ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศกับสหภาพยุโรป : ศึกษาผลกระทบของคดีคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดี C-362/14 ต่อโครงการเซฟฮาร์เบอร์ (Safe Harbour)

โดย

นางสาววรรณรัชชา ทรัพย์รดาพัดชา

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
สาขากฎหมายมหาชน
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2558

ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศกับสหภาพยุโรป : ศึกษาผลกระทบของคดีคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดี C-362/14 ต่อโครงการเซฟฮาร์เบอร์ (Safe Harbour)

โดย

นางสาววรรณรัชชา ทรัพย์รดาพัดชา

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
สาขากฎหมายมหาชน
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2558

HOW THE COURT OF JUSTICE OF THE EUROPEAN UNION JUDGMENT IN CASE C-362/14 ON PROTECTION PROVIDED BY SAFE HARBOUR PRIVACY PRINCIPLES AFFECTS PERSONAL DATA PROTECTION PROBLEMS IN INTERNATIONAL DATA TRANSFER WITH THE EUROPEAN UNION.

BY

MISS WANRATCHA SUPRADAPATCHA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF MASTER OF LAWS

PUBLIC LAW

FACULTY OF LAW

THAMMASAT UNIVERSITY

ACADEMIC YEAR 2015

มหาวิทยาลัยธรรมศาสตร์
คณะนิติศาสตร์

วิทยานิพนธ์

ของ

นางสาววรรณรัชชา ทรัพย์รดาพัดชา

เรื่อง

ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศกับสหภาพยุโรป
: ศึกษาผลกระทบของคดีคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดี C-362/14
ต่อโครงการเซฟฮาร์เบอร์ (Safe Harbour)

ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต

เมื่อวันที่ 11 สิงหาคม พ.ศ. 2559

ประธานกรรมการสอบวิทยานิพนธ์ _____
(รองศาสตราจารย์ คณาธิป ทองรวีวงศ์)

กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์ _____
(ผู้ช่วยศาสตราจารย์ ดร.จันทจิรา เอี่ยมมยุรา)

กรรมการสอบวิทยานิพนธ์ _____
(อาจารย์ ดร.จอมพล พิทักษ์สันตโยธิน)

กรรมการสอบวิทยานิพนธ์ _____
(อาจารย์ อาทิตย์ สุริยะวงศ์กุล)

คณบดี _____
(ศาสตราจารย์ ดร.อุดม รัฐอมฤต)

หัวข้อวิทยานิพนธ์	ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศกับสหภาพยุโรป : ศึกษาผลกระทบของคดีคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดี C-362/14 ต่อโครงการเซฟฮาร์เบอร์ (Safe Harbour)
ชื่อผู้เขียน	นางสาววรรณรัชชา ทรัพย์รดาพัดชา
ชื่อปริญญา	นิติศาสตรมหาบัณฑิต
สาขา/คณะ/มหาวิทยาลัย	กฎหมายมหาชน นิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ผู้ช่วยศาสตราจารย์ ดร.จันทจิรา เอี่ยมมยุรา
ปีการศึกษา	2558

บทคัดย่อ

สหภาพยุโรปได้บัญญัติ Directive 95/46/EC เพื่อเป็นหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปและได้วางหลักให้การโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปจะทำได้เมื่อประเทศที่รับโอนข้อมูลมีการรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ประเทศสหรัฐอเมริกาจึงมีความจำเป็นต้องจัดทำข้อตกลงโครงการเซฟฮาร์เบอร์ (Safe Harbour) กับสหภาพยุโรปเพื่อที่จะรับโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปได้ แต่ต่อมาศาลยุติธรรมแห่งสหภาพยุโรปได้มีคำพิพากษาให้คำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2000/520 ซึ่งเป็นฐานรองรับโครงการเซฟฮาร์เบอร์ตกเป็นโมฆะ อันทำให้การโอนข้อมูลส่วนบุคคลระหว่างสหภาพยุโรปและประเทศสหรัฐอเมริกาภายใต้โครงการเซฟฮาร์เบอร์มิอาจกระทำได้อีกต่อไป

วิทยานิพนธ์เล่มนี้มีวัตถุประสงค์เพื่อศึกษาเหตุผลที่ศาลยุติธรรมแห่งสหภาพยุโรปใช้ในการวินิจฉัยว่าการคุ้มครองข้อมูลส่วนบุคคลตามโครงการเซฟฮาร์เบอร์ไม่สามารถรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพออีกต่อไป พร้อมทั้งนำมาเปรียบเทียบกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย

จากการศึกษาพบว่าเหตุผลหลักที่ศาลใช้ในการตัดสินว่าโครงการเซฟฮาร์เบอร์มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ เนื่องจากโครงการเซฟฮาร์เบอร์ได้มีการกำหนดข้อยกเว้นให้องค์กรและหน่วยงานที่เข้าร่วมกับโครงการฯไม่ต้องปฏิบัติตามหลักเกณฑ์คุ้มครองข้อมูลส่วนบุคคลได้ในกรณีที่มีเหตุผลด้านการคุ้มครองความมั่นคงในประเทศหรือมีข้อยกเว้นโดยกฎหมายภายในของ

ประเทศสหรัฐอเมริกาบัญญัติหลักเกณฑ์ที่ขัดหรือแย้งกับการคุ้มครองข้อมูลส่วนบุคคลของโครงการดังกล่าว อีกทั้งกฎหมายภายในของประเทศสหรัฐอเมริกายังเปิดช่องให้อำนาจหน่วยงานด้านความมั่นคงสามารถเข้าถึงและประมวลผลข้อมูลส่วนบุคคลได้ในปริมาณมาก โดยไม่เฉพาะเจาะจงเป้าหมาย ส่งผลให้ข้อมูลส่วนบุคคลของประชาชนในสหภาพยุโรปเมื่อถูกโอนมายังประเทศสหรัฐอเมริกาไม่ได้รับการคุ้มครองที่เพียงพอตามมาตรฐานของสหภาพยุโรปอีกต่อไป

ส่วนในประเทศไทยได้มีการจัดทำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งกฎหมายดังกล่าวได้มีข้อยกเว้นเปิดช่องให้นำกฎหมายอื่นมาบังคับใช้โดยมิต้องปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคลได้เช่นกัน ในขณะเดียวกันได้มีร่างกฎหมายอื่นบางฉบับที่ให้อำนาจพนักงานเจ้าหน้าที่ในการตรวจสอบการสื่อสารของประชาชนได้ทุกช่องทางโดยไม่ต้องมีหมายศาลหรือให้อำนาจเจ้าหน้าที่รัฐไว้อย่างกว้างขวางอันจะก่อให้เกิดการใช้อำนาจเข้าถึงข้อมูลของประชาชนอย่างเกินขอบเขตได้ ดังนั้นกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยจึงเข้ากรณีที่เป็นสาเหตุให้ศาลยุติธรรมแห่งสหภาพยุโรปตัดสินว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอทุกประการ จึงส่งผลให้ในอนาคตประเทศไทยอาจไม่สามารถรับโอนข้อมูลส่วนบุคคลที่มาจากสหภาพยุโรปได้

ข้อเสนอแนะในการพัฒนามาตรการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยนั้น ผู้เขียนเห็นว่าควรมีการปรับปรุงแก้ไขร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลก่อนการบังคับใช้ รวมทั้งแก้ไขกฎหมายที่เกี่ยวข้องด้วย ดังนี้

1. ในแง่เนื้อหาของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลควรระบุเพิ่มเติมไว้ในบททั่วไปว่าการบังคับใช้ตามกฎหมายอื่นจะสามารถกระทำได้เท่าที่จำเป็นโดยไม่กระทบกระเทือนต่อสาระสำคัญแห่งสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล อีกทั้งควรเพิ่มเติมความชัดเจนของบทบัญญัติที่ให้ผู้ควบคุมข้อมูลแจ้งแก่เจ้าของข้อมูลส่วนบุคคลในกรณีที่ข้อมูลนั้นถูกละเมิด และเพิ่มเติมสิทธิของเจ้าของข้อมูลส่วนบุคคลในการจัดการและเยียวยาความเสียหายที่เกิดขึ้นด้วย

2. ในแง่องค์กรที่ทำหน้าที่บังคับการให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลควรมีความเป็นอิสระอย่างแท้จริง เพื่อที่จะคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ

3. ในแง่ของกฎหมายอื่นที่เป็นการแทรกแซงสิทธิในข้อมูลส่วนบุคคล ควรปรับปรุงบทบัญญัติที่ให้อำนาจรัฐในการเข้าสอดแนมข้อมูลส่วนบุคคลต้องกระทำได้อย่างจำกัด เฉพาะเจาะจงบุคคล และการเข้าถึงข้อมูลนั้นจะต้องขออนุญาตจากศาลด้วย

คำสำคัญ : การคุ้มครองข้อมูลส่วนบุคคล, การโอนข้อมูลส่วนบุคคลระหว่างประเทศ, Directive95/46/EC, โครงการ Safe Harbour, กฎหมาย PIPEDA, การสอดแนมข้อมูลโดยรัฐ, คำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปที่ C-362/14

Thesis Title	HOW THE COURT OF JUSTICE OF THE EUROPEAN UNION JUDGMENT IN CASE C-362/14 ON PROTECTION PROVIDED BY SAFE HARBOUR PRIVACY PRINCIPLES AFFECTS PERSONAL DATA PROTECTION PROBLEMS IN INTERNATIONAL DATA TRANSFER WITH THE EUROPEAN UNION.
Author	Miss Wanratcha Supradapatcha
Degree	Master of Laws
Department/Faculty/University	Public Law Faculty of Law Thammasat University
Thesis Advisor	Assistant Professor Dr. Jantajira Iammayura
Year	2016

ABSTRACT

Directive 95/46/EC legislated the protection of personal data in the European Union (EU), setting principles for personal data transfer to countries outside the EU. This can be done when countries receiving transfers ensure adequate levels of protection. The United States established Safe Harbour Privacy Principles (SHPP) for receiving transferred personal data from the EU. Later, the Court of Justice of the European Union (CJEU) declared invalid the European Commission's Decision 2000/520, the basis for ensuring adequate level of protection in the SHPP. This made transfer of personal data between the EU and the United States (US) under SHPP impossible to continue.

The court decided that SHPP offered inadequate levels of protection since it included exceptions for State authorities to avoid following principles to protect personal data. In cases of national security or exceptions in US law, legislation conflicted with personal data protection. U.S. intelligence agencies could access and process personal data with large-scale, indiscriminate collection by intelligence agency

programs (PRISM). EU personal data transferred to the US would no longer have sufficient protection.

Thailand's Personal Data Protection Act (PDPA) and related laws provide exceptions to enforcement by not requiring the protection of personal data in practice. At the same time, other laws give officers authority for surveillance of private communications beyond boundaries, without the use of writs. For this reason, Thailand's PDPA contains similar features that made the CJEU judge the protection level of personal data insufficient in all respects. The future of Thailand will be seriously affected if it cannot receive personal data from the EU.

These findings suggest that Thailand's PDPA should be improved in specific ways before it is enforced. Revising of related laws would also be advised.

Keywords: Protection of personal data, Directive 95/46/EC, Safe Harbour Privacy Principles, The Personal Information Protection and Electronic Documents Act, Public surveillance.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จสมบูรณ์ได้ด้วยความเมตตาอย่างยิ่งจากผู้ช่วยศาสตราจารย์ ดร.จันทจิรา เอี่ยมมยุรา ที่ได้กรุณารับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ โดยท่านได้ให้คำปรึกษา ให้แนวความคิดและกรอบในการศึกษาแก่ข้าพเจ้า เสนอแนวทางการเรียบเรียงเนื้อหาในวิทยานิพนธ์เล่มนี้ ตลอดจนให้ความช่วยเหลือและชี้แนะแนวทางการแก้ปัญหาแก่ข้าพเจ้าตลอดมา และด้วยความเมตตาของอาจารย์ ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล ผู้ให้คำปรึกษาเกี่ยวกับกรอบการศึกษาเริ่มต้นแก่ข้าพเจ้า รวมทั้งให้ความรู้ คำแนะนำเกี่ยวกับกฎหมายต่างประเทศอันมีค่ายิ่ง วิทยานิพนธ์ฉบับนี้คงจะสำเร็จลุล่วงไม่ได้หากปราศจากท่านอาจารย์ทั้งสองนี้ ข้าพเจ้าน้อมระลึกในพระคุณของอาจารย์พร้อมกราบขอบพระคุณเป็นอย่างสูงมา ณ ที่นี้

ข้าพเจ้าขอกราบขอบพระคุณรองศาสตราจารย์ คณาธิป ทองรวีวงศ์ ที่ได้ให้เกียรติเป็นประธานกรรมการวิทยานิพนธ์นี้ พร้อมทั้งกราบขอบพระคุณอาจารย์ ดร.จอมพล พิทักษ์สันตโยธิน และ อาจารย์ อาทิตย์ สุริยะวงศ์กุล ที่ให้ความกรุณารับเป็นกรรมการวิทยานิพนธ์เล่มนี้ โดยทุกท่านต่างเสนอแนวทางอันเป็นประโยชน์อย่างยิ่งต่อวิทยานิพนธ์เล่มนี้ ทำให้ข้าพเจ้าได้นำแนวคิด ความรู้มาพัฒนาปรับปรุงวิทยานิพนธ์ให้สมบูรณ์ครบถ้วน ข้าพเจ้าขอกราบขอบพระคุณท่านอาจารย์ทุกท่าน

นอกจากนี้ ข้าพเจ้าขอขอบพระคุณคณาจารย์คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ที่ได้ให้ความรู้ด้านกฎหมายแก่ข้าพเจ้ามาตั้งแต่ระดับนิติศาสตรบัณฑิตจนถึงระดับนิติศาสตรมหาบัณฑิต ความรู้ที่ได้จากการศึกษาวิชากฎหมายนั้นมีค่ายิ่งและเป็นส่วนสำคัญที่ทำให้เกิดวิทยานิพนธ์เล่มนี้ และข้าพเจ้าขอขอบคุณเพื่อนๆ หลักสูตรนิติศาตรมหาบัณฑิต สาขากฎหมายมหาชน รหัส 55 ทุกท่าน ที่คอยช่วยเหลือและเป็นกำลังใจให้แก่กันจนสำเร็จลุล่วง

สุดท้ายนี้ข้าพเจ้าขอขอบพระคุณนายวิริทธิพล ทรัพย์รดาพัดชา และ นางนันท์นภัส ทรัพย์รดาพัดชา ผู้เป็นบิดามารดาของข้าพเจ้า รวมทั้งครอบครัวที่ให้การสนับสนุนและเป็นกำลังใจให้ข้าพเจ้าในทุกๆด้านเสมอมา

ข้าพเจ้าหวังเป็นอย่างยิ่งว่าวิทยานิพนธ์ฉบับนี้จะยังประโยชน์ในทางวิชาการ และยังประโยชน์ต่อระบบการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยต่อไป หากวิทยานิพนธ์ฉบับนี้มีข้อบกพร่องหรือผิดพลาดประการใด ข้าพเจ้าขอน้อมรับความผิดพลาดนั้นไว้แต่เพียงผู้เดียว

นางสาววรรณรัชชา ทรัพย์รดาพัดชา

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	(1)
บทคัดย่อภาษาอังกฤษ	(3)
กิตติกรรมประกาศ	(5)
อภิธานศัพท์	(10)
บทที่ 1 บทนำ	1
1.1 สภาพและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ในการศึกษา	4
1.3 ขอบเขตการศึกษา	5
1.4 วิธีการศึกษา	5
บทที่ 2 แนวคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกับสถานการณ์การโอนข้อมูลส่วนบุคคลระหว่างประเทศ	6
2.1 แนวคิดว่าด้วยการคุ้มครองความเป็นส่วนตัว	6
2.2 แนวคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล	13
2.3 สถานการณ์การโอนข้อมูลส่วนบุคคลระหว่างประเทศกับปัญหาการคุ้มครองข้อมูลส่วนบุคคล	26
2.3.1 ความสำคัญและความจำเป็นในการโอนข้อมูลส่วนบุคคลระหว่างประเทศ	26
2.3.2 รูปแบบการโอนข้อมูลส่วนบุคคลระหว่างประเทศ	27
2.3.3 ปัญหาการคุ้มครองการโอนข้อมูลส่วนบุคคลระหว่างประเทศในปัจจุบัน	28
2.4 แนวทางการแก้ปัญหาการโอนข้อมูลส่วนบุคคลระหว่างประเทศ	29

2.4.1 มาตรการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลส่วนบุคคลระหว่างประเทศขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines) 29
2.4.2 มาตรการคุ้มครองข้อมูลส่วนบุคคลของสภายุโรป 31
2.4.3 มาตรการคุ้มครองข้อมูลส่วนบุคคลขององค์การสหประชาชาติ 32

บทที่ 3 กฎหมายต่างประเทศเกี่ยวกับการโอนข้อมูลส่วนบุคคลระหว่างประเทศ 35

3.1 Directive 95/46/EC โดยสหภาพยุโรป 36
3.1.1 วัตถุประสงค์และหลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลตาม Directive 95/46/EC 36
3.1.2 หลักการและวิธีการในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ 38
3.1.3 ข้อยกเว้นในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ 41
3.1.4 องค์กรที่มีหน้าที่บังคับการให้เป็นไปตามกฎหมาย 42
3.2 โครงการเซฟฮาร์เบอร์ (Safe Harbour Privacy Principles) ของประเทศสหรัฐอเมริกา 44
3.2.1 ความเป็นมาและวัตถุประสงค์ของโครงการ Safe Harbour 44
3.2.2 หลักการและวิธีการในการรับโอนข้อมูลระหว่างประเทศตามโครงการ Safe Harbour 49
3.2.3 ข้อยกเว้นของโครงการ Safe Harbour 52
3.2.4 องค์กรที่มีหน้าที่บังคับการให้เป็นไปตามกฎหมาย 53
3.3 กฎหมาย Personal Information Protection and Electronic Documents Act 2000 (PIPEDA) โดยประเทศแคนาดา 54
3.3.1 วัตถุประสงค์และหลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลของกฎหมาย PIPEDA 54
3.3.2 หลักการและวิธีการในการรับโอนและการโอนข้อมูลระหว่างประเทศ 60
3.3.3 ข้อยกเว้นของกฎหมาย PIPEDA 63
3.3.4 องค์กรที่มีหน้าที่บังคับการให้เป็นไปตามกฎหมาย 64

บทที่ 4 การคุ้มครองการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศในคำพิพากษาศาลยุติธรรมยุโรปในคดีเลขที่ C-362/14 66

4.1 ความสำคัญของคดีเลขที่ C-362/14 66
4.2 สรุปย่อคำพิพากษาศาลยุติธรรมยุโรปในคดีเลขที่ C-362/14 68
4.3 วิเคราะห์เหตุผลและหลักเกณฑ์ที่ศาลยุติธรรมแห่งยุโรปใช้ในการพิพากษาคดีเลขที่ C-362/14 85
4.4 ผลกระทบที่เกิดจากคำพิพากษาคดีเลขที่ C-362/14 และแนวทางการแก้ไข 97

บทที่ 5 วิเคราะห์ปัญหาการโอนข้อมูลส่วนบุคคลระหว่างประเทศในต่างประเทศเปรียบเทียบกับกฎหมายไทย 109

5.1 มาตรการทางกฎหมายที่ประเทศไทยใช้ในการคุ้มครองข้อมูลส่วนบุคคลในปัจจุบัน 109
5.1.1 การคุ้มครองข้อมูลส่วนบุคคลโดยบทบัญญัติของรัฐธรรมนูญ 111
5.1.2 การคุ้มครองข้อมูลส่วนบุคคลตามประมวลกฎหมายแพ่งและกฎหมายอาญา 113
5.1.3 การคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่องตามพระราชบัญญัติต่างๆ 116
5.2 มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 122
5.2.1 แนวคิดและความเป็นมาในการยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 122
5.2.2 ขอบเขตการใช้บังคับของร่างพระราชบัญญัติ 125
5.2.3 มาตรการในการคุ้มครองข้อมูลส่วนบุคคล 126
5.2.4 องค์กรที่มีหน้าที่ควบคุมและบังคับการให้เป็นไปตามกฎหมาย 129
5.3 วิเคราะห์ผลจากการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยเทียบกับแนวคำพิพากษาศาลยุติธรรมยุโรปในคดีเลขที่ C-362/14 130

บทที่ 6 บทสรุปและข้อเสนอแนะ 149

6.1 บทสรุป 149
6.2 ข้อเสนอแนะ 152

บรรณานุกรม 165

ภาคผนวก

ภาคผนวก ก คำพิพากษาศาลยุติธรรมยุโรป คดีเลขที่ C-362/14 173

ภาคผนวก ข คำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2000/520 200

ภาคผนวก ค ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 252

ภาคผนวก ง สัญญาแม่แบบตามคำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2001/497 269

ประวัติผู้เขียน 279

อภิธานศัพท์

Advocate General	: ที่ปรึกษาทางกฎหมาย
Canadian Security Intelligence Service	: หน่วยสืบราชการลับของประเทศแคนาดา
Central Intelligence Agency (CIA)	: สำนักงานสืบราชการลับกลาง
Charter of Fundamental Rights of the European Union	: กฎบัตรสิทธิขั้นพื้นฐานแห่งสหภาพยุโรป
Convention for the protection of Individuals with Regard to Automatic Processing of Personal (Convention 108)	: อนุสัญญาว่าด้วยการคุ้มครองปัจเจกชนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ
Commission Nationale de l'informatique et des Libertés (CNIL)	: คณะกรรมการแห่งชาติว่าด้วยข้อมูลข่าวสารและเสรีภาพประเทศฝรั่งเศส
Council of Europe	: สภายุโรป
Council of the European Union	: คณะมนตรีแห่งสหภาพยุโรป
Data Protection Authority	: หน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคล
Electronic Communication Privacy Act 1987	: รัฐบัญญัติคุ้มครองความเป็นส่วนตัวในการสื่อสารทางอิเล็กทรอนิกส์
European Commission	: คณะกรรมาธิการยุโรป
European Convention for the Protection of Human Rights and Fundamental Freedoms	: อนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานแห่งยุโรป
European Data Protection Supervisor (EPDS)	: ที่ปรึกษาการคุ้มครองข้อมูลของยุโรป

European Parliament	: รัฐสภายุโรป
“FAQs”	: ข้อสงสัยที่ได้รับการซักถามบ่อยครั้ง
Federal Bureau of Investigation	: หน่วยสืบสวนของรัฐบาลกลาง
Federal Trade Commission (FTC)	: คณะกรรมาธิการการค้าของสหรัฐอเมริกา
Foreign Intelligence Surveillance Act 1978 (FISA)	: รัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศ
Foreign Intelligence Surveillance Court (FISC)	: ศาลสืบราชการลับต่างประเทศ
Guidelines for Processing Personal Data Across Borders	: คู่มือการปฏิบัติงานว่าด้วยการประมวลผลข้อมูลส่วนบุคคลข้ามพรมแดน
Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data (OECD Guidelines)	: แนวปฏิบัติด้านการคุ้มครองความเป็นส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ
National Security Agency (NSA)	: สำนักงานความมั่นคงแห่งชาติ
Office of the Privacy Commissioner of Canada	: สำนักงานคณะกรรมาธิการสิทธิความเป็นส่วนตัวแห่งแคนาดา
U.S. Department of Commerce	: กระทรวงพาณิชย์สหรัฐอเมริกา
U.S. Department of Transportation	: กระทรวงการขนส่งสหรัฐอเมริกา
Universal Declaration of Human Rights (UDHR)	: ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน
Working Party	: คณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล

บทที่ 1
บทนำ

1.1 สภาพและความสำคัญของปัญหา

ในสังคมปัจจุบันเป็นยุคสังคมสารสนเทศ ซึ่งเป็นสังคมที่ตั้งอยู่บนพื้นฐานของเทคโนโลยีว่าด้วยข้อมูลข่าวสารและการติดต่อสื่อสารรูปแบบใหม่ๆ ท่ามกลางการพัฒนาของเทคโนโลยีสารสนเทศและการสื่อสารที่เจริญก้าวหน้าอย่างรวดเร็ว มีการพัฒนาการสื่อสารผ่านทางเครือข่ายอินเทอร์เน็ตส่งผลให้การสื่อสารและการเคลื่อนไหวของข้อมูลสามารถทำได้อย่างเสรี สะดวกรวดเร็ว ไร้ขีดจำกัดทั้งในเชิงคุณภาพและปริมาณ ไม่มีอุปสรรคทางด้านระยะทางอีกต่อไป ข้อมูลข่าวสารจึงกลายเป็นองค์ประกอบสำคัญที่มีอิทธิพลต่อการดำเนินการของทั้งภาครัฐและเอกชนในหลายๆด้าน ในระบบเศรษฐกิจนั้นย่อมอาศัยข้อมูลข่าวสารมาเป็นปัจจัยที่ใช้ในการตัดสินใจอย่างใดอย่างหนึ่งในการดำเนินธุรกิจ ธุรกิจบางประเภทใช้ข้อมูลข่าวสารเป็นกลไกหลักในการดำเนินกิจการ เช่น ธุรกิจเกี่ยวกับการเงินธนาคาร บริษัทประกันภัย ตลาดหลักทรัพย์ เป็นต้น ทางด้านการแพทย์ก็ใช้ข้อมูลข่าวสารในการส่งเสริมในการรักษาพยาบาลให้มีมาตรฐานสูงขึ้นและช่วยเหลือผู้ป่วยได้มากขึ้น เช่น การจัดทำข้อมูลสุขภาพ เวชทะเบียนหรือข้อมูลบันทึกการรักษาของบุคคล

ข้อมูลส่วนบุคคล (personal data) คือข้อมูลที่เกี่ยวกับสิ่งเฉพาะตัวบุคคลและเป็นข้อมูลที่สามารถพิสูจน์ตัวบุคคลได้ ข้อมูลประเภทนี้ได้แก่ ข้อมูลประวัติของบุคคล ข้อมูลเกี่ยวกับการนับถือความเชื่อลัทธิศาสนา ข้อมูลสุขภาพ ข้อมูลที่เกี่ยวกับการดำเนินคดีอาญา หรือแม้แต่ข้อมูลทางด้านพฤติกรรมการใช้ชีวิตของบุคคล ข้อมูลส่วนบุคคลนี้เป็นข้อมูลสำคัญที่มีการประมวลผล ใช้และโอนข้อมูลระหว่างกันอย่างแพร่หลาย อีกทั้งในยุคสมัยการสื่อสารแบบไร้พรมแดนนั้นทำให้การโอนข้อมูลส่วนบุคคลมิได้จำกัดเฉพาะการโอนข้อมูลส่วนบุคคลภายในประเทศแต่เพียงอย่างเดียว การโอนข้อมูลส่วนบุคคลระหว่างประเทศก็มีความสำคัญไม่ยิ่งหย่อนไปกว่ากัน เนื่องจากการดำเนินกิจการต่างๆมิได้จำกัดเฉพาะแค่ในประเทศใดประเทศหนึ่งอีกต่อไป แต่กลับมีลักษณะเปิดกว้างให้สามารถดำเนินกิจการต่างๆระหว่างกันได้แม้จะอยู่คนละประเทศ อีกทั้งทุกประเทศในโลกไม่สามารถจะหลีกเลี่ยงการประกอบธุรกิจกับต่างประเทศหรือประเทศในภูมิภาคเดียวกันได้ ยกตัวอย่างเช่น การโอนข้อมูลส่วนบุคคลของผู้ถือบัตรเครดิตเพื่อการเรียกเก็บเงินอันเนื่องจากการใช้บัตรเครดิตในต่างประเทศ การโอนข้อมูลของสายการบินต่างๆเพื่อจัดทำข้อมูลผู้โดยสาร หรือการโอนข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐเพื่อประโยชน์ในการบังคับใช้กฎหมาย การตรวจคนเข้าเมือง เป็นต้น

ปัญหาในการคุ้มครองข้อมูลส่วนบุคคลในปัจจุบันนี้เกิดขึ้นเนื่องจากการการเข้าถึงข้อมูลที่ทำได้อย่างสะดวกและรวดเร็วมาก ข้อมูลเหล่านั้นนั้นมิได้ถูกบันทึกไว้ในแผ่นกระดาษอีกต่อไป แต่ถูกประมวลผลและจัดเก็บไว้ในคอมพิวเตอร์หรือในระบบอินเทอร์เน็ต การสืบค้นข้อมูลสามารถทำได้ง่ายดายใช้เวลาเพียงเสี้ยววินาทีผ่านโปรแกรมช่วยเหลือในการสืบค้นข้อมูลบนอินเทอร์เน็ต (search engine) การแลกเปลี่ยนข้อมูลระหว่างกันเกิดขึ้นตลอดเวลาและมีอยู่ทั่วไป การสะสมข้อมูลส่วนบุคคลไว้ในครอบครองเพื่อหาประโยชน์จากข้อมูลนั้นมีเพิ่มมากขึ้นและมีอยู่ในทุกๆวงการธุรกิจ ซึ่งผลกระทบที่ตามมาคือการละเมิดและแทรกแซงสิทธิของเจ้าของข้อมูลส่วนบุคคลนั้นเอง เช่นทำให้เกิดการนำข้อมูลส่วนบุคคลไปใช้ ประมวลผล หรือเปิดเผย ที่อาจส่งผลให้บุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย อาจมีผลเกี่ยวกับความปลอดภัยต่อชีวิต ร่างกาย ตลอกจนรบกวนและสร้างความเสียหายต่อความเป็นส่วนตัวของบุคคลได้

ด้วยเหตุนี้เองนานาประเทศจึงได้สร้างมาตรการเพื่อปกป้องคุ้มครองสิทธิในข้อมูลส่วนบุคคลขึ้น โดยมีการพัฒนาหลักเกณฑ์หรือกฎหมายที่สร้างความสมดุลระหว่างเสรีภาพในการสื่อสารกับการคุ้มครองความเป็นส่วนตัว กฎหมายคุ้มครองข้อมูลส่วนบุคคลส่วนใหญ่จะครอบคลุมประเด็นเกี่ยวกับอำนาจควบคุมเหนือข้อมูลส่วนบุคคลในการรวบรวมและนำข้อมูลไปใช้ประโยชน์มากกว่าประเด็นว่าข้อมูลอยู่ที่ใดหรืออยู่ในการครอบครองของใคร แต่อย่างไรก็ตามด้วยความแตกต่างของสภาพสังคมและการพัฒนาแนวคิดทางด้านการคุ้มครองข้อมูลส่วนบุคคล ย่อมส่งผลให้ในแต่ละประเทศมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เท่าเทียมกัน ปัญหาของระดับความไม่เท่าเทียมกันของมาตรการคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศนี้เองได้ส่งผลเมื่อจำเป็นต้องมีการโอนข้อมูลส่วนบุคคลระหว่างประเทศ เนื่องจากเมื่อข้อมูลส่วนบุคคลถูกโอนไปยังอีกประเทศหนึ่งแล้วหากมีการดำเนินการใดๆต่อข้อมูลนั้นอันเป็นการกระทบหรือละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลย่อมเป็นการยากที่เจ้าของข้อมูลส่วนบุคคลจะสามารถเรียกร้องและได้รับการเยียวยาความเสียหายเหมือนดังวิธีการที่ใช้ในประเทศของตนก่อนที่จะมีการโอนข้อมูลส่วนบุคคลไป เพื่อแก้ปัญหาในเรื่องความไม่เท่าเทียมของกฎหมายคุ้มครองข้อมูลส่วนบุคคล องค์การระหว่างประเทศต่างๆจึงมีความพยายามสร้างหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลขึ้นเพื่อเป็นแนวทางในการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศต่างๆ เช่นแนวปฏิบัติขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines), สภายุโรป (Council of Europe), องค์การสหประชาชาติ (United Nations) เป็นต้น

นอกจากการพยายามสร้างหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลให้มีมาตรฐานเดียวกันแล้ว ในกลุ่มประเทศที่มีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลสูงจะมีการสร้างข้อจำกัดในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศด้วย เห็นได้จากการที่กลุ่มประเทศสมาชิกสหภาพยุโรป ได้มีการบัญญัติกฎหมาย Directive 95/46/EC ว่าด้วยการคุ้มครองบุคคลเกี่ยวกับการประมวลผลข้อมูล

ส่วนบุคคลเพื่อการถ่ายโอนข้อมูลบุคคลนั้น (the Protection of Individuals with regard to the Processing of Personal Data on the Free Movement of Such Data) ใน Directive นี้ได้สร้างหลักเกณฑ์สำคัญในการโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปว่า ห้ามมิให้มีการโอนข้อมูลส่วนบุคคลจากประเทศสมาชิกสหภาพยุโรปไปยังประเทศอื่นที่มิได้เป็นสมาชิกสหภาพยุโรป หากประเทศดังกล่าวมิได้มีการรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (adequate level of protection) เพื่อเป็นการสร้างหลักประกันว่าเมื่อมีการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศข้อมูลเหล่านั้นจะยังคงได้รับการคุ้มครองต่อไปจากประเทศที่เป็นฝ่ายรับโอนข้อมูลส่วนบุคคล

Directive 95/46/EC ได้ส่งผลกระทบต่อบรรดาประเทศต่างๆที่แม้มิได้เป็นสมาชิกสหภาพยุโรปให้จำเป็นต้องสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศเพื่อให้คณะกรรมาธิการยุโรป (European Commission) ตัดสินชี้ขาดว่าประเทศของตนมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ มิฉะนั้นแล้วจะไม่สามารถรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรปได้อย่างไร้ข้อจำกัด ซึ่งที่ผ่านมานั้นแนวทางที่แต่ละประเทศใช้เพื่อให้ได้รับการชี้ขาดว่ามีระดับการคุ้มครองที่เพียงพอมีหลายวิธีการ เช่นการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลภายในประเทศของตนให้ได้มาตรฐานและมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามแนวทางของประเทศสมาชิกสหภาพยุโรป เช่นกฎหมาย PIPEDA ของประเทศแคนาดา หรือการจัดทำข้อตกลงเพื่อคุ้มครองข้อมูลส่วนบุคคลและให้องค์กรภายในประเทศสามารถเข้าร่วมได้ตามสมัครใจ ดังเช่นโครงการเซฟฮาร์เบอร์ (Safe Harbour) ของประเทศสหรัฐอเมริกา

โครงการเซฟฮาร์เบอร์เป็นแนวทางที่ประเทศสหรัฐอเมริกาใช้เพื่อแก้ปัญหาการรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรป เกิดขึ้นจากการเจรจาระหว่างรัฐบาลสหรัฐอเมริกาโดยกระทรวงพาณิชย์กับคณะกรรมาธิการยุโรป ผลของการเจรจาทำให้เกิดข้อตกลงโครงการเซฟฮาร์เบอร์ขึ้นเมื่อวันที่ 26 กรกฎาคม ค.ศ. 2000 ข้อตกลงดังกล่าวมีหลักการสำคัญว่าบริษัทหรือองค์กรใดที่เข้าร่วมโครงการเซฟฮาร์เบอร์จะสามารถรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรปได้อย่างปราศจากข้อจำกัดใดๆ การเข้าร่วมโครงการเซฟฮาร์เบอร์เป็นไปโดยสมัครใจ โดยองค์กรที่ประสงค์จะเข้าร่วมโครงการเซฟฮาร์เบอร์นั้นจะต้องปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคล 7 ประการ ซึ่งหน่วยงานหรือองค์กรภายในประเทศสหรัฐอเมริกาต่างใช้โครงการเซฟฮาร์เบอร์เป็นวิธีการสำคัญในการรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรปเรื่อยมา

แต่เมื่อวันที่ 6 ตุลาคม ค.ศ. 2015 ได้มีการพิพากษาคดีของศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14 ข้อพิพาทระหว่างนายแม็กซิมิเลียน เชร็มส์ (Maximilian Schrems) ผู้ฟ้องคดี กับกรรมาธิการคุ้มครองข้อมูลประเทศไอร์แลนด์ ผู้ถูกฟ้องคดี ผลของคำพิพากษานั้นศาลได้

ตัดสินว่าคำวินิจฉัยที่ 2000/520 (Decision 2000/520) อันเป็นคำวินิจฉัยของคณะกรรมาธิการยุโรปที่เป็นฐานรับรองว่าโครงการเซฟฮาร์เบอร์มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอนั้นสิ้นผลไป ประเทศสหรัฐอเมริกาไม่สามารถรับโอนข้อมูลส่วนบุคคลโดยใช้โครงการเซฟฮาร์เบอร์ได้อีกต่อไป ผลของคำพิพากษาเป็นการวางหลักเกณฑ์ใหม่ในการพิจารณาว่าระดับการคุ้มครองข้อมูลส่วนบุคคลระดับใดที่เพียงพอซึ่งส่งผลกระทบอย่างมหาศาลต่อนานาประเทศให้ต้องกลับมาพิจารณากฎหมายคุ้มครองข้อมูลส่วนบุคคลภายในประเทศของตนอีกครั้งว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามแนวทางของศาลยุติธรรมแห่งสหภาพยุโรปหรือไม่ อย่างไร

การศึกษาและวิเคราะห์คำพิพากษาของศาลยุติธรรมแห่งสหภาพยุโรป ในคดีเลขที่ C-362/14 ว่ามีองค์ประกอบและเหตุผลใดบ้างที่ศาลใช้เพื่อการตัดสินชี้ขาดให้คำวินิจฉัยที่ 2000/520 สิ้นผลไป จึงเป็นเรื่องสำคัญและจำเป็นอย่างยิ่งสำหรับการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยที่อยู่ในขั้นตอนการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อใช้บังคับเป็นกฎหมายกลาง การศึกษาและเปรียบเทียบสถานการณ์ปัญหาการโอนข้อมูลส่วนบุคคลที่เกิดขึ้นในต่างประเทศแล้วนำเอาบทเรียนนั้นมาปรับปรุงแก้ไขกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ย่อมส่งผลดีในการยกระดับกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้ได้มาตรฐานสากล เป็นที่ยอมรับของนานาประเทศ และเพื่อความจำเป็นในอนาคตในฐานะที่ประเทศไทยจะต้องรับโอนข้อมูลส่วนบุคคลจากต่างประเทศ โดยเฉพาะการรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรป

1.2 วัตถุประสงค์ในการศึกษา

1. ศึกษาหลักเกณฑ์และวิธีการโอนข้อมูลส่วนบุคคลระหว่างประเทศ โดยเฉพาะหลักเกณฑ์ตาม Directive 95/46/EC โดยสหภาพยุโรป และหลักเกณฑ์โครงการเซฟฮาร์เบอร์ (Safe Harbour Privacy Principles) ของประเทศสหรัฐอเมริกา เพื่อทำความเข้าใจพื้นฐานของมาตรการที่ใช้ในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

2. ศึกษาและวิเคราะห์คำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14 โดยเฉพาะเหตุผลที่ทำให้ศาลตัดสินว่าคำวินิจฉัยที่ 2000/520 สิ้นผล เพื่อทำความเข้าใจสาเหตุข้อเท็จจริงและข้อกฎหมายที่เป็นเหตุให้ศาลตัดสินตามคำพิพากษา

3. ศึกษาและวิเคราะห์ปัญหาการโอนข้อมูลส่วนบุคคลระหว่างประเทศในต่างประเทศตามคดีเลขที่ C-362/14 เปรียบเทียบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย เพื่อให้ประเทศไทยมีการพัฒนามาตรการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนานาประเทศ และสามารถบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพ

1.3 ขอบเขตการศึกษา

วิทยานิพนธ์ฉบับนี้มุ่งศึกษาคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14 เพื่อให้ทราบปัญหาการคุ้มครองข้อมูลส่วนบุคคลที่โอนไปยังประเทศสหรัฐอเมริกา รวมทั้งศึกษาหลักเกณฑ์การโอนข้อมูลระหว่างประเทศในต่างประเทศ เช่น การโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปไปยังประเทศแคนาดา และนำมาปรับใช้กับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย โดยการวิเคราะห์ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ฉบับที่ผ่านการตรวจของคณะกรรมการกฤษฎีกา (คณะที่ 11) เรื่องเสร็จที่ 1135/2558 และร่างพระราชบัญญัติที่เกี่ยวข้อง เพื่อประโยชน์ในการเตรียมการรองรับการรับโอนข้อมูลส่วนบุคคลจากต่างประเทศมายังประเทศไทย

ทั้งนี้มีกรอบระยะเวลาการศึกษาตั้งแต่ช่วงการคุ้มครองข้อมูลส่วนบุคคลก่อนมีคำพิพากษาของศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14 จนถึงผลกระทบในของคำพิพากษาในช่วงเวลาปัจจุบัน (มิถุนายน 2559)

1.4 วิธีการศึกษา

1. ศึกษาโดยการค้นคว้าวิจัยเอกสารและตำราที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ จากหนังสือกฎหมาย วิทยานิพนธ์ รายงานการวิจัย บทความวิชาการ รวมถึงสื่อทางเว็บไซต์ต่างๆ

2. ศึกษาวิเคราะห์ Directive 95/46/EC, คำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2000/520, กฎหมายPIPEDA และ คำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14 ร่วมกับเอกสารของหน่วยงานที่เกี่ยวข้อง

3. ศึกษาวิเคราะห์กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย โดยเฉพาะร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... และกฎหมายอื่นที่เกี่ยวข้อง เช่น พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519, พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547, ร่างพระราชบัญญัติว่าด้วยการรักษาความปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ...., ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... เป็นต้น

บทที่ 2
แนวคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกับสถานการณ์การโอนข้อมูลส่วนบุคคลระหว่างประเทศ

2.1 แนวคิดว่าด้วยการคุ้มครองความเป็นส่วนตัว

แนวคิดด้านการคุ้มครองความเป็นส่วนตัว แรกเริ่มเกิดจากแนวคิดทางปรัชญาในทฤษฎีกฎหมายธรรมชาติ (Natural Law) ซึ่งสอนว่าความเป็นส่วนตัวเป็นสิทธิที่แสดงถึงคุณค่าประจำตัวของมนุษย์ เป็นสิทธิที่จำเป็นต่อการดำรงชีวิตของมนุษย์ เป็นสิทธิตามธรรมชาติที่ไม่ต้องมีการพิสูจน์ และเป็นสิทธิที่ติดตัวมนุษย์ตั้งแต่เกิดจนตาย[1] แต่การศึกษาและกำหนดขอบเขตของความเป็นส่วนตัวนั้น ในทางวิชาการยอมรับว่าเป็นเรื่องยากที่จะกำหนดให้แน่นอนและชัดเจนลงไปได้ เนื่องจากความเป็นส่วนตัวนั้นก่อร่างขึ้นจากวิถีชีวิตของมนุษย์ เกิดขึ้นจากแนวทางปฏิบัติของขนบธรรมเนียมและวัฒนธรรมของแต่ละสังคม แนวคิดของการคุ้มครองความเป็นส่วนตัวจึงมีลักษณะที่เคลื่อนไหว หรือเปลี่ยนแปลงไปได้ตามทัศนคติและความเชื่อของคนที่สังคมที่แปรเปลี่ยนไปตามยุคสมัย

แม้แนวคิดในการคุ้มครองความเป็นส่วนตัวจะพัฒนามาจากแนวความคิดทางปรัชญากฎหมายธรรมชาติหลายๆสำนักมาประกอบกัน เช่น แนวความคิดมนุษย์นิยม แนวความคิดเสรีนิยม แนวความคิดปัจเจกชนนิยม และทฤษฎีเสรีนิยมประชาธิปไตย[2] แต่แท้ที่จริงแล้วแนวคิดเรื่องความเป็นส่วนตัวนั้นได้มีพัฒนาการมาอย่างยาวนานนับหลายพันปี แนวคิดนี้มีมาก่อนบทบัญญัติกฎหมาย ความเป็นส่วนตัวจึงมีความหมายกว้างกว่าที่กฎหมายบัญญัติรับรองไว้ ในสมัยโบราณนั้นความเข้าใจเบื้องต้นเกี่ยวกับความเป็นส่วนตัว คือการไม่อยู่ร่วมกับคนอื่นหรือการปลีกตัวออกจากสังคม ดังเช่นในสมัยโรมัน แนวความคิดเกี่ยวกับเรื่องส่วนตัวยอมรับว่าบุคคลแต่ละคนมีเขตแดนของตนเอง ซึ่งในเขตแดนดังกล่าวเสมือนเป็นที่พำนักพักพิงไม่เกี่ยวข้องกับกิจกรรมทางสังคมในช่วงเวลาใดเวลาหนึ่ง ภายในดินแดนส่วนตัวนี้เป็นดินแดนเฉพาะตัวของแต่ละบุคคลเท่านั้น และเป็นที่ปราศจากการเข้ามาเกี่ยวของของคนในสังคม[3] ส่วนในยุคกรีกโบราณนั้นก็ได้มีการบัญญัติหลักเกณฑ์ที่เกี่ยวข้องกับการคุ้มครองความเป็นส่วนตัวเอาไว้ใน Mishnah ซึ่งเป็นประมวลกฎหมายสำหรับชาวยิวในสมัยนั้น ในบท

---

[1] ศิริกุล ภู่พันธ์, “ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), น.11.

[2] *เพิ่งอ้าง*, น.8.

[3] นคร เสรีรักษ์, <u>ความเป็นส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย</u>, (กรุงเทพมหานคร : สำนักพิมพ์พีเพรส, 2557), น.62.

หนึ่งของประมวลกฎหมายฉบับนี้ได้ระบุหลักเกณฑ์ว่า “ในบริเวณที่โล่งซึ่งมีการใช้สอยพื้นที่ร่วมกันระหว่างบ้านที่อยู่ใกล้เคียงกันนั้น ห้ามมิให้สร้างประตูหรือหน้าต่างตรงกับประตูหรือหน้าต่างของบ้านหลังอื่น หรือหากมีการสร้างในลักษณะดังกล่าวอยู่แล้วจะต้องไม่ทำการขยายให้ประตูหรือหน้าต่างนั้นมีขนาดใหญ่ขึ้นไปกว่าเดิม”[4] การคุ้มครองความเป็นส่วนตัวในลักษณะนี้เป็นการให้ความคุ้มครองความเป็นส่วนตัวในด้านพฤติกรรม (behavior) ของบุคคลในสถานที่ส่วนตัว (private space) เพื่อมิให้บุคคลอื่นก้าวล่วงในความเป็นส่วนตัวได้ ทั้งนี้จะเห็นได้ว่าการกำหนดหลักเกณฑ์ใน Mishan มิได้จำกัดเฉพาะห้ามมิให้กระทำการอันเป็นการละเมิดความเป็นส่วนตัว แต่ยังไม่รวมถึงการห้ามมิให้สร้างพฤติการณ์แวดล้อมอันเอื้อให้เกิดการละเมิดความเป็นส่วนตัวอีกด้วย

นักปรัชญาสมัยโบราณหลายท่านได้พยายามหาคำจำกัดความและกำหนดขอบเขตของความเป็นส่วนตัวขึ้น โดยคำสอนที่มักได้รับการกล่าวถึงมากที่สุดคือ คำสอนของอริสโตเติ้ล ซึ่งได้อธิบายว่าความเป็นส่วนตัวได้แก่เรื่องเกี่ยวกับร่างกายและการดำเนินชีวิตของสมาชิกภายในครอบครัว โดยมีเจ้าบ้านคือผู้เป็นพ่อ หรือผู้ชายที่เป็นผู้อาวุโสที่เป็นเจ้าบ้าน และเป็นผู้ทรงสิทธิในความเป็นส่วนตัวนั้น ซึ่งสถานะของความเป็นส่วนตัวในทางปรัชญาหมายถึงภาวะพื้นฐานของบุคคลที่ไม่ต้องต่อสู้ ยื้อแย่ง และไม่ต้องการข้อพิสูจน์ ความเป็นส่วนตัวเป็นสิทธิขั้นพื้นฐานโดยธรรมชาติของความเป็นมนุษย์ซึ่งแฝงอยู่ในตัวบุคคลนั้นๆมาตั้งแต่เกิด[5] การคุ้มครองความเป็นส่วนตัวในยุคดั้งเดิมนั้นจึงมุ่งเน้นที่การป้องกันมิให้บุคคลอื่นเข้ามารับรู้ถึงชีวิตส่วนตัวของตนเองเป็นหลัก

นับแต่ศตวรรษที่ 16 เป็นต้นมา แนวความคิดเกี่ยวกับขอบเขตความเป็นส่วนตัวเริ่มมีความชัดเจนและเป็นรูปธรรมมากยิ่งขึ้น โดยอธิบายความเป็นส่วนตัวว่าได้แก่เรื่องเกี่ยวกับเนื้อตัวร่างกาย ครอบครัวและรวมถึงทรัพย์สินด้วย เนื่องจากในช่วงเวลาดังกล่าวแนวความคิดการแบ่งขอบเขตระหว่างความเป็นส่วนตัวออกจากขอบเขตสาธารณะมีความชัดเจนมากขึ้น บนพื้นฐานแนวความคิดว่าความเป็นส่วนตัวเป็นสิทธิของมนุษย์ที่สามารถป้องกันมิให้รัฐหรือบุคคลใดล่วงล้ำดินแดนส่วนตัวของปัจเจกบุคคล กระแสการเรียกร้องให้รัฐรับรองและประกันสิทธิเสรีภาพและทรัพย์สินของประชาชนเกิดขึ้นทั่วไป มีการแบ่งแยกทรัพย์สินส่วนตัวออกจากสาธารณะ โดยอธิบายว่าเอกชนย่อมมีกรรมสิทธิ์ในทรัพย์สินของตนและมีความชอบธรรมที่จะหวงแหนทรัพย์สินและกีดกัน

---

[4] ปฏิวัติ อุ่นเรือน, “ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ,” (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), น.7.

[5] ชื่นอารี มาลีศรีประเสริฐ, “การคุ้มครองสิทธิส่วนตัวกับสื่อสารสนเทศ,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2539), น.10. อ้างถึงในนคร เสรีรักษ์, ความเป็นส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, (กรุงเทพมหานคร : สำนักพิมพ์พีเพรส , 2557), น.63.

บุคคลอื่น หรือแม้กระทั่งฝ่ายปกครองไม่ให้เข้ามาแทรกแซงทรัพย์สินของตนโดยพลการ ทรัพย์สินที่บุคคลหามาได้ตัวตนเองนั้นถือว่าทรัพย์นั้นเป็นทรัพย์ส่วนตัว[6]

ความเป็นส่วนตัวในยุคนี้โดยทั่วไป จึงหมายถึงความเป็นส่วนตัวในครอบครัวและสมาชิกครอบครัว ทรัพย์สิน และอาจหมายถึงส่วนที่ปลอดจากผู้คน และเป็นสิทธิของบุคคลในการแสดงความคาดหมายในเรื่องส่วนตัวของบุคคลใดบุคคลหนึ่ง[7] ความเป็นส่วนตัวในครอบครัวดูจะเป็นประเด็นใหญ่ที่สุด เพราะมีความหมายรวมถึงวิถีชีวิตความเป็นอยู่ของคนในครอบครัว ความสัมพันธ์ของบุคคลในครอบครัว การสืบพันธุ์ การเกิด การตายของคนในครอบครัว และยังรวมไปถึงความเป็นส่วนตัวในบริเวณบ้าน บริเวณที่อยู่อาศัย ซึ่งสิทธิในความเป็นส่วนตัวในลักษณะนี้เน้นการคุ้มครองจากการถูกละเมิดหรือแทรกแซงโดยรัฐ รัฐไม่สามารถจำกัดเสรีภาพในวิถีชีวิตครอบครัวหรือจำกัดเสรีภาพในการสร้างครอบครัวได้[8]

การพัฒนาแนวคิดด้านการคุ้มครองความเป็นส่วนตัวที่มีความชัดเจน และได้รับการยอมรับมากที่สุดเกิดขึ้นในศตวรรษที่ 19 เมื่อมีการเผยแพร่บทความเรื่องเดอะไรท์ทูไพรเวซี่ (The Right to Privacy) โดยซามูเอล ดี. วอร์เรน (Samuel D. Warren) และหลุยส์ ดี. แบรนดี้ส์ (Louis D. Brandies) ซึ่งเป็นนักกฎหมายชาวอเมริกัน บทความดังกล่าวเป็นผลสะท้อนของการพัฒนาเทคโนโลยีในช่วงปี ค.ศ. 1890 เนื่องจากมีการเกิดขึ้นของโทรเลข โทรศัพท์ มีแท่นพิมพ์ที่สามารถพิมพ์หนังสือได้อย่างรวดเร็ว วอร์เรนและแบรนดี้ส์ได้กล่าวว่าความก้าวหน้าดังกล่าวนี้ทำให้มีความจำเป็นต้องให้ความคุ้มครองแก่บุคคลเพราะพัฒนาการของเทคโนโลยีดังกล่าวทำให้เกิดการคุกคามสิทธิของบุคคลอย่างน่ากลัว

ในบทความของเดอะไรท์ทูไพรเวซี่ได้ให้คำจำกัดความความเป็นส่วนตัว (privacy) ว่าหมายถึงสิทธิที่จะอยู่โดยลำพัง (the right to be let alone) เป็นการมองความเป็นส่วนตัวในสอง

---

[6] ปรีดี เกษมทรัพย์, นิติปรัชญา, พิมพ์ครั้งที่5 (กรุงเทพมหานคร : โครงการประกอบตำราและเอกสารคำสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2543) น.197-198 อ้างถึงใน นคร เสรีรักษ์, ความเป็นส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย (กรุงเทพมหานคร : สำนักพิมพ์พีเพรส, 2557), น.64.

[7] Andreas S. Voss, "The Right to Privacy & Assisted Reproductive Technologies : A Comparative Study of Law of Germany and the U.S.," New York Law Journal of International & Comparative Law Volume 21, p.229 (2002). อ้างถึงใน ศิริกุล ภู่พันธ์, "ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล," (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), น.67.

[8] ศิริกุล ภู่พันธ์, *อ้างแล้ว เชิงอรรถที่ 1*, น.67.

แง่มุม คือความเป็นส่วนตัวในแง่นามธรรม ได้แก่ การที่บุคคลมีสิทธิและเสรีภาพในการแสดงอารมณ์ความรู้สึกนึกคิดตลอดจนความเชื่อศรัทธาในลัทธิศาสนา ส่วนความเป็นส่วนตัวในทางรูปธรรมคือสิทธิที่จะอยู่โดยลำพังปราศจากการรบกวนและการแทรกแซงจากสังคม การอยู่อย่างสันโดษไม่ติดต่อสัมพันธ์กับสังคม ซึ่งภายใต้แนวคิดนี้ข้อมูลใดก็ตามที่สามารถเก็บรักษาความลับเกี่ยวกับตัวบุคคลย่อมมีสิทธิได้รับการคุ้มครองตามกฎหมายจากการละเมิดโดยบุคคลอื่น[9] กล่าวคือนอกจากการคุ้มครองความเป็นส่วนตัวจากการกระทำของรัฐแล้ว บุคคลควรได้รับความคุ้มครองจากการกระทำที่เกิดจากเอกชนคนอื่นๆด้วย ไม่ว่าจะเป็นเพื่อนบ้าน นายจ้าง หรือแม้แต่นักหนังสือพิมพ์ก็ตาม[10] ความเป็นส่วนตัวจึงเป็นสิทธิของคนใดคนหนึ่งในส่วนที่มีลักษณะเฉพาะตัวบุคคลเพื่อป้องกันตัวเองออกจากสาธารณะชน บุคคลมีสิทธิที่จะปฏิเสธข้อมูลอันเป็นความลับของตนต่อสาธารณะได้ หรืออาจจำกัดความสามารถในการเข้าถึงข้อมูลที่เกี่ยวกับตนได้[11]

ด้วยเหตุนี้จึงอาจกล่าวได้ว่าแนวคิดด้านความเป็นส่วนตัวในช่วงศตวรรษที่ 19 มีการพัฒนาขึ้นโดยได้ยอมรับความเป็นส่วนตัวในฐานะเป็นสิทธิส่วนบุคคล (Personal Right) แต่อย่างไรก็ตามการดำเนินการให้ได้มาซึ่งสิทธิดังกล่าวยังคงตั้งอยู่บนพื้นฐานของการเก็บรักษาความลับ (secrecy paradism) ในเรื่องราวที่เกี่ยวกับชีวิตความเป็นส่วนตัวในทำนองเดียวกับแนวความคิดดั้งเดิมอยู่นั่นเอง

แต่ในสถานการณ์ปัจจุบันเทคโนโลยีเกี่ยวกับการติดต่อสื่อสารได้พัฒนาก้าวหน้าไปอย่างมาก การคุ้มครองความเป็นส่วนตัวโดยการเก็บข้อมูลที่เกี่ยวกับบุคคลไว้เป็นความลับอย่างเดียวนั้นไม่เพียงพออีกต่อไป เนื่องจากมีความจำเป็นในการเก็บรวบรวม การประมวลผลหรือใช้ข้อมูลที่เกี่ยวข้องกับบุคคลหนึ่งโดยบุคคลอื่นเพื่อประโยชน์ทางด้านเศรษฐกิจการค้า การแพทย์ การขนส่งระหว่างประเทศ ซึ่งการดำเนินการใดๆต่อข้อมูลดังกล่าวข้างต้นได้มีการเปลี่ยนแปลงรูปแบบจากเดิมที่ใช้ระบบกระดาษเป็นหลักไปสู่การใช้เทคโนโลยีคอมพิวเตอร์เข้ามาช่วยในการบริหารจัดการข้อมูล การประมวลผลข้อมูล ตลอดจนการส่งผ่านข้อมูลจากที่หนึ่งไปอีกที่หนึ่งได้อย่างรวดเร็ว เมื่อการส่งต่อข้อมูลทำได้อย่างรวดเร็ว[12] และส่งถึงกันได้อย่างง่ายดายขึ้น ทำให้แนวคิดในการคุ้มครองความเป็นส่วนตัวได้เปลี่ยนแปลงจากการมุ่งเน้นในการเก็บรักษาข้อมูลไว้เป็นความลับไปเป็นการมีความสามารถ

---

[9] ปฏิวัติ อุ่นเรือน, *อ้างแล้ว เชิงอรรถที่ 4*, น.8.

[10] กิตติพงศ์ กมลธรรมวงศ์, “การคุ้มครองข้อมูลข่าวสารส่วนบุคคล ในระบบกฎหมายไทย : ปัญหาและแนวทางแก้ไข,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2549), น.20.

[11] ศิริกุล ภู่พันธ์, *อ้างแล้ว เชิงอรรถที่ 1*, น.69.

[12] กิตติพงศ์ กมลธรรมวงศ์, *อ้างแล้ว เชิงอรรถที่ 10*, น.20.

ในการควบคุมการเปิดเผย (control of distribution) และการใช้ (use) ข้อมูลที่เกี่ยวข้องกับชีวิตมนุษย์เป็นสำคัญ[13]

แนวทฤษฎีการควบคุม (Control Theory) อยู่บนพื้นฐานแนวคิดที่ว่าบุคคลมีอิสระในการกำหนดชะตากรรมของตนเอง[14] การที่แต่ละคนจะสามารถมีอิสระในการกำหนดชะตากรรมของตัวเองได้อย่างแท้จริงก็ต่อเมื่อแต่ละคนมีแดนแห่งเสรีภาพ (sphere of individual liberty) ซึ่งภายในขอบเขตดังกล่าวนี้บุคคลย่อมมีอำนาจในการจะกำหนดชะตากรรมของตนเอง (self determination) โดยบุคคลย่อมมีอำนาจในการเลือกวิถีชีวิตของตนได้ด้วยตนเอง[15] กล่าวคือบุคคลย่อมมีอำนาจที่จะตัดสินใจได้ว่าในขณะใดที่เราต้องการแยกตัวออกจากผู้อื่นหรือออกจากสังคม ไม่ต้องการให้บุคคลใดเข้ามาร่วมในความเป็นส่วนตัวของเราได้ หรือจะเลือกอนุญาตให้บุคคลใดเข้ามาร่วมในความเป็นส่วนตัวของเราก็ได้ ดังนั้นการมีอิสระในการกำหนดชะตากรรมของตนเองคือการที่บุคคลสามารถวางกฎเกณฑ์ของตนเอง กำหนดชะตากรรมของตนเองโดยการมีอำนาจควบคุมสิ่งที่เกี่ยวกับตนเองได้

การคุ้มครองความเป็นส่วนตัวในยุคสมัยใหม่บนพื้นฐานของทฤษฎีการควบคุมมีหลักการสำคัญว่าบุคคลจะมีความเป็นส่วนตัวได้ก็ต่อเมื่อสามารถควบคุมข้อมูลข่าวสารเกี่ยวกับตัวเองได้ (one has privacy if and only if one has control over information about oneself) หรือสามารถควบคุมการเผยแพร่และใช้ข้อมูลโดยบุคคลอื่นที่เกี่ยวข้องกับชีวิตของตนเอง (control of distribution and use by other of knowledge regarding our life) ซึ่งคำจำกัดความที่มีชื่อเสียงและเป็นที่ยอมรับกันทั่วไปโดยการใช้ทฤษฎีควบคุมนี้ คือคำจำกัดความของอลัน เอฟ. เวสติน (Alan F. Westin) ที่ว่า ความเป็นส่วนตัวคืออำนาจในการกล่าวอ้างของปัจเจกชน คณะบุคคลที่จะตัดสินใจ

---

[13] ปฏิวัติ อุ่นเรือน, *อ้างแล้ว เชิงอรรถที่ 4*, น.10.

[14] Maurizio Passerin d' Entreves and Ursula Vogel Editor, Public and Private : Legal ,political and philosophical perspectives, (New York : Routledge, 2000), p.14 อ้างถึงใน ศิริกุล ภู่พันธ์, "ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล," (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), น.69.

[15] วรพจน์ วิศรุตพิชญ์, "สิทธิเสรีภาพตามรัฐธรรมนูญ (ศึกษารูปแบบการจำกัดสิทธิและเสรีภาพที่รัฐธรรมนูญให้ไว้อย่างเหมาะสม)", วารสารกฎหมายจุฬา, เล่มที่3, ปีที่17, น.7. อ้างถึงใน ศิริกุล ภู่พันธ์, "ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล," (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), น.70.

ว่า ข้อมูลที่เกี่ยวข้องกับตนเองนั้นจะถูกเปิดเผยไปยังบุคคลอื่นเมื่อใด อย่างไร และมากน้อยเพียงใด[16] โดยผู้เป็นเจ้าของข้อมูลมีสิทธิกำหนดว่าจะให้ใครเป็นผู้เข้าถึงข้อมูลของตนได้บ้าง อีกทั้งความสามารถในการตัดสินใจนี้ต้องเกิดจากการไม่ถูกฉ้อฉล หลอกลวง หรือไม่มีสติ คือบุคคลต้องสามารถคาดเดาได้ถึงผลที่จะเกิดขึ้นกับตนในอนาคตว่าหากตัดสินใจเช่นนั้นตนจะได้รับผลอย่างไร

แนวคิดการมีอิสระในการปกครองตนเองนั้นเป็นแนวทางที่พยายามแสดงให้เห็นว่าอำนาจบังคับหรือควบคุมตัวเองมีความสำคัญมาก บุคคลย่อมมีอำนาจในการตัดสินใจในเรื่องที่สำคัญต่อสิ่งที่จะเกิดขึ้นต่อไปในชีวิตของตน หรือสิ่งที่จะกระทบต่อสาระสำคัญที่เป็นมูลฐานรากเหง้าของความเป็นคน สิ่งนี้ฟรอยด์ (Freund) เรียกว่า “ความเป็นตัวตน” (Personhood) ซึ่งลักษณะประจำตัวของแต่ละปัจเจกบุคคลนั้นไม่สามารถลดหรือถูกแยกไปจากความเป็นคนของบุคคล (Selfhood) นั้นเองได้[17]

ในปัจจุบันนี้ หากจะสรุปแนวคิดเกี่ยวกับการคุ้มครองความเป็นส่วนตัวในปัจจุบัน จะสามารถจำแนกตามสภาพแห่งสิทธิความเป็นส่วนตัวที่ปรากฏออกมาให้เห็นภายนอกได้ โดยมีการจำแนกออกมาเป็น 4 แขนง ได้แก่[18]

(1) ความเป็นส่วนตัวในชีวิตร่างกาย (bodily privacy)

เป็นการให้ความคุ้มครองในชีวิตร่างกายของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใดๆ อันละเมิดความเป็นส่วนตัว อาทิ การทดลองทางพันธุกรรม (genetic tests) หรือการทดลองยา (drug testing) เป็นต้น

(2) ความเป็นส่วนตัวในการติดต่อสื่อสาร (communication privacy)

เป็นการให้ความคุ้มครองในความปลอดภัยและความเป็นส่วนตัวในการติดต่อสื่อสารที่ได้กระทำในรูปแบบต่างๆ เช่น ทางจดหมาย ทางโทรศัพท์ หรือวิธีการอื่นใดที่ผู้อื่นจะล่วงรู้มิได้

(3) ความเป็นส่วนตัวในดินแดนหรืออาณาเขต (territorial privacy)

เป็นการกำหนดขอบเขตหรือข้อจำกัดที่บุคคลอื่นจะบุกรุกเข้าไปในสถานที่ส่วนตัวมิได้ ทั้งนี้ รวมทั้งการติดกล้องวีดิโอ และการตรวจสอบรหัสประจำตัวบุคคล (ID checks)

---

[16] Alan F. Westin, Privacy and Freedom (New York : Atheneum, 1967), p.7. อ้างถึงใน ปฏิวัติ อุ่นเรือน, “ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ,” (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), น.10-11.

[17] ศิริกุล ภู่พันธ์, *อ้างแล้ว เชิงอรรถที่ 1*, น.71.

[18] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร : ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2547), น.17-19.

(4) ความเป็นส่วนตัวในข้อมูลข่าวสาร (information privacy)

เป็นการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล หรือเป็นที่รู้จักกันภายใต้คำว่า Data Protection

ทั้งนี้การศึกษาในสารนิพนธ์ของปฏิวัติ อุ่นเรือน[19]นั้น ได้ให้ความเห็นว่าความเป็นส่วนตัวโดยทั่วไปนั้นจะอยู่ภายใต้ทฤษฎีเกี่ยวกับการรักษาความลับ (Secrecy or Confidentiality Theory) และทฤษฎีการจำกัดการเข้าถึง (Restricted Access Theory) เป็นหลัก ในขณะที่ความเป็นส่วนตัวในข้อมูลข่าวสารนั้นจะต้องอาศัยหลักเกณฑ์ในการพิจารณาจากทฤษฎีควบคุมเพื่อให้สอดคล้องกับสภาพสังคมและเศรษฐกิจในปัจจุบันที่มีการใช้ประโยชน์จากข้อมูลส่วนบุคคลอย่างแพร่หลาย การเก็บรักษาข้อมูลส่วนบุคคลของตนเอาไว้เป็นความลับเพียงอย่างเดียวมิอาจกระทำได้อีกต่อไป การคุ้มครองความเป็นส่วนตัวในข้อมูลข่าวสารจึงมีลักษณะให้อำนาจบุคคลในการยินยอมให้มีการรวบรวมหรือประมวลผลข้อมูลเกี่ยวกับตนได้

ในปัจจุบันนี้ความเป็นส่วนตัวเป็น “สิทธิและเสรีภาพขั้นพื้นฐาน” (Fundamental Right and Liberty) ประการหนึ่งของมนุษย์ทุกคน โดยได้รับการรับรองและคุ้มครองในกฎหมายและกฎเกณฑ์ระหว่างประเทศด้านสิทธิมนุษยชนทั้งหลาย เช่น

ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights หรือ UDHR) ซึ่งเป็นกฎเกณฑ์พื้นฐานสากลเกี่ยวกับสิทธิมนุษยชน ได้มีการรับรองและคุ้มครองสิทธิในความเป็นส่วนตัวเอาไว้ในข้อ 12 ความว่า “บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศหรือชื่อเสียงมิได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงหรือการลบหลู่เช่นนั้น”[20]

อนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานแห่งยุโรป (European Convention for the Protection of Human Rights and Fundamental Freedom) ได้รับรองสิทธิที่จะได้รับการเคารพในชีวิตส่วนตัวและชีวิตครอบครัว (Right to respect for private and family life) โดยมีการกำหนดไว้ในข้อ 8 ของอนุสัญญาฯว่า “1.ทุกคนมีสิทธิที่จะได้รับการเคารพต่อชีวิตส่วนตัว ที่อยู่อาศัย และการสื่อสาร 2.จะต้องไม่มีการแทรกแซงโดยเจ้าหน้าที่

---

[19] ปฏิวัติ อุ่นเรือน, *อ้างแล้ว เชิงอรรถที่ 4*, น.10.

[20] Article 12 UDHR. “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” คำแปลปฏิญญาสากลว่าด้วยสิทธิมนุษยชน โปรดดู www.mfa.go.th/humanrights/images/stories/book.pdf.

ของรัฐในการใช้สิทธิดังกล่าว เว้นแต่ในกรณีเป็นไปตามกฎหมายและเป็นการจำเป็นในสังคมประชาธิปไตย เพื่อประโยชน์เกี่ยวกับความมั่นคงแห่งรัฐ ความปลอดภัยสาธารณะ หรือความมั่งคั่งทางเศรษฐกิจของประเทศ เพื่อป้องกันความไม่สงบเรียบร้อย หรือการกระทำความผิดอาญา เพื่อคุ้มครองสุขภาพหรือศีลธรรม หรือเพื่อคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น”[21] นอกจากนี้ในอนุสัญญาฯยังได้ให้การคุ้มครองสิทธิในการได้รับการเยียวยาอย่างแท้จริง (Right to an effective remedy) อีกด้วย โดยได้มีการกำหนดเอาไว้ในข้อ 13 ว่า “บุคคลซึ่งสิทธิและเสรีภาพตามที่กำหนดไว้ในอนุสัญญานี้ถูกละเมิด จะต้องได้รับการเยียวยาอย่างจริงจังโดยองค์กรของรัฐ แม้ว่าการละเมิดนั้นจะได้กระทำโดยผู้ซึ่งปฏิบัติหน้าที่ตามอำนาจหน้าที่ของตน”[22]

2.2 แนวคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของการคุ้มครองความเป็นส่วนตัว โดยแนวคิดในการคุ้มครองข้อมูลส่วนบุคคลได้มีการพัฒนาขึ้นโดยเริ่มจากภาคพื้นยุโรปเป็นที่แรก[23] ปัจจัยสำคัญที่ทำให้มีการพัฒนาหลักเกณฑ์ในเรื่องการคุ้มครองข้อมูลส่วนบุคคลอย่างจริงจังคือการถือว่าการคุ้มครองความเป็นส่วนตัวโดยการคุ้มครองข้อมูลส่วนบุคคลเป็นสิทธิมนุษยชนขั้นพื้นฐานของ

---

[21] Article 8 Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[22] Article 13 Right to an effective remedy

Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

[23] ปฏิวัติ อุ่นเรือน, *อ้างแล้ว เชิงอรรถที่ 4*, น.14.

ประชาชน[24] บุคคลจึงได้รับการคุ้มครองอย่างเสมอหน้ากัน ไม่จำกัดให้แก่เฉพาะบุคคลที่เป็นสมาชิกรัฐใดรัฐหนึ่งเท่านั้น ทั้งนี้เป็นเพราะว่าความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นสิ่งที่ติดตัวมากับความเป็นมนุษย์ กฎหมายเพียงแต่รับรองการมีอยู่หรือดำรงอยู่ตามธรรมชาติของสิทธินั้นเท่านั้น[25]

สิทธิเกี่ยวกับข้อมูลส่วนบุคคลเป็นสิทธิขั้นพื้นฐานที่ได้รับการรับรองและคุ้มครองโดยกฎหมายและกฎเกณฑ์ระหว่างประเทศ เป็นสิทธิที่จะต้องได้รับการเคารพจากบุคคลทั้งหลายในอันที่จะต้องไม่กระทำการใดๆที่เป็นการแทรกแซงและละเมิดสิทธินั้น ไม่ว่าจะโดยเจ้าหน้าที่ของรัฐหรือปัจเจกชนอื่น ในส่วนของภาครัฐเองนั้นนอกจากจะต้องไม่กระทำการใดๆที่เป็นการแทรกแซงหรือละเมิดสิทธิในข้อมูลส่วนบุคคลของบุคคลทั้งหลายแล้ว รัฐหรือองค์กรของรัฐยังมีหน้าที่ในการกำหนดกลไกหรือมาตรการทางกฎหมายเพื่อให้ความคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคล อันเป็นหน้าที่กระทำการของรัฐอีกด้วย[26]

อย่างไรก็ตามสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้นมิใช่สิทธิเด็ดขาด อาจมีบางกรณีที่รัฐสามารถกำหนดมาตรการหรือการกระทำบางอย่างอันมีผลเป็นการแทรกแซงสิทธิในข้อมูลส่วนบุคคลได้เช่นกัน โดยรัฐจะแทรกแซงสิทธิของบุคคลได้ก็ต่อเมื่อปฏิบัติตามเงื่อนไขที่กำหนดไว้ในกฎหมายหรือกฎเกณฑ์ระหว่างประเทศด้านสิทธิมนุษยชนโดยเคร่งครัด ซึ่งตั้งอยู่บนหลักการพื้นฐานสำคัญสามประการคือ[27]

(1) หลักความโปร่งใส (transparency) รัฐหรือองค์กรของรัฐจะดำเนินมาตรการใดๆอันมีผลเป็นการแทรกแซงสิทธิเกี่ยวกับข้อมูลส่วนบุคคลได้ก็ต่อเมื่อมีกฎหมายบัญญัติให้กระทำได้ เพื่อให้บุคคลทั้งหลายสามารถรับทราบได้ล่วงหน้าว่าในสถานการณ์เช่นใดที่ข้อมูลส่วนบุคคลของตนอาจจะถูกแทรกแซงโดยองค์กรของรัฐหรือเจ้าหน้าที่ของรัฐ และการดำเนินการเช่นนั้นจะต้องเป็นไปภายใต้หลักเกณฑ์และเงื่อนไขอย่างไร

(2) หลักประโยชน์สาธารณะ (public Interest) การที่รัฐหรือองค์กรของรัฐจะใช้มาตรการอันมีผลเป็นการแทรกแซงสิทธิเกี่ยวกับข้อมูลส่วนบุคคลได้นั้นจะต้องเป็นไปเพื่อประโยชน์สาธารณะ เกี่ยวกับความมั่นคงแห่งรัฐ ความปลอดภัยสาธารณะ ความมั่งคั่งทางเศรษฐกิจของประเทศ เพื่อดูแลความสงบเรียบร้อยหรือการกระทำความผิดอาญา เพื่อคุ้มครองสุขภาพหรือศีลธรรม หรือเพื่อ

---

[24] อนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานแห่งยุโรป ข้อที่ 8

[25] นนทวัชร์ นวตระกูลพิสุทธิ์, “สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล กับมาตรการคุ้มครองตาม ร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...,” วารสารนิติศาสตร์, ปีที่ 43 ฉบับที่ 4, น.740 (ธันวาคม 2557).

[26] *เพิ่งอ้าง*, น.740.

[27] *เพิ่งอ้าง*, น.742.

คุ้มครองสิทธิและเสรีภาพของบุคคลอื่น กล่าวอีกนัยหนึ่งคือในสถานการณ์นั้นประโยชน์ของสาธารณะมีสถานะเหนือกว่าประโยชน์ส่วนตัวของบุคคล

(3) หลักความจำเป็นและความได้สัดส่วน (necessity and proportionality) มาตรการของรัฐหรือองค์กรของรัฐที่จะดำเนินการและมีผลเป็นการแทรกแซงสิทธิเกี่ยวกับข้อมูลส่วนบุคคลจะต้องเป็นสิ่งจำเป็นในสังคมประชาธิปไตย เพื่อบรรลุวัตถุประสงค์อันเป็นประโยชน์สาธารณะเช่นนั้น และจะต้องได้สัดส่วนกับผลกระทบที่จะเกิดขึ้นจากการดำเนินมาตรการดังกล่าวของรัฐด้วย อีกทั้งต้องมีมาตรการเยียวยาความเสียหายแก่บุคคลนั้นในกรณีที่เกิดความเสียหายจากการแทรกแซงสิทธิด้วย

ทั้งนี้รัฐหรือองค์กรของรัฐจะสามารถดำเนินการใดๆที่มีผลเป็นการแทรกแซงสิทธิหรือละเมิดสิทธิของบุคคลได้ก็ต่อเมื่อปฏิบัติตามเงื่อนไขข้างต้นโดยเคร่งครัดเท่านั้น โดยมาตรการแทรกแซงสิทธิอันเป็นข้อยกเว้นนั้นจำกัดอยู่เฉพาะกรณีที่กระทำโดยรัฐหรือองค์กรของรัฐซึ่งจะต้องเป็นไปตามหลักการและเงื่อนไขที่กฎหมายและกฎเกณฑ์ระหว่างประเทศด้านสิทธิมนุษยชนกำหนดไว้อีกด้วย

ส่วนปัจเจกชนหรือเอกชนด้วยกันเองนั้นมิอาจยกประโยชน์สาธารณะขึ้นมาเป็นข้ออ้างในการกระทำการใดๆอันจะมีผลเป็นการแทรกแซงหรือละเมิดสิทธิของบุคคลอื่นได้ เนื่องจากบุคคลทุกคนย่อมเสมอภาคกันในกฎหมายและได้รับความคุ้มครองตามกฎหมายเท่าเทียมกัน อย่างไรก็ตามถ้าบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้นได้ให้ความยินยอมโดยสมัครใจ ก็จะมีผลทำให้บุคคลอื่นสามารถแทรกแซงหรือใช้ข้อมูลของเจ้าของข้อมูลส่วนบุคคลได้

ในปัจจุบันนี้หลักการคุ้มครองข้อมูลส่วนบุคคลได้มีการบัญญัติเอาไว้ในอนุสัญญาต่างๆ เช่นอนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานแห่งยุโรป ในปี ค.ศ. 1950 ตลอดจนกฎบัตรสิทธิขั้นพื้นฐานแห่งสหภาพยุโรป (Charter of Fundamental Rights of the European Union) โดยในข้อ 8 ของกฎบัตรนั้นได้บัญญัติให้การคุ้มครองข้อมูลส่วนบุคคลเอาไว้อย่างชัดเจนว่า

(1) บุคคลทุกคนมีสิทธิที่จะได้รับการคุ้มครองในข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเอง

(2) การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปด้วยความยุติธรรม (fairly) ภายใต้วัตถุประสงค์ที่เฉพาะเจาะจง (specified) บนพื้นฐานของการให้ความยินยอมจากบุคคลที่เกี่ยวข้องกับข้อมูลดังกล่าว หรือภายใต้ขอบวัตถุประสงค์อื่นตามที่กฎหมายบัญญัติ นอกจากนี้บุคคลทุกคนยังมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับตนที่ได้มีการเก็บรวบรวมไว้ และมีสิทธิในการร้องขอให้มีการแก้ไขข้อมูลดังกล่าวให้ถูกต้อง

(3) ในการบังคับการให้เป็นไปตามหลักการคุ้มครองข้อมูลส่วนบุคคลข้างต้นจะต้องจัดให้มีการควบคุมการปฏิบัติดังกล่าวโดยองค์กรของรัฐที่เป็นอิสระ (Independent Authority)

แม้ว่าในปัจจุบันสิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคลจะมีการรับรองในกฎเกณฑ์ระหว่างประเทศด้านสิทธิมนุษยชน และนานาประเทศก็ได้ให้ความสำคัญกับการกำหนดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลในประเทศของตน แต่อย่างไรก็ตามด้วยแนวคิดพื้นฐานในนิติวิธีของแต่ละประเทศมีความแตกต่างกัน ทำให้แต่ละประเทศกำหนดรูปแบบและมาตรการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกันตามไปด้วย โดยสามารถจำแนกรูปแบบการคุ้มครองข้อมูลส่วนบุคคลในปัจจุบันที่ใช้ในประเทศต่างๆ ออกเป็น 3 รูปแบบที่สำคัญดังนี้

2.2.1 การคุ้มครองข้อมูลส่วนบุคคลโดยการบัญญัติเป็นกฎหมาย ซึ่งแบ่งเป็น 2 ลักษณะคือ

2.2.1.1 การคุ้มครองข้อมูลส่วนบุคคลโดยการบัญญัติเป็นกฎหมายกลางหรือกฎหมายทั่วไป (Comprehensive Law)

การคุ้มครองข้อมูลส่วนบุคคลในลักษณะนี้จะรวบรวมเอาหลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลมาบัญญัติเป็นกฎหมายเพียงฉบับเดียวที่ครอบคลุมการคุ้มครองข้อมูลส่วนบุคคลในทุกเรื่อง ทุกกิจกรรม ไม่เจาะจงข้อมูลส่วนบุคคลประเภทใดประเภทหนึ่ง ซึ่งแนวทางการตรากฎหมายเช่นนี้ส่วนใหญ่จะบังคับใช้ในประเทศภาคพื้นยุโรป สหราชอาณาจักรและประเทศที่ใช้ระบบประมวลกฎหมาย (Civil Law) ได้แก่สวีเดน เยอรมนี ฝรั่งเศส เป็นต้น[28]

การบัญญัติการคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายกลางนั้นเป็นการให้หลักประกันขั้นต่ำที่สุด ดังนั้นหากมีหลักเกณฑ์ทางกฎหมายเฉพาะใดหรือหน่วยงานใดให้การคุ้มครองข้อมูลส่วนบุคคลได้มากกว่าก็ย่อมบังคับใช้กฎหมายนั้นแทนได้ แต่ในทางกลับกันถ้าหากหลักเกณฑ์ของกฎหมายเฉพาะใดให้ความคุ้มครองข้อมูลส่วนบุคคลต่ำกว่ากฎหมายกลาง ก็ต้องบังคับใช้กฎหมายกลางแทน[29]

การบัญญัติกฎหมายกลางที่ใช้คุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปนั้นเกิดขึ้นครั้งแรกในภาคพื้นยุโรป โดยบัญญัติเป็นกฎหมายระดับมลรัฐที่รัฐเฮสเซน (Hessen) ซึ่งเป็นรัฐหนึ่งของประเทศสหพันธ์สาธารณรัฐเยอรมนี เมื่อปี ค.ศ. 1970 ซึ่งถือเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกของโลก หลังจากนั้นจึงได้มีการบัญญัติกฎหมายระดับสหพันธรัฐเยอรมนีขึ้นในปี ค.ศ. 1977 จากแนวคิดของการบัญญัติกฎหมายกลางขึ้นมาเพื่อใช้คุ้มครองข้อมูลส่วนบุคคลนี้ได้กลาย

---

[28] กิตติพงศ์ กมลธรรมวงศ์, *อ้างแล้ว เชิงอรรถที่ 10*, น.79.

[29] จันทจิรา เอี่ยมมยุรา, “แนวคิดและหลักการยกร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย,” วารสารนิติศาสตร์, ปีที่ 34, ฉบับที่ 4, น.658 (ธันวาคม 2547).

มาเป็นต้นแบบให้อีกหลายประเทศบัญญัติกฎหมายลักษณะเดียวกันนี้ เช่น ประเทศสวีเดนในปี ค.ศ. 1973 ประเทศสหรัฐอเมริกาในปี ค.ศ. 1974 และประเทศฝรั่งเศสในปี ค.ศ. 1978 เป็นต้น[30]

ในระยะแรกนั้นกฎหมายส่วนใหญ่ที่บัญญัติขึ้นล้วนมีวัตถุประสงค์เพื่อควบคุมการประมวลผลข้อมูล โดยเฉพาะอย่างยิ่งการประมวลผลโดยหน่วยงานที่ให้บริการทางด้านสวัสดิการสังคม ซึ่งได้เน้นไปที่การใช้ระบบการให้อนุญาต (licensing) และจดทะเบียน (registration) เพื่อควบคุมการประมวลผลข้อมูลโดยใช้เครื่องคอมพิวเตอร์เป็นหลัก ต่อมาหลังจากที่เทคโนโลยีการใช้งานคอมพิวเตอร์เริ่มแพร่หลายมากขึ้นในช่วงปี ค.ศ. 1980 ทำให้เนื้อหาในการคุ้มครองข้อมูลส่วนบุคคลได้พัฒนาขึ้นโดยให้มีการคำนึงถึงสิทธิในข้อมูลของประชาชนเพิ่มมากขึ้น โดยเน้นไปที่การควบคุมการรวบรวมข้อมูล (collection) การเก็บ (storage) การใช้ (use) และการโอนข้อมูล (transfer) เป็นสำคัญ[31]

โดยทั่วไปนั้นการบัญญัติเนื้อหาของกฎหมายกลางมักจะครอบคลุมหลักการที่จำเป็นและเพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคล ซึ่งประกอบด้วย 3 ส่วนหลัก คือ (1) หลักการสารบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (2) องค์กรหรือหน่วยงานที่ทำหน้าที่กำกับดูแลการประมวลผลข้อมูลและ/หรือทำหน้าที่วินิจฉัยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล (3) การกำหนดให้หน่วยงานที่ทำหน้าที่ประมวลผลข้อมูลต้องแต่งตั้งนายทะเบียนผู้รับผิดชอบโดยเฉพาะ[32]

ในส่วนของการจัดตั้งองค์กรหรือหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Authority) มีความจำเป็นเพื่อให้การบังคับใช้กฎหมายกลางมีประสิทธิภาพ โดยบทบาทขององค์กรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะมีการดำเนินงานแบ่งได้เป็น 2 ลักษณะ คือ[33]

(1) องค์กรที่ทำหน้าที่กำกับดูแล (Regulatory Body)

ประเทศที่จัดตั้งองค์กรในลักษณะเช่นนี้ ได้แก่ ประเทศสวีเดน และประเทศฝรั่งเศส ในกรณีของประเทศสวีเดนนั้นได้จัดตั้ง Data Inspection Board and National

---

[30] Victor Mayer-Schonberger, “Generational Development of Data Protection in Europe,” in Technology and Privacy : The New Landscape, ed. P. Agre. And M. Rotenberg, (Cambridge : The MIT Press,1997) ,pp. 219-242 อ้างถึงใน ปฏิวัติ อุ่นเรือน, “ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ,” (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), น.15.

[31] ปฏิวัติ อุ่นเรือน, *อ้างแล้ว เชิงอรรถที่ 4*, น.15.

[32] จันทจิรา เอี่ยมมยุรา, *อ้างแล้ว เชิงอรรถที่ 29*, น.658.

[33] ปฏิวัติ อุ่นเรือน, *อ้างแล้ว เชิงอรรถที่ 4*, น.16.

Commission on Informatics and Liberties ซึ่งมีบทบาทค่อนข้างกว้างในการกำกับดูแลการประมวลผลข้อมูลในประเทศ เช่น อำนาจในการอนุญาตหรือไม่อนุญาตให้มีการประมวลผลข้อมูลทั้งโดยหน่วยงานของรัฐและหน่วยงานเอกชน ส่วนในประเทศฝรั่งเศสได้มีการจัดตั้ง Commission nationale de l'informatique et des libertés (CNIL) ซึ่งมีบทบาทในทำนองเดียวกับประเทศสวีเดน แต่จะแตกต่างกันตรงที่มีการจัดตั้งอนุกรรมการ (submissions) ขึ้นเพื่อทำหน้าที่ศึกษาวิจัยเกี่ยวกับข้อมูลทางสถิติ การประมวลผลโดยหน่วยงานของรัฐส่วนท้องถิ่นด้านเทคโนโลยีและการรักษาความปลอดภัยขึ้นเป็นการเฉพาะด้วย

อย่างไรก็ตามการจัดให้มีองค์กรที่มีโครงสร้างการทำงานเป็นอิสระและมีอำนาจที่กว้างขวางดังเช่นที่ใช้ในประเทศสวีเดนและประเทศฝรั่งเศส ก็หาได้มีผลทำให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพแต่อย่างใด เนื่องจากองค์กรนั้นได้รับงบประมาณอย่างจำกัด ในขณะที่มีภาระหน้าที่ที่ต้องรับผิดชอบอยู่เป็นอันมาก ไม่ว่าจะเป็นการจดทะเบียนหน่วยงานที่ทำการประมวลผลข้อมูล การไต่สวนข้อร้องเรียน การประชาสัมพันธ์ให้ประชาชนเข้าใจเกี่ยวกับหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลเป็นต้น

(2) องค์กรที่ทำหน้าที่ให้คำปรึกษา (Advisory Body)

ประเทศที่ได้จัดตั้งองค์กรในลักษณะนี้ได้แก่ ประเทศเยอรมนี ซึ่งได้มีการจัดตั้งกรรมการคุ้มครองข้อมูลส่วนบุคคล (Federal Data Protection Commissioner) ขึ้นเป็นองค์กรหนึ่งในกระทรวงมหาดไทย (Ministry of the Interior) และอยู่ภายใต้การกำกับดูแลของรัฐมนตรีว่าการกระทรวงมหาดไทย

กรรมการคุ้มครองข้อมูลส่วนบุคคลมีหน้าที่หลักในการให้คำปรึกษา ให้ความช่วยเหลือ และว่ากล่าวตักเตือนหน่วยงานต่างๆ ในกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูล นอกจากนี้กรรมการดังกล่าวยังสามารถยื่นคำตำหนิอย่างเป็นทางการ (formal complaints) เกี่ยวกับการประมวลผลข้อมูลที่เห็นว่าไม่ถูกต้องไปยังกระทรวงซึ่งมีหน้าที่รับผิดชอบ แต่ไม่มีอำนาจในการออกคำสั่งหรือให้ดำเนินการอย่างหนึ่งอย่างใดโดยอาศัยอำนาจของกรรมการเอง

ต่อมาประเทศอื่นๆที่บัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นมาภายหลังก็ได้พัฒนารูปแบบขององค์กรหรือหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลในลักษณะที่ผสมผสานกันระหว่างหลักการกำกับดูแลที่ใช้อยู่ในประเทศสวีเดนและประเทศฝรั่งเศส และหลักการให้คำปรึกษาที่ใช้อยู่ในประเทศเยอรมนี ด้วยเหตุนี้เองจึงทำให้ระบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภาคพื้นยุโรปในช่วงต้นนั้นมีความแตกต่างหลากหลายค่อนข้างมาก

ต่อมาภายหลังประเทศต่างๆในภาคพื้นยุโรปก็ได้บัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีความสอดคล้องและไปในทิศทางเดียวกันมากขึ้น เนื่องจากได้มีการพัฒนากรอบนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในระดับสากลโดยองค์การระหว่างประเทศต่างๆ

รวมทั้งการบัญญัติ Directive 95/46/EC เพื่อคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศสมาชิกสหภาพยุโรป ซึ่งส่งผลให้ประเทศในกลุ่มสหภาพยุโรปต้องบัญญัติกฎหมายภายในเพื่อคุ้มครองข้อมูลส่วนบุคคลให้ได้มาตรฐานและเป็นไปในแนวทางเดียวกัน

2.2.1.2 การคุ้มครองข้อมูลส่วนบุคคลโดยการบัญญัติกฎหมายเป็นการเฉพาะ (Sectorial Law)

ลักษณะสำคัญของการคุ้มครองข้อมูลส่วนบุคคลโดยการบัญญัติกฎหมายเป็นการเฉพาะคือการบัญญัติกฎหมายขึ้นมาเพื่อคุ้มครองข้อมูลส่วนบุคคลในแต่ละเรื่องเป็นการเฉพาะ ประเทศที่ใช้การคุ้มครองข้อมูลส่วนบุคคลลักษณะนี้ได้แก่ประเทศสหรัฐอเมริกา ที่แม้จะมีการบังคับใช้กฎหมายคุ้มครองสิทธิส่วนบุคคล (Privacy Act 1974) ซึ่งเป็นกฎหมายหลักคุ้มครองอยู่แล้วก็ตาม แต่รัฐสภาจะตรากฎหมายเฉพาะออกมาเมื่อเกิดปัญหาการป้องกันความลับหรือความเป็นส่วนตัวของประชาชนถูกละเมิดขึ้น รัฐสภาก็จะตรากฎหมายเกี่ยวกับเรื่องนั้นๆออกมาเพื่อแก้ไขปัญหา เช่น[34]

กรณีการบัญญัติกฎหมายคุ้มครองความเป็นส่วนตัวของผู้ขับขี่ (The Driver Privacy Protection Act) เนื่องจากว่านักแสดงหญิงชื่อว่ารีเบ็กก้า เชฟเฟอร์ (Rebecca Shaeffer) ได้ถูกฆาตกรรมที่บ้านของเธอเองเมื่อปี ค.ศ. 1988 ซึ่งคนร้ายสามารถสืบหาที่อยู่ของเธอได้โดยการหาข้อมูลในใบขับขี่ของเธอจากแผนกยานยนต์แห่งรัฐแคลิฟอร์เนีย (California Department of Motor Vehicles)

กรณีการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการเงิน เหตุเกิดจากมีบริษัทเอกชนที่ชื่อว่า U.S. Bankcorp ได้เปิดเผยบัญชีของลูกค้าแก่บุคคลภายนอกซึ่งเป็นบุคคลที่สามโดยปราศจากความยินยอมของลูกค้า จึงต้องมีการบัญญัติกฎหมายว่าด้วยนวัตกรรมทางการเงิน (Gramm-Leach-Bliley Financial Modernization Act 1999) เพื่อให้สถาบันการเงินต่างๆเพิ่มระดับการคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคในกิจกรรมที่เกี่ยวข้องกับการเงินเพิ่มมากขึ้น เช่น การประกาศนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลให้ลูกค้าทราบ และเพิ่มหน้าที่ในการปฏิบัติตามข้อเรียกร้องของผู้บริโภคที่เกี่ยวกับข้อมูลส่วนบุคคล เป็นต้น

นอกเหนือจากกฎหมายที่ยกขึ้นมาข้างต้นแล้ว ยังมีกฎหมายเฉพาะอื่นๆ อีกมากที่บัญญัติขึ้นในประเทศสหรัฐอเมริกา เช่น กฎหมายว่าด้วยการรายงานข้อมูลผู้บริโภคที่เป็นธรรม (Fair Credit Reporting Act 1970) ซึ่งเป็นกฎหมายที่มีวัตถุประสงค์เพื่อควบคุมการใช้ข้อมูลเครดิตโดยภาคธุรกิจ, กฎหมายว่าด้วยการโอนถ่ายความรับผิดด้านการประกันสุขภาพ (Health Insurance Portability and Accountability Act 1996) ซึ่งบัญญัติขึ้นเพื่อคุ้มครองข้อมูลส่วนบุคคล

---

[34] ประสิทธิ์ ปิวาวัฒนพานิช, “กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย,” วารสารนิติศาสตร์, ปีที่ 34, ฉบับที่ 4, น.537-538 (2547).

ที่เกี่ยวข้องกับการรักษาพยาบาล, กฎหมายคุ้มครองข้อมูลส่วนบุคคลทางอินเทอร์เน็ตของเด็ก (Children's Online Privacy Protection Act 1998) ซึ่งเป็นกฎหมายที่มีวัตถุประสงค์ห้ามไม่ให้ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์และบริการออนไลน์แบบต่างๆ ทำการเก็บรวบรวมข้อมูลจากผู้เยี่ยมชมเว็บไซต์ (website) หรือผู้ใช้บริการที่เป็นเด็กอายุต่ำกว่า 13 ปี เป็นต้น

เหตุผลสำคัญที่อยู่เบื้องหลังการเลือกวิธีการคุ้มครองข้อมูลส่วนบุคคลโดยการบัญญัติไว้เป็นกฎหมายเฉพาะของประเทศสหรัฐอเมริกาคือ ต้องการให้มีกฎหมายที่สามารถปรับเปลี่ยนให้ทันกับเทคโนโลยีที่เปลี่ยนแปลงไปตลอดเวลา[35] นอกจากนี้ยังมีการวิเคราะห์โดยประสิทธิ์ ปิวาวัฒนาพานิช[36] ที่ว่าอาจมีเหตุผลจากปรัชญาหรือที่มาทางประประวัติศาสตร์สร้างชาติของประเทศสหรัฐอเมริกาที่พยายามจะมิให้เจ้าหน้าที่ของรัฐลิดรอนสิทธิเสรีภาพของประชาชน ในขณะเดียวกันประชาชนก็มีสิทธิเสรีภาพที่จะดำเนินธุรกิจแบบทุนนิยมหรือธุรกิจแบบเสรี (free enterprise) อันเป็นปรัชญาที่ชาวอเมริกันยึดถือมานาน โดยทั่วไปแล้วประเทศสหรัฐอเมริกาไม่มีกฎหมายที่กำหนดให้ประชาชนต้องให้ความยินยอมในเรื่องของการประมวลผลข้อมูล การจัดทำการตลาดและการขายข้อมูลส่วนบุคคลให้กับบุคคลที่สาม จึงจะเห็นได้ว่าประเทศสหรัฐอเมริกามีบริษัทเอกชนขนาดใหญ่หลายแห่งที่ทำธุรกิจเกี่ยวกับการจัดเก็บและขายข้อมูลส่วนบุคคลของชาวอเมริกัน เช่นบริษัท Catalina Marketing Corporation, บริษัท Aristotle Industries, บริษัท Winland Services เป็นต้น

ทั้งนี้ในบางประเทศนั้นก็เลือกมาตรการในการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะเพื่อขยายความหรือให้รายละเอียดเพิ่มเติมจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ใช้เป็นการทั่วไป โดยจำแนกตามประเภทของข้อมูล เช่น ข้อมูลเครดิต ข้อมูลที่จัดเก็บโดยหน่วยงานภาครัฐ[37]

---

[35] Electronic Privacy Information Center, "Privacy & Human Rights 2003 : An International Survey of Privacy Laws and Developments", Retrieved from http://www.privacyinternational.org/survey/phr2003/. อ้างถึงใน ปฏิวัติ อุ่นเรือน, "ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ," (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), น.23.

[36] ประสิทธิ์ ปิวาวัฒนพานิช, *อ้างแล้ว เชิงอรรถที่ 34*, น.537-538.

[37] Electronic Privacy Information Center, *supra note* 35.

2.2.2 การคุ้มครองข้อมูลส่วนบุคคลโดยการใช้กลไกการกำกับดูแลตนเอง (Self-Regulation)

กลไกการกำกับดูแลตนเองเป็นรูปแบบหนึ่งของการคุ้มครองข้อมูลส่วนบุคคลในยุคปัจจุบันที่นำมาใช้เพื่อคลายความเข้มงวดหรือความเคร่งครัดของกฎหมายที่ออกโดยรัฐ เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลโดยการบัญญัติเป็นกฎหมายนั้นมีความยืดหยุ่นต่ำและใช้ระยะเวลานานในการบัญญัติและตราออกมาบังคับใช้จึงไม่ทันต่อการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีการสื่อสาร กลไกการกำกับดูแลตนเองจึงถูกนำมาใช้เพื่อแก้ปัญหาดังกล่าว โดยการให้หน่วยงานและองค์กรภาคเอกชนต่างๆสามารถวางหลักเกณฑ์ข้อปฏิบัติขึ้นมาเพื่อใช้ดำเนินงานภายในหน่วยงานและยอมตนที่จะปฏิบัติตามกฎเกณฑ์ที่สร้างขึ้นมาเองนั้น หลักเกณฑ์ปฏิบัติดังกล่าวจึงมีความยืดหยุ่นสามารถแก้ปัญหาได้อย่างทันท่วงทีและสอดคล้องกับแนวทางการดำเนินงานในหน่วยงาน นอกจากนี้การใช้กลไกการกำกับดูแลตนเองยังมีข้อดีในด้านการประหยัดต้นทุนในการผลิตหรือการให้บริการที่เกิดขึ้นอันเนื่องมาจากการเปลี่ยนแปลงกฎหมายหรือกฎเกณฑ์ที่ออกโดยรัฐได้อีกด้วย[38]

การคุ้มครองข้อมูลส่วนบุคคลโดยใช้กลไกการกำกับดูแลตนเองสามารถกระทำได้หลายรูปแบบ เช่น การที่กลุ่มผู้ประกอบวิชาชีพหรือกลุ่มผู้ประกอบธุรกิจในสาขาเดียวกันได้ร่วมกันจัดทำประมวลแนวปฏิบัติ (code of practice) เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยถือว่าประมวลแนวปฏิบัติดังกล่าวเป็นส่วนหนึ่งของนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบวิชาชีพหรือองค์กรที่ร่วมเป็นสมาชิกจำเป็นต้องปฏิบัติตาม โดยการออกประมวลแนวปฏิบัตินี้เป็นไปเพื่อให้มีการปฏิบัติตามมาตรฐานวิชาชีพหรือควบคุมตามจรรยาบรรณวิชาชีพ[39] หรือการจัดทำแนวนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล (privacy policy) ซึ่งเป็นกรณีที่องค์กรใดองค์กรหนึ่งได้ประกาศให้สาธารณชนได้รับทราบว่าองค์กรนั้นๆมีแนวนโยบายในการปฏิบัติต่อข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการไปในทางใดบ้าง มีวิธีการคุ้มครอง รักษาความลับและดำเนินการด้านความปลอดภัยต่อข้อมูลส่วนบุคคลอย่างไร เพื่อทำให้ผู้ใช้บริการเกิดความเชื่อมั่นในความปลอดภัยของข้อมูลส่วนบุคคลที่ถูกดำเนินการโดยองค์กรนั้นๆ

---

[38] ธนัท สุวรรณปริญญา, “ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ : กรณีศึกษาการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของธนาคาร สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ, 2550), น.22-23.

[39] กองบรรณาธิการเว็บไซต์สมาคมนักข่าวนักหนังสือพิมพ์แห่งประเทศไทย, “การปฏิรูปสื่อ,” สืบค้นเมื่อวันที่ 10 มีนาคม 2559, จาก http://www.tja.or.th.

กลไกการกำกับดูแลตนเองเป็นรูปแบบการคุ้มครองข้อมูลส่วนบุคคลที่ตั้งอยู่บนพื้นฐานของความสมัครใจ (voluntary) ต่างจากการรูปแบบการคุ้มครองโดยการบังคับใช้กฎหมายที่มีความเคร่งครัดและมีอำนาจบังคับลงโทษผู้ที่ไม่ปฏิบัติตามหรือละเมิดสิทธิในข้อมูลส่วนบุคคล[40] ซึ่งพื้นฐานความสมัครใจนั้นเองกลายเป็นจุดอ่อนสำคัญของกลไกการกำกับดูแลตนเอง เนื่องจากกลไกนี้มิใช่กฎหมายจึงขาดประสิทธิภาพในการควบคุมและลงโทษในกรณีที่ไม่ได้ปฏิบัติตามกลไกดังกล่าว เช่น การที่องค์กรเอกชนสามารถกำหนดนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลขึ้นมาเอง องค์กรนโยบายที่กำหนดนั้นอาจมุ่งเน้นเพียงประกาศให้ผู้ใช้บริการเกิดความเชื่อถือแต่มิสามารถดำเนินการได้จริงในทางปฏิบัติ อีกทั้งการปฏิบัติต่อข้อมูลส่วนบุคคลนั้นไม่มีการตรวจสอบและควบคุมโดยภาครัฐ ในบางกรณีจึงเป็นเพียงการที่องค์กรภาคเอกชนสร้างกลไกนี้ขึ้นเพื่อรักษาผลประโยชน์ในการดำเนินกิจการขององค์กรเองเท่านั้น แต่มิได้คำนึงถึงสิทธิของบุคคลหรือประโยชน์สาธารณะอย่างแท้จริง[41]

จากปัญหาของรูปแบบกลไกการกำกับดูแลตนเองทำให้เกิดการพัฒนาไปสู่รูปแบบการคุ้มครองข้อมูลส่วนบุคคลอีกแบบหนึ่งซึ่งเรียกว่าการกำกับดูแลร่วมกัน (Co-Regulation) เพื่อเพิ่มระดับในการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพและมีสภาพบังคับมากยิ่งขึ้น

2.2.3 การคุ้มครองข้อมูลส่วนบุคคลโดยการใช้กลไกการกำกับดูแลร่วมกัน (Co-Regulation)

การใช้กลไกการกำกับดูแลร่วมกันเป็นรูปแบบการคุ้มครองข้อมูลส่วนบุคคลโดยผสมผสานองค์ประกอบของการควบคุมโดยภาครัฐและการกำกับดูแลตนเองในภาคเอกชนเข้าด้วยกัน[42] ซึ่งการกำกับดูแลร่วมกันกระทำได้โดยให้ผู้ประกอบกิจการหรือภาคเอกชนกับองค์กรในภาครัฐร่วมกันกำหนดหลักเกณฑ์และข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลขึ้น หรือการที่องค์กรของรัฐได้กำหนดกฎเกณฑ์แนวปฏิบัติขึ้นมาและให้ผู้ประกอบการภาคเอกชนเข้าร่วมและปฏิบัติตาม

---

[40] คณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ, “รายงานการอบรมหลักสูตร Broadcasting Regulation,” ในการอบรมหลักสูตรทางวิชาการ 30 มิถุนายน – 4 กรกฎาคม 2557 โดย Thomson Foundation ณ กรุงลอนดอน สหราชอาณาจักร, 2557 : น.3-4.

[41] *เพิ่งอ้าง*, น.4.

[42] *เพิ่งอ้าง*, น.3-5.

แนวปฏิบัติที่รัฐกำหนดขึ้น ซึ่งหลักเกณฑ์ที่ได้กำหนดขึ้นนั้นจะมีมาตรการในการควบคุม (controlling) หรือบังคับ (enforcing) ให้ผู้ประกอบการต้องปฏิบัติตาม[43]

กลไกการกำกับดูแลร่วมกันเป็นการพัฒนารูปแบบการคุ้มครองข้อมูลส่วนบุคคล โดยการเปิดพื้นที่ให้ผู้มีส่วนได้เสียเข้ามามีส่วนร่วมในการวางหลักเกณฑ์ บริหารและจัดการกับปัญหาได้มากกว่ารูปแบบการบังคับใช้กฎหมาย กลไกนี้ได้มีการถ่ายโอนอำนาจบางส่วนให้องค์กรภาคเอกชนและภาควิชาชีพสร้างกลไกในการกำกับดูแลตนเองได้ โดยมีหน่วยงานภาครัฐเป็นอำนาจสุดท้ายในการควบคุมกลไกให้ดำเนินไปในทิศทางที่ตรงกับเป้าหมายเชิงนโยบาย หรือในบางกรณีภาครัฐอาจใช้อำนาจในการกำหนดแนวทางการจัดทำหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลขึ้นมาให้องค์กรเอกชนได้ปฏิบัติโดยภาครัฐมีอำนาจในการเฝ้าตรวจสอบการดำเนินงานขององค์กรนั้นๆ รวมถึงมีอำนาจในการลงโทษในกรณีที่กลไกการกำกับดูแลตนเองไม่สัมฤทธิ์ผล รูปแบบการกำกับดูแลร่วมกันจึงเป็นการสร้างกลไกในการคุ้มครองข้อมูลส่วนบุคคลสองระดับ คือการกำกับดูแลขั้นแรกโดยองค์กรภาคเอกชนและภาควิชาชีพและขั้นที่สองโดยการกำกับดูแลของรัฐ[44]

รูปแบบกลไกการกำกับดูแลร่วมกันสามารถกระทำได้หลายวิธี เช่นการที่รัฐออกกฎหมายเพื่อจัดตั้งสภาวิชาชีพหรือสมาคมผู้ประกอบการ[45] โดยกำหนดให้เป็นหน่วยงานกลางที่ทำหน้าที่กำกับดูแลผู้ประกอบวิชาชีพหรือผู้ประกอบการให้อยู่ภายใต้หลักเกณฑ์และมาตรฐานเดียวกัน ซึ่งสภาวิชาชีพที่ตั้งขึ้นตามกฎหมายนั้นสามารถสร้างกลไกในการกำกับดูแลตนเองทางด้านจรรยาบรรณหรือแนวปฏิบัติขององค์กรเพื่อคุ้มครองข้อมูลส่วนบุคคลได้เอง

นอกจากนี้แล้วผู้ประกอบการหรือองค์กรที่มีการจัดทำแนวนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลมักจะหาวิธีในการสร้างความน่าเชื่อถือเพิ่มเติมโดยการให้มีองค์กรภายนอกเข้ามาตรวจสอบหรือรับรองการปฏิบัติตามแนวนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล โดยการใช้วิธีขอเครื่องหมายรับรองความน่าเชื่อถือ (Trustmark) จากหน่วยงานหรือองค์กรที่ให้บริการ

---

[43] พรพักตร์ สถิตเวโรจน์, “หลักกฎหมายเกี่ยวกับผู้ให้บริการเครื่องหมายแสดงความน่าเชื่อถือในพาณิชย์อิเล็กทรอนิกส์,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2547), น.37-38.

[44] คณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ, *อ้างแล้ว เชิงอรรถที่ 40*, น.5.

[45] กองบรรณาธิการเว็บไซต์สมาคมนักข่าวนักหนังสือพิมพ์แห่งประเทศไทย, *อ้างแล้ว เชิงอรรถที่ 39.*

เครื่องหมายดังกล่าว[46] การขอเครื่องหมายรับรองความน่าเชื่อถือสามารถสร้างความเชื่อมั่นให้แก่ผู้ใช้บริการและสร้างความน่าเชื่อถือให้กับผู้ประกอบการเองว่ามีการปฏิบัติหลักเกณฑ์ต่างๆ ตามที่หน่วยงานหรือองค์กรที่มีหน้าที่ออกเครื่องหมายรับรองดังกล่าวได้กำหนดไว้ โดยส่วนมากนั้นจะใช้เครื่องหมายรับรองความน่าเชื่อถือในการให้บริการทางเว็บไซต์ต่างๆ

องค์กรที่ทำหน้าที่ให้บริการเครื่องหมายรับรองความน่าเชื่อถือสามารถกระทำได้ทั้งโดยภาครัฐ ภาคเอกชน หรือการร่วมมือกันระหว่างภาครัฐกับภาคเอกชน ขึ้นอยู่กับความเหมาะสมในแต่ละประเทศ เช่นในประเทศที่กำลังพัฒนาระบบในการคุ้มครองข้อมูลส่วนบุคคลและเพิ่งก้าวเข้าสู่ยุคการคุ้มครองทางอิเล็กทรอนิกส์มักจะให้ภาครัฐเป็นผู้ให้บริการเครื่องหมายรับรองความน่าเชื่อถือ เช่นประเทศในแถบทวีปเอเชีย เช่น ประเทศญี่ปุ่น ประเทศสิงคโปร์ เป็นต้น ในขณะที่บางประเทศจะให้องค์กรภาคเอกชนทำหน้าที่ให้บริการเครื่องหมายรับรองความน่าเชื่อถือ เนื่องจากภาคเอกชนมีบุคลากรที่มีประสิทธิภาพและมีระบบการจัดการทางเทคโนโลยีได้ดีกว่า อีกทั้งยังเอื้อต่อการดำเนินธุรกิจการค้าระหว่างประเทศด้วย ดังเช่น ประเทศสหรัฐอเมริกามีองค์กรที่ทำหน้าที่ให้บริการเครื่องหมายรับรองความน่าเชื่อถือคือองค์กรภาคเอกชนที่ไม่แสวงหากำไร เช่น TRUSTe และ BBBOnLine ส่วนประเทศที่มีการจัดระบบร่วมกันระหว่างภาครัฐและเอกชนนั้นได้แก่ประเทศในกลุ่มทวีปยุโรป โดยองค์กรภาครัฐจะทำหน้าที่ในการควบคุมดูแลผู้ให้บริการเครื่องหมายรับรองความน่าเชื่อถือภาคเอกชนอีกชั้นหนึ่งเพื่อรับประกันการคุ้มครองส่วนบุคคล ภาครัฐอาจทำหน้าที่เป็นผู้ควบคุมตรวจสอบดูแลการดำเนินงานของภาคเอกชนทั้งทางเทคนิคและการจัดการ โครงสร้างการทำงานในรูปแบบนี้จะใช้การรับรองแบบลำดับชั้น (hierarchy) ซึ่งแต่ละชั้นจะมีหน้าที่แตกต่างกัน ได้แก่ TrustUK, Webtrader, QWEB เป็นต้น[47]

เครื่องหมายรับรองความน่าเชื่อถือแบ่งบอกได้เป็นหลายประเภท ขึ้นอยู่กับวัตถุประสงค์ในการใช้งาน[48] เช่น “Reliability Trustmark” มีวัตถุประสงค์เพื่อรับประกันความน่าเชื่อถือ ความมีตัวตนของผู้ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์, “Privacy Trustmark” เป็นเครื่องหมายแสดงว่าผู้ประกอบการมีนโยบายในการรักษาความเป็นส่วนตัวเป็นไปตามมาตรฐานของ

---

[46] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารและสำนักงานเลขานุการคณะกรรมการ ธุรกรรมทางอิเล็กทรอนิกส์, Privacy Policy & Trustmark : กลไกการคุ้มครองข้อมูลส่วนบุคคล กับการสร้างความน่าเชื่อถือในการทำ e-Business, (กรุงเทพมหานคร : สำนักงานเลขานุการ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ , 2548), น.13.

[47] พรพักตร์ สถิตเวโรจน์, *อ้างแล้ว เชิงอรรถที่ 43*, น.58-60.

[48] *เพิ่งอ้าง*, น.48-51.

หน่วยงานที่ให้บริการออกเครื่องหมาย, “Security Trustmark” เป็นเครื่องหมายรับรองที่แสดงความปลอดภัยในขั้นตอนการดำเนินการด้านต่างๆของผู้ประกอบการ

เครื่องหมายรับรองความน่าเชื่อถือที่รับรองความน่าเชื่อถือในเรื่องการคุ้มครองข้อมูลส่วนบุคคล คือ Privacy Trustmark โดยหน่วยงานที่เป็นผู้ให้บริการเครื่องหมายอาจมีการกำหนดหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขึ้น ถ้าหากผู้ประกอบการที่ยื่นขอเครื่องหมายรับรองนั้นมีแนวนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลที่เป็นไปตามหลักเกณฑ์นั้นก็จะได้เครื่องหมายรับรองความน่าเชื่อถือด้านการคุ้มครองข้อมูลส่วนบุคคล ในประเทศสหรัฐอเมริกาเครื่องหมายประเภทนี้ได้แก่[49] TRUSTe ที่ออกโดยองค์กรอิสระไม่แสวงหากำไรที่มีชื่อว่า TRUSTe ซึ่งตั้งขึ้นโดย Electronic Frontier Foundation (EFF) และเครื่องหมาย BBBOnLine ที่ออกโดย Better Business Bureau ในปัจจุบันนี้เครื่องหมายรับรองความน่าเชื่อถือในด้านการคุ้มครองข้อมูลส่วนบุคคลสามารถรับรองข้อมูลได้หลากหลายลักษณะ ขึ้นอยู่กับวัตถุประสงค์ในการใช้งาน เช่น เครื่องหมายรับรองการคุ้มครองข้อมูลส่วนบุคคลทั่วไป เครื่องหมายรับรองความเป็นส่วนตัวของเด็ก รวมถึงเครื่องหมายรับรองการปฏิบัติตามข้อตกลงโครงการเซฟฮาร์เบอร์เป็นต้น

อย่างไรก็ตาม เนื่องจากกลไกการกำกับดูแลร่วมกันได้พัฒนามาจากกลไกการกำกับดูแลตนเองและยังมีการใช้กลไกทั้งสองนี้คาบเกี่ยวกันอยู่มาก ผู้เขียนเห็นว่าวิธีการจำแนกรูปแบบการคุ้มครองข้อมูลส่วนบุคคลระหว่างการใช้กลไกการกำกับดูแลตนเองกับกลไกการกำกับดูแลร่วมกันสามารถพิจารณาจากระดับการมีส่วนร่วมของภาครัฐที่มีส่วนในการคุ้มครองข้อมูลบุคคล กลไกการกำกับดูแลตนเองจะเป็นการกำหนดหลักเกณฑ์โดยภาคเอกชนหรือผู้ประกอบวิชาชีพเป็นหลักกฎเกณฑ์เหล่านั้นจะไม่มีสภาพบังคับตามกฎหมาย ส่วนกลไกการกำกับดูแลร่วมกันให้ภาครัฐจะเข้ามามีส่วนร่วมในฐานะเป็นอำนาจสุดท้ายในควบคุมให้มีการปฏิบัติตามหลักเกณฑ์ โดยหลักเกณฑ์นั้นจะกำหนดขึ้นโดยภาคเอกชนหรือภาครัฐตกลงร่วมกับภาคเอกชนก็ได้ การจำแนกรูปแบบการคุ้มครองข้อมูลส่วนบุคคลด้วยหลักเกณฑ์ดังกล่าวเอื้อประโยชน์ต่อพัฒนาการด้านการคุ้มครองข้อมูลส่วนบุคคลในอนาคต ที่ทั้งหน่วยงานภาครัฐและภาคเอกชนจำเป็นต้องดำเนินกลไกเพื่อคุ้มครองข้อมูลส่วนบุคคลร่วมกันเพื่อให้ทันต่อสภาพสังคมและเทคโนโลยีที่เปลี่ยนแปลงไป

---

[49] *เพิ่งอ้าง,* น.64-67.

2.3 สถานการณ์การโอนข้อมูลส่วนบุคคลระหว่างประเทศกับปัญหาการคุ้มครองข้อมูลส่วนบุคคล

2.3.1 ความสำคัญและความจำเป็นในการโอนข้อมูลส่วนบุคคลระหว่างประเทศ

ข้อมูลส่วนบุคคลมีบทบาทสำคัญยิ่งต่อการดำเนินกิจกรรมในระบบเศรษฐกิจที่เป็นยุคสังคมสารสนเทศ กิจกรรมทางเศรษฐกิจส่วนใหญ่จะนำข้อมูลส่วนบุคคลมาเป็นพื้นฐานในการตัดสินใจเพื่อดำเนินกิจการในทางเศรษฐกิจแทบทั้งสิ้น อาจกล่าวได้ว่าท่ามกลางการขยายตัวของเศรษฐกิจที่มีการแข่งขันสูง หากผู้ประกอบการมีข้อมูลของผู้บริโภคอยู่ในครอบครองมากเพียงใดย่อมทำให้สามารถนำไปใช้เพื่อการศึกษาวิจัยทางการตลาด อำนวยความสะดวกหรือเพิ่มศักยภาพทางธุรกิจได้มากเท่านั้น เมื่อรวมกับแนวคิดในการคุ้มครองข้อมูลส่วนบุคคลสมัยใหม่ที่เน้นเรื่องการมีอำนาจควบคุมในการเก็บรวบรวมข้อมูลหรือการนำข้อมูลไปใช้ประโยชน์มากกว่าการพิจารณาว่าข้อมูลอยู่ที่ใดหรืออยู่ในการครอบครองของใคร[50] ทำให้การส่งหรือโอนข้อมูลส่วนบุคคลทำได้อย่างแพร่หลายและมีปริมาณเพิ่มมากขึ้นเรื่อยๆ

ในปัจจุบันนี้การดำเนินการต่างๆทั้งหน่วยงานของรัฐหรือภาคเอกชนเองต่างมีความจำเป็นต้องโอนข้อมูลส่วนบุคคลระหว่างกันตลอดเวลา ข้อมูลส่วนบุคคลเป็นดั่งปัจจัยสำคัญที่ทำให้การดำเนินกิจกรรมต่างๆทำได้อย่างต่อเนื่องและบรรลุเป้าหมาย เช่น หน่วยงานหนึ่งๆอาจมีความจำเป็นต้องใช้ข้อมูลที่อยู่ในความครอบครองของหน่วยงานอื่น บริษัทเอกชนประเภทหนึ่งอาจจำเป็นต้องใช้ข้อมูลส่วนบุคคลจากบริษัทเอกชนอีกประเภทเพื่อเกื้อหนุนการทำธุรกิจของตน

เมื่อเทคโนโลยีสารสนเทศและการสื่อสารได้มีความก้าวหน้าอย่างรวดเร็ว เทคโนโลยีต่างๆถูกนำมาประยุกต์ใช้กับกิจการต่างๆมากมาย ไม่ว่าจะเป็นด้านการโทรคมนาคม การขนส่ง การแพทย์ การศึกษา และเศรษฐกิจ โดยเฉพาะการใช้เทคโนโลยีเพื่อประมวลผลข้อมูลหรือการโอนข้อมูลระหว่างกัน อีกทั้งผลจากการพัฒนาเทคโนโลยีการสื่อสารผ่านทางเครือข่ายอินเทอร์เน็ตทำให้เกิดช่องทางในการโอนข้อมูลส่วนบุคคลที่สามารถทำได้สะดวก รวดเร็ว ไม่มีข้อจำกัดในเรื่องเวลาและระยะทางอีกต่อไป การโอนข้อมูลผ่านเครือข่ายอินเทอร์เน็ตถูกนำมาใช้อย่างแพร่หลาย โดยเฉพาะอย่างยิ่งการประกอบพาณิชย์อิเล็กทรอนิกส์ (electronic commerce) ซึ่งจำเป็นต้องมีการรวบรวมข้อมูลส่วนบุคคลหลายประเภทเพื่อให้ธุรกิจสามารถดำเนินต่อไปได้ เช่น หมายเลขบัตรเครดิต หมายเลขบัญชีธนาคาร ทำให้มีความจำเป็นที่จะต้องโอนข้อมูลระหว่างกันเพื่อการรวบรวมข้อมูลดังกล่าว

---

[50] นคร เสรีรักษ์, การคุ้มครองข้อมูลส่วนบุคคล ข้อเสนอสำหรับประเทศไทย, (กรุงเทพมหานคร : สำนักพิมพ์พีเพรส, 2558), น.11.

การโอนข้อมูลส่วนบุคคลมิได้จำกัดเฉพาะการโอนข้อมูลส่วนบุคคลภายในประเทศแต่เพียงอย่างเดียว ยุคการสื่อสารแบบไร้พรมแดนทำให้การโอนข้อมูลส่วนบุคคลระหว่างประเทศมีความสำคัญไม่ยิ่งหย่อนไปกว่ากัน เนื่องจากการดำเนินกิจการต่างๆมิได้จำกัดเฉพาะแค่ในประเทศใดประเทศหนึ่ง อาณาเขตใดอาณาเขตหนึ่งอีกต่อไป แต่กลับมีลักษณะเปิดกว้างให้สามารถทำกิจการต่างๆระหว่างกันได้แม้จะอยู่คนละประเทศ ยกตัวอย่างเช่น การโอนข้อมูลพนักงานบริษัทไปยังสำนักงานใหญ่หรือสำนักงานสาขาที่ตั้งอยู่ในต่างประเทศ การโอนข้อมูลของผู้ถือบัตรเครดิตเพื่อการเรียกเก็บเงินอันเนื่องจากการใช้บัตรเครดิตในต่างประเทศ การโอนข้อมูลการเดินทางของผู้โดยสารสายการบินต่างๆ หรือแม้แต่การโอนข้อมูลส่วนบุคคลโดยภาครัฐเพื่อประโยชน์ในการบังคับใช้กฎหมาย การตรวจคนเข้าเมือง การเก็บภาษีศุลกากร เป็นต้น

2.3.2 รูปแบบการโอนข้อมูลส่วนบุคคลระหว่างประเทศ

รูปแบบการโอนข้อมูลส่วนบุคคลจากประเทศหนึ่งไปยังอีกประเทศหนึ่งสามารถกระทำได้หลายวิธี การโอนข้อมูลดังกล่าวอาจอยู่ในรูปแบบของการโอนข้อมูลทางกายภาพ เช่น การส่งอุปกรณ์บันทึกข้อมูลส่วนไปยังอีกประเทศหนึ่งทางไปรษณีย์ การส่งข้อมูลผ่านสื่ออิเล็กทรอนิกส์ต่างๆ ไม่ว่าจะเป็นดาวเทียม สายเคเบิ้ล หรือแม้แต่การส่งข้อมูลผ่านทางเครือข่ายคอมพิวเตอร์แบบออนไลน์เป็นต้น ทั้งนี้สามารถจำแนกรูปแบบการโอนข้อมูลส่วนบุคคลตามลักษณะของข้อมูลและประเภทขององค์กรที่มีความจำเป็นต้องโอนข้อมูลออกเป็น 4 ลักษณะ ได้แก่[51]

(1) การโอนข้อมูลส่วนบุคคลภายในองค์กรเดียวกันที่ตั้งอยู่คนละประเทศ

การโอนข้อมูลรูปแบบนี้มีความจำเป็นเพื่อประโยชน์ในการบริหารจัดการในองค์กรโดยเฉพาะอย่างยิ่งในการบริหารจัดการงานบุคคล (human resource) เช่นการโอนข้อมูลพนักงานระหว่างบริษัทสำนักงานสาขาในประเทศหนึ่งไปยังสำนักงานสาขาอื่น หรือสำนักงานใหญ่ที่ตั้งอยู่ในต่างประเทศ เพื่อการจัดทำฐานข้อมูลพนักงานกลางให้บริษัทในเครือซึ่งตั้งอยู่ในประเทศต่างๆ สามารถเข้าถึงข้อมูลและใช้ประโยชน์จากข้อมูลดังกล่าวได้ หรือการจ่ายเงินให้แก่พนักงานที่ทำงานอยู่ในสำนักงานสาขาในต่างประเทศ

---

[51] Ian Walden and Nagel Savage , “Transborder Data Flows,” in Information Technology and The Law, ed. Chris Edwards, Nagel Savage, Ian Walden (United Kingdom : Macmillan Publishers, 1990), p. 121. อ้างถึงใน ปฏิวัติ อุ่นเรือน, “ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ,” (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), น.26.

(2) การโอนข้อมูลส่วนบุคคลไปยังองค์กรอื่นที่ตั้งอยู่ในต่างประเทศ

การโอนข้อมูลส่วนบุคคลรูปแบบนี้ได้แก่ การโอนข้อมูลระหว่างกลุ่มธุรกิจธนาคารระหว่างประเทศ ธุรกิจประกันภัย ธุรกิจบัตรเครดิต ธุรกิจการบินในกรณีการจองตั๋วเครื่องบิน ธุรกิจท่องเที่ยว การให้บริการทางการแพทย์ ธุรกิจการตลาดแบบตรง (direct marketing) การประกอบพาณิชย์อิเล็กทรอนิกส์ ที่จะต้องมีการโอนข้อมูลของลูกค้าจากประเทศหนึ่งยังอีกประเทศหนึ่งอยู่ตลอดเวลา

(3) การโอนข้อมูลส่วนบุคคลเพื่อประโยชน์ของหน่วยงานภาครัฐ

ตัวอย่างเช่น การโอนข้อมูลส่วนบุคคลโดยภาครัฐเพื่อประโยชน์ในการบังคับใช้กฎหมาย การตรวจคนเข้าเมือง การเก็บภาษีศุลกากร เป็นต้น

(4) การโอนข้อมูลส่วนบุคคลเพื่อประโยชน์ในการประมวลผลหรือการจัดเก็บฐานข้อมูลในต่างประเทศ

การโอนข้อมูลส่วนบุคคลในรูปแบบนี้มักเกิดขึ้นในกรณีที่มีการมอบหมายงานด้านสารสนเทศให้กับหน่วยงานภายนอก (outsourcing) จากผู้ประกอบการในประเทศหนึ่งไปให้ผู้ประกอบการที่อยู่ในประเทศอื่นซึ่งส่วนใหญ่จะมีข้อมูลส่วนบุคคลปะปนไปด้วยเสมอ เพื่อลดต้นทุนในการประมวลผล หรือการบริหารจัดการต่างๆเกี่ยวกับข้อมูล เช่น การจัดตั้งศูนย์ให้บริการลูกค้า (call center) ในราคาที่ถูกกว่า

2.3.3 ปัญหาการคุ้มครองการโอนข้อมูลส่วนบุคคลระหว่างประเทศในปัจจุบัน

แม้ในปัจจุบันมีความจำเป็นต้องโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเพื่อประโยชน์ในกิจการของรัฐและเอกชนในหลายๆด้าน แต่อย่างไรก็ตามการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศนั้นก็ย่อมส่งผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลเช่นเดียวกัน เนื่องจากประเทศแต่ละประเทศย่อมมีนิติวิธี ระบบกฎหมายและหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน บางประเทศอาจมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เข้มงวด แต่ในบางประเทศก็อาจจะไม่มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลหรือมีแต่ไม่เข้มงวดมากนักเป็นต้น

โดยหลักการแล้วการคุ้มครองข้อมูลส่วนบุคคลเมื่อถูกโอนไปยังต่างประเทศนั้นสมควรที่จะได้รับการคุ้มครองเช่นเดียวกันกับเมื่อข้อมูลส่วนบุคคลนั้นอยู่ภายในประเทศ กล่าวคือเจ้าของข้อมูลส่วนบุคคลมีสิทธิใดๆต่อข้อมูลของตนที่อยู่ในประเทศก่อนที่ข้อมูลนั้นจะถูกโอนไปเช่นใดก็สมควรจะมีสิทธิดังกล่าวเมื่อข้อมูลของตนอยู่ในต่างประเทศด้วย แต่ในทางปฏิบัติแล้วการบังคับใช้สิทธิใดๆในข้อมูลส่วนบุคคลของเจ้าของข้อมูลย่อมไม่สามารถกระทำได้อย่างเต็มที่ในทันใดที่ข้อมูลส่วนบุคคลของตนได้ถูกโอนไปยังต่างประเทศ เหตุเนื่องจากเมื่อข้อมูลส่วนบุคคลได้ถูกโอนไปยังประเทศอื่นแล้วย่อมต้องข้อมูลส่วนบุคคลย่อมตกอยู่ภายใต้มาตรการทางกฎหมายของประเทศนั้น ทำให้มาตรการคุ้มครองข้อมูลส่วนบุคคลแบบที่ใช้ในประเทศที่รับโอนข้อมูลส่วนบุคคลอาจไม่เหมือนกับ

มาตรการคุ้มครองข้อมูลที่ใช้ในประเทศที่เป็นฝ่ายโอนข้อมูล จากปัญหาระดับความไม่เท่ากันของการคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศ ข้อมูลส่วนบุคคลจึงมิได้รับการคุ้มครองไปจนสุดตลอดสายเมื่อมีการโอนข้อมูลส่วนบุคคลนั้นไปยังต่างประเทศ

ปัญหาการคุ้มครองข้อมูลส่วนบุคคลเมื่อมีการโอนข้อมูลไปยังต่างประเทศนั้น หากประเทศที่เป็นฝ่ายรับโอนข้อมูลส่วนบุคคลมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่สูงกว่า เข้มงวดกว่าประเทศที่ข้อมูลส่วนบุคคลถูกโอนไปย่อมไม่เกิดปัญหาในการคุ้มครองข้อมูลส่วนบุคคลนั้น แต่ในทางกลับกันถ้าหากประเทศที่รับโอนข้อมูลส่วนบุคคลไม่มีหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลหรือมีแต่อยู่ในระดับที่ไม่เพียงพอก็ย่อมส่งผลกระทบต่อความเป็นส่วนตัวในข้อมูลส่วนบุคคลของเจ้าของข้อมูลได้ ข้อมูลส่วนบุคคลที่ถูกโอนไปยังต่างประเทศที่ไม่มีการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอนั้นจึงอาจถูกแทรกแซงและละเมิดสิทธิอันจะทำให้ผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายได้

2.4 แนวทางการแก้ปัญหาการโอนข้อมูลส่วนบุคคลระหว่างประเทศ

จากปัญหาการโอนข้อมูลส่วนบุคคลระหว่างประเทศที่จะเกิดขึ้นในกรณีที่แต่ละประเทศมีหลักเกณฑ์และมาตรการในการคุ้มครองข้อมูลส่วนบุคคลไม่เท่ากัน ทำให้องค์การความร่วมมือระหว่างประเทศได้วางหลักการในการคุ้มครองข้อมูลส่วนบุคคลขึ้น เพื่อสร้างแนวทางให้แต่ละประเทศมีหลักในการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้มีความสอดคล้องและเป็นไปในแนวทางเดียวกัน ซึ่งจะทำให้แต่ละประเทศที่นำเอาหลักการที่องค์การความร่วมมือระหว่างประเทศได้กำหนดไว้มาบัญญัติเป็นกฎหมายภายในมีการคุ้มครองข้อมูลส่วนบุคคลที่ได้มาตรฐาน อันจะแก้ปัญหาระดับความไม่เท่ากันของการคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศได้

2.4.1 มาตรการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลส่วนบุคคลระหว่างประเทศขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines)

องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนาได้มีการพัฒนากรอบนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลขึ้นในปี ค.ศ. 1980 โดยการออกแนวปฏิบัติด้านการคุ้มครองความเป็นส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ (Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data) เรียกโดยย่อว่า OECD Guidelines ซึ่งมีวัตถุประสงค์เพื่อเป็นข้อเสนอแนะแก่ประเทศสมาชิกในการนำเอาหลักการคุ้มครองข้อมูลส่วนบุคคลขั้นพื้นฐาน (basic principles) ไปใช้บังคับในประเทศสมาชิก ซึ่งอาจอยู่ในรูปของ

การบัญญัติกฎหมายหรือมาตรการอื่นใดที่มีสภาพบังคับได้ โดยหลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวปฏิบัติขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนามีทั้งสิ้น 8 ประการ คือ[52]

(1) หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)

หลักการข้อนี้กำหนดหลักเกณฑ์เกี่ยวกับข้อจำกัดในการรวบรวมข้อมูลส่วนบุคคลว่าจะสามารถรวบรวมได้ต่อเมื่อข้อมูลดังกล่าวได้มาโดยชอบด้วยกฎหมาย ด้วยวิธีการที่เป็นธรรมและเหมาะสม ภายใต้การรับรู้หรือความยินยอมจากเจ้าของข้อมูลเท่านั้น

(2) หลักคุณภาพของข้อมูล (Data Quality Principle)

กล่าวคือจะต้องใช้ข้อมูลส่วนบุคคลภายในขอบวัตถุประสงค์ในการจัดเก็บ หรืออาจใช้เพื่อวัตถุประสงค์อื่นได้ตามความจำเป็น โดยข้อมูลดังกล่าวจะต้องเป็นข้อมูลที่มีความถูกต้องสมบูรณ์ และเป็นปัจจุบัน

(3) หลักการระบุวัตถุประสงค์โดยเฉพาะเจาะจง (Purpose Specification Principle)

กล่าวคือจะต้องแจ้งวัตถุประสงค์ของการรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลได้ทราบก่อนการรวบรวมข้อมูล อีกทั้งจะต้องใช้ข้อมูลส่วนบุคคลภายในวัตถุประสงค์ดังกล่าวด้วย

(4) หลักการจำกัดการใช้ข้อมูล (Use Limitation Principle)

ข้อมูลส่วนบุคคลจะต้องไม่ถูกเปิดเผย ทำให้แพร่หลาย หรือใช้เพื่อวัตถุประสงค์อื่นใดนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลทราบก่อนหน้านั้น เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลหรือมีกฎหมายบัญญัติเป็นอย่างอื่น

(5) หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)

ผู้ควบคุมข้อมูลจะต้องรักษาความปลอดภัยของข้อมูลโดยใช้มาตรการรักษาความปลอดภัยตามสมควร เพื่อป้องกันการเข้าถึงข้อมูลโดยปราศจากอำนาจ การทำลาย การใช้ การเปลี่ยนแปลง หรือการเปิดเผยข้อมูลโดยมิชอบ

(6) หลักการเปิดเผย (Openness Principle)

ผู้ควบคุมข้อมูลควรมีการประกาศนโยบายเกี่ยวกับการดำเนินการใดๆ ต่อข้อมูลส่วนบุคคลให้ทราบโดยทั่วไป รวมทั้งกำหนดลักษณะของข้อมูล วัตถุประสงค์ของการใช้ข้อมูล รายละเอียดเกี่ยวกับผู้ควบคุมดูแล (controller) ถิ่นที่อยู่ของผู้ควบคุม เป็นต้น

(7) หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Confirmation)

---

[52] ปฏิวัติ อุ่นเรือน, *อ้างแล้ว เชิงอรรถที่ 4*, น.18.

หลักการข้อนี้กำหนดให้เจ้าของข้อมูลมีสิทธิได้รับการยืนยัน (confirmation) จากผู้ควบคุมข้อมูลว่าผู้ควบคุมข้อมูลมีข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลหรือไม่เพียงใด โดยจะต้องได้รับทราบผลการยืนยันภายในเวลาอันสมควร ทั้งนี้ผู้ควบคุมข้อมูลอาจคิดค่าใช้จ่ายในการดำเนินการได้ในอัตราที่เหมาะสม และในกรณีที่ไม่สามารถดำเนินการตามที่เจ้าของข้อมูลร้องขอข้างต้น ผู้ควบคุมข้อมูลจะต้องแจ้งเหตุผลให้เจ้าของข้อมูลทราบ อีกทั้งบอกกล่าวให้เจ้าของข้อมูลทราบถึงสิทธิในการโต้แย้งการไม่ปฏิบัติตามคำร้องดังกล่าว และหากต่อมาปรากฏว่าข้อโต้แย้งของเจ้าของข้อมูลสามารถรับฟังได้ เจ้าของข้อมูลก็มีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลทำการลบ แก้ไข ปรับปรุงหรือทำให้ข้อมูลมีความสมบูรณ์

(8) หลักความรับผิดชอบ (Accountability Principle)

ผู้ควบคุมข้อมูลจะต้องมีความรับผิดชอบในการปฏิบัติตามมาตรการต่างๆ เพื่อดำเนินการให้เป็นไปตามหลักการข้างต้น

แนวปฏิบัติขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนาถือเป็นแนวปฏิบัติขั้นต่ำของหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ประเทศสมาชิกสามารถนำไปปฏิบัติตามภายในประเทศของตนได้ แนวปฏิบัติฉบับนี้ใช้บังคับได้กับการประมวลผลข้อมูลส่วนบุคคลทั้งที่อยู่ในความครอบครองของหน่วยงานของรัฐและหน่วยงานเอกชน และไม่ได้แบ่งแยกว่าเป็นการประมวลผลข้อมูลส่วนบุคคลโดยวิธีการอัตโนมัติหรือโดยวิธีการประมวลผลด้วยมือแต่อย่างใด[53]

2.4.2 มาตรการคุ้มครองข้อมูลส่วนบุคคลของสภายุโรป

ในปีถัดมาหลังจากที่มีการออกแนวปฏิบัติขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา สภายุโรป (Council of Europe) ก็ได้มีการจัดทำอนุสัญญาว่าด้วยการคุ้มครองปัจเจกชนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ (Convention for the Protection of Individuals with Regard to Automatic Processing of Personal) หรือเรียกโดยย่อว่า Convention 108

อนุสัญญานี้มีวัตถุประสงค์ในการสร้างความสมดุลระหว่างการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลธรรมดาและความจำเป็นในการใช้หรือถ่ายโอนข้อมูลส่วนบุคคลในกิจกรรมทางเศรษฐกิจต่างๆ ความสำคัญของอนุสัญญาฯคือการเปิดให้ประเทศต่างๆที่แม้ไม่ได้เป็นสมาชิกของสภายุโรปก็สามารถเข้าร่วมเป็นภาคีของอนุสัญญานี้ได้ จึงอาจกล่าวได้ว่าอนุสัญญาว่าด้วยการคุ้มครองปัจเจกชนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติเป็นกรอบความร่วมมือระหว่างประเทศฉบับแรกที่มีผลบังคับใช้ด้านการคุ้มครองข้อมูลส่วนบุคคล[54] โดยประเทศภาคีอนุสัญญา

---

[53] นคร เสรีรักษ์, *อ้างแล้ว เชิงอรรถที่ 3*, น.147.

[54] ปฏิวัติ อุ่นเรือน, *อ้างแล้ว เชิงอรรถที่ 4*, น.20.

จะต้องบัญญัติกฎหมายภายในให้สอดคล้องกับหลักการที่ได้ระบุไว้ในอนุสัญญาฯ ซึ่งหลักการดังกล่าวมีดังนี้[55]

(1) หลักการเก็บรวบรวมและประมวลผลข้อมูลต้อดำเนินการโดยถูกต้อง และการเปิดเผยข้อมูลต้องกระทำด้วยเจตนาที่สุจริต

(2) หลักการกำหนดระยะเวลาในการใช้ข้อมูล เมื่อสิ้นสุดความจำเป็นในการใช้ข้อมูลจะต้องยกเลิกการจัดเก็บทันที

(3) หลักการจัดเก็บและประมวลผลข้อมูลต้องทำภายใต้วัตถุประสงค์และเพียงเท่าที่จำเป็น

(4) หลักความถูกต้องของข้อมูล ต้องมีคุณภาพและมีการปรับปรุงให้ทันสมัยอยู่เสมอ

(5) หลักการรักษาความปลอดภัยของข้อมูล มาตรการคุ้มครองข้อมูลตามกฎหมายและให้ความคุ้มครองในทางเทคนิค

จะเห็นได้ว่าหลักการตามอนุสัญญาดังกล่าวนั้นเป็นไปในทางเดียวกับแนวปฏิบัติขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา แต่อนุสัญญานี้มีขอบเขตครอบคลุมเฉพาะแต่การประมวลผลโดยระบบอัตโนมัติเท่านั้น ส่วนแนวปฏิบัติขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนาครอบคลุมการประมวลผลข้อมูลทุกรูปแบบ นอกจากนี้ขอบเขตการคุ้มครองตามอนุสัญญาสามารถขยายการคุ้มครองไปถึงคณะบุคคล บริษัท หรือองค์กรต่างๆได้อีกด้วย แตกต่างจากแนวปฏิบัติขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนาที่ใช้บังคับกับบุคคลธรรมดาเท่านั้น

2.4.3 มาตรการคุ้มครองข้อมูลส่วนบุคคลขององค์การสหประชาชาติ

องค์การสหประชาชาติโดยคณะมนตรีด้านสังคมและเศรษฐกิจแห่งสหประชาชาติ (United Nations Economic and Social Council) ได้ให้การรับรองคู่มือว่าด้วยการกำกับการประมวลผลข้อมูลส่วนบุคคลโดยคอมพิวเตอร์ (Guidelines for the Regulation of Computerized Personal Data File)[56] ในวันที่ 14 ธันวาคม ค.ศ. 1990 เพื่อให้ประเทศสมาชิกปฏิบัติตามหลักเกณฑ์ในการกำหนดมาตรฐานขั้นต่ำเกี่ยวกับการบัญญัติกฎหมายภายในของรัฐดังต่อไปนี้

---

[55] นคร เสรีรักษ์, *อ้างแล้ว เชิงอรรถที่ 3*, น.149.

[56] United Nations, “Guidelines for the Regulation of Computerized Personal Data File,” Retrieved from http://www.unhchr.ch/html/menu3/b/71.htm. 1990

(1) หลักความชอบด้วยกฎหมายและความเป็นธรรม[57] (Principle of Lawfulness and Fairness)

ข้อมูลที่ได้รับการประมวลผลจะต้องได้มาโดยชอบธรรม และชอบด้วยกฎหมาย ทั้งนี้โดยไม่ขัดหรือแย้งกับกฎบัตรสหประชาชาติ (Charter of the United Nations)

(2) หลักความถูกต้อง[58] (Principle of Accuracy)

บุคคลที่มีหน้าที่รับผิดชอบในการเก็บรักษาข้อมูลจะต้องทำการตรวจสอบข้อมูลตลอดเวลาเพื่อให้แน่ใจว่าข้อมูลที่จัดเก็บนั้นถูกต้อง เพื่อมิให้เกิดความผิดพลาด

(3) หลักการระบุวัตถุประสงค์โดยเฉพาะเจาะจง[59] (Principle of the Purpose Specification)

ข้อมูลส่วนบุคคลต้องจัดเก็บและรวบรวมอย่างพอเพียง ตามวัตถุประสงค์ที่ได้ระบุไว้โดยเฉพาะ โดยห้ามมิให้มีการใช้หรือเปิดเผยข้อมูลโดยมิได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง อีกทั้งระยะเวลาในการจัดเก็บจะต้องไม่เกินไปกว่าในวัตถุประสงค์ที่ระบุไว้

(4) หลักการเข้าถึงข้อมูลโดยบุคคลที่เกี่ยวข้อง[60] (Principle of Interested-person Access)

บุคคลมีสิทธิที่จะเข้าถึงข้อมูลของตนเองโดยการแสดงหลักฐานสำคัญเพื่อแสดงว่าตนเป็นใคร

(5) หลักการไม่เลือกปฏิบัติ[61] (Principle of Non-discrimination)

ในการจัดทำข้อยกเว้นจะต้องไม่มีเลือกปฏิบัติไม่ว่าบุคคลนั้นจะมีเชื้อชาติ สัญชาติ ศาสนา เพศ ความเห็นทางการเมือง ความคิด ความเชื่อ ความเป็นสมาชิกภาพสถาบัน หรือสมาชิกภาพองค์กร แตกต่างกันก็ตาม

(6) หลักการรักษาความปลอดภัย[62] (Principle of Security)

จะต้องมีการนำมาตรการที่เหมาะสมมาใช้เพื่อป้องกันข้อมูลส่วนบุคคล ทั้งจากเหตุอันอาจเกิดขึ้นตามธรรมชาติ ความเสียหายอันเกิดจากการกระทำของมนุษย์ เช่นการเข้าถึงข้อมูล

---

[57] *Ibid*., Article 1

[58] *Ibid*., Article 2

[59] *Ibid*., Article 3

[60] *Ibid*., Article 4

[61] *Ibid*., Article 5

[62] *Ibid*., Article 7

โดยไม่ได้รับอนุญาต การนำข้อมูลไปใช้โดยไม่ชอบหรือการใส่โปรแกรมไวรัสเข้าไปในระบบคอมพิวเตอร์เพื่อทำลายล้างข้อมูล

ทั้งนี้เนื้อหาของหลักการต่างๆที่ปรากฏอยู่ในแนวปฏิบัติขององค์การสหประชาชาติจะมีลักษณะเป็นไปในทิศทางเดียวกันกับแนวปฏิบัติขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา หากแต่แตกต่างกันตรงที่ได้เพิ่มหลักการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลชนิดที่มีความอ่อนไหว (sensitive data) ไว้ในหลักการไม่เลือกปฏิบัติด้วย กล่าวคือห้ามมิให้ทำการรวบรวมข้อมูลซึ่งอาจทำให้เกิดการเลือกปฏิบัติต่อบุคคลที่แตกต่างกัน[63]

แม้ว่าแนวทางการแก้ปัญหาการคุ้มครองข้อมูลส่วนบุคคลที่องค์การระหว่างประเทศต่างๆได้สร้างขึ้นจากตัวอย่างข้างต้น จะมีวัตถุประสงค์เพื่อให้แต่ละประเทศได้พัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลภายในประเทศให้เป็นไปตามมาตรฐานสากลและสร้างมาตรการคุ้มครองข้อมูลส่วนบุคคลให้อยู่ในระดับที่ทัดเทียมกัน มีหลักเกณฑ์มาตรฐานที่เป็นอันหนึ่งอันเดียวกันก็ตาม แต่หลักเกณฑ์ขององค์การระหว่างประเทศดังกล่าวไม่ได้มีสภาพบังคับมากนัก เนื่องจากขึ้นอยู่กับแต่ละประเทศนั้นเองว่าจะมีการดำเนินการบัญญัติกฎหมายภายในให้เป็นไปตามแนวทางขององค์การระหว่างประเทศนั้นมากน้อยเพียงใด

[63] ปฏิวัติ อุ่นเรือน, *อ้างแล้ว เชิงอรรถที่ 4*, น.23.

บทที่ 3
กฎหมายต่างประเทศเกี่ยวกับการโอนข้อมูลส่วนบุคคลระหว่างประเทศ

แม้ว่าองค์การความร่วมมือระหว่างประเทศต่างๆจะได้พยายามวางกรอบและหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้แต่ละประเทศนำไปใช้เป็นแนวทางในการกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศแล้วก็ตาม แต่กฎหมายคุ้มครองข้อมูลส่วนบุคคลในภาคพื้นยุโรปนั้นก็ยังมิได้เป็นเอกรูปหรือสอดคล้องกันมากนัก เนื่องจากแนวปฏิบัติขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนานั้นมีลักษณะเป็นเพียงการกำหนดหลักเกณฑ์พื้นฐานทั่วไปที่สมควรนำไปบัญญัติไว้เป็นกฎหมายภายในประเทศเท่านั้น ทำให้ในรายละเอียดของการคุ้มครองข้อมูลส่วนบุคคลย่อมแตกต่างกันไปในแต่ละประเทศ ส่วนอนุสัญญาของสภายุโรปแม้จะเป็นข้อตกลงระหว่างประเทศที่มีสภาพบังคับแล้วก็ตาม แต่ก็มิได้ทำให้กฎหมายที่บัญญัติภายในประเทศมีความสอดคล้องเท่าที่ควรเช่นกัน เนื่องจากขณะที่ประเทศส่วนใหญ่ลงนามเป็นภาคีในอนุสัญญานี้ได้มีการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศของตนเสร็จสิ้นไปเรียบร้อยแล้ว อีกทั้งอนุสัญญาดังกล่าวยังเป็นเพียงกรอบอย่างกว้างในการคุ้มครองข้อมูลส่วนบุคคลเท่านั้น ส่งผลให้ประเทศภาคีสามารถกำหนดรายละเอียดในการคุ้มครองข้อมูลส่วนบุคคลภายในที่แตกต่างกันออกไป[1]

ต่อมาสหภาพยุโรปได้พัฒนาหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลขึ้น เพื่อมุ่งคุ้มครองสิทธิในความเป็นส่วนตัวอันเนื่องมาจากการประมวลผลข้อมูลในปี ค.ศ. 1995 โดยการบัญญัติ Directive 95/46/EC ขึ้น Directive นี้มีความสำคัญยิ่งในการสร้างข้อบังคับที่ผูกพันประเทศสมาชิกสหภาพยุโรปให้ต้องมีการบัญญัติหรือปรับปรุงกฎหมายภายในให้มีความสอดคล้องกับหลักเกณฑ์ตาม Directive ด้วย จากข้อบังคับดังกล่าวจึงส่งผลให้หลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศสมาชิกสหภาพยุโรปมีความเป็นเอกรูปและสอดคล้องกัน อันส่งผลตามมาต่อระบบการไหลเวียนข้อมูลและโอนข้อมูลส่วนบุคคลในระหว่างประเทศที่เกิดขึ้นจากการบัญญัติ Directive 95/46/EC ดังจะได้ศึกษาต่อไปนี้

---

[1] ปฏิวัติ อุ่นเรือน, “ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ,” (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), น.20-21.

3.1 Directive 95/46/EC โดยสหภาพยุโรป

3.1.1 วัตถุประสงค์และหลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลตาม Directive 95/46/EC

บทบัญญัติ Directive 95/46/EC ว่าด้วยการคุ้มครองบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเพื่อการถ่ายโอนข้อมูลบุคคล (Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data on the Free Movement of Such Data) หรือเรียกโดยย่อว่า Directive 95/46/EC เป็นกฎเกณฑ์ที่บัญญัติขึ้นโดยคณะกรรมาธิการยุโรป (European Commission) แห่งประชาคมเศรษฐกิจยุโรป (European Economic Community) ในปี ค.ศ. 1995 Directive นี้ถือเป็นหลักเกณฑ์ต้นแบบหรือเป็นที่มาของการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั่วสหภาพยุโรป[2] เนื่องจากได้มีการกำหนดให้ประเทศสมาชิกให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เทียบเท่ากันในยุโรป โดยใช้ Directive ดังกล่าวเป็นแนวทางในการยกร่าง

---

[2] กฎหมายพื้นฐานที่สำคัญที่สุดของสหภาพยุโรปคือสนธิสัญญา (Treaty) โดยที่มาอันดับแรกของกฎหมายสหภาพยุโรปคือสนธิสัญญาจัดตั้งประชาคมยุโรป ส่วนกฎข้อบังคับลำดับรองของสหภาพยุโรป แบ่งออกเป็น 3 ประเภทหลัก ดังนี้

(1) กฎระเบียบ (Regulation) ใช้บังคับแก่ประเทศสมาชิกทั้งปวง โดยประเทศสมาชิกสหภาพยุโรปจะต้องรับไปใช้ทั้งหมดไม่สามารถปรับเปลี่ยนข้อบทใดๆได้ หากกฎหมายภายในของประเทศสมาชิกมีบทบัญญัติที่ขัดแย้งกับกฎระเบียบแล้ว กฎหมายภายในนั้นจะบังคับใช้มิได้

(2) บทบัญญัติ (Directive) เป็นการกำหนดแนวปฏิบัติให้แก่ประเทศสมาชิกเพื่อนำไปจัดทำกฎหมายภายในประเทศ หรือแก้ไขกฎหมายภายในที่มีอยู่ให้สอดคล้องกับบทบัญญัติของสหภาพยุโรป โดยประเทศสมาชิกจะใช้รูปแบบและวิธีการใดก็ได้เพื่อให้สอดคล้องกับบทบัญญัติ หากประเทศสมาชิกใดไม่ดำเนินการตามแนวปฏิบัติที่กำหนดไว้ คณะกรรมาธิการยุโรปสามารถใช้อำนาจตักเตือนชี้แนะให้มีการปฏิบัติตามบทบัญญัตินั้นได้

(3) คำวินิจฉัย (Decision) เป็นมาตรการเกี่ยวพันกับองค์กร สถาบันหรือประเทศสมาชิกประเทศใด ประเทศหนึ่งโดยตรงในเรื่องใดเรื่องหนึ่งโดยเฉพาะ มีผลผูกพันเฉพาะองค์กรหรือประเทศสมาชิกที่ได้รับคำวินิจฉัย โดยเป็นเครื่องมือด้านการบริหารเพื่อดำเนินการตามกฎหมายของสหภาพยุโรป

นอกจากนี้ยังมีรูปแบบเอกสารที่ไม่มีผลผูกพันทางกฎหมาย ไม่มีสภาพบังคับและผลผูกพันองค์กรหรือประเทศใด ได้แก่ คำแนะนำ (Recommendations) และ ความเห็น (Opinions)

กฎหมาย ทั้งนี้เพื่อให้กฎหมายมีลักษณะเป็นเอกภาพทั่วทั้งยุโรป (for the purpose of creation a uniform level of data protection in europe)[3]

Directive 95/46/EC มีวัตถุประสงค์เพื่อคุ้มครองสิทธิขั้นพื้นฐานและเสรีภาพของบุคคลธรรมดาโดยเฉพาะอย่างยิ่งสิทธิในความเป็นส่วนตัวอันเนื่องจากการประมวลผลข้อมูลส่วนบุคคล ตามที่บัญญัติไว้อย่างชัดเจนในข้อ 1 นอกจากนี้อารัมภบท 2 ยังได้กล่าวขยายเพิ่มเติมอีกด้วยว่า “ระบบประมวลผลข้อมูลนั้นถูกออกแบบมาเพื่ออำนวยประโยชน์แก่มนุษย์ ... ระบบเหล่านี้ต้องเคารพสิทธิและเสรีภาพขั้นพื้นฐานของบุคคลธรรมดาโดยไม่เลือกสัญชาติหรือถิ่นที่อยู่ของบุคคลนั้น โดยเฉพาะสิทธิในความเป็นส่วนตัว”

Directive 95/46/EC ยังมีวัตถุประสงค์เพื่อเป็นต้นแบบในปรับกฎหมายภายในประเทศสมาชิกสหภาพยุโรปให้ได้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในระดับสูงอย่างเท่าเทียมกันด้วย ดังจะเห็นได้จากอารัมภบท 10 ได้วางหลักว่า “ประมวลกฎหมายภายในประเทศว่าด้วยการประมวลผลข้อมูลส่วนบุคคลมีวัตถุประสงค์เพื่อคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐาน โดยเฉพาะสิทธิในความเป็นส่วนตัว ซึ่งได้รับการเห็นชอบทั้งในข้อ 8 ของอนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานแห่งยุโรปและในหลักทั่วไปของกฎหมาย ด้วยเหตุนั้นการปรับกฎหมายเหล่านี้ให้สอดคล้องกันจะต้องมิทำให้การคุ้มครองที่พึงได้ของบุคคลนั้นย่อหย่อนลง แต่ในทางกลับกันจะต้องแสวงหาวิธีที่จะรับรองการคุ้มครองขั้นสูงในประชาคม”

ดังนั้น Directive นี้จึงได้กำหนดให้ประเทศสมาชิกสหภาพยุโรปทั้ง 15 ประเทศ (ในขณะนั้น) มีพันธกรณีที่จะต้องบัญญัติกฎหมายภายในให้สอดคล้องกับหลักเกณฑ์ตาม Directive ภายในสามปีนับแต่ Directive 95/46/EC ได้ปรับปรุงแก้ไขแล้วเสร็จ ต่อมา Directive 95/46/EC ได้ปรับปรุงแก้ไขแล้วเสร็จเมื่อวันที่ 24 ตุลาคม ค.ศ. 1995 ประเทศสมาชิกจึงต้องออกกฎหมายภายในให้แล้วเสร็จภายในวันที่ 24 ตุลาคม ค.ศ. 1998[4]

ขอบเขตของ Directive 95/46/EC ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลทั้งวิธีการประมวลผลโดยอัตโนมัติและวิธีการประมวลผลด้วยมือ (manual) สำหรับวิธีการประมวลผลด้วยมือนั้นข้อมูลส่วนบุคคลที่ถูกประมวลผลด้วยวิธีนี้ต้องเป็นส่วนหนึ่งหรือมีเจตนาที่จะให้เป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูล (filling system) เช่นระบบการจัดเก็บข้อมูลประวัติคนไข้ของโรงพยาบาลต่างๆ

---

[3] กิตติพงศ์ กมลธรรมวงศ์, “การคุ้มครองข้อมูลข่าวสารส่วนบุคคล ในระบบกฎหมายไทย : ปัญหาและแนวทางแก้ไข,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2549), น.91.

[4] *เพิ่งอ้าง*, น.92.

ในหลักการทั่วไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลนั้น ตาม Directive 95/46/EC ได้กำหนดว่าประเทศสมาชิกจะต้องปฏิบัติต่อไปนี้ในการดำเนินการต่อข้อมูลส่วนบุคคล[5]

(1) ข้อมูลส่วนบุคคลต้องถูกประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย

(2) ข้อมูลส่วนบุคคลต้องถูกจัดเก็บโดยมีวัตถุประสงค์ที่ชัดเจน แน่นอน และชอบด้วยกฎหมาย (specified, explicit and legitimate purposes) นอกจากนี้จะต้องไม่มีการประมวลผลข้อมูลที่ขัดแย้งกับวัตถุประสงค์นั้น เว้นแต่เป็นการประมวลผลข้อมูลที่มีวัตถุประสงค์ทางด้านประวัติศาสตร์ สถิติ หรือ วิทยาศาสตร์

(3) ข้อมูลส่วนบุคคลต้องพอเหมาะพอควร (adequate) ไม่มากเกินความจำเป็น (not excessive) และสอดคล้องกับวัตถุประสงค์ในการจัดเก็บ หรือ ประมวลผลข้อมูลนั้น

(4) ข้อมูลส่วนบุคคลต้องมีความถูกต้องครบถ้วน และในกรณีจำเป็นต้องเป็นปัจจุบันด้วย

(5) ไม่ควรเก็บไว้ในรูปแบบที่สามารถระบุตัวบุคคลผู้เป็นเจ้าของไว้นานเกินไป อีกทั้งต้องใช้มาตรการที่เหมาะสมในการรักษาความปลอดภัยของข้อมูล

นอกจากนี้ตาม Directive ยังได้กำหนดให้มีข้อมูลชนิดที่มีความอ่อนไหว (sensitive data) ซึ่งกฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมการประมวลผลข้อมูลส่วนบุคคลที่ต้องใช้มาตรการทางเทคนิคและการจัดการที่เหมาะสม

หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลใน Directive 95/46/EC ในภาพรวมนั้นมีเนื้อหาที่กว้างขวางกว่าหลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวปฏิบัติขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา ตัวอย่างเช่น ได้มีการเพิ่มเติมหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคลชนิดที่มีความอ่อนไหวว่าห้ามมิให้มีการประมวลผลข้อมูลดังกล่าวเว้นแต่จะเข้ากรณีข้อยกเว้น, หลักเกณฑ์การเปิดเผยรายละเอียดต่างๆ เกี่ยวกับการประมวลผลข้อมูล, หลักเกณฑ์การแจ้งรายละเอียดเกี่ยวกับการประมวลผลต่อองค์กรด้านการคุ้มครองข้อมูลส่วนบุคคล, สิทธิในการขอให้ยุติ (Opt-out) การนำข้อมูลส่วนบุคคลไปใช้เพื่อประโยชน์ในธุรกิจการตลาดแบบตรง และสิทธิในการได้รับการชดใช้ค่าเสียหาย

3.1.2 หลักการและวิธีการในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

Directive 95/46/EC ได้วางหลักเกณฑ์ว่าด้วยการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเอาไว้เพื่อให้ความคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมีความต่อเนื่องตลอดสายไม่สะดุดลงเมื่อมีการโอนข้อมูลส่วนบุคคลข้ามประเทศที่มีบริบทของกฎหมาย

[5] *เพิ่งอ้าง*, น.94.

แตกต่างจากประเทศที่ข้อมูลส่วนบุคคลได้ถูกถ่ายโอนไป ซึ่งสามารถจำแนกประเภทการโอนข้อมูลส่วนบุคคลตาม Directive นี้ออกเป็น 2 ประเภท คือ

(1) การโอนข้อมูลส่วนบุคคลไปยังประเทศที่เป็นสมาชิกของสหภาพยุโรป

วิธีการโอนข้อมูลส่วนบุคคลไปยังประเทศที่เป็นสมาชิกของสหภาพยุโรปอยู่แล้วนั้นไม่เป็นปัญหาแต่อย่างใด ประเทศแต่ละประเทศในกลุ่มสมาชิกสหภาพยุโรปสามารถโอนข้อมูลระหว่างกันได้ตามปกติเสมือนเป็นการโอนข้อมูลภายในประเทศเดียวกัน เนื่องจากวัตถุประสงค์ของ Directive 95/46/EC ต้องการให้การโอนถ่ายข้อมูลส่วนบุคคลภายในกลุ่มประเทศสมาชิกสามารถทำได้โดยสะดวก จึงมีการบัญญัติให้ Directive 95/46/EC เป็นดั่งกฎหมายกลางที่ใช้กำหนดวิธีการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มประเทศสมาชิกสหภาพยุโรปให้มีมาตรฐานเดียวกัน อีกทั้งตาม Directive นี้กำหนดให้ประเทศสมาชิกของสหภาพยุโรปมีหน้าที่ต้องบัญญัติกฎหมายภายในให้สอดคล้องกับกฎเกณฑ์ตาม Directive ด้วย กฎหมายภายในที่ประเทศสมาชิกสหภาพยุโรปบัญญัติขึ้นแม้จะมีความแตกต่างกันในรายละเอียดบ้างก็ตาม แต่ในสาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศนั้นต่างบัญญัติตามแนวทางของ Directive 95/46/EC ดังนั้นกลุ่มประเทศสมาชิกสหภาพยุโรปจึงมีมาตรการการคุ้มครองข้อมูลส่วนบุคคลที่เป็นมาตรฐานเดียวกัน ส่งผลให้การโอนข้อมูลส่วนบุคคลระหว่างกลุ่มประเทศสมาชิกเป็นไปโดยสะดวกราบรื่น

(2) การโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรป

การโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มประเทศสมาชิกสหภาพยุโรปมีข้อจำกัดและข้อพิจารณาหลายประการ เนื่องจากประเทศเหล่านั้นอาจมีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่ต่ำกว่ามาตรฐานของ Directive ซึ่งหากมีการอนุญาตให้โอนข้อมูลส่วนบุคคลไปยังประเทศเหล่านั้นได้โดยสะดวกปราศจากข้อจำกัด อาจจะทำให้สิทธิเสรีภาพขั้นพื้นฐานโดยเฉพาะสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลถูกทำลายลง Directive 95/46/EC จึงมีบทบัญญัติในข้อ 25 เพื่อคุ้มครองการโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปไว้

ตามข้อที่ 25 ได้บัญญัติหลักปฏิบัติเอาไว้ว่า ประเทศสมาชิกสหภาพยุโรปนั้นจะถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรป[6] ได้ ก็ต่อเมื่อประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้นสามารถรับรองระดับการคุ้มครองที่เพียงพอ[7] (adequate level of protection) ดังนั้นตาม Directive นี้ จึงห้ามประเทศสมาชิกสหภาพยุโรปโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่มิได้รับรองระดับการคุ้มครองที่เพียงพอ

---

[6] บทบัญญัติของ Directive 95/49/EC ใช้ภาษาอังกฤษคำว่า third country ซึ่งหมายถึงประเทศนอกกลุ่มสมาชิกสหภาพยุโรป

[7] Directive 95/46/EC, ข้อ 25(1)

ในส่วนของระดับการคุ้มครองที่เพียงพอนั้นจะต้องได้ประเมินโดยพิจารณาจากทุกพฤติการณ์แวดล้อม โดยจะต้องไตร่ตรองจากลักษณะของข้อมูล วัตถุประสงค์และระยะเวลาที่ใช้ในการประมวลผล ประเทศที่เป็นจุดเริ่มต้นและประเทศปลายทางในการโอนข้อมูล หลักกฎหมายทั้งกฎหมายทั่วไปและกฎหมายเฉพาะภาคส่วนที่มีผลบังคับใช้ในประเทศนอกกลุ่มสมาชิกสหภาพยุโรปและข้อปฏิบัติทางวิชาชีพรวมถึงมาตรการความปลอดภัยที่ได้รับการปฏิบัติภายในประเทศนั้น[8] ซึ่งเป็นการกำหนดหลักเกณฑ์อย่างกว้าง ไม่ได้ระบุลงรายละเอียดอย่างชัดเจน ทำให้ต่อมาทางประเทศสมาชิกสหภาพยุโรปได้เสนอให้มีแนวทางในการประเมินระดับการคุ้มครองข้อมูลส่วนบุคคล โดยคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล[9] (Working Party) ในปี ค.ศ. 1997 ซึ่งได้กำหนดหลักเกณฑ์ในการพิจารณาที่สำคัญไว้ 2 ประการ[10] คือ ประการที่ 1 เนื้อหาในการคุ้มครองข้อมูลส่วนบุคคล โดยหลักเกณฑ์ที่ใช้บังคับในประเทศนั้นจะต้องมีคุณสมบัติ 6 ประการคือ หลักการประมวลผลข้อมูลภายในขอบวัตถุประสงค์, หลักคุณภาพและความได้สัดส่วนของข้อมูล, หลักความโปร่งใส, หลักการรักษาความปลอดภัย, หลักการให้สิทธิในการเข้าถึงเพื่อขอแก้ไขหรือคัดค้านการประมวลผลของเจ้าของข้อมูล, ข้อจำกัดในการโอนข้อมูลส่วนบุคคลไปต่อ ส่วนหลักเกณฑ์ประการที่ 2 กระบวนการบังคับใช้ โดยกระบวนการบังคับใช้จะต้องประกอบด้วยคุณสมบัติ 3 ประการคือ สามารถบังคับใช้ได้อย่างมีประสิทธิภาพ, การสนับสนุนหรือช่วยเหลือให้เจ้าของข้อมูลให้สามารถใช้สิทธิของตนได้อย่างรวดเร็ว มีประสิทธิภาพและมีค่าใช้จ่ายที่ไม่มากจนเกินไป, สามารถให้การช่วยเหลือเจ้าของข้อมูลเพื่อให้ได้รับการชดใช้ค่าเสียหายในกรณีที่มีการละเมิดข้อมูลส่วนบุคคลอย่างเหมาะสม ทั้งนี้ต้องมีองค์กรอิสระเพื่อทำหน้าที่กำกับดูแลและพิจารณาข้อร้องเรียนต่างเพื่อทำให้มีการปฏิบัติตามหลักเกณฑ์ข้างต้นได้อีกด้วย โดยคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลได้ระบุเอาไว้อย่างชัดเจนว่าการคุ้มครองข้อมูลส่วนบุคคลตามวิธีการดังกล่าว ไม่จำเป็นต้องอยู่ในรูปแบบกฎหมายเสมอไป แต่อาจเป็นวิธีการอื่นใดที่ทำให้บรรลุวัตถุประสงค์ข้างต้นก็ได้เช่นกัน

---

[8] Directive 95/46/EC, ข้อ 25(2)

[9] คณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล (Working Party) ได้ตั้งขึ้นตามข้อ 29 Directive95/46/EC มีสถานะเป็นที่ปรึกษาในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีการดำเนินงานอย่างเป็นอิสระ คณะทำงานนี้มาจากผู้แทนของหน่วยงานที่มีหน้าที่คุ้มครองข้อมูลส่วนบุคคลภายในประเทศสมาชิกสหภาพยุโรปหรือเป็นบุคคลที่หน่วยงานที่มีอำนาจในประเทศนั้นๆแต่งตั้งขึ้น

[10] Article 29 Working Party, “First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy,” Retrieved from <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1997/wp4_en.pdf>, June 1997

3.1.3 ข้อยกเว้นหลักการโอนข้อมูลส่วนบุคคลไปต่างประเทศ

ข้อยกเว้นหลักการห้ามมิให้โอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่ไม่รับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอได้มีการบัญญัติไว้ในข้อ 26 โดยแบ่งเป็น 2 ประเภทคือ

3.1.3.1 ข้อยกเว้นตามกฎหมาย

ในข้อ 26(1) ของ Directive 95/46/EC อนุญาตให้มีการโอนข้อมูลส่วนบุคคลได้หากเข้ากรณีดังต่อไปนี้

(1) เจ้าของข้อมูลยินยอมให้มีการโอนข้อมูลอย่างชัดแจ้ง

(2) การโอนข้อมูลเป็นสิ่งจำเป็นเพื่อการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลหรือการดำเนินการก่อนเข้าทำสัญญาตามที่เจ้าของข้อมูลร้องขอ

(3) การโอนข้อมูลเป็นสิ่งจำเป็นต่อการหาข้อสรุปของสัญญาหรือการปฏิบัติตามสัญญาซึ่งทำเพื่อผลประโยชน์ของเจ้าของข้อมูลที่ได้จัดทำขึ้นระหว่างผู้ควบคุมข้อมูลและบุคคลภายนอก

(4) การโอนข้อมูลเป็นสิ่งจำเป็นหรือเป็นข้อกำหนดตามกฎหมายในการดำรงไว้ซึ่งประโยชน์สาธารณะที่สำคัญ หรือเพื่อการก่อตั้งสิทธิเรียกร้อง การดำเนินการหรือต่อสู้คดีทางกฎหมาย

(5) การโอนข้อมูลเป็นสิ่งจำเป็นในการคุ้มครองผลประโยชน์สำคัญของเจ้าของข้อมูล

(6) การโอนข้อมูลโดยเก็บบันทึกข้อมูลซึ่งตามกฎหมายหรือระเบียบมีหน้าที่ให้ต่อสาธารณชน และซึ่งเปิดให้มีการเข้าค้นหาข้อมูลได้ทั้งโดยบุคคลทั่วๆไปหรือโดยบุคคลใดบุคคลหนึ่งซึ่งสามารถแสดงได้ว่าตนมีประโยชน์ส่วนได้เสียที่ชอบด้วยกฎหมายโดยเฉพาะ ภายใต้ขอบเขตว่าประโยชน์ดังกล่าวนั้นจะต้องเป็นไปตามเงื่อนไขที่กำหนดไว้โดยกฎหมายที่ให้เปิดเผยในกรณีนั้นๆ

3.1.3.2 ข้อยกเว้นจากการตกลงทำสัญญา

นอกจากข้อยกเว้นตามกฎหมายข้างต้นที่ทำให้ประเทศสมาชิกสหภาพยุโรปสามารถโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่ไม่มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอแล้ว ยังสามารถใช้วิธีการโอนข้อมูลส่วนบุคคลในรูปของการทำข้อสัญญาที่เหมาะสม (appropriate contractual clauses) ตามข้อ 26(2) ซึ่งเป็นสัญญาที่มีการกำหนดแม่แบบของสัญญาเอาไว้โดยคณะกรรมาธิการยุโรป โดยหากผู้โอนและผู้รับโอนข้อมูลได้ทำสัญญาระหว่างกันตามสัญญาแม่แบบก็จะสามารถโอนข้อมูลส่วนบุคคลตามข้อยกเว้นได้เช่นกัน

สัญญาแม่แบบ[11] (standard contractual clauses) ที่ใช้ในการโอนข้อมูลนั้นจะต้องมีเนื้อหาสำคัญเกี่ยวกับหน้าที่ของผู้โอนข้อมูล (data exporter) และ ผู้รับโอนข้อมูล (data importer), สัญญาเพื่อประโยชน์ของบุคคลภายนอก (third-party beneficiary clause) โดยให้สิทธิแก่เจ้าของข้อมูลซึ่งเป็นบุคคลภายนอกสัญญาสามารถเข้าใช้สิทธิเรียกร้องให้มีการปฏิบัติตามสัญญา หรือเรียกร้องค่าเสียหายที่เกิดขึ้นในกรณีที่มีการละเมิดข้อสัญญาได้และเพื่อให้เจ้าของข้อมูลสามารถบังคับใช้สิทธิของตนได้อย่างมีประสิทธิภาพ สัญญาแม่แบบดังกล่าวจึงได้กำหนดให้ผู้ส่งออกและผู้นำเข้าข้อมูลต้องรับผิดร่วมกันในหลายกรณี โดยเจ้าของข้อมูลสามารถใช้สิทธิเรียกร้องที่เกิดขึ้นจากการที่ผู้รับโอนข้อมูลละเมิดข้อสัญญาต่อผู้โอนข้อมูลได้โดยตรง นอกจากนี้ในสัญญาควรระบุเกี่ยวกับการไกล่เกลี่ยข้อพิพาทและเขตอำนาจศาล, การให้ความร่วมมือกับหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคล, การสิ้นสุดของสัญญา, กฎหมายที่นำมาใช้บังคับแก่สัญญา เป็นต้น[12]

จะเห็นได้ว่าสัญญาแม่แบบได้กำหนดเนื้อหาที่จำเป็นต้องมีเกี่ยวกับสิทธิและหน้าที่ของคู่กรณีอันเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลไว้เท่านั้น ทำให้ผู้โอนข้อมูลหรือผู้รับโอนข้อมูลส่วนบุคคลสามารถเพิ่มเติมข้อสัญญาอื่นใดที่เกี่ยวข้องกับการดำเนินการทางธุรกิจที่นอกเหนือไปจากที่ระบุไว้ในสัญญาแม่แบบนี้ได้เช่นกัน เช่น ข้อตกลงเกี่ยวกับความร่วมมือ (mutual assistance) กับเจ้าของข้อมูลหรือกับหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีข้อโต้แย้งหรือข้อพิพาทต่างๆ ซึ่งการเพิ่มเติมข้อสัญญานั้นสามารถกระทำได้ตราบเท่าที่เนื้อหาไม่ขัดแย้งกับสัญญาแม่แบบ

3.1.4 องค์กรที่มีหน้าที่บังคับการให้เป็นไปตามกฎหมาย

องค์กรที่ทำหน้าที่เกี่ยวข้องกับการคุ้มครองข้อมูลและการโอนข้อมูลตาม Directive 95/46/EC แบ่งเป็น 2 องค์กรหลักๆคือ คณะกรรมาธิการยุโรป (European Commission) และหน่วยงานในประเทศที่หน้าที่คุ้มครองข้อมูลส่วนบุคคล (Supervisory Authority)

3.1.4.1 คณะกรรมาธิการยุโรป

คณะกรรมาธิการยุโรปเป็นองค์กรด้านบริหารองค์กรหนึ่งของสหภาพยุโรป โดยเป็นอิสระจากรัฐบาลของแต่ละชาติ คณะกรรมาธิการยุโรปประกอบด้วยกรรมาธิกร 28 คน จากแต่ละประเทศสมาชิกตามความเชี่ยวชาญ โดยภารกิจหลักของคณะกรรมาธิการยุโรปคือการเสนอร่างกฎหมาย นอกจากนั้นยังดูแลการบริหารงบประมาณของสหภาพยุโรป ตาม Directive 95/46/EC ได้ให้อำนาจแก่คณะกรรมาธิการยุโรปในการพิจารณาชี้ขาดว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่รับโอนข้อมูลส่วนบุคคลมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่

---

[11] โปรดดูตัวอย่างสัญญาแม่แบบตามคำวินิจฉัยของคณะกรรมาธิการยุโรป ที่ภาคผนวก ง

[12] ปฏิวัติ อุ่นเรือน, *อ้างแล้ว เชิงอรรถที่ 1*, น.74.

ในกรณีที่ประเทศนอกกลุ่มสมาชิกสหภาพยุโรปสามารถรับรองว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอจะทำให้ประเทศนั้นๆสามารถรับโอนข้อมูลจากกลุ่มประเทศสมาชิกสหภาพยุโรปอย่างไร้ข้อจำกัดเสมือนกับว่าเป็นการโอนข้อมูลเฉกเช่นเดียวกับการโอนข้อมูลระหว่างกลุ่มประเทศสมาชิกสหภาพยุโรปด้วยกันโดยมีผลใช้กับประเทศสมาชิกทุกประเทศ แต่ในกรณีที่มีประเด็นการถกเถียงเกิดขึ้นว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้นมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่ ประเด็นถกเถียงนั้นจะต้องเข้าสู่การตัดสินชี้โดยคณะกรรมาธิการยุโรป

ในกรณีที่คณะกรรมาธิการยุโรปได้ตัดสินว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปมิได้รับรองระดับการคุ้มครองข้อมูลที่เพียงพอ ประเทศสมาชิกจะต้องใช้มาตรการที่จำเป็นในการป้องกันมิให้มีการโอนข้อมูลประเภทเดียวกันนี้ไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่อยู่ในประเด็นถกเถียง[13] ซึ่งเป็นข้อบังคับห้ามโอนข้อมูลส่วนบุคคลในทุกประเทศสมาชิกสหภาพยุโรป

วิธีการแก้ไขปัญหาที่เกิดขึ้นจากการไม่สามารถโอนข้อมูลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปได้นั้นคณะกรรมาธิการยุโรปจะต้องเข้าร่วมการเจรจาต่อรองกับตัวแทนประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่เกี่ยวข้องโดยมีจุดมุ่งหมายที่จะฟื้นฟูแก้ไขสถานการณ์ที่มิสามารถโอนข้อมูลส่วนบุคคลได้ภายในระยะเวลาที่เหมาะสม[14] หลังจากมีการเจรจาจนเกิดข้อสรุปในการจัดทำข้อกฎหมายภายในหรือพันธะสัญญาระหว่างแล้ว คณะกรรมาธิการยุโรปมีสิทธิตัดสินชี้ขาดอีกครั้งว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปได้รับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอแล้วหรือไม่ โดยประเทศสมาชิกสหภาพยุโรปจะมีผลผูกพันต้องปฏิบัติตามคำชี้ขาดและกำหนดมาตรการที่สอดคล้องกับผลที่เกิดจากคำชี้ขาดของคณะกรรมการยุโรปด้วย

3.1.4.2 หน่วยงานในประเทศที่มีหน้าที่คุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคลให้ได้มีประสิทธิภาพนั้นจำเป็นต้องมีการจัดตั้งหน่วยงานที่ทำหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลในประเทศสมาชิกที่สามารถทำหน้าที่ได้อย่างอิสระสมบูรณ์ ข้อ 28 ของ Directive 95/46/EC จึงได้บัญญัติให้ประเทศสมาชิกสหภาพยุโรปแต่ละประเทศจัดตั้งและมอบหมายให้มีเจ้าหน้าที่รัฐผู้หน้าที่กำกับดูแลและตรวจสอบการนำบทบัญญัติซึ่งประเทศสมาชิกได้ลงมติยอมรับตาม Directive นี้มาปรับใช้ภายในอาณาเขตของประเทศตน

---

[13] Directive 95/46/EC, ข้อ 25(4)

[14] Directive 95/46/EC, ข้อ 25(5)

เจ้าหน้าที่ของหน่วยงานคุ้มครองข้อมูลส่วนบุคคลแต่ละประเทศนั้นมีสิทธิในการปฏิบัติหน้าที่ที่ได้รับมอบหมายอย่างอิสระสมบูรณ์ โดยเจ้าหน้าที่แต่ละคนได้มีอำนาจดำเนินการหลักๆ ต่อไปนี้[15]

(1) อำนาจในการสืบสวน เช่น อำนาจในการเข้าถึงข้อมูลหลักที่ใช้ในการประมวลผลข้อมูลและอำนาจในการเก็บรวบรวมทุกข้อมูลที่จำเป็นในการทำหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(2) อำนาจในการแทรกแซง เช่น อำนาจในการเสนอข้อคิดเห็นก่อนที่ประมวลผลข้อมูลจะเสร็จสิ้นลงและรับรองให้การเผยแพร่ข้อคิดเห็นเหล่านั้นเป็นไปอย่างเหมาะสม อำนาจในการสั่งกีดกัน ลบ หรือทำลายข้อมูล ในการสั่งระงับมิให้มีการประมวลผลทั้งโดยชั่วคราวหรือโดยถาวรในการตักเตือนหรือท้วงติงผู้ควบคุมข้อมูลหรือในการอ้างปัญหานั้นๆในรัฐสภาแห่งชาติหรือสถาบันทางการเมืองอื่นๆ

(3) อำนาจในการเข้าไปมีส่วนร่วมกับกระบวนการพิจารณาทางกฎหมายในกรณีที่มีการฝ่าฝืนบทบัญญัติภายในประเทศที่ได้รับมติให้มีผลบังคับใช้ตาม Directive หรือในการนำกรณีที่ฝ่าฝืนบทบัญญัติเข้าสู่การพิจารณาคดีขององค์กรตุลาการ

เจ้าหน้าที่แต่ละคนมีหน้าที่ต้องรับฟังข้อร้องเรียนเกี่ยวกับการคุ้มครองสิทธิเสรีภาพที่อาจได้รับผลกระทบจากการประมวลผลข้อมูลส่วนบุคคลของบุคคลนั้น โดยเฉพาะอย่างยิ่งข้อเรียกร้องให้ตรวจสอบความชอบธรรมของกฎหมายที่บัญญัติขึ้นจากการนำเอาหลักการตาม Directive นี้มาบังคับใช้

3.2 โครงการเซฟฮาร์เบอร์ (Safe Harbour Privacy Principles) ของประเทศสหรัฐอเมริกา

3.2.1 ความเป็นมาและวัตถุประสงค์ของโครงการเซฟฮาร์เบอร์

3.2.1.1 ความเป็นมาของโครงการเซฟฮาร์เบอร์

ประเทศสหรัฐอเมริกาเป็นประเทศที่มีความเป็นมาทางประวัติศาสตร์ที่แตกต่างจากประเทศในภาคพื้นยุโรปค่อนข้างมาก ทำให้แนวคิดพื้นฐานทางกฎหมายของประเทศสหรัฐอเมริกามีความแตกต่างจากประเทศในภาคพื้นยุโรปพอสมควร กฎหมายเกี่ยวกับความเป็นส่วนตัวของประเทศสหรัฐอเมริกาจะมีลักษณะการคุ้มครองความเป็นส่วนตัวที่ต้องการป้องกันการใช้

[15] Directive 95/46/EC, ข้อ 28(3)

ข้อมูลในทางที่จะก่อให้เกิดความเสียหาย (harmful use of information) ขณะที่ในภาคพื้นยุโรปนั้นมุ่งคุ้มครองความเป็นส่วนตัวในฐานะที่เป็นสิทธิมนุษยชน[16]

ระบบการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในประเทศสหรัฐอเมริกานั้นมีลักษณะการบัญญัติเป็นระบบกฎหมายเฉพาะเรื่องเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในแต่ละเรื่องเป็นการเฉพาะ เช่นกฎหมายว่าด้วยการรายงานข้อมูลผู้บริโภคที่เป็นธรรม ค.ศ. 1970, กฎหมายคุ้มครองข้อมูลส่วนบุคคลทางอินเทอร์เน็ตของเด็ก ค.ศ. 1998, กฎหมายว่าด้วยนวัตกรรมทางการเงิน ค.ศ. 1999 เป็นต้น ประเทศสหรัฐอเมริกาไม่มีกฎหมายแม่บทหรือกฎหมายกลางที่วางหลักเกณฑ์เป็นการทั่วไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รัฐสภาสหรัฐฯจะตรารัฐบัญญัติก็ต่อเมื่อเกิดปัญหาการป้องกันความลับหรือเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวของประชาชนเมื่อถูกละเมิด เหตุผลที่อยู่เบื้องหลังการเลือกให้การคุ้มครองข้อมูลส่วนบุคคลโดยการบัญญัติกฎหมายเป็นการเฉพาะคือเพื่อต้องการให้มีกฎหมายที่สามารถปรับใช้ได้กับเทคโนโลยีที่มีการเปลี่ยนแปลงไปตลอดเวลา[17] การออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอเมริกาจึงมีลักษณะเป็นการวิ่งไล่แก้ปัญหาที่เกิดขึ้นมากกว่าที่จะวางหลักเกณฑ์ทั่วไปในการแก้ไขปัญหา[18]

นอกจากการบัญญัติกฎหมายเฉพาะเรื่องแล้วประเทศสหรัฐอเมริกายังใช้รูปแบบการคุ้มครองข้อมูลส่วนบุคคลด้วยกลไกกำกับดูแลตนเอง ซึ่งเป็นผลจากแนวคิดในการส่งเสริมการดำเนินธุรกิจแบบเสรี ทำให้ในประเทศสหรัฐอเมริกามีระบบที่เน้นให้องค์กรภาคเอกชนได้สร้างกลไกในการคุ้มครองและควบคุมกันเอง เช่น การกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล รวมไปถึงการรวมตัวของผู้ประกอบธุรกิจเพื่อทำหน้าที่ให้บริการเครื่องหมายรับรองความน่าเชื่อถือสำหรับการคุ้มครองความเป็นส่วนตัวในระบบพาณิชย์อิเล็กทรอนิกส์ เช่น TRUSTe, BBBOnline, WebTrust เป็นต้น

แต่อย่างไรก็ตามเมื่อสหภาพยุโรปมีการประกาศใช้ Directive 95/46/EC เพื่อคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศสมาชิกสหภาพยุโรปนั้น ตามข้อ 25 ของ Directive ดังกล่าววางหลักว่าด้วยการโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรป ซึ่งจะสามารถโอนข้อมูลส่วนบุคคลไปได้เมื่อประเทศที่รับโอนข้อมูลมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ มิฉะนั้นจะไม่สามารถรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรปได้ ซึ่ง

---

[16] ชวิน อุ่นภัทร, “ความเป็นส่วนตัวและการคุ้มครองจากการล่วงล้ำของรัฐในประเทศสหรัฐอเมริกา,”วารสารนิติศาสตร์, ปีที่ 44 ฉบับที่ 4, น.981, (ธันวาคม 2558).

[17] Electronic Privacy Information Center, *supra note* 35.

[18] ประสิทธิ์ ปิวาวัฒนพานิช, “กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย,” วารสารนิติศาสตร์, ปีที่ 34, ฉบับที่ 4, น.537 (2547).

กลุ่มประเทศสมาชิกสหภาพยุโรปต้องปฏิบัติตาม Directive นี้ ทำให้ในช่วงแรกนั้นเกิดปัญหาในการโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรปมายังประเทศสหรัฐอเมริกา เพราะเหตุว่าประเทศสหรัฐอเมริกาไม่ได้รับการพิจารณาจากประเทศสมาชิกสหภาพยุโรปว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอแต่อย่างใด ปัจจัยสำคัญเนื่องจากประเทศสหรัฐอเมริกามีบทบัญญัติที่ใช้คุ้มครองความเป็นส่วนตัวแยกเป็นส่วนๆ กระจัดกระจายอยู่ตามบทบัญญัติ กฎเกณฑ์ข้อบังคับหลายๆฉบับ และใช้กลไกกำกับดูแลตนเองภายในองค์กร ต่างจากประเทศสมาชิกสหภาพยุโรปที่ใช้ระบบกฎหมายแม่บทเป็นกฎหมายกลาง ความแตกต่างดังกล่าวทำให้สหภาพยุโรปมองว่าการไม่มีกฎหมายกลางที่เป็นบททั่วไปในการคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาเป็นมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอตามที่สหภาพยุโรปกำหนด[19] ปัจจัยสำคัญอีกประการหนึ่งคือประเทศสหรัฐอเมริกาไม่มีองค์กรระดับชาติที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ[20] ทำให้ประเทศสมาชิกสหภาพยุโรปตัดสินว่าประเทศสหรัฐอเมริกาไม่มีมาตรการด้านคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ

ผลจากการที่ประเทศสหรัฐอเมริกาไม่ได้ดำเนินการเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลอยู่ในระดับที่เพียงพอตามมาตรฐานของกลุ่มประเทศสมาชิกสหภาพยุโรปได้ส่งผลกระทบขึ้นอย่างเป็นรูปธรรมในปี ค.ศ. 1998 ในกรณีข้อพิพาทระหว่างคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประเทศสวีเดนกับบริษัทสายการบินอเมริกัน โดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประเทศสวีเดน ได้มีคำสั่งให้บริษัทสายการบินอเมริกันลบข้อมูลด้านสุขภาพ ข้อมูลด้านการรักษาพยาบาลของผู้โดยสารสัญชาติสวีเดนในทันทีภายหลังจากได้เดินทางถึงที่หมายแล้วในทุกเที่ยวบิน เว้นแต่จะได้รับการยินยอมจากผู้โดยสารโดยชัดแจ้ง (explicit consent) ว่าอนุญาตให้ทำการเก็บข้อมูลนั้นต่อไปนี้ ซึ่งปกติแล้วจะมีการเก็บข้อมูลต่างๆเหล่านี้ในขณะที่ทำการจองตั๋วเครื่องบิน ผลของคำสั่งดังกล่าวนี้เองส่งผลให้บริษัทสายการบินอเมริกันไม่สามารถส่งข้อมูลไปยังศูนย์กลางระบบการจองตั๋วโดยสาร (SABRE central reservation system) ที่ตั้งอยู่ในประเทศสหรัฐอเมริกาได้ ต่อมาบริษัทสายการบินอเมริกันก็ได้ยื่นอุทธรณ์คำสั่งข้างต้นต่อศาลปกครองชั้นต้นในประเทศสวีเดน

---

[19] นคร เสรีรักษ์, <u>ความเป็นส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย</u>, (กรุงเทพมหานคร : สำนักพิมพ์พีเพรส, 2557), น.166.

[20] John R. Vacca, “The European Data Protection Directive : A Roadblock to International Trade?”, in <u>The Privacy Papers : Managing Technology, Consumer, Employee, and Legislative Action</u>, ed.Pebecca Herole (New York : CRC Press LLC , 2002), p.570 อ้างถึงใน ปฏิวัติ อุ่นเรือน, “ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ” (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), น.42.

โดยให้เหตุผลว่าการขอความยินยอมจากผู้โดยสารโดยชัดแจ้งเพื่อให้มีการโอนข้อมูลส่วนบุคคลไปยังสหรัฐอเมริกานั้นไม่สามารถทำได้ในทางปฏิบัติ (impractical) อีกทั้งก่อให้เกิดความไม่สะดวกแก่ผู้โดยสารเนื่องจากจำเป็นต้องให้ข้อมูลใหม่ทุกครั้งที่จองตั๋วเครื่องบินกับทางบริษัท อย่างไรก็ตามศาลปกครองก็ไม่เห็นด้วยกับข้ออุทธรณ์ดังกล่าว โดยให้เหตุผลว่าความไม่สะดวกของผู้โดยสารไม่อาจนำมาใช้เป็นข้อยกเว้นในการบังคับใช้กฎหมายได้ หลังจากนั้นก็ได้มีการยื่นอุทธรณ์ต่อไปยังศาลปกครองสูงสุดซึ่งศาลปกครองสูงสุดก็ได้ยกคำร้องอุทธรณ์ดังกล่าวเช่นกัน[21]

จากกรณีข้างต้นจะเห็นว่าผู้ประกอบการและองค์กรต่างๆในประเทศสหรัฐอเมริกาได้รับผลกระทบจากหลักเกณฑ์การโอนข้อมูลส่วนบุคคลที่เข้มงวดซึ่งเป็นผลมาจากการบัญญัติ Directive 95/46/EC แนวทางการแก้ปัญหาเฉพาะนั้นผู้ประกอบการมักจะจัดทำสัญญาโอนข้อมูลส่วนบุคคลเพื่อทำให้สามารถรับโอนข้อมูลจากลูกค้าหรือพนักงานในประเทศสมาชิกสหภาพยุโรปได้ แต่การทำสัญญาโอนข้อมูลส่วนบุคคลนั้นใช้งบประมาณและระยะเวลาในการดำเนินการมาก ส่วนอีกวิธีหนึ่งที่นำมาใช้ในการแก้ปัญหาคือการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแต่วิธีดังกล่าวก็ประสบปัญหาในทางปฏิบัติเช่นกัน เนื่องจากประสบปัญหาว่าจะใช้หลักเกณฑ์ใดมาพิจารณาว่าได้รับความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้งแล้ว เนื่องจากประเทศสมาชิกสหภาพยุโรปแต่ละประเทศได้กำหนดหลักเกณฑ์การให้ความยินยอมที่แตกต่างกันไป

เพื่อหลีกเลี่ยงปัญหาที่กำลังเกิดขึ้นและอาจนำมาสู่ความขัดแย้งที่รุนแรงขึ้นในอนาคตจากการรับโอนข้อมูลส่วนบุคคลจากประเทศสมาชิกสหภาพยุโรป รัฐบาลประเทศสหรัฐอเมริกาโดยกระทรวงพาณิชย์ (Department of Commerce) จึงได้เริ่มเจรจากับคณะกรรมาธิการยุโรปเพื่อหาทางออกในการสร้างความเชื่อมั่นว่าประเทศสหรัฐอเมริกามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและสร้างความมั่นใจให้ประเทศสมาชิกสหภาพยุโรปในการโอนข้อมูลส่วนบุคคลมายังสหรัฐอเมริกาได้

ผลจากการเจรจาเป็นระยะเวลาสองปีระหว่างคณะกรรมาธิการยุโรปและสหรัฐอเมริกา ก่อให้เกิดข้อตกลงระหว่างคณะกรรมาธิการยุโรปกับรัฐบาลสหรัฐอเมริกาที่เรียกว่า “Safe Harbour Privacy Principles” หรือโครงการเซฟฮาร์เบอร์ เมื่อวันที่ 21 กรกฎาคม ค.ศ. 2000 และคณะกรรมาธิการยุโรปได้รับรองว่าประเทศสหรัฐอเมริกามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอโดยการออกคำวินิจฉัยที่ 2000/520 ตามมาเมื่อวันที่ 26 กรกฎาคม ค.ศ. 2000

---

[21] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารและสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, การโอนข้อมูลส่วนบุคคลระหว่างประเทศ, (กรุงเทพมหานคร : สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี, 2548), น.31-32.

3.2.1.2 วัตถุประสงค์ของโครงการเซฟฮาร์เบอร์

หลักการของโครงการเซฟฮาร์เบอร์ในช่วงต้นระบุเอาไว้ว่า “...ภายใต้อำนาจตามกฎหมายในการส่งเสริม สนับสนุน และพัฒนาการค้าระหว่างประเทศ หลักการเซฟฮาร์เบอร์ได้กำหนดขึ้นโดยการปรึกษาหารือกับภาคอุตสาหกรรมและประชาชนโดยทั่วไปเพื่ออำนวยความสะดวกให้แก่การค้าและการพาณิชย์ระหว่างสหรัฐอเมริกาและสหภาพยุโรป หลักการของโครงการเซฟฮาร์เบอร์มีจุดมุ่งหมายเพื่อให้องค์กรของสหรัฐอเมริกาที่ได้รับข้อมูลส่วนบุคคลจากสหภาพยุโรปปฏิบัติตามเพื่อปรับองค์กรให้มีคุณสมบัติเหมาะสมกับโครงการเซฟฮาร์เบอร์และเพื่อตอบสนองต่อระดับการคุ้มครองที่เพียงพอที่ได้สร้างขึ้นไว้เท่านั้น เนื่องจากโครงการเซฟฮาร์เบอร์ได้รับการออกแบบมาเพื่อจุดประสงค์เฉพาะนี้เพียงอย่างเดียว การนำหลักการนี้ไปใช้กับจุดประสงค์อื่นๆอาจเป็นการไม่เหมาะสม...” จากหลักการดังกล่าวจะเห็นได้ว่าวัตถุประสงค์ของโครงการเซฟฮาร์เบอร์มีขึ้นเพื่อให้ประเทศสหรัฐอเมริกาสามารถรับโอนข้อมูลจากกลุ่มประเทศสมาชิกสหภาพยุโรปได้โดยสะดวกปราศจากอุปสรรค และเพื่ออำนวยความสะดวกให้ภาคธุรกิจองค์กรเอกชนต่างๆที่กำลังขยายตัวอย่างรวดเร็วในประเทศสหรัฐอเมริกาสามารถถ่ายโอนข้อมูลจากกลุ่มประเทศสมาชิกสหภาพยุโรปเพื่อนำข้อมูลมาประมวลผลและใช้เพื่อประโยชน์ทางธุรกิจได้สะดวกยิ่งขึ้น สามารถลดขั้นตอนการโอนข้อมูลส่วนบุคคลที่ยุ่งยากได้โดยปราศจากปัญหา ไม่สิ้นเปลืองทรัพยากรและใช้เวลานานดังเช่นกรณีปัญหาที่เกิดขึ้นก่อนการจัดให้มีโครงเซฟฮาร์เบอร์นั่นเอง

ต่อมาหลักการเซฟฮาร์เบอร์ได้รับการรับรองจากคณะกรรมาธิการยุโรปโดยการออกคำวินิจฉัยที่ 2000/520 ซึ่งในอารัมภบท 2 ของคำวินิจฉัยดังกล่าวได้บัญญัติไว้ว่า “คณะกรรมาธิการอาจตัดสินว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปได้รับรองระดับการคุ้มครองที่เพียงพอ ในกรณีนี้ข้อมูลส่วนบุคคลอาจถูกถ่ายโอนจากประเทศสมาชิกได้โดยไม่จำเป็นต้องมีการยื่นหลักประกันเพิ่มเติม” แสดงการยืนยันว่าเมื่อคณะกรรมาธิการยุโรปตัดสินว่าประเทศสหรัฐอเมริกาได้รับรองระดับการคุ้มครองข้อมูลที่เพียงพอแล้วจะทำให้สามารถรับโอนข้อมูลจากกลุ่มประเทศสมาชิกสหภาพยุโรปได้โดยไม่มีเงื่อนไขและข้อจำกัดอื่นใดเพิ่มเติม

อีกทั้งข้อ 1(1) ของคำวินิจฉัยดังกล่าวก็ได้บัญญัติว่า “ตามวัตถุประสงค์ของข้อ 25(2) ของ Directive 95/46/EC สำหรับทุกกิจกรรมที่อยู่ในขอบข่ายของ Directive หลักคุ้มครองความเป็นส่วนตัวของโครงการเซฟฮาร์เบอร์ดังที่บรรยายไว้ในภาคผนวกที่ 1 ของคำวินิจฉัยซึ่งได้รับการดำเนินงานตามแนวทางปฏิบัติที่กำหนดโดยข้อสงสัยที่ได้รับการซักถามบ่อยครั้ง (FAQs) ที่ออกโดยกระทรวงพาณิชย์สหรัฐในวันที่ 21 กรกฎาคม ค.ศ. 2000 ดังที่บรรยายไว้ในภาคผนวกที่ 2 ของคำวินิจฉัยนี้ได้รับการพิจารณาว่าสามารถรับรองระดับการคุ้มครองที่เพียงพอสำหรับข้อมูลส่วนบุคคลที่ถูกถ่ายโอนจากประชาคมไปยังองค์กรที่จัดตั้งขึ้นในประเทศสหรัฐอเมริกา” เป็นการยืนยันการ

พิจารณาตัดสินโดยคณะกรรมาธิการยุโรปว่าประเทศสหรัฐอเมริกาได้รับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

จะเห็นได้ว่าเมื่อมีการตัดสินจากคณะกรรมาธิการยุโรปว่าประเทศสหรัฐอเมริกาได้รับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอดังกล่าว ส่งผลให้ประเทศสหรัฐอเมริกาสามารถรับโอนข้อมูลจากกลุ่มประเทศสมาชิกสหภาพยุโรปได้อย่างไม่มีข้อจำกัด อันเป็นการตอบโจทย์วัตถุประสงค์ในการจัดให้มีโครงการเซฟฮาร์เบอร์ดังที่ได้กล่าวไว้ในตอนต้น

3.2.2 หลักการและวิธีการในการรับโอนข้อมูลระหว่างประเทศตามโครงการเซฟฮาร์เบอร์

องค์กรบริษัทหรือผู้ประกอบการใดก็ตามที่รับส่งข้อมูลกับประเทศสมาชิกสหภาพยุโรปจะต้องได้รับการรับรองตามข้อตกลงของโครงการเซฟฮาร์เบอร์จึงจะถือว่ามีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอในการรับโอนข้อมูลส่วนบุคคลจากประเทศสมาชิกสหภาพยุโรปได้[22] โดยบริษัทหรือองค์กรใดก็ตามที่มีความประสงค์เข้าร่วมในโครงการเซฟฮาร์เบอร์จะต้องปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคล 7 ประการดังต่อไปนี้

(1) หลักการแจ้งให้ทราบ (Notice)

องค์กรต้องแจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์ในการรวบรวมและประมวลผลข้อมูลส่วนบุคคล รวมไปถึงการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยในกรณีใดบ้าง อีกทั้งวิธีการที่เจ้าของข้อมูลจะใช้สิทธิในการควบคุมหรือจำกัดการประมวลผลข้อมูลส่วนบุคคลของตน

(2) หลักการให้สิทธิเลือก (Choice)

องค์กรต้องให้สิทธิแก่เจ้าของข้อมูลในการเลือกที่จะปฏิเสธไม่ให้ข้อมูลของเขาถูกเผยแพร่แก่บุคคลที่สาม หรือปฏิเสธการนำข้อมูลที่เกี่ยวกับตนไปใช้ในวัตถุประสงค์อื่นๆที่ไม่เกี่ยวข้องหรือไม่สอดคล้องกับวัตถุประสงค์ที่ได้ให้ไว้ในตอนแรก หรือหากเป็นกรณีข้อมูลส่วนบุคคลที่มีความอ่อนไหว อาทิ ข้อมูลด้านสุขภาพ เชื้อชาติ การใช้หรือการเปิดเผยต้องได้รับความยินยอมอย่างชัดแจ้งและได้รับการยืนยันจากเจ้าของข้อมูลว่าสามารถเปิดเผยหรือถูกนำไปใช้ได้ ในกรณีที่ต้องมีการเปิดเผยแก่บุคคลภายนอกหรือมีการใช้ในวัตถุประสงค์อื่นๆ

(3) หลักการห้ามโอนข้อมูลต่อ (Onward Transfer)

องค์กรต้องให้การรับรองว่าจะไม่โอนหรือเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลอื่นต่อไป เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลเสียก่อน ทั้งนี้บุคคลผู้รับโอนข้อมูลส่วนบุคคลต่อไปนั้นจะต้องเป็นองค์กรที่เข้าร่วมโครงการเซฟฮาร์เบอร์หรือเป็นองค์กรที่ตกอยู่ภายใต้ผลการบังคับของ Directive หรือได้ทำสัญญาการโอนข้อมูลส่วนบุคคล

(4) หลักการรักษาความปลอดภัย (Security)

---

[22] นคร เสรีรักษ์, *อ้างแล้ว เชิงอรรถที่ 19*, น.167.

องค์กรต้องมีนโยบายและมาตรการรักษาความปลอดภัยในข้อมูลส่วนบุคคลที่เพียงพอ เพื่อป้องกันการใช้หรือเปิดเผยโดยมิชอบ ตลอดจนมีมาตรการป้องกันการสูญหาย การเปลี่ยนแปลงแก้ไข การทำลาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(5) หลักความถูกต้องแท้จริงของข้อมูล (Data Integrity)

ข้อมูลที่บริษัทหรือองค์กรจะนำไปประมวลผลต้องเป็นข้อมูลที่มีความเกี่ยวข้องกับวัตถุประสงค์ในการจัดเก็บและองค์กรต้องจัดให้มีวิธีการที่เหมาะสมและเชื่อถือได้ว่าข้อมูลที่จะถูกนำไปใช้นั้นมีความถูกต้องแท้จริง ครบถ้วน และเป็นปัจจุบัน

(6) หลักการเข้าถึงข้อมูล (Access)

องค์กรต้องเปิดโอกาสให้เจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคลของตน ตลอดจนให้สิทธิแก่เจ้าของข้อมูลในการลบ เปลี่ยนแปลงหรือปรับปรุงข้อมูลส่วนบุคคลของตนให้ถูกต้องภายใต้เงื่อนไขและวิธีการอันสมเหตุสมผล

(7) หลักการบังคับใช้ (Enforcement)

ผู้ประกอบการจะต้องเผยแพร่วิธีการระงับข้อพิพาทที่เกิดขึ้นอันเนื่องจากข้อมูลส่วนบุคคลและต้องปฏิบัติตามวิธีการดังกล่าว ทั้งนี้ วิธีการระงับข้อพิพาทดังกล่าวจะต้องครอบคลุมถึงการให้สิทธิแก่เจ้าของข้อมูลในการร้องเรียน (complain) เพื่อให้มีการสอบสวนและชี้ขาดในกรณีที่มิได้ปฏิบัติตามหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลตามโครงการเซฟฮาร์เบอร์ด้วย

การตัดสินขององค์กรที่จะเข้าร่วมกับโครงการเซฟฮาร์เบอร์เป็นไปด้วยความสมัครใจทั้งหมด (voluntary) โดยองค์กรต่างๆสามารถปรับองค์กรให้มีคุณสมบัติเหมาะสมสอดคล้องกับหลักการทั้ง 7 ประการของโครงการเซฟฮาร์เบอร์ได้ด้วยวิธีที่แตกต่างกัน ซึ่งบริษัทหรือองค์กรดังกล่าวสามารถเลือกที่จะดำเนินการในทางใดทางหนึ่งดังนี้

(1) เข้าร่วมโครงการกลไกกำกับดูแลตนเองที่มีหลักการสอดคล้องกับหลักเกณฑ์ของเซฟฮาร์เบอร์ เช่น เข้าร่วมเป็นสมาชิกขององค์กรให้บริการเครื่องหมายรับรองความน่าเชื่อถือด้านการคุ้มครองข้อมูลส่วนบุคคลที่ผ่านการรับรองจากคณะกรรมาธิการยุโรปแล้วว่าสามารถบังคับให้มีการปฏิบัติตามกลไกกำกับดูแลตนเองขององค์กรดังกล่าวได้อย่างมีประสิทธิภาพ อาทิ TRUSTe และ WebTrust เป็นต้น

(2) จัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (privacy policy) ของตนเองที่สอดคล้องกับหลักเกณฑ์ของเซฟฮาร์เบอร์[23]

---

[23] International Trade Administration, Department of Commerce, “Safe Harbor Overviews” in The Privacy Papers : Managing Technology, Consumer, Employee, and Legislative Action, ed.Pebecca Herole (New York : CRC Press LLC, 2002), p.620 อ้าง

ต่อจากนั้นองค์กรที่จะเข้าร่วมโครงการเซฟฮาร์เบอร์ต้องทำการรับรองตนเอง (self-certify) ว่าจะปฏิบัติตามหลักการของโครงการเซฟฮาร์เบอร์โดยการยื่นเอกสารรับรองตนเองที่ลงชื่อเจ้าหน้าที่บริษัทในนามขององค์กรต่อกระทรวงพาณิชย์ประเทศสหรัฐอเมริกา (หรือผู้ที่ได้รับมอบหมายหน้าที่) ในเอกสารรับรองตนเองต้องประกอบไปด้วยข้อมูลอย่างน้อยดังต่อไปนี้[24]

(1) ชื่อ ที่อยู่ไปรษณีย์ ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ หมายเลขโทรศัพท์และหมายเลขโทรสารขององค์กร

(2) คำอธิบายลักษณะของกิจกรรมที่องค์กรจะกระทำต่อข้อมูลส่วนบุคคลที่ได้รับมาจากสหภาพยุโรป

(3) คำอธิบายลักษณะของนโยบายความเป็นส่วนตัวขององค์กรในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าว รวมทั้ง :

(ก) สถานที่ซึ่งสาธารณชนสามารถอ่านนโยบายความเป็นส่วนตัวได้

(ข) วันที่เริ่มมีผลบังคับใช้

(ค) สำนักงานที่สามารถติดต่อยื่นข้อร้องเรียน ขอสิทธิ์การเข้าถึงและรับมือกับปัญหาอื่นๆที่เกิดขึ้นภายใต้โครงการเซฟฮาร์เบอร์ได้

(ง) เจ้าหน้าที่ตามกฎหมายที่มีอำนาจทางกฎหมายในการรับฟังข้อร้องเรียนใดๆก็ตามต่อองค์กรเกี่ยวกับการกระทำที่ไม่เป็นธรรมหรืออาจก่อให้เกิดความหลงผิดหรือการฝ่าฝืนกฎหมายหรือกฎระเบียบข้อบังคับที่คุ้มครองความเป็นส่วนตัว

(จ) ชื่อของแผนงานคุ้มครองความเป็นส่วนตัวใดๆก็ตามที่องค์กรเป็นสมาชิก

(ฉ) วิธีที่ใช้ในการพิสูจน์การปฏิบัติตามกฎ (เช่น โดยคนในองค์กรหรือโดยบุคคลภายนอก) และ

(ช) กลไกในการขอความช่วยเหลืออย่างอิสระซึ่งสามารถใช้ประโยชน์ในการสืบสวนข้อเรียกร้องที่ยังมิได้รับการตัดสินได้

โดยองค์กรจะได้รับสิทธิประโยชน์ในการเข้าร่วมโครงการเซฟฮาร์เบอร์นับตั้งแต่วันที่องค์กรนั้นได้รับรองตนเองต่อกระทรวงพาณิชย์สหรัฐอเมริกาว่าจะปฏิบัติตามหลักแนวทางปฏิบัติดังกล่าวของโครงการเซฟฮาร์เบอร์

เมื่อกระทรวงพาณิชย์สหรัฐอเมริกาผ่านการตรวจรายละเอียดต่างๆ เกี่ยวในการสมัครเรียบร้อยแล้วก็จะประกาศการเป็นสมาชิกโครงการเซฟฮาร์เบอร์ผ่านเว็บไซต์ของกระทรวงการ

ถึงใน ปฏิวัติ อุ่นเรือน, “ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ”, (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), น.45.

[24] คำวินิจฉัยที่ 2000/520, ภาคผนวกที่ 2 ข้อสงสัยที่ได้รับการซักถามบ่อยครั้งที่ 6

ส่งออก (Department of Export) และจะเก็บรักษารายชื่อขององค์กรทั้งหมดที่ได้ยื่นเอกสารดังกล่าวเพื่อประกันสิทธิประโยชน์ที่ได้รับจากการเข้าร่วมกับโครงการเซฟฮาร์เบอร์ไว้เช่นนั้น และจะแก้ไขรายชื่อดังกล่าวให้ทันสมัยโดยพิจารณาจากเอกสารประจำปี

โครงการเซฟฮาร์เบอร์สามารถใช้บังคับแก่องค์กรทางการค้าหรือองค์กรธุรกิจอื่นๆที่ได้เข้าร่วมเป็นสมาชิกซึ่งไม่จำกัดว่าต้องเป็นองค์กร บริษัทหรือผู้ประกอบการของประเทศสหรัฐอเมริกาเท่านั้น แต่ยังเปิดโอกาสให้องค์กรหรือผู้ประกอบการจากประเทศอื่นๆเข้าร่วมเป็นสมาชิกเพื่อได้รับการรับรองดังกล่าวได้อีกด้วย

3.2.3 ข้อยกเว้นของโครงการเซฟฮาร์เบอร์

องค์กรหรือหน่วยงานต่างๆจะต้องปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลของโครงการเซฟฮาร์เบอร์ แต่อย่างไรก็ตามโครงการเซฟฮาร์เบอร์ได้กำหนดข้อยกเว้นหรือจำกัดให้ไม่จำต้องปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลได้เอาไว้ในหลักเกณฑ์โครงการเซฟฮาร์เบอร์ (Safe Harbour Privacy Principles) วรรคสี่ ซึ่งได้แก่กรณีดังต่อไปนี้

(1) มีความจำเป็นสำหรับความมั่นคงของชาติ ประโยชน์สาธารณะ หรือสอดคล้องกับข้อกำหนดการบังคับใช้กฎหมาย

(2) มีรัฐบัญญัติ ระเบียบของราชการ หรือกฎหมายที่มาจากบรรทัดฐานคำพิพากษาของศาลซึ่งได้สร้างข้อผูกพันที่ขัดแย้งกับหลักการเซฟฮาร์เบอร์รวมไปถึงการให้อำนาจตามกฎหมายอย่างชัดแจ้ง (explicit legal authorisations) โดยองค์กรต้องแสดงให้เห็นว่าการไม่ปฏิบัติตามหลักการของโครงการเซฟฮาร์เบอร์อยู่ในขอบเขตอันชอบธรรมตามกฎหมายอันเป็นฐานที่มาแห่งอำนาจนั้นได้

(3) Directive หรือ กฎหมายของประเทศสมาชิกอนุญาตให้มีข้อยกเว้นหรือการหลีกเลี่ยงไม่ทำตามกฎได้ โดยมีเงื่อนไขว่าข้อยกเว้นหรือการหลีกเลี่ยงไม่ทำตามกฎนั้นๆต้องถูกนำมาใช้ในบริบทที่คล้ายกัน

องค์กรต่างๆควรมุ่งมั่นที่จะปฏิบัติตามหลักของโครงการเซฟฮาร์เบอร์อย่างเต็มที่และโปร่งใส โดยยังคงเป้าหมายที่จะยกระดับการคุ้มครองความเป็นส่วนตัวอย่างสม่ำเสมอ และระบุในนโยบายคุ้มครองความเป็นส่วนตัวในกรณีที่จะมีการนำข้อยกเว้นที่ได้รับความเห็นชอบตาม ข้อ (2) มาใช้เป็นประจำด้วย

ด้วยเหตุผลเดียวกันนี้ ในกรณีที่ทางเลือกนั้นสามารถกระทำได้ภายใต้หลักของโครงการเซฟฮาร์เบอร์และ/หรือกฎหมายสหรัฐอเมริกา องค์กรนั้นๆจะต้องเลือกทางเลือกที่สามารถคุ้มครองข้อมูลส่วนบุคคลได้สูงสุดเท่าที่จะเป็นไปได้

3.2.4 องค์กรที่มีหน้าที่บังคับการให้เป็นไปตามกฎหมาย

เนื่องจากโครงการเซฟฮาร์เบอร์มีวัตถุประสงค์เพื่อรับรองการโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรปเพื่อประโยชน์ในการประกอบธุรกิจการค้าการลงทุนของภาคเอกชนเป็นหลัก องค์กรที่มีอำนาจในการบังคับการกรณีที่เกิดการปฏิบัติที่ไม่เป็นไปตามหลักการเซฟฮาร์เบอร์จึงมุ่งเน้นการไกล่เกลี่ยและระงับข้อพิพาททางการค้าเป็นสำคัญ

กลไกในการแก้ไขข้อพิพาทและการจัดการในกรณีที่องค์กรล้มเหลวในการปฏิบัติตามหลักการโครงการเซฟฮาร์เบอร์ติดต่อกันหลายครั้งนั้นสามารถทำได้หลากหลายรูปแบบ แต่วิธีการนั้นต้องเป็นไปตามข้อกำหนดของข้อสงสัยที่ได้รับการซักถามบ่อยครั้งว่าด้วยการพิสูจน์การปฏิบัติตามกฎ องค์กรต่างๆอาจปฏิบัติตามข้อกำหนดเหล่านั้นได้ผ่านวิธีดังต่อไปนี้[25]

(1) การปฏิบัติตามแผนงานคุ้มครองความเป็นส่วนตัวที่พัฒนาขึ้นโดยภาคเอกชนซึ่งได้รวมหลักการของโครงการเซฟฮาร์เบอร์ไว้ในกฎระเบียบของโครงการและมีวิธีการบังคับใช้ที่มีประสิทธิภาพตามที่ได้กำหนดไว้ในหลักการบังคับใช้

(2) การร่วมมือกับหน่วยงานควบคุมระเบียบกฎหมายที่จัดเตรียมวิธีรับมือกับข้อร้องเรียนจากปัจเจกบุคคลและวิธีการแก้ไขข้อพิพาท

(3) ข้อผูกมัดที่จะร่วมมือกับหน่วยงานคุ้มครองข้อมูลที่ตั้งอยู่ในสหภาพยุโรปหรือตัวแทนที่มีอำนาจจากหน่วยงานนั้นๆ

วิธีการข้างต้นนี้เป็นเพียงการยกตัวอย่างให้เห็นภาพเท่านั้น มิใช่วิธีการให้ปฏิบัติโดยเคร่งครัด องค์กรเอกชนต่างๆมีสิทธิออกแบบกลไกแบบอื่นในการบังคับใช้ได้โดยอิสระเช่นกัน

องค์กรและบริษัทต่างๆนั้นจะอยู่ภายใต้อำนาจของหน่วยงานรัฐบาลสหรัฐอเมริกา 2 หน่วยงานด้วยกัน คือ คณะกรรมาธิการการค้าของสหรัฐอเมริกา (Federal Trade Commission หรือ FTC) กับกระทรวงการขนส่งแห่งสหรัฐอเมริกา (U.S. Department of Transportation) โดยหน่วยงานทั้งสองมีอำนาจในการสืบสวนข้อร้องเรียนและระงับการปฏิบัติที่ไม่เป็นธรรมและอาจก่อให้เกิดความหลงผิด รวมไปถึงหากมีการฝ่าฝืนหลักการโครงการเซฟฮาร์เบอร์หน่วยงานดังกล่าวสามารถกำหนดให้มีการชดเชยแก้ไขให้แก่ปัจเจกบุคคลได้ โดยไม่จำกัดสัญชาติหรือประเทศอันเป็นถิ่นที่อยู่บุคคลนั้น

คณะกรรมาธิการการค้าของสหรัฐอเมริกามีข้อผูกมัดในการพิจารณาตรวจสอบข้อพิพาทที่ถูกส่งมาจากองค์กรเอกชนที่มีกลไกกำกับดูแลตนเอง เช่น BBBonline และ TRUSTe และประเทศสมาชิกสหภาพยุโรปที่กล่าวอ้างว่าได้มีการฝ่าฝืนหลักการของโครงการเซฟฮาร์เบอร์เพื่อพิจารณาว่ามีการฝ่าฝืนมาตรา 5 ของรัฐบัญญัติกรรมาธิการการค้าของสหรัฐอเมริกา (Federal Trade

---

[25] คำวินิจฉัยที่ 2000/520, ภาคผนวกที่ 2 ข้อสงสัยที่ได้รับการซักถามที่ 11

Commission Act) ที่ว่าด้วยการป้องกันมิให้มีการกระทำหรือวิธีปฏิบัติทางการค้าที่ไม่เป็นธรรมและอาจก่อให้เกิดความหลงผิด ซึ่งคณะกรรมาธิการการค้าสามารถกำหนดให้องค์กรต่างๆต้องชดใช้ค่าเสียหายให้แก่ปัจเจกบุคคลได้ หากมีการปฏิบัติหรือวิธีทางการค้าที่เข้าข่ายว่าไม่เป็นธรรม และเป็นการหลอกลวงผู้บริโภค

ส่วนกระทรวงการขนส่งแห่งสหรัฐอเมริกามีอำนาจพื้นฐานตามหัวข้อ 49 United States Code Section 41712 กระทรวงการขนส่งแห่งสหรัฐอเมริกามีอำนาจในการตรวจสอบข้อร้องเรียนทั้งที่เป็นทางการและไม่เป็นทางการที่ได้ร้องเรียนโดยปัจเจกบุคคล ตัวแทนบริษัทท่องเที่ยวสายการบิน และหน่วยงานภาครัฐทั้งในประเทศและต่างประเทศ

3.3 กฎหมาย Personal Information Protection and Electronic Documents Act 2000 (PIPEDA) โดยประเทศแคนาดา

3.3.1 วัตถุประสงค์และหลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลของกฎหมาย PIPEDA

กฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ของประเทศแคนาดา (Personal Information Protection and Electronic Documents Act 2000) หรือเรียกโดยย่อว่า “กฎหมาย PIPEDA” เกิดจากผลกระทบในการบัญญัติ Directive 95/46/EC โดยสหภาพยุโรป เฉกเช่นเดียวกับประเทศสหรัฐอเมริกาและประเทศอื่นๆ ที่ต้องมีการพัฒนากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้เทียบเท่ากับมาตรฐานของสหภาพยุโรป เพื่อที่จะสามารถรับโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปได้[26]

กฎหมาย PIPEDA มีการบัญญัติในลักษณะเป็นกฎหมายกลาง โดยเป็นกฎหมายที่ใช้ควบคุมการจัดเก็บ การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่อยู่ภายใต้ความควบคุมหรือการครอบครองขององค์กรธุรกิจและภาคเอกชน ขอบเขตของกฎหมายฉบับนี้ใช้บังคับกับองค์กรทั้งหลาย (organizations) ที่มีการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผยเพื่อการประกอบกิจการขององค์กร ลูกจ้างขององค์กร หรือใช้ในกิจการธุรกิจของสหพันธรัฐ โดยองค์กรเหล่านี้จะต้องเป็นองค์กรภาคเอกชนที่มีกิจกรรมในลักษณะเชิงพาณิชย์ รวมทั้งการขายแลกเปลี่ยนสินค้า หรือการให้เช่าของผู้บริจาค สมาชิก หรือกิจกรรมการหาทุนอื่นๆตามที่ระบุขององค์กรที่อยู่ในรูปแบบสมาคม หุ้นส่วน นิติบุคคล และสหภาพแรงงาน

---

[26] นคร เสรีรักษ์, *อ้างแล้ว เชิงอรรถที่ 19*, น.173.

แต่อย่างไรก็ตามกฎหมาย PIPEDA ไม่มีผลต่อองค์กรของรัฐบาลที่อยู่ใต้อำนาจของพระราชบัญญัติคุ้มครองความเป็นส่วนตัวของรัฐบาลกลาง (Privacy Act) หรือองค์กรที่ขึ้นกับกฎหมายคุ้มครองความเป็นส่วนตัวในระดับมณฑล (provincial) และยังไม่มีผลกับองค์กรที่ไม่แสวงหาผลกำไรและองค์กรการกุศล ยกเว้นในกรณีที่องค์กรเหล่านั้นมีส่วนเกี่ยวข้องกับกิจกรรมที่มีลักษณะเป็นไปในทางการค้า เช่น การแลกเปลี่ยนสินค้าและการซื้อขายรายนามผู้บริจาค เป็นต้น[27]

องค์กรหรือผู้ที่อยู่ภายใต้บทบังคับของกฎหมายฉบับนี้จะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ในกรณีที่มีการเก็บ การใช้ และการเปิดเผยข้อมูล โดยเจ้าของข้อมูลมีสิทธิเข้าถึงข้อมูลของตนที่อยู่ในความควบคุมหรือภายใต้การครอบครองขององค์กรภาคเอกชน ตลอดจนมีสิทธิการเรียกร้องให้ปรับปรุงแก้ไขข้อมูลของตนให้มีความถูกต้องในกรณีที่จำเป็น ซึ่งการได้รับความยินยอมจากเจ้าของข้อมูลนั้น เจ้าของข้อมูลอาจแสดงออกซึ่งความยินยอมในรูปแบบที่ชัดแจ้งเป็นลายลักษณ์อักษรหรือด้วยวาจา หรือโดยไม่ชัดแจ้งจากการตีความการดำเนินการหรือไม่ดำเนินการของเจ้าของข้อมูลส่วนบุคคลก็ได้ ทั้งนี้ กฎหมายดังกล่าวยังได้ให้ความสำคัญกับการชั่งน้ำหนักระหว่างสิทธิความเป็นส่วนตัวของบุคคลในส่วนที่เกี่ยวกับข้อมูลส่วนบุคคลกับความจำเป็นขององค์กรที่ต้องมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ซึ่งวิญญูชนเห็นว่าเหมาะสมกับสถานการณ์อีกด้วย

องค์กรธุรกิจหรือภาคเอกชนสามารถนำข้อมูลส่วนบุคคลไปใช้เพื่อวัตถุประสงค์ตามที่ระบุไว้เท่านั้น สำหรับกรณีที่มีการใช้ข้อมูลดังกล่าวเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้ระบุไว้นั้นจำเป็นที่จะต้องได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลส่วนบุคคล

ตามกฎหมาย PIPEDA นั้นองค์กรธุรกิจและภาคเอกชนรวมถึงสมาคม ห้างหุ้นส่วนนิติบุคคล และสหภาพแรงงานจำเป็นต้องยึดหลักปฏิบัติที่ดีด้านข้อมูลส่วนบุคคล 10 ประการตามที่กำหนดไว้ในเอกสารที่ 1 (Schedule 1) แนบท้ายกฎหมายซึ่งเป็นแบบปฏิบัติเพื่อการคุ้มครองข้อมูลส่วนบุคคล (Model Code for the Protection of Personal Information) เพื่อให้การดำเนินการที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างถูกต้องตามมาตรฐานแห่งชาติแคนาดา (National Standard of Canada) ดังนี้[28]

---

[27] European Commission, “Frequently Asked Questions on the Commission's adequacy finding on the Canadian Personal Information Protection and electronic Documents Act,” สืบค้นเมื่อวันที่ 1 ธันวาคม 2558, จาก http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/third-countries-faq/index_en.htm.

[28] สมศักดิ์ นวตระกูลพิสุทธิ์, “กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา,” รายงานการวิจัยโครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์

(1) หลักความรับผิดชอบ (Accountability)

องค์กรหรือหน่วยงานต่างๆต้องมีความรับผิดชอบต่อข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของตน และต้องแต่งตั้งบุคคลหนึ่งหรือหลายคนรับผิดชอบต่อการปฏิบัติขององค์กร ตามหลักปฏิบัติต่างๆ ที่กำหนดในแบบปฏิบัตินี้

องค์กรต้องกำหนดนโยบายและแนวทางปฏิบัติเพื่อให้หลักปฏิบัติต่างๆที่กำหนดในแบบปฏิบัตินี้บังเกิดผล ได้แก่

1. กำหนดกระบวนการคุ้มครองข้อมูลส่วนบุคคล

2. กำหนดกระบวนการรับและตอบคำร้องเรียน (complaints) หรือข้อซักถาม (inquiries) ต่างๆ

3. ฝึกอบรมและแจ้งให้พนักงานที่เกี่ยวข้องทราบเกี่ยวกับนโยบายและแนวทางปฏิบัติในเรื่องนี้ขององค์กร

4. จัดทำข้อมูลชี้แจงนโยบายและกระบวนการต่างๆขององค์กร

(2) หลักการแจ้งวัตถุประสงค์ (Identifying Purposes)

องค์กรต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลก่อนหรือในขณะทำการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น ทั้งนี้การแจ้งอาจกระทำด้วยวาจาหรือเป็นลายลักษณ์อักษรก็ได้ตามลักษณะของการเก็บรวบรวมข้อมูลนั้น และมีหน้าที่ต้องดำเนินการดังนี้

1.จัดพิมพ์ประกาศหรือเอกสารเพื่อแจ้งให้ทราบเกี่ยวกับสัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้สอดคล้องกับหลักการเปิดเผย และหลักการเข้าตรวจดูข้อมูลส่วนบุคคล

2. ต้องเก็บรวบรวมข้อมูลส่วนบุคคลแต่เพียงข้อมูลที่จำเป็นต่อวัตถุประสงค์ที่ได้แจ้งให้ทราบแล้วเท่านั้น ทั้งนี้ เป็นไปตามหลักการเก็บรวบรวมข้อมูลอย่างจำกัด

3. ในกรณีที่จะนำข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ไปใช้ประโยชน์เพื่อวัตถุประสงค์อย่างอื่นที่มิได้แจ้งให้ทราบล่วงหน้า องค์กรต้องแจ้งวัตถุประสงค์ใหม่นั้นให้บุคคลนั้นทราบเสียก่อน และจะต้องได้รับความยินยอมก่อนที่จะนำข้อมูลนั้นไปใช้ประโยชน์ตามวัตถุประสงค์ใหม่นั้น ทั้งนี้ เว้นแต่วัตถุประสงค์ใหม่นั้นเป็นไปตามที่กฎหมายกำหนด

(3) หลักความยินยอม (Consent)

และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (กรุงเทพมหานคร : สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2547) น.97.

บุคคลที่ให้ข้อมูลส่วนบุคคลต้องได้รับทราบและให้ความยินยอมแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลของบุคคลนั้น ทั้งนี้ เว้นแต่เป็นกรณีที่ไม่สมควรตามที่กำหนดในกฎหมาย

ตามปกติองค์กรจะต้องขอความยินยอมสำหรับการใช้หรือเปิดเผยข้อมูลนั้นในขณะที่ทำการเก็บรวบรวม แต่อย่างไรก็ตาม ในบางสถานการณ์อาจมีการขอความยินยอมนำข้อมูลไปใช้หรือเปิดเผยภายหลังการเก็บรวบรวมข้อมูลแต่ต้องก่อนนำข้อมูลนั้นไปใช้ โดยการขอความยินยอมนั้นองค์กรต้องจัดให้มีการขอความยินยอมโดยวิธีการดำเนินการที่เหมาะสมเพื่อให้บุคคลได้รับแจ้งถึงวัตถุประสงค์ของการที่จะนำข้อมูลนั้นไปใช้ และจะต้องไม่ขอความยินยอมในการดำเนินการเกินความจำเป็นสำหรับการดำเนินการตามวัตถุประสงค์ที่ชอบด้วยกฎหมายและที่ได้แจ้งให้ทราบ

รูปแบบของความยินยอมอาจแตกต่างกันไปขึ้นอยู่กับสถานการณ์และประเภทของข้อมูล ทั้งนี้ ในการกำหนดรูปแบบของความยินยอม องค์กรต้องคำนึงถึงประเภทของข้อมูลโดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ต้องขอความยินยอมอย่างชัดแจ้ง ในกรณีที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวน้อยก็อาจขอความยินยอมโดยปริยายได้ เช่นบันทึกทางการแพทย์และบันทึกรายได้ เป็นต้น

(4) หลักการเก็บรวบรวมข้อมูลอย่างจำกัด (Limiting Collection)

การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องจำกัดเฉพาะแต่ข้อมูลที่จำเป็นและเป็นไปตามวัตถุประสงค์ขององค์กรที่ได้แจ้งให้ทราบและต้องเก็บรวบรวมโดยวิธีการที่เป็นธรรมและชอบด้วยกฎหมาย องค์กรจะต้องไม่เก็บรวบรวมข้อมูลส่วนบุคคลโดยวิธีการที่เป็นการเลือกปฏิบัติและจะต้องเก็บรวบรวมข้อมูลอย่างจำกัดเพียงเท่าที่จำเป็นต่อวัตถุประสงค์ อีกทั้งต้องระบุประเภทของข้อมูลที่เก็บรวบรวมโดยการจัดทำเป็นประกาศ หรือคู่มือเกี่ยวกับนโยบายและแนวทางปฏิบัติขององค์การแจ้งแก่ผู้เป็นเจ้าของข้อมูล ซึ่งหลักการนี้มีความสัมพันธ์อย่างใกล้ชิดกับหลักการแจ้งวัตถุประสงค์และหลักความยินยอม

(5) หลักการจำกัดการใช้ การเปิดเผย และการเก็บรักษา (Limiting Use, Disclosure and Retention)

องค์การจะต้องไม่นำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยเพื่อวัตถุประสงค์อย่างอื่นนอกเหนือจากวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้น เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลหรือเป็นไปตามที่กฎหมายกำหนด และข้อมูลส่วนบุคคลจะต้องถูกเก็บรักษาไว้ในระยะเวลาเพียงเท่าที่จำเป็นสำหรับการดำเนินการตามวัตถุประสงค์ดังกล่าวเท่านั้น หากมีการใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่กำหนดขึ้นใหม่ต้องจัดทำเอกสารเกี่ยวกับวัตถุประสงค์ใหม่แจ้งแก่เจ้าของข้อมูล นอกจากนี้การจัดทำคู่มือตามหลักข้อ 4 ต้องกำหนดกระบวนการเกี่ยวกับการเก็บรักษาข้อมูลส่วนบุคคล และควรกำหนดระยะเวลาต่ำสุดและสูงสุดของการเก็บรักษาข้อมูลด้วย

ภายใต้หลักการนี้ข้อมูลส่วนบุคคลที่ไม่ถูกต้องตรงกับวัตถุประสงค์ที่ได้แจ้งหรือได้ใช้เสร็จสิ้นแล้วต้องถูกทำลาย ลบทิ้ง หรือทำให้ไม่ปรากฏชื่อของบุคคลนั้น (anonymous) ทั้งนี้ องค์กรจะต้องจัดทำคู่มือแนวทางปฏิบัติและกำหนดกระบวนการเกี่ยวกับการทำลายข้อมูลส่วนบุคคลดังกล่าวด้วย

(6) หลักความถูกต้อง (Accuracy)

ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้จะต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบัน (up-to-date) ตามความจำเป็นเพื่อวัตถุประสงค์ของการนำข้อมูลนั้นไปใช้ หลักการที่ว่าข้อมูลส่วนบุคคลต้องถูกต้องสมบูรณ์นี้เพื่อลดความเป็นไปได้ของการนำข้อมูลที่ไม่ถูกต้องไปใช้

องค์กรจะต้องไม่ปรับปรุงข้อมูลส่วนบุคคลโดยกระทำในลักษณะเป็นงานประจำ (routinely update) เว้นแต่กระบวนการเช่นนั้นมีความจำเป็นเพื่อสนองตอบต่อวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้น

(7) หลักการรักษาความปลอดภัย (Safeguards)

ข้อมูลส่วนบุคคลจะต้องได้รับการรักษาความปลอดภัยที่เหมาะสม การรักษาความปลอดภัยจะต้องให้ความคุ้มครองข้อมูลส่วนบุคคลต่อการสูญหายหรือการโจรกรรม ตลอดจนการเข้าตรวจดู การเปิดเผย การทำซ้ำ การใช้ หรือการแก้ไขเพิ่มเติมโดยไม่ได้รับอนุญาต ทั้งนี้ ไม่ว่าข้อมูลนั้นจะอยู่ในรูปแบบใด ลักษณะของการรักษาความปลอดภัยจะแตกต่างกันไปขึ้นอยู่กับระดับความเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว รูปแบบและปริมาณข้อมูลที่เก็บรวบรวม ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ควรได้รับการรักษาความปลอดภัยโดยให้การคุ้มครองในระดับที่สูงกว่าข้อมูลธรรมดาหรือข้อมูลข่าวสารทั่วๆไป

มาตรการในการรักษาความปลอดภัยประกอบไปด้วยมาตรการคุ้มครองในทางกายภาพ (physical measure) เช่นการปิดล็อคตู้เอกสาร มาตรการจัดระบบรักษาความปลอดภัยในองค์กร และมาตรการทางเทคโนโลยี เช่น การใช้รหัสผ่าน (password) และการเข้ารหัส (encryption) เพื่อป้องกันมิให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าตรวจดูข้อมูลนั้นได้ รวมถึงการฝึกอบรมและดำเนินการให้พนักงานลูกจ้างตระหนักถึงความสำคัญของการรักษาความลับของข้อมูลส่วนบุคคลและการกำจัดหรือทำลายข้อมูลส่วนบุคคลจะต้องกระทำด้วยความระมัดระวัง

(8) หลักการเปิดเผย (Openness)

องค์กรจะต้องจัดทำนโยบายและแนวทางปฏิบัติขององค์กรในการจัดการข้อมูลส่วนบุคคล กล่าวคือ การจัดการวิธีการเข้าถึงข้อมูลหรือจัดข้อมูลที่ต้องเผยแพร่แก่ประชาชนในสถานที่และวิธีการที่เหมาะสม บุคคลทั่วไปจะต้องสามารถได้รับข้อมูลนั้นได้โดยไม่ลำบากและข้อมูลดังกล่าวจะต้องเปิดเผยในลักษณะที่สามารถเข้าใจได้โดยทั่วไป โดยข้อมูลที่ได้เปิดเผยหรือเผยแพร่อย่างน้อยต้องประกอบด้วยรายการดังต่อไปนี้

1. ชื่อ ตำแหน่ง และที่อยู่ของบุคคลที่รับผิดชอบนโยบาย และแนวทางปฏิบัติขององค์กรหรือผู้รับคำร้องหรือซักถามต่างๆ

2. วิธีการเข้าตรวจดูข้อมูลส่วนบุคคลที่อยู่ในความครอบครองขององค์กร

3. รายละเอียดเกี่ยวกับข้อมูล ประเภทของข้อมูล ตลอดจนรายละเอียดเกี่ยวกับการนำข้อมูลส่วนบุคคลนั้นไปใช้

4. สำเนาเอกสารแผ่นปลิว หรือข้อมูลอื่นใดเกี่ยวกับนโยบายมาตรฐาน และประมวลจริยธรรมขององค์กร

5. ข้อมูลส่วนบุคคลที่จัดหาให้แก่องค์กรที่เกี่ยวข้อง หน่วยงาน สาขา หรือ บริษัทในเครือ

(9) หลักการเข้าตรวจดูข้อมูลของบุคคล (Individual Access)

เมื่อมีการร้องขอ บุคคลผู้เป็นเจ้าของข้อมูลจะต้องได้รับการรายงานหรือเข้าตรวจดูเกี่ยวกับการมีอยู่ (existence) การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลของตน นอกจากนี้บุคคลสามารถโต้แย้งหากพบว่าข้อมูลดังกล่าวไม่ถูกต้องหรือสมบูรณ์ และมีสิทธิเรียกร้องให้มีการแก้ไขเพิ่มเติมข้อมูลนั้นได้ตามความเหมาะสม อย่างไรก็ตาม ในบางสถานการณ์อาจไม่สามารถให้บุคคลเข้าตรวจดูข้อมูลส่วนบุคคลทั้งหมด แต่ข้อยกเว้นการเข้าตรวจดูนั้นควรมีลักษณะจำกัด ในกรณีที่องค์กรปฏิเสธการขอเข้าตรวจดูข้อมูลนั้นองค์กรจะต้องแจ้งเหตุผลของการปฏิเสธ เหตุผลการปฏิเสธอาจได้แก่กรณีที่การขอเข้าตรวจดูต้องมีการเสียค่าใช้จ่ายในการจัดหาข้อมูลดังกล่าวสูงมาก หรือในกรณีที่ข้อมูลที่ขอเข้าตรวจดูมีข้อมูลที่เกี่ยวข้องกับบุคคลอื่นรวมอยู่ด้วย หรือในกรณีของข้อมูลซึ่งไม่สามารถเปิดเผยได้ด้วยเหตุผลทางกฎหมาย ด้านความปลอดภัย ด้านการค้า เป็นต้น

เมื่อบุคคลผู้เป็นเจ้าของข้อมูลขอเข้าถึงข้อมูลส่วนบุคคลของตน องค์กรจะต้องแจ้งให้บุคคลดังกล่าวทราบว่าองค์กรมีข้อมูลส่วนบุคคลของบุคคลนั้นอยู่ในความครอบครองหรือไม่ ชี้แจงถึงแหล่งที่มาของข้อมูลนั้น ในกรณีที่มีการเข้าถึงข้อมูลทางการแพทย์ซึ่งเป็นข้อมูลส่วนบุคคลชนิดที่มีความอ่อนไหว องค์กรอาจเลือกที่จะเปิดเผยโดยผ่านแพทย์ก็ได้

ในการเปิดเผยข้อมูลส่วนบุคคลที่สามารถเปิดเผยได้ องค์กรอาจต้องจัดทำบัญชีรายละเอียดเกี่ยวกับการนำข้อมูลไปเปิดเผย ลักษณะของการนำข้อมูลไปใช้ และจัดทำบัญชีรายชื่อของบุคคลภายนอกที่จะสามารถเข้าถึงข้อมูลส่วนบุคคลดังกล่าวได้

เมื่อบุคคลเห็นว่าข้อมูลส่วนบุคคลของตนที่อยู่ในความครอบครองขององค์กรนั้นๆไม่ถูกต้องหรือไม่สมบูรณ์และบุคคลได้โต้แย้งให้แก้ไขเปลี่ยนแปลง องค์กรจะต้องแก้ไขเพิ่มเติมข้อมูลดังกล่าวตามที่ร้องขอซึ่งอาจกระทำโดยการแก้ไข การตัดออก หรือการเพิ่มเติมข้อมูล แล้วแต่กรณี และหากข้อมูลดังกล่าวไม่ได้รับการแก้ไขให้เป็นที่พอใจตามคำโต้แย้ง ให้องค์กรบันทึกเรื่องที่ไม่ดำเนินการแก้ไขนั้นไว้

(10) หลักการโต้แย้งการปฏิบัติขององค์กร (Challenging Compliance)

บุคคลผู้เป็นเจ้าของข้อมูลสามารถทำคำโต้แย้งการดำเนินการเกี่ยวกับข้อมูลที่เกี่ยวกับตน โดยการทำคำโต้แย้งไปยังบุคคลที่ได้รับแต่งตั้งให้เป็นผู้รับผิดชอบการปฏิบัติหน้าที่ขององค์กรได้

ในการทำคำร้องขอหรือคำโต้แย้ง องค์กรต้องจัดให้มีกระบวนการที่เหมาะสมในการรับคำร้อง ข้อโต้แย้ง หรือข้อซักถามเกี่ยวกับนโยบายและแนวทางปฏิบัติขององค์กรเกี่ยวกับการจัดการข้อมูลส่วนบุคคล ทั้งนี้ กระบวนการดังกล่าวต้องกระทำได้โดยไม่ยุ่งยากซับซ้อน อีกทั้งองค์กรจะต้องแจ้งหรืออธิบายให้บุคคลทราบเกี่ยวกับกระบวนการร้องเรียน การรับคำร้อง การตอบข้อซักถาม และต้องทำการสอบสวนเกี่ยวกับคำร้องทั้งหลาย ในกรณีที่คำร้องนั้นมีเหตุอันสมควร องค์กรจะต้องมีการดำเนินการที่เหมาะสม รวมทั้งการแก้ไขเพิ่มเติมหรือมีมาตรการที่เหมาะสมเกี่ยวกับนโยบายและแนวทางปฏิบัติขององค์กรที่จำเป็น

3.3.2 หลักการและวิธีการในการรับโอนและการโอนข้อมูลระหว่างประเทศ

ในส่วนของการโอนข้อมูลไปยังต่างประเทศของประเทศแคนาดานั้น ได้มีการออกคู่มือการปฏิบัติงานว่าด้วยการประมวลผลข้อมูลส่วนบุคคลข้ามพรมแดน (Guidelines for Processing Personal Data Across Borders) โดยสำนักงานคณะกรรมาธิการสิทธิความเป็นส่วนตัวแห่งแคนาดา เพื่ออธิบายลักษณะการบังคับใช้กฎหมาย PIPEDA ในการควบคุมการถ่ายโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สามเพื่อนำไปประมวลผล โดยรวมถึงบุคคลที่สามที่ดำเนินงานภายนอกประเทศแคนาดาด้วย เนื่องจากกฎหมาย PIPEDA เอง มีวัตถุประสงค์ที่จะสนับสนุนและส่งเสริมการค้าทางอิเล็กทรอนิกส์โดยการให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลที่เก็บรวบรวม ใช้ หรือเปิดเผยในสถานการณ์เฉพาะ วัตถุประสงค์นี้แสดงให้เห็นว่าการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมชัดเจน และโปร่งใสนั้นจะสามารถอำนวยความสะดวกและส่งเสริมในธุรกิจการค้าได้เพราะเป็นการสร้างความมั่นใจและความเชื่อถือให้แก่ผู้บริโภค ดังนั้นการให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคเมื่อเกิดการถ่ายโอนข้อมูลข้ามพรมแดนนั้นเป็นสิ่งที่หลีกเลี่ยงมิได้ เพราะในปัจจุบันนี้ระบบเศรษฐกิจการค้ามีเครือข่ายครอบคลุมไปทั้งโลก จึงต้องพึ่งพาการถ่ายโอนข้อมูลระหว่างประเทศเป็นหลัก[29]

---

[29] Office of the Privacy Commissioner of Canada, “Guidelines for Processing Personal Data Across Borders,” สืบค้นเมื่อวันที่ 10 ธันวาคม 2558, จาก https://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp

มาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลที่ถูกโอนไปยังต่างประเทศของประเทศแคนาดานั้นมีความแตกต่างจากกลุ่มประเทศสมาชิกสหภาพยุโรป กล่าวคือประเทศสมาชิกสหภาพยุโรปนั้นห้ามมิให้มีการถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรป เว้นเสียแต่ประเทศเหล่านั้นมีการรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ส่วนประเทศแคนาดานั้น ตามกฎหมาย PIPEDA มิได้ห้ามองค์กรภายในประเทศแคนาดาถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศอื่น อย่างไรก็ตาม องค์กรเหล่านี้มีความรับผิดชอบที่จะต้องให้การคุ้มครองการถ่ายโอนข้อมูลส่วนบุคคลภายใต้การจัดการและจัดจ้างบุคคลภายนอกของแต่ละองค์กร โดยมีสำนักงานคณะกรรมาธิการสิทธิความเป็นส่วนตัวแห่งแคนาดาทำหน้าที่ตรวจสอบวิธีการที่องค์กรใช้ในการจัดการกับข้อมูลส่วนบุคคลได้

ตามหลักปฏิบัติที่ 1 ของเอกสารที่ 1 ของ PIPEDA ได้กำหนดระดับสมดุลระหว่างการคุ้มครองข้อมูลส่วนบุคคลและความจำเป็นทางธุรกิจในการโอนข้อมูลส่วนบุคคลสำหรับหลายๆเหตุผล รวมไปถึงเรื่องความพร้อมของผู้ให้บริการ ประสิทธิภาพ และเศรษฐกิจ ซึ่งหลักปฏิบัติที่ 1 ได้กำหนดให้องค์กรต้องรับผิดชอบในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในการควบคุมขององค์กรนั้น โดยบัญญัติไว้ว่า “องค์กรมีหน้าที่ต้องรับผิดชอบข้อมูลส่วนบุคคลที่มีอยู่ในความครอบครองและการควบคุมดูแล รวมไปถึงข้อมูลที่ถูกถ่ายโอนไปให้บุคคลที่สามเพื่อการประมวลผลด้วย โดยองค์กรอาจใช้สัญญาหรือวิธีการอื่นๆในการให้ความคุ้มครองในระดับที่เท่าเทียมในระหว่างที่มีการประมวลผลข้อมูลโดยบุคคลที่สาม”

ตามหลักปฏิบัติที่ 4.1.3 ของเอกสารที่ 1 ของ PIPEDA กำหนดไว้โดยเฉพาะว่าข้อมูลส่วนบุคคลอาจถูกถ่ายโอนไปยังบุคคลที่สามเพื่อนำไปประมวลผลได้ อีกทั้งยังกำหนดให้องค์กรเหล่านั้นใช้สัญญาหรือวิธีการอื่นๆที่สามารถให้การคุ้มครองในระดับที่เท่าเทียมกันในระหว่างที่มีการประมวลผลข้อมูลโดยบุคคลที่สามอีกด้วย

จะเห็นได้ว่าตามกฎหมาย PIPEDA นั้นไม่ได้กำหนดมาตรการให้ประเทศที่รับโอนข้อมูลส่วนบุคคลจะต้องมีรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ดังเช่นกลุ่มประเทศสมาชิกสหภาพยุโรป แต่ใช้มาตรการว่าประเทศที่รับโอนข้อมูลส่วนบุคคลจะต้องให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เท่าเทียม (comparable level of protection) กับการคุ้มครองข้อมูลส่วนบุคคลในประเทศแคนาดา กล่าวคือผู้ประมวลผลบุคคลที่สามต้องจัดให้มีการคุ้มครองในระดับที่ใกล้เคียงกันกับระดับการคุ้มครองที่ข้อมูลส่วนบุคคลพึงได้รับหากไม่มีการถ่ายโอน แต่มิได้หมายความว่าการคุ้มครองจะต้องเป็นรูปแบบเดียวกัน หากแต่หมายความว่าการคุ้มครองนี้จะต้องมีระดับที่เท่าเทียมกัน อีกทั้งตามกฎหมาย PIPEDA ไม่ได้แบ่งแยกระหว่างการโอนข้อมูลภายในและระหว่างประเทศ แต่ระบุไว้ในกรณีการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สามที่จะต้องให้การคุ้มครองในระดับที่เท่าเทียมตามที่กล่าวมาแล้วเท่านั้น

ตามที่หลักปฏิบัติได้กำหนดไว้ วิธีการเบื้องต้นที่องค์กรมีสิทธิใช้เพื่อการคุ้มครองข้อมูลส่วนบุคคลที่ถูกถ่ายโอนไปยังบุคคลที่สามคือวิธีการทำสัญญาไม่ว่าข้อมูลนี้จะถูกประมวลผลที่ใดก็ตาม ไม่ว่าจะเป็นภายในประเทศแคนาดาหรือต่างประเทศ องค์กรจะต้องดำเนินการตามขั้นตอนที่สมเหตุสมผลในการคุ้มครองมิให้ข้อมูลถูกใช้หรือเปิดเผยโดยไม่ได้รับอนุญาตในระหว่างที่ข้อมูลเหล่านั้นอยู่ในความครอบครองของผู้ประมวลผลบุคคลที่สาม โดยองค์กรนั้นต้องมั่นใจได้ว่านโยบายและวิธีการดำเนินงานของบุคคลที่สามมีความเหมาะสม รวมไปถึงมีการฝึกมาตรการรักษาความปลอดภัยที่มีประสิทธิภาพให้กับพนักงานเพื่อรับรองว่าข้อมูลที่อยู่ในความดูแลนั้นได้รับการคุ้มครองอย่างเหมาะสมอยู่ตลอดเวลาด้วย นอกจากนี้ องค์กรยังจะต้องให้สิทธิในการตรวจสอบบัญชีและตรวจสอบด้วยว่าบุคคลที่สามได้จัดการและจัดเก็บข้อมูลส่วนบุคคลอย่างไร รวมไปถึงการใช้สิทธิในการตรวจสอบในกรณีที่มีหมายค้นด้วย

ส่วนการรับโอนข้อมูลส่วนบุคคลจากต่างประเทศมายังประเทศแคนาดานั้นมีส่วนที่ต้องพิจารณาในกรณีการรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรปเนื่องจากประเทศแคนาดาจะรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรปได้ต่อเมื่อประเทศแคนาดามีการรับรองระดับการคุ้มครองที่เพียงพอตาม Directive 95/46/EC ซึ่งประเทศแคนาดาได้รับการตัดสินจากคณะกรรมาธิการยุโรปในคำวินิจฉัยที่ 2002/2 แล้วว่าประเทศแคนาดามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหากเป็นการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ภายใต้บังคับของกฎหมาย PIPEDA นี้ ดังที่ข้อ 1 ของคำวินิจฉัยที่ 2002/2 ได้บัญญัติว่า “เพื่อจุดประสงค์ของข้อ 25(2) แห่ง Directive 95/46/EC ประเทศแคนาดาถูกจัดว่าเป็นประเทศที่มีระดับการคุ้มครองที่เพียงพอในการถ่ายโอนข้อมูลส่วนบุคคลจากประชาคมไปยังผู้รับตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (กฎหมาย PIPEDA)”

ตามคำวินิจฉัยที่ 2002/2 นี้ได้อธิบายถึงกฎหมาย PIPEDA ว่ามีความครอบคลุมทุกข้อปฏิบัติพื้นฐานที่จำเป็นต่อการให้ความคุ้มครองที่เพียงพอต่อบุคคล ถึงแม้จะมีการกำหนดข้อยกเว้นและข้อจำกัดต่างๆเพื่อคุ้มครองประโยชน์สาธารณะและเพื่อค้นข้อมูลเฉพาะที่ปรากฏในขอบเขตและเครือข่ายสาธารณะ การนำมาตรฐานเหล่านี้มาบังคับใช้จะได้รับการรับประกันจากการแก้ไขเยียวยาทางตุลาการและการควบคุมดูแลอิสระที่จัดให้มีขึ้นโดยเจ้าหน้าที่ที่มีอำนาจ เช่น กรรมาธิการสิทธิความเป็นส่วนตัวของรัฐบาลกลาง (Federal Privacy Commissioner) ที่มีอำนาจในการสืบสวนสอบสวนและแทรกแซง นอกเหนือไปจากนั้นบทบัญญัติของกฎหมายแคนาดาว่าด้วยการรับผิดทางแพ่งยังมีผลบังคับใช้ในเหตุการณ์ที่มีการประมวลผลข้อมูลโดยไม่ชอบด้วยกฎหมายซึ่งก่อให้เกิดความเสียหายต่อบุคคลที่เกี่ยวข้องอีกด้วย[30]

[30] คำวินิจฉัยของคณะกรรมาธิการยุโรป 2002/2/EC, อารัมภบทที่ 9

อย่างไรก็ตามจากข้อสงสัยที่ได้รับการซักถามบ่อยครั้งเกี่ยวกับคำวินิจฉัยระดับความเพียงพอของกฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ประเทศแคนาดา[31] (Frequently Asked Questions on the Commission's adequacy finding on the Canadian Personal Information Protection and electronic Documents Act) การโอนข้อมูลส่วนบุคคลไปยังประเทศแคนาดาอย่างไม่มีข้อจำกัดนั้น คณะกรรมาธิการยุโรปได้ตัดสินให้เฉพาะกรณีการโอนข้อมูลส่วนบุคคลที่ผู้รับโอนอยู่ภายใต้บังคับของกฎหมาย PIPEDA เท่านั้น เช่น ทุกองค์กรในภาคส่วนเอกชนที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในระหว่างทำกิจกรรมทางการค้า รวมไปถึงองค์กรที่ดำเนินงานในระดับรัฐบาลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลด้วย เช่น สายการบิน ธนาคาร บริษัทแพร่ภาพกระจายเสียง บริษัทขนส่งระหว่างมณฑล และเครือข่ายโทรคมนาคม เป็นต้น

หากผู้รับโอนข้อมูลส่วนบุคคลไม่ได้อยู่ภายใต้ขอบเขตอำนาจของกฎหมายนี้ จะต้องจัดให้มีการป้องกันที่เพียงพอและถูกต้องตามกฎหมายก่อนที่ข้อมูลจะถูกโอนออกจากสหภาพยุโรป วิธีการหนึ่งที่จะทำได้คือการทำสัญญาแม่แบบ โดยข้อความที่ใช้ในสัญญาดังกล่าวได้รับการอนุมัติจากคณะกรรมาธิการยุโรปแล้วในเดือนมิถุนายน ค.ศ. 2001[32] ในคำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2001/497[33] การใช้มาตรการดังกล่าวทำให้สามารถรับรองได้ว่าการโอนข้อมูลส่วนบุคคลจะมีมาตรฐานเดียวกันทั่วทั้งประเทศแคนาดา

3.3.3 ข้อยกเว้นของกฎหมาย PIPEDA[34]

แม้ว่าตามกฎหมาย PIPEDA จะมิได้ห้ามองค์กรต่างๆในประเทศแคนาดาโอนข้อมูลส่วนบุคคลไปยังเขตอำนาจอื่นหรือประเทศอื่นเพื่อการประมวลผล แต่อย่างไรก็ตามกฎหมายได้กำหนดหน้าที่ให้องค์กรที่เป็นฝ่ายโอนข้อมูลส่วนบุคคลมีความรับผิดชอบต่อข้อมูลส่วนบุคคลที่อยู่ในครอบครองขององค์กรที่ข้อมูลนั้นถูกโอนไปถึงด้วย ซึ่งวิธีการชั้นต้นในการคุ้มครองข้อมูลส่วนบุคคลคือการคุ้มครองผ่านทางการทำสัญญาดังที่กล่าวมาแล้ว

อย่างไรก็ตาม ในคู่มือการปฏิบัติงานว่าด้วยการประมวลผลข้อมูลส่วนบุคคลข้ามพรมแดนก็ได้ยอมรับไว้ชัดเจนว่าไม่มีสัญญาใดที่มีผลผูกผันเหนือกฎหมายอาญา ความมั่นคงแห่งชาติหรือกฎหมายอื่นๆของประเทศปลายทางที่ข้อมูลถูกถ่ายโอนไปได้ จึงเป็นเรื่องสำคัญอย่างยิ่งที่องค์กรต่างๆจะต้องประเมินความเสี่ยงที่อาจส่งผลกระทบต่อความปลอดภัยหรือการรักษาข้อมูลส่วนบุคคล

---

[31] European Commission, *supra note 27*.

[32] *Ibid.*

[33] โปรดดูเนื้อหาของสัญญาแม่แบบตามคำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2001/497 ที่ภาคผนวก ง

[34] Office of the Privacy Commissioner of Canada, *supra note 29*.

ของผู้ใช้บริการให้เป็นความลับในกรณีที่ข้อมูลนั้นถูกส่งไปให้ผู้บริการบุคคลที่สามซึ่งดำเนินกิจการภายนอกประเทศแคนาดา

ในทางปฏิบัติองค์กรต่างๆจะต้องแสดงความโปร่งใสเกี่ยวกับวิธีการที่องค์กรใช้ในการจัดการกับข้อมูลส่วนบุคคลของผู้ใช้บริการ ซึ่งรวมไปถึงการให้คำแนะนำแก่ผู้ใช้บริการด้วยว่าข้อมูลส่วนบุคคลของตนนั้นอาจจะถูกส่งไปยังประเทศอื่นเพื่อนำไปประมวลผล และในระหว่างที่ข้อมูลส่วนบุคคลนั้นอยู่ในประเทศอื่น ศาลหรือหน่วยงานที่บังคับใช้กฎหมายและรักษาความมั่นคงแห่งชาติมีสิทธิที่จะเข้าถึงข้อมูลส่วนบุคคลเหล่านั้นได้

3.3.4 องค์กรที่มีหน้าที่บังคับการให้เป็นไปตามกฎหมาย

ภายใต้กฎหมาย PIPEDA ได้กำหนดให้จัดตั้งสำนักงานคณะกรรมาธิการสิทธิความเป็นส่วนตัวแห่งแคนาดา (Office of the Privacy Commissioner of Canada) เป็นองค์กรที่คอยช่วยเหลือ ให้คำปรึกษาบุคคลเกี่ยวกับสิทธิในความเป็นส่วนตัว ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และการคุ้มครองข้อมูลทางอิเล็กทรอนิกส์ที่ได้รับการคุ้มครองภายใต้กฎหมายฉบับนี้ โดยสำนักงานนี้มีอำนาจในการควบคุมองค์กรเอกชนและหน่วยงานที่เกี่ยวข้องตามกฎหมาย PIPEDA ให้กระทำการตามภาระหน้าที่ที่ได้กำหนดไว้เป็นแบบปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

นอกจากการจัดตั้งสำนักงานคณะกรรมาธิการสิทธิความเป็นส่วนตัวแห่งแคนาดาแล้ว ตามกฎหมายฉบับนี้ได้กำหนดให้มีเจ้าหน้าที่ซึ่งมีอำนาจควบคุมและบังคับการให้เป็นไปตามกฎหมาย คือกรรมาธิการสิทธิความเป็นส่วนตัว (Privacy Commissioner) ซึ่งมีอำนาจหน้าที่ที่สำคัญดังต่อไปนี้คือ[35]

(1) รับคำร้องของบุคคลในกรณีที่องค์กรฝ่าฝืนบทบัญญัติ หรือในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล และแจ้งให้องค์กรที่ถูกร้องเรียนทำการสอบสวนและพิจารณาคำร้องดังกล่าว

(2) หากกรรมาธิการพิจารณาแล้วเห็นว่ามีเหตุอันสมควรในอันที่จะต้องทำการสอบสวนเรื่องใดๆ ที่เห็นว่ามีการละเมิดข้อมูลส่วนบุคคล กรรมาธิการสามารถหยิบยกเรื่องดังกล่าวขึ้นมาพิจารณาได้

(3) เพื่อให้บรรลุวัตถุประสงค์ในการดำเนินการสอบสวน กรรมาธิการอาจใช้อำนาจเรียกให้บุคคลใดมาให้คำชี้แจงหรือเรียกให้ส่งหลักฐานใดๆที่เกี่ยวข้องกับเรื่องที่มีการร้องเรียนนั้น รับหลักฐานและข้อมูลอื่นใดตามที่กรรมาธิการเห็นสมควร เข้าไปในสถานที่ขององค์กรใดๆในเวลาที่เหมาะสม และมีอำนาจซักถามบุคคลในสถานที่นั้นได้ตามที่เห็นสมควร ตลอดจนเจรจาเป็นการส่วนตัวกับบุคคลที่อยู่ในสถานที่ดังกล่าว

---

[35] นคร เสรีรักษ์, *อ้างแล้ว เชิงอรรถที่ 19*, น.183.

(4) กรรมาธิการต้องจัดทำรายงานผลการพิจารณาและแก้ไขปัญหาประกอบด้วย คำวินิจฉัยและคำแนะนำของกรรมาธิการในคดีต่างๆ การระงับข้อโต้แย้งที่คู่กรณีได้ตกลงกัน คำร้องที่องค์กรส่งให้แก่กรรมาธิการ คำบอกกล่าวเกี่ยวกับการดำเนินการที่ได้กระทำไปแล้วหรือที่จะกระทำตามคำแนะนำที่ระบุไว้ในรายงาน หรือเหตุผลที่ไม่ดำเนินการหรือจะไม่ดำเนินการ และความช่วยเหลือที่ผู้ยื่นคำร้องอาจได้รับตามที่กำหนดในกฎหมาย

บทที่ 4
การคุ้มครองการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ในคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14

4.1 ความสำคัญของคดีเลขที่ C-362/14

จากการศึกษาพบว่าแต่ละประเทศมีแนวทางการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน โดยความแตกต่างนั้นมีทั้งเรื่องรูปแบบที่นำมาใช้เพื่อการคุ้มครองข้อมูลส่วนบุคคลหรือความแตกต่างในรายละเอียดของกฎเกณฑ์ มาตรการที่ใช้บังคับในแต่ละประเทศ เมื่อมีความจำเป็นในการโอนข้อมูลส่วนบุคคลระหว่างประเทศทำให้เกิดหลักเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศขึ้น ดังที่สหภาพยุโรปมีการกำหนดใน Directive 95/46/EC บัญญัติให้สามารถถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศนอกสมาชิกสหภาพยุโรปได้เมื่อประเทศนั้นๆมีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ

อย่างไรก็ตามสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลอาจถูกจำกัดด้วยคุณค่า (value) ที่กฎหมายคุ้มครองในเรื่องอื่นๆ เช่น เหตุผลเกี่ยวกับเรื่องความมั่นคงของรัฐ (national security) ทำให้บางกรณีการรักษาความมั่นคงปลอดภัยอาจทำให้เกิดการละเมิดสิทธิในความเป็นส่วนตัวได้ การใช้มาตรการทางกฎหมายจึงต้องหาจุดสมดุลระหว่างการคุ้มครองประโยชน์สาธารณะกับการคุ้มครองสิทธิในข้อมูลส่วนบุคคล ซึ่งมักมีปัญหาในการพิจารณาว่าการจำกัดสิทธิของบุคคลนั้นสามารถกระทำได้ในขอบเขตเพียงใด และต้องใช้กฎเกณฑ์ใดมาพิจารณาเมื่อมีข้อขัดแย้งเกิดขึ้น

การขัดกันระหว่างสิทธิความเป็นส่วนตัวในข้อมูลส่วนบุคคลกับเหตุผลในเรื่องความมั่นคงของรัฐปรากฏให้เห็นอย่างชัดเจนเมื่อนายเอ็ดเวิร์ด สโนว์เดน (Adward Snowden) ผู้เคยปฏิบัติงานเป็นเจ้าหน้าที่สำนักงานสืบราชการลับกลาง (Central Intelligence Agency หรือ CIA) ออกมาเปิดเผยถึงโครงการปริซึม (PRISM)[1] ซึ่งเป็นแผนงานรวบรวมข่าวกรองขนาดใหญ่ที่มีวัตถุประสงค์ในด้านการป้องกันความปลอดภัยจากผู้ก่อการร้ายในประเทศสหรัฐอเมริกา โครงการนี้ให้อำนาจสำนักงานความมั่นคงแห่งชาติ (National Security Agency หรือ NSA) รวมทั้งหน่วยงานทางด้านความมั่นคงอื่นๆ เช่น สำนักงานสืบราชการลับกลาง, หน่วยสืบสวนของรัฐบาลกลาง (Federal Bureau of Investigation หรือ FBI) สามารถดักฟังข้อมูลทางโทรศัพท์และเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการทางอินเทอร์เน็ตผ่านผู้ให้บริการที่มีการใช้งานอย่างแพร่หลาย เช่น เฟซบุ๊ค

[1] ชาญเชาวน์ ไชยานุกิจ, “เสรีภาพทุกตารางนิ้วในสหรัฐอเมริกา,” สืบค้นเมื่อวันที่ 1 เมษายน 2559, จาก http://www.bangkokbiznews.com/mobile/view/blog/513103.

(Facebook), กูเกิ้ล (Google), ยาฮู (Yahoo!) และ แอปเปิ้ล (Apple) เป็นต้น โดยโครงการปริซึม สามารถนำเอาข้อมูลของบุคคลมาตรวจสอบและเก็บรักษาไว้ในระบบได้ นายสโนว์เดนได้เปิดเผยในหนังสือพิมพ์เดอะการ์เดียน (The Guardian) ว่าภายใต้โครงการปริซึมหน่วยงานของสหรัฐอเมริกาสามารถเข้าถึงข้อมูลจากเซิร์ฟเวอร์ (server) ของบริษัทสื่อสารทั้ง 9 แห่งได้โดยตรงโดยไม่ต้องขอหมายศาลเพื่อทำการเก็บรวบรวมข้อมูลส่วนตัวของผู้ใช้บริการได้เป็นจำนวนมาก[2]

โครงการปริซึมเป็นโครงการลับของหน่วยงานความมั่นคงแห่งชาติที่มีฐานการให้อำนาจมาจากมาตรา 702 ของรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศ (Foreign Intelligence Surveillance Act 1978) หรือเรียกโดยย่อว่า “FISA” กฎหมายนี้มีวัตถุประสงค์ใช้ในการสืบข้อมูลผู้ก่อการร้ายต่างชาติ โดยมีการแก้ไขเพิ่มเติมใน ค.ศ. 2008 เพื่อเพิ่มเติมเกี่ยวกับการสอดแนมข้อมูลในต่างประเทศ โดยได้ขยายอำนาจของรัฐในการสอดแนมข้อมูลส่วนบุคคลที่ไม่ใช่คนชาติสหรัฐอเมริกาและอยู่นอกประเทศสหรัฐอเมริกา รวมทั้งบุคคลต่างชาติใด ๆ ซึ่งมีการสื่อสารโดยผ่านบริการเก็บข้อมูลทางอินเทอร์เน็ตและโดยสำนักงานนั้นตั้งอยู่ในสหรัฐอเมริกา

อย่างไรก็ตามมีการถกเถียงถึงความโปร่งใสของการใช้อำนาจตามกฎหมายดังกล่าว รวมถึงประเด็นว่าสำนักงานความมั่นคงแห่งชาติได้กระทำเกินขอบเขตอำนาจกฎหมายจากการเก็บรวมรวมข้อมูลขนาดใหญ่อันนำมาสู่การฟ้องคดีต่อศาลในประเทศสหรัฐอเมริกาด้วยเช่นกัน[3]

การเปิดเผยของนายสโนว์เดนก่อให้เกิดความหวั่นวิตกต่อผู้ใช้บริการอินเทอร์เน็ตทั้งในประเทศสหรัฐอเมริกาและต่างประเทศ โดยเฉพาะผู้เป็นเจ้าของข้อมูลส่วนบุคคลในกลุ่มสมาชิกสหภาพยุโรปที่ใช้บริการอินเทอร์เน็ตผ่านเครือข่ายสังคมออนไลน์ (social network) เนื่องจากข้อมูลต่างๆของผู้ให้บริการนั้นสามารถถ่ายโอนไปยังสำนักงานใหญ่ของผู้ให้บริการซึ่งอยู่ในประเทศสหรัฐอเมริกาผ่านทางโครงการเซฟฮาร์เบอร์ได้ ความไม่ไว้วางใจในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้เป็นที่มาของคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14 เมื่อ

---

[2] การเปิดเผยถึงรายงานการเข้าถึงข้อมูล พบว่าที่ผ่านมามีการใช้ข้อมูลจากโครงการปริซึมเพื่ออ้างอิงในรายงานราชการลับกว่า 77,000 ฉบับ แต่จากเอกสารลับของนายสโนว์เดนเปิดเผยว่าเพียงแค่เดือนเดียวเท่านั้น สำนักงานความมั่นคงแห่งชาติได้รวบรวมข้อมูลข่าวสารอิเล็กทรอนิกส์เกือบ 3,000 ล้านชิ้น โปรดศึกษาเพิ่มเติมในสรินณา อารีธรรมศิริกุล, “สายลับคอมพิวเตอร์กระทบความไว้วางใจรัฐบาลโอบามา,” จาก http://www.siamintelligence.com/prism-program-spying-system-of-obama/.

[3] ประชาไท, “วิกิมีเดียฟ้อง NSA หวังหยุดสอดแนมการสื่อสารประชาชน,” สืบค้นเมื่อวันที่ 10 เมษายน 2559, จาก http://prachatai.com/journal/2015/03/58382.

ผู้ใช้บริการอินเทอร์เน็ตไม่ไว้วางใจในความปลอดภัยของข้อมูลส่วนบุคคลของตนที่ถูกโอนไปยังสหรัฐอเมริกา จึงได้ร้องเรียนต่อองค์กรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลในประเทศของตนเพื่อขอให้ระงับการถ่ายโอนข้อมูลส่วนบุคคลของตนไปยังประเทศสหรัฐอเมริกา ดังคำร้องเรียนของนายแม็กซิมิเลียน เชร็มส์ (Maximilian Schrems) ที่จะได้ศึกษาในส่วนต่อไป

คำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14 มีความสำคัญต่อการศึกษาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างยิ่ง เนื่องจากเป็นการวางหลักเกณฑ์สำคัญในการพิจารณาระดับการคุ้มครองส่วนบุคคลที่เพียงพอ อีกทั้งมีการอธิบายขอบเขตอำนาจขององค์กรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรป รวมถึงขอบเขตในการเข้าแทรกแซงข้อมูลส่วนบุคคลโดยเจ้าหน้าที่รัฐอีกด้วย คำพิพากษานี้จึงถือเป็นจุดเริ่มต้นการเปลี่ยนแปลงมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะกรณีที่ต้องมีการโอนและรับโอนข้อมูลส่วนบุคคลระหว่างประเทศ

4.2 สรุปย่อคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14

คดีเลขที่ C-362/14

ระหว่าง	นายแม็กซิมิเลียน เชร็มส์ (Maximilian Schrems)	ผู้ฟ้องคดี
	กรรมาธิการคุ้มครองข้อมูลไอร์แลนด์ (Data Protection Commissioner)	ผู้ถูกฟ้องคดี

กฎหมายที่เกี่ยวข้อง

กฎบัตรสิทธิขั้นพื้นฐานแห่งสหภาพยุโรป ข้อ 7, 8, 47

Directive 95/46/EC ข้อ 25 และ 28

คำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2000/520

Communication COM (2013) 846 final

Communication COM (2013) 847 final

สรุปข้อเท็จจริง

นายเชร็มส์เป็นชาวออสเตรียนซึ่งอาศัยอยู่ในประเทศออสเตรียจึงเป็นผู้อาศัยอยู่ในกลุ่มประเทศสมาชิกเครือสหภาพยุโรป เขาเป็นผู้ใช้เครือข่ายสังคมออนไลน์เฟซบุ๊คมาตั้งแต่ปี ค.ศ. 2008 โดยผู้ใช้เฟซบุ๊คในยุโรปจะมีการทำข้อตกลงกับบริษัทเฟซบุ๊คไอร์แลนด์ ซึ่งเป็นบริษัทสาขาของบริษัทเฟซบุ๊คที่มีสาขาใหญ่อยู่ในประเทศสหรัฐอเมริกา ข้อมูลส่วนบุคคลของผู้ใช้บริการบริษัทเฟซบุ๊คในสหภาพยุโรปจะถูกถ่ายโอนไปยังบริษัทเฟซบุ๊คในสหรัฐอเมริกาเพื่อทำการประมวลผลข้อมูล (ย่อหน้าที่ 26-27)[4]

วันที่ 25 มิถุนายน ค.ศ. 2013 นายเชร็มส์ได้ร้องเรียนต่อคณะกรรมาธิการคุ้มครองข้อมูลไอร์แลนด์เพื่อร้องขอให้คณะกรรมาธิการคุ้มครองข้อมูลไอร์แลนด์ใช้อำนาจทางกฎหมายในการห้ามมิให้บริษัทเฟซบุ๊คไอร์แลนด์ถ่ายโอนข้อมูลส่วนบุคคลของตนไปยังประเทศสหรัฐอเมริกา เขายืนยันในข้อร้องเรียนว่ากฎหมายและวิธีปฏิบัติที่มีผลบังคับใช้ในประเทศสหรัฐอเมริกานั้นไม่มีการคุ้มครองที่เพียงพอสำหรับข้อมูลส่วนบุคคลจากการสอดส่องดูแลโดยเจ้าหน้าที่รัฐในประเทศสหรัฐอเมริกา นายเชร็มส์ได้อ้างถึงคำเปิดเผยของนายเอ็ดเวิร์ด สโนว์เดนเกี่ยวกับการกระทำของหน่วยงานที่ทำหน้าที่สืบราชการลับในสหรัฐอเมริกา โดยเฉพาะอย่างยิ่งการกระทำของสำนักงานความมั่นคงแห่งชาติสหรัฐอเมริกา (ย่อหน้าที่ 28)

คณะกรรมาธิการคุ้มครองข้อมูลไอร์แลนด์ปฏิเสธไม่รับข้อร้องเรียนของนายเชร็มส์ เนื่องจากเห็นว่าไม่มีมูลไม่มีหลักฐานที่แสดงว่าข้อมูลส่วนบุคคลของนายเชร็มส์ได้ถูกเข้าถึงและตรวจสอบโดยสำนักงานความมั่นคงแห่งชาติจริง และเสริมว่านายเชร็มส์ไม่สามารถยื่นข้อกล่าวหาต่อบริษัทเฟซบุ๊คตามที่ได้ร้องเรียน เนื่องจากการตัดสินข้อสงสัยใดๆก็ตามที่เกี่ยวข้องกับความเหมาะสมของระดับการคุ้มครองในสหรัฐอเมริกานั้นต้องพิจารณาตามคำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2000/520 และคณะกรรมาธิการยุโรปได้ตัดสินว่าสหรัฐอเมริกาได้รับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอเอาไว้แล้วในคำวินิจฉัยนั้น (ย่อหน้าที่ 29)

นายเชร็มส์ได้ดำเนินการฟ้องร้องต่อศาลสูงไอร์แลนด์เพื่อคัดค้านคำตัดสินปัญหาในการดำเนินคดีหลัก โดยศาลสูงไอร์แลนด์ได้ตัดสินว่าการสอดแนมทางอิเล็กทรอนิกส์ (electronic surveillance) และการดักรับข้อมูล (interception) ในการถ่ายโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปไปยังสหรัฐอเมริกานั้นเป็นสิ่งจำเป็นในทางสาธารณประโยชน์ แต่อย่างไรก็ตาม ศาลสูงได้เสริมไว้ด้วยว่า คำเปิดเผยของนายเอ็ดเวิร์ด สโนว์เดนนั้นได้แสดงให้เห็นว่าสำนักงานความมั่นคงแห่งชาติและ

---

[4] เนื่องจากเป็นการแปลความมาจากคำพิพากษาภาษาต่างประเทศ จึงมีการแสดงหมายเลขว่าเป็นสรุปจากย่อหน้าใดในคำพิพากษาฉบับเต็ม โปรดดูคำพิพากษาฉบับเต็มในภาคผนวก ก

หน่วยงานของรัฐบาลอื่นๆได้กระทำการเกินเลยจริง เพราะหน่วยงานเหล่านี้สามารถเข้าถึงข้อมูลอย่างไม่เฉพาะเจาะจง (indiscriminate) และกระทำในขอบข่ายที่กว้าง (large scale) (ย่อหน้าที่ 30-31)

ตามกฎหมายของประเทศไอร์แลนด์ได้จำกัดการถ่ายโอนข้อมูลส่วนบุคคลไปนอกอาณาเขตยกเว้นแต่ประเทศนอกกลุ่มสมาชิกสหภาพยุโรปมีการรับรองระดับการคุ้มครองความเป็นส่วนตัวและสิทธิเสรีภาพขั้นพื้นฐานที่เพียงพอ สิทธิในความเป็นส่วนตัวและความละเมิดมิได้ของเคหสถานซึ่งได้รับการรับรองโดยรัฐธรรมนูญของประเทศไอร์แลนด์นั้นมีความสำคัญ การแทรกแซงสิทธิเหล่านั้นจะต้องได้สัดส่วน (proportionate) และเป็นไปตามกฎหมาย (accordance with the law) การเข้าถึงข้อมูลจำนวนมากโดยไม่เฉพาะเจาะจงบุคคลนั้นเป็นการกระทำที่ขัดกับหลักการพื้นฐานที่รัฐธรรมนูญไอร์แลนด์ได้ให้การคุ้มครองไว้อย่างชัดเจน เพราะการดักรับข้อมูลการสื่อสารทางอิเล็กทรอนิกส์ที่สอดคล้องกับรัฐธรรมนูญของประเทศไอร์แลนด์จะต้องพิสูจน์ได้ว่าการดักรับข้อมูลนั้นมีจุดมุ่งหมาย เป็นการสอดแนมที่เจาะจงบุคคลหรือกลุ่มคนที่แน่นอนเพื่อประโยชน์ทางความมั่นคงแห่งชาติหรือการยับยั้งอาชญากรรมโดยมีการป้องกันที่เหมาะสมและตรวจสอบได้ ดังนั้นประเด็นเรื่องนี้มีข้อพิจารณาเป็นอย่างยิ่งเกี่ยวกับระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศสหรัฐอเมริกา คณะกรรมาธิการคุ้มครองข้อมูลไอร์แลนด์ควรจะมีการสอบสวนตามข้อเรียกร้องของนายเชร็มส์ ดังนั้นคณะกรรมาธิการคุ้มครองข้อมูลไอร์แลนด์เป็นฝ่ายผิดที่ปฏิเสธไม่สอบสวนข้อเรียกร้องดังกล่าว (ย่อหน้าที่ 32-33)

นอกจากนี้ศาลสูงไอร์แลนด์ได้พิจารณาว่ากรณีนี้มีส่วนเกี่ยวข้องกับการปฏิบัติตามกฎหมายของสหภาพยุโรป และคำตัดสินปัญหาในคดีหลักต้องมีการพิจารณาความถูกต้องทางกฎหมาย โดยศาลสูงไอร์แลนด์พิจารณาว่าคำวินิจฉัยที่ 2000/520 มิได้ปฏิบัติตามข้อกำหนดที่อยู่ในข้อที่ 7[5] และ 8[6] ของกฎบัตรสิทธิขั้นพื้นฐานแห่งสหภาพยุโรปและจากหลักปฏิบัติที่กำหนดโดยศาล

---

[5] ข้อ 7 ความเคารพต่อความเป็นส่วนตัวและชีวิตครอบครัว

บุคคลมีสิทธิได้รับความเคารพในความเป็นส่วนตัว ชีวิตครอบครัวและการสื่อสาร

[6] ข้อ 8 การคุ้มครองข้อมูลส่วนบุคคล

(1) บุคคลมีสิทธิได้รับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับตน

(2) การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปด้วยความยุติธรรม ภายใต้วัตถุประสงค์ที่เฉพาะเจาะจง บนพื้นฐานของการให้ความยินยอมจากเจ้าของข้อมูลดังกล่าว หรือภายใต้ขอบวัตถุประสงค์อื่นตามที่กฎหมายบัญญัติ นอกจากนี้บุคคลยังมีสิทธิเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตน และมีสิทธิร้องขอให้มีการแก้ไขข้อมูลดังกล่าวให้ถูกต้อง

(3) ในการบังคับการให้เป็นไปตามหลักการคุ้มครองข้อมูลส่วนบุคคลข้างต้นจะต้องจัดให้มีการควบคุมการปฏิบัติดังกล่าวโดยองค์กรของรัฐที่เป็นอิสระ

ยุติธรรมในคำพิพากษาคดี Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238) ที่ว่าสิทธิในการเคารพชีวิตส่วนตัวซึ่งรับรองโดยข้อ 7 ของกฎบัตรฯจะไร้ความหมายถ้าหากหน่วยงานของประเทศสมาชิกได้รับอำนาจในการเข้าถึงการสื่อสารทางอิเล็กทรอนิกส์ได้โดยไม่มีกฎเกณฑ์แน่นอน (casual) และเป็นการทั่วไป (generalised) โดยไม่มีการให้เหตุผลเกี่ยวกับความมั่นคงของชาติหรือการป้องกันอาญากรรมที่เฉพาะเจาะจงบุคคลที่เกี่ยวข้องและไม่มีวิธีปฏิบัติซึ่งมีการป้องกันที่เหมาะสมและตรวจสอบได้ (ย่อหน้าที่ 34)

ศาลสูงไอร์แลนด์ยังได้พิจารณาต่อไปว่าการร้องเรียนของนายเชร็มส์ได้ทำให้เกิดประเด็นข้อสงสัยว่ากรรมาธิการคุ้มครองข้อมูลไอร์แลนด์ต้องผูกพันตามข้อ 25(6)[7] ของ Directive 95/46/EC ที่ให้อำนาจคณะกรรมาธิการยุโรปในการตัดสินชี้ขาดว่าประเทศใดมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอซึ่งคณะกรรมาธิการยุโรปได้ตัดสินชี้ขาดแล้วในคำวินิจฉัยที่ 2000/520 ว่าประเทศสหรัฐอเมริกาได้รับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอจึงเป็นเหตุให้กรรมาธิการคุ้มครองข้อมูลไอร์แลนด์ต้องยึดตามคำวินิจฉัยนี้ด้วยเช่นกัน หรือกรรมาธิการคุ้มครองข้อมูลไอร์แลนด์เป็นอิสระจากคำตัดสินของคณะกรรมาธิการยุโรป ตามที่ข้อ 8(3) ของกฎบัตรสิทธิขั้นพื้นฐานแห่งสหภาพยุโรปได้ให้อำนาจไว้ (ย่อหน้าที่ 35)

ศาลสูงไอร์แลนด์จึงได้ตัดสินให้มีการดำเนินคดีต่อไป และส่งประเด็นข้อสงสัยดังต่อไปนี้ให้ศาลยุติธรรมแห่งสหภาพยุโรปได้พิจารณาคดีต่อ โดยมีการอ้างประเด็นข้อสงสัยดังนี้ (ย่อหน้าที่ 36)

(1) ในระหว่างพิจารณาข้อร้องเรียนเจ้าหน้าที่ผู้ดูแลและบังคับใช้กฎหมายคุ้มครองข้อมูลจะต้องปฏิบัติตามเนื้อความในคำวินิจฉัยที่ 2000/520 ซึ่งเป็นผลจากข้อ 25(6) ของ Directive 95/46/EC หรือจะต้องปฏิบัติตาม ข้อที่ 7, 8 และ 47 ของกฎบัตรสิทธิขั้นพื้นฐานแห่งสหภาพยุโรป

(2) เจ้าหน้าที่อาจ/หรือต้องทำการสอบสวนปัญหาโดยพิจารณาจากสถานการณ์ที่เปลี่ยนแปลงไปตั้งแต่ที่มีการออกคำวินิจฉัยของคณะกรรมาธิการยุโรปหรือไม่

---

[7] ข้อ 25(6) คณะกรรมาธิการยุโรปมีสิทธิตัดสินตามขั้นตอนที่ได้อ้างถึงในข้อที่ 31(2) ว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปรับรองระดับการคุ้มครองที่เพียงพอ ... โดยเหตุที่มาจากกฎหมายภายในประเทศและพันธะสัญญาระหว่างประเทศที่ประเทศนั้นได้มีเข้าไปมีส่วนร่วม โดยเฉพาะที่มีขึ้นจากข้อสรุปของการเจรจาต่อรองที่อ้างถึงในวรรคห้า เพื่อการคุ้มครองชีวิตส่วนตัวและสิทธิเสรีภาพของปัจเจกบุคคลขั้นพื้นฐาน

การพิจารณา

ประเด็นข้อสงสัยนั้นจะต้องพิจารณาตรวจสอบร่วมกันระหว่างข้อ 25(6) ของ Directive 95/46/EC กับข้อที่ 7, 8 และ 47[8] ของกฎบัตรสิทธิขั้นพื้นฐานแห่งสหภาพยุโรป ในกรณีที่คณะกรรมาธิการยุโรปได้ใช้อำนาจตาม Directive ในการออกคำวินิจฉัยเพื่อตัดสินชี้ขาดว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้นมีระดับการคุ้มครองที่เพียงพอ จะเป็นการขัดขวางการใช้อำนาจของหน่วยงานคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิก (National Supervisory Authorities) ตามข้อ 28 ของ Directive หรือไม่ หากเกิดกรณีที่บุคคลได้มีการยื่นร้องเรียนต่อหน่วยงานคุ้มครองข้อมูลส่วนบุคคลในประเทศของตนเนื่องจากเห็นว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่รับโอนข้อมูลส่วนบุคคลไปนั้นไม่สามารถคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอได้ และต้องตีความในขอบเขตเพียงใด (ย่อหน้าที่ 37)

ตามบทบัญญัติของ Directive 95/46/EC พิจารณาตามข้อ 1[9] และอารัมภบท 2[10] และ 10[11] Directive นั้นมีจุดประสงค์ที่จะรับรองไม่ใช่แค่การคุ้มครองสิทธิขั้นพื้นฐานในชีวิตส่วนตัวที่

---

[8] ข้อ 47 สิทธิที่จะได้รับการเยียวยาที่มีประสิทธิภาพและการพิจารณาคดีอย่างยุติธรรม

(1) บุคคลผู้ซึ่งสิทธิและเสรีภาพที่ได้รับรองโดยกฎหมายของสหภาพยุโรปถูกละเมิดมีสิทธิที่จะได้รับการเยียวยาที่มีประสิทธิภาพก่อนการพิจารณาของศาลภายใต้การปฏิบัติตามเงื่อนไขที่กำหนดไว้ในข้อนี้ได้

(2) บุคคลมีสิทธิที่จะได้รับการรับฟังภายในเวลาอันสมควรโดยศาลที่อิสระและเป็นกลางที่จัดตั้งขึ้นตามกฎหมาย ทุกคนสามารถได้รับคำแนะนำ ได้สิทธิในการแก้ต่าง และตั้งตัวแทน

(3) ผู้ที่ขาดแคลนทรัพยากรที่เพียงพออาจได้รับความช่วยเหลือทางกฎหมาย ความช่วยเหลือดังกล่าวเป็นสิ่งที่จำเป็นเพื่อให้สามารถเข้าถึงความยุติธรรมได้อย่างมีประสิทธิภาพ

[9] ข้อ 1 วัตถุประสงค์ของ Directive

ตาม Directive นี้ ประเทศสมาชิกจะต้องคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานของบุคคลธรรมดา โดยเฉพาะอย่างยิ่งสิทธิในความเป็นส่วนตัวในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

[10] อารัมภบท 2 ระบบประมวลผลข้อมูลนั้นถูกออกแบบมาเพื่ออำนวยประโยชน์แก่มนุษย์ ... ระบบเหล่านี้ต้องเคารพสิทธิเสรีภาพขั้นพื้นฐานของบุคคลธรรมดาโดยไม่เลือกสัญชาติหรือถิ่นที่อยู่ของบุคคลนั้น โดยเฉพาะสิทธิในความเป็นส่วนตัว และนำมาซึ่ง ... สวัสดิภาพของแต่ละบุคคล

[11] อารัมภบท 10 ประมวลกฎหมายภายในประเทศว่าด้วยการประมวลผลข้อมูลส่วนบุคคลมีวัตถุประสงค์เพื่อคุ้มครองสิทธิเสรีภาพขั้นพื้นฐาน โดยเฉพาะสิทธิในความเป็นส่วนตัวซึ่งได้รับการเห็นชอบทั้งในข้อที่ 8 ของอนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานแห่ง

เกี่ยวข้องกับการประมวลผลข้อมูลส่วนตัวเท่านั้น แต่ยังรับรองการคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานเหล่านั้นในระดับสูงด้วย ความสำคัญของสิทธิที่จะได้รับการเคารพชีวิตส่วนตัวซึ่งได้รับการรับรองโดยข้อที่ 7 ของกฎบัตรฯ และสิทธิขั้นพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจากข้อที่ 8 ของกฎบัตรฯนั้นยังได้ถูกเน้นย้ำในคำพิพากษาบรรทัดฐานของศาลเช่นกัน[12] (ย่อหน้าที่ 39)

ตามข้อ 28(1)[13] ของ Directive 95/46/EC กำหนดให้ประเทศสมาชิกแต่งตั้งเจ้าหน้าที่ของรัฐทำหน้าที่รับผิดชอบการควบคุมดูแลการถ่ายโอนข้อมูลส่วนบุคคลซึ่งสามารถทำหน้าที่ได้อย่างอิสระ โดยต้องมีการรับรองความอิสระในการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อทำให้การคุ้มครองสิทธิของบุคคลมีประสิทธิภาพมากยิ่งขึ้น การจัดตั้งเจ้าหน้าคุ้มครองข้อมูลส่วนบุคคลที่ทำงานได้โดยอิสระของประเทศสมาชิกจึงเป็นองค์ประกอบที่จำเป็นในการให้ความคุ้มครองแก่ปัจเจกบุคคลในกรณีที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามที่ได้แถลงไว้ในอารัมภบท 62[14] ในบทนำของ Directive 95/46/EC นอกจากนี้เจ้าหน้าคุ้มครองข้อมูลส่วนบุคคลยังมีขอบเขตอำนาจที่กว้างขวางตามข้อ 28(3) ของ Directive อีกด้วย เช่นอำนาจในการสอบสวน อำนาจในการแทรกแซง และอำนาจในการเข้าร่วมกับกระบวนการพิจารณาคดีตามกฎหมาย[15] (ย่อหน้าที่ 40-43)

ยุโรป (ลงนาม ณ กรุงโรม วันที่ 4 พฤศจิกายน ค.ศ. 1950) และในหลักทั่วไปของกฎหมายประชาคม ... ด้วยเหตุนั้น การปรับกฎหมายเหล่านี้ให้สอดคล้องกันจะต้องมิทำให้การคุ้มครองที่พึงได้ของบุคคลนั้นย่อหย่อนลง แต่ในทางกลับกันจะต้องแสวงหาวิธีที่จะรับรองการคุ้มครองขั้นสูงขึ้นไปในประชาคม

[12] ดูเพิ่มเติมในคำพิพากษาในคดี *Rijkeboer*, C-553/07, EU:C:2009:293, วรรค 47; *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, วรรค 53; และ *Google Spain and Google*, C-131/12, EU:C:2014:317, วรรค 53, 66, 74.

[13] ข้อ 28(1) หน่วยงานที่มีอำนาจคุ้มครองข้อมูลส่วนบุคคล

ประเทศสมาชิกแต่ละประเทศจะต้องมอบหมายเจ้าหน้าที่รัฐจำนวนหนึ่งหรือมากกว่าหนึ่งคนให้มีหน้าที่รับผิดชอบเฝ้าดูแลและตรวจสอบการนำบทบัญญัติซึ่งประเทศสมาชิกได้ลงมติยอมรับตาม Directive มาปรับใช้ภายในประเทศของตน

เจ้าหน้าที่เหล่านี้มีสิทธิในการปฏิบัติหน้าที่ที่ได้รับมอบหมายอย่างอิสระสมบูรณ์

[14] อารัมภบท 62 การจัดตั้งหน่วยงานที่มีอำนาจคุ้มครองข้อมูลส่วนบุคคลในประเทศสมาชิกซึ่งใช้อำนาจหน้าที่ได้อย่างอิสระสมบูรณ์เป็นองค์ประกอบสำคัญของการคุ้มครองปัจเจกชนสำหรับการประมวลผลข้อมูลส่วนบุคคล

[15] อ่านรายละเอียดอำนาจของหน่วยงานคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติม ในบทที่ 3 ส่วนที่ 3.1.4

อำนาจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้นจำกัดให้มีผลเฉพาะการประมวลผลข้อมูลส่วนบุคคลที่กระทำภายในอาณาเขตประเทศสมาชิกนั้นๆ ตามข้อ 28(1) และ (6) แต่อย่างไรก็ตามการดำเนินการในระหว่างการถ่ายโอนข้อมูลส่วนบุคคลจากประเทศสมาชิกไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้น ได้ก่อให้เกิดการประมวลผลข้อมูลส่วนบุคคลในตัวมันเองเช่นกัน (ย่อหน้าที่ 44-45)

ตามข้อ 8(3) ของกฎบัตรฯและข้อ 28 ของ Directive 95/46/EC เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่รับผิดชอบในการควบคุมดูแลให้มีการปฏิบัติตามกฎหมายของสหภาพยุโรปว่าด้วยการให้ความคุ้มครองแก่ปัจเจกบุคคลที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่แต่ละคนจะได้รับมอบอำนาจในการตรวจสอบว่าการถ่ายโอนข้อมูลส่วนบุคคลจากประเทศสมาชิกของตนไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้นเป็นไปตามบทบัญญัติใน Directive 95/46/EC หรือไม่ ซึ่งตามข้อ 25(1) Directive 95/46/EC การถ่ายโอนข้อมูลเหล่านั้นจะกระทำได้ในกรณีที่ประเทศนอกกลุ่มสมาชิกสหภาพยุโรปได้รับรองการคุ้มครองในระดับที่เพียงพอเท่านั้น และตามอารัมภบท 57[16] ยังได้กำหนดไว้ด้วยว่าการถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่มิได้รับรองการคุ้มครองในระดับที่เพียงพอจะต้องถูกสั่งห้าม (ย่อหน้าที่ 47-49)

การควบคุมดูแลการถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปให้มีระดับการคุ้มครองตามที่ได้ตกลงไว้ในแต่ละประเทศนั้น ข้อ 25 Directive 95/46/EC ได้กำหนดข้อผูกพันให้แก่ประเทศสมาชิกและคณะกรรมาธิการยุโรปอย่างชัดเจน นอกจากนี้คณะกรรมาธิการยุโรปอาจตัดสินได้ว่าการคุ้มครองข้อมูลในประเทศนอกกลุ่มสมาชิกสหภาพยุโรปอยู่ในระดับที่เพียงพอตามข้อ 25(6) ของ Directive 95/46/EC โดยการออกคำวินิจฉัยซึ่งผลของคำวินิจฉัยที่ออกมานี้จะผูกพันประเทศสมาชิกทุกประเทศและทุกองค์กรของประเทศนั้น[17] (ย่อหน้าที่ 50-51)

ดังนั้นจนกว่าจะถึงเวลาที่คำวินิจฉัยของคณะกรรมาธิการยุโรปได้รับการตัดสินจากศาลให้สิ้นผลไป ประเทศสมาชิกและองค์กรในประเทศรวมไปถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จะไม่สามารถนำมาตรการใดๆที่ขัดกับคำวินิจฉัยนี้มาใช้ได้ มาตรการขององค์กรในสหภาพยุโรปมีความถูกต้องตามกฎหมายและมีผลทางกฎหมายจนกว่าจะถูกเพิกถอน หรือมีการประกาศให้สิ้นผลไปตามกฎ

---

[16] อารัมภบท 57 การถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปซึ่งมิได้รับรองระดับการคุ้มครองที่เพียงพอจะต้องถูกสั่งห้าม

[17] ดูเพิ่มเติมในคำพิพากษาคดี Albako Margarinefabrik, 249/85, EU:C:1987:245, วรรค 17, และ Mediaset, C-69/13, EU:C:2014:71, วรรค 23.

ในการบอกล้าง หรือประกาศไม่ให้มีผลบังคับใช้ตามคำตัดสินด้วยเหตุที่คำวินิจฉัยนั้นไม่ชอบด้วยกฎหมาย[18] (ย่อหน้าที่ 52)

อย่างไรก็ตามคำตัดสินของคณะกรรมาธิการยุโรปซึ่งมีผลบังคับใช้ตามข้อ 25(6) Directive 95/46/EC เช่น คำวินิจฉัยที่ 2000/520 นั้น ไม่สามารถตัดสิทธิบุคคลจากการยื่นคำร้องต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามข้อ 28(4)[19] ได้ นอกจากนี้ที่ปรึกษาทางกฎหมาย (Advocate General) ได้ให้ข้อสังเกตไว้ในหัวข้อที่ 61, 93 และ 116 ของข้อคิดเห็น (Opinion) ว่าคำวินิจฉัยไม่สามารถทำลายหรือลดทอนอำนาจซึ่งได้มอบให้แก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแห่งชาติตามข้อที่ 8(3) ของกฎบัตรฯและข้อ 28 ของ Directive นี้ได้ (ย่อหน้าที่ 53)

หากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลถูกขัดขวางมิให้ตรวจสอบข้อร้องเรียนของบุคคลว่าด้วยการคุ้มครองสิทธิและเสรีภาพเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่ถูกหรืออาจถูกถ่ายโอนจากประเทศสมาชิกไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรป จะเป็นการขัดต่อระบบของ Directive 95/46/EC และวัตถุประสงค์ของข้อ 25 และ 28 (ย่อหน้าที่ 56)

กล่าวคือตามข้อ 28 ของ Directive 95/46/EC มีผลบังคับใช้กับการประมวลผลข้อมูลส่วนบุคคลใดๆก็ตาม ถึงแม้คณะกรรมาธิการแห่งยุโรปจะได้นำคำวินิจฉัยซึ่งมาจากอำนาจตามข้อที่ 25(6) ของ Directive นี้มาใช้ ก็ไม่จำกัดอำนาจเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่เมื่อได้รับข้อร้องเรียนก็สามารถดำเนินการตรวจสอบอย่างอิสระได้ มิฉะนั้นจะถือว่าบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลถูกปฏิเสธสิทธิที่ได้รับรองโดยข้อที่ 8(1) และ (3) ของกฎบัตรฯ ในการยื่นข้อเรียกร้องต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแห่งชาติเพื่อคุ้มครองสิทธิขั้นพื้นฐานของตน (ย่อหน้าที่ 57-58)

ถึงแม้จะมีคำวินิจฉัยของคณะกรรมาธิการยุโรปที่มีผลบังคับใช้ตามข้อ 25(6) ของ Directive นี้ แต่ถ้าหากบุคคลที่ข้อมูลส่วนบุคคลของตนได้ถูกถ่ายโอนไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปได้ร้องเรียนทักท้วงว่ากฎหมายและวิธีปฏิบัติที่ใช้ในประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้นมิได้รับรองระดับการคุ้มครองที่เพียงพอตามข้อ 28(4) ดังเช่นที่มีการพิจารณาในคดีนี้ คำ

---

[18] ดูเพิ่มเติมในคำพิพากษา *Commission* v *Greece*, C-475/01, EU:C:2004:585, วรรค 18 และ case-law ที่ได้ยกมา

[19] ข้อ 28(4) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องรับฟังข้อร้องเรียนของบุคคลเกี่ยวกับการคุ้มครองสิทธิเสรีภาพที่บุคคลนั้นอาจได้รับผลกระทบจากการประมวลผลข้อมูลส่วนบุคคลของตนที่ยื่นโดยบุคคลนั้นเองหรือโดยสมาคมใดๆก็ตามที่เป็นตัวแทนของบุคคลนั้น โดยเฉพาะอย่างยิ่งข้อเรียกร้องจากบุคคลใดก็ตามที่เรียกร้องให้ตรวจสอบความชอบธรรมตามกฎหมายของการประมวลผลข้อมูลหากมีการนำบทบัญญัติแห่งชาติที่ยอมรับตาม Directive เข้ามาบังคับใช้ ทั้งนี้ เจ้าหน้าที่ต้องแจ้งให้บุคคลที่ยื่นคำร้องเรียนทราบด้วยว่าได้กระทำการตรวจสอบเรียบร้อยแล้ว

วินิจฉัยดังกล่าวจะต้องถูกพิจารณาต่อไปว่ามีความเหมาะสมในการใช้เพื่อคุ้มครองความเป็นส่วนตัวและสิทธิและเสรีภาพของปัจเจกบุคคลหรือไม่ (ย่อหน้าที่ 59)

ในการพิจารณานี้ควรมีการนำคำพิพากษาบรรทัดฐาน (case-law) ที่ศาลได้วางไว้มาพิจารณา ตามข้อเท็จจริงที่ว่าสหภาพยุโรปเป็นสหภาพที่มีพื้นฐานมาจากหลักกฎหมายที่ทุกกฎหมายของสถาบันในสหภาพนั้นต้องอยู่ภายใต้อำนาจของหลักกฎหมายนั้น ดังนั้นคำวินิจฉัยของคณะกรรมาธิการยุโรปที่มีผลบังคับใช้ตามข้อ 25(6) ของ Directive 95/46/EC จึงอยู่ในขอบเขตของพิจารณาดังกล่าวเช่นกัน ศาลมีอำนาจตัดสินว่าคำวินิจฉัยของสหภาพยุโรป เช่น คำวินิจฉัยของคณะกรรมาธิการยุโรปที่มีผลบังคับใช้ตามข้อ 25(6) ของ Directive 95/46/EC ไม่ชอบด้วยกฎหมาย โดยอำนาจสิทธิขาดในการตัดสินดังกล่าวนั้นมีจุดประสงค์เพื่อรับรองให้มีความแน่นอนทางกฎหมายว่ากฎหมายสหภาพยุโรปดังกล่าวจะถูกบังคับใช้อย่างเทียมกัน (ย่อหน้าที่ 60-61)

ตามคำตัดสินเหล่านั้นในกรณีที่บุคคลซึ่งข้อมูลส่วนบุคคลของตนได้ถูกหรืออาจถูกถ่ายโอนไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่อยู่ใต้อำนาจบังคับของคำวินิจฉัยของคณะกรรมาธิการยุโรปตามข้อ 25(6) ของ Directive 95/46/EC ได้ยื่นข้อร้องเรียนต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภายในประเทศ โดยทักท้วงความเหมาะสมในการนำคำวินิจฉัยนั้นไปใช้ในการคุ้มครองข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ในการตรวจสอบข้อเรียกร้องดังกล่าวด้วยความระมัดระวัง ในกรณีที่เจ้าหน้าที่คุ้มครองข้อมูลเห็นว่าข้อเรียกร้องดังกล่าวไม่มีมูลความจริงและปฏิเสธรับข้อเรียกร้องนั้นมาพิจารณา บุคคลที่ยื่นข้อเรียกร้องนั้นมีสิทธิตามข้อ 28(3) ของ Directive 95/46/EC ร่วมกับข้อที่ 47 ของกฎบัตรฯ โดยกฎหมายอนุญาตให้บุคคลนั้นทักท้วงคำตัดสินที่ส่งผลกระทบต่อตนในทางลบต่อศาลแห่งชาติ (ย่อหน้าที่ 63-64)

ส่วนกรณีที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลพิจารณาแล้วเห็นว่าข้อเรียกร้องของบุคคลที่ได้ยื่นร้องเรียนมีมูลเหตุตามความจริง เจ้าหน้าที่ดังกล่าวสามารถเข้าร่วมการพิจารณาคดีตามกฎหมายข้อ 28(3) ของ Directive 95/46/EC ร่วมกับข้อที่ 8(3) ของกฎบัตรฯ ได้ (ย่อหน้าที่ 65)

ดังนั้นการพิจารณาข้อสงสัยตามข้อ 25(6) ของ Directive 95/46/EC ร่วมกับข้อที่ 7 8 และ 47 ของกฎบัตรฯจะต้องถูกตีความไปในแนวทางที่ว่าคำวินิจฉัยที่มีผลบังคับใช้ตามบทบัญญัติดังกล่าว เช่น คำวินิจฉัยที่ 2000/520 ซึ่งคณะกรรมาธิการยุโรปใช้ในการตัดสินว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปได้รับรองระดับการคุ้มครองที่เพียงพอนั้นไม่สามารถขัดขวางมิให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกตรวจสอบข้อเรียกร้องของบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคล เมื่อบุคคลนั้นทักท้วงว่ากฎหมายและข้อปฏิบัติที่บังคับใช้ในประเทศนอกกลุ่มสมาชิกสหภาพยุโรปดังกล่าวนั้นไม่สามารถรับรองระดับการคุ้มครองที่เพียงพอได้อีกต่อไป (ย่อหน้าที่ 66)

พิจารณาความชอบด้วยกฎหมายของคำวินิจฉัยที่ 2000/520

นายเชร็มส์ยืนยันว่ากฎหมายและข้อปฏิบัติในประเทศสหรัฐอเมริกาไม่สามารถรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามความหมายของข้อ 25 Directive 95/46/EC ได้ อีกทั้งตามที่ที่ปรึกษาทางกฎหมายได้แสดงความสงสัยในความชอบด้วยกฎหมายของคำวินิจฉัยที่ 2000/520 จึงต้องตรวจสอบว่าคำวินิจฉัยดังกล่าวเป็นไปตามข้อกำหนดของ Directive 95/46/EC ซึ่งพิจารณาร่วมกับกฎบัตรฯหรือไม่ (ย่อหน้าที่ 67)

พิจารณาบทบัญญัติตาม Directive 95/46/EC

ตามข้อ 25(1) ของ Directive 95/46/EC มีข้อกำหนดห้ามไม่ให้ถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่ไม่ได้รับรองระดับการคุ้มครองข้อมูลที่เพียงพอ และเพื่อสอดส่องดูแลการถ่ายโอนเหล่านั้น ข้อ 25(6) ของ Directive 95/46/EC ได้กำหนดให้คณะกรรมาธิการยุโรปมีอำนาจตัดสินว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปรับรองระดับการคุ้มครองที่เพียงพอตามความหมายของวรรคสองของข้อนี้ได้ ด้วยเหตุผลอันเนื่องมาจากกฎหมายภายในประเทศหรือข้อผูกพันระหว่างประเทศที่ประเทศนั้นเข้าไปมีส่วนร่วมเพื่อให้การคุ้มครองแก่ชีวิตส่วนตัวและสิทธิเสรีภาพของปัจเจกบุคคล (ย่อหน้าที่ 68-69)

แต่อย่างไรก็ตาม Directive 95/46/EC ไม่มีการให้คำจำกัดความลักษณะการคุ้มครองที่เพียงพอว่าเป็นอย่างไร ตามข้อ 25(2) กำหนดไว้เพียงว่าระดับที่เพียงพอของการคุ้มครองข้อมูลส่วนบุคคลซึ่งประเทศนอกกลุ่มสมาชิกสหภาพยุโรปเป็นผู้จัดให้มีขึ้นต้องประเมินโดยพิจารณาจากทุกพฤติการณ์ที่แวดล้อมกระบวนการหรือชุดของกระบวนการถ่ายโอนข้อมูล และได้กำหนดรายการของพฤติการณ์ที่ต้องนำมาพิจารณาในการประเมินระดับการคุ้มครองไว้อย่างคร่าวๆเท่านั้น ไม่ได้มีการบัญญัติคำจำกัดความลักษณะของระดับการคุ้มครองที่เพียงพอแต่อย่างใด (ย่อหน้าที่ 70)

ตามข้อ 25(6) ของ Directive 95/46/EC บทบัญญัตินี้กำหนดไว้ชัดเจนว่าให้ประเทศนอกกลุ่มสมาชิกสหภาพยุโรป “รับรอง” (ensures) ระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามเหตุผลอันเนื่องมาจากกฎหมายภายในประเทศหรือข้อผูกพันระหว่างประเทศ นอกจากนี้ตามบทบัญญัติเดียวกันระดับการคุ้มครองที่เพียงพอซึ่งรับรองโดยประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้นจะต้องถูกประเมินเพื่อให้การคุ้มครองแก่ชีวิตส่วนตัวและสิทธิเสรีภาพขั้นพื้นฐานของปัจเจกบุคคล ดังนั้นข้อ 25(6) ของ Directive 95/46/EC จึงทำหน้าที่อนุวัติการให้เป็นไปตามพันธกิจที่ได้กำหนดไว้อย่างชัดแจ้งในข้อที่ 8(1) ของกฎบัตรฯ ในการคุ้มครองข้อมูลส่วนบุคคล และมีจุดมุ่งหมายที่จะรับรองว่าการคุ้มครองข้อมูลส่วนบุคคลในระดับสูงจะดำเนินต่อไปในกรณีที่ข้อมูลได้ถูกถ่ายโอนไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรป (ย่อหน้าที่ 71-72)

ส่วนคำว่า “เพียงพอ” (adequate) ตามข้อ 25(6) ของ Directive 95/46/EC เป็นการยอมรับว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปไม่อาจถูกเรียกร้องให้ต้องรับรองระดับการคุ้มครองในระดับเดียวกันทุกประการกับที่สหภาพยุโรปรับรองไว้ในกฎหมาย อย่างไรก็ตามที่ปรึกษาทางกฎหมายได้แสดงความคิดเห็นไว้ในข้อคิดเห็นที่ 141 ว่าระดับการคุ้มครองที่เพียงพอนั้น แท้ที่จริงแล้วต้องหมายถึงการที่ประเทศนอกกลุ่มสมาชิกสหภาพยุโรปรับรองระดับการคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานเท่ากับระดับการคุ้มครองที่ได้รับรองไว้ภายในสหภาพยุโรปตามอำนาจของ Directive 95/46/EC ซึ่งพิจารณาร่วมกับกฎบัตรฯ โดยเหตุผลอันเนื่องมาจากกฎหมายภายในประเทศและข้อผูกพันระหว่างประเทศ หากไม่มีข้อกำหนดดังกล่าววัตถุประสงค์ซึ่งได้อ้างถึงในวรรคก่อนๆของคำพิพากษาปัจจุบันจะไม่ได้รับการปฏิบัติให้บรรลุผล นอกจากนี้การคุ้มครองระดับสูงซึ่งได้รับการรับรองโดย Directive 95/46/EC ซึ่งพิจารณาร่วมกับกฎบัตรอาจถูกเลี่ยงไม่ปฏิบัติตามโดยง่ายในการถ่ายโอนข้อมูลส่วนบุคคลจากประเทศสมาชิกไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่มีความประสงค์จะใช้ข้อมูลนั้นในการประมวลผล (ย่อหน้าที่ 73)

ตามข้อ 25(6) ของ Directive 95/46/EC ได้กำหนดไว้อย่างชัดเจนว่าคณะกรรมาธิการยุโรปมีสิทธิตัดสินชี้ขาดว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปมีการรับรองระดับการคุ้มครองข้อมูลที่เพียงพอ ถึงแม้วิธีการที่ประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้นๆกระทำเพื่อรับรองระดับการคุ้มครองดังกล่าวจะแตกต่างจากวิธีที่กระทำภายในสหภาพยุโรปในการรับรองให้มีการปฏิบัติตามข้อกำหนดจาก Directive 95/46/EC แต่วิธีการเหล่านั้นก็จะต้องมีประสิทธิภาพในการรับรองระดับการคุ้มครองที่เท่ากับระดับที่ได้รับการรับรองภายในสหภาพยุโรปในทางปฏิบัติ โดยการตรวจสอบระดับการคุ้มครองคณะกรรมาธิการยุโรปจะต้องประเมินเนื้อหาของกฎเกณฑ์ที่มาจากกฎหมายภายในประเทศหรือข้อผูกพันระหว่างประเทศที่ได้บังคับใช้ภายในประเทศนั้นๆและวิธีปฏิบัติซึ่งได้ออกแบบมาเพื่อรับรองให้มีการปฏิบัติตามกฎเกณฑ์เหล่านั้น ตามข้อ 25(2) ของ Directive 95/46/EC ว่ากฎเกณฑ์เหล่านั้นจะต้องรับทุกพฤติการณ์แวดล้อมในการถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้นเข้ามาพิจารณา ถ้าหากข้อเท็จจริงปรากฏว่าระดับการคุ้มครองที่ได้รับการรับรองโดยประเทศนอกกลุ่มสมาชิกสหภาพยุโรปมีแนวโน้มที่จะเปลี่ยนแปลงไปหลังจากที่คณะกรรมาธิการได้นำคำวินิจฉัยตามข้อ 25(6) ของ Directive 95/46/EC มาใช้แล้ว คณะกรรมาธิการยุโรปมีหน้าที่จะต้องตรวจสอบระดับการคุ้มครองอยู่เป็นระยะ ว่าระดับการคุ้มครองนั้นยังถูกต้องตามความเป็นจริงและกฎหมายตามคำตัดสินของศาลอยู่หรือไม่ การตรวจสอบดังกล่าวจะต้องกระทำในเหตุการณ์ใดก็ตามเมื่อมีเหตุที่ทำให้เกิดข้อสงสัยดังกล่าว (ย่อหน้าที่ 74-76)

พิจารณาข้อที่ 1 ของ คำวินิจฉัยที่ 2000/520[20]

คณะกรรมาธิการยุโรปได้วางหลักข้อ 1(1)[21] ของคำวินิจฉัยที่ 2000/520 ว่าโครงการเซฟฮาร์เบอร์ที่ได้กำหนดไว้ในภาคผนวกที่ 1 ซึ่งดำเนินการสอดคล้องตามแนวทางปฏิบัติที่กำหนดโดยข้อสงสัยที่ได้รับการซักถามบ่อยครั้งในภาคผนวกที่ 2 นั้น มีระดับการคุ้มครองที่เพียงพอต่อข้อมูลส่วนบุคคลที่ถูกถ่ายโอนจากประเทศสมาชิกไปยังองค์กรซึ่งก่อตั้งในสหรัฐอเมริกา เป็นที่ชัดเจนจากบทบัญญัติดังกล่าวว่า ทั้งโครงการเซฟฮาร์เบอร์และข้อสงสัยที่ได้รับการซักถามบ่อยครั้งนั้นได้ถูกกำหนดโดยกระทรวงพาณิชย์ของสหรัฐอเมริกา (ย่อหน้าที่ 79)

ตามข้อ 1(2) และ (3) ของคำวินิจฉัยที่ 2000/520 โดยอ่านร่วมกับข้อสงสัยที่ได้รับการซักถามบ่อยครั้งที่ 6[22] ที่ได้กำหนดไว้ในภาคผนวกที่ 2 ทำให้เห็นได้ว่าองค์กรที่ยึดหลักการของโครงการเซฟฮาร์เบอร์อยู่บนพื้นฐานของระบบการรับรองตนเอง (self-certification) (ย่อหน้าที่ 80)

---

[20] โปรดดูคำวินิจฉัยที่ 2000/520 ฉบับเต็ม ที่ภาคผนวก ข

[21] ข้อ 1(1) ตามวัตถุประสงค์ของข้อ 25(2) Directive 95/46/EC สำหรับทุกกิจกรรมที่อยู่ในขอบข่ายของ Directive หลักคุ้มครองความเป็นส่วนตัวของโครงการเซฟฮาร์เบอร์ (ตามคำพิพากษาแทนด้วยคำว่า Principles) ดังที่บรรยายไว้ในภาคผนวกที่ 1 ของคำวินิจฉัยซึ่งได้รับการดำเนินงานตามแนวทางปฏิบัติที่กำหนดโดยข้อสงสัยที่ได้รับการซักถามบ่อยครั้ง (FAQs) ที่ออกโดยกระทรวงพาณิชย์สหรัฐในวันที่ 21 กรกฎาคม ค.ศ. 2000 ดังที่บรรยายไว้ในภาคผนวกที่ 2 ของคำวินิจฉัยนี้ได้รับการพิจารณาว่าสามารถรับรองระดับการคุ้มครองที่เพียงพอสำหรับข้อมูลส่วนบุคคลที่ถูกถ่ายโอนจากประเทศสมาชิกสหภาพยุโรปไปยังองค์กรที่จัดตั้งขึ้นในสหรัฐอเมริกา โดยมีความเกี่ยวข้องกับเอกสารที่ออกโดยกระทรวงพาณิชย์สหรัฐดังนี้ :

(a) ข้ออธิบายโดยสรุปเกี่ยวกับการบังคับใช้หลักการของโครงการเซฟฮาร์เบอร์ที่บรรยายไว้ในภาคผนวกที่ 3

(b) บันทึกข้อความว่าด้วยค่าเสียหายอันเนื่องมาจากการละเมิดความเป็นส่วนตัวและการอนุญาตอย่างชัดแจ้งในกฎหมายสหรัฐที่บรรยายไว้ในภาคผนวกที่ 4

(c) หนังสือจากคณะกรรมาธิการการค้าของสหรัฐอเมริกาที่บรรยายไว้ในภาคผนวกที่ 5

(d) หนังสือจากกระทรวงคมนาคมสหรัฐที่บรรยายไว้ในภาคผนวกที่ 6

[22] ข้อสงสัยที่ได้รับการซักถามบ่อยครั้งที่ 6 คือการอธิบายวิธีการในการรับรองตนเองขององค์กรที่ประสงค์จะเข้าร่วมโครงการเซฟฮาร์เบอร์ ทั้งนี้สามารถดูรายละเอียดเพิ่มเติมได้ในบทที่ 3 ส่วนที่ 3.2.2

ถึงแม้ว่าระบบการรับรองตนเองของประเทศนอกกลุ่มสมาชิกสหภาพยุโรปมิได้ขัดกับข้อกำหนดในข้อ 25(6) ของ Directive 95/46/EC ซึ่งกำหนดให้ประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่อยู่ภายใต้อำนาจบังคับรับรองระดับการคุ้มครองที่เพียงพอตามเหตุอันเนื่องมาจากกฎหมายภายในประเทศหรือข้อผูกพันระหว่างประเทศ ความน่าเชื่อถือของระบบการรับรองตนเองต้องมีกลไกในการตรวจสอบและควบคุมดูแลซึ่งสามารถชี้ระบุและลงโทษการฝ่าฝืนกฎเกณฑ์ในการรับรองคุ้มครองสิทธิขึ้นพื้นฐานโดยเฉพาะสิทธิในชีวิตส่วนบุคคลและสิทธิในการคุ้มครองข้อมูลส่วนบุคคลได้ (ย่อหน้าที่ 81)

ในกรณีปัจจุบันตามภาคผนวกที่ 1 วรรคสอง[23] ของคำวินิจฉัยที่ 2000/520 หลักการของโครงการเซฟฮาร์เบอร์มีจุดประสงค์เพื่อใช้โดยองค์กรของสหรัฐอเมริกาในการรับโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปเพื่อวัตถุประสงค์ในการปรับองค์กรให้มีคุณสมบัติตามโครงการเซฟฮาร์เบอร์และปรับระดับการคุ้มครองให้มีระดับ “เพียงพอ” ดังที่ได้คาดการณ์ไว้เท่านั้น ดังนั้นหลักการเหล่านี้จะมีผลบังคับใช้ในการรับรองตนเองขององค์กรในสหรัฐอเมริกาในการรับข้อมูลส่วนบุคคลจากสหภาพยุโรปเท่านั้น ส่งผลให้หน่วยงานรัฐบาลของสหรัฐอเมริกามิได้ถูกกำหนดให้ต้องปฏิบัติตามหลักการเหล่านั้นด้วย (ย่อหน้าที่ 82)

ยิ่งไปกว่านั้นข้อ 2 ของคำวินิจฉัยที่ 2000/520 ยังระบุไว้เพียงว่าหลักการเหล่านี้มีความเกี่ยวข้องกับระดับความเพียงพอของการคุ้มครองข้อมูลส่วนบุคคลที่จัดให้มีในประเทศสหรัฐอเมริกาภายใต้หลักการของโครงการเซฟฮาร์เบอร์ซึ่งได้รับการดำเนินงานตามข้อสงสัยที่ได้รับการซักถามบ่อยครั้งซึ่งเป็นไปตามข้อกำหนดของข้อ 25(1) Directive 95/46/EC เท่านั้น โดยมิได้ระบุวิธีการตรวจสอบที่จำเป็นในการตรวจสอบมาตรการที่ประเทศสหรัฐอเมริกาใช้รับรองระดับการคุ้มครองที่เพียงพอโดยเหตุอันเนื่องมาจากกฎหมายภายในประเทศและข้อผูกพันระหว่างประเทศตามความหมายของข้อ 25(6) Directive นี้ด้วย (ย่อหน้าที่ 83)

ภายใต้ภาคผนวกที่ 1 วรรคสี่ของคำวินิจฉัยที่ 2000/520 การบังคับใช้ของหลักการเซฟฮาร์เบอร์อาจถูกจำกัดโดยวัตถุประสงที่จำเป็นต่อความมั่นคงแห่งชาติ ประโยชน์สาธารณะ หรือข้อกำหนดในการบังคับใช้กฎหมาย และ โดยรัฐบัญญัติ ระเบียบของราชการ หรือ กฎหมายเฉพาะกาลที่ได้สร้างข้อกำหนดที่ขัดแย้งกับหลักการเซฟฮาร์เบอร์ หรือการอนุญาตอย่างชัดแจ้งโดยจะกระทำ

---

[23] ภาคผนวกที่ 1 วรรคสอง การตัดสินใจขององค์กรต่างๆที่จะปรับองค์กรให้มีคุณสมบัติเหมาะสมสำหรับโครงการเซฟฮาร์เบอร์นั้นเป็นไปโดยความสมัครใจทั้งหมด และองค์กรเหล่านั้นก็มีสิทธิ์ที่จะปรับองค์กรมีคุณสมบัติเหมาะสมสำหรับโครงการเซฟฮาร์เบอร์ด้วยวิธีที่แตกต่างกันไป...

ได้ในกรณีที่องค์กรนั้นสามารถแสดงให้เห็นว่าการไม่ปฏิบัติตามหลักของโครงการเซฟฮาร์เบอร์อยู่ในขอบเขตอันชอบธรรมตามกฎหมายอันเป็นฐานที่มาแห่งอำนาจนั้นได้ (ย่อหน้าที่ 84)

ในความเกี่ยวเนื่องนี้คำวินิจฉัยที่ 2000/520 แถลงไว้ในส่วน B ของภาคผนวกที่ 4 เกี่ยวกับข้อจำกัดในการใช้หลักการของโครงการเซฟฮาร์เบอร์ไว้ว่าองค์กรของสหรัฐอเมริกาทั้งที่ได้และมิได้เข้าร่วมโครงการเซฟฮาร์เบอร์จะต้องปฏิบัติตามกฎหมาย โดยเฉพาะในกรณีที่กฎหมายในประเทศสหรัฐอเมริกาได้ประกาศข้อกำหนดที่ขัดกับหลักการโครงการเซฟฮาร์เบอร์ (ย่อหน้าที่ 85)

ดังนั้นคำวินิจฉัยที่ 2000/520 ได้แสดงให้เห็นแล้วว่าความมั่นคงแห่งชาติ ประโยชน์สาธารณะและข้อกำหนดในการบังคับใช้กฎหมายมีความสำคัญมากกว่าหลักการของโครงการเซฟฮาร์เบอร์ เนื่องจากให้องค์กรของสหรัฐอเมริกาที่ได้รับรองตนเองในการรับโอนข้อมูลส่วนบุคคลมาจากสหภาพยุโรปมีสิทธิเพิกเฉยต่อหลักการโครงการเซฟฮาร์เบอร์อย่างไม่มีข้อจำกัด ในกรณีที่หลักการคุ้มครองข้อมูลส่วนบุคคลตามโครงการเซฟฮาร์เบอร์ขัดกับข้อกำหนดในการบังคับใช้กฎหมายภายในและหากเกิดกรณีนี้ไม่สามารถนำหลักการคุ้มครองข้อมูลส่วนบุคคลตามโครงการเซฟฮาร์เบอร์มาใช้ได้ (ย่อหน้าที่ 86)

ตามลักษณะโดยทั่วไปของการหลีกเลี่ยงไม่ทำตามกฎดังที่ได้บรรยายไว้ในภาคผนวกที่ 1 วรรคสี่ ของคำวินิจฉัยที่ 2000/520 คำวินิจฉัยนั้นได้อนุญาตให้มีการแทรกแซงด้วยเหตุอันเนื่องมาจากความมั่นคงแห่งชาติ และข้อกำหนดในการรักษาประโยชน์สาธารณะ หรือข้อกฎหมายภายในประเทศสหรัฐอเมริกา ในการใช้สิทธิขั้นพื้นฐานของบุคคลที่ข้อมูลส่วนบุคคลได้ถูกถ่ายโอนจากสภาพยุโรปไปยังประเทศสหรัฐอเมริกาได้ โดยการแทรกแซงสิทธิขั้นพื้นฐานในการได้รับความเคารพชีวิตส่วนตัวนี้สามารถกระทำได้โดยไม่สำคัญว่าเนื้อหาของข้อมูลเกี่ยวกับชีวิตส่วนตัวที่อยู่ในประเด็นถกเถียงจะมีความอ่อนไหวหรือจะทำให้บุคคลที่เกี่ยวข้องประสบความเสียหายจากผลที่ตามมาหรือไม่[24] (ย่อหน้าที่ 87)

นอกจากนั้นคำวินิจฉัยที่ 2000/520 ยังมิได้ระบุวิธีการตรวจสอบใดๆที่เกี่ยวกับกฎเกณฑ์ที่สหรัฐอเมริกานำมาใช้ในการแทรกแซงสิทธิขั้นพื้นฐานของบุคคลผู้ซึ่งข้อมูลส่วนตัวได้ถูกถ่ายโอนจากสหภาพยุโรปไปยังประเทศสหรัฐอเมริกา ในกรณีที่เป็นการแทรกแซงโดยหน่วยงานของรัฐที่กระทำการตามวัตถุประสงค์ทางกฎหมาย เช่นวัตถุประสงค์ในการรักษาความมั่นคงแห่งชาติ (ย่อหน้าที่ 88)

---

[24] ดูเพิ่มเติมในคำพิพากษา Digital Rights Ireland and Others, C-293/12 และ C-594/12, EU:C:2014:238, วรรค 33 และ case-law ที่ได้ยกมา

อีกทั้งคำวินิจฉัยที่ 2000/520 มิได้ระบุถึงวิธีการป้องกันที่มีประสิทธิภาพตามกฎหมายในการป้องกันการแทรกแซง มีเพียงอำนาจตามข้อสงสัยที่ได้รับการซักถามบ่อยครั้งที่ 11[25] ในภาคผนวกที่ 2 ซึ่งถูกจำกัดให้ใช้ในเฉพาะข้อพิพาททางการค้า ไม่สามารถบังคับใช้ในข้อพิพาทที่เกี่ยวกับความชอบด้วยกฎหมายอันเกิดจากการแทรกแซงสิทธิขั้นพื้นฐานได้ ก่อนหน้านี้คำวินิจฉัยที่ 2000/520 ยังถูกวิเคราะห์จากการประเมินสถานการณ์ที่เป็นผลมาจากการปฏิบัติตามคำวินิจฉัยของคณะกรรมาธิการยุโรปเองด้วย โดยเฉพาะในหัวข้อที่ 2 และ 3.2 ของ Communication COM (2013) 846 Final และในหัวข้อที่ 7.1 7.2 และ 8 ของ Communication COM (2013) 847 Final[26] ซึ่งคณะกรรมาธิการยุโรปได้ตัดสินว่าหน่วยงานของสหรัฐอเมริกาสามารถเข้าถึงข้อมูลส่วนบุคคลที่ถูกถ่ายโอนจากประเทศสมาชิกไปยังสหรัฐอเมริกาและได้ประมวลผลข้อมูลเหล่านั้นมากเกินความจำเป็นด้วยเหตุในการคุ้มครองความมั่นคงแห่งชาติ จึงเป็นการเข้าถึงข้อมูลส่วนบุคคลในวิถีทางที่ขัดแย้งกับจุดประสงค์ในการโอนข้อมูลในตอนต้น อีกทั้งคณะกรรมาธิการยังได้ระบุอีกด้วยว่าเจ้าของข้อมูลไม่มีวิธีด้านการจัดการหรือด้านกฎหมายใดๆที่ห้ามมิให้มีการประมวลผลข้อมูลที่เกี่ยวข้องกับตน หรือสามารถปรับปรุงแก้ไขและลบข้อมูลได้เลย (ย่อหน้าที่ 89-90)

ตามระดับการคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานที่ได้รับการรับรองในสหภาพยุโรปตัวบทกฎหมายสหภาพยุโรปที่เกี่ยวข้องกับการแทรกแซงสิทธิขั้นพื้นฐานที่ได้รับการรับรองโดยข้อที่ 7 และ 8 ของกฎบัตรฯ จะต้องระบุกฎเกณฑ์ที่ชัดเจน (clear) และแน่นอน (precise) ในการกำหนดขอบเขตบังคับใช้มาตรการอันเป็นการแทรกแซงสิทธิและต้องกำหนดให้มีการป้องกันขั้นต่ำตามกฎหมายจากการตัดสินของศาล เพื่อให้บุคคลที่ข้อมูลส่วนบุคคลของตนเข้ามาเกี่ยวข้องกับคดีได้รับการรับรองที่เพียงพอว่าจะมีการคุ้มครองข้อมูลของตนอย่างมีประสิทธิภาพจากความเสี่ยงที่จะถูกนำข้อมูลไปใช้ในทางที่ผิดและการเข้าถึงหรือการนำข้อมูลไปใช้ในทางใดๆที่ขัดกับกฎหมาย การคุ้มครองดังกล่าวนั้นมีความสำคัญมากโดยเฉพาะในกรณีที่ข้อมูลส่วนบุคคลนั้นได้รับการประมวลผลแบบอัตโนมัติที่มีความเสี่ยงอย่างมีนัยสำคัญที่จะถูกเข้าถึงข้อมูลนั้นอย่างผิดกฎหมาย (ย่อหน้าที่ 91)

---

[25] ดูรายละเอียดเพิ่มเติมได้ใน บทที่ 3 ส่วนที่ 3.2.4

[26] Communication คือเอกสารที่คณะกรรมาธิการยุโรปทำขึ้นเพื่อรายงานต่อรัฐสภายุโรป โดยแจ้งและให้ข้อมูลที่เกี่ยวข้องกับนโยบายภายในสหภาพยุโรปผ่านการเก็บรวบรวมข้อมูลทั้งจากนักวิชาการ สื่อ เครือข่ายข้อมูลภายในประเทศสมาชิก อีกทั้งยังเป็นการรายงานแนวโน้มความคิดเห็นของสาธารณชนและทัศนะของพลเมืองยุโรปต่อนโยบายทางการเมืองอีกด้วย

Communication ทั้งสองฉบับนี้จะมีการกล่าวรายละเอียดในเรื่องการวิเคราะห์เหตุผลและหลักเกณฑ์ที่ศาลยุติธรรมแห่งสหภาพยุโรปใช้ในการพิพากษาคดีเลขที่ C-362/14 ซึ่งเป็นส่วนถัดไป

เหนือสิ่งอื่นใดการคุ้มครองสิทธิขั้นพื้นฐานในการได้รับการเคารพชีวิตส่วนตัวในระดับของสหภาพยุโรปนั้นกำหนดให้การหลีกเลี่ยงไม่ทำตามกฎและข้อจำกัดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลให้กระทำได้เท่าที่จำเป็นเท่านั้น (strictly necessary) โดยกฎหมายต้องมีวัตถุประสงค์เพื่อกำหนดขีดจำกัดในการเข้าถึงข้อมูลและวิธีการนำข้อมูลไปใช้ซึ่งได้จำกัดไว้อย่างเข้มงวดและสามารถรับรองความถูกต้องให้กับการแทรกแซงอันเป็นผลมาจากการเข้าถึงและนำข้อมูลนั้นไปใช้ให้แก่เจ้าหน้าที่รัฐ โดยเฉพาะกฎหมายที่อนุญาตให้เจ้าหน้าที่รัฐเข้าถึงเนื้อหาของการสื่อสารทางอิเล็กทรอนิกส์เป็นการทั่วไปได้นั้นจะต้องไม่กระทบต่อสาระสำคัญของสิทธิขั้นพื้นฐานในการได้รับความเคารพต่อชีวิตส่วนตัว ดังที่ได้รับการรับรองจากข้อที่ 7 ของกฎบัตรฯ (ย่อหน้าที่ 92-94)

นอกจากนั้นกฎหมายที่ไม่ได้ให้สิทธิแก่ปัจเจกบุคคลในการได้รับการเยียวยาแก้ไขทางกฎหมายในการเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน หรือไม่สามารถแก้ไขหรือลบข้อมูลของตนได้นั้น ถือว่าไม่ได้เคารพสาระสำคัญของสิทธิขั้นพื้นฐานในการได้รับความคุ้มครองทางกฎหมายที่มีประสิทธิภาพ ดังที่ได้รับรองไว้เป็นพิเศษในข้อที่ 47 ของกฎบัตรฯ ซึ่งกำหนดไว้ว่าบุคคลที่ถูกละเมิดสิทธิและเสรีภาพที่ได้รับรองไว้โดยกฎหมายของสหภาพยุโรปมีสิทธิในการได้รับการเยียวยาแก้ไขจากศาลที่ปฏิบัติตามเงื่อนไขในข้อนั้นได้ การพิจารณาทบทวนทางกฎหมายที่มีประสิทธิภาพที่กำหนดขึ้นเพื่อรับรองให้มีการปฏิบัติตามกฎหมายของสหภาพยุโรปนั้น เป็นสิ่งที่มีอยู่ตามธรรมชาติในหลักของกฎหมาย (Rule of Law) (ย่อหน้าที่ 95)

ดังนั้นคณะกรรมาธิการยุโรปจะบังคับใช้คำวินิจฉัยโดยอาศัยข้อ 25(6) ของ Directive 95/46/EC คณะกรรมาธิการต้องตัดสินได้ว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปที่เกี่ยวข้องได้รับรองระดับการคุ้มครองสิทธิขั้นพื้นฐานในระดับที่เท่าเทียมกันกับกฎหมายของสหภาพยุโรปในทางปฏิบัติ ซึ่งเป็นระดับที่ได้อธิบายถึงอย่างชัดเจนตามการพิจารณาที่กล่าวมา[27] แต่อย่างไรก็ตามคณะกรรมาธิการยุโรปไม่ได้แถลงไว้ในคำวินิจฉัยที่ 2000/520 ว่า ประเทศสหรัฐอเมริกาได้รับรองระดับการคุ้มครองที่เพียงพอตามเหตุอันเนื่องมาจากกฎหมายภายในประเทศหรือข้อผูกพันระหว่างประเทศ ดังนั้นจึงไม่มีความจำเป็นในการตรวจสอบเนื้อความของหลักการของโครงการเซฟฮาร์เบอร์ ศาลมีอำนาจตัดสินว่าข้อ 1 ของคำวินิจฉัยที่ 2000/520 ล้มเหลวในการปฏิบัติตามข้อกำหนดของข้อ 25(6) Directive 95/46/EC พิจารณาร่วมกับกฎบัตรฯ ทำให้ข้อ 1 ของคำวินิจฉัยที่ 2000/520 สิ้นผลไป (ย่อหน้าที่ 96-98)

---

[27] จากคำพิพากษาย่อหน้าที่ 71, 73 และ 74

ข้อที่ 3 ของ คำวินิจฉัยที่ 2000/520

ภายใต้ข้อ 28 ของ Directive 95/46/EC พิจารณาร่วมกับข้อที่ 8 ของกฎบัตรฯ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแห่งชาติต้องสามารถตรวจสอบข้อเรียกร้องใดๆก็ตามที่เกี่ยวข้องกับการคุ้มครองสิทธิและเสรีภาพให้แก่บุคคลในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบุคคลนั้นโดยอิสระสมบูรณ์ได้ กรณีนี้เป็นกรณีเฉพาะที่การยื่นข้อเรียกร้องดังกล่าวนั้น บุคคลได้ตั้งข้อสงสัยเกี่ยวกับความเหมาะสมในการคุ้มครองความเป็นส่วนตัวอันมาจากคำวินิจฉัยที่มีผลบังคับใช้ตามข้อ 25(6) ของ Directive นี้ (ย่อหน้าที่ 99)

ตามข้อ 3(1) ของคำวินิจฉัยที่ 2000/520 กำหนดกฎเกณฑ์เฉพาะเกี่ยวกับอำนาจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามการวินิจฉัยของคณะกรรมาธิการยุโรปเกี่ยวกับระดับการคุ้มครองที่เพียงพอตามความหมายของข้อ 25 ของ Directive 95/46/EC เอาไว้ ภายใต้บทบัญญัตินั้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจสั่งระงับการถ่ายโอนข้อมูลไปยังองค์กรที่ได้รับรองตนเองที่จะปฏิบัติตามหลักของคำวินิจฉัยที่ 2000/520 โดยปราศจากผลกระทบต่อหน้าที่ในการรับรองให้มีการปฏิบัติตามบทบัญญัติแห่งชาติที่มีผลบังคับใช้ตามบทบัญญัติอื่นที่มิใช่ข้อ 25 ของ Directive 95/46/EC ได้ แต่ถึงแม้บทบัญญัตินี้จะไม่มีผลกระทบต่ออำนาจหน้าที่ของเจ้าหน้าที่ดังกล่าวในการรับรองให้มีการปฏิบัติตามบทบัญญัติที่มีผลบังคับใช้ตาม Directive 95/46/EC อย่างไรก็ตาม บทบัญญัตินี้ก็ไม่ได้กำหนดความเป็นไปได้ที่เจ้าหน้าที่เหล่านั้นจะทำการรับรองให้มีการปฏิบัติตามข้อที่ 25 ของ Directive นั้นอย่างจริงจัง (ย่อหน้าที่ 100-101)

ดังนั้นตามข้อ 3(1) ของคำวินิจฉัยที่ 2000/520 จึงเป็นการปฏิเสธอำนาจของเจ้าหน้าที่คุ้มครองข้อมูลตามข้อ 28 ของ Directive 95/46/EC ที่ใช้ในกรณีมีบุคคลยื่นร้องเรียนโดยการตั้งข้อสงสัยว่าคำตัดสินของคณะกรรมาธิการยุโรปตามข้อ 25(6) ที่ได้ตัดสินว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปได้รับรองระดับการคุ้มครองที่เพียงพอนั้นมีความเพียงพอจะใช้ในการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคลหรือไม่ (ย่อหน้าที่ 102)

การปฏิบัติตามอำนาจที่คณะกรรมาธิการยุโรปได้รับจากสภานิติบัญญัติแห่งสหภาพยุโรปตามข้อ 25(6) ของ Directive 95/46/EC ไม่ได้รวมความสามารถในการจำกัดอำนาจของเจ้าหน้าที่คุ้มครองข้อมูลแต่อย่างใด ดังนั้นต้องถือว่าในการบังคับใช้ข้อ 3 ของคำวินิจฉัยที่ 2000/520 คณะกรรมาธิการยุโรปได้กระทำเกินกว่าอำนาจที่ได้รับตามข้อ 25(6) ของ Directive 95/46/EC พิจารณาร่วมกับกฎบัตรฯ ดังนั้นข้อ 3 ของคำวินิจฉัยนี้จึงสิ้นผลไป (ย่อหน้าที่ 103-104)

เนื่องจากข้อ 1 และ 3 ของคำวินิจฉัยที่ 2000/520 แบ่งแยกออกไม่ได้กับข้อ 2, 4 และภาคผนวกของคำวินิจฉัยนั้น ดังนั้นความสิ้นผลของข้อเหล่านี้จึงส่งผลกระทบต่อความสมบูรณ์ของคำวินิจฉัยทั้งหมด ตามการพิจารณาที่ได้กล่าวมาศาลจึงตัดสินว่าคำวินิจฉัยที่ 2000/520 สิ้นผลไป (ย่อหน้าที่ 105-106)

ตามมูลเหตุดังกล่าวศาลสูงสุดจึงตัดสินว่า :

(1) ข้อที่ 25(6) ของ Directive 95/46/EC พิจารณาร่วมกับกฎบัตรสิทธิขั้นพื้นฐานของสหภาพยุโรปจะต้องได้รับการตีความหมายไปในแนวทางที่ว่าคำวินิจฉัยซึ่งมีผลบังคับใช้ตามบทบัญญัตินั้น เช่น คำตัดสินของคณะกรรมาธิการยุโรปตามคำวินิจฉัยที่ 2000/520/EC ว่าด้วยระดับการคุ้มครองที่เหมาะสมตามหลักการของโครงการเซฟฮาร์เบอร์ที่คณะกรรมาธิการยุโรปใช้ในการตัดสินว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรประดับการคุ้มครองเพียงพอนั้น มิได้เป็นการจำกัดอำนาจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกในการตรวจสอบข้อร้องเรียนของบุคคลตามอำนาจแห่งข้อ 28 ของ Directive นี้ ในกรณีที่บุคคลดังกล่าวทักท้วงว่ากฎหมายและวิธีปฏิบัติที่บังคับใช้ในประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้นไม่สามารถคุ้มครองข้อมูลส่วนบุคคลของตนที่ถูกถ่ายโอนไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปในระดับที่เพียงพอได้

(2) คำวินิจฉัยที่ 2000/520 สิ้นผลไป

4.3 วิเคราะห์เหตุผลและหลักเกณฑ์ที่ศาลยุติธรรมแห่งสหภาพยุโรปใช้ในการพิพากษาคดีเลขที่ C-362/14

ตามที่ศาลยุติธรรมแห่งสหภาพยุโรปได้มีคำตัดสินในคดีที่ C-362/14 ให้คำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2000/520 อันเป็นบทกฎหมายที่รองรับการโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปไปยังประเทศสหรัฐอเมริกาตามโครงการเซฟฮาร์เบอร์สิ้นผลไป จึงต้องพิจารณาหลักเกณฑ์ที่ศาลใช้ตัดสินชี้ขาดว่าคำวินิจฉัยที่ 2000/520 ขัดแย้งกับหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลไปยังต่างประเทศอย่างไร

จากการฟ้องคดีในชั้นศาลของนายเชร็มส์ โจทก์ ต่อคณะกรรมาธิการคุ้มครองข้อมูลไอร์แลนด์ จำเลย เหตุเพราะคณะกรรมาธิการคุ้มครองข้อมูลไอร์แลนด์ไม่รับข้อร้องเรียนของนายเชร็มส์ที่ว่าประเทศสหรัฐอเมริกาไม่ได้ให้การคุ้มครองข้อมูลส่วนบุคคลของตนที่ได้รับโอนไปอย่างเพียงพอ โดยคณะกรรมาธิการคุ้มครองข้อมูลไอร์แลนด์ได้อ้างคำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2000/520 ซึ่งออกตามอำนาจของข้อ 25(6) Directive 95/46/EC มาเป็นเหตุในการปฏิเสธข้อร้องเรียนของนายเชร็มส์ว่าไม่มีมูล เพราะคณะกรรมาธิการยุโรปได้ออกคำวินิจฉัยนี้เอาไว้โดยตัดสินไว้แล้วว่าประเทศสหรัฐอเมริกาได้รับรองระดับการคุ้มครองที่เพียงพอ อันเป็นที่มาของคำพิพากษาดังกล่าวที่ได้ตัดสินชี้ขาดถึงความชอบธรรมของคำวินิจฉัยนั่นเอง

พิจารณาระดับความคุ้มครองในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ตามข้อ 25(1) ของ Directive 95/46/EC ได้วางหลักเกณฑ์ทั่วไปว่าด้วยการโอนข้อมูลส่วนบุคคลไปยังประเทศที่มิใช่สมาชิกของสหภาพยุโรปประเทศว่าการจะโอนข้อมูลจากสมาชิกสหภาพยุโรปไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปได้โดยไร้ข้อจำกัดเมื่อประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้นรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ปัญหาจากการพิจารณาคือไม่มีการบัญญัติคำจำกัดความกำหนดรายละเอียดของลักษณะการคุ้มครองที่ “เพียงพอ” เอาไว้ ไม่ว่าจะในข้อใดของ Directive นี้ มีเพียงข้อ 25(2) ที่ได้กำหนดให้พิจารณาโดยประเมินจากทุกพฤติการณ์ที่แวดล้อมกระบวนการหรือชุดของกระบวนการถ่ายโอนข้อมูลและได้กำหนดรายการของพฤติการณ์ที่ต้องนำมาพิจารณาในการประเมินระดับการคุ้มครองไว้อย่างคร่าวๆเท่านั้น ในคดีนี้ศาลจึงได้วางหลักในเรื่องระดับการคุ้มครองที่เพียงพอเอาไว้ดังนี้

ตามเนื้อหาในข้อ 25(6) ของ Directive 95/46/EC กำหนดชัดเจนว่าให้ประเทศนอกกลุ่มสมาชิกสหภาพยุโรปรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามเหตุอันเนื่องมาจากกฎหมายภายในประเทศหรือข้อผูกพันระหว่างประเทศ โดยระดับที่เพียงพอของการคุ้มครองจะต้องถูกประเมินเพื่อให้การคุ้มครองแก่ชีวิตส่วนตัวและสิทธิเสรีภาพขั้นพื้นฐานของปัจเจกบุคคล จากข้อดังกล่าวเป็นการปฏิบัติตามพันธะหน้าที่ที่ได้กำหนดไว้ในข้อที่ 8 ของกฎบัตรสิทธิขั้นพื้นฐานแห่งสหภาพยุโรปในเรื่องการคุ้มครองข้อมูลส่วนบุคคล จึงทำให้พิเคราะห์ได้ว่าการโอนข้อมูลส่วนบุคคลต่อไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปควรมีผลการคุ้มครองในระดับสูงต่อไปเช่นกันเพื่อให้ความต่อเนื่องของการคุ้มครองสิทธิขั้นพื้นฐานของบุคคลไม่สะดุดลง

ที่ปรึกษาทางกฎหมายได้แสดงข้อคิดเห็นไว้ว่าระดับการคุ้มครองที่เพียงพอนั้น แท้ที่จริงแล้วจะต้องหมายถึงการที่ประเทศนอกกลุ่มสมาชิกสหภาพยุโรปรับรองระดับการคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานเท่ากับ (equivalent) ระดับการคุ้มครองที่ได้รับรองไว้ภายในสหภาพยุโรปตามอำนาจของ Directive 95/46/EC พิจารณาร่วมกับกฎบัตรฯ หากไม่มีข้อกำหนดดังกล่าววัตถุประสงค์ของการคุ้มครองสิทธิเสรีภาพของบุคคลจะไม่ได้รับการปฏิบัติให้บรรลุผล นอกจากนี้ยังอาจถูกเลี่ยงไม่ปฏิบัติตามได้โดยง่ายเพียงแค่ถ่ายโอนข้อมูลไปประเทศนอกกลุ่มสมาชิกสหภาพยุโรปเพื่อประมวลผล

จากเหตุผลดังที่ได้กล่าวมานั้น แม้ว่าวิธีการที่ประเทศนอกกลุ่มสมาชิกสหภาพยุโรปได้กระทำเพื่อรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลอาจแตกต่างจากวิธีที่กระทำภายในสหภาพยุโรปซึ่งต้องผูกพันตาม Directive 95/46/EC แต่อย่างไรก็ตามศาลได้วางหลักว่าวิธีการที่ประเทศนอกกลุ่มสมาชิกสหภาพยุโรปรับรองนั้นต้องมีประสิทธิภาพของระดับการคุ้มครองที่ “เท่ากับ” ระดับที่ได้รับการรับรองภายในสหภาพยุโรปในทางปฏิบัติ จึงจะถือว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปรับรองระดับการคุ้มครองที่ “เพียงพอ”

พิจารณาเหตุที่ศาลตัดสินให้คำวินิจฉัยที่ 2000/520 สิ้นผลไป

ในอันดับแรกนั้นควรเข้าใจเกี่ยวกับวัตถุประสงค์อันเป็นที่มาของการจัดตั้งโครงการเซฟฮาร์เบอร์ดังที่ได้กล่าวมาในบทก่อว่าเกิดจากการตกลงกันของกระทรวงพาณิชย์สหรัฐอเมริกากับคณะกรรมาธิการยุโรปเพื่อทำให้การโอนข้อมูลส่วนบุคคลไปยังประเทศสหรัฐอเมริกาสามารถกระทำได้ไม่ขัดกับ Directive 95/46/EC โดยคณะกรรมาธิการยุโรปมีอำนาจในการออกคำวินิจฉัยเพื่อระบุว่าประเทศนอกกลุ่มสมาชิกสหภาพยุโรปมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามข้อ 25(6) ของ Directive 95/46/EC

สำหรับเนื้อหาของคำวินิจฉัยที่ 2000/520 ตามข้อ 1(1) ได้อธิบายว่ากิจกรรมที่ได้ดำเนินการภายใต้โครงการเซฟฮาร์เบอร์ตามรายละเอียดที่แนบไว้ในภาคผนวกที่ 1 ได้รับการพิจารณาว่าสามารถรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอสำหรับการถ่ายโอนข้อมูลจากประเทศในสหภาพยุโรปไปยังองค์กรที่จัดตั้งขึ้นในสหรัฐอเมริกาและมีการดำเนินงานตามแนวทางปฏิบัติที่กำหนดโดยข้อสงสัยที่ได้รับการซักถามบ่อยครั้ง ซึ่งองค์กรที่ยึดหลักการของโครงการเซฟฮาร์เบอร์ในการรับรองตนเองว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอจะต้องปฏิบัติตามข้อกำหนดตามคำวินิจฉัยข้อที่ 1(2) และ (3) อนึ่งคำวินิจฉัยนี้มีจุดมุ่งหมายเพียงเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในสหรัฐอเมริกาให้มีคุณสมบัติตามที่กำหนดในข้อที่ 25(1) ของDirective 95/46/EC เท่านั้น มิได้กระทบต่อการปรับใช้บทบัญญัติอื่นๆของ Directive ที่เกี่ยวข้องกับการประมวลผลข้อมูลภายในประเทศสมาชิกเอง

อย่างไรก็ตามเมื่อวิเคราะห์ในรายละเอียดของโครงการเซฟฮาร์เบอร์แล้วพบว่ามีองค์ประกอบและข้อยกเว้นบางประการที่ทำให้คำวินิจฉัยนี้สิ้นผลไปตามคำตัดสินของศาลยุติธรรมแห่งสหภาพยุโรป ดังจะอธิบายต่อไปนี้

(1) โครงการเซฟฮาร์เบอร์มีการกำหนดข้อยกเว้นให้องค์กรที่เข้าร่วมไม่ต้องปฏิบัติตามหลักการของโครงการเซฟฮาร์เบอร์ได้

ตามภาคผนวกที่ 1 ของคำวินิจฉัยที่ 2000/520 ได้มีการบัญญัติเกี่ยวกับหลักในการคุ้มครองความเป็นส่วนตัวของโครงการเซฟฮาร์เบอร์ ซึ่งในวรรคสี่ของภาคผนวกดังกล่าวได้บัญญัติเกี่ยวกับข้อยกเว้นของโครงการเซฟฮาร์เบอร์ไว้ 2 กรณีใหญ่ๆ คือ

1. ข้อยกเว้นเนื่องจากความจำเป็นในการคุ้มครองความมั่นคงของชาติ ประโยชน์สาธารณะ

2. ข้อยกเว้นโดยรัฐบัญญัติ ระเบียบของราชการ หรือกฎหมายที่มาจากบรรทัดฐานคำพิพากษาของศาล ซึ่งได้สร้างข้อผูกพันที่ขัดแย้งกับหลักการเซฟฮาร์เบอร์รวมไปถึงการให้อำนาจตามกฎหมายอย่างชัดแจ้ง

สำหรับการให้อำนาจตามกฎหมายอย่างชัดแจ้งมีการอธิบายเพิ่มเติมเอาไว้ในภาคผนวกที่ 4 ซึ่งเป็นภาคผนวกที่ได้จัดทำขึ้นตามข้อเรียกร้องของคณะกรรมาธิการยุโรปในการอรรถาธิบายกฎหมายสหรัฐอเมริกา ในส่วนที่เกี่ยวข้องกับการให้อำนาจตามกฎหมายอย่างชัดแจ้งโดยมีข้อความตามภาคผนวกดังต่อไปนี้ “หลักการของโครงการเซฟฮาร์เบอร์ประกอบไปด้วยข้อยกเว้นในกรณีที่รัฐบัญญัติ กฎระเบียบข้อบังคับ หรือกฎหมายที่มาจากบรรทัดฐานคำพิพากษาของศาลได้ก่อให้เกิดข้อผูกพันที่ขัดแย้งหรือมีการให้อำนาจตามกฎหมายอย่างชัดแจ้ง โดยมีเงื่อนไขว่าในการอนุญาตเหล่านี้ องค์กรต้องแสดงให้เห็นว่าการฝ่าฝืนหลักการของโครงการเซฟฮาร์เบอร์อยู่ในขอบเขตอันชอบธรรมตามกฎหมายอันเป็นฐานที่มาแห่งอำนาจนั้น เป็นที่ชัดเจนว่าในกรณีที่กฎหมายสหรัฐอเมริกาได้กำหนดข้อผูกพันที่ขัดแย้งกับหลักกาเซฟฮาร์เบอร์ขึ้นมานั้น องค์กรสหรัฐฯทั้งที่ได้เข้าร่วมและมิได้เข้าร่วมโครงการเซฟฮาร์เบอร์จะต้องปฏิบัติตามกฎหมาย สำหรับการให้อำนาจตามกฎหมายอย่างชัดแจ้งนั้น ถึงแม้ว่าหลักของโครงการเซฟฮาร์เบอร์จะมีจุดมุ่งหมายในการเชื่อมความแตกต่างระหว่างกฎหมายเกี่ยวกับความเป็นส่วนตัวของสหรัฐอเมริกาและสหภาพยุโรป แต่ประเทศสหรัฐอเมริกาเองก็ต้องเคารพอำนาจพิเศษในการบัญญัติกฎหมายของสมาชิกสภานิติบัญญัติที่มาจากการเลือกตั้ง...” ดังนั้นองค์กรของสหรัฐฯทั้งที่ได้และมิได้เข้าร่วมโครงการเซฟฮาร์เบอร์จะต้องปฏิบัติตามกฎหมายโดยเฉพาะในกรณีที่กฎหมายสหรัฐอเมริกาได้ประกาศข้อกำหนดที่ขัดกับหลักเซฟฮาร์เบอร์

การกำหนดข้อยกเว้นให้ไม่ต้องปฏิบัติตามหลักการของเซฟฮาร์เบอร์ตามภาคผนวกที่ 1 วรรคสี่ของคำวินิจฉัยที่ 2000/520 เป็นการเปิดช่องให้หน่วยงานของรัฐบาลสามารถเข้าแทรกแซงข้อมูลส่วนบุคคลที่ถ่ายโอนจากสภาพยุโรปไปยังสหรัฐอเมริกาได้ อีกทั้งโครงการเซฟฮาร์เบอร์มีผลบังคับเฉพาะองค์กรที่เข้าร่วมผูกพันตนตามโครงการเท่านั้น ตามภาคผนวกที่ 1 วรรคสอง ของคำวินิจฉัยที่ 2000/520 ที่ได้วางหลักว่าโครงการเซฟฮาร์เบอร์มีจุดประสงค์เพื่อใช้โดยองค์กรของสหรัฐในการรับข้อมูลส่วนบุคคลจากสหภาพยุโรปเพื่อวัตถุประสงค์ในการปรับองค์กรให้มีคุณสมบัติและระดับการคุ้มครองให้มีระดับเพียงพอดังที่ได้คาดการณ์ไว้เท่านั้น ดังนั้นหลักการเหล่านี้จะมีผลบังคับใช้สำหรับการรับรองตนเองขององค์กรเอกชนในสหรัฐฯเพื่อการรับข้อมูลส่วนบุคคลจากสหภาพยุโรปเท่านั้น หน่วยงานรัฐบาลของสหรัฐอเมริกามิได้ถูกกำหนดให้ปฏิบัติตามหลักการดังกล่าว

การแทรกแซงข้อมูลส่วนบุคคลที่ถ่ายโอนจากสหภาพยุโรปไปยังสหรัฐอเมริกาโดยการให้หน่วยงานของรัฐใช้ฐานจากกฎหมายภายในของสหรัฐอเมริกา ตามที่โครงการเซฟฮาร์เบอร์มีข้อยกเว้นเปิดช่องเอาไว้นั้น ได้มีการประเมินสถานการณ์ในการปฏิบัติตามคำวินิจฉัยที่ 2000/520 ของคณะกรรมาธิการเอาไว้เช่นกันตาม Communication COM (2013) 846 Final และ Communication COM (2013) 847 Final ซึ่งเนื้อหาของ Communicationทั้งสองมีดังต่อไปนี้

Communication COM (2013) 846 Final[28] เป็นรายงานที่ได้ร่างขึ้นร่วมกับสหรัฐอเมริกาหลังมีการตรวจพบว่ามีแผนงานสอดแนม (surveillance program) ข้อมูลส่วนบุคคลในสหรัฐอเมริกาจำนวนมากที่เกี่ยวข้องกับการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลขนาดใหญ่ (large-scale) โดยในรายงานได้อธิบายและวิเคราะห์บทกฎหมายสหรัฐอเมริกาอย่างละเอียด โดยเฉพาะฐานกฎหมายที่ให้อำนาจในการสอดแนมรวมไปถึงการรวบรวมและประมวลผลข้อมูลส่วนตัวโดยเจ้าหน้าที่ผู้มีอำนาจในสหรัฐอเมริกาด้วย

ในหัวข้อที่ 1 คณะกรรมาธิการได้แถลงไว้ว่าการแลกเปลี่ยนเชิงพาณิชย์นั้นจะต้องถูกกำหนดโดยคำวินิจฉัยที่ 2000/520 โดยในปัจจุบันการถ่ายโอนข้อมูลส่วนบุคคลที่มีมากขึ้น สาเหตุมาจากการเติบโตของเศรษฐกิจแบบดิจิทัลซึ่งทำให้ ปริมาณ คุณภาพ ความหลากหลาย รวมไปถึงลักษณะธรรมชาติของกิจกรรมการประมวลผลข้อมูลมีการเติบโตและมีจำนวนเพิ่มขึ้นแบบทวีคูณอีกด้วย

ในหัวข้อที่ 2 ของ Communication นี้ คณะกรรมาธิการได้สังเกตและรับทราบว่าประชาชนในสหภาพยุโรปมีความกังวลต่อระดับของการคุ้มครองข้อมูลส่วนบุคคลที่ถูกถ่ายโอนไปยังสหรัฐอเมริกาภายใต้แผนงานของโครงการเซฟฮาร์เบอร์เพิ่มมากขึ้น และเห็นว่าลักษณะตามธรรมชาติของแผนงานที่เป็นไปโดยสมัครใจและเปิดเผยนั้นทำให้ต้องพิจารณาความโปร่งใสและสภาพการบังคับใช้ของแผนงานนี้ให้ชัดเจนมากยิ่งขึ้น คณะกรรมาธิการยุโรปได้แถลงต่อไปในหัวข้อที่ 2 ว่าข้อมูลส่วนตัวของประชาชนในสหภาพยุโรปที่ถูกส่งไปยังสหรัฐอเมริกาภายใต้โครงการเซฟฮาร์เบอร์นั้นอาจถูกเข้าถึงและประมวลผลโดยเจ้าหน้าที่ผู้มีอำนาจของสหรัฐอเมริกาด้วยวิธีการที่ไม่สอดคล้องกับมูลเหตุแต่เดิมที่ข้อมูลนั้นได้ถูกเก็บรวบรวมในสหภาพยุโรปและถ่ายโอนไปยังสหรัฐอเมริกา และพบว่าบริษัทที่ให้บริการทางอินเทอร์เน็ตในสหรัฐอเมริกาส่วนใหญ่ที่ผ่านการรับรองจากโครงการเซฟฮาร์เบอร์แล้วนั้นมีส่วนเกี่ยวข้องโดยตรงกับแผนงานสอดแนมที่เป็นปัญหาอยู่

ในหัวข้อที่ 3.2 ของ Communication นี้ คณะกรรมาธิการยุโรปได้ชี้ให้เห็นข้อบกพร่องหลายประการในการนำคำวินิจฉัยที่ 2000/520 ไปปรับใช้กับการถ่ายโอนข้อมูลส่วนบุคคล ประการแรกมีปัญหาว่าบางบริษัทในสหรัฐอเมริกาที่ผ่านการรับรองโดยกระทรวงพาณิชย์

---

[28] Communication COM (2013) 846 Final คือเอกสารแนวนโยบายว่าด้วยการฟื้นฟูความเชื่อมั่นด้านความปลอดภัยในการถ่ายโอนข้อมูลระหว่างสหภาพยุโรปและสหรัฐอเมริกา ที่คณะกรรมาธิการยุโรปได้ยื่นต่อรัฐสภายุโรปและคณะมนตรี พร้อมกับรายงานผลการตรวจสอบโดยคณะกรรมการร่วมของสหภาพยุโรปในคณะทำงานเพื่อคุ้มครองความเป็นส่วนตัวเฉพาะกิจสหภาพยุโรป-สหรัฐอเมริกา

สหรัฐอเมริกาแล้วนั้นมิได้ปฏิบัติตามหลักการที่อ้างอิงถึงในข้อ 1(1) ของคำวินิจฉัยที่ 2000/520 (หลักของโครงการเซฟฮาร์เบอร์) และควรมีการปรับปรุงแก้ไขข้อบกพร่องทางโครงสร้างในคำวินิจฉัยที่เกี่ยวข้องกับความโปร่งใสและประสิทธิภาพในการบังคับใช้หลักของโครงการเซฟฮาร์เบอร์และข้อบกพร่องที่เกิดจากการปฏิบัติตามข้อยกเว้นด้านความมั่นคงแห่งชาติ ในประการที่สอง คณะกรรมาธิการยุโรปเห็นว่ามีการใช้โครงการเซฟฮาร์เบอร์เป็นประหนึ่งช่องทางให้มีการถ่ายโอนข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรปไปยังสหรัฐอเมริกาโดยบริษัทที่ได้รับโอนข้อมูลส่วนบุคคลนั้นถูกกำหนดให้ส่งมอบข้อมูลให้กับหน่วยสืบราชการลับสหรัฐอเมริกาภายใต้แผนงานเก็บรวมรวมข่าวกรองของสหรัฐอเมริกาด้วย

ส่วน Communication COM (2013) 847 final ว่าด้วยผลการดำเนินการของโครงการเซฟฮาร์เบอร์ในทัศนะของพลเมืองยุโรปและบริษัทที่ก่อตั้งในสหภาพยุโรป ดังที่เห็นได้ชัดเจนจากหัวข้อที่ 1 Communication นี้ได้เขียนขึ้นตามข้อมูลที่ได้รับจากคณะดำเนินการคุ้มครองความเป็นส่วนตัวเฉพาะกิจสหภาพยุโรป-สหรัฐอเมริกา และตามรายงานการประเมินของคณะกรรมาธิการที่ออกในปี ค.ศ. 2002 และ 2004 ตามลำดับ

หัวข้อที่ 1 ของ Communication ได้อธิบายว่าการปฏิบัติงานตามคำวินิจฉัยที่ 2000/520 ขึ้นอยู่กับข้อผูกมัดและการรับรองตนเองของบริษัทที่ทำตาม โดยเสริมว่าการลงชื่อเข้าร่วมในข้อตกลงเหล่านี้เป็นไปโดยสมัครใจและกฎระเบียบเหล่านี้ผูกพันอยู่กับองค์กรที่ได้ลงชื่อเข้าร่วมเท่านั้น

นอกจากนี้หัวข้อที่ 2.2 ของ Communication ยังแถลงไว้อย่างชัดเจนอีกด้วยว่าในวันที่ 26 กันยายน ค.ศ. 2013 มีบริษัทจำนวน 3,246 บริษัทที่อยู่ในภาคอุตสาหกรรมและบริการหลายภาคส่วนที่ได้ผ่านการรับรองแล้ว และบริษัทเหล่านี้ได้ให้บริการตลาดภายในสหภาพยุโรปเป็นส่วนหลักโดยเฉพาะภาคส่วนที่ให้บริการอินเทอร์เน็ต โดยบางบริษัทดังกล่าวนั้นเป็นบริษัทในสหภาพยุโรปที่มีสำนักงานสาขาอยู่ในสหรัฐอเมริกาและได้ประมวลผลข้อมูลของพนักงานภายในบริษัทที่ถูกถ่ายโอนไปยังสหรัฐอเมริกาเพื่อจุดประสงค์ทางด้านทรัพยากรบุคคล ซึ่งจุดบกพร่องในด้านความโปร่งใสหรือการบังคับใช้หลักการในฝั่งของประเทศสหรัฐอเมริกามีผลทำให้ภาระความรับผิดชอบเปลี่ยนไปอยู่กับเจ้าหน้าที่คุ้มครองข้อมูลในสหภาพยุโรปและบริษัทที่ได้ดำเนินการตามแผนงาน

หัวข้อที่ 3 ถึง 5 และ 8 ของ Communication เห็นได้อย่างชัดเจนว่าในทางปฏิบัติแล้ว มีบริษัทที่ได้รับการรับรองจำนวนมากมิได้ปฏิบัติตามหลักของโครงการเซฟฮาร์เบอร์อย่างเต็มที่

นอกเหนือจากนี้คณะกรรมาธิการยังได้แถลงในหัวข้อที่ 7 ของ Communication ไว้ว่าทุกบริษัทที่ได้เข้าร่วมกับโครงการปริซึมซึ่งเป็นแผนงานรวบรวมข่าวกรองขนาดใหญ่ที่อนุญาตให้เจ้าหน้าที่ผู้มีอำนาจได้เข้าถึงข้อมูลเพื่อการจัดเก็บและประมวลผลในสหรัฐอเมริกานั้น ล้วนเป็นโครงการที่ผ่านการรับรองของโครงการเซฟฮาร์เบอร์และใช้โครงการเซฟฮาร์เบอร์เป็นประหนึ่ง

ช่องทางที่ทำให้เจ้าหน้าที่สืบราชการลับสหรัฐสามารถเข้าไปเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับการประมวลผลขั้นต้นในสหภาพยุโรปได้ จากข้อเท็จจริงดังกล่าวคณะกรรมาธิการยุโรปจึงได้ชี้แจงในหัวข้อ 7.1 ของ Communication นี้ว่ามีฐานกฎหมายภายใต้กฎหมายสหรัฐจำนวนมากที่อนุญาตให้มีการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลขนาดใหญ่ซึ่งถูกจัดเก็บหรือประมวลผลโดยบริษัทที่ก่อตั้งในสหรัฐอเมริกาแต่ดั้งเดิมได้ และลักษณะตามธรรมชาติของแผนงานนี้ที่สามารถเก็บรวบรวมและประมวลผลข้อมูลจำนวนมากได้อาจมีผลทำให้เจ้าหน้าที่ที่มีอำนาจของสหรัฐอเมริกาเข้าถึงและประมวลผลข้อมูลที่ถูกถ่ายโอนภายใต้โครงการเซฟฮาร์เบอร์ต่อไปโดยเกินขอบเขตที่จำเป็นและไม่สัมพันธ์กับระดับความมั่นคงแห่งชาติดังที่คาดการณ์ไว้ภายใต้ข้อยกเว้นในคำวินิจฉัยที่ 2000/520 ได้

จาก Communication ทั้งสองฉบับนั้นได้สร้างน้ำหนักให้ศาลตัดสินว่าหน่วยงานของสหรัฐอเมริกาสามารถเข้าถึงข้อมูลส่วนบุคคลที่ถูกถ่ายโอนจากประเทศสมาชิกไปยังประเทศสหรัฐอเมริกา และสามารถประมวลผลข้อมูลเหล่านั้นในแนวทางที่ขัดแย้งกับจุดประสงค์ในการถ่ายโอนเพราะสามารถเข้าถึงข้อมูลได้เกินกว่าที่จำเป็น เข้าถึงข้อมูลได้ในปริมาณมาก เข้าถึงได้ตามอำเภอใจ ไม่เฉพาะเจาะจงบุคคล ต่างจากกฎหมายของสหภาพยุโรปที่ได้บัญญัติให้การแทรกแซงสิทธิขั้นพื้นฐานที่ได้รับการรับรองโดยข้อที่ 7 และ 8 ของกฎบัตร จะต้องระบุกฎเกณฑ์ที่ชัดเจนและเฉพาะเจาะจง มีการกำหนดขอบเขตและมีวิธีการบังคับใช้มาตรการที่ชัดเจนตามกฎหมาย ส่วนข้อยกเว้นหรือข้อจำกัดที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้มีการบังคับใช้เท่าที่จำเป็นเท่านั้น[29] ในสหภาพยุโรปนั้นให้เจ้าหน้าที่รัฐเข้าถึงข้อมูลส่วนบุคคลโดยจำกัดวิธีการไว้อย่างเข้มงวด การเข้าถึงหรือแทรกแซงข้อมูลจะต้องสามารถรับรองความถูกต้องตามกฎหมายได้[30]

ดังนั้นคำวินิจฉัยที่ 2000/520 ได้แสดงให้เห็นแล้วว่า ความมั่นคงแห่งชาติ ประโยชน์สาธารณะ และข้อกำหนดในการบังคับใช้กฎหมาย มีความสำคัญมากกว่าหลักการของโครงการเซฟฮาร์เบอร์โดยให้องค์กรของสหรัฐอเมริกาที่ได้รับรองตนเองในการรับข้อมูลส่วนบุคคลที่มาจากสหภาพยุโรปแล้วมีสิทธิเพิกเฉยต่อหลักการเซฟฮาร์เบอร์อย่างไม่มีข้อจำกัด ในกรณีที่หลัก

---

[29] ตามคำพิพากษา Digital Rights Ireland and Others, C-293/12 และ C-594/12, EU:C:2014:238, วรรคที่ 52 และ case-law ที่ได้ยกมา

[30] ศึกษาเพิ่มเติมใน Directive 2006/24/EC ของรัฐสภายุโรปและคณะมนตรีแห่งสหภาพยุโรปวันที่ 15 มีนาคม ค.ศ. 2006 เกี่ยวกับการเก็บรักษาข้อมูลที่ได้สร้างหรือประมวลผลตามบทบัญญัติสำหรับการบริการการสื่อสารสาธารณะทางอิเล็กทรอนิกส์หรือเครือข่ายการสื่อสารสาธารณะ

เซฟฮาร์เบอร์นั้นขัดกับข้อจำกัดหรือข้อยกเว้นที่ได้กล่าวมา ตามการวิเคราะห์ข้อ 1(1) ร่วมกับภาคผนวกที่ 1

นอกจากนี้มีข้อพิจารณาว่าก่อนมีโครงการปริซึมและการสอดแนมข้อมูลจำนวนมากนั้นประเทศสหรัฐอเมริกาก็มีกฎหมายที่เกี่ยวกับการสอดแนมทางอิเล็กทรอนิกส์หรือกฎหมายที่ใช้ดักรับข้อมูลข่าวสารอยู่หลายฉบับด้วยกัน ยกตัวอย่างเช่น รัฐบัญญัติคุ้มครองความเป็นส่วนตัวในการสื่อสารทางอิเล็กทรอนิกส์ (Electronic Communication Privacy Act 1987) แต่เหตุใดการเข้าถึงข้อมูลส่วนบุคคลตามกฎหมายเหล่านั้นมิได้เป็นเหตุให้ศาลยุติธรรมแห่งสหภาพยุโรปพิพากษาว่าประเทศสหรัฐอเมริกามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ จึงต้องวิเคราะห์ลักษณะกฎหมายที่ให้อำนาจหน่วยงานของรัฐเข้าถึงข้อมูลส่วนบุคคลเหล่านั้นด้วย ดังนี้

รัฐบัญญัติคุ้มครองความเป็นส่วนตัวในการสื่อสารทางอิเล็กทรอนิกส์ หรือเรียกโดยย่อว่า “ECPA” กฎหมายนี้ได้ประกอบไปด้วย 3 ส่วนย่อย คือ กฎหมายว่าด้วยการดักฟังการติดต่อสื่อสาร (Wiretap Act), กฎหมายว่าด้วยการสื่อสารที่ถูกเก็บรักษาไว้ (Stored Communication Act หรือ SCA) และกฎหมายว่าด้วยอุปกรณ์เพื่อถอดรหัสการสื่อสาร (Pen Register Act) กฎหมายนี้ใช้บังคับทั้งภาครัฐและเอกชน

ตามกฎหมายว่าด้วยการดักฟังการติดต่อสื่อสารกำหนดให้การดักรับเนื้อหาในการสื่อสารจะกระทำได้โดยชอบด้วยกฎหมายโดยการขอคำสั่งศาล (court order) โดยจะต้องระบุเหตุจำเป็น (probable cause) และแสดงให้ศาลเห็นว่าการกระทำเพื่อให้ได้มาซึ่งพยานหลักฐานโดยวิธีอื่นนั้นไม่สามารถกระทำได้หรือถ้ากระทำจะเป็นอันตรายเกินไป ส่วนกฎหมายว่าด้วยการสื่อสารที่ถูกเก็บรักษาไว้ เป็นการกำหนดวิธีเข้าถึงการสื่อสารที่ถูกเก็บไว้ในรูปแบบอิเล็กทรอนิกส์ โดยบัญญัติให้เจ้าหน้าที่รัฐสามารถเข้าถึงข้อมูลดังกล่าวได้ต่อเมื่อเป็นไปตามเงื่อนไขที่กฎหมายกำหนด เช่น กรณีที่ 1.การเก็บข้อมูลไม่เกิน 180 วัน จะต้องขอหมายศาล (court warrant) โดยแสดงให้เห็นถึงเหตุจำเป็น กรณีที่ 2.การเก็บข้อมูลไว้เกิน 180 วัน เจ้าหน้าที่ของรัฐจะต้องทำคำบอกกล่าวผู้ใช้บริการล่วงหน้า (prior notice) มีคำสั่งเรียกพยานหลักฐาน (subpoena) หรือ คำสั่งเป็นต้น ในส่วนสุดท้าย

คือ กฎหมายว่าด้วยอุปกรณ์เพื่อถอดรหัสการสื่อสารก็ได้กำหนดให้การใช้อุปกรณ์เพื่อดักการสื่อสาร[31] จะต้องมีคำสั่งศาลเช่นเดียวกัน[32]

ส่วนกฎหมายที่เป็นฐานที่มาของโครงการปริซึมคือรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศนั้นเป็นกฎหมายที่ใช้ในการสืบหาข่าวกรองจากผู้มีอำนาจต่างประเทศหรือตัวแทน ซึ่งกฎหมายนี้มีการแก้ไขเพิ่มเติมหลายครั้งหลังเหตุการณ์ก่อการร้าย 9/11 รัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศนี้ได้กำหนดวิธีการสอดแนมทางอิเล็กทรอนิกส์ รวมถึงการค้นหาทางกายภาพ (physical search) ภายในประเทศเพื่อให้ได้มาซึ่งข้อมูลข่าวกรองต่างประเทศ (foreign intelligence information) รวมถึงการใช้อุปกรณ์เพื่อถอดรหัสการสื่อสาร ตลอดจนการเข้าถึงข้อมูลทางธุรกิจ โดยเป็นข้อมูลเกี่ยวกับการกระทำของต่างชาติที่มีลักษณะเป็นการโจมตี ก่อวินาศกรรม ก่อการร้ายระหว่างประเทศ การสืบข้อมูลลับหรือข้อมูลเกี่ยวกับการป้องกันประเทศเป็นต้น การใช้อำนาจตามรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศนี้จะต้องเป็นกรณีที่มีวัตถุประสงค์เกี่ยวกับการราชการลับต่างประเทศ คือข้อมูลนั้นจะต้องมีจุดเชื่อมโยงกับผู้มีอำนาจต่างประเทศ (foreign power) หรือตัวแทน

อำนาจของเจ้าหน้าที่รัฐในการเข้าถึงข้อมูลส่วนบุคคลตามรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศสามารถทำได้ง่ายกว่ารัฐบัญญัติคุ้มครองความเป็นส่วนตัวในการสื่อสารทางอิเล็กทรอนิกส์ เนื่องจากมีทั้งกรณีที่มีทั้งการเข้าถึงข้อมูลแบบต้องขอหมายศาลและกรณีที่ไม่ต้องขอหมายศาล[33] อีกทั้งตามรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศมีการดำเนินการโดยศาลพิเศษที่แยกออกมาจากศาลปกติ เรียกว่าศาลสืบราชการลับต่างประเทศ (Foreign Intelligence

---

[31] อุปกรณ์เพื่อถอดรหัสการสื่อสาร ได้แก่ Pen Register และ Trap and Trace devices ซึ่งกฎหมาย 18 U.S.C. มาตรา 3127(3) ของประเทศสหรัฐอเมริกา ได้นิยามไว้ว่า Pen Register คืออุปกรณ์หรือกระบวนการที่ใช้บันทึกหรือถอดรหัสสารสนเทศเกี่ยวกับการโทรศัพท์ การติดต่อ ที่อยู่หรือสัญญาณ ซึ่งมีการส่งโดยใช้อุปกรณ์หรือเครื่องมือที่ส่งตามสายหรือทางอิเล็กทรอนิกส์ แต่สื่ออิเล็กทรอนิกส์ดังกล่าวต้องไม่มีเนื้อหาในการสื่อสาร ส่วนอุปกรณ์ trap and trace คืออุปกรณ์เก็บข้อมูลขาเข้าซึ่งจับกระแสอิเล็กทรอนิกส์หรือสิ่งอื่นที่ส่งเข้ามาโดยแสดงข้อมูลทางอิเล็กทรอนิกส์ที่เป็นหมายเลขผู้โทรเข้า หรือการติดต่อ ที่อยู่ หรือสัญญาณ ที่สามารถระบุถึงแหล่งที่มาของการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ที่ให้บริการได้

[32] ชวิน อุ่นภัทร, “ความเป็นส่วนตัวและการคุ้มครองจากการล่วงล้ำของรัฐในประเทศสหรัฐอเมริกา,”วารสารนิติศาสตร์, ปีที่ 44 ฉบับที่ 4, น.988-990 (ธันวาคม 2558).

[33] *เพิ่งอ้าง*, น.993.

Surveillance Court หรือ FISC) ซึ่งทำหน้าที่พิจารณาทบทวนการใช้อำนาจตามกฎหมายฉบับนี้ และการพิจารณาคดีของศาลนี้จะต้องดำเนินการโดยลับ

รัฐบาลสหรัฐอเมริกาอ้างว่าฐานที่มาของโครงการปริซึมมาจากอำนาจตามมาตรา 702[34] แห่งรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศและเป็นการใช้อำนาจตามกฎหมาย[35] ตามมาตรา 702 นั้นให้อำนาจเจ้าที่ของรัฐเข้าถึงข้อมูลของบุคคลที่ไม่ใช่คนอเมริกันและไม่ได้มีถิ่นฐานอยู่ในประเทศสหรัฐอเมริกา แต่ห้ามมิให้เก็บข้อมูลจากคนอเมริกันหรือผู้อาศัยอยู่ในสหรัฐอเมริกา แต่อย่างไรก็ตามได้มีการเปิดเผยคำตัดสินของศาลสืบราชการลับต่างประเทศ เมื่อปี ค.ศ. 2011 ว่าสำนักงานความมั่นคงแห่งชาติได้เก็บข้อมูลการสื่อสารทางอีเมลของคนอเมริกันไว้หลายหมื่นฉบับด้วยกัน[36] แสดงให้เห็นว่าคนอเมริกันเองก็ถูกเก็บข้อมูลและสอดแนมจากหน่วยงานทางด้านความมั่นคงด้วยเช่นกัน นอกจากนี้ตามการเปิดเผยของนายเอ็ดเวิร์ด สโนว์เดนพบว่าโครงการปริซึมซึ่งเป็นโครงการลับสุดยอดของหน่วยงานความมั่นคงของสหรัฐอเมริกาไม่ได้มาจากอำนาจมาตรา 702 แห่งรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศ แต่มาจากคำสั่งปฏิบัติการ (Executive Order) ที่

---

[34] Section 702 permits the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are “not United States persons” and are reasonably believed to be located outside the United State. Before doing so, the Attorney General and the Director of National Intelligence normally must obtain the Foreign Intelligence Surveillance Court’s (FISC) approval.

มาตรา 702 อนุญาตให้อัยการสูงสุดและผู้อำนวยการหน่วยสืบราชการลับแห่งชาติได้รับข้อมูลข่าวกรองต่างประเทศ โดยการตรวจสอบเฝ้าระวังบุคคลที่ “ไม่ใช่คนสหรัฐอเมริกา” และมีเหตุอันควรเชื่อว่าอยู่ภายนอกประเทศสหรัฐอเมริกา ก่อนที่จะทำเช่นนั้นอัยการสูงสุดและผู้อำนวยการหน่วยสืบราชการลับแห่งชาติ ต้องได้รับการอนุมัติจากศาลสืบราชการลับต่างประเทศ

[35] นาย Rajesh De ที่ปรึกษาทั่วไปของสำนักงานความมั่นคงแห่งชาติ ได้เปิดเผยว่าการเข้าถึงและจัดเก็บข้อมูลส่วนบุคคล ไม่ได้จัดเก็บจากข้อมูลการสื่อสารที่เป็นของบริษัทโดยตรง แต่เป็นการจัดเก็บข้อมูลระหว่างการสื่อสารผ่านระบบอินเทอร์เน็ต ตามมาตรา 702 แห่งรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศ

[36] Spencer Ackerman, “US tech giants knew of NSA data collection, agency’s top lawyer insists,” สืบค้นเมื่อวันที่ 5 พฤษภาคม 2559, จาก http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de.

12333[37] ซึ่งเป็นการออกคำสั่งโดยลับ ส่งผลให้โครงการปริซึมสามารถเก็บรวบรวมข้อมูลโดยตรงจากแหล่งข้อมูลขนาดใหญ่จำนวนมาก ไม่ต้องมีหมายศาล และไม่ได้จำกัดเพียงบุคคลที่ไม่ใช่คนอเมริกันอีกด้วย

แม้ว่าฐานของกฎหมายอันเป็นที่มาของโครงการปริซึมจะยังไม่มีการเปิดเผยอย่างกระจ่างชัด แต่ก็สามารถวิเคราะห์ได้ว่ารัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศเองมีจุดที่แตกต่างจากรัฐบัญญัติคุ้มครองความเป็นส่วนตัวในการสื่อสารทางอิเล็กทรอนิกส์หลายประการ ตามรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศนั้นมีการบัญญัติให้การเข้าถึงข้อมูลส่วนบุคคลกระทำได้ง่ายกว่ารัฐบัญญัติคุ้มครองความเป็นส่วนตัวในการสื่อสารทางอิเล็กทรอนิกส์ อีกทั้งการเข้าถึงข้อมูลส่วนบุคคลในกรณีที่ไม่ต้องขอหมายศาลยังมีข้อจำกัดน้อยกว่าด้วย[38] ปัญหาสำคัญของรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศคือการพิจารณาของศาลกระทำโดยลับ การกำหนดให้มีการพิจารณาโดยลับนี้เองส่งผลให้เกิดความไม่โปรงใส ไม่สามารถเปิดเผยและอธิบายอย่างชัดเจนให้แก่สาธารณชนได้ และยังเป็นการเปิดโอกาสให้หน่วยงานของรัฐสามารถอ้างเหตุผลในเรื่องความมั่นคงมาใช้ในการเข้าถึงข้อมูลส่วนบุคคลได้อย่างไร้การตรวจสอบ อันจะนำมาสู่การละเมิดสิทธิของบุคคลในที่สุด

ตามการวิเคราะห์คำพิพากษาข้างต้นสรุปได้ว่ากรณีที่จะเข้าเหตุให้ศาลตัดสินว่ากฎหมายหรือมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของประเทศนอกกลุ่มสมาชิกสหภาพยุโรปให้การรับรองการคุ้มครองข้อมูลส่วนบุคคลได้ไม่เพียงพอ จะต้องเข้าองค์ประกอบดังต่อไปนี้

(1) กฎหมายหรือมาตรการที่มีขึ้นเพื่อวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคลได้มีการกำหนดข้อยกเว้นให้ไม่ต้องปฏิบัติตามหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลเอาไว้ ไม่ว่าจะด้วยเหตุผลเพื่อความมั่นคงแห่งชาติ ประโยชน์สาธารณะ หรืออาศัยอำนาจตามกฎหมายอื่นใด และ

(2) กฎหมายหรือคำสั่งอื่นใดในประเทศนอกสมาชิกสหภาพยุโรปมีการบัญญัติเปิดช่องให้อำนาจหน่วยงานของรัฐสามารถเข้าถึงข้อมูลส่วนบุคคลได้อย่างไม่มีขอบเขตจำกัด โดยสามารถเก็บรวบรวมและประมวลผลข้อมูลได้ในจำนวนมาก (large scale) และไม่เฉพาะเจาะจงเป้าหมาย (indiscriminate)

อนึ่งในการพิจารณาของศาลยุติธรรมแห่งสหภาพยุโรปนั้นเป็นการพิจารณาองค์ประกอบทั้งสองประการข้างต้นควบคู่กัน และจะต้องเป็นกรณีที่เข้าองค์ประกอบทั้งสองประการนี้จึงจะทำให้ศาลพิจารณาได้ว่าประเทศนั้นๆมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ ดังจะเห็นได้ว่าข้อยกเว้นให้ไม่ต้องปฏิบัติตามโครงการเซฟฮาร์เบอร์ได้บัญญัติขึ้นตั้งแต่เมื่อ ค.ศ. 2000 แล้ว

---

[37] *เพิ่งอ้าง.*

[38] ชวิน อุ่นภัทร, *อ้างแล้ว เชิงอรรถที่ 32*, น.993.

แต่คณะกรรมาธิการยุโรปก็ยังให้การรับรองตามคำวินิจฉัยที่ 2000/520 ว่าประเทศสหรัฐอเมริกามีการรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เนื่องจากในขณะนั้นไม่ปรากฏว่ามีกฎหมายของประเทศสหรัฐอเมริกาที่เปิดช่องให้หน่วยงานของรัฐสามารถเข้าถึงข้อมูลส่วนบุคคลได้แบบไม่มีข้อจำกัด แต่เมื่อสถานการณ์เปลี่ยนแปลงไป ประเทศสหรัฐอเมริกาได้บัญญัติกฎหมายให้อำนาจหน่วยงานเกี่ยวกับความมั่นคงแห่งชาติสามารถเข้าถึงข้อมูลส่วนบุคคลได้เป็นจำนวนมากตามที่ได้รับการประเมินใน Communication ทั้งสองฉบับข้างต้น จึงเป็นการเข้าองค์ประกอบทั้งสองประการที่จะทำให้ศาลตัดสินว่าการคุ้มครองข้อมูลส่วนบุคคลตามโครงการเซฟฮาร์เบอร์ไม่สามารถคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพออีกต่อไป

(2) คำวินิจฉัยที่ 2000/520 ไม่ได้ระบุมาตรการในการป้องกันตรวจสอบ ในกรณีที่มีการแทรกแซงสิทธิในข้อมูลส่วนบุคคล

ตามบทบัญญัติของคำวินิจฉัยนี้มิได้ระบุถึงวิธีการป้องกันการแทรกแซงข้อมูลส่วนบุคคลจากหน่วยงานของรัฐที่มีประสิทธิภาพตามกฎหมาย โดยในข้อสงสัยที่ได้รับการซักถามบ่อยครั้งที่ 11 ภาคผนวกที่ 2 ของ คำวินิจฉัยนั้นมีเพียงการกำหนดแนวทางการแก้ไขในกรณีที่มีข้อพิพาทหรือมีความล้มเหลวจากการไม่ปฏิบัติตามหลักของโครงการเซฟฮาร์เบอร์ซึ่งถูกจำกัดเฉพาะข้อพิพาททางการค้าเท่านั้น ไม่สามารถบังคับใช้ในข้อพิพาทที่เกี่ยวกับความถูกต้องตามกฎหมายในการแทรกแซงการใช้สิทธิขั้นพื้นฐานที่เป็นผลมาจากมาตรการของประเทศสมาชิกได้

อีกทั้งคำวินิจฉัยที่ 2000/520 ยังมิได้ระบุวิธีการตรวจสอบใดๆที่เกี่ยวกับกฎเกณฑ์ที่สหรัฐอเมริกานำมาใช้เพื่อแทรกแซงสิทธิขั้นพื้นฐานของบุคคลผู้ซึ่งข้อมูลส่วนตัวได้ถูกถ่ายโอนจากสหภาพยุโรปไปยังสหรัฐอเมริกา จึงเป็นกรณีที่คำวินิจฉัยได้มีข้อยกเว้นที่เปิดช่องให้หน่วยงานของรัฐใช้อำนาจแทรกแซงและเข้าถึงข้อมูลส่วนบุคคลได้ แต่กลับไม่มีการกำหนดวิธีป้องกันหรือตรวจสอบการใช้อำนาจนั้นว่าเป็นไปตามกฎหมายหรือไม่อย่างไร ทำให้หน่วยงานของรัฐสามารถใช้อำนาจได้ไม่จำกัด ขัดกับหลักสิทธิขั้นพื้นฐานที่ได้รับการรับรองตามข้อที่ 7 และ 8 ของกฎบัตรฯ ที่อนุญาตให้เจ้าหน้าที่ของรัฐเข้าถึงเนื้อหาของการสื่อสารได้อย่างจำกัด เข้มงวด และไม่กระทบต่อสิทธิขั้นพื้นฐานที่จะได้รับความเคารพต่อชีวิตส่วนตัว

(3) คำวินิจฉัยที่ 2000/520 ไม่ได้ให้สิทธิในการเยียวยาแก้ไขทางกฎหมายในกรณีที่มีการสอดแนมข้อมูลส่วนบุคคล

ตามบทบัญญัติของคำวินิจฉัยไม่ได้มีบทบัญญัติที่เปิดโอกาสให้เจ้าของข้อมูลส่วนบุคคลทั้งในสหภาพยุโรปหรือสหรัฐอเมริกาสามารถเข้าถึง แก้ไข ลบข้อมูล หรือได้รับการชดเชยด้านการจัดการหรือด้านกฎหมายเกี่ยวกับการที่หน่วยงานของรัฐได้เข้าเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคล จึงเป็นการที่กฎหมายไม่ได้ให้สิทธิเยียวยาแก้ไขทางกฎหมาย

กฎหมายที่ไม่ได้ให้สิทธิแก่ปัจเจกบุคคลได้รับการเยียวยาแก้ไขทางกฎหมายในการเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน หรือการแก้ไขหรือการลบข้อมูลนั้น ถือว่าไม่ได้เคารพสาระสำคัญของสิทธิขั้นพื้นฐานที่จะได้รับการคุ้มครองทางกฎหมายที่มีประสิทธิภาพ ดังที่ได้รับรองไว้เป็นพิเศษในข้อที่ 47 ของกฎบัตรฯ โดยข้อที่ 47 วรรคหนึ่ง ของกฎบัตรฯวางหลักไว้ว่าบุคคลทุกคนที่ถูกละเมิดสิทธิและเสรีภาพที่ได้รับรองไว้โดยกฎหมายของสหภาพยุโรป มีสิทธิในการได้รับการเยียวยาแก้ไขจากศาลที่ปฏิบัติตามเงื่อนไขในข้อนั้นได้ การเยียวยาตามกฎหมายกำหนดขึ้นเพื่อรับรองให้การปฏิบัติตามกฎหมายของสหภาพยุโรปนั้นมีประสิทธิภาพโดยเป็นสิ่งที่มีอยู่ตามธรรมชาติในหลักของกฎหมาย[39]

การจะบังคับใช้คำวินิจฉัยของคณะกรรมาธิการยุโรปตามข้อ 25(6) ของ Directive 95/46/EC ได้นั้นคณะกรรมาธิการต้องพิสูจน์ให้เห็นว่าประเทศสหรัฐอเมริกาได้รับรองระดับการคุ้มครองสิทธิขั้นพื้นฐานในระดับที่เท่าเทียมกันกับกฎหมายของสหภาพยุโรปจึงจะเป็นการรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ แต่เนื้อหาและข้อยกเว้นของคำวินิจฉัยดังที่กล่าวมาข้างต้นได้มีส่วนที่ขัดหรือแย้งกับหลักกฎหมายของสหภาพยุโรปอย่างชัดแจ้ง ดังนั้นประเทศสหรัฐอเมริกาจึงไม่มีการรับรองระดับการคุ้มครองที่เพียงพอตามเหตุอันเนื่องมาจากกฎหมายภายในประเทศหรือข้อผูกพันระหว่างประเทศตามความเป็นจริง อันเป็นผลให้ศาลตัดสินว่าคำวินิจฉัยที่ 2000/520 สิ้นผลไปในที่สุด

4.4 ผลกระทบที่เกิดจากคำพิพากษาคดีเลขที่ C-362/14 และแนวทางการแก้ไข

หลังจากศาลยุติธรรมแห่งสหภาพยุโรปได้ตัดสินให้คำวินิจฉัยที่ 2000/520 สิ้นผลไป คำพิพากษาของศาลยุติธรรมแห่งสหภาพยุโรปถือเป็นที่สุด ไม่สามารถอุทธรณ์หรือฎีกาได้ ส่งผลให้โครงการเซฟฮาร์เบอร์ซึ่งใช้ในการรับส่งข้อมูลระหว่างประเทศสหรัฐอเมริกาและกลุ่มประเทศสมาชิกสหภาพยุโรปมาตลอด 15 ปี ไม่มีผลบังคับใช้ได้อีกต่อไป ผลจากคำพิพากษาดังกล่าวได้สร้างความ

[39] ดูเพิ่มเติมในคำพิพากษา Les Verts v Parliament, 294/83, EU:C:1986:166, วรรคที่ 23; Johnston, 222/84, EU:C:1986:206, วรรคที่ 18 and 19; Heylens and Others, 222/86, EU:C:1987:442, วรรคที่14; และ UGT-Rioja and Others, C-428/06 ถึง C-434/06, EU:C:2008:488, วรรคที่ 80

สั่นสะเทือนและเกิดผลกระทบต่อบริษัทต่างๆกว่า 5,000 ราย[40] ที่ต้องอาศัยโครงการเซฟฮาร์เบอร์ในการรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรปมายังประเทศสหรัฐอเมริกา

ความสิ้นผลไปดังกล่าวส่งผลให้การส่งข้อมูลไปยังประเทศสหรัฐอเมริกาด้วยโครงการเซฟฮาร์เบอร์ไม่สามารถรับรองได้ว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามข้อ 25(1) Directive 95/46/EC อีกต่อไป นอกจากนี้ผลแห่งคำพิพากษายังกระทบต่อความเชื่อมั่นว่าประเทศนอกสมาชิกสหภาพยุโรปอื่นๆที่ได้รับการวินิจฉัยว่ามีการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอโดยคณะกรรมการยุโรปตามข้อ 25(6) นั้นยังมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพออยู่หรือไม่ เช่นการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย PIPEDA ที่ได้รับการรับรองโดยคำวินิจฉัยที่ 2002/2

ในการวิเคราะห์ว่าประเทศอื่นๆนอกกลุ่มสมาชิกสหภาพยุโรปอาจถูกตัดสินว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอโดยศาลยุติธรรมแห่งสหภาพยุโรปได้ ประเทศนั้นๆต้องมีองค์ประกอบ 2 ประการดังนี้ (1) กฎหมายหรือมาตรการที่มีขึ้นเพื่อวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคลได้มีการกำหนดข้อยกเว้นให้ไม่ต้องปฏิบัติตามหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลเอาไว้ ไม่ว่าจะด้วยเหตุผลเพื่อความมั่นคงแห่งชาติ ประโยชน์สาธารณะ หรืออาศัยอำนาจตามกฎหมายอื่นใด และ (2) กฎหมายหรือคำสั่งอื่นใดในประเทศนอกสมาชิกสหภาพยุโรปมีการบัญญัติเปิดช่องให้อำนาจหน่วยงานของรัฐสามารถเข้าถึงข้อมูลส่วนบุคคลได้อย่างไม่มีขอบเขตจำกัด โดยสามารถเก็บรวบรวมและประมวลผลข้อมูลได้ในจำนวนมาก และไม่เฉพาะเจาะจงเป้าหมาย

ในกรณีของกฎหมาย PIPEDA พบว่ามีข้อยกเว้น[41] ตามหมวด 1 มาตรา 7(3) ที่มีการอนุญาตให้ใช้หรือเปิดเผยข้อมูลส่วนบุคคลในหลากหลายวัตถุประสงค์ด้วยกัน เช่น โดยหมายศาลหรือคำสั่งศาล, การดำเนินการเพื่อประโยชน์ในการจัดทำประวัติอาชญากรรม, การดำเนินการโดยหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลในข้อมูลที่น่าสงสัยว่ามีความเกี่ยวข้องกับความมั่นคงของรัฐ, เพื่อการป้องกันประเทศและการดำเนินการในต่างประเทศ[42]

---

[40] Scott J. Shackelford JD, “Seeking a Safe Harbor in a widening sea : Unpacking the EJC’s SCHREMS decision and what it means for transatlantic relations,” Forthcoming Seton Hall Journal of Diplomacy and International Relations, p.1 (2016).

[41] โปรดดูรายละเอียดเพิ่มเติมในบทที่ 3 ส่วนที่ 3.3.2

[42] กฎหมาย PIPEDA หมวด 1 มาตรา7(3) “For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is ...

แม้ว่าข้อยกเว้นดังกล่าวได้มีการบัญญัติไว้ตั้งแต่ต้นเมื่อมีการออกคำวินิจฉัยที่ 2002/2 แต่ในขณะนั้นไม่มีกฎหมายที่เปิดช่องให้อำนาจหน่วยงานของรัฐสามารถเข้าถึงข้อมูลส่วนบุคคลได้อย่างไม่มีขอบเขตจำกัด จึงไม่เข้าองค์ประกอบข้อ (2) ที่จะทำให้ประเทศแคนาดาถูกตัดสินว่ามีระดับการคุ้มครองครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ แต่อย่างไรก็ตาม ในปัจจุบันนี้ประเทศแคนาดาได้บัญญัติกฎหมายต่อต้านการก่อการร้าย (Anti-terrorism Act 2015) หรือ Bill C-51 กฎหมายดังกล่าวได้มีการให้อำนาจหน่วยสืบราชการลับของประเทศแคนาดา (Canadian Security Intelligence Service) ในการเข้าถึงและสอดแนมข้อมูลส่วนบุคคลอย่างกว้างขวาง กฎหมายใหม่นี้ยังได้ขยายขอบเขตคำว่าก่อการร้ายให้กว้างขวางขึ้น หน่วยสืบราชการลับมีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลรวมไปถึงการเข้าควบคุมตัวผู้ที่ต้องสงสัยว่าจะเกี่ยวกับการก่อการร้ายได้โดยตรง ไม่ต้องขอหมายศาล รวมถึงอำนาจในการลบข้อมูลใดๆที่เข้าข่ายสนับสนุนผู้ก่อการร้ายจากเว็บไซต์ใดๆก็ได้ กฎหมายเพื่อต่อต้านการก่อการร้ายนี้จึงเป็นกฎหมายที่ให้อำนาจหน่วยงานของรัฐเข้าสอดแนมข้อมูลส่วนบุคคลได้อย่างไม่จำกัด สามารถเก็บรวบรวมและประมวลผลข้อมูลได้ในจำนวนมากและไม่เฉพาะเจาะจงเป้าหมาย จึงเข้าองค์ประกอบข้อ (2) อันเป็นเหตุผลในการตัดสินให้โครงการเซฟฮาร์เบอร์สิ้นผลไปตามคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรป ดังนั้นกฎหมาย PIPEDA ของประเทศแคนาดาจึงมีความเสี่ยงที่จะถูกตัดสินว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอตามมาตรฐานของสหภาพยุโรปเช่นเดียวกัน

นอกจากนี้จากสถานการณ์ปัจจุบันภายในประเทศแคนาดาพบว่ารัฐสภายุโรปเคยมีการตั้งข้อสงสัยต่อประเทศแคนาดาเกี่ยวกับการเข้าร่วมปฏิบัติการสอดแนมข้อมูลขนาดใหญ่ เนื่องจากประเทศแคนาดาเป็นหนึ่งในกลุ่มพันธมิตรเพื่อการสอดแนม 5 ชาติ (Five Eyes) ซึ่งเป็นกลุ่มประเทศที่ให้ความร่วมมือกันในการสอดแนมข้อมูลตามโครงการต่างๆ โดยประเทศแคนาดาให้ความร่วมมือในการเก็บรวบรวมข้อมูลผ่านหน่วยงานด้านความมั่นคงของประเทศแคนาดา (Communications

---

(c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

(I) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,

(II) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law”

Security Establishment Canada หรือ CSEC) หน่วยงานความมั่นคงนี้สามารถดักรับข้อมูลจากองค์กรและบริษัทเอกชนทั่วไป โดยที่ไม่มีการตรวจสอบอย่างเพียงพอโดยกระบวนการศาลและปราศจากสิทธิที่เจ้าของข้อมูลจะได้รับการเยียวยาตามกฎหมาย[43] หากปรากฏหลักฐานข้อเท็จจริงว่าประเทศแคนาดามีโครงการสอดแนมข้อมูลขนาดใหญ่จะยิ่งเป็นการเพิ่มน้ำหนักให้ศาลพิจารณาว่าประเทศแคนาดามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอได้ เหมือนดังเช่นการเปิดเผยของนายเอ็ดเวิร์ด สโนว์เดน เกี่ยวกับโครงการปริซึมในประเทศสหรัฐอเมริกา ทำให้เกิดการร้องเรียนของเจ้าของข้อมูลส่วนบุคคลและนำมาสู่การตัดสินคดีโดยศาลยุติธรรมแห่งสหภาพยุโรปในที่สุด

แม้ว่าการตัดสินของศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14 ไม่ได้มีผลต่อความสิ้นผลของคำวินิจฉัยอื่นๆด้วย แต่อย่างไรก็ตามคำพิพากษานี้เป็นการวางรากฐานแนวความคิดที่สำคัญในการคุ้มครองข้อมูลส่วนบุคคล อีกทั้งยังยืนยันถึงอำนาจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลว่าสามารถรับเรื่องร้องเรียนจากเจ้าของข้อมูลส่วนบุคคลที่คาดว่าข้อมูลส่วนบุคคลของตนได้รับการคุ้มครองที่ไม่เพียงพอเมื่อถูกถ่ายโอนไปยังต่างประเทศได้ ดังนั้นในอนาคตอาจมีผู้ร้องเรียนต่อองค์กรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศสมาชิกสหภาพยุโรปว่าการโอนข้อมูลส่วนบุคคลไปยังประเทศแคนาดาตามคำวินิจฉัยที่ 2002/2 ไม่สามารถให้การคุ้มครองข้อมูลส่วนบุคคลที่เพียงพออีกต่อไปได้เช่นกัน โดยคำวินิจฉัยที่ 2002/2 จะสิ้นผลไปได้ต่อเมื่อมีการตัดสินโดยศาลยุติธรรมแห่งสหภาพยุโรปหรือถูกเพิกถอนโดยคณะกรรมาธิการยุโรปโดยอาศัยเหตุผลตามคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรป[44]

ส่วนแนวทางในการแก้ปัญหาความสิ้นผลไปของโครงการเซฟฮาร์เบอร์ในเบื้องต้นคือให้บริษัทและองค์ต่างๆที่มีความต้องการรับส่งข้อมูลส่วนบุคคลหลังจากวันที่ 6 ตุลาคม ค.ศ. 2015 จะต้องเปลี่ยนไปใช้วิธีการอื่นที่มีความถูกต้องตามกฎหมายแทน เช่น การทำสัญญาแม่แบบ, การทำกฎเกณฑ์ให้ความคุ้มครองที่จัดทำขึ้นในองค์กร (Binding Corporate Rules) เป็นต้น

สำหรับการจัดทำสัญญาแม่แบบได้มีการอธิบายไว้ในบทที่ 3 เรื่องข้อยกเว้นในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศตาม Directive 95/46/EC แล้ว ทั้งนี้ในปัจจุบันมีสัญญาแม่แบบที่

---

[43] Colin Bennett, “Could Europe end up targeting Canada over C-51 and digital privacy,” สืบค้นเมื่อวันที่ 10 มีนาคม 2559, จาก http://ipolitics.ca/2015/10/13/could-europe-end-up-targeting-canada-over-c-51-and-digital-privacy/.

[44] Barry Sookman, “Schrems, what the CJEU decided and why it is a problem for Canadian and other non-EU businesses” สืบค้นเมื่อวันที่ 1 กุมภาพันธ์ 2559, จาก http://www.barrysookman.com/2015/10/12/schrems-what-the-cjeu-decided-and-why-it-is-a-problem-for-canadian-and-other-non-eu-businesses/

คณะกรรมาธิการยุโรปพิจารณาให้ความเห็นชอบหลายฉบับได้แก่[45] (1) สัญญาแม่แบบในการโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลในต่างประเทศ[46] (2) สัญญาแม่แบบในการโอนข้อมูลส่วนบุคคลไปยังผู้ประมวลผลข้อมูลในต่างประเทศ[47]

ส่วนกฎเกณฑ์การให้ความคุ้มครองที่จัดทำขึ้นในองค์กร[48] จะใช้ในกรณีที่องค์กรเดียวกันมีสำนักงานสาขาในหลายประเทศ วิธีการนี้ช่วยลดขั้นตอนและความยุ่งยากในการปฏิบัติตามหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกันในแต่ละประเทศได้ เนื่องจากผู้ที่ต้องการโอนข้อมูลส่วนบุคคลไปยังสำนักงานสาขาที่อยู่ต่างประเทศไม่จำเป็นต้องพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคลในระดับประเทศแต่อย่างใด แต่สามารถพิจารณาเพียงแค่ว่าผู้รับโอนข้อมูลนั้นมีกลไกการคุ้มครองข้อมูลส่วนบุคคลในระดับที่ได้มาตรฐานหรือไม่ แต่อย่างไรก็ตามกลไกหรือนโยบายดังกล่าวจะมีประสิทธิภาพได้ก็ต่อเมื่อมีสภาพบังคับในทางกฎหมาย เช่น ต้องผ่านการพิจารณาให้ความเห็นชอบโดยองค์กรที่ทำหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลเป็นต้น

อย่างไรก็ตามวิธีการข้างต้นเป็นเพียงการแก้ปัญหาจากการสิ้นผลไปของโครงการเซฟฮาร์เบอร์ในระยะสั้นเท่านั้น แต่ปัญหาพื้นฐานที่เกิดขึ้นจากการที่ศาลตัดสินให้โครงการเซฟฮาร์เบอร์สิ้นผลไปยังคงมีอยู่ กลไกการโอนข้อมูลส่วนบุคคลโดยวิธีเหล่านี้ยังมิอาจป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยหน่วยงานด้านความมั่นคงของสหรัฐอเมริกา เนื่องจากบริษัทหรือองค์กรต่างๆเหล่านี้ย่อมต้องผูกพันตามกฎหมายของประเทศสหรัฐอเมริกาอยู่นั่นเอง[49] ฉะนั้นในอนาคตอาจมีกรณีที่หน่วยงาน

---

[45] ปฏิวัติ อุ่นเรือน, “ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ,” (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), น.73.

[46] คำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2001/497 (สัญญารูปแบบที่ 1) และคำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2004/915 (สัญญารูปแบบที่ 2)

[47] คำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2010/87 (ฉบับแทนที่คำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2002/16) โปรดดูรายละเอียดสัญญาที่ http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

[48] ข้อ 29 Working Party. “Transfer of personal data to third countries : Applying Article 26(2) of the E.U. Data Protection Directive to Binding Corporate Rules for International Data Transfers.”

[49] Jens-Henrik Jeppesen, “Replacing the Safe Harbor – Robust privacy protections in a new EU-US data transfer agreement,” สืบค้นเมื่อวันที่ 20 เมษายน 2559, จาก https://cdt.org/blog/replacing-the-safe-harbor-robust-privacy-protections-in-a-new-eu-us-data-transfer-agreement

ด้านการคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศหรือศาลตัดสินให้มีการระงับการโอนข้อมูลส่วนบุคคลไปยังประเทศสหรัฐอเมริกาในวิธีการอื่นได้เช่นกัน

หากศาลระงับมิให้มีการถ่ายโอนข้อมูลจริงความร่วมมือทางเศรษฐกิจระหว่างสหรัฐอเมริกาและสหภาพยุโรปจะเกิดความยุ่งเหยิงขึ้นอย่างมาก บางบริษัทอาจจะต้องทำการปรับโครงสร้างด้านการดำเนินงานครั้งใหญ่ที่ใช้ค่าใช้จ่ายสูงและสิ้นเปลืองเวลาเพื่อที่จะให้บริการแก่ลูกค้าในสหภาพยุโรป และบางบริษัทก็อาจต้องหยุดดำเนินการซึ่งเป็นผลเสียต่อทั้งตัวธุรกิจและผู้ใช้บริการเอง

ฉะนั้นเพื่อเป็นการแก้ปัญหาจากผลกระทบคำพิพากษา C-362/14 ที่เกิดขึ้น และเพื่อเป็นประโยชน์ในด้านความราบรื่นในการถ่ายโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปไปยังประเทศสหรัฐอเมริกาในระยะยาว คณะกรรมาธิการยุโรปและกระทรวงพาณิชย์สหรัฐอเมริกาจึงทำการเจรจาเพื่อทำการหาข้อตกลงฉบับใหม่ที่จะนำมาใช้แทนที่โครงการเซฟฮาร์เบอร์ จนเมื่อวันที่ 2 กุมภาพันธ์ ค.ศ. 2016 จึงเกิดร่างข้อตกลงการโอนข้อมูลรูปแบบใหม่ระหว่างสหภาพยุโรปกับสหรัฐอเมริกาขึ้น โดยใช้ชื่อว่า “EU-U.S. Privacy Shield”[50]

ร่างข้อตกลง EU-U.S. Privacy Shield ได้กำหนดให้บริษัทหรือองค์กรภายในประเทศสหรัฐอเมริกามีข้อผูกพันที่แน่นหนาขึ้นเพื่อจะสามารถคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปที่ถูกถ่ายโอนไปยังประเทศสหรัฐอเมริกาได้ ตามข้อตกลงใหม่นี้เรียกร้องให้สหรัฐอเมริกามีการควบคุมและบังคับใช้กฎหมายอย่างเข้มงวดขึ้น นอกจากนี้ยังมีการเขียนเกี่ยวกับข้อผูกพันและประกันการเข้าถึงข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐอีกด้วย[51]

---

[50] ร่างข้อตกลง EU-U.S. Privacy Shield ฉบับที่มีการอ้างถึงในวิทยานิพนธ์นี้คือร่างข้อตกลงฉบับวันที่ 2 กุมภาพันธ์ ค.ศ. 2016 ซึ่งมิใช่กรอบข้อตกลงฉบับสมบูรณ์และยังไม่ผ่านการรับรองโดยคณะกรรมาธิการยุโรป ทั้งนี้ได้มีกรอบข้อตกลง EU-U.S. Privacy Shield ฉบับที่ผ่านการรับรองโดยคณะกรรมาธิการยุโรปแล้ว เมื่อวันที่ 12 กรกฎาคม ค.ศ. 2016 ผู้อ่านสามารถศึกษารายละเอียดเกี่ยวกับกรอบข้อตกลงดังกล่าวเพิ่มเติมได้ที่ http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.

[51] European Commission, “Press release EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield,” สืบค้นเมื่อวันที่ 15 กุมภาพันธ์ 2559, จาก http://europa.eu/rapid/press-release_IP-16-216_en.htm.

ตามร่างข้อตกลง EU-U.S. Privacy Shield ฉบับวันที่ 2 กุมภาพันธ์ ค.ศ. 2016 สามารถสรุปสาระสำคัญได้ 3 ประการ ดังนี้[52]

(1) เพิ่มมาตรฐานและมาตรการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในสหภาพยุโรปโดยการกำหนดให้บริษัทต่างๆในประเทศสหรัฐอเมริกา ต้องดำเนินการตอบและแก้ไขข้อร้องเรียนภายในระยะเวลาที่กำหนด รวมทั้งบริษัทต่างๆ ต้องจัดให้มีกระบวนการระงับข้อพิพาททั้งทางเลือกและโดยวิธีอนุญาโตตุลาการ

(2) กำหนดให้กระทรวงพาณิชย์สหรัฐอเมริกาและคณะกรรมาธิการการค้าของสหรัฐอเมริกามีหน้าที่ตรวจตราการละเมิดข้อมูลส่วนบุคคลของประชาชนในสหภาพยุโรปและดำเนินการบังคับตามกฎหมายต่อบริษัทหรือองค์กรที่ไม่ปฏิบัติตาม และหากบริษัทใดเก็บข้อมูลส่วนบุคคลของประชาชนในสหภาพยุโรปต้องตกลงปฏิบัติตามคำตัดสินของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทุกประเทศในสหภาพยุโรป

(3) หน่วยงานและองค์กรของประเทศสหรัฐอเมริกาต้องมีการกำหนดข้อจำกัดที่ชัดเจนในการเข้าสอดแนมข้อมูลส่วนบุคคล อีกทั้งยังสร้างวิธีการป้องกันและตรวจสอบการสอดแนมโดยรัฐที่มิชอบโดยกฎหมาย โดยข้อยกเว้นที่อนุญาตให้มีการสอดแนมข้อมูลส่วนบุคคลได้นั้นจะต้องใช้อย่างจำกัด จำเป็น และได้สัดส่วน โดยหน่วยงานของสหรัฐอเมริกาตกลงที่จะประชุมกับสหภาพยุโรปเป็นประจำทุกปีเพื่อแจ้งถึงการดำเนินงานทั้งหมด

หลังจากการทำร่างข้อตกลง EU-U.S. Privacy Shield แล้วเมื่อวันที่ 29 กุมภาพันธ์ ค.ศ. 2016 คณะกรรมาธิการยุโรปได้เปิดเผยร่างคำวินิจฉัยระดับความเพียงพอในการคุ้มครองข้อมูลส่วนบุคคล (Adequacy Decision) และพันธกรณีที่เกี่ยวข้องโดยหน่วยงานของสหรัฐอเมริกาด้วยเพื่อรับรองว่ากรอบข้อตกลง EU-U.S. Privacy Shield มีการรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ หลังจากนั้นคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลซึ่งประกอบด้วยหน่วยงานคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกสหภาพยุโรป 28 ประเทศและที่ปรึกษาการคุ้มครองข้อมูลของยุโรป (European Data Protection Supervisor) จะทำการพิจารณาให้ความเห็นตามข้อ 29 Directive 95/46/EC แต่ถึงแม้ว่าคณะกรรมาธิการยุโรปจะได้อธิบายว่ากรอบข้อตกลง EU-U.S. Privacy Shield และร่างคำวินิจฉัยระดับความเพียงพอในการคุ้มครองข้อมูลส่วนบุคคลได้นำคำพิพากษาของศาลยุติธรรมแห่งสหภาพยุโรปมาปรับใช้ แต่สถานะทางกฎหมายของกรอบความตกลงใหม่นี้จะชัดเจนก็ต่อเมื่อศาลยุติธรรมแห่งสหภาพยุโรปได้ตัดสินชี้ขาดว่าคำวินิจฉัยของ

---

[52] อรรถพล พานิชย์ไพศาลกูล, “EU-U.S. Privacy Shield” กรอบข้อตกลงการโอนข้อมูลระหว่างสหภาพยุโรปและสหรัฐอเมริกาฉบับใหม่,” สืบค้นเมื่อวันที่ 1 มีนาคม 2559, จาก http://ictlawcenter.etda.or.th/contents/detail/article-eu-us-privacy-shield.

คณะกรรมาธิการยุโรปเป็นไปตามกฎหมายของสหภาพยุโรปหรือไม่ เมื่อมีผู้ยื่นฟ้องเช่นเดียวกับกรณีโครงการเซฟฮาร์เบอร์ซึ่งเป็นที่มาของการเจรจาความตกลงฉบับใหม่ดังกล่าว[53]

อย่างไรก็ตามกรอบข้อตกลงใหม่ EU-U.S. Privacy Shield ก็ถูกวิพากษ์วิจารณ์จากนักวิชาการและองค์กรด้านการคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปเช่นกัน แอนนา ฟิลเดอร์ (Anna Fielder) ได้ให้ความเห็นผ่านองค์กรไพรเวซีอินเตอร์เนชันแนล[54] (Privacy International) ว่าโครงการ Privacy Shield นั้นมีช่องโหว่มากมาย[55] เหตุผลประการสำคัญคือประเทศสหรัฐอเมริกาไม่ได้บัญญัติหลักเกณฑ์กฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปหรือมีการปฏิรูปมาตรการคุ้มครองความเป็นส่วนตัวให้มีความเข้มแข็งขึ้น ส่งผลให้เมื่อมีการโอนข้อมูลส่วนบุคคลไปยังประเทศสหรัฐอเมริกา ข้อมูลส่วนบุคคลของพลเมืองยุโรปก็เสี่ยงต่อการถูกรุกล้ำจากระบบสอดแนมของรัฐบาลสหรัฐอเมริกาเช่นเดิม การที่ประเทศสหรัฐอเมริกาไม่มีหลักเกณฑ์ทางกฎหมายเพื่อให้ความคุ้มครองความเป็นส่วนตัวทำให้ในทัศนะของพลเมืองยุโรปนั้นประเทศสหรัฐอเมริกาไม่ได้ให้การคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานเทียบเท่ากับในสหภาพยุโรป

การโอนข้อมูลส่วนบุคคลของกรอบข้อตกลง Privacy Shield นั้น แม้จะมีความพยายามให้การคุ้มครองข้อมูลส่วนบุคคลในการถ่ายโอนจากสหภาพยุโรปไปยังสหรัฐอเมริกามีความแน่นหนาขึ้น แต่ข้อตกลงดังกล่าวก็ยังไม่เพียงพอเนื่องจากไม่สามารถให้ความชัดเจนและไม่มีการคุ้มครองข้อมูลส่วนบุคคลที่หนาแน่นรัดกุมในกรณีที่ข้อมูลส่วนบุคคลได้ถูกถ่ายโอนไปยังประเทศสหรัฐอเมริกา ข้อตกลงนี้ยังคงไม่เป็นไปตามหลักเกณฑ์สำคัญหลายประการที่ตั้งโดยศาลยุติธรรมแห่งสหภาพยุโรป[56] อีกทั้งเมื่อได้วิเคราะห์เทียบสิทธิที่ชาวยุโรปพึงมีภายใต้กฎหมายสหภาพยุโรปมาเทียบกับสิทธิที่ชาวยุโรปมีภายใต้ข้อตกลง Privacy Shield แล้ว จะพบว่าข้อตกลงนี้มีช่องโหว่ที่ชัดเจนมากมาย ภายใต้ข้อตกลง Privacy Shield ชาวยุโรปไม่มีสิทธิบางอย่างที่ปรากฏอยู่ในกฎหมายของสหภาพยุโรป เช่น

(1) ใช้สิทธิอย่างเต็มที่ในการให้ความยินยอมกรณีที่มีการประมวลผลข้อมูลส่วนบุคคลของตน

---

[53] คณะผู้แทนไทยประจำสหภาพยุโรป, “คณะกรรมาธิการยุโรปเผยแพร่สาระสำคัญความตกลง EU – US Privacy Shield,” สืบค้นเมื่อวันที่ 14 เมษายน 2559, จาก http://www2.thaieurope.net/ec-eu-us-privacy-shield-march-2016.

[54] องค์กรไพรเวซีอินเตอร์เนชันแนลคือองค์กรสิทธิมนุษยชนที่ผลักดันและส่งเสริมการคุ้มครองสิทธิในความเป็นส่วนตัวและต่อต้านกับการสอดแนมควบคุมเนื้อหาข้อมูลทั่วโลก

[55] Anna Fielder, “From an unSafe Harbour to a Privacy Shield full of holes,” สืบค้นเมื่อวันที่ 15 เมษายน 2558, จาก http://www.privacyinternational.org/node/832

[56] *เพิ่งอ้าง.*

(2) ใช้สิทธิในการคุ้มครองข้อมูลส่วนบุคคลของตนได้อย่างเต็มที่

(3) ใช้สิทธิในการแก้ไขหรือลบข้อมูลของตนได้อย่างเต็มที่

(4) ใช้สิทธิในการคัดค้านไม่ให้มีการประมวลผลข้อมูลของตนเพื่อผลประโยชน์ทางการค้าโดยตรงได้

(5) มีช่องทางในการร้องเรียนอย่างอิสระและกลไกการแก้ไขที่ง่ายและรวดเร็ว เป็นต้น

ในที่สุดเมื่อวันที่ 14 เมษายน ค.ศ. 2016 คณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลได้ให้ความเห็นยืนยันว่า ความคุ้มครองข้อมูลส่วนบุคคลตามกรอบข้อตกลง Privacy Shield นั้นไม่เพียงพอ[57] ในการแสดงความคิดเห็นของคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลได้แยกออกเป็น 2 ส่วน คือ (1) ส่วนที่เกี่ยวกับการคุ้มครองเจ้าของข้อมูลส่วนบุคคล (2) ส่วนที่เกี่ยวข้องกับหลักประกันการต่อต้านการสอดแนมโดยรัฐอย่างผิดกฎหมาย

ส่วนที่เกี่ยวกับการคุ้มครองเจ้าของข้อมูลส่วนบุคคลนั้น คณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลมีความกังวลที่ตามกรอบข้อตกลงใหม่นั้นหลักคุ้มครองข้อมูลส่วนบุคคลบางประการได้ขาดหายไป เช่น ข้อจำกัดเกี่ยวกับวัตถุประสงค์ในการนำข้อมูลส่วนบุคคลไปใช้ และไม่มีระยะเวลาในการเก็บข้อมูลส่วนบุคคล นอกจากนี้ในภาพรวมแล้วกรอบข้อตกลง Privacy Shield ไม่สามารถให้การคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ อีกทั้งยังให้ความเห็นว่าเพื่อความก้าวหน้าของการค้าและการพัฒนาเศรษฐกิจที่ทันสมัย ประเทศสหรัฐอเมริกาควรออกจากยุคมืด (Dark Ages) และดำเนินการให้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เป็นระบบและเข้มแข็ง

ในส่วนที่เกี่ยวข้องกับการสอดแนมโดยหน่วยงานของรัฐนั้น คณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลได้ตั้งข้อสังเกตว่าข้อตกลงใหม่นี้ให้การคุ้มครองข้อมูลส่วนบุคคลที่อาจถูกเก็บรวบรวมในปริมาณมากและตามอำเภอใจโดยหน่วยงานของรัฐได้ไม่เพียงพอ ทั้งนี้คณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลได้ประเมินจากหลักเกณฑ์พื้นฐานต่อไปนี้คือ กฎเกณฑ์ในการเข้าถึงข้อมูล (accessible rules), หลักความจำเป็นและได้สัดส่วนในการแทรกแซงความเป็นส่วนตัว (necessity and proportionality of the interference with privacy), กลไกการตรวจสอบที่เป็นอิสระ (independent oversight mechanisms) และการเยียวยาที่มีประสิทธิภาพ (effective remedy) หลักการเหล่านี้ได้ฝังอยู่ในหลักสิทธิมนุษยชนยุโรปและกฎหมายของสหภาพยุโรปซึ่งได้สะท้อนผ่านคำตัดสินของศาลยุติธรรมแห่งสหภาพยุโรปนั่นเอง

---

[57] Privacy International, “Press Statement: Data Protection Regulators say Privacy Shield is Not Strong Enough,” สืบค้นเมื่อวันที่ 15 เมษายน 2558 จาก https://www.privacyinternational.org/node/835.

แม้ว่าความเห็นของคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลจะไม่ได้มีสถานะเป็นกฎหมาย แต่ก็มีพื้นฐานมาจากหน่วยงานที่ทำหน้าที่กำกับดูแลข้อมูลส่วนบุคคลในแต่ละประเทศสมาชิก ฉะนั้นจากการให้ความเห็นของคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมาธิการยุโรปควรจะนำกรอบข้อตกลงดังกล่าวไปพิจารณาทบทวนอีกครั้งก่อนจะนำมาบังคับใช้[58]

นอกจากนี้นักวิชาการและองค์กรเกี่ยวกับการคุ้มครองสิทธิในความเป็นส่วนตัวได้มีการเสนอแนะแนวทางการแก้ไขสำหรับกรณีที่โครงการเซฟฮาร์เบอร์ได้ถูกประกาศสิ้นผลไป รวมถึงข้อตกลงใหม่ Privacy Shield ที่ยังเป็นที่ถกเถียงถึงระดับการคุ้มครองข้อมูลส่วนบุคคลว่าไม่เพียงพอ โดยมุ่งเน้นให้ประเทศสหรัฐอเมริกาทำการปฏิรูปกฎหมายภายในให้มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ได้มาตรฐาน

ในการแก้ปัญหาแบบเร่งด่วนชั่วคราวนั้น องค์กรไพรเวซีอินเตอร์เนชันแนลได้เสนอแนะให้ย้อนกลับไปปฏิบัติตามแนวปฏิบัติด้านการคุ้มครองความเป็นส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา[59] ซึ่งแนวปฏิบัตินี้ได้รับการลงนามจากทั้งฝั่งสหภาพยุโรปและประเทศสหรัฐอเมริกา อีกทั้งยังประกอบไปด้วยชุดข้อปฏิบัติที่ให้สิทธิที่จำเป็นในการคุ้มครองข้อมูลส่วนบุคคล

ส่วนในระยะยาวองค์กรไพรเวซีอินเตอร์เนชันแนล[60] สนับสนุนการปฏิรูปกฎหมายที่มาจากข้อเสนอร่วมกันระหว่างที่ปรึกษาทางกฎหมายในเรื่องความเป็นส่วนตัว (Privacy Advocates) และกลุ่มผู้ใช้บริการทั้งจากฝั่งสหรัฐอเมริกาและสหภาพยุโรป สิ่งที่สำคัญประการแรกสุดคือการสร้างพันธกรณีให้ประเทศสหรัฐอเมริกาทำการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎหมายเกี่ยวกับการสอดแนมโดยรัฐ การปฏิรูปนี้มิได้เป็นไปเพียงเพื่อให้ประเทศสหรัฐอเมริกามีการคุ้มครองข้อมูลส่วนบุคคลที่ได้มาตรฐานตามศาลยุติธรรมแห่งสหภาพยุโรป แต่ยังจำเป็นต่อการคุ้มครองความเป็นส่วนตัวของบุคคลทั่วทุกแห่งรวมทั้งคนอเมริกันด้วย

เมื่อวิเคราะห์รายละเอียดกฎหมายเกี่ยวกับการสอดแนมของประเทศสหรัฐอเมริกา นักวิชาการส่วนหนึ่งได้เสนอว่าวิธีแก้ไขที่ครอบคลุมสำหรับประเด็นปัญหาที่ถูกยกขึ้นมาโดยศาลยุติธรรมแห่งสหภาพยุโรป คือการปฏิรูปรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศ โดยเฉพาะ

---

[58] Samuel Gibbs and agencies, “Data regulators reject EU-US Privacy Shield safe harbour deal,” สืบค้นเมื่อวันที่ 15 เมษายน 2558 จาก https://www.theguardian.com/technology/2016/apr/14/data-regulators-reject-eu-us-privacy-shield-safe-harbour-deal

[59] Anna Fielder, *อ้างแล้ว เชิงอรรถที่ 55.*

[60] *เพิ่งอ้าง*.

มาตรา 702 อันเป็นที่มาของปัญหาว่าโครงการปริซึมให้อำนาจหน่วยงานด้านความมั่นคงแห่งชาติเข้าถึงข้อมูลส่วนบุคคลของประชาชนได้อย่างไร้ข้อจำกัด รวมทั้งต้องทบทวนเกี่ยวกับคำสั่งปฏิบัติการที่ 12333 ด้วย โดยประเทศสหรัฐอเมริกาควรต้องทบทวนกฎหมาย ข้อกำหนดและกระบวนการของระบบที่ทำให้โครงการเหล่านี้ไม่โปร่งใส ไม่สามารถอธิบายให้ชัดเจนแก่สาธารณชนได้ กรณีที่เกิดขึ้นถือเป็นความล้มเหลวที่กฎหมายควบคุมการปฏิบัติงานของหน่วยงานทางด้านความมั่นคงแห่งชาติทำให้เกิดคดีดังกล่าวขึ้นและอาจจะทำให้เกิดอีกหลายๆคดีตามมาได้[61]

ในขณะเดียวกันมีข้อเสนอแนะบางส่วนที่เห็นว่าประเทศสหรัฐอเมริกาสามารถดำเนินการยกระดับมาตรการคุ้มครองข้อมูลส่วนบุคคลได้ โดยไม่ต้องมีการปฏิรูปกฎหมายของสหรัฐอเมริกา[62] ยกตัวอย่างเช่น การกำหนดให้บริษัทและองค์กรต่างๆต้องเปิดเผยข้อมูลทางสถิติเกี่ยวกับคำขอในการเข้าถึงหรือสอดแนมข้อมูลส่วนบุคคลโดยรัฐบาลสหรัฐอเมริกาและมีการกำหนดให้การเปิดเผยข้อมูลทางสถิตินั้นเป็นส่วนหนึ่งที่จะต้องรายงานตามกรอบข้อตกลงใหม่ด้วย อีกทั้งควรให้มีการเปิดเผยข้อมูลที่รัฐบาลสหรัฐเมริกาได้ขอหรือผ่านการพิจารณาโดยศาลสืบราชการลับต่างประเทศภายใต้มาตรา 702 แห่งรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศ เป็นต้น

การกำหนดให้มีการเปิดเผยข้อมูลโดยหน่วยสืบราชการลับหรือองค์กรที่ทำหน้าที่เกี่ยวกับความมั่นคงนั้นจะส่งผลให้ขอบเขตการสอดแนมโดยรัฐมีความชัดเจนมากยิ่งขึ้น อีกทั้งควรกำหนดให้มีการชี้แจงเป็นเอกสารเพิ่มเติมที่ระบุเหตุผลว่าทำไมบุคคลนั้นๆจึงถูกกำหนดเป็นเป้าหมายในการสอดแนมโดยเจ้าหน้าที่ของรัฐ การระบุเป้าหมายโดยเฉพาะเจาะจงและให้เหตุผลอย่างชัดเจนจะเป็นการแสดงให้เห็นว่าการเข้าถึงหรือสอดแนมข้อมูลส่วนบุคคลตามมาตรา 702 แห่งรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศได้กระทำไปตามหลักความจำเป็นและได้สัดส่วน มีความเหมาะสมเพียงพอ อันจะก่อให้เกิดความชอบธรรมในการปฏิบัติการมากยิ่งขึ้น

และในที่สุดแล้วกรอบข้อตกลงใหม่อาจต้องกำหนดว่าการสอดแนมหรือตรวจตราภายใต้มาตรา702 แห่งรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศนั้นจะต้องถูกใช้เพื่อความมั่นคงของประเทศสหรัฐอเมริกาและพันธมิตร (Allies) แต่เพียงอย่างเดียว การกำหนดดังกล่าวจะทำให้หน่วยงานด้านความมั่นคงของรัฐไม่สามารถกระทำการที่เกินกว่าเหตุแล้วเป็นการล่วงล้ำสิทธิในความเป็นส่วนตัวได้ ซึ่งจะก่อให้เกิดความชัดเจนและช่วยสร้างเสริมให้การคุ้มครองความเป็นส่วนตัวของพลเมืองในสหภาพยุโรปมีความเข้มแข็งมากยิ่งขึ้น

---

[61] Danny O'Brien, “No Safe Harbor: How NSA Spying Undermined U.S. Tech and Europeans' Privacy,” สืบค้นเมื่อวันที่ 1 กุมภาพันธ์ 2559, จาก https://www.eff.org/th/deeplinks/2015/10/europes-court-justice-nsa-surveilance.

[62] Jens-Henrik Jeppesen, *อ้างแล้ว เชิงอรรถที่ 49.*

อย่างไรก็ตามไม่ใช่เพียงแต่ประเทศสหรัฐอเมริกาเท่านั้น ประเทศต่างๆทั่วโลกก็ควรตระหนักว่าการสอดแนมตรวจตราและเข้าถึงข้อมูลส่วนบุคคลแบบหว่านแห (dragnet) เช่นนี้ เป็นการบั่นทอนความมั่นคงของประเทศและทำให้ระดับความปลอดภัยของข้อมูลส่วนบุคคลทั่วโลกลดลง การกระทำดังกล่าวจะส่งผลกระทบทางเศรษฐกิจ เพราะองค์กรบริษัทต่างๆรวมถึงปัจเจกบุคคลสูญเสียความเชื่อมั่นในผู้ให้บริการทางด้านอินเทอร์เน็ตจนอาจไม่ไว้วางใจในการดำเนินธุรกรรมต่างๆทางอินเทอร์เน็ต และจะส่งผลกระทบในทางการเมืองเพราะแต่ละประเทศแข่งขันกันที่จะเก็บข้อมูลในประเทศของตนให้พ้นจากการสอดแนมโดยประเทศอื่นๆ ในขณะที่พยายามสอดแนมข้อมูลของประเทศอื่นๆโดยหน่วยสืบราชการลับของประเทศตนเช่นกัน

วิธีการที่ดีที่สุดที่จะยับยั้งความขัดแย้งในครั้งนี้โดยที่ยังสามารถดำเนินระบบอินเทอร์เน็ตต่อไปและสามารถคุ้มครองความเป็นส่วนตัวของบุคคลเอาไว้ได้ คือทุกประเทศต้องตกลงกันอย่างชัดเจนว่าการสอดแนมตรวจตราข้อมูลส่วนบุคคลปริมาณมากของประชาชนทั่วไปที่ไม่เข้าข่ายผู้ก่อการร้ายนั้นเป็นการละเมิดสิทธิมนุษยชน ไม่ว่ากระบวนการในการสอดแนมนั้นจะกระทำในหรือนอกเขตแดน สอดแนมชาวต่างชาติหรือคนในประเทศเอง อีกทั้งรัฐบาลต้องควบคุมโครงการสอดแนมข้อมูลเหล่านั้นให้มีการปฏิบัติการอย่างโปร่งใส มีระบบการตรวจสอบที่มีประสิทธิภาพ

บทที่ 5
วิเคราะห์ปัญหาการโอนข้อมูลส่วนบุคคลระหว่างประเทศในต่างประเทศเปรียบเทียบกับกฎหมายไทย

จากพัฒนาการของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศทำให้หลักการคุ้มครองข้อมูลส่วนบุคคลได้เริ่มเป็นระบบแบบแผน มีกลไกในการบังคับใช้ที่มีประสิทธิภาพ รวมทั้งมีการสร้างหลักเกณฑ์ในการโอนข้อมูลไปยังต่างประเทศขึ้นมา ในประเทศที่มีระบบการคุ้มครองข้อมูลส่วนบุคคลมาอย่างยาวนาน ดังเช่นในสหภาพยุโรป เมื่อมีการกำหนดกฎเกณฑ์ทางกฎหมายเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศมาบังคับใช้ในกลุ่มประเทศสมาชิกย่อมเกิดผลกระทบต่อประเทศอื่นๆที่จำเป็นต้องสร้างหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลให้มีระดับการคุ้มครองที่เพียงพอตามมาตรฐานของสหภาพยุโรป โดยระดับความคุ้มครองที่เพียงพอได้กำหนดหลักเกณฑ์ให้มีความชัดเจนขึ้นตามลำดับ ดังจะเห็นได้จากคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดีที่ C-362/14 ที่ศาลวางหลักเกณฑ์ในการพิจารณาระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอเพิ่มขึ้นใหม่

สำหรับประเทศไทยนั้นแม้ว่าการพัฒนาแนวคิดเรื่องสิทธิในความเป็นส่วนตัวกับการคุ้มครองข้อมูลส่วนบุคคลจะมีมาไม่ยาวนานมากนัก แต่สังคมไทยก็เริ่มตื่นตัวและตระหนักถึงความจำเป็นในการคุ้มครองข้อมูลส่วนบุคคลมากขึ้น เหตุเพราะเทคโนโลยีการสื่อสารเจริญก้าวหน้าอย่างรวดเร็วจนทำให้การเข้าถึงข้อมูลส่วนบุคคลเป็นเรื่องที่สะดวกและง่ายดาย การละเมิดสิทธิของบุคคลจึงเพิ่มสูงขึ้นตามไปด้วย แนวคิดเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยจึงเริ่มก่อตัวและเป็นรูปธรรมมากยิ่งขึ้นในปัจจุบัน การศึกษามาตรการในการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยเปรียบเทียบกับปัญหาที่เกิดขึ้นในการโอนข้อมูลส่วนบุคคลตามคดี C-362/14 จึงเป็นเรื่องจำเป็นเพราะจะทำให้ประเทศไทยมีแนวทางในการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สามารถรับโอนข้อมูลจากนานาประเทศได้มากยิ่งขึ้น

5.1 มาตรการทางกฎหมายที่ประเทศไทยใช้ในการคุ้มครองข้อมูลส่วนบุคคลในปัจจุบัน

การบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีพัฒนาการขึ้นตามลำดับ ในยุคแรกประเทศไทยไม่มีการแยกบัญญัติเกี่ยวกับสิทธิในความเป็นส่วนตัวเอาไว้อย่างชัดเจน จนมาถึงรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 สิทธิในความเป็นส่วนตัวจึงเพิ่งได้รับการรับรองและ

คุ้มครองเอาไว้อย่างชัดแจ้งเป็นฉบับแรก[1] และได้รับการรับรองและคุ้มครองต่อมาในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ด้วย อย่างไรก็ตามนอกเหนือจากบทบัญญัติตามรัฐธรรมนูญแล้วกลับพบว่ากฎหมายที่ให้การคุ้มครองข้อมูลส่วนบุคคลรองจากรัฐธรรมนูญยังคงมีลักษณะการบัญญัติเอาไว้กระจัดกระจายและให้การคุ้มครองเฉพาะที่เกี่ยวกับเรื่องนั้นๆ จึงอาจกล่าวได้ว่าในปัจจุบันประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป มีเพียงกฎหมายคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่องเท่านั้น[2]

ทั้งนี้การจำแนกบรรดากฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่ใช้บังคับอยู่ในขณะนี้ นักกฎหมายไทยได้ให้การจำแนกเอาไว้โดยมีหลักเกณฑ์ที่แตกต่างกัน เช่น จันทจิรา เอี่ยมมยุรา[3] ได้แบ่งกฎหมายคุ้มครองส่วนบุคคลไทยออกเป็น 3 กลุ่มใหญ่ และ อีก 1 กลุ่มที่ควรตั้งข้อสังเกตไว้เป็นพิเศษ โดยพิจารณาว่ามีการคุ้มครองข้อมูลส่วนบุคคลเอาไว้อย่างชัดแจ้งหรือไม่เป็นเกณฑ์ในการแบ่ง ดังนี้ 1.กลุ่มกฎหมายที่บัญญัติรับรองคุ้มครองสิทธิในความเป็นส่วนตัวและข้อมูลส่วนบุคคลไว้อย่างชัดแจ้ง 2.กลุ่มกฎหมายที่บัญญัติยกเว้นหลักประกันเรื่องสิทธิส่วนบุคคลไว้อย่างชัดแจ้ง 3.กลุ่มกฎหมายที่การคุ้มครองข้อมูลส่วนบุคคลมิได้ถูกกำหนดไว้อย่างชัดแจ้งแต่แฝงอยู่ในรูปของแนวปฏิบัติในการประกอบวิชาชีพหรือจรรยาวิชาชีพ 4.กลุ่มงานอาชีพหรือกิจกรรมบางประเภทซึ่งเกี่ยวข้องกับการจัดเก็บและใช้ข้อมูลส่วนบุคคล แต่ไม่แน่ชัดว่ามีกฎหมายควบคุมดูแลการปฏิบัติต่อข้อมูลส่วนบุคคลหรือไม่ ส่วนกิตติพงศ์ กมลธรรมวงศ์[4] ได้ใช้เกณฑ์ในเรื่องของลักษณะเนื้อหาและประเภทของข้อมูลส่วนบุคคลแบ่งกฎหมายข้อมูลส่วนบุคคลออกเป็น 6 ลักษณะ ได้แก่ 1.การคุ้มครองโดยกฎหมายประกอบรัฐธรรมนูญและกฎหมายสำคัญที่ออกตามความในรัฐธรรมนูญ 2.การคุ้มครองตามประมวลกฎหมายแพ่งและประมวลกฎหมายอาญาและกฎหมายที่เกี่ยวข้องกับคดีอาญา 3.การคุ้มครองตามกฎหมายปกครองและที่เกี่ยวข้องกับบุคคล 4.การคุ้มครองตามกฎหมายที่เกี่ยวข้องกับการติดต่อสื่อสาร สื่อมวลชนและสถิติ 5.การคุ้มครองตามกฎหมายที่เกี่ยวข้องกับการขออนุมัติอนุญาตการประกอบธุรกิจและกิจการที่เกี่ยวข้องกับการเงินการธนาคารและธุรกรรมทางอิเล็กทรอ

---

[1] จันทจิรา เอี่ยมมยุรา, “การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย,”วารสารนิติศาสตร์, ปีที่ 34 ฉบับที่ 4, น.627 (ธันวาคม 2547).

[2] ปฏิวัติ อุ่นเรือน, “ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ,” (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), น.52.

[3] ศึกษารายละเอียดเพิ่มเติมได้ที่ จันทจิรา เอี่ยมมยุรา, *อ้างแล้ว เชิงอรรถที่ 1*, น.638-651.

[4] ศึกษารายละเอียดเพิ่มเติมได้ที่ กิตติพงศ์ กมลธรรมวงศ์, “การคุ้มครองข้อมูลข่าวสารส่วนบุคคล ในระบบกฎหมายไทย : ปัญหาและแนวทางแก้ไข,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัย ธรรมศาสตร์, 2549), น.246-280.

นิกส์ 6.การคุ้มครองตามกฎหมายที่เกี่ยวข้องกับการควบคุมการประกอบวิชาชีพต่างๆ และ นคร เสรีรักษ์[5] จำแนกข้อมูลส่วนบุคคลออกเป็น 5 ลักษณะ ได้แก่ 1.การคุ้มครองโดยบทบัญญัติรัฐธรรมนูญ 2.การคุ้มครองตามประมวลกฎหมายแพ่งและประมวลกฎหมายอาญา 3.การคุ้มครองตามกฎหมายปกครอง 4.การคุ้มครองตามกฎหมายที่เกี่ยวข้องกับธุรกิจและการเงินการธนาคาร 5.การคุ้มครองตามกฎหมายที่เกี่ยวข้องกับการควบคุมการประกอบวิชาชีพ

ในที่นี้จะขอจำแนกกฎหมายหลักที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยปัจจุบัน โดยแบ่งตามลักษณะของกฎหมายออกเป็นประเภท 3 ประเภทใหญ่ๆ ดังนี้

5.1.1 การคุ้มครองข้อมูลส่วนบุคคลโดยบทบัญญัติของรัฐธรรมนูญ

เมื่อพิจารณาในเชิงสิทธิขั้นพื้นฐานตามรัฐธรรมนูญของประเทศไทยนั้น แม้มีการบัญญัติรับรองเกี่ยวกับสิทธิเสรีภาพของบุคคลตั้งแต่รัฐธรรมนูญฉบับแรก วันที่ 10 ธันวาคม พ.ศ. 2475 มาตรา 14[6] แต่ก็มิได้มีการแยกบัญญัติเรื่องสิทธิในความเป็นส่วนตัวเอาไว้แต่อย่างใด ต่อมารัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2492 ได้รับรองคุ้มครองวัตถุแห่งสิทธิซึ่งจัดรวมอยู่ในสิทธิในความเป็นส่วนตัวเอาไว้ เช่น สิทธิในการติดต่อสื่อสาร ในมาตราที่ 35[7] 40[8] และ สิทธิในครอบครัวตาม

---

[5] ศึกษารายละเอียดเพิ่มเติมได้ที่ นคร เสรีรักษ์, <u>ความเป็นส่วนตัว : ความคิด ความรู้ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย</u>, (กรุงเทพมหานคร : สำนักพิมพ์พีเพรส, 2557), น.241-258.

[6] มาตรา 14 ภายในบังคับแห่งกฎหมายบุคคลย่อมมีเสรีภาพบริบูรณ์ในร่างกาย เคหสถาน ทรัพย์สิน การพูด การเขียน การโฆษณา การศึกษาอบรม การประชุมโดยเปิดเผย การตั้งสมาคม การอาชีพ

[7] มาตรา 35 บุคคลย่อมมีเสรีภาพบริบูรณ์ในการพูด การเขียน การพิมพ์และการโฆษณา การจำกัดเสรีภาพเช่นว่านี้จะกระทำได้ก็แต่โดยบทบัญญัติแห่งกฎหมายเฉพาะเพื่อคุ้มครองเสรีภาพของบุคคลอื่น หรือเพื่อหลีกเลี่ยงภาวะคับขัน หรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเพื่อป้องกันความเสื่อมทรามทางจิตใจของยุวชน

[8] มาตรา 40 บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางไปรษณีย์หรือทางอื่นที่ชอบด้วยกฎหมาย

การตรวจ การกัก หรือการเปิดเผยจดหมาย โทรเลข โทรศัพท์ หรือสิ่งสื่อสารอื่นใดที่บุคคลมีติดต่อถึงกันจะกระทำได้ก็แต่โดยอำนาจตามบทบัญญัติแห่งกฎหมาย

บุคคลย่อมมีสิทธิเสมอภาคในการใช้การสื่อสารที่จัดไว้เป็นบริการสาธารณะ

มาตรา 43[9] เป็นต้น แต่มิได้บัญญัติเกี่ยวกับสิทธิในความเป็นส่วนตัวเอาไว้อย่างชัดแจ้ง

ต่อมารัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 ได้บัญญัติรับรองและคุ้มครองเกี่ยวกับสิทธิในความเป็นส่วนตัวเอาไว้อย่างชัดแจ้งเป็นครั้งแรกในมาตรา 34 ซึ่งบัญญัติว่า “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง... การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีการใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่เป็นกรณีที่เป็นประโยชน์ต่อสาธารณชน” แม้ว่าในรัฐธรรมนูญฉบับนี้จะมิได้กำหนดนิยามหรือให้ความหมายของคำว่าสิทธิในความเป็นส่วนตัวเอาไว้ แต่ก็เป็นการรับรองโดยกฎหมายสูงสุดว่าสิทธิในความเป็นส่วนตัวเป็นสิทธิขั้นพื้นฐาน การละเมิดสิทธิดังกล่าวจะกระทำไม่ได้เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

ล่าสุดรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ได้กำหนดบทบัญญัติเพื่อการรับรองและคุ้มครองสิทธิของบุคคลเอาไว้เช่นเดียวกัน โดยบัญญัติไว้ในมาตรา 4 ความว่า “ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาคของบุคคลย่อมได้รับความคุ้มครอง” ส่วนในมาตรา 35 วรรคหนึ่งและสองได้บัญญัติเกี่ยวกับสิทธิในความเป็นส่วนตัวเอาไว้อย่างชัดแจ้งความว่า “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่เป็นกรณีที่เป็นประโยชน์ต่อสาธารณะ” นอกจากนี้รัฐธรรมนูญฉบับนี้ยังได้กำหนดเกี่ยวกับการคุ้มครองสิทธิในข้อมูลส่วนบุคคลไว้เป็นการเฉพาะอีกด้วย ตามบัญญัติมาตรา 35 วรรคสาม ว่า “บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงหาประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ตามที่กฎหมายบัญญัติ”

ดังนั้นในประเทศไทยสิทธิในข้อมูลส่วนบุคคลได้รับการคุ้มครองโดยรัฐธรรมนูญอันเป็นกฎหมายสูงสุด บุคคลผู้ทรงสิทธิตามที่รัฐธรรมนูญรับรองหรือให้ความคุ้มครองสามารถใช้สิทธิทางศาลได้โดยการกล่าวอ้างบทบัญญัติตามรัฐธรรมนูญในการป้องกันสิทธิเสรีภาพของตน[10] อย่างไรก็ตามแม้จะมีการรับรองสิทธิในความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลเอาไว้ในรัฐธรรมนูญแล้วก็ควรมีกฎหมายที่กำหนดมาตรการและวิธีการต่างๆเพื่อรองรับหลักการตามรัฐธรรมนูญอีกชั้นหนึ่งเช่นกัน เพื่อทำให้การคุ้มครองสิทธิของบุคคลมีประสิทธิภาพและมีแนวทางการปฏิบัติที่ชัดเจน

---

[9] มาตรา 43 สิทธิของบุคคลในครอบครัวย่อมได้รับการคุ้มครอง

[10] บรรเจิด สิงคะเนติ, “หลักประกันสิทธิและเสรีภาพตามรัฐธรรมนูญฉบับใหม่”, วารสารกฎหมายปกครอง, เล่มที่17, ตอนที่2, น.37-38.

5.1.2 การคุ้มครองแบบดั้งเดิมตามประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญา

นอกจากการคุ้มครองโดยรัฐธรรมนูญแล้ว ก่อนมีการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติเฉพาะเรื่องต่างๆ การคุ้มครองข้อมูลส่วนบุคคลในอดีตนั้นเป็นการคุ้มครองตามประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญาเป็นหลัก โดยเป็นการคุ้มครองตามกรอบของกฎหมายว่าด้วยความรับผิดในความเสียหายต่อสิทธิส่วนตัวที่มุ่งคุ้มครองในลักษณะของการแก้ไขเยียวยาเมื่อเกิดความเสียหายต่อสิทธิความเป็นส่วนตัวของบุคคลขึ้นแล้ว[11] เมื่อความเสียหายเกิดขึ้นบุคคลจะต้องฟ้องเป็นคดีแพ่งหรือคดีอาญาต่อศาลยุติธรรมให้ดำเนินการเยียวยาแก้ไขต่อไป

ทั้งนี้การคุ้มครองสิทธิในกฎหมายแพ่งและพาณิชย์จะอยู่ในกฎหมายลักษณะละเมิด ตามมาตรา 420[12] และ 423[13] โดยมาตรา 420 เป็นหลักทั่วไปในความรับผิดทางละเมิดที่ให้บุคคลรับผิดต่อความเสียหายที่ได้ทำต่อสิทธิของบุคคลที่ได้กำหนดไว้ในกฎหมาย ได้แก่ สิทธิในชีวิต ร่างกาย อนามัยเสรีภาพ ทรัพย์สิน หรือสิทธิอย่างใดอย่างหนึ่ง ซึ่งสิทธิในความเป็นส่วนตัวเป็นสิทธิอย่างใดอย่างหนึ่งที่ได้รับการคุ้มครองตามประมวลกฎหมายนี้นั่นเอง

ส่วนการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายอาญาปรากฏอยู่ในประมวลกฎหมายอาญา 2 หมวด[14] คือ หมวด 2 ความผิดฐานเปิดเผยความลับ และ หมวด 3 ความผิดฐาน

---

[11] นคร เสรีรักษ์, ความเป็นส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, (กรุงเทพมหานคร : สำนักพิมพ์พีเพรส, 2557), น.239.

[12] มาตรา 420 ผู้ใดจงใจหรือประมาทเลินเล่อทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างใดอย่างหนึ่งก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น

[13] มาตรา 423 ผู้ใดกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนต่อความจริงเป็นที่เสียหายแก่ชื่อเสียงหรือเกียรติคุณของบุคคลอื่นก็ดีหรือเป็นที่เสียหายแก่ทางทำมาหาได้หรือทางเจริญของเขาโดยประการอื่นก็ดี ท่านว่าผู้นั้นจะต้องใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อความเสียหายอย่างใดๆ อันเกิดแต่การนั้น แม้ทั้งเมื่อตนมิได้รู้ว่าข้อความนั้นไม่จริงแต่หากควรจะรู้ได้

ผู้ใดส่งข่าวสารอันตนมิได้รู้ว่าเป็นความไม่จริง หากว่าตนเองหรือผู้รับข่าวสารนั้นมีทางได้เสียโดยชอบในการนั้นด้วยแล้ว ท่านว่าเพียงที่ส่งข่าวสารเช่นนั้นหาทำให้ผู้นั้นต้องรับผิดใช้ค่าสินไหมทดแทนไม่

[14] นคร เสรีรักษ์, *อ้างแล้ว เชิงอรรถที่ 11*, น.246.

หมิ่นประมาท ในความผิดฐานเปิดเผยความลับนั้นบัญญัติไว้ในมาตรา 322[15] และ 323[16] ซึ่งความรับผิดทางอาญาฐานเปิดเผยความลับนี้มักเกิดขึ้นบ่อยกับลักษณะงานของผู้ประกอบวิชาชีพ ในทางปฏิบัติแล้วบุคคลจะเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ในทางวิชาชีพ เช่น เพื่อประโยชน์ในการรักษาทางการแพทย์ การนำข้อมูลส่วนบุคคลที่ผู้ประกอบวิชาชีพได้ล่วงรู้มาจากเจ้าของข้อมูลส่วนบุคคลไปเปิดเผยแก่บุคคลภายนอกโดยที่เจ้าของข้อมูลส่วนบุคคลไม่อนุญาตจึงเป็นการละเมิดสิทธิส่วนบุคคลตามมาตรา 323 แต่จุดอ่อนของมาตรานี้ คือกรณีเปิดเผยข้อมูลส่วนบุคคลโดยความยินยอมของเจ้าข้อมูลส่วนบุคคลแต่ต่อมาการเปิดเผยได้ก่อให้เกิดความเสียหายขึ้น การกระทำนั้นไม่ผิดตามมาตรา 323[17]

ส่วนความผิดฐานหมิ่นประมาทได้มีการบัญญัติไว้ตามมาตรา 326 ถึง มาตรา 333 ความผิดฐานนี้มีขึ้นเพื่อคุ้มครองเสรีภาพและชื่อเสียงของบุคคล มีมาตราสำคัญที่อธิบายลักษณะ

---

[15] มาตรา 322 ผู้ใดเปิดผนึก หรือเอาจดหมาย โทรเลข หรือเอกสารใด ๆ ซึ่งปิดผนึกของผู้อื่นไป เพื่อล่วงรู้ข้อความก็ดี เพื่อนำข้อความในจดหมาย โทรเลข หรือเอกสารเช่นว่านั้นออกเปิดเผยก็ดี ถ้าการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ

[16] มาตรา 323 ผู้ใดล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น โดยเหตุที่เป็นเจ้าพนักงานผู้มีหน้าที่ โดยเหตุที่ประกอบอาชีพเป็นแพทย์ เภสัชกร คนจำหน่ายยา นางผดุงครรภ์ ผู้พยาบาล นักบวช หมอความ ทนายความ หรือผู้สอบบัญชี หรือโดยเหตุที่เป็นผู้ช่วยในการประกอบอาชีพนั้น แล้วเปิดเผยความลับนั้น ในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ

ผู้รับการศึกษาอบรมในอาชีพดังกล่าวในวรรคแรก เปิดเผยความลับของผู้อื่น อันตนได้ล่วงรู้หรือได้มาในการศึกษาอบรมนั้น ในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษเช่นเดียวกัน

[17] กิตติพันธุ์ เกียรติสุนทร, “มาตรการทางอาญาในการคุ้มครองข้อมูลส่วนบุคคล,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2538), น.34. อ้างถึงในนคร เสรีรักษ์, <u>ความเป็นส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย</u>, (กรุงเทพมหานคร : สำนักพิมพ์พีเพรส, 2557), น.247.

การละเมิดสิทธิความเป็นส่วนตัวที่ถือว่าเป็นการหมิ่นประมาท ได้แก่ มาตรา 326[18] 327[19] และ 328[20] ซึ่งความรับผิดฐานหมิ่นประมาทนั้นมีการเปิดโอกาสให้พิสูจน์ ถ้าหากพิสูจน์ได้ว่าการกล่าวข้อเท็จจริงนั้นเข้าข้อยกเว้นที่กฎหมายกำหนด ก็ไม่ถือเป็นการหมิ่นประมาท ข้อยกเว้นดังกล่าวนั้นได้แก่ การแสดงความคิดเห็นหรือข้อความโดยสุจริต การติชมด้วยความเป็นธรรมซึ่งในวิสัยของประชาชนย่อมกระทำ เป็นต้น

ทั้งนี้จันทจิรา เอี่ยมมยุรา ได้ให้ข้อสังเกตเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญาเอาไว้โดยสรุปได้ดังนี้[21]

(1) ประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญาเป็นกฎหมายที่คุ้มครองสิทธิในข้อมูลส่วนบุคคลในฐานะที่เป็นสิทธิส่วนตัวทั่วไปเช่นเดียวกับสิทธิอื่นๆ เช่น สิทธิในทรัพย์สิน ร่างกาย อนามัย โดยไม่ได้มุ่งคุ้มครองเฉพาะเรื่องข้อมูลส่วนบุคคลโดยตรง ทั้งๆที่สาระสำคัญแห่งสิทธิประเภทอื่นกับสิทธิในข้อมูลส่วนบุคคลมีลักษณะแตกต่างกัน อีกทั้งบุคคลจะได้รับการคุ้มครองสิทธิตามประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญาเมื่อเกิดความเสียหายขึ้นแล้ว การชดใช้ค่าความเสียหายที่เกิดขึ้นจึงเป็นมาตรการเยียวยาความเสียหาย

---

[18] มาตรา 326 ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สามโดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นหรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือ ปรับไม่เกินสองหมื่นบาทหรือทั้งจำทั้งปรับ

[19] มาตรา 327 ผู้ใดใส่ความผู้ตายต่อบุคคลที่สามและการใส่ความนั้นน่าจะเป็นเหตุให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่นหรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท ต้องระวางโทษดังบัญญัติไว้ใน มาตรา 326 นั้น

[20] มาตรา 328 ถ้าความผิดฐานหมิ่นประมาทได้กระทำโดยการโฆษณา ด้วยเอกสาร ภาพวาด ภาพระบายสี ภาพยนตร์ ภาพหรือตัวอักษรที่ ทำให้ปรากฏด้วยวิธีใด ๆ แผ่นเสียง หรือสิ่งบันทึกเสียง บันทึกภาพ หรือบันทึกอักษร กระทำโดยการกระจายเสียง หรือการกระจายภาพ หรือโดยกระทำการป่าวประกาศด้วยวิธีอื่น ผู้กระทำต้องระวางโทษ จำคุกไม่เกินสองปีและปรับไม่เกินสองแสนบาท

[21] จันทจิรา เอี่ยมมยุรา, “กฎหมายเกี่ยวกับข้อมูลส่วนบุคคลในประเทศไทย,” รายงานการวิจัยโครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคล และจัดทำคู่มือปฏิบัติงานเกี่ยวกับข้อมูลข่าวสารส่วนบุคคลภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (กรุงเทพมหานคร : สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2547) น.6.

มากกว่าการป้องกัน ซึ่งจะขัดแย้งกับหลักการคุ้มครองข้อมูลส่วนบุคคลตามระบบกฎหมายของประเทศต่างๆที่มุ่งจะให้การคุ้มครองในลักษณะการป้องกัน

(2) กฎหมายทั้งสองฉบับผลักภาระการพิสูจน์ไปให้แก่ผู้เสียหาย เว้นแต่จะมีบทกฎหมายเฉพาะบัญญัติไว้เป็นอย่างอื่นหรือบัญญัติคุ้มครองสิทธิในข้อมูลส่วนบุคคลเป็นการเฉพาะ

(3) กฎหมายทั้งสองฉบับยังขาดบทบัญญัติเกี่ยวกับหลักเกณฑ์ วิธีการ เงื่อนไข และมาตรการที่จำเป็นและเฉพาะเจาะจงเพื่อให้หลักประกันในการคุ้มครองสิทธิได้อย่างเพียงพอตามหลักสากล

5.1.3 การคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่องตามพระราชบัญญัติต่างๆ

ก่อนปี พ.ศ. 2540 ประเทศไทยยังมิได้ตระหนักถึงความจำเป็นในการคุ้มครองข้อมูลส่วนบุคคลมากนัก ความคุ้มครองส่วนใหญ่เป็นไปตามประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญาซึ่งเป็นเพียงมาตรการเยียวยาหลังจากความเสียหายเกิดขึ้นแล้วจึงไม่สามารถคุ้มครองสิทธิในข้อมูลส่วนบุคคลได้อย่างครอบคลุมทุกแง่มุม ส่วนพระราชบัญญัติต่างๆที่บัญญัติขึ้นไม่ได้มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคลเป็นหลักและมักบัญญัติขึ้นเพื่อให้ควบคุมและกำกับดูแลหน่วยงานของรัฐที่ทำหน้าที่เก็บรักษาและควบคุมดูแลข้อมูลส่วนบุคคลเป็นเรื่องๆไป เช่น พระราชบัญญัติไปรษณีย์ พ.ศ. 2477 มีการบัญญัติเกี่ยวกับการมิให้เปิดถุงไปรษณีย์ หรือไปรษณียภัณฑ์ในระหว่างส่งทางไปรษณีย์ พระราชบัญญัติการทะเบียนราษฎร พ.ศ. 2534 ที่ให้ความคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคลที่จัดเก็บและครอบครองโดยนายทะเบียนราษฎรของรัฐ เป็นต้น จึงอาจกล่าวได้ว่าก่อน พ.ศ. 2540 นั้นประเทศไทยยังไม่มีระบบในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล

จนเมื่อปี พ.ศ. 2540 ได้มีการบังคับใช้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งถือเป็นจุดเริ่มต้นสู่การพัฒนาระบบการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ประกอบกับความจำเป็นในเรื่องของการคุ้มครองสิทธิของบุคคลที่อาจถูกละเมิดจากความเจริญก้าวหน้าทางเทคโนโลยีสมัยใหม่ทำให้กฎหมายที่บัญญัติต่อๆมาเริ่มให้ความสำคัญกับสิทธิในความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลมากยิ่งขึ้น แต่อย่างไรก็ตามการคุ้มครองตามพระราชบัญญัติต่างๆยังมีลักษณะกระจัดกระจายเฉพาะเรื่องนั้นๆ ไม่ได้ครอบคลุมระบบในการคุ้มครองข้อมูลส่วนบุคคลในภาพรวม เช่นพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีการให้ความคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐเท่านั้น พระราชบัญญัติฟื้นฟูสมรรถภาพผู้ติดยาเสพติด พ.ศ. 2545 มุ่งคุ้งครองมิให้นำข้อมูลส่วนบุคคลของผู้ติดยาเสพติดไปเปิดเผยต่อ พระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 มุ่งคุ้มครองมิให้เปิดเผยข้อมูลของเด็ก พระราชบัญญัติโรงแรมพ.ศ. 2547 ก็มุ่งคุ้มครองข้อมูลของผู้พักในการประกอบกิจการโรงแรม เป็นต้น จะเห็นได้ว่ามีพระราชบัญญัติจำนวนมากที่มีการบัญญัติเพื่อคุ้มครองข้อมูลเฉพาะเรื่องนั้นๆใน

บางมาตรา ในที่นี้จึงขอยกพระราชบัญญัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่มีความสำคัญในปัจจุบันมาพอสังเขป เพื่อให้เห็นเนื้อหาและลักษณะการคุ้มครองข้อมูลส่วนบุคคลที่กระจายอยู่ในกฎหมายต่างๆดังนี้

5.1.3.1 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

พัฒนาการสำคัญที่ส่งผลต่อระบบการคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นเมื่อมีการบัญญัติพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 โดยกฎหมายฉบับนี้มีผลบังคับใช้เมื่อพ้นกำหนด 90 วันนับแต่วันที่ประกาศในราชกิจจานุเบกษา คือวันที่ 9 ธันวาคม พ.ศ. 2540 เป็นต้นมา พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ถือเป็นกฎหมายฉบับแรกของประเทศไทยที่บัญญัติให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของรัฐในลักษณะเป็นกฎหมายกลาง อีกทั้งยังเป็นกฎหมายฉบับเดียวในประเทศไทยในขณะนี้ที่ให้คำนิยามของ “ข้อมูลส่วนบุคคล” เอาไว้ตามมาตรา 4[22] โดยใช้คำว่าข้อมูลข่าวสารส่วนบุคคล

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีขอบเขตการคุ้มครองเฉพาะข้อมูลส่วนบุคคลที่จัดเก็บและอยู่ในความครอบครองของราชการ โดยไม่ครอบคลุมถึงข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของเอกชน โดยให้ความคุ้มครองทั้งการจัดเก็บข้อมูลที่กระทำโดยบุคคลและจัดเก็บโดยระบบอัตโนมัติคอมพิวเตอร์ นอกจากนี้กฎหมายดังกล่าวยังมีความสำคัญเนื่องจากได้บัญญัติเกี่ยวกับการควบคุมการปฏิบัติการจัดระบบข้อมูลส่วนบุคคลครบทั้งวงจร[23] ตั้งแต่

(1) ให้ระบุแหล่งข้อมูล

(2) ให้ระบุประเภทของบุคคลที่มีการเก็บข้อมูลและประเภทของระบบข้อมูล

(3) ให้ระบุลักษณะการใช้ข้อมูลตามปกติ

(4) ให้ระบุวิธีการขอตรวจดูข้อมูล และการขอแก้ไขข้อมูลของเจ้าของข้อมูล

---

[22] มาตรา 4 ... ข้อมูลข่าวสารส่วนบุคคล หมายความว่าข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือ ประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีหมายเลข รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมทั้งข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

[23] จันทจิรา เอี่ยมมยุรา, *อ้างแล้ว เชิงอรรถที่ 1*, น.641.

(5) กำหนดหลักการเก็บข้อมูลโดยตรงจากเจ้าของข้อมูล วิธีการเก็บ และการเก็บเท่าที่จำเป็นเพื่อให้สำเร็จตามวัตถุประสงค์

(6) ให้มีระบบรักษาความปลอดภัยของข้อมูล

(7) กำหนดหลักการใช้และเปิดเผยข้อมูลเฉพาะเมื่อได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูล เว้นแต่จะเข้าข้อยกเว้นที่กฎหมายกำหนดไว้โดยชัดแจ้ง

นอกจากนี้กฎหมายยังกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่สำคัญ 2 ประการ คือ สิทธิในการเข้าถึงและรับทราบข้อมูลส่วนบุคคลเกี่ยวกับตนตามมาตรา 25 วรรคหนึ่ง[24] และ สิทธิที่จะขอเปลี่ยนแปลงข้อมูลส่วนบุคคลให้ถูกต้องตรงตามความเป็นจริงตามมาตรา 25 วรรคสามและสี่[25]

องค์กรที่มีหน้าที่ควบคุมและบังคับการให้เป็นไปตามกฎหมายตามพระราชบัญญัตินี้คือคณะกรรมการข้อมูลข่าวสารของราชการ โดยมีหน้าที่ที่สำคัญได้แก่ (1) สอดส่องดูแลและให้ปรึกษาเกี่ยวกับการดำเนินงานของเจ้าหน้าที่ของรัฐและหน่วยงานของรัฐเพื่อปฏิบัติการให้เป็นไปตามกฎหมาย (2) เสนอแนะในการตราพระราชกฤษฎีกาและการออกกฎกระทรวงหรือระเบียบของคณะรัฐมนตรี (3) พิจารณาอุทธรณ์ของเจ้าของข้อมูล ในกรณีที่หน่วยงานของรัฐไม่แก้ไขเปลี่ยนแปลงตามที่ผู้นั้นร้องขอ

---

[24] มาตรา 25 วรรคหนึ่ง ภายใต้บังคับมาตรา 14 และมาตรา 15 บุคคลย่อมมีสิทธิที่จะได้รู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น และให้นำมาตรา 9 วรรคสอง และวรรคสามมาใช้บังคับโดยอนุโลม

[25] มาตรา 25 วรรคสามและสี่ ถ้าบุคคลใดเห็นว่าข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้องตามที่เป็นจริง ให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนนั้นได้ซึ่งหน่วยงานของรัฐจะต้องพิจารณาคำขอดังกล่าว และแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า

ในกรณีที่หน่วยงานของรัฐไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารให้ตรงตามที่มีคำขอ ให้ผู้นั้นมีสิทธิอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายในสามสิบวันนับแต่วันได้รับแจ้งคำสั่งไม่ยินยอมแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสาร โดยยื่นคำอุทธรณ์ต่อคณะกรรมการ และไม่ว่ากรณีใด ๆ ให้เจ้าของข้อมูลมีสิทธิร้องขอให้หน่วยงานของรัฐหมายเหตุคำขอของตนแนบไว้กับข้อมูลข่าวสารส่วนที่เกี่ยวข้องได้

อย่างไรก็ตามจันทจิรา เอี่ยมมยุรา ได้ให้ข้อสังเกตเกี่ยวกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เอาไว้โดยสรุปว่า[26]

(1) ขอบเขตของกฎหมายนี้ไม่คุ้มครองระบบการจัดเก็บและการใช้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานภาคเอกชน

(2) คณะกรรมการข้อมูลข่าวสารของราชการไม่มีอำนาจในการสืบสวนสอบสวนการกระทำที่ฝ่าฝืนการคุ้มครองข้อมูลส่วนบุคคล (investigation power) อย่างเช่นอำนาจของ ป.ป.ช. ในเรื่องของการทุจริตคอร์รัปชั่นในภาครัฐ ซึ่งส่วนใหญ่องค์กรนี้ในต่างประเทศมีอำนาจ

(3) คณะกรรมการข้อมูลข่าวสารของราชการไม่มีอำนาจในการให้ความเห็นชอบประมวลหรือกฎเกณฑ์เกี่ยวกับจริยธรรมในวิชาชีพขององค์กรวิชาชีพที่จัดตั้งขึ้นตามกฎหมาย แม้ว่าจะมีอำนาจในการควบคุมดูแลองค์กรทางวิชาชีพด้วยก็ตาม

5.1.3.2 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

พระราชบัญญัติฉบับนี้มีวัตถุประสงค์เพื่อควบคุมบริษัทข้อมูลเครดิต ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลในการจัดระบบการจัดข้อมูลสินเชื่อหรือข้อมูลเครดิตส่วนบุคคล การตรวจสอบความน่าเชื่อถือเพื่อพิจารณาการอนุมัติสินเชื่อของสถาบันการเงินต่างๆ โดยอาศัยข้อมูลเครดิตที่ได้รับการเก็บไว้โดยผู้ให้บริการข้อมูลและผู้ให้บริการสินเชื่อ[27]

ขอบเขตของพระราชบัญญัตินี้มุ่งคุ้มครองเฉพาะข้อมูลเครดิตหรือข้อมูลส่วนบุคคลที่เกี่ยวกับสินเชื่อของผู้ขอสินเชื่อจากสถาบันการเงินไม่รวมถึงข้อมูลส่วนบุคคลประเภทอื่นๆ จึงเป็นกฎหมายที่ให้การคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่อง ไม่ใช่กฎหมายที่คุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป แต่อย่างไรก็ดีกฎหมายฉบับนี้เป็นกฎหมายฉบับแรกที่พยายามวางหลักเกณฑ์เพื่อคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในภาคเอกชน[28]

กฎหมายฉบับนี้มีสาระสำคัญในการมุ่งควบคุมและคุ้มครองข้อมูลส่วนบุคคลที่เป็นข้อมูลสินเชื่อหรือข้อมูลเครดิตหลายประการ เช่น[29]

(1) มีการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขเกี่ยวกับระบบในการรวบรวม เก็บรักษา แก้ไขข้อมูล การเปิดเผย การทำลายข้อมูล ฯลฯ เห็นได้จากการกำหนดนิยามคำว่าการประมวลผลข้อมูล

---

[26] จันทจิรา เอี่ยมมยุรา, *อ้างแล้ว เชิงอรรถที่ 21*, น.9.

[27] นคร เสรีรักษ์, *อ้างแล้ว เชิงอรรถที่ 11*, น.255.

[28] *เพิ่งอ้าง*, น. 257.

[29] จันทจิรา เอี่ยมมยุรา, *อ้างแล้ว เชิงอรรถที่ 1*, น.644.

(2) การบัญญัติห้ามจัดเก็บข้อมูลที่ไม่เกี่ยวกับการรับบริการหรือการขอสินเชื่อหรือข้อมูลบางอย่างโดยชัดแจ้ง ตามมาตรา 10 หรือห้ามประมวลผลข้อมูลที่มีอายุเกินกว่าที่คณะกรรมการกำหนด ตามมาตรา 13

(3) การกำหนดให้มีการรักษาความลับ ความปลอดภัย เพื่อป้องกันการนำข้อมูลไปใช้ผิดวัตถุประสงค์ หรือป้องกันการแก้ไข การทำให้เสียหาย การเปิดเผยต่อบุคคลอื่นโดยมิได้รับอนุญาต

(4) มีการรับรองหลักการแนวคิดที่เป็นสากลเกี่ยวกับการใช้หรือเปิดเผยข้อมูลเครดิต กล่าวคือผู้ประกอบการต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูล ยกเว้นเข้าข้อยกเว้นตามกฎหมาย โดยผู้ประการจะต้องแจ้งเป็นหนังสือให้เจ้าของข้อมูลทราบถึงการเปิดเผยดังกล่าวภายใน 30 วัน นับแต่วันที่ได้เปิดเผยข้อมูลตามมาตรา 20

สำหรับสิทธิของเจ้าของข้อมูลเครดิตนั้น ได้มีการให้ความคุ้มครองไว้ตามบทบัญญัติในมาตรา 25 ดังนี้

(1) สิทธิที่จะรับรู้ว่าบริษัทข้อมูลเครดิตเก็บรักษาข้อมูลใดของตน

(2) สิทธิที่จะตรวจสอบข้อมูลของตน

(3) สิทธิที่จะขอแก้ไขข้อมูลที่ไม่ถูกต้อง

(4) สิทธิที่จะโต้แย้งเมื่อทราบว่าข้อมูลของตนไม่ถูกต้อง

(5) สิทธิที่จะได้รับแจ้งผลการตรวจสอบข้อมูลของตนภายในระยะเวลาที่กำหนด

(6) สิทธิที่จะได้รับทราบเหตุแห่งการปฏิเสธคำขอสินเชื่อหรือบริการจากสถาบันการเงิน ในกรณีที่สถาบันการเงินใช้ข้อมูลของบริษัทข้อมูลเครดิตมาเป็นเหตุแห่งการปฏิเสธคำขอสินเชื่อหรือบริการ

(7) สิทธิที่จะอุทธรณ์ต่อคณะกรรมการคุ้มครองข้อมูลเครดิต

ทั้งนี้จันทจิรา เอี่ยมมยุราได้ให้ข้อสังเกตและข้อคิดเห็นเกี่ยวกับพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 เอาไว้ดังนี้[30]

(1) กฎหมายฉบับนี้แม้ว่าจะครอบคลุมหลักเกณฑ์ วิธีการ และกระบวนการในการคุ้มครองและควบคุมการใช้ข้อมูลส่วนบุคคลของผู้ขอสินเชื่อ ซึ่งควบคุมทั้งหน่วยงานภาครัฐและเอกชนก็ตาม แต่ก็มีฐานะเพียงกฎหมายที่คุ้มครองเฉพาะเรื่องข้อมูลส่วนบุคคลทางการเงินสินเชื่อเท่านั้น

---

[30] จันทจิรา เอี่ยมมยุรา, *อ้างแล้ว เชิงอรรถที่ 1*, น.645.

(2) กฎหมายฉบับนี้กำหนดให้ธนาคารแห่งประเทศไทยมีฐานะเป็นผู้เสียหาย ตามประมวลกฎหมายวิธีพิจารณาความอาญาแทนผู้เสียหายที่แท้จริง แต่ไม่ตัดสิทธิบุคคลธรรมดาที่เป็นผู้เสียหายที่แท้จริงในการฟ้องร้องผู้กระทำละเมิด

(3) กฎหมายฉบับนี้บัญญัติความผิดที่กระทำต่อข้อมูลในระบบความจำของคอมพิวเตอร์เป็นกรณีพิเศษ แสดงให้เห็นว่ากฎหมายฉบับนี้ให้ความสำคัญกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ นอกเหนือจากระบบประมวลผลด้วยมือ

นอกจากนี้ยังมีกลุ่มพระราชบัญญัติที่ไม่ได้บัญญัติคุ้มครองข้อมูลส่วนบุคคลเอาไว้อย่างชัดแจ้งในบทบัญญัติ แต่ปรากฏเป็นแนวประพฤติปฏิบัติทั่วไปในการประกอบวิชาชีพหรือที่เรียกว่าจรรยาบรรณหรือจริยธรรมแห่งวิชาชีพ การคุ้มครองข้อมูลส่วนบุคคลที่เป็นไปตามจรรยาบรรณวิชาชีพนั้นมักเป็นกลุ่มอาชีพซึ่งโดยสภาพมักจะสามารถล่วงรู้ข้อมูลส่วนบุคคลของบุคคลอื่นได้[31] ยกตัวอย่างเช่น กลุ่มพระราชบัญญัติเกี่ยวกับวิชาชีพทางเวชกรรม ทันตกรรม เภสัชกรรม วิชาชีพการพยาบาลการผดุงครรภ์ พระราชบัญญัติผู้สอบบัญชี พ.ศ. 2505 พระราชบัญญัติทนายความ พ.ศ. 2528 เป็นต้น

ในภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยมีการบัญญัติกฎหมายกระจัดกระจายอยู่ตามพระราชบัญญัติเฉพาะต่างๆ การคุ้มครองข้อมูลส่วนบุคคลมิได้ถูกบัญญัติไว้บนกฎหมายฉบับเดียว จึงกล่าวได้ว่าในปัจจุบันนี้ยังไม่มีกฎหมายกลางที่วางหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป แม้ว่ากฎหมายข้อมูลข่าวสารของราชการจะมีความโน้มเอียงในการเป็นกฎหมายกลางที่พยายามวางหลักเกณฑ์ทั่วไปในการคุ้มครองข้อมูลส่วนบุคคล แต่การคุ้มครองข้อมูลดังกล่าวก็ครอบคลุมเฉพาะข้อมูลที่อยู่ในความครอบครองของหน่วยงานของรัฐเท่านั้น กฎหมายนี้จึงมีข้อจำกัดในการคุ้มครองข้อมูลส่วนบุคคลส่วนบุคคลที่ทำให้ข้อมูลที่อยู่ในความครอบครองของภาคเอกชนไม่ได้รับการคุ้มครอง

สภาพของกฎหมายไทยที่ไม่ครอบคลุมข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชนถือเป็นปัญหาสำคัญยิ่งในระบบการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากข้อมูลส่วนบุคคลที่อยู่ในภาคเอกชนมีปริมาณข้อมูลที่ถูกจัดเก็บปริมาณมาก การไม่มีกฎหมายกลางบังคับใช้เป็นการทั่วไปย่อมก่อให้เกิดช่องว่างในการบังคับใช้ที่ทำให้ข้อมูลส่วนบุคคลบางประเภทมิได้รับการคุ้มครองโดยกฎหมาย ครั้นจะให้ได้รับการคุ้มครองตามประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญาก็จะต้องมีความเสียหายเกิดขึ้นก่อนแล้วจึงเยียวยาในภายหลัง ซึ่งขัดกับหลักในการคุ้มครองข้อมูลส่วนบุคคลในประเทศต่างๆที่เป็นสากล ที่มุ่งคุ้มครองข้อมูลส่วนบุคคลในลักษณะป้องกันก่อนความเสียหายจะบังเกิดขึ้น ดังนั้นสภาพของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของ

---

[31] จันทจิรา เอี่ยมมยุรา, *อ้างแล้ว เชิงอรรถที่ 1*, น.650.

ประเทศไทยจึงมีความลักลั่น สิทธิของบุคคลตามรัฐธรรมนูญในเรื่องข้อมูลส่วนบุคคลจึงอยู่ในสภาพที่ได้รับการคุ้มครองไม่ครบวงจร

ด้วยความจำเป็นดังกล่าวประเทศไทยจึงมีความพยายามในการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เป็นกฎหมายกลางขึ้น โดยการยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เพื่อใช้คุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป ปัจจุบันนี้ร่างกฎหมายดังกล่าวได้ผ่านการพิจารณาของคณะกรรมการกฤษฎีกาแล้ว การศึกษาร่างพระราชบัญญัติดังกล่าวจึงมีความจำเป็นเพื่อทำให้เข้าใจภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยในอนาคต

5.2 มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

5.2.1 แนวคิดและความเป็นมาในการยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

เมื่อการคุ้มครองข้อมูลส่วนบุคคลตามระบบกฎหมายไทยไม่ได้ถูกกำหนดเอาไว้ในกฎหมายเพียงฉบับเดียว แต่กระจัดกระจายอยู่ตามกฎหมายเฉพาะต่างๆ ส่งผลให้ยังคงมีข้อมูลส่วนบุคคลอีกจำพวกหนึ่งที่ไม่ได้อยู่ภายใต้บังคับพระราชบัญญัติฉบับดังกล่าว ซึ่งก็คือข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชนนั่นเอง

สถานการณ์ดังกล่าวได้ก่อให้เกิดช่องว่างของการบังคับใช้กฎหมายที่ไม่ครอบคลุมข้อมูลส่วนบุคคลทั้งหมด ซึ่งเป็นปัญหาสำคัญประการแรกของการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยเนื่องจากข้อมูลส่วนบุคคลที่ได้รับการจัดเก็บอยู่ในภาคเอกชนมีปริมาณมาก อีกทั้งมีความสำคัญของข้อมูลไม่ยิ่งหย่อนไปกว่าข้อมูลของภาครัฐ เช่นข้อมูลในโรงพยาบาลเอกชน ข้อมูลพนักงานลูกจ้างในบริษัทห้างร้านต่างๆ ข้อมูลสมาชิกกิจกรรมทางธุรกิจต่างๆเป็นต้น ซึ่งหากไม่มีการบัญญัติกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปก็จะก่อให้เกิดการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล ซึ่งทำให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลตามมา

ประการที่สอง ความก้าวหน้าด้านวิทยาศาสตร์และเทคโนโลยีในยุคโลกาภิวัตน์ทำให้เกิดพัฒนาการที่ไร้ขีดจำกัดในการติดต่อสื่อสาร จากการใช้เทคโนโลยีคอมพิวเตอร์และอินเทอร์เน็ต การสื่อสารผ่านดาวเทียม ทำให้แต่ละวันนั้นมีการถ่ายโอนแลกเปลี่ยนข้อมูลกันเป็นจำนวนมหาศาล และท่ามกลางการแข่งขันทางเศรษฐกิจที่ผู้ผลิตมุ่งหมายครอบครองส่วนแบ่งทางการตลาดให้มากที่สุด ฝ่ายใดมีข้อมูลมากย่อมได้เปรียบกว่าผู้อื่น ส่งผลให้บริษัทเอกชนต้องการที่จะได้ข้อมูลของผู้บริโภคให้มากที่สุดเพื่อใช้ในการศึกษาวิจัยทางการตลาด หากไม่มีกฎหมายที่ให้ความ

คุ้มครองข้อมูลส่วนบุคคลจะทำให้เกิดการนำข้อมูลไปใช้เกินขอบเขตและส่งผลเสียต่อผู้เป็นเจ้าของข้อมูลได้ ยิ่งเทคโนโลยีเจริญก้าวหน้าขึ้นความเสียหายจากการละเมิดสิทธิในข้อมูลส่วนบุคคลย่อมเพิ่มมากขึ้นตามไปด้วย

ประการที่สาม กระแสของนานาประเทศที่ให้ความสำคัญในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล กฎหมายของต่างประเทศโดยเฉพาะกลุ่มประเทศที่พัฒนาแล้วมักมีการบัญญัติกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลขึ้นเป็นการเฉพาะ หากกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยไม่มีมาตรฐานการคุ้มครองที่เพียงพอในมุมมองของต่างประเทศ จะส่งผลกระทบต่อการรับโอนข้อมูลส่วนบุคคลจากต่างประเทศให้ถูกจำกัดห้ามรับโอนข้อมูลได้ดังที่ได้กล่าวมาแล้วในบทก่อนๆ ซึ่งเหตุนี้เองจะเป็นอุปสรรคหากประเทศไทยต้องติดต่อธุรกิจการค้าระหว่างประเทศในอนาคต เนื่องจากบริษัทที่เข้ามาลงทุนทำธุรกิจจากต่างประเทศอาจกังวลและไม่ให้ความเชื่อมั่นว่าประเทศไทยจะสามารถให้การคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพเพียงพอ

จากสภาพปัญหาที่จะเกิดขึ้นข้างต้น ภาครัฐจึงมีความจำเป็นต้องบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เป็นกฎหมายกลาง ใช้บังคับกับข้อมูลโดยทั่วไปได้ เพื่อเป็นการแก้ไขช่องว่างของกฎหมายและจัดระบบการคุ้มครองข้อมูลส่วนบุคคลให้ได้มาตรฐานเฉกเช่นเดียวกับการคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศที่ได้พัฒนามาก่อน

จุดเริ่มต้นในการคุ้มครองข้อมูลส่วนบุคคลเริ่มปรากฏอย่างเป็นรูปธรรมจากมติคณะรัฐมนตรี เมื่อวันที่ 28 กุมภาพันธ์ พ.ศ. 2539 ที่ได้เห็นชอบต่อนโยบายเทคโนโลยีสารสนเทศที่เสนอโดยกระทรวงวิทยาศาสตร์และเทคโนโลยีสิ่งแวดล้อมซึ่งมีจุดมุ่งหมายสำคัญเพื่อพัฒนาสังคมและเสริมสร้างความแข็งแกร่งทางธุรกิจ อุตสาหกรรมและการค้าระหว่างประเทศ เพื่อก้าวเข้าสู่สังคมสารสนเทศ โดยมีหนึ่งในมาตรการที่สำคัญคือการปฏิรูปกฎหมายเทคโนโลยีสารสนเทศ

กฎหมายเทคโนโลยีสารสนเทศดังกล่าวประกอบไปด้วยกฎหมาย 6 ฉบับ ได้แก่[32]

(1) กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

(2) กฎหมายเกี่ยวกับลายมือชื่อทางอิเล็กทรอนิกส์

(3) กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

(4) กฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์

(5) กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(6) กฎหมายลำดับรองของรัฐธรรมนูญมาตรา 78 ว่าด้วยการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน

---

[32] นคร เสรีรักษ์, *อ้างแล้ว เชิงอรรถที่ 11*, น.264

การดำเนินงานเริ่มต้นเมื่อวันที่ 15 ธันวาคม พ.ศ. 2541 โดยมีการแต่งตั้งคณะอนุกรรมการเฉพาะกิจยกร่างกฎหมายเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อทำการศึกษาและดำเนินการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยมีศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ทำหน้าที่เป็นฝ่ายเลขานุการของคณะอนุกรรมการ โดยอนุกรรมการชุดดังกล่าวได้ดำเนินการยกร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ขึ้น โดยให้เหตุผลและความจำเป็นในการยกร่างกฎหมายดังกล่าวไว้ดังนี้

(1) เนื่องจากประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ

(2) เพื่อพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลให้เป็นระบบและสอดคล้องกับกฎหมายที่มีอยู่

(3) เพื่อรักษาดุลยภาพระหว่างเสรีภาพในการติดต่อสื่อสาร สิทธิในความเป็นส่วนตัว และความมั่นคงแห่งรัฐ

(4) เพื่อพัฒนากฎเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับที่อารยะประเทศยอมรับ

ในการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของคณะอนุกรรมการเฉพาะกิจนี้ ก่อนที่ร่างจะผ่านความเห็นชอบจากคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติได้มีการปรับเปลี่ยนแนวทางในการยกร่างสองครั้ง[33] ในการยกร่างครั้งแรกนั้น ผู้ร่างกฎหมายได้ยกร่างตามแนวทางของ Directive 95/46/EC ของสหภาพยุโรป โดยเน้นกฎหมายประเทศอิตาลีเป็นหลักร่วมกับประเทศอื่นๆในภาคพื้นยุโรปด้วย เนื่องจากเห็นว่าประเทศในภาคพื้นยุโรปมีหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ผ่านการพัฒนามาแล้วระดับหนึ่ง แต่อย่างไรก็ตามหลักการและกลไกทางกฎหมายบางประการจะต้องพิจารณาอย่างรอบคอบ เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลในปัจจุบันมีความเกี่ยวข้องกับเทคโนโลยีซึ่งเป็นเรื่องใหม่ การบังคับใช้มาตรการที่เข้มงวดอาจก่อให้เกิดปัญหาในทางปฏิบัติได้ ดังนั้นจึงมีการศึกษากฎหมายของประเทศอื่นๆเพิ่มเติม จนได้มีการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นใหม่ โดยมีทิศทางไปในแนวเดียวกับประเทศออสเตรเลีย ฮ่องกง นิวซีแลนด์ เนื่องจากประเทศดังกล่าวเป็นประเทศที่เพิ่งมีพัฒนาการเกี่ยวกับแนวคิดการคุ้มครองข้อมูลส่วนบุคคลได้ไม่นาน จึงทำให้มีมาตรการในการบังคับใช้กฎหมายที่ไม่เข้มงวดจนเกินไป อีกทั้งยัง

---

[33] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร : ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2547), น.12-13.

วางกลไกในการกำกับดูแลตนเอง เพื่อให้ผู้ที่เก็บรวบรวมข้อมูลสามารถวางหลักเกณฑ์ในทางปฏิบัติที่สอดคล้องกับกฎหมายและการดำเนินการของตนเองได้ โดยแนวทางนี้มีความยืดหยุ่นมากกว่าและน่าจะเหมาะสมกับประเทศไทยซึ่งยังอยู่ในช่วงเริ่มต้นของการพัฒนาแนวคิดเรื่องการคุ้มครองข้อมูลส่วนบุคคล

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้เข้าสู่กระบวนการยกร่างกฎหมายและพิจารณาตามขั้นตอนการออกกฎหมายอยู่หลายครั้ง รวมทั้งมีการเปลี่ยนหน่วยงานที่ทำหน้าที่ยกร่างกฎหมายจากกระทรวงวิทยาศาสตร์และเทคโนโลยีไปยังกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร มีการแสดงความคิดเห็นในรายละเอียดของร่างกฎหมายนี้จากหลายหน่วยงาน ทำให้มีการปรับปรุงเนื้อหาของบทบัญญัติเรื่อยมา ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้ถูกยกขึ้นเสนอโดยรัฐบาลในแต่ละยุคแต่ยังไม่ผ่านการพิจาณาให้แล้วเสร็จตามกระบวนการก็มักจะเปลี่ยนรัฐบาลเสียก่อน จนในที่สุดเมื่อวันที่ 22 กรกฎาคม พ.ศ. 2557 คณะรักษาความสงบแห่งชาติได้เห็นชอบให้นำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเสนอต่อสภานิติบัญญัติแห่งชาติตามที่ฝ่ายกฎหมายและกระบวนการยุติธรรม (ฝกย.) เสนอว่าร่างพระราชบัญญัติดังกล่าวเป็นกฎหมายที่ควรเร่งรัดให้มีผลบังคับใช้ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจึงได้เสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ต่อคณะรัฐมนตรี โดยคณะรัฐมนตรีได้มีมติอนุมัติหลักการร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เมื่อวันที่ 6 มกราคม พ.ศ. 2558 และส่งให้สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณา โดยให้รับข้อสังเกตของส่วนราชการที่เกี่ยวข้องไปประกอบการพิจารณาด้วยแล้วจึงส่งให้คณะกรรมการประสานงานสภานิติบัญญัติแห่งชาติพิจารณา ก่อนเสนอสภานิติบัญญัติแห่งชาติต่อไป ซึ่งบัดนี้คณะกรรมการกฤษฎีกา (คณะที่ 11) ได้พิจารณาตรวจร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เสร็จเรียบร้อยแล้ว

5.2.2 ขอบเขตการใช้บังคับของร่างพระราชบัญญัติ

ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่ผ่านการตรวจพิจารณาของคณะกรรมการกฤษฎีกา (คณะที่ 11) เรื่องเสร็จที่ 1135/2558 ได้มีขอบเขตการบังคับใช้กฎหมายดังต่อไปนี้

(1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เป็นกฎหมายกลาง หากมีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้วให้เป็นไปตามกฎหมายนั้น เว้นแต่

1. บทบัญญัติเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล และบทกำหนดโทษที่เกี่ยวข้อง จะต้องนำบทบัญญัติแห่งพระราชบัญญัตินี้ไปใช้บังคับเป็นการเพิ่มเติมไม่ว่าจะซ้ำกับกฎหมายนั้นหรือไม่ก็ตาม

2. บทบัญญัติในเรื่องการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามพระราชบัญญัตินี้ เฉพาะในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

(2) กำหนดกรณียกเว้นไม่นำร่างพระราชบัญญัตินี้ไปบังคับใช้ โดยระบุถึงผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดที่ได้รับการยกเว้นให้ชัดเจนซึ่งได้แก่

1. บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนของบุคคลนั้น โดยมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลอื่น

2. บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อสารมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือประโยชน์สาธารณะ

3. สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการ ซึ่งเก็บรวบรวม ใช้ และ เปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามอำนาจหน้าที่

4. การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

5. การดำเนินกิจการขององค์การทางศาสนา

6. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิต และสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

นอกจากนี้ยังสามารถกำหนดยกเว้นไม่นำพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใดให้ตราเป็นพระราชกฤษฎีกา

(3) มีการกำหนดนิยามข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่งสถานที่ทำงาน หรือ ที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

(4) มีการกำหนดนิยามคำว่า “บุคคล” ให้หมายความรวมถึงแต่บุคคลธรรมดาเท่านั้น เนื่องจากนิติบุคคลไม่มีความเป็นส่วนตัวและย่อมไม่มีข้อมูลส่วนบุคคลของนิติบุคคล

5.2.3 มาตรการในการคุ้มครองข้อมูลส่วนบุคคล

ตามร่างพระราชบัญญัตินี้ได้วางหลักการทั่วไปว่าผู้ควบคุมข้อมูลส่วนบุคคลจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ โดยเจ้าของข้อมูลส่วนบุคคลจะต้องให้ความยินยอม

ไว้ก่อนหรือในขณะนั้น และการขอความยินยอมต้องทำเป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์อัตโนมัติ เว้นแต่โดยสภาพไม่สามารถดำเนินการได้ ทั้งนี้เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้ เว้นแต่ถูกจำกัดไว้โดยกฎหมายหรือสัญญาที่ได้ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล และในกรณีที่มีการถอนความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมด้วย

นอกจากหลักการทั่วไปแล้ว ตามร่างพระราชบัญญัตินี้ได้กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลไว้ในหลักการเฉพาะด้วย ซึ่งมีรายละเอียดดังต่อไปนี้

5.2.3.1 หลักการเก็บรวบรวมข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล โดยการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงวัตถุประสงค์ของการเก็บรวบรวม ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลที่เก็บรวบรวมอาจจะถูกเปิดเผย ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูล

ข้อยกเว้นที่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ได้แก่

(1) เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติและได้เก็บข้อมูลส่วนบุคคลนั้นเอาไว้เป็นความลับ

(2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยายของเจ้าของข้อมูลส่วนบุคคล

(4) เป็นการปฏิบัติตามกฎหมาย

(5) กรณีอื่นตามที่กำหนดในกฎกระทรวง

อีกทั้งยังมีการห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว (sensitive Data) เช่นข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในศาสนา เป็นต้น โดยมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ยกเว้นแต่เป็นการป้องกันหรือระงับอันตรายต่อชีวิตร่างกายหรือสุขภาพของบุคคล, เป็นการปฏิบัติตามกฎหมายและกรณีอื่นๆที่กำหนดในกฎกระทรวง

5.2.3.2 หลักการใช้หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลจะใช้หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ยกเว้นแต่เป็นข้อมูลส่วนบุคคลที่สามารถเก็บรวบรวมได้

โดยได้รับการยกเว้นไม่ต้องขอความยินยอม กล่าวคือเป็นข้อมูลส่วนบุคคลประเภทใดที่ได้รับการยกเว้นให้เก็บรวบรวมได้โดยมิต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลก็สามารถใช้หรือเปิดเผยข้อมูลนั้นโดยมิต้องขอความยินยอมอีกเช่นกัน

อีกทั้งยังมีข้อยกเว้นการใช้หรือเปิดเผยข้อมูลที่เป็นข้อมูลที่เปิดเผยต่อสาธารณะ เนื่องจากเมื่อข้อมูลดังกล่าวมีความเป็นสาธารณะอยู่แล้วย่อมไม่มีความเป็นส่วนบุคคลอีกต่อไปและไม่อยู่ภายใต้ความคุ้มครองของกฎหมายนี้

5.2.3.3 หลักการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนี้ ได้กำหนดให้การโอนข้อมูลส่วนบุคคลเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด โดยคณะกรรมการกฤษฎีกาได้ให้เหตุผลว่าเพื่อที่จะไม่ต้องระบุชื่อประเทศซึ่งมีสาระสำคัญในหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ต่ำกว่าพระราชบัญญัตินี้เพื่อมิให้อาจส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศได้

ส่วนข้อยกเว้นให้สามารถโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ โดยมิต้องเป็นไปตามหลักเกณฑ์ที่คณะกรรมกาคุ้มครองข้อมูลส่วนบุคคลกำหนด มีดังต่อไปนี้

(1) เป็นการปฏิบัติตามกฎหมาย

(2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(3) เป็นการปฏิบัติตามสัญญาที่ทำระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล

(4) เป็นการกระทำเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่สามารถให้ความยินยอมในขณะนั้นได้

(5) เป็นการโอนไปยังผู้ซึ่งได้รับเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

(6) กรณีอื่นตามที่กำหนดในกฎกระทรวง

5.2.3.4 มาตรการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล

(1) สิทธิขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตน

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม โดยผู้ควบคุมข้อมูลจะปฏิเสธคำขอได้เฉพาะในกรณีต่อไปนี้เท่านั้น

1. เป็นการขัดหรือแย้งกับบทบัญญัติแห่งกฎหมาย หรือการปฏิบัติตามคำสั่งศาล

2. มีผลต่อการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย

3. การเปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลนั้นอาจเป็นอันตรายต่อสิทธิและเสรีภาพของบุคคลอื่น

4. กรณีอื่นตามที่กำหนดในกฎกระทรวง

ผู้ควบคุมข้อมูลส่วนบุคคลนั้นต้องดำเนินการตามคำขอในการเข้าถึงข้อมูลส่วนบุคคลภายในสามสิบวันนับแต่วันที่ได้รับคำขอ

(2) สิทธิขอให้ผู้ควบคุมข้อมูลดำเนินการลบ ทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลได้

หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ เช่น มีการเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคลโดยมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลและไม่เข้าข้อยกเว้นต่างๆ เป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลที่จะขอให้ผู้ควบคุมข้อมูลดำเนินการลบ ทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลได้

อีกทั้งหากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามที่ขอ เจ้าของข้อมูลส่วนบุคคลสามารถร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

(3) สิทธิในการร้องเรียนกรณีที่เกิดความเสียหายขึ้น

เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้ เพื่อเยียวยาความเสียหายที่เกิดขึ้นจากการถูกละเมิดสิทธิได้ หากผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลจริง ผู้ควบคุมข้อมูลจะต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นให้แก่เจ้าของข้อมูลส่วนบุคคลอันเป็นความรับผิดทางแพ่ง และหากการกระทำของผู้ควบคุมข้อมูลส่วนบุคคลเป็นผิดอาญาตามที่กฎหมายบัญญัติไว้ ผู้ควบคุมข้อมูลก็อาจถูกระวางโทษปรับหรือจำคุก อันเป็นมาตรการทางกฎหมายอาญาได้เช่นกัน

5.2.4 องค์กรที่มีหน้าที่ควบคุมและบังคับการให้เป็นไปตามกฎหมาย

ตามร่างพระราชบัญญัตินี้มีองค์กรที่ทำหน้าที่ควบคุมและบังคับการให้เป็นไปตามกฎหมาย 2 องค์กรด้วยกัน ได้แก่

5.2.4.1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกอบไปด้วย (1) ประธานกรรมการ ซึ่งคณะรัฐมนตรีแต่งตั้ง (2) กรรมการโดยตำแหน่ง จำนวนเจ็ดคน ได้แก่ ปลัดสำนัก

นายกรัฐมนตรี ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ผู้แทนสภาหอการค้าแห่งประเทศไทย และผู้แทนสมาคมแห่งประเทศไทย (3) กรรมการผู้ทรงคุณวุฒิ จำนวนห้าคน ซึ่งคณะรัฐมนตรีแต่งตั้ง (4) ให้เลขาธิการสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นกรรมการและเลขานุการ

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีอำนาจหน้าที่ในการจัดทำแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริมและคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบายและแผนระดับชาติที่เกี่ยวข้อง กำหนดมาตรการหรือแนวทางการดำเนินการที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ให้คำแนะนำหรือคำปรึกษาเกี่ยวกับการดำเนินการใดๆเพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานภาครัฐหรือเอกชนในการปฏิบัติตามพระราชบัญญัตินี้ เป็นต้น

5.2.4.2 คณะกรรมการผู้เชี่ยวชาญ

คณะกรรมการผู้เชี่ยวชาญได้รับการแต่งตั้งโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยลักษณะ คุณสมบัติ วาระการดำรงตำแหน่งและการดำเนินงานอื่นของคณะกรรมการผู้เชี่ยวชาญเป็นไปตามประกาศที่คณะกรรมการกำหนด

คณะกรรมการผู้เชี่ยวชาญมีอำนาจหน้าที่ในการพิจารณาเรื่องร้องเรียนต่างๆตามพระราชบัญญัตินี้ ตรวจสอบการกระทำใดๆของผู้ควบคุมข้อมูลส่วนบุคคลหรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล เป็นต้น

5.3 วิเคราะห์ผลจากการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย เทียบกับแนวคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14

ในปัจจุบันประเทศไทยอยู่ในขั้นตอนการออกกฎหมายกลางที่ใช้คุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป โดยการจัดทำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เพื่อให้การคุ้มครองสิทธิในข้อมูลส่วนบุคคลได้มีการรับรองตามกฎหมายอย่างครอบคลุม อันจะก่อให้เกิดมาตรการในคุ้มครองข้อมูลส่วนบุคคลและกลไกการบังคับใช้ที่มีประสิทธิภาพ อย่างไรก็ตามมีประเด็นที่ต้องพิจารณาว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยมีระดับการคุ้มครองที่เพียงพอตามมาตรฐานสากล โดยเฉพาะตาม Directive 95/46/EC หรือไม่ เพราะในอนาคตการโอนข้อมูลส่วนบุคคลจากต่างประเทศมายังประเทศไทยจะมีความสำคัญมากยิ่งขึ้น หากประเทศไทยได้รับการรับรองว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอย่อมทำให้ผู้ประกอบการจากทั่วโลกมีความเชื่อมั่นที่

จะลงทุนทำธุรกิจในประเทศไทย สามารถหลีกเลี่ยงปัญหาในการรับโอนข้อมูลส่วนบุคคลที่อาจเกิดขึ้นจากการประกอบธุรกิจการค้าและการบริการระหว่างประเทศระหว่างผู้ประกอบการในไทยกับประเทศสมาชิกสหภาพยุโรป และประเทศอื่นๆที่ได้อาศัย Directive 95/46/EC เป็นแนวทางในการบัญญัติกฎหมายอีกด้วย

ในการพิจารณาว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลมีการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามอาศัย Directive 95/46/EC หรือไม่นั้น จะวิเคราะห์เทียบจากแนวคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14 โดยจะแบ่งพิจารณาเป็น 2 ประเด็นคือ 1.ประเทศไทยในฐานะผู้รับโอนข้อมูลส่วนบุคคลจากต่างประเทศ 2.ประเทศไทยในฐานะผู้โอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

5.3.1 ประเทศไทยในฐานะผู้รับโอนข้อมูลส่วนบุคคลจากต่างประเทศ

ประเทศไทยจะรับโอนข้อมูลส่วนบุคคลจากต่างประเทศได้หรือไม่นั้น ขึ้นอยู่กับว่าประเทศที่เป็นฝ่ายโอนข้อมูลส่วนบุคคลได้มีกฎหมายระบุหลักเกณฑ์ในการโอนข้อมูลส่วนบุคคลเอาไว้อย่างไร ในกรณีประเทศที่เป็นผู้โอนข้อมูลส่วนบุคคลไม่มีกฎหมายระบุหลักการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศก็คงไม่มีปัญหาใดๆ ประเทศไทยสามารถรับโอนข้อมูลส่วนบุคคลจากประเทศเหล่านั้นได้

แต่ในกรณีประเทศที่เป็นผู้โอนข้อมูลส่วนบุคคลมีการกำหนดมาตรการในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเอาไว้ การโอนข้อมูลส่วนบุคคลก็จะต้องเป็นไปตามเงื่อนไขที่กฎหมายประเทศนั้นๆกำหนด

จากการศึกษาการโอนข้อมูลระหว่างประเทศตามแนวทางของ Directive 95/46/EC อันเป็นแม่แบบของกฎหมายที่ใช้บังคับในกลุ่มประเทศสมาชิกสหภาพยุโรป รวมถึงประเทศอื่นๆที่ใช้ Directive 95/46/EC เป็นแนวทางในการบัญญัติกฎหมาย กำหนดให้ประเทศเหล่านั้นจะสามารถถ่ายโอนข้อมูลส่วนบุคคลมายังประเทศไทยได้โดยไม่มีข้อจำกัด เมื่อประเทศไทยสามารถรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

ปัจจุบันประเทศไทยไม่มีการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายกลางที่ใช้บังคับเป็นการทั่วไป ทำให้การคุ้มครองข้อมูลส่วนบุคคลไม่ครอบคลุมข้อมูลบางประเภท โดยเฉพาะข้อมูลส่วนบุคคลที่อยู่ในความควบคุมดูแลของภาคเอกชน ด้วยเหตุนี้ประเทศไทยจึงจะถูกตัดสินโดยสหภาพยุโรปว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอได้ เหมือนดังเช่นกรณีของประเทศสหรัฐอเมริกาก่อนมีการจัดทำข้อตกลงโครงการเซฟฮาร์เบอร์ อันจะส่งผลให้ประเทศไทยไม่สามารถรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรปได้โดยสะดวก ปราศจากเงื่อนไข

ในอนาคตประเทศไทยจะมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลออกมาบังคับใช้ พระราชบัญญัตินี้จะเป็นกฎหมายกลางที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคล การที่ประเทศไทยมีกฎหมายกลางที่มีบททั่วไปใช้ในการคุ้มครองข้อมูลส่วนบุคคลจะทำให้ประเทศสมาชิกสหภาพยุโรปหรือคณะกรรมาธิการยุโรปมีแนวโน้มที่จะพิจารณาว่าประเทศไทยนั้นมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอได้มากยิ่งขึ้น

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ผู้ร่างได้ตราขึ้นตามแนวทางของ Directive 95/46/EC แต่ปรับปรุงให้มีความยืดหยุ่นมากยิ่งขึ้นเพื่อให้รองรับกับการพัฒนาแนวความคิดในการคุ้มครองข้อมูลส่วนบุคคลที่เพิ่งมีขึ้นได้ไม่นาน หากประเทศไทยมีประเด็นพิพาทกับกลุ่มประเทศสมาชิกสหภาพยุโรปว่าประเทศไทยมีการรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่นั้น คณะกรรมาธิการยุโรปจะตัดสินชี้ขาดโดยการเทียบกับหลักการคุ้มครองข้อมูลส่วนบุคคลที่คณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล ได้เคยวางหลักไว้ 2 ประการ คือ หลักประการที่ 1 เนื้อหาในการคุ้มครองข้อมูลส่วนบุคคลว่าประเทศที่รับโอนข้อมูลส่วนบุคคลนั้นมีหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลเพียงพอ และหลักเกณฑ์ประการที่ 2 คือกระบวนการบังคับใช้มีประสิทธิภาพเพียงพอ

อย่างไรก็ตามการพิจารณาเฉพาะหลักการของคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลนั้นไม่เพียงพออีกต่อไป เมื่อศาลยุติธรรมแห่งสหภาพยุโรปได้วางหลักเกณฑ์การพิจารณาระดับการคุ้มครองข้อมูลส่วนบุคคลเอาไว้เพิ่มขึ้นตามคำพิพากษาคดีเลขที่ C-362/14 ที่แสดงในเห็นว่าแม้ประเทศที่รับโอนข้อมูลส่วนบุคคลจะได้รับการตัดสินชี้ขาดจากคณะกรรมาธิการยุโรปว่ามาตรการของประเทศที่รับโอนข้อมูลส่วนบุคคลนั้นมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอแล้วก็ตาม แต่ถ้าหากมาตรการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศนั้นพิจารณาแล้วเข้าตามกรณีต่อไปนี้ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศนั้นก็จะไม่มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพออีกต่อไปตามแนวคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรป

หลักเกณฑ์ที่ทำให้ศาลตัดสินว่ากฎหมายหรือมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของประเทศนอกกลุ่มสมาชิกสหภาพยุโรปมีการคุ้มครองข้อมูลส่วนบุคคลไม่เพียงพอ จะต้องเข้าองค์ประกอบดังต่อไปนี้

(1) กฎหมายหรือมาตรการอื่นใดที่มีขึ้นเพื่อวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคลได้มีการกำหนดข้อยกเว้นให้ไม่ต้องปฏิบัติตามหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลเอาไว้ ไม่ว่าจะด้วยเหตุผลเพื่อความมั่นคงแห่งชาติ ประโยชน์สาธารณะ หรืออาศัยอำนาจตามกฎหมายอื่นใด และ

(2) กฎหมายหรือคำสั่งอื่นใดในประเทศนั้นเปิดช่องให้อำนาจหน่วยงานของรัฐสามารถเข้าถึงข้อมูลส่วนบุคคลได้อย่างไม่มีขอบเขตจำกัด ไม่เฉพาะเจาะจงเป้าหมาย โดยสามารถเก็บรวบรวมและประมวลผลข้อมูลได้ในจำนวนมาก

ฉะนั้นการพิจารณาว่าการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยมีกฎหมายหรือพฤติการณ์อื่นใดที่จะทำให้มีระดับการคุ้มครองข้อมูลส่วนบุคคลไม่เพียงพอตามเหตุผลของคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปหรือไม่นั้น จะต้องแยกพิจารณาเป็นขั้นตอนทีละลำดับดังต่อไปนี้

(1) กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยได้กำหนดข้อยกเว้นให้ไม่ต้องปฏิบัติตามหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลเอาไว้หรือไม่

เมื่อพิจารณาบทบัญญัติของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... บททั่วไปได้วางหลักการว่าผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้[34] และผู้ควบคุมข้อมูลส่วนบุคคลอาจเก็บรวบรวบ ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ได้ หากมีบทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้เช่นกัน[35] จะเห็นได้ว่าตามร่างพระราชบัญญัตินี้ได้เปิดช่องให้สามารถนำกฎหมายอื่นใดมาบังคับใช้เพื่อยกเว้นหลักการทั่วไปของการคุ้มครองข้อมูลส่วนบุคคลได้

เมื่อพิจารณาในบทเฉพาะต่อไปในส่วนของการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นได้บัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลจะทำการเก็บรวบรวมข้อมูลส่วนบุคคลได้ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล แต่อย่างไรก็ตามกฎหมายได้กำหนดข้อยกเว้นที่ไม่ต้องขอความยินยอมไว้ในกรณีดังต่อไปนี้[36]

1. เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ และได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ

2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

3. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยายของเจ้าของข้อมูลส่วนบุคคล

4. เป็นการปฏิบัติตามกฎหมาย

---

[34] ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... , มาตรา 17

[35] *เพิ่งอ้าง*, มาตรา 18

[36] *เพิ่งอ้าง*, มาตรา 21

5. กรณีอื่นตามที่กำหนดในกฎกระทรวง

จากบทบัญญัติดังกล่าวได้มีบทยกเว้นที่เปิดช่องให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้ถ้าหากมีกฎหมายอื่นให้อำนาจไว้ ยิ่งไปกว่านั้นตามร่างพระราชบัญญัตินี้ยังให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้และเปิดเผยข้อมูลส่วนบุคคลประเภทที่สามารถเก็บรวบรวมไว้โดยไม่ต้องขอความยินยอมได้อีกด้วย[37]

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยจึงเป็นบทบัญญัติที่มีการกำหนดข้อยกเว้นเอาไว้ให้ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องปฏิบัติตามหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลได้หากมีกฎหมายอื่นให้อำนาจกระทำการเป็นอย่างอื่น เมื่อเปรียบเทียบกับคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14 จะพบว่าโครงการเซฟฮาร์เบอร์ได้มีบทยกเว้นเช่นเดียวกันนี้ที่กำหนดให้องค์กรที่เข้าร่วมไม่ต้องปฏิบัติตามหลักการของโครงการเซฟฮาร์เบอร์ได้หากมีข้อจำกัดโดยรัฐบัญญัติ ระเบียบของราชการ หรือกฎหมายที่มาจากบรรทัดฐานคำพิพากษาของศาลที่ได้สร้างข้อผูกพันที่ขัดแย้งกับหลักการเซฟฮาร์เบอร์

(2) กฎหมายหรือคำสั่งอื่นใดในประเทศไทยเปิดช่องให้อำนาจหน่วยงานของรัฐสามารถเข้าถึงข้อมูลส่วนบุคคลได้อย่างไม่มีขอบเขตจำกัด ไม่เฉพาะเจาะจงเป้าหมาย โดยสามารถเก็บรวบรวมและประมวลผลข้อมูลได้ในจำนวนมาก

การกระทำของรัฐบาลสหรัฐอเมริกาที่ส่งผลทำให้ศาลยุติธรรมแห่งสหภาพยุโรปไม่ไว้วางใจในระบบการคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาอีกต่อไป มาจากการที่หน่วยงานความมั่นคงแห่งชาติสหรัฐอเมริกาได้ใช้รัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศ ซึ่งเป็นกฎหมายเกี่ยวกับความมั่นคงของรัฐจัดทำโครงการปริซึมที่อนุญาตให้เจ้าหน้าที่ผู้มีอำนาจได้เข้าถึงข้อมูลเพื่อการจัดเก็บและประมวลผลในสหรัฐอเมริกาได้ โดยเป็นการจัดเก็บข้อมูลแบบไม่เฉพาะเจาะจงเป้าหมาย หน่วยงานของรัฐสามารถเข้าถึงข้อมูลการติดต่อทางโทรศัพท์ในประเทศสหรัฐอเมริกา การเข้าถึงบันทึกรายชื่อทางอิเล็กทรอนิกส์ของบุคคล และการสื่อสารข้อมูลดิจิทัลปริมาณมหาศาลได้ ผลจากการบังคับใช้กฎหมายด้านความมั่นคงดังกล่าว ส่งผลให้องค์กรที่เข้าร่วมโครงการเซฟฮาร์เบอร์ไม่จำเป็นต้องปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลของเซฟฮาร์เบอร์ เนื่องจากมีข้อยกเว้นเอาไว้ให้องค์กรเหล่านั้นต้องปฏิบัติตามกฎหมายของประเทศสหรัฐอเมริกา อันเป็นผลให้ศาลยุติธรรมแห่งสหภาพยุโรปตัดสินให้โครงการเซฟฮาร์เบอร์สิ้นผลไปในที่สุด

ส่วนในประเทศไทยนั้นการพิจารณาว่ามีกฎหมายที่ให้อำนาจหน่วยงานของรัฐเข้าถึงข้อมูลส่วนบุคคลหรือไม่นั้นควรจะต้องพิเคราะห์ทั้งกฎหมายที่ใช้บังคับอยู่ในปัจจุบันและกฎหมายที่จะมีการบัญญัติใช้ในอนาคตด้วย โดยจะแยกพิจารณาดังนี้

---

[37] *เพิ่งอ้าง*, มาตรา 24

(1) กฎหมายในปัจจุบันที่ให้อำนาจหน่วยงานของรัฐเข้าถึงข้อมูลส่วนบุคคล

โดยทั่วไปแล้วกฎหมายจะให้อำนาจรัฐในการเข้าถึงและดักรับข้อมูลส่วนบุคคลได้ในกรณีที่เป็นเรื่องเกี่ยวกับความมั่นคงของรัฐหรือเพื่อการควบคุมอาชญากรรม (crime control)[38] ที่ให้อำนาจพนักงานเจ้าหน้าที่ในการรวบรวมพยานหลักฐานอันเกี่ยวกับความผิดโดยเฉพาะ บทบัญญัติกฎหมายในประเทศไทยที่ให้อำนาจหน่วยงานของรัฐเข้าถึงหรือดักรับข้อมูลส่วนบุคคลนั้นได้กระจายอยู่ตามพระราชบัญญัติต่างๆ ยกตัวอย่างเช่น[39]

พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 พระราชบัญญัตินี้ให้อำนาจเจ้าพนักงานได้มาซึ่งข้อมูลข่าวสารที่ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด ตามมาตรา 14 จัตวา ซึ่งวางหลักว่า “ในกรณีที่มีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทาง ไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดตามกฎหมายเกี่ยวกับยาเสพติด เจ้าพนักงานซึ่งได้รับอนุมัติจากเลขาธิการเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญา เพื่อมีคำสั่งอนุญาตให้เจ้าพนักงานได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้..”

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พระราชบัญญัตินี้ให้อำนาจเจ้าพนักงานที่เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินมอบหมายเป็นหนังสือมีอำนาจเข้าถึงข้อมูลส่วนบุคคลได้ ตามมาตรา 46 ซึ่งวางหลักว่า “ในกรณีที่มีเหตุอันควรเชื่อถือได้ว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้ หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน พนักงานเจ้าหน้าที่ ซึ่งเลขาธิการมอบหมายเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลแพ่ง เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชี ข้อมูลทางการสื่อสาร หรือ ข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็ได้..”

---

[38] คณาธิป ทองรวีวงศ์, “ข้อพิจารณา 9 ประการ ต่อการเสนอร่างกฎหมายใหม่ที่ให้อำนาจเจ้าพนักงานดักรับข้อมูลการสื่อสาร,” ในการสัมมนาทางวิชาการ 22 ธันวาคม 2557, จัดโดยเครือข่ายพลเมืองเน็ต ณ คณะเศรษฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2557 : น.1.

[39] คณาธิป ทองรวีวงศ์, “มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวของผู้ถูกดักฟังการสื่อสารข้อมูล,” วารสารกระบวนการยุติธรรม, เล่มที่ 1, ปีที่ 6, น.14-16, (มกราคม-เมษายน 2556).

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 พระราชบัญญัตินี้ให้อำนาจพนักงานสอบสวนคดีพิเศษดำเนินการเพื่อให้ได้มาซึ่งข้อมูลข่าวสารที่ถูกใช้หรืออาจถูกใช้เพื่อกระทำความผิดที่เป็นคดีพิเศษ ตามมาตรา 25 ที่วางหลักว่า “ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษพนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือ จะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญา เพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้..”

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัตินี้ให้อำนาจเจ้าพนักงานในการสืบสวนและสอบสวน ในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ตามมาตรา 18 เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด โดยในมาตรา 18(6) ได้ให้อำนาจเจ้าพนักงานในการ “ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้..” การใช้อำนาจของพนักงานเจ้าหน้าที่เป็นไปตามบังคับของมาตรา 19 ซึ่งวางหลักว่า “ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง”

ประมวลกฎหมายวิธีพิจารณาความอาญา ในประมวลกฎหมายวิธีพิจารณาความอาญามีบทบัญญัติที่เกี่ยวข้องกับการได้มาซึ่งข้อมูลข่าวสารในการสืบสวนสอบสวนคดีอาญา ตามมาตรา 93 ซึ่งวางหลักว่าห้ามมิให้ค้นในที่รโหฐาน โดยไม่มีหมายค้นหรือคำสั่งของศาล”

จากกฎหมายไทยที่ให้อำนาจเจ้าหน้าที่ของรัฐในการเข้าถึงข้อมูลส่วนบุคคลดังที่ได้กล่าวมานั้นเห็นได้ว่าฐานความผิดที่ให้อำนาจเจ้าพนักงานเข้าถึงข้อมูลส่วนบุคคลได้นั้นมีการระบุเป็นกรณีเฉพาะ กล่าวคือเจ้าพนักงานจะเข้าถึงหรือดักรับข้อมูลส่วนบุคคลได้ต้องเข้าข่ายความผิดที่กฎหมายฉบับนั้นๆบัญญัติไว้ นอกจากนี้คณาธิป ทองรวีวงศ์[40] ได้ให้ข้อเสนอเกี่ยวกับลักษณะของกฎหมายที่ให้อำนาจเจ้าพนักงานดักรับข้อมูลการสื่อสารไว้ 9 ประการ ได้แก่ กฎหมายที่ให้อำนาจดักรับข้อมูลการสื่อสารควรมีลักษณะเฉพาะเจาะจงในเชิงมาตรการ, กฎหมายที่ให้อำนาจดักรับข้อมูลการสื่อสารควรมีลักษณะเฉพาะเจาะจงในแง่ของบุคคลที่ตกเป็นเป้าหมายของการดักรับข้อมูล, กฎหมายที่

[40] คณาธิป ทองรวีวงศ์, *อ้างแล้ว เชิงอรรถที่ 38*, น.3.

ให้อำนาจดักรับข้อมูลต้องมีการกำหนดช่วงระยะเวลาในการดักรับข้อมูลที่ชัดเจน เป็นต้น และได้ให้ความเห็นเรื่องวิธีการเข้าถึงหรือดักรับข้อมูลตามกฎหมายไทยไว้ว่า บทบัญญัติได้ให้อำนาจเจ้าพนักงานกระทำการเกี่ยวกับการดักรับข้อมูลไว้ค่อนข้างกว้างและไม่เฉพาะเจาะจง ดังจะเห็นได้จากการใช้ถ้อยคำว่า “เพื่อให้ได้มาซึ่งข้อมูล...” เช่น ตามพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519, พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547, พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 เป็นต้น ซึ่งการบัญญัติมาตรการในการให้ได้มาซึ่งข้อมูลส่วนบุคคลไว้อย่างกว้างนั้น จะเป็นการเปิดโอกาสให้เจ้าพนักงานใช้อำนาจอย่างเกินขอบเขตได้

อย่างไรก็ตาม เมื่อพิจารณาเนื้อหาของกฎหมายที่ให้อำนาจเจ้าหน้าที่ของรัฐเข้าถึงหรือดักรับข้อมูลส่วนบุคคลในปัจจุบันเพิ่มเติม พบว่าตามกฎหมายได้ระบุหลักเกณฑ์ให้เจ้าหน้าที่ต้องขออนุญาตต่อศาลก่อนด้วย โดยกฎหมายแต่ละฉบับได้บัญญัติให้ขออนุญาตศาลแตกต่างกัน เช่น พระราชบัญญัติป้องกันและปราบปรามยาเสพติด, พระราชบัญญัติการสอบสวนคดีพิเศษ กำหนดให้ขออนุญาตจากอธิบดีผู้พิพากษาศาลอาญา ส่วนพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน ให้ยื่นคำขอต่อศาลแพ่ง เป็นต้น จะเห็นได้ว่าการบัญญัติให้เจ้าหน้าที่ของรัฐต้องขออนุญาตต่อศาลก่อนที่จะดำเนินการเพื่อเข้าถึงข้อมูลส่วนบุคคลนั้นเพื่อให้เกิดการตรวจสอบถ่วงดุลอำนาจโดยฝ่ายตุลาการ ซึ่งทำให้การกระทำการของหน่วยงานของรัฐที่ก่อให้เกิดการละเมิดสิทธิของบุคคลนั้นมีข้อจำกัดมิให้เจ้าหน้าที่ของรัฐกระทำการเกินขอบเขต

ดังนั้นหากพิจารณาเฉพาะกฎหมายที่บังคับใช้อยู่ในปัจจุบัน พบว่าแม้จะมีการบัญญัติให้อำนาจเจ้าหน้าที่ของรัฐใช้วิธีการในการเข้าถึงข้อมูลส่วนบุคคลได้อย่างกว้างขวาง แต่ก็ได้มีการระบุขอบข่ายของข้อมูลที่จะเข้าถึงได้นั้นต้องเข้าข่ายฐานความผิดที่กฎหมายบัญญัติไว้ อีกทั้งยังต้องขออนุญาตและได้รับความเห็นชอบจากศาลก่อนด้วย จึงไม่เข้ากรณีที่กฎหมายอื่นในประเทศไทยเปิดช่องให้อำนาจหน่วยงานของรัฐสามารถเข้าถึงข้อมูลส่วนบุคคลได้อย่างไม่มีขอบเขตจำกัด โดยสามารถเก็บรวบรวมและประมวลผลข้อมูลได้ในจำนวนมาก หากพิจารณาตามเหตุผลตามคำพิพากษาของศาลยุติธรรมแห่งสหภาพยุโรปกฎหมายไทยในปัจจุบันยังอยู่ในเกณฑ์ที่จะไม่ถูกตัดสินว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ

(2) กฎหมายที่จะมีการประกาศใช้ในอนาคต

เพื่อรองรับการพัฒนาเศรษฐกิจและสังคมในยุคที่เทคโนโลยีเจริญก้าวหน้าอย่างรวดเร็ว ขณะนี้ประเทศไทยจึงมีกระบวนการตรากฎหมายที่เรียกว่า “ชุดกฎหมายความมั่นคงดิจิทัล” ชุดกฎหมายนี้เป็นไปเพื่อนโยบายในการพัฒนาเศรษฐกิจดิจิทัล โดยในขณะนี้ชุดกฎหมายดังกล่าวได้ผ่านขั้นตอนการรองรับหลักการของคณะรัฐมนตรีไปเรียบร้อยแล้ว ในชุดกฎหมายความมั่นคงดิจิทัลทั้ง 10 ฉบับนั้นปรากฏว่ามีร่างพระราชบัญญัติบางฉบับให้อำนาจหน่วยงานของรัฐเข้าถึงและดักรับข้อมูลส่วนบุคคลได้ ดังพิจาณาต่อไปนี้

(2.1) ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ....

ร่างพระราชบัญญัติฉบับนี้มีวัตถุประสงค์ในการป้องกันและรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม ซึ่งกระทบต่อความมั่นคงของชาติในมิติต่างๆ

ตามร่างพระราชบัญญัตินี้ได้ให้คำนิยามของคำว่าความมั่นคงปลอดภัยไซเบอร์ไว้ว่า “มาตรการและการดำเนินการที่กำหนดขึ้น เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติ ซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และ ความมั่นคงทางเศรษฐกิจ”[41] จากคำนิยามของคำว่าความมั่นคงปลอดภัยไซเบอร์นั้นเห็นได้ว่ามีการเขียนบรรยายไว้อย่างกว้างๆ ไม่ได้ระบุความให้ชัดเจน เช่น คำว่าภัยคุกคาม ซึ่งสามารถตีความได้หลากหลายตามแต่ดุลยพินิจของเจ้าหน้าที่ อีกทั้งตามบัญญัตินี้แม้ยังไม่มีผลกระทบเกิดขึ้นแต่เพียงมีความเสี่ยงที่จะเกิดผลกระทบขึ้นก็สามารถใช้อำนาจตามกฎหมายได้เช่นกัน จึงเป็นการบัญญัติกฎหมายที่ให้อำนาจหน่วยงานของรัฐใช้ดุลยพินิจได้อย่างกว้างขวางมากเกินสมควร

ในส่วนของอำนาจเจ้าหน้าที่ของรัฐตามพระราชบัญญัตินี้ได้มีการจัดตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) ขึ้น คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีอำนาจสำคัญดังต่อไปนี้

1. สั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ดำเนินการอื่นใดที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ[42]

2. เมื่อมีเหตุฉุกเฉินหรือภยันตรายอันเนื่องมาจากภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดผลกระทบต่อความมั่นคงของประเทศ ให้ กปช. มีอำนาจสั่งการให้หน่วยงานของรัฐทุกแห่งดำเนินการอย่างหนึ่งอย่างใดเพื่อป้องกัน แก้ไขปัญหา หรือบรรเทาความเสียหายที่เกิดหรืออาจจะ

---

[41] ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ...., มาตรา 3

[42] *เพิ่งอ้าง*, มาตรา 7(8)

เกิดขึ้นได้ตามที่เห็นสมควร และอาจให้หน่วยงานของรัฐ หรือบุคคลใด รวมทั้งบุคคลซึ่งได้รับอันตรายหรืออาจได้รับอันตรายหรือความเสียหายดังกล่าว กระทำหรือร่วมกันกระทำการใด ๆ อันจะมีผลเป็นการควบคุม ระงับ หรือบรรเทาผลร้ายจากอันตรายและความเสียหายที่เกิดขึ้นนั้นได้อย่างทันท่วงที[43]

3. ในกรณีที่มีความจำเป็นเพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่อาจกระทบต่อความมั่นคงทางการเงินและการพาณิชย์ หรือความมั่นคงของประเทศ กปช. อาจสั่งการให้หน่วยงานภาคเอกชนกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง และให้รายงานผลการปฏิบัติการต่อ กปช. ตามที่ กปช.ประกาศกำหนด[44]

จะเห็นได้ว่า กปช. ซึ่งเป็นหน่วยงานของรัฐตามร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. .... มีอำนาจมากมาย สามารถสั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ดำเนินการอื่นใดที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ ซึ่งตามกฎหมายนี้เป็นการให้อำนาจ กปช. ไว้อย่างไม่จำกัด เมื่อมีการให้อำนาจหน่วยงานของรัฐด้วยเหตุผลทางด้านความมั่นคงไว้ไม่จำกัดมากเพียงใดก็ย่อมกระทบต่อสิทธิเสรีภาพของบุคคลมากขึ้นเช่นกัน เนื่องจากเจ้าหน้าที่ของรัฐอาจใช้อำนาจที่มีมากเกินขอบเขตจนก้าวล่วงละเมิดสิทธิของบุคคลได้

อีกทั้งร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. .... ยังมีบทกฎหมายที่ให้อำนาจพนักงานเจ้าหน้าที่เข้าถึงข้อมูลส่วนบุคคลได้อย่างไม่จำกัดอีกด้วย ตามมาตรา 35 ได้บัญญัติเอาไว้ว่า “เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่ที่ได้รับมอบหมายเป็นหนังสือจากเลขาธิการ มีอำนาจดังต่อไปนี้

1. มีหนังสือสอบถามหรือเรียกให้หน่วยงานของรัฐ หรือบุคคลใดๆ มาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบหรือให้ข้อมูลเพื่อประโยชน์ในการปฏิบัติการตามพระราชบัญญัตินี้

2. มีหนังสือขอให้หน่วยงานราชการ หรือหน่วยงานเอกชนดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช.

3. เข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

---

[43] *เพิ่งอ้าง*, มาตรา 33

[44] *เพิ่งอ้าง*, มาตรา 34

ตามร่างพระราชบัญญัตินี้โดยเฉพาะในข้อ 3. นั้น ได้ให้อำนาจพนักงานเจ้าหน้าที่ที่ได้รับมอบหมายเป็นหนังสือจากเลขาธิการสามารถเข้าถึงข้อมูลการติดต่อสื่อสาร ทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งกฎหมายนี้ใช้บังคับได้กับหน่วยงานของภาคธุรกิจทุกประเภท จึงเป็นการให้อำนาจเจ้าหน้าที่ของรัฐอย่างกว้างขวางเนื่องจากสามารถตรวจสอบการสื่อสารของประชาชนได้ทุกช่องทาง โดยไม่มีขอบเขตข้อจำกัด และไม่ต้องมีหมายศาล (warrant) ทำให้ปราศจากกระบวนการตรวจสอบใดๆ กฎหมายดังกล่าวจึงมีความคล้ายคลึงกับกฎหมายที่หน่วยงานความมั่นคงแห่งชาติของประเทศสหรัฐอเมริกาได้ใช้ในการจัดทำโครงการปริซึมที่อนุญาตให้เจ้าหน้าที่ผู้มีอำนาจสามารถเข้าถึงข้อมูลเพื่อการจัดเก็บและประมวลผลในสหรัฐอเมริกาได้อย่างไม่มีข้อจำกัด

(2.2) ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ..) พ.ศ. .... ร่างพระราชบัญญัติฉบับนี้เป็นการแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เนื่องจากพระราชบัญญัติเดิมมีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบันที่มีรูปแบบการกระทำความผิดที่ซับซ้อนมากขึ้นตามเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว

ปัจจุบันคณะรัฐมนตรีได้พิจารณาและให้ความเห็นชอบพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในวันที่ 26 เมษายน พ.ศ. 2559 พร้อมทั้งส่งต่อให้สภานิติบัญญัติแห่งชาติพิจารณาประกาศใช้เป็นกฎหมายแล้ว โดยร่างพระราชบัญญัตินี้ได้ผ่านวาระที่หนึ่งขั้นรับหลักการเรียบร้อยแล้ว และจะมีการพิจารณาวาระที่สองในช่วงเดือนมิถุนายน พ.ศ. 2559

เมื่อพิจารณาเนื้อหาของร่างพระราชบัญญัติที่แก้ไขใหม่นี้ ปรากฏว่าร่างมาตรา 14 ที่เป็นการยกเลิกและใช้แทนมาตรา 20 ของพระราชบัญญัติเดิมนั้น ได้ให้อำนาจรัฐมนตรีในการออกประกาศเพิ่มเติมเรื่องหลักเกณฑ์ ขั้นตอน ระยะเวลาและแนวทางปฏิบัติสำหรับระงับการทำให้แพร่หลายและลบข้อมูลคอมพิวเตอร์ของผู้ให้บริการได้ ส่วนร่างมาตรา 9 ที่เป็นการยกเลิกและใช้แทนมาตรา 15 ของพระราชบัญญัติเดิม ได้มีการบัญญัติความรับผิดของผู้ให้บริการ และให้อำนาจรัฐมนตรีออกประกาศขั้นตอนการแจ้งเตือน การระงับข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ด้วย ซึ่งหลักการและเหตุผลในการบัญญัติมาตราดังกล่าวได้ปรากฏว่ามีเอกสารนำเสนอโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้อธิบายการหลักการและเหตุผลแก้ไขมาตรา 20 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ว่าด้วยให้รัฐมนตรีสามารถออกประกาศกำหนดให้มีวิธีการในการปิดกั้นข้อมูลที่ถูกเข้ารหัสได้ โดยระบุในหน้า 7 ของ

เอกสารนำเสนอ[45] ว่า “รัฐมนตรีอาจประกาศกำหนดหลักเกณฑ์ ระยะเวลาและแนวทางการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของผู้ให้บริการให้เป็นไปในแนวทางเดียวกันภายใต้พัฒนาการทางเทคโนโลยีที่เปลี่ยนไป เช่น ข้อมูลคอมพิวเตอร์ที่เข้ารหัสด้วยเทคโนโลยี SSL (Secure Socket Layer) ซึ่งถูกสร้างขึ้นมาเพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ตที่มีการเข้ารหัสแบบ Public-key encryption นั้น จำเป็นต้องมีวิธีการและเครื่องมือพิเศษในการดำเนินการจึงจะสามารถกระทำได้สำเร็จ ...”

SSL เป็นเทคโนโลยีในการเข้ารหัสข้อมูล (encryption) อย่างหนึ่ง เป็นการช่วยรักษาความลับของข้อมูลมิให้บุคคลอื่นนอกจากผู้รับ (recipient) ล่วงรู้เนื้อหาของข้อมูลนั้นได้ เนื่องจากข้อมูลที่ถูกส่งไปนั้นจะถูกเข้ารหัสให้ไม่สามารถอ่านออกได้ มีเพียงผู้รับเท่านั้นที่จะสามารถถอดรหัสข้อมูลนั้นได้ ซึ่ง ระบบอีเมล ระบบการสื่อสาร และการพาณิชย์อิเล็กทรอนิกส์ เช่น ข้อมูลบัตรเครดิตในปัจจุบัน ได้ใช้เทคโนโลยี SSL ในการเข้ารหัสข้อมูลเป็นการทั่วไปเพื่อเพิ่มความปลอดภัยให้กับผู้ใช้อินเทอร์เน็ต จึงเป็นเรื่องที่น่ากังวลถ้าหากร่างพระราชบัญญัติมาตรา 9 และมาตรา 14 ได้มีการให้อำนาจรัฐมนตรีกำหนดหลักเกณฑ์และวิธีการระงับข้อมูลต่างๆเพิ่มเติมได้ เพราะอาจเป็นการให้อำนาจเจ้าหน้าที่ของรัฐใช้วิธีการใดๆในการเข้าถึงข้อมูลส่วนบุคคลได้ แม้ว่าข้อมูลส่วนบุคคลนั้นจะถูกคุ้มครองป้องกันด้วยวิธีการเข้ารหัสข้อมูลไว้แล้วก็ตาม

นอกจากนี้ยังปรากฏว่ามีการออกคำสั่งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ 163/2557 เรื่องแต่งตั้งคณะทำงานทดสอบระบบเฝ้าติดตามสื่อออนไลน์[46] เนื่องจากก่อนหน้านั้นได้มีการแต่งตั้งคณะทำงานด้านสื่อออนไลน์ ภายใต้คณะกรรมการเพื่อติดตามการเผยแพร่ข่าวสารต่อสาธารณะ เพื่อทำหน้าที่ในการติดตาม กลั่นกรอง ตรวจสอบ รวบรวมวิเคราะห์การเผยแพร่ข้อมูลข่าวสารด้านสื่อออนไลน์ทุกประเภท และให้มีอำนาจพิจารณากำหนดแนวทางในการปฏิบัติมาตรการป้องกันและยับยั้ง เพื่อแก้ไขปัญหาในระยะยาวให้เกิดความชัดเจนและมีความรวดเร็ว แต่อย่างไรก็ตามการดำเนินงานภายใต้อำนาจหน้าที่ตามคำสั่งดังกล่าวได้พบอุปสรรคในการตรวจสอบและปิดกั้นเว็บไซต์ที่มีการเข้ารหัสป้องกันข้อมูล ดังนั้นกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงเห็นควรให้มีการจัดหาและทดสอบประสิทธิภาพของอุปกรณ์ระบบเฝ้าติดตามสื่อออนไลน์เพื่อสนับสนุนการปฏิบัติงานของคณะทำงานด้านสื่อออนไลน์ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ และแต่งตั้งคณะทำงานทดสอบระบบเฝ้าติดตามสื่อออนไลน์ขึ้นด้วย

---

[45] เครือข่ายพลเมืองเน็ต, “Single Gateway คืนชีพ ก.ไอซีทีเสนอในพ.ร.บ.คอมฯ ให้มีวิธีระงับข้อมูลที่เข้ารหัส SSL” สืบค้นเมื่อวันที่ 28 พฤษภาคม 2559, จาก https://thainetizen.org/2016/05/single-gateway-back-ssl-censorship/

[46] *เพิ่งอ้าง*.

คำสั่งของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ 163/2557 ยังได้ให้อำนาจหน้าที่คณะทำงานทดสอบระบบเฝ้าติดตามสื่อออนไลน์ สามารถกระทำการดังต่อไปนี้

(1) ควบคุมการทดสอบระบบเฝ้าติดตามสื่อออนไลน์ที่มีการเข้ารหัสป้องกันข้อมูล และประเมินผล เพื่อให้ได้ระบบที่มีประสิทธิภาพสูงสุด เหมาะสมในการใช้งานสำหรับประเทศไทย

(2) ประสานทางเทคนิคกับผู้ประกอบการและผู้ให้บริการอินเทอร์เน็ตภายในประเทศและที่เชื่อมต่อกับต่างประเทศโดยตรง (International Internet Gateway) ในการทดสอบระบบเฝ้าติดตามสื่อออนไลน์

(3) ประสานหน่วยงานและบุคคลที่เกี่ยวข้องกับข้อกำหนดในการทดสอบระบบเฝ้าติดตามออนไลน์

(4) เสนอแนะ ปัญหา อุปสรรค แนวทางการปรับปรุงแก้ไขในส่วนที่เกี่ยวข้องและดำเนินการอื่นๆ ตามที่ได้รับมอบหมายจากรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

จากคำสั่งข้างต้นเห็นได้ว่าคณะทำงานด้านสื่อออนไลน์ ซึ่งมีการแต่งตั้งก่อนคณะทำงานทดสอบระบบเฝ้าติดตามสื่อออนไลน์ มีอำนาจอย่างกว้างขวางในการเข้าถึงและรวบรวมข้อมูลส่วนบุคคลทางด้านสื่อออนไลน์ได้ทุกประเภท รวมทั้งสามารถประมวลข้อมูลส่วนบุคคลที่ได้เข้าถึงนั้นอีกด้วย คำสั่งดังกล่าวจึงเป็นการให้อำนาจหน่วยงานของรัฐเข้าสอดแนมข้อมูลได้อย่างไม่มีขอบเขตจำกัด แต่อย่างไรก็ตาม การทำงานของคณะทำงานด้านสื่อออนไลน์ประสบปัญหาเนื่องจากไม่สามารถเข้าถึงข้อมูลที่มีการเข้ารหัสป้องกันข้อมูลได้ จึงเป็นที่มาของคำสั่งแต่งตั้งคณะทำงานทดสอบระบบเฝ้าติดตามสื่อออนไลน์นั่นเอง

ถ้าหากคำสั่งของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารข้างต้น ได้ใช้โดยฐานอำนาจของร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ที่ได้แก้ไขให้อำนาจรัฐมนตรีออกประกาศเพิ่มเติมเรื่องหลักเกณฑ์และขั้นตอนวิธีการปิดกั้นเว็บไซต์ได้ จะทำให้การสอดแนมข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐทำได้อย่างง่ายดายมากยิ่งขึ้น เนื่องจากการจะเข้าไประงับตัวข้อมูลได้นั้นย่อมต้องมีการเข้าถึงข้อมูลส่วนบุคคลให้ทราบได้ก่อนว่าข้อมูลนั้นคืออะไร ดังนั้นหน่วยงานของรัฐจึงสามารถใช้อำนาจในการเข้าถึงข้อมูลส่วนบุคคลได้อย่างกว้างขวาง แม้แต่ข้อมูลที่ต้องมีการป้องกันอย่างสูงจึงได้เข้ารหัสป้องกันข้อมูลไว้ เช่นข้อมูลเกี่ยวกับการทำธุรกรรมทางการธนาคาร การสั่งซื้อสินค้าออนไลน์ ก็สามารถเข้าถึงได้เช่นกัน การจะบัญญัติกฎหมายในลักษณะดังกล่าวจึงเปิดช่องให้หน่วยงานของรัฐสามารถเข้าถึง เก็บรวบรวมและประมวลผลข้อมูลอย่างไม่มีขอบเขตจำกัด และสามารถเข้าถึงข้อมูลได้ในปริมาณมาก ทุกประเภทข้อมูลอีกด้วย

นอกจากนี้ตามมาตรา 9 ของร่างพระราชบัญญัติฉบับใหม่ที่ได้แก้ไขมาตรา 15 ของพระราชบัญญัติเดิม ได้วางหลักว่าถ้าหากผู้ให้บริการร่วมมือ ให้ความยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดที่ระบุไว้ตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตนจะต้องได้รับโทษด้วยเช่นกัน เมื่อพิจารณาควบคู่กับคำสั่งของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ 163/2557 ที่ให้อำนาจคณะทำงานทดสอบระบบเฝ้าติดตามสื่อออนไลน์ประสานทางเทคนิคกับผู้ประกอบการและผู้ให้บริการอินเทอร์เน็ตภายในประเทศและที่เชื่อมต่อกับต่างประเทศโดยตรง ในการทดสอบระบบเฝ้าติดตามสื่อออนไลน์ จะพบว่าการบัญญัติกฎหมายลักษณะนี้เป็นการควบคุมผู้ให้บริการเว็บไซต์ หรือ อินเทอร์เน็ตเกตเวย์ต่างๆ ให้จำเป็นต้องร่วมมือและช่วยเหลือเจ้าหน้าที่ของรัฐในการเข้าถึงและระงับข้อมูลที่ถูกเข้ารหัส เพราะถ้าหากไม่ให้ความร่วมมือจะได้รับโทษตามกฎหมาย ร่างกฎหมายดังกล่าวจึงเป็นการบัญญัติเปิดช่องให้หน่วยงานของรัฐควบคุมผู้ให้บริการทางอินเทอร์เน็ตต่างๆได้ เพื่อเอื้อประโยชน์ต่อการเข้าถึง ดักรับและประมวลผลข้อมูลส่วนบุคคลที่อยู่ในระบบอินเทอร์เน็ต

ฉะนั้นตามร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มาตรา 9 และ 14 ที่มีการบัญญัติให้รัฐมนตรีสามารถออกประกาศเพิ่มเติมเกี่ยวกับหลักเกณฑ์และขั้นตอนวิธีการระงับการเข้าถึงข้อมูลคอมพิวเตอร์นั้น เป็นบทบัญญัติที่จะเป็นบ่อเกิดการใช้อำนาจของเจ้าหน้าที่ของรัฐอย่างกว้างขวางตามมา โดยอำนาจของเจ้าหน้าที่ของรัฐรวมไปถึงอำนาจในการเข้าถึงและระงับข้อมูลที่มีการเข้ารหัสอีกด้วย การบัญญัติกฎหมายดังกล่าวทำให้ระบบอินเทอร์เน็ตไม่มีความปลอดภัยอีกต่อไป ภาคเอกชนและปัจเจกบุคคลย่อมอาจถูกหน่วยงานของรัฐเข้าสอดแนมหรือรวบรวมประมวลผลข้อมูลส่วนบุคคลของตนที่ไหน เมื่อไหร่ เวลาใดก็ได้ จึงเป็นการบัญญัติให้อำนาจหน่วยงานของรัฐอย่างกว้างขวางเพื่อสร้างความชอบธรรมที่จะแทรกแซงข้อมูลส่วนบุคคล เมื่อเทียบเคียงกับโครงการปริซึมซึ่งเป็นโครงการลับที่ให้อำนาจเจ้าหน้าที่ของรัฐสามารถเข้าถึงข้อมูลส่วนบุคคลได้ในปริมาณมาก และไม่เฉพาะเจาะจงเป้าหมาย พบว่ามีลักษณะคล้ายคลึงกับการให้อำนาจหน่วยงานของรัฐตามร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พิจารณาประกอบกับคำสั่งของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ 163/2557 เป็นอย่างยิ่ง

นอกจากนี้ร่างพระราชบัญญัติดังกล่าวยังมีข้อให้พิจารณาต่อไปได้อีกว่าการบัญญัติกฎหมายที่ให้อำนาจรัฐมนตรีซึ่งเป็นฝ่ายบริหารสามารถออกประกาศและคำสั่งเพิ่มเติมได้ ถ้าหากคำสั่งที่ออกตามมานั้นกระทบกระเทือนต่อสิทธิในความเป็นส่วนตัวของบุคคลจะเป็นการขัดต่อหลักนิติรัฐ เนื่องจากสาระสำคัญของหลักนิติรัฐนั้นอำนาจในการบัญญัติกฎหมายที่จะละเมิดสิทธิและเสรีภาพของบุคคลนั้นจะต้องออกโดยฝ่ายนิติบัญญัติ ซึ่งเป็นตัวแทนที่ได้รับเลือกโดยประชาชนเข้าไปตรากฎหมาย ดังนั้นการกำหนดให้อำนาจฝ่ายบริหารสามารถออกกฎเกณฑ์ที่เป็นการละเมิดสิทธิของ

บุคคลจึงเป็นการให้อำนาจฝ่ายบริหารมากเกินไป เพราะเป็นการให้อำนาจนิติบัญญัติแก่ฝ่ายบริหาร ซึ่งจะขัดต่อหลักการแบ่งแยกอำนาจได้

(2.3) ร่างประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่องมาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัวและเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม อาศัยอำนาจตามพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์และกิจการโทรคมนาคม พ.ศ. 2553 โดยหลักของประกาศนี้ผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมจะประมวลผลข้อมูลส่วนบุคคลได้เมื่อได้รับความยินยอมจากผู้ใช้บริการ และเป็นการกระทำเพื่อประโยชน์ในการดำเนินกิจการโทรคมนาคมเท่านั้น อย่างไรก็ตามได้มีข้อยกเว้นให้ไม่ต้องปฏิบัติตามหลักการได้รับความยินยอมหากเป็นการเปิดเผยข้อมูลส่วนบุคคลต่อหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเพื่อรักษาความมั่นคงของรัฐหรือเพื่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนและปฏิบัติครบถ้วนตามกระบวนการที่กฎหมายนั้นบัญญัติ[47] ร่างประกาศนี้ยังกำหนดให้ผู้รับใบอนุญาตสามารถดักฟัง ตรวจ กักสัญญาณหรือเปิดเผยสิ่งสื่อสารถึงกันโดยทางโทรคมนาคมที่บุคคลติดต่อถึงกันได้ ถ้าหากมีบทบัญญัติแห่งกฎหมายเฉพาะเพื่อรักษาความมั่นคงของรัฐหรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนให้กระทำได้[48] อีกทั้งยังมีการกำหนดให้ผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมมีหน้าที่ส่งข้อมูลส่วนบุคคลที่ผู้รับใบอนุญาตครอบครองให้แก่คณะกรรมการและสำนักงานเมื่อคณะกรรมการและสำนักงานร้องขอได้อีกด้วย[49] ประกาศดังกล่าวจึงมีการให้อำนาจแก่หน่วยงานของรัฐอย่างกว้างขวางในการเข้าถึงข้อมูลส่วนบุคคลได้อย่างไม่มีข้อจำกัด โดยอาศัยเหตุแห่งความมั่นคงของรัฐเช่นกัน การกำหนดให้หน่วยงานของรัฐเข้าถึงและประมวลผลข้อมูลส่วนบุคคลได้หากเป็นกรณีที่เกี่ยวกับความมั่นคงของรัฐนั้น เหมือนกับกรณีที่สำนักงานความมั่นคงแห่งชาติสหรัฐอเมริกาสามารถเข้าถึงและประมวลผลข้อมูลส่วนบุคคลในประเทศสหรัฐอเมริกาได้โดยอ้างเหตุกระทำการเพื่อความมั่นคงของรัฐเช่นเดียวกัน

แม้ประเทศไทยจะมีความพยายามในการออกกฎหมายกลางที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป ดังที่ได้มีการจัดทำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

---

[47] ร่างประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่องมาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัวและเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม, ข้อ 6

[48] *เพิ่งอ้าง*, ข้อ 15

[49] *เพิ่งอ้าง*, ข้อ 19

พ.ศ. .... แต่เมื่อพิจารณากฎหมายไทยเทียบตามหลักเกณฑ์การตัดสินของศาลยุติธรรมแห่งสหภาพยุโรปในคดีเลขที่ C-362/14 ที่ได้ตัดสินชี้ขาดให้โครงการเซฟฮาร์เบอร์สิ้นผลไปนั้น พบว่ามีความเหมือนกันในสาระสำคัญดังต่อไปนี้

(1) ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ได้มีการบัญญัติข้อยกเว้นให้ไม่ต้องปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคลได้ ในกรณีที่มีกฎหมายอื่นบัญญัติให้กระทำการเป็นอย่างอื่น ตามมาตรา 17, 18 และ 21

(2) ประเทศไทยมีกฎหมายที่จะประกาศใช้ต่อไปบางฉบับที่ได้บัญญัติให้หน่วยงานของรัฐมีอำนาจกว้างขวางในการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล โดยหน่วยงานของรัฐสามารถเข้าถึงข้อมูลส่วนบุคคลได้อย่างไม่มีขอบเขตจำกัด สามารถเก็บรวบรวมและประมวลผลข้อมูลได้ในจำนวนมาก ดังเช่น ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. .... มาตรา 35, ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... มาตรา 9 และ 14, คำสั่งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ 163/2557, ร่างประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ ข้อ 6, 15 และ 19

จะเห็นได้ว่ามาตรการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยที่จะบังคับใช้ต่อไปภายภาคหน้านั้นเข้าองค์ประกอบทั้งสองประการอันเป็นเหตุผลของศาลยุติธรรมแห่งสหภาพยุโรปในการวินิจฉัยว่าประเทศนั้นๆ มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ เมื่อเปรียบเทียบกับการที่ศาลยุติธรรมแห่งสหภาพยุโรปได้ตัดสินให้โครงการเซฟฮาร์เบอร์สิ้นผลไปเพราะเหตุที่มีข้อยกเว้นเอาไว้ให้องค์กรที่เข้าร่วมโครงการไม่ต้องปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลของโครงการเซฟฮาร์เบอร์ได้ หากมีกฎหมายของประเทศสหรัฐอเมริกาให้กระทำการเป็นอย่างอื่น หลักการของกฎหมายคุ้มครองส่วนบุคคลของประเทศไทยก็ไม่แตกต่างกัน ดังนั้นหากประเทศไทยประสงค์จะรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรป หรือประเทศอื่นๆที่บังคับใช้กฎหมายตามแนว Directive 95/46/EC ก็อาจถูกตัดสินชี้ขาดได้ว่าประเทศไทยมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ อันจะทำให้ไม่สามารถรับโอนข้อมูลส่วนบุคคลจากประเทศเหล่านั้นได้

อนึ่ง ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ยังมีการบัญญัติให้ไม่ต้องปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคลตามกรณีอื่นที่กำหนดในกฎกระทรวง ข้อยกเว้นตามการกำหนดในกฎกระทรวงนี้ปรากฏอยู่ในเรื่องของหลักการเก็บรวบรวมข้อมูลส่วนบุคคลที่ไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล[50], การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว

[50] ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...., มาตรา 21

โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล[51], การปฏิเสธสิทธิของเจ้าของข้อมูลส่วนบุคคลในการขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตน[52] เป็นต้น

แม้ว่าการบัญญัติกฎหมายให้สามารถกำหนดหลักเกณฑ์เพิ่มเติมโดยออกกฎกระทรวงนั้นจะบัญญัติได้เพื่อสร้างความยืดหยุ่นในการบังคับใช้กฎหมาย และให้ทันต่อสถานการณ์ที่มีความเปลี่ยนแปลงไป แต่การออกกฎกระทรวงก็ควรจะใช้ในกรณีที่เป็นลักษณะการอธิบายขยายความ ชี้แจงรายละเอียดหรือแนวทางปฏิบัติที่ไม่ได้กำหนดไว้ในพระราชบัญญัติเท่านั้น แต่ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้มีการให้อำนาจรัฐมนตรีออกกฎกระทรวงในเรื่องที่เกี่ยวกับการยกเว้นไม่ต้องปฏิบัติตามมาตรการในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งการออกกฎเกณฑ์ที่ละเมิดต่อสิทธิในข้อมูลส่วนบุคคลโดยหลักแล้วจะต้องกระทำโดยฝ่ายนิติบัญญัติ ในกรณีการกำหนดให้ข้อยกเว้นสามารถออกโดยกฎกระทรวงได้จึงเป็นข้อยกเว้นที่ให้อำนาจฝ่ายบริหารมากเกินไป และเป็นการเปิดโอกาสให้ฝ่ายบริหารใช้อำนาจนิติบัญญัติเสียเองซึ่งขัดกับหลักการแบ่งแยกอำนาจ

นอกจากเหตุผลด้านการบัญญัติเนื้อหาของมาตรการคุ้มครองส่วนบุคคลข้างต้นนั้น กฎหมายที่บังคับใช้ในสหภาพยุโรปรวมถึงคำพิพากษาของศาลยุติธรรมแห่งสหภาพยุโรปล้วนให้ความสำคัญกับองค์กรที่มีหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นอย่างยิ่ง ดังจะเห็นได้จากอารัมภบท 62 ของDirective 95/46/EC ที่บัญญัติว่า “การจัดตั้งหน่วยงานที่มีอำนาจคุ้มครองข้อมูลส่วนบุคคลในประเทศสมาชิกซึ่งใช้อำนาจหน้าที่ได้อย่างอิสระสมบูรณ์เป็นองค์ประกอบสำคัญของการคุ้มครองปัจเจกชนสำหรับการประมวลผลข้อมูลส่วนบุคคล” หรือในคำพิพากษาคดี C-362/14 เองก็ได้อธิบายว่าการรับรองความเป็นอิสระของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแห่งชาตินั้นเป็นไปเพื่อรับรองความมีประสิทธิภาพและความน่าเชื่อถือในการทำหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล[53]

แต่เมื่อพิจารณาในแง่ขององค์กรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามกฎหมายไทยปรากฏว่าสำนักงานที่ทำหน้าที่ปฏิบัติงานวิชาการและงานธุรการให้แก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลคือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[54] คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจึงต้องพึ่งพาสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นอย่างมาก อีกทั้งยังต้องทำงานภายใต้โครงสร้างของ

---

[51] *เพิ่งอ้าง*, มาตรา 23

[52] *เพิ่งอ้าง*, มาตรา 26

[53] คำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปคดีเลขที่ C-362/14 ย่อหน้าที่ 41

[54] ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...., มาตรา 5 และ 16

กระทรวง การปฏิบัติงานอาจติดอยู่กับระบบราชการ อันจะให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลไม่มีความเป็นอิสระอย่างแท้จริง

นอกจากนี้เมื่อพิจารณาให้ดีแล้วคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นองค์กรที่ทำหน้าที่ปกป้องคุ้มครองสิทธิของบุคคล ในขณะเดียวกันคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นองค์กรที่ดำเนินมาตรการเพื่อป้องกันสถานการณ์ด้านภัยคุกคามทางไซเบอร์อันจะกระทบต่อความมั่นคงของชาติ จะเห็นได้ว่าวัตถุประสงค์ของกฎหมายอันเป็นที่มาขององค์กรทั้งสองนั้นมีความขัดกันเองระหว่างการคุ้มครองสิทธิของบุคคลกับความมั่นคงของชาติ จึงไม่ควรที่จะให้องค์กรทั้งสองดำเนินการอยู่ภายใต้กำกับของหน่วยงานเดียวกัน อีกทั้งการมีหน่วยงานในการดูแลเป็นหน่วยงานเดียวกันย่อมทำให้เจ้าหน้าที่ใช้อำนาจโดยมิชอบหรือตามอำเภอใจได้โดยง่าย เนื่องจากไม่มีการตรวจสอบและคานอำนาจ การใช้อำนาจจึงเป็นการรวมศูนย์อยู่ที่องค์กรใดองค์กรหนึ่งเพียงองค์กรเดียว ดังนั้นในแง่ของการจัดตั้งองค์กรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... จึงยังไม่มีความเป็นอิสระสมบูรณ์ และจะส่งผลให้การคุ้มครองข้อมูลส่วนบุคคลไม่สามารถทำได้อย่างมีประสิทธิภาพ[55]

5.3.2 ประเทศไทยในฐานะผู้โอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ฉบับที่ผ่านการพิจารณาโดยสำนักงานคณะกรรมการกฤษฎีกาไม่ได้ระบุหลักเกณฑ์ในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเอาไว้ โดยบัญญัติไว้เพียงให้เป็นหน้าที่ของคณะกรรมการคุ้มครองส่วนบุคคลในการกำหนดหลักเกณฑ์การโอนข้อมูลไปยังต่างประเทศต่อไป ตามร่างพระราชบัญญัตินี้ได้บัญญัติไว้เฉพาะในส่วนของข้อยกเว้นที่ทำให้สามารถโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้โดยไม่ต้องทำตามหลักเกณฑ์ทั่วไป จึงต้องรอประกาศจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าจะกำหนดให้การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเป็นไปในทิศทางใด มีระดับการคุ้มครองเพียงใด

อย่างไรก็ตามในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับเดิมที่ผ่านความเห็นชอบโดยคณะรัฐมนตรีนั้น ได้วางหลักเกณฑ์ในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเอาไว้ว่า ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยข้อมูลส่วนบุคคลไปยังประเทศที่มิได้มีบทบัญญัติในการให้ความคุ้มครองข้อมูลส่วนบุคคล หรือมีแต่บทบัญญัติของกฎหมายในประเทศนั้นมีมาตรการในการให้ความคุ้มครองข้อมูลส่วนบุคคลในสาระสำคัญต่ำกว่าบทบัญญัติแห่งพระราชบัญญัตินี้ โดยมิได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล ซึ่งหลักเกณฑ์ดังกล่าวก็สาระสำคัญคล้ายกับ Directive 95/46/EC เพราะเป็นการกำหนดข้อจำกัดในการโอนข้อมูลส่วนบุคคลไปยัง

[55] โปรดดูแนวทางการแก้ปัญหาในบทที่ 6 ส่วนข้อเสนอแนะ หน้า 155-156

ต่างประเทศเพื่อให้ข้อมูลส่วนบุคคลที่ถูกโอนไปยังต่างประเทศได้รับการคุ้มครองเฉกเช่นเดียวกับการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศ

แต่การกำหนดรายละเอียดในร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับเดิมมีรายละเอียดที่แตกต่างออกไปจาก Directive 95/46/EC อยู่บ้าง กล่าวคือตามกฎหมายไทยนั้นจะโอนข้อมูลส่วนบุคคลไปยังประเทศใดได้นั้น ประเทศนั้นจะต้องมีกฎหมายในการคุ้มครองส่วนบุคคล และกฎหมายนั้นต้องมีการคุ้มครองข้อมูลส่วนบุคคลในสาระสำคัญไม่ต่ำกว่ากฎหมายไทย แต่ตาม Directive 95/46/EC นั้น กำหนดไว้ว่าจะสามารถโอนข้อมูลส่วนบุคคลไปยังประเทศที่ไม่ใช่กลุ่มสมาชิกสหภาพยุโรปได้ ก็ต่อเมื่อประเทศนั้นมีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ การคุ้มครองดังกล่าวไม่จำกัดเฉพาะในรูปแบบของการบัญญัติกฎหมายเสมอไป จะเป็นวิธีการหรือมาตรการอื่นใดก็ได้ ต่างจากประเทศไทยมีบัญญัติให้เฉพาะประเทศที่มีการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบการบัญญัติกฎหมายเท่านั้นที่จะสามารถรับโอนข้อมูลส่วนบุคคลได้

ส่วนร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับปัจจุบันที่ผ่านการพิจารณาจากคณะกรรมการกฤษฎีกาแล้ว แม้จะไม่มีบัญญัติหลักเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเอาไว้ แต่เมื่อร่างพระราชบัญญัติฉบับนี้บังคับใช้ก็เป็นหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าจะกำหนดหลักเกณฑ์และรายละเอียดไปในทิศทางใด ซึ่งผู้เขียนมีความเห็นว่าควรวางหลักการให้สามารถโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ ถ้าหากประเทศนั้นมีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ ไม่ต่ำไปกว่าระดับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายไทย ซึ่งประเทศที่รับโอนข้อมูลส่วนบุคคลจะให้การคุ้มครองในลักษณะของการบัญญัติเป็นกฎหมายหรือเป็นมาตรการอื่นใดก็ได้

นอกจากนี้ถ้าหากมีการประกาศหลักเกณฑ์ในการโอนข้อมูลส่วนบุคคลขึ้นแล้ว หากประเทศที่เป็นฝ่ายรับโอนข้อมูลส่วนบุคคลไม่ผ่านคุณสมบัติตามหลักเกณฑ์ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด องค์กรในประเทศไทยที่เป็นผู้โอนข้อมูลส่วนบุคคลย่อมสามารถกลับไปใช้วิธีการทางเลือกอื่นในการคุ้มครองข้อมูลส่วนบุคคล เช่น การทำสัญญาเพื่อโอนข้อมูลส่วนบุคคล หรือ การให้ผู้รับโอนข้อมูลได้รับเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 34 เป็นต้น

บทที่ 6
บทสรุปและข้อเสนอแนะ

6.1 บทสรุป

ในยุคสมัยปัจจุบันข้อมูลส่วนบุคคลมีบทบาทสำคัญต่อการดำเนินกิจการทั้งในภาครัฐและเอกชน องค์กรต่างๆมีความจำเป็นต้องประมวลผลและถ่ายโอนข้อมูลระหว่างกันเป็นปกติ ยิ่งเทคโนโลยีเจริญก้าวหน้ามากเพียงใด ความเสี่ยงที่จะเกิดการล่วงละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลก็ย่อมมากขึ้นตามไปด้วย ด้วยเหตุนี้นานาประเทศจึงได้กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลขึ้นเพื่อปกป้องคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมิให้ถูกล่วงละเมิดได้ แต่ด้วยความแตกต่างทางด้านระบบกฎหมายและพื้นฐานแนวความคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่พัฒนามาไม่เหมือนกัน ส่งผลให้แต่ละประเทศนั้นมีมาตรการและวิธีการในการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน ในสถานการณ์เช่นนี้เองทำให้เมื่อต้องมีการโอนข้อมูลส่วนบุคคลจากประเทศหนึ่งไปยังอีกประเทศหนึ่งย่อมเกิดกรณีปัญหาว่าข้อมูลส่วนบุคคลเหล่านั้นจะยังคงได้รับการคุ้มครองอยู่หรือไม่ หรือได้รับการคุ้มครองเฉกเช่นเดียวกับก่อนที่ข้อมูลส่วนบุคคลจะถูกโอนไปหรือไม่ จะทำอย่างไรให้ข้อมูลส่วนบุคคลที่ถูกโอนไปยังต่างประเทศนั้นไม่ถูกละเมิดหรือกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล เพื่อแก้ปัญหาดังกล่าวบางกลุ่มประเทศจึงได้สร้างหลักเกณฑ์และข้อจำกัดในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศขึ้น

หลักเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่ถือเป็นแม่แบบและมีอิทธิพลต่อการสร้างหลักเกณฑ์การคุ้มครองให้กับประเทศอื่นๆคือ Directive 95/46/EC ซึ่งนอกจาก Directive นี้มีวัตถุประสงค์ในการสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้มีความเท่าเทียมกันทั่วทั้งสหภาพยุโรปแล้ว ยังได้สร้างข้อกำหนดในการโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปอีกด้วย ตามที่ข้อ 25 ได้บัญญัติหลักปฏิบัติเอาไว้ว่าประเทศสมาชิกสหภาพยุโรปจะถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปได้ ก็ต่อเมื่อประเทศที่รับโอนข้อมูลส่วนบุคคลนั้นสามารถรับรองระดับการคุ้มครองข้อมูลที่เพียงพอ โดยมีคณะกรรมาธิการยุโรปเป็นองค์กรที่ทำหน้าที่ตัดสินชี้ขาดว่าประเทศใดบ้างที่มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ซึ่งที่ผ่านมาคณะกรรมาธิการยุโรปจะพิจารณาโดยมีแนวทางจากคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลเพื่อใช้ในการประเมินระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

ผลกระทบจากการบัญญัติ Directive 95/46/EC ทำให้ประเทศอื่นๆที่ต้องการรับโอนข้อมูลจากกลุ่มประเทศสมาชิกสหภาพยุโรป จำเป็นต้องยกระดับกฎหมายคุ้มครองข้อมูลส่วนบุคคลใน

ประเทศของตน และหาวิธีการที่ทำให้มาตรการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศนั้นได้รับการรับรองจากคณะกรรมาธิการยุโรปว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เช่นวิธีการบัญญัติกฎหมายคุ้มครองส่วนบุคคลที่เป็นกฎหมายกลางขึ้นมา อย่างเช่นกฎหมาย PIPEDA ที่บังคับใช้ในประเทศแคนาดา หรือใช้วิธีการกำหนดแนวปฏิบัติที่องค์กรต่างๆสามารถเข้าร่วมได้โดยสมัครใจ ดังเช่น โครงการเซฟฮาร์เบอร์ที่ใช้ในประเทศสหรัฐอเมริกา

โครงการเซฟฮาร์เบอร์มีวัตถุประสงค์เพื่อให้องค์กรภายในประเทศสหรัฐอเมริกาสามารถรับโอนข้อมูลจากกลุ่มประเทศสมาชิกสหภาพยุโรปได้โดยสะดวกปราศจากอุปสรรค โดยองค์กรที่เข้าร่วมโครงการเซฟฮาร์เบอร์จะต้องปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคล 7 ประการ ซึ่งโครงการเซฟฮาร์เบอร์นั้นได้รับการรับรองจากคณะกรรมาธิการยุโรปโดยการออกคำวินิจฉัยที่ 2000/520 ว่าประเทศสหรัฐอเมริกาได้รับการพิจารณาว่ามีระดับการคุ้มครองที่เพียงพอสำหรับข้อมูลส่วนบุคคลที่ถูกถ่ายโอนจากสหภาพยุโรปไปยังองค์กรที่ได้รับการรับรองภายใต้โครงการเซฟฮาร์เบอร์ ส่งผลให้องค์กรของประเทศสหรัฐอเมริกาที่เข้าร่วมโครงการเซฟฮาร์เบอร์สามารถรับโอนข้อมูลจากกลุ่มประเทศสมาชิกสหภาพยุโรปได้อย่างไม่มีข้อจำกัดหรือเงื่อนไขอื่นใดเพิ่มเติม ประเทศสหรัฐอเมริกาสามารถรับโอนข้อมูลที่มาจากกลุ่มประเทศสมาชิกสหภาพยุโรปภายใต้โครงการเซฟฮาร์เบอร์เรื่อยมา

แต่อย่างไรก็ตาม ศาลยุติธรรมแห่งสหภาพยุโรปได้สร้างหลักเกณฑ์ในการพิจารณาระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอขึ้นเพิ่มเติมในการพิพากษาคดีเลขที่ C-362/14 เมื่อวันที่ 6 ตุลาคม ค.ศ. 2015 โดยได้พิพากษาให้คำวินิจฉัยที่ 2000/520 ที่ใช้รับรองโครงการเซฟฮาร์เบอร์สิ้นผลไป ในคดีนี้ศาลยุติธรรมแห่งสหภาพยุโรปได้วางหลักเอาไว้ชัดเจนว่าระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอนั้นคือการที่ประเทศนอกกลุ่มสมาชิกสหภาพยุโรปต้องรับรองระดับการคุ้มครองสิทธิและเสรีภาพขึ้นพื้นฐาน“เท่ากับ”ระดับการคุ้มครองที่ได้รับรองไว้ภายในสหภาพยุโรปตาม Directive 95/46/EC โดยประเทศนอกกลุ่มสมาชิกสหภาพยุโรปจะใช้มาตรการคุ้มครองข้อมูลส่วนบุคคลเป็นวิธีการใดก็ได้แต่จะต้องมีประสิทธิภาพในการคุ้มครองข้อมูลส่วนบุคคลเท่ากับระดับการคุ้มครองที่ใช้ภายในสหภาพยุโรปในทางปฏิบัติ

เหตุผลหลักของคำพิพากษาที่ทำให้ศาลตัดสินว่าโครงการเซฟฮาร์เบอร์มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ คือโครงการเซฟฮาร์เบอร์มีการกำหนดข้อยกเว้นให้องค์กรที่เข้าร่วมไม่ต้องปฏิบัติตามหลักการของโครงการเซฟฮาร์เบอร์ได้ หากเป็นกรณีเนื่องจากความจำเป็นในการคุ้มครองความมั่นคงของประเทศสหรัฐอเมริกา ประโยชน์สาธารณะ หรือข้อจำกัดโดยรัฐบัญญัติระเบียบของราชการ หรือกฎหมายที่มาจากบรรทัดฐานคำพิพากษาของศาลซึ่งได้สร้างข้อผูกพันที่ขัดแย้งกับหลักการเซฟฮาร์เบอร์ หากมีกฎหมายของประเทศสหรัฐอเมริกาบัญญัติขึ้น องค์กรของ

ประเทศสหรัฐอเมริกาจะต้องปฏิบัติตามกฎหมายภายในประเทศและสามารถเพิกเฉยต่อหลักการคุ้มครองข้อมูลส่วนบุคคลของโครงการเซฟฮาร์เบอร์ได้

แม้ว่าข้อจำกัดหรือยกเว้นมิให้ต้องปฏิบัติตามโครงการเซฟฮาร์เบอร์จะมีการบัญญัติขึ้นตั้งแต่ที่คณะกรรมาธิการยุโรปได้ออกคำวินิจฉัยที่ 2000/520 เพื่อรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลขององค์กรภายใต้โครงการเซฟฮาร์เบอร์ก็ตาม แต่เนื่องด้วยกฎหมายภายในของประเทศสหรัฐอเมริกาเปลี่ยนแปลงไปทำให้คำวินิจฉัยดังกล่าวไม่มีความชอบธรรมอีกต่อไป ดังจะเห็นได้จากในคำพิพากษาได้อ้างถึงการประเมินสถานการณ์จากการปฏิบัติตามคำวินิจฉัยของคณะกรรมาธิการยุโรปใน Communication COM (2013) 846 Final และ Communication COM (2013) 847 Final ซึ่งมีเนื้อความเกี่ยวกับแผนงานของหน่วยงานความมั่นคงแห่งชาติประเทศสหรัฐอเมริกาที่ได้จัดทำโครงการปริซึมซึ่งเป็นแผนงานรวบรวมข่าวกรองขนาดใหญ่อันมีฐานมาจากรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศที่ได้แก้ไขขึ้นใหม่

โครงการปริซึมให้อำนาจหน่วยงานของรัฐสามารถเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลขนาดใหญ่ได้ อันส่งผลให้หน่วยงานรัฐของประเทศสหรัฐอเมริกาสามารถเข้าถึงข้อมูลส่วนบุคคลที่ถูกโอนมาจากประเทศสมาชิกสหภาพยุโรปได้อย่างไร้ข้อจำกัด เป็นการเข้าถึงข้อมูลในปริมาณมาก สามารถเข้าถึงได้ตามอำเภอใจ ไม่เฉพาะเจาะจงบุคคล จึงเป็นการแทรกแซงสิทธิในข้อมูลส่วนบุคคลอันเป็นสิทธิขั้นพื้นฐาน การคุ้มครองข้อมูลส่วนบุคคลภายใต้โครงการเซฟฮาร์เบอร์จึงไม่เท่ากับระดับการคุ้มครองที่ใช้ภายในสหภาพยุโรปในทางปฏิบัติ ส่งผลทำให้คำวินิจฉัยที่ 2000/520 ล้มเหลวในการปฏิบัติตามข้อกำหนดตาม Directive 95/46/EC พิจารณาร่วมกับกฎบัตรสิทธิขั้นพื้นฐานแห่งสหภาพยุโรป คำวินิจฉัยที่ 2000/520 ที่เป็นการรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามโครงการเซฟฮาร์เบอร์จึงสิ้นผลไป คำพิพากษานี้เป็นการสร้างหลักเกณฑ์ใหม่ของการคุ้มครองข้อมูลส่วนบุคคลที่ส่งผลกระทบต่อนานาประเทศที่ต้องรับโอนข้อมูลจากกลุ่มประเทศสมาชิกสหภาพยุโรป

ในส่วนประเทศไทยขณะนี้ได้ดำเนินการบัญญัติกฎหมายกลางที่ใช้คุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น คือร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... โดยมีวัตถุประสงค์เพื่อขจัดช่องว่างของการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ยังกระจัดกระจายอยู่ตามพระราชบัญญัติต่างๆซึ่งไม่ครอบคลุมข้อมูลส่วนบุคคลทั้งหมด และเพื่อสร้างมาตรการในคุ้มครองข้อมูลส่วนบุคคลและกลไกการบังคับใช้ที่มีประสิทธิภาพมากยิ่งขึ้น แต่อย่างไรก็ตามเมื่อพิจารณาในแง่ของการรับโอนข้อมูลส่วนบุคคลจากต่างประเทศ โดยเทียบเคียงจากกรณีโครงการเซฟฮาร์เบอร์ตามคำพิพากษาคดีที่ C-362/14 จะพบว่าตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้นได้มีการเปิดช่องให้สามารถนำกฎหมายอื่นใดมาบังคับใช้เพื่อยกเว้นหลักการทั่วไปของการคุ้มครองข้อมูลส่วนบุคคลได้เช่นกัน ขณะเดียวกันประเทศไทยเองก็ได้ดำเนินกระบวนการบัญญัติกฎหมายอื่นที่ให้อำนาจ

หน่วยงานของรัฐสามารถเข้าแทรกแซงและเข้าถึงข้อมูลส่วนบุคคลได้อย่างไม่มีขอบเขตจำกัด และปราศจากการตรวจสอบใดๆ ดังเช่นร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ให้อำนาจคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติซึ่งเป็นหน่วยงานของรัฐมีอำนาจมากมายไร้ข้อจำกัด สามารถสั่งการให้หน่วยงานภาครัฐและภาคเอกชนปฏิบัติการใดๆ ตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ อีกทั้งร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติยังมีบทกฎหมายที่ให้อำนาจพนักงานเจ้าหน้าที่ให้สามารถตรวจสอบการสื่อสารของประชาชนได้ทุกช่องทาง และไม่ต้องมีหมายศาล ทำให้พนักงานเจ้าหน้าที่ของรัฐมีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลโดยไม่มีขอบเขตจำกัด โดยปราศจากกระบวนการตรวจสอบใดๆเลย หรือร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ที่มีบทบัญญัติให้อำนาจรัฐมนตรีอย่างกว้างขวาง อันจะก่อให้เกิดการใช้อำนาจในการเข้าถึงและประมวลผลข้อมูลส่วนบุคคลได้อย่างไร้ข้อจำกัด กฎหมายดังกล่าวจึงมีความคล้ายคลึงกับกฎหมายที่หน่วยงานความมั่นคงแห่งชาติของประเทศสหรัฐอเมริกาได้ใช้ในการจัดทำโครงการปริซึมที่อนุญาตให้เจ้าหน้าที่ผู้มีอำนาจได้เข้าถึงข้อมูลเพื่อการจัดเก็บและประมวลผลในสหรัฐอเมริกาได้อย่างไม่มีข้อจำกัดเช่นกัน เมื่อกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยมีข้อยกเว้นเปิดช่องให้นำกฎหมายอื่นมาใช้บังคับได้และจะมีการบังคับใช้กฎหมายอื่นๆที่มีบทบัญญัติให้อำนาจหน่วยงานของรัฐเข้าแทรกแซงสิทธิในข้อมูลส่วนบุคคลได้ไม่จำกัดเช่นกัน จึงเป็นกรณีที่ต้องตรงกับกรณีที่เกิดขึ้นกับโครงการเซฟฮาร์เบอร์ตามคำพิพากษาคดีที่ C-362/14 ทุกประการ ดังนั้นหากประเทศไทยต้องมีการรับโอนข้อมูลกับกลุ่มประเทศสมาชิกสหภาพยุโรปจะส่งผลให้ประเทศไทยถูกตัดสินชี้ขาดว่ามีการรับรองระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอได้

6.2 ข้อเสนอแนะ

การพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยเพื่อให้ได้รับการรับรองจากกลุ่มประเทศสมาชิกสหภาพยุโรปว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอจะส่งผลดีต่อประเทศไทยในอนาคต เนื่องจากจะทำให้ประเทศไทยสามารถรับโอนข้อมูลส่วนบุคคลจากกลุ่มประเทศสมาชิกสหภาพยุโรปและประเทศอื่นๆที่ใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลตามแนวทางกลุ่มสหภาพยุโรปได้ ทำให้การประกอบธุรกิจหรือกิจการระหว่างประเทศเป็นไปอย่างราบรื่นไร้ข้อจำกัด นอกจากนี้หากประเทศไทยพัฒนาระดับการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานของสหภาพยุโรปได้ ย่อมทำให้สิทธิในข้อมูลส่วนบุคคลของชาวไทยได้รับการคุ้มครองในระดับสูงอีกด้วย

การพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ทำได้โดยการเพิ่มเติมและแก้ไขเนื้อหาของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นๆที่เกี่ยวข้อง โดยจะแบ่งเป็น 2 ส่วนหลักๆคือ 1. ส่วนของกฎหมายคุ้มครองข้อมูลส่วนบุคคล 2. ส่วนของกฎหมายที่เป็นการยกเว้นหลักการคุ้มครองข้อมูลส่วนบุคคล ดังต่อไปนี้

6.2.1 กฎหมายคุ้มครองข้อมูลส่วนบุคคล

จากการศึกษามาตรการคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศรวมไปถึงคำพิพากษาของศาลยุติธรรมแห่งสหภาพยุโรปจะเห็นว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มีจุดที่ต้องปรับปรุงแก้ไขก่อนการบังคับใช้ เพื่อให้มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพและสามารถคุ้มครองสิทธิของบุคคลได้อย่างแท้จริง ดังจะแยกเป็นส่วนเนื้อหาของมาตรการในการคุ้มครองข้อมูลส่วนบุคคล มาตรการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวกับตน และ องค์กรที่ทำหน้าที่ในการตรวจสอบและบังคับการให้เป็นไปตามกฎหมาย

(1) เนื้อหาของมาตรการในการคุ้มครองข้อมูลส่วนบุคคล

ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ได้วางระบบในการจัดการข้อมูลส่วนบุคคล ทั้งการกำหนดกฎเกณฑ์ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลบนพื้นฐานของหลักการสากลในการคุ้มครองข้อมูลส่วนบุคคล เช่น หลักความยินยอมของเจ้าของข้อมูลส่วนบุคคล หลักความจำเป็น หลักการระบุวัตถุประสงค์เป็นต้น

แต่อย่างไรก็ตาม การคุ้มครองข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติดังกล่าวได้มีการบัญญัติข้อยกเว้นมิให้ต้องปฏิบัติตามมาตรการในการคุ้มครองข้อมูลส่วนบุคคลได้ ทั้งข้อยกเว้นโดยเฉพาะเจาะจงที่ระบุไว้ในบทบัญญัติ และข้อยกเว้นทั่วไปที่เป็นการเปิดช่องให้ใช้บังคับตามกฎหมายอื่นหรือตามกฎกระทรวงที่ออกมาภายหลัง การที่ร่างพระราชบัญญัตินี้ได้มีการบัญญัติข้อยกเว้นที่มีขอบเขตกว้างขวางเอาไว้จะเกิดปัญหาในการคุ้มครองข้อมูลส่วนบุคคลได้

ผู้เขียนจึงเห็นว่าการบัญญัติข้อยกเว้น โดยเฉพาะข้อยกเว้นที่อาจใช้บังคับตามกฎหมายอื่นได้นั้น ควรมีการระบุขอบเขตการบังคับใช้ให้ชัดเจน เช่น ระบุเพิ่มเติมไว้ในบททั่วไปว่าการบังคับใช้ตามกฎหมายอื่นจะสามารถกระทำได้เท่าที่จำเป็นโดยไม่กระทบกระเทือนต่อสาระสำคัญแห่งสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล และเพื่อป้องกันกรณีที่หน่วยงานของรัฐอาจใช้ช่องทางตามกฎหมายเข้าสอดแนมข้อมูลส่วนบุคคลอย่างไร้ข้อจำกัด ผู้เขียนเห็นด้วยกับมาตรา 29(4) ที่กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่จะต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า แต่ควรกำหนดระยะเวลาให้ชัดเจนลงไปด้วยว่าต้องแจ้งเจ้าของข้อมูลส่วนบุคคลภายในระยะเวลาเท่าใด เช่น ต้องแจ้งภายใน 24 ชั่วโมงหลังจากที่มีการละเมิดเป็นต้น

นอกจากนี้ควรเพิ่มเติมกรณีที่มีการขอเข้าถึงข้อมูลส่วนบุคคลจากหน่วยงานของรัฐ ไม่ว่าผู้ควบคุมข้อมูลส่วนบุคคลจะยินยอมปฏิบัติตามคำขอหรือไม่ก็ตามก็ควรรายงานการขอเข้าถึงข้อมูลส่วนบุคคลนั้นให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบด้วย โดยจะใช้วิธีการจัดทำเป็นรายงานสรุปประจำปีของผู้ควบคุมข้อมูลก็ได้ เพื่อให้เป็นไปตามหลักความโปร่งใสและสามารถตรวจสอบได้

ในส่วนของข้อยกเว้นที่ให้อำนาจรัฐมนตรีออกกฎกระทรวงมาบังคับใช้เป็นการเพิ่มเติมนั้น ผู้เขียนเห็นว่าไม่ควรจะบัญญัติไว้ในมาตราที่เป็นการกำหนดข้อยกเว้นให้ไม่ต้องปฏิบัติตามมาตรการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล เช่นมาตรา 21(5), มาตรา 23(5), มาตรา 26(6) เป็นต้น เนื่องจากการให้อำนาจออกกฎกระทรวงนั้นควรเป็นไปเพื่อการลงรายละเอียด หรือขยายความเพิ่มเติมจากบทบัญญัติเท่านั้น อีกทั้งในร่างพระราชบัญญัติดังกล่าวก็มีการระบุข้อยกเว้นเอาไว้เฉพาะเจาะจงเป็นข้อๆชัดเจนอยู่แล้ว มิจำต้องเปิดโอกาสให้มีการออกกฎกระทรวงเพิ่มเติมอีก

นอกจากนี้การเก็บข้อมูลชนิดที่มีความอ่อนไหว ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มาตรา 23 มิได้มีการระบุหลักเกณฑ์การเก็บรวบรวมข้อมูลที่แตกต่างจากข้อมูลส่วนบุคคลทั่วไป ทั้งที่โดยสภาพแล้วข้อมูลชนิดนี้มีความละเอียดอ่อน และต้องใช้ความระมัดระวังในการประมวลผลข้อมูลมากกว่าข้อมูลชนิดอื่นเนื่องจากเป็นข้อมูลที่สามารถกระทบต่อความเป็นส่วนตัวของบุคคลได้สูงกว่าข้อมูลทั่วไป จึงควรมีการกำหนดให้การเก็บข้อมูลชนิดนี้มีความเข้มงวดมากกว่าข้อมูลชนิดอื่น เช่น การให้ความยินยอมโดยเจ้าของข้อมูลนั้นต้องกระทำโดยชัดแจ้งเป็นหนังสือ

(2) มาตรการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวกับตน

ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ได้กำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล และกำหนดให้เจ้าของข้อมูลส่วนบุคคลขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งพระราชบัญญัติเท่านั้น แต่อย่างไรก็ตามแนวทางในการคุ้มครองข้อมูลส่วนบุคคลตาม Directive ของสหภาพยุโรปที่ได้มีการปรับปรุงใหม่นั้น ได้เพิ่มเติมสิทธิในการลบข้อมูลทั้งหมด (Right to be Forgotten) ให้แก่เจ้าของข้อมูลส่วนบุคคล ซึ่งเป็นการเพิ่มสิทธิให้แก่เจ้าของข้อมูลส่วนบุคคลในการจัดการข้อมูลที่เกี่ยวกับตนโดยเฉพาะข้อมูลที่อยู่ในระบบออนไลน์ ถ้าหากเจ้าของข้อมูลส่วนบุคคลไม่ยินยอมให้มีการเผยแพร่ข้อมูลส่วนบุคคลอีกต่อไป หรือข้อมูลนั้นมีความไม่ถูกต้องล้าสมัย ก่อให้เกิดความเข้าใจผิด เจ้าของข้อมูลส่วนบุคคลก็มีสิทธิในการขอให้มีการลบหรือทำลายข้อมูลส่วนบุคคลเหล่านั้นได้ ดังนั้นผู้เขียนเห็นว่าเพื่อทำให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการจัดการเกี่ยวกับข้อมูลของตนได้เต็มที่และรองรับกับสิทธิที่มีการเพิ่มเติมขึ้นใหม่ในสหภาพยุโรป ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจึงไม่ควรบัญญัติให้เจ้าของข้อมูลจะขอลบหรือทำลายข้อมูล

ส่วนบุคคลได้เฉพาะในกรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งพระราชบัญญัติเท่านั้น แต่เห็นควรให้เป็นไปตามหลักความยินยอม กล่าวคือถ้าหากเจ้าของข้อมูลส่วนบุคคลไม่ยินยอมให้มีการจัดเก็บหรือประมวลข้อมูลส่วนบุคคลนั้นอีกต่อไป ก็เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่จะต้องจัดการลบ ซ่อน หรือจัดการทำให้ข้อมูลเหล่านั้นไม่สามารถระบุตัวเจ้าของข้อมูลได้

ส่วนการเยียวยาความเสียหายในกรณีที่ผู้ควบคุมข้อมูลได้ดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลอันทำให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล ร่างพระราชบัญญัตินี้ได้มีการบัญญัติให้ผู้ควบคุมข้อมูลต้องชดใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคลตามมาตรา 42 แต่มีการกำหนดเหตุยกเว้นความรับผิดเอาไว้ ในกรณีที่ผู้ควบคุมข้อมูลปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามอำนาจหน้าที่ตามกฎหมาย ผู้เขียนเห็นว่าการกำหนดยกเว้นความรับผิดของผู้ควบคุมข้อมูลเอาไว้เช่นนี้เป็นการเปิดโอกาสให้หน่วยงานของรัฐใช้อำนาจตามกฎหมายอื่นในการเข้าถึงและดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลโดยที่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้เหตุนี้เป็นการยกเว้นมิให้ต้องชดใช้ค่าสินไหมทดแทนได้ ทำให้เจ้าของข้อมูลส่วนบุคคลไม่ได้รับการเยียวยาตามกฎหมายอย่างแท้จริง

(3) องค์กรที่ทำหน้าที่ในการตรวจสอบและบังคับการให้เป็นไปตามกฎหมาย

ผู้เขียนเห็นว่าควรมีการกำหนดสัดส่วนของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่มาจากสายข้าราชการและบุคคลภายนอกผู้ทรงคุณวุฒิในอัตราส่วนที่เท่าๆกัน อีกทั้งควรเพิ่มกรรมการที่มาจากภาคเอกชนที่เกี่ยวข้องกับการดำเนินการจัดเก็บและประมวลข้อมูลจำนวนมากด้วย เพื่อให้เกิดการถ่วงดุลระหว่างฝ่ายการเมืองกับผู้เชี่ยวชาญทางวิชาการและองค์กรอิสระต่างๆ ซึ่งจะส่งผลให้การใช้อำนาจเป็นไปเพื่อประโยชน์ของประชาชนอย่างแท้จริง

นอกจากนี้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลควรมีอำนาจในการรับเรื่องร้องเรียนและพิจารณาข้อพิพาทด้วย เพื่อให้องค์กรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบและดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลได้อย่างเบ็ดเสร็จสมบูรณ์ในองค์กรเดียว ตามที่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลให้มีการแต่งตั้งคณะกรรมการผู้เชี่ยวชาญขึ้นมาพิจารณาเรื่องดังกล่าวอีกย่อมทำให้เกิดความล่าช้าและซ้ำซ้อนในการปฏิบัติหน้าที่ จึงควรมีการให้อำนาจพิจารณาข้อร้องเรียน ตรวจสอบและไกล่เกลี่ยข้อพิพาทเป็นอำนาจของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามแนวทางของ Directive 95/46/EC

ยิ่งไปกว่านั้นเพื่อให้องค์กรที่ทำหน้าที่ตรวจสอบและบังคับการให้เป็นตามกฎหมายในประเทศไทยมีความเข้มแข็งและมีอำนาจคุ้มครองข้อมูลส่วนบุคคลได้จริง ผู้เขียนเห็นว่าควรกำหนดองค์กรให้มีอำนาจหน้าที่คล้ายกับคณะกรรมการแห่งชาติว่าด้วยข้อมูลข่าวสารและเสรีภาพประเทศฝรั่งเศส (Commission Nationale de l'informatique et des Libertés หรือ CNIL) ซึ่งเป็นองค์กรอิสระที่มีอำนาจในการควบคุมบังคับการให้มีการปฏิบัติตามกฎหมายคุ้มครอง

ข้อมูลทั้งระบบ โดยกฎหมายคุ้มครองข้อมูลของฝรั่งเศสมีขอบเขตครอบคลุมระบบข้อมูลทั้งที่อยู่ในความดูแลของภาครัฐและภาคเอกชน คณะกรรมการแห่งชาติว่าด้วยข้อมูลข่าวสารและเสรีภาพของฝรั่งเศสจึงมีอำนาจรอบด้านรวมไปถึงอำนาจในเชิงรุกด้วย อีกทั้งคณะกรรมการฯยังมีอำนาจตรวจสอบผู้ประกอบการทางธุรกิจในการประมวลผลข้อมูลส่วนบุคคลได้และสามารถตรวจสอบดูแลกลไกการคุ้มครองและการพิจารณาคดีในองค์กรต่างๆด้วย

ส่วนสำนักงานที่มีหน้าที่ปฏิบัติงานวิชาการและงานธุรการเพื่อประโยชน์ในการปฏิบัติงานของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลนั้นไม่ควรให้อยู่ในความดูแลของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แต่ควรจัดตั้งสำนักงานข้อมูลข่าวสารแห่งชาติขึ้นเป็นองค์กรกลางที่มีอำนาจปฏิบัติงานครอบคลุมข้อมูลทั้งที่อยู่ในภาครัฐและภาคเอกชน การรวมองค์กรที่ทำหน้าที่คุ้มครองข้อมูลเป็นองค์กรเดียวจะทำให้ระบบการคุ้มครองข้อมูลมีเอกภาพ ไม่เหลื่อมล้ำซ้ำซ้อน และมีประสิทธิภาพในการคุ้มครองข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่กฎหมายมุ่งคุ้มครอง สำนักงานนี้ควรเป็นส่วนราชการไม่สังกัดสำนักนายกรัฐมนตรี กระทรวง ทบวง หรือ กรมใดๆ ซึ่งจะทำให้การปฏิบัติงานของสำนักงานมีความเป็นอิสระและคล่องตัว เนื่องจากไม่ขึ้นกับระบบราชการและอยู่ภายใต้กำกับของกระทรวงใด องค์กรนี้จึงจะเป็นอิสระจากฝ่ายบริหารและฝ่ายการเมืองอย่างแท้จริง

6.2.2 เนื้อหาของกฎหมายที่เป็นการยกเว้นหลักการคุ้มครองข้อมูลส่วนบุคคล

กฎหมายบางฉบับอาจมีเนื้อหาที่เป็นการจำกัดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งเป็นไปเพื่อประโยชน์สาธารณะหรือความมั่นคงของชาติเป็นต้น อย่างไรก็ตามกฎหมายที่เป็นการล่วงล้ำสิทธิของประชาชนนั้นจะต้องพอสมควรแก่เหตุ และไม่กระทบกระเทือนถึงสาระสำคัญแห่งสิทธินั้นด้วย

ส่วนของกฎหมายที่ให้อำนาจรัฐเข้าสอดแนมข้อมูลส่วนบุคคลได้นั้นเป็นกฎหมายที่แทรกแซงก้าวล่วงสิทธิของบุคคลจึงต้องมีการบัญญัติโดยระมัดระวัง ซึ่งปัจจุบันมีหลักการระหว่างประเทศว่าด้วยการใช้หลักสิทธิมนุษยชนกับการสอดแนมการสื่อสาร[1] (International Principles on the Application of Human Rights to Communications Surveillance) ได้กำหนดหลักความจำเป็นและได้สัดส่วนในเรื่องการสอดแนมข้อมูลของรัฐเอาไว้ 13 ประการ ดังนี้

(1) ไม่มีกฎหมายไม่มีอำนาจ

การจำกัดสิทธิความเป็นส่วนตัวต้องมีกฎหมายรองรับ รัฐต้องไม่ปฏิบัติหรือนำมาตรการที่แทรกแซงสิทธิความเป็นส่วนตัวมาใช้โดยปราศจากข้อกฎหมายรองรับ โดยข้อกฎหมาย

[1] ดูฉบับภาษาไทยแปลโดยเครือข่ายพลเมืองเน็ตที่ https://necessaryandproportionate.org/th/ หรือ ดูต้นฉบับภาษาอังกฤษและคำแปลภาษาอื่นได้ที่ https://necessaryandproportionate.org/

ดังกล่าวต้องเป็นกฎหมายที่การบังคับใช้อยู่ก่อนแล้วและเปิดเผยต่อสาธารณชน อีกทั้งบทบัญญัตินั้นต้องมีความชัดเจนและแม่นยำเพียงพอที่สามารถรับรองว่าบุคคลจะคาดหมายได้ถึงการใช้กฎหมายและเล็งเห็นผลที่จะเกิดขึ้นจากการใช้กฎหมายได้ โดยเมื่อพิจารณาถึงการเปลี่ยนแปลงของเทคโนโลยีที่เป็นอยู่ กฎหมายที่จำกัดสิทธิความเป็นส่วนตัวควรได้รับการทบทวนเป็นระยะ ทั้งนี้โดยผ่านกระบวนการนิติบัญญัติหรือการกลไกกำกับดูแล

หลักการดังกล่าวมีความสำคัญในการควบคุมการใช้อำนาจรัฐให้อยู่ภายในกรอบของกฎหมาย โดยกฎหมายนั้นต้องมีความชัดเจนเพียงพอด้วย เห็นได้จากตัวอย่างในประเทศสหรัฐอเมริกาเองที่ขณะนี้มูลนิธิวิกิมีเดีย (Wikimedia Foundation) ได้ฟ้องสำนักงานความมั่นคงแห่งชาติและกระทรวงยุติธรรมของสหรัฐอเมริกาต่อศาล เนื่องจากปัญหาของโครงการสอดแนมข้อมูลประชาชนโดยเฉพาะการสอดแนมแบบอัพสตรีม (Upstream) ที่สามารถเจาะเข้าไปในโครงข่ายหลักของอินเทอร์เน็ตเพื่อดักรับข้อมูลจากระดับผู้ให้บริการอินเทอร์เน็ต ทำให้สำนักงานความมั่นคงแห่งชาติสามารถทำสำเนาการสื่อสารผ่านตัวหนังสือ ตั้งแต่อีเมล ข้อความพูดคุยออนไลน์ทางอินเทอร์เน็ต (chat) การค้นหาผ่านเว็บไซต์ รวมถึงสามารถค้นหาข้อมูลต่างๆผ่านการค้นหาคำที่เกี่ยวข้อง

ในคำฟ้องของมูลนิธิวิกิมีเดียระบุว่าการกระทำของสำนักงานความมั่นคงแห่งชาติเป็นการละเมิดบทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญฉบับที่ 4 (Fourth Amendment) ซึ่งปกป้องสิทธิความเป็นส่วนตัวและบทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญฉบับที่ 1 (First Amendment) ซึ่งปกป้องเสรีภาพในการแสดงออก นอกจากนี้สำนักงานความมั่นคงแห่งชาติยังใช้อำนาจเกินกว่าที่กฎหมายได้ให้ไว้ตามรัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศ เนื่องจากการสอดแนมข้อมูลได้กระทำในวงกว้าง และไม่ใช่แค่สอดแนมการสื่อสารเฉพาะบุคคลอันเป็นเป้าหมาย แต่รวมถึงผู้ที่มีเพียงความเกี่ยวข้องกับเป้าหมายและบุคคลผู้บริสุทธิ์ที่ไม่เกี่ยวข้องหลายล้านคนด้วย[2] คดีดังกล่าวอยู่ในระหว่างการพิจารณาของศาล ซึ่งคำตัดสินอาจกระทบต่ออำนาจการสอดแนมโดยหน่วยงานของรัฐในสหรัฐอเมริกาให้ต้องผูกพันและอยู่ภายใต้ขอบเขตที่กฎหมายรองรับและอาจส่งผลต่อการปฏิรูปกฎหมายที่ให้อำนาจรัฐสอดแนมข้อมูลส่วนบุคคลให้มีบทบัญญัติที่ชัดเจนแน่นอนมากยิ่งขึ้น

(2) วัตถุประสงค์ที่ชอบด้วยกฎหมายและเสมอภาค

กฎหมายควรอนุญาตให้การสอดแนมการสื่อสารทำได้โดยหน่วยงานของรัฐที่ถูกระบุอย่างเฉพาะเจาะจง เพื่อให้บรรลุวัตถุประสงค์อันชอบด้วยกฎหมายที่มีความสำคัญและจำเป็น

---

[2] ประชาไท, “วิกิมีเดียฟ้อง NSA หวังหยุดสอดแนมการสื่อสารประชาชน,” สืบค้นเมื่อวันที่ 15 มิถุนายน 2559, จาก http://prachatai.com/journal/2015/03/58382.

ต่อสังคมประชาธิปไตย และไม่ควรนำมาตรการใดๆมาใช้ในลักษณะที่เป็นการเลือกปฏิบัติบนพื้นฐานของเชื้อชาติ สีผิว เพศ ภาษา ศาสนา ความเห็นทางการเมืองหรือความเห็นอื่นๆ เป็นต้น

จากหลักการข้างต้นพิจารณาได้ว่ากฎหมายที่แยกวิธีการปฏิบัติระหว่างคนในชาติหรือผู้ที่อยู่ในดินแดนของรัฐให้แตกต่างจากบุคคลที่ไม่ใช่คนในชาติหรือผู้ที่อาศัยอยู่นอกประเทศทำให้เกิดการเลือกปฏิบัติและส่งผลให้บุคคลไม่ได้รับความคุ้มครองข้อมูลส่วนบุคคลได้อย่างเท่าเทียมกัน และถ้าหากไม่มีการระบุที่ชัดเจนว่าข้อมูลประเภทใดเป็นข้อมูลต่างชาติหรือข้อมูลในประเทศในทางปฏิบัติหน่วยสืบราชการลับต่างๆจะปฏิบัติในทางตีความว่าข้อมูลเหล่านั้นล้วนเป็นข้อมูลจากต่างชาติ ซึ่งส่งผลให้ข้อมูลเหล่านั้นไม่ได้รับการคุ้มครองตามสิทธิในความเป็นส่วนตัว ดังจะเห็นได้จากการบังคับใช้รัฐบัญญัติว่าด้วยการสืบราชการลับต่างประเทศในประเทศสหรัฐอเมริกา พระราชบัญญัติหน่วยงานด้านความมั่นคงของรัฐบาลในประเทศนิวซีแลนด์ พระราชบัญญัติการป้องกันประเทศในประเทศแคนาดา เป็นต้น

(3) ความจำเป็น

กฎหมายที่อนุญาตให้รัฐสอดแนมการสื่อสารต้องจำกัดการสอดแนมไว้อย่างเข้มงวดและต้องสามารถพิสูจน์ให้เห็นได้ว่าการสอดแนมเป็นสิ่งจำเป็นเพื่อบรรลุวัตถุประสงค์ที่ชอบด้วยกฎหมาย การสอดแนมการสื่อสารจะทำได้ต่อเมื่อเป็นหนทางเดียวที่จะบรรลุวัตถุประสงค์ที่ชอบธรรมนั้นได้ หรือในกรณีที่มีหนทางอื่นวิธีนี้ต้องเป็นหนทางที่น่าจะละเมิดสิทธิมนุษยชนน้อยสุด ภาระในการพิสูจน์เหตุผลเพื่อการสอดแนมดังกล่าวต้องตกเป็นของรัฐ ทั้งในกระบวนการทางศาลและกระบวนการนิติบัญญัติ

(4) ความเพียงพอ

การสอดแนมการสื่อสารแต่ละครั้งที่ได้รับอนุญาตให้กระทำได้ตามกฎหมายต้องมีความเหมาะสมเพื่อให้บรรลุเป้าหมายที่ชอบธรรมได้ ตามที่ระบุไว้อย่างเจาะจง

(5) ความได้สัดส่วน

การสอดแนมการสื่อสารถือเป็นการกระทำที่รุกล้ำและแทรกแซงสิทธิในความเป็นส่วนตัวและเสรีภาพในความคิดเห็นและการแสดงออกอย่างมาก จึงเป็นการคุกคามรากฐานของสังคมประชาธิปไตย การตัดสินใจใดๆเกี่ยวกับการสอดแนมการสื่อสารต้องกระทำโดยชั่งน้ำหนักประโยชน์ที่เล็งเห็นว่าจะได้เปรียบเทียบกับความเสียหายที่จะเกิดกับสิทธิของบุคคลและผลประโยชน์อื่นๆ และควรคำนึงถึงความอ่อนไหวของข้อมูลและความร้ายแรงของการละเมิดสิทธิความเป็นส่วนตัวด้วย

กล่าวอย่างเฉพาะเจาะจง หลักการนี้กำหนดว่าหากรัฐพยายามเข้าถึงหรือใช้ข้อมูลที่ได้รับการคุ้มครองไว้ผ่านการสอดแนมการสื่อสารในบริบทของการสอบสวนทางอาญา รัฐจะต้องพิสูจน์ยืนยันต่อองค์กรตุลาการที่มีอำนาจ เป็นอิสระและเป็นกลาง ได้ว่า

1. มีความเป็นไปได้อย่างสูงว่าอาชญากรรมร้ายแรงได้เกิดขึ้นแล้วหรือกำลังจะเกิดขึ้น

2. พยานหลักฐานของอาชญากรรมดังกล่าวจะสามารถได้มาด้วยการเข้าถึงข้อมูลที่ได้รับการคุ้มครอง

3. ได้ใช้วิธีการสอบสวนอื่นๆที่ละเมิดความเป็นส่วนตัวน้อยกว่านี้จนไม่เหลือวิธีที่ใช้ได้แล้ว

4. การเข้าถึงข้อมูลจะจำกัดอยู่เฉพาะส่วนที่เกี่ยวข้องโดยตรงกับอาชญากรรมตามที่มีการกล่าวหา และข้อมูลส่วนเกินที่ได้รับมาจะต้องถูกทำลายหรือถูกส่งกลับโดยทันที และ

5. ข้อมูลจะถูกเข้าถึงโดยหน่วยงานเฉพาะตามที่ระบุไว้ และจะถูกใช้สำหรับวัตถุประสงค์ที่ชอบด้วยกฎหมายตามที่ได้รับอนุญาตเท่านั้น

ส่วนกรณีที่รัฐพยายามเข้าถึงข้อมูลที่ได้รับการคุ้มครองผ่านการสอดแนมการสื่อสารสำหรับเป้าประสงค์ที่จะไม่เป็นเหตุให้บุคคลเสี่ยงต่อการถูกฟ้องคดีอาญา การถูกสอบสวน การถูกเลือกปฏิบัติ หรือการถูกละเมิดสิทธิมนุษยชน รัฐจะต้องพิสูจน์ยืนยันต่อองค์กรตุลาการที่เป็นอิสระและเป็นกลาง ได้ว่า

1. ได้พิจารณาวิธีการสอบสวนอื่นๆที่รุกล้ำความเป็นส่วนตัวน้อยกว่านี้แล้ว

2. การเข้าถึงข้อมูลจะจำกัดอยู่เฉพาะส่วนที่เกี่ยวข้องโดยตรง และข้อมูลส่วนเกินที่ได้รับมาจะต้องถูกทำลายหรือถูกส่งกลับไปยังบุคคลที่ได้รับผลกระทบโดยทันที และ

3. ข้อมูลจะถูกเข้าถึงโดยหน่วยงานเฉพาะตามที่ระบุไว้ และจะถูกใช้สำหรับวัตถุประสงค์เฉพาะตามที่ได้รับอนุญาตเท่านั้น

(6) องค์กรตุลาการที่มีอำนาจ

การตัดสินใจเกี่ยวกับการสอดแนมการสื่อสารต้องอยู่ภายใต้อำนาจวินิจฉัยขององค์ตุลาการที่มีความเป็นอิสระ เป็นกลาง และควรระบุหลักเกณฑ์ในการขออนุญาตต่อศาลเอาไว้อย่างชัดเจน อีกทั้งรัฐต้องระบุเหตุผลในการสอดแนมให้ศาลพิจารณาอย่างเหมาะสม[3] เพื่อป้องกันมิให้เกิดการใช้อำนาจที่ปราศจากการควบคุมโดยฝ่ายตุลาการ ยกตัวอย่างเช่น รัฐบัญญัติกำกับดูแลและดักรับการสื่อสาร ค.ศ. 2010 (Regulation of Interception of Communications Act) ของประเทศยูกันดาที่กำหนดเพียงให้หน่วยงานที่บังคับใช้กฎหมายแสดง “เหตุผลที่เหมาะสม” ต่อศาลเพื่อ

---

[3] คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ, “รายงานของผู้รายงานพิเศษว่าด้วยการส่งเสริมและคุ้มครองสิทธิและเสรีภาพด้านความเห็นและการแสดงออก แฟรงค์ ลารัว,” แปลโดยเครือข่ายพลเมืองเน็ต, สืบค้นเมื่อวันที่ 1 กุมภาพันธ์ 2559, จาก https://thainetizen.org/docs/a-hrc-23-40-surveillance-of-communications/.

อนุญาตให้สามารถสอดแนมข้อมูลเท่านั้น จึงเป็นเพียงการระบุหลักเกณฑ์ไว้เพียงเป็นพิธี ในกรณีดังกล่าวหน่วยงานของรัฐมีภาระพิสูจน์เพื่อแสดงความจำเป็นในการสอดแนมน้อยมาก จึงอาจส่งผลกระทบรุนแรงต่อการสอบสวน การเลือกปฏิบัติ หรือการละเมิดสิทธิมนุษยชนตามมา

นอกจากนี้ผู้เขียนเห็นว่าควรนำหลักการห้ามตีความของศาลแบบลับมาใช้ด้วย ตามที่ระบุรายงานประจำปีของข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติ[4] โดยต้องถือว่าการตีความหรือวินิจฉัยโดยลับของฝ่ายตุลาการไม่มีคุณสมบัติที่ชอบด้วยกฎหมาย ดังเช่นการพิจารณาโดยลับของศาลสืบราชการลับต่างประเทศในสหรัฐอเมริกา เนื่องจากการให้อำนาจสอดแนมโดยผ่านการวินิจฉัยจากฝ่ายตุลาการโดยปิดลับทำให้มีความเสี่ยงที่จะใช้อำนาจวินิจฉัยโดยพลการ ขัดกับหลักความโปร่งใสและไม่สามารถตรวจสอบได้

(7) กระบวนการอันชอบด้วยกฎหมาย

กระบวนการอันชอบด้วยกฎหมายกำหนดให้รัฐต้องเคารพและประกันสิทธิมนุษยชนของบุคคล โดยรัฐต้องรับรองได้ว่ามีการปฏิบัติตามขั้นตอนที่ถูกต้องทางกฎหมายที่กำกับดูแลการแทรกแซงสิทธิมนุษยชน มีการปฏิบัติตามอย่างสม่ำเสมอ และกระบวนการนั้นประชาชนทั่วไปสามารถรับรู้และเข้าถึงได้

บุคคลทุกคนย่อมมีสิทธิเข้าถึงการพิจารณาคดีอย่างเป็นธรรมและอย่างเปิดเผยต่อสาธารณะภายในระยะเวลาที่เหมาะสม โดยองค์กรตุลาการที่เป็นอิสระและเป็นกลาง เว้นแต่กรณีเร่งด่วนฉุกเฉิน กล่าวคือเมื่อมีภัยเฉพาะหน้าซึ่งจะทำให้เกิดอันตรายต่อชีวิตมนุษย์ ในกรณีเช่นนั้นจำเป็นให้มีการขออนุมัติย้อนหลังภายในระยะเวลาที่เหมาะสม การอ้างความเสี่ยงเพียงว่าอาจมีการหลบหนีหรือการทำลายพยานหลักฐานไม่อาจถือเป็นเหตุผลที่เพียงพอสำหรับการลงมือปฏิบัติก่อนแล้วขออนุมัติย้อนหลัง

(8) การแจ้งให้ผู้ใช้ทราบ

บุคคลพึงได้รับแจ้งข้อวินิจฉัยที่อนุญาตให้ทำการสอดแนมการสื่อสาร การแจ้งดังกล่าวต้องให้เวลาและข้อมูลมากพอที่บุคคลจะสามารถอุทธรณ์คำวินิจฉัยได้ บุคคลต้องสามารถเข้าถึงเอกสารหลักฐานที่ใช้เพื่อสนับสนุนการขออนุมัติดังกล่าว การชะลอการแจ้งออกไปจะกระทำได้เฉพาะในสถานการณ์ต่อไปนี้

---

[4] คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ, “การส่งเสริมและคุ้มครองสิทธิมนุษยชน สิทธิพลเมือง การเมือง เศรษฐกิจ สังคมและวัฒนธรรม รวมทั้งสิทธิด้านการพัฒนาสิทธิความเป็นส่วนตัวในยุคดิจิทัล รายงานของสำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติ,” แปลโดยเครือข่ายพลเมืองเน็ต, สืบค้นเมื่อวันที่ 15 ธันวาคม 2558, จาก https://thainetizen.org/docs/un-right-to-privacy-in-digital-age/

1. การแจ้งให้ทราบอาจส่งผลกระทบร้ายแรงต่อเป้าประสงค์ของการสอดแนมที่ได้รับอนุมัติ หรือมีภัยเฉพาะหน้าซึ่งจะทำให้เกิดอันตรายต่อชีวิตมนุษย์ หรือ

2. ในขณะที่อนุมัติให้สอดแนมได้ องค์กรตุลาการที่มีอำนาจได้อนุมัติให้ชะลอการแจ้งให้ทราบถึงการสอดแนมดังกล่าวได้ด้วย และ

3. บุคคลที่ได้รับผลกระทบได้รับแจ้งทันทีที่ภัยผ่านพ้นไปแล้ว หรือภายในระยะเวลาที่เหมาะสมที่สามารถปฏิบัติได้แล้วแต่ว่าเวลาใดจะถึงก่อน และจะต้องมีการแจ้งโดยทันทีเมื่อการสอดแนมการสื่อสารเสร็จสมบูรณ์แล้วไม่ว่าในสภาพการณ์ใด พันธกรณีในการแจ้งให้ทราบเป็นภาระของรัฐ แต่ในกรณีที่รัฐไม่แจ้งให้ทราบ ผู้ให้บริการการสื่อสารย่อมมีอิสระที่จะแจ้งให้บุคคลที่เกี่ยวข้องกับการสอดแนมการสื่อสารดังกล่าวได้ทราบโดยสมัครใจหรือเมื่อมีการร้องขอ

(9) ความโปร่งใส

รัฐควรมีความโปร่งใสเกี่ยวกับการใช้และขอบเขตของการสอดแนมการสื่อสารทั้งในเรื่องเทคนิคและอำนาจ โดยอย่างน้อยควรตีพิมพ์เผยแพร่ข้อมูลภาพรวมเกี่ยวกับจำนวนการร้องขอที่ได้อนุมัติและปฏิเสธ ข้อมูลการร้องขอที่จำแนกตามผู้ให้บริการแต่ละรายตามประเภทและเป้าประสงค์ของการสอบสวน รัฐควรจัดหาข้อมูลให้บุคคลอย่างเพียงพอเพื่อช่วยให้เข้าใจอย่างเต็มที่ถึงขอบเขต ลักษณะ และการบังคับใช้กฎหมายที่อนุญาตให้มีการสอดแนมการสื่อสาร รัฐยังควรดำเนินการให้ผู้ให้บริการสามารถเผยแพร่ขั้นตอนปฏิบัติที่ผู้ให้บริการจะใช้ในกรณีต้องยุ่งเกี่ยวกับการสอดแนมการสื่อสารโดยรัฐสามารถยึดถือขั้นตอนปฏิบัติดังกล่าว และสามารถเผยแพร่ประวัติการสอดแนมการสื่อสารโดยรัฐได้

(10) การตรวจสอบโดยสาธารณะ

รัฐควรกำหนดให้มีกลไกตรวจสอบที่เป็นอิสระเพื่อประกันความโปร่งใสและความรับผิดในการสอดแนมการสื่อสาร หากขาดการตรวจสอบโดยสาธารณะจะทำให้เกิดการแทรกแซงสิทธิได้โดยพลการและไม่ชอบด้วยกฎหมาย โดยกลไกการตรวจสอบจากภาคประชาชนที่เป็นอิสระและมีหน้าที่กำกับดูแลเป็นปัจจัยสำคัญในการประกันให้มีการคุ้มครองสิทธินั้นสัมฤทธิ์ผล

กลไกตรวจสอบควรมีอำนาจเข้าถึงข้อมูลทุกอย่างที่อาจเกี่ยวข้องกับการปฏิบัติงานของรัฐ และควรมีอำนาจเข้าถึงข้อมูลที่เป็นความลับหรือที่ถูกปกปิดได้ตามความเหมาะสม กลไกตรวจสอบควรมีอำนาจประเมินว่ารัฐได้ใช้อำนาจตามกฎหมายอย่างชอบธรรมหรือไม่ มีอำนาจประเมินว่ารัฐได้ตีพิมพ์เผยแพร่ข้อมูลการใช้และขอบเขตของเทคนิคและอำนาจเกี่ยวกับการสอดแนมการสื่อสารอย่างโปร่งใสและอย่างแม่นยำหรือไม่ และมีอำนาจตีพิมพ์เผยแพร่รายงานตามกำหนดเวลาและข้อมูลอื่นที่เกี่ยวข้องกับการสอดแนมการสื่อสาร กลไกตรวจสอบที่เป็นอิสระนี้ควรกำหนดให้มีควบคู่ไปกับการตรวจสอบใดๆ ที่มีอยู่แล้วโดยหน่วยงานอื่นของรัฐ

(11) ความคงสภาพของการสื่อสารและระบบ

เพื่อเป็นการประกันความคงสภาพ ความมั่นคงปลอดภัย และความเป็นส่วนตัวของระบบการสื่อสาร รัฐไม่ควรบังคับให้ผู้ให้บริการหรือผู้ขายฮาร์ดแวร์หรือซอฟต์แวร์ใส่ความสามารถในการสอดแนมหรือการติดตามลงในระบบของพวกเขาและไม่ควรบังคับให้รวบรวมหรือรักษาข้อมูลใดๆ ที่เป็นไปเพื่อเป้าประสงค์ในการสอดแนมของรัฐเท่านั้น

หลักความคงสภาพของการสื่อสารและระบบปรากฏอย่างชัดเจนในคดีระหว่างบริษัทแอปเปิ้ลกับหน่วยสืบสวนของรัฐบาลกลางสหรัฐอเมริกา คดีนี้เกิดขึ้นเมื่อหน่วยสืบสวนของรัฐบาลกลางได้โทรศัพท์มือถือไอโฟน (iPhone) ของผู้ก่อการร้ายในคดีหนึ่ง จึงต้องการค้นหาข้อมูลภายในโทรศัพท์เพื่อนำมาใช้ประกอบสำนวนคดี แต่ไม่สามารถเข้าถึงข้อมูลนั้นได้เพราะโทรศัพท์ได้ล็อครหัสไว้ อีกทั้งซอฟต์แวร์ของโทรศัพท์ไอโฟน (iOS) มีระบบรักษาความปลอดภัยของข้อมูลในระดับสูงมาก ตั้งแต่การเพิ่มเวลาหน่วงการเข้าถึงตัวเครื่องเมื่อใส่รหัสผ่านผิดพลาด และเมื่อใส่รหัสผิดครบตามจำนวนครั้งที่ตั้งไว้ ระบบโทรศัพท์จะลบข้อมูลทุกอย่างออกจากเครื่องทั้งหมด ซึ่งในอดีตบริษัทแอปเปิ้ลเก็บกุญแจในการเข้ารหัส (encryption key) เอาไว้เพื่อสามารถเข้าถึงเครื่องได้โดยไม่ต้องใช้รหัสผ่านในกรณีจำเป็น แต่ปัจจุบันบริษัทแอปเปิ้ลได้ยกเลิกเก็บกุญแจเข้ารหัสไปแล้วตามหลักนโยบายด้านความเป็นส่วนตัวและความปลอดภัยของข้อมูล

เพื่อให้เจ้าหน้าที่เข้าถึงข้อมูลในโทรศัพท์ หน่วยสืบสวนของรัฐบาลกลางจึงได้ขอต่อศาลแขวงในรัฐแคลิฟอร์เนียให้สั่งบริษัทแอปเปิ้ลจัดทำซอฟต์แวร์แบบพิเศษที่ปิดระบบรักษาความปลอดภัยทั้งหมดในโทรศัพท์มือถือไอโฟน เพื่อทำให้ระบบซอฟต์แวร์ไม่ลบข้อมูลในเครื่องในกรณีที่ใส่รหัสผิดจากการพยายามเข้าถึงข้อมูลโดยการไล่รหัส โดยศาลได้อนุมัติคำสั่งดังกล่าว อย่างไรก็ตามบริษัทแอปเปิ้ลได้อุทธรณ์คำสั่งศาลนั้นพร้อมแถลงการณ์ว่าบริษัทไม่ยินยอมกระทำตามคำสั่งศาล เนื่องจากกระทบต่อความปลอดภัยและความเป็นส่วนตัวของผู้ใช้บริการทั้งหมด อีกทั้งเครื่องมือที่สร้างให้รัฐนั้นไม่มีหลักประกันว่าจะไม่ตกไปอยู่กับฝ่ายก่อการร้าย และหากบริษัทแอปเปิ้ลยอมทำตามในกรณีนี้จะเป็นบรรทัดฐานในอนาคตให้หน่วยงานของรัฐสามารถใช้คำสั่งศาลขอเข้าถึงข้อมูลส่วนบุคคลของผู้ใดก็ได้ อันจะทำให้ระบบการคุ้มครองข้อมูลและสิทธิขั้นพื้นฐานที่รัฐต้องคุ้มครองนั้นถูกทำลายลง

นอกจากนี้การรักษาหรือรวบรวมข้อมูลเอาไว้ก่อนไม่ควรถูกกำหนดเป็นหน้าที่ของผู้ให้บริการ บุคคลมีสิทธิแสดงออกถึงความคิดเห็นของพวกเขาโดยไม่ระบุชื่อ รัฐจึงควรงดเว้นจากการบังคับให้มีการระบุตัวตนผู้ใช้ โดยห้ามกำหนดเป็นเงื่อนไขก่อนการให้บริการ

(12) หลักประกันสำหรับความร่วมมือระหว่างประเทศ

เพื่อตอบสนองต่อการเปลี่ยนแปลงในการไหลของข้อมูลและการเปลี่ยนแปลงของเทคโนโลยีและบริการด้านการสื่อสาร รัฐอาจต้องขอความช่วยเหลือจากผู้ให้บริการนอกประเทศ

ดังนั้นสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันทางกฎหมายและความตกลงอื่นใดที่รัฐได้เข้าเป็นภาคี ควรประกันว่าในกรณีที่กฎหมายของรัฐมากกว่าหนึ่งแห่งมีผลบังคับใช้ต่อการสอดแนมการสื่อสาร รัฐจะต้องเลือกปฏิบัติตามมาตรฐานการคุ้มครองบุคคลในระดับที่สูงกว่าเสมอ

ในกรณีที่รัฐขอความช่วยเหลือเพื่อวัตถุประสงค์ในการบังคับใช้กฎหมาย ควรมีการนำหลักความผิดอาญาสองรัฐ (dual criminality) มาใช้ รัฐไม่อาจหลีกเลี่ยงการปฏิบัติตามข้อจำกัดของกฎหมายในประเทศที่ว่าด้วยการสอดแนมการสื่อสาร กระบวนการช่วยเหลือซึ่งกันและกันทางกฎหมายและความตกลงอื่นๆควรมีการจัดทำเป็นเอกสารอย่างชัดเจน มีการเผยแพร่ต่อสาธารณะ และอยู่ภายใต้หลักประกันความเป็นธรรมในกระบวนการปฏิบัติ

(13) หลักประกันเพื่อป้องกันการเข้าถึงโดยมิชอบด้วยกฎหมาย

รัฐควรบัญญัติกฎหมายเพื่อเอาผิดทางอาญากับการสอดแนมการสื่อสารที่ไม่ชอบด้วยกฎหมายทั้งที่กระทำโดยรัฐและเอกชน กฎหมายดังกล่าวควรกำหนดบทลงโทษทั้งทางแพ่งและอาญาอย่างเพียงพอและอย่างมีนัยสำคัญ อีกทั้งควรกำหนดความคุ้มครองให้กับผู้เปิดเผยความไม่ชอบด้วยกฎหมายและกำหนดช่องทางเยียวยาสำหรับบุคคลผู้ได้รับผลกระทบ กฎหมายต่างๆควรระบุเงื่อนไขด้วยว่าข้อมูลใดๆที่ได้มาในลักษณะที่ไม่สอดคล้องกับหลักการทั้งหมดนี้ ย่อมไม่สามารถนำมาใช้เป็นพยานหลักฐานในศาลหรือกระบวนการยุติธรรมได้

นอกจากนี้รัฐควรหลักเกณฑ์ว่าข้อมูลใดๆที่ได้มาจากการสอดแนมการสื่อสารภายหลังที่ถูกใช้ตามเป้าประสงค์ของการค้นหาข้อมูลดังกล่าวแล้ว ข้อมูลเหล่านั้นจะต้องถูกทำลายหรือถูกส่งกลับไปยังบุคคลที่เกี่ยวข้อง

ผู้เขียนเห็นว่าการบัญญัติกฎหมายที่ให้อำนาจรัฐในการสอดแนมข้อมูลของประชาชนได้นั้นควรสอดคล้องกับหลักการข้างต้น อีกทั้งในอนาคตประเทศไทยควรจะพิจารณาเรื่องการบัญญัติกฎหมายที่ห้ามเกี่ยวกับการดักฟังและสอดแนมโดยรัฐเป็นกฎหมายกลางเพื่อเป็นการจำกัดอำนาจของหน่วยงานของรัฐมิให้กระทำการสอดแนมข้อมูลส่วนบุคคลตามอำเภอใจ โดยกฎหมายต้องบัญญัติให้อำนาจรัฐในการสอดแนมข้อมูลนั้นเป็นข้อยกเว้น ซึ่งบทบัญญัติกฎหมายต้องกำหนดมาตรการและวิธีการที่หน่วยงานของรัฐจะสามารถเข้าถึงข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมายอย่างชัดเจน ป้องกันการดักรับข้อมูลในวงกว้างอย่างไม่มีขอบเขตจำกัด

ส่วนในปัจจุบันประเทศไทยควรมีการพิจารณาชุดกฎหมายความมั่นคงดิจิทัลอย่างละเอียด เพื่อให้ชุดกฎหมายที่จะบังคับใช้ต่อไปนี้เป็นไปเพื่อวัตถุประสงค์ในการพัฒนาประเทศสู่สังคมเศรษฐกิจดิจิทัลอย่างแท้จริง มิใช่เป็นชุดกฎหมายที่มีบทบัญญัติเปิดช่องให้หน่วยงานของรัฐใช้อำนาจเข้าถึงข้อมูลส่วนบุคคลหรือกระทำการอันจำกัดสิทธิเสรีภาพของบุคคลได้ เพราะหากเป็นเช่นนั้นย่อมนำมาสู่ความไม่ไว้วางใจต่อระบบอินเทอร์เน็ต ซึ่งกระทบโดยตรงต่อความไว้วางใจของหน่วยงานภาคเอกชนทั้งในและต่างประเทศในการดำเนินกิจการทางเศรษฐกิจ

ในรายละเอียดนั้นผู้เขียนเห็นว่าร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. .... มาตรา 35 ควรมีการตรวจสอบถ่วงดุลโดยฝ่ายตุลาการเหมือนดังเช่นกฎหมายฉบับอื่นๆ ดังนั้นการเข้าถึงข้อมูลส่วนบุคคลโดยวิธีการต่างๆนั้นจะต้องขออนุญาตจากศาลก่อนด้วย อีกทั้งควรกำหนดนิยามความมั่นคงปลอดภัยไซเบอร์ให้มีความชัดเจน ไม่ต้องมีการตีความ เพื่อที่จะได้ไม่ทำให้เจ้าหน้าที่ใช้ดุลยพินิจในการตีความให้อำนาจตนอย่างเกินขอบเขต

ส่วนร่างพระราชบัญญัติด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ที่เป็นการแก้ไขเพิ่มเติมนั้น ผู้เขียนเห็นว่าตามมาตรา 14 ที่ได้มีการให้อำนาจรัฐมนตรีกำหนดหลักเกณฑ์และวิธีการระงับข้อมูลต่างๆเพิ่มเติมได้นั้น ควรมีการจำกัดขอบเขตอำนาจว่ารัฐมนตรีสามารถกำหนดหลักเกณฑ์ได้เพียงใด ซึ่งตามที่ได้อธิบายไปแล้วนั้นว่าหลักเกณฑ์ที่กำหนดโดยฝ่ายบริหารนั้นควรจะเป็นการกำหนดรายละเอียดเพื่อความชัดเจนในการปฏิบัติงาน ขยายความเพิ่มเติมที่ไม่เป็นการกระทบสิทธิเสรีภาพของประชาชน เพื่อทำให้เกิดความยืดหยุ่นในการบังคับใช้กฎหมาย แต่การกำหนดกฎเกณฑ์ที่จะกระทบต่อสิทธิเสรีภาพหรือมีแนวโน้มจะขยายอำนาจเกินขอบเขตกว่าที่กฎหมายให้อำนาจไว้นั้น ควรจะต้องดำเนินการโดยกระบวนการทางนิติบัญญัติ

ข้อเสนอแนะดังกล่าวเป็นความคิดเห็นต่อร่างพระราชบัญญัติในปัจจุบันนี้ แต่อย่างไรก็ตามการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายไทยนั้นยังมีการเปลี่ยนแปลงและต้องปรับปรุงพัฒนาอยู่ เช่นเดียวกับในต่างประเทศเองที่แนวคิดและระบบการคุ้มครองข้อมูลส่วนบุคคลยังมีการพัฒนาไม่หยุดนิ่งตามเทคโนโลยีที่เปลี่ยนแปลงเช่นกัน เห็นได้จากการปรับปรุง Directive 95/46/EC ที่บังคับใช้มานานเพื่อให้ทันต่อระบบเทคโนโลยีและการสื่อสารผ่านอินเทอร์เน็ตที่มีการพัฒนาไปไกล การเรียกร้องให้มีการปฏิรูปกฎหมายที่เกี่ยวกับการสอดแนมข้อมูลส่วนบุคคลในประเทศสหรัฐอเมริกา รวมไปถึงกรอบข้อตกลง Privacy Shield ที่ยังมีข้อคัดค้านจากหลายฝ่าย ระบบการคุ้มครองข้อมูลส่วนบุคคลภายใต้บริบทของความก้าวหน้าทางเทคโนโลยีการสื่อสารที่ต้องสร้างความสมดุลระหว่างความมั่นคงแห่งชาติและประโยชน์สาธารณะจึงเป็นเรื่องที่ควรทำการศึกษาอย่างต่อเนื่องเพื่อที่สิทธิในข้อมูลส่วนบุคคลจะได้รับความคุ้มครองอย่างแท้จริง

บรรณานุกรม

หนังสือ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารและสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. การโอนข้อมูลส่วนบุคคลระหว่างประเทศ. กรุงเทพมหานคร : สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี, 2548.

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารและสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. Privacy Policy & Trustmark : กลไกการคุ้มครองข้อมูลส่วนบุคคล กับการสร้างความน่าเชื่อถือในการทำ e-Business. กรุงเทพมหานคร : สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2548.

กิตติศักดิ์ ปกติ. ความรู้เบื้องต้นเกี่ยวกับสิทธิรับรู้ข้อมูลข่าวสารตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540. กรุงเทพมหานคร : สำนักพิมพ์วิญญูชน, 2541.

นคร เสรีรักษ์. การคุ้มครองข้อมูลส่วนบุคคล ข้อเสนอสำหรับประเทศไทย. กรุงเทพมหานคร : สำนักพิมพ์พีเพรส, 2558.

_____. ความเป็นส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย. กรุงเทพมหานคร : สำนักพิมพ์พีเพรส, 2557.

สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ. คู่มือสิทธิของประชาชนในการเข้าถึงข้อมูลข่าวสารของราชการ. กรุงเทพมหานคร, 2557.

สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล. พิมพ์ครั้งที่ 2 . กรุงเทพมหานคร : ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2547.

อภิญญา เลื่อนฉวี. กฎหมายสหภาพยุโรป. กรุงเทพมหานคร : สำนักพิมพ์วิญญูชน, 2548.

วิทยานิพนธ์และสารนิพนธ์

กิตติพงศ์ กมลธรรมวงศ์. “การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2549.

ธนชัย นักสอน. “การตรวจสอบและถ่วงดุลการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ ตามมาตรา 25 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2552.

ธนัท สุวรรณปริญญา. “ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ : กรณีศึกษาการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของธนาคาร สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ, 2550.

ปฏิวัติ อุ่นเรือน. “ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ.” สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547.

พรพักตร์ สถิตเวโรจน์. “หลักกฎหมายเกี่ยวกับผู้ให้บริการเครื่องหมายแสดงความน่าเชื่อถือในพาณิชย์อิเล็กทรอนิกส์.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2547.

ศิริกุล ภู่พันธ์. “ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548.

บทความ

คณาธิป ทองรวีวงศ์. “มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวของผู้ถูกดักฟังการสื่อสารข้อมูล.” วารสารกระบวนการยุติธรรม. เล่มที่ 1. ปีที่ 6. (มกราคม-เมษายน 2556) : 1-24.

จันทจิรา เอี่ยมมยุรา. “การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย.”วารสารนิติศาสตร์. ปีที่ 34 ฉบับที่ 4. (ธันวาคม 2547) : 627-652.

_____. “แนวคิดและหลักการยกร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย.” วารสารนิติศาสตร์. ปีที่ 34 ฉบับที่ 4 (ธันวาคม 2547) : 653-688.

ชวิน อุ่นภัทร. “ความเป็นส่วนตัวและการคุ้มครองจากการล่วงล้ำของรัฐในประเทศสหรัฐอเมริกา.” วารสารนิติศาสตร์. ปีที่ 44 ฉบับที่ 4. (ธันวาคม 2558) : 968-1004.

นนทวัชร์ นวตระกูลพิสุทธิ์. “สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลกับมาตรการคุ้มครองตาม ร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....” วารสารนิติศาสตร์. ปีที่ 43 ฉบับที่ 4 (ธันวาคม 2557) : 732-771.

บรรเจิด สิงคะเนติ. “หลักประกันสิทธิและเสรีภาพตามรัฐธรรมนูญฉบับใหม่.” วารสารกฎหมายปกครอง. เล่มที่17. ตอนที่2. : 37-38.

ประสิทธิ ปิวาวัฒนพานิช. “กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย.” วารสารนิติศาสตร์. ปีที่ 34 ฉบับที่ 4. : 535-556.

วรพจน์ วิศรุตพิชญ์. “สิทธิเสรีภาพตามรัฐธรรมนูญ (ศึกษารูปแบบการจำกัดสิทธิและเสรีภาพที่รัฐธรรมนูญให้ไว้อย่างเหมาะสม).” วารสารกฎหมายจุฬา. เล่มที่3. ปีที่17. : 70-73.

เอกสารงานวิจัย

สมศักดิ์ นวตระกูลพิสุทธิ์. “กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา.” รายงานการวิจัยโครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและจัดทำคู่มือปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540. กรุงเทพมหานคร : สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2547.

สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์. “รายงานผลการดำเนินการฉบับสมบูรณ์ โครงการพัฒนามาตรการใยการดำเนินการ การพิจารณาความเหมาะสม ความเป็นไปได้ เพื่อจัดทำแนวทางขั้นตอนและวิธีการในการเข้าร่วมหรือทำความตกลงตามกรอบว่าด้วยการคุ้มครองความเป็นส่วนตัวของ APEC (APEC Privacy Framework)” เสนอต่อสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ. มหาวิทยาลัยธรรมศาสตร์, 2557.

เอกสารอื่นๆ

คณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ. “รายงานการอบรมหลักสูตร Broadcasting Regulation.” ในการอบรมหลักสูตรทางวิชาการ 30 มิถุนายน–4 กรกฎาคม 2557 โดย Thomson Foundation ณ กรุงลอนดอน สหราชอาณาจักร, 2557.

คณาธิป ทองรวีวงศ์. “ข้อพิจารณา 9 ประการ ต่อการเสนอร่างกฎหมายใหม่ที่ให้อำนาจเจ้าพนักงานดักรับข้อมูลการสื่อสาร.” ในการสัมมนาทางวิชาการ 22 ธันวาคม 2557. จัดโดยเครือข่ายพลเมืองเน็ต ณ คณะเศรษฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2557.

คำสั่งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ 163/2557 เรื่องแต่งตั้งคณะทำงานทดสอบระบบเฝ้าติดตามสื่อออนไลน์.

ประมวลกฎหมายแพ่งและพาณิชย์.

ประมวลกฎหมายวิธีพิจารณาความอาญา.

ประมวลกฎหมายอาญา.

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547.

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540.

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542.

พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519.

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550.

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550.

ร่างประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่องมาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัวและเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม.

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ฉบับที่ผ่านการตรวจของคณะกรรมการกฤษฎีกา (คณะที่ 11) เรื่องเสร็จที่ 1135/2558.

ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ..) พ.ศ. ....

ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ....

เอกสารอิเล็กทรอนิกส์

กองบรรณาธิการเว็บไซต์สมาคมนักข่าวนักหนังสือพิมพ์แห่งประเทศไทย. “การปฏิรูปสื่อ.” http://www.tja.or.th, 10 มีนาคม 2559.

คณะผู้แทนไทยประจำสหภาพยุโรป. “คณะกรรมาธิการยุโรปเผยแพร่สาระสำคัญความตกลง EU – US Privacy Shield.” http://www2.thaieurope.net/ec-eu-us-privacy-shield-march-2016/, 14 เมษายน 2559.

คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ. “การส่งเสริมและคุ้มครองสิทธิมนุษยชน สิทธิพลเมือง การเมือง เศรษฐกิจ สังคมและวัฒนธรรม รวมทั้งสิทธิด้านการพัฒนาสิทธิความเป็นส่วนตัวในยุคดิจิทัล รายงานของสำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติ.” แปลโดยเครือข่ายพลเมืองเน็ต. https://thainetizen.org/docs/un-right-to-privacy-in-digital-age/, 15 ธันวาคม 2558.

คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ. “รายงานของผู้รายงานพิเศษว่าด้วยการส่งเสริมและคุ้มครองสิทธิและเสรีภาพด้านความเห็นและการแสดงออก แฟรงค์ ลารัว.” แปลโดยเครือข่ายพลเมืองเน็ต. https://thainetizen.org/docs/a-hrc-23-40-surveillance-of-communications/, 1 กุมภาพันธ์ 2559.

เครือข่ายพลเมืองเน็ต. “Single Gateway คืนชีพ ก.ไอซีทีเสนอในพ.ร.บ.คอมฯ ให้มีวิธีระงับข้อมูลที่เข้ารหัส SSL.” https://thainetizen.org/2016/05/single-gateway-back-ssl-censorship/, 28 พฤษภาคม 2559.

ชาญเชาวน์ ไชยานุกิจ. “เสรีภาพทุกตารางนิ้วในสหรัฐอเมริกา.” http://www.bangkokbiznews.com/mobile/view/blog/513103, 1 เมษายน 2559.

ประชาไท. “วิกิมีเดียฟ้อง NSA หวังหยุดสอดแนมการสื่อสารประชาชน.” http://prachatai.com/journal/2015/03/58382, 10 เมษายน 2559.

สรินณา อารีธรรมศิริกุล. “สายลับคอมพิวเตอร์กระทบความไว้วางใจรัฐบาลโอบามา.” http://www.siamintelligence.com/prism-program-spying-system-of-obama/, 1เมษายน 2559.

อรรถพล พานิชย์ไพศาลกูล. “EU-U.S. Privacy Shield” กรอบข้อตกลงการโอนข้อมูลระหว่างสหภาพยุโรปและสหรัฐอเมริกาฉบับใหม่.” http://ictlawcenter.etda.or.th/contents/detail/article-eu-us-privacy-shield, 1 มีนาคม 2559.

ARTICLES

International Trade Administration, Department of Commerce. “Safe Harbor Overviews.” in The Privacy Papers : Managing Technology, Consumer, Employee, and Legislative Action. Edited by Pebecca Herole. New York : CRC Press LLC, 2002.

Scott J. Shackelford JD. “Seeking a Safe Harbor in a widening sea : Unpacking the EJC’s SCHREMS decision and what it means for transatlantic relations.” Forthcoming Seton Hall Journal of Diplomacy and International Relations, 2016.

Vacca,John R. “The European Data Protection Directive : A Roadblock to International Trade?.” in The Privacy Papers : Managing Technology, Consumer, Employee, and Legislative Action. Edited by Pebecca Herole. New York : CRC Press LLC, 2002.

Victor Mayer-Schonberger. “Generational Development of Data Protection in Europe.” in Technology and Privacy : The New Landscape. ed. P. Agre. And M. Rotenberg. Cambridge. The MIT Press, 1997.

ELECTRONIC MEDIA

Anna Fielder. “From an unSafe Harbour to a Privacy Shield full of holes.” <https://www.privacyinternational.org/node/832>

Barry Sookman. “Schrems , what the CJEU decided and why it is a problem for Canadian and other non-EU businesses.” <http://www.barrysookman.com/2015/10/12/schrems-what-the-cjeu-decided-and-why-it-is-a-problem-for-canadian-and-other-non-eu-businesses/>

Colin Bennett. “Could Europe end up targeting Canada over C-51 and digital privacy.” <http://ipolitics.ca/2015/10/13/could-europe-end-up-targeting-canada-over-c-51-and-digital-privacy/>

Danny O'Brien. “No Safe Harbor: How NSA Spying Undermined U.S. Tech and Europeans' Privacy.” <https://www.eff.org/th/deeplinks/2015/10/europes-court-justice-nsa-surveilance>

Electronic Privacy Information Center. “Privacy & Human Rights 2003 : An International Survey of Privacy Laws and Developments.” < http://www.privacyinternational.org/survey/phr2003/>

European Commission. “Frequently Asked Questions on the Commission's adequacy finding on the Canadian Personal Information Protection and electronic Documents Act.” <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/third-countries-faq/index_en.htm.>

European Commission. “Press release EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield.” <http://europa.eu/rapid/press-release_IP-16-216_en.htm>

Jens-Henrik Jeppesen. “Replacing the Safe Harbor – Robust privacy protections in a new EU-US data transfer agreement.” <https://cdt.org/blog/replacing-the-safe-harbor-robust-privacy-protections-in-a-new-eu-us-data-transfer-agreement>

Office of the Privacy Commissioner of Canada. “Guidelines for Processing Personal Data Across Borders.” <https://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp>

Privacy International. “Press Statement: Data Protection Regulators say Privacy Shield is Not Strong Enough.” <https://www.privacyinternational.org/node/835>

Samuel Gibbs and agencies. “Data regulators reject EU-US Privacy Shield safe harbour deal.” <https://www.theguardian.com/technology/2016/apr/14/data-regulators-reject-eu-us-privacy-shield-safe-harbour-deal>

Spencer Ackerman. “US tech giants knew of NSA data collection, agency's top lawyer insists.” <http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de>

United Nations. “Guidelines for the Regulation of Computerized Personal Data File.” <http://www.unhchr.ch/html/menu3/b/71.htm>

Working Party. “First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy.” <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1997/wp4_en.pdf>

ภาคผนวก

ภาคผนวก ก

คำพิพากษาศาลยุติธรรมยุโรป คดีเลขที่ C-362/14

JUDGMENT OF THE COURT (Grand Chamber)

6 October 2015 (*)

(Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities)

In Case C-362/14,

REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings

Maximillian Schrems

v

Data Protection Commissioner,

joined party:

Digital Rights Ireland Ltd,

THE COURT (Grand Chamber),

composed of V. Skouris, President, K. Lenaerts, Vice-President, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), S. Rodin and K. Jürimäe, Presidents of Chambers, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen and C. Lycourgos, Judges,

Advocate General: Y. Bot,

Registrar: L. Hewlett, Principal Administrator,

having regard to the written procedure and further to the hearing on 24 March 2015,

after considering the observations submitted on behalf of:

– Mr Schrems, by N. Travers, Senior Counsel, P. O'Shea, Barrister-at-Law, G. Rudden, Solicitor, and H. Hofmann, Rechtsanwalt,

– the Data Protection Commissioner, by P. McDermott, Barrister-at-Law, S. More O'Ferrall and D. Young, Solicitors,

– Digital Rights Ireland Ltd, by F. Crehan, Barrister-at-Law, and S. McGarr and E. McGarr, Solicitors,

– Ireland, by A. Joyce, B. Counihan and E. Creedon, acting as Agents, and D. Fennelly, Barrister-at-Law,

– the Belgian Government, by J.-C. Halleux and C. Pochet, acting as Agents,

– the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,

– the Italian Government, by G. Palmieri, acting as Agent, and P. Gentili, avvocato dello Stato,

– the Austrian Government, by G. Hesse and G. Kunnert, acting as Agents,

– the Polish Government, by M. Kamejsza, M. Pawlicka and B. Majczyna, acting as Agents,

– the Slovenian Government, by A. Grum and V. Klemenc, acting as Agents,

– the United Kingdom Government, by L. Christie and J. Beeko, acting as Agents, and J. Holmes, Barrister,

– the European Parliament, by D. Moore, A. Caiola and M. Pencheva, acting as Agents,

– the European Commission, by B. Schima, B. Martenczuk, B. Smulders and J. Vondung, acting as Agents,

– the European Data Protection Supervisor (EDPS), by C. Docksey, A. Buchta and V. Pérez Asinari, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 23 September 2015,

gives the following

Judgment

1 This request for a preliminary ruling relates to the interpretation, in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union ('the Charter'), of Articles 25(6) and 28 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 (OJ 2003 L 284, p. 1) ('Directive 95/46'), and, in essence, to the validity of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

2 The request has been made in proceedings between Mr Schrems and the Data Protection Commissioner ('the Commissioner') concerning the latter's refusal to investigate a complaint made by Mr Schrems regarding the fact that Facebook Ireland Ltd ('Facebook Ireland') transfers the personal data of its users to the United States of America and keeps it on servers located in that country.

Legal context

Directive 95/46

3 Recitals 2, 10, 56, 57, 60, 62 and 63 in the preamble to Directive 95/46 are worded as follows:

'(2) ... data-processing systems are designed to serve man; … they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to … the well-being of individuals;

…

(10) … the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950,] and in the general principles of Community law; …, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

…

(56) … cross-border flows of personal data are necessary to the expansion of international trade; … the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; … the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) … on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

…

(60) … in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

…

(62) … the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) … such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; ...'

4 Articles 1, 2, 25, 26, 28 and 31 of Directive 95/46 provide:

'*Article 1*

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

...

Article 2

Definitions

For the purposes of this Directive:

(a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

...

(d) "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

...

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both

general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorisations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31(2).

Member States shall take the necessary measures to comply with the Commission's decision.

...

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

– investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

– effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

– the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and

freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

...

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

...

Article 31

...

2. Where reference is made to this Article, Articles 4 and 7 of [Council] Decision 1999/468/EC [of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (OJ 1999 L 184, p. 23)] shall apply, having regard to the provisions of Article 8 thereof.

...'

Decision 2000/520

5 Decision 2000/520 was adopted by the Commission on the basis of Article 25(6) of Directive 95/46.

6 Recitals 2, 5 and 8 in the preamble to that decision are worded as follows:

'(2) The Commission may find that a third country ensures an adequate level of protection. In that case personal data may be transferred from the Member States without additional guarantees being necessary.

…

(5) The adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, should be attained if organisations comply with the safe harbour privacy principles for the protection of personal data transferred from a Member State to the United States (hereinafter "the Principles") and the frequently asked questions (hereinafter "the FAQs") providing guidance for the implementation of the Principles issued by the Government of the United States on 21 July 2000. Furthermore the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles implemented in accordance with the FAQs.

…

(8) In the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection.'

7 Articles 1 to 4 of Decision 2000/520 provide:

'*Article 1*

1. For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the "Safe Harbour Privacy Principles" (hereinafter "the Principles"), as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked questions (hereinafter "the FAQs") issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States, having regard to the following documents issued by the US Department of Commerce:

(a) the safe harbour enforcement overview set out in Annex III;

(b) a memorandum on damages for breaches of privacy and explicit authorisations in US law set out in Annex IV;

(c) a letter from the Federal Trade Commission set out in Annex V;

(d) a letter from the US Department of Transportation set out in Annex VI.

2. In relation to each transfer of data the following conditions shall be met:

(a) the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs; and

(b) the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles implemented in accordance with the FAQs.

3. The conditions set out in paragraph 2 are considered to be met for each organisation that self-certifies its adherence to the Principles implemented in accordance with the FAQs from the date on which the organisation notifies to the US Department of Commerce (or its designee) the public disclosure of the commitment referred to in paragraph 2(a) and the identity of the government body referred to in paragraph 2(b).

Article 2

This Decision concerns only the adequacy of protection provided in the United States under the Principles implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect the application of other provisions of that Directive that pertain to the processing of personal data within the Member States, in particular Article 4 thereof.

Article 3

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:

(a) the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or

(b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof.

2. Member States shall inform the Commission without delay when measures are adopted on the basis of paragraph 1.

3. The Member States and the Commission shall also inform each other of cases where the action of bodies responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States fails to secure such compliance.

4. If the information collected under paragraphs 1, 2 and 3 provides evidence that any body responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States is not effectively fulfilling its role, the Commission shall inform the US Department of Commerce and, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC with a view to reversing or suspending the present Decision or limiting its scope.

Article 4

1. This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation.

The Commission shall in any case evaluate the implementation of the present Decision on the basis of available information three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the evaluation that the provisions set out in Article 1 of this Decision provide adequate protection within the meaning of Article 25 of Directive 95/46/EC and any evidence that the present Decision is being implemented in a discriminatory way.

2. The Commission shall, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC.'

8 Annex I to Decision 2000/520 is worded as follows:

'Safe Harbour Privacy Principles

issued by the US Department of Commerce on 21 July 2000

... the Department of Commerce is issuing this document and Frequently Asked Questions ("the Principles") under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of "adequacy" it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. …

Decisions by organisations to qualify for the safe harbour are entirely voluntary, and organisations may qualify for the safe harbour in different ways. ...

Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation; or (c) if the effect of the Directive [or] Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organisations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or US law, organisations are expected to opt for the higher protection where possible.

...'

9 Annex II to Decision 2000/520 reads as follows:

'Frequently Asked Questions (FAQs)

...

FAQ 6 — Self-Certification

Q: *How does an organisation self-certify that it adheres to the Safe Harbour Principles?*

A: Safe harbour benefits are assured from the date on which an organisation self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.

To self-certify for the safe harbour, organisations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organisation that is joining the safe harbour, that contains at least the following information:

1. name of organisation, mailing address, e-mail address, telephone and fax numbers;

2. description of the activities of the organisation with respect to personal information received from the [European Union]; and

3. description of the organisation's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbour, (d) the specific statutory body that has jurisdiction to hear any claims against the organisation regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programmes in which the organisation is a member, (f) method of verification (e.g. in-house, third party) …, and (g) the independent recourse mechanism that is available to investigate unresolved complaints.

Where the organisation wishes its safe harbour benefits to cover human resources information transferred from the [European Union] for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organisation arising out of human resources information that is listed in the annex to the Principles. ...

The Department (or its designee) will maintain a list of all organisations that file such letters, thereby assuring the availability of safe harbour benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11. ...

...

FAQ 11 — Dispute Resolution and Enforcement

Q: *How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organisation's persistent failure to comply with the Principles be handled?*

A: The Enforcement Principle sets out the requirements for safe harbour enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ on verification (FAQ 7). This FAQ 11 addresses points (a) and (c), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Enforcement Principle's requirements. Organisations may satisfy the requirements through the following: (1) compliance with private sector developed privacy programmes that incorporate the Safe Harbour Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Union or their authorised representatives. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle's requirements are additional to the requirements set forth in paragraph 3 of the introduction to the Principles that self-regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.

Recourse Mechanisms

Consumers should be encouraged to raise any complaints they may have with the relevant organisation before proceeding to independent recourse mechanisms. ...

...

FTC Action

The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organisations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbour Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. ...

…'

10 Annex IV to Decision 2000/520 states:

'Damages for Breaches of Privacy, Legal Authorisations and Mergers and Takeovers in US Law

This responds to the request by the European Commission for clarification of US law with respect to (a) claims for damages for breaches of privacy, (b) "explicit authorisations" in US law for the use of personal information in a manner inconsistent with the safe harbour principles, and (c) the effect of mergers and takeovers on obligations undertaken pursuant to the safe harbour principles.

...

B. Explicit Legal Authorisations

The safe harbour principles contain an exception where statute, regulation or case-law create "conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the principles is limited to the extent necessary to meet the overriding legitimate interests further[ed] by such authorisation". Clearly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law. As for explicit authorisations, while the safe harbour principles are intended to bridge the differences between the US and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected lawmakers. The limited exception from strict adherence to the safe harbour principles seeks to strike a balance to accommodate the legitimate interests on each side.

The exception is limited to cases where there is an explicit authorisation. Therefore, as a threshold matter, the relevant statute, regulation or court decision must affirmatively authorise the particular conduct by safe harbour organisations ... In other words, the exception would not apply where the law is silent. In addition, the exception would apply only if the explicit authorisation conflicts with adherence to the safe harbour principles. Even then, the exception "is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation". By way of illustration, where the law simply authorises a company to provide personal information to government authorities, the exception would not apply. Conversely, where the law specifically authorises the company to provide personal information to government agencies without the individual's consent, this would constitute an "explicit authorisation" to act in a manner that conflicts with the safe harbour principles. Alternatively, specific exceptions from affirmative requirements to provide notice and consent would fall within the exception (since it would be the equivalent of a specific authorisation to disclose the information without notice and consent). For example, a statute which authorises doctors to provide their patients' medical records

to health officials without the patients' prior consent might permit an exception from the notice and choice principles. This authorisation would not permit a doctor to provide the same medical records to health maintenance organisations or commercial pharmaceutical research laboratories, which would be beyond the scope of the purposes authorised by the law and therefore beyond the scope of the exception ... The legal authority in question can be a "stand alone" authorisation to do specific things with personal information, but, as the examples below illustrate, it is likely to be an exception to a broader law which proscribes the collection, use, or disclosure of personal information.

...'

Communication COM(2013) 846 final

11 On 27 November 2013 the Commission adopted the communication to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final) ('Communication COM(2013) 846 final'). The communication was accompanied by the 'Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection', also dated 27 November 2013. That report was drawn up, as stated in point 1 thereof, in cooperation with the United States after the existence in that country of a number of surveillance programmes involving the large-scale collection and processing of personal data had been revealed. The report contained inter alia a detailed analysis of United States law as regards, in particular, the legal bases authorising the existence of surveillance programmes and the collection and processing of personal data by United States authorities.

12 In point 1 of Communication COM(2013) 846 final, the Commission stated that '[c]ommercial exchanges are addressed by Decision [2000/520]', adding that '[t]his Decision provides a legal basis for transfers of personal data from the [European Union] to companies established in the [United States] which have adhered to the Safe Harbour Privacy Principles'. In addition, the Commission underlined in point 1 the increasing relevance of personal data flows, owing in particular to the development of the digital economy which has indeed 'led to exponential growth in the quantity, quality, diversity and nature of data processing activities'.

13 In point 2 of that communication, the Commission observed that 'concerns about the level of protection of personal data of [Union] citizens transferred to the [United States] under the Safe Harbour scheme have grown' and that '[t]he voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement'.

14 It further stated in point 2 that '[t]he personal data of [Union] citizens sent to the [United States] under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the [European Union] and the purposes for which it was transferred to the [United States]' and that '[a] majority of the US internet companies that appear to be more directly concerned by [the surveillance] programmes are certified under the Safe Harbour scheme'.

15 In point 3.2 of Communication COM(2013) 846 final, the Commission noted a number of weaknesses in the application of Decision 2000/520. It stated, first, that some certified United States companies did not comply with the principles referred to in Article 1(1) of Decision 2000/520 ('the safe harbour principles') and that improvements had to be made to that decision regarding 'structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception'. It observed, secondly, that 'Safe Harbour also acts as a conduit for the transfer of the personal data of EU citizens from

the [European Union] to the [United States] by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes'.

16 The Commission concluded in point 3.2 that whilst, '[g]iven the weaknesses identified, the current implementation of Safe Harbour cannot be maintained, ... its revocation would[, however,] adversely affect the interests of member companies in the [European Union] and in the [United States]'. Finally, the Commission added in that point that it would 'engage with the US authorities to discuss the shortcomings identified'.

Communication COM(2013) 847 final

17 On the same date, 27 November 2013, the Commission adopted the communication to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the [European Union] (COM(2013) 847 final) ('Communication COM(2013) 847 final'). As is clear from point 1 thereof, that communication was based inter alia on information received in the ad hoc EU-US Working Group and followed two Commission assessment reports published in 2002 and 2004 respectively.

18 Point 1 of Communication COM(2013) 847 final explains that the functioning of Decision 2000/520 'relies on commitments and self-certification of adhering companies', adding that '[s]igning up to these arrangements is voluntary, but the rules are binding for those who sign up'.

19 In addition, it is apparent from point 2.2 of Communication COM(2013) 847 final that, as at 26 September 2013, 3 246 companies, falling within many industry and services sectors, were certified. Those companies mainly provided services in the EU internal market, in particular in the internet sector, and some of them were EU companies which had subsidiaries in the United States. Some of those companies processed the data of their employees in Europe which was transferred to the United States for human resource purposes.

20 The Commission stated in point 2.2 that '[a]ny gap in transparency or in enforcement on the US side results in responsibility being shifted to European data protection authorities and to the companies which use the scheme'.

21 It is apparent, in particular, from points 3 to 5 and 8 of Communication COM(2013) 847 final that, in practice, a significant number of certified companies did not comply, or did not comply fully, with the safe harbour principles.

22 In addition, the Commission stated in point 7 of Communication COM(2013) 847 final that 'all companies involved in the PRISM programme [a large-scale intelligence collection programme], and which grant access to US authorities to data stored and processed in the [United States], appear to be Safe Harbour certified' and that '[t]his has made the Safe Harbour scheme one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the [European Union]'. In that regard, the Commission noted in point 7.1 of that communication that 'a number of legal bases under US law allow large-scale collection and processing of personal data that is stored or otherwise processed [by] companies based in the [United States]' and that '[t]he large-scale nature of these programmes may result in data transferred under Safe Harbour being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in [Decision 2000/520]'.

23 In point 7.2 of Communication COM(2013) 847 final, headed 'Limitations and redress possibilities', the Commission noted that 'safeguards that are provided under US law

are mostly available to US citizens or legal residents' and that, '[m]oreover, there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes'.

24 According to point 8 of Communication COM(2013) 847 final, the certified companies included '[w]eb companies such as Google, Facebook, Microsoft, Apple, Yahoo', which had 'hundreds of millions of clients in Europe' and transferred personal data to the United States for processing.

25 The Commission concluded in point 8 that 'the large-scale access by intelligence agencies to data transferred to the [United States] by Safe Harbour certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data is transferred to the [United States]'.

The dispute in the main proceedings and the questions referred for a preliminary ruling

26 Mr Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network ('Facebook') since 2008.

27 Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland's users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing.

28 On 25 June 2013 Mr Schrems made a complaint to the Commissioner by which he in essence asked the latter to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the United States. He contended in his complaint that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency ('the NSA').

29 Since the Commissioner took the view that he was not required to investigate the matters raised by Mr Schrems in the complaint, he rejected it as unfounded. The Commissioner considered that there was no evidence that Mr Schrems' personal data had been accessed by the NSA. He added that the allegations raised by Mr Schrems in his complaint could not be profitably put forward since any question of the adequacy of data protection in the United States had to be determined in accordance with Decision 2000/520 and the Commission had found in that decision that the United States ensured an adequate level of protection.

30 Mr Schrems brought an action before the High Court challenging the decision at issue in the main proceedings. After considering the evidence adduced by the parties to the main proceedings, the High Court found that the electronic surveillance and interception of personal data transferred from the European Union to the United States serve necessary and indispensable objectives in the public interest. However, it added that the revelations made by Edward Snowden had demonstrated a 'significant over-reach' on the part of the NSA and other federal agencies.

31 According to the High Court, Union citizens have no effective right to be heard. Oversight of the intelligence services' actions is carried out within the framework of an *ex parte* and secret procedure. Once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of the indiscriminate surveillance and interception carried out by them on a large scale.

32 The High Court stated that Irish law precludes the transfer of personal data outside national territory save where the third country ensures an adequate level of protection for privacy and fundamental rights and freedoms. The importance of the rights to privacy and to inviolability of the dwelling, which are guaranteed by the Irish Constitution, requires that any interference with those rights be proportionate and in accordance with the law.

33 The High Court held that the mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution. In order for interception of electronic communications to be regarded as consistent with the Irish Constitution, it would be necessary to demonstrate that the interception is targeted, that the surveillance of certain persons or groups of persons is objectively justified in the interests of national security or the suppression of crime and that there are appropriate and verifiable safeguards. Thus, according to the High Court, if the main proceedings were to be disposed of on the basis of Irish law alone, it would then have to be found that, given the existence of a serious doubt as to whether the United States ensures an adequate level of protection of personal data, the Commissioner should have proceeded to investigate the matters raised by Mr Schrems in his complaint and that the Commissioner was wrong in rejecting the complaint.

34 However, the High Court considers that this case concerns the implementation of EU law as referred to in Article 51 of the Charter and that the legality of the decision at issue in the main proceedings must therefore be assessed in the light of EU law. According to the High Court, Decision 2000/520 does not satisfy the requirements flowing both from Articles 7 and 8 of the Charter and from the principles set out by the Court of Justice in the judgment in *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238). The right to respect for private life, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States, would be rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards.

35 The High Court further observes that in his action Mr Schrems in reality raises the legality of the safe harbour regime which was established by Decision 2000/520 and gives rise to the decision at issue in the main proceedings. Thus, even though Mr Schrems has not formally contested the validity of either Directive 95/46 or Decision 2000/520, the question is raised, according to the High Court, as to whether, on account of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission's finding in Decision 2000/520 that the United States ensures an adequate level of protection or whether Article 8 of the Charter authorised the Commissioner to break free, if appropriate, from such a finding.

36 In those circumstances the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is

being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?

(2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?'

Consideration of the questions referred

37 By its questions, which it is appropriate to examine together, the referring court asks, in essence, whether and to what extent Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, prevents a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from being able to examine the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

The powers of the national supervisory authorities, within the meaning of Article 28 of Directive 95/46, when the Commission has adopted a decision pursuant to Article 25(6) of that directive

38 It should be recalled first of all that the provisions of Directive 95/46, inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter (see judgments in *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68; *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 68; and *Ryneš*, C-212/13, EU:C:2014:2428, paragraph 29).

39 It is apparent from Article 1 of Directive 95/46 and recitals 2 and 10 in its preamble that that directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms. The importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8 thereof, is, moreover, emphasised in the case-law of the Court (see judgments in *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 47; *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 53; and *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraphs, 53, 66, 74 and the case-law cited).

40 As regards the powers available to the national supervisory authorities in respect of transfers of personal data to third countries, it should be noted that Article 28(1) of Directive 95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU (see, to this effect, judgments

in *Commission* v *Austria*, C-614/10, EU:C:2012:631, paragraph 36, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 47).

41 The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data (see judgments in*Commission* v *Germany*, C-518/07, EU:C:2010:125, paragraph 25, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 48 and the case-law cited).

42 In order to guarantee that protection, the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data (see, to this effect, judgments in *Commission* v *Germany*, C-518/07, EU:C:2010:125, paragraph 24, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 51).

43 The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings.

44 It is, admittedly, apparent from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, so that they do not have powers on the basis of Article 28 in respect of processing of such data carried out in a third country.

45 However, the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 2(b) of Directive 95/46 (see, to this effect, judgment in *Parliament* v *Council and Commission*, C-317/04 and C-318/04, EU:C:2006:346, paragraph 56) carried out in a Member State. That provision defines 'processing of personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means' and mentions, by way of example, 'disclosure by transmission, dissemination or otherwise making available'.

46 Recital 60 in the preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to the directive. In that regard, Chapter IV of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data (see, to this effect, judgment in *Lindqvist*, C-101/01, EU:C:2003:596, paragraph 63).

47 As, in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of

personal data, each of them is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46.

48 Whilst acknowledging, in recital 56 in its preamble, that transfers of personal data from the Member States to third countries are necessary for the expansion of international trade, Directive 95/46 lays down as a principle, in Article 25(1), that such transfers may take place only if the third country ensures an adequate level of protection.

49 Furthermore, recital 57 states that transfers of personal data to third countries not ensuring an adequate level of protection must be prohibited.

50 In order to control transfers of personal data to third countries according to the level of protection accorded to it in each of those countries, Article 25 of Directive 95/46 imposes a series of obligations on the Member States and the Commission. It is apparent, in particular, from that article that the finding that a third country does or does not ensure an adequate level of protection may, as the Advocate General has observed in point 86 of his Opinion, be made either by the Member States or by the Commission.

51 The Commission may adopt, on the basis of Article 25(6) of Directive 95/46, a decision finding that a third country ensures an adequate level of protection. In accordance with the second subparagraph of that provision, such a decision is addressed to the Member States, who must take the measures necessary to comply with it. Pursuant to the fourth paragraph of Article 288 TFEU, it is binding on all the Member States to which it is addressed and is therefore binding on all their organs (see, to this effect, judgments in *Albako Margarinefabrik*, 249/85, EU:C:1987:245, paragraph 17, and *Mediaset*, C-69/13, EU:C:2014:71, paragraph 23) in so far as it has the effect of authorising transfers of personal data from the Member States to the third country covered by it.

52 Thus, until such time as the Commission decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, admittedly cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality (judgment in *Commission* v *Greece*, C-475/01, EU:C:2004:585, paragraph 18 and the case-law cited).

53 However, a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, such as Decision 2000/520, cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim, within the meaning of Article 28(4) of that directive, concerning the protection of their rights and freedoms in regard to the processing of that data. Likewise, as the Advocate General has observed in particular in points 61, 93 and 116 of his Opinion, a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive.

54 Neither Article 8(3) of the Charter nor Article 28 of Directive 95/46 excludes from the national supervisory authorities' sphere of competence the oversight of transfers of personal data to third countries which have been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46.

55 In particular, the first subparagraph of Article 28(4) of Directive 95/46, under which the national supervisory authorities are to hear 'claims lodged by any person … concerning the protection of his rights and freedoms in regard to the processing of personal data', does not provide for any exception in this regard where the Commission has adopted a decision pursuant to Article 25(6) of that directive.

56 Furthermore, it would be contrary to the system set up by Directive 95/46 and to the objective of Articles 25 and 28 thereof for a Commission decision adopted pursuant to Article 25(6) to have the effect of preventing a national supervisory authority from examining a person's claim concerning the protection of his rights and freedoms in regard to the processing of his personal data which has been or could be transferred from a Member State to the third country covered by that decision.

57 On the contrary, Article 28 of Directive 95/46 applies, by its very nature, to any processing of personal data. Thus, even if the Commission has adopted a decision pursuant to Article 25(6) of that directive, the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive.

58 If that were not so, persons whose personal data has been or could be transferred to the third country concerned would be denied the right, guaranteed by Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights (see, by analogy, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 68).

59 A claim, within the meaning of Article 28(4) of Directive 95/46, by which a person whose personal data has been or could be transferred to a third country contends, as in the main proceedings, that, notwithstanding what the Commission has found in a decision adopted pursuant to Article 25(6) of that directive, the law and practices of that country do not ensure an adequate level of protection must be understood as concerning, in essence, whether that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.

60 In this connection, the Court's settled case-law should be recalled according to which the European Union is a union based on the rule of law in which all acts of its institutions are subject to review of their compatibility with, in particular, the Treaties, general principles of law and fundamental rights (see, to this effect, judgments in *Commission and Others* v *Kadi*, C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518, paragraph 66; *Inuit Tapiriit Kanatami and Others* v *Parliament and Council*, C-583/11 P, EU:C:2013:625, paragraph 91; and *Telefónica* v *Commission*, C-274/12 P, EU:C:2013:852, paragraph 56). Commission decisions adopted pursuant to Article 25(6) of Directive 95/46 cannot therefore escape such review.

61 That said, the Court alone has jurisdiction to declare that an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, is invalid, the exclusivity of that jurisdiction having the purpose of guaranteeing legal certainty by ensuring that EU law is applied uniformly (see judgments in *Melki and Abdeli*, C-188/10 and C-189/10, EU:C:2010:363, paragraph 54, and *CIVAD*, C-533/10, EU:C:2012:347, paragraph 40).

62 Whilst the national courts are admittedly entitled to consider the validity of an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, they are not, however, endowed with the power to declare such an act invalid themselves (see, to this effect, judgments in *Foto-Frost*, 314/85, EU:C:1987:452, paragraphs 15 to 20, and *IATA and ELFAA*, C-344/04, EU:C:2006:10, paragraph 27). A fortiori, when the national supervisory authorities examine a claim, within the

meaning of Article 28(4) of that directive, concerning the compatibility of a Commission decision adopted pursuant to Article 25(6) of the directive with the protection of the privacy and of the fundamental rights and freedoms of individuals, they are not entitled to declare that decision invalid themselves.

63 Having regard to those considerations, where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46 lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim, as in the main proceedings, the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence.

64 In a situation where the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are unfounded and therefore rejects it, the person who lodged the claim must, as is apparent from the second subparagraph of Article 28(3) of Directive 95/46, read in the light of Article 47 of the Charter, have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. Having regard to the case-law cited in paragraphs 61 and 62 of the present judgment, those courts must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded (see, to this effect, judgment in *T & L Sugars and Sidul Açúcares* v *Commission*, C-456/13 P, EU:C:2015:284, paragraph 48 and the case-law cited).

65 In the converse situation, where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are well founded, that authority must, in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46, read in the light in particular of Article 8(3) of the Charter, be able to engage in legal proceedings. It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity.

66 Having regard to the foregoing considerations, the answer to the questions referred is that Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

The validity of Decision 2000/520

67 As is apparent from the referring court's explanations relating to the questions submitted, Mr Schrems contends in the main proceedings that United States law and practice do not ensure an adequate level of protection within the meaning of Article 25 of Directive 95/46. As the Advocate General has observed in points 123 and 124 of his Opinion, Mr Schrems expresses doubts, which the referring court indeed seems

essentially to share, concerning the validity of Decision 2000/520. In such circumstances, having regard to what has been held in paragraphs 60 to 63 of the present judgment and in order to give the referring court a full answer, it should be examined whether that decision complies with the requirements stemming from Directive 95/46 read in the light of the Charter.

The requirements stemming from Article 25(6) of Directive 95/46

68 As has already been pointed out in paragraphs 48 and 49 of the present judgment, Article 25(1) of Directive 95/46 prohibits transfers of personal data to a third country not ensuring an adequate level of protection.

69 However, for the purpose of overseeing such transfers, the first subparagraph of Article 25(6) of Directive 95/46 provides that the Commission 'may find … that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into …, for the protection of the private lives and basic freedoms and rights of individuals'.

70 It is true that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection. In particular, Article 25(2) does no more than state that the adequacy of the level of protection afforded by a third country 'shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations' and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.

71 However, first, as is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country 'ensures' an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed 'for the protection of the private lives and basic freedoms and rights of individuals'.

72 Thus, Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country.

73 The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.

74 It is clear from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union in order to ensure that the

requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.

75 Accordingly, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country.

76 Also, in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard.

77 Moreover, as the Advocate General has stated in points 134 and 135 of his Opinion, when the validity of a Commission decision adopted pursuant to Article 25(6) of Directive 95/46 is examined, account must also be taken of the circumstances that have arisen after that decision's adoption.

78 In this regard, it must be stated that, in view of, first, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and, secondly, the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection, the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict (see, by analogy, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 47 and 48).

Article 1 of Decision 2000/520

79 The Commission found in Article 1(1) of Decision 2000/520 that the principles set out in Annex I thereto, implemented in accordance with the guidance provided by the FAQs set out in Annex II, ensure an adequate level of protection for personal data transferred from the European Union to organisations established in the United States. It is apparent from that provision that both those principles and the FAQs were issued by the United States Department of Commerce.

80 An organisation adheres to the safe harbour principles on the basis of a system of self-certification, as is apparent from Article 1(2) and (3) of Decision 2000/520, read in conjunction with FAQ 6 set out in Annex II thereto.

81 Whilst recourse by a third country to a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection 'by reason of its domestic law or … international commitments', the reliability of such a system, in the light of that requirement, is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice.

82 In the present instance, by virtue of the second paragraph of Annex I to Decision 2000/520, the safe harbour principles are 'intended for use solely by US organisations

receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of "adequacy" it creates'. Those principles are therefore applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them.

83 Moreover, Decision 2000/520, pursuant to Article 2 thereof, 'concerns only the adequacy of protection provided in the United States under the [safe harbour principles] implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive [95/46]', without, however, containing sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25(6) of that directive, by reason of its domestic law or its international commitments.

84 In addition, under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'.

85 In this connection, Decision 2000/520 states in Part B of Annex IV, with regard to the limits to which the safe harbour principles' applicability is subject, that, '[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law'.

86 Thus, Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.

87 In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 33 and the case-law cited).

88 In addition, Decision 2000/520 does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.

89 Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind. As the Advocate General has observed in points 204 to 206 of his Opinion, procedures before the Federal Trade Commission — the powers of which, described in particular in FAQ 11 set out in Annex II to that decision, are limited to commercial disputes — and the private dispute resolution mechanisms concern

compliance by the United States undertakings with the safe harbour principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State.

90 Moreover, the foregoing analysis of Decision 2000/520 is borne out by the Commission's own assessment of the situation resulting from the implementation of that decision. Particularly in points 2 and 3.2 of Communication COM(2013) 846 final and in points 7.1, 7.2 and 8 of Communication COM(2013) 847 final, the content of which is set out in paragraphs 13 to 16 and paragraphs 22, 23 and 25 of the present judgment respectively, the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

91 As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55 and the case-law cited).

92 Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52 and the case-law cited).

93 Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61).

94 In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39).

95 Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental

right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (see, to this effect, judgments in *Les Verts* v *Parliament*, 294/83, EU:C:1986:166, paragraph 23; *Johnston*, 222/84, EU:C:1986:206, paragraphs 18 and 19; *Heylens and Others*, 222/86, EU:C:1987:442, paragraph 14; and *UGT-Rioja and Others*, C-428/06 to C-434/06, EU:C:2008:488, paragraph 80).

96 As has been found in particular in paragraphs 71, 73 and 74 of the present judgment, in order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment.

97 However, the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments.

98 Consequently, without there being any need to examine the content of the safe harbour principles, it is to be concluded that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid.

Article 3 of Decision 2000/520

99 It is apparent from the considerations set out in paragraphs 53, 57 and 63 of the present judgment that, under Article 28 of Directive 95/46, read in the light in particular of Article 8 of the Charter, the national supervisory authorities must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him. That is in particular the case where, in bringing such a claim, that person raises questions regarding the compatibility of a Commission decision adopted pursuant to Article 25(6) of that directive with the protection of the privacy and of the fundamental rights and freedoms of individuals.

100 However, the first subparagraph of Article 3(1) of Decision 2000/520 lays down specific rules regarding the powers available to the national supervisory authorities in the light of a Commission finding relating to an adequate level of protection, within the meaning of Article 25 of Directive 95/46.

101 Under that provision, the national supervisory authorities may, '[w]ithout prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive [95/46], … suspend data flows to an organisation that has self-certified its adherence to the [principles of Decision 2000/520]', under restrictive conditions establishing a high threshold for intervention. Whilst that provision is without prejudice to the powers of those authorities to take action to ensure compliance with national provisions adopted pursuant to Directive 95/46, it excludes, on the other hand, the possibility of them taking action to ensure compliance with Article 25 of that directive.

102 The first subparagraph of Article 3(1) of Decision 2000/520 must therefore be understood as denying the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46, where a person, in bringing a claim under

that provision, puts forward matters that may call into question whether a Commission decision that has found, on the basis of Article 25(6) of the directive, that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.

103 The implementing power granted by the EU legislature to the Commission in Article 25(6) of Directive 95/46 does not confer upon it competence to restrict the national supervisory authorities' powers referred to in the previous paragraph of the present judgment.

104 That being so, it must be held that, in adopting Article 3 of Decision 2000/520, the Commission exceeded the power which is conferred upon it in Article 25(6) of Directive 95/46, read in the light of the Charter, and that Article 3 of the decision is therefore invalid.

105 As Articles 1 and 3 of Decision 2000/520 are inseparable from Articles 2 and 4 of that decision and the annexes thereto, their invalidity affects the validity of the decision in its entirety.

106 Having regard to all the foregoing considerations, it is to be concluded that Decision 2000/520 is invalid.

Costs

107 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. **Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.**

2. **Decision 2000/520 is invalid.**

[Signatures]

ภาคผนวก ข

คำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2000/520

2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.)

Official Journal L 215 , 25/08/2000 P. 0007 - 0047

Commission Decision

of 26 July 2000

pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce

(notified under document number C(2000) 2441)

(Text with EEA relevance)

(2000/520/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(1), and in particular Article 25(6) thereof,

Whereas:

(1) Pursuant to Directive 95/46/EC Member States are required to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection and the Member State laws implementing other provisions of the Directive are respected prior to the transfer.

(2) The Commission may find that a third country ensures an adequate level of protection. In that case personal data may be transferred from the Member States without additional guarantees being necessary.

(3) Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations and in respect of given conditions. The Working Party on Protection of Individuals with regard to

the Processing of Personal Data established under that Directive(2) has issued guidance on the making of such assessments(3).

(4) Given the different approaches to data protection in third countries, the adequacy assessment should be carried out and any decision based on Article 25(6) of Directive 95/46/EC should be enforced in a way that does not arbitrarily or unjustifiably discriminate against or between third countries where like conditions prevail nor constitute a disguised barrier to trade taking into account the Community's present international commitments.

(5) The adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, should be attained if organisations comply with the safe harbour privacy principles for the protection of personal data transferred from a Member State to the United States (hereinafter "the Principles") and the frequently asked questions (hereinafter "the FAQs") providing guidance for the implementation of the Principles issued by the Government of the United States on 21 July 2000. Furthermore the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles implemented in accordance with the FAQs.

(6) Sectors and/or data processing not subject to the jurisdiction of any of the government bodies in the United States listed in Annex VII to this Decision should fall outside the scope of this Decision.

(7) To ensure the proper application of this Decision, it is necessary that organisations adhering to the Principles and the FAQs can be recognised by interested parties, such as data subjects, data exporters and data protection authorities. To this end the US Department of Commerce or its designee should undertake to maintain and make available to the public a list of organisations self-certifying their adherence to the Principles implemented in accordance with the FAQs and falling within the jurisdiction of at least one of the government bodies listed in Annex VII to this Decision.

(8) In the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection.

(9) The "safe harbor" created by the Principles and the FAQs, may need to be reviewed in the light of experience, of developments concerning the protection of privacy in circumstances in which technology is constantly making easier the transfer and processing of personal data and in the light of reports on implementation by enforcement authorities involved.

(10) The Working Party on Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of Directive 95/46/EC has delivered opinions on the level of protection provided by the "safe harbor" Principles in the United States which have been taken into account in the preparation of the present Decision(4).

(11) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31 of Directive 95/46/EC,

HAS ADOPTED THIS DECISION:

Article 1

1. For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the "Safe Harbor Privacy Principles" (hereinafter "the Principles"), as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked questions (hereinafter "the FAQs") issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States, having regard to the following documents issued by the US Department of Commerce:

(a) the safe harbour enforcement overview set out in Annex III;

(b) a memorandum on damages for breaches of privacy and explicit authorisations in US law set out in Annex IV;

(c) a letter from the Federal Trade Commission set out in Annex V;

(d) a letter from the US Department of Transportation set out in Annex VI.

2. In relation to each transfer of data the following conditions shall be met:

(a) the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs; and

(b) the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles implemented in accordance with the FAQs.

3. The conditions set out in paragraph 2 are considered to be met for each organisation that self-certifies its adherence to the Principles implemented in accordance with the FAQs from the date on which the organisation notifies to the US Department of Commerce (or its designee) the public disclosure of the commitment referred to in paragraph 2(a) and the identity of the government body referred to in paragraph 2(b).

Article 2

This Decision concerns only the adequacy of protection provided in the United States under the Principles implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect the application of other provisions of that Directive that pertain to the processing of personal data within the Member States, in particular Article 4 thereof.

Article 3

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:

(a) the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or

(b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof.

2. Member States shall inform the Commission without delay when measures are adopted on the basis of paragraph 1.

3. The Member States and the Commission shall also inform each other of cases where the action of bodies responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States fails to secure such compliance.

4. If the information collected under paragraphs 1, 2 and 3 provides evidence that any body responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States is not effectively fulfilling its role, the Commission shall inform the US Department of Commerce and, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC with a view to reversing or suspending the present Decision or limiting its scope.

Article 4

1. This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation.

The Commission shall in any case evaluate the implementation of the present Decision on the basis of available information three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the evaluation that the provisions set out in Article 1 of this Decision provide adequate protection within the meaning of Article 25 of Directive 95/46/EC and any evidence that the present Decision is being implemented in a discriminatory way.

2. The Commission shall, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC.

Article 5

Member States shall take all the measures necessary to comply with this Decision at the latest at the end of a period of 90 days from the date of its notification to the Member States.

Article 6

This Decision is addressed to the Member States.

Done at Brussels, 26 July 2000.

For the Commission

Frederik Bolkestein

Member of the Commission

(1) OJ L 281, 23.11.1995, p. 31.

(2) The web address of the Working Party is: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

(3) WP 12: Transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection Directive, adopted by the Working Party on 24 July 1998.

(4) WP 15: Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States.

WP 19: Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19 April 1999.

WP 21: Opinion 4/99 on the Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed "Safe Harbor Principles" on the adequacy of the "International Safe Harbor Principles".

WP 23: Working document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the "International Safe Harbor Principles".

WP 27: Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce.

WP 31: Opinion 3/200 on the EU/US dialogue concerning the "Safe Harbor" arrangement.

WP 32: Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles".

ANNEX I

SAFE HARBOR PRIVACY PRINCIPLES

issued by the US Department of Commerce on 21 July 2000

The European Union's comprehensive privacy legislation, the Directive on Data Protection (the Directive), became effective on October 25, 1998. It requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy standard" on personal data transfers from the European Union to the United States.

To diminish this uncertainty and provide a more predictable framework for such data transfers, the Department of Commerce is issuing this document and Frequently Asked Questions ("the Principles") under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. The Principles cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States.

Decisions by organizations to qualify for the safe harbor are entirely voluntary, and organizations may qualify for the safe harbor in different ways. Organizations that decide to adhere to the Principles must comply with the Principles in order to obtain and retain the benefits of the safe harbor and publicly declare that they do so. For example, if an organization joins a self-regulatory privacy program that adheres to the Principles, it qualifies for the safe harbor. Organizations may also qualify by developing their own self-regulatory privacy policies provided that they conform with the Principles. Where in complying with the Principles, an organization relies in whole or in part on self-regulation, its failure to comply with such self-regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts. (See the annex for the list of U.S. statutory bodies recognized by the EU.) In addition, organizations subject to a statutory, regulatory, administrative or other body of law (or of rules) that effectively protects personal privacy may also qualify for safe harbor benefits. In all instances, safe harbor benefits are assured from the date on which each organization wishing to qualify for the safe harbor self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth in the Frequently Asked Question on Self-Certification.

Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding

legitimate interests furthered by such authorization; or (c) if the effect of the Directive of Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

Organizations may wish for practical or other reasons to apply the Principles to all their data processing operations, but they are only obligated to apply them to data transferred after they enter the safe harbor. To qualify for the safe harbor, organizations are not obligated to apply these Principles to personal information in manually processed filing systems. Organizations wishing to benefit from the safe harbor for receiving information in manually processed filing systems from the EU must apply the Principles to any such information transferred after they enter the safe harbor. An organization that wishes to extend safe harbor benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department of Commerce (or its designee) and conform to the requirements set forth in the Frequently Asked Question on Self-Certification. Organizations will also be able to provide the safeguards necessary under Article 26 of the Directive if they include the Principles in written agreements with parties transferring data from the EU for the substantive privacy provisions, once the other provisions for such model contracts are authorized by the Commission and the Member States.

U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbor organizations, except where organizations have committed to cooperate with European Data Protection Authorities. Unless otherwise stated, all provisions of the Safe Harbor Principles and Frequently asked Questions apply where they are relevant.

"Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form.

NOTICE

An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

CHOICE

An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(2) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party identifies and treats it as sensitive.

ONWARD TRANSFER

To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

SECURITY

Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

DATA INTEGRITY

Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

ACCESS

Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's

privacy in the case in question, or where the rights of persons other than the individual would be violated.

ENFORCEMENT

Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

(1) It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

(2) It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

Annex

List of U.S. Statutory Bodies Recognized by the European Union

The European Union recognizes the following U.S. government bodies as being empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals in case of non-compliance with the Principles implemented in accordance with the FAQs:

- The Federal Trade Commission on the basis of its authority under Section 5 of the Federal Trade Commission Act,

- The Department of Transportation on the basis of its authority under Title 49 United States Code Section 41712.

ANNEX II

FREQUENTLY ASKED QUESTIONS (FAQs)

FAQ 1 - Sensitive Data

Q: Must an organization always provide explicit (opt in) choice with respect to sensitive data?

A: No, such choice is not required where the processing is: (1) in the vital interests of the data subject or another person; (2) necessary for the establishment of legal claims or defenses; (3) required to provide medical care or diagnosis; (4) carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political,

philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; (5) necessary to carry out the organization's obligations in the field of employment law; or (6) related to data that are manifestly made public by the individual.

FAQ 2 - Journalistic Exceptions

Q: Given U.S. constitutional protections for freedom of the press and the Directive's exemption for journalistic material, do the Safe Harbor Principles apply to personal information gathered, maintained, or disseminated for journalistic purposes?

A: Where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Safe Harbor Principles.

FAQ 3 - Secondary Liability

Q: Are Internet Service Providers (ISPs), telecommunications carriers, or other organizations liable under the Safe Harbor Principles when on behalf of another organization they merely transmit, route, switch or cache information that may violate their terms?

A: No. As is the case with the Directive itself, the safe harbor does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.

FAQ 4 - Investment Banking and Audits

Q: The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. Under what circumstances is this permitted by the Notice, Choice, and Access Principles?

A: Investment bankers or auditors may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of companies' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

FAQ 5 - The Role of the Data Protection Authorities

Q: How will companies that commit to cooperate with European Union Data Protection Authorities (DPAs) make those commitments and how will they be implemented?

A: Under the safe harbor, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Safe Harbor Principles. More specifically as set out in the Enforcement Principle, they must provide (a) recourse for individuals to whom the data relate, (b) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true, and (c) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a) and (c) of the Enforcement Principle if it adheres to the requirements of this FAQ for cooperating with the DPAs.

An organization may commit to cooperate with the DPAs by declaring in its safe harbor certification to the Department of Commerce (see FAQ 6 on self-certification) that the organization:

1. elects to satisfy the requirement in points (a) and (c) of the Safe Harbor Enforcement Principle by committing to cooperate with the DPAs;

2. will cooperate with the DPAs in the investigation and resolution of complaints brought under the safe harbor; and

3. will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Safe Harbor Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.

The cooperation of the DPAs will be provided in the form of information and advice in the following way:

- The advice of the DPAs will be delivered through an informal panel of DPAs established at the European Union level, which will inter alia help ensure a harmonized and coherent approach.

- The panel will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the safe harbor. This advice will be designed to ensure that the Safe Harbor Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.

- The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for safe harbor purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.

- Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60

days after receiving a complaint or referral and more quickly where possible.

- The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.

- The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.

As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to submit the matter to the Federal Trade Commission or other U.S. federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been seriously breached and must therefore be considered null and void. In the latter case, the panel will inform the Department of Commerce (or its designee) so that the list of safe harbor participants can be duly amended. Any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Safe Harbor Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act or other similar statute.

Organizations choosing this option will be required to pay an annual fee which will be designed to cover the operating costs of the panel, and they may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The annual fee will not exceed USD 500 and will be less for smaller companies.

The option of co-operating with the DPAs will be available to organizations joining the safe harbor during a three-year period. The DPAs will reconsider this arrangement before the end of that period if the number of U.S. organizations choosing this option proves to be excessive.

FAQ 6 - Self-Certification

Q: How does an organization self-certify that it adheres to the Safe Harbor Principles?

A: Safe harbor benefits are assured from the date on which an organization self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.

To self-certify for the safe harbor, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the safe harbor, that contains at least the following information:

1. name of organization, mailing address, e-mail address, telephone and fax numbers;

2. description of the activities of the organization with respect to personal information received from the EU; and

3. description of the organization's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the

handling of complaints, access requests, and any other issues arising under the safe harbor, (d) the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programs in which the organization is a member, (f) method of verification (e.g. in-house, third party)(1), and (g) the independent recourse mechanism that is available to investigate unresolved complaints.

Where the organization wishes its safe harbor benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organization arising out of human resources information that is listed in the annex to the Principles. In addition the organization must indicate this in its letter and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with FAQ 9 and FAQ 5 as applicable and that it will comply with the advice given by such authorities.

The Department (or its designee) will maintain a list of all organizations that file such letters, thereby assuring the availability of safe harbor benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11. Such self-certification letters should be provided not less than annually. Otherwise the organization will be removed from the list and safe harbor benefits will no longer be assured. Both the list and the self-certification letters submitted by the organizations will be made publicly available. All organizations that self-certify for the safe harbor must also state in their relevant published privacy policy statements that they adhere to the Safe Harbor Principles.

The undertaking to adhere to the Safe Harbor Principles is not time-limited in respect of data received during the period in which the organization enjoys the benefits of the safe harbor. Its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the safe harbor for any reason.

An organization that will cease to exist as a separate legal entity as a result of a merger or a takeover must notify the Department of Commerce (or its designee) of this in advance. The notification should also indicate whether the acquiring entity or the entity resulting from the merger will (1) continue to be bound by the Safe Harbor Principles by the operation of law governing the takeover or merger or (2) elect to self-certify its adherence to the Safe Harbor Principles or put in place other safeguards, such as a written agreement that will ensure adherence to the Safe Harbor Principles. Where neither (1) nor (2) applies, any data that has been acquired under the safe harbor must be promptly deleted.

An organization does not need to subject all personal information to the Safe Harbor Principles, but it must subject to the Safe Harbor Principles all personal data received from the EU after it joins the safe harbor.

Any misrepresentation to the general public concerning an organization's adherence to the Safe Harbor Principles may be actionable by the Federal Trade Commission or other relevant government body. Misrepresentations to the Department of Commerce (or its designee) may be actionable under the False Statements Act (18 U.S.C. § 1001).

FAQ 7 - Verification

Q: How do organizations provide follow up procedures for verifying that the attestations and assertions they make about their safe harbor privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Safe Harbor Principles?

A: To meet the verification requirements of the Enforcement Principle, an organization may verify such attestations and assertions either through self-assessment or outside compliance reviews.

Under the self-assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It would also need to indicate that its privacy policy conforms to the Safe Harbor Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self-assessment should be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.

Organizations should retain their records on the implementation of their safe harbor privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction.

Where the organization has chosen outside compliance review, such a review needs to demonstrate that its privacy policy regarding personal information received from the EU conforms to the Safe Harbor Principles, that it is being complied with and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include without limitation auditing, random reviews, use of "decoys", or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed should be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance.

FAQ 8 - Access

Access Principle:

Individuals must have access to personal information about them that an organization holds and be able to correct, amend or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the legitimate rights of persons other than the individual would be violated.

1. Q: Is the right of access absolute?

1. A: No. Under the safe Harbor Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. Nonetheless, the obligation of an organization to provide access to the personal information it holds about an individual is subject to the principle of proportionality or reasonableness and has to be tempered in certain instances. Indeed, the Explanatory Memorandum to the 1980 OECD Privacy Guidelines makes clear that an organization's access obligation is not absolute. It does not require the exceedingly thorough search mandated, for example, by a subpoena, nor does it require access to all the different forms in which the information may be maintained by the organization.

Rather, experience has shown that in responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with and/or about the nature of the information (or its use) that is the subject of the access request. Individuals do not, however, have to justify requests for access to their own data.

Expense and burden are important factors and should be taken into account but they are not controlling in determining whether providing access is reasonable. For example, if the information is used for decisions that will significantly affect the individual (e.g., the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these FAQs, the organization would have to disclose that information even if it is relatively difficult or expensive to provide.

If the information requested is not sensitive or not used for decisions that will significantly affect the individual (e.g., non-sensitive marketing data that is used to determine whether or not to send the individual a catalog), but is readily available and inexpensive to provide, an organization would have to provide access to factual information that the organization stores about the individual. The information concerned could include facts obtained from the individual, facts gathered in the course of a transaction, or facts obtained from others that pertain to the individual.

Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be denied in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

2. Q: What is confidential commercial information and may organizations deny access in order to safeguard it?

2. A: Confidential commercial information (as that term is used in the Federal Rules of Civil Procedure on discovery) is information which an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. The particular computer program an

organization uses, such as a modeling program, or the details of that program may be confidential commercial information. Where confidential commercial information can be readily separated from other information subject to an access request, the organization should redact the confidential commercial information and make available the non-confidential information. Organizations may deny or limit access to the extent that granting it would reveal its own confidential commercial information as defined above, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another where such information is subject to a contractual obligation of confidentiality in circumstances where such an obligation of confidentiality would normally be undertaken or imposed.

3. Q: In providing access, may an organization disclose to individuals personal information about them derived from its data bases or is access to the data base itself required?

3. A: Access can be provided in the form of disclosure by an organization to the individual and does not require access by the individual to an organization's data base.

4. Q: Does an organization have to restructure its data bases to be able to provide access?

4. A: Access needs to be provided only to the extent that an organization stores the information. The access principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

5. Q: These replies make clear that access may be denied in certain circumstances. In what other circumstances may an organization deny individuals access to their personal information?

5. A: Such circumstances are limited, and any reasons for denying access must be specific. An organization can refuse to provide access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:

a. interference with execution or enforcement of the law, including the prevention, investigation or detection of offenses or the right to a fair trial;

b. interference with private causes of action, including the prevention, investigation or detection of legal claims or the right to a fair trial;

c. disclosure of personal information pertaining to other individual(s) where such references cannot be redacted;

d. breaching a legal or other professional privilege or obligation;

e. breaching the necessary confidentiality of future or ongoing negotiations, such as those involving the acquisition of publicly quoted companies;

f. prejudicing employee security investigations or grievance proceedings;

g. prejudicing the confidentiality that may be necessary for limited periods in connection with employee succession planning and corporate re-organizations; or

h. prejudicing the confidentiality that may be necessary in connection with monitoring, inspection or regulatory functions connected with sound economic or financial management; or

i. other circumstances in which the burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated.

An organization which claims an exception has the burden of demonstrating its applicability (as is normally the case). As noted above, the reasons for denying or limiting access and a contact point for further inquiries should be given to individuals.

6. Q: Can an organization charge a fee to cover the cost of providing access?

6. A: Yes. The OECD Guidelines recognize that organizations may charge a fee, provided that it is not excessive. Thus organizations may charge a reasonable fee for access. Charging a fee may be useful in discouraging repetitive and vexatious requests.

Organizations that are in the business of selling publicly available information may thus charge the organization's customary fee in responding to requests for access. Individuals may alternatively seek access to their information from the organization that originally compiled the data.

Access may not be refused on cost grounds if the individual offers to pay the costs.

7. Q: Is an organization required to provide access to personal information derived from public records?

7. A: To clarify first, public records are those records kept by government agencies or entities at any level that are open to consultation by the public in general. It is not necessary to apply the Access Principle to such information as long as it is not combined with other personal information, apart from when small amounts of non-public record information are used for indexing or organizing public record information. However, any conditions for consultation established by the relevant jurisdiction are to be respected. Where public record information is combined with other non-public record information (other than as specifically noted above), however, an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.

8. Q: Does the Access Principle have to be applied to publicly available personal information?

8. A: As with public record information (see Q7), it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information.

9. Q: How can an organization protect itself against repetitious or vexatious requests for access?

9. A: An organization does not have to respond to such requests for access. For these reasons, organizations may charge a reasonable fee and may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency

with which information is updated, the purpose for which the data are used, and the nature of the information.

10. Q: How can an organization protect itself against fraudulent requests for access?

10. A: An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.

11. Q: Is there a time within which responses must be provided to access requests?

11. A: Yes, organizations should respond without excessive delay and within a reasonable time period. This requirement may be satisfied in different ways as the explanatory memorandum to the 1980 OECD Privacy Guidelines states. For example, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests.

FAQ 9 - Human Resources

1. Q: Is the transfer from the EU to the United States of personal information collected in the context of the employment relationship covered by the safe harbor?

1. A: Yes, where a company in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the safe harbor, the transfer enjoys the benefits of the safe harbor. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.

The Safe Harbor Principles are relevant only when individually identified records are transferred or accessed. Statistical reporting relying on aggregate employment data and/or the use of anonymized or pseudonymized data does not raise privacy concerns.

2. Q: How do the Notice and Choice Principles apply to such information?

2. A: A U.S. organization that has received employee information from the EU under the safe harbor may disclose it to third parties and/or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with choice before doing so, unless they have already authorized the use of the information for such purposes. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.

It should be noted that certain generally applicable conditions for transfer from some Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.

In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.

To the extent and for the period necessary to avoid prejudicing the legitimate interests of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

3. Q: How does the Access Principle apply?

3. A: The FAQs on access provide guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The safe harbor requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

4. Q: How will enforcement be handled for employee data under the Safe Harbor Principles?

4. A: In so far as information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the company in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employee works. This also includes cases where the alleged mishandling of their personal information has taken place in the United States, is the responsibility of the U.S. organization that has received the information from the employer and not of the employer and thus involves an alleged breach of the Safe Harbor Principles, rather than of national laws implementing the Directive. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.

A U.S. organization participating in the safe harbor that uses EU human resources data transferred from the European Union in the context of the employment relationship and that wishes such transfers to be covered by the safe harbor must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases. The DPAs that have agreed to cooperate in this way will notify the European Commission and the Department of Commerce. If a U.S. organization participating in the safe harbor wishes to transfer human resources data from a Member State where the DPA has not so agreed, the provisions of FAQ 5 will apply.

FAQ 10 - Article 17 contracts

Q: When data is transferred from the EU to the United States only for processing purposes, will a contract be required, regardless of participation by the processor in the safe harbor?

A: Yes. Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU. The purpose of the contract is to protect the interests of the data controller, i.e. the person or body who determines the purposes and means of processing, who retains full responsibility for the data vis-à-vis the individual(s) concerned. The contract thus specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure.

A U.S. organization participating in the safe harbor and receiving personal information from the EU merely for processing thus does not have to apply the Principles to this information, because the controller in the EU remains responsible for it vis-à-vis the individual in accordance with the relevant EU provisions (which may be more stringent than the equivalent Safe Harbor Principles).

Because adequate protection is provided by safe harbor participants, contracts with safe harbor participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the Member States) as would be required for contracts with recipients not participating in the safe harbor or otherwise not providing adequate protection.

FAQ No 11 - Dispute Resolution and Enforcement

Q: How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organization's persistent failure to comply with the Principles be handled?

A: The Enforcement Principle sets out the requirements for safe harbor enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ on verification (FAQ 7). This FAQ 11 addresses points (a) and (c), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Enforcement Principle's requirements. Organizations may satisfy the requirements through the following: (1) compliance with private sector developed privacy programs that incorporate the Safe Harbor Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Union or their authorized representatives. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle's requirements are additional to the requirements set forth in paragraph 3 of the introduction to the Principles that self-regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.

Recourse Mechanisms.

Consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Whether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record. As required by the enforcement principle, the recourse available to individuals must be readily available and affordable. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organization operating the recourse mechanism, but such requirements should be transparent and justified (for example to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Safe Harbor Principles(2). They should also co-operate in the development of tools such as standard complaint forms to facilitate the complaint resolution process.

Remedies and Sanctions.

The result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, in so far as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who has brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances(3). Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive orders. Private sector dispute resolution bodies and self-regulatory bodies must notify failures of safe harbor organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department of Commerce (or its designee).

FTC Action.

The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organizations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbor Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that is has reason(s) to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal

contempt for violation of a federal court order. The FTC will notify the Department of Commerce of any such actions it takes. The Department of Commerce encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Safe Harbor Principles.

Persistent Failure to Comply.

If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the safe harbor. Persistent failure to comply arises where an organization that has self-certified to the Department of Commerce (or its designee) refuses to comply with a final determination by any self-regulatory or government body or where such a body determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce (or its designee) of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001).

The Department (or its designee) will indicate on the public list it maintains of organizations self-certifying adherence to the Safe Harbor Principles any notification it receives of persistent failure to comply, whether it is received from the organization itself, from a self-regulatory body, or from a government body, but only after first providing thirty (30) days' notice and an opportunity to respond to the organization that has failed to comply. Accordingly, the public list maintained by the Department of Commerce (or its designee) will make clear which organizations are assured and which organizations are no longer assured of safe harbor benefits.

An organization applying to participate in a self-regulatory body for the purposes of requalifying for the safe harbor must provide that body with full information about its prior participation in the safe harbor.

FAQ 12 - Choice - Timing of Opt Out

Q: Does the Choice Principle permit an individual to exercise choice only at the beginning of a relationship or at any time?

A: Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" (or choice) of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out". In the United States, individuals may be able to exercise this option through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.

Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization

promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.

FAQ 13 - Travel Information

Q: When can airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, be transferred to organizations located outside the EU?

A: Such information may be transferred in several different circumstances. Under Article 26 of the Directive, personal data may be transferred "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" on the condition that it (1) is necessary to provide the services requested by the consumer or to fulfill the terms of an agreement, such as a "frequent flyer" agreement; or (2) has been unambiguously consented to by the consumer. U.S. organizations subscribing to the safe harbor provide adequate protection for personal data and may therefore receive data transfers from the EU without meeting those conditions or other conditions set out in Article 26 of the Directive. Since the safe harbor includes specific rules for sensitive information, such information (which may need to be collected, for example, in connection with customers' needs for physical assistance) may be included in transfers to safe harbor participants. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may inter alia impose special conditions for the handling of sensitive data.

FAQ 14 - Pharmaceutical and Medical Products

1. Q: If personal data are collected in the EU and transferred to the United States for pharmaceutical research and/or other purposes, do Member State laws or the Safe Harbor Principles apply?

1. A: Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Safe Harbor Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.

2. Q: Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the safe harbor, may the organization use the data for a new scientific research activity?

2. A: Yes, if appropriate notice and choice have been provided in the first instance. Such a notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is

not consistent with the general research purpose(s) for which the data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.

3. Q: What happens to an individual's data if a participant decides voluntarily or at the request of the sponsor to withdraw from the clinical trial?

3. A: Participants may decide or be asked to withdraw from a clinical trial at any time. Any data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, however, if this was made clear to the participant in the notice at the time he or she agreed to participate.

4. Q: Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Are similar transfers allowed to parties other than regulators, such as company locations and other researchers?

4. A: Yes, consistent with the Principles of Notice and Choice.

5. Q: To ensure objectivity in many clinical trials, participants, and often investigators, as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Will participants in such clinical trials (referred to as "blinded" studies) have access to the data on their treatment during the trial?

5. A: No, such access does not have to be provided to a participant if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring company.

6. Q: Does a pharmaceutical or medical device firm have to apply the Safe Harbor Principles with respect to notice, choice, onward transfer, and access in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices (e.g. a pacemaker)?

6. A: No, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers, to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.

7. Q: Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he/she can identify the research subject under special circumstances (e.g. if follow-up medical attention is required). Does a transfer from the

EU to the United States of data coded in this way constitute a transfer of personal data that is subject to the Safe Harbor Principles?

7. A: No. This would not constitute a transfer of personal data that would be subject to the Principles.

FAQ 15 - Public Record and Publicly Available Information

Q: Is it necessary to apply the Notice, Choice and Onward Transfer Principles to public record information or publicly available information?

A: It is not necessary to apply the Notice, Choice or Onward Transfer Principles to public record information, as long as it is not combined with non-public record information and as long as any conditions for consultation established by the relevant jurisdiction are respected.

Also, it is generally not necessary to apply the Notice, Choice or Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.

Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the safe harbor.

(1) See FAQ 7 on verification.

(2) Dispute resolution bodies are not required to conform with the enforcement principle. They may also derogate from the Principles where they encounter conflicting obligations or explicit authorizations in the performance of ther specific tasks.

(3) Dispute resolution bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used or disclosed information in blatant contravention of the Principles.

ANNEX III

Safe Harbor Enforcement Overview

Federal and State "Unfair and Deceptive Practices" Authority and Privacy

This memorandum outlines the authority of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act (15 U.S.C. §§ 41-58, as amended) to take action against those who fail to protect the privacy of personal information in accordance with their representations and/or commitments to do so. It also addresses the exceptions to that authority and the ability of other federal and state agencies to take action where the FTC does not have authority(1).

FTC Authority over Unfair or Deceptive Practices

Section 5 of the Federal Trade Commission Act declares "unfair or deceptive acts or practices in or affecting commerce" to be illegal. 15 U.S.C. § 45(a)(1). Section 5 confers on the FTC the plenary power to prevent such acts and

practices. 15 U.S.C. § 45(a)(2). Accordingly, the FTC may, upon conducting a formal hearing, issue a "cease and desist" in order to stop the offending conduct. 15 U.S.C. § 45(b). If it would be in the public interest to do so, the FTC can also seek a temporary restraining order or temporary or permanent injunction in the U.S. district court. 15 U.S.C. § 53(b). In cases where there is a widespread pattern of unfair or deceptive acts or practices, or where it has already issued cease and desist orders on the matter, the FTC may promulgate an administrative rule prescribing the acts or practices involved. 15 U.S.C. § 57a.

Anyone who does not comply with an FTC order is subject to a civil penalty of up to USD 11000, with each day of a continuing violation constituting a separate violation(2). 15 U.S.C. § 45(1). Likewise, anyone who knowingly violates an FTC rule is liable for USD 11000 for each violation. 15 U.S.C. § 45(m). Enforcement actions can be brought by either the Department of Justice, or if it declines, by the FTC. 15 U.S.C. § 56.

FTC Authority and Privacy

In exercising its Section 5 authority, the FTC takes the position that misrepresenting why information is being collected from consumers or how the information will be used constitutes a deceptive practice(3). For example, in 1998, the FTC filed a complaint against GeoCities for disclosing information it had collected on its website to third parties for purposes of solicitation, and without prior permission, despite its representations to the contrary(4). The FTC staff has also asserted that the collection of personal information from children, and sale and disclosure of that information, without the parents' consent is likely to be an unfair practice(5).

In a letter to Director-General John Mogg of the European Commission, FTC Chairman Pitofsky noted the limitations on the FTC's authority to protect privacy where there has not been a misrepresentation (or no representation at all) as to how the information collected will be used. FTC Chairman Pitofsky letter to John Mogg (September 23, 1998). However, companies that want to avail themselves of the proposed "safe harbor" will have to certify that they will protect the information they collect in accordance with prescribed guidelines. Consequently, where a company certifies that it will safeguard the privacy of information and then fails to do so, such action would be a misrepresentation and a "deceptive practice" within the meaning of Section 5.

As the FTC's jurisdiction extends to unfair or deceptive acts or practices "in or affecting commerce", the FTC will not have jurisdiction over the collection and use of personal information for non-commercial purposes, charitable fund-raising for example. See Pitofsky letter, p. 3. However, the use of personal information in any commercial transaction will satisfy this jurisdictional predicate. Thus, for example, the sale by an employer of personal information on its employees to a direct marketer would bring the transaction within the purview of Section 5.

Section 5 Exceptions

Section 5 established exceptions to the FTC's authority over unfair or deceptive acts or practices with respect to:

- financial institutions, including banks, savings and loans, and credit unions;

- telecommunications and interstate transportation common carriers;

- air carriers; and

- packers and stockyard operators.

See 15 U.S.C. § 45(a)(2). We discuss each exception, and the regulatory authority that takes its place, below.

Financial institutions(6)

The first exception applies to "banks, savings and loan institutions described in section 18(f)(3) [15 U.S.C. § 57a(f)(3)]" and "Federal credit unions described in section 18(f)(4) [15 U.S.C. § 57a(f)(4)]"(7). These financial institutions are instead subject to regulations issued by the Federal Reserve Board, the Office of Thrift Supervision(8), and the National Credit Union Administration Board, respectively. See 15 U.S.C. § 57a(f). These regulatory agencies are directed to prescribe the regulations necessary to prevent unfair and deceptive practices by these financial institutions(9) and to establish a separate division to handle consumer complaints. 15 U.S.C. § 57a(f)(1). Finally, authority for enforcement derives from section 8 of the Federal Deposit Insurance Act (12 U.S.C. § 1818), for banks and savings and loans, and sections 120 and 206 of the Federal Credit Union Act, for Federal credit unions. 15 U.S.C. §§ 57a(f)(2)-(4).

Although the insurance industry is not specifically included in the list of exceptions in Section 5, the McCarran-Ferguson Act (15 U.S.C. § 1011 et seq.) generally leaves the regulation of the business of insurance to the individual states(10). Furthermore, pursuant to section 2(b) of the McCarran-Ferguson Act, no federal law will invalidate, impair, or supersede state regulation "unless such Act specifically relates to the business of insurance." 15 U.S.C. § 1012(b). However, the provisions of the FTC Act apply to the insurance industry "to the extent that such business is not regulated by State law." Id. It should also be noted that McCarran-Ferguson defers to the states only with respect to "the business of insurance." Therefore, the FTC retains residual authority over unfair or deceptive practices by insurance companies when they are not engaged in the business of insurance. This could include, for example, when insurers sell personal information about their policy holders to direct marketers of non-insurance products(11).

Common carriers

The second Section 5 exception extends to those common carriers that are "subject to the acts to regulate commerce." 15 U.S.C. § 45(a)(2). In this case, the "Acts to regulate commerce" refer to subtitle IV of Title 49 of the United States Code and to the Communications Act of 1934 (47 U.S.C. § 151 et seq.) (the Communications Act). See 15 U.S.C. § 44.

49 U.S.C. subtitle IV (Interstate Transportation) covers rail carriers, motor carriers, water carriers, brokers, freight forwarders, and pipeline carriers. 49 U.S.C. § 10101 et seq. These various common carriers are subject to regulation by the Surface Transportation Board, an independent agency within the Department of Transportation. 49 U.S.C. §§ 10501, 13501, and 15301. In each instance, the carrier is prohibited from disclosing information about the nature, destination, and other aspects of its cargo that might be used to the shipper's detriment. See 49 U.S.C. §§ 11904, 14908, and 16103. We note that these provisions refer to information regarding the shipper's cargo and thus do not appear to extend to

personal information about the shipper that is unrelated to the shipment in question.

As for the Communications Act, it provides for the regulation of "interstate and foreign commerce in communication by wire and radio" by the Federal Communications Commission (FCC). See 47 U.S.C. §§ 151 and 152. In addition to common carrier telecommunications companies, the Communications Act also applies to companies such as television and radio broadcasters and cable service providers which are not common carriers. As such, these latter companies do not qualify for the exception under Section 5 of the FTC Act. Thus, the FTC has jurisdiction to investigate these companies for unfair and deceptive practices, while the FCC has concurrent jurisdiction to enforce its independent authority in this area as described below.

Under the Communications Act, "every telecommunications carrier", including local exchange carriers, has a duty to protect the privacy of customer proprietary information(12). 47 U.S.C. § 222(a). In addition to this general privacy-protection authority, the Communications Act was amended by the Cable Communications Policy Act of 1984 (the Cable Act), 47 U.S.C. § 521 et seq., to mandate specifically that cable operators protect the privacy of "personally identifiable information" on cable subscribers. 47 U.S.C. § 551(13). The Cable Act restricts the collection of personal information by cable operators and requires the cable operator to notify the subscriber of the nature of the information collected and how that information will be used. The Cable Act gives subscribers the right of access to the information about them and requires cable operators to destroy that information when it is no longer needed.

The Communications Act empowers the FCC to enforce these two privacy provisions, either at its own initiation or in response to an outside complaint(14). 47 U.S.C. §§ 205, 403; id. § 208. If the FCC determines that a telecommunications carrier (including a cable operator) has violated the privacy provisions of section 222 or section 551, there are three basic actions it may take. First, after a hearing and determination of violation, the Commission may order the carrier to pay monetary damages(15). 47 U.S.C. § 209. Alternatively, the FCC may order the carrier to cease and desist from the offending practice or omission. 47 U.S.C. § 205(a). Finally, the Commission may also order an offending carrier to "conform to and observe [any] regulation or practice" that the FCC may prescribe. Id.

Private persons who believe a telecommunications carrier or cable operator has violated the relevant provisions of the Communications Act or the Cable Act may either file a complaint with the FCC or take their claims to a federal district court. 47 U.S.C. § 207. A complainant who prevails in a federal court action against a telecommunications carrier for failure to protect customer proprietary information under the broader section 222 of the Communications Act may be awarded actual damages and attorneys' fees. 47 U.S.C. § 206. A complainant who files suit claiming a privacy violation under the cable-specific section 551 of the Cable Act may, in addition to actual damages and attorneys' fees, also be awarded punitive damages and reasonable litigation costs. 47 U.S.C. § 551(f).

The FCC has adopted detailed rules to implement section 222. See 47 CFR 64.2001-2009. The rules set out specific safeguards to protect against

unauthorized access to customer proprietary network information. The regulations require telecommunications carriers to:

- develop and implement software systems that "flag" a customer's notice/approval status when the customer's service record first comes on-screen;

- maintain an electronic "audit trail" to track access to a customer's account, including when a customer's record is opened, by whom, and for what purpose;

- train their personnel on the authorized use of customer proprietary network information, with appropriate disciplinary processes in place;

- establish a supervisory review process to ensure compliance when conducting outbound marketing; and

- certify to the FCC, on an annual basis, how they are complying with these regulations.

Air carriers

U.S. and foreign air carriers that are subject to the Federal Aviation Act of 1958 are also exempt from Section 5 of the FTC Act. See 15 U.S.C. § 45(a)(2). This includes anyone who provides interstate or foreign transportation of goods or passengers, or who transports mail, by aircraft. See 49 U.S.C. § 40102. Air carriers are subject to the authority of the Department of Transportation. In this regard, the Secretary of Transportation is authorized to take action "preventing unfair, deceptive, predatory, or anticompetitive practices in air transportation." 49 U.S.C. § 40101(a)(9). The Secretary of Transportation can investigate whether a U.S. or foreign air carrier, or a ticket agent, has engaged in an unfair or deceptive practice if it is in the public interest. 49 U.S.C. § 41712. After a hearing, the Secretary of Transportation can issue an order to stop the illegal practice. Id. To our knowledge, the Secretary of Transportation has not exercised this authority to address the issue of protecting the privacy of personal information about airline customers(16).

There are two provisions protecting the privacy of personal information that apply to air carriers in specific contexts. First, the Federal Aviation Act protects the privacy of pilot applicants. See 49 U.S.C. § 44936(f). While allowing air carriers to obtain an applicant's employment records, the Act gives the applicant the right to notice that the records have been requested, to give consent to the request, to correct inaccuracies, and to have the records divulged only to those involved in the hiring decision. Second, DOT regulations require passenger manifest information collected for government use in the event of an aviation disaster to "be kept confidential and released only to the U.S. Department of State, the National Transportation Board (upon the NTSB's request), and the U.S. Department of Transportation." 14 CFR part 243, § 243.9(c) (as added by 63 FR 8258).

Packers and stockyards

With regard to the Packers and Stockyards Act of 1921 (7 U.S.C. § 181 et seq.), the Act makes it unlawful for "any packer with respect to livestock, meats, meat food products, or livestock products in unmanufactured form, or for any live poultry dealer with respect to live poultry, to engage in or use any

unfair, unjustly discriminatory, or deceptive practice or device." 7 U.S.C. § 192(a); see also 7 U.S.C. § 213(a) (prohibiting "any unfair, unjustly discriminatory, or deceptive practice or device" in connection with livestock). The Secretary of Agriculture has the primary responsibility to enforce these provisions, while the FTC retains jurisdiction over retail transactions and those involving the poultry industry. 7 U.S.C. § 227(b)(2).

It is not clear whether the Secretary of Agriculture will interpret the failure by a packer or stockyard operator to protect personal privacy in accordance with stated policy to be a "deceptive" practice under the Packers and Stockyards Act. However, the Section 5 exception applies to persons, partnerships, or corporations only "insofar as they are subject to the Packers and Stockyards Act." Therefore, if personal privacy is not an issue within the purview of the Packers and Stockyards Act, then the exception in Section 5 may very well not apply and packers and stockyard operators would be subject to the authority of the FTC in that regard.

State "Unfair and Deceptive Practices" Authority

According to an analysis prepared by FTC staff, "All 50 states plus the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted laws more or less like the Federal Trade Commission Act ('FTCA') to prevent unfair or deceptive trade practices." FTC fact sheet, reprinted in "Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation", 59 Tul, L. Rev. 427 (1984). In all cases, an enforcement agency has the authority "to conduct investigations through the use of subpoenas or civil investigative demands, obtain assurances of voluntary compliance, to issue cease and desist orders or obtain court injunctions preventing the use of unfair, unconscionable or deceptive trade practices. Id. In 46 jurisdictions, the law allows private actions for actual, double, treble, or punitive damages and, in some cases, recovery of costs and attorney's fees. Id."

Florida's Deceptive and Unfair Trade Practices Act, for example, authorizes the attorney general to investigate and file civil actions against "unfair methods of competition, unfair, unconscionable or deceptive trade practices," including false or misleading advertising, misleading franchise or business opportunities, fraudulent telemarketing, and pyramid schemes. See also N.Y. General Business Law § 349 (prohibiting unfair acts and deceptive practices carried out in the course of business).

A survey conducted this year by the National Association of Attorneys General (NAAG) confirms these findings. Of 43 states that responded, all have "mini-FTC" statutes or other statutes that provide comparable protection. Also according to the NAAG survey, 39 states indicated they would have the authority to hear complaints by non-residents. With respect to consumer privacy, in particular, 37 out of 41 states that responded indicated that they would respond to complaints alleging that a company within their jurisdiction was not adhering to its self-declared privacy policy.

(1) We do not discuss here all the various federal statutes that address privacy in specific contexts or state statutes and common law that might apply. Statutes at the federal level that regulate the commercial collection and use of personal information include the Cable Communications Policy Act (47 U.S.C. § 551), the Driver's Privacy Protection Act (18 U.S.C. § 2721), the Electronic Communications Privacy Act (18 U.S.C. § 2701 et seq.), the Electronic Funds Transfer Act (15 U.S.C. §§ 1693, 1693m), the Fair Credit

Reporting Act (15 U.S.C. § 1681 et seq.), the Right to Financial Privacy Act (12 U.S.C. § 3401 et seq.), the Telephone Consumer Protection Act (47 U.S.C. § 227), and the Video Privacy Protection Act (18 U.S.C. § 2710), among others. Many states have analogous legislation in these areas. See, e.g., Mass. Gen. Laws ch. 167B, § 16 (prohibiting financial institutions from disclosing a customer's financial records to a third party without either the customer's consent or legal process) N.Y. Pub. Health Law § 17 (limiting use and disclosure of medical or mental health records and giving patients the right of access thereto).

(2) In such an action, the United States district court can also order injunctive and equitable relief appropriate to enforcing the FTC order. 15 U.S.C. § 45(1).

(3) "Deceptive practice" is defined as a representation, omission or practice that is likely to mislead reasonable consumers in a material fashion.

(4) See www.ftc.gov/opa/1998/9808/geocitie.htm.

(5) See staff letter to Center for Media Education, www.ftc.gov/os/1997/9707/cenmed.htm. In addition, the Children's Online Privacy Protection Act of 1998 confers on the FTC specific legal authority to regulate the collection of personal information from children by website and online service operators. See 15 U.S.C. §§ 6501-6506. In particular, the act requires online operators to give notice and to obtain verifiable parental consent before collecting, using, or disclosing personal information from children. Id., § 6502(b). The act also gives parents a right of access and to refuse permission for the continued use of the information. Id.

(6) On November 12, 1999, President Clinton signed the Gramm-Leach-Bliley Act (Pub. L. 106-102, codified at 15 U.S.C. § 6801 et seq.) into law. The Act limits the disclosure by financial institutions of personal information about their customers. The Act requires financial institutions to, inter alia, notify all customers of their privacy policies and practices with respect to the sharing of personal information with affiliates and non-affiliates. The Act authorizes the FTC, the Federal banking authorities and other authorities to promulgate regulations to implement the privacy protections required by the statute. The agencies have issued proposed regulations for this purpose.

(7) By its terms, this exception does not apply to the securities sector. Therefore, brokers, dealers and others in the securities industry are subject to the concurrent jurisdiction of the Securities and Exchange Commission and the FTC with respect to unfair or deceptive acts and practices.

(8) The exception in Section 5 originally referred to the Federal Home Loan Bank Board which was abolished in August 1989 by the Financial Institutions Reform, Recovery and Enforcement Act of 1989. Its functions were transferred to the Office of Thrift Supervision and to the Resolution Trust Corporation, the Federal Deposit Insurance Corporation, and the Housing Finance Board.

(9) While removing financial institutions from the FTC's jurisdiction, Section 5 also stipulates that whenever the FTC issues a rule on unfair or deceptive acts and practices, the financial regulatory Boards should adopt parallel regulations within 60 days. See 15 U.S.C. § 57a(f)(1).

(10) "The business of insurance, and every person engaged therein, shall be subject to the laws of the several States which relate to the regulation or taxation of such business." 15 U.S.C. § 1012(a).

(11) The FTC has exercised jurisdiction over insurance companies in different contexts. In one case, the FTC took action against a firm for deceptive advertising in a state in which it was not licensed to do business. The FTC's jurisdiction was upheld on the basis that there was no effective state regulation because the firm was effectively beyond the reach of the state. See FTC v. Travelers Health Association, 362 U.S. 293 (1960).

As for the states, 17 have adopted the model "Insurance Information and Privacy Protection Act" prepared by the National Association of Insurance Commissioners (NAIC). The Act includes provisions for notice, use and disclosure, and access. Also, almost all states have adopted the NAIC's model "Unfair Insurance Practices Act", which specifically targets unfair trade practices in the insurance industry.

(12) The term "customer proprietary network information" means information that relates to "the quantity, technical configuration, type, destination, and amount of use of a telecommunications service" by a customer and telephone billing information. 47 U.S.C. § 222(f)(1). However, the term does not include subscriber list information. Id.

(13) The legislation does not expressly define "personally identifiable information".

(14) This authority encompasses the right to redress for privacy violations under both section 222 of the Communications Act or, with respect to cable subscribers, under section 551 of the Cable Act amendment to the Act. See also 47 U.S.C. § 551(f)(3) (civil action in federal district court is a non-exclusive remedy, offered "in addition to any other lawful remedy available to a cable subscriber").

(15) However, the absence of direct damage to a complainant is not grounds to dismiss a complaint. 47 U.S.C. § 208(a).

(16) We understand there are efforts underway within the industry to address the privacy issue. Industry representatives have discussed the proposed safe harbor principles and their possible application to air carriers. The discussion has included a proposal to adopt an industry privacy policy with participating firms expressly subjecting themselves to DOT authority.

ANNEX IV

Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law

This responds to the request by the European Commission for clarification of U.S. law with respect to (a) claims for damages for breaches of privacy, (b) "explicit authorizations" in U.S. law for the use of personal information in a manner inconsistent with the safe harbor principles, and (c) the effect of mergers and takeovers on obligations undertaken pursuant to the safe harbor principles.

A. Damages for Breaches of Privacy

Failure to comply with the safe harbor principles could give rise to a number of private claims depending on the relevant circumstances. In particular, safe

harbor organizations could be held liable for misrepresentation for failing to adhere to their stated privacy policies. Private causes of action for damages for breaches of privacy are also available under common law. Many federal and state statutes on privacy also provide for the recovery of damages by private individuals for violations.

The right to recover damages for invasion of personal privacy is well established under U.S. common law.

Use of personal information in a manner inconsistent with the safe harbor principles can give rise to legal liability under a number of different legal theories. For example, both the transferring data controller and the individuals affected could sue the safe harbor organization which fails to honor its safe harbor commitments for misrepresentation. According to the Restatement of the Law, Second, Torts(1):

One who fraudulently makes a misrepresentation of fact, opinion, intention or law for the purpose of inducing another to act or to refrain from action in reliance upon it, is subject to liability to the other in deceit for pecuniary loss caused to him by his justifiable reliance upon the misrepresentation.

Restatement, § 525. A misrepresentation is "fraudulent" if it is made with the knowledge or in the belief that it is false. Id., § 526. As a general rule, the maker of a fraudulent misrepresentation is potentially liable to everyone who he intends or expects to rely on that misrepresentation for any pecuniary loss they might suffer as a result. Id. 531. Furthermore, a party who makes a fraudulent misrepresentation to another could be liable to a third-party if the tortfeasor intends or expects that his misrepresentation would be repeated to and acted upon by the third-party. Id., § 533.

In the context of the safe harbor, the relevant representation is the organization's public declaration that it will adhere to the safe harbor principles. Having made such a commitment, a conscious failure to abide by the principles could be grounds for a cause of action for misrepresentation by those who relied on the misrepresentation. Because the commitment to adhere to the principles is made to the public at large, the individuals who are the subjects of that information as well as the data controller in Europe that transfers personal information to the U.S. organization could all have causes of action against the U.S. organization for misrepresentation(2). Moreover, the U.S. organization remains liable to them for the "continuing misrepresentation" for as long as they rely on the misrepresentation to their detriment. Restatement, § 535.

Those who rely on a fraudulent misrepresentation have a right to recover damages. According to the Restatement.

The recipient of a fraudulent misrepresentation is entitled to recover as damages in an action of deceit against the maker the pecuniary loss to him of which the misrepresentation is a legal cause.

Restatement, § 549. Allowable damages include actual out-of-pocket loss as well as the lost "benefit of the bargain" in a commercial transaction. Id.; see, e.g., Boling v. Tennessee State Bank, 890 S.W.2d 32 (1994) (bank liable to borrowers for USD 14825 in compensatory damages for disclosing borrowers' personal information and business plans to bank president who had a conflicting interest).

Whereas fraudulent misrepresentation requires either actual knowledge or at least the belief that the representation is false, liability can also attach for negligent misrepresentation. According to the Restatement, whoever makes a false statement in the course of his business, profession, or employment, or in any pecuniary transaction can be held liable "if he fails to exercise reasonable care or competence in obtaining or communicating the information." Restatement, § 552(1). In contrast with fraudulent misrepresentations, damages for negligent misrepresentation are limited to out-of-pocket loss. Id., § 552B(1).

In a recent case, for example, the Superior Court of Connecticut held that a failure by an electric utility to disclose its reporting of customer payment information to national credit agencies sustained a cause of action for misrepresentation. See Brouillard v. United Illuminating Co., 1999 Conn. Super. LEXIS 1754. In that case, the plaintiff was denied credit because the defendant reported payments not received within thirty days of the billing date as "late". The plaintiff alleged that he had not been informed of this policy when he opened a residential electric service account with the defendant. The court specifically held that "a claim for negligent misrepresentation may be based on the defendant's failure to speak when he has a duty to do so." This case also shows that "scienter" or fraudulent intent is not a necessary element in a cause of action for negligent misrepresentation. Thus, a U.S. organization which negligently fails to fully disclose how it will use personal information received under the safe harbor could be held liable for misrepresentation.

Insofar as a violation of the safe harbor principles entailed a misuse of personal information, it could also support a claim by the data subject for the common law tort of invasion of privacy. American law has long recognized causes of action relating to invasions of privacy. In a 1905 case(3), the Georgia Supreme Court found a right to privacy rooted in natural law and common law precepts in holding for a private citizen whose photograph had been used by a life insurance company, without his consent or knowledge, to illustrate a commercial advertisement. Articulating now-familiar themes in American privacy jurisprudence, the court found that the usage of the photograph was "malicious", "false", and tended to "bring plaintiff into ridicule before the world."(4) The foundations of the Pavesich decision have prevailed with minor variations to become the bedrock of American law on this topic. State courts have consistently upheld causes of action in the realm of invasion of privacy, and at least 48 states now judicially recognize some such cause of action(5). Moreover, at least 12 states have constitutional provisions safeguarding their citizens' right to be free from intrusive actions(6), which in some cases could extend to protect against intrusion by non-governmental entities. See, e.g., Hill v. NCAA, 865 P.2d 633 (Ca. 1994); see also S. Ginder, Lost and Found in Cyberspace: Informational Privacy in the age of the Internet, 34 S.D.L. Rev. 1153 (1997) ("Some state constitutions include privacy protections which surpass privacy protections in the U.S. Constitution. Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington have broader privacy protection.")

The Second Restatement of Torts provides an authoritative overview of the law in this area. Reflecting common judicial practice, the Restatement explains that the "right to privacy" encompasses four distinct causes of action in tort under that umbrella. See Restatement, § 652A. First, a cause of action

for "intrusion upon seclusion" may lie against a defendant who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns(7). Second, an "appropriation" case may exist when one takes the name or likeness of another for his own use or benefit(8). Third, the "publication of private facts" is actionable when the matter publicized is of a kind that would be highly offensive to a reasonable person and is not of legitimate concern to the public(9). Lastly, an action for "false light publicity" is appropriate when the defendant knowingly or recklessly places another before the public in a false light that would be highly offensive to a reasonable person(10).

In the context of the safe harbor framework, "intrusion upon seclusion" could encompass the unauthorized collection of personal information whereas the unauthorized use of personal information for commercial purposes could give rise to a claim of appropriation. Similarly, the disclosure of personal information that is inaccurate would give rise to a tort of "false light publicity" if the information meets the standard of being highly offensive to a reasonable person. Finally, the invasion of privacy that results from the publication or disclosure of sensitive personal information could give rise to a cause of action for "publication of private facts." (See examples of illustrative cases below).

On the issue of damages, invasions of privacy give the injured party the right to recover damages for:

(a) the harm to his interest in privacy resulting from the invasion;

(b) his mental distress proved to have been suffered if it is of a kind that normally results from such an invasion; and

(c) special damage of which the invasion is a legal cause.

Restatement, § 652H. Given the general applicability of tort law and the multiplicity of causes of action covering different aspects of privacy interests, monetary damages are likely to be available to those who suffer invasion of their privacy interests as a result of a failure to adhere to the safe harbor principles.

Indeed, state courts are replete with cases alleging invasion of privacy in analogous situations. Ex Parte AmSouth Bancorporation et al., 717 So. 2d 357, for example, involved a class action that alleged the defendant "exploited the trust depositors placed in the Bank, by sharing confidential information regarding Bank depositors and their accounts" to enable a bank affiliate to sell mutual funds and other investments. Damages are often awarded in such cases. In Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580 (D.C.App. 1985), an appellate court reversed a lower court judgement to hold that the use of photographs of the plaintiff "before" and "after" plastic surgery in a presentation in a department store constituted an invasion of privacy through the publication of private facts. In Candebat v. Flanagan, 487 So.2d 207 (Miss. 1986), the defendant insurance company used an accident in which the plaintiff's wife was seriously injured in an advertising campaign. The plaintiff sued for invasion of privacy. The court held that the plaintiff could recover damages for emotional distress and appropriation of identity. Actions for misappropriation can be maintained even if the plaintiff is not personally famous. See, e.g., Staruski v. Continental Telephone Co., 154 Vt. 568

(1990) (defendant derived commercial benefit in using employee's name and photograph in newspaper advertisement). In Pulla v. Amoco Oil Co., 882 F.Supp. 836 (S.D Iowa 1995), an employer intruded on the plaintiff employee's seclusion by having another employee investigate his credit card records in order to verify his sick day absences. The court upheld a jury award of USD 2 in actual damages and USD 500000 in punitive damages. Another employer was held liable for publishing a story in the company newspaper about an employee who was terminated for allegedly falsifying his employment records. See Zinda v. Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis.App. 1987). The story invaded the plaintiff's privacy by publication of a private matter because the newspaper circulated in the community. Finally, a college which tested students for HIV after telling them the blood test was for rubella only was held liable for intrusion upon seclusion. See Doe v. High-Tech Institute, Inc., 972 P.2d 1060 (Colo.App. 1998). (For other reported cases, see Restatement, § 652H, Appendix.)

The United States is often criticized for being overly litigious, but this also means that individuals actually can, and do, pursue legal recourse when they believe they have been wronged. Many aspects of the U.S. judicial system make it easy for plaintiffs to bring suit, either individually or as a class. The legal bar, comparatively larger than in most other countries, makes professional representation readily available. Plaintiffs' counsel representing individuals in private claims will typically work on a contingency fee basis, allowing even poor or indigent plaintiffs to seek redress. This brings up an important factor - in the United States, each side typically bears its own lawyers' fees and other costs. This contrasts with the prevailing rule in Europe wherein the losing party has to reimburse the other side for costs. Without debating the relative merits of the two systems, the U.S. rule is less likely to deter legitimate claims by individuals who would not be able to pay the costs on both sides if they should lose.

Individuals can sue for redress even if their claims are relatively small. Most, if not all U.S. jurisdictions, have small claims courts which provide simplified and less costly procedures for disputes below the statutory limits(11). The potential for punitive damages also offers a financial reward for individuals who might have suffered little direct injury to bring suit against reprehensible misconduct. Finally, individuals who have been injured in the same way can marshal their resources as well as their claims to bring a class-action lawsuit.

A good example of the ability of individuals to bring suit to obtain redress is the pending litigation against Amazon.com for invasion of privacy. Amazon.com, the large online retailer, is the target of a class action, in which the plaintiffs allege that they were not told about, and did not consent to, the collection of personal information about them when they used a software program owned by Amazon called "Alexa." In that case, plaintiffs have alleged violations of the Computer Fraud and Abuse Act in unlawful access to their stored communications and of the Electronic Communications Privacy Act for unlawful interception of their electronic and wire communications. They also claim an invasion of privacy under common law. This stems from a complaint filed by an Internet security expert in December. The suit seeks damages of USD 1000 per class member, plus attorneys' fees and profits earned as a result of violations of laws. Given that the number of class members could be in the millions,

damages could total billions of dollars. The FTC is also investigating the charges.

Federal and state privacy legislation often provides private causes of action for money damages.

In addition to giving rise to civil liability under tort law, non-compliance with the safe harbor principles could also violate one or another of the hundreds of federal and state privacy laws. Many of these laws, which address both government and private-sector handling of personal information, allow individuals to sue for damages when violations occur. For example:

Electronic Communications Privacy Act of 1986. The ECPA prohibits the unauthorized interception of cellular telephone calls and computer-to-computer transmissions. Violations can result in civil liability of not less than USD 100 for each day of violation. The protection of the ECPA also extends to unauthorized access or disclosure of stored electronic communications. Violators are liable for damages suffered or forfeiture of profits generated by a violation.

Telecommunications Act of 1996. Under section 702, customer proprietary network information (CPNI) may not be used for any purpose other than to provide telecommunications services. Service subscribers can either submit a complaint to the Federal Communications Commission or file suit in federal district court to recover damages and attorneys' fees.

Consumer Credit Reporting Reform Act of 1996. The 1996 Act amended the Fair Credit Reporting act of 1970 (FCRA) to require improved notice and right of access for credit reporting subjects. The Reform Act also imposed new restrictions on resellers of consumer credit reports. Consumers can recover damages and attorneys' fees for violations.

State laws also protect personal privacy in a broad range of situations. Areas where the states have taken action include bank records, cable television subscriptions, credit reports, employment records, government records, genetic information and medical records, insurance records, school records, electronic communications, and video rentals(12).

B. Explicit Legal Authorizations

The safe harbor principles contain an exception where statute, regulation or case-law create "conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the principles is limited to the extent necessary to meet the overriding legitimate interests further by such authorization." Clearly, where U.S. law imposes a conflicting obligation, U.S. organizations whether in the safe harbor or not must comply with the law. As for explicit authorizations, while the safe harbor principles are intended to bridge the differences between the U.S. and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected lawmakers. The limited exception from strict adherence to the safe harbor principles seeks to strike a balance to accommodate the legitimate interests on each side.

The exception is limited to cases where there is an explicit authorization. Therefore, as a threshold matter, the relevant statute, regulation or court decision must affirmatively authorize the particular conduct by safe harbor organizations(13). In other words, the exception would not apply where

the law is silent. In addition, the exception would apply only if the explicit authorization conflicts with adherence to the safe harbor principles. Even then, the exception "is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization." By way of illustration, where the law simply authorizes a company to provide personal information to government authorities, the exception would not apply. Conversely, where the law specifically authorizes the company to provide personal information to government agencies without the individual's consent, this would constitute an "explicit authorization" to act in a manner that conflicts with the safe harbor principles. Alternatively, specific exceptions from affirmative requirements to provide notice and consent would fall within the exception (since it would be the equivalent of a specific authorization to disclose the information without notice and consent). For example, a statute which authorizes doctors to provide their patients' medical records to health officials without the patients' prior consent might permit an exception from the notice and choice principles. This authorization would not permit a doctor to provide the same medical records to health maintenance organizations or commercial pharmaceutical research laboratories, which would be beyond the scope of the purposes authorized by the law and therefore beyond the scope of the exception(14). The legal authority in question can be a "stand alone" authorization to do specific things with personal information, but, as the examples below illustrate, it is likely to be an exception to a broader law which proscribes the collection, use, or disclosure of personal information.

Telecommunications Act of 1996

In most cases, the authorized uses are either consistent with the requirements of the Directive and the principles, or would be permitted by one of the other allowed exceptions. For example, section 702 of the Telecommunications Act (codified at 47 U.S.C. § 222) imposes a duty on telecommunications carriers to maintain the confidentiality of personal information that they obtain in the course of providing their services to their customers. This provision specifically allows telecommunications carriers to:

(1) use customer information to provide telecommunications service, including the publication of subscriber directories;

(2) provide customer information to others at the written request of the customer; and

(3) provide customer information in aggregate form.

See 47 U.S.C. § 222(c)(1)-(3). The Act also allows telecommunications carriers an exception to use customer information:

(1) to initiate, render, bill, and collect for their services;

(2) to protect against fraudulent, abusive or illegal conduct; and

(3) to provide telemarketing, referral or administrative services during a call initiated by the customer(15).

Id., § 222(d)(1)-(3). Finally, telecommunications carriers are required to provide subscriber list information, which can only include the names, addresses, telephone numbers and line of business for commercial customers to publishers of telephone directories. Id., § 222(e).

The exception for "explicit authorizations" might come into play when telecommunications carriers use CPNI to prevent fraud or other unlawful conduct. Even here, such actions could qualify as being in the "public interest" and allowed by the principles for that reason.

Department of Health and Human Services Proposed Rules

The Department of Health and Human Services (HHS) has proposed rules regarding standards for the privacy of individually identifiable health information. See 64 Fed. Reg. 59.918 (November 2, 1999) (to be codified at 45 C.F.R. pts. 160-164). The rules would implement the privacy requirements of the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191. The proposed rules generally would prohibit covered entities (i.e. health plans, health care clearinghouses, and health providers that transmit health information in electronic format) from using or disclosing protected health information without individual authorization. See proposed 45 C.F.R. § 164.506. The proposed rules would require disclosure of protected health information for only two purposes: 1. to permit individuals to inspect and copy health information about themselves, see id. at § 164.514; and 2. to enforce the rules, see id. at § 164.522.

The proposed rules would permit use or disclosure of protected health information, without specific authorization by the individual, in limited circumstances. These include for example oversight of the health care system, law enforcement, and emergencies. See id. at § 164.510. The proposed rules set out in detail the limits on these uses and disclosures. Moreover, permitted uses and disclosures of protected health information would be limited to the minimum amount of information necessary. See id. at § 164.506.

The permissive uses explicitly authorized by the proposed regulations are generally consistent with the safe harbor principles or are otherwise allowed by another exception. For example, law enforcement and judicial administration are permitted, as is medical research. Other uses, such as oversight of the health care system, public health function, and government health data systems, serve the public interest. Disclosures to process health care payments and premiums are necessary to the provision of health care. Uses in emergencies, to consult with next of kin regarding treatment where the patient's consent "cannot practicably or reasonably be obtained," or to determine the identity or cause of death of the deceased protect the vital interests of the data subject and others. Uses for the management of active duty military and other special classes of individuals aid the proper execution of the military mission or similar exigent situations; and in any event, such uses will have little if any application to consumers in general.

This leaves only the use of personal information by health care facilities to produce patient directories. While such use might not rise to the level of a "vital" interest, the directories do benefit patients and their friends and relations. Also, the scope of this authorized use is inherently limited. Therefore, reliance on the exception in the principles for uses "explicitly authorized" by law for this purpose presents minimal risk to the privacy of patients.

Fair Credit Reporting Act

The European Commission has expressed the concern that the "explicit authorizations" exception would "effectively create an adequacy finding" for the Fair Credit Reporting Act (FCRA). This would not be the case. In the absence of a specific adequacy finding for the FCRA, those U.S. organizations that would otherwise rely on such a finding, would have to promise to adhere to the safe harbor principles in all respects. This means that where FCRA requirements exceed the level of protection embodied in the principles, the U.S. organizations need only to obey the FCRA. Conversely, where the FCRA might fall short, then those organizations would need to bring their information practices into conformity with the principles. The exception would not alter this basic assessment. By its terms, the exception applies only where the relevant law explicitly authorizes conduct that would be inconsistent with the safe harbor principles. The exception would not extend to where FCRA requirements merely do not meet the safe harbor principles(16).

In other words, we do not intend the exception to mean that whatever is not required is therefore "explicitly authorized." Furthermore, the exception applies only when what is explicitly authorized by U.S. law conflicts with the requirements of the safe harbor principles. The relevant law must meet both of these elements before non-adherence with the principles would be permitted.

Section 604 of the FCRA, for example, explicitly authorizes consumer reporting agencies to issue consumer reports in various enumerated situations. See FCRA, § 604. If in so doing, section 604 authorizes credit reporting agencies to act in conflict with the safe harbor principles, then the credit reporting agencies would need to rely on the exception (unless, of course, some other exception applied). Credit reporting agencies must obey court orders and grand jury subpoenas, and use of credit reports by government licensing, social and child support enforcement agencies serves a public purpose. Id., § 604(a)(1), (3)(D), and (4). Consequently, the credit reporting agency would not need to rely on the "explicit authorization" exception for these purposes. Where it acts in accordance with written instructions by the consumer, the consumer reporting agency would be fully in compliance with the safe harbor principles. Id., § 604(a)(2). Likewise, consumer reports can be procured for employment purposes only with the consumer's written authorization. (id., §§ 604(a)(3)(B) and (b)(2)(A)(ii)) and for credit or insurance transactions that are not initiated by the consumer only if the consumer had not opted out from such solicitations (id., § 604(c)(1)(B)). Also, FCRA prohibits credit reporting agencies from providing medical information for employment purposes without the consent of the consumer. Id., § 604(g). Such uses comport with the notice and choice principles. Other purposes authorized by section 604 entail transactions involving the consumer and would be permitted by the principles for that reason. See id., § 604(a)(3)(A) and (F).

The remaining use "authorized" by section 604 relates to secondary credit markets. Id., § 604(a)(3)(E). There is no conflict between use of consumer reports for this purpose and the safe harbor principles per se. It is true that the FCRA does not require credit reporting agencies, for example, to give notice and consent to consumers when they issue reports for this purpose. However, we reiterate the point that the absence of a requirement does not connote an "explicit authorization" to act in a manner other than as required. Similarly, section 608 allows credit

reporting agencies to provide some personal information to government agencies. This "authorization" would not justify a credit reporting agency ignoring its commitments to adhere to the safe harbor principles. This contrasts with our other examples where exceptions from affirmative notice and choice requirements operate to explicitly authorize uses of personal information without notice and choice.

Conclusion

A distinct pattern emerges even from our limited review of these statutes:

- The "explicit authorization" in the law generally permits the use or disclosure of personal information without the individual's prior consent; thus, the exception would be limited to the notice and choice principles.

- In most cases, the exceptions authorized by the law are narrowly drawn to apply in specific situations for specific purposes. In all cases, the law otherwise prohibits the unauthorized use or disclosure of personal information that does not fall within these limits.

- In most cases, reflecting their legislative character, the authorized use or disclosure serves a public interest.

- In almost all cases, the authorized uses are either fully consistent with the safe harbor principles or fall into one of the other allowed exceptions.

In conclusion, the exception for "explicit authorizations" in the law will, by its nature, likely be rather limited in scope.

C. Mergers and Takeovers

The Article 29 Working Party expressed concern over situations where an organization within the safe harbor is taken over by, or merged with, a firm which has not made a commitment to follow the safe harbor principles. The Working Party, however, appears to have assumed that the surviving firm would not be bound to apply the safe harbor principles to personal information held by the firm that is taken over, but that is not necessarily the case under U.S. law. The general rule in the United States as to mergers and takeovers is that a company which acquires the outstanding stock of another corporation generally assumes the obligations and liabilities of the acquired firm. See 15 Fletcher Cyclopedia of the Law of Private Corporations § 7117 (1990); see also Model Bus. Corp. Act § 11.06(3) (1979) ("the surviving corporation has all liabilities of each corporation party to the merger"). In other words, the surviving firm in a merger or takeover of a safe harbor organization by this method would be bound by the latter's safe harbor commitments.

Moreover, even if the merger or takeover were effectuated through the acquisition of assets, the liabilities of the acquired enterprise could nevertheless bind the acquiring firm in certain circumstances. 15 Fletcher, § 7122. Even where liabilities did not survive the merger, however, it is worth noting that they also would not survive a merger where the data were transferred from Europe pursuant to a contract - the only viable alternative to the safe harbor for data transfers to the United States. In addition, the safe harbor documents as revised now require any safe harbor organization to notify the Department of Commerce of any takeover and permit data to continue to be transferred to the successor organization only if the successor organization joins the safe harbor. See FAQ 6.

Indeed, the United States has now revised the safe harbor framework to require U.S. organizations in this situation to delete information they have received under the safe harbor framework if their safe harbor commitments will not continue or other suitable safeguards are not put in place.

(1) Second Restatement of the Law - Torts; American Law Institute (1997).

(2) This might be the case, for example, where the individuals relied on the U.S. organization's safe harbor commitments in giving their consent to the data controller to transfer their personal information to the United States.

(3) Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).

(4) Id., at 69.

(5) An electronic search of the Westlaw database found 2703 reported cases of civil actions in state courts that pertained "privacy" since 1995. We have previously provided the results of this search to the Commission.

(6) See, e.g., Alaska Constitution, Art. 1 Sec. 22; Arizona, Art. 2, Sec. 8; California, Art. 1, Sec. 1; Florida, Art. 1, Sec. 23; Hawaii, Art. 1, Sec. 5; Illinois, Art. 1, Sec. 6; Louisiana, Art. 1, Sec. 5; Montana, Art. 2, Sec. 10; New York, Art. 1, Sec. 12; Pennsylvania, Art. 1, Sec. 1; South Carolina, Art. 1, Sec. 10; and Washington, Art. 1 Sec. 7.

(7) Id., at Chapter 28, Section 62B.

(8) Id., at Chapter 28, Section 652C.

(9) Id., at Chapter 28, Section 652D.

(10) Id., at Chapter 28, Section 652E.

(11) We had previously provided the Commission with information on small-claims actions.

(12) A recent electronic search of the Westlaw database yielded 994 reported states cases that related to damages and invasion of privacy.

(13) As a point of clarification, the relevant legal authority will not have to specifically reference the safe harbor principles.

(14) Similarly, the doctor in this example could not rely on the statutory authority to override the individual's exercise of the opt-out from direct marketing provided by FAQ 12. The scope of any exception for "explicit authorizations" is necessarily limited to the scope of the authorization under relevant law.

(15) The scope of this exception is very limited. By its terms, the telecommunciations carrier can use CPNI only during a call initiated by the customer. Furthermore, we have been advised by the FCC that the telecommunications carrier may not use CPNI to market services beyond the scope of the customer's inquiry. Finally, since the customer must approve the use of CPNI for this purpose, this provision is not really an "exception" at all.

(16) Our discussion here should not be taken as an admission that the FCRA does not provide "adequate" protection. Any assessment of the FCRA must

consider the protection provided by the statute in its entirety and not focus only on the exceptions as we do here.

ANNEX V

14 July 2000

John Mogg

Director, DG XV

European Commission Office C 107-6/72 Rue de la Loi/Wetstraat 200 B - 1049 Brussels

Dear Mr Mogg

I understand a number of questions have arisen with regard to my letter to you of March 29, 2000. To clarify our authority on those areas where questions have arisen, I am sending this letter, which, for future ease of reference, adds to and recapitulates the text of previous correspondence.

In your visits to our offices and in your correspondence, you have raised several questions about the United States Federal Trade Commission's authority in the online privacy area. I thought it would be useful to summarize my prior responses concerning the FTC's activities in this area and to provide additional information about the agency's jurisdiction over consumer privacy issues raised in your most recent letter. Specifically, you ask whether: (1) the FTC has jurisdiction over transfers of employment-related data if done in violation of the U.S. safe harbor principles; (2) the FTC has jurisdiction over non-profit privacy "seal" programs; (3) the FTC Act applies equally to the offline as well as online world; and (4) what happens when the FTC's jurisdiction overlaps with other law enforcement agencies.

FTC Act Application to Privacy

As you know, during the past five years, the FTC has taken a leadership role in facilitating efforts by United States industry and consumer groups to develop a comprehensive response to consumer privacy issues, including the collection and use of personal information on the Internet. Through public workshops and continuous consultation with industry members, consumer representatives and our colleagues at the Department of Commerce and throughout the U.S. Government, we have helped to identify key policy issues and develop sensible solutions.

The Federal Trade Commission's legal authority in this area is found in Section 5 of the Federal Trade Commission Act ("FTC Act"), which prohibits "unfair or deceptive acts or practices" in or affecting commerce(1). A deceptive practice is defined as a representation, omission or practice that is likely to mislead reasonable consumers in a material fashion. A practice is unfair if it causes, or is likely to cause, substantial injury to consumers which is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or competition(2).

Certain information collection practices are likely to violate the FTC Act. For example, if a website falsely claims to comply with a stated privacy policy or a set of self-regulatory guidelines, Section 5 of the FTC Act provides a legal basis for challenging such a misrepresentation as deceptive. Indeed, we have successfully enforced the law to establish this principle(3). In addition, the Commission has taken the position it may challenge

particularly egregious privacy practices as unfair under Section 5 if such practices involve children, or the use of highly sensitive information, such as financial records(4) and medical records. The Federal Trade Commission has and will continue to pursue such law enforcement actions through our active monitoring and investigative efforts, and through referrals we receive from self-regulatory organizations and others, including European Union Member States.

FTC Support for Self-Regulation

The FTC has long been supportive of efforts by the industry to develop effective self-regulatory programs to ensure privacy protection for consumers on the Internet. If these efforts are to succeed, however, there must be widespread participation by industry members. At the same time, self-regulation must be backed by law enforcement. For these reasons, the FTC will give priority to referrals of non-compliance with self-regulatory guidelines received from organizations such as BBBOnline and TRUSTe. This approach would be consistent with our longstanding relationship with the National Advertising Review Board (NARB) of the Better Business Bureau, which refers advertising complaints to the FTC. The National Advertising Division (NAD) of NARB resolves complaints, through an adjudicative process, concerning national advertising. When a party refuses to comply with an NAD decision, a referral is made to the FTC. FTC staff review the challenged advertising on a priority basis to determine if it violates the FTC Act, and often is successful in stopping the challenged conduct or convincing the party to return to the NARB process.

Similarly, the FTC will give priority to referrals of non-compliance with safe harbor principles from EU Member States. As with referrals from U.S. self-regulatory organizations, our staff will consider any information bearing upon whether the conduct complained of violates Section 5 of the FTC Act. This commitment can also be found in the safe harbor principles under the Frequently Asked Question (FAQ 11) on enforcement.

GeoCities: The FTC's First Online Privacy Case

The Federal Trade Commission's first Internet privacy case, GeoCities, was based on the Commission's authority under Section 5(5). In that case, the FTC alleged that GeoCities misrepresented, both to adults and children, how their personal information would be used. The Federal Trade Commission's complaint alleged that GeoCities represented that certain personal identifying information it collected on its website was to be used only for internal purposes or to provide consumers with the specific advertising offers and products or services they requested, and that certain additional "optional" information would not be released to anyone without the consumer's permission. In fact, this information was disclosed to third parties who used it to target members for solicitations beyond those agreed to by the member. The complaint also charged that GeoCities engaged in deceptive practices relating to its collection of information from children. According to the FTC's complaint, GeoCities represented that it operated a children's area on its website and that the information collected there was maintained by GeoCities. In fact, those areas on the website were run by third-parties who collected and maintained the information.

The settlement prohibits GeoCities from misrepresenting the purpose for which it collects or uses personal identifying information from or about consumers, including children. The order requires the company to post on its website a

clear and prominent Privacy Notice, telling consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information. To ensure parental control, the settlement also requires GeoCities to obtain parental consent before collecting personal identifying information from children 12 and under. Under the order, GeoCities is required to notify its members and provide them with an opportunity to have their information deleted from GeoCities' and any third parties' databases. The settlement specifically requires GeoCities to notify the parents of children 12 and under and to delete their information, unless a parent affirmatively consents to its retention and use. Finally, GeoCities also is required to contact third parties to whom it previously disclosed the information and request that those parties delete that information as well(6).

ReverseAuction.com

More recently, this agency brought a case challenging alleged privacy breaches by another online company. In January 2000, the Commission approved a complaint against, and consent agreement with, ReverseAuction.com, an online auction site that allegedly obtained consumers' personally identifying information from a competitor site (eBay.com) and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business(7). Our complaint alleged that ReverseAuction violated Section 5 of the FTC Act in obtaining the personally identifiable information, which included eBay users' e-mail addresses and personalized user identification names ("user IDs"), and in sending out the deceptive e-mail messages.

As described in the complaint, before obtaining the information, ReverseAuction registered as an eBay user and agreed to comply with eBay's User Agreement and Privacy Policy. The agreement and policy protect consumers' privacy by prohibiting eBay users from gathering and using personal identifying information for unauthorized purposes, such as sending unsolicited commercial e-mail messages. Thus, our complaint first alleged that ReverseAuction misrepresented that it would comply with eBay's User Agreement and Privacy Policy, a deceptive practice under Section 5. In the alternative, the complaint alleged that ReverseAuction's use of the information to send the unsolicited commercial e-mail, in violation of the User Agreement and Privacy Policy, was an unfair trade practice under Section 5.

Second, the complaint alleged that the e-mail messages to consumers contained a deceptive subject line informing each of them that his or her eBay user ID "will expire soon." Finally, the complaint alleged that the e-mail messages falsely represented that eBay directly or indirectly provided Reverse auction with eBay users' personally identifiable information, or otherwise participated in dissemination of the unsolicited e-mail.

The settlement obtained by the FTC bars ReverseAuction from committing these violations in the future. It also requires ReverseAuction to provide notice to consumers who, as a result of receiving ReverseAuction's e-mail, registered or will register with ReverseAuction. The notice informs these consumers that their eBay users IDs were not about to expire on eBay, and that eBay did not know of, or authorize, ReverseAuction's dissemination of the unsolicited e-mail. The notice also provides these consumers with the opportunity to cancel registration with ReverseAuction and have their personal identifying information deleted from

ReverseAuctions's database. In addition, the order requires Reverse auction to delete, and refrain from using or disclosing, the personal identifying information of eBay members who received ReverseAuction's e-mail but who have not registered with ReverseAuction. Finally, consistent with prior privacy orders obtained by this agency, the settlement requires Reverse auction to disclose its own privacy policy on its Internet site, and contains comprehensive record keeping provisions to allow the FTC to monitor compliance.

The ReverseAuction case demonstrates that the FTC is committed to using enforcement to buttress industry self-regulatory efforts in the area of online consumer privacy. Indeed, this case directly challenged conduct that undermined a Privacy Policy and User Agreement protecting consumers' privacy, and that could erode consumer confidence in privacy measures undertaken by online companies. Because this case involved the misappropriation by one company of consumer information protected by another company's privacy policy, it also may have particular relevance to the privacy concerns raised by the transfer of data between companies in different countries.

Notwithstanding the Federal Trade Commission's law enforcement actions in GeoCities, Liberty Financial Cos., and ReverseAuction, the agency's authority in some areas of online privacy is more limited. As noted above, to be reachable under the FTC Act, the collection and use of personal information without consent must constitute either a deceptive or unfair trade practice. Thus, the FTC Act likely would not address the practices of a website that collected personally identifiable information from consumers, but neither misrepresented the purpose for which the information was collected, nor used or released the information in a way that was likely to cause substantial injury to consumers. Also, it may not be within he FTC's power to broadly require that entities collecting information on the Internet adhere to a privacy policy or to any particular privacy policy(8). As stated above, however, a company's failure to abide by a stated privacy policy is likely to be a deceptive practice.

Furthermore, the FTC's jurisdiction in this area covers unfair or deceptive acts or practices only if they are "in or affecting commerce." Information collection by commercial entities that are promoting products or services, including collecting and using information for commercial purposes, would presumably meet the "commerce" requirement. On the other hand, many individuals or entities may be collecting information online without any commercial purpose, and thereby may fall outside the Federal Trade Commission's jurisdiction. An example of this limitation involves "chat rooms" if operated by non-commercial entities, e.g., a charitable organization.

Finally, there are a number of full or partial statutory exclusions from the FTC's basic jurisdiction over commercial practices that limit the FTC's ability to provide a comprehensive response to Internet privacy concerns. These include exemptions for many information intensive consumer businesses such as banks, insurance companies and airlines. As you are aware, other federal or state agencies would have jurisdiction over those entities, such as the federal banking agencies or the Department of Transportation.

In cases where it does have jurisdiction, the FTC accepts and, resources permitting, acts on consumer complaints received by mail and telephone in

its Consumer Response Center ("CRC"), and, more recently, on its website(9). The CRC accepts complaints from all consumers, including those residing in European Union Member States. The FTC Act provides the Federal Trade Commission equitable power to obtain injunctive relief against future violations of the FTC Act, as well as redress for injured consumers. We would, however, look to see whether the company has engaged in a pattern of improper conduct, as we do not resolve individual consumer disputes. In the past, the Federal Trade Commission has provided redress for citizens of both the United States and other countries(10). The FTC will continue to assert its authority, in appropriate cases, to provide redress to citizens of other countries who have been injured by deceptive practices under its jurisdiction.

Employment Data

Your most recent letter sought additional clarification concerning the FTC's jurisdiction in the area of employment data. First, you pose the question whether the FTC could take action under Section 5 against a company that represents it complies with U.S. safe harbor principles but transfers or uses employment-related data in a manner that violates these principles. We want to assure you that we have carefully reviewed the FTC authorizing legislation, related documents, and relevant case-law and have concluded that the FTC has the same jurisdiction in the employment-related data situation as it would generally under Section 5 of the FTC Act(11). That is to say, assuming a case met our existing criteria (unfairness or deception) for a privacy-related enforcement action, we could take action in the employment-related data situation.

We also would like to dispel any view that the FTC's ability to take privacy-related enforcement action is limited to situations where a company has deceived individual consumers. In fact, as the Commission's recent action in the ReverseAuction(12) matter makes clear, the FTC will bring privacy-related enforcement actions in situations involving data transfers between companies, where one company allegedly has acted unlawfully vis à vis another company, leading to possible injury to both consumers and companies. We expect this situation is the one in which the employment issue is most likely to arise, as employment data about Europeans is transferred from European companies to American companies that have pledged to abide by the safe harbor principles.

We do wish to note one circumstance in which FTC action would be circumscribed, however. This would occur in situations in which the matter is already being addressed in a traditional labor law dispute resolution context, most likely a grievance/arbitration claim or an unfair labor practice complaint at the National Labor Relations Board. This would occur, for example, if an employer had made a commitment in a collective bargaining agreement regarding the use of personal data and an employee or union claimed that the employer had breached that agreement. The Commission would likely defer to that proceeding(13).

Jurisdiction Over "Seal" Programs

Second, you ask whether the FTC would have jurisdiction over "seal" programs administering dispute resolution mechanisms in the United States that misrepresented their role in enforcing the "safe harbor" principles and handling individual complaints, even if such entities were technically "not for profit." In determining whether we have jurisdiction over an entity that

holds itself out as a non-profit, the Commission closely analyzes whether the entity, while not seeking a profit for itself, furthers the profit of its members. The Commission has successfully asserted jurisdiction over such entities and as recently as May 24, 1999, the United States Supreme Court, in California Dental Association v. Federal Trade Commission, unanimously affirmed the Commission's jurisdiction over a voluntary non-profit association of local dental societies in an antitrust matter. The Court held:

The FTC Act is at pains to include not only an entity "organized to carry on business for its own profit," 15 U.S.C. § 44, but also one that carries on business for the profit "of its members." ... It could, indeed, hardly be supposed that Congress intended such a restricted notion of covered supporting organizations, with the opportunity this would bring with it for avoiding jurisdiction where the purposes of the FTC Act would obviously call for asserting it.

In sum, determining whether to assert jurisdiction over a particular "non-profit" entity administering a seal program would require a factual review of the extent to which the entity provided economic benefit to its for-profit members. If such an entity operated its seal program in a manner that provided an economic benefit to its members, the FTC likely would assert its jurisdiction. As a separate point, the FTC likely would have jurisdiction over a fraudulent seal program that misrepresents its status as a non-profit entity.

Privacy on the Offline World

Third, you note that our prior correspondence has focused on privacy in the online world. While online privacy has been a major concern of the FTC as a critical component to the development of electronic commerce, the FTC Act dates back to 1914 and applies equally in the offline world. Thus, we can pursue offline firms that engage in unfair or deceptive trade practices with regard to consumers' privacy(14). In fact, in a case brought by the Commission last year, FTC v. TouchTone Information, Inc.(15), an "information broker" was charged with illegally obtaining and selling consumers' private financial information. The Commission alleged that Touch Tone obtained consumers' information by "pretexting," a term of art coined by the private investigation industry to describe the practice of getting personal information about others under false pretenses, typically on the telephone. The case, filed April 21, 1999, in federal court in Colorado, seeks an injunction and all illegally gained profits.

Overlapping Jurisdiction

Finally, you pose the question of the interplay of the FTC's jurisdiction with that of other law enforcement agencies, particularly in cases where there is potentially overlapping jurisdiction. We have developed strong working relationships with numerous other law enforcement agencies, including the federal banking agencies and the state attorneys general. We very often coordinate investigations to maximize our resources in instances of overlapping jurisdiction. We also often refer matters to the appropriate federal or state agency for investigation.

I hope this review is helpful. Please let me know if you need any further information.

Sincerely,

Robert Pitofsky

(1) 15 U.S.C. § 45. The Fair Credit Reporting Act would also apply to Internet data collection and sales that meet the statutory definitions of "consumer report" and "consumer reporting agency."

(2) 15 U.S.C. § 45(n).

(3) See GeoCities, Docket No C-3849 (Final Order Feb. 12, 1999) (available at www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos., Docket No C-3891 (Final Order Aug. 12, 1999) (available at www.ftc.gov/opa/1999/9905/younginvestor.htm). See also Children's Online Privacy Protection Act Rule (COPPA), 16 C.F.R. Part 312 (available at www.ftc.gov/opa/1999/9910/childfinal.htm). The COPPA Rule, which became effective last month, requires operators of websites directed to children under 13, or who knowingly collect personal information from children under 13, to implement the fair information practice standards enunciated in the Rule.

(4) See FTC v. Touch Tone, Inc., Civil Action No 99-WM-783 (D.Co.) (filed April 21, 1999) at www.ftc.gov/opa/1999/9904/touchtone.htm. Staff Opinion Letter, July 17, 1997, issued in response to a petition filed by the Center for Media Education, at www.ftc.gov/os/1997/9707/cenmed.htm.

(5) GeoCities, Docket No C-3849 (Final Order Feb. 12, 1999) (available at www.ftc.gov/os/1999/9902/9823015d%26o.htm).

(6) The Commission subsequently settled another matter involving the collection of personal information from children online. Liberty Financial Companies, Inc., operated the Young Investor website which was directed to children and teens, and focused on issues relating to money and investing. The Commission alleged that the site falsely represented that personal information collected from children in a survey would be maintained anonymously, and that participants would be sent an e-mail newsletter as well as prizes. In fact, the personal information about the child and the family's finances was maintained in an identifiable manner, and no newsletter or prizes were sent. The consent agreement prohibits such misrepresentations in the future and requires Liberty Financial to post a privacy notice on its children's sites and obtain verifiable parental consent before collecting personal identifying information from children. Liberty Financial Cos., Docket No C-3891 (Final Order Aug. 12, 1999) (available at www.ftc.gov/opa/1999/9905/younginvestor.htm).

(7) See ReverseAuction.com, Inc., Civil Action No 000032 (D.D.C.) (filed January 6, 2000) (press release and pleadings at www.ftc.gov/opa/2000/01/reverse4.htm).

(8) For this reason, the Federal Trade Commission stated in Congressional testimony that additional legislation probably would be required to mandate that all U.S. commercial websites directed toward consumers abide by specified fair information practices. "Consumer Privacy on the World Wide Web," Before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce United States House of Representatives, July 21, 1998 (the testimony can be found at www.ftc.gov/os/9807/privac98.htm). The FTC deferred calling for such legislation in order to give self-regulatory efforts the opportunity to demonstrate widespread adoption of fair information practices on

websites. In the Federal Trade Commission's report to Congress on online privacy, "Privacy Online: A Report to Congress," June 1998 (the report can be found at www.ftc.gov/reports/privacy3/toc.htm), the FTC recommended legislation to require that commercial websites obtain parental consent before collecting personally identifiable information from children under 13 years old. See footnote 3 supra. Last year, the Commission's report, "Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress," July 1999 (the report can be found at www.ftc.gov/os/1999/9907/index.htm

13,) found sufficient progress in self-regulation and, accordingly, chose not to recommend legislation at that time. The Commission will report again to Congress in the coming weeks on the progress of self-regulation.

(9) See http://www.ftc.gov/ftc/complaint.htm for the Federal Trade Commission's online complaint form.

(10) For example, in a recent case involving an Internet pyramid scheme, the Commission obtained refunds for 15622 consumers totaling approximately USD 5,5 million. The consumers resided in the United States and 70 foreign countries. See www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm.

(11) Except as specifically excluded by the FTC's authorizing statute, the FTC's jurisdiction under the FTC Act over practices "in or affecting commerce" is coextensive with the constitutional power of Congress under the Commerce Clause, United States v. American Building Maintenance Industries, 422 U.S. 271, 277 n. 6 (1975). The FTC's jurisdiction would thus encompass employment-related practices in firms and industries in international commerce.

(12) See "Online Auction Site Settles FTC Privacy Charges", FTC News Release (January 6, 2000) available at http://www.ftc.gov/opa/2000/01/reverse4.htm.

(13) The determination whether conduct is an "unfair labor practice" or a violation of a collective bargaining agreement is a technical one that is ordinarily reserved to the expert labor tribunals who will hear the complaints, such as arbitrators and the NRLB.

(14) As you know from earlier discussions, the Fair Credit Reporting Act also gives the FTC the authority to protect consumers' financial privacy within the purview of the Act and the Commission recently issued a decision pertaining to this issue. See In the Matter of Trans Union, Docket No 9255 (March 1, 2000) (press release and opinion available at www.ftc.gov/os/2000/03/index.htm

1).

(15) Civil Action 99-WM-783 (D.Colo.) (available at http://www.ftc.gov/opa/1999/9904/touchtone.htm) (tentative consent decree pending).

ANNEX VI

John Mogg

Director, DG XV

European Commission Office C 107-6/72 Rue de la Loi/Wetstraat 200 B - 1049 Brussels

Dear Director-General Mogg:

I am providing you this letter at the request of the U.S. Department of Commerce to explain the role of the Department of Transportation in protecting the privacy of consumers with respect to information provided by them to airlines.

The Department of Transportation encourages self-regulation as the least intrusive and most efficient means of ensuring the privacy of information provided by consumers to airlines and accordingly supports the establishment of a "safe harbor" regime that would enable airlines to comply with the requirements of the European Union's privacy directive as regards transfers outside the EU. The Department recognizes, however, that for self-regulatory efforts to work, it is essential that the airlines that commit to the privacy principles set forth in the "safe harbor" regime in fact abide by them. In this regard, self-regulation should be backed by law enforcement. Therefore, using its existing consumer protection statutory authority, the Department will ensure airline compliance with privacy commitments made to the public, and pursue referrals of alleged non-compliance that we receive from self-regulatory organizations and others, including European Union Member States.

The Department's authority to take enforcement action in this area is found in 49 U.S.C. 41712 which prohibits a carrier from engaging in "an unfair or deceptive practice or an unfair method of competition" in the sale of air transportation that results or is likely to result in consumer harm. Section 41712 is patterned after Section 5 of the Federal Trade Commission Act (15 U.S.C. 45). However, air carriers are exempt from Section 5 regulation by the Federal Trade Commission under 15 U.S.C. 45(a)(2).

My office investigates and prosecutes cases under 49 U.S.C. 41712. (See, e.g., DOT Orders 99-11-5, November 9, 1999; 99-8-23, August 26, 1999; 99-6-1, June 1, 1999; 98-6-24, June 22, 1998; 98-6-21, June 19, 1998; 98-5-31, May 22, 1998; and 97-12-23, December 18, 1997.) We institute such cases based on our own investigations, as well as on formal and informal complaints we receive from individuals, travel agents, airlines, and U.S. and foreign government agencies.

I would point out that the failure by a carrier to maintain the privacy of information obtained from passengers would not be a per se violation of section 41712. However, once a carrier formally and publicly commits to the "safe harbor" principle of providing privacy to the consumer information it obtains, then the Department would be empowered to use the statutory powers of section 41712 to ensure compliance with those principles. Therefore, once a passenger provides information to a carrier that has committed to honoring the "safe harbor" principles, any failure to do so would likely cause consumer harm and be a violation of section 41712. My office would give the investigation of any such alleged activity and the prosecution of any case evidencing such activity a high priority. We will also advise the Department of Commerce of the outcome of any such case.

Violations of section 41712 can result in the issuance of cease and desist orders and the imposition of civil penalties for violations of those orders. Although

we do not have the authority to award damages or provide pecuniary relief to individual complainants, we do have the authority to approve settlements resulting from investigations and cases brought by the Department that provide items of value to consumers either in mitigation or as an offset to monetary penalties otherwise payable. We have done so in the past, and we can and will do so in the context of the safe harbor principles when circumstances warrant. Repeated violations of section 41712 by any U.S. airline would also raise questions regarding the airline's compliance disposition which could, in egregious situations, result in an airline being found to be no longer fit to operate and, therefore, losing its economic operating authority. (See, DOT Orders 93-6-34, June 23, 1993, and 93-6-11, June 9, 1993. Although this proceeding did not involve section 41712, it did result in the revocation of the operating authority of a carrier for a complete disregard for the provisions of the Federal Aviation Act, a bilateral agreement, and the Department's rules and regulations.)

I hope that this information proves helpful. If you have any questions or need further information, please feel free to contact me.

Sincerely,

Samuel Podberesky

Assistant General Counsel for Aviation Enforcement and Proceeding

ANNEX VII

With reference to Article 1(2)(b), the government bodies in the United States empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles implemented in accordance with the FAQs are:

1. The Federal Trade Commission, and

2. The US Department of Transportation.

The Federal Trade Commission acts on the basis of its authority under Section 5 of the Federal Trade Commission Act. The jurisdiction of the Federal Trade Commission under Section 5 is excluded with respect to banks, saving and loans and credit unions; telecommunications and interstate transportation common carriers, air carriers and packers and stockyard operators. Although the insurance industry is not specifically included in the list of exceptions in Section 5, the McCarran-Ferguson Act(1) leaves the regulation of the business of insurance to the individual states. However, the provisions of the FTC Act apply to the insurance industry to the extent that such business is not regulated by State law. The FTC retains residual authority over unfair or deceptive practices by insurance companies when they are not engaged in the business of insurance.

The US Department of Transportation acts on the basis of its authority under Title 49 United States Code Section 41712. The US Department of Transportation institutes cases based on its own investigations as well as formal and informal complaints received from individuals, travel agents, airlines, US and foreign government agencies.

(1) 15 U.S.C. § 1011 et seq.

ภาคผนวก ค
ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

ร่างฯ ที่ สคก. ตรวจพิจารณาแล้ว
เรื่องเสร็จที่ ๑๑๓๕/๒๕๕๘

บันทึกหลักการและเหตุผล
ประกอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ....

หลักการ

ให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

เหตุผล

เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว สามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้

ร่าง
พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ....

.....
.....
.....

.....
.....

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

.....
.....

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยแปดสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(๑) บทบัญญัติเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล และบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

(๒) บทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ในกรณีดังต่อไปนี้

(ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

(ข) ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล แต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มี

อำนาจตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคล ผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้ แล้วแต่กรณี

มาตรา ๔ พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(๑) บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนของบุคคลนั้นเท่านั้น โดยมิให้ผู้อื่นใช้ข้อมูลส่วนบุคคลนั้น หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อผู้อื่น

(๒) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(๓) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามอำนาจหน้าที่ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

(๔) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(๕) การดำเนินกิจการทางศาสนาขององค์การทางศาสนา

(๖) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา

มาตรา ๕ ในพระราชบัญญัตินี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“เจ้าของข้อมูลส่วนบุคคล” ให้หมายความรวมถึง

(๑) ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

(๒) ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือ

(๓) ผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

“บุคคล” หมายความว่า บุคคลธรรมดา

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

"เลขาธิการ" หมายความว่า เลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๖ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้ว ให้ใช้บังคับได้

หมวด ๑
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา ๗ ให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

(๑) ประธานกรรมการ ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

(๒) กรรมการโดยตำแหน่ง จำนวนเจ็ดคน ได้แก่ ปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ผู้แทนสภาหอการค้าแห่งประเทศไทย และผู้แทนสมาคมธนาคารไทย

(๓) กรรมการผู้ทรงคุณวุฒิ จำนวนห้าคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งเจ้าหน้าที่ของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

หลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อแต่งตั้งเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ รวมทั้งการสรรหากรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระตามมาตรา ๑๐ ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด

มาตรา ๘ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) มีสัญชาติไทย

(๒) ไม่เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(๓) ไม่เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๔) ไม่เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

มาตรา ๙ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิมีวาระการดำรงตำแหน่งคราวละสามปี

เมื่อครบกำหนดตามวาระในวรรคหนึ่ง หากยังมิได้มีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่

ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้

มาตรา ๑๐ นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา ๙ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ลาออก

(๓) คณะรัฐมนตรีให้ออก เพราะบกพร่องต่อหน้าที่ มีความประพฤติเสื่อมเสีย หรือหย่อนความสามารถ

(๔) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา ๘

ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระ ให้ผู้ที่ได้รับแต่งตั้งแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งตนแทน เว้นแต่วาระที่เหลืออยู่ไม่ถึงเก้าสิบวันจะไม่แต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนก็ได้

ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระ ให้คณะกรรมการประกอบด้วยกรรมการทั้งหมดเท่าที่มีอยู่จนกว่าจะมีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิตามวรรคสอง และในกรณีที่ประธานกรรมการพ้นจากตำแหน่งก่อนวาระ ให้กรรมการที่เหลือเลือกกรรมการคนหนึ่งทำหน้าที่ประธานกรรมการเป็นการชั่วคราว

มาตรา ๑๑ การประชุมคณะกรรมการ ต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมด จึงจะเป็นองค์ประชุม

ให้ประธานกรรมการเป็นประธานในที่ประชุม ในกรณีที่ประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้กรรมการซึ่งมาประชุมเลือกกรรมการคนหนึ่งเป็นประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

การประชุมของคณะกรรมการอาจกระทำได้โดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นได้ตามที่คณะกรรมการกำหนด

มาตรา ๑๒ กรรมการผู้ใดมีส่วนได้เสียไม่ว่าโดยตรงหรือโดยอ้อมในเรื่องที่ที่ประชุมพิจารณา ให้แจ้งการมีส่วนได้เสียของตนให้คณะกรรมการทราบล่วงหน้าก่อนการประชุม และห้ามมิให้ผู้นั้นเข้าร่วมประชุมพิจารณาในเรื่องดังกล่าว

มาตรา ๑๓ คณะกรรมการมีอำนาจหน้าที่ ดังต่อไปนี้

(๑) จัดทำแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคล ที่สอดคล้องกับนโยบายและแผนระดับชาติที่เกี่ยวข้อง รวมทั้งเสนอแผนยุทธศาสตร์และมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติการตามนโยบายและแผนระดับชาติดังกล่าว

(๒) ส่งเสริมและสนับสนุนหน่วยงานของรัฐและภาคเอกชน ดำเนินกิจกรรมตามแผนยุทธศาสตร์ตาม (๑) รวมทั้งจัดให้มีการประเมินผลการดำเนินงานตามแผนยุทธศาสตร์ดังกล่าว เพื่อเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

(๓) กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

(๔) ออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัตินี้

(๕) ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ

(๖) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(๗) เสนอแนะต่อคณะรัฐมนตรีหรือรัฐมนตรีในการตราพระราชกฤษฎีกาหรือออกกฎกระทรวงตามพระราชบัญญัตินี้

(๘) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใด ๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐและภาคเอกชนในการปฏิบัติตามพระราชบัญญัตินี้

(๙) ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน

(๑๐) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(๑๑) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการ

มาตรา ๑๔ ให้กรรมการได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

อนุกรรมการและกรรมการผู้เชี่ยวชาญที่คณะกรรมการแต่งตั้ง ให้ได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะกรรมการกำหนด

มาตรา ๑๕ คณะกรรมการมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติการอย่างใดอย่างหนึ่งตามที่คณะกรรมการมอบหมายได้

การประชุมคณะอนุกรรมการ ให้นำความในมาตรา ๑๑ มาใช้บังคับโดยอนุโลม

มาตรา ๑๖ ให้สำนักงานมีหน้าที่ปฏิบัติงานวิชาการและงานธุรการให้แก่คณะกรรมการ คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการ รวมทั้งให้มีอำนาจหน้าที่ ดังต่อไปนี้

(๑) ประสานงานกับส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(๒) ให้คำปรึกษาแก่หน่วยงานของรัฐและภาคเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

(๓) กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง หรือประชาชนทั่วไป

(๔) ติดตามและประเมินผลการปฏิบัติตามพระราชบัญญัตินี้

(๕) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของสำนักงาน

หมวด ๒
การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ ๑
บททั่วไป

มาตรา ๑๗ ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

มาตรา ๑๘ ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่

(๑) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว

(๒) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

ส่วนที่ ๒
การเก็บรวบรวมข้อมูลส่วนบุคคล

มาตรา ๑๙ การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา ๒๐ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้

(๑) วัตถุประสงค์ของการเก็บรวบรวม

(๒) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม

(๓) ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(๔) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ

(๕) สิทธิของเจ้าของข้อมูลตามมาตรา ๒๖ มาตรา ๒๗ และมาตรา ๒๘

กรณีมีเหตุที่ไม่อาจแจ้งรายละเอียดตามวรรคหนึ่งให้แก่เจ้าของข้อมูลส่วนบุคคลตามกำหนดเวลาในวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดตามวรรคหนึ่งแก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า

มาตรา ๒๑ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ

(๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(๓) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยายของเจ้าของข้อมูลส่วนบุคคล

(๔) เป็นการปฏิบัติตามกฎหมาย

(๕) กรณีอื่นตามที่กำหนดในกฎกระทรวง

มาตรา ๒๒ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(๑) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ชักช้า

(๒) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากการใช้และเปิดเผยที่ได้รับการยกเว้นตามมาตรา ๒๔

(๓) เป็นข้อมูลที่เปิดเผยต่อสาธารณะ

มาตรา ๒๓ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นใดซึ่งกระทบความรู้สึกของประชาชนตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) ได้รับยกเว้นตามมาตรา ๒๑ (๒) หรือ (๔)

(๒) กรณีอื่นตามที่กำหนดในกฎกระทรวง

ส่วนที่ ๓
การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

มาตรา ๒๔ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๑ หรือมาตรา ๒๓ หรือเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ตามมาตรา ๒๒ (๓) แล้วแต่กรณี

บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้และเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้และการเปิดเผยนั้นไว้ในรายการตามมาตรา ๓๐

มาตรา ๒๕ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา ๑๓ (๕) เว้นแต่

(๑) เป็นการปฏิบัติตามกฎหมาย

(๒) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๓) เป็นการปฏิบัติตามสัญญาที่ทำระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) เป็นการกระทำเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่สามารถให้ความยินยอมในขณะนั้นได้

(๕) เป็นการโอนไปยังผู้ซึ่งได้รับเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๓๒ หรือมาตรา ๓๔

(๖) กรณีอื่นตามที่กำหนดในกฎกระทรวง

หมวด ๓
สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรา ๒๖ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอตามวรรคหนึ่ง จะปฏิเสธคำขอได้เฉพาะในกรณีดังต่อไปนี้

(๑) เป็นการขัดหรือแย้งกับบทบัญญัติแห่งกฎหมาย หรือปฏิบัติตามคำสั่งศาล

(๒) มีผลต่อการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย

(๓) การเปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลนั้นอาจจะเป็นอันตรายต่อสิทธิและเสรีภาพของบุคคลอื่น

(๔) กรณีอื่นตามที่กำหนดในกฎกระทรวง

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอตามวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา ๓๐

เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม่อาจปฏิเสธคำขอได้ตามวรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอภายในสามสิบวันนับแต่วันที่ได้รับคำขอ ทั้งนี้ คณะกรรมการจะประกาศกำหนดระยะเวลาในการดำเนินการตามคำขอให้เร็วขึ้นหรือขยายระยะเวลาดังกล่าวหรือกำหนดหลักเกณฑ์อื่นตามความเหมาะสมก็ได้

มาตรา ๒๗ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้

มาตรา ๒๘ ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามวรรคหนึ่ง หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลและเหตุผลที่ไม่ดำเนินการตามวรรคหนึ่งไว้ในรายการตามมาตรา ๓๐

มาตรา ๒๙ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(๒) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(๓) ทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการพิสูจน์หรือการตรวจสอบ ทั้งนี้ ให้นำความในมาตรา ๒๗ วรรคสาม มาใช้บังคับกับการทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(๔) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนด ให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

มาตรา ๓๐ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกทำรายการดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้และการเปิดเผยตามมาตรา ๒๔ วรรคสาม

(๗) การปฏิเสธคำขอตามมาตรา ๒๖ วรรคสาม และมาตรา ๒๘ วรรคสอง

หมวด ๔
ข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

มาตรา ๓๑ ให้คณะกรรมการประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติ

มาตรา ๓๒ ให้มีเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับใบรับรองจากสำนักงานมีสิทธิใช้หรือแสดงเครื่องหมายดังกล่าว

ผู้ควบคุมข้อมูลส่วนบุคคลที่ประสงค์จะมีสิทธิใช้หรือแสดงเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ให้ยื่นคำขอรับใบรับรองต่อสำนักงานตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

ในการพิจารณาคำขอตามวรรคสอง ให้สำนักงานประเมินผลการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลเป็นไปตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการประกาศกำหนดตามมาตรา ๓๑ ให้สำนักงานออกใบรับรองแก่ผู้ควบคุมข้อมูลส่วนบุคคลนั้น

ลักษณะและรายละเอียดของเครื่องหมายรับรองมาตรฐาน การใช้หรือการแสดงเครื่องหมาย วิธีการประเมินผล การตรวจติดตามผล อัตราค่าธรรมเนียมการประเมินผลหรือการตรวจติดตามผล และการเพิกถอนใบรับรองให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

ในกรณีที่สำนักงานเพิกถอนใบรับรองของผู้ควบคุมข้อมูลส่วนบุคคลใด ให้ผู้ควบคุมข้อมูลส่วนบุคคลนั้นคืนใบรับรองให้แก่สำนักงานภายในสิบห้าวันนับแต่วันที่ได้รับแจ้งการเพิกถอน

คณะกรรมการจะประกาศกำหนดให้หน่วยงานอื่นของรัฐหรือหน่วยงานของเอกชนทั้งในประเทศหรือต่างประเทศเป็นผู้ประเมินผลและตรวจติดตามผลการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อขอรับใบรับรองจากสำนักงานตามวรรคสามด้วยก็ได้

ห้ามมิให้ผู้ใดใช้หรือแสดงเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเว้นแต่เป็นผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับใบรับรองจากสำนักงาน

มาตรา ๓๓ มาตรฐานของผู้ประเมินผลและตรวจติดตามผล การตรวจสอบมาตรฐานและอัตราค่าธรรมเนียมการตรวจสอบมาตรฐานสำหรับหน่วยงานของเอกชน รวมทั้งการเพิกถอนรายชื่อจากประกาศตามมาตรา ๓๒ วรรคหก ให้เป็นไปตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

มาตรา ๓๔ คณะกรรมการจะประกาศยอมรับเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานต่างประเทศหรือองค์การระหว่างประเทศก็ได้ หากปรากฏว่า การคุ้มครองข้อมูลส่วนบุคคลดังกล่าวมีข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามที่คณะกรรมการประกาศกำหนดตามมาตรา ๓๑

หมวด ๕
การร้องเรียน

มาตรา ๓๕ ให้คณะกรรมการแต่งตั้งคณะกรรมการผู้เชี่ยวชาญขึ้นคณะหนึ่งหรือหลายคณะก็ได้ตามความเชี่ยวชาญในแต่ละเรื่องหรือตามที่คณะกรรมการเห็นสมควร

คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่ง การพ้นจากตำแหน่ง และการดำเนินงานอื่นของคณะกรรมการผู้เชี่ยวชาญให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

มาตรา ๓๖ คณะกรรมการผู้เชี่ยวชาญมีอำนาจหน้าที่ ดังต่อไปนี้

(๑) พิจารณาเรื่องร้องเรียนตามพระราชบัญญัตินี้

(๒) ตรวจสอบการกระทำใด ๆ ของผู้ควบคุมข้อมูลส่วนบุคคลหรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล

(๓) ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล

(๔) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้กำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการผู้เชี่ยวชาญ

มาตรา ๓๗ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้

การยื่น การไม่รับเรื่อง การยุติเรื่อง และวิธีพิจารณาคำร้องเรียน ให้เป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนด

มาตรา ๓๘ ในกรณีที่ผู้ร้องเรียนตามมาตรา ๓๗ ไม่ได้ปฏิบัติให้ถูกต้องตามระเบียบที่กำหนดไว้ในมาตรา ๓๗ วรรคสอง หรือเป็นเรื่องร้องเรียนที่ระเบียบนั้นได้กำหนดไม่ให้รับไว้พิจารณา ให้คณะกรรมการผู้เชี่ยวชาญไม่รับเรื่องร้องเรียนไว้พิจารณา

เมื่อคณะกรรมการผู้เชี่ยวชาญพิจารณาเรื่องร้องเรียนตามมาตรา ๓๖ (๑) หรือตรวจสอบการกระทำใด ๆ ตามมาตรา ๓๖ (๒) แล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นไม่มีมูล ให้คณะกรรมการผู้เชี่ยวชาญมีคำสั่งยุติเรื่อง

ในกรณีที่คณะกรรมการผู้เชี่ยวชาญพิจารณาหรือตรวจสอบตามวรรคสองแล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่มิได้เป็นความผิดอาญาซึ่งดำเนินการไกล่เกลี่ยได้ และคู่กรณีประสงค์จะให้ไกล่เกลี่ย ให้คณะกรรมการผู้เชี่ยวชาญดำเนินการไกล่เกลี่ย แต่หากเรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่ไม่อาจไกล่เกลี่ยได้ หรือเป็นกรณีที่ไกล่เกลี่ยไม่สำเร็จ ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจออกคำสั่ง ดังต่อไปนี้

(๑) สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติหรือดำเนินการแก้ไขการกระทำของตนให้ถูกต้องภายในระยะเวลาที่กำหนด

(๒) สั่งห้ามผู้ควบคุมข้อมูลส่วนบุคคลกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือให้กระทำการใดเพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ยอมดำเนินการตามคำสั่งตามวรรคสาม (๑) หรือ (๒) ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม ทั้งนี้ ในกรณีที่ต้องมีการยึด อายัด หรือขายทอดตลาดทรัพย์สินของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อบังคับตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง ให้คณะกรรมการผู้เชี่ยวชาญเป็นผู้มีอำนาจสั่งยึด อายัด หรือขายทอดตลาดทรัพย์สินเพื่อการนั้น

การจัดทำคำสั่งตามวรรคหนึ่ง วรรคสอง หรือวรรคสาม (๑) หรือ (๒) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

คำสั่งของคณะกรรมการผู้เชี่ยวชาญ ให้ประธานกรรมการผู้เชี่ยวชาญเป็นผู้ลงนามแทน

มาตรา ๓๙ คำสั่งไม่รับเรื่องร้องเรียนไว้พิจารณาตามมาตรา ๓๘ วรรคหนึ่ง หรือยุติเรื่องตามมาตรา ๓๘ วรรคสอง หรือคำสั่งตามมาตรา ๓๘ วรรคสาม (๑) หรือ (๒) ให้เป็นที่สุด

มาตรา ๔๐ ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งให้บุคคลหนึ่งบุคคลใดส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน หรือเรื่องอื่นใดที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ รวมทั้งจะเรียกให้บุคคลใดมาชี้แจงข้อเท็จจริงด้วยก็ได้

มาตรา ๔๑ ในการปฏิบัติการตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจหน้าที่ ดังต่อไปนี้

(๑) มีหนังสือแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดมาให้ข้อมูลหรือส่งเอกสารหรือหลักฐานใด ๆ เกี่ยวกับการดำเนินการหรือการกระทำความผิดตามพระราชบัญญัตินี้

(๒) ตรวจสอบและรวบรวมข้อเท็จจริง แล้วรายงานต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดได้กระทำผิดหรือทำให้เกิดความเสียหายเพราะฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้

ในการดำเนินการตาม (๒) หากมีความจำเป็นเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือเพื่อประโยชน์สาธารณะ ให้พนักงานเจ้าหน้าที่มีอำนาจเข้าไปในสถานที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดเกี่ยวกับการกระทำความผิดตามพระราชบัญญัตินี้ ในระหว่างเวลาพระอาทิตย์ขึ้นจนถึงพระอาทิตย์ตกหรือในเวลาทำการของสถานที่นั้น เพื่อตรวจสอบและรวบรวมข้อเท็จจริง และยึดหรืออายัดเอกสารและหลักฐาน รวมถึงสิ่งอื่นใดที่เกี่ยวกับการกระทำความผิดหรือสงสัยว่ามีไว้หรือใช้เพื่อกระทำความผิด

ในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ตามมาตรานี้ ให้ผู้ที่เกี่ยวข้องอำนวยความสะดวกตามสมควร

หมวด ๖
ความรับผิดทางแพ่ง

มาตรา ๔๒ ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อของผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

(๑) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

(๒) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามอำนาจหน้าที่ตามกฎหมาย

(๓) เป็นการปฏิบัติครบถ้วนตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการประกาศกำหนดตามมาตรา ๓๑

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

หมวด ๗
บทกำหนดโทษ

มาตรา ๔๓ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๒๐ มาตรา ๒๖ วรรคสี่ มาตรา ๓๐ หรือมาตรา ๓๒ วรรคห้า หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา ๑๗ วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา ๑๗ วรรคห้า ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๔๔ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา ๑๘ มาตรา ๑๙ มาตรา ๒๑ มาตรา ๒๒ มาตรา ๒๔ วรรคหนึ่งหรือวรรคสอง มาตรา ๒๕ หรือมาตรา ๒๙ หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือผู้ใดฝ่าฝืนมาตรา ๓๒ วรรคเจ็ด ต้องระวางโทษปรับไม่เกินสามแสนบาท

การกระทำตามความในวรรคหนึ่ง หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือเพื่อให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๕ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา ๒๓ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

การกระทำตามความในวรรคหนึ่ง หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองล้านบาท หรือทั้งจำทั้งปรับ

การฝ่าฝืนตามมาตรา ๒๔ วรรคหนึ่งหรือวรรคสอง หรือมาตรา ๒๕ เกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา ๒๓ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

การฝ่าฝืนตามวรรคสาม หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองล้านบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๖ ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา ๔๐ หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา ๔๑ วรรคสาม ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๔๗ ผู้ใดต่อสู้หรือขัดขวางพนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๘ ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผยในกรณีดังต่อไปนี้

(๑) การเปิดเผยตามหน้าที่

(๒) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(๓) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

(๔) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

(๕) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

มาตรา ๔๙ บรรดาความผิดตามพระราชบัญญัตินี้ ให้คณะกรรมการมีอำนาจเปรียบเทียบได้ และคณะกรรมการอาจมอบอำนาจให้คณะอนุกรรมการใช้อำนาจดังกล่าวด้วยก็ได้

เมื่อผู้กระทำความผิดได้เสียค่าปรับตามที่เปรียบเทียบแล้ว ให้ถือว่าคดีเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา

บทเฉพาะกาล

มาตรา ๕๐ ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วยกรรมการตามมาตรา ๗ (๒) และกรรมการตามวรรคสองเพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อนแต่ไม่เกินเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ และให้กรรมการดังกล่าวเลือกกรรมการคนหนึ่งทำหน้าที่ประธานกรรมการเป็นการชั่วคราว

ให้สำนักงานดำเนินการให้มีการแต่งตั้งประธานกรรมการตามมาตรา ๗ (๑) และกรรมการผู้ทรงคุณวุฒิตามมาตรา ๗ (๓) ภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

มาตรา ๕๑ ในวาระเริ่มแรกที่ยังไม่มีเลขาธิการตามพระราชบัญญัตินี้ ให้ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ปฏิบัติหน้าที่เลขาธิการตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีเลขาธิการตามพระราชบัญญัตินี้

ในกรณีที่ยังไม่มีผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามวรรคหนึ่ง ให้ผู้ดำรงตำแหน่งผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. ๒๕๕๔ ปฏิบัติหน้าที่ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และเลขาธิการตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์หรือเลขาธิการตามพระราชบัญญัตินี้ แล้วแต่กรณี

มาตรา ๕๒ ในวาระเริ่มแรกที่ยังไม่มีสำนักงานตามพระราชบัญญัตินี้ ให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ปฏิบัติหน้าที่สำนักงานตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีสำนักงานตามพระราชบัญญัตินี้

มาตรา ๕๓ ผู้ใดเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้อยู่ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ กฎกระทรวง หรือประกาศที่ออกตามพระราชบัญญัตินี้ เว้นแต่การปฏิบัติตามมาตรา ๒๙ (๑) ให้ปฏิบัติตามบทบัญญัติดังกล่าวภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

ผู้รับสนองพระบรมราชโองการ

.....

นายกรัฐมนตรี

ภาคผนวก ง

สัญญาแม่แบบตามคำวินิจฉัยของคณะกรรมาธิการยุโรปที่ 2001/497

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision 2001/497/EC

Standard contractual clauses for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to third countries which do not ensure an adequate level of protection (controller to controller transfers)

Name of the data exporting organisation:
.....

.....

Address:

.....

Tel..... fax..... e-mail:

.....

Other information needed to identify the

organisation:

.....

('the data **exporter')**

and

Name of the data exporting organisation:
.....

.....

Address:

.....

Tel..... fax..... e-mail:

.....

Other information needed to identify the

organisation:

.....

('the data **importer')**

HAVE AGREED on the following contractual clauses ('the Clauses') in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1:

Clause 1

Definitions

For the purposes of the Clauses:

a) **'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'** and **'supervisory authority** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('hereinafter the Directive');

b) the **'data exporter'** shall mean the controller who transfers the personal data;

c) the **'data importer** shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection.

Clause 2

Details of the transfer

The details of the transfer, and in particular the categories of personal data and the purposes for which they are transferred, are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

The data subjects can enforce this Clause, Clause 4(b), (c) and (d). Clause 5(a), (b), (c) and (e), Clause 6(1) and (2), and Clauses 7, 9 and 11 as third-party beneficaries. The parties do not object to the data subjects being represented by an association or other bodies if they so wish and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data by him has been and, up to the moment of the transfer, will continue to be carried out in accordance with the relevant provisions of the Member State in which the data exporter is established (and where applicable has been notified to the relevant authorities of that State) and does not violate the relevant provisions ofthat State;

(b) that if the transfer involves special categories of data the data subject has been informed or will be informed before the transfer that this data could be transmitted to a third country not providing adequate protection;

(c) to make available to the data subjects upon request a copy of the Clauses; and

(d) to respond in a reasonable time and to the extent reasonably possible to enquries from the supervisory authority on the

processing of the relevant personal data by the data importer and to any enquiries from the data subject concerning the processing of this personal data by the data importer.

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) that he has no reason to believe that the legislation applicable to him prevents him from fulfilling his obligations under the contract and that in the event of a change in that legislation which is likely to have a substantial adverse effect on the guarantees provided by the Clauses, he will notify the change to the data exporter and to the supervisory authority where the data exporter is established, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) to process the personal data in accordance with the mandatory data protection principles set out in Appendix 2;
or, if explicitly agreed by the parties by ticking below and subject to compliance with the mandatory data protection principles set out in Appendix 3, to process in all other respects the data in accordance with:

— the relevant provisions of national law (attached to these Clauses) protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data applicable to a data controller in the country in which the data exporter is established, or

— the relevant provisions of any Commission Decision under Article 25(6) of Directive 95/46/EC finding that a third country provides adequate protection in certain sectors of activity only, if the data importer is based in that third country and is not covered by those provisions, in so far as those provisions are of a nature which makes them applicable in the sector of the transfer;

(c) to deal promptly and properly with all reasonable inquiries from the data exporter or the data subject relating to his processing of the personal data subject to the transfer and to cooperate with the competent supervisory authority in the course of all its inquries and abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(d) at the request of the data exporter to submit its data processing facilities for audit which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(e) to make available to the data subject upon request a copy of the Clauses and indicate the office which handles complaints.

Clause 6

Liability

1. The parties agree that a data subject who has suffered damage as a result of any violation of the provisions referred to in Clause 3 is entitled to receive compensation from the parties for the damage suffered. The parties agree that they may be exempted from this liability only if they prove that neither of them is responsible for the violation of those provisions.

2. The data exporter and the data importer agree that they will be jointly and severally liable for damage to the data subject resulting from any violation referred to in paragraph 1. In the event of such a violation, the data exporter or the data importer or both.

3. The parties agree that if one party is held liable for a violation referred to in paragraph 1 by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.[5].

Clause 7

Mediation and jurisdiction

1. The parties agree that if there is a dispute between a data subject and either party which is not amicably resolved and the data subject invokes the third-party beneficiary provision in clause 3, they accept the decision of the data subject:

   (a) to refer the dispute to mediation by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

---

5 Paragraph 3 is optional

2. The parties agree that by agreement between a data subject and the relevant party a dispute can be referred to an arbitration body, if that party is established in a country which has ratified the New York convention on enforcement of arbitration awards.

3. The parties agree that paragraphs 1 and 2 apply without prejudice to the data subject's substantiive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

The parties agree to deposit a copy of this contract with the supervisory authority ifit so requests or if such deposit is required under national law.

Clause 9
Termination of the Clauses

The parties agree that the termination of the Clauses at any time, in any circumstances and for whatever reason does not exempt them from the obligations and/or conditions under the Clauses as regards the processing of the data transferred.

Clause 10
Governing Law

The Clauses shall be governed by the law of the Member State in which the Data Exporter is established,

namely

.....

.....

Clause 11
Variation of the contract

The parties undertake not to vary or modify the terms of the clauses.

On behalf of the data exporter:

Name (written out in full):

.....

Position:

.....

Address:

.....

Other information necessary in order for the contract to be binding (if any):

.....

.....

.....

(signature)

(stamp of organisation)

On behalf of the data importer

Name (written out in full):

.....

Position:

.....

Address:

.....

Other information necessary in order for the contract to be binding (if any):

.....

.....

.....

(signature)

(stamp of organisation)

Appendix 1
to the standard contractual clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

(The Member States may complete or specify, according to their national procedures, any additional necessaiy information to be contained in this Appendix.)

Data *exporter*

The data exporter is (please specify briefly your activities relevant to the transfer):

.....
.....
.....

Data *importer*

The data importer is (please specify briefly your activities relevant to the transfer):

.....
.....
.....

Data *subjects*

The personal data transferred concern the following categories of data subjects (please specify):

.....
.....
.....

Purposes of the transfer

The transfer is necessary for the following purposes (please specify):

.....
.....
.....

Categories of data

The personal data transferred fall within the following categories of data (please specify):

.....
.....
.....

Sensitive *data* (if appropriate)

The personal data transferred fall within the following categories of sensitive data (please specify):

.....
.....
.....

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients (please specify):

.....
.....
.....

Storage limit

The personal data transferred may be stored for no more than (please indicate): .....
(months/years)

Data exporter	Data importer
Name:	Name:
.....	
.....	
.....	
(Authorised signature)	(Authorised signature)

Appendix 2
to the standard contractual clauses
Mandatory data protection principles referred to in the first paragraph of Clause 5(b)

These data protection principles should be read and interpreted in the light of the provisions (principles and relevant exceptions) of Directive 95/46/EC.

They shall apply subject to the mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others.

1. *Purpose limitation:* data must be processed and subsequently used or further communicated only for the specific purposes in Appendix I to the Clauses. Data must not be kept longer than necessary for the purposes for which they are transferred.

2. Dara *quality and proportionality:* data must be accurate and, where necessary, kept up to date. The data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. *Transparency:* data subjects must be provided with information as to the purposes of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fair processing, unless such information has already been given by the data exporter.

4. *Security and confidentiality:* technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as unauthorised access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the controller.

5. *Rights of access, rectification, erasure and blocking of data:* as provided for in Article 12 of Directive 95/46/EC, the data subject must have a right of access to all data relating to him that are processed and, as appropriate, the right to the rectification, erasure or blocking of data the processing of which does not comply with the principles set out in this Appendix, in particular because the data are incomplete or inaccurate. He should also be able to object to the processing of the data relating to him on compelling legitimate grounds relating to his particular situation.

6. *Restrictions on onwards transfers:* further transfers of personal data from the data importer to another controller established in a third country not providing adequate protection or not covered by a decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46/EC (onward transfer) may take place only if either:

(a) data subjects have, in the case of special categories of data, given their unambiguous consent to the onward transfer or, in other cases, have been given the opportunity to object.

The minimum information to be provided to data subjects must contain in a language understandable to them:

— the purposes of the onward transfer,

— the identification of the data exporter established in the Community,

— the categories of further recipients of the data and the countries of destination, and

— an explanation that, after the onward transfer, the data may be processed by a controller established in a country where there is not an adequate level of protection of the privacy of individuals; or

(b) the data exporter and the data importer agree to the adherence to the Clauses of another controller which thereby becomes a party to the Clauses and assumes the same obligations as the data importer.

7. *Special categories of data:* where data revealing racial or ehtnic origin, political opinions, religious or philosophical beliefe or trade union memberships and data concerning health or sex life and data relating to offences, criminal convictions or security measures are processed, additional safeguards should be in place within the meaning of Directive 95/46/EC, in particular, appropriate security measures such as strong encryption for transmission or such as keeping a record of access to sensitive data.

8. *Direct marketing:* where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to 'opt-out' from having his data used for such purposes.

9. *Automated individual decisions:* data subjects are entitled not to be subject to a decision which is based soley on automated processing of data, unless other measures are taken to safeguard the individual's legitimate interests as provided for in Article 15(2) of Directive 95/46/EC. Where the purpose of the transfer is the taking of an automated decision as referred to in Article 15 of Directive 95/46/EC, which produces legal effects concerning the individual or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc., the individual should have the right to know the reasoning for this decision.

Appendix 3
to the standard contractual clauses
Mandatory data protection principles referred to in the second paragraph of Clause 5(b)

1. Purpose *limitation:* data must be processed and subsequently used or further communicated only for the specific purposes in Appendix I to the Clauses. Data must not be kept longer than necessary for the purposes for which they are transferred.

2. *Rights of access, rectification, erasure and blocking of data:* as provided for in Article 12 of Directive 95/46/EC, the data subject must have a right of access to all data relating to him that are processed and, as appropriate, the right to the rectification, erasure or blocking of data the processing of which does not comply with the principles set out in this Appendix, in particular because the data is incomplete or inaccurate. He should also be able to object to the processing of the data relating to him on compelling legitimate grounds relating to his particular situation.

3. *Restrictions on onward transfers:* further transfers of personal data from the data importer to another controller established in a third country not providing adequate protection or not covered by a decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46/EC (onward transfer) may take place only if either:

(a) data subjects have, in the case of special categories of data, given their unambiguous consent to the onward transfer, or, in other cases, have been given the opportunity to object.

The minimum information to be provided to data subjects must contain in a language understandable to them:

— the purposes of the onward transfer,
— the identification of the data exporter established in the Community,
— the categories of further recipients of the data and the countries of destination, and
— an explanation that, after the onward transfer, the data may be processed by a controller established in a country where there is not an adequate level of protection of the privacy of indidividuals; or

(b) the data exporter and the data importer agree to the adherence to the Clauses of another controller which thereby becomes a party to the Clauses and assumes the same obligations as the data importer.

ประวัติผู้เขียน

ชื่อ	นางสาววรรณรัชชา ทรัพย์รดาพัดชา
วันเดือนปีเกิด	9 มกราคม 2533
วุฒิการศึกษา	ปีการศึกษา 2554: นิติศาสตรบัณฑิต (เกียรตินิยมอันดับ 2) มหาวิทยาลัยธรรมศาสตร์