



**พระราชบัญญัติการรักษาความ
มั่นคงปลอดภัยไซเบอร์ของ
ประเทศไทย:
ข้อปฏิบัติ & ข้อห้ามปฏิบัติ**

สู่กฎหมายที่มีมนุษยเป็นศูนย์กลาง
เพื่อคุ้มครองเสรีภาพและความเป็น
ส่วนตัวออนไลน์พร้อมกับแก้ปัญหา
ภัยคุกคามทางไซเบอร์

กันยายน 2019



MANUSHYA
Empowering Communities | Advancing Social Justice

กิตติกรรมประกาศ:

มูลนิธิมานุษยะขอขอบคุณอย่างจริงใจต่อ **สถานเอกอัครราชทูตเนเธอร์แลนด์ประจำประเทศไทย แอคเซส นาว เครือข่ายพลเมืองเน็ต** และสหพันธ์ระหว่างประเทศเพื่อสิทธิมนุษยชนสากล (FIDH) สำหรับการให้ความสนับสนุนและร่วมเป็นพันธมิตรในโครงการ 'พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย'



Kingdom of the Netherlands



accessnow



fidh

จัดทำโดย:

เอมีลี ประดิจิต

ผู้ก่อตั้งและผู้อำนวยความสะดวก

และ

อนันยา รามานี

เจ้าหน้าที่ฝ่ายวิจัยและรณรงค์ด้านสิทธิมนุษยชน

มูลนิธิมานุษยะ

ออกแบบสื่อสารโดย:

ลอริน เคลโลเซ่

อาสาสมัครฝ่ายสนับสนุนและรณรงค์

มูลนิธิมานุษยะ

รูปภาพประกอบโดย:

การ์ตูนโดย Patrick Chappatte for the International Herald Tribune (known now as The International New York Times); และ รูปดิจิทัลสำหรับการสื่อสาร โดย shutterstock.com



This work is licensed under Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License ("Public License"). To view a copy of this license, visit:

<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

ลิขสิทธิ์ @ManushyaFoundation2019

ข้อมูลเพิ่มเติมเกี่ยวกับมูลนิธิมานุษยะ ในโครงการ สิทธิดิจิทัล โปรดติดต่อ:



เอมีลี ปาลามี ประดิจิต ผู้ก่อตั้งและผู้อำนวยความสะดวก

emilie@manushyafoundation.org



อนันยา รามานี เจ้าหน้าที่ฝ่ายวิจัยและรณรงค์ด้านสิทธิมนุษยชน

ananya@manushyafoundation.org



ข้อกำหนดที่ 1 ขอบเขตการบังคับใช้และนิยามที่กว้างเกินไป

อ้างอิงถึงความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร

และความสงบเรียบร้อยภายในประเทศ ในการบังคับใช้และติดตามผลของพระราชบัญญัตินี้

ข้อปฏิบัติ

- 1 ต้องประกัน**ว่าขอบเขตและนิยามของภัยคุกคามทางไซเบอร์ และแง่มุมอื่นๆ ถูกกำหนดขึ้นโดยมีการพิจารณาอย่างเหมาะสมต่อหลักการประชาธิปไตยและสิทธิมนุษยชน
- 2 ต้องประกัน**ว่าการอธิบายอย่างชัดเจนเพียงพอถึงข้อจำกัดใดๆ ต่อสิทธิ สอดคล้องตามหลักนิติธรรม และเท่าที่จำเป็นตามกฎหมายในประเทศสอดคล้องกับพันธกรณีด้านสิทธิมนุษยชนระหว่างประเทศของไทยตามกติกา ICCPR
- 3 ต้องพิจารณา**ถึงผลกระทบจากภัยคุกคามทางไซเบอร์ต่อการมีอยู่การรักษาความลับและความมั่นคงทางข้อมูลและในส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐานรวมทั้งความมั่นคงปลอดภัยของบุคคล
- 4 ต้องคุ้มครอง**ข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลอื่นๆ ตามพระราชบัญญัตินี้ โดยให้อยู่ภายใต้อำนาจหน้าที่ของหน่วยงานที่มีความรับผิดชอบเป็นการเฉพาะเพื่อคุ้มครองการเก็บรวบรวมข้อมูลและข้อมูลสนเทศอื่นๆ

ข้อห้ามปฏิบัติ

- 1 ต้องไม่เน้น**กำหนดขอบเขตของพระราชบัญญัตินี้ เฉพาะเจาะจงเรื่องความมั่นคงและความมั่นคงในรูปแบบอื่นๆ อย่างเช่น ความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ โดยไม่มีการชี้แจงในรายละเอียดว่าความมั่นคงดังกล่าวมีองค์ประกอบอย่างไร
- 2 ต้องไม่จำกัด**สิทธิและเสรีภาพอย่างกว้างขวางเนื่องจากเป็นสิ่งที่ได้รับการคุ้มครองตามรัฐธรรมนูญ โดยอ้างเพียงว่าเป็นความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ทั้งที่ไม่มีการนิยามอย่างเหมาะสม
- 3 ต้องไม่กำหนด**ให้มีการตอบโต้ต่อภัยคุกคามในทุกกรณี ซึ่งเชื่อว่าส่งผลกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ โดยถูกมองว่าส่งผลกระทบต่ออำนาจและเสถียรภาพของรัฐ
- 4 ต้องไม่อนุญาต**ให้หน่วยงานตามพ.ร.บ.นี้ สามารถบังคับให้มีการละเมิดสิทธิระหว่างการปฏิบัติตามพ.ร.บ.นี้แต่ให้ดูแลให้มีการปฏิบัติตามหลักเกณฑ์ในขั้นตอนปฏิบัติเพื่อความเป็นธรรม กระบวนการอันควรตามกฎหมายและให้มีการใส่ใจดูแลอย่างเหมาะสม โดยเป็นการดำเนินงานตามระยะเวลาอันควร



ข้อกำหนดที่ 2 ข้อบัญญัติสำคัญที่มีปัญหาและไม่มีการนิยามอย่างชัดเจน

ในส่วนของภัยคุกคามทางไซเบอร์ทั้งสามระดับ (ภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง ร้ายแรง และวิกฤติ)

ข้อปฏิบัติ

- 1 ต้องนิยาม** ข้อจำกัดและเงื่อนไขเพื่อการพิสูจน์ว่าได้เกิดภัยคุกคามทางไซเบอร์ การประเมินความเสียหายเนื่องจากภัยคุกคามดังกล่าว และการกำหนดมาตรการเพื่อป้องกันแก้ไข และบรรเทาภัยคุกคาม และคุ้มครองสิทธิมนุษยชนตามที่กำหนดไว้ในรัฐธรรมนูญกฎหมายในประเทศและกฎหมายสิทธิมนุษยชนระหว่างประเทศในระหว่างกระบวนการนี้
- 2 ต้องกำหนด**หลักเกณฑ์ที่ชัดเจนในการจำแนกภัยคุกคามทางไซเบอร์ ประกาศให้คนทั่วไปทราบถึงหลักเกณฑ์นั้น และประกันให้มีข้อมูลหลักฐานสนับสนุน
- 3 ต้องกำหนด**ให้ใช้มาตรฐานการพิสูจน์ระดับสูงในการจำแนกพยานหลักฐานเพื่อชี้ว่าได้เกิดภัยคุกคามทางไซเบอร์ขึ้นจริง ทั้งนี้โดยผ่านกระบวนการสอบสวนที่เป็นผลและมีพยานหลักฐานสนับสนุนว่าอาจกำลังเกิดความเสียหายที่จะมีอันตรายร้ายแรง
- 4 ต้องคุ้มครอง**สิทธิมนุษยชนตามที่กำหนดไว้ในรัฐธรรมนูญกฎหมายในประเทศ และกฎหมายสิทธิมนุษยชนระหว่างประเทศในระหว่างการดำเนินงาน โดยมีการจำแนกและตอบโต้ต่อภัยคุกคามและความเสียหายตามที่เกิดขึ้น
- 5 ต้องจำกัด**ความเสียหายให้น้อยสุดและต้องมีการชดเชยต่อค่าเสียหายกรณีที่ไม่อาจหลีกเลี่ยงได้
- 6 ต้องให้**บุคคลมีทางเลือกว่าจะตอบโต้กับมาตรการที่ใช้ตามพระราชบัญญัตินี้อย่างไร

ข้อห้ามปฏิบัติ

- 1 ต้องไม่กำหนด**ให้การกระทำใดเป็นภัยคุกคามทางไซเบอร์ เมื่อซ้ำกับการกระทำที่มีอยู่แล้วและเป็นการกำหนดโดยใช้หลักเกณฑ์ที่คิดขึ้นมาเอง
- 2 ต้องไม่ดำเนินการ**ใดๆ หากขาดการประเมินอย่างชัดเจนถึงการมีอยู่ของภัยคุกคามทางไซเบอร์
- 3 ต้องไม่จำแนก**และดำเนินการตอบโต้ภัยคุกคามใดๆ เพียงเพราะมีข้อสงสัยว่าอาจมีภัยคุกคามเกิดขึ้น ทั้งนี้โดยไม่มีการสอบสวนเนื่องจากการคาดการณ์ว่าได้เกิดความผิดขึ้นและไม่ได้อยู่บนพื้นฐานของหลักฐานที่พิสูจน์ได้
- 4 ต้องไม่อนุญาต**ให้มีความขัดแย้งระหว่างสิทธิและปฏิบัติการที่ใช้เพื่อแก้ปัญหากลภัยคุกคามทางไซเบอร์เช่น การละเมิดสิทธิความเป็นส่วนตัว รวมทั้งการเข้าถึงระบบข้อมูลคอมพิวเตอร์ และการขุดข้อมูลออกมาเฉพาะ 'เท่าที่จำเป็น'
- 5 ต้องไม่บังคับ**ให้บุคคลอนุญาตให้สามารถเข้าถึงและตรวจค้นอาคารสถานที่ตามพระราชบัญญัตินี้เว้นแต่เป็นการเข้าไปโดยสมัครใจ
- 6 ต้องไม่อนุญาต**ให้มีการดำเนินงานใดๆ กรณีที่เป็นภัยคุกคามระดับวิกฤติ โดยไม่มีการอธิบายถึงข้อมูลเกี่ยวกับมาตรการที่จะนำมาใช้





ข้อกำหนาทที่ 3 กลไกควบคุมที่มีปัญหาตามพระราชบัญญัตินี้ (หน่วยงานและองค์กรของรัฐ) โครงสร้างการบริหารแบบบนลงล่าง อำนาจที่กว้างขวางที่มอบให้กับหน่วยงานต่าง ๆ เป็นเหตุให้พลเมืองเน็ตตกเป็นเป้าการสอดส่องติดตาม ขาดความโปร่งใสและมาตรฐาน

ข้อปฏิบัติ

- 1 ต้องประกัน**ว่าพระราชบัญญัตินี้บังคับใช้เฉพาะที่จำเป็นเพื่อบรรลุเป้าหมายอันชอบธรรมได้สัดส่วนกับเป้าหมายนั้น และต้องเป็นการแก้ปัญหาโดยใช้การดำเนินงานอย่างเหมาะสมด้วยเหตุดังกล่าว ต้องประกันให้มีการอบรมสร้างศักยภาพล่วงหน้ารวมทั้งการอบรมสำหรับเจ้าหน้าที่บังคับใช้กฎหมายและการอบรมให้เข้าใจถึงประเด็นสิทธิมนุษยชนและความเป็นส่วนตัวรวมทั้งการมีความรู้ความเข้าใจทางไซเบอร์ เพื่อไม่ให้เกิดการใช้อำนาจอย่างมิชอบ
- 2 ต้องประกัน**ว่าหน่วยงานและองค์กรตามพระราชบัญญัตินี้ รวมทั้งผู้เชี่ยวชาญอิสระเป็นตัวแทนของผู้มีส่วนได้ส่วนเสียทุกกลุ่มมีการสรรหาโดยผ่านกระบวนการที่โปร่งใส และมีการตรวจสอบเพื่อประกันว่าเป็นการมอบอำนาจให้กับหน่วยงานที่เป็นอิสระและไม่เป็นส่วนหนึ่งของโครงสร้างฝ่ายบริหาร ซึ่งมีหน้าที่ดูแลความมั่นคงปลอดภัยของบุคคล
- 3 ต้องประกัน**ว่า หน่วยงานและองค์กรใดๆ ตามพระราชบัญญัตินี้ ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองแรงงาน แรงงานสัมพันธ์ ประกันสังคม และการชดเชย
- 4 ต้องประกัน**ว่านโยบายและการปฏิบัติใด ๆ ตามพระราชบัญญัตินี้ มีพื้นฐานจากการพิสูจน์ด้วยหลักฐาน มีเหตุผลสนับสนุนชัดเจน มีเนื้อหาที่เฉพาะเจาะจง รอบด้าน มีการประกาศให้สาธารณชนทราบและสามารถเข้าถึงได้
- 5 ต้องกำหนด**ให้มีหลักประกันที่เหมาะสมและเป็นผลในการจัดการกับข้อมูลส่วนบุคคล ซึ่งหน่วยงานได้เก็บรวบรวมเพื่อประโยชน์ในการสอบสวนปัญหาภัยคุกคามทางไซเบอร์ พร้อมทั้งใช้ประโยชน์จากนวัตกรรมและความร่วมมือต้องกำหนดให้มีแนวปฏิบัติหรือขั้นตอนการดำเนินงานที่เป็นมาตรฐานทั้งในแง่ของอำนาจและหน่วยงานที่รับผิดชอบตามพระราชบัญญัตินี้โดยให้สอดคล้องกับการปฏิบัติที่ดีที่สุดระหว่างประเทศอันเป็นที่ยอมรับของประเทศอื่น ๆ

ข้อห้ามปฏิบัติ

- 1 ต้องไม่**อนุญาตให้มีการใช้อำนาจของหน่วยงานและองค์กรของรัฐบาลอย่างกว้างขวางโดยไม่อธิบายว่าจะมีการใช้อำนาจนั้นอย่างไร หากปราศจากการตรวจสอบและถ่วงดุลอำนาจนั้น
- 2 ต้องไม่**อนุญาตให้หน่วยงานและองค์กรที่ตั้งขึ้นตามพระราชบัญญัตินี้มีอำนาจในการบังคับใช้โดยมีเพียงเจ้าหน้าที่รัฐบาลที่มีอำนาจเพียงไม่กี่คนซึ่งที่ผ่านมาได้ตีความและใช้กฎหมายที่เกี่ยวข้องอย่างมิชอบแล้วไม่ว่าจะเป็นพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์รวมทั้งหน่วยงานซึ่งมีหน้าที่ตรวจสอบดูแลข่าวปลอม
- 3 ต้องไม่**อนุญาตให้มีข้อยกเว้นอันเป็นเหตุให้หน่วยงานสามารถใช้อำนาจอย่างกว้างขวางรวมทั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งมีสถานะเป็นนิติบุคคลแทนที่จะถือเป็นหน่วยงานสาธารณะอันเป็นเหตุให้มีการยกเว้นไม่ต้องอยู่ใต้การบังคับของกฎหมายปกครอง
- 4 ต้องไม่**ดำเนินงานโดยไม่ปฏิบัติตามหลักประกันให้เกิดความเป็นธรรมเชิงขั้นตอน และกระบวนการอันควรตามกฎหมาย รวมทั้งให้คำปรึกษาหารือกับผู้มีส่วนได้ส่วนเสียทุกกลุ่ม รวมทั้งหน่วยงานตามพ.ร.บ.นี้ภาคเอกชน ภาคประชาสังคมและผู้เชี่ยวชาญด้านเทคนิค
- 5 ต้องไม่**เรียกร่องข้อมูลเอกสาร สำเนาของเอกสาร ซึ่งถือว่าจำเป็นต่อการประเมินภัยคุกคามทางไซเบอร์ไม่เข้าไปตรวจค้นอาคารสถานที่ คอมพิวเตอร์และ/หรือระบบคอมพิวเตอร์ และยึดเอกสารและ/หรือคอมพิวเตอร์เพื่อจุดประสงค์ดังกล่าว ทั้งนี้โดยไม่มีการแจ้งในเบื้องต้นให้ผู้ใช้งานทราบว่ามี การเข้าถึงหรือเก็บข้อมูลส่วนใดไว้บ้าง



ข้อกำหนาทที่ 4 การใช้ความได้เปรียบเชิงอำนาจในการบังคับใช้พระราชบัญญัตินี้ อำนาจควบคุมเหนือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการบังคับให้หน่วยงานเหล่านี้ต้องรายงานข้อมูล

ข้อปฏิบัติ

- 1 ต้องกำหนด**หลักเกณฑ์ที่ชัดเจนในการจำแนกโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การรับฟังข้อมูลจากผู้มีส่วนได้ส่วนเสียทุกกลุ่มการให้ตัวอย่างที่เป็นรูปธรรม จำกัดการควบคุมต่อสถานการณ์ เฉพาะที่ถือว่าชอบธรรมในระบอบประชาธิปไตยและอนุญาตให้มีการตรวจสอบโดยหน่วยงานอิสระที่เป็นตัวแทนของหลากหลายภาคส่วนที่เกี่ยวข้อง
- 2 ต้องสามารถ**เชื่อมโยงระหว่างความเสียหายที่เกิดขึ้นกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และผลกระทบต่อองค์ประกอบที่สำคัญที่ได้รับการคุ้มครอง
- 3 ต้องนำ**มาตรฐานเดียวกันมาใช้ทั้งกับหน่วยงานของรัฐและภาคเอกชน ที่ถือว่าเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- 4 ต้องอนุญาต**ให้บุคคลและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีเวลาและโอกาสมากเพียงพอ ในการให้ข้อมูลเพื่อพิสูจน์ว่าไม่สามารถดำเนินงานตามได้ รวมทั้งปัญหาจากข้อจำกัดทางกฎหมายและเทคนิค

ข้อห้ามปฏิบัติ

- 1 ต้องไม่**ให้อำนาจอย่างกว้างขวางกับหน่วยงานของรัฐใด ๆ ซึ่งไม่มีความเป็นอิสระและไม่ลำเอียง ซึ่งจะทำให้หน่วยงานนั้นสามารถจำแนกได้ว่าองค์กรใดถือเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- 2 ต้องไม่**จำแนกว่า โครงสร้างพื้นฐานสำคัญทางสารสนเทศหมายถึงทุกสิ่งทุกอย่างที่เกี่ยวข้องกับความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ
- 3 ต้องไม่**กำหนดให้ต้องมีกรรายงานข้อมูลภัยคุกคามทางไซเบอร์จนมากเกินไป กรณีที่ยังไม่เกิด 'ความเสี่ยงอย่างแท้จริงว่าจะเกิดอันตราย'
- 4 ต้องไม่**กำหนดพันธกรณีที่เคร่งครัดต่อบุคคลและโครงสร้างพื้นฐานสำคัญทางสารสนเทศอันเป็นเหตุให้ต้องรายงานภัยคุกคามทางไซเบอร์ หรือต้องปฏิบัติตามคำสั่งให้แก้ไขสถานการณ์ดังกล่าวโดยเป็นพันธกรณีที่ไม่สามารถปฏิบัติตามได้หรือการกำหนดค่าปรับที่สูงและมีบทลงโทษที่รุนแรงเพื่อให้ปฏิบัติตามพันธกรณีนั้น

NATIONAL SECURITY





ข้อท้าทายที่ 5 การขาดการตรวจสอบและถ่วงดุล

ภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์ การขาดการตรวจสอบ และการใช้ระบบศาล

ข้อปฏิบัติ

- 1 ต้องประกัน**ให้หน่วยงานและองค์กรตามพระราชบัญญัตินี้ มีความโปร่งใสและตรวจสอบได้ และให้รายงานข้อมูลการปฏิบัติงานทุกปี และกำหนดให้มีกลไกอิสระเพื่อติดตามตรวจสอบองค์กร โดยประกอบด้วยตัวแทนจากผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง (รัฐบาล ภาคเอกชน คณะกรรมการสิทธิมนุษยชนแห่งชาติ ภาคประชาสังคม และผู้เชี่ยวชาญ) ทั้งนี้เพื่อติดตามและประเมินผลการดำเนินงานของหน่วยงานและองค์กรตามพระราชบัญญัตินี้
- 2 ต้องกำหนด**ให้มีศาลชำนาญพิเศษและมีผู้พิพากษาชำนาญพิเศษ ซึ่งมีความเชี่ยวชาญที่จำเป็นด้านกฎหมายและเทคนิคและมีความรู้เกี่ยวกับเนื้อหาและกระบวนการตามพระราชบัญญัตินี้ เพื่อพิจารณาคดีและกำหนดการเยียวยา รวมทั้งการมีคำสั่งคุ้มครองชั่วคราวเมื่อเป็นการปฏิบัติที่มีข้อสงสัย
- 3 ต้องอนุญาต**ให้มีการสอบสวนตามข้อร้องเรียน การพิจารณาและติดตามการดำเนินงาน โดยให้เป็นหน้าที่ของหน่วยงานที่เป็นอิสระจากหลากหลายภาคส่วน ซึ่งทำหน้าที่โดยมีสัดส่วนตัวแทนที่เท่าเทียมกันระหว่างที่ปรึกษาของรัฐบาล ภาคเอกชน และภาคประชาสังคม
- 4 ต้องประกัน**ให้มีการคุ้มครองบุคคลโดยจำกัดผลกระทบด้านลบที่อาจเกิดขึ้นจากการใช้ข้อมูลอย่างมีขอบ โดยเป็นข้อมูลที่จัดเก็บมาได้ตามพระราชบัญญัตินี้
- 5 ต้องประกัน**ให้มีการจำแนกมาตรการที่ใช้เพื่อจัดการกับภัยคุกคามทางไซเบอร์ระดับวิกฤติหลังมีการขออำนาจศาลและเป็นการดำเนินงานที่อยู่ใต้การตรวจสอบของคณะผู้เชี่ยวชาญที่เป็นอิสระจากหลากหลายภาคส่วน

ข้อห้ามปฏิบัติ

- 1 ต้องไม่**ให้อำนาจอย่างกว้างขวางกับหน่วยงานและองค์กรตามพระราชบัญญัตินี้ อันเป็นเหตุให้ขาดการตรวจสอบและถ่วงดุลในกระบวนการตัดสินใจและการปฏิบัติของหน่วยงานเหล่านี้
- 2 ต้องไม่**ขัดขวางไม่ให้มีการฟ้องคดีต่อหน่วยงานซึ่งใช้อำนาจอย่างมีขอบมีการบังคับใช้อย่างมีขอบ หรือมีการปฏิบัติที่เกินขอบเขตตามพระราชบัญญัตินี้ ทั้งนี้โดยให้สามารถเข้าถึงศาล เพื่อคัดค้านการดำเนินงานใด ๆ กับภัยคุกคามทางไซเบอร์ระดับร้ายแรงและวิกฤติ
- 3 ต้องไม่**ตัดสินใจกำหนดระดับภัยคุกคาม ความเสียหายและการชดเชย โดยเป็นการพิจารณาเฉพาะจากคณะรัฐมนตรีและไม่มีการรับฟังความเห็นจากหน่วยงานที่เป็นอิสระ ไม่ลำเอียง หรือมีอำนาจหรือหากปราศจากความสนับสนุนจากผู้ตรวจการแผ่นดิน
- 4 ต้องไม่**อนุญาตให้มีการนำข้อมูลที่จัดเก็บตามพระราชบัญญัตินี้ ไปใช้เพื่อการฟ้องคดีตามกฎหมายอื่น โดยเฉพาะคดีหมิ่นประมาท หมิ่นประมาททางโฆษณา การดูหมิ่นต่อเจ้าพนักงาน และการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์
- 5 ต้องไม่**เข้าถึงข้อมูลคอมพิวเตอร์ตามเวลาจริง(real time) หรือวิเคราะห์เนื้อหาของข้อมูล กรณีที่เป็นการรับมือกับภัยคุกคามทางไซเบอร์ระดับวิกฤติ และไม่ดำเนินการใด ๆ หากไม่มีการขออำนาจศาล

GUILTY



ข้อท้าทายที่ 6 ไม่ประกันให้มีการเยียวยา

การรับข้อร้องเรียนและการเยียวยา การจำคุก การสั่งปรับ และการชดเชย

ข้อปฏิบัติ

- 1 ต้องกำหนด**ให้มีการเยียวยาและการชดเชยอย่างเป็นผล สำหรับผู้เสียหายจากการประเมินผลที่ผิดพลาดต่อภัยคุกคามทางไซเบอร์ และการบังคับใช้พระราชบัญญัตินี้โดยมีขอบ อันเป็นเหตุให้ข้อมูลของบุคคลดังกล่าวถูกยึดไปอย่างไม่เป็นธรรมและไม่เหมาะสม
- 2 ต้องอนุญาต**ให้สามารถอุทธรณ์บทลงโทษทางอาญาและค่าปรับที่กำหนดขึ้นตามพระราชบัญญัตินี้กรณีที่ผู้ร้องเรียนถูกเก็บข้อมูลและมีการเปิดเผยข้อมูลนั้น เพื่อให้พวกเขาได้รับการปฏิบัติที่เป็นธรรม ได้รับการชดเชยตามความเสียหาย และป้องกันไม่ให้เกิดสถานการณ์เช่นนั้นขึ้นอีก
- 3 ต้องให้**โอกาสในการให้คำอธิบายอย่างมีเหตุผลหรือให้มีการเยียวยาในกรณีใด ๆ ซึ่งบุคคลต้องมีส่วนรับผิดชอบต่อการกระทำที่เกิดขึ้นกับหน่วยงานเอกชนของเขาและเป็นหน่วยงานที่เขาเป็นผู้มีอำนาจตัดสินใจ

ข้อห้ามปฏิบัติ

- 1 ต้องไม่**อนุญาตให้บุคคลหรือเจ้าพนักงานเข้าถึงข้อมูลตามที่กำหนดในพระราชบัญญัตินี้ ขณะที่ยังไม่มีความคุ้มครองทางไซเบอร์อย่างแท้จริง และต้องไม่ขัดขวางไม่ให้หน่วยงานต้องเยียวยาเมื่อเกิดการใช้อำนาจอย่างมีขอบ การนำกฎหมายไปบังคับใช้อย่างมีขอบหรือเป็นการปฏิบัติที่เกินขอบเขตตามพระราชบัญญัตินี้ โดยเฉพาะการฟ้องคดีต่อศาล เมื่อเกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรงและวิกฤติขึ้น
- 2 ต้องไม่**อนุญาตให้บุคคลหรือเจ้าพนักงานซึ่งสามารถเข้าถึงข้อมูลตามที่กำหนดในพระราชบัญญัตินี้ นำข้อมูลไปใช้ในทางที่มีขอบหรือเปิดเผยข้อมูลนั้นเพราะความเลินเล่อ ทั้งนี้โดยไม่มีกลไกรับข้อร้องเรียนเพื่อขอการเยียวยาที่เป็นผลและสามารถเข้าถึงได้
- 3 ต้องไม่**บังคับให้บุคคลต้องรับผิดชอบต่อการกระทำความผิดของนิติบุคคลอันเป็นผลมาจากการปฏิบัติหรือละเว้นการปฏิบัติ ภายหลังจากคำสั่งของนิติบุคคลนั้น



MANUSHYA

Empowering Communities | Advancing Social Justice

เกี่ยวกับ มูลนิธิมานุษยะ

มูลนิธิมานุษยะ ก่อตั้งขึ้นเมื่อปี พ.ศ.2560 ทำหน้าที่เป็นสะพานเชื่อม ขับเคลื่อน และเสริมสร้างผู้นำการเปลี่ยนแปลงโดยการเชื่อมต่อบุคคลผ่านการสร้างพันธมิตรร่วมกันและมีการพัฒนากลยุทธ์ที่มุ่งไปที่การสร้างเสียงของชุมชน ก่อตั้งให้เป็นศูนย์กลางในการสนับสนุนสิทธิมนุษยชนและการปฏิบัติตามพันธสัญญาและมาตรฐานด้านสิทธิมนุษยชนสากล

มูลนิธิมานุษยะเสริมสร้างความเข้มแข็งและความเป็นน้ำหนึ่งใจเดียวกันของชุมชนและประชาชนในระดับรากหญ้าเพื่อให้เป็นการรับรองว่าชุมชนจะสามารถนำเสนอข้อกังวลของตนเองและจัดหาวิธีการเพื่อพัฒนาการดำรงชีวิตและสถานการณ์สิทธิมนุษยชนในพื้นที่ได้

ติดต่อเรา :



5/4 ถนนสุทธิสารวินิจฉัย 1 สามเสนใน พญาไท
กรุงเทพฯ 10400 ประเทศไทย



www.manushyafoundation.org



contact@manushyafoundation.org



facebook.com/ManushyaFdn



+66 (0) 945-811-827



twitter.com/ManushyaFdn