไม่จงใจโดยผู้เอาประกันภัย

ผู้เขียนมีข้อสังเกตว่า การละเมิดความเป็นส่วนตัว ในความหมายของกรมธรรม์ประกันภัยจะมีขอบเขตกว้างกว่าคำว่าการละเมิดข้อมูลส่วนบุคคลตามความหมายของ GDPR เพราะองค์ประกอบสำคัญของการละเมิดข้อมูลส่วนบุคคล คือ การละเมิดความปลอดภัยที่นำไปสู่การทำลาย สูญเสีย เปลี่ยนแปลง เปิดเผยโดย หรือการเข้าถึงข้อมูลส่วนบุคคลโดย

[44] Chubb Insurance Australia Limited, 'Cyber Enterprise Risk Management Insurance Policy' (insuring clauses 1.1 A) <https://www.steel-line.com.au/wpcontent/uploads/2020/04/cyber_certificate_of_currency.pdf> accessed on 19th Jan 2021.

[45] ibid insuring clauses 1.1 C.

ไม่ชอบด้วยกฎหมาย แต่ในความหมายของกรมธรรม์ประกันภัย เพียงผู้เอาประกันภัยใช้ถ้อยคำหรือข้อความใด ๆ อันผิดพลาด คลาดเคลื่อน หรือกำกวมจนทำให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยความเข้าใจผิดก็เพียงพอจะเป็นการละเมิดความเป็นส่วนตัวแล้ว

ตัวอย่างความคุ้มครองการละเมิดความเป็นส่วนตัว เช่น พนักงานฝ่ายบุคคลของบริษัทแห่งหนึ่งได้แนบเอกสารอิเล็กทรอนิกส์ผิดไปให้แก่ผู้สมัครงานรายหนึ่ง ในเอกสารนั้นมีข้อมูลส่วนบุคคลของผู้สมัครงานคนอื่น ๆ เช่น ชื่อนามสกุล วันเดือนปีเกิด เลขที่บัตรประชาชน ที่อยู่ เป็นต้น ตามตัวอย่างบริษัทแห่งนี้อยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล กระทำบกพร่องหรือผิดพลาดในการบริหารจัดการข้อมูลส่วนบุคคล ซึ่งผู้เขียนเห็นว่าเป็นกรณีนี้เป็นการเปิดเผยข้อมูลส่วนบุคคลโดยฝ่าฝืนมาตรา 27 วรรคหนึ่ง เพราะผู้สมัครงานแต่ละคนนั้นยินยอมเปิดเผยข้อมูลส่วนบุคคลของตนแก่บริษัทที่ตนสมัครงาน แต่ไม่ได้ให้ความยินยอมแก่บริษัทในการนำไปเปิดเผยแก่บุคคลอื่น และไม่เข้าข้อยกเว้นที่จะเปิดเผยได้โดยไม่ต้องได้รับความยินยอม จึงเป็นการไม่ปฏิบัติตามบทบัญญัติกฎหมาย แม้ไม่ถึงขนาดเป็นการกระทำที่มีโทษทางอาญาเพราะไม่มีเจตนาและกฎหมายก็ไม่ได้บัญญัติให้รับผิดทางอาญากรณีประมาท แต่ถ้าข้อมูลส่วนบุคคลที่ถูกส่งไปผิดนั้น ทำให้เจ้าของข้อมูลรายใดเสียหาย ก็อาจถูกเรียกร้องค่าเสียหายทางแพ่งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77 และหากข้อมูลส่วนบุคคลที่ถูกส่งผิดไปมีส่วนที่เป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน ก็อาจต้องถูกดำเนินการทางปกครองตามมาตรา 84 ซึ่งมีโทษปรับสูงสุดถึง 5 ล้านบาทด้วย นอกจากนั้น เหตุการณ์ตามตัวอย่างนี้ยังเข้าลักษณะของการละเมิดข้อมูลส่วนบุคคลที่ทำให้บริษัทแห่งนี้อยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และอาจจะต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลด้วยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 34 (4)

ตามตัวอย่างนี้ จำนวนที่กรมธรรม์ประกันภัยจะคุ้มครอง ได้แก่ ค่าใช้จ่ายในการต่อสู้คดีแพ่งและคดีปกครองเกี่ยวกับการละเมิดความเป็นส่วนตัว จำนวนค่าปรับทางปกครองอันเกี่ยวกับการละเมิดความเป็นส่วนตัว ค่าเสียหายที่ต้องชดใช้ให้แก่เจ้าของข้อมูลส่วนบุคคลรวมถึงค่าใช้จ่ายที่เกิดขึ้นแก่เจ้าของข้อมูลส่วนบุคคล ที่เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการชดใช้ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77 วรรคสอง และค่าใช้จ่ายในการบอกกล่าวการละเมิดข้อมูลส่วนบุคคล ซึ่งจะได้มีการอธิบายต่อไปในส่วนของค่าใช้จ่ายในการตอบสนองต่อเหตุการณ์

3.1.2 ความคุ้มครองความรับผิดจากความปลอดภัยของเครือข่าย

ความคุ้มครองส่วนนี้จะชดใช้ค่าเสียหายและค่าใช้จ่ายในการเรียกร้องค่าสินไหมทดแทนเพื่อความปลอดภัยของเครือข่าย (network security claims expenses) ที่เกิดจากการเรียกร้องค่าสินไหมทดแทนเพื่อความปลอดภัยของเครือข่าย (network security claim) ที่ได้กระทำขึ้นเป็นครั้งแรกในระหว่างระยะเวลาเอาประกันภัยและได้รายงานต่อผู้รับประกันภัยตามเงื่อนไขของกรมธรรม์ประกันภัยเกี่ยวกับเหตุการณ์การละเมิดความปลอดภัยของเครือข่าย (network security wrongful act)

เช่นเดียวกับความคุ้มครองการเรียกร้องค่าสินไหมทดแทนเพื่อความเป็นส่วนตัว ในชั้นแรกจะต้องมีการเรียกร้องค่าสินไหมทดแทนเพื่อความปลอดภัยของเครือข่ายเกิดอันเกิดจากการละเมิดความปลอดภัยของเครือข่ายขึ้นก่อน การละเมิดความปลอดภัยของเครือข่าย หมายถึง ความผิดพลาด การแถลงที่คลาดเคลื่อน การแถลงที่ทำให้เกิดความเข้าใจผิด การกระทำ การละเว้นการกระทำ ความประมาท การฝ่าฝืนต่อหน้าที่ หรือความเสียหายส่วนบุคคล ทั้งที่อาจจะเกิดขึ้นจริง หรือถูกกล่าวหา หรือได้พยายามกระทำโดยผู้เอาประกันภัย เป็นผลให้เกิดความผิดพลาดต่อความปลอดภัยของเครือข่าย รวมถึงความผิดพลาดในการยับยั้ง การจัดให้มี การป้องกันหรือตรวจจับการกระทำความผิดทางคอมพิวเตอร์ใด

ๆ อันได้แก่ มัลแวร์ (malware) หรือ การจารกรรมข้อมูล (hacking) หรือ การโจมตีเพื่อให้เกิดการปฏิเสธการให้บริการ (denial of services attacks) หรือ การเข้าใช้งานหรือเข้าถึงโดยไม่ได้รับอนุญาต (unauthorized use or access)[46]

กรมธรรม์ประกันภัยส่วนนี้ให้ความคุ้มครองความรับผิดตามกฎหมายอันเกิดจากความบกพร่องในความปลอดภัยของเครือข่ายของผู้เอาประกันภัย ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77 ได้บัญญัติให้ผู้เอาประกันภัยในฐานะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับผิดโดยเคร่งครัดหากความบกพร่องนั้นก่อความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล

ผู้เขียนมีข้อสังเกตว่า ความคุ้มครองส่วนนี้มีเพื่อความรับผิดของผู้เอาประกันภัยที่กฎหมายกำหนดให้ต้องรับผิด แม้สาเหตุจะเกิดจากการกระทำของบุคคลอื่น เช่น แฮกเกอร์ แต่ทั้งนี้ ก็ต้องมีความบกพร่องหรือความประมาทของผู้เอาประกันภัย เป็นผลให้เกิดความผิดพลาดต่อความปลอดภัยของเครือข่าย หากระบบของผู้เอาประกันภัยเหมาะสม เป็นไปตามมาตรฐาน และมีการตรวจสอบอยู่เสมอแล้ว ผู้เอาประกันภัยก็ไม่มีความรับผิดและกรมธรรม์ประกันภัยก็จะไม่คุ้มครองชดใช้ค่าเสียหาย แต่ผู้เอาประกันภัยอาจได้รับความคุ้มครองในส่วนอื่น เช่น ค่าใช้จ่ายในการต่อสู้คดี

ตัวอย่าง กรณีแฮกเกอร์ได้เจาะเข้าสู่เครือข่ายของโรงพยาบาลแห่งหนึ่ง ซึ่งมีระบบรักษาความปลอดภัยทางไซเบอร์ที่ไม่เพียงพอ ไม่ได้มาตรฐาน ทำให้แฮกเกอร์สามารถเข้าถึงข้อมูลส่วนบุคคลในบัญชีของผู้ป่วย ข้อมูลส่วนบุคคลเช่น ชื่อนามสกุล วันเดือนปีเกิด ที่อยู่ อีเมล เลขบัตรประชาชน เลขที่บัญชี เลขที่บัตรเครดิต ได้รั่วไหล ตามตัวอย่างนี้ นอกจากเกิดการละเมิดความเป็นส่วนตัวแล้ว ก็ยังเกิดการละเมิดความปลอดภัยของเครือข่ายเกิดขึ้นด้วย ซึ่งเป็นหน้าที่ของผู้ควบคุมข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) ในการจัดให้มีระบบรักษาความปลอดภัยแก่ข้อมูลส่วนบุคคลที่มีความเหมาะสมและเพียงพอต่อการปกป้องข้อมูลส่วนบุคคล ตามตัวอย่างนี้ จำนวนที่กรมธรรม์ประกันภัยจะคุ้มครอง ได้แก่ ค่าใช้จ่ายในการต่อสู้คดีแพ่งและคดีปกครอง จำนวนค่าปรับทางปกครองจากความบกพร่องในการจัดให้มีระบบรักษาความปลอดภัยแก่ข้อมูลส่วนบุคคล ค่าเสียหายที่ต้องชดใช้ให้แก่เจ้าของข้อมูลส่วนบุคคลรวมทั้งค่าใช้จ่ายที่เกิดขึ้นแก่เจ้าของข้อมูลส่วนบุคคล ที่เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการชดใช้ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77 วรรคสอง และค่าใช้จ่ายในการต่อสู้คดีแพ่งที่เกิดแก่ผู้เอาประกันภัย และค่าใช้จ่ายในการบอกกล่าวการละเมิดข้อมูลส่วนบุคคล

3.1.3 ค่าใช้จ่ายที่เกี่ยวข้องการเรียกร้องค่าสินไหมทดแทน

เมื่อเกิดเหตุการณ์หรือถูกกล่าวหาว่ามีการละเมิดความเป็นส่วนตัว หรือ การละเมิดความปลอดภัยของเครือข่ายขึ้น นอกจากค่าเสียหายที่ต้องชดใช้ให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นผู้เสียหาย ย่อมเกิดค่าใช้จ่ายบางประการแก่ผู้เอาประกันภัยเพื่อการตรวจสอบเหตุการณ์หรือต่อสู้คดี

ค่าใช้จ่ายที่กรมธรรม์ประกันภัยคุ้มครองเกี่ยวกับการเรียกร้องค่าสินไหมทดแทนเพื่อความเป็นส่วนตัว และ การเรียกร้องค่าสินไหมทดแทนเพื่อความปลอดภัยของเครือข่ายมีลักษณะที่คล้ายกัน ผู้เขียนจึงนำมาวิเคราะห์รวมไว้ในส่วนเดียวกัน โดยมีสามประเภท ได้แก่

1. ค่าใช้จ่ายตามที่จำเป็นเพื่อเป็นค่าทนายความ ค่าตอบแทนพยานผู้เชี่ยวชาญ และค่าใช้จ่ายอื่น ๆ ที่เกี่ยวข้อง ค่าใช้จ่ายสองประเภทแรกค่อนข้างชัดเจนในตัวเอง แต่ค่าใช้จ่ายอื่น ๆ นั้น เมื่อกรมธรรม์ประกันภัยไม่ได้จำกัดความไว้ คู่สัญญาอาจจะต้องมาพิจารณาร่วมกันว่าเกี่ยวข้องกับการต่อสู้คดีหรือการตรวจสอบการเกิดเหตุการณ์หรือไม่ เช่น ค่าวิชาชีพนักบัญชี ค่าจ้างนักคอมพิวเตอร์ เป็นต้น จึงอาจเกิดข้อโต้แย้งกันในภายหลัง กรมธรรม์ประกันภัยจึงกำหนด

[46] ibid insuring clauses 1.2 C.

ไว้ว่าบรรดาค่าใช้จ่ายเหล่านี้ต้องเกิดขึ้นโดยฝ่ายผู้รับประกันภัยเป็นผู้ตัดสินใจก่อให้เกิดขึ้นเอง หรือผู้เอาประกันภัยอาจก่อให้เกิดขึ้นโดยได้รับความยินยอมจากผู้รับประกันภัยล่วงหน้าก่อน[47]

2. ค่าใช้จ่ายเพื่อเป็นค่าธรรมเนียมการจัดเตรียมหลักทรัพย์เพื่อเป็นประกันในชั้นอุทธรณ์ (appeal bond) หรือ หลักทรัพย์เพื่อเป็นประกันแทนการอายัดทรัพย์ (attachment bond) หรือ หลักประกันอื่นในลักษณะเดียวกัน ข้อนี้หมายถึง ผู้รับประกันภัยจะคุ้มครองค่าใช้จ่ายในการจัดเตรียมหลักทรัพย์เท่านั้น แต่ไม่ได้มีหน้าที่ต้องเป็นผู้จัดเตรียมหรือจัดหาหลักทรัพย์เหล่านี้[48]

3. ค่าใช้จ่ายในการตอบสนองต่อเหตุการณ์ (incident respond expenses) หมายถึง ค่าใช้จ่ายที่ผู้เอาประกันภัยก่อให้เกิดขึ้นหรือค่าใช้จ่ายที่ผู้เอาประกันภัยผูกพันตามกฎหมายต้องชำระเพื่อเป็นค่าใช้จ่ายต่อไปนี้[49]

ก. เพื่อการว่าจ้างผู้เชี่ยวชาญด้านการตรวจสอบระบบคอมพิวเตอร์ (computer forensics firm) ในการตรวจสอบหาสาเหตุและขอบเขตความบกพร่องของระบบความปลอดภัยของเครือข่ายของผู้เอาประกันภัยหรือของบุคคลที่ผู้เอาประกันภัยอาจจะต้องร่วมรับผิด เพื่อให้การบริหารจัดการ จัดเก็บ ทำลายหรือควบคุมข้อมูลส่วนบุคคล

ข. เพื่อให้เป็นไปตามระเบียบว่าด้วยความเป็นส่วนตัว (privacy regulation) รวมถึงการบอกกล่าวแก่เจ้าของข้อมูลส่วนบุคคลตามข้อกำหนดข้างต้น คำว่าระเบียบในที่นี้ ผู้เขียนตีความว่าน่าจะหมายถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และบรรดากฎกระทรวงหรือประกาศต่าง ๆ ที่เป็นกฎหมายลำดับรอง ซึ่งอาจจะมีออกมาในอนาคต โดยข้อนี้ตรงกับค่าใช้จ่ายที่จะเกิดขึ้นเพื่อแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 37 (4)

ค. เพื่อว่าจ้างที่ปรึกษากฎหมายในการเข้าชี้แจงต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และดำเนินการใด ๆ ให้เป็นไปตามข้อกำหนดว่าด้วยความเป็นส่วนตัว และการส่งมอบข้อมูลตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรียกตรวจสอบเกี่ยวกับการละเมิดข้อกำหนดความเป็นส่วนตัว และค่าใช้จ่ายเพื่อการประเมินผลกระทบ และการเข้าสู่กระบวนการสืบพยาน

ง. ค่าใช้จ่ายประเภทที่ต้องได้รับความยินยอมจากผู้รับประกันภัยก่อนการก่อให้เกิดขึ้น เช่น ค่าใช้จ่ายในการให้คำบอกกล่าวเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบให้เจ้าของข้อมูลส่วนบุคคลทราบโดยสมัครใจ ค่าใช้จ่ายเพื่อว่าจ้างผู้ให้บริการส่งคำบอกกล่าว เช่น ศูนย์บริการข้อมูล (call center) ค่าใช้จ่ายเพื่อว่าจ้างสำนักงานบริหารวิกฤตการณ์ (crisis management firm) เป็นต้น

3.2 ข้อยกเว้นความคุ้มครอง

กรมธรรม์ประกันภัยการบริหารความเสี่ยงทางไซเบอร์ขององค์กร แบบที่ 1 มีข้อยกเว้นทั่วไปที่ใช้บังคับกับความคุ้มครองทุกหมวดอยู่ 16 ข้อ ผู้เขียนขอยกเฉพาะบางข้อที่เห็นว่ามีความสำคัญเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคลขึ้นมาวิเคราะห์

3.2.1 การกระทำโดยจงใจ[50]

---

[47] ibid insuring clauses 1.1 B i, 1.2 B i.

[48] ibid insuring clauses 1.1 B ii, 1.2 B ii.

[49] ibid insuring clauses 1.1 B iii, 1.2 B iii, general definitions 3.17.

[50] ibid general exclusions 4.1.

กรมธรรม์ประกันภัยยกเว้นความคุ้มครองสำหรับการเรียกร้องค่าสินไหมทดแทนอันเป็นผลโดยตรงหรือโดยทางอ้อม หรือเกี่ยวข้องกับจากกระทำโดยจงใจ หรือรู้อยู่ว่าจะเป็นการฝ่าฝืนหน้าที่หรือผิดต่อกฎหมาย การกระทำผิดทางอาญาหรือมีเจตนาทุจริต รวมทั้งการหาประโยชน์ส่วนตัวโดยมิชอบ ทั้งโดยตัวผู้เอาประกันภัยเองหรืออนุญาตให้บุคคลอื่นกระทำ ทั้งนี้ ข้อยกเว้นนี้จะมีผลเมื่อมีคำพิพากษาของศาลถึงที่สุด หรือผู้เอาประกันภัยได้รับผิดเป็นลายลักษณ์อักษร ข้อยกเว้นนี้สอดคล้องกับความคุ้มครองการละเมิดความเป็นส่วนตัว ที่จะคุ้มครองเฉพาะการละเมิดที่เกิดโดยไม่จงใจ

3.2.2 การบาดเจ็บแก่ร่างกายและความเสียหายต่อทรัพย์สิน[51]

กรมธรรม์ประกันภัยนี้มุ่งคุ้มครองความเสียหายทางการเงินอันเกิดจากความรับผิดทางไซเบอร์ ดังนั้นจึงไม่คุ้มครองการบาดเจ็บแก่ร่างกายของบุคคลภายนอก คำว่าการบาดเจ็บแก่กายนี้ รวมถึงการบาดเจ็บหรือความเสียหายต่อจิตใจด้วย เช่น ความเครียด ความตกใจ ความทุกข์ทรมานใจ

อย่างไรก็ตาม มีข้อยกเว้นในกรณีที่การบาดเจ็บหรือเสียหายต่อจิตใจนี้เกิดจากการการละเมิดความเป็นส่วนตัว ก็จะได้รับความคุ้มครอง

สำหรับความเสียหายต่อทรัพย์สิน กรมธรรม์ประกันภัยจะยกเว้นความคุ้มครองความเสียหายทางกายภาพต่อทรัพย์ รวมถึงการสูญเสียการใช้ประโยชน์ (Loss of use) เว้นแต่เป็นการสูญเสียการใช้ประโยชน์ การสูญเสีย การถูกทำลายแก่ตัวข้อมูล ซึ่งอาจได้รับความคุ้มครองหากมีการระบุไว้ชัดแจ้ง

3.2.3 การกระทำละเมิดเกี่ยวกับการจ้างแรงงาน[52]

กรมธรรม์ประกันภัยยกเว้นความคุ้มครองสำหรับการเรียกร้องค่าสินไหมทดแทนที่เกี่ยวข้องกับการกระทำละเมิดที่เกี่ยวข้องกับการเลือกปฏิบัติ (discrimination) การล้อเลียน (humiliation) การข่มขู่คุกคาม (harassment) การกระทำที่มิชอบ (misconduct) ซึ่งเกี่ยวข้องกับการเลือกปฏิบัติ และการละเมิดเกี่ยวกับการปฏิบัติด้านแรงงาน (wrongful employment practices) อย่างไรก็ตาม หากเป็นกรณีการสูญเสียข้อมูลส่วนบุคคลจากการละเมิดความเป็นส่วนตัวและการละเมิดความปลอดภัยของเครือข่าย ที่ทำให้ลูกจ้างเกิดความตึงเครียดทางจิตใจ (emotional distress) กรณีนี้จะไม่ตกภายใต้ข้อยกเว้นและยังคงได้รับความคุ้มครอง

3.2.4 การละเมิดทรัพย์สินทางปัญญา[53]

กรมธรรม์ประกันภัยยกเว้นความคุ้มครองสำหรับการเรียกร้องค่าสินไหมทดแทนที่เกี่ยวข้องกับการละเมิดทรัพย์สินทางปัญญา เว้นแต่การกระทำนั้นจะเป็นการละเมิดความเป็นส่วนตัว

3.2.5 การเก็บข้อมูลส่วนบุคคลโดยมิชอบ[54]

กรมธรรม์ประกันภัยยกเว้นความคุ้มครองสำหรับการเรียกร้องค่าสินไหมทดแทนที่เกี่ยวข้องกับการเก็บข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม โดยลักลอบ หรือโดยมิชอบ รวมทั้งการไม่บอกกล่าวให้เจ้าของข้อมูลทราบถึงการเก็บข้อมูลส่วนบุคคล แต่อย่างไรก็ตามข้อยกเว้นนี้ไม่ใช้กับการไม่จงใจกระทำผิดข้อกำหนดเกี่ยวกับความเป็นส่วนตัว หรือการไม่จงใจเก็บข้อมูลส่วนบุคคลโดยมิชอบ

---

[51] ibid general exclusions 4.2.

[52] ibid general exclusions 4.5.

[53] ibid general exclusions 4.12.

[54] ibid general exclusions 4.13.

4. บทสรุปและข้อเสนอแนะ

ผู้เขียนสรุปผลการศึกษาตามบทความนี้ และมีข้อเสนอบางประการเพื่อผู้ประกอบการที่มีความสนใจอาจนำไปพิจารณาใช้กับการประเมินความเสี่ยงด้านไซเบอร์ขององค์กรของตนดังต่อไปนี้

4.1 บทสรุป

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหลักเกณฑ์ และควบคุมการเก็บรวมรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ถ้าผู้ควบคุมข้อมูลส่วนบุคคล และ ผู้ประมวลผลข้อมูลส่วนบุคคลบริหารจัดการข้อมูลส่วนบุคคลโดยฝ่าฝืนต่อบทบัญญัติของกฎหมาย และก่อความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล และ/หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลย่อมมีความรับผิดทางแพ่ง โดยต้องความรับผิดโดยเคร่งครัด หากการฝ่าฝืนบทบัญญัตินั้นเกิดโดยเจตนาก็จะมีโทษทางอาญา นอกจากนี้ ยังมีโทษทางปกครองซึ่งเป็นโทษปรับที่มีมูลค่าสูง

ยิ่งไปกว่านั้น การเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ไม่ว่าจะเกิดจากการจงใจหรือไม่ ผู้ควบคุมข้อมูลส่วนบุคคล และ ผู้ประมวลผลข้อมูลส่วนบุคคลก็ไม่สามารถหลีกเลี่ยงการเกิดค่าใช้จ่ายในการตอบสนองต่อเหตุการณ์ เช่น เพื่อการบอกกล่าวการเกิดเหตุละเมิดแก่เจ้าของข้อมูลส่วนบุคคล และการบอกกล่าวการเกิดเหตุละเมิดสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งการเฝ้าระวัง การเยียวยาแก้ไขการละเมิดข้อมูลส่วนบุคคลนั้น

กรมธรรม์ประกันภัยความรับผิดทางไซเบอร์ เป็นประกันภัยที่สามารถบรรเทาความเสียหายให้แก่ผู้เอาประกันภัย โดยผู้เขียนพบว่ากรมธรรม์ประกันภัยการบริหารความเสี่ยงทางไซเบอร์ขององค์กร แบบที่ 1 ของกลุ่มชับบ์ฯ ประเทศไทย ซึ่งผู้เขียนนำมาศึกษา มีความคุ้มครองการชดใช้ค่าเสียหายที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล อาจต้องรับผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อยู่หลายกรณี ซึ่งอาจเป็นจำนวนเงินค่าเสียหายตามคำพิพากษาของศาล อนุญาโตตุลาการ รวมถึงค่าเสียหายเชิงลงโทษ และค่าปรับทางปกครอง หรือ จำนวนที่เจรจาตกลงชดใช้ให้แก่ผู้เสียหายเพื่อมิให้ข้อพิพาทขึ้นสู่ศาล นอกจากนี้ ยังมีความคุ้มครองถึงค่าใช้จ่ายที่เกิดขึ้นแก่ผู้เอาประกันภัย เช่น ค่าทนายความ ค่าตอบแทนพยานผู้เชี่ยวชาญ ค่าใช้จ่ายเพื่อเป็นค่าธรรมเนียมการจัดเตรียมหลักทรัพย์เพื่อเป็นประกัน ค่าใช้จ่ายที่จะเกิดขึ้นเพื่อแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น

แต่อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ก็ต้องพึงระลึกว่ากรมธรรม์ประกันภัยมีข้อยกเว้นความคุ้มครองอยู่บางประการ แม้ว่าการกระทำนั้นจะเป็นความรับผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ก็ตาม ตัวอย่างเช่น ค่าปรับทางอาญา และ การกระทำผิดที่เกิดจากการกระทำโดยจงใจ หรือมีเจตนาทุจริต รวมทั้งการหาประโยชน์ส่วนตัวโดยมิชอบทั้งโดยตัวผู้เอาประกันภัยเองในฐานะผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล หรืออนุญาตให้บุคคลอื่นกระทำ ตัวอย่างเช่น การจงใจเก็บข้อมูลส่วนบุคคลโดยมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เป็นต้น การกระทำเหล่านี้จะไม่ได้รับความคุ้มครองจากการประกันภัย

ผู้เขียนจัดทำตารางสรุปความคุ้มครองของกรมธรรม์ประกันภัยการบริหารความเสี่ยงทางไซเบอร์ขององค์กร แบบที่ 1 ของกลุ่มชับบ์ฯ ประเทศไทย ต่อการไม่ปฏิบัติพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไว้ในภาคผนวกของบทความนี้

4.2 ข้อเสนอแนะ

ผู้เขียนมีข้อเสนอแนะบางประการเกี่ยวกับการประกันภัยความรับผิดทางไซเบอร์ โดยมีทั้งข้อเสนอในส่วนของภาคเอกชนและภาครัฐ ดังต่อไปนี้

4.2.1 การประเมินความเสี่ยงด้านไซเบอร์ขององค์กร

ผลของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทำให้ผู้ประกอบการทุกภาคส่วน ไม่ว่าเล็กหรือใหญ่ อยู่ในรูปบุคคลธรรมดาหรือนิติบุคคล เว้นแต่กิจการบางอย่างที่กฎหมายยกเว้น จะมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามความหมายของกฎหมาย เพราะอย่างน้อยที่สุดแต่ละองค์กรก็ต้องมีข้อมูลส่วนบุคคลของพนักงานในองค์กรนั้นเอง แต่อย่างไรก็ตาม ก่อนการตัดสินใจทำประกันภัยไซเบอร์ ควรมีการบริหารความเสี่ยงทางไซเบอร์ขององค์กร

หลักการบริหารความเสี่ยงโดยทั่วไปมี 6 ขั้นตอน[55] ซึ่งสามารถปรับใช้กับการบริหารความเสี่ยงทางไซเบอร์ เพื่อนำไปประกอบการพิจารณาถึงความจำเป็นในการเลือกความคุ้มครองของการประกันภัยความรับผิดทางไซเบอร์ ได้แก่

ขั้นที่ 1 การกำหนดนโยบายการบริหารความเสี่ยงภัยทางไซเบอร์ขององค์กร (establish cyber risks management policy) – โดยองค์กรต้องประเมินว่าความเสี่ยงต่อความเสียหายทางไซเบอร์ลักษณะใดที่องค์กรต้องให้ความสำคัญ ความเสี่ยงระดับใดสามารถยอมรับได้ (acceptable risks) ระดับใดยอมรับไม่ได้ (unacceptable risks) และต้องมีมาตรการจัดการ ในข้อนี้การไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลย่อมเป็นความเสียหายทางไซเบอร์ที่องค์กรต้องให้ความสำคัญ เพราะมีมูลค่าความเสียหายที่สูงและเกิดผลกระทบต่อชื่อเสียงขององค์กร

ขั้นที่ 2 การระบุความเสี่ยงภัยทางไซเบอร์ (identify cyber risks) และความเป็นไปได้ของความเสียหาย – องค์กรต้องประเมินว่าเหตุการณ์อะไรจะเกิดขึ้น เช่น การรั่วไหลของข้อมูลส่วนบุคคลเพราะการทุจริตของบุคคลในองค์กร การถูกจารกรรมจากบุคคลภายนอก เป็นต้น และเหตุการณ์นั้นสามารถเกิดขึ้นได้หรือไม่ ซึ่งข้อนี้จะสอดคล้องกับการเลือกส่วนความคุ้มครองของกรมธรรม์ประกันภัย เพราะหากองค์กรไม่มีความเสี่ยงภัยทางไซเบอร์บางประเภทก็อาจไม่ต้องเลือกความคุ้มครองนั้น

ขั้นที่ 3 การวิเคราะห์ความเสี่ยงทางไซเบอร์ (analyze the cyber risks) – องค์กรต้องนำความเสี่ยงภัยทางไซเบอร์ที่ระบุได้มาประเมินว่ามีความถี่ของการเกิดเหตุและสิ่งที่อาจเป็นผลลัพธ์โดยเฉพาะผลกระทบทางการเงิน เช่น การถูกดำเนินคดีทางปกครอง การชดใช้ค่าเสียหาย รวมทั้งมาตรการป้องกันและบรรเทาความเสี่ยง

ขั้นที่ 4 การประเมินความเสี่ยงทางไซเบอร์ (evaluate the cyber risks) – โดยการเปรียบเทียบระดับความเสี่ยง (levels of risks) กับ ระดับความเสี่ยงที่ยอมรับได้โดยเปรียบเทียบเป็นมูลค่าเงิน

ขั้นที่ 5 การจัดการกับความเสี่ยงภัยทางไซเบอร์ (treat the cyber risks) – ความเสี่ยงภัยที่ไม่สามารถยอมรับได้ มีวิธีการจัดการห้าวิธี ได้แก่ การหลีกเลี่ยง การยอมรับ การควบคุม การถ่ายโอน และการรับความเสี่ยงภัยเอาไว้บางส่วน การประกันภัยไซเบอร์ ก็คือการจัดการกับความเสี่ยงภัยวิธีหนึ่ง โดยการถ่ายโอนความเสี่ยงไปยังผู้รับประกันภัย

ขั้นที่ 6 การเฝ้าติดตามและทบทวนความเสี่ยงภัยทางไซเบอร์ (monitor and review the cyber risks) – องค์กรต้องเฝ้าติดตามว่ามาตรการที่กำหนดนั้นเป็นไปตามเป้าหมายหรือต้องมีการปรับปรุงแก้ไข

[55] Australian and New Zealand Institute of Insurance and Finance, GI404-00 Introduction to General Insurance Underwriting Study Material, (2017) 13.

4.2.2 ศึกษาความเป็นไปได้ในการกำหนดให้ประกันภัยความรับผิดทางไซเบอร์เป็นการประกันภัยภาคบังคับ

ประเทศไทยใช้การประกันภัยภาคบังคับเป็นเครื่องมือในการคุ้มครองความเสียหายให้แก่บุคคลภายนอก เช่น พระราชบัญญัติความรับผิดทางแพ่งต่อความเสียหายจากมลพิษน้ำมันอันเกิดจากเรือ พ.ศ. 2560 มาตรา 15 พระราชบัญญัติควบคุมอาคาร พ.ศ.2522 มาตรา 32 ตรี พระราชบัญญัติคุ้มครองผู้ประสบภัยจากรถ พ.ศ. 2535 มาตรา 7 พระราชบัญญัติทรัสต์เพื่อธุรกรรมในตลาดทุน พ.ศ. 2550 มาตรา 58 พระราชบัญญัติธุรกิจนำเที่ยวและมัคคุเทศก์ พ.ศ. 2551 มาตรา 26 (9) และ มาตรา 34 เป็นต้น โดยมีบทกำหนดโทษหากไม่จัดให้มีการประกันภัยตามกฎหมายดังกล่าวเหล่านี้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายที่มุ่งคุ้มครองเจ้าของข้อมูลส่วนบุคคล ซึ่งก็คือประชาชนทั่วไปเช่นกัน ดังนั้น ผู้เขียนจึงเห็นว่า สมควรมีการศึกษาแนวโน้มความเป็นไปได้ในการนำประกันภัยความรับผิดทางไซเบอร์มาเป็นการประกันภัยภาคบังคับ โดยศึกษาแนวทางของต่างประเทศ เช่น ข้อกำหนดในการประกันภัยภาคบังคับ การกำหนดขอบเขตขั้นต่ำในเรื่องของขอบเขตการคุ้มครอง ว่าต้องมีขอบเขตแค่ไหน เพียงใด

4.2.3 ควรมีกรมธรรม์ประกันภัยแบบมาตรฐานภาษาไทย

เนื่องจากกรมธรรม์ประกันภัยความเสี่ยงภัยทางไซเบอร์ที่ใช้ในประเทศไทยยังไม่มีฉบับมาตรฐาน เพื่อให้สอดคล้องกับข้อเสนอ 4.2.2 ผู้เขียนเสนอให้มีการจัดทำกรมธรรม์ประกันภัยความรับผิดทางไซเบอร์แบบมาตรฐานภาษาไทย ซึ่งอย่างน้อยต้องมีความคุ้มครองความรับผิดอันเกิดจากการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น คุ้มครองความรับผิดจากการละเมิดข้อมูลส่วนบุคคล ความรับผิดจากการละเมิดความปลอดภัยของเครือข่าย ค่าใช้จ่ายในการต่อสู้คดี เป็นต้น

บรรณานุกรม

บทความ

บรรเจิด ภาคาพันธุ์, ‘ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในธุรกิจประกันชีวิต’ (2563) 1 วารสารบัณฑิตศึกษานิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

สื่ออิเล็กทรอนิกส์

Australian and New Zealand Institute of Insurance and Finance, GI404-00 Introduction to General Insurance Underwriting Study Material, (2017).

เอกสารประกอบการสัมมนา

ญาดา กาศยปนันท์, ‘เจาะลึกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และแนวปฏิบัติที่ถูกต้องสำหรับธุรกิจเช่าซื้อและลีสซิ่ง’ (โครงการอบรมวิชาการด้านธุรกิจเช่าซื้อ, สมาคมธุรกิจเช่าซื้อไทย, โรงแรมสยามแอทสยาม, 10 พฤศจิกายน 2563).

เอกสารอื่น ๆ

ภาษาไทย

กมลชัย รัตนสกาวงศ์, ‘ทฤษฎีและแนวคิดเกี่ยวกับการกำหนดโทษทางปกครองในการตรากฎหมาย’ (โครงการสัมมนาเรื่อง หลักเกณฑ์ในการกำหนดโทษทางปกครองในการตรากฎหมาย, สำนักงานคณะกรรมการกฤษฎีกา, 2560), <http://web.krisdika.go.th/data/outsitedata/article77/file77/c06.pdf.> สืบค้นเมื่อ 12 มกราคม 2564.

กลุ่มงานบริการวิชาการ สำนักวิชาการ, “เอกสารประกอบการพิจารณา ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...,” อ.พ. 6/2556 สมัยสามัญทั่วไป, สำนักงานเลขาธิการสภาผู้แทนราษฎร (ตุลาคม 2556)

ภาษาต่างประเทศ

Chubb Insurance Australia Limited, ‘Cyber Enterprise Risk Management Insurance Policy’ (insuring clauses 1.1 A) <https://www.steel-line.com.au/wpcontent/uploads/2020/04/cyber_certificate_of_currency.pdf> accessed on 19th Jan 2021.

Lesley Fair, ‘FTC’s $5 billion Facebook settlement: Record-breaking and history-making’ (Federal Trade Commission, 2019) <https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record breaking-history> accessed 16th Nov 2020.